Volume 1

Introducing the Alcatel OmniAccess System

AOS-W User Guide

Version 2.5.3

ALCATEL

Copyright

Specifications in this manual are subject to change without notice.

Originated in the USA.

Trademarks

AOS-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 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

This preface includes the following information:

- An overview of the contents of 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

The *AOS-W User Guide* is now in eight separate volumes for easier download and information access. The volumes are as follows:

- Volume 1 (this volume) contains an overview of the OmniAccess System.
- Volume 2 describes how to install the OmniAccess System in a wired network.
- Volume 3 describes WLAN configuration, including remote Access Points.
- Volume 4 describes wireless encryption and authentication configuration.
- Volume 5 describes configuring multi-WLAN switch environments.
- Volume 6 describes intrusion prevention configuration.
- Volume 7 describes managing the OmniAccess System.
- Volume 8 describes configuring advanced services, such as Quality of Service (QoS) for voice and the External Services Interface module.

Related Documents

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

- *AOS-W User Guide*
- *Alcatel Wireless LAN Switch Installation Guides*
- *Alcatel Access Point Installation Guides*
- *Release Notes*

Text Conventions

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

TABLE 1 Text Conventions

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>	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: # **send** *<text message>* 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 | Item B }	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Contacting Alcatel

Contact Center Online		
■	Main Site	http://www.alcatel.com/enterprise
■	Support Site	http://eservice.ind.alcatel.com
■	Email	support@ind.alcatel.com
Sales & Support Contact Center Telephone		
■	North America	1-800-995-2696
■	Latin America	1-877-919-9526
■	Europe	+33 (0) 38 85 56 92 9
■	Asia Pacific	+65 6586 1555
■	Worldwide	1-818-880-3500

Overview of the Alcatel OmniAccess System

1

Wireless local area networks (WLANs) allow users of personal computers with wireless network interface adapters to communicate with each other and connect to existing wired networks. The Alcatel OmniAccess system allows you to implement WLANs in enterprise environments with lower cost of deployment, simplified management, and multiple layers of security.

This chapter describes the components and features of the Alcatel OmniAccess system, in the following topics:

- "Alcatel OmniAccess System Components" on page 2
- "Basic WLAN Configuration" on page 11
- "Wireless Client Access to the WLAN" on page 18
- "Configuring and Managing the Alcatel OmniAccess System" on page 21

Alcatel OmniAccess System Components

The Alcatel OmniAccess system consists of the following components:

- "Alcatel Access Points"
- "Alcatel WLAN Switches"
- "AOS-W"
- "Alcatel Mobility Manager"

The following sections describe each of these components.

Alcatel Access Points

Alcatel Access Points (APs) operate exclusively with Alcatel WLAN Switches to provide network access for wireless clients. Alcatel APs support Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g standards for wireless systems.

NOTE: Alcatel offers a range of APs that support various antenna types and radio specifications. Refer to the *Installation Guides* for your Alcatel AP for specific information about supported features.

An AP broadcasts its configured *service set identifier* (SSID), which corresponds to a specific *wireless local area network* (WLAN). Wireless clients discover APs by listening for broadcast beacons or by sending active probes to search for APs with a specific SSID.

You can connect an Alcatel AP to an Alcatel WLAN Switch either directly with an Ethernet cable or remotely through an IP network. Figure 1-1 shows two Alcatel APs connected to an Alcatel WLAN Switch. One AP is connected to a switch in the wiring closet that is connected to a router in the data center where the WLAN Switch is located. The Ethernet port on the other AP is cabled directly to a port on the WLAN Switch.

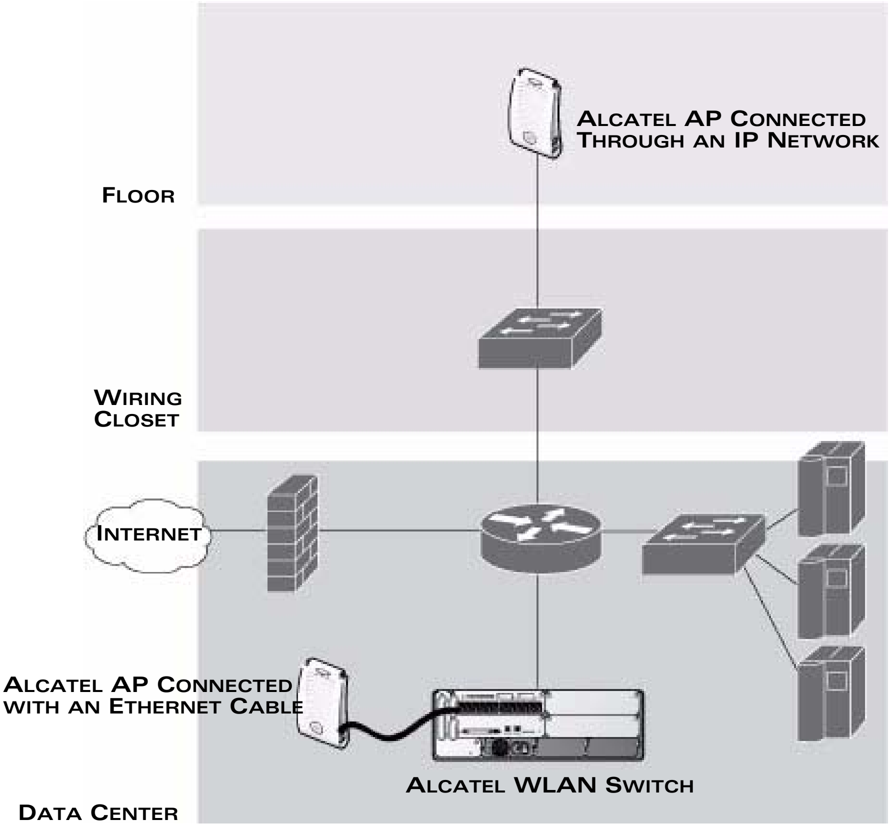


FIGURE 1-1 Connecting APs to the Alcatel WLAN Switch

Alcatel APs are *thin* APs, which means their primary function is to receive and transmit electromagnetic signals; other WLAN processing is left to the WLAN Switch. When powered on, an Alcatel AP locates its host WLAN Switch through a variety of methods, including the Alcatel Discovery Protocol (ADP), Domain Name Service (DNS), or Dynamic Host Configuration Protocol (DHCP). When an Alcatel AP locates its host WLAN Switch, it automatically builds a secure Generic Routing Encapsulation (GRE) tunnel (Figure 1-2) to the WLAN Switch. The AP then downloads its software and configuration from the WLAN Switch through the tunnel.

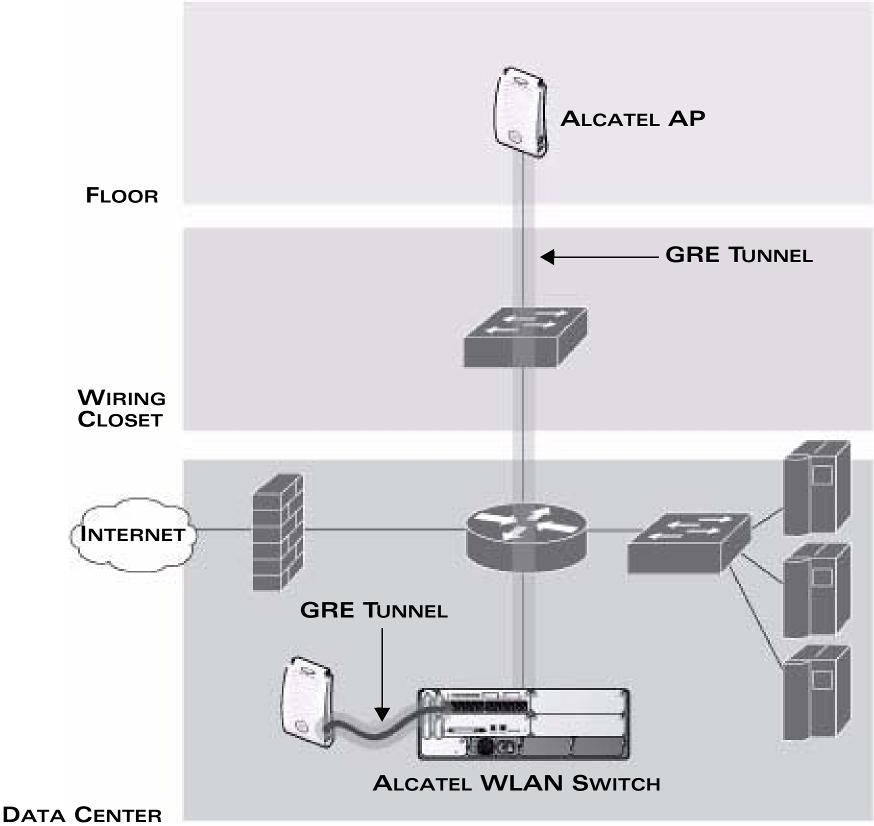


FIGURE 1-2 Alcatel APs Establish GRE Tunnels to the WLAN Switch

Client traffic received by the AP is immediately sent through the tunnel to the host WLAN Switch (Figure 1-3), which performs packet processing such as encryption and decryption, authentication, and policy enforcement.

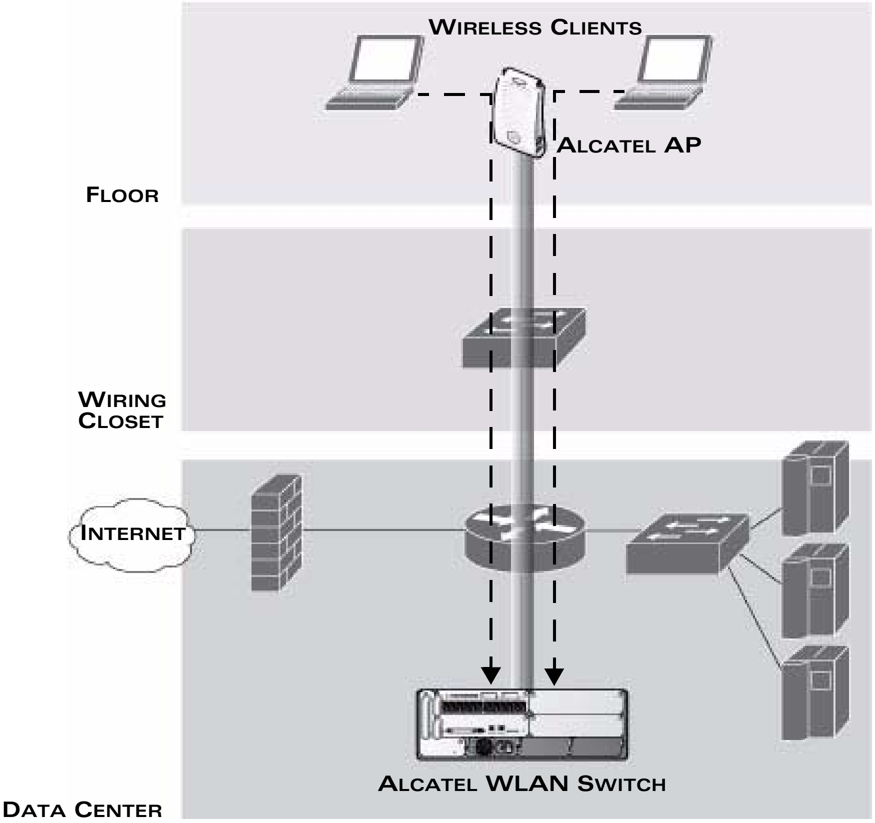


FIGURE 1-3 Client Traffic is Tunneled to the WLAN Switch

Automatic RF Channel and Power Settings

Adaptive Radio Management (ARM) is a radio frequency (RF) resource allocation algorithm that you can enable and configure in the Alcatel Mobility Edge system. When ARM is enabled, each Alcatel AP can determine the optimum channel selection and transmit power setting to minimize interference and maximize coverage and throughput. The APs scan for better channels at periodic intervals and report information to the WLAN Switch. The WLAN Switch analyzes reports from all APs and coordinates changes, resulting in a higher performing RF environment.

If an AP fails for any reason, the Alcatel OmniAccess system's *self-healing* mechanism automatically ensures coverage for wireless users. The WLAN Switch detects the failed AP and instructs neighboring APs to increase power levels to compensate.

You can also enable the system to detect *coverage holes*, or areas where a good RF signal is not adequately reaching wireless clients.

RF Monitoring

An Alcatel AP can function as either a dedicated or shared *Air Monitor* (AM) to monitor radio frequency (RF) spectrums to detect intrusions, denial of service (DoS) attacks, and other vulnerabilities. A *dedicated* AM performs monitoring functions exclusively and does not service wireless clients or advertise SSIDs. A *shared* AM performs monitoring functions in addition to servicing wireless clients.

Every AP automatically monitors the channel on which it services wireless clients. You can configure the AP to perform off-channel scanning, where the AP spends brief time intervals scanning other channels. However, the more clients an AP services, the less time it has to perform off-channel scanning. If air monitoring functions are critical to your network, Alcatel recommends that a few APs be designated as dedicated AMs.

For example, you can configure dedicated AMs to perform the following functions:

- Detect, locate, and disable rogue APs (APs that are not authorized or sanctioned by network administrators)
- Detect and disable ad-hoc networks
- Detect and disable honeypot APs
- Detect wireless bridges
- Capture remote packets

If air monitoring functions are only needed periodically, you can configure APs to operate temporarily as AMs. You can also configure dedicated AMs to automatically convert into APs if there is an AP failure or when there is high level of traffic on the network.

Alcatel WLAN Switches

All Alcatel APs are connected either directly or remotely through an IP network to an Alcatel WLAN Switch. The WLAN Switch is an enterprise-class switch that bridges wireless client traffic to and from traditional wired networks and performs high-speed Layer-2 or Layer-3 packet forwarding between Ethernet ports. While Alcatel APs provide radio services only, the WLAN Switch performs upper-layer media access control (MAC) processing, such as encryption and authentication, as well as centralized configuration and management of SSIDs and RF characteristics for Alcatel APs. This allows you to deploy APs with little or no physical change to an existing wired infrastructure.

WLAN Switches provide 10/100 Mbps Fast Ethernet, IEEE 802.3af-compliant ports that can provide Power over Ethernet (PoE) to directly-connected APs. When you connect a PoE-capable port on the WLAN Switch to a PoE-compatible device such as an Alcatel AP, the port automatically detects the device and provides operating power through the connected Ethernet cable. This allows APs to be installed in areas where electrical outlets are unavailable, undesirable, or not permitted, such as in the plenum or in air handling spaces.

NOTE: Alcatel offers a range of WLAN Switches that provide different port types and traffic capacities. Refer to the *Installation Guide* for your Alcatel WLAN Switch for specific information about supported features.

In an Alcatel OmniAccess system, at least one WLAN Switch is the *master* WLAN Switch while non-master WLAN Switches are referred to as *local* WLAN Switches (Figure 1-4). A master WLAN Switch offers a single point of configuration which is automatically replicated from the master to local WLAN Switches throughout the network.

Local WLAN Switches offer local points of traffic aggregation and management for Alcatel APs and services. A local WLAN Switch can perform any supported function (for example, WLAN management, policy enforcement, VPN services, and so on), however these services are always configured on the master WLAN Switch and are “pushed” to specified local WLAN Switches.

An Alcatel AP obtains its software image and configuration from a master WLAN Switch; it can also be instructed by a master WLAN Switch to obtain its software from a local WLAN Switch.

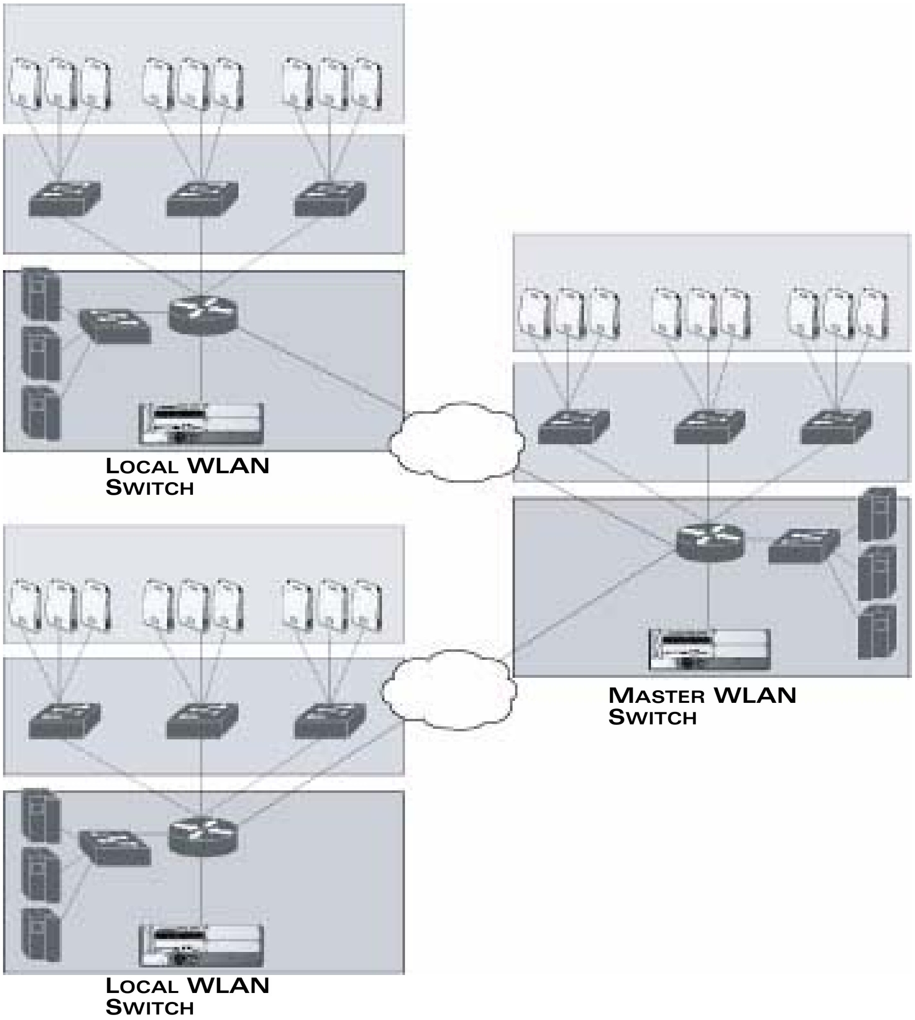


FIGURE 1-4 Master and Local WLAN Switches

A typical OmniAccess system includes one master WLAN Switch, one or more *backup* master WLAN Switches and any number of local WLAN Switches. It is important to note that master WLAN Switches do not share information with each other. Thus, APs that share roaming tables, security policies, and other configurations should be managed by the same master WLAN Switch.

AOS-W

AOS-W is a suite of mobility applications that runs on all Alcatel WLAN Switches and allows you to configure and manage the wireless and mobile user environment.

AOS-W consists of a base software package with optional software modules that you can activate by installing the appropriate license key (Table 1-1). The base AOS-W software includes the following functions:

- Centralized configuration and management of APs
- Wireless client authentication to an external authentication server or to the WLAN Switch's local database
- Encryption
- Mobility with fast roaming
- RF management and analysis tools

TABLE 1-1 Optional Software Modules

Optional Software Module	Description
Policy Enforcement Firewall	Provides identity-based security for wired and wireless users. Stateful firewall enables user classification based on user identity, device type, location, and time of day, and provides differentiated access for different classes of users.
Wireless Intrusion Protection	Detects, classifies and limits designated wireless security threats such as rogue APs, DoS attacks, malicious wireless attacks, impersonations, and unauthorized intrusions. Eliminates need for separate system of RF sensors and security appliances.
VPN Server	Enables WLAN Switches to provide Virtual Private Networks (VPN) tunnel termination to local and remote users. Provides site-to-site VPN tunnels between Alcatel WLAN Switches and third-party VPN concentrators.

TABLE 1-1 Optional Software Modules

Optional Software Module	Description
Remote AP	Allows an Alcatel AP to be securely connected from a remote location to a WLAN Switch across the Internet. Allows the remote AP to be plugged directly into an Internet-connected DSL router; a WLAN Switch does not need to be installed at the remote location. There are three Remote AP licenses available that allow the WLAN Switch to support a maximum of 6, 128, or 256 Remote APs.
xSec	Enables support for xSec, a Federal Information Processing Standard (FIPS)-certifiable Layer-2 encryption protocol.
Client Integrity	Enables wireless and wired client remediation services before network access is granted. Integrates Sygate Technologies Sygate On-Demand Agent (SODA).
External Services Interface (ESI)	Supports automatic redirect of users to authentication servers based on a fully-qualified domain name or realm and policy-based redirect of wireless and wired traffic to external devices that provide inline network services such as anti-virus, intrusion detection system (IDS), and content filtering.

Each optional module has a software license (either permanent or evaluation) that you must install on an Alcatel WLAN Switch as a software license key. Contact your sales account manager or authorized reseller to obtain software licenses.

NOTE: After installing a software license key, you must reboot the Alcatel WLAN Switch for the new feature to become available.

Basic WLAN Configuration

You have a wide variety of options for authentication, encryption, access management, and user rights when you configure a WLAN in the Alcatel OmniAccess system. However, you *must* configure the following basic elements:

- An SSID that uniquely identifies the WLAN
- Layer-2 authentication to protect against unauthorized access to the WLAN
- Layer-2 encryption to ensure the privacy and confidentiality of the data transmitted to and from the network
- A user role and virtual local area network (VLAN) for the authenticated client

This section describes authentication, encryption, VLAN, and user role configuration in the Alcatel OmniAccess system.

Authentication

A user must authenticate to the Alcatel OmniAccess system in order to access WLAN resources. There are several types of Layer-2 security mechanisms allowed by the IEEE 802.11 standard that you can employ in the OmniAccess system, including those that require an external RADIUS authentication server:

None (Also called open system authentication) This is the default authentication protocol. The client's identity, in the form of the Media Access Control (MAC) address of the wireless adapter in the wireless client, is passed to the WLAN Switch. Essentially any client requesting access to the WLAN is authenticated.

IEEE 802.1x

The IEEE 802.1x authentication standard allows for the use of keys that are dynamically generated on a per-user basic (as opposed to a static key that is the same on all devices in the network).

NOTE: The 802.1x standard requires the use of a RADIUS authentication server. Most Lightweight Directory Access Protocol (LDAP) servers do *not* support 802.1x.

With 802.1x authentication, a *supplicant* is the wireless client that wants to gain access to the network and the device that communicates with both the supplicant and the authentication server is the *authenticator*. In the Alcatel OmniAccess system, the WLAN Switch is the 802.1x authenticator, relaying authentication requests between the authentication server and the supplicant.

NOTE: During the authentication process, the supplicant (the wireless client) and the RADIUS authentication server negotiate the type of Extensible Authentication Protocol (EAP) they will use for the authentication transaction. The EAP type is completely transparent to the WLAN Switch and has no impact on its configuration.

Wi-Fi Protected Access (WPA)

WPA implements most of the IEEE 802.11i standard. It is designed for use with an 802.1x authentication server (the Wi-Fi Alliance refers to this mode as WPA-Enterprise). WPA uses the Temporal Key Integrity Protocol (TKIP) to dynamically change keys and RC4 stream cipher to encrypt data.

WPA in pre-shared key (PSK) mode (WPA-PSK)

With WPA-PSK, all clients use the same key (the Wi-Fi Alliance refers to this mode as WPA-Personal).

NOTE: In PSK mode, users must enter a passphrase from 8-63 characters to access the network. PSK is intended for home and small office networks where operating an 802.1x authentication server is not practical.

WPA2

WPA2 implements the full IEEE 802.11i standard. In addition to WPA features, WPA2 provides Counter Mode with Cipher Blocking Chaining Message Authentication Code Protocol (CCMP) for encryption which uses the Advanced Encryption Standard (AES) algorithm. (The Wi-Fi Alliance refers to this mode as WPA2-Enterprise.)

WPA2-PSK

WPA2-PSK is WPA2 used in PSK mode, where all clients use the same key. (The Wi-Fi Alliance refers to this mode as WPA2-Personal.)

Encryption

The Layer-2 encryption option you can select depends upon the authentication method chosen (Table 1-2).

TABLE 1-2 Encryption Options by Authentication Method

Authentication Method	Encryption Option
None	Null or Static WEP
802.1x	Dynamic WEP
WPA or WPA-PSK only	TKIP
WPA2 or WPA2-PSK only	AES
Combination of WPA or WPA-PSK and WPA2 or WPA2-PSK	Mixed TKIP/AES

You can configure the following data encryption options for the WLAN:

Null

Null means that no encryption is used and packets passing between the wireless client and WLAN Switch are in clear text.

Wired Equivalent Protocol (WEP)

Defined by the original IEEE 802.11 standard, WEP uses the RC4 stream cipher with 40-bit and 128-bit encryption keys. The management and distribution of WEP keys is performed outside of the 802.11 protocol. There are two forms of WEP keys:

- Static WEP requires you to manually enter the key for each client and on the WLAN Switch.
- Dynamic WEP allows the keys to be automatically derived for each client for a specific authentication method during the authentication process. Dynamic WEP requires 802.1x authentication.

Temporal Key Integrity Protocol (TKIP)

TKIP ensures that the encryption key is changed for every data packet. You specify TKIP encryption for WPA and WPA-PSK authentication.

Advanced Encryption Standard (AES)

AES is an encryption cipher that uses the Counter-mode CBC-MAC (Cipher Block Chaining-Message Authentication Code) Protocol (CCMP) mandated by the IEEE 802.11i standard. AES-CCMP is specifically designed for IEEE 802.11 encryption and encrypts parts of the 802.11 MAC headers as well as the data payload. You can specify AES-CCMP encryption with WPA2 or WPA2-PSK authentication.

Mixed TKIP/AES-CCM

This option allows the WLAN Switch to use TKIP encryption with WPA or WPA-PSK clients and use AES encryption with WPA2 or WPA2-PSK clients. This option allows you to deploy the Alcatel OmniAccess system in environments that contain existing WLANs that use different authentication and encryption.

xSec (Extreme Security)

xSec is a Federal Information Processing Standard (FIPS)-certifiable Layer-2 encryption. xSec can encrypt and tunnel Layer-2 traffic between a WLAN Switch and wired and wireless clients, or between two Alcatel WLAN Switches. To use xSec encryption:

- You must use 802.1x authentication, which means that you must use a RADIUS authentication server.
- You must install the AOS-W xSec license in the Alcatel WLAN Switch. If you are using xSec between two Alcatel WLAN Switches, you must install a license in each device.
- For encryption and tunneling of data between the client and WLAN Switch, you must install the Funk Odyssey client that supports xSec in the wired or wireless client.

VLAN

Each authenticated user is placed into a VLAN, which determines the user’s DHCP server, IP address, and Layer-2 connection. While you could place all authenticated wireless users into a single VLAN, the Alcatel OmniAccess system allows you to group wireless users into separate VLANs. This enables you to differentiate groups of wireless users and their access to network resources. For example, you can place authorized employee users into one VLAN and itinerant users, such as contractors or guests, into a separate VLAN.

NOTE: You create the VLANs for wireless users *only* on the WLAN Switch. You do not need to create the VLANs anywhere else on your network. Because wireless clients are tunneled to the WLAN Switch (see Figure 1-3 on page 5) to the rest of the network it appears as if the clients were directly connected to the WLAN Switch.

For example, in the topology shown in Figure 1-5, authenticated wireless users are placed on VLAN 20. You configure VLAN 20 *only* on the WLAN Switch; you do not need to configure VLAN 20 on any other device in the network.

NOTE: To allow data to be routed to VLAN 20, you need to configure a static route to VLAN 20 on an upstream router in the wired network.

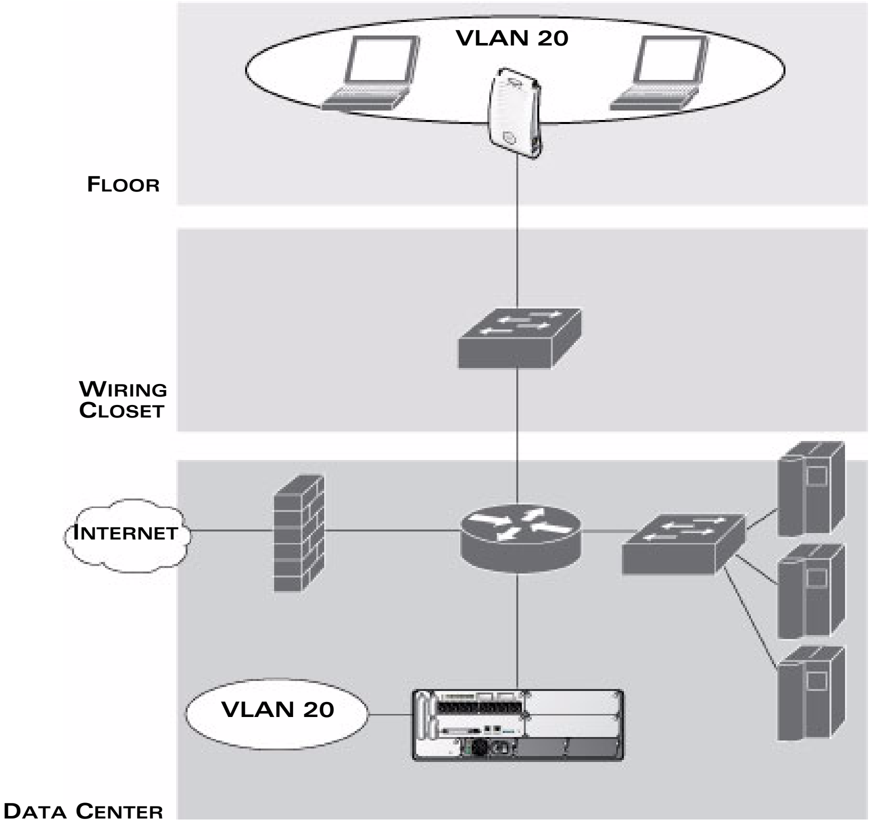


FIGURE 1-5 VLANs for Wireless Users Configured on WLAN Switch

A user is assigned to a VLAN by one of several methods. There is an order of precedence by which VLANs are assigned. The assignment of VLANs are (from lowest to highest precedence):

1. The VLAN is configured for the AP location.
2. The VLAN is derived from rules based on user attributes (SSID, BSSID, user MAC, location, and encryption type). Within the set of possible user-derivation rules, a rule that derives a specific VLAN takes precedence over a rule that derives a user role that may have a VLAN configured for it.
3. The VLAN is configured for a default role for an authentication method, such as 802.1x or VPN.
4. The VLAN is derived from attributes returned by the authentication server (*server-derived rule*). Within a set of server-derived rules, a rule that derives a specific VLAN takes precedence over a rule that derives a user role that may have a VLAN configured for it.

5. The VLAN is derived from Microsoft Tunnel attributes (Tunnel-Type, Tunnel Medium Type, and Tunnel Private Group ID). All three attributes must be present. This does not require any server-derived rule.
6. The VLAN is derived from Vendor Specific Attributes (VSA) for RADIUS server authentication. This does not require any server-derived rule.

   NOTE: If a VSA is present, it overrides any previous VLAN assignment.

User Role

Every user in an Alcatel OmniAccess system is associated with a *user role*, which determines what a client is allowed to do, where and when it can operate, how often it must re-authenticate, and which bandwidth contracts are applicable. User roles can be simply defined; for example, you can define an “employee” role which allows unrestricted access to all network resources at all times of the day and a “guest” role which allows only HTTP access to the Internet during regular business hours. Or you can define more granular user roles that are specific to jobs in an enterprise environment, such as “IT staff” or “payroll”.

All wireless clients start in a default user role called the *logon* role. The logon role has only enough privileges to allow the user to be authenticated. From the logon role, users can be placed into less restrictive user roles as they pass authentication.

NOTE: User roles and policies (described in the next section) require the installation of a Policy Enforcement Firewall license in the WLAN Switch. See Table 1-1 on page 9 for descriptions of optional AOS-W software licenses.

Policies and User Roles

In an Alcatel OmniAccess system, a *policy* identifies a set of rules that applies to traffic that passes through the WLAN Switch. A policy can consist of firewall rules that permit or deny traffic, quality of service (QoS) actions such as setting a data packet to high priority, or an administrative actions such as logging.

Whenever you create a user role, you specify one or more policies for the role. You can apply policies to users to give different treatment to users on the same network. The following example shows policies that might be applied for the user roles “Employee” and “Guest”:

“Employee” User Role Policy:	“Guest” User Role Policy:
“Permit all traffic from any source to any destination”	“Permit DHCP traffic from the user to corporate DHCP server during business hours” “Permit DNS traffic from the user to a public DNS server during business hours” “Permit HTTP traffic from the user to any destination during business hours” “Permit HTTPS traffic from the user to any destination during business hours” “Drop all traffic from the user to the Internal Corporate network”

NOTE: In the examples shown above, all users should be securely authenticated before network access is granted.

Assignment of User Roles

A user is assigned a user role by one of several methods. There is an order of precedence by which user roles are assigned. That is, a user role assigned by one method may take precedence over a user role assigned by a different method. The methods of assigning user roles are (from lowest to highest precedence):

1. The default *logon* user role.
2. The user role is derived from user attributes upon the client’s association with an AP (also known as a *user-derived* role). You can configure rules that assign a user role to users who match a certain set of criteria. For example, you can use any of the following values to derive a user role:
   - Basic Service Set Identifier (BSSID) of the AP to which a client is associated
   - Encryption type used by the client
   - Extended Service Set Identifier (ESSID) to which the client is associated
   - Location of the AP to which the client is associated
   - Media Access Control (MAC) address of the client
3. The user role is the default user role configured for an authentication method, such as 802.1x or VPN. Each authentication method can have a default role for users who are successfully authenticated using that method.

4. The user role is derived from Vendor Specific Attributes (VSA) for RADIUS server authentication. A role derived from a VSA takes precedence over any other user roles, including a server-derived role.
5. The user role is derived from attributes returned by the authentication server (also known as a *server-derived* role). If the user is authenticated via an authentication server, the user role for the user can be based on one or more attributes returned by the server during authentication.

Wireless Client Access to the WLAN

Wireless clients communicate with the wired network and other wireless clients through a WLAN in an Alcatel OmniAccess system. There are two phases to the process by which a wireless client gains access to a WLAN in an Alcatel OmniAccess system:

1. Association of the radio network interface card (NIC) in the PC with an AP, as described by the IEEE 802.11 standard. This association allows data link (Layer-2) connectivity.
2. Authentication of the client/user before network access is allowed.

Association

APs send out beacons that contain the SSIDs of specific WLANs; the user can select the network they want to join. Wireless clients can also send out probes to locate a WLAN within range or to locate a specific SSID; APs within range of the client respond. Along with the SSID, an AP also sends out the following information:

- Data rates supported by the WLAN. Clients can determine which WLAN to associate with based on the supported data rate.
- WLAN requirements for the client. For example, clients may need to use TKIP for encrypting data transmitted on the WLAN.

The client determines which AP is best for connecting to the WLAN and attempts to associate with it. It sends an association request to become a member of the service set. During the association exchange, the client and WLAN Switch negotiate the data rate, authentication method, and other options.

NOTE: Because an Alcatel AP is a “thin” AP, all wireless traffic it receives is immediately sent through a GRE tunnel to the WLAN Switch. The WLAN Switch responds to client requests and communicates with an authentication server on behalf of the client. Therefore, the client authentication and association processes occur between the wireless client and the Alcatel WLAN Switch.

Authentication

Authentication provides a way to identify a user and provide appropriate access to the network for that user. By default, all wireless users in an Alcatel OmniAccess system start in the logon role and use an authentication method to move to an identified, authenticated role. One or more authentication methods may be used, ranging from secure authentication methods such as 802.1x, VPN, and captive portal to less secure methods such as MAC address authentication.

NOTE: User access to the network depends upon whether the Policy Enforcement Firewall license is installed in the WLAN Switch and what policies are configured. For example, if the Policy Enforcement Firewall license is *not* installed, any authenticated user can connect to the network. If the Policy Enforcement Firewall license is installed, then the policies associated with the user role that the user is given determines the network access that the user is allowed. Subsequent chapters in this manual demonstrate the configuration of user roles and policies.

802.1x Authentication

802.1x is an IEEE standard used for authenticating clients on any IEEE 802 network. It is an open authentication framework, allowing multiple authentication protocols to operate within the framework. 802.1x operates as a Layer-2 protocol. Successful 802.1x authentication must complete before any higher-layer communication with the network, such as a DHCP exchange to obtain an IP address, is allowed.

802.1x is key-generating, which means that the output of the authentication process can be used to assign dynamic per-user encryption keys. While the configuration of 802.1x authentication on the WLAN Switch is fairly simple, 802.1x can require significant work in configuring an external authentication server and wireless client devices.

VPN

VPN technology has been in use for Internet-based remote access for many years and client/server components are widely available. Generally, the VPN client is installed on mobile devices and is used to provide secure communication with a corporate network across a non-secure network such as the Internet. VPN technology operates at Layer-3, which means that an IP address is required on the client device before the VPN client can operate.

With VPN, the MAC and outer IP header information is transmitted cleartext, while inner IP header and data are encrypted. Because the IP layer is unprotected, some form of Layer-2 encryption (such as WEP) should be used on a wireless network.

Captive Portal

Captive portal allows a wireless client to authenticate using a web-based portal. Captive portals are typically used in public access wireless hotspots or for hotel in-room Internet access. After a user associates to the wireless network, their device is assigned an IP address. The user must start a web browser and pass an authentication check before access to the network is granted.

Captive portal authentication is the simplest form of authentication to use and requires no software installation or configuration on the client. The username/password exchange is encrypted using standard SSL encryption. However, portal authentication does not provide any form of encryption beyond the authentication process; to ensure privacy of user data, some form of link-layer encryption (such as WEP or WPA-PSK) should be used when sensitive data will be sent over the wireless network.

MAC Address Authentication

MAC address authentication is the process of examining the media access control (MAC) address of an associated device, comparing it to an internal or RADIUS database, and changing the user role to an authenticated state. MAC address authentication is not a secure form of authentication as the MAC address of a network interface card (NIC) can be changed in software. MAC address authentication is useful for devices that cannot support a more secure form of authentication, such as barcode scanners, voice handsets, or manufacturing instrumentation sensors.

User roles mapped to MAC address authentication should be linked to restrictive policies to permit only the minimum required communication. Whenever possible, WEP encryption should also be employed to prevent unauthorized devices from joining the network.

Client Mobility and AP Association

When a wireless client associates with an AP, it retains the association for as long as possible. Generally, a wireless client only drops the association if the number of errors in data transmission is too high or the signal strength is too weak.

When a wireless client roams from one AP to another in an Alcatel OmniAccess system, the WLAN Switch can automatically maintain the client’s authentication and state information; the client only changes the radio that it uses. Clients do not need to reauthenticate or reassociate. When a client roams between APs that are connected to the same WLAN Switch, the client maintains its original IP address and existing IP sessions.

You can also enable client mobility on all WLAN Switches in a master WLAN Switch’s hierarchy. This allows clients to roam between APs that are connected to different WLAN Switches without needing to reauthenticate or obtain a new IP address. When a client associates with an AP, the client information is sent to the master WLAN Switch. The master WLAN Switch pushes out the client information to all local WLAN Switches in its hierarchy. When a client roams to an AP connected to a different WLAN Switch, the new WLAN Switch recognizes the client and tunnels the client traffic back to the original WLAN Switch.

Configuring and Managing the Alcatel OmniAccess System

There are several interfaces that you can use to configure and manage components of the Alcatel OmniAccess system:

- The Web User Interface (WebUI) allows you to configure and manage Alcatel WLAN Switches. The WebUI is accessible through a standard Web browser from a remote management console or workstation.
- The command line interface (CLI) allows you to configure and manage Alcatel WLAN Switches. The CLI is accessible from a local console connected to the serial port on the WLAN Switch or through a Telnet or Secure Shell (SSH) session from a remote management console or workstation.

  NOTE: By default, you can only access the CLI from the serial port or from an SSH session. To use the CLI in a Telnet session, you must explicitly enable Telnet on the WLAN Switch.
- The Alcatel OmniVista Mobility Management System is a suite of applications for monitoring multiple master WLAN Switches and their related local WLAN Switches and APs. Each application provides a Web-based user interface. The Mobility Management System is available as an integrated appliance and as a software application that runs on a dedicated system. See the *Mobility Manager User Guide* for more information.

NOTE: Before you can use the management interface from a remote console or workstation you must configure the WLAN Switch with an IP address and default gateway and connect it to your network. See “Deploying a Basic System” in Volume 2 of the *AOS-W User Guide* for more information.

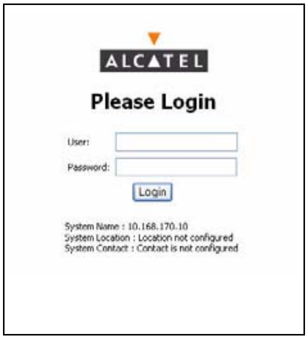
All Alcatel WLAN Switches have a serial port for connecting to a local console. The OmniAccess 6000 WLAN Switch contains a 10/100 Mbps Fast Ethernet port for out-of-band management (see the Installation Guide for your WLAN Switch for more information).

Web Access

To use the WebUI, enter the IP address of the WLAN Switch in the URL of a browser window.

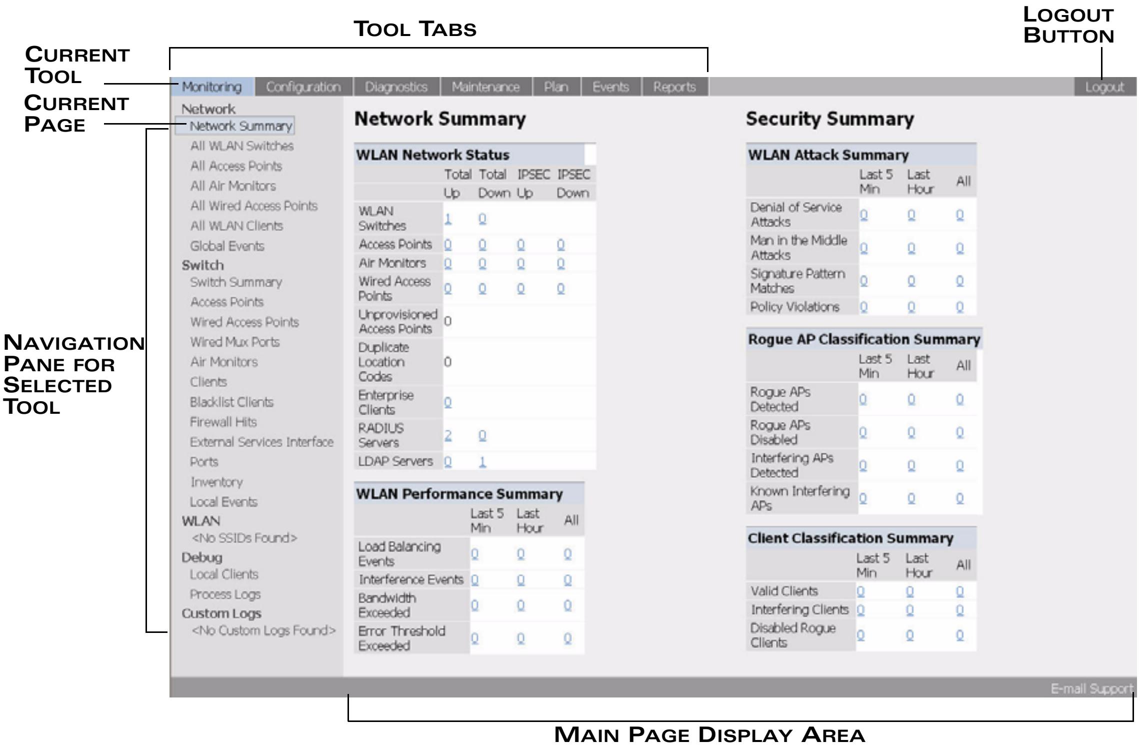
NOTE: The WebUI requires Internet Explorer 6.0 or higher. Other browsers may work but with limited functionality and are therefore not supported.

When you connect to the WLAN Switch using the WebUI, the system displays the login page. Log in using the administrator user account (the password does not display). For example:



System Name : 10.168.170.10
System Location : Location not configured
System Contact : Contact is not configured

When you are logged in, the browser window shows the default Monitor Summary page. For example:



Network Summary

WLAN Network Status

	Total Up	Total Down	IPSEC Up	IPSEC Down
WLAN Switches	1	0		
Access Points	0	0	0	0
Air Monitors	0	0	0	0
Wired Access Points	0	0	0	0
Unprovisioned Access Points	0			
Duplicate Location Codes	0			
Enterprise Clients	0			
RADIUS Servers	2	0		
LDAP Servers	0	1		

WLAN Performance Summary

	Last 5 Min	Last Hour	All
Load Balancing Events	0	0	0
Interference Events	0	0	0
Bandwidth Exceeded	0	0	0
Error Threshold Exceeded	0	0	0

Security Summary

WLAN Attack Summary

	Last 5 Min	Last Hour	All
Denial of Service Attacks	0	0	0
Man in the Middle Attacks	0	0	0
Signature Pattern Matches	0	0	0
Policy Violations	0	0	0

Rogue AP Classification Summary

	Last 5 Min	Last Hour	All
Rogue APs Detected	0	0	0
Rogue APs Disabled	0	0	0
Interfering APs Detected	0	0	0
Known Interfering APs	0	0	0

Client Classification Summary

	Last 5 Min	Last Hour	All
Valid Clients	0	0	0
Interfering Clients	0	0	0
Disabled Rogue Clients	0	0	0

The following describes the elements in all WebUI pages:

- The tabs at the top of the page allow you to select tools available in the Web UI software. Click on a tab to select the tool.
- When you select a tab, the tool and its available pages appear in the navigation pane. You can navigate to any of the listed pages by clicking on the page name.

  NOTE: Some of the items in the listed pages are merely headings for their sub-pages and cannot be selected. Selectable pages become highlighted when you place the cursor over them. Non-selectable items do not react.
- The name of the currently-selected page is highlighted in the page tree.
- The main page display area displays all the information and/or input fields relevant to the current page of the current tool.
- The Logout button at the top right corner of the page allows you to end your WebUI session.

Tools

The tool bar at the top of the WebUI browser window contains tabs for the various tools available. Click on the tab to select the tool. Table 1-3 lists the tools that are available in the WebUI.

TABLE 1-3 WebUI Tools

Menu	Description
Monitoring	This tool allows you to view the status of the Alcatel components and clients in the Alcatel OmniAccess system, the connections on the local WLAN Switch, WLANs, and custom logs.
Configuration	This tool allows you to configure the Alcatel OmniAccess system.
Diagnostics	This tool allows you to run ping and traceroute, store and view output files for technical support, and view AP configuration and statistics.
Maintenance	This tool allows you to upgrade the image file, load licenses, copy files to/from flash, configure and reboot APs, and configure the captive portal feature.
Plan	This tool enables you to design the WLAN deployment for your environment and provides coverage maps and AP and AM placement locations.
Events	This tool allows you to view events in the OmniAccess system and create event reports.
Reports	This tool allows you to view reports on APs (including rogue and interfering APs) and clients and create custom reports.

Configuration Tool

The Configuration pages are divided into two main branches: Basic pages provide a way to configure common network tasks, while the Advanced pages allow you to configure other features of the Alcatel OmniAccess system.

Table 1-4 describes the Basic Configuration pages.

TABLE 1-4 Configuration Pages (Basic)

Page	Description
WLAN	These pages allow you to configure an SSID and related WLAN options.
RF Management	These pages allow you to configure basic RF management features while assigning defaults for related options (which you can modify from the Advanced configuration pages).
Security	These pages allow you to configure various security settings including wireless intrusion detection and firewall settings. You can select from three predefined security levels—basic, medium, or high—or define a customized combination of selected options.
Network	These pages allow you to configure ports, VLANs, IP interfaces, and DHCP-related information.
Management	These pages allow you to configure the system clock, SNMP-related information, and management access.

The following buttons are available on Basic and Advanced Configuration pages:

Apply Accepts all configuration changes made on the current page.

Save Configuration (Appears in top right corner of the WebUI when the Configuration tool is selected) Saves all applied configuration changes made during the current configuration session. Saved settings are retained when the WLAN Switch is rebooted or powered off while unsaved configuration changes are lost.

Clear Resets options on current page to the last-applied or saved settings.

Add Adds a new item to the current page. Typically a set of relevant configuration fields for the item to be added is displayed.

Edit Allows you to edit the configuration of the selected item.

Delete Removes the selected item from the page configuration.

CLI Access

The CLI is available through the serial console connection or from a Telnet or SSH session.

NOTE: Telnet access is disabled by default on Alcatel WLAN Switches. To enable Telnet access, enter the **telnet cli** command from a serial connection or from an SSH session.

When you connect to the WLAN Switch using the CLI, the system displays its host name followed by the login prompt. Log in using the administrator user account (the password displays as asterisks). For example:

```
<alcatel>
user: admin
password: *****
```

When you are logged in, the user mode CLI prompt displays. For example:

```
<alcatel> >
```

User mode provides only limited access for basic operational testing such as running `ping` and `traceroute`.

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

```
<alcatel> > enable
Password: ******
```

When you are in privileged mode, the > prompt changes to a pound sign (#):

```
<alcatel> #
```

Saving Configuration Changes

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

```
<alcatel> # write memory
Saving Configuration...
Saved Configuration
```

Command Completion

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

```
(alcatel) # configure terminal
```

could also be entered as:

```
(alcatel) # con t
```

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

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

Command Help

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

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

```
<alcatel> > ?

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

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

```
<alcatel> > c?

clear                    Clear configuration
clock                    Configure the system clock
```

```
configure               Configuration Commands
copy                    Copy Files
```

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

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

```
<alcatel> # write ?
erase                   Erase and start from scratch
file                    Write to a file in the file system
memory                  Write to memory
terminal                Write to terminal
<cr>
```

The <cr> indicates that the command can be entered without additional parameters. Any other parameters are optional.

Command Line Editing

The command line editing feature allows you to make corrections or changes to a command without retyping. Table 1-5 lists the editing controls:

TABLE 1-5 Line Editing Keys

Key	Effect	Description
<Ctrl-a>	Home	Move the cursor to the beginning of the line.
<Ctrl-b> or <left arrow>	Back	Move the cursor one character left.
<Ctrl-d>	Delete Right	Delete the character to the right of the cursor.
<Ctrl-e>	End	Move the cursor to the end of the line.
<Ctrl-f> or <right arrow>	Forward	Move the cursor one character right.
<Ctrl-k>	Kill Right	Delete all characters to the right of the cursor.
<Ctrl-n> or <down arrow>	Next	Display the next command in the command history.
<Ctrl-p> or <up arrow>	Previous	Display the previous command in the command history.

TABLE 1-5 Line Editing Keys (Continued)

Key	Effect	Description
<Ctrl-t>	Transpose	Swap the character to the left of the cursor with the character to the right of the cursor.
<Ctrl-u>	Clear	Clear the line.
<Ctrl-w>	Delete Word	Delete the characters from the cursor up to and including the first space encountered.
<Ctrl-x>	Kill Left	Delete all characters to the left of the cursor.

Alphanumeric characters are always inserted into the line at the cursor position.

Command History

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

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

Viewing the Configuration

You can view two configuration images from the CLI:

- `startup-config` holds the configuration options which will be used the next time the WLAN Switch is rebooted. It contains all the options last saved using the `write memory` command. Presently unsaved changes are not included.

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

  ```
  <alcatel> # show startup-config
  ```

- `running-config` holds the current switch configuration, including all pending changes which have yet to be saved.

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

  ```
  <alcatel> # show running-config
  ```

Both configurations can also be saved to a file or sent to a TFTP server for backup or transfer to another system.

Alcatel Mobility Manager

Alcatel Mobility Manager is an element management system (EMS) application that enables you to manage Alcatel APs and WLAN Switches from a single platform.

The management interface, which runs on Windows, Linux, or MacOS clients, is a Java-based graphical user interface (GUI) that enables scoping, filtering, monitoring, and planning of the wireless network. Multiple clients can access the management interface simultaneously. Each client must have the compatible Java Runtime Environment (JRE) installed; you can download the appropriate JRE from the Mobility Manager application.

The Mobility Manager software is embedded on the OmniVista Mobility Manager Appliance. You can also install the Mobility Manager software on a dedicated server platform.

For more information about the OmniVista Mobility Manager, see the *Mobility Manager User Guide*.

Volume 2

Installing the Alcatel OmniAccess System

AOS-W User Guide

Version 2.5.3

Copyright

Specifications in this manual are subject to change without notice.

Originated in the USA.

Trademarks

AOS-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 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

This preface includes the following information:

- An overview of the contents of 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

The *AOS-W User Guide* is now in eight separate volumes for easier download and information access. The volumes are as follows:

- Volume 1 contains an overview of the OmniAccess System.
- Volume 2 (this volume) describes how to install the OmniAccess System in a wired network.
- Volume 3 describes WLAN configuration, including remote Access Points.
- Volume 4 describes wireless encryption and authentication configuration.
- Volume 5 describes configuring multi-WLAN switch environments.
- Volume 6 describes intrusion prevention configuration.
- Volume 7 describes managing the OmniAccess System.
- Volume 8 describes configuring advanced services, such as Quality of Service (QoS) for voice and the External Services Interface module.

Related Documents

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

- *AOS-W User Guide*
- *Alcatel Wireless LAN Switch Installation Guides*
- *Alcatel Access Point Installation Guides*
- *Release Notes*

Text Conventions

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

TABLE 1 Text Conventions

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>	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: # **send** *<text message>* 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 | Item B }	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Contacting Alcatel

Contact Center Online		
■	Main Site	http://www.alcatel.com/enterprise
■	Support Site	http://eservice.ind.alcatel.com
■	Email	support@ind.alcatel.com
Sales & Support Contact Center Telephone		
■	North America	1-800-995-2696
■	Latin America	1-877-919-9526
■	Europe	+33 (0) 38 85 56 92 9
■	Asia Pacific	+65 6586 1555
■	Worldwide	1-818-880-3500

Deploying a Basic OmniAccess System

1

This chapter describes how to connect an Alcatel WLAN Switch and Alcatel APs to your wired network.

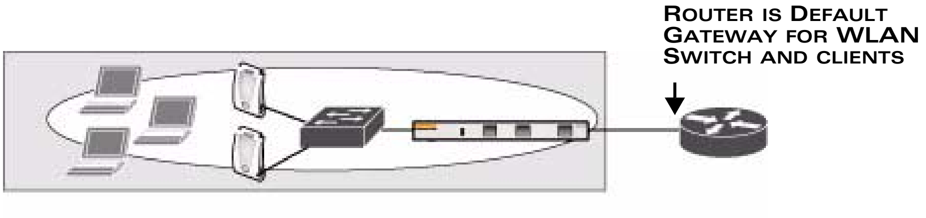
This chapter describes the following topics:

NOTE: AOS-W 2.5.3 introduces a simplified installation procedure that includes a Java-based RF Plan tool and a new Access Point Installation Wizard in the WebUI. The Access Point Installation Wizard automatically performs much of the configuration described in this chapter. You can either perform the manual configuration described in this chapter, or follow the simplified installation procedure described in the *Alcatel Quick Start Guide*. The *Alcatel Quick Start Guide* also describes using the Access Point Installation Wizard.

Configuration Overview

This section describes typical deployment scenarios and the tasks you need to perform in connecting an Alcatel WLAN Switch and Alcatel APs to your wired network.

Deployment Scenario #1



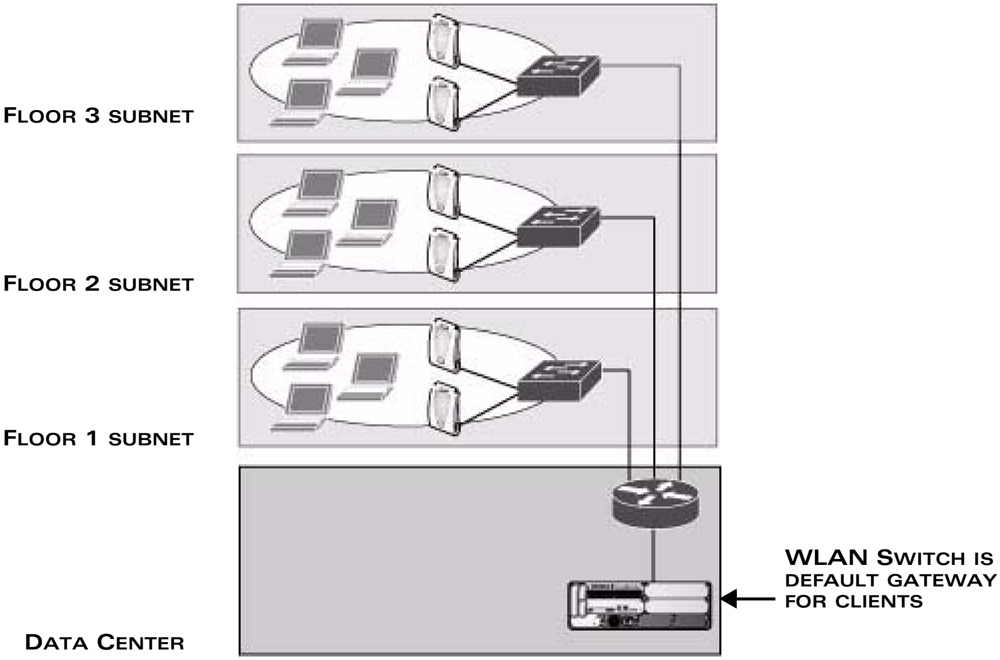
In this deployment scenario, the Alcatel APs and WLAN Switch are on the same subnetwork and will use IP addresses assigned to the subnetwork. In this scenarios, there are no routers between the APs and the WLAN Switch. APs can be physically connected directly to the WLAN Switch. The uplink port on the WLAN Switch is connected to a layer-2 switch or router.

You need to perform the following tasks:

1. Run the Initial Setup.
   - Set the IP address of VLAN 1.
   - Set the default gateway to the IP address of the interface of the upstream router to which you will connect the WLAN Switch.
2. Connect the uplink port on the WLAN Switch to the switch or router interface. By default, all ports on the WLAN Switch are access ports and will carry traffic for a single VLAN.
3. Deploy APs. The APs will use the Alcatel Discovery Protocol (ADP) to locate the WLAN Switch.

You would then configure the SSID(s) with VLAN 1 as the assigned VLAN for all users.

Deployment Scenario #2



In this deployment scenario, the Alcatel APs and the WLAN Switch are on different subnetworks and the APs are on multiple subnetworks. The WLAN Switch acts as a router for the wireless user subnetworks (the WLAN Switch is the default gateway for the wireless clients). The uplink port on the WLAN Switch is connected to a layer-2 switch or router; this port is an access port in VLAN 1.

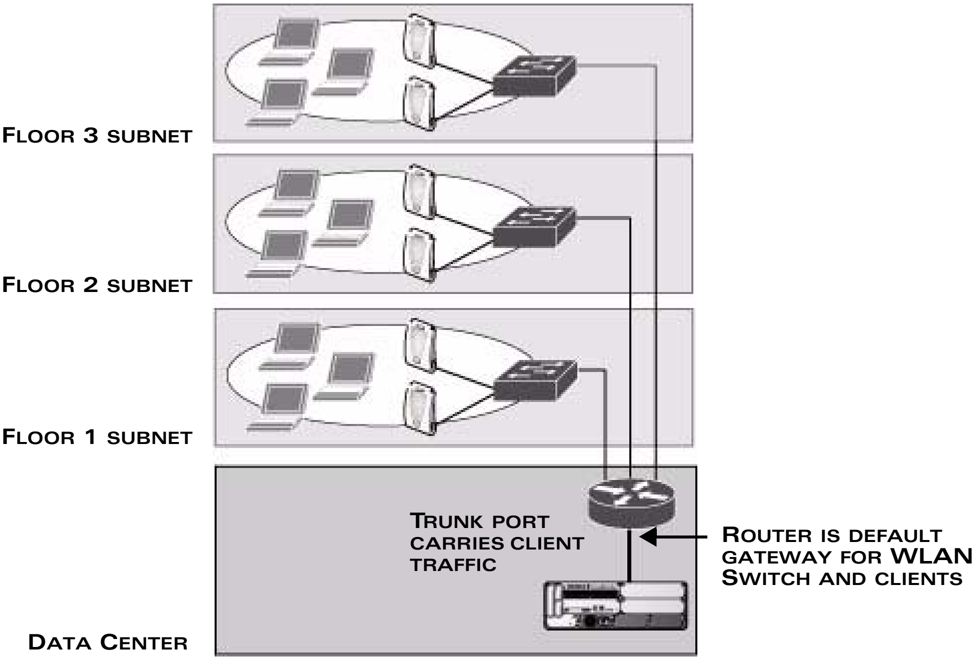
You need to perform the following tasks:

1. Run the Initial Setup.
   - Set the IP address for VLAN 1.
   - Set the default gateway to the IP address of the interface of the upstream router to which you will connect the WLAN Switch.
2. Connect the uplink port on the WLAN Switch to the switch or router interface.
3. Deploy APs. The APs will use DNS or DHCP to locate the WLAN Switch.

You would then need to configure VLANs for the wireless user subnetworks on the WLAN Switch, and configure SSIDs with the VLANs assigned for each wireless user subnetwork.

Note: Each wireless user VLAN must be configured on the WLAN Switch with an IP address. On the uplink switch or router, you must configure static routes for each user VLAN, with the WLAN Switch’s VLAN 1 IP address as the next hop.

Deployment Scenario #3


Floor 3 subnet
Floor 2 subnet
Floor 1 subnet
Trunk port carries client traffic
Router is default gateway for WLAN Switch and clients
Data Center

In this deployment scenario, the Alcatel APs and the WLAN Switch are on different subnetworks and the APs are on multiple subnetworks. There are routers between the APs and the WLAN Switch. The WLAN Switch is connected to a layer-2 switch or router through a trunk port that carries traffic for all wireless user VLANs. An upstream router functions as the default gateway for the wireless users.

Note: This deployment scenario does *not* use VLAN 1 to connect to the layer-2 switch or router through the trunk port. The Initial Setup prompts you for the IP address and default gateway for VLAN 1; use the default values. In later steps, you will configure the appropriate VLAN to connect to the switch or router as well as the default gateway.

You need to perform the following tasks:

1. Run the Initial Setup.

- Use the *default* IP address for VLAN 1. Since VLAN 1 is *not* used to connect to the layer-2 switch or router through the trunk port, you need to configure the appropriate VLAN in a later step.
- Do *not* specify a default gateway (use the default “none”). In a later step, you configure the default gateway.

2. Create a VLAN that has the same VLAN ID as the VLAN on the switch or router to which you will connect the WLAN Switch. Add the uplink port on the WLAN Switch to this VLAN and configure the port as a trunk port.
3. Add user VLANs to the trunk port.
4. Configure the default gateway on the WLAN Switch. This gateway is the IP address of the router to which you will connect the WLAN Switch.
5. Configure the loopback interface for the WLAN Switch.
6. Connect the uplink port on the WLAN Switch to the switch or router interface.
7. Deploy APs. The APs will use DNS or DHCP to locate the WLAN Switch.

You would then configure VLANs on the WLAN Switch for the wireless user subnetworks and configure SSIDs with the VLANs assigned for each wireless user subnetwork .

Configuring the Alcatel WLAN Switch

The tasks in deploying a basic Alcatel OmniAccess system fall into two main areas:

- Configuring and connecting the Alcatel WLAN Switch to the wired network (described in this section)
- Deploying Alcatel APs (described later in this section)

To connect the WLAN Switch to the wired network, you need to perform the following steps:

1. Run the Initial Setup to configure administrative information for the WLAN Switch.
2. (Deployment #3) Configure a VLAN to connect the WLAN Switch to your network. You do *not* need to perform this step if you are using VLAN 1 to connect the WLAN Switch to the wired network.
3. Connect the ports on the WLAN Switch to your network.
4. (Optional) Configure a loopback address for the WLAN Switch. You do *not* need to perform this step if you are using the VLAN 1 IP address as the WLAN Switch’s IP address.

This section describes the steps in detail.

Run the Initial Setup

When you connect to the WLAN Switch for the first time using either a serial console or a Web browser, the Initial Setup automatically launches. The Initial Setup requires you to set the role (master or local) for the WLAN Switch and passwords for administrator and configuration access. The Initial Setup also requires that you specify the country code for the country in which the WLAN Switch will operate; this sets the regulatory domain for the radio frequencies that the APs use.

The Initial Setup requires that you configure an IP address for the VLAN 1 interface, which you can use to access and configure the WLAN Switch remotely via an SSH or WebUI session. Configuring an IP address for the VLAN 1 interface ensures that there is an IP address and default gateway assigned to the WLAN Switch upon completion of the Initial Setup.

After you complete the Initial Setup, the WLAN Switch reboots using the new configuration. See the *Alcatel Quick Start Guide* for information about using the Initial Setup.

You can connect to and configure the WLAN Switch in several ways using the administrator password you entered during the Initial Setup:

- You can continue to use the connection to the serial port on the WLAN Switch to enter the command line interface (CLI). (Refer to "Overview of the Alcatel OmniAccess System" in Volume 1 of the *AOS-W User Guide* for information on how to access the CLI and enter configuration commands.)
- You can connect an Ethernet cable from a PC to an Ethernet port on the WLAN Switch. You can then use one of the following access methods:
  - Use the VLAN 1 IP address to start an SSH session where you can enter CLI commands.
  - Enter the VLAN 1 IP address in a browser window to start the WebUI. The WebUI contains an AP Installation Wizard that guides you through the setup of the WLAN Switch and APs. Refer to the *Alcatel Quick Start Guide*.

Configure a VLAN for Network Connection

You need to follow the instructions in this section only if you need to configure a trunk port between the Alcatel WLAN Switch and another layer-2 switch (shown in "Deployment Scenario #3" on page 4).

This section shows how to use both the WebUI and CLI for the following configurations (subsequent steps show how to use the WebUI only):

- Create a VLAN on the WLAN Switch and assign it an IP address.
- Assign to the VLAN the port(s) that you will use to connect the WLAN Switch to the network. (For example, the uplink ports that you connect to a router are usually Gigabit ports.)

- Configure the ports as trunk ports.
- Configure a default gateway for the WLAN Switch.

Create the VLAN

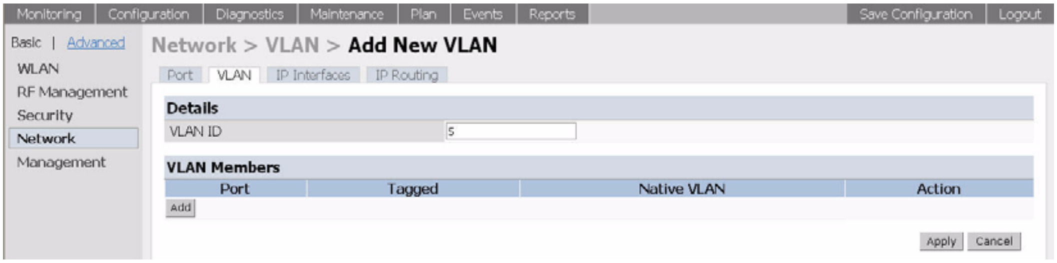
The following configurations create VLAN 5 and assign it the IP address 10.3.22.20/24.

WebUI

1. Click the **Configuration** tab in the menu bar. Under **Basic**, click the **Network** page. Click the **VLAN** tab.

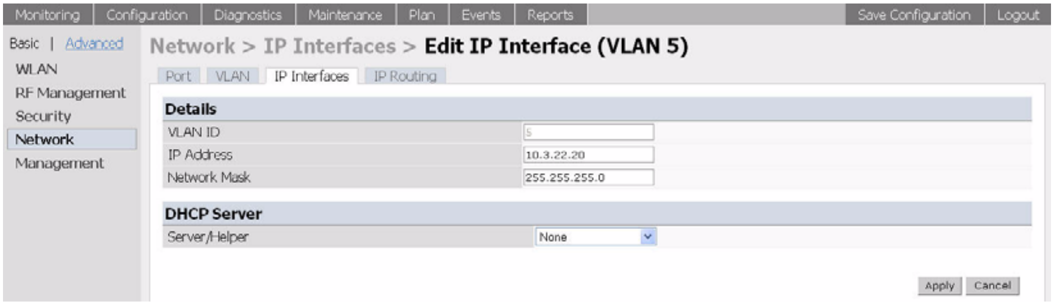
   NOTE: In the remainder of this manual, the instructions for reaching a specific WebUI page are shortened to specify the sequence of tab or page selections; for example, "Navigate to the **Configuration** > **Basic** > **Network** > **VLAN** page."

2. Click **Add** to create a new VLAN.
3. On the **Add New VLAN** screen (shown below), enter **5** for the VLAN ID and click **Apply**.



VLAN ID: 5

4. Navigate to the **Configuration** > **Basic** > **Network** > **IP Interfaces** page on the WebUI. Click **Edit** for the VLAN you just added. Enter the IP address and network mask of the VLAN interface. If required, you can also configure the address of the DHCP server for the VLAN by clicking **Add**.



VLAN ID: 5
IP Address: 10.3.22.20
Network Mask: 255.255.255.0
Server/Helper: None

5. Click **Apply** to apply this configuration.

NOTE: In the WebUI configuration pages, clicking the Apply button saves configuration changes so they are retained after the WLAN Switch is rebooted.

CLI

```
(alcatel)
User: admin
Password: *****
(alcatel) >enable
Password:******
(alcatel) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(alcatel) (config) #vlan 5
(alcatel) (config) #interface vlan 5
(alcatel) (config-subif)#ip address 10.3.22.20 255.255.255.0
(alcatel) (config-subif)#exit
(alcatel) (config) #write memory
```

NOTE: In the remainder of this manual, only the CLI configuration commands are shown.

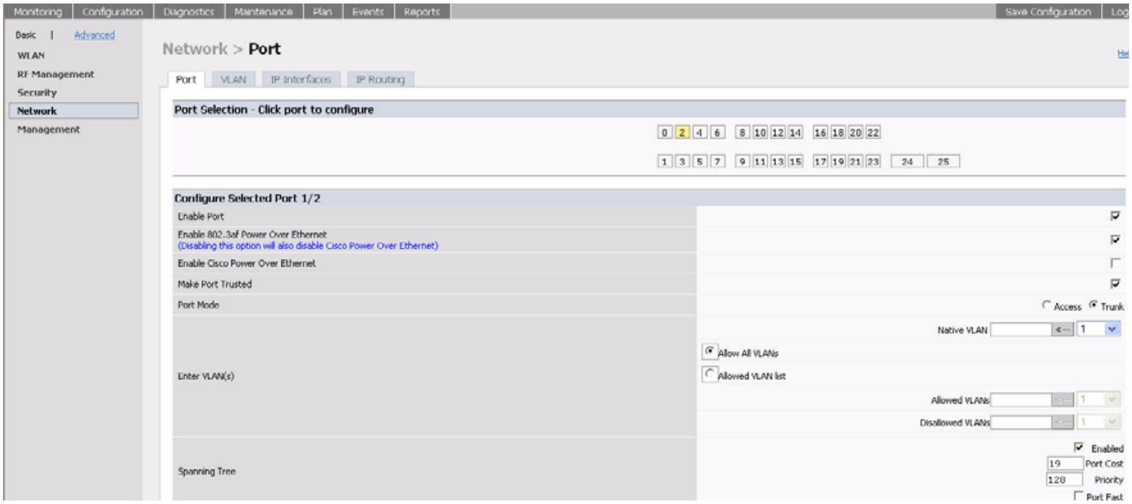
Configure the Trunk Port

The following configuration configures a Gigabit Ethernet port as a trunk port.

WebUI

1. Navigate to the **Configuration > Basic > Network > Port** page on the WebUI.
2. To add a port to the VLAN, click the port in the Port Selection section.
3. For Port Mode, select **Trunk**.

4. For Native VLAN, select VLAN 5 from the scrolling list, then click the <-- arrow.



Port Selection - Click port to configure

0 2 4 6 8 10 12 14 16 18 20 22
1 3 5 7 9 11 13 15 17 19 21 23 24 25

Configure Selected Port 1/2

Enable Port	☑
Enable 802.3af Power Over Ethernet (Disabling this option will also disable Cisco Power Over Ethernet)	☑
Enable Cisco Power Over Ethernet	☐
Make Port Trusted	☑
Port Mode	○ Access ● Trunk
Enter VLAN(s)	Native VLAN [ ] <-- 1 ● Allow All VLANs ○ Allowed VLAN list Allowed VLANs [ ] <-- 1 Disallowed VLANs [ ] <-- 1
Spanning Tree	☑ Enabled 19 Port Cost 128 Priority ☐ Port Fast

5. Click **Apply**.

CLI

```
interface range gigabitethernet 1/24
   switchport mode trunk
   switchport trunk native vlan 5
```

To confirm the port assignments, use the **show vlan** command:

```
(alcatel) (config) #show vlan

VLAN CONFIGURATION
------------------
VLAN   Name       Ports
----   ----       -----
1      Default    Fa1/0-23
5      VLAN0005   Gig1/24-25
```

Configure the Default Gateway

The following configurations assign a default gateway for the WLAN Switch.

WebUI

1. Navigate to the **Configuration > Advanced > Switch > General > IP Routing** page.
2. In the Default Gateway field, enter 10.3.22.1.
3. Click **Apply**.

CLI

```
ip default-gateway 10.3.22.1
```

Connect the WLAN Switch to the Network

Connect the ports on the WLAN Switch to the appropriately-configured ports on an L2 switch or router. Make sure that you have the correct cables and that the port LEDs indicate proper connections. Refer to the *Installation Guide* for the Alcatel WLAN Switch for port LED and cable descriptions.

To verify that the WLAN Switch is accessible on the network:

- If you are using VLAN 1 to connect the WLAN Switch to the network ("Deployment Scenario #1" and "Deployment Scenario #2"), ping the VLAN 1 IP address from a workstation on the network.
- If you created and configured a new VLAN ("Deployment Scenario #3"), ping the IP address of the new VLAN from a workstation on the network.

Configure the Loopback for the WLAN Switch

You need to configure a loopback address if you are not using VLAN 1 to connect the WLAN Switch to the network (see "Deployment Scenario #3" on page 4).

If configured, the loopback address is used as the WLAN Switch's IP address. If you do not configure a loopback address for the WLAN Switch, the IP address assigned to VLAN 1 is used as the WLAN Switch's IP address.

NOTE: After you configure or modify a loopback address, you need to reboot the WLAN Switch.

AOS-W allows the loopback address to be part of the IP address space assigned to a VLAN interface. In the example topology, the VLAN 5 interface on the WLAN Switch was previously configured with the IP address 10.3.22.20/24. The loopback IP address in this example will be 10.3.22.220.

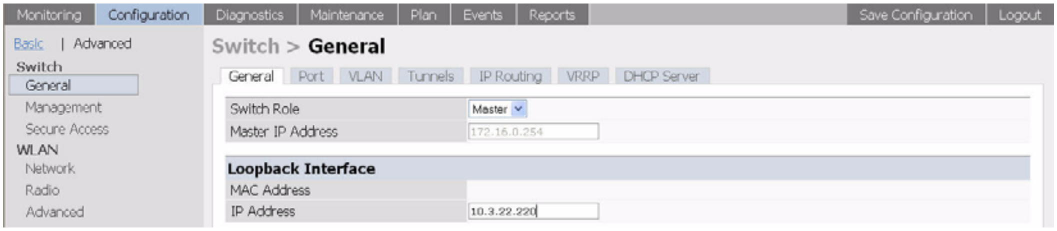
NOTE: You configure the loopback address as a host address with a 32-bit netmask. The loopback address should be routable from all external networks.

To set the loopback address through the WebUI:

WebUI

1. Navigate to the **Configuration** > **Advanced** > **Switch** > **General** page.

2. Enter the IP address for the loopback address.



Switch > General

Switch Role	Master
Master IP Address	172.16.0.254

Loopback Interface

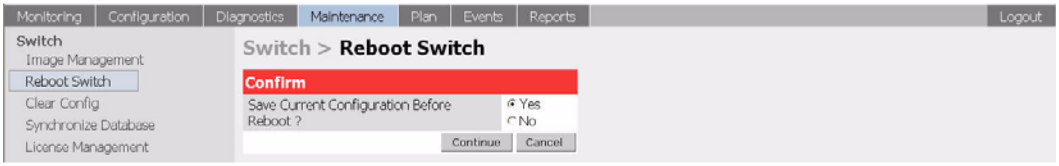
MAC Address	
IP Address	10.3.22.220

3. Click **Apply** at the bottom of the page (you may need to scroll down the page).

4. At the top of the page, click **Save Configuration**.

   You need to reboot the WLAN Switch for the new IP address to take effect.

5. Navigate to the **Maintenance > Switch > Reboot Switch** page.



Switch > Reboot Switch

Confirm

Save Current Configuration Before Reboot ? ● Yes ○ No

6. Click **Continue**.

CLI

```
interface loopback
   ip address 10.3.22.220
```

To verify that the WLAN Switch is accessible on the network, ping the loopback address from a workstation on the network.

Deploying APs

Alcatel APs and AMs are designed to require only minimal provisioning to make them fully operational in an Alcatel OmniAccess system. Once APs have established communication with the WLAN Switch, you can apply advanced configuration to individual APs or globally across the entire OmniAccess system using the WebUI on the WLAN Switch.

NOTE: AOS-W 2.5.3 introduces a new Access Point Installation Wizard in the WebUI that simplifies some of the deployment tasks described in this section. The Access Point Installation Wizard appears on the master WLAN Switch and guides you through configuring APs that are to be installed in your network. You can then install the programmed APs in their permanent locations in the network. To use the Access Point Installation Wizard instead of performing the manual configurations described in this section, see the *Alcatel Quick Start Guide*.

If you choose not to use the AP Installation Wizard, you can deploy APs by doing the following steps:

1. Run the Java-based RF Plan tool to help position APs and import floorplans for your installation.
2. Ensure that the APs can locate the WLAN Switch when they are connected to the network. There are several ways in which APs can locate the WLAN Switch.
3. Install the APs by connecting the AP to an Ethernet port and, optionally, to a power source.
4. On the WLAN Switch, configure the APs.

This section describes the steps.

Run Alcatel RF Plan

The Java-based RF Plan tool is an application that allows you to determine AP placement based on your specified coverage and capacity requirements without impacting the live network. For more information about using RF Plan, see the *RF Plan Installation and User Guide*.

Enable APs to Connect to the WLAN Switch

Before you install APs in a network environment, you must ensure that the APs will be able to locate and connect to the WLAN Switch when powered on. Specifically, you need to ensure the following:

- When connected to the network, each AP is assigned a valid IP address
- APs are able to locate the WLAN Switch

NOTE: Alcatel APs use Trivial File Transfer Protocol (TFTP) the first time they boot to obtain their software image and configuration from the WLAN Switch. After the initial boot, the APs use FTP to obtain software images and configurations from the WLAN Switch.

Enable APs to Obtain IP Addresses

Each Alcatel AP requires a unique IP address on a subnetwork that has connectivity to a WLAN Switch. Alcatel recommends using the Dynamic Host Configuration Protocol (DHCP) to provide IP addresses for APs; the DHCP server can be an existing network server or an Alcatel WLAN Switch configured as a DHCP server.

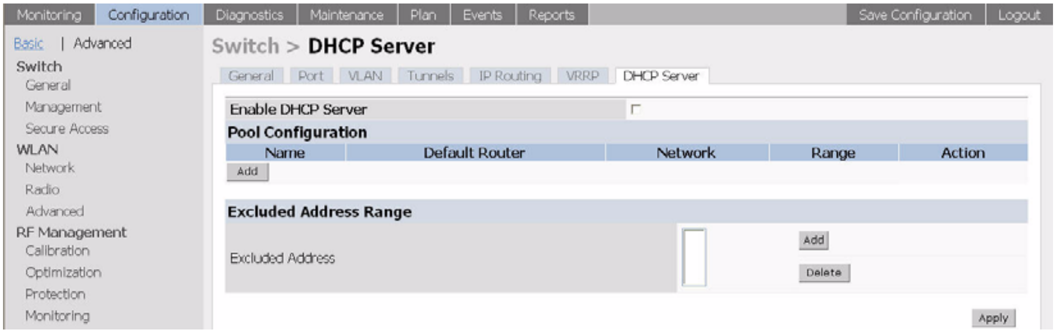
You can use an existing DHCP server in the same subnetwork as the AP to provide the AP with its IP information. You can also configure a device in the same subnetwork to act as a relay agent for a DHCP server on a different subnetwork. Refer to the vendor documentation for the DHCP Server or relay agent for information.

If an AP is on the same subnetwork as the master WLAN Switch, you can configure the WLAN Switch as a DHCP server to assign an IP address to the AP. The WLAN Switch must be the only DHCP server for this subnetwork.

To enable DHCP server capability on a WLAN Switch:

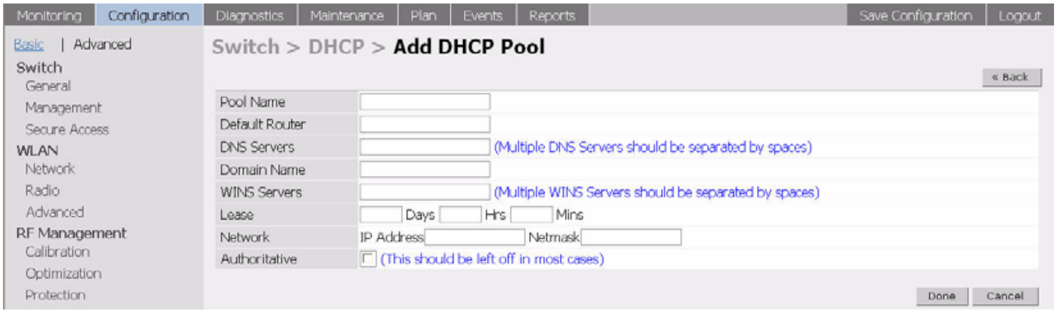
WebUI

1. Navigate to the **Configuration** > **Advanced** > **Switch** > **General** > **DHCP Server** page.



2. Select the **Enable DHCP Server** checkbox.

3. In the Pool Configuration section, click **Add**.



Switch > DHCP > **Add DHCP Pool**

Pool Name	
Default Router	
DNS Servers	(Multiple DNS Servers should be separated by spaces)
Domain Name	
WINS Servers	(Multiple WINS Servers should be separated by spaces)
Lease	Days Hrs Mins
Network	IP Address Netmask
Authoritative	□ (This should be left off in most cases)

4. Enter information about the subnetwork for which IP addresses are to be assigned. Click **Done**.
5. If there are addresses that should not be assigned in the subnetwork:
   - **A.** Click **Add** in the Excluded Address Range section.
   - **B.** Enter the address range in the Add Excluded Address section.
   - **C.** Click **Done**.
6. Click **Apply** at the bottom of the page.
7. At the top of the page, click **Save Configuration**.

CLI

```
ip dhcp excluded-address ipaddr ipaddr2
ip dhcp pool name
   default-router ipaddr
   dns-server ipaddr
   domain-name name
   network ipaddr mask
```

Locate the WLAN Switch

An Alcatel AP can discover the IP address of the WLAN Switch in one of the following ways:

- From a DNS server
- From a DHCP server
- Using the Alcatel Discovery Protocol (ADP)

From a DNS Server

Alcatel APs are factory-configured to use the host name `oaw-master` for the WLAN Switch. For the DNS server to resolve this host name to the IP address of the WLAN Switch, you must configure an entry on the DNS server for the name `oaw-master`.

For information on how to configure a host name entry on the DNS server, refer to the vendor documentation for your server.

NOTE: Alcatel recommends using a DNS server to provide APs with the IP address of the master WLAN Switch because it involves minimal changes to the network and provides the greatest flexibility in the placement of APs.

From a DHCP Server

You can configure a DHCP server to provide the WLAN Switch's IP address. You need to configure the DHCP server to send the WLAN Switch's IP address using the DHCP vendor-specific attribute option 43. Alcatel APs identify themselves with a vendor class identifier set to `ArubaAP` in their DHCP request. When the DHCP server responds to the request, it will send the WLAN Switch's IP address as the value of option 43.

For more information on how to configure vendor-specific information on a DHCP server, see Appendix A, "Configuring DHCP with Vendor-Specific Options,"or refer to the vendor documentation for your server.

Using the Alcatel Discovery Protocol (ADP)

ADP is enabled by default on all Alcatel APs and WLAN Switches. To use ADP, all Alcatel APs and WLAN Switches must be connected to the same Layer-2 network. If the devices are on different networks, a Layer-3 compatible discovery mechanism, such as DNS, DHCP, or IGMP forwarding, must be used instead.

With ADP, APs send out periodic multicast and broadcast queries to locate the WLAN Switch. You may need to perform additional network configuration, depending on whether the APs are in the same broadcast domain as the WLAN Switch:

- If the APs are in the same broadcast domain as the WLAN Switch, the WLAN Switch automatically responds to the APs' queries with its IP address.
- If the APs are not in the same broadcast domain as the WLAN Switch, you need to enable multicast on the network (ADP multicast queries are sent to the IP multicast group address 224.0.82.11) for the WLAN Switch to respond to the APs' queries. You also need to make sure that all routers are configured to listen for Internet Group Management Protocol (IGMP) join requests from the WLAN Switch and can route these multicast packets.

  To verify that ADP and IGMP join options are enabled on the WLAN Switch, use the following CLI command:

```
(WLAN_Switch) #show adp config
ADP Configuration
-----------------
key          value
---          -----
discovery  enable
igmp-join  enable
```

If ADP or IGMP join options are not enabled, use the following CLI commands:

```
(WLAN_Switch) (config) #adp discovery enable
(WLAN_Switch) (config) #adp igmp-join enable
```

Install APs

Use the AP placement map generated by RF Plan to install APs. When deploying APs, note the AP's MAC address and serial number as well as the physical location on the placement map. This is useful in assigning location code identifiers to APs (see "Configure the AP Location Code"), which greatly enhances location-based services and wireless network calibration.

You can either connect the AP directly to a port on the WLAN Switch, or connect the AP to another switch or router that has Layer-2 or Layer-3 connectivity to the WLAN Switch.

If the Ethernet port is an 802.3af Power over Ethernet (PoE) port, the AP automatically uses it to power up. If a PoE port is not available, you need to obtain an AC adapter for the AP from Alcatel. For more information, see the *Installation Guide* for the specific AP.

Once an AP is connected to the network and powered up, it attempts to locate its WLAN Switch using one of the methods described in "Locate the WLAN Switch" on page 14.

Provision APs

The next step in AP deployment is to configure or provision each AP. You must minimally configure each AP with a unique location code which is used for location servicing. The location code is in the numerical format *1.2.3*, where *1* specifies the building, *2* specifies the floor, and *3* specifies the location.

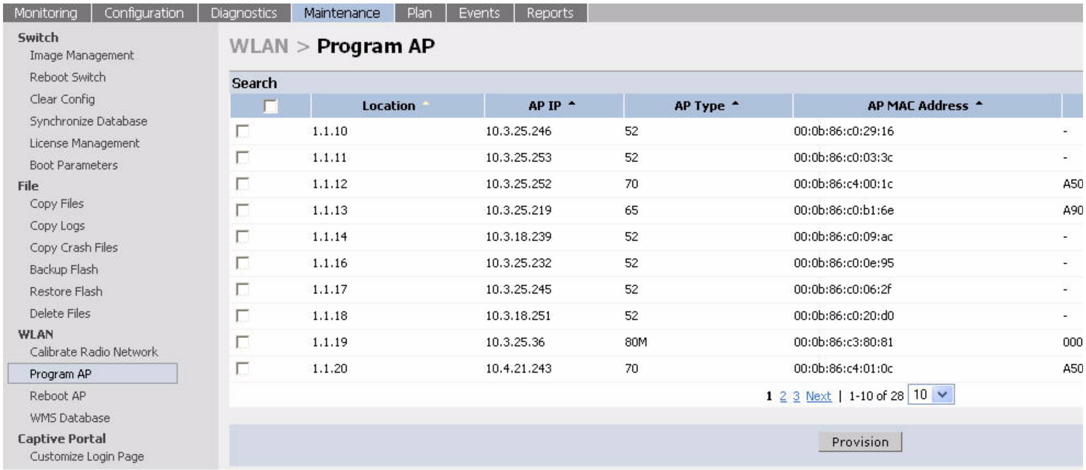
You can also configure Adaptive Radio Management, a mechanism that enables Alcatel APs to optimize their functions in any RF environment (see "Automatic RF Channel and Power Settings" on page 5).

Configure the AP Location Code

To configure the location code for an AP:

1. Navigate to the **Maintenance > Program AP** page.

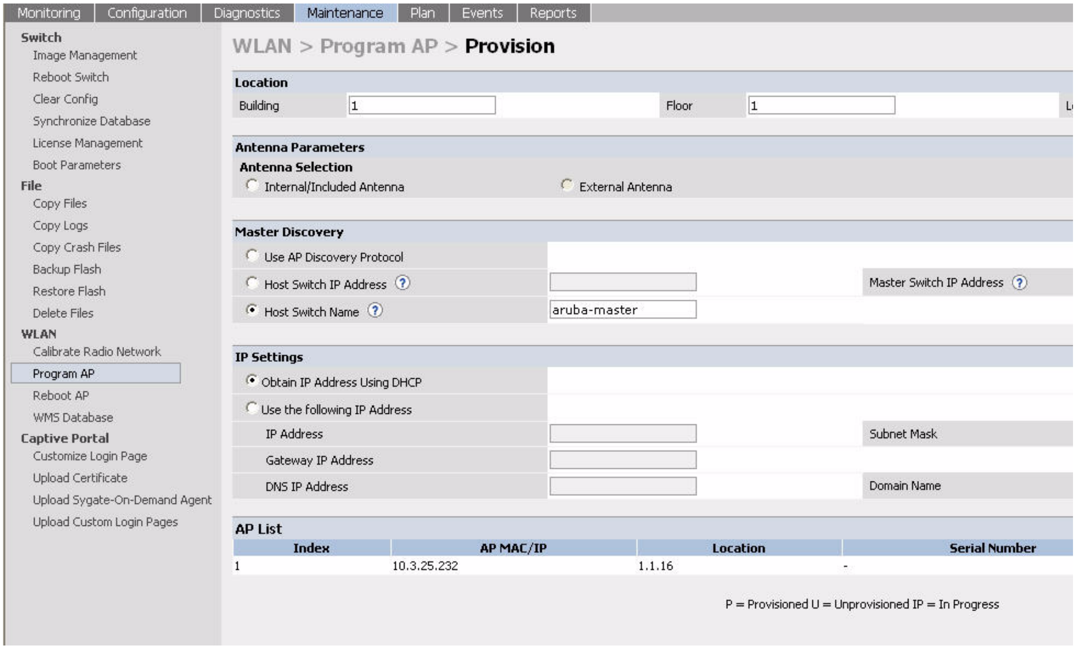
   This page displays a list of APs that have registered with the WLAN Switch with either their default location code (-1.-1.-1) or their currently-configured location code (if the AP has already been provisioned).



□	Location	AP IP	AP Type	AP MAC Address	
□	1.1.10	10.3.25.246	52	00:0b:86:c0:29:16	-
□	1.1.11	10.3.25.253	52	00:0b:86:c0:03:3c	-
□	1.1.12	10.3.25.252	70	00:0b:86:c4:00:1c	A50
□	1.1.13	10.3.25.219	65	00:0b:86:c0:b1:6e	A90
□	1.1.14	10.3.18.239	52	00:0b:86:c0:09:ac	-
□	1.1.16	10.3.25.232	52	00:0b:86:c0:0e:95	-
□	1.1.17	10.3.25.245	52	00:0b:86:c0:06:2f	-
□	1.1.18	10.3.18.251	52	00:0b:86:c0:20:d0	-
□	1.1.19	10.3.25.36	80M	00:0b:86:c3:80:81	000
□	1.1.20	10.4.21.243	70	00:0b:86:c4:01:0c	A50

1 2 3 Next | 1-10 of 28 10

2. Select the AP that is to be configured from the list by selecting the checkbox to the left of the AP and then clicking **Provision**.



WLAN > Program AP > Provision

Location

Building 1 Floor 1 L

Antenna Parameters

Antenna Selection

○ Internal/Included Antenna ○ External Antenna

Master Discovery

○ Use AP Discovery Protocol

○ Host Switch IP Address ? Master Switch IP Address ?

● Host Switch Name ? aruba-master

IP Settings

● Obtain IP Address Using DHCP

○ Use the following IP Address

IP Address Subnet Mask

Gateway IP Address

DNS IP Address Domain Name

AP List

Index	AP MAC/IP	Location	Serial Number
1	10.3.25.232	1.1.16	-

P = Provisioned U = Unprovisioned IP = In Progress

3. Enter the location code in the format explained above.

4. 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, enter **4.0**). This information is mandatory for all detachable antenna models as the AP cannot bring up its radio interface or function as an AP without it.

5. Click **Apply and Reboot** to apply the configuration to the AP.

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

Update RF Plan

The final step after deploying APs is to update the AP placement map in RF Plan. This allows more accurate reconciliation of location tracking features provided by the Alcatel OmniAccess system—for example, locating users, intruders, rogue APs and other security threats, assets, and sources of RF interference—with the physical environment.

Additional Configuration

After you have installed a basic Alcatel OmniAccess system, the Alcatel APs advertise the default `alcatel-ap` SSID. Wireless users can connect to this SSID but because you have not yet configured authentication, policies, or user roles, they will not have access to the network. Other volumes describe how to build upon this basic deployment to configure user roles, firewall policies, authentication, authentication servers, and other wireless features.

Volume 3 "Configuring WLANs" in the *AOS-W User Guide* describes how to configure WLANs using the WebUI. If you used the AP Installation Wizard in the WebUI to program and install your APs, you are redirected to the WLAN Basic Configuration page where you can configure the SSID and authentication for a WLAN.

The other volumes in the *AOS-W User Guide* provide more information about configuring and using features of the Alcatel OmniAccess system.

Configuring Network Parameters

2

This chapter describes some basic network configuration on the Alcatel WLAN Switch. This chapter describes the following topics:

- "Configuring VLANs" on page 21
- "Configuring Static Routes" on page 29
- "Configuring the Loopback IP Address" on page 30

Configuring VLANs

The Alcatel WLAN Switch operates as a layer-2 switch that uses a VLAN as a broadcast domain. As a layer-2 switch, the WLAN Switch requires an external router to route traffic between VLANs. The WLAN Switch can also operate as a layer-3 switch which can route traffic between VLANs defined on the WLAN Switch.

You can configure one or more physical ports on the WLAN Switch to be members of a VLAN. Additionally, each wireless client association constitutes a connection to a *virtual port* on the WLAN Switch, with membership in a specified VLAN. You can place all authenticated wireless users into a single VLAN or into different VLANs, depending upon your network. VLANs can exist only inside the Alcatel WLAN Switch or they can extend outside the WLAN Switch through 802.1q VLAN tagging.

You can optionally configure an IP address and netmask for a VLAN on the Alcatel WLAN Switch. The IP address is *up* when at least one physical port in the VLAN is up. The VLAN IP address can be used as a gateway by external devices; packets directed to a VLAN IP address that are not destined for the WLAN Switch are forwarded according to the Alcatel WLAN Switch's IP routing table.

To create or edit a VLAN:

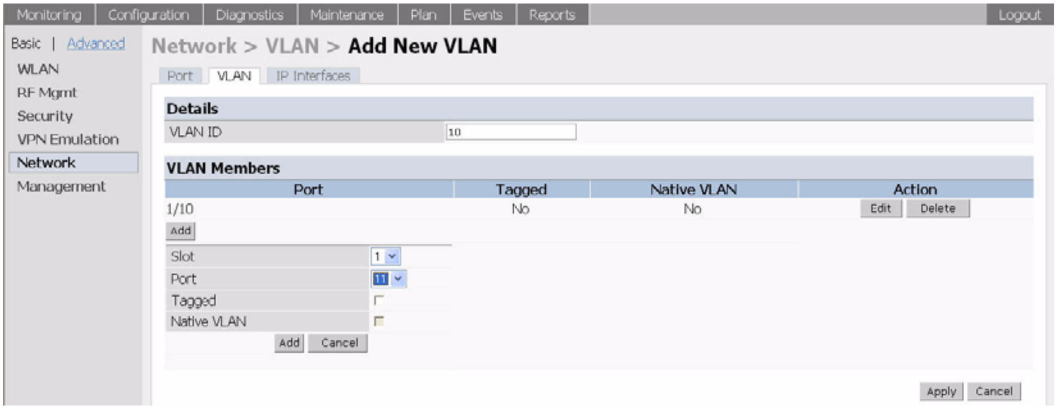
WebUI

1. Navigate to the **Configuration** > **Basic** > **Network** > **VLAN** page on the WebUI.
2. Click **Add** to create a new VLAN. (To edit an existing VLAN click **Edit** for the VLAN entry.)
3. On the **Add New VLAN** screen (shown below), enter the VLAN ID.
4. To add physical ports to the VLAN, click **Add** in the **VLAN Members** section. Select the port to add to the VLAN.

- For each port, you can specify whether the port uses 802.1q tagging.
- For ports that use 802.1q tagging, you can also specify whether the VLAN is the native VLAN for the port (frames on the native VLAN are not tagged).

Click **Add**.

5. Click **Apply**.



Network > VLAN > **Add New VLAN**

Details

VLAN ID	10

VLAN Members

Port	Tagged	Native VLAN	Action
1/10	No	No	Edit Delete

Slot	1
Port	11
Tagged	□
Native VLAN	□

CLI

```
vlan n
interface vlan n
```

Either:

```
interface port_name
   switchport mode access
   switchport access vlan vlan-id
```

or:

```
interface port_name
   switchport mode trunk
   switchport trunk native vlan vlan-id
```

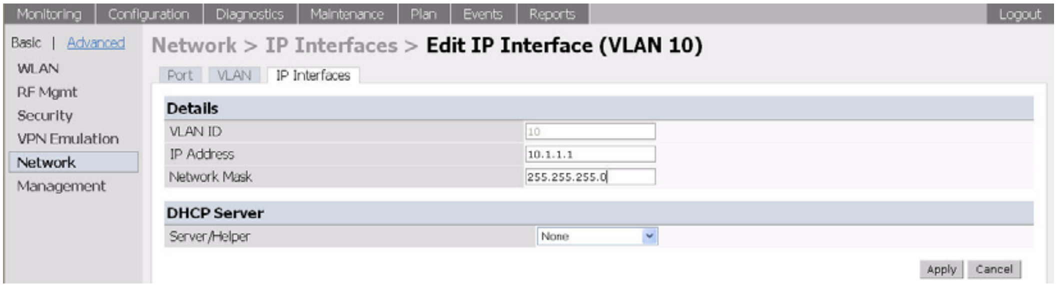
Assigning a Static Address to a VLAN

To assign a static IP address to a VLAN:

WebUI

1. Navigate to the **Configuration > Basic > Network > IP Interfaces** page on the WebUI. Click **Edit** for the VLAN you just added.

2. Enter the IP address and network mask of the VLAN interface. If required, you can also configure the address of the DHCP server for the VLAN by clicking **Add**.



Network > IP Interfaces > **Edit IP Interface (VLAN 10)**

Details

VLAN ID	10
IP Address	10.1.1.1
Network Mask	255.255.255.0

DHCP Server

Server/Helper	None

3. Click **Apply**.

CLI

```
interface vlan n
   ip address address netmask
```

Configuring a VLAN to Receive a Dynamic Address

A VLAN on the Alcatel WLAN Switch obtains its IP address in one of the following ways:

- Manually configured by the network administrator. This is the default method and is described in “Assigning a Static Address to a VLAN” on page 22. At least one VLAN on the WLAN Switch must be assigned a static IP address.
- Dynamically assigned from a Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE) server. These methods are described in the following section.

In a branch office, you can connect an Alcatel WLAN Switch to an uplink switch or server that dynamically assigns IP addresses to connected devices. For example, the WLAN Switch can be connected to a DSL or cable modem, or a broadband remote access server (BRAS). Figure 2-1 shows a branch office where an Alcatel WLAN Switch connects to a cable modem. VLAN 1 has a static IP address, while VLAN 2 has a dynamic IP address assigned via DHCP or PPPoE on the uplink device. The DHCP server on the Alcatel WLAN Switch assigns IP addresses to users on the local network from a configured pool of IP addresses.

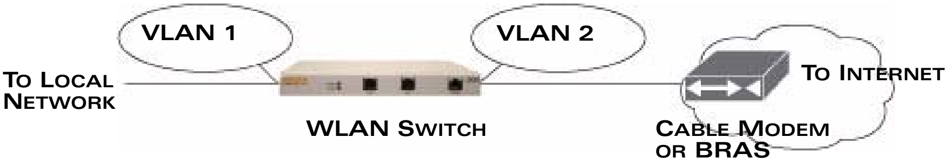


FIGURE 2-1 IP Address Assignment to VLAN via DHCP or PPPoE

To allow the WLAN Switch to obtain a dynamic IP address for a VLAN, you enable the DHCP or PPPoE client on the WLAN Switch for the VLAN.

The following restrictions apply when enabling the DHCP or PPPoE client on the WLAN Switch:

- You can enable the DHCP/PPPoE client on only one VLAN on the WLAN Switch; this VLAN cannot be VLAN 1.
- Only one port in the VLAN can be connected to the modem or uplink switch.
- At least one interface in the VLAN must be in the up state before the DHCP/PPPoE client requests an IP address from the server.
- Only one VLAN on the WLAN Switch can obtain its IP address through DHCP or PPPoE. You cannot enable both the DHCP and PPPoE client on the WLAN Switch at the same time.

Enabling the DHCP Client

The DHCP server assigns an IP address for a specified amount of time called a lease. The WLAN Switch automatically renews the lease before it expires. When you shut down the VLAN, the DHCP lease is released.

To enable the DHCP client on a VLAN:

WebUI

1. Navigate to the **Configuration** > **Advanced** > **Switch** > **General** > **VLAN** page.
2. Click **Add** to create a new VLAN or click **Edit** for a previously-created VLAN.
3. Select **Obtain an IP address from DHCP**.
4. Select the port that is connected to the modem or uplink switch.
5. Click **Apply**.

CLI

```
vlan vlan
interface vlan vlan
   ip address dhcp-client

interface port
   switchport access vlan vlan
```

Enabling the PPPoE Client

To authenticate to the BRAS and request a dynamic IP address, the WLAN Switch must have the following configured:

- PPPoE user name and password to connect to the DSL network
- PPPoE service name — either an ISP name or a class of service configured on the PPPoE server

When you shut down the VLAN, the PPPoE session terminates.

To enable the PPPoE client on a VLAN:

WebUI

1. Navigate to the **Configuration** > **Advanced** > **Switch** > **General** > **VLAN** page.
2. Click **Add** to create a new VLAN or click **Edit** for a previously-created VLAN.
3. Select **Obtain an IP address from PPPoE**.
4. Enter the service name, username, and password for the PPPoE session.
5. Select the port that is connected to the modem or uplink switch.
6. Click **Apply**.

CLI

```
ip pppoe-service-name service-name
ip pppoe-username name
ip pppoe-password password

vlan vlan
interface vlan vlan
   ip address pppoe

interface port
   switchport access vlan vlan
```

Default Gateway from DHCP/PPPoE

You can specify that the router IP address obtained from the DHCP or PPPoE server be used as the default gateway for the WLAN Switch. To do this:

WebUI

1. Navigate to the **Configuration** > **Advanced** > **Switch** > **IP Routing** page.
2. For Default Gateway, select **(Obtain an IP address automatically)**.
3. Select **Apply**.

CLI

```
ip default-gateway import
```

DNS/WINS Server from DHPC/PPPoE

The DHCP or PPPoE server can also provide the IP address of a DNS server or NetBIOS name server, which can be passed to wireless clients through the WLAN Switch's internal DHCP server.

For example, the following configures the DHCP server on the Alcatel WLAN Switch to assign addresses to authenticated employees; the IP address of the DNS server obtained by the WLAN Switch via DHCP/PPPoE is provided to clients along with their IP address.

WebUI

1. Navigate to the **Configuration** > **Advanced** > **Switch** > **General** > **DHCP Server** page.
2. Select **Enable DCHP Server**.
3. Under Pool Configuration, select **Add**.
4. For Pool Name, enter employee-pool.
5. For Default Router, enter 10.1.1.254.
6. For DNS Servers, select **Import from DHCP/PPPoE**.
7. For WINS Servers, select **Import from DHCP/PPPoE**.
8. For Network, enter 10.1.1.0 for IP Address and 255.255.255.0 for Netmask.
9. Click **Done**.

CLI

```
ip dhcp pool employee-pool
   default-router 10.1.1.254
   dns-server import
   netbios-name-server import
   network 10.1.1.0 255.255.255.0
```

Source NAT to Dynamic VLAN Address

When a VLAN interface obtains an IP address through DHCP or PPPoE, a NAT pool (dynamic-srcnat) and a session ACL (dynamic-session-acl) are automatically created which reference the dynamically-assigned IP addresses. This allows you to configure policies that map private local addresses to the public address(es) provided to the DHCP or PPPoE client. Whenever the IP address on the VLAN changes, the dynamic NAT pool address also changes to match the new address.

For example, the following rules for a guest policy deny traffic to internal network addresses. Traffic to other (external) destinations are source NATed to the IP address of the DHCP/PPPoE client on the WLAN Switch.

WebUI

1. Navigate to the **Configuration** > **Advanced** > **Security** > **Firewall Policies** page. Click **Add** to add the policy **guest**.
2. To add a rule, click **Add**.
   A. For Source, select **any**.
   B. For Destination, select **network** and enter 10.1.0.0 for Host IP and 255.255.0.0 for Mask.
   C. For Service, select **any**.
   D. For Action, select **reject**.
   E. Click **Add**.
3. To add another rule, click **Add**.
   A. Leave Source, Destination, and Service as **any**.
   B. For Action, select **src-nat**.
   C. For NAT Pool, select **dynamic-srcnat**.
   D. Click **Add**.
4. Click **Apply**.

CLI

```
ip access-list session guest
   any network 10.1.0.0 255.255.0.0 any deny
   any any any src-nat pool dynamic-srcnat
```

Configuring Source NAT for VLAN Interfaces

The example configuration in the previous section illustrates how to configure source NAT using a firewall rule that is applied to a user role. You can also enable source NAT for a VLAN interface to cause NAT to be performed on the source address for *all* traffic that exits the VLAN.

Packets that exit the VLAN are given a source IP address of the "outside" interface, which is determined by the following:

- If you configure "private" IP addresses for the VLAN, the Alcatel WLAN Switch is assumed to be the default gateway for the subnetwork. Packets that exit the VLAN are given the IP address of the WLAN Switch for their source IP address.
- If the WLAN Switch is forwarding the packets at Layer-3, packets that exit the VLAN are given the IP address of the next-hop VLAN for their source IP address.

Example Configuration

In the following example, the Alcatel WLAN Switch operates within an enterprise network. VLAN 1 is the outside VLAN. Traffic from VLAN 6 is source NATed using the IP address of the WLAN Switch. In this example, the IP address assigned to VLAN 1 is used as the WLAN Switch's IP address; thus traffic from VLAN 6 would be source NATed to 66.1.131.5.

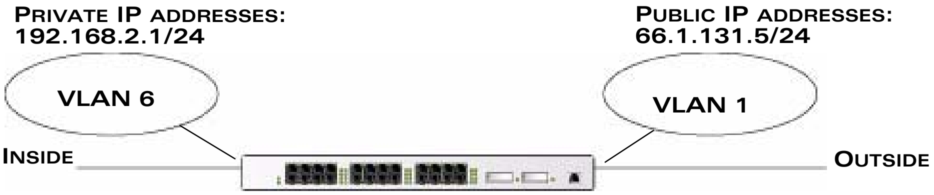


FIGURE 2-2 Example: Source NAT using WLAN Switch IP Address

WebUI

1. Navigate to the **Configuration** > **Advanced** > **Switch** > **General** > **VLAN** page. Click **Add** to configure VLAN 6.
2. Configure VLAN 6 as follows (VLAN 1 is configured through the Initial Setup):
   A. Enter **6** for the VLAN ID.
   B. Enter 192.168.2.1 for the IP Address and 255.255.255.0 for the Net Mask.
   C. Select the Enable source NAT for this VLAN checkbox.
3. Click **Apply**.

CLI

```
interface vlan 1
   ip address 66.1.131.5 255.255.255.0
```

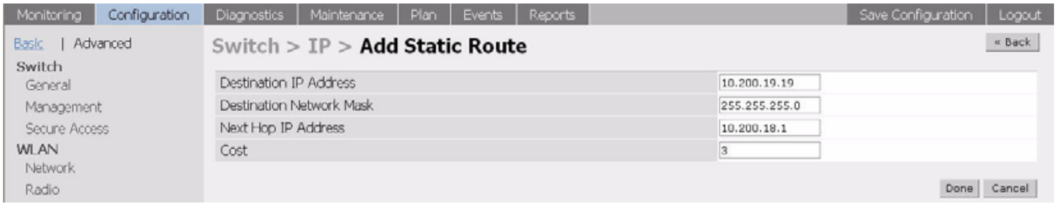
```
interface vlan 6
   ip address 192.168.2.1 255.255.255.0
   ip nat inside
ip default-gateway 66.1.131.1
```

Configuring Static Routes

To configure a static route (such as a default route) on the WLAN Switch, do the following:

WebUI

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



Switch > IP > **Add Static Route**

Destination IP Address	10.200.19.19
Destination Network Mask	255.255.255.0
Next Hop IP Address	10.200.18.1
Cost	3

3. Click **Done** to add the entry.

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

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

CLI

```
ip route address netmask next_hop
```

Configuring the Loopback IP Address

The loopback IP address is a logical IP interface that is used by the WLAN Switch to communicate with APs. If you do not configure a loopback address for the WLAN Switch, the IP address of the lowest-numbered VLAN interface (typically VLAN 1) is used as the WLAN Switch's IP address.

The loopback address is used as the WLAN Switch's IP address for terminating VPN and GRE tunnels, originating requests to RADIUS servers, and accepting administrative communications. You configure the loopback address as a host address with a 32-bit netmask. The loopback address is not bound to any specific interface and is operational at all times. To make use of this interface, ensure that the IP address is reachable through one of the VLAN interfaces. It should be routable from all external networks.

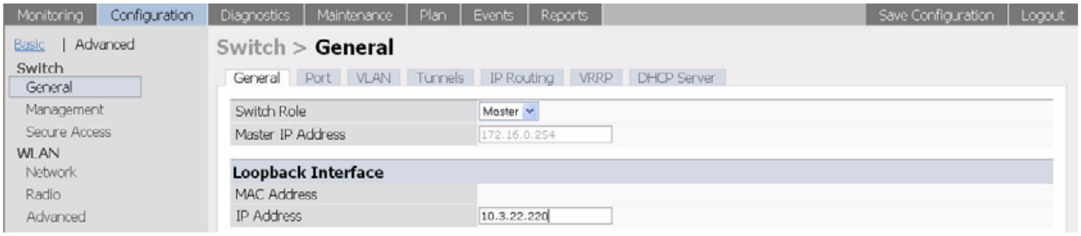
You can modify or delete the IP address of the loopback interface on the WLAN Switch. However, you cannot delete the loopback address if there is no IP address configured for the VLAN 1 interface. If you delete the loopback address when there is no IP address configured for the VLAN 1 interface, you will be prompted for a new IP address for the VLAN 1 interface. You also cannot delete the IP address for the VLAN 1 interface if there is no loopback address configured; you will be prompted for a new loopback address.

NOTE: Any change in the WLAN Switch's IP address requires a reboot.

To configure or change the loopback IP address on the WLAN Switch:

WebUI

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

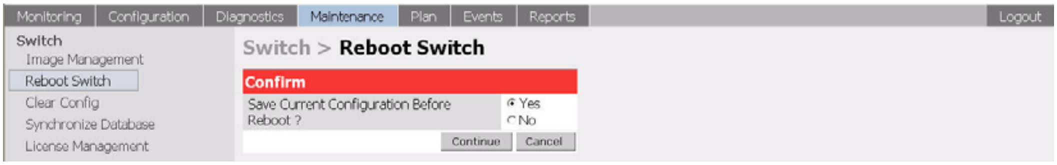


Switch Role: Master
Master IP Address: 172.16.0.254
IP Address: 10.3.22.220

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, changing the loopback IP address will result in loss of connectivity. Alcatel recommends that you use one of the VLAN interface IP addresses to access the WebUI.

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



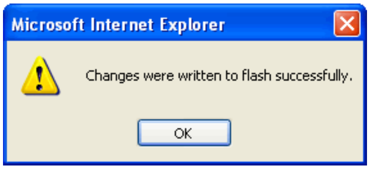
Switch > **Reboot Switch**

Confirm

Save Current Configuration Before Reboot ? ● Yes ○ No

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

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



Changes were written to flash successfully.

6. The WLAN Switch boots up with the changed loopback IP address.

CLI

```
interface loopback ip address address
write memory
```

To reboot the WLAN Switch, enter the following command in Enable mode:

```
reload
```

RF Plan 3

RF Plan is a wireless deployment modeling tool that enables you to design an efficient Wireless Local Area Network (WLAN) for your corporate environment, optimizing coverage and performance, and eliminating complicated WLAN network setup.

This chapter describes the following topics:

- "Overview" on page 33
- "Before You Begin" on page 35
- "Using RF Plan" on page 36
- "RF Plan Example" on page 55

NOTE: A Java-based RF Plan tool allows you to input the serial number or MAC address of each AP. You can import this information into the AP Installation Wizard (available in the WebUI in AOS-W 2.5.3) so that the system can program the APs before you physically install them. For information about using the Java-based RF Plan tool, see the *RF Plan Installation and User Guide*.

Overview

RF Plan provides the following critical functionality:

- Defines WLAN coverage.
- Defines WLAN environment security coverage.
- Assesses equipment requirements.
- Optimizes radio resources.
- Creates an exportable WLAN profile that may be imported into an Alcatel WLAN Switch and used to configure and deploy the WLAN.

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

Unlike other static site survey tools that require administrators to have intricate knowledge of building materials and other potential radio frequency (RF) hazards, RF Plan calibrates coverage in real-time through a sophisticated RF calibration algorithm. This real-time calibration lets you characterize the indoor propagation of RF signals to determine the best channel and transmission power settings for each AP. You can program the calibration to occur automatically or you can manually launch the calibration at any time to quickly adapt to changes in the wireless environment.

Before You Begin

Before you use RF Plan, review the following steps to create a building model and plan the WLAN for the model.

Task Overview

1. Gather information about your building's dimensions and floor plan.
2. Determine the level of coverage you want for your APs and AMs.
3. Create a new building and add its dimensions.
4. Enter the parameters of your AP coverage.
5. Enter the parameters of your AM coverage.
6. Add floors to your building and import the floor plans.
7. Define special areas.
8. Generate suggested AP and AM tables by executing the AP/AM Plan features.

Planning Requirements

You should collect the following information before using RF Plan. Having this information readily available will expedite your planning efforts.

- Building dimensions
- Number of floors
- Distance between floors
- Number of users and number of users per AP
- Radio type(s)
- Overlap Factor
- Desired data rates for APs
- Desired monitoring rates for AMs
- Areas of your building(s) that you do not necessarily want coverage
- Areas of your building(s) where you do not want or cannot deploy an AP or AM
- Any area where you want to deploy a fixed AP or AM

Use the following worksheets to collect your information:

Building Dimensions	
Height:	Width:
Number of Floors:	

User Information	
Number of Users:	Users per AP:
Radio Types:	
Overlap Factor:	

AP Desired Rates	
802.11blg:	802.11a:
AM Desired Rates	
802.11blg:	802.11a:

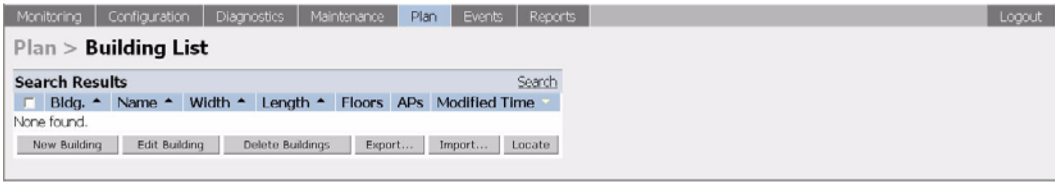
Don't Care/Don't Deploy Areas

Using RF Plan

This section describes how to use RF Plan and how to enter information in RF Plan pages.

To start RF Plan from the WebUI, click the **Plan** tab in the WebUI menu bar.

When you start RF Plan, the browser window shows the Building List page.



Plan > **Building List**

Search Results

☐	Bldg.	Name	Width	Length	Floors	APs	Modified Time

None found.

Building List Page

The Building List is the first page you see when you start RF Plan. This list contains all the buildings you have defined using the RF Plan software. The first time you run the application, there are no buildings in the list.

You may add, edit, and delete buildings using this page. You may also import and export building information. This page includes the following buttons:

New Building
Use this button to create a new building. When you add or edit a building, you can access other RF Plan pages.

Edit Buildings
Use this button to edit existing buildings in the building list. To edit a building, select the checkbox next to the building ID, then click **Edit Building**. When you add or edit a building, you can access other RF Plan pages.

Delete Buildings
Use this button to delete existing buildings in the building list. To delete a building, select the checkbox next to the building ID, then click **Delete Building**.

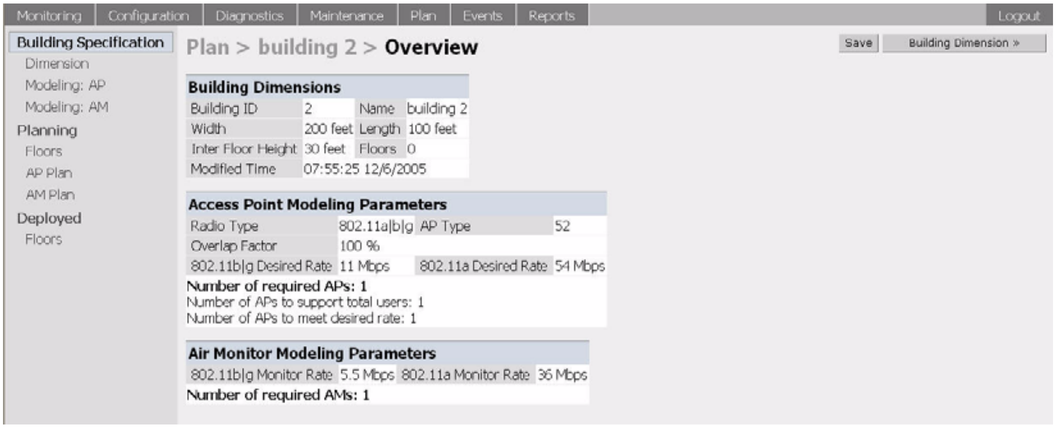
Export
Use this button to export a database file with all the specifications and background images of one or more selected buildings in the building list. See "Exporting and Importing Files" on page 54.

Import
Use this button to import database files that define buildings into the RF Plan building list. See "Exporting and Importing Files" on page 54.

Locate
Use this button to find a building.

Building Specifications Overview Page

The Building Specification Overview page shows the default values for a building that you are adding or the current values for a building that you are modifying.



Plan > building 2 > **Overview**

Building Dimensions

Building ID	2	Name	building 2
Width	200 feet	Length	100 feet
Inter Floor Height	30 feet	Floors	0
Modified Time	07:55:25 12/6/2005		

Access Point Modeling Parameters

Radio Type	802.11a|b|g	AP Type	52
Overlap Factor	100 %		
802.11b|g Desired Rate	11 Mbps	802.11a Desired Rate	54 Mbps

Number of required APs: 1
Number of APs to support total users: 1
Number of APs to meet desired rate: 1

Air Monitor Modeling Parameters

802.11b|g Monitor Rate	5.5 Mbps	802.11a Monitor Rate	36 Mbps

Number of required AMs: 1

The Overview page includes the following:

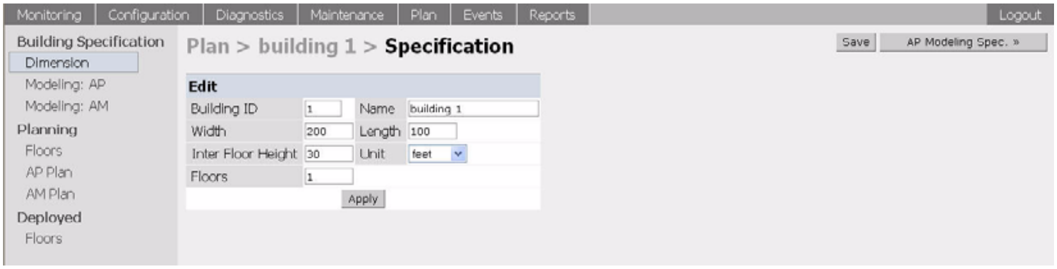
- Building Dimensions: Your building's name and dimensions
- Access Point Modeling Parameters
- Air Monitor Modeling Parameters
- **Building Dimensions** button (in the upper right-hand portion of the page). Click on this button to edit the building dimensions settings.

When you create or edit information for a building, there are several ways you can navigate through RF Plan pages:

- The navigation pane on the left side of the browser window displays RF Plan pages in the order in which they should be accessed when you are creating a new building. If you are editing a building, simply click on the page you want to display or modify.
- A button for the next page appears in the upper right-hand portion of the page. You can click on this button to display the next page. For example, the **Building Dimensions** button appears in the Building Specifications Overview page.
- Clicking **Apply** on editable pages sequences you to the next page. For example, when you click **Apply** in the Building Dimensions page, the AP Modeling Parameters page displays.

Building Dimension Page

The Building Dimension page allows you to specify the name and identification for the building and its dimensions.



Plan > building 1 > Specification

Edit

Building ID	1	Name	building 1
Width	200	Length	100
Inter Floor Height	30	Unit	feet
Floors	1		

Enter the following information:

Building ID — The valid range for this field is any integer from 1 to 255.

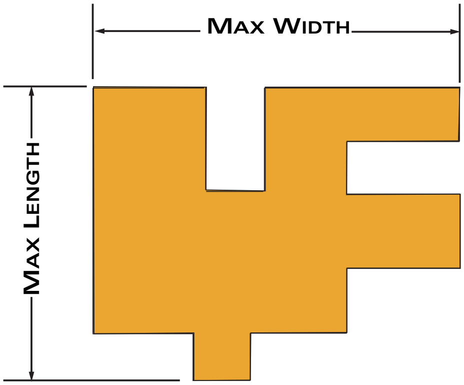
Building Name — The Building Name is an alphanumeric string up to 64 characters in length.

Width and Length

Enter the rectangular exterior dimensions of the building.

The valid range for this field is any integer from 1 to a value corresponding to $1x10^{12}$.

If your building has an irregular shape, the width and length should represent the maximum width and length of the overall footprint of the building as seen from above. For example:



When width and length are specified, RF Plan creates a rectangular area in the Planning feature pages that represent the overall area covered by the building. You need to import an appropriate background image (see "Floor Editor Dialog Box" on page 46.) to aid you in defining areas that don't require coverage or areas in which you do not wish to deploy APs and AMs (see "Area Editor Dialog Box" on page 47).

Inter-Floor Height

This is the distance between floor surfaces in the building.

The valid range for this field is any integer from 1 to a value corresponding to $1x10^{12}$.

NOTE: This is ***not*** the distance from floor to ceiling. Some buildings have a large space between the interior ceilings and the floor above.

Floors

Enter the number of floors in your building here.

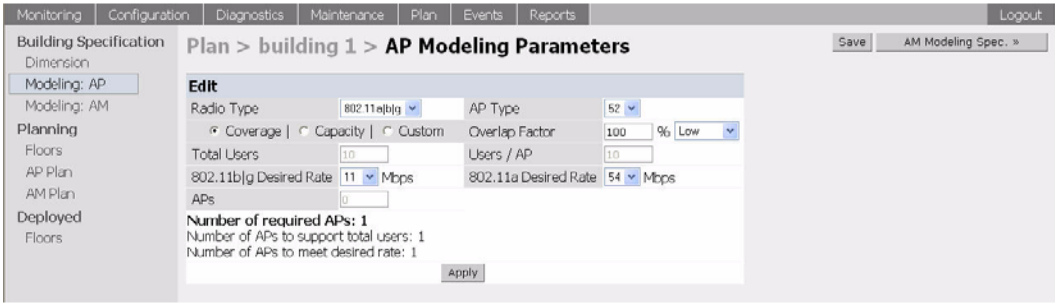
The valid range for this field is any integer from 1 to a value corresponding to $1x10^{12}$.

Unit

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

AP Modeling Parameters Page

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



Plan > building 1 > **AP Modeling Parameters**

Edit

Radio Type	802.11a|b|g	AP Type	52
● Coverage | ○ Capacity | ○ Custom		Overlap Factor	100 % Low
Total Users	10	Users / AP	10
802.11b|g Desired Rate	11 Mbps	802.11a Desired Rate	54 Mbps
APs	0		

Number of required APs: 1
Number of APs to support total users: 1
Number of APs to meet desired rate: 1

Controls on this page allow you to select or control the following functions, which are described in further detail in this section:

Radio Type Use this pull-down menu to specify the radio type.

AP Type Use this drop box to select the Alcatel AP model.

Overlap Factor Use this field and pull-down to specify an overlap factor.

Design Model Use these radio buttons to specify a design model to use in the placement of APs.

Users Use this field to specify the number of users on your WLAN.

Rates Use this pull-down to specify the data rates desired on APs.

Radio Type

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

801.11a 5GHz, Orthogonal Frequency Division Multiplexing (OFDM) with data rates up to 54Mbps.

802.11b 2.4GHz, Direct Spread Spectrum (DSSS) multiplexing with data rates up to 11Mbps.

802.11g 2.4GHZ, OFDM/CCK (Complementary Code Keying) with data rates up to 54Mbps.

Overlap Factor

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

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

Design Model

Three radio buttons on the page allow you to control the kind of model used to determine the number and type of APs:

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

Capacity Use this option to let RF Plan determine the number of APs based on the total number of users, ratio of users to APs, and desired data rates.

Custom Use this option to specify a fixed number of APs.

The desired rate is selectable from 1 to 54 Mbps in both the Coverage and Capacity models.

Users

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

Enter the number of users you expect to have on your WLAN in the Users text box. Enter the number of users per AP you expect in the Users/AP text box.

The numbers entered in the these two text boxes must be non-zero integers between 1-255 inclusive.

Rates

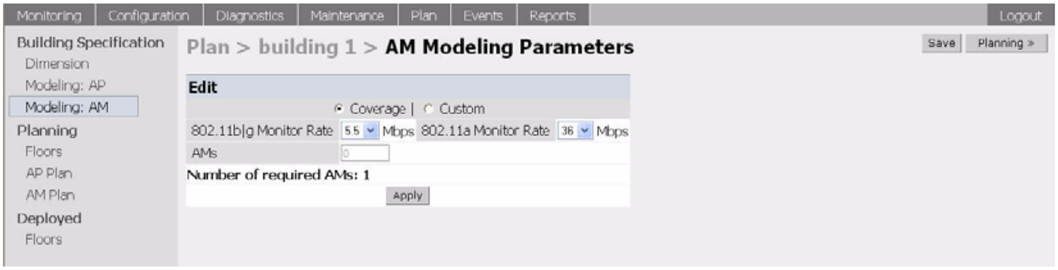
NOTE: The Rate pull-down menus are active only when the Coverage or Capacity design models are selected.

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

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

AM Modeling Page

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



Plan > building 1 > **AM Modeling Parameters**

Edit

● Coverage | ○ Custom

802.11b|g Monitor Rate 5.5 Mbps 802.11a Monitor Rate 36 Mbps

AMs 0

Number of required AMs: 1

Controls on this page allow you to select the following functions, which are described in more detail in this section:

Design Model
Use these radio buttons to specify a design model to use in the placement of AMs.

Monitor Rate
Use this pull-down menu to specify the desired monitor rate for the AMs.

AMs
Use this field to manually specify the number of AMs to deploy (Custom Model only).

Design Models

Two radio buttons on the page allow you to specify the model used to determine the number and type of APs.

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

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

Custom
Use this option to specify a fixed number of AMs. When the AM Plan portion of RF Plan is executed, RF Plan distributes the AMs evenly.

NOTE: The monitor rates you select for the AMs should be less than the data rates you selected for the APs. If you set the rate for the AMs at a value equal to that specified for the corresponding PHY type AP, RF Plan allocates one AM per AP. If you specify a monitor rate greater than the data rate, RF Plan allocates more than one AM per AP.

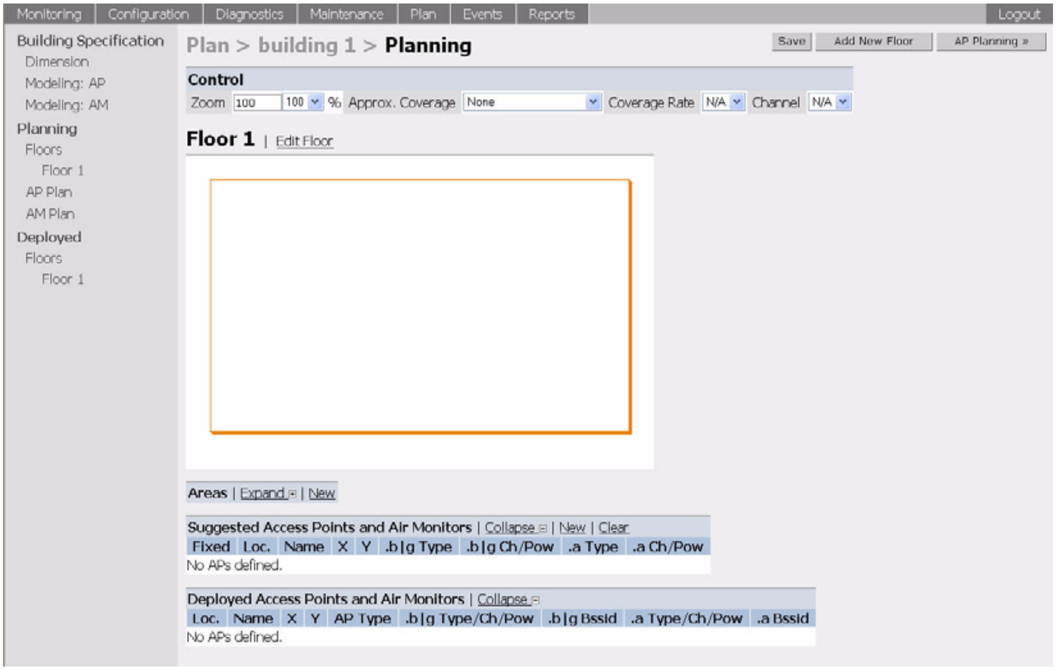
Monitor Rates

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

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

Planning Floors Pages

The Planning Floors page enables you to see the footprint of your floors.



Plan > building 1 > Planning

Control

Zoom 100 100 % Approx. Coverage None Coverage Rate N/A Channel N/A

Floor 1 | Edit Floor

Suggested Access Points and Air Monitors | Collapse | New | Clear

Fixed	Loc.	Name	X	Y	.b|g Type	.b|g Ch/Pow	.a Type	.a Ch/Pow

No APs defined.

Deployed Access Points and Air Monitors | Collapse

Loc.	Name	X	Y	AP Type	.b|g Type/Ch/Pow	.b|g Bssid	.a Type/Ch/Pow	.a Bssid

No APs defined.

You can select or adjust the following features, which are described in more detail in this section:

Zoom
Use this pull-down menu or type a zoom factor in the text field to increase or decrease the size of the displayed floor area.

Approximate Coverage Map (select radio type)
Use this pull-down to select a particular radio type for which to show estimated coverage.

Coverage Rate
Use this pull-down to modify the coverage areas based on a different data rate.

Edit Floor
Click on this link to launch the Floor Editor dialog box. See "Floor Editor Dialog Box" on page 46.

New in Areas section	Click on this link to launch the Area Editor dialog box. See "Area Editor Dialog Box" on page 47.
New in Suggested Access Points and Air Monitors section	Click on this link to launch the Suggested Access Point Editor dialog box. See "Access Editor Page" on page 49.

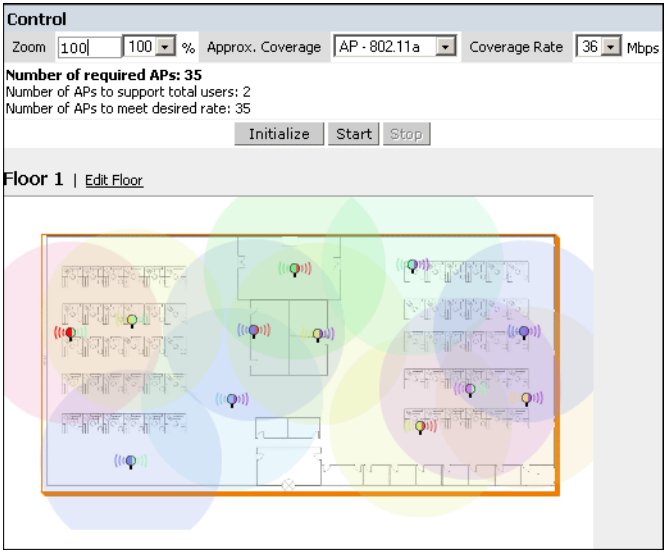
Zoom

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

Coverage

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

NOTE: You will not see coverage areas displayed here until you have executed either an AP Plan or an AM Plan.



Control

Zoom 100 100 % Approx. Coverage AP - 802.11a Coverage Rate 36 Mbps

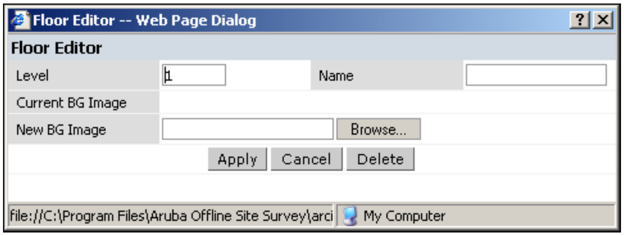
Number of required APs: 35
Number of APs to support total users: 2
Number of APs to meet desired rate: 35

Coverage Rate

Adjusting the coverage rate also affects the size of the coverage areas for AMs. Adjusting the rate values help you to understand how the coverage works in your proposed building.

Floor Editor Dialog Box

The Floor Editor dialog box allows you to specify the background image, and name the floor. The Floor Editor is accessible from the Floors Page by clicking on the **Edit Floor** link.



Floor Editor -- Web Page Dialog

Floor Editor

Level	1	Name	
Current BG Image			
New BG Image	Browse...		

Naming

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

Background Images

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

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

- File Type and Size

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

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

- Image Scaling

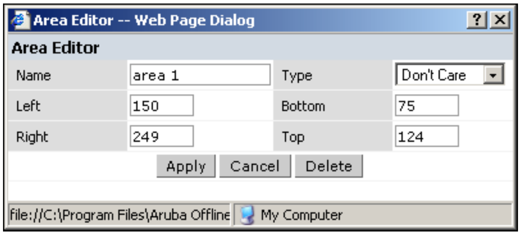
  Images are scaled (stretched) to fit the display area. The display area aspect ratio is determined by the building dimensions specified on the Dimension page.

Area Editor Dialog Box

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

Open the Area Editor dialog box by clicking **New** in the Areas section.

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



Area Editor -- Web Page Dialog

Area Editor

Name	area 1	Type	Don't Care
Left	150	Bottom	75
Right	249	Top	124

Naming

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

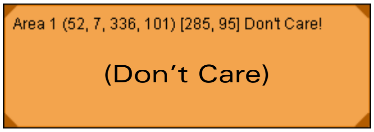
Locating and Sizing

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

NOTE: The location is zero-based. Values range from 0 to (height - 1 and width - 1). For example: If you defined your building to be 200 feet wide and 400 feet long, the coordinates of the upper right-hand corner would be (199, 399).

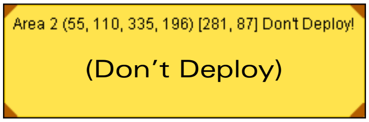
You may also use the drag and drop feature of the Area Editor to drag your area to where you want it and resize it by dragging one or more of the handles displayed in the corners of the area.

Don't Care areas are displayed as orange rectangles and Don't Deploy areas are displayed as yellow



Area 1 (52, 7, 336, 101) [285, 95] Don't Care!

(Don't Care)

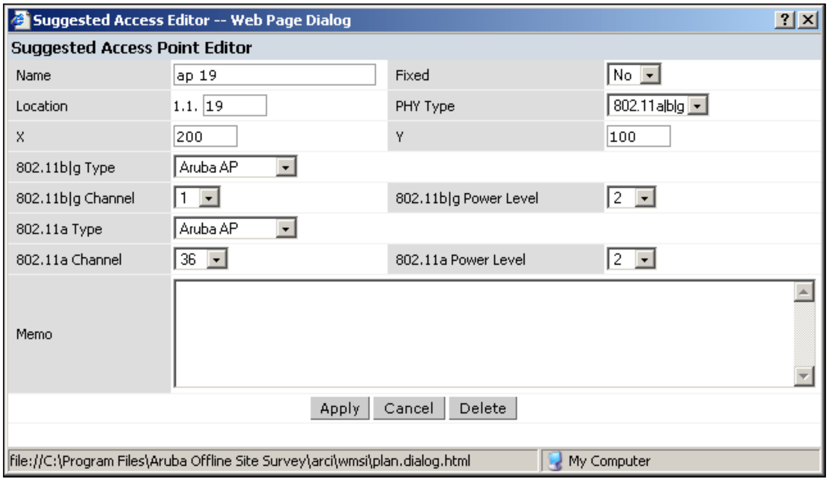


Area 2 (55, 110, 335, 196) [281, 87] Don't Deploy!

(Don't Deploy)

Access Editor Page

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



Suggested Access Editor -- Web Page Dialog

Suggested Access Point Editor

Name	ap 19	Fixed	No
Location	1.1. 19	PHY Type	802.11a|b|g
X	200	Y	100
802.11b|g Type	Aruba AP		
802.11b|g Channel	1	802.11b|g Power Level	2
802.11a Type	Aruba AP		
802.11a Channel	36	802.11a Power Level	2
Memo			

file://C:\Program Files\Aruba Offline Site Survey\arci\wmsi\plan.dialog.html

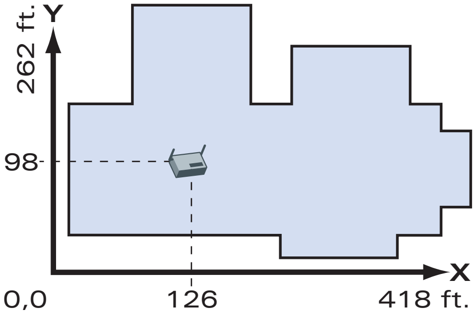
Naming

RF Plan automatically names APs using the default convention `ap` *number*, where *number* starts at 1 and increments by one for each new AP. When you manually create an AP, the new AP is assigned the next number and is added to the bottom of the suggested AP list.

You may name an AP anything you wish. The name must consist of alphanumeric characters and be 64 characters or less in length.

X and Y Coordinates

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



Fixed

Fixed APs do not move when RF Plan executes the positioning algorithm.

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

Choose Yes or No from the drop-down menu. Choosing Yes locks the position of the AP as it is shown in the coordinate boxes of the Access Editor. Choosing No allows RF Plan to move the AP as necessary to achieve best performance.

PHY Types

The PHY Type drop-down menu allows you to specify what radio mode the AP uses. You can choose from one of the following:

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

802.11 Types

The 802.11 b/g and 802.11a Type drop-down menus allow you to choose the mode of operation for the AP. You may choose to set the mode of operation to Access Point or Air Monitor.

802.11 Channels

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

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

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

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

802.11 Power Levels

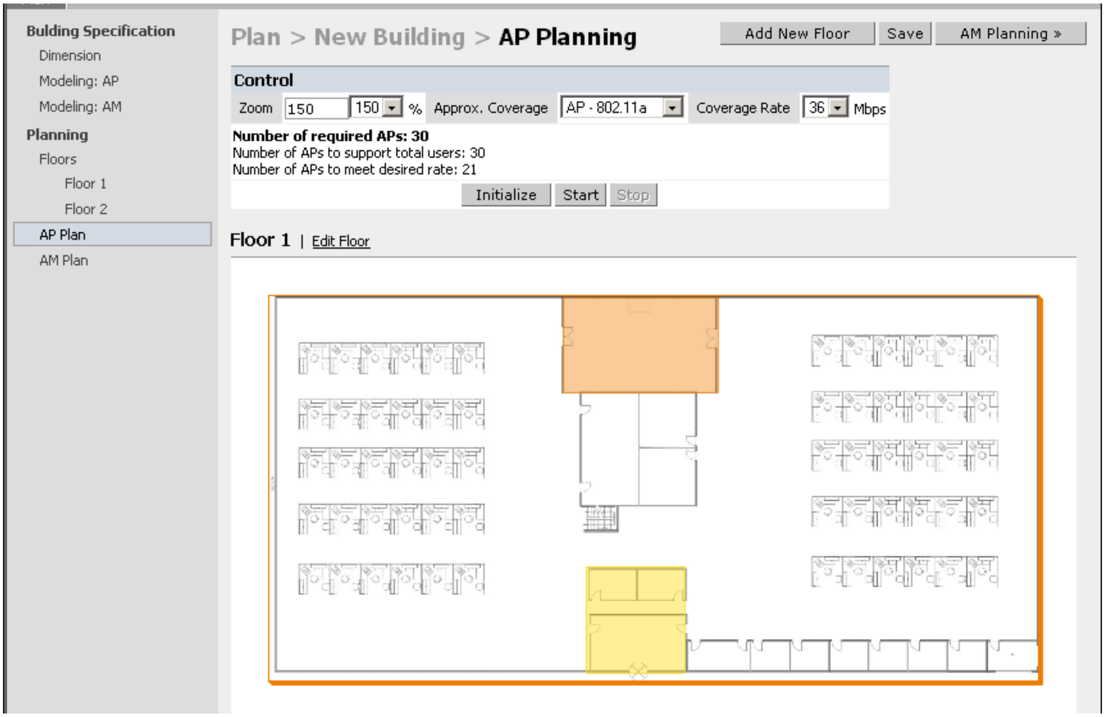
The power level drop-down menus allow you to specify the transmission power of the AP. Choices are OFF, 0, 1, 2, 3, and 4. A setting of 4 applies the maximum Effective Isotropic Radiated Power (EIRP) allowed in the regulatory domain (country) in which you are operating the AP.

Memo

The Memo text field allows you to enter notes regarding the AP. You can enter a maximum of 256 alphanumeric characters in the Memo field.

AP Plan Page

The AP Plan page uses the information entered in the modeling pages to locate APs in the building(s) you described.



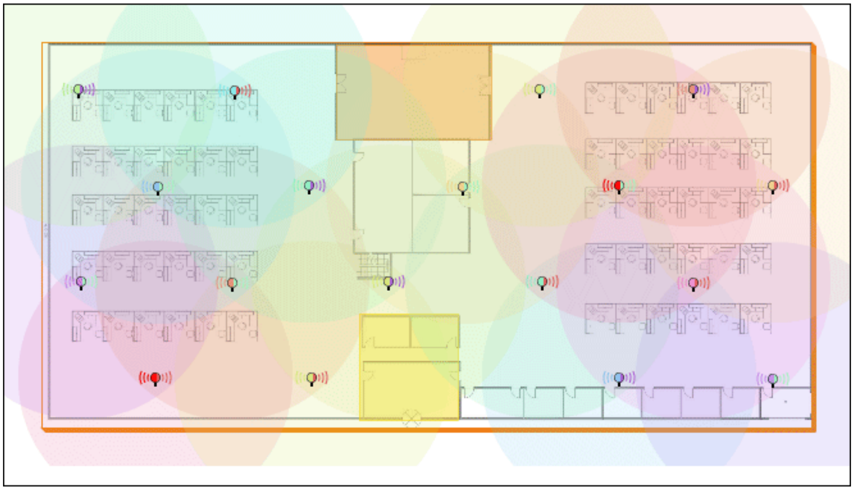
Zoom 150 150 % Approx. Coverage AP - 802.11a Coverage Rate 36 Mbps

Number of required APs: 30
Number of APs to support total users: 30
Number of APs to meet desired rate: 21

Initialize

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

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



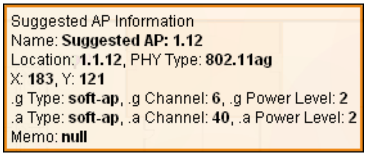
Start

Click **Start** to launch the optimizing algorithm. The AP symbols move on the page as RF Plan finds the optimum location for each.

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

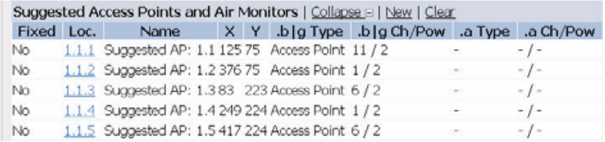
Viewing the Results

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



Suggested AP Information
Name: **Suggested AP: 1.12**
Location: **1.1.12**, PHY Type: **802.11ag**
X: **183**, Y: **121**
.g Type: **soft-ap**, .g Channel: **6**, .g Power Level: **2**
.a Type: **soft-ap**, .a Channel: **40**, .a Power Level: **2**
Memo: **null**

The Suggested Access Points and Air Monitors table lists the coordinates, power, location, power setting, and channel for each of the APs that are shown in the floor plan.



Suggested Access Points and Air Monitors | Collapse | New | Clear

Fixed	Loc.	Name	X	Y	.b|g Type	.b|g Ch/Pow	.a Type	.a Ch/Pow
No	1.1.1	Suggested AP: 1.1	125	75	Access Point	11 / 2	-	- / -
No	1.1.2	Suggested AP: 1.2	376	75	Access Point	1 / 2	-	- / -
No	1.1.3	Suggested AP: 1.3	83	223	Access Point	6 / 2	-	- / -
No	1.1.4	Suggested AP: 1.4	249	224	Access Point	1 / 2	-	- / -
No	1.1.5	Suggested AP: 1.5	417	224	Access Point	6 / 2	-	- / -

AM Plan Page

The AM Plan page calculates the optimum placement for the AMs.

Initialize

Initialize the Algorithm by clicking **Initialize**. This makes an initial placement of the AMs and prepares RF Plan for the task of determining the optimum location for each of the AMs. When you click **Initialize**, the AM symbols appear on the floor plan.

Start

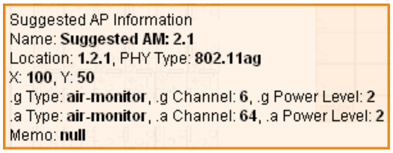
Click **Start** to launch the optimizing algorithm. The AM symbols move on the page as RF Plan finds the optimum location for each.

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

Viewing the Results

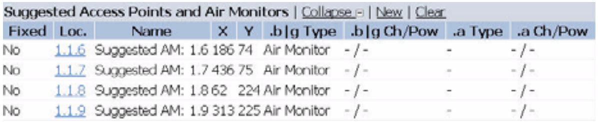
Viewing the results of the AM Plan feature is similar to that for the AP Plan feature.

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



Suggested AP Information
Name: **Suggested AM: 2.1**
Location: **1.2.1**, PHY Type: **802.11ag**
X: **100**, Y: **50**
.g Type: **air-monitor**, .g Channel: **6**, .g Power Level: **2**
.a Type: **air-monitor**, .a Channel: **64**, .a Power Level: **2**
Memo: **null**

The Suggested Access Points and Air Monitors table lists the coordinates, power, location, power setting, and channel for each of the AMs that are shown in the floor plan.



Suggested Access Points and Air Monitors | Collapse ⊟ | New | Clear

Fixed	Loc.	Name	X	Y	.b|g Type	.b|g Ch/Pow	.a Type	.a Ch/Pow
No	1.1.6	Suggested AM: 1.6	186	74	Air Monitor	- / -	-	- / -
No	1.1.7	Suggested AM: 1.7	436	75	Air Monitor	- / -	-	- / -
No	1.1.8	Suggested AM: 1.8	62	224	Air Monitor	- / -	-	- / -
No	1.1.9	Suggested AM: 1.9	313	225	Air Monitor	- / -	-	- / -

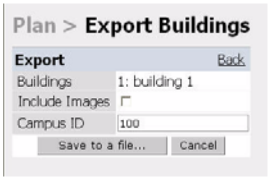
Exporting and Importing Files

The **Export** and **Import** buttons on the Building List page allow you to export and import files that define the parameters of your buildings. You can export a file so that it may be imported into and used to automatically configure an Alcatel WLAN Switch. On an Alcatel WLAN Switch, you can import a file that has been exported from another WLAN Switch or from the standalone version of RF Plan that runs as a Windows application.

The files that you export and import are XML files and, depending on how many floors are in your buildings and how many background images you have for your floors, the XML files may be quite large. (See "Background Images" on page 47.)

Export Buildings Page

To export a file that defines the parameters of one or more buildings, select the building(s) to be exported in the Building List page and then click **Export**.



Plan > **Export Buildings**

Export	Back
Buildings	1: building 1
Include Images	□
Campus ID	100

When exporting a building file Alcatel recommends that you select the **Include Images** checkbox.

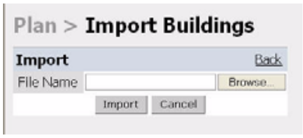
When you click the **Save to a file...** button, you are prompted for the location and name for the exported file. When naming your exported file, be sure to give the file the *.XML* file extension, for example, *My_Building.XML.*

Import Buildings Page

You can import only XML files exported from another Alcatel WLAN Switch or from the standalone version of RF Plan that runs as a Windows application.

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

To import a file that defines the parameters of one or more buildings, click the **Import** button in the Building List page.



In the Import Buildings page, click **Browse** to select the file to be imported, then click the **Import** button.

Locate

The **Locate** button on the Building List page allows you to search for APs, AMs, etc. on a building by building basis. To use this feature, select the building in which you want to search, and click **Locate**.

The Deployed Access Points and Air Monitors table displays information on each of these devices. To add a device, click **Add Device**. To delete a device, click **Remove Device**. To select a device, click **Choose Devices**.

RF Plan Example

This section guides you through the process of creating a building and populating it with APs and AMs using RF Plan.

NOTE: This section uses example floor plans that are provided with the Windows application version of RF Plan.

Sample Building

The following planning table shows the information to be used in this example.

Building Dimensions	
Height: *100*	Width: *100*
Number of Floors: *2*	

User Information	
Number of Users:	Users per AP: *N/A*
Radio Types: *a, b, g*	
Overlap Factor: *Medium (150%)*	

AP Desired Rates	
802.11blg: *48 Mbps*	802.11a: *48 Mbps*
AM Desired Rates	
802.11blg: *24*	802.11a: *24*

Don’t Care/Deploy Areas
Shipping & Receiving = Don’t Care
Lobby = Don’t Deploy

Create a Building

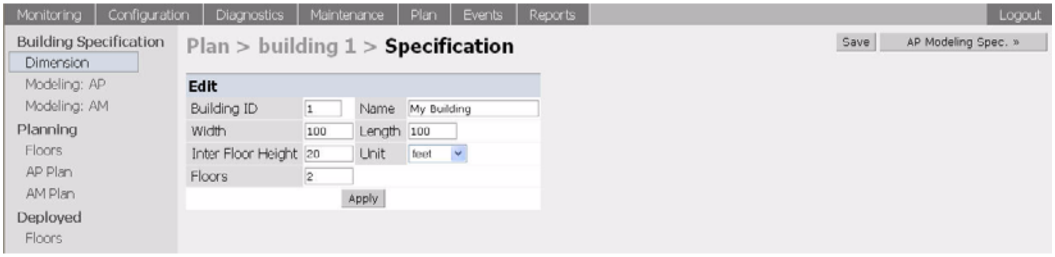
In this section you create a building using the information supplied in the planning table.

1. Click **New Building**.

   The Overview page appears.

2. Click **Save**.
3. Click **Building Dimension**.

The Specification page appears.



Plan > building 1 > **Specification**

Edit

Building ID	1	Name	My Building
Width	100	Length	100
Inter Floor Height	20	Unit	feet
Floors	2		

4. Enter the following information in the text boxes.

Text Box	**Information**
Building ID	1
Building Name	My Building
Width	100
Length	100
Inter Floor Height	20
Units	Feet
Floors	2

5. Click **Save**.
6. Click **Apply**.

   Notice that when you click **Apply**, RF Plan automatically moves to the next page in the list. In this case RF Plan moves to the AP Modeling Parameters page.

Model the Access Points

You now determine how many APs are required to cover your building with a specified data transfer rate and overlap.

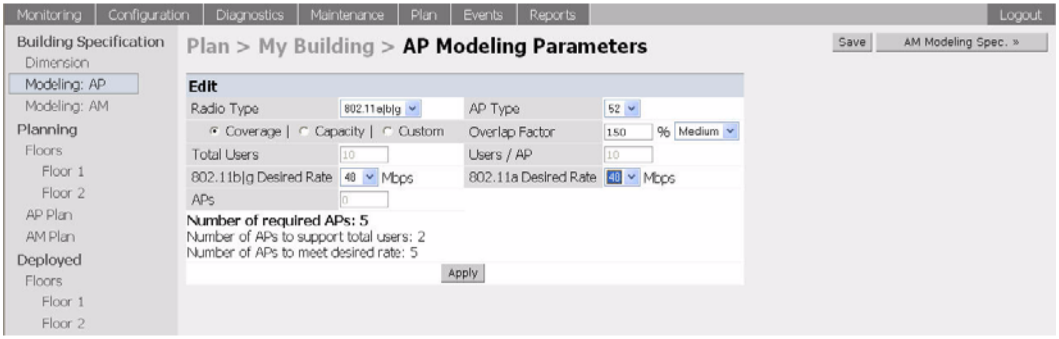
In this example, you use the Coverage Model. The following are assumed about the performance of the WLAN:

- Radio Types: a/b/g
- Overlap factor: Medium (150%)
- 802.11a desired rate: 48 Mbps
- 802.11b desired rate: 48 Mbps

1. Select **801.11 a|b|g** from the Radio Type drop-down menu.
2. Select **Medium** from the Overlap Factor drop-down menu.

   Notice that the percentage show at the left of the drop-down menu changes to 150%.
3. Select **48** from the 802.11 b|g Desired Rate drop-down menu.
4. Select **48** from the 801.11 a Desired Rate drop-down menu.

   Notice that the number of required APs has changed to 5.



Plan > My Building > **AP Modeling Parameters**

Edit

Radio Type	802.11a|b|g	AP Type	52
● Coverage | ○ Capacity | ○ Custom		Overlap Factor	150 % Medium
Total Users	10	Users / AP	10
802.11b|g Desired Rate	48 Mbps	802.11a Desired Rate	48 Mbps
APs	0		

Number of required APs: 5
Number of APs to support total users: 2
Number of APs to meet desired rate: 5

5. Click **Save**, then **Apply**.

   RF Plan moves to the AM Modeling Parameters page.

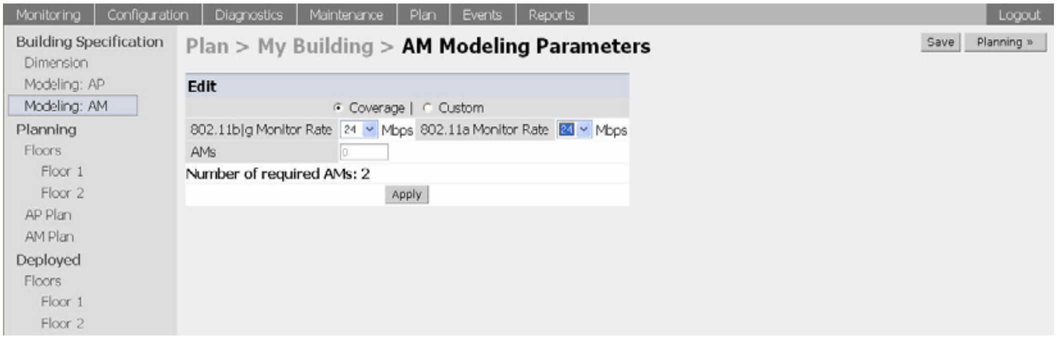
Model the Air Monitors

You now determine how many AMs are required to provide a specified monitoring rate. In this example you continue to use the Coverage Model and make the following assumptions:

- 802.11 b|g monitor rate: 48 Mbps
- 802.11 a monitor rate: 48 Mbps

1. Select **24** from the 802.11 b|g Monitor Rate drop-down menu.
2. Select **24** from the 802.11 a Monitor Rate drop-down menu.

Notice that the number of required AMs is now 2.



Plan > My Building > **AM Modeling Parameters**

Edit

● Coverage | ○ Custom

802.11b|g Monitor Rate 24 Mbps 802.11a Monitor Rate 24 Mbps

AMs 0

Number of required AMs: 2

3. Click **Save**, then **Apply**.

   RF Plan moves to the Planning page.

Add and Edit a Floor

You now add floor plans to your floors. In this section you:

- Add a background image floor plan for each floor
- Name the floors

NOTE: This section uses example floor plans that are provided with the Windows application version of RF Plan.

To add the background image and name the first floor:

1. In the Planning page, click the **Edit Floor** link at the right of the Floor 1 indicator.
2. Type **`Entrance Level`** in the Name box of the Floor Editor Dialog.
3. Use the Browse button to locate the background image for the 1st floor.

   The file is located in the following directory:

   `C:\Program Files\Alcatel RF Plan\Tutorial\tutorial floor 1.jpg`
4. Click **Apply**.

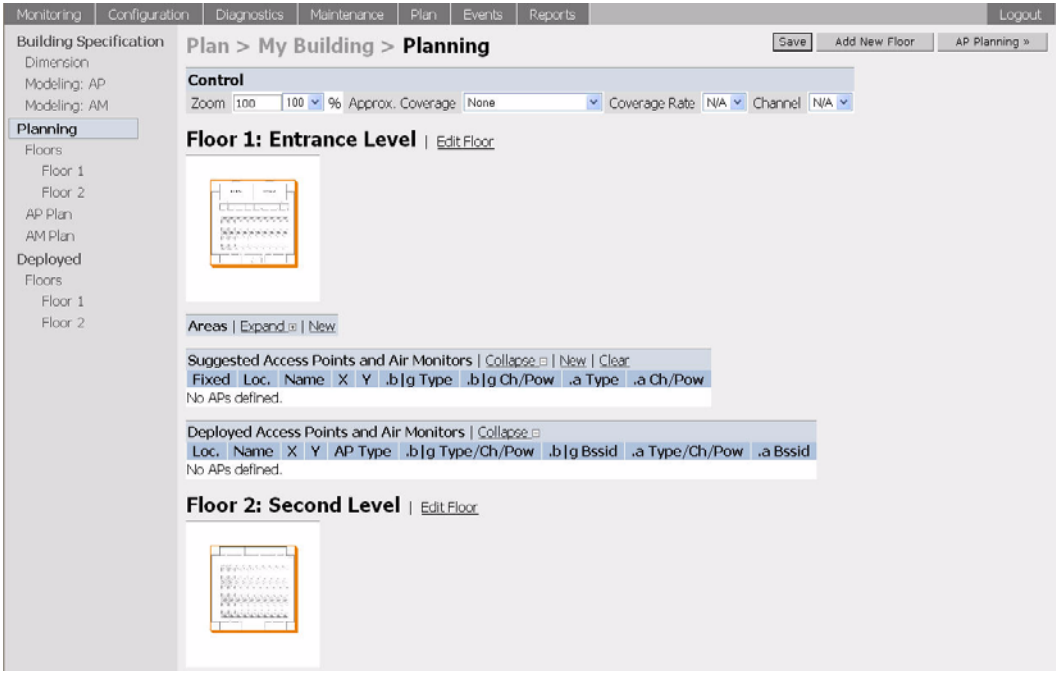
To add the background image and name the second floor:

1. Click the **Edit Floor** link at the right of the Floor 2 indicator.
2. Type **`Second Level`** in the Name box of the Floor Editor Dialog.
3. Use the Browse button to locate the background image for the 1st floor.

   The file is located in the following directory:

```
C:\Program Files\Alcatel RF Plan\Tutorial\tutorial floor 2.jpg
```

4. Click **Apply**.
5. Click **Save** on the Planning page.



Plan > My Building > **Planning**

Control

Zoom 100 100 % Approx. Coverage None Coverage Rate N/A Channel N/A

Floor 1: Entrance Level | Edit Floor

Areas | Expand ⊞ | New

Suggested Access Points and Air Monitors | Collapse ⊟ | New | Clear

Fixed	Loc.	Name	X	Y	.b|g Type	.b|g Ch/Pow	.a Type	.a Ch/Pow

No APs defined.

Deployed Access Points and Air Monitors | Collapse ⊟

Loc.	Name	X	Y	AP Type	.b|g Type/Ch/Pow	.b|g Bssid	.a Type/Ch/Pow	.a Bssid

No APs defined.

Floor 2: Second Level | Edit Floor

Defining Areas

Before you advance to the AP and AM Planning pages you want to define special areas. In this section you define areas where you do not want to physically deploy an AP, or where you do not care if there is coverage or not.

This step assumes the following:

- We do not care if we have coverage in the Shipping and Receiving areas
- We do not want to deploy APs or AMs in the Lobby Area

Create a Don’t Care Area

To create a Don’t Care area:

1. Click on AP Plan in the Feature Tree at the left side of the browser window.

NOTE: You can zoom in on the floor plan using the Zoom pull-down near the top of the AP Planning page, or type a zoom value in the text box at the left of the pull-down and press the enter key on your keyboard. For example, enter a zoom factor of 400.

2. In the Planning page, click the **New** link in the Areas section under Floor 1.

   This opens the Area Editor.

3. Type **`Shipping and Receiving`** in the Name text box in the Area Editor.
4. Select **Don't Care** from the Type pull-down menu box.
5. Click **Apply**.

   Notice that an orange box appears near the center of the floor plan.

6. Use your mouse (or other pointing device) to place the cursor over the box.

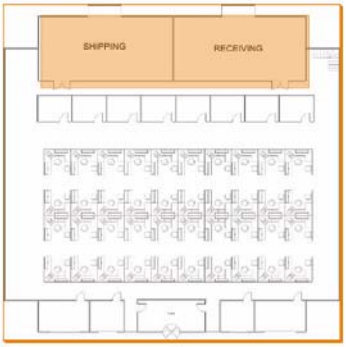
   Notice that the information you typed in the editor appears in the box. You see the name and type of area, as well as the coordinates of the lower left corner and upper right corner of the box.

   NOTE: The x = 0 and y = 0 coordinates correspond to the lower left corner of the layout space.

7. Using your mouse, left-click and drag the box over the Shipping and Receiving area.

   Drag one corner of the box to a corresponding corner of the Shipping and Receiving area and using one of the corner handles of the box, stretch it to fit exactly over the Shipping and Receiving area.

   Your floor plan with the **Don't Care** box should look similar to this:



8. Click **Save**.

Create a Don’t Deploy Area

To create a Don’t Deploy area:

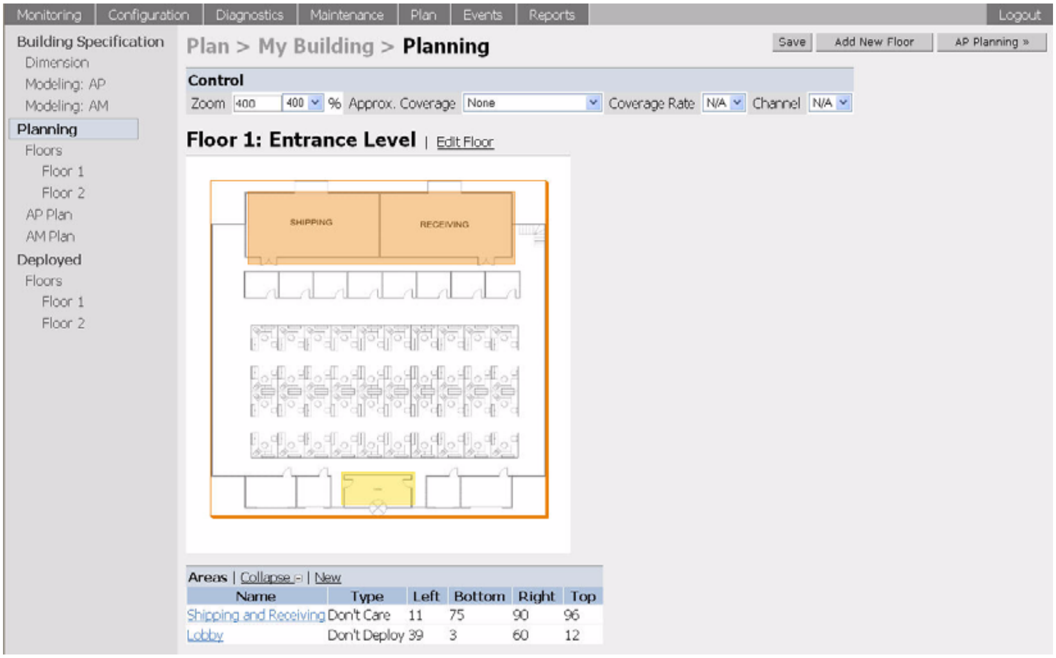
1. Click the **New** link in the Areas section under Floor 1 to open the Area Editor.
2. Type **Lobby** in the Name text box in the Area Editor.
3. Select **Don’t Deploy** from the Type pull-down menu box.
4. Click **Apply**.

   Notice that an yellow box appears near the center of the floor plan.
5. Use your mouse (or other pointing device) to place the cursor over the box.

   Notice that the information you typed in the editor appears in the box. You see the name and type of area, as well as the coordinates of the lower left corner and upper right corner of the box.

   NOTE: The x = 0 and y = 0 coordinates correspond to the lower left corner of the layout space.
6. Using your mouse, left-click and drag the box over the Lobby area on the floor plan.
7. Drag one corner of the box to a corresponding corner of the lobby and using one of the corner handles of the box, stretch it to fit exactly over the lobby area.

Your floor plan with the Don’t Deploy box should look similar to this:



Plan > My Building > Planning

Control

Zoom 400 400 % Approx. Coverage None Coverage Rate N/A Channel N/A

Floor 1: Entrance Level | Edit Floor

Areas | Collapse | New

Name	Type	Left	Bottom	Right	Top
Shipping and Receiving	Don't Care	11	75	90	96
Lobby	Don't Deploy	39	3	60	12

8. Click **Save**.

9. When you are finished defining area in the Floors page, click **AP Planning** to advance to the next step in the process (the AP Plan page).

Running the AP Plan

In this section you run the algorithm that searches for the best place to put the APs.

You might want to zoom in on the floor plan. Zoom using the Zoom pull-down near the top of the AP Planning page, or type a zoom factor in the text box at the left of the pull-down and press the enter key on your keyboard.

Try entering a zoom factor of 400.

Notice that the number of required APs is 5, the same value that you saw when you modeled your APs above. Notice also that none of the APs show on the floor plan yet.

1. Click **Initialize**.

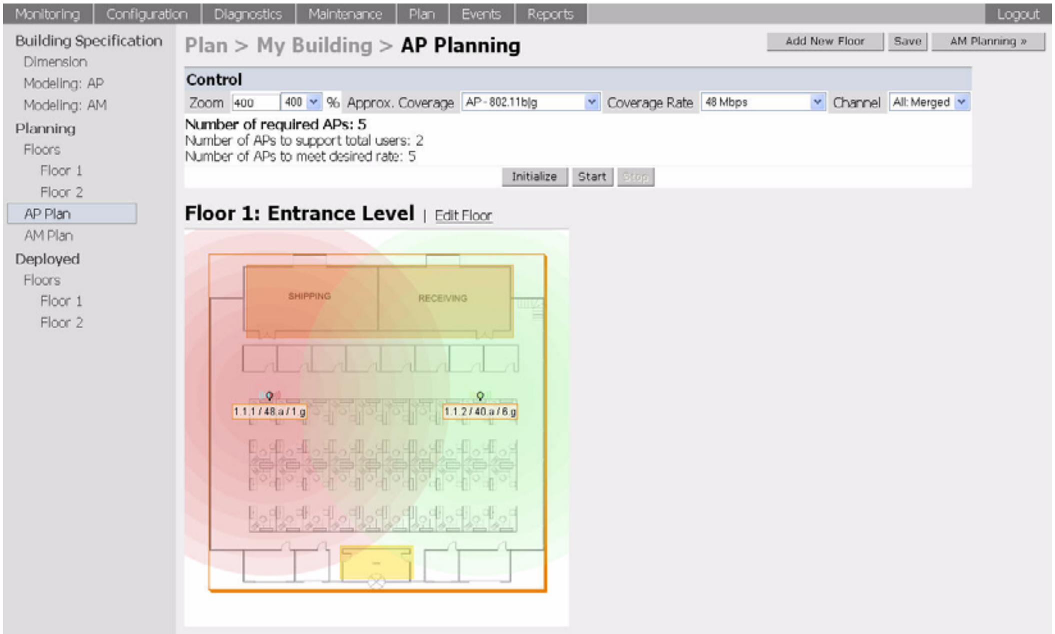
   You should see a total of five AP symbols appear on the two floor diagrams: three on Floor 1 and two on Floor 2. Also notice that the Suggested Access Points tables below each floor diagram have been populated with information about the suggested APs for each corresponding floor.

2. Click **Start**.

After you Initialize the APs you must start the algorithm. The APs move around on the floor plans as the algorithm is running.

The algorithm stops when the movement is less than a threshold value calculated based on the number of APs. The threshold value may be seen in the status bar at the bottom of the browser window.

NOTE: To see the approximate coverage areas of each of the APs, select an AP type from the **Approx. Coverage** pull-down box and select a rate from the **Coverage Rate** pull-down box.



Plan > My Building > AP Planning

Control

Zoom 400 400 % Approx. Coverage AP - 802.11b|g Coverage Rate 48 Mbps Channel All: Merged

Number of required APs: 5
Number of APs to support total users: 2
Number of APs to meet desired rate: 5

Floor 1: Entrance Level

3. Click **Save**, then click **AM Planning**.

Running the AM Plan

Running the AM Plan algorithm is similar to running the AP Plan.

1. Click **Initialize** then **Start**.

The algorithm stops when the movement is less than a threshold value calculated based on the number of AMs. The threshold value may be seen in the status bar at the bottom of the browser window.

2. Click **Save**.

Configuring DHCP with Vendor-Specific Options

A

A standards-compliant DHCP server can be configured to return the host Alcatel WLAN Switch's IP address through the Vendor-Specific Option Code (option 43) in the DHCP reply. In the Alcatel OmniAccess system, this information can allow an Alcatel AP to automatically discover the IP address of a master WLAN Switch for its configuration and management.

This appendix describes how to configure vendor-specific option 43 on various DHCP servers.

Overview

DHCP servers are a popular way of configuring clients with basic networking information such as an IP address, a default gateway, network mast, DNS server, and so on. Most DHCP servers have the ability to also send a variety of optional information, including the Vendor-Specific Option Code, also called option 43.

Here is how option 43 works:

1. The DHCP client on an Alcatel AP adds an optional piece of information called the Vendor Class Identifier Code (option 60) to its DHCP request. The value of this code is **ArubaAP**.
2. The DHCP server sees the Vendor Class Identifier Code in the request and checks to see if it has option 43 configured. If it does, it sends the Vendor-Specific Option Code (option 43) to the client. The value of this option is the loopback address of the Alcatel master WLAN Switch.
3. The AP receives a response from the DHCP server and checks if option 43 is returned. If it is, the AP contacts the master WLAN Switch using the supplied IP address.

Windows-Based DHCP Server

Configuring a Microsoft Windows-based DHCP server to send option 43 to the DHCP client on an Alcatel AP consists of the following two tasks:

- Configuring Option 60
- Configuring Option 43

Configuring Option 60

This section describes how to configure the Vendor Class Identifier Code (option 60) on a Microsoft Windows-based DHCP server.

As mentioned in the overview section, option 60 identifies and associates a DHCP client with a particular vendor. Any DHCP server configured to take action based on a client's vendor ID should also have this option configured.

Since option 60 is not a predefined option on a Windows DHCP server, you must add it to the option list for the server.

To configure option 60 on the Windows DHCP server:

1. On the DHCP server, open the DHCP server administration tool by clicking Start > Administration Tools > DHCP.
2. Find your server and right-click on the scope to be configured under the server name. Select **Set Predefined Options**.
3. In the Predefined Options and Values dialog box, click the **Add** button.
4. In the Option Type dialog box, enter the following information:

Name	Alcatel Access Point
Data Type	String
Code	60
Description	Alcatel AP vendor class identifier

5. Click the **OK** button to save this information.
6. In the Predefined Options and Values dialog box, make sure 060 Alcatel Access Point is selected from the Option Name drop-down list.
7. In the Value field, enter the following information:

String	Alcatel Access Point

8. Click the **OK** button to save this information.

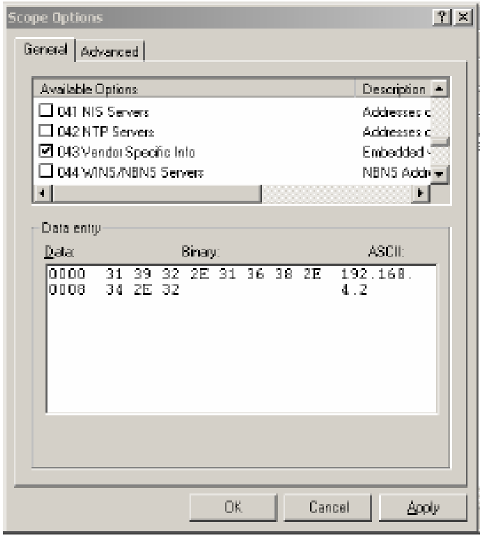
Configuring Option 43

Option 43 returns the IP address of the Alcatel master WLAN Switch to an Alcatel DHCP client. This information allows Alcatel APs to auto-discover the master WLAN Switch and obtain their configuration.

To configure option 43 on the Windows DHCP server:

1. On the DHCP server, open the DHCP server administration tool by clicking Start > Administration Tools > DHCP.
2. Find your server and right-click on the scope to be configured under the server name. Click on the Scope Options entry and select **Configure Options**.

3. In the Scope Options dialog box, scroll down and select 043 Vendor Specific Info.



Available Options	Description
☐ 041 NIS Servers	Addresses o
☐ 042 NTP Servers	Addresses o
☑ 043 Vendor Specific Info	Embedded
☐ 044 WINS/NBNS Servers	NBNS Addr

```
Data:       Binary:                      ASCII:
0000   31 39 32 2E 31 36 38 2E   192.168.
0008   34 2E 32                  4.2
```

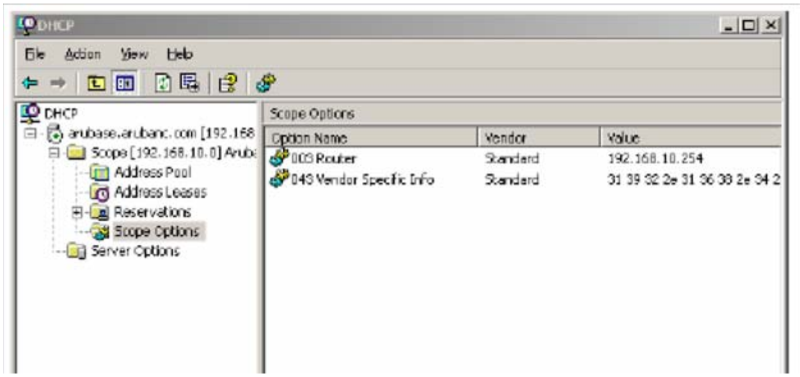
FIGURE A-1 Scope Options Dialog Box

4. In the Data Entry field, click anywhere in the area under the ASCII heading and enter the following information:

ASCII	*Loopback address of the master WLAN Switch*

5. Click the **OK** button to save the configuration.

   Option 43 is configured for this DHCP scope. Note that even though you entered the IP address in ASCII text, it displays in binary form.



Option Name	Vendor	Value
003 Router	Standard	192.168.10.254
043 Vendor Specific Info	Standard	31 39 32 2e 31 36 38 2e 34 2

FIGURE A-2 DHCP Scope Values

Linux DHCP Servers

The following is an example configuration for the Linux dhcpd.conf file:

NOTE: After you enter the configuration, you must restart the DHCP service.

```
option serverip code 43 = ip-address;
class "vendor-class" {
      match option vendor-class-identifier;
}
.
.
.
subnet 10.200.10.0 netmask 255.255.255.0 {
   default-lease-time 200;
   max-lease-time 200;
   option subnet-mask 255.255.255.0;
   option routers 10.200.10.1;
   option domain-name-servers 10.4.0.12;
   option domain-name "vlan10.aa.alcatel.com";
   subclass "vendor-class" "ArubaAP" {
      option vendor-class-identifier "ArubaAP";
      option serverip 10.200.10.10;
   }
   range 10.200.10.200 10.200.10.252;
}
```

Volume 3

Configuring WLANs

AOS-W User Guide

Release 2.5.3

ALCATEL

Copyright

Specifications in this manual are subject to change without notice.

Originated in the USA.

Trademarks

AOS-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 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

This preface includes the following information:

- An overview of the contents of 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

The *AOS-W User Guide* is now in eight separate volumes for easier download and information access. The volumes are as follows:

- Volume 1 contains an overview of the OmniAccess System.
- Volume 2 describes how to install the OmniAccess System in a wired network.
- Volume 3 (this volume) describes WLAN configuration, including remote Access Points.
- Volume 4 describes wireless encryption and authentication configuration.
- Volume 5 describes configuring multi-WLAN switch environments.
- Volume 6 describes intrusion prevention configuration.
- Volume 7 describes managing the OmniAccess System.
- Volume 8 describes configuring advanced services, such as Quality of Service (QoS) for voice and the External Services Interface module.

Related Documents

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

- *AOS-W User Guide*
- *Alcatel Wireless LAN Switch Installation Guides*

- *Alcatel Access Point Installation Guides*
- *Release Notes*

Text Conventions

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

TABLE 1 Text Conventions

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*>	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: # **send** <*text message*> 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 | Item B }	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Contacting Alcatel

Contact Center Online		
■	Main Site	http://www.alcatel.com/enterprise
■	Support Site	http://eservice.ind.alcatel.com
■	Email	support@ind.alcatel.com
Sales & Support Contact Center Telephone		
■	North America	1-800-995-2696
■	Latin America	1-877-919-9526
■	Europe	+33 (0) 38 85 56 92 9
■	Asia Pacific	+65 6586 1555
■	Worldwide	1-818-880-3500

Configuring WLANs 1

This chapter explains how to configure a wireless LAN (WLAN) using the Web interface. This chapter describes the following topics:

- "Before You Begin" on page 1.
- "Basic WLAN Configuration in the WebUI" on page 7.
- "Advanced WLAN Configuration in the WebUI" on page 13.
- "Adaptive Radio Management" on page 21

Before You Begin

This section describes tasks that you need to do prior to configuring a WLAN.

You have a wide variety of options for authentication, encryption, access management, and user rights when you configure a WLAN in the Alcatel OmniAccess system. However, you *must* configure the following basic elements:

- A Service Set Identifier (SSID) that uniquely identifies the WLAN.
- Layer-2 authentication to protect against unauthorized access to the WLAN. The authentication method you choose determines the following:
  - Layer-2 encryption to ensure the privacy and confidentiality of the data transmitted to and from the network.
  - Authentication server used to validate the user. In the Alcatel OmniAccess system, authentication can be performed using an external authentication server, such as a RADIUS server, or the WLAN Switch's internal database.
- Virtual local area network (VLAN) on the WLAN Switch into which wireless clients who successfully associate to the AP are placed.

Determine the Authentication Method

A user must authenticate to the Alcatel OmniAccess system in order to access WLAN resources. Table 1-1 describes the types of authentication that you can configure for a WLAN.

TABLE 1-1 Authentication Methods

None	(Also called open system authentication) This is the default authentication protocol. The client's identity, in the form of the Media Access Control (MAC) address of the wireless adapter in the wireless client, is passed to the WLAN Switch. Essentially any client requesting access to the WLAN is authenticated.
IEEE 802.1x	The IEEE 802.1x authentication standard allows for the use of keys that are dynamically generated on a per-user basic (as opposed to a static key that is the same on all devices in the network). **NOTE:** The 802.1x standard requires the use of a RADIUS authentication server. Most Lightweight Directory Access Protocol (LDAP) servers do *not* support 802.1x.
Wi-Fi Protected Access (WPA)	WPA implements most of the IEEE 802.11i standard. It is designed for use with an 802.1x authentication server (the Wi-Fi Alliance refers to this mode as WPA-Enterprise). WPA uses the Temporal Key Integrity Protocol (TKIP) to dynamically change keys and RC4 stream cipher to encrypt data.
WPA in pre-shared key (PSK) mode (WPA-PSK)	With WPA-PSK, all clients use the same key (the Wi-Fi Alliance refers to this mode as WPA-Personal). **NOTE:** In PSK mode, users must enter a passphrase from 8-63 characters to access the network. PSK is intended for home and small office networks where operating an 802.1x authentication server is not practical.
WPA2	WPA2 implements the full IEEE 802.11i standard. In addition to WPA features, WPA2 provides Counter Mode with Cipher Blocking Chaining Message Authentication Code Protocol (CCMP) for encryption which uses the Advanced Encryption Standard (AES) algorithm. (The Wi-Fi Alliance refers to this mode as WPA2-Enterprise.)
WPA2-PSK	WPA2-PSK is WPA2 used in PSK mode, where all clients use the same key. (The Wi-Fi Alliance refers to this mode as WPA2-Personal.)

TABLE 1-1 Authentication Methods (Continued)

xSec (Extreme Security)	(Requires installation of xSec software license) xSec is a Federal Information Processing Standard (FIPS)-certifiable Layer-2 encryption. xSec can encrypt and tunnel Layer-2 traffic between a WLAN Switch and wired and wireless clients, or between two Alcatel WLAN Switches. To use xSec encryption: ■ You must use a RADIUS authentication server. ■ If you are using xSec between two Alcatel WLAN Switches, you must install an xSec license in each device. ■ For encryption and tunneling of data between the client and WLAN Switch, you must install the Funk Odyssey client that supports xSec in the wired or wireless client. For more information, see the “Configuring xSec” chapter in Volume 4 of the *AOS-W User Guide*.
Captive Portal	Captive Portal allows users to authenticate using a web-based portal. Captive Portal users can be authenticated to an external authentication server or to the internal database on the WLAN Switch. Captive Portal authentication does not provide any type of data encryption beyond the SSL encryption used during the authentication. You can configure WEP encryption or WPA-PSK, or WPA2-PSK authentication in conjunction with Captive Portal.
VPN	Configures a VPN tunnel. Configuring this option requires user authentication against an external RADIUS server. You can configure VPN authentication in conjunction with WPA-PSK or WPA2-PSK authentication.
MAC	Allows the media access control (MAC) address of a device to be authenticated to an external authentication server or to the internal database on the WLAN Switch. You can configure MAC authentication in conjunction with WPA-PSK or WPA2-PSK authentication.

Encryption

The Layer-2 encryption depends upon the authentication method chosen (Table 1-2).

TABLE 1-2 Encryption Options by Authentication Method

Authentication Method	Encryption Option
None	Open (Null) or Static WEP
802.1x	Dynamic WEP
WPA or WPA-PSK	TKIP
WPA2, WPA2-PSK, or xSec	AES
Combination of WPA or WPA-PSK and WPA2 or WPA2-PSK	Mixed TKIP/AES

You can configure the following data encryption options for the WLAN:

Open (Null) No encryption is used and packets passing between the wireless client and WLAN Switch are in clear text.

Wired Equivalent Protocol (WEP) Defined by the original IEEE 802.11 standard, WEP uses the RC4 stream cipher with 40-bit and 128-bit encryption keys. The management and distribution of WEP keys is performed outside of the 802.11 protocol. There are two forms of WEP keys:

- Static WEP requires you to manually enter the key for each client and on the WLAN Switch.
- Dynamic WEP allows the keys to be automatically derived for each client for a specific authentication method during the authentication process. Dynamic WEP requires 802.1x authentication.

Temporal Key Integrity Protocol (TKIP) TKIP ensures that the encryption key is changed for every data packet. You specify TKIP encryption for WPA and WPA-PSK authentication.

Advanced Encryption Standard (AES)

AES is an encryption cipher that uses the Counter-mode CBC-MAC (Cipher Block Chaining-Message Authentication Code) Protocol (CCMP) mandated by the IEEE 802.11i standard. AES-CCMP is specifically designed for IEEE 802.11 encryption and encrypts parts of the 802.11 MAC headers as well as the data payload. You can specify AES-CCMP encryption with WPA2 or WPA2-PSK authentication.

Mixed TKIP/AES-CCM

This option allows the WLAN Switch to use TKIP encryption with WPA or WPA-PSK clients and use AES encryption with WPA2 or WPA2-PSK clients. This option allows you to deploy the Alcatel OmniAccess system in environments that contain existing WLANs that use different authentication and encryption.

This option is only available on the WLAN Advanced Configuration page. For more information, see "Advanced WLAN Configuration in the WebUI" on page 13.

Authentication Server

If an external authentication server, such as a RADIUS server, will be used to validate the wireless user, the server administrator must configure the server to support this authentication. The administrator must also configure the server to allow communication with the Alcatel WLAN Switch.

If the internal database in the WLAN Switch will be used to validate the wireless user, you must configure user entries in the database.

Table 1-3 is a summary of the authentication servers that you can configure for each authentication type in an Alcatel WLAN.

TABLE 1-3 Supported Authentication Servers by Authentication Types

	Authentication Servers		
Authentication Type	**RADIUS**	**LDAP**	**Internal DB**
802.1x	Yes	Yes**	Yes*
WPA	Yes	Yes**	Yes*
WPA-PSK	n/a	n/a	n/a
WPA2	Yes	Yes**	Yes*
WPA2-PSK	n/a	n/a	n/a
Captive Portal	Yes	Yes	Yes
VPN	Yes	Yes	Yes
MAC	Yes	Yes	Yes

* Only when the AAA FastConnect feature is enabled. See the "Configuring 802.1x Authentication" chapter in Volume 4 of the *AOS-W User Guide*.

** Only when the AAA FastConnect feature is enabled and EAP-Generic Token Card (EAP-GTC) is used within the Protected EAP tunnel. See the "Configuring 802.1x Authentication" chapter in Volume 4 of the *AOS-W User Guide*.

Determine the Default VLAN

Each SSID is linked to a VLAN on the WLAN Switch. Successful wireless client association to an AP places the user into the default VLAN specified by the SSID configuration. The default VLAN can be overridden by authentication server attributes; if you are authenticating a user to an external authentication server, the user VLAN can be based on attributes returned by the server during authentication.

Basic WLAN Configuration in the WebUI

The WLAN Basic Configuration page in the WebUI allows you to define many useful options that pertain to a specific SSID without having to navigate to other configuration pages. These options include:

- SSID
- Radio type: 802.11a, 802.11b/g, or 802.11a/b/g
- Layer-2 authentication and encryption type
- "Advanced" authentication features such as Captive Portal, VPN, and MAC authentication, in addition to Layer-2 authentication
- Authentication server: either RADIUS or the WLAN Switch's internal database (if the authentication server is a RADIUS server, you can configure server parameters on the WLAN Basic Configuration page)
- VLAN into which wireless clients are placed
- Firewall policy for the user of the SSID (you can add a new policy or modify a predefined policy)

When you configure a WLAN in the WLAN Basic Configuration page, the SSID will not be hidden in beacons sent by the AP. In addition, the Alcatel system does not send the SSID in response to broadcast probe requests sent by clients.

Note the following about using the WLAN Basic Configuration page:

- The SSID configuration is *global*, that is, it applies to all APs in the network. If you need to configure a WLAN for a set of APs in a specific location—for example, a WLAN that only applies to a particular building or floor—you must configure the SSID using the WLAN Advanced Configuration pages.
- You can assign only one VLAN to the SSID. If you need to have multiple VLANs configured for a WLAN, you must configure the SSID using the WLAN Advanced Configuration pages.
- The authentication server must be a RADIUS server or the WLAN Switch's internal database.

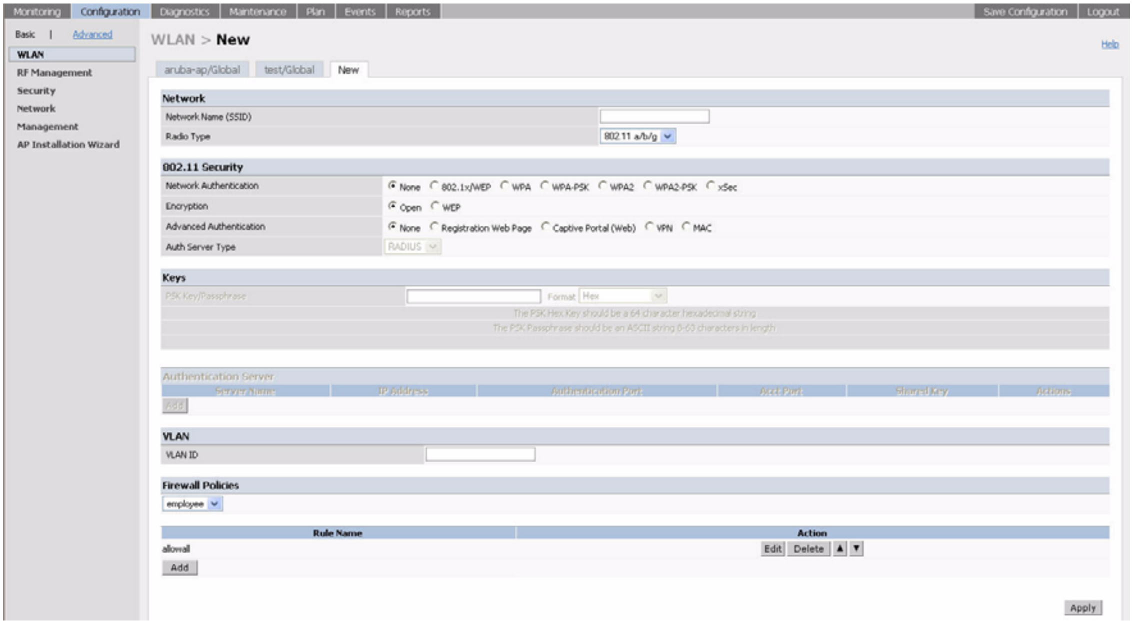
  If you specify a RADIUS server, you can configure the server's IP address, authentication and accounting ports, and shared key.

  NOTE: The RADIUS server administrator must configure the server for communication with the Alcatel WLAN Switch.

  If you specify the WLAN Switch's internal database, you will need to navigate to the Configuration > Advanced > Security > Authentication Servers > Internal DB to add entries to the database.

- You can only assign one firewall policy to the SSID. The policy must be either a predefined policy or a firewall policy that you create on the WLAN Basic Configuration page.

To configure an SSID in the WLAN Basic Configuration page, navigate to the **Configuration > Basic > WLAN** page.



WLAN > New

Network

Network Name (SSID)
Radio Type: 802.11 a/b/g

802.11 Security

Network Authentication: ● None ○ 802.1x/WEP ○ WPA ○ WPA-PSK ○ WPA2 ○ WPA2-PSK ○ xSec
Encryption: ● Open ○ WEP
Advanced Authentication: ● None ○ Registration Web Page ○ Captive Portal (Web) ○ VPN ○ MAC
Auth Server Type: RADIUS

Keys

PSK Key/Passphrase Format: Hex
The PSK Hex Key should be a 64 character hexadecimal string
The PSK Passphrase should be an ASCII string 8-63 characters in length

Authentication Server

Server Name	IP Address	Authentication Port	Acct Port	Shared Key	Actions

VLAN

VLAN ID

Firewall Policies

employee

Rule Name	Action
allowall	Edit Delete ▲ ▼

Table 1-4 describes the options available from the WLAN Basic Configuration page.

TABLE 1-4 WLAN Basic Configuration Parameters

Parameter	Definition
Network Section:	
Network Name (SSID)	A name that uniquely identifies the WLAN.
Radio Type	The radio type on which this SSID is configured: 802.11a only, 802.11b/g only, or 802.11a/b/g.
802.11 Security:	
Network Authentication	The Layer-2 security mechanism used to protect unauthorized access to the WLAN. See "Determine the Authentication Method" on page 1.

TABLE 1-4 WLAN Basic Configuration Parameters (Continued)

Encryption	The Layer-2 encryption used on the WLAN to ensure the privacy and confidentiality of the data transmitted to and from the network. The encryption type is dependent upon the type of network authentication selected.
Advanced Authentication	The default is None, however, you can select one of the following methods: ■ Registration Web Page: Allows users to access the WLAN using a web-based portal. Users typically enter an email address as an identification but are not authenticated. ■ Captive Portal (Web): Allows users to authenticate using a web-based portal. Captive Portal requires users to be authenticated to an external authentication server or to the internal database on the WLAN Switch. ■ VPN: Configures a VPN tunnel. Configuring this option requires user authentication against an external RADIUS server. ■ MAC: Allows the media access control (MAC) address of a device to be authenticated to an external authentication server or to the internal database on the WLAN Switch. **NOTE:** You can select one of the Advanced Authentication methods only if the Network Authentication is None, WPA-PSK, or WPA2-PSK.
Auth Server Type	(Activated only if 802.1x/WEP, WPA, WPA2, xSec, Captive Portal, VPN, or MAC authentication is configured) Either the internal database or an external RADIUS server.
Keys	(Activated only if static or PSK-based security options are configured) Configures the static WEP key or TKIP key for WPA-PSK or WPA2-PSK authentication. For Static WEP, enter either a 10-hexadecimal digit key or a 26-hexadecimal digit key. For TKIP, enter either a 64-character hexadecimal string or an 8-63 character ASCII passphrase.

TABLE 1-4 WLAN Basic Configuration Parameters (Continued)

Authentication Server	(Activated only if the authentication requires an authentication server and the server type is RADIUS) Configures the RADIUS authentication server. If you have previously configured a RADIUS authentication server, select the server from the drop-down list. To configure a RADIUS server, click the **New** button and enter the following information: ■ Server name ■ IP address of the server ■ Authentication port ■ Accounting port ■ Shared key Click **Add** when you are done. The information for the server appears. **NOTE:** If you are using an LDAP server or internal database for authentication, you need to configure the authentication server by navigating to the **Configuration** > **Advanced** > **Security** > **AAA Servers** page.
VLAN	Specifies the user VLAN for wireless clients that associate to the SSID.
Firewall Policies	Specifies the policies that are to be applied to the client after they have been successfully authenticated.

Example Configuration

This section describes how to use the WLAN Basic Configuration page to configure a WLAN to provide network access for company employees who use wireless PCs. Employees are typically validated against a corporate database on an authentication server before they are allowed access to the network. Once validated, users are placed into a specified VLAN and assigned a user role that permits access to resources on the corporate network.

In this example, the WLAN has the following characteristics:

SSID	corpnet
Radio Type	802.11 b/g
Authentication	WPA
Encryption	TKIP
VLAN	10
Firewall Policy	employee (allows unrestricted access to network resources)

A RADIUS server is used to authenticate users. The following is the RADIUS server information for this example:

Server Name	RadiusO1
IP Address	10.3.22.253
Authentication Port	1812
Acct Port	1813
Shared Key	radius123

NOTE: The administrator for the RADIUS server must configure the server to support authentication. The administrator must also configure the server to allow communication with the Alcatel WLAN Switch.

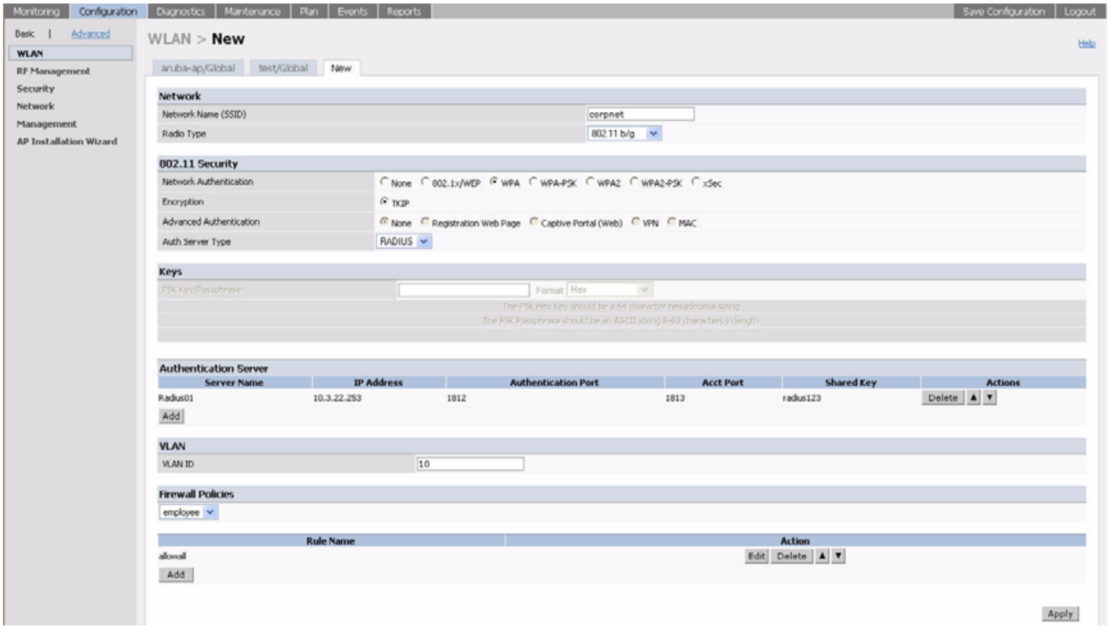
To configure the WLAN in the WLAN Basic Configuration page:

1. In the WebUI, navigate to the Configuration > Basic > WLAN page. Enter corpnet for Network Name (SSID).
2. Select 802.11 b/g for Radio Type.
3. Select WPA for Network Authentication

   TKIP is automatically selected for the encryption and Auth Server Type is activated with RADIUS selected.
4. Under Authentication Server, click **Add**.

5. Under Choose an Authentication Server, select NEW and click **Add**.
   - **A.** Enter Radius01 for Server Name.
   - **B.** Enter 10.3.22.253 for IP Address.
   - **C.** Enter radius123 for Shared Key.
   - **D.** Click **Add**. The server information appears under Authentication Server.
6. Enter 10 for VLAN ID.
7. Select employee for Firewall Policies.

   The page should look like the following:



WLAN > **New**

Network

Network Name (SSID): corpnet

Radio Type: 802.11 b/g

802.11 Security

Network Authentication: ○ None ○ 802.1x/WEP ● WPA ○ WPA-PSK ○ WPA2 ○ WPA2-PSK ○ xSec

Encryption: ● TKIP

Advanced Authentication: ● None ○ Registration Web Page ○ Captive Portal (Web) ○ VPN ○ MAC

Auth Server Type: RADIUS

Keys

PSK Key/Passphrase: Format Hex

The PSK Hex Key should be a 64 character hexadecimal string

The PSK Passphrase should be an ASCII string 8-63 characters in length

Authentication Server

Server Name	IP Address	Authentication Port	Acct Port	Shared Key	Actions
Radius01	10.3.22.253	1812	1813	radius123	Delete ▲ ▼

Add

VLAN

VLAN ID: 10

Firewall Policies

employee

Rule Name	Action
allowall	Edit Delete ▲ ▼

Add

8. Click **Apply**.

Advanced WLAN Configuration in the WebUI

In the WebUI, the Advanced WLAN configuration pages allow you to configure the following features:

- Configure global SSID and radio parameters that affect all APs in the network.
- Configure SSID and radio parameters for APs in specific locations in the network.

The parameters that you configure for global or location-specific SSID and radio configurations are identical. However, if the same parameters are configured for global and location-specific APs for a WLAN, the location-specific values override global values. For example, if you set the maximum number of clients to 30 in the global configuration for WLAN-01 and set the maximum number of clients to 15 for location 1.2.1 for the same SSID, the APs in location 1.2.1 will have a maximum of 15 clients.

Configuring Global Parameters

To configure global parameters that affect all APs in the network:

- Navigate to the **Configuration** > **Advanced** > **WLAN** > **Network** > **SSID** page to add or modify SSIDs.
- Navigate to the **Configuration** > **Advanced** > **WLAN** > **Network** > **General** page to configure or modify AP parameters.
- Navigate to the **Configuration** > **Advanced** > **WLAN** > **Radio** page to configure radio settings.

Configuring Location-Specific Parameters

To configure parameters that only affect APs in specific locations in the network:

1. Navigate to the **Configuration** > **Advanced** > **WLAN** > **Advanced** page.
2. Click **Add** to add a new location.
3. Enter a location ID in the format *building.floor.plan*, where each value is an integer.
4. Click **Add**.
5. You can customize the configuration of the specified location:
   - Select the **SSID** tab to add or modify SSIDs.
   - Select the **General** tab to configure AP parameters.
   - Select the **802.11b/g** or **802.11a** tab to configure radio settings.

NOTE: The global pages and location-specific configuration tabs contain identical configuration parameters, which are described in the following sections. Remember that location-specific values override global values for the same parameters.

Add or Modify SSIDs

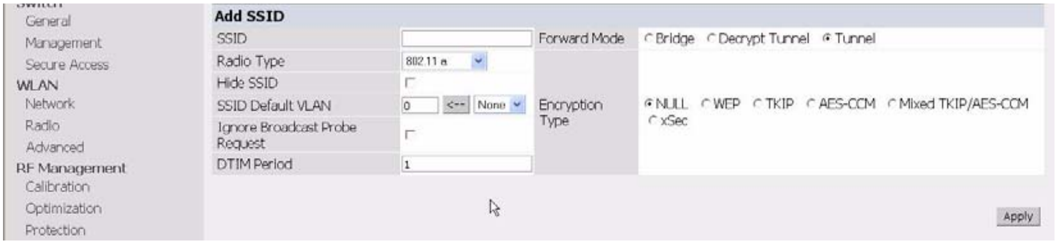
In the WebUI, you can configure 802.11 settings for an SSID in the Basic or Advanced WLAN configuration pages. The SSID configuration in the Advanced WLAN pages also allow you to configure additional SSID settings that are not available in the Basic configuration page; these settings are described later in this section.

To add or modify an SSID that affects all APs in the network:

1. Navigate to the **Configuration > Advanced > WLAN > Network > SSID** page.
2. To add a new SSID, click **Add**. To edit an existing SSID click **Edit**. The SSID configuration page appears.

To add or modify an SSID for APs in a specific location in the network:

1. Navigate to the **Configuration > Advanced > WLAN > Advanced** page.
2. Click **Add** to add a new location.
3. Enter a location ID in the format *building.floor.plan*, where each value is an integer.
4. Click **Add**.
5. Select the **SSID** tab to add or modify SSIDs.



Add SSID

SSID		Forward Mode	○ Bridge ○ Decrypt Tunnel ● Tunnel
Radio Type	802.11 a		
Hide SSID	□		
SSID Default VLAN	0 <-- None	Encryption Type	● NULL ○ WEP ○ TKIP ○ AES-CCM ○ Mixed TKIP/AES-CCM ○ xSec
Ignore Broadcast Probe Request	□		
DTIM Period	1		

Apply

Default SSID

The default SSID is alcatel-ap. This will be broadcast as a valid SSID if the value is not changed. This is the only SSID that permits a name change. To change the name of other SSIDs but retain the configurations:

1. Create a new SSID with the desired name and settings.
2. Delete the existing SSID entry.

Advanced SSID Configuration Settings

The SSID configuration in the Advanced WLAN pages allow you to configure the following SSID settings that are not available in the Basic configuration page:

Forward Mode

Controls whether 802.11 frames are tunneled to the WLAN Switch using generic routing encapsulation (GRE), or bridged into the local Ethernet LAN.

This setting can also be configured on a per-radio basis in the radio settings pages.

Hide SSID

Enables or disables hiding of the SSID name in beacon frames. Note that hiding the SSID does very little to increase security.

This setting can also be configured on a per-radio basis in the radio settings pages.

Ignore Broadcast Probe Request

When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.

This setting can also be configured on a per-radio basis in the radio settings pages.

DTIM Period

Specifies the interval between the sending of Delivery Traffic Indication Messages (DTIMs) in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed. When using wireless clients that employ power management features to sleep, the client must revive at least once during the DTIM period to receive broadcasts. The default is 2.

This setting can also be configured on a per-radio basis in the radio settings pages.

Mixed TKIP/AES-CCM encryption

Selecting this option displays additional selections:

- PSK TKIP/AES-CCM for static TKIP and AES key configuration
- WPA/2 TKIP/AES-CCM for dynamic TKIP and AES

If you select PSK TKIP/AES-CCM, the key can be hex or ASCII. Enter a 64-character hex key or an 8– to 63-character ASCII key.

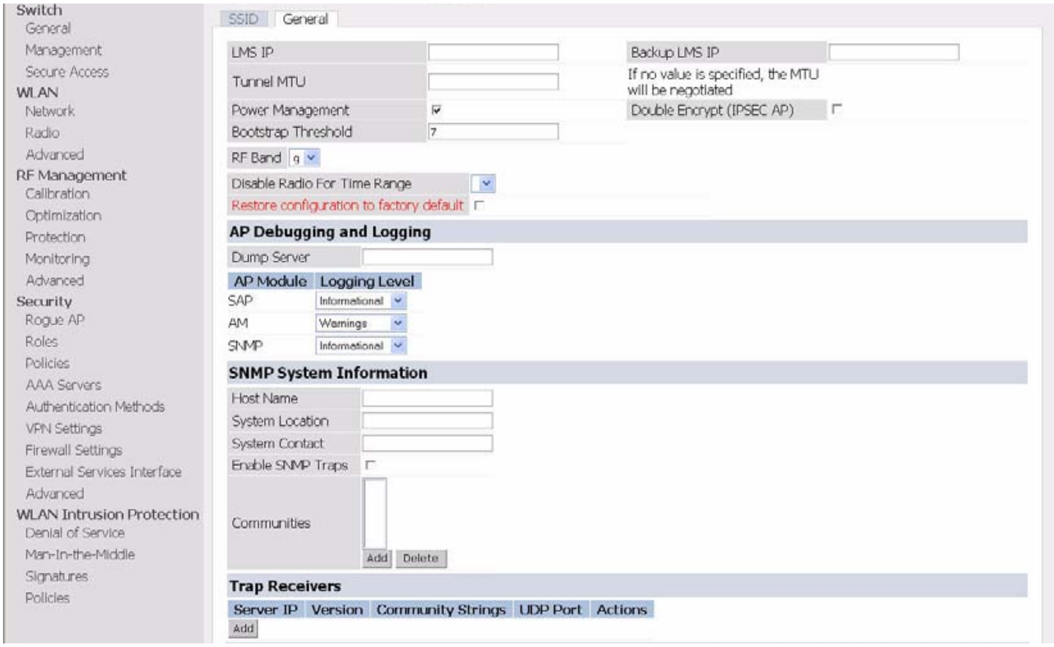
Configure AP Information

Use the General configuration in the Advanced WLAN pages to configure AP logging and debugging, SNMP system information and trap receivers, and other information.

To configure information that applies to all APs in the network, navigate to the **Configuration > Advanced > WLAN > Network > General** page.

To configure information that applies to APs in a specific location in the network:

1. Navigate to the **Configuration > Advanced > WLAN > Advanced** page.
2. Click **Add** to add a new location.
3. Enter a location ID in the format *building.floor.plan*, where each value is an integer.
4. Click **Add**.
5. Select the **General** tab.



LMS IP		Backup LMS IP	
Tunnel MTU		If no value is specified, the MTU will be negotiated	
Power Management	☑	Double Encrypt (IPSEC AP)	□
Bootstrap Threshold	7		

RF Band: g

Disable Radio For Time Range:

Restore configuration to factory default □

AP Debugging and Logging

Dump Server:

AP Module	Logging Level
SAP	Informational
AM	Warnings
SNMP	Informational

SNMP System Information

Host Name:

System Location:

System Contact:

Enable SNMP Traps □

Communities

Trap Receivers

Server IP	Version	Community Strings	UDP Port	Actions

The General configuration in the Advanced WLAN pages allow you to configure the following settings:

LMS IP and Backup LMS IP	Specifies the local management switch (LMS) that the AP uses in multi-WLAN Switch networks. The LMS is responsible for terminating user traffic from the APs, processing it, and forwarding it to the wired network. An AP can boot up from any WLAN Switch on the WLAN network (in a setup with master and local WLAN Switches), if all of the WLAN Switches are on the same VLAN and if load balancing is enabled on the WLAN Switches. To force the AP to boot with a particular WLAN Switch, configure the LMS IP with the address of the desired WLAN Switch. When using redundant WLAN Switches as the LMS, set this parameter to be the VRRP IP address to ensure that APs always have an active IP address with which to terminate sessions.
Tunnel MTU	Maximum transmission unit (MTU) size of the wired link for the AP. If no value is specified, he MTU size is negotiated.
Power Management	Enables power management
Double Encrypt (IPSec AP)	Encrypts 802.11 data frames using IPSec.
Bootstrap Threshold	Number of heartbeat misses before an AP reboots.
RF Band	RF band in which the AP should operate: g = 2.4 GHz, a=5GHz.
Disable Radio For Time Range	Specifies the time range for which the AP will deny access from clients.

Configuring Radio Settings

You can fine tune radio settings on a per-radio (802.11a or 802.11b/g) basis.

NOTE: Selecting these options may affect roaming performance.

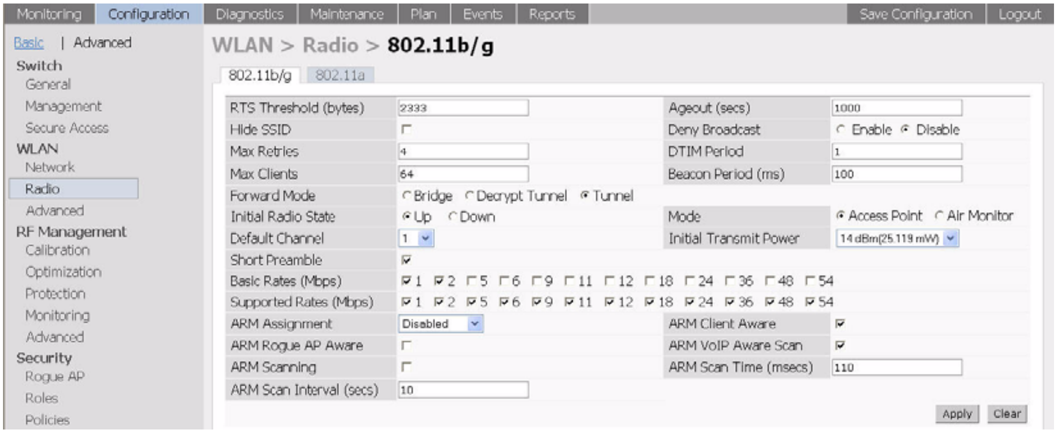
To configure radio settings that affect all APs in the network, navigate to the **Configuration > Advanced > WLAN > Network > Radio** page.

To configure radio settings for APs in a specific location in the network:

1. Navigate to the **Configuration > Advanced > WLAN > Advanced** page.
2. Click **Add** to add a new location.
3. Enter a location ID in the format *building.floor.plan*, where each value is an integer.

4. Click **Add**.

5. Select the **802.11b/g** or **802.11a** tab to configure radio settings



WLAN > Radio > **802.11b/g**

RTS Threshold (bytes)	2333	Ageout (secs)	1000
Hide SSID	☐	Deny Broadcast	○ Enable ● Disable
Max Retries	4	DTIM Period	1
Max Clients	64	Beacon Period (ms)	100
Forward Mode	○ Bridge ○ Decrypt Tunnel ● Tunnel		
Initial Radio State	● Up ○ Down	Mode	● Access Point ○ Air Monitor
Default Channel	1	Initial Transmit Power	14 dBm(25.119 mW)
Short Preamble	☑		
Basic Rates (Mbps)	☑ 1 ☑ 2 ☐ 5 ☐ 6 ☐ 9 ☐ 11 ☐ 12 ☐ 18 ☐ 24 ☐ 36 ☐ 48 ☐ 54		
Supported Rates (Mbps)	☑ 1 ☑ 2 ☑ 5 ☑ 6 ☑ 9 ☑ 11 ☑ 12 ☑ 18 ☑ 24 ☑ 36 ☑ 48 ☑ 54		
ARM Assignment	Disabled	ARM Client Aware	☑
ARM Rogue AP Aware	☐	ARM VoIP Aware Scan	☑
ARM Scanning	☐	ARM Scan Time (msecs)	110
ARM Scan Interval (secs)	10		

The radio configuration in the Advanced WLAN pages allow you to configure the following settings:

RTS Threshold
Wireless clients transmitting frames larger than this threshold must issue Request to Send (RTS) and wait for the AP to respond with Clear to Send (CTS). This helps prevent mid-air collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting. The default is 2333 bytes.

Ageout
Specifies the amount of time, in seconds, that a client is allowed to remain idle before being aged out. The default is 1000 seconds.

Hide SSID
Enables or disables hiding of the SSID name in beacon frames. Note that hiding the SSID does very little to increase security.

Deny Broadcast
When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.

Max Retries
Specifies the maximum number of retries allowed for the AP to send a frame. The recommended range is between 3 and 7. The default is 3.

DTIM Period — Specifies the interval between the sending of Delivery Traffic Indication Messages (DTIMs) in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed. When using wireless clients that employ power management features to sleep, the client must revive at least once during the DTIM period to receive broadcasts. The default is 2.

Max Clients — Specifies the maximum number of wireless clients for a radio on an AP. The default is 0, but is set to 64 if the initial setup dialog is used to configure the WLAN Switch.

Beacon Period — Specifies the time between successive beacons being transmitted. The default is 100 milliseconds.

Forward Mode — Controls whether 802.11 frames are tunneled to the WLAN Switch using generic routing encapsulation (GRE), or bridged into the local Ethernet LAN.

Initial Radio State — Used to enable or disable the radio. Select Up to ensure that the AP radio is up on reboot.

Mode — Specifies whether the AP should act as an access point or an air monitor.

Default Channel — Specifies the default channel on which the AP operates, unless a better choice is available through either calibration or from RF Plan.

Initial Transmit Power — Sets the initial transmit power on which the AP operates, unless a better choice is available through either calibration or from RF Plan.

Short Preamble — Enables or disables short preamble for 802.11b/g radios. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using short preamble. To use only long preamble, disable short preamble. Legacy client devices that use only long preamble generally can be updated to support short preamble. The default is enabled.

Basic Rates — Specifies the list of supported rates that are advertised in beacon frames and probe responses.

Supported Rates — Specifies the set of rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error/loss rate of the client.

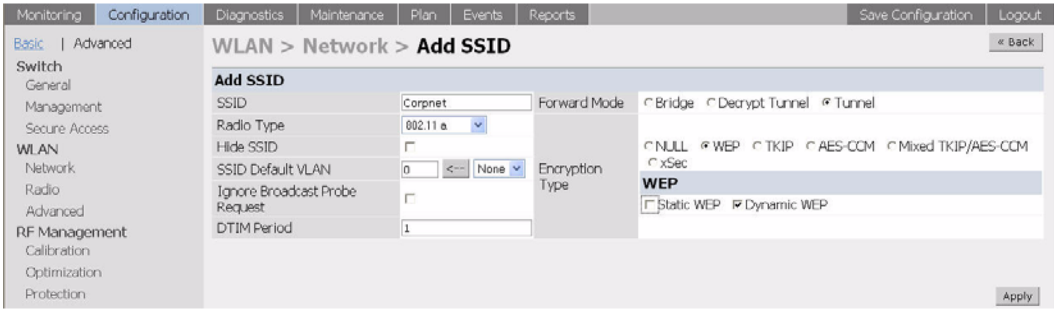
The radio configuration in the Advanced WLAN pages also allow you to configure Adaptive Radio Management (ARM) parameters, which are described in "Adaptive Radio Management" on page 21.

Example Configuration

The following example includes:

- An 802.11 a/b/g SSID called Corpnet with dynamic WEP.
- An 802.11 b/g SSID called Voice with static WEP.
- The AP in location **`4.2.6`** is set to have a guest SSID in addition to the other two SSIDs. The guest SSID is open.

1. Configure the 802.11 a/b/g SSID Corpnet in the global location 0.0.0 with dynamic WEP.

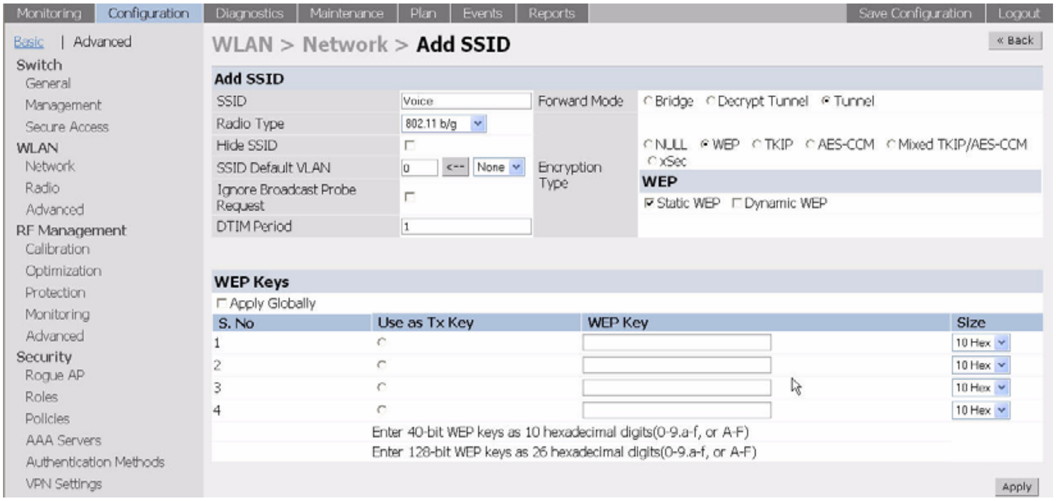


WLAN > Network > **Add SSID**

Add SSID

SSID	Corpnet	Forward Mode	○ Bridge ○ Decrypt Tunnel ● Tunnel
Radio Type	802.11 a	Encryption Type	○ NULL ● WEP ○ TKIP ○ AES-CCM ○ Mixed TKIP/AES-CCM ○ xSec
Hide SSID	□		**WEP**
SSID Default VLAN	0 <-- None		□ Static WEP ☑ Dynamic WEP
Ignore Broadcast Probe Request	□		
DTIM Period	1		

2. Configure the 802.11 b/g Voice SSID in the global location 0.0.0 with static WEP.



WLAN > Network > **Add SSID**

Add SSID

SSID	Voice	Forward Mode	○ Bridge ○ Decrypt Tunnel ● Tunnel
Radio Type	802.11 b/g	Encryption Type	○ NULL ● WEP ○ TKIP ○ AES-CCM ○ Mixed TKIP/AES-CCM ○ xSec
Hide SSID	□		**WEP**
SSID Default VLAN	0 <-- None		☑ Static WEP □ Dynamic WEP
Ignore Broadcast Probe Request	□		
DTIM Period	1		

WEP Keys

□ Apply Globally

S. No	Use as Tx Key	WEP Key	Size
1	○		10 Hex
2	○		10 Hex
3	○		10 Hex
4	○		10 Hex

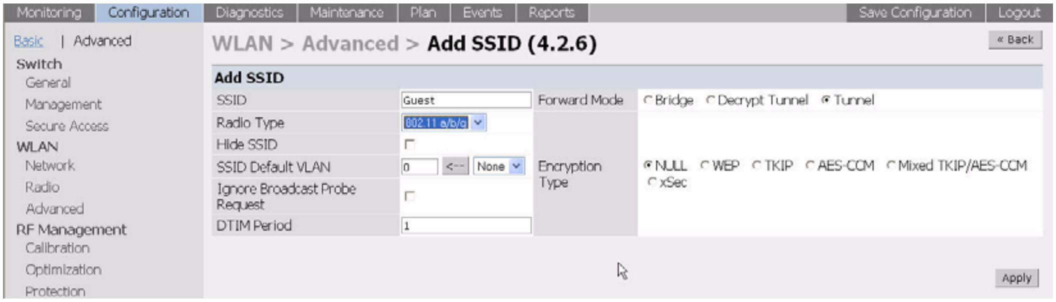
Enter 40-bit WEP keys as 10 hexadecimal digits(0-9.a-f, or A-F)
Enter 128-bit WEP keys as 26 hexadecimal digits(0-9.a-f, or A-F)

3. Configure the Guest SSID for location 4.2.6.

   A. Add the location 4.2.6.

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

C. Configure the SSID with open system and native VLAN.



WLAN > Advanced > Add SSID (4.2.6)

Add SSID

SSID	Guest	Forward Mode	○ Bridge ○ Decrypt Tunnel ● Tunnel
Radio Type	802.11 a/b/g	Encryption Type	● NULL ○ WEP ○ TKIP ○ AES-CCM ○ Mixed TKIP/AES-CCM ○ xSec
Hide SSID	☐		
SSID Default VLAN	0 <-- None		
Ignore Broadcast Probe Request	☐		
DTIM Period	1		

Adaptive Radio Management

Adaptive Radio Management (ARM) is the next-generation RF resource allocation algorithm in AOS-W 2.3 and later. ARM is an RF management technology for a stable, self-healing RF design. ARM takes the distributed algorithm approach, allowing APs to determine their transmit power and channel settings based on what they hear in the air. The APs make their channel and power setting decisions based on the RF environment as they hear it, independent of the WLAN Switch. This results in a highly-scalable and reliable RF environment while also significantly reducing the time the AP takes to adapt to changes in the 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.

Channel Setting

In addition to the interference index, the APs use the free-channel index to determine the optimal channel setting. The free-channel index is a configurable parameter on the WLAN Switch used by an AP to qualify a channel before moving to it. An AP chooses 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 this criteria is not met, the AP remains on the current channel.

Power Setting

Power assignment decisions are based on the AP's coverage index. The benchmark used here is the ideal-coverage index. The ideal-coverage index is the power setting that an AP should have for good coverage. It is a configurable parameter on the WLAN Switch. The AP increases or decreases 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 or decrement by a single unit at any given time.

Advantages of Using ARM

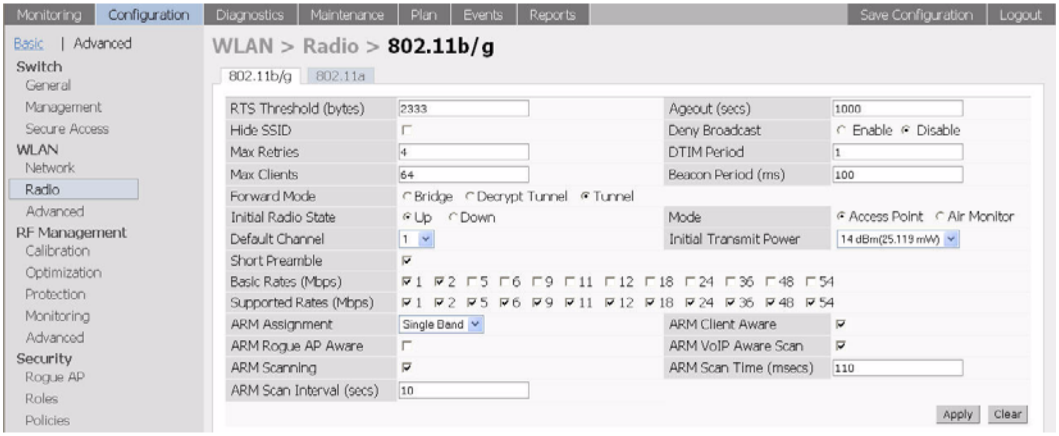
Using ARM provides the following benefits:

- With ARM, the WLAN Switch does not require a downtime for initial calibration.
- The AP response time to noise is quick and reliable, even to non-802.11 noise, especially when client traffic starts generating errors due to the noise.

  NOTE: Non-802.11 noise detection is disabled by default and must be explicitly enabled.
- The 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 taken into account.
- ARM complements Alcatel's next generation AOS-W architecture.

Configuring ARM

1. You enable ARM under the global setting or for each AP by navigating to either **Configuration > Advanced > WLAN > Radio** or **Configuration > Advanced > WLAN > Advanced**. To enable ARM on the 802.11b/g radio, navigate to the **Configuration > Advanced > WLAN > Radio** page.



WLAN > Radio > 802.11b/g

RTS Threshold (bytes)	2333	Ageout (secs)	1000
Hide SSID	☐	Deny Broadcast	○ Enable ● Disable
Max Retries	4	DTIM Period	1
Max Clients	64	Beacon Period (ms)	100
Forward Mode	○ Bridge ○ Decrypt Tunnel ● Tunnel		
Initial Radio State	● Up ○ Down	Mode	● Access Point ○ Air Monitor
Default Channel	1	Initial Transmit Power	14 dBm(25.119 mW)
Short Preamble	☑		
Basic Rates (Mbps)	☑ 1 ☑ 2 ☐ 5 ☐ 6 ☐ 9 ☐ 11 ☐ 12 ☐ 18 ☐ 24 ☐ 36 ☐ 48 ☐ 54		
Supported Rates (Mbps)	☑ 1 ☑ 2 ☑ 5 ☑ 6 ☑ 9 ☑ 11 ☑ 12 ☑ 18 ☑ 24 ☑ 36 ☑ 48 ☑ 54		
ARM Assignment	Single Band	ARM Client Aware	☑
ARM Rogue AP Aware	☐	ARM VoIP Aware Scan	☑
ARM Scanning	☑	ARM Scan Time (msecs)	110
ARM Scan Interval (secs)	10		

2. To enable ARM, set **ARM Assignment** to **Single Band** from the pull down menu.

   NOTE: The **Multi Band** option is currently unavailable. Selecting the **Multi Band** option sets the selection to **Single Band** automatically.

3. Select **ARM Scanning** to enable scanning on the AP.

4. You can set the **ARM Scan Interval** and **ARM Scan Time** 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 scans the network and hop to the best available channel based on the ARM 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, select **ARM Client Aware**.

6. Click **Apply** to apply the configurations.

Configuring Remote APs 2

The Secure Remote Access Point Service allows users to connect APs at remote sites to an Alcatel WLAN Switch over the Internet. This capability allows remote locations equipped with Access Points (APs) to connect to a corporate office, for example, over the Internet.

This chapter describes the following topics:

Overview

Remote APs use Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPSec) to connect to the WLAN Switch with Network Address Translation-Traversal (NAT-T) support (UDP port 4500 only). All of the AP control traffic and 802.11 data are carried through this tunnel to the WLAN Switch.

Since the Internet is involved, securing data between the AP and WLAN Switch becomes key. Also most branch/home office deployments sit behind a firewall or a Network Address Translation (NAT) device. In the case of remote AP, all traffic between the WLAN Switch and the remote AP is VPN encapsulated, and all control traffic between the WLAN Switch and AP is encrypted. You have the choice of encrypting data in addition to the control traffic for additional security.

The advantage of using the Secure Remote Access Point Service for a remote AP is that the corporate office is now virtually extended to the remote site. Remote users can enjoy similar features as corporate office users and Voice over IP (VoIP) applications can be extended to remote sites while the servers and the PBX sit securely in the corporate office.

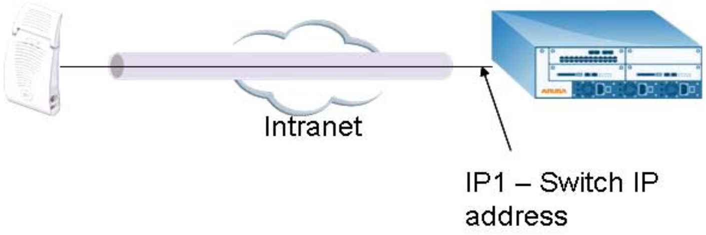
Remote AP configurations can also be used to secure control traffic between the AP and the WLAN Switch in a corporate environment. In this case, the AP and WLAN Switch are in the company's private address space. The Remote AP is similar to the Alcatel AP while tunneling and encrypting all data and control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

NOTE: The Secure Remote Access Point Service requires that you install a Remote AP license in the WLAN Switch. Each Remote AP license supports a maximum number of APs.

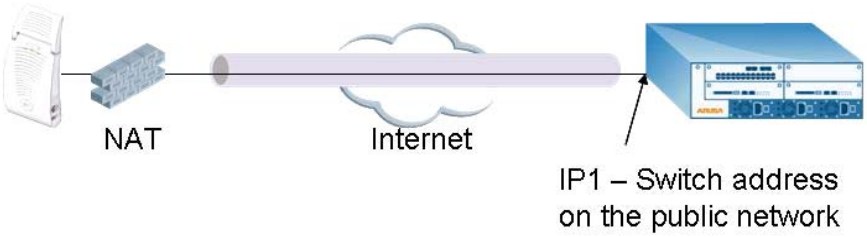
How the Secure Remote Access Point Service Works

You can deploy APs with Secure Remote Access Point Service in one of the following ways:

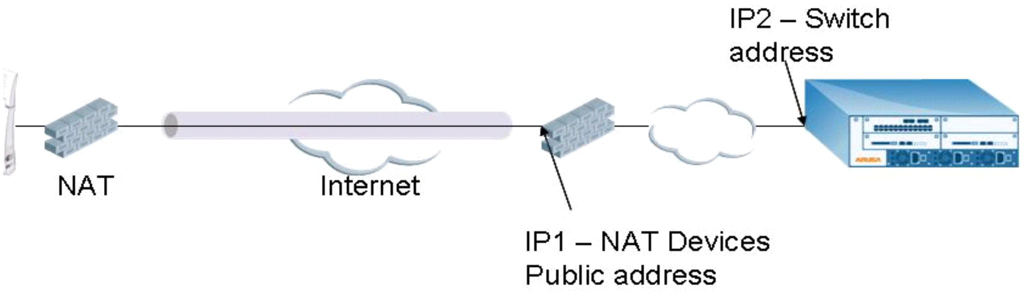
- Deployment Scenario 1: The remote AP and WLAN Switch reside in a private network which is used to secure AP-to-WLAN Switch communication. (Alcatel recommends this deployment when AP-to-WLAN Switch communications need to be secured.)



- Deployment Scenario 2: The remote AP is on the public network or behind a NAT device and the WLAN Switch is on the public network.



- Deployment Scenario 3: The remote AP is on the public network or behind a NAT device and the WLAN 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 is highlighted in the steps below.

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

In the case where the WLAN 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 WLAN Switch.

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

Configuring the Secure Remote Access Point Service

Refer to the three deployment scenarios described previously. To configure the Secure Remote Access Point Service:

- Configure the AP as a remote AP with the IP address of the master WLAN Switch, the LMP IP, IKE PSK, and the username and password for authentication.

- Configure IPSec VPN tunnels on the WLAN Switch which the AP will use before it bootstraps.

- Configure the Secure Remote Access Point Service user role and permissions.
- Add an 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 WLAN Switch connects (deployment scenario 3 only).

These task are explained below:

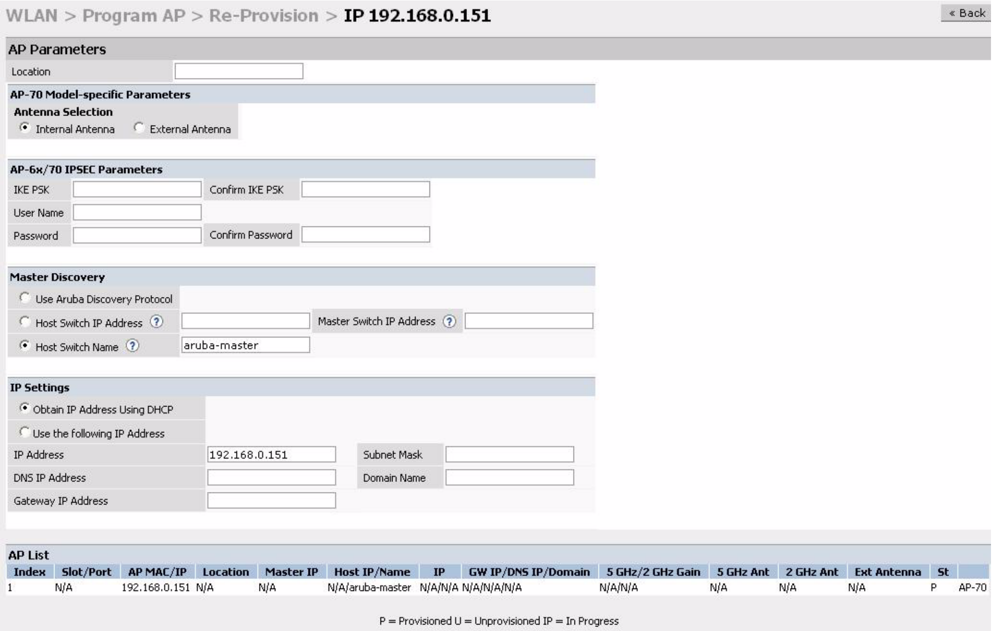
1. Configure the AP with the master WLAN Switch's IP address and username and password for authentication.

   All Alcatel Access Points, with the exception of the AP 52, can be provisioned to offer Secure Remote Access Point Service. The easiest way is to use the Program AP Web configuration page to configure AP settings.

   A. Once the AP boots up, it appears as an un-provisioned AP if it is a new AP.

If the AP is an already provisioned AP that has to be re-configured to provide Secure Access Point Service, continue with the next step. Otherwise, navigate to the **Maintenance > WLAN > Program AP > Provision AP** page and provision the AP with its location and master IP address. Apply the changes and reboot the AP. This step ensures that the AP now boots with AOS-W 2.3 or later release that supports this feature.

Deployment Scenario	Master IP Address Value while Provisioning the AP
Deployment 1	WLAN Switch IP address
Deployment 2	WLAN Switch public IP address
Deployment 3	Public address of the NAT device to which the WLAN Switch is connected



WLAN > Program AP > Re-Provision > IP 192.168.0.151

« Back

AP Parameters

Location

AP-70 Model-specific Parameters

Antenna Selection

● Internal Antenna ○ External Antenna

AP-6x/70 IPSEC Parameters

IKE PSK | Confirm IKE PSK

User Name

Password | Confirm Password

Master Discovery

○ Use Aruba Discovery Protocol

○ Host Switch IP Address | Master Switch IP Address

● Host Switch Name: aruba-master

IP Settings

● Obtain IP Address Using DHCP

○ Use the following IP Address

IP Address: 192.168.0.151 | Subnet Mask

DNS IP Address | Domain Name

Gateway IP Address

AP List

Index	Slot/Port	AP MAC/IP	Location	Master 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	AP-70

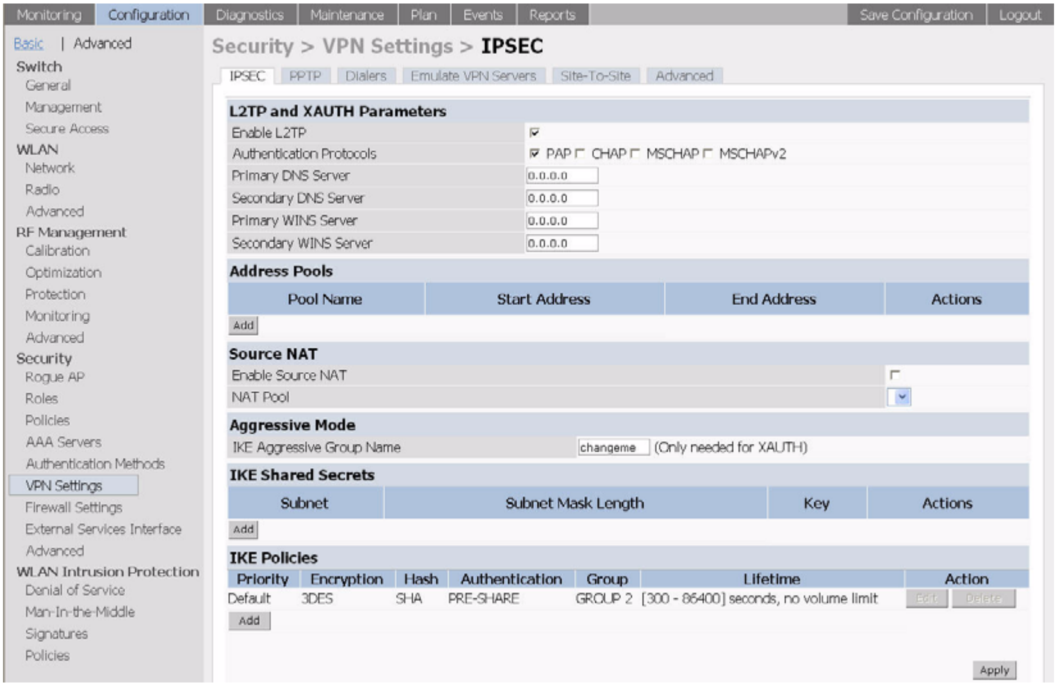
P = Provisioned U = Unprovisioned IP = In Progress

B. Select the AP that needs to be configured to provide Secure Remote Access Point Service on the **Maintenance > WLAN > Program AP > Re-provision** page. Configure the AP username and password, and the Internet Key Exchange (IKE) Pre-Shared Key (PSK) for the IPSec settings. Set the master IP to the public IP address if the AP is connected to the WLAN Switch over the Internet.

C. Regardless of the deployment type, Alcatel recommends that the LMS IP of the AP be set to the WLAN Switch IP address (either the loopback address of the WLAN Switch or the VLAN 1 IP address).

D. Navigate to the **Configuration** > **Advanced** > **WLAN** > **Advanced** page. Select the AP to be configured as a remote AP. Set the LMS IP to the WLAN Switch IP address.

2. Configure the IPSec VPN settings on the WLAN Switch by navigating to the **Configuration** > **Advanced** > **Security** > **VPN Settings** > **IPSec** page.



L2TP and XAUTH Parameters

Enable L2TP	☑
Authentication Protocols	☑ PAP ☐ CHAP ☐ MSCHAP ☐ MSCHAPv2
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Primary WINS Server	0.0.0.0
Secondary WINS Server	0.0.0.0

Address Pools

Pool Name	Start Address	End Address	Actions

Source NAT

Enable Source NAT	☐
NAT Pool	

Aggressive Mode

IKE Aggressive Group Name	changeme (Only needed for XAUTH)

IKE Shared Secrets

Subnet	Subnet Mask Length	Key	Actions

IKE Policies

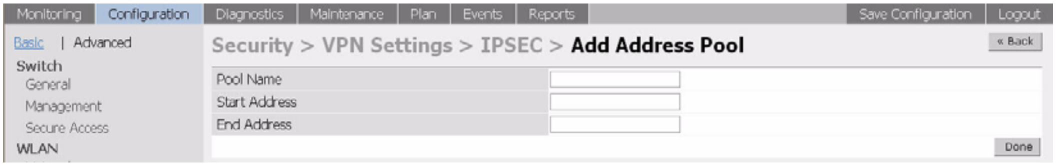
Priority	Encryption	Hash	Authentication	Group	Lifetime	Action
Default	3DES	SHA	PRE-SHARE	GROUP 2	[300 - 86400] seconds, no volume limit	Edit Delete

A. To configure Password Authentication Protocol (PAP) authentication for L2TP, make sure that PAP is selected. Click **Apply** to apply the configuration changes made.

From the CLI enter:

```
(WLAN_Switch)# configure terminal
(WLAN_Switch) (config)# vpdn group l2tp
(WLAN_Switch) (config-vpdn-l2tp)# ppp authentication PAP
(WLAN_Switch) (config-vpdn-l2tp)# exit
(WLAN_Switch) (config)#
```

B. 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.



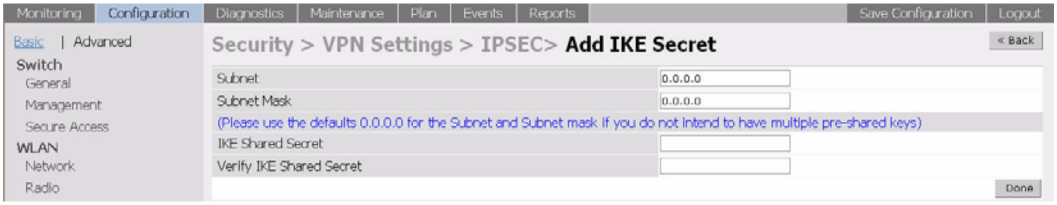
Security > VPN Settings > IPSEC > **Add Address Pool**

Pool Name	
Start Address	
End Address	

From the CLI enter:

```
(WLAN_Switch)# configure terminal
(WLAN_Switch) (config)# ip local pool l2tppool1 192.168.69.1 192.168.69.254
(WLAN_Switch) (config)#
```

C. To configure an Internet Security Association and Key Management Protocol (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” in Volume 4 of the *AOS-W User Guide*.



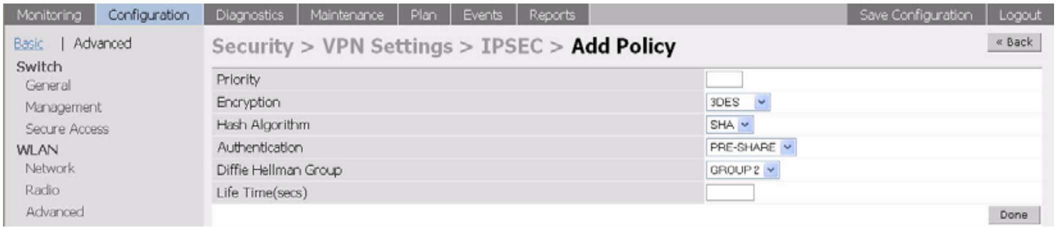
Security > VPN Settings > IPSEC> **Add IKE Secret**

Subnet	0.0.0.0
Subnet Mask	0.0.0.0
(Please use the defaults 0.0.0.0 for the Subnet 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:

```
(WLAN_Switch)# configure terminal
(WLAN_Switch) (config)# crypto isakmp key testkey address 0.0.0.0 netmask 0.0.0.0
(WLAN_Switch) (config)#
```

D. To create an ISAKMP policy, click **Add** in the **IKE Policies** panel.



Security > VPN Settings > IPSEC > **Add Policy**

Priority	
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:

```
(WLAN_Switch)# configure terminal
(WLAN_Switch) (config)# crypto isakmp policy 1
(WLAN_Switch) (config-isakmp)# authentication pre-share
(WLAN_Switch) (config-isakmp)# exit
```

3. Create a user-role for the remote AP.

   Once the remote AP is authenticated successfully for the VPN, the remote AP is assigned a role. This role is a temporary role assigned to the 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 WLAN Switch to the AP and back to facilitate the bootstrap process.

   From the CLI enter:

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

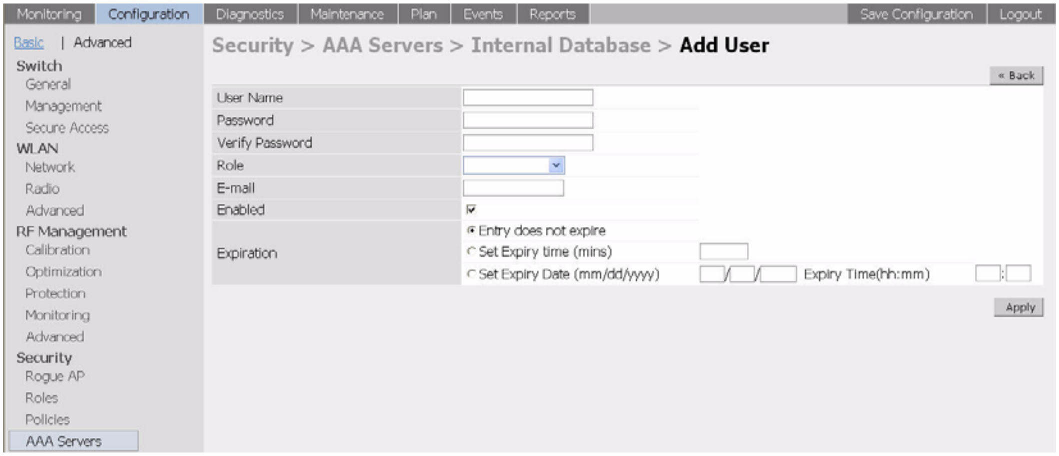
   (The ACLs in this step contain the following rules:

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

4. Add a 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 WLAN Switch internal database for authentication, navigate to the **Configuration > Advanced> Security > AAA Servers > Internal Database** page and click **Add User**.



Security > AAA Servers > Internal Database > **Add User**

User Name
Password
Verify Password
Role
E-mail
Enabled ☑
Expiration
● Entry does not expire
○ Set Expiry time (mins)
○ Set Expiry Date (mm/dd/yyyy) Expiry Time(hh:mm)

Add the username and password. If the default VPN role is not the 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:

```
(WLAN_Switch) #local-userdb add username remoteap1 password remote role remote-ap
```

By default, no authentication server is defined under VPN authentication. When using VPN authentication, make sure an authentication server is configured. For example, if the internal database is to be used for VPN authentication, enable this configuration using the following commands:

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

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

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

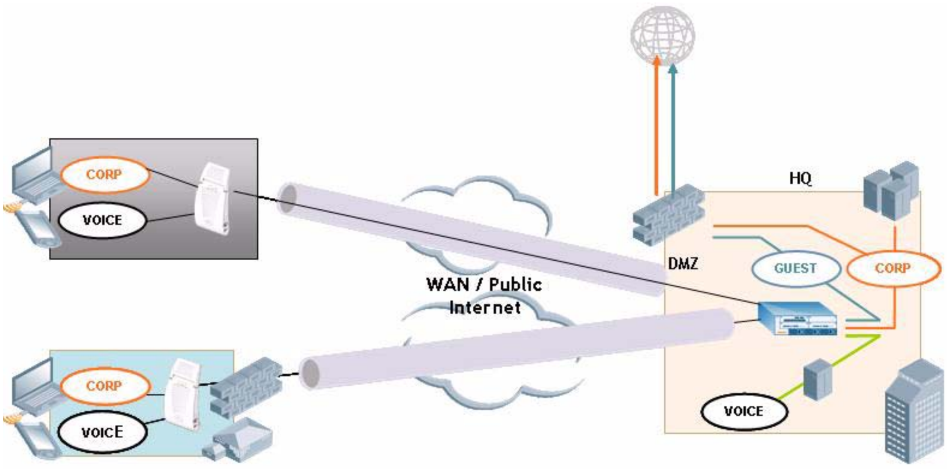
For more information on configuring IPSec and VPNs, see "Configuring Virtual Private Networks" in Volume 4 of the *AOS-W User Guide.*

5. Configuring the NAT device that is connected to the Alcatel WLAN Switch.

   Communication between the AP and secure WLAN Switch uses the UDP 4500 port. When both the WLAN Switch and the AP are behind NAT devices, configure the AP to use the NAT device's public address as its master address. On the NAT device, you must 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 WLAN Switch to ensure that the remote AP boots successfully.

Deploying a Branch Office/Home Office Solution

To deploy a remote AP in a branch office or home office as shown in the illustration below, the WLAN environment must be a single WLAN Switch environment.



In a branch office, the AP is deployed in a separate IP network from the corporate network. Typically, there are one or two NAT devices between the two networks. Branch office users need access to corporate resources like printers and servers but traffic to and from these resources must not impact the corporate head office.

Branch office users also want continued operation of the branch office WLAN even if the link to the corporate network goes down. The branch office AP solves these requirements by providing:

- Local termination of 802.11 management frames which provides survivability of the branch office WLAN.
- Implementation of an 802.1x authenticator split. All 802.1x authenticator functionality is implemented in the AP. The WLAN Switch is used as a RADIUS pass-through when the authenticator has to communicate with a RADIUS server (which also supports survivability).
- 802.11 encryption/decryption is in the AP to provide access to local resources.
- Local bridging of client traffic connected to the WLAN or to an AP 70 enet1 port to provide access to local resources.

As of AOS-W 2.4.1.0, you must configure the branch office AP from the CLI; the WebUI is not supported.

To configure the remote AP, refer to "Configuring the Secure Remote Access Point Service" on page 27.

To configure the branch office AP, you must:

- Specify forward mode for the Extended Service Set Identifier (ESSID) in the base AP configuration and virtual-ap command
- Set how long the AP stays up after connectivity to WLAN Switch has gone down
- Set the VLAN ID in the base AP configuration and virtual-ap command
- Set the native VLAN ID in the base AP configuration
- Set forward mode for enet1 port

For example:

```
(WLAN_Switch) #configure terminal ap location 0.0.0 essid sw-test-ap
(WLAN_Switch) #configure terminal ap location 0.0.0 opmode opensystem
(WLAN_Switch) #configure terminal ap location 0.0.0 max-imalive-retries 200
(WLAN_Switch) #configure terminal ap location 0.0.0 forward-mode bridge
(WLAN_Switch) #configure terminal ap location 0.0.0 vlan-id 100
(WLAN_Switch) #configure terminal ap location 0.0.0 native-vlan-id 100
(WLAN_Switch) #configure terminal ap location 0.0.0 virtual-ap sw-remote-ap vlan-id 200
opmode staticwep forward-mode bridge
(WLAN_Switch) #configure terminal ap location 0.0.0 ap-logging level informational stm
(WLAN_Switch) #configure terminal ap location 0.0.0 phy-type enet1 mode bridge
```

NOTE: Remote APs support 802.1q VLAN tagging. In the example above, the native VLAN ID is 100 while the Virtual AP ID is 200. Thus data from the remote AP will be tagged on the wired side.

To troubleshoot your branch office AP configuration, use the following commands.

To query the STM state in an AP, enter:

```
(WLAN_Switch) #show stm ap connectivity 10.3.3.6

Alcatel AP Table
--------------
bss                ess           s/p  ip        phy  type  ch/pwr  cur-cl  loc    in-t(s)  tot-t  mtu   acl-state
---                ---           ---  --        ---  ----  ------  ------  ---    -------  -----  ---   ---------
00:0b:86:c0:05:00  sw-test-ap   ?/?  10.3.3.6  g    ap    6/0     0      0.0.0  0        0s     1500  -
00:0b:86:c0:05:01  sw-remote-ap  ?/?  10.3.3.6  g    ap    6/0     0      0.0.0  0        0s     1500  -
00:0b:86:c0:05:08  sw-test-ap   ?/?  10.3.3.6  a    ap    149/0   0      0.0.0  0        0s     1500  -
00:0b:86:c0:05:09  sw-remote-ap  ?/?  10.3.3.6  a    ap    149/0   0      0.0.0  0        0s     1500  -
Num APs:4
Num Associations:0
```

To see station management AP counters, enter:

```
(WLAN_Switch) #show stm ap counters 10.3.3.8
Counters
--------
Name                          Value
----                          -----
Configure AP Response         1
Remote AP Config Request      1
Remote AP Log Level Message   1
Remote AP Bootstrap Request   1
Remote AP Bootstrap Response  1
Remote AP State               1665
Remote AP Global Config       1
reassoc-req                   1
reassoc-resp                  1
auth                          4
```

To see AP associations, enter:

```
(WLAN_Switch) #show stm ap association 10.3.3.6 00:0b:86:c0:05:00

Association Table

----------------

bssid  mac  auth  assoc  aid  l-int  essid  vlan-id  tunnel-id

-----  ---  ----  -----  ---  -----  -----  -------  ---------

(WLAN_Switch) #
```

To see AP traffic statistics, enter:

```
(WLAN_Switch) #show stm ap packets 10.3.3.8


STM Packets
```

```
-----------
Timestamp        stype         SA                 DA                 BSS                signal  Misc
---------        -----         --                 --                 ---                ------  ----
May 18 11:10:30  reassoc-resp  00:0b:86:a0:d4:c0  00:0b:fd:52:de:c2  00:0b:86:a0:d4:c0  15      Success
May 18 11:10:30  reassoc-req   00:0b:fd:52:de:c2  00:0b:86:a0:d4:c0  00:0b:86:a0:d4:c0  0       -
May 18 11:10:30  auth          00:0b:86:a0:d4:c0  00:0b:fd:52:de:c2  00:0b:86:a0:d4:c0  15      Success
May 18 11:10:30  auth          00:0b:fd:52:de:c2  00:0b:86:a0:d4:c0  00:0b:86:a0:d4:c0  0       -
May 18 11:10:30  auth          00:0b:86:a0:d4:c0  00:0b:fd:52:de:c2  00:0b:86:a0:d4:c0  15      Success
May 18 11:10:30  auth          00:0b:fd:52:de:c2  00:0b:86:a0:d4:c0  00:0b:86:a0:d4:c0  0       -
```

To see the AP configuration, enter:

```
(WLAN_Switch) #show stm ap-config


Alcatel AP Config Table
---------------------
bss                ess             vlan  ip        phy  type  fw-mode  max-cl  rates  tx-rates  preamble  mtu  status
---                ---             ----  --        ---  ----  -------  ------  -----  --------  --------  ---  ------
00:0b:86:c0:05:00  sw-test-ap     1     10.3.3.6  g    am    tunnel   64      0x3    0xfff     enable    0    enable
00:0b:86:c0:05:08  sw-test-ap     ?     10.3.3.6  a    ap    tunnel   64      0x150  0xff0     -         0    enable
00:0b:86:c0:05:09  sw-remote-ap    ?     10.3.3.6  a    ap    bridge   64      0x150  0xff0     -         0    enable
00:0b:86:c0:05:0a  sw-remote-ap-2  ?     10.3.3.6  a    ap    tunnel   64      0x150  0xff0     -         0    enable
00:0b:86:c4:00:51  N/A             1     10.3.3.6  e    N/A   tunnel   N/A     N/A    N/A       N/A       0    N/A
Num APs:5
Num Associations:0


(WLAN_Switch) #
```

NOTE: Branch office support in AOS-W 2.4.1 has the following limitation: The number of encrypted BSSIDs in bridge mode plus the number of BSSIDs in tunnel mode cannot exceed three. For example:

- Three bridge mode BSSIDs with WEP, TKIP, and AES is OK (3+0).
- Four bridge mode BSSIDs with WEP, TKIP, AES and opensystem is *not* OK (4+0).
- Two bridge mode BSSIDs with WEP, TKIP, and two tunnel mode BSSIDs with TKIP is OK (2+1—as multiple tunnel mode BSSIDs count as one).
- Four bridge mode BSSIDs with WEP, TKIP, AES, and TKIP is *not* OK (4+0).
- Three bridge mode BSSIDs with WEP, TKIP, AES and one tunnel mode BSSID with TKIP is *not* OK (3+1).

Encryption on APs is limited to one static type (WEP, TKIP, or AES). There is no limitation on the encryption on the WLAN Switch.

Encryption on APs is limited to two dynamic types (802.1x). There is no limitation on encryption on the WLAN Switch.

Encryption on APs is limited to three dynamic types (802.1x) if there is no encryption on the WLAN Switch.

Double Encryption

The Remote AP control traffic is sent to the WLAN Switch over an IPSec tunnel. The user traffic is 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.

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

NOTE: Alcatel recommends that double-encryption not be turned on for inter-device communication over untrusted networks in AOS-W version 2.3 or later, as doing so is redundant and adds significant processing overhead for APs.

AOS-W System Defaults

A

Basic System Defaults

The default administrator user name is admin, and the default password is also admin.

Firewall Defaults

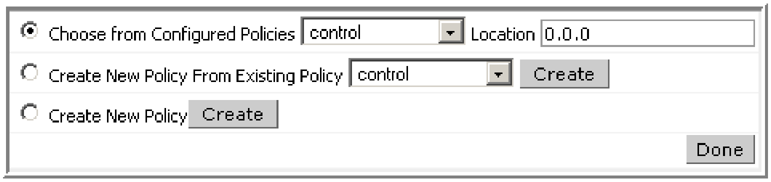
The following default netservices firewall policies and roles are included in AOS-W 2.5.

```
netservice svc-snmp-trap udp 162
netservice svc-syslog udp 514
netservice svc-l2tp udp 1701
netservice svc-ike udp 500
netservice svc-https tcp 443
netservice svc-smb-tcp tcp 445
netservice svc-dhcp udp 67 68
netservice svc-pptp tcp 1723
netservice svc-telnet tcp 23
netservice svc-tftp udp 69
netservice svc-kerberos udp 88
netservice svc-adp udp 8200
netservice svc-pop3 tcp 110
netservice svc-msrpc-tcp tcp 135 139
netservice svc-dns udp 53
netservice svc-http tcp 80
netservice svc-nterm tcp 1026 1028
netservice svc-papi udp 8211
netservice svc-ftp tcp 21
netservice svc-svp 119
netservice svc-smtp tcp 25
netservice svc-gre 47
netservice svc-smb-udp udp 445
netservice svc-esp 50
netservice svc-snmp udp 161
netservice svc-bootp udp 67 69
netservice svc-msrpc-udp udp 135 139
netservice svc-ntp udp 123
netservice svc-icmp 1
netservice svc-ssh tcp 22



ip access-list session control
  any any svc-icmp permit
  any any svc-dns permit
  any any svc-papi permit
  any any svc-adp permit
  any any svc-tftp permit
  any any svc-dhcp permit
!
ip access-list session validuser
  any any any permit
!
ip access-list session captiveportal
  user   alias mswitch svc-https permit
  user any svc-http dst-nat 8080
  user any svc-https dst-nat 8081
!
ip access-list session allowall
  any any any permit
!
ip access-list session srcnat
  user any any src-nat
!
ip access-list session vpnlogon
  user any svc-ike permit
  user any svc-esp permit
  any any svc-l2tp permit
  any any svc-pptp permit
  any any svc-gre permit
!
ip access-list session cplogout
  user   alias mswitch svc-https permit
!
ip access-list session guest
!
ip access-list session ap-acl
  any any svc-gre permit
  any any svc-syslog permit
  any user svc-snmp permit
  user any svc-snmp-trap permit
  user any svc-ntp permit
!
user-role ap-role
 session-acl control
 session-acl ap-acl
!
user-role trusted-ap
 session-acl allowall
!
user-role employee
 vlan 1
 session-acl allowall
!
user-role default-vpn-role
 session-acl allowall
!
user-role guest
 session-acl control
 session-acl cplogout
 session-acl guest1
!
user-role stateful-dot1x
!
user-role stateful
 session-acl control
!
user-role logon
 session-acl control
 session-acl captiveportal
 session-acl vpnlogon
!
```

Firewall Policies

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

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



● Choose from Configured Policies: control ▾ Location: 0.0.0

○ Create New Policy From Existing Policy: control ▾ Create

○ Create New Policy Create

Done

FIGURE A-1 User Role Traffic Policies

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

Choose from Configured Policies – Select this option to apply a traffic policy already configured in the system. By default, the policy will be applied to the user role regardless of where the user is physically located (indicated by Location 0.0.0). However, if the policy only applies while the user is associated to a particular AP or is located in a particular building or floor, fill in the "Location" field on this line. See the chapter entitled "WLAN Configuration – Advanced Location-Based AP Configuration" for more information on location codes.

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

Default Open Ports

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

TABLE A-1 Default (Trusted) Open Ports

Port Number	Protocol	Where Used	Description
17	TCP	WLAN Switch	This is use for certain types of VPN clients that accept a banner (QOTD). During normal operation, this port will only accept a connection and immediately close it.
21	TCP	WLAN Switch	FTP server for AP6X software download.
22	TCP	WLAN Switch	SSH
23	TCP	AP and WLAN Switch	Telnet is disabled by default but the port is still open
53	UDP	WLAN Switch	Internal domain
67	UDP	AP (and WLAN Switch if DHCP server is configured)	DHCP server
68	UDP	AP (and WLAN Switch if DHCP server is configured)	DHCP client
69	UDP	WLAN Switch	TFTP
80	TCP	AP and WLAN Switch	HTTP Used for remote packet capture where the capture is saved on the Access Point. Provides access to the WebUI on the WLAN Switch.

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

Port Number	Protocol	Where Used	Description
123	UDP	WLAN Switch	NTP
161	UDP	AP and WLAN Switch	SNMP. Disabled by default.
443	TCP	WLAN Switch	Used internally for captive portal authentication (HTTPS) and is exposed to wireless users. A default self-signed certificate is installed after the user explicitly selects this port to be open. Users in a production environment are urged to install a certificate from a well known CA such as Verisign. Self-signed certs are open to man-in-the-middle attacks and should only be used for testing.
500	UDP	WLAN Switch	ISAKMP
514	UDP	WLAN Switch	Syslog
1701	UDP	WLAN Switch	L2TP
1723	TCP	WLAN Switch	PPTP
2300	TCP	WLAN Switch	Internal terminal server opened by `telnet soe` command.
3306	TCP	WLAN Switch	Remote wired MAC lookup.

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

Port Number	Protocol	Where Used	Description
4343	TCP	WLAN Switch	HTTPS. A different port is used from 443 in order to not conflict with captive portal. A default self-signed certificate is installed after the user explicitly selects this port to be open. Users in a production environment are urged to install a certificate from a well known CA such as Verisign. Self-signed certs are open to man-in-the-middle attacks and should only be used for testing
4500	UDP	WLAN Switch	sae-urn
8080	TCP	WLAN Switch	Used internally for captive portal authentication (HTTP-proxy). Not exposed to wireless users.
8081	TCP	WLAN Switch	Used internally for captive portal authentication (HTTPS). Not exposed to wireless users. A default self-signed certificate is installed after the user explicitly selects this port to be open. Users in a production environment are urged to install a certificate from a well known CA such as Verisign. Self-signed certs are open to man-in-the-middle attacks and should only be used for testing.
8082	TCP	WLAN Switch	Used internally for single sign-on authentication (HTTP). Not exposed to wireless users.
8083	TCP	WLAN Switch	Used internally for single sign-on authentication (HTTPS). Not exposed to wireless users.
8088	TCP	WLAN Switch	Internal

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

Port Number	Protocol	Where Used	Description
8200	UDP	WLAN Switch	Alcatel Discovery Protocol (ADP)
8211	UDP	WLAN Switch	Internal
8888	TCP	WLAN Switch	Used for HTTP access.

Radius Server Defaults

```
# aaa radius-server <name of RADIUS server> <acctport portnumber>...<mode enable|disable> <Enter>
```

The parameters and defaults for this command are:

acctport	Port number used for accounting	default = 1813
authport	Port number used for authentication	default = 1812
host	The IP address of the RADIUS server.	default = 0.0.0.0
inservice	Bring server in service immediately.	default = Y
key	Shared secret text string	default = “changeme”
mode	Enable or Disable as an authentication server	default = disabled
retransmit	Maximum times a RADIUS request is retried	default = 3
timeout	Specify time period between RADIUS requests.	default = 10

Volume 4

Configuring Wireless Encryption and Authentication

AOS-W User Guide

Release 2.5.3

Copyright

Specifications in this manual are subject to change without notice.

Originated in the USA.

Trademarks

AOS-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 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

This preface includes the following information:

- An overview of the contents of 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

The *AOS-W User Guide* is now in eight separate volumes for easier download and information access. The volumes are as follows:

- Volume 1 contains an overview of the OmniAccess System.
- Volume 2 describes how to install the OmniAccess System in a wired network.
- Volume 3 describes WLAN configuration, including remote Access Points.
- Volume 4 (this volume) describes wireless encryption and authentication configuration.
- Volume 5 describes configuring multi-WLAN switch environments.
- Volume 6 describes intrusion prevention configuration.
- Volume 7 describes managing the OmniAccess System.
- Volume 8 describes configuring advanced services, such as Quality of Service (QoS) for voice and the External Services Interface module.

Related Documents

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

- *AOS-W User Guide*
- *Alcatel Wireless LAN Switch Installation Guides*

- *Alcatel Access Point Installation Guides*
- *Release Notes*

Text Conventions

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

TABLE 1 Text Conventions

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>	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: # **send** *<text message>* 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 | Item B }	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Contacting Alcatel

Contact Center Online		
■	Main Site	http://www.alcatel.com/enterprise
■	Support Site	http://eservice.ind.alcatel.com
■	Email	support@ind.alcatel.com
Sales & Support Contact Center Telephone		
■	North America	1-800-995-2696
■	Latin America	1-877-919-9526
■	Europe	+33 (0) 38 85 56 92 9
■	Asia Pacific	+65 6586 1555
■	Worldwide	1-818-880-3500

Configuring Firewall Roles and Policies 1

Firewall roles and policies form the cornerstone of all functionality in an Alcatel WLAN Switch. Every user in an Alcatel network is associated with a role, which is a set of network privileges defined by firewall policies.

This chapter describes the following topics:

User Roles

Every user that associates to the Alcatel network is placed in a pre-defined role called the *"logon"* role that has enough privileges to allow one of the authentication methods to authenticate the user. After authentication, the user can assume a different role. The role of an authenticated user can be derived from the following mechanisms:

- Server derivation rules: The administrator can configure rules to match attributes returned by the authentication server (such as attributes returned by a RADIUS server) 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 Chapter 2, "Configuring AAA Servers" for explanation on how to configure rules.

- User derivation rules: The administrator can configure rules to match a user characteristic to derive a role for the user. The various user characteristics that can be used to derive a user role are:

  - **BSSID** of the AP to which the client is associated
  - **Encryption type** used by the client
  - **ESSID** to which the client is associated
  - **Location** of the AP to which the client is associated
  - **MAC address** of the client

  For example, you 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.*

- Default role for an authentication method: Every authentication method can have a default role for users that are successfully authenticated using that method. For example, you can configure the default role of all users authenticated using 802.1x as *"employee"*. Refer to the chapters that explain the various authentication methods (802.1x, VPN, captive portal) for more details on how to configure the default user role.

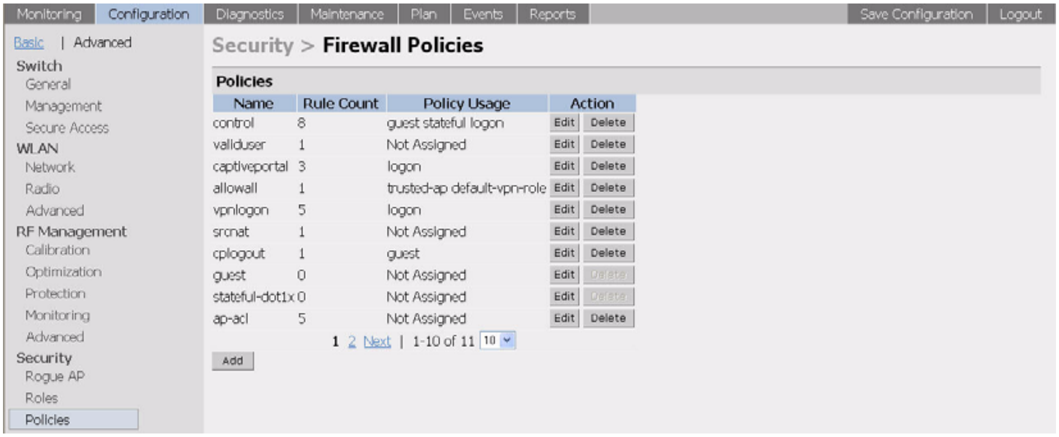
Configuring Policies

This section describes the steps to configure the rules that constitute a policy. A 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 > Advanced > Security > Policies** page on the WebUI.

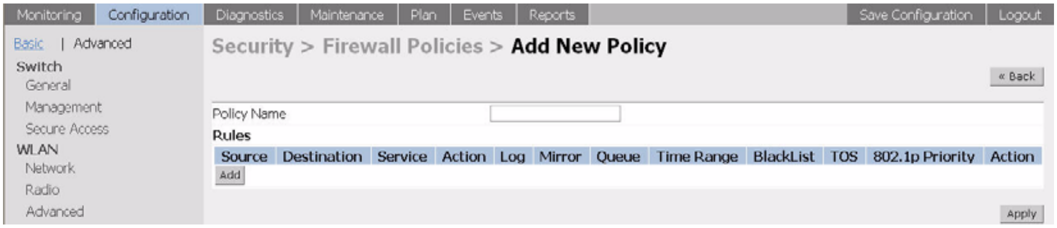


Security > Firewall Policies

Policies

Name	Rule Count	Policy Usage	Action
control	8	guest stateful logon	Edit Delete
validuser	1	Not Assigned	Edit Delete
captiveportal	3	logon	Edit Delete
allowall	1	trusted-ap default-vpn-role	Edit Delete
vpnlogon	5	logon	Edit Delete
srcnat	1	Not Assigned	Edit Delete
cplogout	1	guest	Edit Delete
guest	0	Not Assigned	Edit Delete
stateful-dot1x	0	Not Assigned	Edit Delete
ap-acl	5	Not Assigned	Edit Delete

2. Click **Add** to create a new policy.



Security > Firewall Policies > Add New Policy

Policy Name

Rules

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Action

3. Click **Add** to add a rule to the policy being created. The following table describes required and optional fields for a rule.

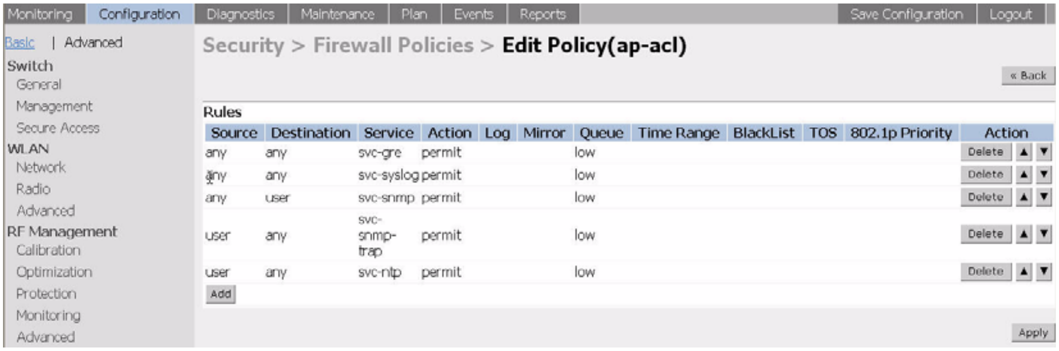
TABLE 1-1 Required and Optional Rule Fields

Field	Required/ Optional	Description
Source	Required	Source of the traffic, which can 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, you must 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, you must configure the IP address and network mask of the subnet. ■ ***alias****:* This refers to using an alias for a host or network. You configure the alias by navigating to the **Configuration > Advanced > Security > Advanced > Destinations** page.
Destination	Required	Destination of the traffic, which can be configured in the same manner as Source.
Service	Required	Type of traffic, which can be one of the following: ■ ***any***: This option specifies that this rule applies to any type of traffic. ■ ***tcp***: Using this option, you configure a range of TCP port(s) to match for the rule to be applied. ■ ***udp***: Using this option, you configure a range of UDP port(s) to match for the rule to be applied. ■ ***service****:* Using this option, you use one of the pre-defined services (common protocols such as HTTPS, HTTP, and others) as the protocol to match for the rule to be applied. ■ ***protocol***: Using this option, you specify a different layer 4 protocol (other than TCP/UDP) by configuring the IP protocol value.

TABLE 1-1 Required and Optional Rule Fields (Continued)

Action	Required	The action that you want the WLAN Switch to perform on a packet that matches the specified criteria. This can be one of the following: ■ ***permit:*** Permits traffic matching this rule. ■ ***drop:*** Drops packets matching this rule without any notification. ■ ***reject:*** Drops the packet and sends an ICMP notification to the traffic source. ■ ***src-nat:*** Performs network address translation (NAT) on packets matching the rule. When this option is selected, you need to select a NAT pool. (If this pool is not configured, you configure a NAT pool by navigating to the **Configuration > Advanced > Security > Advanced > NAT Pools**.) ■ ***dst-nat:*** This option redirects 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 WLAN Switch as used in the pre-defined policy called *"captiveportal"*. ■ ***redirect to tunnel:*** This option redirects traffic into a GRE tunnel. This option is used primarily to redirect all guest traffic into a GRE tunnel to a DMZ router/switch.
Log	Optional	Select this option to log a match to this rule. This is recommended 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.
Queue	Optional	The queue in which a packet matching this rule should be placed. Select **High** for higher priority data, such as voice, and **Low** for lower priority traffic.
Black List	Optional	Select this option if it is required to automatically blacklist a client that is the source or destination of traffic matching this rule. This option is recommended for rules that indicate a security breach where the blacklisting option can be used to prevent access to clients that are attempting to breach the security.
TOS	Optional	Value of type of service (TOS) bits to be marked in the IP header of a packet matching this rule when it leaves the WLAN Switch.
802.1p Priority	Optional	Value of 802.1p priority bits to be marked in the frame of a packet matching this rule when it leaves the WLAN Switch.

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.



Security > Firewall Policies > **Edit Policy(ap-acl)**

Rules

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Action
any	any	svc-gre	permit			low					Delete ▲ ▼
any	any	svc-syslog	permit			low					Delete ▲ ▼
any	user	svc-snmp	permit			low					Delete ▲ ▼
user	any	svc-snmp-trap	permit			low					Delete ▲ ▼
user	any	svc-ntp	permit			low					Delete ▲ ▼

NOTE: Rules can be re-ordered by the using the up and down buttons provided for each rule.

5. When all the required rules are created and ordered in the policy, click **Apply** to apply this configuration.

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

Editing an Existing Policy

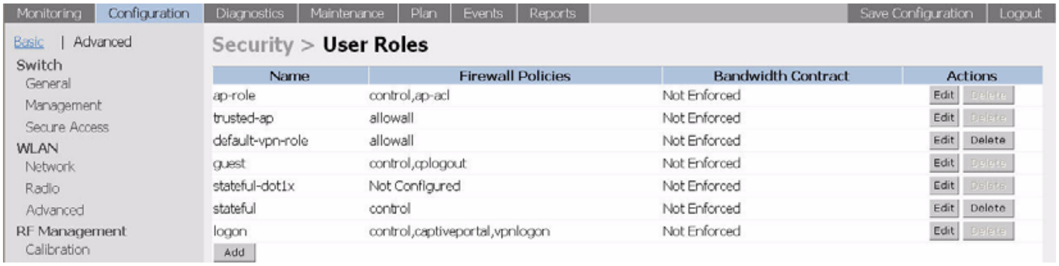
1. Navigate to the **Configuration** > **Advanced** > **Security** > **Policies** page. This page shows the list of current policies.
2. Click **Edit** in the **Action** column for the policy that is to be edited.
3. On the Edit policy page, you can delete existing rules, add new rules (following the same procedure in step 3 of "Creating a New Policy" on page 3), or reorder the policies.
4. When all rules have been edited as required, click **Apply** to apply the configuration.

NOTE: The changes do not take effect until the configuration is applied.

Creating a New User Role

This section describes how to create a new user role. When you create a user role, you specify one or more firewall policies for the role.

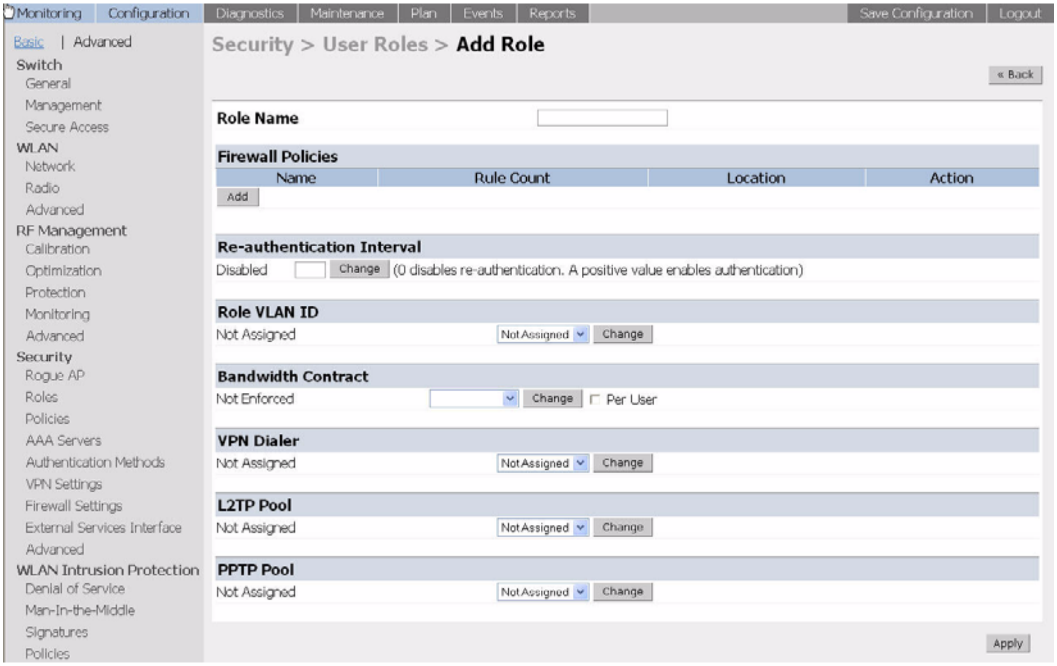
1. Navigate to the **Configuration** > **Advanced** > **Security** > **Roles** page.



Security > **User Roles**

Name	Firewall Policies	Bandwidth Contract	Actions
ap-role	control,ap-acl	Not Enforced	Edit Delete
trusted-ap	allowall	Not Enforced	Edit Delete
default-vpn-role	allowall	Not Enforced	Edit Delete
guest	control,cplogout	Not Enforced	Edit Delete
stateful-dot1x	Not Configured	Not Enforced	Edit Delete
stateful	control	Not Enforced	Edit Delete
logon	control,captiveportal,vpnlogon	Not Enforced	Edit Delete

2. Click **Add** to create and configure a new user role.



Security > User Roles > **Add Role**

Role Name

Firewall Policies

Name	Rule Count	Location	Action

Re-authentication Interval

Disabled (0 disables re-authentication. A positive value enables authentication)

Role VLAN ID

Not Assigned — Not Assigned

Bandwidth Contract

Not Enforced □ Per User

VPN Dialer

Not Assigned — Not Assigned

L2TP Pool

Not Assigned — Not Assigned

PPTP Pool

Not Assigned — Not Assigned

3. Enter the desired name for the role.

The following table describes the different fields for the user role.

TABLE 1-2 User Role Fields

Field	Description
Firewall Policies	This consists of the policies that define the 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 *building.floor.location* format to represent either a specific AP or a set of APs (use the wildcard value 0). There are three ways to add a firewall policy to a user role: ■ Choose from configured policies (see "Creating a New Policy" on page 3): 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 a configured policy: This option can be used to create a new policy that is derived from an existing policy. ■ Create a new policy: The rules for the policy can be added as explained "Creating a New Policy" on page 3.
Role Vlan-ID	By default, a user is assigned a VLAN on the basis of the ingress VLAN for the user to the WLAN Switch. You can override this assignment and 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.
Bandwidth contract	You can assign a bandwidth contract to provide an upper limit to the bandwidth utilized by users in this role. As an example, the administrator may want to cap the total bandwidth used by the guest users in a network to 2Mbps. You can select the Per User option to apply the bandwidth contracts on a per-user basis instead of to all users in the role. To create a new bandwidth contract, select the *"Add New"* option from the drop-down menu. 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.

TABLE 1-2 User Role Fields (Continued)

VPN Dialer	This assigns a VPN dialer to a user role. For details about VPN dialer, refer to the "Configuring Remote APs" chapter. 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.
L2TP Pool	This assigns an L2TP pool to the user role. For more details about L2TP pools, refer to the "Configuring VPNs" chapter. 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.
PPTP Pool	This assigns a PPTP pool to the user role. For more details about PPTP pools, refer to the "Configuring VPNs" chapter. 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.

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

NOTE: The role is not created until the configuration is applied.

To edit an existing role, click **Edit** for the user role. The fields are the same as for a new user role. For example, you can add a firewall policy to a user role.

Configuring AAA Servers 2

The AOS-W software allows you to use an external authentication server or an internal user database to authenticate users who need to access the wireless network.

This chapter describes how to configure AOS-W to interface with an external Remote Authentication Dial-In User Service (RADIUS) or Lightweight Directory Access Protocol (LDAP) authentication server, and how to add entries into the internal database.

NOTE: In order for an external authentication server to process requests from the Alcatel WLAN Switch, you must configure the server to recognize the WLAN Switch. Refer to the vendor documentation for the external authentication server for information on how to do this.

This chapter describes the following topics:

Configuring External Authentication Servers

This section describes how to configure RADIUS and LDAP authentication servers on the WLAN Switch.

Configuring a RADIUS Server

1. Collect the following information required for RADIUS server configuration:

TABLE 2-1 RADIUS Server Configuration Information

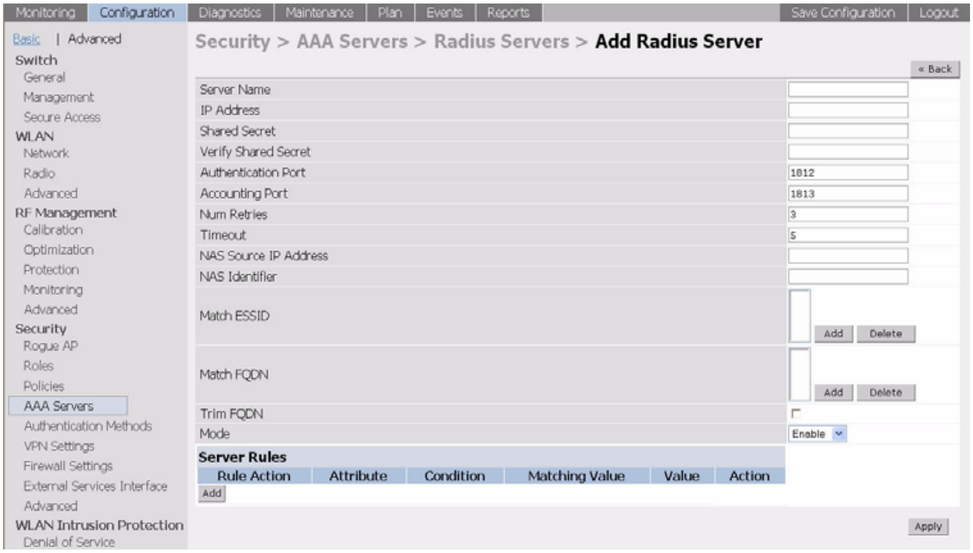
Parameter	Description
Server Name	Name of the RADIUS authentication server
IP Address	IP address of the authentication server

TABLE 2-1 RADIUS Server Configuration Information (Continued)

Shared Secret	Shared secret between the WLAN Switch and the authentication server
Authentication Port	Authentication port on the server (default is 1812)
Accounting Port	Accounting port on the server (default is 1813)
Num Retries	Maximum number of retries sent to the server by the WLAN Switch before the server is marked as down (default is 3)
Timeout	Maximum time, in seconds, that the WLAN Switch waits before timing out the request and resending it (default is 5 seconds)

2. Navigate to the **Configuration > Advanced > Security > AAA Servers > RADIUS Servers** page.

3. Click **Add** to add a new RADIUS server entry. Enter the values gathered in the earlier step.



Security > AAA Servers > Radius Servers > **Add Radius Server**

Server Name	
IP Address	
Shared Secret	
Verify Shared Secret	
Authentication Port	1812
Accounting Port	1813
Num Retries	3
Timeout	5
NAS Source IP Address	
NAS Identifier	
Match ESSID	
Match FQDN	
Trim FQDN	□
Mode	Enable

Server Rules

Rule Action	Attribute	Condition	Matching Value	Value	Action

NOTE: If you installed the ESI license in the Alcatel WLAN Switch, users can be authenticated by specific servers based on the fully-qualified domain name (FQDN) and Extended Service Set Identifier (ESSID) of the client. See "Configuring the External Services Interface License" on page 19 for more information.

4. Set the **Mode** to **Enable** to activate the authentication server.

NOTE: When you configure a server, you can set the VLAN and role for users based on attributes returned for the user during authentication. These values take precedence over the default role and VLAN configured for the user. See "Configuring Server Rules" on page 16 for more information.

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

   NOTE: The configuration does not take effect until you perform this step.

To edit or delete a RADIUS Server entry, click **Edit** or **Delete** in the **Action** column of the RADIUS server entry.

- If you are editing the entry, enter your changes, then click **Apply** to save the configuration.
- If you are deleting the entry, a pop-up window displays the message "Are you sure you want to delete the RADIUS server <server_name>?" Click **OK** to delete the entry.

Configuring an LDAP Server

NOTE: AOS-W v2.4 and later support Secure LDAP.

1. Collect the following information required for LDAP server configuration:

TABLE 2-2 LDAP Server Configuration Information

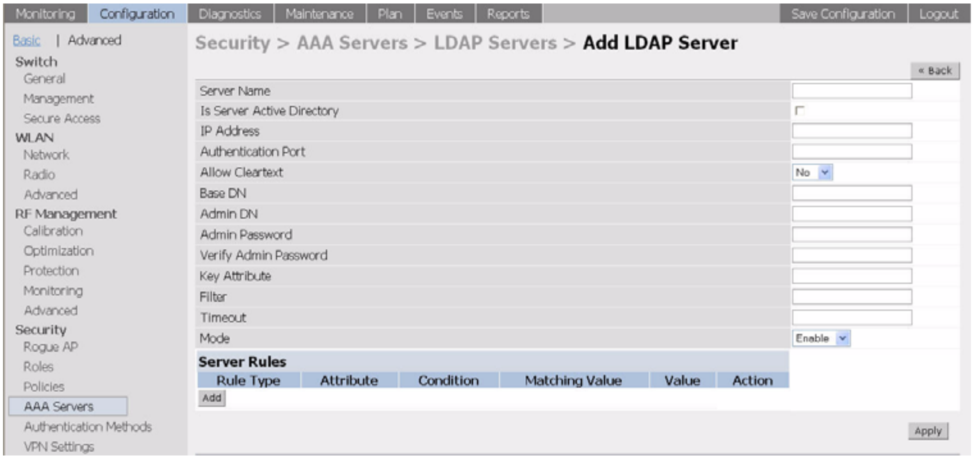
Parameters	Description
Server Name	Name of the LDAP server
IP Address	IP address of the LDAP server
Authentication Port	Port on which the LDAP server is configured (default is 389)
Base DN	Distinguished Name of the node which contains the entire user database to use
Admin DN	User who has read/search privileges across all the entries in the LDAP database (the user need not have write privileges but the user should be able to search the database, and read attributes of other users in the database)

TABLE 2-2 LDAP Server Configuration Information (Continued)

Key Attribute	Attribute that contains the unique key for the LDAP object (This is the name of the attribute that contains the login ID of the users.)
Filter	Filter that should be applied to search of the user in the LDAP database (default filter string is: ì(objectclass=*)î)
Timeout	Timeout period of a LDAP request in seconds (default is 10 seconds)

2. Navigate to the **Configuration** > **Advanced** > **Security** > **AAA Servers** > **LDAP Servers** page.

3. Click **Add** to add a new LDAP server entry. Enter the values collected in the earlier step.



Security > AAA Servers > LDAP Servers > **Add LDAP Server**

Server Name	
Is Server Active Directory	□
IP Address	
Authentication Port	
Allow Cleartext	No
Base DN	
Admin DN	
Admin Password	
Verify Admin Password	
Key Attribute	
Filter	
Timeout	
Mode	Enable

Server Rules

Rule Type	Attribute	Condition	Matching Value	Value	Action

4. Set the **Mode** to **Enable** to activate the authentication server.

   NOTE: When you configure a server, you can set the VLAN and role for users based on attributes returned for the user during authentication. These values take precedence over the default role and VLAN configured for the user. See “Configuring Server Rules” on page 16 for more information.

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

   NOTE: The configuration does not take effect until you perform this step.

To edit or delete an LDAP Server entry, click **Edit** or **Delete** in the **Action** column of the LDAP server entry.

- If you are editing the entry, enter your changes, then click **Apply** to save the configuration.

- If you are deleting the entry, a pop-up window displays the message “Are you sure you want to delete the LDAP server <server_name>?” Click **OK** to delete the entry.

Adding Users to the Internal Database

You can create entries in an internal database that can be used to authenticate users. The internal database contains a list of users along with the password and default role for each user. When you configure the WLAN Switch as the primary server, user information in incoming authentication requests is checked against the internal database.

NOTE: When you configure a server, you can set the VLAN and role for users based on attributes returned for the user during authentication. These values take precedence over the default role and VLAN configured for the user. See “Configuring Server Rules” on page 16 for more information.

To add a user to the internal database:

1. Collect the following information required for internal database entries:

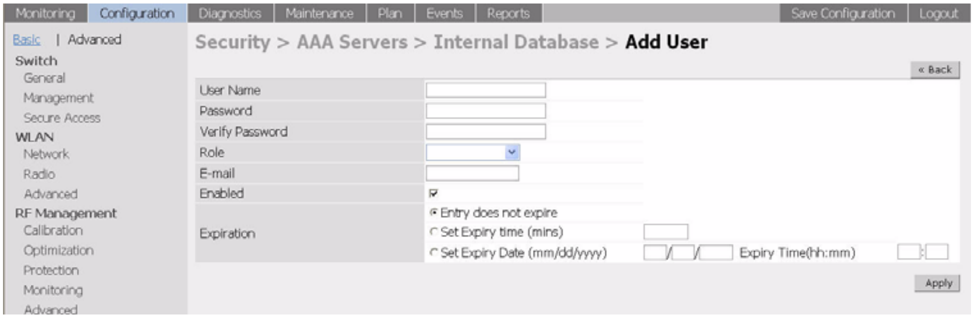
TABLE 2-3 Internal Database Configuration Information

Parameters	Description
User Name	User name (mandatory field)
Password	Password (mandatory field)
Role	Role for the user if not otherwise configured (optional field, default is guest)
E-mail	E-mail address of the user
Entry does not expire/Expiration	No expiration on user entry, expiration duration (in minutes), or specific time and date of expiration

2. Navigate to the **Configuration > Advanced > Security > AAA Servers > Internal Database** page.

   NOTE: When you add users to the internal database, you can set the VLAN and role for users based on attributes returned for the user during authentication. These values take precedence over the default role and VLAN configured for the user. See “Configuring Server Rules” on page 16 for more information.

3. Click **Add User** in the Users section. The user configuration page displays.



Security > AAA Servers > Internal Database > **Add User**

User Name	
Password	
Verify Password	
Role	
E-mail	
Enabled	☑
Expiration	● Entry does not expire ○ Set Expiry time (mins) ○ Set Expiry Date (mm/dd/yyyy) / / Expiry Time(hh:mm) :

4. Enter the information for the user.
5. Click **Enabled** to activate this entry on creation.
6. Click **Apply** to apply the configuration.

   NOTE: The configuration does not take effect until you perform this step.

To edit or delete an internal database entry, click **Edit** or **Delete** in the **Action** column of the entry.

- If you are editing the entry, enter your changes, then click **Apply** to save the configuration.
- If you are deleting the entry, a pop-up window displays the message "Are you sure you want to delete user <user_name>?" Click **OK** to delete the entry.

Configuring Server Rules

When you configure an external authentication server or the internal database, you can set the VLAN or role for users based on attributes returned for the user during authentication. These values take precedence over the default role and VLAN configuration for the authenticated user.

The parameters are:

TABLE 2-4 Server Rules

Parameter	**Description**
Rule Type	This can be either Role Assignment or VLAN Assignment. With Role assignment, a user can be assigned a specific role based on the attributes returned. In case of VLAN assignment, the user can be placed in a specific VLAN based on the attributes returned.
Attribute	This is the attribute returned by the authentication server that is examined for *Condition* and *Value* match.
Condition	This is the match method by which the string in *Value* is matched with the attribute value returned by the authentication server. ■ contains – The rule is applied if and only if the attribute value contains the string in parameter *Value.* ■ starts-with – The rule is applied if and only if the attribute value returned starts with the string in parameter *Value.* ■ ends-with – The rule is applied if and only if the attribute value returned ends with the string in parameter *Value.* ■ equals - The rule is applied if and only if the attribute value returned equals the string in parameter *Value.* ■ not-equals - The rule is applied if and only if the attribute value returned is not equal to the string in parameter *Value.* ■ 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. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the WLAN Switch when the rule is applied.
Value	This is the string to which the value of the returned attribute is matched.
Role / VLAN	The role or the VLAN applied to the user when the rule is matched.

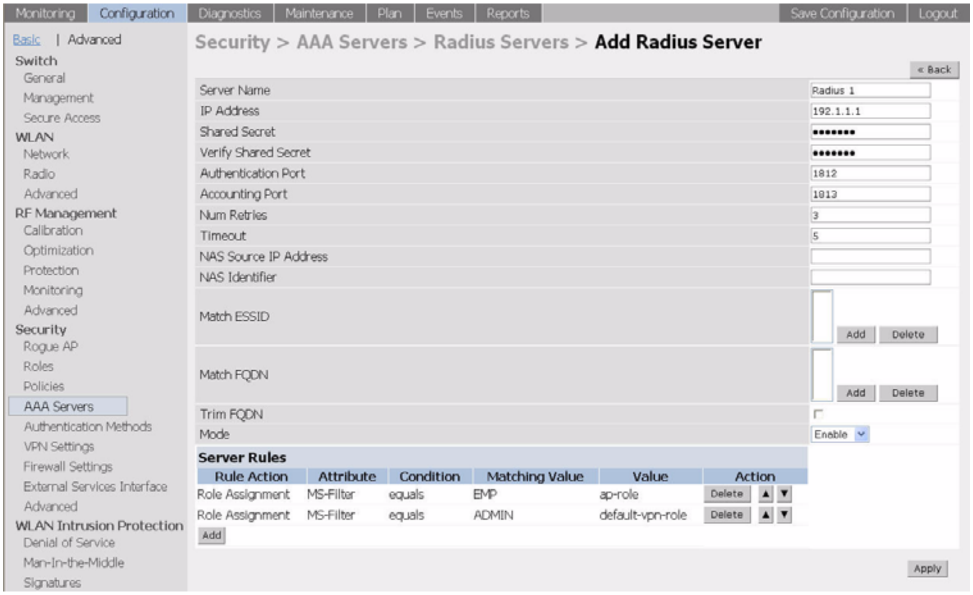
The server rules are applied based on the first match principle. The first rule that is applicable for the server and the attribute returned is applied to the user and would be the only rule applied from the server rules.

These rules are applied uniformly across all the authentication types that use the server as the primary authentication server.

In the following example, users will be classified as admin or employee based on the filter-ID returned.

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.



Security > AAA Servers > Radius Servers > **Add Radius Server**

Server Name	Radius 1
IP Address	192.1.1.1
Shared Secret	•••••••
Verify Shared Secret	•••••••
Authentication Port	1812
Accounting Port	1813
Num Retries	3
Timeout	5
NAS Source IP Address	
NAS Identifier	
Match ESSID	
Match FQDN	
Trim FQDN	□
Mode	Enable

Server Rules

Rule Action	Attribute	Condition	Matching Value	Value	Action
Role Assignment	MS-Filter	equals	EMP	ap-role	Delete ▲ ▼
Role Assignment	MS-Filter	equals	ADMIN	default-vpn-role	Delete ▲ ▼

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

Configuring Authentication Timers

You can configure the following timers that apply to all users and RADIUS servers:

- User Idle Timeout is the time, in minutes, that a client has to respond to the WLAN Switch before it has to re-authenticate itself to gain access to the network. To prevent users from timing out, set the value in the field to 0.

- Authentication Server Dead Time is the maximum period, in minutes, that the WLAN Switch considers an unresponsive authentication server to be down. This timer only applies when there are two or more authentication servers configured.

  This field is only applicable if there are two or more authentication servers configured on the WLAN Switch. If there is only one authentication server configured, the server is never considered down and all requests are sent to the server.

  If one or more backup servers are configured and a server is unresponsive, it is marked as down for the dead time; subsequent requests are sent to the next server on the priority list for the duration of the dead time. If the server is responsive after the dead time has elapsed, it can take over servicing requests from a lower-priority server; if the server continues to be unresponsive, it is marked as down for the dead time.
- Logon User Lifetime

These timers can be left at the default values for most implementations.

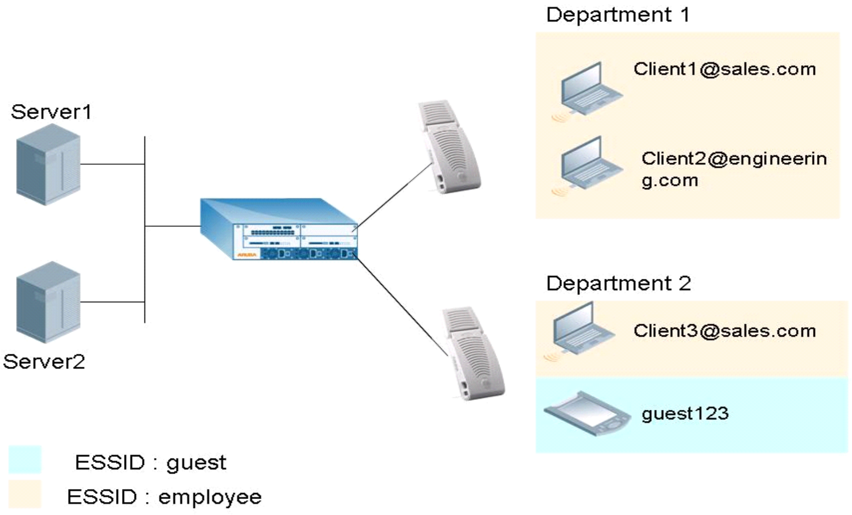
To set an authentication timer:

1. Navigate to the **Configuration** > **Advanced** > **Security** > **AAA Servers** page; click the **General** tab if it is not already selected.
2. Configure the timers as described above.
3. Click **Apply** before moving on to another page or closing the browser window. Failure to do this results in loss of configuration and you will have to reconfigure the settings.

Configuring the External Services Interface License

Alcatel's External Services Interface (ESI) license allows 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 by the client-associated Extended Service Set Identifier (ESSID).

NOTE: To use this feature, you must have the ESI license installed in the Alcatel WLAN Switch.



In the topology shown above, all clients authenticate using the same method (for example, captive portal). With the ESI license installed in the WLAN Switch, AOS-W allows all users using `sales.com` in their user name (Client1 and Client3 in the example) to always authenticate against authentication server *Server1* and the users using `engineering.com` in their user name (Client2 in the example) to always authenticate against *Server2*. AOS-W also supports users associating with the guest ESSID to authenticate against *Server2*.

This feature adds flexibility to AAA configuration by allowing IT managers to maintain authentication servers by departments or ESSIDs in different campuses, or merge clients and servers from two different companies.

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

Selecting the Right Server

The selection of an authentication server occurs in the following order of server prioritization:

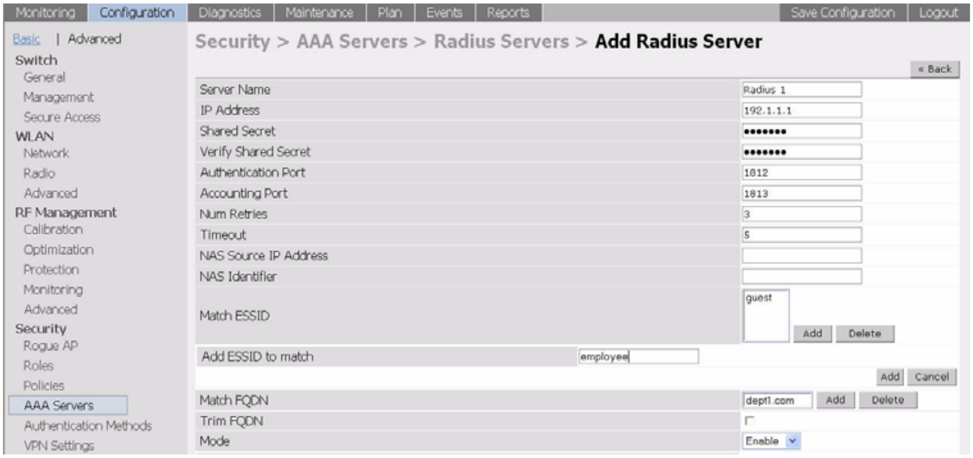
1. Server is skipped if it is disabled or out of service.
2. Server is selected if there are no FQDN and ESSID filters configured.
3. Server is selected if the user ESSID matches any ESSID attached with the server.

4. Server is selected if the user name has a FQDN component and it matches any FQDN attached with the server.

NOTE: An FQDN match is attempted if, and only if, the user name has a FQDN component and the server has at least one FQDN configured for matching. If the server has a FQDN list configured, but the user name does not have a FQDN component, the server is not selected.

Configuring FQDN or ESSID on the Server

1. Navigate to the **Configuration** > **Advanced** > **Security** > **AAA Servers** > **RADIUS** page.
2. To add a new server, follow the steps described in "Configuring a RADIUS Server" on page 11.
3. To modify server settings, click **Edit** in the Action column of the server entry.
4. To add a new ESSID to be used by this server, click **Add** in the Match ESSID section.
5. In the Add ESSID to match field, add the ESSID as configured (the ESSID is case sensitive) and click **Add**. Repeat this step to add more ESSIDs to be used by this server.



Security > AAA Servers > Radius Servers > **Add Radius Server**

Server Name	Radius 1
IP Address	192.1.1.1
Shared Secret	•••••••
Verify Shared Secret	•••••••
Authentication Port	1812
Accounting Port	1813
Num Retries	3
Timeout	5
NAS Source IP Address	
NAS Identifier	
Match ESSID	guest
Add ESSID to match	employee
Match FQDN	dept1.com
Trim FQDN	□
Mode	Enable

6. To add the domains that this server will use, click **Add** in the Match FQDN section.
7. In the Add FQDN to match field, add the entry and click **Add**. To add more entries, repeat this step.

8. To trim the FQDN portion of the user name before sending the credentials to the authentication server, select the Trim FQDN option. If this option is not selected, the user name 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 user name the user uses to authenticate. If Trim FQDN is selected, only `Client3` is sent to the server. If not selected, `Client3@sales.com` is sent to the server for authentication.

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

Configuring 802.1x Authentication 3

802.1x is an Institute of Electrical and Electronics Engineers (IEEE) standard that provides an authentication framework for WLANs. 802.1x uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1x framework that are suitable for wireless networks include EAP-Transport Layer Security (EAP-TLS), Protected EAP (PEAP), and EAP-Tunneled TLS (EAP-TTLS). These protocols allow the network to authenticate the client while also allowing the client to authenticate the network.

This chapter describes the following topics:

802.1x Authentication

802.1x authentication consists of three components:

- The *supplicant,* or client, is the device attempting to gain access to the network. You can configure the Alcatel OmniAccess system to support 802.1x authentication for wired users as well as wireless users.
- The *authenticator* is the gatekeeper to the network and permits or denies access to the supplicants.

  The Alcatel WLAN Switch acts as the authenticator, relaying information between the authentication server and supplicant. The EAP type must be consistent between the authentication server and supplicant and is transparent to the WLAN Switch.
- The *authentication server* provides a database of information required for authentication and informs the authenticator to deny or permit access to the supplicant.

  The 802.1x authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS) server which can authenticate either users (through passwords or certificates) or the client computer.

In Alcatel OmniAccess systems, you can terminate the 802.1x authentication on the WLAN Switch. The WLAN Switch passes user authentication to its internal database or to a "backend" non-802.1x server. This feature, also called *"AAA FastConnect*," is useful for deployments where an 802.1x EAP-compliant RADIUS server is not available or required for authentication.

Authentication with a RADIUS Server

Figure 3-1 is an overview of the parameters that you need to configure on authentication components when the authentication server is an 802.1x EAP-compliant RADIUS server.

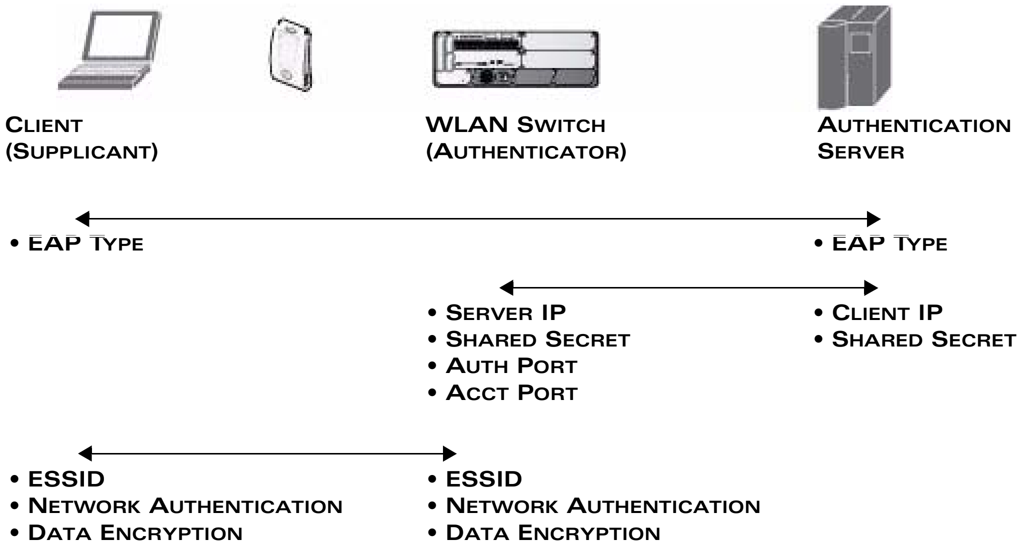


Figure 3-1 802.1x Authentication with RADIUS Server

The supplicant and authentication server must be configured to use the same EAP type. The WLAN Switch does not need to know the EAP type used between the supplicant and authentication server.

For the WLAN Switch to communicate with the authentication server, you must configure the IP address, authentication port, and accounting port of the server on the WLAN Switch. The authentication server must be configured with the IP address of the RADIUS client, which is the WLAN Switch in this case. Both the WLAN Switch and the authentication server must be configured to use the same shared secret.

As described in the "Overview of the Alcatel OmniAccess System" in Volume 1, the client communicates with the WLAN Switch through a GRE tunnel in order to form an association with an AP and to authenticate to the network. Therefore, the network authentication and encryption configured for an ESSID must be the same on both the client and the WLAN Switch.

"Configuring 802.1x Authentication" on page 26 describes 802.1x configuration on the WLAN Switch.

Authentication Terminated on WLAN Switch

Figure 3-2 is an overview of the parameters that you need to configure on 802.1x authentication components when 802.1x authentication is terminated on the WLAN Switch (AAA FastConnect). User authentication is performed either via the WLAN Switch's internal database or a non-802.1x server.

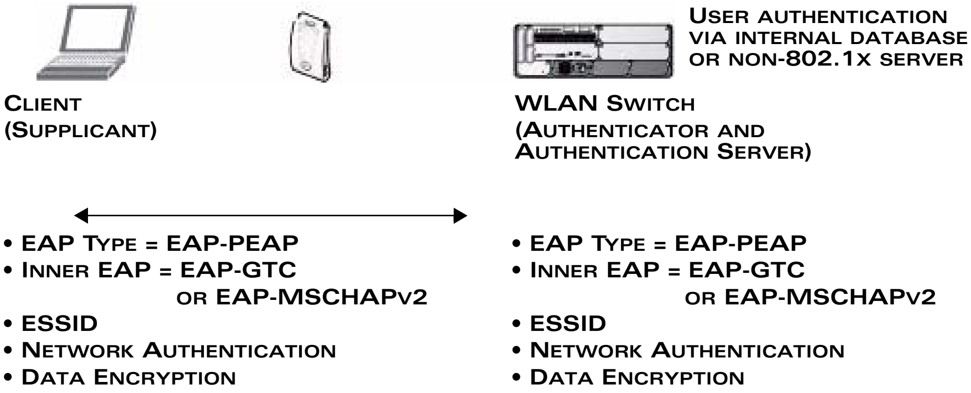

User Authentication via internal database or non-802.1x server
Client (Supplicant)
WLAN Switch (Authenticator and Authentication Server)
• EAP Type = EAP-PEAP
• Inner EAP = EAP-GTC or EAP-MSCHAPv2
• ESSID
• Network Authentication
• Data Encryption
• EAP Type = EAP-PEAP
• Inner EAP = EAP-GTC or EAP-MSCHAPv2
• ESSID
• Network Authentication
• Data Encryption

Figure 3-2 802.1x Authentication with Termination on WLAN Switch

In this scenario, the supplicant must be configured for Protected EAP (PEAP) as the WLAN Switch only supports PEAP. PEAP uses Transport Layer Security (TLS) to create an encrypted tunnel. Within the tunnel, one of the following EAP methods is used:

- EAP-Generic Token Card (GTC): Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of an LDAP or RADIUS server as the user authentication server. You can also enable caching of user credentials on the WLAN Switch as a backup to an external authentication server.
- EAP-Microsoft Challenge Authentication Protocol version 2 (MS-CHAPv2): Described in RFC 2759, this EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the backend authentication server.

If you are using the WLAN Switch's internal database for user authentication, you need to add the names and passwords of the users to be authenticated. If you are using an LDAP server for user authentication, you need to configure the LDAP server on the WLAN Switch, and configure user IDs and passwords. If you are using a RADIUS server for user authentication, you need to configure the RADIUS server on the WLAN Switch.

The following section describes how to configure 802.1x authentication on the WLAN Switch.

Configuring 802.1x Authentication

On the WLAN Switch, use the following steps to configure a wireless network that uses 802.1x authentication:

1. Configure policies and roles. You can specify a default role for users who are successfully authenticated using 802.1x. You can also configure server derivation rules to assign a user role based on attributes returned by the authentication server; server-derived user roles take precedence over default roles. For more information about policies and roles, see Chapter 1, "Configuring Firewall Roles and Policies."

   NOTE: The AOS-W Policy Enforcement Firewall module provides identity-based security for wired and wireless users and must be installed on the WLAN Switch. The stateful firewall allows user classification based on user identity, device type, location and time of day and provides differentiated access for different classes of users. For information about obtaining and installing licenses, see "Managing Software Feature Licenses" in Volume 7 of the *AOS-W User Guide*.

2. Configure the authentication server. The server can be an 802.1x RADIUS server or, if you are using AAA FastConnect, a non-802.1x server or the WLAN Switch's internal database. If you are using EAP-GTC within a PEAP tunnel, you can configure an LDAP or RADIUS server as the authentication server. See Chapter 2, "Configuring AAA Servers."

3. Configure 802.1x authentication. In the WebUI, you can enable and configure 802.1x authentication by navigating to the Configuration > Advanced > Security > Authentication Methods > 802.1x Authentication page. See "802.1x Authentication Page" on page 27.

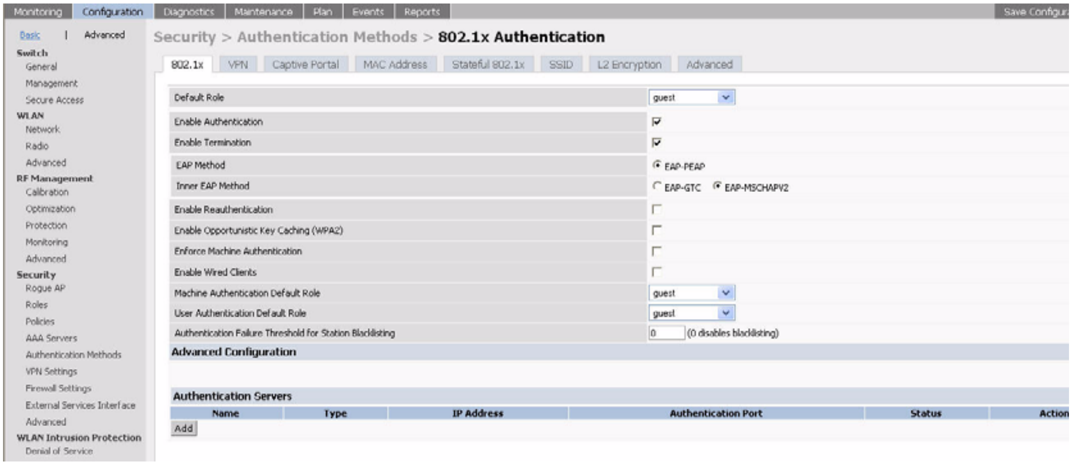
4. Configure the VLANs to which the authenticated users will be assigned. See "Configuring Network Parameters" in Volume 2 of the *AOS-W User Guide*.

5. Configure the WLAN, specifying the authentication and encryption that matches the wireless client configuration.

For details on how to complete the above steps, see "Example Configurations" on page 32.

802.1x Authentication Page

In the WebUI, you configure 802.1x authentication in the Configuration > Advanced > Security > Authentication Methods > 802.1x Authentication page (shown below).



Security > Authentication Methods > **802.1x Authentication**

Default Role	guest
Enable Authentication	☑
Enable Termination	☑
EAP Method	● EAP-PEAP
Inner EAP Method	○ EAP-GTC ● EAP-MSCHAPV2
Enable Reauthentication	☐
Enable Opportunistic Key Caching (WPA2)	☐
Enforce Machine Authentication	☐
Enable Wired Clients	☐
Machine Authentication Default Role	guest
User Authentication Default Role	guest
Authentication Failure Threshold for Station Blacklisting	0 (0 disables blacklisting)

Advanced Configuration

Authentication Servers

Name	Type	IP Address	Authentication Port	Status	Action

FIGURE 3-3 802.1x Authentication Page

Table 3-1 describes the options on the 802.1x Authentication page:

NOTE: In the CLI, you configure these options with the **aaa dot1x** and **dot1x** commands.

TABLE 3-1 802.1x Authentication WebUI Page Options

Parameters	Description
Default Role	Select the default role to be assigned to the user after 802.1x authentication. If derivation rules are present, the roles assigned to the user through these rules will take precedence over the default role. Default role: guest
Enable Authentication	Select this option to enable 802.1x authentication. Default: Disabled
Enable Termination	Select this option to terminate 802.1x authentication on the WLAN Switch. Default: Disabled

TABLE 3-1 802.1x Authentication WebUI Page Options (Continued)

EAP Method (when Enable Termination is selected)	The EAP type Protected Extensible Authentication Protocol (PEAP) uses Transport Layer Security (TLS) to create an encrypted tunnel. Within the TLS tunnel, the client can be authenticated using the selected inner EAP method. Default: EAP-PEAP
Inner EAP Method (when Enable Termination is selected)	Select one of the following: ■ EAP-Generic Token Card (GTC): Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the WLAN Switch as a backup to an external authentication server. ■ EAP-Microsoft Challenge Authentication Protocol version 2 (MS-CHAPv2): Described in RFC 2759, this EAP method is widely supported by Microsoft clients. Default: EAP-MSCHAPv2
Enable Token Caching (when EAP-GTC is selected)	If you select EAP-GTC as the inner EAP method, you can enable the WLAN Switch to cache the username and password of each authenticated user. The WLAN Switch continues to reauthenticate users with the remote authentication server, however, if the authentication server is not available, the WLAN Switch will inspect its cached credentials to reauthenticate users. Default: Disabled
Token Caching Period (when EAP-GTC is selected)	If you select EAP-GTC as the inner EAP method, you can specify the timeout period for the cached information. Default: Not specified
Enable Reauthentication	Select this option to force the client to do a 802.1x re-authentication after the expiration of the default timer for re-authentication. The default value of the timer is 24 hours (see "Advanced Configuration Options for 802.1x" on page 59). If the user fails to re-authenticate with valid credentials, the state of the user is cleared. If derivation rules are used to classify 802.1x-authenticated users, then the Re-authentication timer per role overrides this setting. Default: Disabled

TABLE 3-1 802.1x Authentication WebUI Page Options (Continued)

Enable Opportunistic Key Caching (WPA2)	Enables the same pairwise master key (PMK) derived with a client and an associated AP to be used when the client roams to a new AP. This allows users faster roaming without having to reauthenticate. **NOTE:** Make sure that the wireless client (the 802.1x supplicant) supports this feature before you enable this option. If the client does not support this feature, the client will attempt to renegotiate the key whenever it roams to a new AP. As a result, the key cached on the WLAN Switch can be out of sync with the key used by the client. Default: Disabled
Enforce Machine Authentication	(For Windows environments only) Select this option to enforce machine authentication before user authentication. If selected, either the Machine Authentication Default Role or the User Authentication Default Role is assigned to the user, depending on which authentication is successful. See "Configuring User and Computer Authentication" on page 30. Default: Disabled
Enable Wired Clients	Select this option to enable 802.1x authentication for wired users. The principles of role derivation that apply to wireless users also apply to wired users. Default: Disabled
Machine Authentication Default Role	Select the default role to be assigned to the user after machine authentication. See "Configuring User and Computer Authentication" on page 30. Default role: guest
User Authentication Default Role	Select the default role to be assigned to the user after 802.1x authentication. See "Configuring User and Computer Authentication" on page 30. Default role: guest
Authentication Failure Threshold for Station Blacklisting	This option specifies the number of times a user can try to login with wrong credentials after which the user will be blacklisted as a security threat. Set to 0 to disable blacklisting, otherwise enter a non-zero integer to blacklist the user after the specified number of failures. Default: 3

Configuring User and Computer Authentication

When a Windows computer boots, it logs onto the network domain using a machine account. Within the domain, the device is authenticated before computer group policies and software settings can be executed; this process is known as *machine authentication*. Machine authentication ensures that only authorized computers are allowed on the network.

802.1x can be used to perform user and machine authentication (in the 802.1x configuration page, select the Enforce Machine Authentication option). This tightens the authentication process further since both computer and user need to be authenticated.

Enabling machine authentication creates the following scenarios.

- Both machine and user authentication fail
- Machine authentication fails while user authentication passes
- Machine authentication passes while user authentication fails
- Both machine and user authentication pass

Table 3-2 describes the results of each scenario.

TABLE 3-2 User and Machine Authentication Scenarios

Machine Auth Status	User Auth Status	Description	Role	Typical Access Policy
Failed	Failed	Both machine authentication and user authentication failed. L2 authentication failed.	(Not applicable)	No access to network

Table 3-2 User and Machine Authentication Scenarios (Continued)

Failed	Passed	If machine authentication fails (for example, the machine information is not present on the server) and user authentication succeeds, the user is assigned the **User Authentication Default Role**. Derivation roles, if present, do not apply.	User Authentication Default Role	Limited access depending on the role.
Passed	Failed	If machine authentication succeeds and user authentication has not been initiated, the role assigned would be the **Machine Authentication Default Role.** Derivation rules, if present, do not apply	Machine Authentication Default Role	Access depends on the physical security of the device.
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 are applied.	**Default role** or role assigned by derivation rules.	Most secure since both authentications succeeded. Permissions could not depend purely on the user classification like guest, employee, admin, etc.

For example, if the following roles are configured:

Default role:	dot1x_user
Machine Authentication default role:	dot1x_mc
User Authentication default role:	guest
User VLAN:	100 (configured by role)

the role assignments would be as follows:

- 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.

- If both machine and user authentication succeed, the role assigned would be dot1x_user.
- On failure of any type of authentication, the user does not have access to the network.

NOTE: When you enable machine authentication, there are three different role options you configure (as described above) – the User Authentication Default Role, the Machine Authentication Default Role and the Default role. While you can select the same role in all three options, you should define the roles as per the polices that need to be enforced.

Example Configurations

The following examples show basic configurations on the WLAN Switch for:

- "Authentication with an 802.1x RADIUS Server" on page 32
- "Authentication with the Controller's Internal Database" on page 47

In the following examples:

- Wireless clients associate to the ESSID **WLAN-01**.
- The following roles allow different networks access capabilities:
  - student
  - faculty
  - guest
  - system administrators

The examples show how to configure using the WebUI and CLI commands.

Authentication with an 802.1x RADIUS Server

In the following example:

- An EAP-compliant RADIUS server provides the 802.1x authentication.

  NOTE: The RADIUS server administrator must configure the server to support this authentication. The administrator must also configure the server to allow communication with the Alcatel WLAN Switch.

- The authentication type is WPA. From the 802.1x authentication exchange, the client and the WLAN Switch derive dynamic keys to encrypt data transmitted on the wireless network.

- 802.1x authentication based on PEAP with MS-CHAPv2 provides both computer and user authentication. If a user attempts to log in without the computer being authenticated first, the user is placed into a more limited "guest" user role.

  Windows domain credentials are used for computer authentication, and the user's Windows login and password are used for user authentication. A single user sign-on facilitates both authentication to the wireless network and access to the Windows server resources.

NOTE: Appendix A, "Windows Client Example Configuration for 802.1x" provides example configurations for a Windows XP wireless client, Microsoft Active Directory Server, and Microsoft Internet Authentication Server that would operate with the WLAN Switch configuration shown in this section.

Configuring Policies and Roles

Create the following policies and user roles:

- The **student** policy prevents students from using telnet, POP3, FT, SMTP, SNMP, or SSH to the wired portion of the network. The **student** policy is mapped to the **student** user role.
- The **faculty** policy is similar to the **student** policy, however faculty members are allowed to use POP3 and SMTP for VPN remote access from home. (Students are not permitted to use VPN remote access.) The **faculty** policy is mapped to the **faculty** user role.
- The **guest** policy permits only access to the Internet (via HTTP or HTTPS) and only during daytime working hours. The **guest** policy is mapped to the **guest** user role.
- The **allowall** policy, a predefined policy, allows unrestricted access to the network. The **allowall** policy is mapped to both the **sysadmin** user role and the **computer** user role.

WebUI

To create the student policy and role:

1. Navigate to the **Configuration > Advanced > Security > Firewall Policies** page. Select **Add** to add the student policy.
2. For Policy Name, enter **student**.
3. Under Rules, select **Add** to add rules for the policy.
   - A. Under Source, select **user**.
   - B. Under Destination, select **alias**.

NOTE: The following steps define an alias representing all internal network addresses. Once defined, you can use the alias for other rules and policies.

I. Under the alias selection, select **New**.

II. For Destination Name, enter “Internal Network”.

a. Click **Add** to add a rule.

b. For Rule Type, select **network**.

c. For IP Address, enter 10.0.0.0.

d. For Network Mask/Range, enter 255.0.0.0.

e. Click **Add** to add the network range.

f. Repeat steps I-V to add the network range 172.16.0.0 255.255.0.0.

g. Select **Apply**. The alias “Internal Network” appears in the Destination menu

C. Under Destination, select Internal Network.

D. Under Service, select **service**. In the Service scrolling list, select **svc-telnet**.

E. Under Action, select **drop**.

F. Click Add.

4. Under Rules, select Add.

A. Under Source, select **user**.

B. Under Destination, select **alias**. Then select Internal Network.

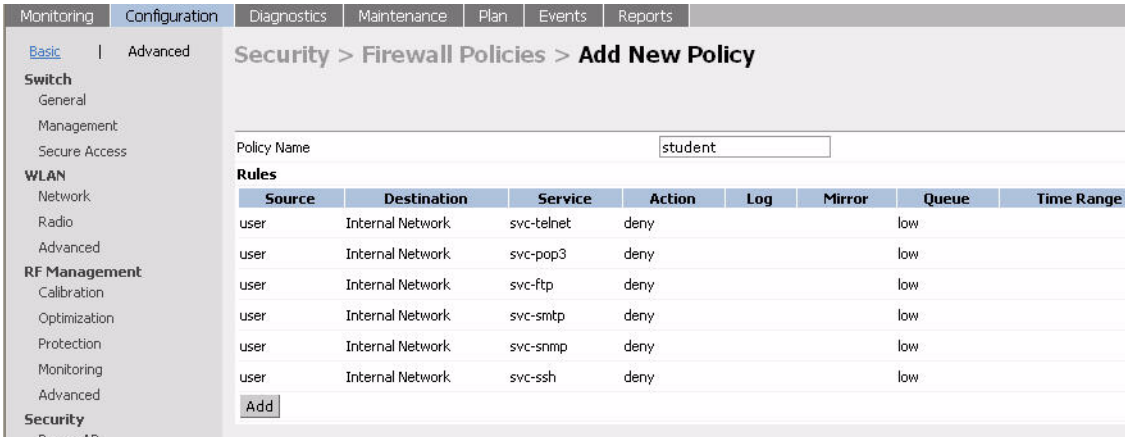
C. Under Service, select **service**. In the Service scrolling list, select **svc-pop3**.

D. Under Action, select **drop**.

E. Click Add.

5. Repeat steps 3A-E to create rules for the following services: svc-ftp, svc-smtp, svc-snmp, and svc-ssh.

The following is an example of the student policy configuration.



Security > Firewall Policies > **Add New Policy**

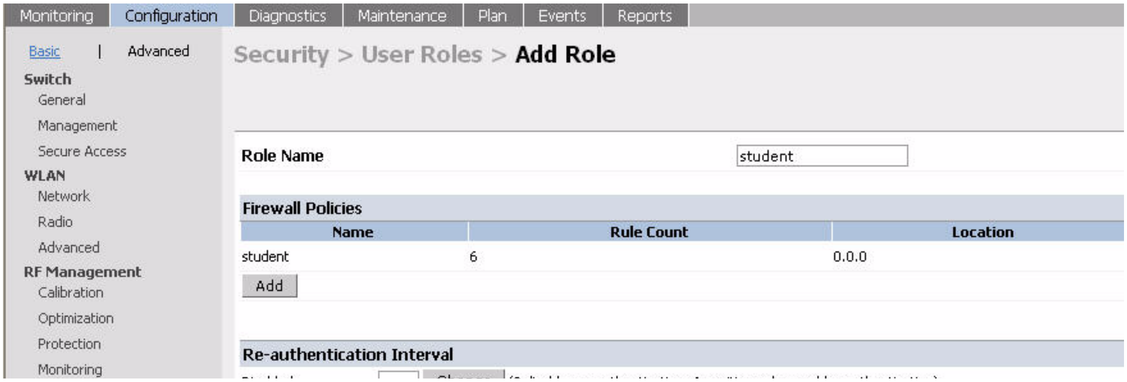
Policy Name: student

Rules

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range
user	Internal Network	svc-telnet	deny			low	
user	Internal Network	svc-pop3	deny			low	
user	Internal Network	svc-ftp	deny			low	
user	Internal Network	svc-smtp	deny			low	
user	Internal Network	svc-snmp	deny			low	
user	Internal Network	svc-ssh	deny			low	

6. Click **Apply**.
7. Navigate to **Configuration** > **Advanced** > **Security** > **User Roles** page. Select **Add** to create the student role.
8. For Role Name, enter student.
9. Under Firewall Policies, click **Add**. In Choose from Configured Policies, select the student policy you previously created. Click **Done**.

   The following is an example of the student role configuration.



Security > User Roles > **Add Role**

Role Name: student

Firewall Policies

Name	Rule Count	Location
student	6	0.0.0

Re-authentication Interval

10. Click **Apply**.

To create the faculty policy and role:

1. Navigate to the **Configuration** > **Advanced** > **Security** > **Firewall Policies** page. Select **Add** to add the faculty policy.
2. For Policy Name, enter **faculty**.

3. Under Rules, select **Add** to add rules for the policy.

   A. Under Source, select **user**.

   B. Under Destination, select **Internal Network**.

   C. Under Service, select **service**. In the Service scrolling list, select **svc-telnet**.

   D. Under Action, select **drop**.

   E. Click **Add**.

   F. Repeat steps A-E to create rules for the following services: svc-ftp, svc-snmp, and svc-ssh.

4. Click **Apply**.

5. Navigate to **Configuration** > **Advanced** > **Security** > **User Roles** page. Select **Add** to create the faculty role.

6. For Role Name, enter **faculty**.

7. Under **Firewall Policies**, click **Add**. In Choose from Configured Policies, select the faculty policy you previously created. Click **Done**.

To create the guest policy and role:

1. Navigate to the **Configuration** > **Advanced** > **Security** > **Advanced** > **Time Range** page to define the time range “working-hours”. Select **Add**.

   A. For Name, enter **working-hours**.

   B. For Type, select **Periodic**.

   C. Click **Add**.

   D. For Start Day, click **Weekday**.

   E. For Start Time, enter **07:30**.

   F. For End Time, enter **17:00**.

   G. Click **Done**.

   H. Click **Apply**.

2. Navigate to the **Configuration** > **Advanced** > **Security** > **Firewall Policies** page. Select **Add** to add the guest policy.

3. For Policy Name, enter **guest**.

4. Under Rules, select **Add** to add rules for the policy.

   To create rules to permit access to DHCP and DNS servers during working hours:

   A. Under Source, select **user**.

- **B.** Under Destination, select **host**. In Host IP, enter **10.1.1.25**.
- **C.** Under Service, select **service**. In the Service scrolling list, select **svc-dhcp**.
- **D.** Under Action, select **permit**.
- **E.** Under Time Range, select **working-hours**.
- **F.** Click **Add**.
- **G.** Repeat steps A-F to create a rule for svc-dns.

To create a rule to deny access to the internal network:

- **A.** Under Source, select **user**.
- **B.** Under Destination, select **alias**. Select **Internal Network**.
- **C.** Under Service, select **any**.
- **D.** Under Action, select **drop**.
- **E.** Click **Add**.

To create rules to permit HTTP and HTTPS access during working hours:

- **A.** Under Source, select **user**.
- **B.** Under Destination, select **any**.
- **C.** Under Service, select service. In the Services scrolling list, select **svc-http**.
- **D.** Under Action, select **permit**.
- **E.** Under Time Range,
- **F.** Click **Add**.
- **G.** Repeat steps A-F for the svc-https service.

To create a rule that denies the user access to all destinations and all services:

- **A.** Under Source, select **user**.
- **B.** Under Destination, select **any**.
- **C.** Under Service, select **any**.
- **D.** Under Action, select **deny**.
- **E.** Click **Add**.

5. Click **Apply**.
6. Navigate to **Configuration > Advanced > Security > User Roles** page. Select **Add** to create the guest role.
7. For Role Name, enter **guest**.

8. Under **Firewall Policies**, click **Add**. In Choose from Configured Policies, select the guest policy you previously created. Click **Done**.

To create the sysadmin role:

1. Navigate to **Configuration** > **Advanced** > **Security** > **User Roles** page. Select **Add** to create the sysadmin role.
2. For Role Name, enter **sysadmin**.
3. Under Firewall Policies, click **Add**. In Choose from Configured Policies, select the predefined **allowall** policy. Click **Done**.
4. Click **Apply**.

To create the computer role:

1. Navigate to **Configuration** > **Advanced** > **Security** > **User Roles** page. Select **Add** to create the computer role.
2. For Role Name, enter **computer**.
3. Under Firewall Policies, click **Add**. In Choose from Configured Policies, select the predefined **allowall** policy. Click **Done**.
4. Click **Apply**.

CLI

To create an alias for the internal network:

```
netdestination “Internal Network”
   network 10.0.0.0 255.0.0.0
   network 172.16.0.0 255.255.0.0
```

To create the student role:

```
ip access-list session student
   user alias “Internal Network” svc-telnet deny
   user alias “Internal Network” svc-pop3 deny
   user alias “Internal Network” svc-ftp deny
   user alias “Internal Network” svc-smtp deny
   user alias “Internal Network” svc-snmp deny
   user alias “Internal Network” svc-ssh deny

user-role student
   session-acl student
   session acl allowall
```

To create the faculty role:

```
ip access-list session faculty
   user alias “Internal Network” svc-telnet deny
   user alias “Internal Network” svc-ftp deny
   user alias “Internal Network” svc-snmp deny
   user alias “Internal Network” svc-ssh deny

user-role faculty
   session-acl faculty
   session acl allowall
```

To create the guest role:

```
time-range working-hours periodic
   weekday 07:30 to 17:00

ip access-list session guest
   user host 10.1.1.25 svc-dhcp permit time-range working-hours
   user host 10.1.1.25 svc-dns permit time-range working-hours
   user alias “Internal Network” any deny
   user any svc-http permit time-range working-hours
   user any svc-https permit time-range working-hours
   user any any deny

user-role guest
   session-acl guest
```

To create the sysadmin role:

```
user-role sysadmin
   session-acl allowall
```

To create the computer role:

```
user-role computer
   session-acl allowall
```

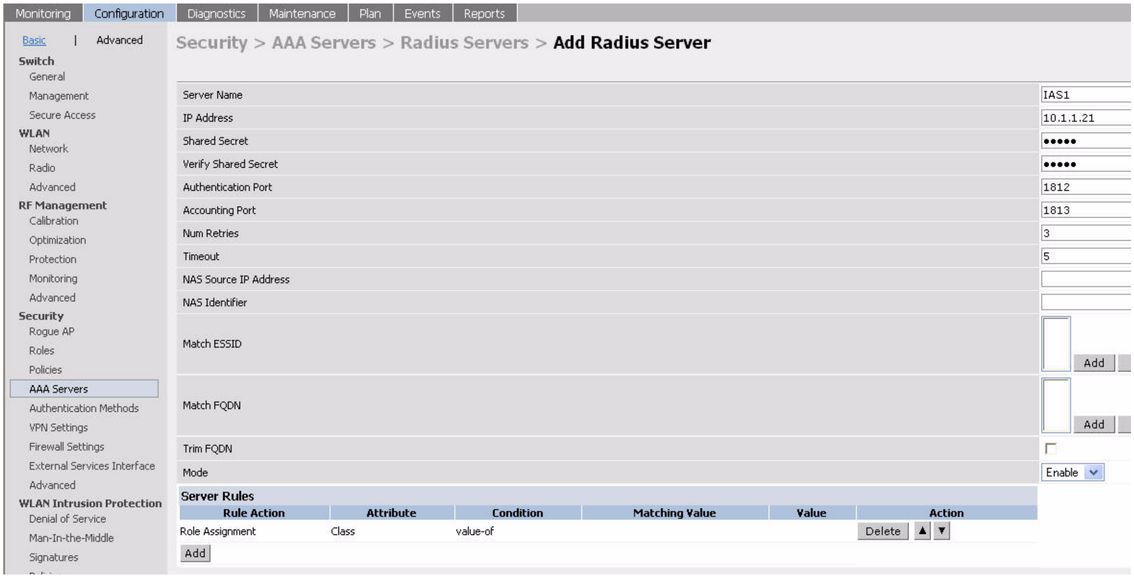
Configuring the RADIUS Authentication Server

Configure the RADIUS server IAS1, with IP address 10.1.1.21 and shared key. The RADIUS server is configured to sent an attribute called Class to the WLAN Switch; the value of this attribute is set to either “student,” “faculty,” or “sysadmin” to identify the user’s group. The WLAN Switch uses the literal value of this attribute to determine the role name.

WebUI

1. Navigate to the **Configuration** > **Advanced** > **Security** > **AAA Servers** > **Radius** page.
2. Under RADIUS Servers, click **Add**.
   A. For Server Name, enter **IAS1**.
   B. For IP Address, enter **10.1.1.21**.
   C. For Shared Secret, enter **`|*a^t%183923!`**.
3. Under Server Rules, click **Add**.
   A. For Rule Type, select **Role Assignment**.
   B. For Attribute, click **Add Attribute**.
   C. For Attribute Name, enter **Class**.
   D. For Attribute Type, select **string**.
   E. Click **Done**.
   F. From the Attribute scrolling menu, select the **Class** attribute you previously configured.
   G. For Condition, select **value-of.**
   H. Select **Done**.

   The following is an example of the Radius server configuration.



Security > AAA Servers > Radius Servers > **Add Radius Server**

Server Name	IAS1
IP Address	10.1.1.21
Shared Secret	•••••
Verify Shared Secret	•••••
Authentication Port	1812
Accounting Port	1813
Num Retries	3
Timeout	5
NAS Source IP Address	
NAS Identifier	
Match ESSID	Add
Match FQDN	Add
Trim FQDN	☐
Mode	Enable

Server Rules

Rule Action	Attribute	Condition	Matching Value	Value	Action
Role Assignment	Class	value-of			Delete ▲ ▼

Add

4. Click **Apply**.

CLI

```
aaa radius-server IAS1 host 10.1.1.21 key |*a^t%183923!

aaa derivation-rules server IAS
   set role condition Class value-of
```

Configure 802.1x Authentication

You enable 802.1x authentication and specify which server to use for the 802.1x authentication. You also configure the default role that an 802.1x client is assigned if a Class attribute is not returned from the RADIUS server.

You also configure enforcement of machine authentication before user authentication. If a user attempts to log in without machine authentication taking place first, the user is placed in the limited guest role.

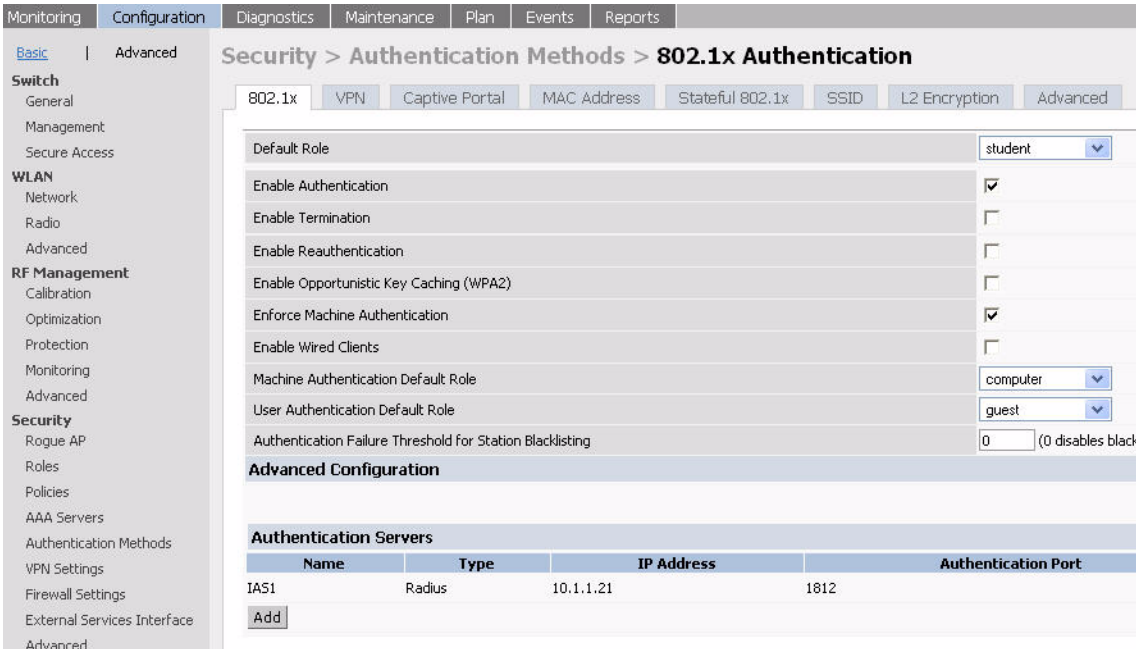
WebUI

1. Navigate to the **Configuration** > **Advanced** > **Security** > **Authentication Methods** > **802.1x Authentication** page.
2. For Default Role, select **student**.
3. Select **Enable Authentication**.
4. Select **Enforce Machine Authentication**.
5. For the Machine Authentication Default Role, select **computer**.
6. For the User Authentication Default Role, select **guest**.
7. Under Authentication Servers, click **Add**.

   A. Select the IAS1 Server you previously configured.

   B. Select **Add**.

   The following is an example of the 802.1x Authentication page.



Security > Authentication Methods > **802.1x Authentication**

Default Role	student
Enable Authentication	☑
Enable Termination	□
Enable Reauthentication	□
Enable Opportunistic Key Caching (WPA2)	□
Enforce Machine Authentication	☑
Enable Wired Clients	□
Machine Authentication Default Role	computer
User Authentication Default Role	guest
Authentication Failure Threshold for Station Blacklisting	0 (0 disables black

Advanced Configuration

Authentication Servers

Name	Type	IP Address	Authentication Port
IAS1	Radius	10.1.1.21	1812

8. Select **Apply**.

CLI

```
aaa dot1x mode enable
aaa dot1x default-role student
aaa dot1x auth-server IAS1
aaa dot1x enforce-machine-authentication
   mode enable
   machine-authentication default-role computer
   user-authentication default-role guest
```

Configure VLANs

In this example, wireless clients are assigned to either VLAN 60 or 61 while guest users are assigned to VLAN 63. VLANs 60 and 61 split users into smaller IP subnetworks, improving performance by decreasing broadcast traffic. The VLANs are internal to the Alcatel WLAN Switch only and do not extend into other parts of the wired network. The clients' default gateway is the Alcatel WLAN Switch, which routes traffic out to the 10.1.1.0 subnetwork.

You configure the VLANs, assign IP addresses to each VLAN, and establish the "helper address" to which client DHCP requests are forwarded.

WebUI

1. Navigate to the Configuration > Advanced > Network > VLAN Page. Click **Add** to add VLAN 60.

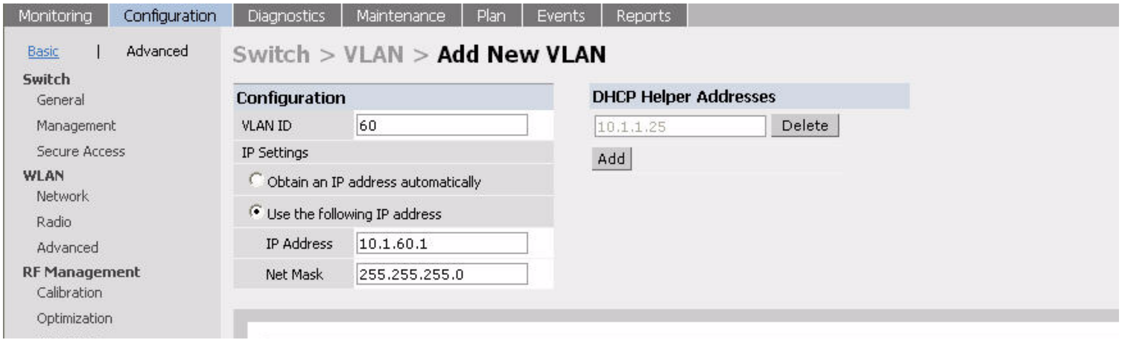
   A. For VLAN ID, enter **60**.

   B. For IP Address, enter **10.1.60.1**.

   C. For Net Mask, enter **255.255.255.0**.

   D. Under DHCP Helper Address, click **Add**. Enter **10.1.1.25** and click **Add**.

   The following is an example of the Add New VLAN page:



VLAN ID: 60

IP Settings

○ Obtain an IP address automatically

● Use the following IP address

IP Address: 10.1.60.1

Net Mask: 255.255.255.0

DHCP Helper Addresses: 10.1.1.25

2. Click **Apply**.
3. Click **Add** to add VLAN 61.

   A. For VLAN ID, enter **61**.

   B. For IP Address, enter **10.1.61.1**.

   C. For Net Mask, enter **255.255.255.0**.

   D. Under DHCP Helper Address, click **Add**. Enter **10.1.1.25** and click **Add**.
4. Click **Apply**.
5. Navigate to the **Configuration** > **Advanced** > **Switch** > **IP Routing** page.
6. For Default Gateway, enter **10.1.1.254**.
7. Click **Apply**.
8. Click **Add** to add VLAN 63.

   A. For VLAN ID, enter **63**.

   B. For IP Address, enter **10.1.63.1**.

   C. For Net Mask, enter **255.255.255.0**.

   D. Under DHCP Helper Address, click **Add**. Enter **10.1.1.25** and click **Add**.

9. Click **Apply**.
10. Navigate to the **Configuration > Advanced > Switch > IP Routing** page.
11. For Default Gateway, enter **10.1.1.254**.
12. Click **Apply**.

CLI

```
interface vlan 60
   ip address 10.1.60.1 255.255.255.0
   ip helper-address 10.1.1.25

interface vlan 61
   ip address 10.1.61.1 255.255.255.0
   ip helper-address 10.1.1.25

interface vlan 63
   ip address 10.1.63.1 255.255.255.0
   ip helper-address 10.1.1.25

ip default-gateway 10.1.1.254
```

Configure the WLAN

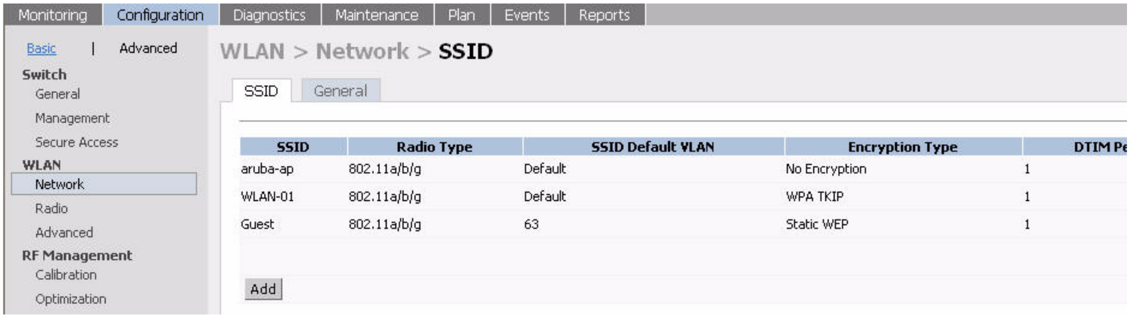
In this example, the default AP parameters for the entire network are as follows: the default ESSID is WLAN-01 and the encryption mode is TKIP. A second ESSID called “guest” has the encryption mode set to static WEP with a configured WEP key.

WebUI

1. Navigate to the **Configuration > Advanced > WLAN > Network > SSID** page. Click **Add** to add the WLAN-01 ESSID.
   - **A.** For SSID, enter **WLAN-01**.
   - **B.** For Encryption Type, select **TKIP**. Select **WPA TKIP**.
   - **C.** Click **Apply**.
2. Click **Add** to add the Guest SSID.
   - **A.** For SSID, enter **Guest**.
   - **B.** For the Radio Types, select **802.11a**.
   - **C.** For SSID Default VLAN, select **VLAN 63**.
   - **D.** For Encryption Type, select **WEP**. Select **Static WEP**.
   - **E.** Enter the WEP Key.

F. Click **Apply**.

The following is an example of the SSID page.



SSID	Radio Type	SSID Default VLAN	Encryption Type	DTIM Pe
aruba-ap	802.11a/b/g	Default	No Encryption	1
WLAN-01	802.11a/b/g	Default	WPA TKIP	1
Guest	802.11a/b/g	63	Static WEP	1

CLI

```
ap location 0.0.0
weptxkey 1
wepkey1 c4f32001f1c25ab20f838312f2

phy-type a
   opmode dynamicTkip
   essid “WLAN-01”
   virtual-ap “Guest” vlan-id 63 opmode opensystem deny-bcast disable
```

In this example, users that associate to an AP are mapped into one of two different user VLANs. Membership in the VLAN is determined by the initial AP to which the user associates. APs are mapped by location to a VLAN: APs in the first floor of building 1 are mapped to VLAN 60 and APs in the second floor of building 1 are mapped to VLAN 61.

WebUI

1. Navigate to the **Configuration** > **Advanced** > **WLAN** > **Advanced** page. Click **Add** to configure the APs at location 1.1.0.

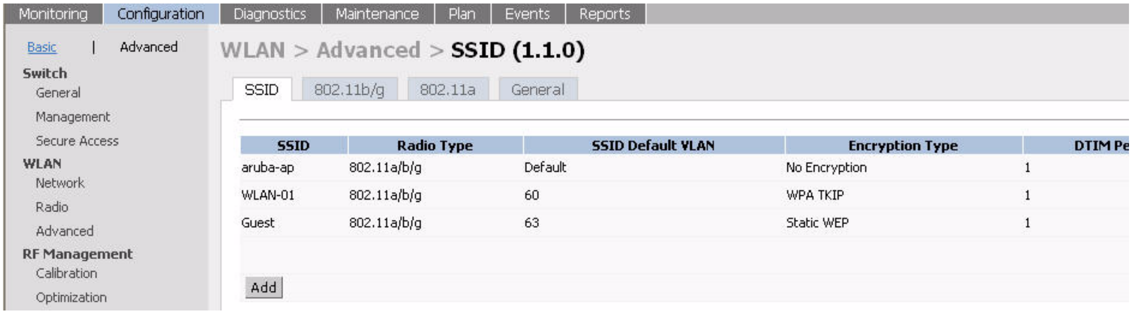
   A. For Location, enter **1.1.0**. Click **Add**.

   B. In the SSID tab, click **Edit** for WLAN-01.

   C. For SSID Default VLAN, select VLAN **60** and click the <-- button.

   D. Click **Apply**.

   The following is an example of the WLAN > Advanced page for location 1.1.0.



WLAN > Advanced > SSID (1.1.0)

SSID	Radio Type	SSID Default VLAN	Encryption Type	DTIM Pe
aruba-ap	802.11a/b/g	Default	No Encryption	1
WLAN-01	802.11a/b/g	60	WPA TKIP	1
Guest	802.11a/b/g	63	Static WEP	1

2. In the **Advanced** page, click **Add** to configure the APs at location 1.2.0.

   A. For Location, enter **1.2.0**. Click **Add**.

   B. In the SSID tab, click **Edit** for WLAN-01.

   C. For SSID Default VLAN, select VLAN **61** and click the <-- button.

   D. Click **Apply**.

CLI

```
ap location 1.1.0
vlan-id 60

ap location 1.2.0
vlan-id 61
```

Authentication with the WLAN Switch's Internal Database

In the following example:

- The WLAN Switch's internal database provides user authentication.
- The authentication type is WPA. From the 802.1x authentication exchange, the client and the WLAN Switch derive dynamic keys to encrypt data transmitted on the wireless network.

Configuring Policies and Roles

Create the following policies and user roles:

- The **student** policy prevents students from using telnet, POP3, FT, SMTP, SNMP, or SSH to the wired portion of the network. The **student** policy is mapped to the **student** user role.
- The **faculty** policy is similar to the **student** policy, however faculty members are allowed to use POP3 and SMTP for VPN remote access from home. (Students are not permitted to use VPN remote access.) The **faculty** policy is mapped to the **faculty** user role.
- The **guest** policy permits only access to the Internet (via HTTP or HTTPS) and only during daytime working hours. The **guest** policy is mapped to the **guest** user role.
- The **allowall** policy, a predefined policy, allows unrestricted access to the network. The **allowall** policy is mapped to both the **sysadmin** user role and the **computer** user role.

WebUI

To create the student policy and role:

1. Navigate to the **Configuration** > **Advanced** > **Security** > **Firewall Policies** page. Select **Add** to add the student policy.
2. For Policy Name, enter **student**.
3. Under Rules, select **Add** to add rules for the policy.

   A. Under Source, select **user**.

   B. Under Destination, select **alias**.

   NOTE: The following steps define an alias representing all internal network addresses. Once defined, you can use the alias for other rules and policies.

   I. Under the alias selection, select **New**.

   II. For Destination Name, enter "Internal Network".

   a. Click **Add** to add a rule.

b. For Rule Type, select **network**.

c. For IP Address, enter 10.0.0.0.

d. For Network Mask/Range, enter 255.0.0.0.

e. Click **Add** to add the network range.

f. Repeat steps I-V to add the network range 172.16.0.0 255.255.0.0.

g. Select **Apply**. The alias "Internal Network" appears in the Destination menu

C. Under Destination, select Internal Network.

D. Under Service, select **service**. In the Service scrolling list, select **svc-telnet**.

E. Under Action, select **drop**.

F. Click Add.

4. Under Rules, select Add.

A. Under Source, select **user**.

B. Under Destination, select **alias**. Then select Internal Network.

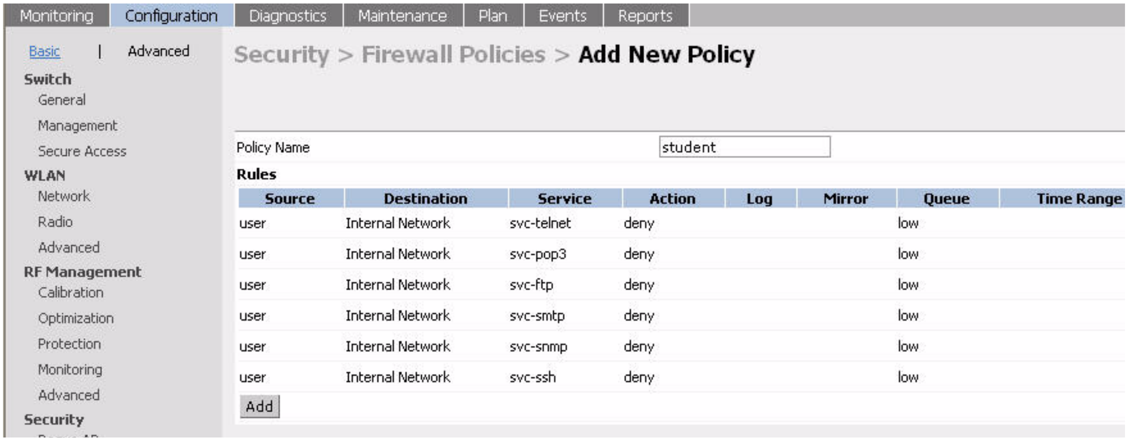
C. Under Service, select **service**. In the Service scrolling list, select **svc-pop3**.

D. Under Action, select **drop**.

E. Click Add.

5. Repeat steps 3A-E to create rules for the following services: svc-ftp, svc-smtp, svc-snmp, and svc-ssh.

The following is an example of the student policy configuration.



Security > Firewall Policies > **Add New Policy**

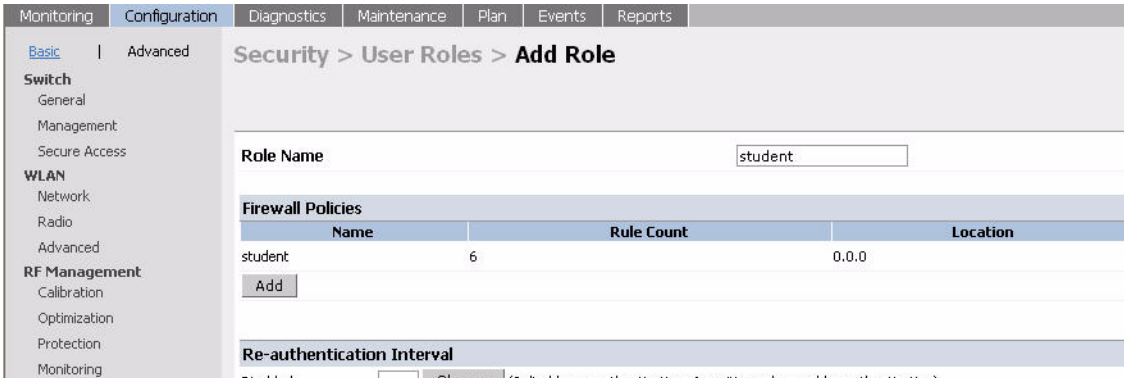
Policy Name: student

Rules

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range
user	Internal Network	svc-telnet	deny			low	
user	Internal Network	svc-pop3	deny			low	
user	Internal Network	svc-ftp	deny			low	
user	Internal Network	svc-smtp	deny			low	
user	Internal Network	svc-snmp	deny			low	
user	Internal Network	svc-ssh	deny			low	

6. Click **Apply**.
7. Navigate to **Configuration > Advanced > Security > User Roles** page. Select **Add** to create the student role.
8. For Role Name, enter student.
9. Under Firewall Policies, click **Add**. In Choose from Configured Policies, select the student policy you previously created. Click **Done**.

   The following is an example of the student role configuration.



Security > User Roles > **Add Role**

Role Name: student

Firewall Policies

Name	Rule Count	Location
student	6	0.0.0

Add

Re-authentication Interval

10. Click **Apply**.

To create the faculty policy and role:

1. Navigate to the **Configuration > Advanced > Security > Firewall Policies** page. Select **Add** to add the faculty policy.
2. For Policy Name, enter **faculty**.
3. Under Rules, select **Add** to add rules for the policy.
   - A. Under Source, select **user**.
   - B. Under Destination, select **Internal Network**.
   - C. Under Service, select **service**. In the Service scrolling list, select **svc-telnet**.
   - D. Under Action, select **drop**.
   - E. Click **Add**.
   - F. Repeat steps A-E to create rules for the following services: svc-ftp, svc-snmp, and svc-ssh.
4. Click **Apply**.

5. Navigate to **Configuration** > **Advanced** > **Security** > **User Roles** page. Select **Add** to create the faculty role.
6. For Role Name, enter **faculty**.
7. Under **Firewall Policies**, click **Add**. In Choose from Configured Policies, select the faculty policy you previously created. Click **Done**.

To create the guest policy and role:

1. Navigate to the **Configuration** > **Advanced** > **Security** > **Advanced** > **Time Range** page to define the time range "working-hours". Select **Add**.
   - A. For Name, enter **working-hours**.
   - B. For Type, select **Periodic**.
   - C. Click **Add**.
   - D. For Start Day, click **Weekday**.
   - E. For Start Time, enter **07:30**.
   - F. For End Time, enter **17:00**.
   - G. Click **Done**.
   - H. Click **Apply**.
2. Navigate to the **Configuration** > **Advanced** > **Security** > **Firewall Policies** page. Select **Add** to add the guest policy.
3. For Policy Name, enter **guest**.
4. Under Rules, select **Add** to add rules for the policy.

   To create rules to permit access to DHCP and DNS servers during working hours:
   - A. Under Source, select **user**.
   - B. Under Destination, select **host**. In Host IP, enter **10.1.1.25**.
   - C. Under Service, select **service**. In the Service scrolling list, select **svc-dhcp**.
   - D. Under Action, select **permit**.
   - E. Under Time Range, select **working-hours**.
   - F. Click **Add**.
   - G. Repeat steps A-F to create a rule for svc-dns.

   To create a rule to deny access to the internal network:
   - A. Under Source, select **user**.
   - B. Under Destination, select **alias**. Select **Internal Network**.

C. Under Service, select **any**.

D. Under Action, select **drop**.

E. Click **Add**.

To create rules to permit HTTP and HTTPS access during working hours:

A. Under Source, select **user**.

B. Under Destination, select **any**.

C. Under Service, select service. In the Services scrolling list, select **svc-http**.

D. Under Action, select **permit**.

E. Under Time Range,

F. Click **Add**.

G. Repeat steps A-F for the svc-https service.

To create a rule that denies the user access to all destinations and all services:

A. Under Source, select **user**.

B. Under Destination, select **any**.

C. Under Service, select **any**.

D. Under Action, select **deny**.

E. Click **Add**.

5. Click **Apply**.
6. Navigate to **Configuration** > **Advanced** > **Security** > **User Roles** page. Select **Add** to create the guest role.
7. For Role Name, enter **guest**.
8. Under **Firewall Policies**, click **Add**. In Choose from Configured Policies, select the guest policy you previously created. Click **Done**.

To create the sysadmin role:

1. Navigate to **Configuration** > **Advanced** > **Security** > **User Roles** page. Select **Add** to create the sysadmin role.
2. For Role Name, enter **sysadmin**.
3. Under Firewall Policies, click **Add**. In Choose from Configured Policies, select the predefined **allowall** policy. Click **Done**.
4. Click **Apply**.

To create the computer role:

1. Navigate to **Configuration** > **Advanced** > **Security** > **User Roles** page. Select **Add** to create the computer role.
2. For Role Name, enter **computer**.
3. Under Firewall Policies, click **Add**. In Choose from Configured Policies, select the predefined **allowall** policy. Click **Done**.
4. Click **Apply**.

CLI

To create an alias for the internal network:

```
netdestination “Internal Network”
   network 10.0.0.0 255.0.0.0
   network 172.16.0.0 255.255.0.0
```

To create the student role:

```
ip access-list session student
   user alias “Internal Network” svc-telnet deny
   user alias “Internal Network” svc-pop3 deny
   user alias “Internal Network” svc-ftp deny
   user alias “Internal Network” svc-smtp deny
   user alias “Internal Network” svc-snmp deny
   user alias “Internal Network” svc-ssh deny

user-role student
   session-acl student
   session acl allowall
```

To create the faculty role:

```
ip access-list session faculty
   user alias “Internal Network” svc-telnet deny
   user alias “Internal Network” svc-ftp deny
   user alias “Internal Network” svc-snmp deny
   user alias “Internal Network” svc-ssh deny

user-role faculty
   session-acl faculty
   session acl allowall
```

To create the guest role:

```
time-range working-hours periodic
   weekday 07:30 to 17:00

ip access-list session guest
   user host 10.1.1.25 svc-dhcp permit time-range working-hours
   user host 10.1.1.25 svc-dns permit time-range working-hours
   user alias “Internal Network” any deny
   user any svc-http permit time-range working-hours
   user any svc-https permit time-range working-hours
   user any any deny

user-role guest
   session-acl guest
```

To create the sysadmin role:

```
user-role sysadmin
   session-acl allowall
```

To create the computer role:

```
user-role computer
   session-acl allowall
```

Configuring the Internal Database

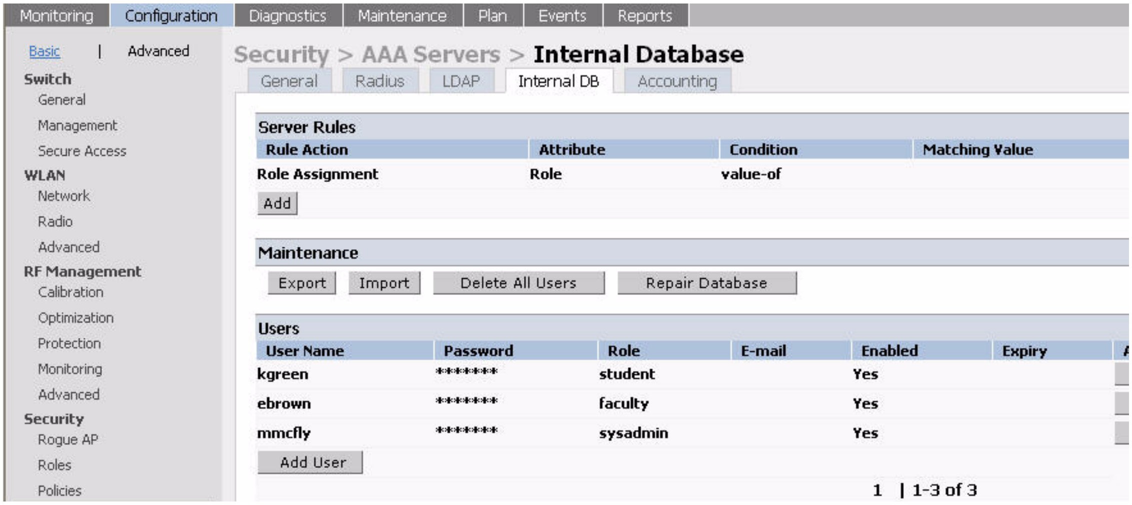
Configure the internal database with the username, password, and role (student, faculty, or sysadmin) for each user. The WLAN Switch uses the literal value of the “role” to determine the user role given to each user.

WebUI

1. Navigate to the **Configuration** > **Advanced** > **Security** > **AAA Servers** > **Internal DB** page.
2. Under Server Rules, click **Add**.
   A. Set Rule Type to **Role Assignment**.
   B. For Attribute, enter **Role**.
   C. For Condition, select **value-of**.
   D. Select **Apply**.
3. Under Users, click **Add User** to add users.
4. For each user, enter a username and password.
5. Select the Role for each user (if a role is not specified, the default role is guest).

6. Select the expiration time for the user account in the internal database.
7. Click **Apply**.

The following is an example of the Internal Database configuration:



Server Rules

Rule Action	Attribute	Condition	Matching Value
Role Assignment	Role	value-of	

Users

User Name	Password	Role	E-mail	Enabled	Expiry
kgreen	********	student		Yes	
ebrown	********	faculty		Yes	
mmcfly	********	sysadmin		Yes	

CLI

```
aaa derivation-rules server “Internal”
   set role condition “Role” value-of
```

NOTE: Use the Enable mode in the CLI to configure users in the WLAN Switch’s internal database.

```
local-userdb add username <user> password <password> role <role>
```

Configure 802.1x Authentication

For this example, you enable both 802.1x authentication and termination on the WLAN Switch.

WebUI

1. Navigate to the **Configuration > Advanced > Security > Authentication Methods > 802.1x Authentication** page.
2. For Default Role, select **student**.
3. Select **Enable Authentication**.
4. Select **Enable Termination**.

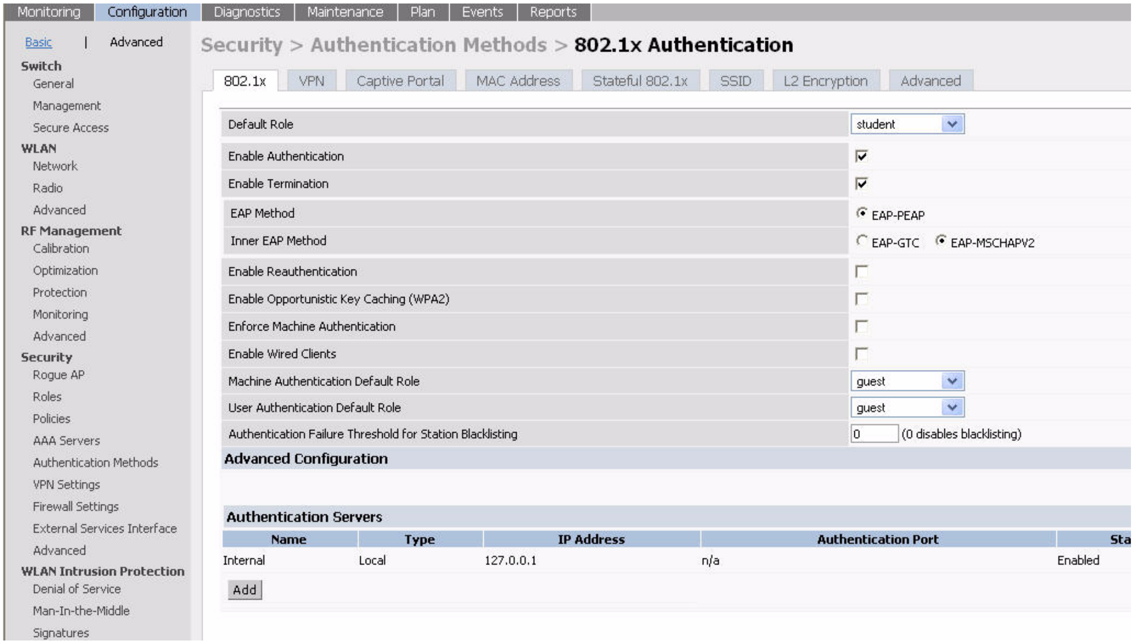
   NOTE: The defaults for EAP Method and Inner EAP Method are EAP-PEAP and EAP-MSCHAPv2, respectively.

5. Under Authentication Servers, click **Add**.

   A. Under Choose an Authentication Server, select **Internal**.

   B. Click **Add**.

   The following is an example of the 802.1x Authentication page.



Security > Authentication Methods > **802.1x Authentication**

Default Role	student
Enable Authentication	☑
Enable Termination	☑
EAP Method	● EAP-PEAP
Inner EAP Method	○ EAP-GTC ● EAP-MSCHAPV2
Enable Reauthentication	□
Enable Opportunistic Key Caching (WPA2)	□
Enforce Machine Authentication	□
Enable Wired Clients	□
Machine Authentication Default Role	guest
User Authentication Default Role	guest
Authentication Failure Threshold for Station Blacklisting	0 (0 disables blacklisting)

Advanced Configuration

Authentication Servers

Name	Type	IP Address	Authentication Port	Sta
Internal	Local	127.0.0.1	n/a	Enabled

6. Select **Apply**.

CLI

```
aaa dot1x mode enable
aaa dot1x default-role student
aaa dot1x auth-server Internal
dot1x termination
```

Configure VLANs

In this example, wireless clients are assigned to either VLAN 60 or 61 while guest users are assigned to VLAN 63. VLANs 60 and 61 split users into smaller IP subnetworks, improving performance by decreasing broadcast traffic. The VLANs are internal to the Alcatel WLAN Switch only and do not extend into other parts of the wired network. The clients' default gateway is the Alcatel WLAN Switch, which routes traffic out to the 10.1.1.0 subnetwork.

You configure the VLANs, assign IP addresses to each VLAN, and establish the "helper address" to which client DHCP requests are forwarded.

WebUI

1. Navigate to the Configuration > Advanced > Network > VLAN Page. Click **Add** to add VLAN 60.

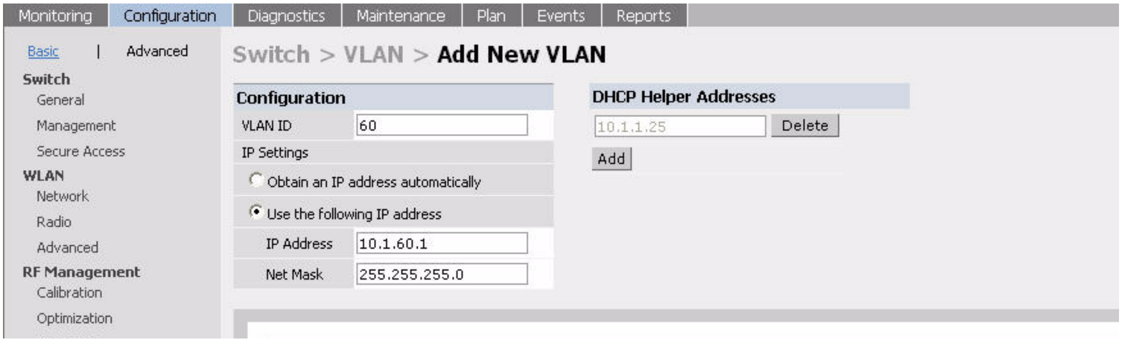
   A. For VLAN ID, enter **60**.

   B. For IP Address, enter **10.1.60.1**.

   C. For Net Mask, enter **255.255.255.0**.

   D. Under DHCP Helper Address, click **Add**. Enter **10.1.1.25** and click **Add**.

   The following is an example of the Add New VLAN page:



Configuration

VLAN ID 60

IP Settings

○ Obtain an IP address automatically

● Use the following IP address

IP Address 10.1.60.1

Net Mask 255.255.255.0

DHCP Helper Addresses

10.1.1.25

2. Click **Apply**.
3. Click **Add** to add VLAN 61.

   A. For VLAN ID, enter **61**.

   B. For IP Address, enter **10.1.61.1**.

   C. For Net Mask, enter **255.255.255.0**.

   D. Under DHCP Helper Address, click **Add**. Enter **10.1.1.25** and click **Add**.
4. Click **Apply**.
5. Navigate to the **Configuration** > **Advanced** > **Switch** > **IP Routing** page.
6. For Default Gateway, enter **10.1.1.254**.
7. Click **Apply**.
8. Click **Add** to add VLAN 63.

   A. For VLAN ID, enter **63**.

   B. For IP Address, enter **10.1.63.1**.

   C. For Net Mask, enter **255.255.255.0**.

   D. Under DHCP Helper Address, click **Add**. Enter **10.1.1.25** and click **Add**.

9. Click **Apply**.
10. Navigate to the **Configuration** > **Advanced** > **Switch** > **IP Routing** page.
11. For Default Gateway, enter **10.1.1.254**.
12. Click **Apply**.

CLI

```
interface vlan 60
   ip address 10.1.60.1 255.255.255.0
   ip helper-address 10.1.1.25

interface vlan 61
   ip address 10.1.61.1 255.255.255.0
   ip helper-address 10.1.1.25

interface vlan 63
   ip address 10.1.63.1 255.255.255.0
   ip helper-address 10.1.1.25

ip default-gateway 10.1.1.254
```

Configure the WLAN

In this example, the default AP parameters for the entire network are as follows: the default ESSID is WLAN-01 and the encryption mode is TKIP. A second ESSID called “guest” has the encryption mode set to static WEP with a configured WEP key.

WebUI

1. Navigate to the **Configuration** > **Advanced** > **WLAN** > **Network** > **SSID** page. Click **Add** to add the WLAN-01 ESSID.
   A. For SSID, enter **WLAN-01**.
   B. For Encryption Type, select **TKIP**. Select **WPA TKIP**.
   C. Click **Apply**.
2. Click **Add** to add the Guest SSID.
   A. For SSID, enter **Guest**.
   B. For the Radio Types, select **802.11a**.
   C. For SSID Default VLAN, select **VLAN 63**.
   D. For Encryption Type, select **WEP**. Select **Static WEP**.

E. Click **Apply**.

CLI

```
ap location 0.0.0
weptxkey 1
wepkey1 c4f32001f1c25ab20f838312f2

phy-type a
   opmode dynamicTkip
   essid “WLAN-01”
   virtual-ap “Guest” vlan-id 63 opmode opensystem deny-bcast disable
```

In this example, users that associate to an AP are mapped into one of two different user VLANs. Membership in the VLAN is determined by the initial AP to which the user associates. APs are mapped by location to a VLAN: APs in the first floor of building 1 are mapped to VLAN 60 and APs in the second floor of building 1 are mapped to VLAN 61.

WebUI

1. Navigate to the **Configuration > Advanced > WLAN > Advanced** page. Click **Add** to configure the APs at location 1.1.0.
   A. For Location, enter **1.1.0**. Click **Add**.
   B. In the SSID tab, click **Edit** for WLAN-01.
   C. For SSID Default VLAN, select VLAN **60** and click the <-- button.
   D. Click **Apply**.
2. In the **Advanced** page, click **Add** to configure the APs at location 1.2.0.
   A. For Location, enter **1.2.0**. Click **Add**.
   B. In the SSID tab, click **Edit** for WLAN-01.
   C. For SSID Default VLAN, select VLAN **61** and click the <-- button.
   D. Click **Apply**.

CLI

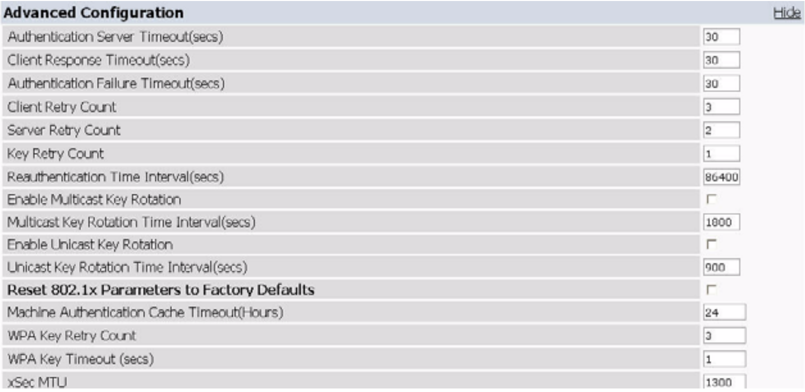
```
ap location 1.1.0
vlan-id60

ap location 1.2.0
vlan-id 61
```

Advanced Configuration Options for 802.1x

This section describes the Advanced Configuration options for 802.1x authentication.

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

In the WebUI, access the Advanced options by clicking the *Show* tab on the right of the Advanced Configuration option on the 802.1x configuration page.



Advanced Configuration	
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
xSec MTU	1300

The following describes the fields:

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 WLAN Switch makes to obtain an authentication from a client.

Server Retry Count	This is the number of attempts the WLAN Switch makes to obtain an authentication from a server.
Key Retry Count	This is the number of attempts the WLAN 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. **NOTE:** Many wireless clients do not support this function.
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	Sets the cache timeout for machine authentication.
WPA Key Retry Count	This is the number of attempts the WLAN 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.
xSec MTU	Sets the MTU size when the 802.1x supplicant is xSec-compliant.

Configuring the Captive Portal 4

One of the methods of authentication supported by AOS-W is Captive Portal. A captive portal presents a Web page which requires action on the part of the wireless user before network access is granted. The required action can be simply viewing and agreeing to an acceptable use policy, or entering a user ID and password which must be validated against a database of authorized users.

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 WLAN Switch. See Chapter 5, "Configuring Virtual Private Networks."

This chapter describes the following topics:

Overview of Captive Portal Functions

There are two forms of Captive Portal you can configure in AOS-W:

- Guest Captive Portal requires no authentication; users typically enter an email address as an identification.
- Captive Portal requires users to be authenticated to an external authentication server or to the internal database on the WLAN Switch.

NOTE: While you can use Captive Portal to authenticate users, it does not provide for encryption of user data and should not be used in networks where data security is required. Captive Portal is most often used for guest access, access to open systems (such as public hot spots), or as a way to connect to a VPN.

You can use one or both forms of Captive Portal at the same time. The default Captive Portal web page provided with AOS-W displays login prompts for both registered users and guests. (You can customize the default Captive Portal page, as described in "Personalizing the Captive Portal Page" on page 70.)

For AOS-W releases prior to 2.5.2, a Policy Enforcement Firewall license is required for the Captive Portal feature. With the Policy Enforcement Firewall license installed, Captive Portal users are first placed into the *logon* user role, which allows users to be given an IP address and placed into a VLAN but otherwise disallows access to the network. You can configure default user roles for authenticated or guest Captive Portal users.

With the AOS-W 2.5.2 release, Captive Portal is available in the base operating system; you do not need to install the Policy Enforcement Firewall license in the WLAN Switch to use this feature. You enable Captive Portal on a per-ESSID basis. Captive Portal users are first placed into the predefined *cpbase* user role, which allows only DNS, DHCP, and HTTP or HTTPS connections to the network. Upon authentication, Captive Portal users are allowed full access to their assigned VLAN.

NOTE: The base operating system allows all users who connect to an ESSID full network access. Captive Portal allows you to control or at least identify who has access to network resources. However, in the base operating system you cannot configure or customize user roles; this function is only available by installing the Policy Enforcement Firewall license.

If you install the Policy Enforcement Firewall license in AOS-W 2.5.2, the Captive Portal feature operates in the same manner as in AOS-W releases prior to 2.5.2. That is, Captive Portal users are first placed into the *logon* user role, which allows users to be given an IP address and placed into a VLAN but otherwise disallows access to the network. You can configure default user roles for authenticated or guest Captive Portal users.

NOTE: MAC-based authentication, if enabled on the WLAN Switch, takes precedence over Captive Portal authentication. If you use Captive Portal, do not enable MAC-based authentication.

Configuring Captive Portal in the Base AOS-W

With the AOS-W 2.5.2 release, Captive Portal is available in the base operating system; you do not need to install the Policy Enforcement Firewall license in the WLAN Switch for this feature.

In the base operating system, Captive Portal users are first placed into the predefined *cpbase* user role, which allows only DNS, DHCP, and HTTP or HTTPS connections to the network. Upon authentication, Captive Portal users are allowed full access to their assigned VLAN.

The following are the basic tasks for configuring Captive Portal in the base operating system:

- Configure the Captive Portal for guest or authenticated users. In the base operating system, you enable Captive Portal on a per-ESSID basis.
- If you are using Captive Portal to authenticate users, configure the authentication server that will be used to validate users. The authentication server can be an external server or the WLAN Switch's internal database.

The easiest way to complete these tasks is by using the WebUI Basic WLAN configuration page. Navigating to the **Configuration** > **Basic** > **WLAN** page allows you to configure an ESSID for either Guest Captive Portal or Captive Portal users.

To configure either Guest Captive Portal or Captive Portal for a single ESSID:

1. Navigate to the **Configuration** > **Basic** > **WLAN** page.
2. Enter the SSID name, for example WLAN-01.
3. Under 802.11 Security, select either **Guest Captive Portal** (for unauthenticated users) or **Captive Portal** (for authenticated users).

   If you select Captive Portal, you need to specify the authentication server that will validate the username and password for Captive Portal users:

   A. Click **Add** under Authentication Servers.

   B. Under **Choose an Authentication Server**, select the authentication server that will be the primary server.

   C. Click **Add** for the selection to be applied.

   D. To add additional authentication servers as backup servers, repeat the steps above.

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

4. Specify the VLAN to which users will be assigned.
5. Click **Apply**.

You can optionally configure other Captive Portal parameters by navigating to the **Configuration > Advanced > Security > Authentication Methods > Captive Portal Authentication** page. For example, if a proxy server is used for HTTP(S) access, you need to explicitly allow TCP traffic between Captive Portal users and the proxy server. See "Configuring Advanced Captive Portal Options" on page 66.

Configuring Captive Portal with the Policy Enforcement Firewall License

This section describes how to configure Captive Portal using role-based access provided by the Policy Enforcement Firewall software module. You must install the Policy Enforcement Firewall license, as described in "Managing Software Feature Licenses" in Volume 7 of the *AOS-W User Guide*.

The following are the basic tasks for configuring Captive Portal using role-based access:

- Configure the policies for guest or authenticated Captive Portal users.

  NOTE: The predefined *captiveportal* policy contains rules that direct users to the Captive Portal when they start a Web browser connection to the WLAN Switch. Ensure that the *logon* role includes the *captiveportal* policy.

- If you are using Captive Portal to authenticate users, configure the authentication server that will be used to validate users.
- Configure the Captive Portal for guest or authenticated users.

The easiest way to complete these steps is by using the WebUI Basic WLAN configuration page. Navigating to the **Configuration > Basic > WLAN** page allows you to configure an ESSID for either Guest Captive Portal or Captive Portal users.

To configure either Guest Captive Portal or Captive Portal for a single ESSID:

1. Navigate to the **Configuration > Basic > WLAN** page.
2. Enter the SSID name, for example WLAN-01.
3. Under 802.11 Security, select either **Guest Captive Portal** (for unauthenticated users) or **Captive Portal** (for authenticated users).

NOTE: If you are supporting both guest and authenticated Captive Portal users on the same ESSID, you need to configure Captive Portal in the Captive Portal Authentication page. Navigate to

If you select Captive Portal, you need to specify the authentication server that will validate the username and password for Captive Portal users:

A. Click **Add** under Authentication Servers.

B. Under **Choose an Authentication Server**, select the authentication server that will be the primary server.

C. Click **Add** for the selection to be applied.

D. To add additional authentication servers as backup servers, repeat the steps above.

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

4. Specify the VLAN to which users will be assigned.

5. The Firewall Policies section allows you to specify the policy for Captive Portal users. You can do one of the following actions:

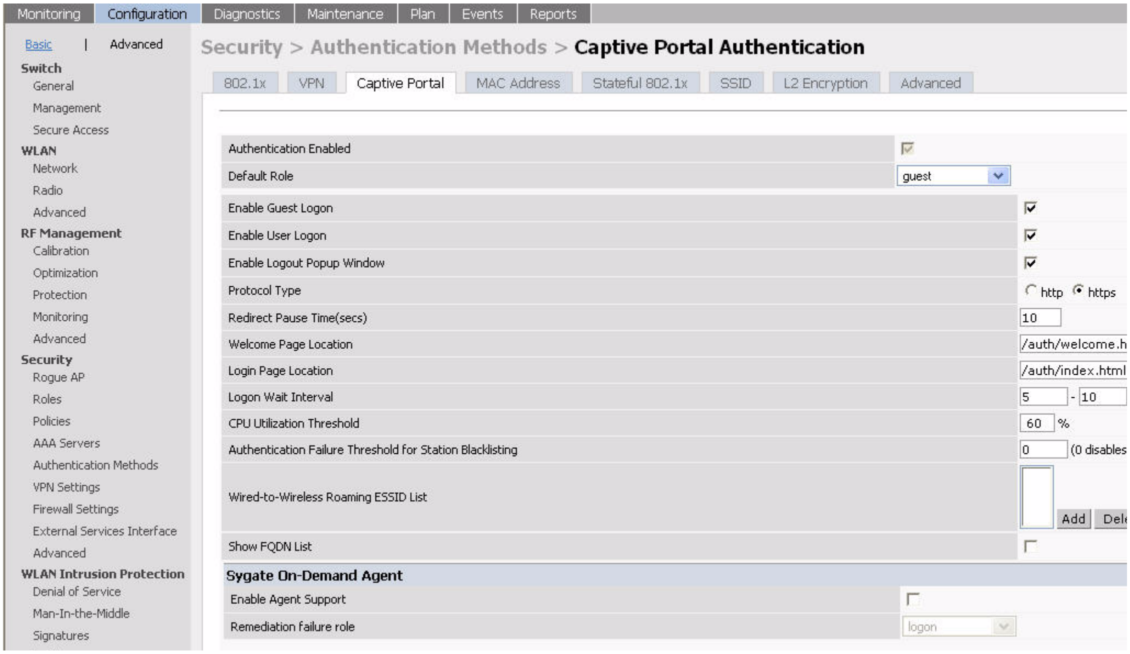
    - Select an existing policy from the scrolling list.
    - Select an existing policy from the scrolling list and then **Add** or **Edit** rules for the policy.
    - To add a new policy, select **NEW** from the scrolling list and then **Add** rules for the policy.

6. Click **Apply**.

You can optionally configure other Captive Portal parameters by navigating to the **Configuration** > **Advanced** > **Security** > **Authentication Methods** > **Captive Portal Authentication** page, as described in the following section.

Configuring Advanced Captive Portal Options

In the WebUI, you configure advanced Captive Portal options in the **Configuration > Advanced > Security > Authentication Methods > Captive Portal > Authentication** page (shown below).



Authentication Enabled	☑
Default Role	guest
Enable Guest Logon	☑
Enable User Logon	☑
Enable Logout Popup Window	☑
Protocol Type	○ http ● https
Redirect Pause Time(secs)	10
Welcome Page Location	/auth/welcome.h
Login Page Location	/auth/index.html
Logon Wait Interval	5 - 10
CPU Utilization Threshold	60 %
Authentication Failure Threshold for Station Blacklisting	0 (0 disables
Wired-to-Wireless Roaming ESSID List	
Show FQDN List	□

Sygate On-Demand Agent

Enable Agent Support	□
Remediation failure role	logon

FIGURE 4-1 Captive Portal Authentication Page

Table 4-1 describes Captive Portal configuration options.

NOTE: In the CLI, you configure these options with the **aaa captive-portal** commands.

TABLE 4-1 Captive Portal Authentication WebUI Page Options

Parameter	Description
Default Role (Only available with Policy Enforcement Firewall license)	The role assigned to the Captive Portal user upon login. When both the user and guest logins are enabled, the default role applies to the user login; users logging in using the guest interface are assigned the guest role. Default: guest
Enable Guest Logon	Select this option to enable Captive Portal logon without authentication. Default: Disabled
Enable User Logon	Select this option to enable Captive Portal with authentication of user credentials. Default: Enabled
Enable Logout Popup Window	When this is enabled, a pop-up window appears with the Logout link for the user to logout after logon. If this is disabled, the user remains logged in until the user timeout period or until the station reloads. Default: Enabled
Protocol type	The protocol used on re-direction to the Captive Portal page. If you select http, modify the *captiveportal* policy to allow http traffic. Default: https
Redirect Pause Time	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 displays until the user clicks on the indicated link. 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

TABLE 4-1 Captive Portal Authentication WebUI Page Options (Continued)

Login Page Location	The login page is the page that appears for the user logon. This can be set to any URL. Default: /auth/index.html
Logon Wait Interval	Time range, in seconds, the user will have to wait for the logon page to pop up if 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 is applied when presenting the user with the logon page. Default value: 60 %
Match ESSID List (Base operating system only)	Specifies the ESSIDs on which Captive Portal is enabled.
Proxy Host: Port (Base operating system only)	Specifies the IP address of the proxy host and port used for HTTP(S) access.

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

Configuring the AAA Server for Captive Portal

The Captive Portal Authentication page allows you to choose the authentication server(s) to be used for user authentication:

1. Under **Choose an Authentication Server** a pull-down menu allows you to select the authentication server that will be the primary server.
2. Click **Add** for the selection to be applied.
3. To add additional authentication servers as backup servers, repeat the steps above.
4. The servers appear in the order of descending priority. The first entry is always the primary server. To change the order, use the up or down arrows to move an entry higher or lower in the list.
5. Click **Apply**.

Changing the Protocol to HTTP

By default, HTTPS is used on redirection to the Captive Portal page. If you need to use HTTP instead, you need to modify the following:

- Change the protocol type to HTTP:
  - In the WebUI, navigate to the **Configuration** > **Advanced** > **Security** > **Authentication Methods** > **Captive Portal** page. For Protocol Type, select **http** and click **Apply**.
  - In the CLI, enter the command **aaa captive-portal protocol-http**.
- Modify the *captiveportal* policy to permit HTTP traffic.
  - In the WebUI, navigate to the **Configuration** > **Advanced** > **Security** > **Policies** page.

    I. Click **Edit** for the *captiveportal* policy.

    II. Delete the rule for “user mswitch svc-https permit”.

    III. Add a new rule for the following and move this rule to the top of the rules list:

    source is user

    destination is the mswitch alias

    service is svc-http

    action is permit

    IV. Click **Apply**.
  - In the CLI, enter the following:

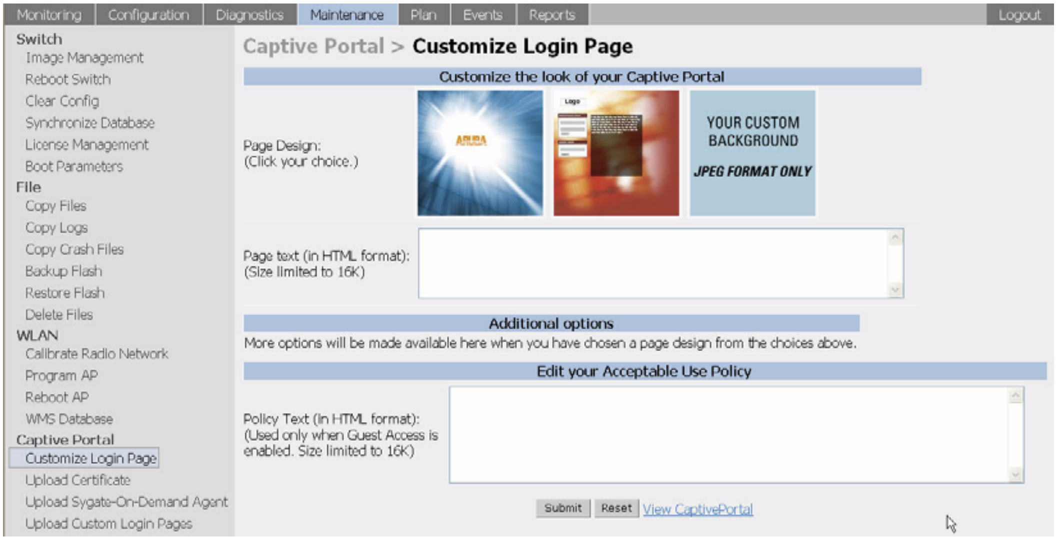
```
ip access-list session "captiveportal"
no alias "user" alias "mswitch" "svc-https" permit
alias "user" alias "mswitch" "svc-http" permit
alias "user" any "svc-http" dst-nat 8080
alias "user" any "svc-https" dst-nat 8081
```

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.



Captive Portal > **Customize Login Page**

Customize the look of your Captive Portal

Page Design:
(Click your choice.)

Page text (in HTML format):
(Size limited to 16K)

Additional options

More options will be made available here when you have chosen a page design from the choices above.

Edit your Acceptable Use Policy

Policy Text (In HTML format):
(Used only when Guest Access is enabled. Size limited to 16K)

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

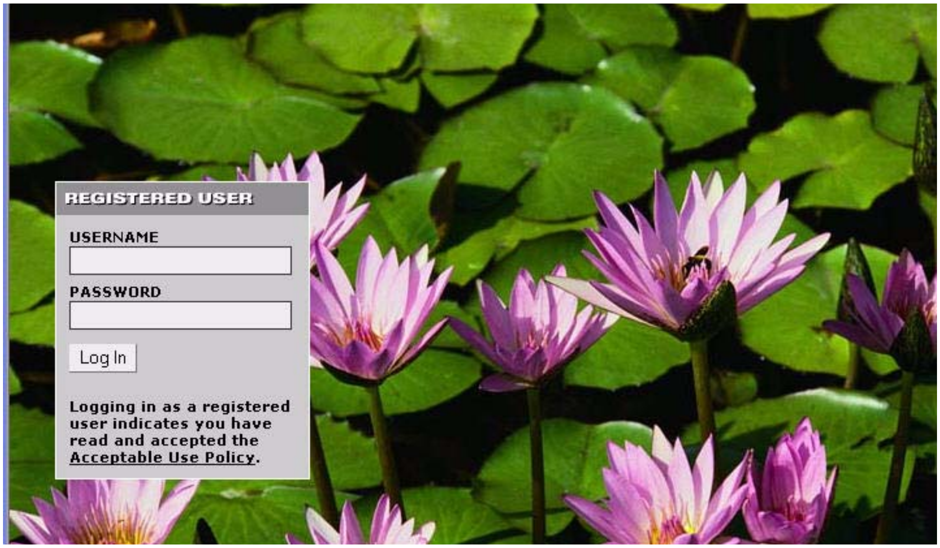
2. To customize the page background:

   A. Select the **YOUR CUSTOM BACKGROUND** page.

   B. Under **Additional options**, enter the location of the JPEG image in the Upload your own custom background field.

   C. You can also set the background color in the Custom page background color field. The color code must a hexadecimal value in the format #hhhhhh.

D. You can view the background setting by first clicking **Submit** on the bottom on the page, then clicking the **View CaptivePortal** link. This displays the Captive Portal page as it will be seen by users.



REGISTERED USER

USERNAME

PASSWORD

Log In

Logging in as a registered user indicates you have read and accepted the Acceptable Use Policy.

To customize the captive portal background text:

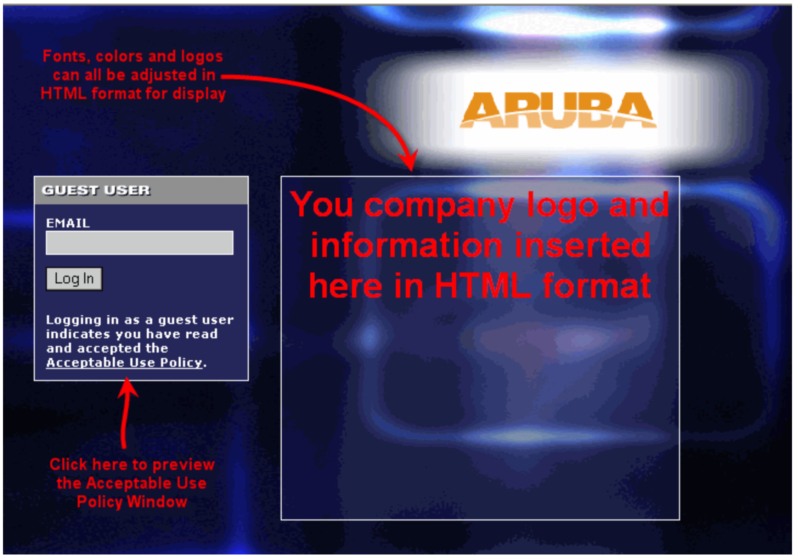
- Enter the text that needs to be displayed in the **Page Text (in HTML format)** message box. To view the changes, click **Submit** at the bottom on the page and then click the **View CaptivePortal** link. This will bring up the captive portal page as seen by the users

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.

E. To view the changes, click **Submit** at the bottom on the page and then click the **View CaptivePortal** link. This displays the Captive Portal page as it will be seen by users.


Fonts, colors and logos can all be adjusted in HTML format for display
ARUBA
GUEST USER
EMAIL
Log In
You company logo and information inserted here in HTML format
Click here to preview the Acceptable Use Policy Window

Logging in as a guest user indicates you have read and accepted the Acceptable Use Policy.

The text you entered appears in a text box when the user clicks the **Acceptable Use Policy** on the Captive Portal web page.

Configuring Virtual Private Networks 5

The combination of Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPSec) is a highly secure technology for making remote access virtual private network (VPN) connections across public networks such as the Internet. For wireless networks, VPN can also be used to further secure the wireless data from attackers. The Alcatel WLAN Switch can be used as a VPN concentrator that terminates all VPN connections from both wired and wireless users. For Windows clients, a dialer can be downloaded from the WLAN Switch to auto configure the tunnel settings on the dialer. This chapter primarily deals with the configuration of L2TP and Point-to-Point Tunneling Protocol (PPTP) VPN tunnels.

This chapter describes the following topics:

- "VPN Configuration" on page 73
- "Example Configurations" on page 77

VPN Configuration

To configure VPN on the WLAN Switch, the VPN authentication method needs to be enabled first.

Enabling VPN Authentication

To enable VPN authentication, you must configure the following prerequisites:

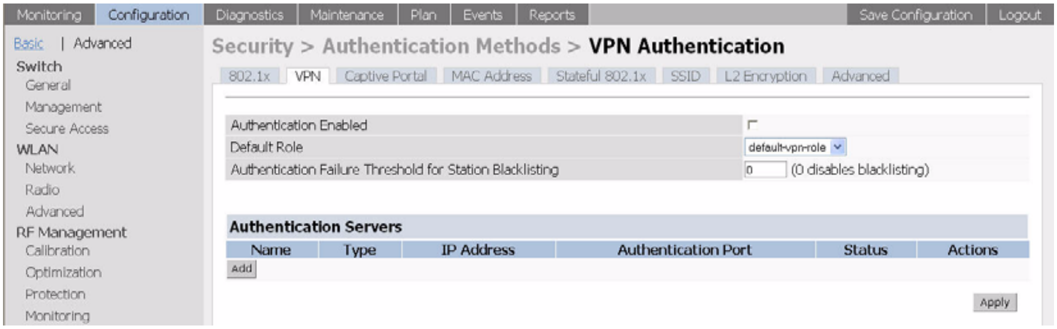
- **Role –** The default user role for the 802.1x users. Refer to Chapter 1, "Configuring Firewall Roles and Policies" to configure roles.

  Derivation rules, if present, take precedence over the default user role.

- **Authentication Server –** The authentication server the WLAN Switch would use to validate the users. Refer to Chapter 2, "Configuring AAA Servers" for configuration details.

To enable VPN authentication:

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



Security > Authentication Methods > **VPN Authentication**

Authentication Enabled	□
Default Role	default-vpn-role
Authentication Failure Threshold for Station Blacklisting	0 (0 disables blacklisting)

Authentication Servers

Name	Type	IP Address	Authentication Port	Status	Actions

2. Select the **Authentication Enabled** checkbox to enable VPN authentication.

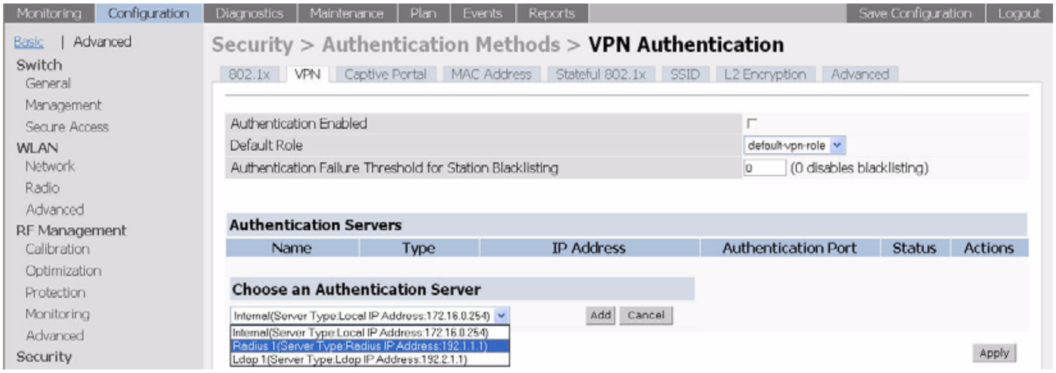
3. Choose the **Default Role** for the users from the pull down menu.

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 **Add** under **Authentication Server** to add a server.

6. From the pull down menu select the server that will be the primary authentication server. Click **Add** after making the choice.

7. To add servers, repeat the steps for each server.



Security > Authentication Methods > **VPN Authentication**

Authentication Enabled	□
Default Role	default-vpn-role
Authentication Failure Threshold for Station Blacklisting	0 (0 disables blacklisting)

Authentication Servers

Name	Type	IP Address	Authentication Port	Status	Actions

Choose an Authentication Server

Internal(Server Type:Local IP Address:172.16.0.254)
Internal(Server Type:Local IP Address:172.16.0.254)
Radius 1(Server Type:Radius IP Address:192.1.1.1)
Ldap 1(Server Type:Ldap IP Address:192.2.1.1)

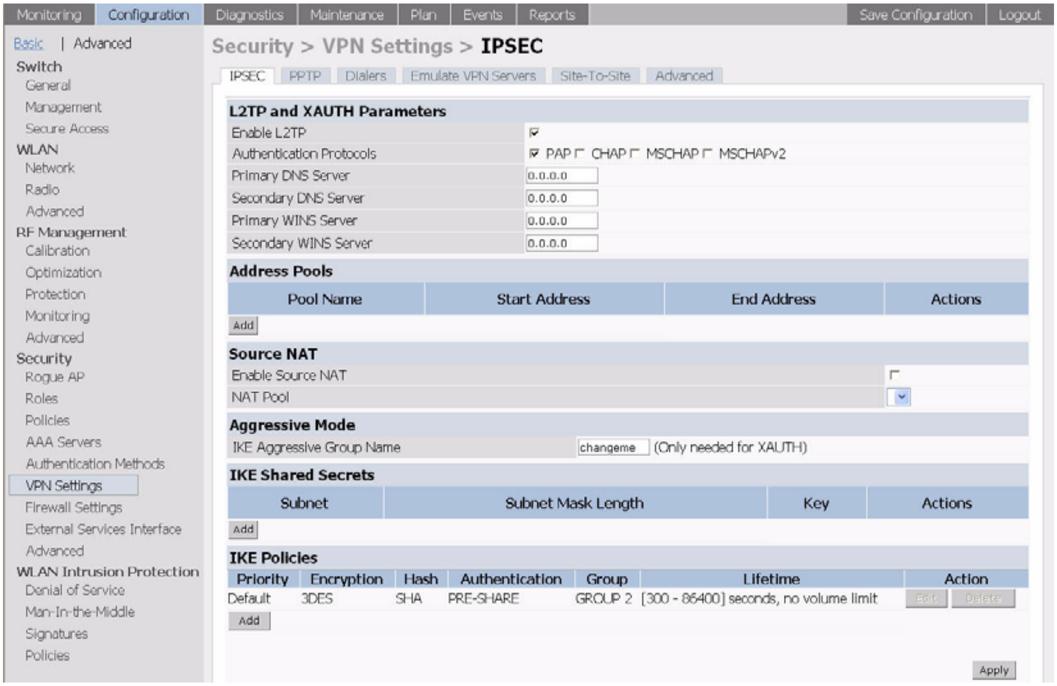
8. The servers appear in the order of descending priority. The first entry is always the primary server. To change the order, use the Up or Down buttons to the right on the entry to move it higher up or lower down in the list.

9. Click **Apply** to apply the configuration changes made before navigating to other pages to avoid losing the changes made.

10. Click **Save Configuration** to save the configuration between reboots.

Configuring VPN with L2TP IPSec

1. Navigate to the **Configuration > Advanced > Security > VPN Settings > IPSEC** page.



Security > VPN Settings > IPSEC

L2TP and XAUTH Parameters

Enable L2TP	☑
Authentication Protocols	☑ PAP ☐ CHAP ☐ MSCHAP ☐ MSCHAPv2
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Primary WINS Server	0.0.0.0
Secondary WINS Server	0.0.0.0

Address Pools

Pool Name	Start Address	End Address	Actions

Source NAT

Enable Source NAT	☐
NAT Pool	

Aggressive Mode

IKE Aggressive Group Name: changeme (Only needed for XAUTH)

IKE Shared Secrets

Subnet	Subnet Mask Length	Key	Actions

IKE Policies

Priority	Encryption	Hash	Authentication	Group	Lifetime	Action
Default	3DES	SHA	PRE-SHARE	GROUP 2	[300 - 86400] seconds, no volume limit	Edit Delete

2. To enable L2TP, check **Enable L2TP**.

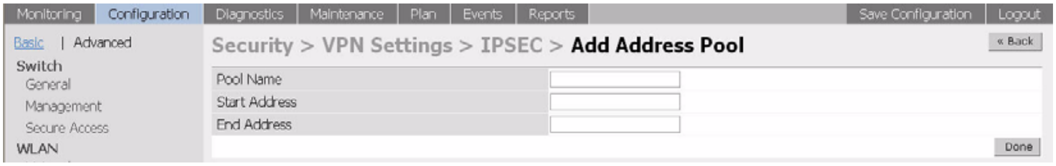
3. Select the authentication method. Currently supported methods are Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MSCHAP) and MSCHAP version 2 (MSCHAPv2).

4. Configure the IP addresses of the primary and secondary Domain Name System (DNS) servers and primary and secondary Windows Internet Naming Service (WINS) Server that will be pushed to the VPN client.

Address Pools

This is the pool from which the clients are assigned addresses.

1. Under Address Pools, click **Add** to open the **Add Address Pool** page.



Security > VPN Settings > IPSEC > **Add Address Pool**

Pool Name	
Start Address	
End Address	

2. Specify the start address, the end address and the pool name.
3. Click **Done** to apply the configuration.

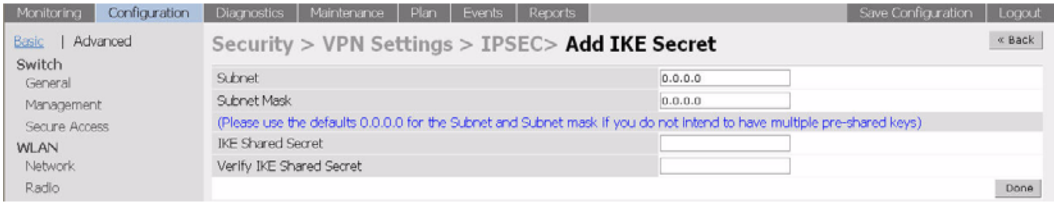
Source NAT

Use this option if the IP addresses of users need to be translated to access the network. To use this option, you must have created a NAT pool by navigating to the **Configuration > Advanced > Security > Advanced > NAT Pools** page.

IKE Shared Secrets

You can configure a global IKE key or configure an IKE key for each subnet. Make sure that this key matches the key on the client.

1. Under IKE Shared Secrets, click **Add** to open the **Add IKE Secret** page.



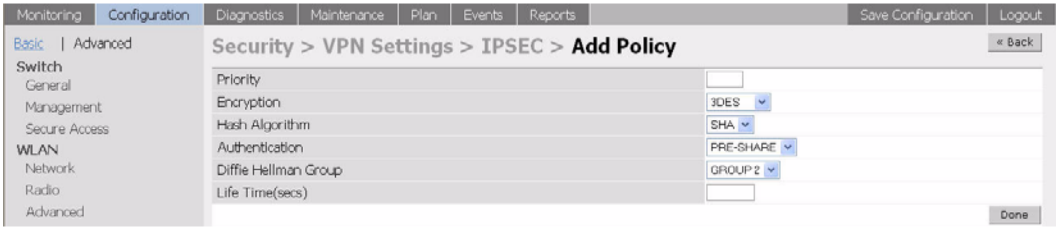
Security > VPN Settings > IPSEC> **Add IKE Secret**

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

2. Enter the subnet and subnet mask. To make the IKE key global, specify 0.0.0.0 and 0.0.0.0 for both values.
3. Enter the **IKE Shared Secret** and **Verify IKE Shared Secret**.
4. Click **Done** to apply the configurations.
5. Click **Back** to return to the main VPN L2TP configuration page.

IKE Policies

1. Under IKE Policies, click **Add** to open the **IPSEC Add Policy** configuration page.



Security > VPN Settings > IPSEC > **Add Policy**

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

2. Set the **Priority** to 1 for this configuration to take priority over the Default setting.
3. Set the **Encryption** type from the drop-down menu**.**
4. Set the **HASH Algorithm** to **SHA** or **MD5**.
5. Set the **Authentication** to **Pre-Share** or **RSA**.
6. Set the **Diffie Hellman Group** to **Group 1** or **Group 2**.

   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.
7. Click **Done** to activate the changes.
8. Click **Back** to return to the main VPN L2TP configuration page.
9. Click **Apply** to apply the changes made before navigating to other pages.

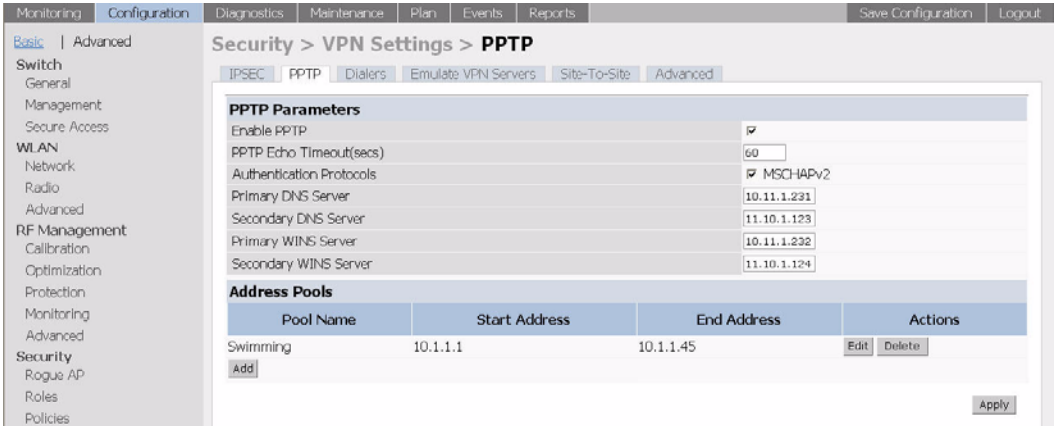
Example Configurations

Configuring VPN with PPTP

You must configure the following prerequisites:

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

2. Navigate to the **Configuration** > **Advanced** > **Security** > **VPN Settings** > **PPTP** *page*



Security > VPN Settings > **PPTP**

PPTP Parameters

Enable PPTP	☑
PPTP Echo Timeout(secs)	60
Authentication Protocols	☑ MSCHAPv2
Primary DNS Server	10.11.1.231
Secondary DNS Server	11.10.1.123
Primary WINS Server	10.11.1.232
Secondary WINS Server	11.10.1.124

Address Pools

Pool Name	Start Address	End Address	Actions
Swimming	10.1.1.1	10.1.1.45	Edit Delete

3. To enable PPTP, select **Enable PPTP**.

4. Select the authentication method. The currently-supported method is MSCHAPv2.

5. Configure the primary and secondary DNS servers and primary and secondary WINS Server that will be pushed to the VPN Dialer.

6. Configure the VPN Address Pool.

   A. Click **Add**. The **Add Address Pool** page displays.

   B. Specify the start address, the end address and the pool name.

   C. Click **Done** on completion to apply the configuration.

7. Click **Back** to access the main PPTP configuration page.

8. Click **Apply** to apply the changes made before navigating to other pages.

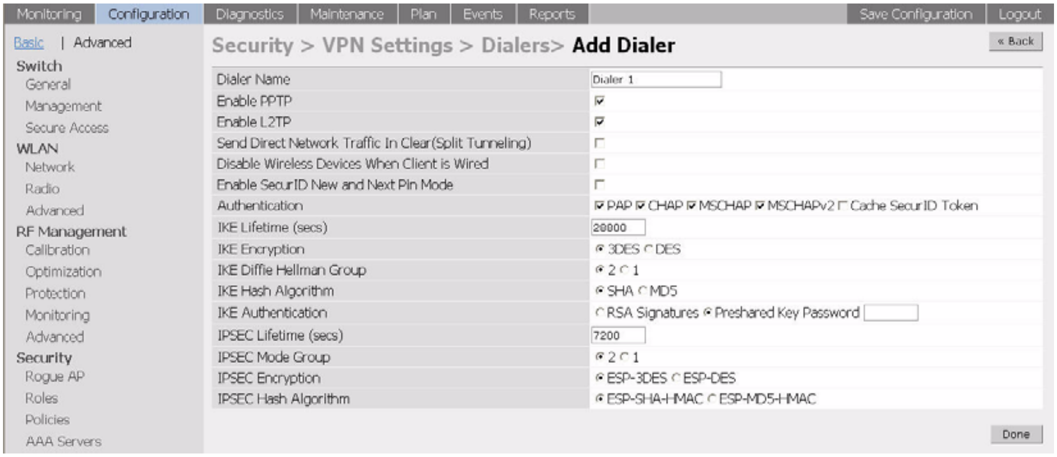
Configuring Alcatel Dialer

1. Navigate to the **Configuration** > **Advanced** > **Security** > **VPN Settings** > **Dialers** page. Click **Add** to add a new dialer or click the **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 selecting the **Enable PPTP** or the **Enable L2TP** checkbox.



Security > VPN Settings > Dialers> Add Dialer

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

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.

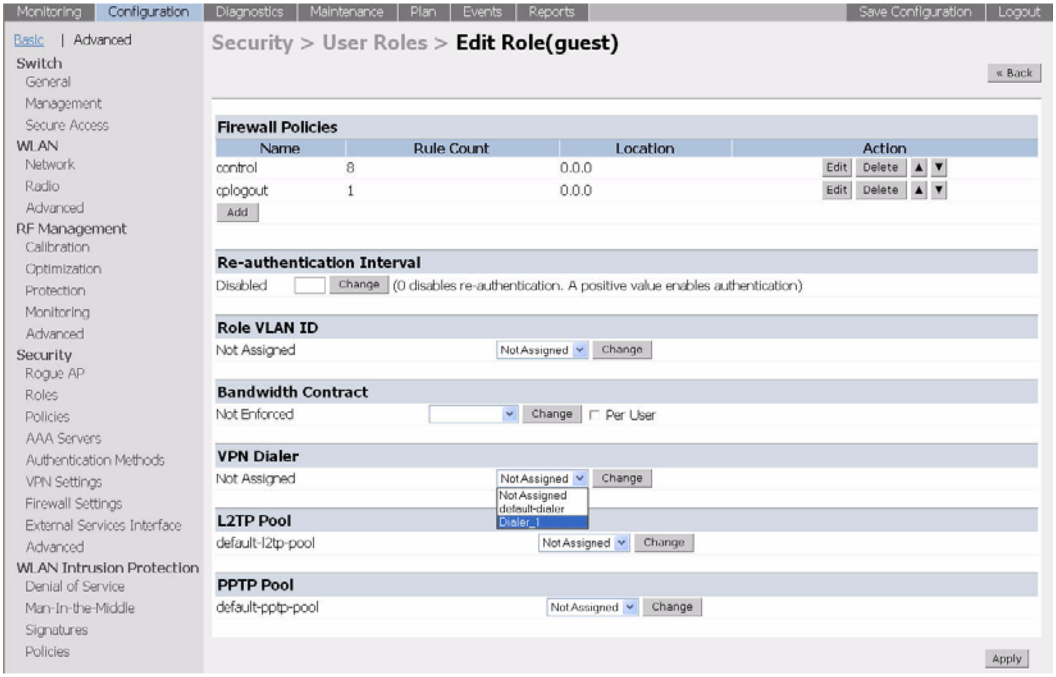
For L2TP:

1. Set the hash algorithm to SHA or MD5 as in the **IKE Policies** page.
2. If Pre-share is selected as the authentication in the **IKE Policies** page, enter the pre-share key used in the L2TP configuration.

   NOTE: The two keys must match.

3. Select the IPSEC Mode Group configuration as in the **IKE Policy** page for **Diffie Hellman Group**.
4. Select the IPSEC Encryption as in the **IKE Policy** page for **Encryption**.
5. Select the IPSEC Hash Algorithm to the **Algorithm** selected in the **IKE Policy** page of IPSEC.
6. Click **Done** to apply the changes made prior to navigating to another page.
7. The VPN dialer can be downloaded using Captive Portal: for the role the user is assigned through captive portal, configure the dialer by the name used to identify the dialer.

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



Security > User Roles > **Edit Role(guest)**

Firewall Policies

Name	Rule Count	Location	Action
control	8	0.0.0	Edit Delete ▲ ▼
cplogout	1	0.0.0	Edit Delete ▲ ▼

Re-authentication Interval

Disabled (0 disables re-authentication. A positive value enables authentication)

Role VLAN ID

Not Assigned — Not Assigned

Bandwidth Contract

Not Enforced — □ Per User

VPN Dialer

Not Assigned — Not Assigned
Not Assigned
default-dialer
Dialer_1

L2TP Pool

default-l2tp-pool — Not Assigned

PPTP Pool

default-pptp-pool — Not Assigned

Configuring Site-to-Site VPN

Site-to-site VPN allows sites at different physical locations to securely communicate with each other over a Layer-3 network such as the Internet. You can use Alcatel WLAN Switches instead of VPN concentrators to connect the sites. Or, you can use a VPN concentrator at one site and a WLAN Switch at the other site.

You must configure VPN settings on the WLAN Switches at both the local and remote sites. In the following figure, a VPN tunnel connects Network A to Network B across the Internet.

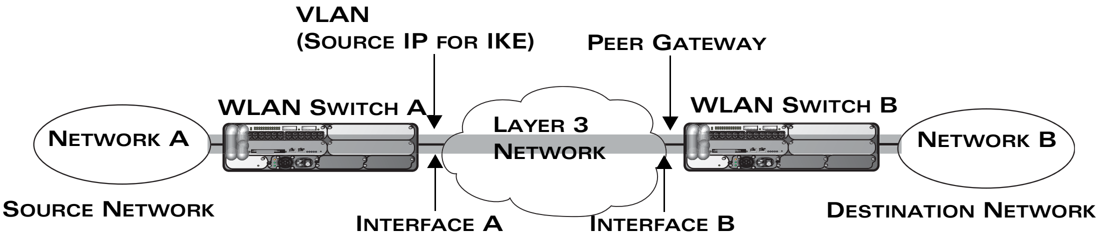


Figure 5-1 Site-to-Site VPN Configuration Components

To configure the VPN tunnel on WLAN Switch A, you need to configure the following:

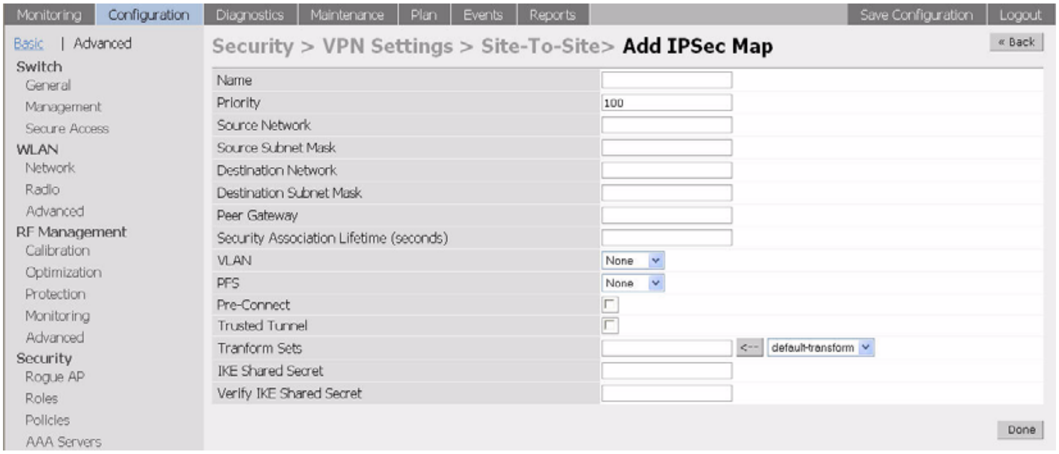
- The source network (Network A)
- The destination network (Network B)
- The VLAN on which the WLAN Switch A's interface to the Layer-3 network is located (Interface A in the figure)
- The peer gateway, which is the IP address of WLAN Switch B's interface to the Layer-3 network (Interface B in the figure)

To configure a site-to-site VPN on the WLAN Switch:

Note: You must configure VPN settings on the WLAN Switches at both the local and remote sites.

1. Navigate to the **Configuration** > **Advanced** > **Security** > **VPN Settings** > **Site-to-Site** page.

2. Under IPSec Maps, click **Add** to open the Add IPSec Map page.



Security > VPN Settings > Site-To-Site> **Add IPSec Map**

Name	
Priority	100
Source Network	
Source Subnet Mask	
Destination Network	
Destination Subnet Mask	
Peer Gateway	
Security Association Lifetime (seconds)	
VLAN	None
PFS	None
Pre-Connect	□
Trusted Tunnel	□
Tranform Sets	<-- default-transform
IKE Shared Secret	
Verify IKE Shared Secret	

3. Enter a name for this VPN connection in the **Name** field.

4. Enter the IP address and netmask for the source (the local network connected to the WLAN Switch) in the **Source Network** and **Source Subnet Mask** fields, respectively. (See WLAN Switch A in Figure 5-1.)

5. Enter the IP address and netmask for the destination (the remote network to which the local network will communicate) in the **Destination Network** and **Destination Subnet Mask** fields, respectively. (See WLAN Switch B in Figure 5-1.)

6. In the **Peer Gateway** field, enter the IP address of the interface on the remote WLAN Switch that connects to the Layer-3 network. (See Interface B in Figure 5-1.)

7. Select the **VLAN** that contains the interface of the local WLAN Switch which connects to the Layer-3 network. (See Interface A in Figure 5-1.)

   This determines the source IP address used to initiate IKE. If you select 0 or None, the default is the VLAN of the WLAN Switch’s IP address (either the VLAN where the loopback IP is configured or VLAN 1 if no loopback IP is configured).

8. Select **Pre-Connect** to have the VPN connection established even if there is no traffic being sent from the local network. If this is not selected, the VPN connection is only established when traffic is sent from the local network to the remote network.

9. Select **Trusted Tunnel** if traffic between the networks is trusted. If this is not selected, traffic between the networks is untrusted.

10. Enter the IKE shared secret.

11. Click **Done** to apply the configuration.

Configuring Advanced Security 6

xSec (or Extreme Security) is a cryptographically secure, Layer-2 tunneling network protocol. xSec is implemented over 802.1x protocol.

This protocol can be used to secure Layer-2 traffic between the WLAN Switch and the wired and wireless clients, and between two Alcatel WLAN Switches.

This chapter describes the following topics:

- "Advantages of Using xSec" on page 83
- "Enabling xSec on the Alcatel WLAN Switch" on page 84
- "xSec Communication" on page 85
- "xSec Configurations" on page 85

Advantages of Using xSec

xSec encrypts the original Layer-2 data frame inside a Layer-2 xSec frame, the contents of which is defined by the protocol. xSec relies on 256-bit AES encryption. Upon authentication, xSec creates tunnel between the client and the WLAN Switch. The xSec frame sent over the air or wire between the user and the WLAN Switch contains all user / WLAN Switch information, as well as the original IP and MAC address, but in encrypted form. The only visible address is the MAC address assigned by the xSec protocol for the tunnel endpoints. All user information is now truly secured using xSec. This concept is also extended to secure information, management and data, between two Alcatel WLAN Switches on the same VLAN.

For xSec tunneling between the client and Alcatel WLAN Switch to work, a version of the Funk Odyssey client[1] that supports xSec needs to be installed on the client machine. Using xSec, it is possible to secure Win 2000 and Win XP operating systems.

xSec provides the following advantages:

- Advanced security as Layer-2 frames are encrypted and tunneled.

[1] For information on the currently supported release, please contact Funk.

- Ease of implementation of advanced encryption in a heterogeneous environment. xSec is designed to support multiple OSs and a wide range of NICs. All encryption and decryption on the client machine is done by the Odyssey client while the NICs are configured with NULL encryption. This ensures that even older OSs that cannot be upgraded to support WPA / WPA2 can be secured using xSec and the xSec-Odyssey client.
- Is compatible with TLS, TTLS and PEAP.
- Extends advanced authentication to wired clients allowing network managers to secure wired ports.

Enabling xSec on the Alcatel WLAN Switch

xSec is a licensed feature. Upon purchasing and installing the xSec license, xSec is automatically enabled on the Alcatel WLAN Switch.

Deployment Scenarios for xSec

xSec can be used to secure traffic in the following scenarios:

- Between the WLAN Switch and the wireless client
- Between the WLAN Switch and a wired client
- Secure communications between two WLAN Switches on the same VLAN.

Each of these deployment scenarios and the configurations / settings for each of them is described in detail in this section.

xSec Communication

Consider the following topology:

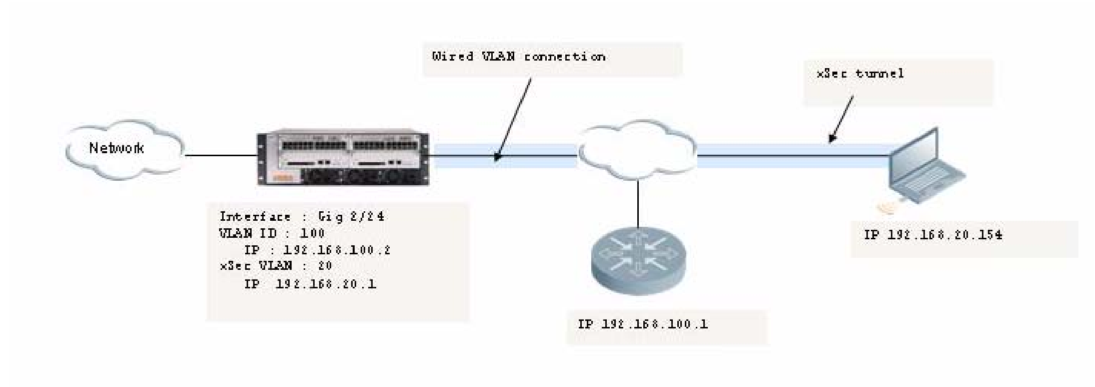


FIGURE 6-1 Securing Client Traffic Over the Internet

For the client to connect to the Internet, it has to complete 802.1x authentication. The use of xSec by the client is indicated during the 802.1x transactions to the WLAN Switch. Upon successful authentication, the xSec tunnel is established between the Alcatel WLAN Switch and the client. Once the tunnel is established, the client laptop is assigned an IP address from the xSec VLAN (for wired clients) or from the user VLAN (for wireless clients). All traffic between the user and the WLAN Switch is now encrypted.

In the case of wired xSec, all traffic to and from the WLAN Switch on the port's native VLAN will be unencrypted whereas all xSec tunnel traffic will be encrypted. This means that Alcatel WLAN Switches can communicate with non-xSec-capable devices as well as xSec-capable devices on the same port.

In Figure 6-1, traffic on VLAN 100 is un-encrypted, whereas traffic on VLAN20 is encrypted. Traffic to and from the Router on VLAN 100 is un-encrypted.

xSec Configurations

This section includes the following configurations:

- Securing wireless clients
- Securing wired clients
- Securing WLAN Switch to WLAN Switch communications

Securing a Wireless Client

Wireless Clients can be secured using xSec by installing the Odyssey client on the client machine and configuring the Alcatel WLAN Switch to support xSec. The APs can connect back to the WLAN Switch across a Layer-2 or a Layer-3 network. All traffic from the wireless client to the WLAN Switch will be encrypted. Traffic on the native VLAN of the ports that connect to the AP network will be unencrypted. Traffic from the AP to the WLAN Switch is encapsulated in a GRE tunnel with the control traffic from the AP being unencrypted.

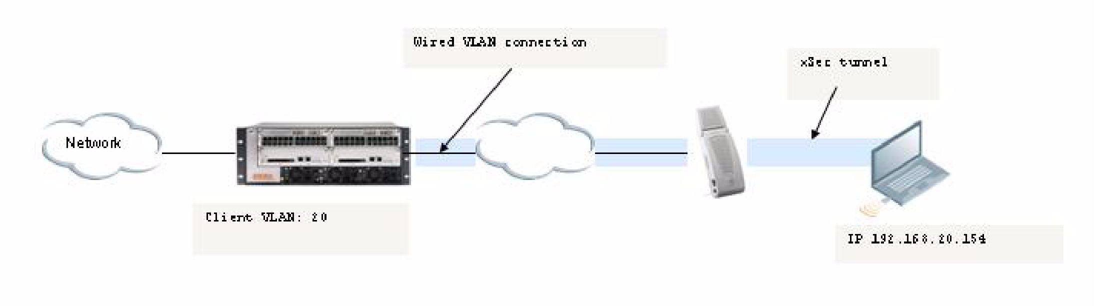


FIGURE 6-2 Securing Wireless Clients

Configuring xSec for Wireless Clients

1. Configure the Access Point.

   xSec requires the APs to be configured with encryption disabled (encryption set to NULL). There are two settings that the APs can operate in based on the encryption. The difference would be based on the type of clients allowed.

   A. Encryption set to xSec

   In this case, the encryption method on the APs is set to NULL and only xSec clients will be allowed to connect to the network. All other connections are dropped.

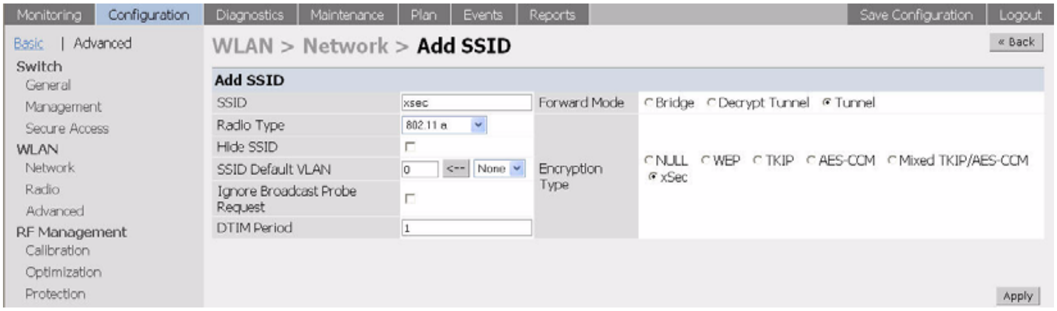
   B. Encryption set to NULL

   Here, clients with authentication disabled would be allowed to connect to the AP along with the xSec client. Though the xSec clients are secured, the data from the non-encrypted clients will be visible in the air in clear text.

   Alcatel strongly recommends the use of the former method (A) as the selected encryption method. Alcatel recommends the use of method B when connecting non-Alcatel APs. In this case, the WLAN Switch port that connects to the third-party AP is protected by xSec.

2. Navigate to the **Configure > Advanced > WLAN > Network > SSID** page.

Configure the AP settings – ESSID and VLAN. Set the encryption type to **xSec** or **NULL**.



WLAN > Network > **Add SSID**

Add SSID

SSID	xsec	Forward Mode	○ Bridge ○ Decrypt Tunnel ● Tunnel
Radio Type	802.11 a	Encryption Type	○ NULL ○ WEP ○ TKIP ○ AES-CCM ○ Mixed TKIP/AES-CCM ● xSec
Hide SSID	□		
SSID Default VLAN	0 <-- None		
Ignore Broadcast Probe Request	□		
DTIM Period	1		

3. Click **Apply** for the configuration changes made to take effect.

4. Configure the Authentication method.

   Enable 802.1x authentication on the Alcatel WLAN Switch. Enable 802.1x and configure the default-role. For information on setting up 802.1x on the Alcatel WLAN Switch refer to Chapter 3, “Configuring 802.1x Authentication.”

5. Configure the client.

   The Funk Odyssey Client needs to be installed and set up on the client to support xSec. Refer to “Configuring the Funk Client on Client Machines” on page 93 for instruction on how to set up xSec.

Configure xSec for Wired Clients

xSec can be used to secure communication between a wired client and a WLAN Switch or to establish a point-point secure connection between two Alcatel WLAN WLAN Switches connected over a Layer-2 network.

To enable xSec on a Fast Ethernet / Gig Ethernet port, the following parameters need to be set at the interface level.

TABLE 6-1 Ethernet Port Parameter Settings

xSec Vlan	The VLAN on which the xSec tunnel terminates. All traffic on this VLAN will be encrypted. In case of the wired client, the clients would be assigned this VLAN. This VLAN *must* have a Layer-3 interface. If the WLAN Switch is a DHCP server or replay on this VLAN, the interface must have an IP address assigned to it.
Native port VLAN	The access VLAN for this port must be a VLAN that is *different* from the xSec VLAN. All the unencrypted and non xSec tunnel traffic will belong to this VLAN
xSec assigned ports	This is of importance only in the WLAN Switch-to-WLAN Switch, point-to-point tunnel setting. This parameter is used to specify the VLANs that will be shared across the two WLAN Switches forming the tunnel end points.

Alcatel WLAN Switches support 802.1x for wired clients as well as wireless clients. xSec can be used as the encryption method for the 802.1x wired clients.

To secure the wired client:

1. Enable wired 802.1x on the Alcatel WLAN Switch.

   Navigate to the **Configuration > Advanced > Security > Authentication Methods > 802.1x** page. Select the **Enable Wired Clients** checkbox. Click **Apply** to apply the configuration. For information on setting up 802.1x on the Alcatel WLAN Switch refer to **Chapter 3, "Configuring 802.1x Authentication."**

2. Configure VLAN and the Layer-3 interface.

   Navigate to the **Configuration > Advanced > Switch > General > VLAN** page. Configure the VLAN to be used for xSec communication and xSec clients. Configure an IP address for the VLAN making it a Layer-3 interface.

3. Ensure that a DHCP server is configured to provide addresses to the xSec clients with addresses from the above mentioned address space.

4. Identify the ports on the Alcatel WLAN Switch which the xSec clients will use to connect. In Figure 6-3, port Fe2/10 connects to the xSec client “Laptop3” and client “Laptop1” and “Laptop2” connect over a Layer-2 network to Gig 2/24. So both ports need to be configured as xSec ports.

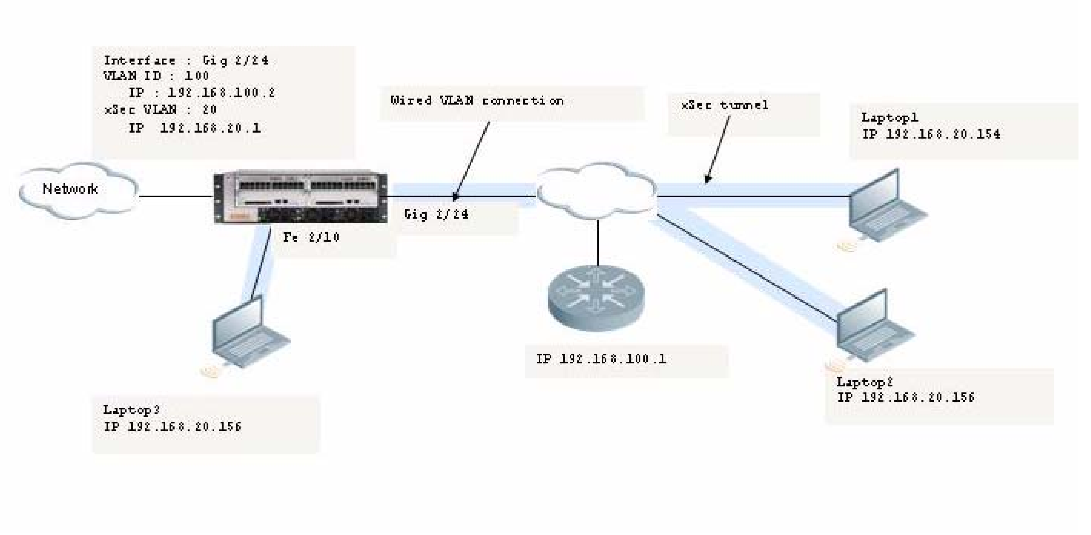
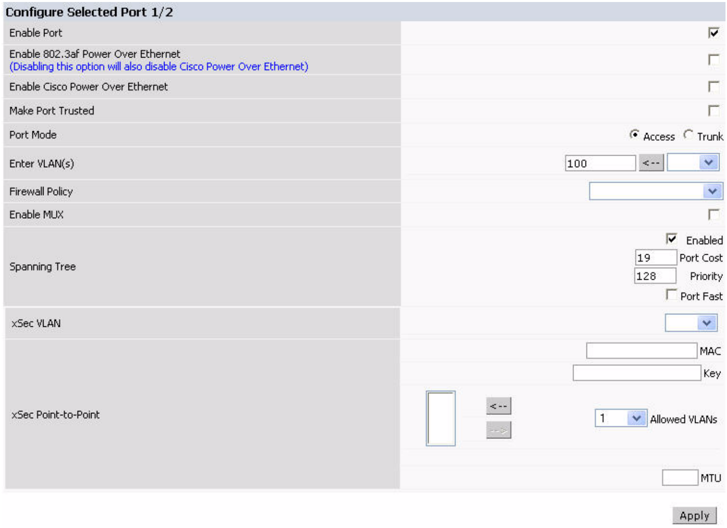


FIGURE 6-3 Configuring Wired Clients for xSec

5. Configure the ports identified in the previous step.

Navigate to the **Configuration > Advanced > Switch > Port** page. Select the port/s that will support xSec clients.



Configure Selected Port 1/2

Enable Port	☑
Enable 802.3af Power Over Ethernet (Disabling this option will also disable Cisco Power Over Ethernet)	□
Enable Cisco Power Over Ethernet	□
Make Port Trusted	□
Port Mode	● Access ○ Trunk
Enter VLAN(s)	100 <--
Firewall Policy	
Enable MUX	□
Spanning Tree	☑ Enabled 19 Port Cost 128 Priority □ Port Fast
xSec VLAN	
xSec Point-to-Point	MAC Key <-- --> 1 Allowed VLANs MTU

Apply

6. Set the native VLAN on the port to ensure Layer-2 connectivity to the network.

7. Set the xSec VLAN to the VLAN configured in Step2. This should be a different VLAN from the native VLAN. In the example above, the native VLAN is VLAN100 and the xSec VLAN is VLAN20

   NOTE: Multiple interfaces can use the same xSec VLAN for the clients connecting via these interfaces. In the above example Gig 2/24 and FE 2/10 can have the same xSec VLAN in which case all 3 laptops will get the addresses from the same subnet. If different xSec VLANs are configured Laptop3 would be on a different subnet than Laptop1 and Laptop2

8. Configure the client.

   The Funk Odyssey Client needs to be installed and set up on the client to support xSec. Refer to "Configuring the Funk Client on Client Machines" on page 93.

Securing WLAN Switch-to-WLAN Switch Communication

xSec can be used to secure communications between two Alcatel WLAN Switches in a WLAN environment. The only requirement is that both WLAN Switches be members of the same VLAN. A point-to-point tunnel is established between the two switches and all control and data traffic between the two switches will be encrypted.

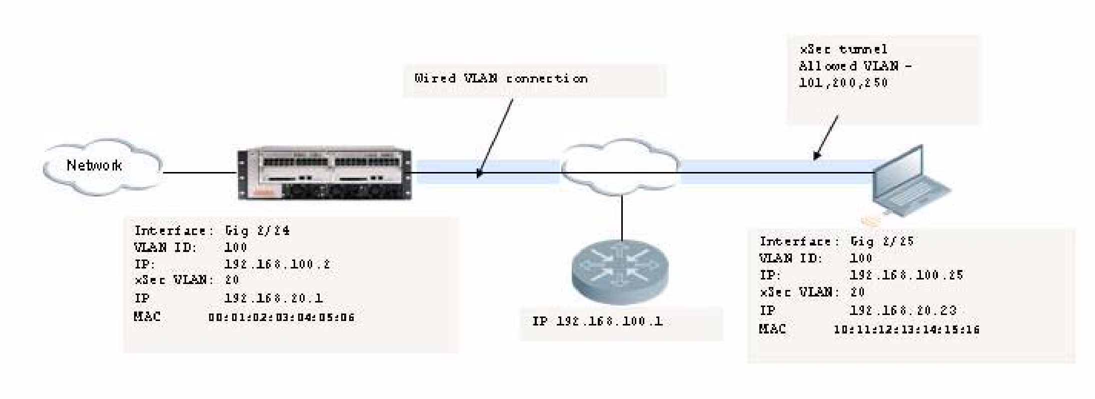


FIGURE 6-4 Configuring xSec for WLAN Switch-to-WLAN Switch Communications

Table 6-2 shows the parameter descriptions and settings used in this example.

TABLE 6-2 Parameter Descriptions and Example Settings

Parameter	Description	WLAN Switch1	WLAN Switch2
Port	The port that is used for the xSec Communication – This can be a FE , gigE port or a port channel	Gig 2/24	Gig 2/25
xSec VLAN	The VLAN that will be used for xSec tunnel termination. This VLAN **should** be different from the ports L2 VLAN settings	VLAN ID 20	VLAN ID 20
xSec Point-to-Point Allowed VLANs	The VLANs that will extend across both the switches via the xSec tunnel	101,200,250	101,200,250
xSec Point-to-Point MAC	MAC address of the tunnel termination points	MAC of WLAN Switch2 11:12:13:14:15:16	MAC of WLAN Switch1 01:02:03:04:05:06
xSec Point-to-Point Key	Shared key used between the two Switches	test123456	test123456

1. Identify the ports that will be used for communication between the two WLAN Switches.

2. Navigate to the **Configuration** > **Advanced** > **General** > **Switch** > **Port** page on WLAN Switch1.

   A. Configure the xSec VLAN setting. Ensure that this VLAN is configured on both WLAN Switches and has an IP address associated with it.

   B. Configure the xSec point-to-point settings.

   C. Configure the MAC address of the tunnel termination point (WLAN Switch2's mac address)

   D. Configure the key used by xSec that will be shared between the two WLAN Switches to establish the tunnel.

   E. Configure the VLANs that would be allowed across the point-to-point connection.

3. Click **Apply** for the configuration changes made to take effect.

4. Repeat steps 1 through 3 on WLAN Switch2 using WLAN Switch1's MAC address in step 2b, and apply the configuration.

Configuring the Funk Client on Client Machines

The Funk Odyssey Clients can be purchased from Funk Software. For information on Funk Software versions, contact Alcatel or Funk Software support.

To install the Odyssey Client:

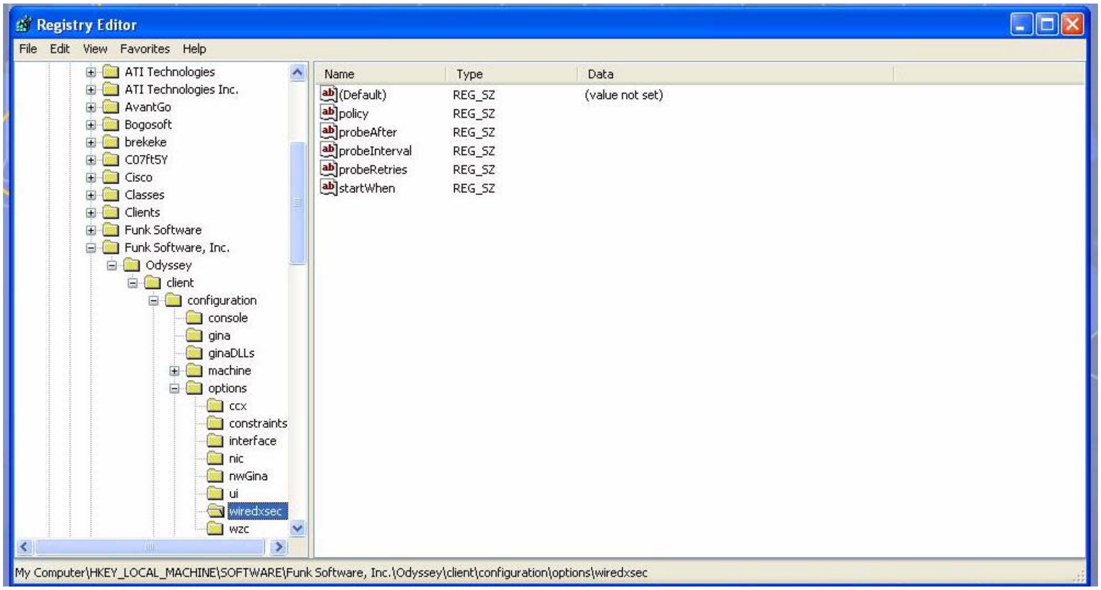
1. Unzip and install the Funk Odyssey client on the client laptop.

2. For wired xSec, to use the Odyssey client to control the wired port, modify the registry:

A. On the windows machine, click **Start** and select **Run**.

B. Type **`regedit`** in the dialog box and click **OK**.

C. Navigate down the tree to `HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\wiredxsec`.



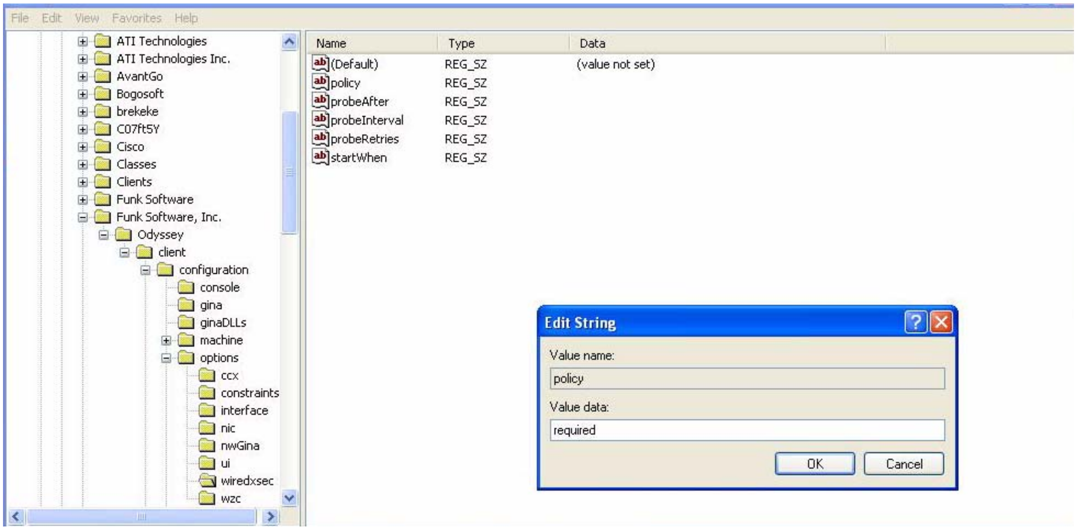
ATI Technologies
ATI Technologies Inc.
AvantGo
Bogosoft
brekeke
C07ft5Y
Cisco
Classes
Clients
Funk Software
Funk Software, Inc.
Odyssey
client
configuration
console
gina
ginaDLLs
machine
options
ccx
constraints
interface
nic
nwGina
ui
wiredxsec
wzc

Name	Type	Data
(Default)	REG_SZ	(value not set)
policy	REG_SZ	
probeAfter	REG_SZ	
probeInterval	REG_SZ	
probeRetries	REG_SZ	
startWhen	REG_SZ	

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\Odyssey\client\configuration\options\wiredxsec

FIGURE 6-5 The regedit Screen

D. Select “policy” from the registry values and right click on it. Select **Modify** to modify the contents of policy. Set the value in the resulting window to `required`.



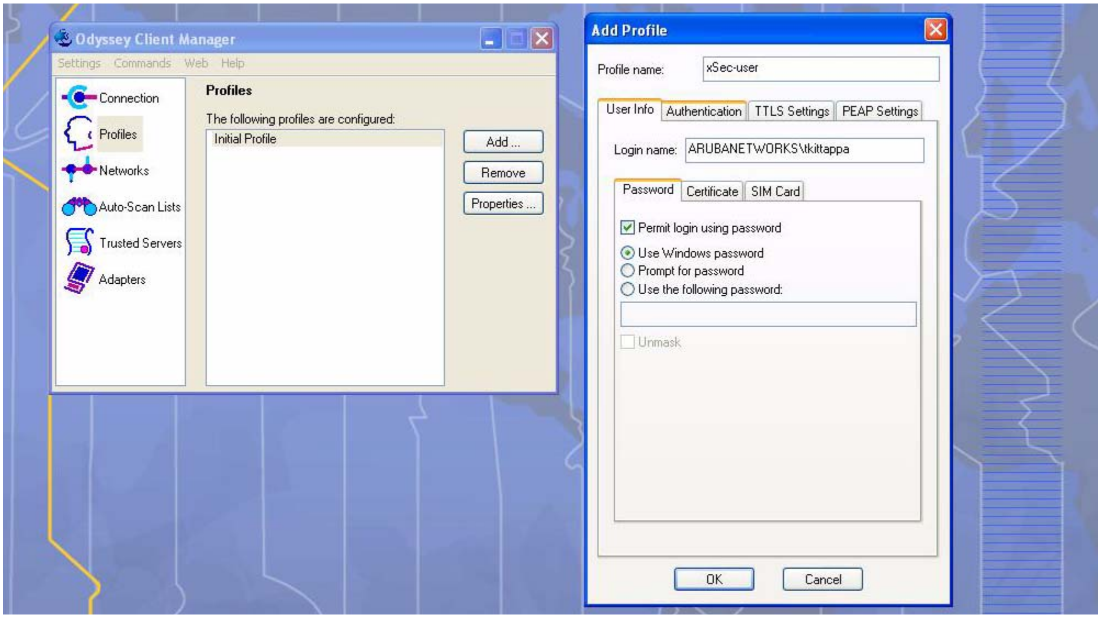
Name	Type	Data
(Default)	REG_SZ	(value not set)
policy	REG_SZ	
probeAfter	REG_SZ	
probeInterval	REG_SZ	
probeRetries	REG_SZ	
startWhen	REG_SZ	

Value name: policy

Value data: required

FIGURE 6-6 Modifying a regedit Policy

3. Open the Funk Odyssey Client. Click the **Profile** tab in the client window. This allows the user to create the user profile for 802.1x authentication.



Profiles

The following profiles are configured:

Initial Profile

Profile name: xSec-user

Login name: ARUBANETWORKS\tkittappa

☑ Permit login using password

● Use Windows password

○ Prompt for password

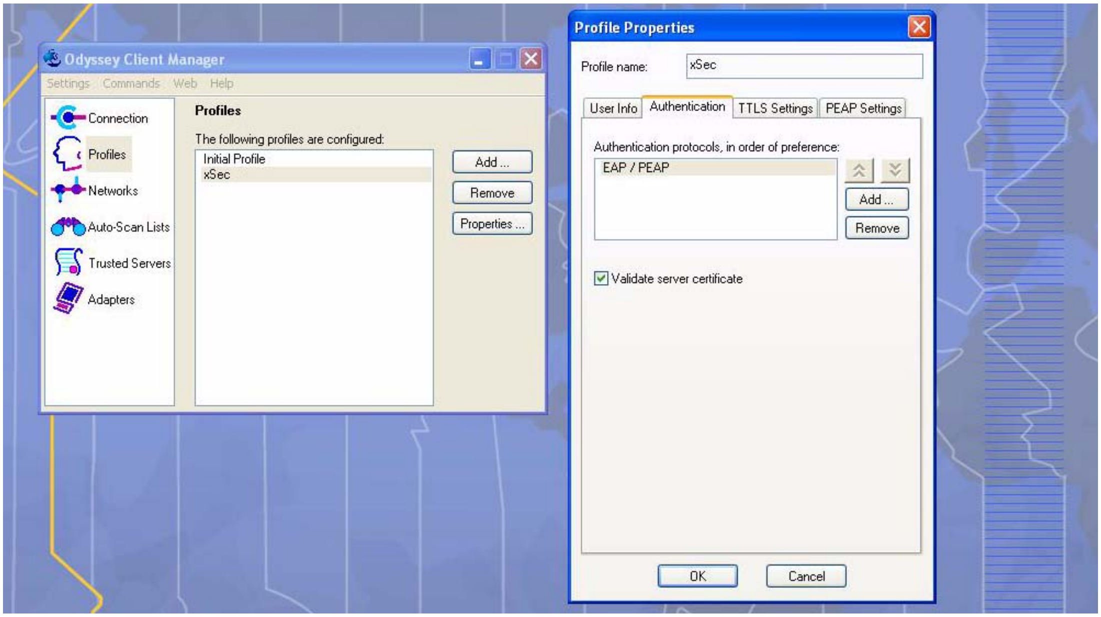
○ Use the following password:

□ Unmask

FIGURE 6-7 The Funk Odyssey Client Profile

A. In the login name dialog box, enter the login name used for 802.1x authentication. For the password, the client could use the WINDOWS password or use the configured password based on the selection made.

B. Click the certificate tab and enter the certificate information required. This example shows the PEAP settings.



Profiles

The following profiles are configured:

Initial Profile
xSec

Profile name: xSec

Authentication protocols, in order of preference:

EAP / PEAP

☑ Validate server certificate

FIGURE 6-8 Certificate Information

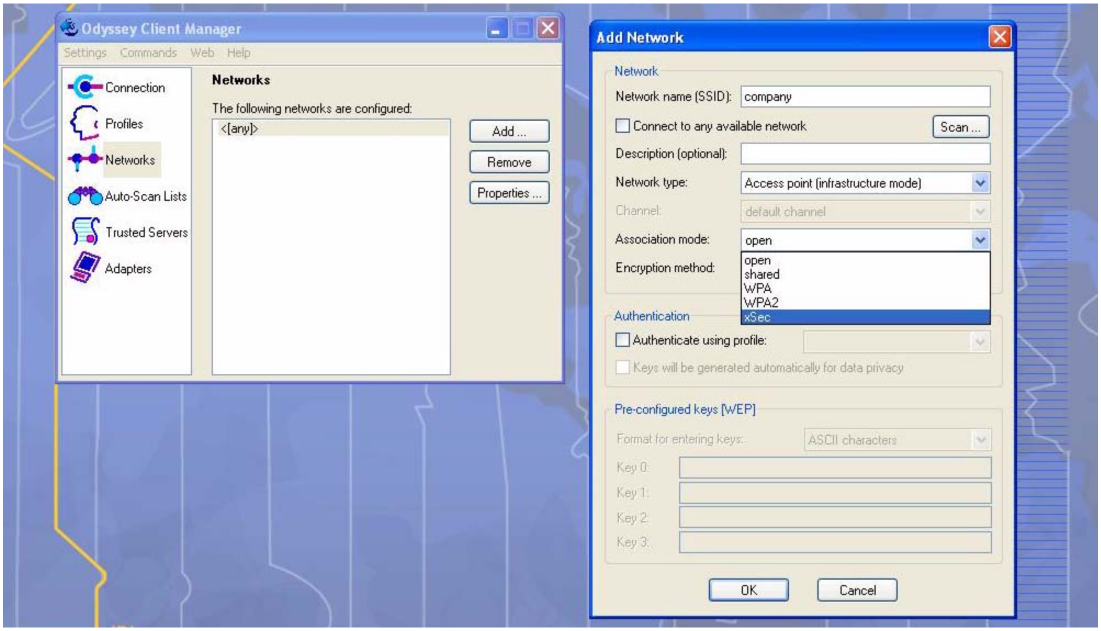
C. Click the **Authentication** tab. In the resultant window, click the **Add** tab and select **EAP/PEAP**. Move this option to the top of the list if PEAP is the method chosen. If certification validation not required, uncheck the **Validate server certificates** setting.

D. Click the **PEAP Settings** tab and select the EAP protocol supported.

E. Click **OK**.

F. To modify an existing profile, select the profile and then click the **Properties** tab.

4. Select the **Network** tab to configure the network for wireless client. For wired clients, skip this step.



Networks

The following networks are configured:

<[any]>

Network

Network name (SSID): company

□ Connect to any available network

Description (optional):

Network type: Access point (infrastructure mode)

Channel: default channel

Association mode: open

open
shared
WPA
WPA2
xSec

Encryption method:

Authentication

□ Authenticate using profile:

□ Keys will be generated automatically for data privacy

Pre-configured keys (WEP)

Format for entering keys: ASCII characters

Key 0:

Key 1:

Key 2:

Key 3:

FIGURE 6-9 Network Profile

A. Click the **Add** tab. Enter the SSID to which the client connects.

B. Set the Network type to **Infrastructure**.

C. Set the Association mode to **xSec**, AES encryption is automatically selected.

D. Under Authentication, select the **Authenticate using profile** checkbox.

E. From the pull down menu, select the profile used for 802.1x authentication. This would be one of the profiles configured in step 2.

F. Select the keys that will be generated automatically for data privacy.

G. Apply the configuration changes made by clicking on the **OK** tab.

H. To modify an existing profile, select the profile and then click the **Properties** tab.

5. Click the **Adapters** tab if the adapter used is not seen under the list of adapters pull down menu under connections.

A. When using a wireless client, click the **Wireless** tab.

B. Select the **Wireless adapters only** radio button. From the resulting list, select the adapter required from the list and click **OK**.

C. For wired 802.1x clients, select the **Wired 802.1x** tab and select the **Wired adapters only** radio button. From the resulting list, select the adapter required from the list and click **OK**.

6. Establish the connection.

   A. Click the **Connection** tab.

   B. From the pull down menu, select the adapter required. If the adapter in use is not visible, add the adapter as explained in Step 5.

   C. Select the **Connect to network** checkbox and select the **Network** option from the pull down menu. To configure a new network, follow the instructions in Step 4.

   D. This will automatically start the connection process. To reconnect to the network, click **Reconnect**.

7. Click **Scan** to display the SSIDs seen by the NIC after a site survey.

Configuring MAC-Based Authentication 7

This chapter describes how to configure MAC-based authentication on the Alcatel WLAN 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 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 prevent other devices from accessing the voice network using what is normally an insecure SSID.

This chapter describes the following topics:

- "Configuring the Mobility Controller" on page 99
- "Configuring Users" on page 101

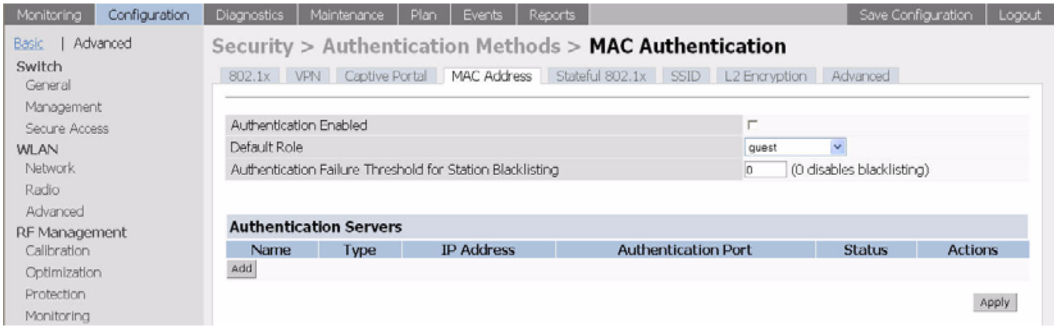
Configuring the WLAN Switch

To enable MAC-based authentication on the Alcatel WLAN Switch:

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

   - **The role** that will be assigned as the default role for the MAC-based authenticated users. (See Chapter 1, "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 WLAN 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 101 for information on configuring the users on the local database. For information on configuring AAA servers, see Chapter 2, "Configuring AAA Servers."

2. Navigate to the **Configuration > Advanced > Security > Authentication Methods > MAC Address** page.



Security > Authentication Methods > **MAC Authentication**

Authentication Enabled	☐
Default Role	guest
Authentication Failure Threshold for Station Blacklisting	0 (0 disables blacklisting)

Authentication Servers

Name	Type	IP Address	Authentication Port	Status	Actions

- **Check the Authentication Enabled** checkbox to enable authentication.
- 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.

Parameters	**Description**
Authentication Enabled	Select this option to enable MAC-based authentication. Default: Unchecked
Default Role	Select a configured 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.
Authentication Failure Threshold for Station Blacklisting	This field specifies the number of times a user can try to login with wrong credentials after which the user will be blacklisted as a security threat. Enter 0 to disable blacklisting, otherwise enter a non-zero integer to have the user blacklisted after the specified number of failures. Default : 3

3. Configure the authentication servers.

- This is the authentication server to which the WLAN 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 WLAN 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 ▲ or ▼ arrows to the right of the entry to move it higher up or lower down in the list.

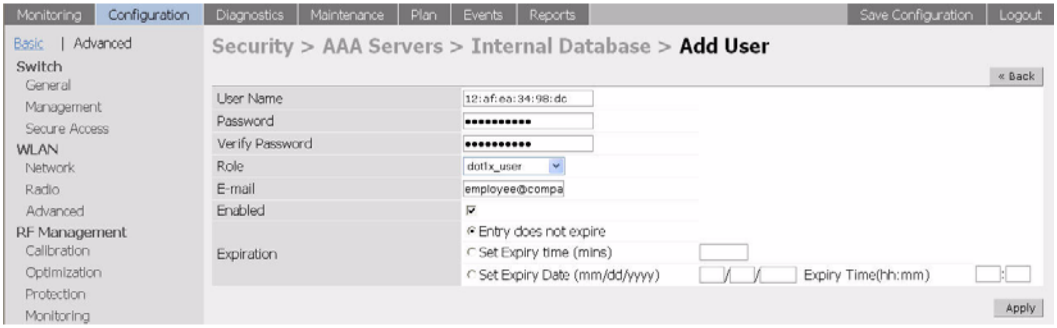
4. Click **Apply** to apply the changes made. Verify that the changes made have taken effect on the resultant page.

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. Navigate to the **Configuration > Advanced > Security > AAA Servers > Internal Database** page.
   - Under the **Users** section click **Add User**. This opens the **Add User** page.



Security > AAA Servers > Internal Database > Add User

User Name	12:af:ea:34:98:dc
Password	●●●●●●●●●●●
Verify Password	●●●●●●●●●●●
Role	dot1x_user
E-mail	employee@compa
Enabled	☑
Expiration	● Entry does not expire ○ Set Expiry time (mins) □ ○ Set Expiry Date (mm/dd/yyyy) □/□/□ Expiry Time(hh:mm) □:□

- 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:xx** format. (If you are using an external RADIUS server, the username/password format is: xxxxxxxx.)
- 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 Servers > 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.

Windows Client Example Configuration for 802.1x

A

This appendix provides an example configuration for a wireless client (the 802.1x supplicant) in a Windows environment.

For detailed information about configuring computers in a Windows environment for PEAP-MS-CHAPv2 and EAP-TLS authentication, see the Microsoft document *Step-by-Step Guide for Setting Up Secure Wireless Access in a Test Lab*, available from Microsoft's Download Center (at www.microsoft.com/downloads).

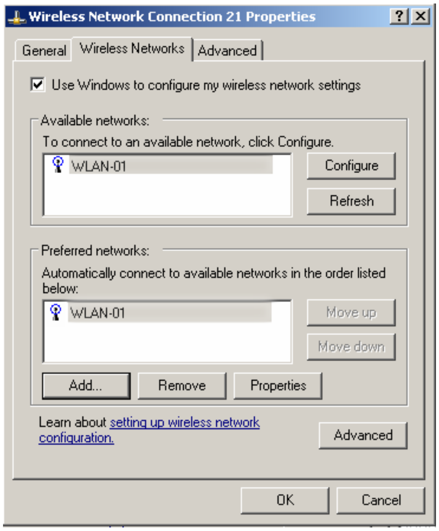
Window XP Wireless Client Example Configuration

This section shows an example of how to configure a Windows XP wireless client using Windows XP's Wireless Zero Configuration service.

NOTE: The following steps apply to a computer running Windows XP Professional Version 2002 with Service Pack 2. To configure a wireless client on other Windows platforms, see your Microsoft Windows documentation.

1. On the desktop, right-click My Network Places and select Properties.
2. In the Network Connections window, right-click on Wireless Network Connection and select Properties.
3. Select the Wireless Networks tab.

This screen displays the available wireless networks and the list of preferred networks. Windows connects to the preferred networks in the order in which they appear in the list.



☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

WLAN-01

Preferred networks:

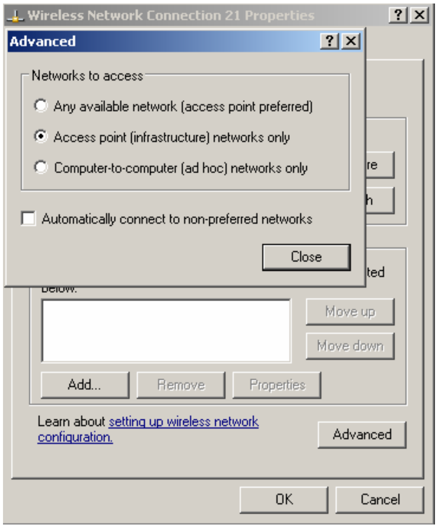
Automatically connect to available networks in the order listed below:

WLAN-01

Learn about setting up wireless network configuration.

FIGURE A-1 Wireless Networks

4. Click the Advanced button to display the Networks to access window.



Networks to access

○ Any available network (access point preferred)

● Access point (infrastructure) networks only

○ Computer-to-computer (ad hoc) networks only

□ Automatically connect to non-preferred networks

Learn about setting up wireless network configuration.

FIGURE A-2 Networks to Access

This window determines what types of wireless networks the client can access. By default, Windows connects to any type of wireless network.

Make sure that the option Computer-to-computer (ad hoc) networks only is *not* selected. Click Close.

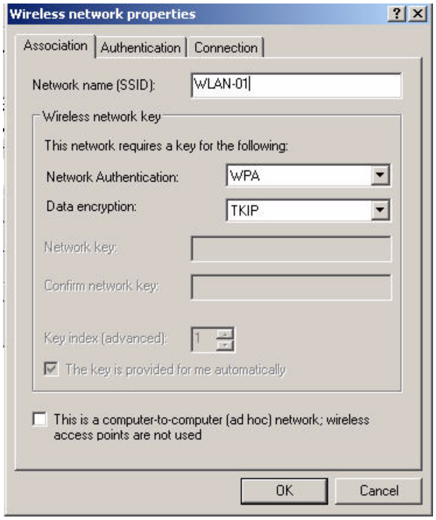
5. In the Wireless Networks tab, click Add to add a wireless network.
6. Click the Association tab to enter the network properties for the ESSID.

NOTE: This tab configures the authentication and encryption used between the wireless client and the Alcatel OmniAccess system. Therefore, the settings for the ESSID that you configure on the client must *match* the configuration for the ESSID on the WLAN Switch.

- For an SSID using dynamic WEP, enter the following:
  - Network Authentication: Open
  - Data Encryption: WEP
  - Select the option “The key is provided for me automatically”. Each client will use a dynamically-generated WEP key that is automatically derived during the 802.1x process.
- For an SSID using WPA, enter the following:
  - Network Authentication: WPA
  - Data Encryption: TKIP
- For an SSID using WPA-PSK, enter the following:
  - Network Authentication: WPA-PSK
  - Data Encryption: TKIP
  - Enter the preshared key.
- For an SSID using WPA2, enter the following:
  - Network Authentication: WPA2
  - Data Encryption: AES
- For an SSID using WPA2-PSK, enter the following:
  - Network Authentication: WPA2-PSK
  - Data Encryption: AES
  - Enter the preshared key

NOTE: Do *not* select the option “This is a computer-to-computer (ad hoc) network; wireless access points are not used”.

Figure A-3 shows the configuration for the ESSID WLAN-01 which uses dynamic WEP.



Network name (SSID): WLAN-01

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key:

Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

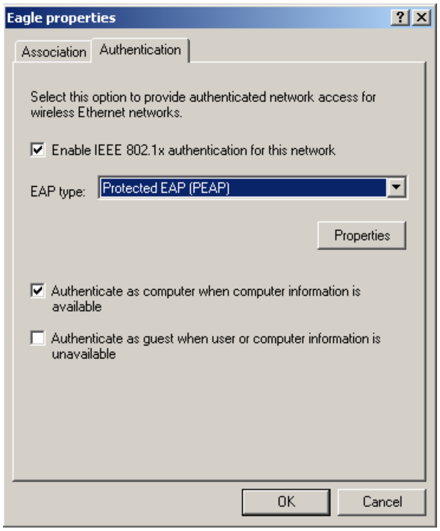
FIGURE A-3 Wireless Network Association

7. Click the Authentication tab to enter the 802.1x authentication parameters for the ESSID.

NOTE: This tab configures the EAP type used between the wireless client and the authentication server.

Configure the following, as shown in Figure A-4:

- Select Enable IEEE 802.1x authentication for this network.
- Select Protected EAP (PEAP) for the EAP type.
- Select Authenticate as computer when computer information is available. The client will perform computer authentication when a user is not logged in.
- Do not select Authenticate as guest when user or computer information is unavailable. The client will not attempt to authenticate as a guest.



Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

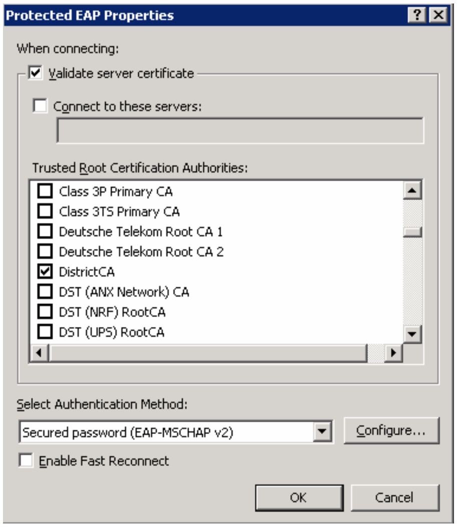
☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

FIGURE A-4 Wireless Network Authentication

8. Under EAP type, select Properties to display the Protected EAP Properties window. Configure the client PEAP properties, as shown in Figure A-5:

   - Select Validate server certificate. This instructs the client to check the validity of the server certificate from an expiration, identity, and trust perspective.
   - Select the trusted Certification Authority (CA) that can issue server certificates for the network.
   - Select Secured password (EAP-MSCHAP v2) — the PEAP “inner authentication” mechanism will be an MS-CHAPv2 password.
   - Select Enable Fast Reconnect to speed up authentication in some cases.



Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ Class 3P Primary CA
□ Class 3TS Primary CA
□ Deutsche Telekom Root CA 1
□ Deutsche Telekom Root CA 2
☑ DistrictCA
□ DST (ANX Network) CA
□ DST (NRF) RootCA
□ DST (UPS) RootCA

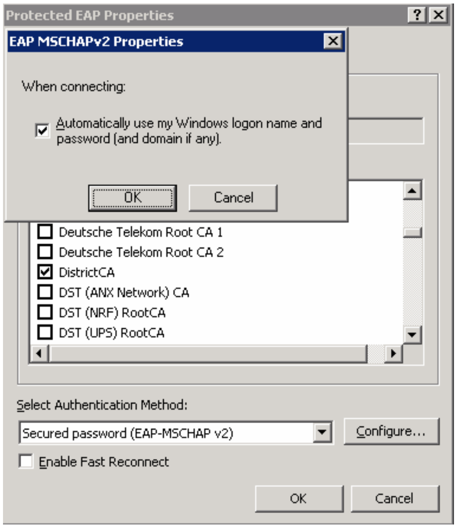
Select Authentication Method:

Secured password (EAP-MSCHAP v2)

□ Enable Fast Reconnect

FIGURE A-5 Protected EAP Properties

9. Under Select Authentication Method, click Configure to display the EAP-MSCHAPv2 Properties window. Select the option Automatically use my Windows logon name and password (and domain if any). This option specifies that the user's Windows logon information is used for authentication to the wireless network. This option enables single sign-on, allowing the same logon to be used for access to the Windows domain as well as the wireless network.



Protected EAP Properties

EAP MSCHAPv2 Properties

When connecting:

☑ Automatically use my Windows logon name and password (and domain if any).

□ Deutsche Telekom Root CA 1
□ Deutsche Telekom Root CA 2
☑ DistrictCA
□ DST (ANX Network) CA
□ DST (NRF) RootCA
□ DST (UPS) RootCA

Select Authentication Method: Secured password (EAP-MSCHAP v2)

□ Enable Fast Reconnect

FIGURE A-6 EAP MSCHAPv2 Properties

Internal Captive Portal B

You can customize the default captive portal page through the WebUI, as described in Chapter 4, “Configuring the Captive Portal.” This appendix discusses creating and installing a new internal captive portal page and other customizations.

Creating a New Internal Web Page

You can also create your own web page to display.

A custom web page must include an authentication form to authenticate a user.

The authentication form can include any of the following variables:

user	(Required)
password	(Required)
FQDN	The fully-qualified domain name (this is dependent on the setting of the WLAN Switch and is supported only in Global Catalog Servers software

The form can use either the "get" or the "post" methods, but the "post" method is recommended. The form's action must absolutely or relatively reference "https://<switch_IP>/auth/index.html/u".

You can construct an authentication form using the following HTML:

```
<FORM method="post" ACTION="/auth/index.html/u">
...
</FORM>
```

A recommended option for the <FORM> element is:

`autocomplete="off"` - this tells Internet Explorer. not to cache form inputs

The form variables can be input using any form control method available such as INPUT, SELECT, TEXTAREA and BUTTON. Example HTML code follows.

Username:

Minimal:

```
    <INPUT type="text" name="user">
```

Recommended Options:

```
    accesskey="u"    Sets the keyboard shortcut to 'u'
    SIZE="25         "Sets the size of the input box to 25
    VALUE=           ""Ensures no default value
```

Password:

Minimal:

```
    <INPUT type="password" name="password">
```

Recommended Options:

```
    accesskey="p"    Sets the keyboard shortcut to 'p'
    SIZE="25         "Sets the size of the input box to 25
    VALUE=           ""Ensures no default value
```

FQDN:

Minimal:

```
<SELECT name=fqdn>
    <OPTION value="fqdn1" SELECTED>
    <OPTION value="fqdn2">
</SELECT>
```

Recommended Options:

None.

Finally, an HTML also requires an input button:

```
<INPUT type="submit">
```

Basic HTML Example

```
<HTML>
  <HEAD>
  </HEAD>
  <BODY>
    <FORM method="post" autocomplete="off" ACTION="/auth/index.html/u">

    Username:<BR>
    <INPUT type="text" name="user" accesskey="u" SIZE="25" VALUE="">
    <BR>

    Password:<BR>
    <INPUT type="password" name="password" accesskey="p" SIZE="25"
        VALUE="">
    <BR>
    <INPUT type="submit">
    </FORM>
  </BODY>
</HTML>
```

You can find a more advanced example simply by using your browser’s "view-source" function while viewing the default captive portal page.

Installing a New Captive Portal Page

You can install the captive portal page by using the Maintenance function of the WebUI.

Log into the WebUI and navigate to Maintenance > Captive Portal > Upload Custom Login Pages.

This page lets you upload your own files to the WLAN Switch. There are three page types that you can choose:

- Captive Portal Login (top level): This type uploads the file into the WLAN Switch and instantly sets the captive portal page to reference the file that you are uploading. Use with caution on a production WLAN Switch as this takes effect immediately.
- Content: The content page type allows you to upload all miscellaneous files that you need to reference from your main captive portal login page. This can be used for images, CSS files, scripts or any other file that you need to reference. These files are uploaded into the same directory as the top level captive portal page and thus all files can be referenced relatively.
- Sygate Remediation Failure: This is used as part of the Alcatel Client Integrity Module and is outside the scope of this appendix.

All uploaded files can also be referenced from your top-level captive portal page using any of the following:

```
https://<switch_IP>/upload/<file>
/upload/<file>
<file>
```

Displaying Authentication Error Message

This section contains a script that performs the following tasks:

- When the user is redirected to the main captive portal login when there is authentication failure, the redirect URL includes a query parameter "errmsg" which java script can extract and display.

- Store the originally requested URL in a cookie so that once the user has authenticated, they are automatically redirected to its original page. Note that for this feature to work, you need AOS-W release 2.4.2.0 or later. If you don't want this feature, delete the part of the script shown in red.

```
<script>
{

function createCookie(name,value,days)
{
            if (days)
            {
                        var date = new Date();
                        date.setTime(date.getTime()+(days*24*60*60*1000));
                        var expires = "; expires="+date.toGMTString();
            }
            else var expires = "";
            document.cookie = name+"="+value+expires+"; path=/";
}

  var q = window.location.search;
  var errmsg = null;


  if (q && q.length > 1) {
    q = q.substring(1).split(/[=&]/);
    for (var i = 0; i < q.length - 1; i += 2) {
      if (q[i] == "errmsg") {
        errmsg = unescape(q[i + 1]);
          break;
      }
       if (q[i] == "host") {
          createCookie('url',q[i+1],0)
        }

    }
  }

  if (errmsg && errmsg.length > 0) {
    errmsg = "<div id='errorbox'>\n" + errmsg + "\n</div>\n";
    document.write(errmsg);
  }
}
</script>
```

Reverting to the Default Captive Portal

You can reassign the default captive portal site using the "Revert to factory default settings" check box in the "Upload Custom Login Pages" section of the Maintenance tab in the WebUI.

Language Customization

The ability to customize the internal captive portal provides you with a very flexible interface to the Alcatel captive portal system. However, other than posting site-specific messages onto the captive portal website, the most common type of customization is likely to be language localization. This section describes a simple method for creating a native language captive portal implementation using the Alcatel internal captive portal system.

1. Customize the configurable parts of the captive portal settings to your liking. To do this, navigate to the Maintenance > Customize Captive Portal in the WebUI:

   For example, choose a page design, upload a custom logo and/or a custom background. Also include any page text and acceptable use policy that you would like to include. Put this in your target language or else you will need to translate this at a later time.

   Also ensure that Guest login is enabled or disabled as you prefer. Navigate to Configuration > Authentication Methods > Captive Portal and select or deselect "Enable Guest Login".

2. Click **Submit** and then click on **View Captive Portal**. Check that your customization and text/html is correct, with the default interface still in English and the character set still autodetects to ISO-8859-1.

   Repeat steps 1 and 2 until you are satisfied with your page.

3. Once you have a page you find acceptable, click on **View Captive Portal** one more time to display your login page. From your browser, choose "View->Source" or its equivalent. Your system will display the HTML source for the captive portal page. Save this source as a file on your local system.

4. Open the file that you saved in step 3 above using a standard text editor.to make the following changes:

   A. Fix the character set. The default <HEAD>...</HEAD> section of the file will look similar to the following:

```
<head>
<title>Portal Login</title>
```

```
<link href="default1/styles.css" rel="stylesheet" media="screen"
type="text/css" />
<script language="javascript" type="text/javascript">
    function showPolicy() {
        win = window.open("/auth/acceptableusepolicy.html", "policy",
"height=550,width=550,scrollbars=1");
    }
</script>
</head>
```

In order to control the character set that the browser will use to show the text with, you will need to insert the following line inside the <HEAD>...</HEAD> element:

```
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS"/>
```

Replace the "Shift_JIS" part of the above line with the character set that is used by your system. In theory, any character encoding that has been registered with IANA can be used, but you must ensure that any text you enter uses this character set and that your target browsers support the required character set encoding.

The final <HEAD>...</HEAD> portion of the document should look similar to this:

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS"/>
<title>Portal Login</title>

<link href="default1/styles.css" rel="stylesheet" media="screen"
type="text/css" />
<script language="javascript" type="text/javascript">
    function showPolicy() {
        win = window.open("/auth/acceptableusepolicy.html", "policy",
"height=550,width=550,scrollbars=1");
    }
</script>
</head>
```

B. Fix references: If you have used the built-in preferences, you will need to update the reference for the logo image and the CSS style sheet.

To update the CSS reference, search the text for "<link href" and update the reference to include "/auth/" in front of the reference. The original link should look similar to the following:

```
<link href="default1/styles.css" rel="stylesheet" media="screen"
type="text/css" />
```

This should be replaced with a link like the following:

```
<link href="/auth/default1/styles.css" rel="stylesheet" media="screen"
type="text/css" />
```

The easiest way to update the image reference is to search for "src" using your text editor and updating the reference to include "/auth/" in front of the image file. The original link should look similar to the following:

```
<img src="default1/logo.gif"/>
```

This should be replaced with a link like this:

```
<img src="/auth/default1/logo.gif"/>
```

C. Insert javascript to handle error cases:

When the WLAN Switch detects an error situation, it will pass the user's page a variable called "errmsg" with a value of what the error is in English. Currently, only "Authentication Failed" is supported as a valid error message.

To localize the authentication failure message, replace the following text (it is just a few lines below the <body> tag):

```
<div id="errorbox" style="display: none;">
</div>
```

with the script below.

You will need to translate the "Authentication Failed" error message into your local language and add it into the script below where it states: localized_msg="...":

```
<script>
```

```
{
  var q = window.location.search;
  var errmsg = null;
  if (q && q.length > 1) {
    q = q.substring(1).split(/[=&]/);
    for (var i = 0; i < q.length - 1; i += 2) {
      if (q[i] == "errmsg") {
        errmsg = unescape(q[i + 1]);
        break;
      }
    }
  }

  if (errmsg && errmsg.length > 0) {
    switch(errmsg) {
    case "Authentication Failed":
    localized_msg="Authentication Failed";
    break;
    default:
      localised_msg=errmsg;
      break;
    }
    errmsg = "<div id='errorbox'>\n" + localised_msg + "\n</div>\n";
    document.write(errmsg);
  };
}
</script>
```

D. Translate the web page text. Once you have made the changes as above, you only need to translate the rest of the text that appears on the page. The exact text that appears will depend on the WLAN Switch settings when you originally viewed the captive portal. You will need to translate all relevant text such as "REGISTERED USER", "USERNAME", "PASSWORD", the value="" part of the INPUT type="submit" button and all other text. Ensure that the character set you use to translate into is the same as you have selected in part i) above.

Feel free to edit the HTML as you go if you are familiar with HTML.

5. After saving the changes made in step 4 above, upload the file to the WLAN Switch using the Maintenance > Upload Custom Login Pages section of the WebUI. Choose "Captive Portal Login (top level)" and browse your local computer for the file you saved above.

Ensure that the "Revert to factory default settings" box is NOT checked and click Apply. This will upload the file to the WLAN Switch and set the captive portal system to use this page as the redirection page.

In order to check that your site is operating correctly, go back to the "Customize Login Page" and click on "View Captive Portal" button to view the page you have uploaded. Check that your browser has automatically detected the character set and that your text is not garbled.

To make any adjustments to your page, edit your file locally and simply re-upload to the WLAN Switch in order to view the page again.

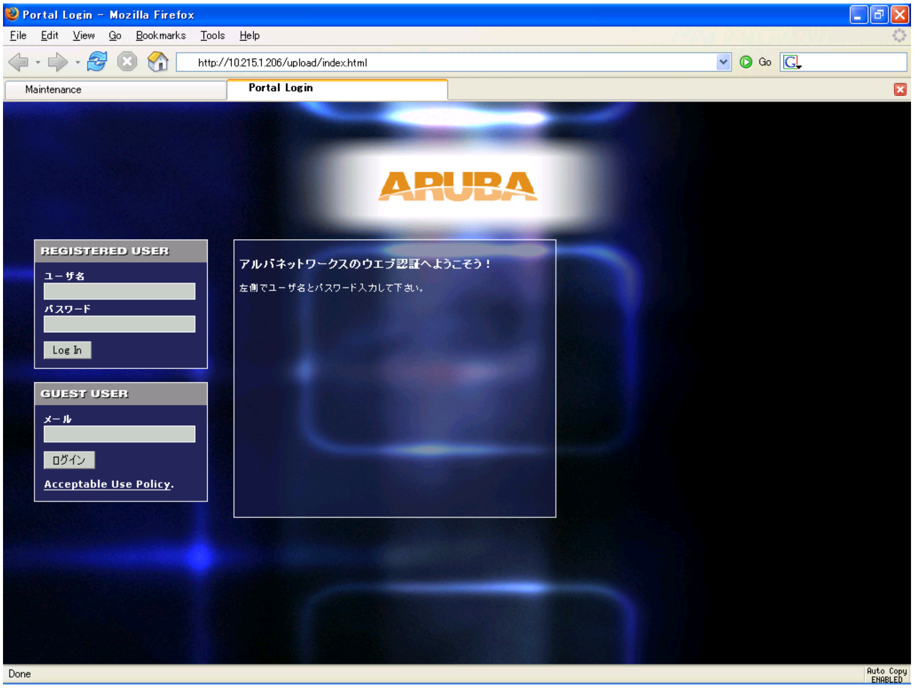
6. Finally, it is possible to customize the welcome page on the WLAN Switch, however for language localization it is recommended to use an "external welcome page" instead. This can be a web site on an external server, or it can be a static page that is uploaded to a WLAN Switch.

You set the welcome page using the CLI command "aaa captive-portal welcome-page <URL>". This is the page that the user will be redirected to after a success authentication.

If this is required to be a page on the WLAN Switch, the user needs to create their own web page (using the charset meta attribute in step 4i above) and upload this page to the designated WLAN Switch in the same manner as uploading the captive portal page, except using "content" as opposed to "Captive Portal Login" under "Maintenance > Captive Portal > Upload Login Pages". Any required CSS, Client side Script files and media files can also be uploaded using content, however file space is limited (check using "show memory" under "flash free" and remember to leave ample room for system files).

NOTE: - The "Registered User" and "Guest User" sections of the login page are implemented as graphics files, referenced by the default CSS styles. In order to change these, you will need to create new graphic files, download the CSS file, edit the reference to the graphics files, change the style reference in your index file and then upload all files as "content" to the WLAN Switch.

A sample of a translated page is show below.

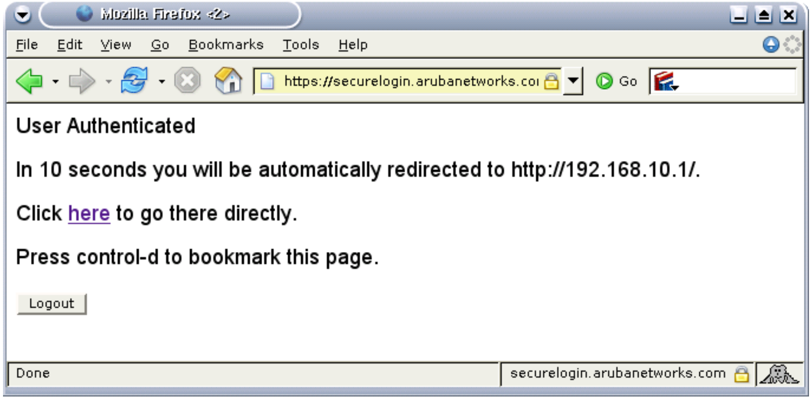


アルバネットワークスのウエブ認証へようこそう！

左側でユーザ名とパスワード入力して下さい。

Customizing the Welcome Page

Once a user has authenticated to the WLAN Switch, they are presented with the Welcome page. The default welcome page will depend slightly on your configuration, but will look similar to this:



Mozilla Firefox <2>
File Edit View Go Bookmarks Tools Help
https://securelogin.arubanetworks.coı
Go

User Authenticated

In 10 seconds you will be automatically redirected to http://192.168.10.1/.

Click here to go there directly.

Press control-d to bookmark this page.

Logout
Done
securelogin.arubanetworks.com

You can customize this welcome page by building your own HTML page and uploading it to the WLAN Switch. You upload it to the WLAN Switch using the GUI under Maintenance > Captive Portal > Upload custom pages and choose "content as the page type. This file is stored in a directory called "/upload/" in the WLAN Switch in the file's original name.

In order to actually use this file, you will need to configure the welcome page on the WLAN Switch. To do this use the CLI command: "aaa captive-portal welcome-page /upload/welc.html" where "welc.html" is the name of the file that you uploaded, or you can change this via the GUI under Configuration->Authentication Methods->Captive-Portal->Welcome Page Login

A simple example that will create the same page as above is shown below:

```
<html>
<head>
<script>
{


function readCookie(name)
{
            var nameEQ = name + "=";
            var ca = document.cookie.split(';');
            for(var i=0;i < ca.length;i++)
            {
                        var c = ca[i];
                        while (c.charAt(0)==' ') c =
c.substring(1,c.length);
                        if (c.indexOf(nameEQ) == 0) return
c.substring(nameEQ.length,c.length);
            }
            return null;
}




var cookieval = readCookie('url');
            if (cookieval.length>0) document.write("<meta
http-equiv=\"refresh\" content=\"2;url=http://"+cookieval+"\""+">");


            }
</script>
```

```
</head>
<body bgcolor=white text=000000>
<font face="Verdana, Arial, Helvetica, sans-serif" size=+1>
  <b>User Authenticated </b>

<p>In 2 seconds you will be automatically redirected to your original web
page</p>
<p> Press control-d to bookmark this page.</p>

<FORM ACTION="/auth/logout.html">
       <INPUT type="submit" name="logout" value="Logout">
</FORM>
</font>
</body>
</html>
```

NOTE: If you customize the Welcome Page, then you must also customize the Pop-Up box if you want to have one.

The part in red will redirect the user to the web page they originally requested. For this to work, please follow the procedure described above in this document.

Customizing the Pop-Up box

In order to customize the Pop-Up box, you must first customize your Welcome page. Once you have customized your welcome page, then you can configure your custom page to make a pop-up box so as to enable your users to log themselves out.

The first step is to generate the HTML that will be displayed within the pop-up box. The default HTML is as shown:

```
<html>
<body bgcolor=white text=000000>
<font face="Verdana, Arial, Helvetica, sans-serif" size=+1>
 <b>Logout</b></font>
 <p>
  <a href="/auth/logout.html"> Click to Logout </a>
</body>
</html>
```

If you wish your users to be able to logout using this pop-up box, then you must include a reference to /auth/logout.html Once a user accesses this URL then the WLAN Switch will log them out. It is easiest to simply edit the above HTML to suit your users and then upload the resulting file to the WLAN Switch using the GUI under Maintenance > Captive Portal > Upload custom pages and choose "content" as the page type.

Once you have completed your HTML, then you must get the clients to create the pop-up box once they have logged into the WLAN Switch. This is done by inserting the following code into your welcome page text and re-uploading the welcome page text to your WLAN Switch.

Common things to change:

- URL: set the URL to be the name of the pop-up HTML file that you created and uploaded. This should be preceded by "/upload/"
- Width: set w to be the required width of the pop-up box
- Height: set h to be the required height of the pop-up box
- Title: set the second parameter in the window.open command to be the title of the pop-up box. Be sure to include quotes

```
<script language="JavaScript">
 var url="/upload/popup.html";
 var w=210;
 var h=80;
 var x=window.screen.width - w - 20;
 var y=window.screen.height - h - 60;
 window.open(url, 'logout',
"toolbar=no,location=no,width="+w+",height="+h+",top="+y+",left="+x+",scree
nX="+x+",screenY="+y);
</script>
```

This will let you customize your pop-up window.

Customizing the Logged Out box

In order to customize the Logged Out box, you must first customize your Welcome page and also your Pop-Up box. To customize the message that occurs after you have logged out then you need to replace the URL that the pop-up box will access in order to log out with your own HTML file.

Firstly you must write the HTML web page that will actually log out the user and will also display page that you wish. An example page is shown below. The key part that must be included is the <iframe>..</iframe> section. This is the part of the HTML that actually does the user logging out. The logout is always performed by the client accessing the /auth/logout.html file on the WLAN Switch and so it is hidden in the html page here in order to get the client to access this page and for the WLAN Switch to update its authentication status. If a client does not support the iframe tag, then the text between the <iframe> and the </iframe> is used. This is simply a 0 pixel sized image file that references /auth/logout.html. Either method should allow the client to logout from the WLAN Switch.

Everything else can be customized.

```
<html>
<body bgcolor=white text=000000>

<iframe src='/auth/logout.html' width=0 height=0 frameborder=0><img
src=/auth/logout.html width=0 height=0></iframe>

<P><font face="Verdana, Arial, Helvetica, sans-serif" size=+1>
You have now logged out.</font></P>

<form> <input type="button" onclick="window.close()" name="close"
value="Close Window"></form>

</body>
</html>
```

After writing your own HTML, then you need to ensure that your customized pop-up box will access your new logged out file. In the pop-up box example above, you simply replace the "/auth/logout.html" with your own file that you upload to the WLAN Switch. For example, if your customized logout HTML is stored in a file called "loggedout.html" then your "pop-up.html" file should reference it like this:

```
<html>
<body bgcolor=white text=000000>
<font face="Verdana, Arial, Helvetica, sans-serif" size=+1>
 <b>Logout</b></font>
 <p>
  <a href="/upload/loggedout.html"> Click to Logout </a>
</body>
</html>
```

Volume 5

Configuring Multiple WLAN Switch Environments

AOS-W User Guide

Release 2.5.3

ALCATEL

Copyright

Specifications in this manual are subject to change without notice.

Originated in the USA.

Trademarks

AOS-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 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

This preface includes the following information:

- An overview of the contents of 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

The *AOS-W User Guide* is now in eight separate volumes for easier download and information access. The volumes are as follows:

- Volume 1 contains an overview of the OmniAccess System.
- Volume 2 describes how to install the OmniAccess System in a wired network.
- Volume 3 describes WLAN configuration, including remote Access Points.
- Volume 4 describes wireless encryption and authentication configuration.
- Volume 5 (this volume) describes configuring multi-WLAN switch environments.
- Volume 6 describes intrusion prevention configuration.
- Volume 7 describes managing the OmniAccess System.
- Volume 8 describes configuring advanced services, such as Quality of Service (QoS) for voice and the External Services Interface module.

Related Documents

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

- *AOS-W User Guide*
- *Alcatel Wireless LAN Switch Installation Guides*

- *Alcatel Access Point Installation Guides*
- *Release Notes*

Text Conventions

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

TABLE 1 Text Conventions

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*>	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: # **send** <*text message*> 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 | Item B }	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Contacting Alcatel

Contact Center Online	
■ Main Site	http://www.alcatel.com/enterprise
■ Support Site	http://eservice.ind.alcatel.com
■ Email	support@ind.alcatel.com
Sales & Support Contact Center Telephone	
■ North America	1-800-995-2696
■ Latin America	1-877-919-9526
■ Europe	+33 (0) 38 85 56 92 9
■ Asia Pacific	+65 6586 1555
■ Worldwide	1-818-880-3500

Adding Local WLAN Switches 1

This chapter explains how to expand your network by adding a local WLAN Switch to a master WLAN Switch configuration. Typically, this is the first expansion of a network with just one WLAN Switch (which is a master WLAN Switch). This chapter is a basic discussion of creating master-local WLAN Switch configurations. More complicated multi-WLAN Switch configurations are discussed in other chapters.

This chapter describes the following topics:

- "Moving to a Multi-Controller Environment" on page 1
- "Configuring Local Mobility Controllers" on page 2

Moving to a Multi-WLAN Switch Environment

For a single WLAN configuration, the master WLAN Switch is the WLAN Switch which controls the RF and security settings of the WLAN. Additional WLAN Switches to the same WLAN serve as local switches to the master WLAN Switch. The local WLAN Switch operates independently of the master WLAN Switch and depends on the master WLAN Switch only for its security and RF settings. You configure the Layer-2 and Layer-3 settings on the local WLAN Switch independent of the master WLAN Switch. The local WLAN Switch needs to have connectivity to the master WLAN Switch at all times to ensure that any changes on the master are propagated to the local WLAN Switch.

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

- Scaling to include a larger coverage area
- Setting up remote Access Points (APs)
- Network setup requires APs to be redistributed from a single WLAN Switch to multiple WLAN Switches

Configuring Local WLAN Switches

A single master WLAN Switch configuration can be one WLAN Switch or a master redundant configuration with one master WLAN Switch and the VRRP redundant backup WLAN Switch. This section highlights the difference in configuration for both of these scenarios.

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

1. Configure the role of the local WLAN Switch to local and specify the IP address of the master.
2. Configure the Layer-2 / Layer-3 settings on the local WLAN Switch (VLANs, IP subnets, IP routes).
3. Configure as trusted ports the ports the master and local WLAN Switch use to communicate with each other.
4. For those APs that need to boot off the local WLAN Switch, configure the LMS IP address to point to the new local WLAN Switch.
5. Reboot the APs that are already on the network, so that they now connect to the local WLAN Switch.

These steps are explained below.

Configuring the Local WLAN 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 WLAN Switch, or reboot a configured Alcatel WLAN Switch (after executing a **`write erase`**, **`reload`** sequence), the Setup Dialog displays.

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

You are then prompted for the master WLAN Switch IP address. Enter the IP address of the master WLAN Switch for the WLAN network.

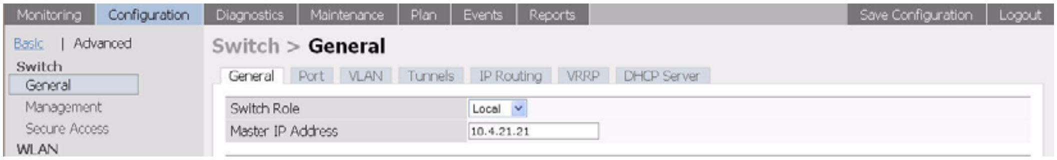
The following example shows the Setup Dialog for an OmniAccess 4324 WLAN Switch:

```
Enter system name [A4324]:
Enter VLAN 1 interface IP address [172.16.0.254]: 10.200.14.6
Enter VLAN 1 interface subnet mask [255.255.255.0]:
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: ******
Do you wish to shutdown all the ports (yes|no)? [no]:
Current choices are:

System name: A4324
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)y
Creating configuration... Done.

System will now restart!
```

Using the Web UI

Once the WLAN Switch is up and operating with Layer-3 connectivity, configure the following to set the WLAN Switch as local:

- Set the mode of the WLAN Switch to local.
- Set the master IP address to the IP address of the master WLAN Switch. If master redundancy is enabled on the master, this address should be the VRRP address for the VLAN instance corresponding to the IP address of the WLAN Switch.



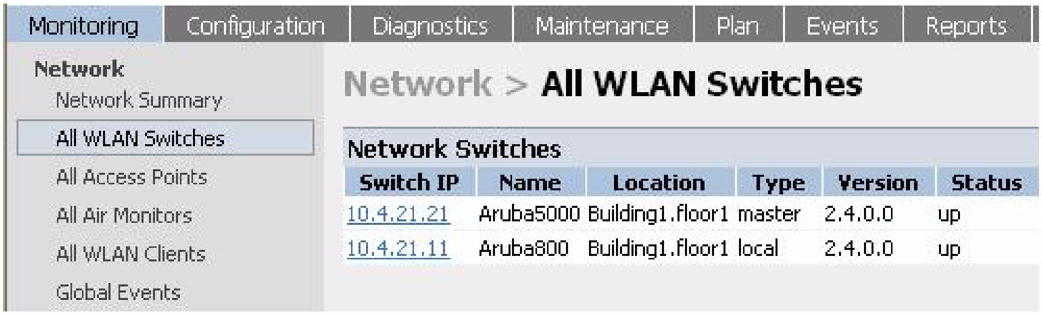
Switch Role: Local
Master IP Address: 10.4.21.21

Configuring L2/L3 Settings

Configure the VLANs, subnets, and IP address on the local WLAN Switch for IP connectivity.

Verify connectivity to the master WLAN Switch by pinging the master WLAN Switch from the local WLAN Switch.

Ensure that the master WLAN Switch recognizes the new WLAN Switch as its local WLAN Switch:



Network Switches

Switch IP	Name	Location	Type	Version	Status
10.4.21.21	Aruba5000	Building1.floor1	master	2.4.0.0	up
10.4.21.11	Aruba800	Building1.floor1	local	2.4.0.0	up

The local WLAN Switch should be listed with type `local` in the **Monitoring > Network > All WLAN Switches** page on the master. It takes about 4 – 5 minutes for the master and local WLAN Switches to synchronize configurations.

Configuring Trusted Ports

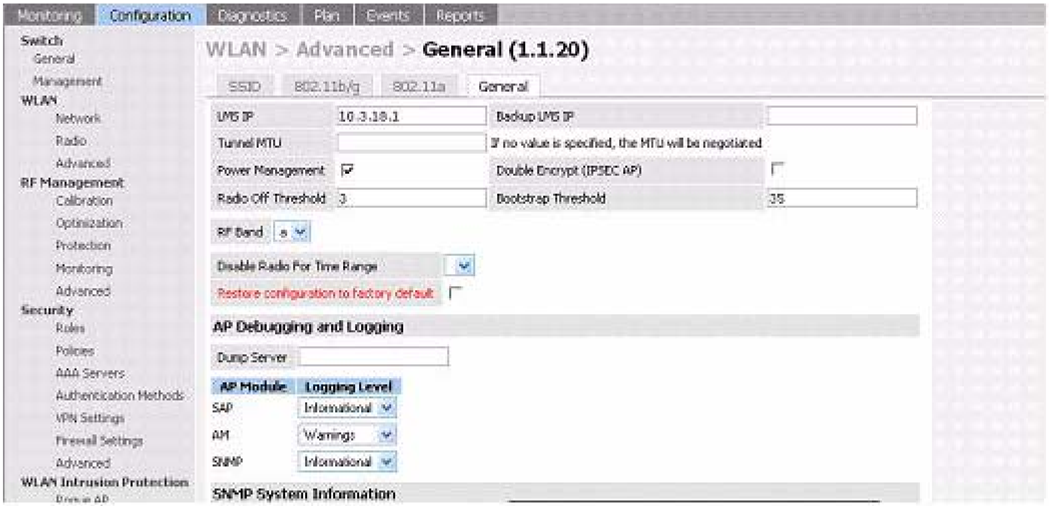
On the local WLAN Switch, navigate to the **Configuration** > **Advanced** > **Switch** > **General** > **Port** page and make sure that the port on the local WLAN Switch connecting to the master is trusted. On the master WLAN Switch, check this for the port on the master WLAN Switch that connects to the local WLAN Switch.

Configuring APs

For APs that boot from the local WLAN Switch, you must configure the LMS IP address. This configuration has to be done on the master WLAN Switch. When the changes are applied, the master WLAN Switch pushes these configurations to the local WLAN Switch.

1. Navigate to the **Configuration** > **Advanced** > **WLAN** > **Advanced** > **General** page. Select the AP that has to boot from the local WLAN 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 WLAN Switch has obtained a copy of the global settings, check the local WLAN Switch for the global configuration changes made on the master such as authentication changes and WMS settings.



WLAN > Advanced > **General (1.1.20)**

LMS IP 10.3.18.1
Backup LMS IP
Tunnel MTU
If no value is specified, the MTU will be negotiated
Power Management ☑
Double Encrypt (IPSEC AP) ☐
Radio Off Threshold 3
Bootstrap Threshold 35
RF Band a
Disable Radio For Time Range
Restore configuration to factory default ☐

AP Debugging and Logging

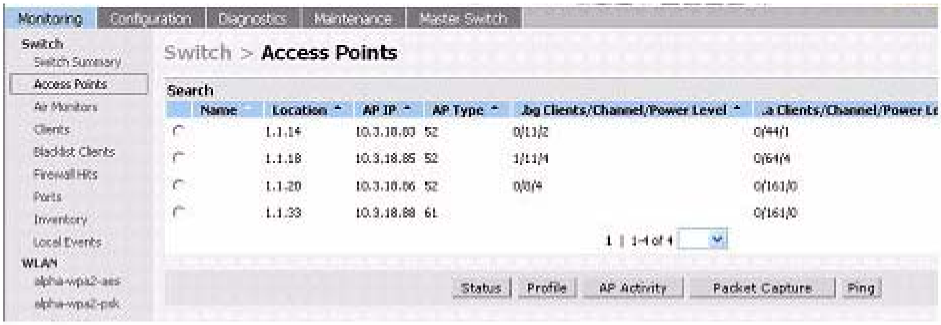
Dump Server

AP Module	Logging Level
SAP	Informational
AM	Warnings
SNMP	Informational

SNMP System Information

Rebooting APs

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



Switch > **Access Points**

Search

	Name	Location	AP IP	AP Type	.bg Clients/Channel/Power Level	.a Clients/Channel/Power Le
○		1.1.14	10.3.18.83	52	0/11/2	0/44/1
○		1.1.18	10.3.18.85	52	1/11/4	0/64/4
○		1.1.20	10.3.18.86	52	0/0/4	0/161/0
○		1.1.33	10.3.18.88	61		0/161/0

1 | 1-4 of 4

Configuring Redundancy 2

This chapter describes the following topics:

- "Virtual Router Redundancy Protocol" on page 7
- "Redundancy Configuration" on page 7

Virtual Router Redundancy Protocol

The underlying mechanism for the Alcatel redundancy solutions is the Virtual Router Redundancy Protocol (VRRP). This mechanism can be used to create various redundancy solutions, including the following:

- Pairs of local Alcatel WLAN Switches acting in an active-active mode or a hot-standby mode
- A master WLAN Switch backing up a set of local WLAN Switches
- A pair of WLAN Switches acting as a redundant pair of master WLAN Switches in a hot standby mode

Each of these modes is explained in greater detail with the required configuration.

VRRP is designed to eliminate a single point of failure by providing an election mechanism amongst WLAN Switches to elect a "master" WLAN Switch. This master WLAN Switch is the owner of the configured Virtual IP address for the VRRP instance. When the master becomes unavailable, one of the backup WLAN Switches takes the place of the master and owns the Virtual IP address. All network elements (such as the APs and other WLAN Switches) 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 APs are controlled by a WLAN Switch. The APs tunnel all data to the WLAN Switch which processes the data, including encryption/decryption, bridging/forwarding, etc.

Local WLAN Switch redundancy refers to providing redundancy for a WLAN Switch such that the APs *"failover"* to a *backup* WLAN Switch if a WLAN Switch becomes unavailable. Local WLAN Switch redundancy is provided by running VRRP between a pair of WLAN Switches.

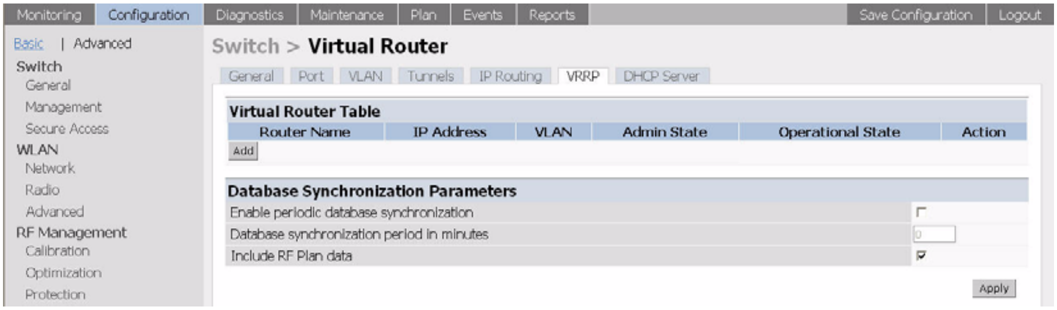
NOTE: The two WLAN Switches need to be connected on the same broadcast domain (or layer-2 connected) for VRRP operation. The two WLAN Switches should be of the same class (for example, OmniAccess 4308 to OmniAccess 4308), and both WLAN Switches should be running the same version of AOS-W.

The APs are then configured to connect to the “virtual-IP” configured for the VRRP instance.

Configuring Local WLAN Switch Redundancy

To configure redundancy for a local WLAN Switch:

1. Collect the following information needed to configure local WLAN Switch redundancy:
   - **VLAN ID** on the two local WLAN Switches that are on the same layer 2 network and is used to configure VRRP.
   - **Virtual IP address** to be used for the VRRP instance.
2. Navigate to the **Configuration > Advanced> Switch > General > VRRP** page on the WebUI for each of the local WLAN Switches. Click **Add** to create a VRRP instance.



Switch > Virtual Router

Virtual Router Table

Router Name	IP Address	VLAN	Admin State	Operational State	Action

Database Synchronization Parameters

Enable periodic database synchronization	□
Database synchronization period in minutes	0
Include RF Plan data	☑

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 or 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 *master*	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 *master.*	Configure this with the Virtual IP address reserved in step i.
Enable Router Pre-emption	Selecting this option means that a WLAN Switch can take over the role of *master* if it detects a lower priority WLAN Switch currently acting as *master*	For this topology it is recommended NOT to select this option.
Priority	Priority level of the VRRP instance for the WLAN Switch. This value is used in the election mechanism for the *master*	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.

5. Click **Apply** to apply the configuration and add the VRRP instance.
6. Configure the APs 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 WLAN Switch as only the Master WLAN Switch controls all APs in the network.

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

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

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

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

(WLAN_Switch) (sap-config location 10.0.0) #
```

Master WLAN Switch Redundancy

The Master WLAN 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 WLAN 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 WLAN Switch.

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

To configure master WLAN Switch redundancy:

1. Collect the following data before configuring master WLAN Switch redundancy.
   - **VLAN ID** on the two WLAN 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 WLAN Switch CLI using Telnet or SSH. After logging into the WLAN Switch, enter the global configuration mode.

To configure VRRP on the VLAN ID.

	Command	**Explanation**	**Expected or Recommended 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 *master*. By default, the value is 100.	The following are the recommended values for the priority on the *"initially preferred"* master and *"initially preferred"* backup switches: *Master:* 110 *Backup:* 100 **Note**: these values are closely related to the value of the *value* to be added to the priority by tracking in step 7.
Step 5	preempt	Enable pre-emption	

Step 6	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 WLAN Switches. This is an optional configuration.
Step 7	description *description* (Optional)	Optional description to the VRRP instance.	Any text description can be configured in this field. This is an optional configuration.
Step 8	tracking master-up-time *duration* add *value*	Configures a tracking mechanism that adds *value* to the priority after a WLAN 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 failures.	The value of *duration* 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 *value* in conjunction to the values for priority 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".*

```
(WLAN_Switch) (config) #vrrp 22
(WLAN_Switch) (config-vrrp) #vlan 22
(WLAN_Switch) (config-vrrp) #ip address 10.200.22.254
(WLAN_Switch) (config-vrrp) #priority 110
(WLAN_Switch) (config-vrrp) #preempt
(WLAN_Switch) (config-vrrp) #authentication password
```

```
(WLAN_Switch) (config-vrrp) #description Preferred-Master
(WLAN_Switch) (config-vrrp) #tracking master-up-time 30 add 20
(WLAN_Switch) (config-vrrp) #no shutdown
```

The following shows the corresponding VRRP configuration for the peer WLAN Switch.

```
(WLAN_Switch) (config) #vrrp 22
(WLAN_Switch) (config-vrrp) #vlan 22

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

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

	Command	**Explanation**	**Expected or Recommended 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 WLAN Switch.

NOTE: All the APs and local WLAN Switches in the network should be configured with the Virtual IP address as Master IP. The Master IP address can be configured for local WLAN 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 WLAN Switch. The WLAN Switch will require a reboot after changing the Master IP of the WLAN Switch.

	Command	Explanation	Expected or Recommended values
Step 1	masterip *ip-address*	Configures the Master IP address of a local WLAN 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 WLAN Switch, ensure that the name *"oaw-master"* resolves to the same Virtual IP address configured as a part of the master redundancy.

Master-Local WLAN Switch Redundancy

This section outlines the concepts behind a redundancy solution where a master can act as a backup for one or more local WLAN Switches and shows how to configure the Alcatel WLAN Switches for such a redundant solution. In this solution, the local WLAN Switches act as the WLAN Switch for the APs. When any one of the local WLAN Switches becomes unavailable, the master takes over the APs controlled by that local WLAN Switch for the time that the local WLAN Switch remains unavailable. It is configured such that when the local WLAN 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 WLAN Switch has a layer-2 connectivity to all the local WLAN Switches.

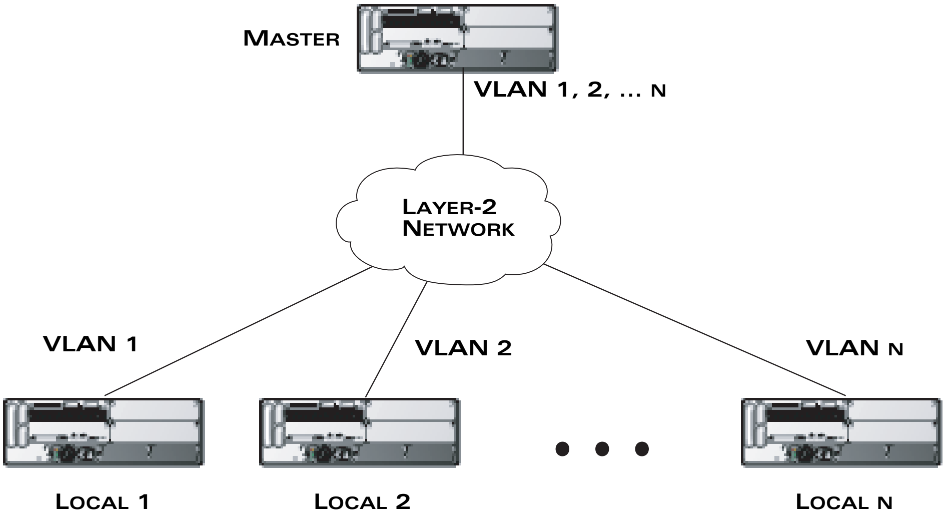


FIGURE 2-1 Redundant Topology: Master-Local Redundancy

In the network shown above, the master WLAN Switch is connected to the local WLAN Switches on VLANs 1, 2... n respectively through a Layer-2 network. 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 WLAN Switch. The VRRP instance on the local WLAN Switch is configured with a higher priority to ensure that when available, the APs always choose the local WLAN Switch to terminate their tunnels.

To configure the master and local WLAN Switches for such a topology:

1. Configure the interface on the master WLAN Switch to be a trunk port with 1, 2... n being member VLANs.
2. Collect the following data before configuring master WLAN Switch redundancy.
   - **VLAN IDs** on the WLAN 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 WLAN Switch CLI using Telnet or SSH. After logging into the WLAN Switch, enter the global configuration mode.

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

	Command	**Explanation**	**Expected or Recommended 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 *master*. By default, the value is 100.	The following are the recommended values for the priority on the master and local WLAN Switches: *Master:* 100 *Local:* 110.
Step 5	preempt	Enable pre-emption	
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 WLAN Switches. This is an optional configuration.
Step 6	description *description* (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 WLAN Switch in such a topology for one of the VLANs (in this case VLAN 22).

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

The following shows the configuration on the corresponding local WLAN Switch.

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

Configure the APs with the appropriate Virtual-IP address depending on which WLAN 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 WLAN Switch 1, all APs on floor 2 are controlled by local WLAN Switch 2 and so on. All the local WLAN Switches are backed up by the master WLAN 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 WLAN Switch 1 and master and so on. This can be done by following these steps:

	Command	**Explanation**	**Expected or Recommended values**
Step 1	ap location *b.f.l*	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 *ip-address*	Configure the IP address of the WLAN 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 WLAN Switch and master WLAN 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 WLAN Switches configured in the above example.

NOTE: This command is executed on the Master WLAN Switch.

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

(WLAN_Switch) (sap-config location 1.1.0) #
```

Volume 6

Configuring Intrusion Protection

AOS-W User Guide

Release 2.5.3

ALCATEL

Copyright

Specifications in this manual are subject to change without notice.

Originated in the USA.

Trademarks

AOS-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 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

This preface includes the following information:

- An overview of the contents of 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

The *AOS-W User Guide* is now in eight separate volumes for easier download and information access. The volumes are as follows:

- Volume 1 contains an overview of the OmniAccess System.
- Volume 2 describes how to install the OmniAccess System in a wired network.
- Volume 3 describes WLAN configuration, including remote Access Points.
- Volume 4 describes wireless encryption and authentication configuration.
- Volume 5 describes configuring multi-WLAN switch environments.
- Volume 6 (this volume) describes intrusion prevention configuration.
- Volume 7 describes managing the OmniAccess System.
- Volume 8 describes configuring advanced services, such as Quality of Service (QoS) for voice and the External Services Interface module.

Related Documents

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

- *AOS-W User Guide*
- *Alcatel Wireless LAN Switch Installation Guides*
- *Alcatel Access Point Installation Guides*
- *Release Notes*

Text Conventions

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

TABLE 1 Text Conventions

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*>	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: # **send** <*text message*> 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 | Item B }	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Contacting Alcatel

Contact Center Online	
■ Main Site	http://www.alcatel.com/enterprise
■ Support Site	http://eservice.ind.alcatel.com
■ Email	support@ind.alcatel.com
Sales & Support Contact Center Telephone	
■ North America	1-800-995-2696
■ Latin America	1-877-919-9526
■ Europe	+33 (0) 38 85 56 92 9
■ Asia Pacific	+65 6586 1555
■ Worldwide	1-818-880-3500

Configuring Intrusion Prevention 1

This document outlines the steps needed to configure various intrusion detection system (IDS) capabilities of the Alcatel OmniAccess system. The Alcatel system offers a variety of IDS/intrusion prevention system (IPS) features that can be configured and deployed as required. Like most other security-related features of the Alcatel system, the IDS configuration is done completely on the master WLAN Switch in the network.

This chapter describes the following topics:

- "IDS Features" on page 1
- "WLAN Policies" on page 3
- "IDS Configuration" on page 4
- "WLAN Policies Configuration" on page 15

IDS Features

Rogue/Interfering AP Detection

The most important IDS functionality offered in the Alcatel system is the ability to classify an Access Point as either a *rogue* AP or an *interfering* AP. An AP is considered to be a rogue AP if it is both unauthorized and plugged into the wired side of the network. An AP is considered to be an interfering AP if it is seen in the RF environment but is not connected to the wired network. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat since it is not connected to the wired network.

You can enable a policy to automatically disable APs that are classified as a rogue APs by the Alcatel system. When a rogue AP is disabled, no wireless stations are allowed to associate to that AP. Refer to *"Configuring Rogue AP Detection" on page 6* for details on how to configure Rogue AP detection, classification, and containment.

You can manually reclassify an interfering AP. Refer to "Classifying APs" on page 5 for details on how to change the classification of an AP.

Denial of Service (DoS) 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 the detection of a specific DoS attack known as Fake AP.

- **Rate Analysis:** Many DoS attacks flood an AP or multiple APs with 802.11 management frames. These can include authenticate/associate frames which are 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 WLAN Switch can be configured with the thresholds that indicate a DoS attack and can detect the same. Refer to "Configuring Denial of Service Attack Detection" on page 8 for more details.
- **Fake AP:** Fake AP 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 "Configuring Denial of Service Attack Detection" on page 8 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 WLAN 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 "Configuring Signature Detection" on page 12.

WLAN 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 WLAN Switch cannot configure the third-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 third-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.

IDS Configuration

Enabling AP Learning

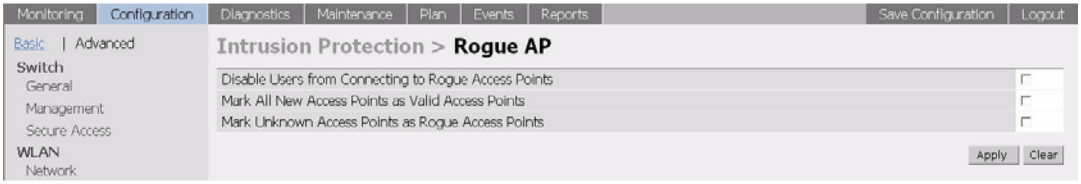
AP learning allows the Alcatel system to classify all newly discovered APs as valid APs. By default, AP learning is not enabled and all newly discovered APs are classified as interfering APs. You can enable or disable AP learning from either the WebUI or the CLI.

NOTE: Enabling AP learning is useful when you install the Alcatel WLAN Switch in an environment with an existing third-party wireless network, especially if there are a large number of installed APs. Leave AP learning enabled until all APs in the network have been detected and classified as valid. Then disable AP learning and reclassify any unknown APs as interfering.

To enable or disable AP learning:

WebUI

1. Navigate to the **Configuration** > **Advanced** > **Security** > **Rogue AP** page on the master WLAN Switch.



Disable Users from Connecting to Rogue Access Points □
Mark All New Access Points as Valid Access Points □
Mark Unknown Access Points as Rogue Access Points □

2. To enable AP learning, select the option “Mark All New Access Points as Valid Access Points”. To disable AP learning, deselect this option.
3. Click **Apply**.

CLI

```
wms
   ap-policy learn-ap { enable | disable }
```

Classifying APs

If AP learning is enabled, every newly-discovered AP is classified as a valid AP. If AP learning is disabled, every newly-discovered AP is classified as an interfering AP. You can also manually classify an AP. For example, if you know about an interfering AP, you can manually reclassify it as a *known* interfering AP. You can manually classify an AP into one of the following categories:

Valid AP — An AP that is part of the enterprise providing WLAN service. Alcatel APs that successfully connect to the WLAN Switch and load software and configuration should be classified as valid APs.

NOTE: Any client that successfully authenticates with a valid AP and passes encrypted traffic is classified as a valid client. (Encrypted traffic includes encrypted 802.11 frames and unencrypted 802.11 frames which are VPN encrypted.)

Interfering AP or Known Interfering AP
An AP that is seen in the RF environment but is not connected to the wired network. An interfering AP is not considered a direct security threat since it is not connected to the wired network.

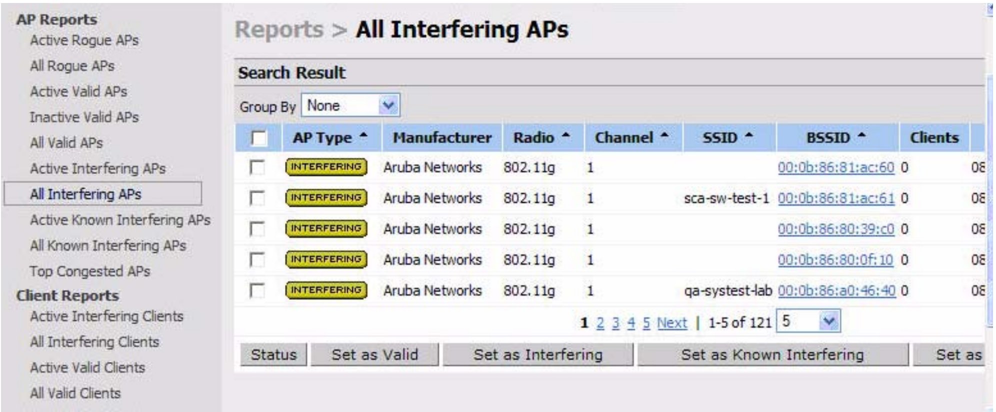
Unsecure AP
An rogue AP that is part of the network. A rogue AP is an unauthorized AP that is plugged into the wired side of the network.

DoS AP
An AP on which denial of service is enabled.

To manually classify an AP:

WebUI

1. Navigate to the **Reports > AP Reports> All Interfering APs** page on the master WLAN Switch.



Group By None

□	AP Type ▲	Manufacturer	Radio ▲	Channel ▲	SSID ▲	BSSID ▲	Clients	
□	INTERFERING	Aruba Networks	802.11g	1		00:0b:86:81:ac:60	0	08
□	INTERFERING	Aruba Networks	802.11g	1	sca-sw-test-1	00:0b:86:81:ac:61	0	08
□	INTERFERING	Aruba Networks	802.11g	1		00:0b:86:80:39:c0	0	08
□	INTERFERING	Aruba Networks	802.11g	1		00:0b:86:80:0f:10	0	08
□	INTERFERING	Aruba Networks	802.11g	1	qa-systest-lab	00:0b:86:a0:46:40	0	08

2. Select the checkbox for the AP(s) you want to classify.

3. Click the appropriate “Set as” button on the page.

4. Click **Apply**.

CLI

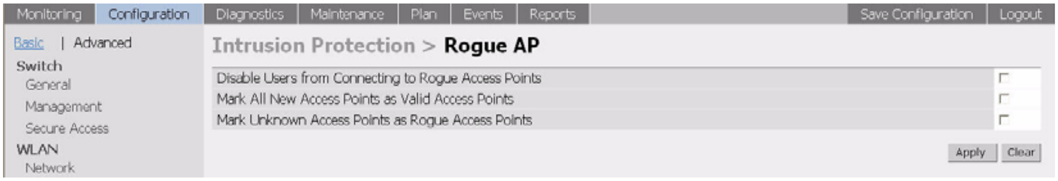
Enter the following command in Enable mode:

```
wms ap <bssid> mode {dos|interfering|known-interfering|unsecure|valid}
```

Configuring Rogue AP Detection

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

Navigate to the **Configuration > Advanced > Security > Rogue AP** page on the WebUI of the Master WLAN Switch.



Intrusion Protection > **Rogue AP**

- Disable Users from Connecting to Rogue Access Points ☐
- Mark All New Access Points as Valid Access Points ☐
- Mark Unknown Access Points as Rogue Access Points ☐

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

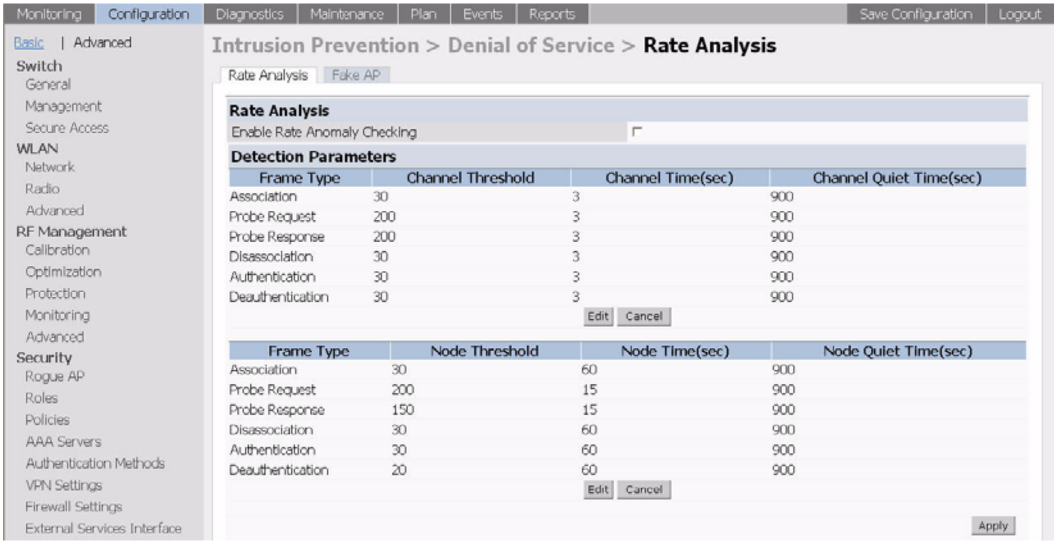
Field	Description
Disable Users from Connecting to Rogue Access Points	By default, rogue APs are only detected, but are not automatically disabled. Enable this option to automatically shut down rogue APs. When this option is enabled, clients attempting to associate to a rogue AP will be disconnected from the rogue AP through a denial of service attack.
Mark All New Access Points as Valid Access Points	When installing an Alcatel WLAN Switch in an environment with an existing third-party wireless network, it is necessary to manually classify existing enterprise APs as valid – a time-consuming process if a large number of APs are installed. Enable this option to mark all detected APs as valid. Leave this option enabled until all enterprise APs have been detected and classified as valid. After this process has completed, disable this option and re-classify any unknown APs as interfering.
Mark Unknown 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 > Advanced > WLAN Intrusion Protection > Denial of Service** page on the WebUI. To configure Rate Analysis, select **Rate Analysis.**



Intrusion Prevention > Denial of Service > **Rate Analysis**

Rate Analysis

Enable Rate Anomaly Checking □

Detection Parameters

Frame Type	Channel Threshold	Channel Time(sec)	Channel Quiet Time(sec)
Association	30	3	900
Probe Request	200	3	900
Probe Response	200	3	900
Disassociation	30	3	900
Authentication	30	3	900
Deauthentication	30	3	900

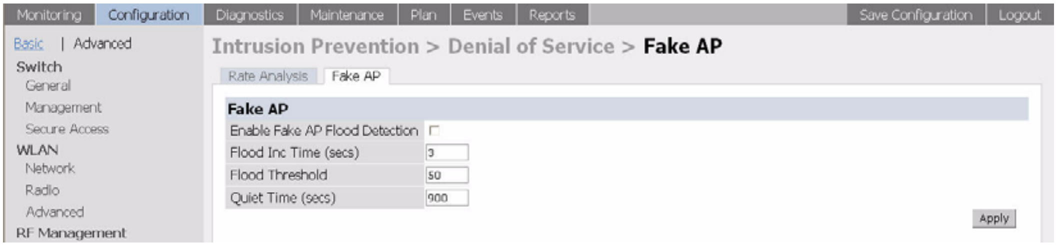
Frame Type	Node Threshold	Node Time(sec)	Node Quiet Time(sec)
Association	30	60	900
Probe Request	200	15	900
Probe Response	150	15	900
Disassociation	30	60	900
Authentication	30	60	900
Deauthentication	20	60	900

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**
Frame Type	Identifies the type of standard frame.
Channel/Node Threshold	Specifies the number of a specific type of frame that must be exceeded within a specific interval to trigger an alarm.
Channel/Node Time (sec)	Specifies the time interval in which the threshold must be exceeded in order to trigger an alarm.
Channel/Node Quiet Time (sec)	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.

3. To configure the Fake AP detection, select the **Fake AP** tab on the **Configuration > Advanced > WLAN Intrusion Protection > Denial of Service** page.



Fake AP

Enable Fake AP Flood Detection	□
Flood Inc Time (secs)	3
Flood Threshold	50
Quiet Time (secs)	900

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

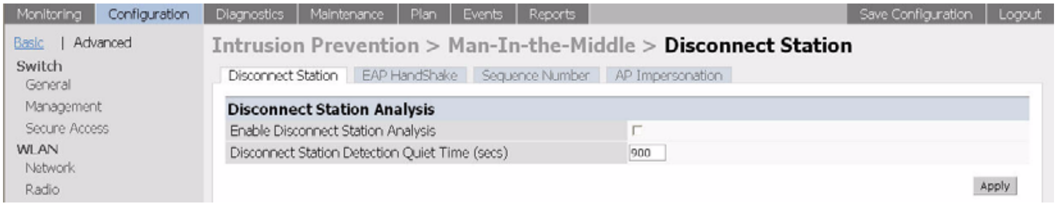
Field	**Description**
Enable Fake AP Flood Detection	Enables or disables the feature
Flood Inc Time (secs)	The time period in which a configured number of FakeAP beacons must be received.
Flood Threshold	The number of FakeAP beacons that must be received within the Flood Inc Time in order to trigger an alarm.

Quiet Time (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 > Advanced > WLAN Intrusion Protection > Man-In-The-Middle** page on the WebUI of the Master WLAN Switch. Select the required tab to configure each of the following:

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



Intrusion Prevention > Man-In-the-Middle > **Disconnect Station**

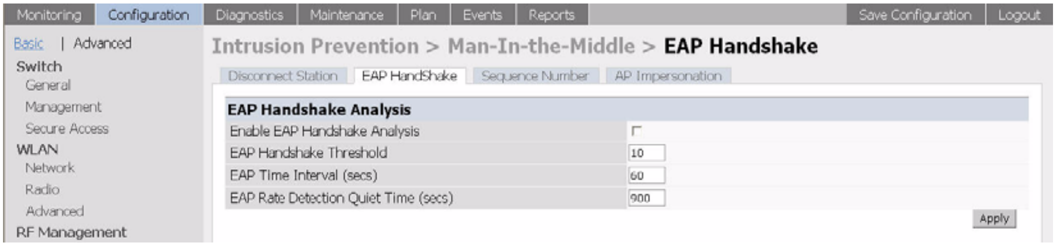
Disconnect Station Analysis

Enable Disconnect Station Analysis	☐
Disconnect Station Detection Quiet Time (secs)	900

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

Field	Description
Enable Disconnect Station Analysis	Enables/disables this feature.
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.

2. To configure EAP Handshake analysis, click the **EAP Handshake**.



Intrusion Prevention > Man-In-the-Middle > **EAP Handshake**

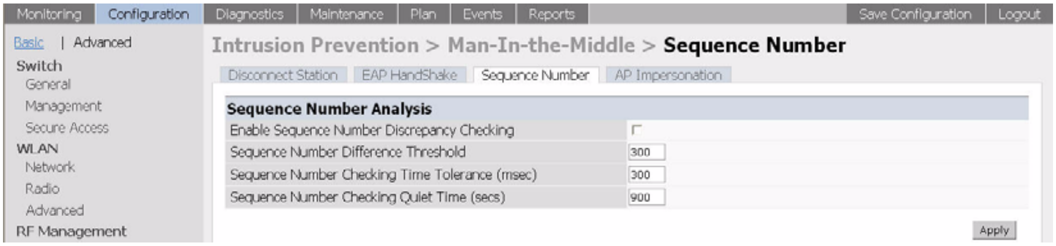
EAP Handshake Analysis

Enable EAP Handshake Analysis	☐
EAP Handshake Threshold	10
EAP Time Interval (secs)	60
EAP Rate Detection Quiet Time (secs)	900

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

Field	**Description**
Enable EAP Handshake Analysis	Enables or disables this feature.
EAP Handshake Threshold	The number of EAP handshakes that must be received within the EAP Time Interval in order to trigger an alarm.
EAP Time Interval (secs)	The time period in which a configured number of EAP handshakes must be received.
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.

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



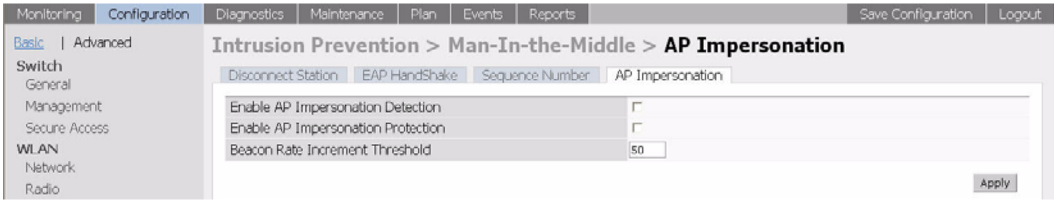
Intrusion Prevention > Man-In-the-Middle > Sequence Number

Sequence Number Analysis	
Enable Sequence Number Discrepancy Checking	□
Sequence Number Difference Threshold	300
Sequence Number Checking Time Tolerance (msec)	300
Sequence Number Checking Quiet Time (secs)	900

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

Field	**Description**
Enable Sequence Number Discrepancy Checking	Enables or disables this feature.
Sequence Number Difference Threshold	The maximum allowable tolerance between sequence numbers within a specific time interval.
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.
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.

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



Intrusion Prevention > Man-In-the-Middle > AP Impersonation

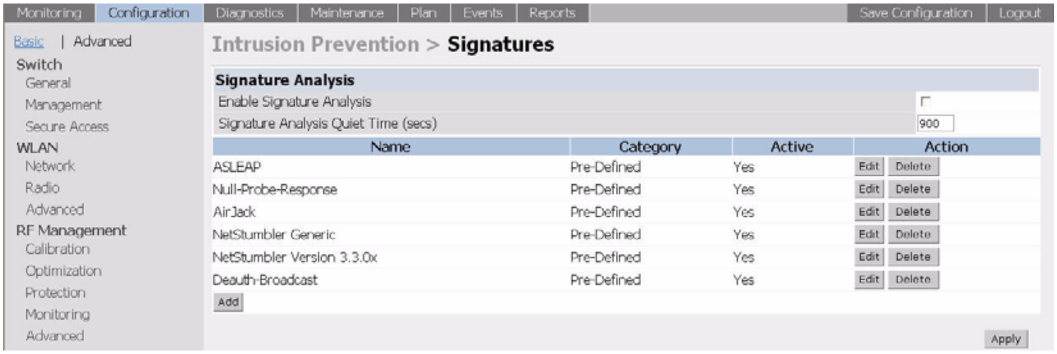
Enable AP Impersonation Detection	☐
Enable AP Impersonation Protection	☐
Beacon Rate Increment Threshold	50

The following table briefly descriptions the fields in this section.

Field	Description
Enable AP Impersonation Detection	Enables detection of AP impersonation.
Enable AP Impersonation Protection	When AP impersonation is detected, both the legitimate and the impersonating AP will be disabled using a denial of service attack.
Beacon Rate Increment Threshold	The percentage increase in beacon rate that will trigger an AP impersonation event.

Configuring Signature Detection

Navigate to the **Configuration** > **Advanced** > **WLAN Intrusion Protection** > **Signatures** page on the WebUI on the Master WLAN Switch.



Intrusion Prevention > Signatures

Signature Analysis

Enable Signature Analysis	☐
Signature Analysis Quiet Time (secs)	900

Name	Category	Active	Action
ASLEAP	Pre-Defined	Yes	Edit Delete
Null-Probe-Response	Pre-Defined	Yes	Edit Delete
AirJack	Pre-Defined	Yes	Edit Delete
NetStumbler Generic	Pre-Defined	Yes	Edit Delete
NetStumbler Version 3.3.0x	Pre-Defined	Yes	Edit Delete
Deauth-Broadcast	Pre-Defined	Yes	Edit Delete

The table below explains the configuration parameters in this section:

Field	Description
Enable Signature Analysis	Enables or disables this feature.
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 the pre-defined signatures that are supported by AirOS version 2.3 or higher.

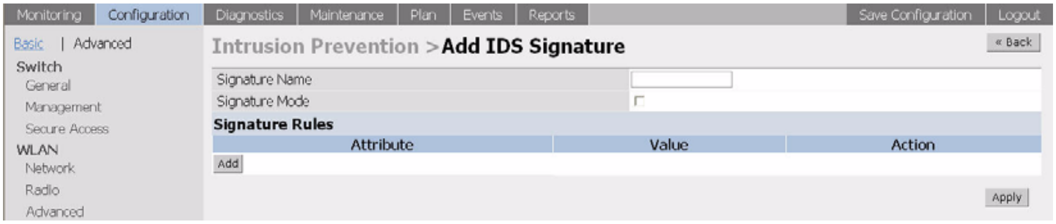
Signature	Description
ASLEAP	A tool created for Linux systems that has been used to attack Cisco LEAP authentication protocol.
Null-Probe-Response	An attack with the potential to crash or lock up the firmware of many 802.11 NICs. In this attack, a client probe-request frame will be answered by a probe response containing a null SSID. A number of popular NIC cards will lock up upon receiving such a probe response.
AirJack	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.
NetStumbler Generic	NetStumbler is a popular wardriving application used to locate 802.11 networks. When used with certain NICs (such as Orinoco), NetStumbler generates a characteristic frame that can be detected.
NetStumbler Version 3.3.0x	Version 3.3.0 of NetStumbler changed the characteristic frame slightly. This signature detects the updated frame.

Deauth-Broadcast	A deauth broadcast attempts to disconnect all stations in range – rather than sending a spoofed deauth to a specific MAC address, this attack sends the frame to a broadcast address.

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** > **Advanced** > **WLAN Intrusion Protection** > **Signatures** page click **Add** to add a new signature pattern.



Intrusion Prevention > **Add IDS Signature**

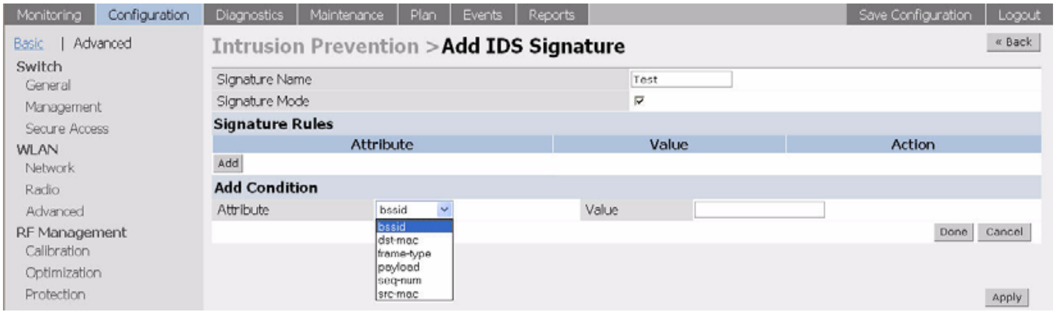
Signature Name □
Signature Mode □

Signature Rules

Attribute	Value	Action

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.



Intrusion Prevention > **Add IDS Signature**

Signature Name: Test
Signature Mode ☑

Signature Rules

Attribute	Value	Action

Add Condition

Attribute: bssid
Value:

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.

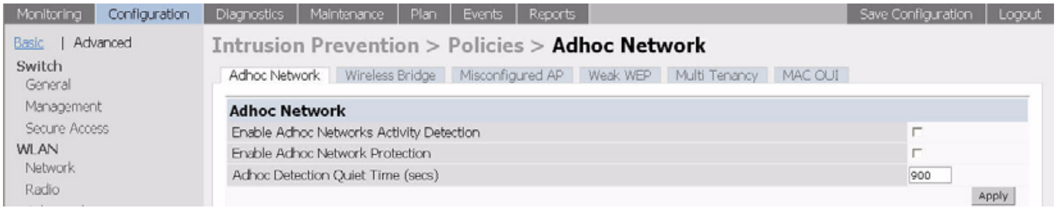
- Frame Type: This refers to the type of 802.11 frame. For each type of frame further details can be specified to filter and detect only the required frames. It can be one of the following:
  - Association
  - Auth
  - Control
  - Data
  - Deauth
  - Deassoc
  - Management
  - Probe-request
  - Probe-response
  - 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 00:00:00:00:00:0a has been added.
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.

WLAN Policies Configuration

Navigate to the **Configuration > Advanced > WLAN Intrusion Protection > Policies** page on the WebUI.



Intrusion Prevention > Policies > Adhoc Network

Adhoc Network	
Enable Adhoc Networks Activity Detection	□
Enable Adhoc Network Protection	□
Adhoc Detection Quiet Time (secs)	900

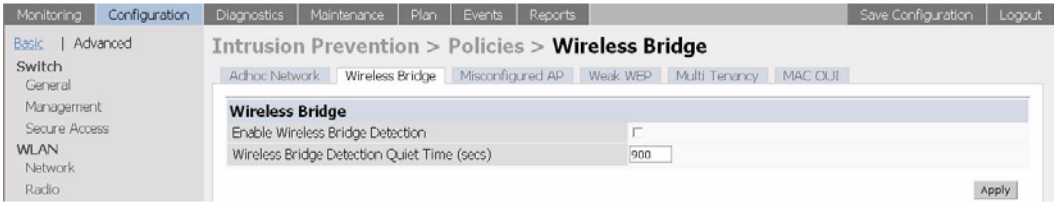
Configuring Ad-hoc Network Protection

The table below describes the data parameters in this section.

Field	Description
Enable Adhoc Networks Activity Detection	Select to enable the detection of adhoc networks.
Enable Adhoc Network Protection	When adhoc networks are detected, they will be disabled using a denial of service attack.
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 the detection of wireless bridges, navigate to **Configuration > Advanced > WLAN Intrusion Protection > Policies > Wireless Bridge**, as shown in the figure below.



Wireless Bridge

Enable Wireless Bridge Detection □

Wireless Bridge Detection Quiet Time (secs) 900

The table below describes the fields in this section.

Field	Description
Enable Wireless Bridge Detection	Select to enable the detection of adhoc networks.
Wireless Bridge Detection Quiet Time (secs)	After an alarm has been triggered, the amount of time that must pass before another identical alarm may be triggered.

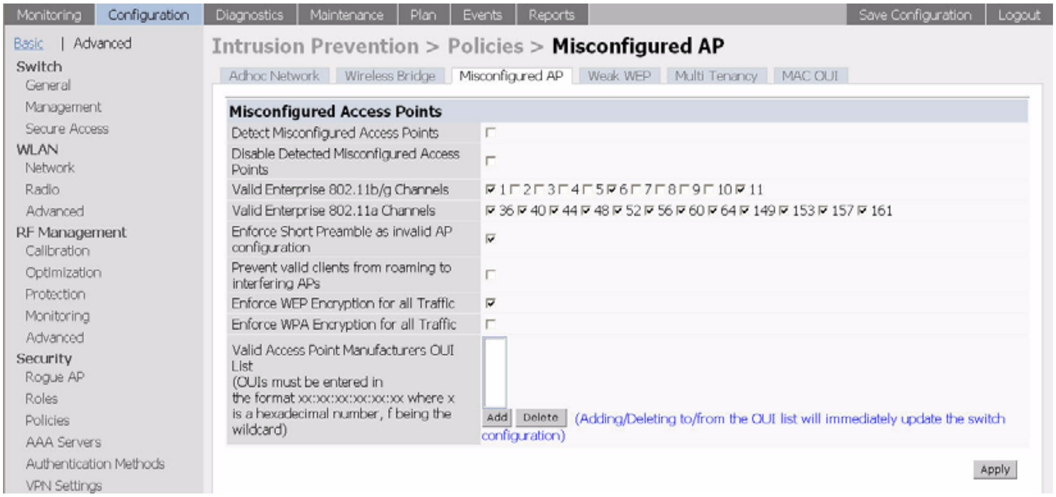
Configuring Misconfigured AP Protection

An AP is classified as misconfigured if it does not meet any of the following following configurable parameters:

- Valid channels
- Encryption type
- Short preamble
- List of valid AP MAC OUIs
- Valid SSID list (exceptions are described in "Use of the Valid Enterprise SSID List" on page 20)

This classification is primarily for enforcing security policies on non-Alcatel APs, although the classification and protection mechanism also applies to all valid Alcatel APs.

To configure protection for misconfigured APs, navigate to **Configuration > Advanced > WLAN Intrusion Protection > Policies > Misconfigured AP** as shown in the figure below.



Intrusion Prevention > Policies > **Misconfigured AP**

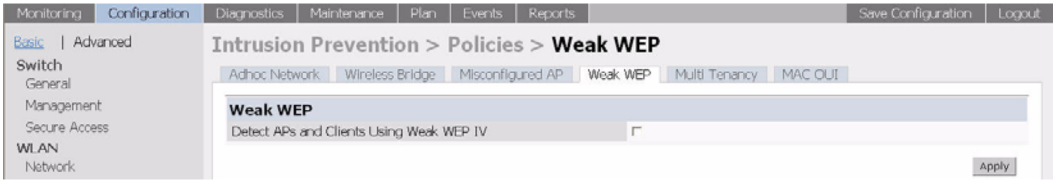
Misconfigured Access Points	
Detect Misconfigured Access Points	☐
Disable Detected Misconfigured Access Points	☐
Valid Enterprise 802.11b/g Channels	☑ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☑ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☑ 11
Valid Enterprise 802.11a Channels	☑ 36 ☑ 40 ☑ 44 ☑ 48 ☑ 52 ☑ 56 ☑ 60 ☑ 64 ☑ 149 ☑ 153 ☑ 157 ☑ 161
Enforce Short Preamble as invalid AP configuration	☑
Prevent valid clients from roaming to interfering APs	☐
Enforce WEP Encryption for all Traffic	☑
Enforce WPA Encryption for all Traffic	☐
Valid Access Point Manufacturers OUI List (OUIs must be entered in the format xx:xx:xx:xx:xx:xx where x is a hexadecimal number, f being the wildcard)	Add Delete (Adding/Deleting to/from the OUI list will immediately update the switch configuration)

The table below describes the fields shown in this section.

Field	Description
Detect Misconfigured Access Points	Select to enable, reselect to disable, the misconfigured AP detection feature.
Disable Detected Misconfigured Access Points	When valid APs are found that violate the list of allowable parameters, select this field to prevent clients from associating to those APs using a denial of service attack.
Valid Enterprise 802.11b/g Channels	Defines the list of valid 802.11b/g channels that third-party APs are allowed to use.
Valid Enterprise 802.11a Channels	Defines the list of valid 802.11a channels that third-party APs are allowed to use.
Enforce Short Preamble as invalid AP configuration	Select to enable, reselect to disable, a short preamble as a valid AP configuration.
Prevent valid clients from roaming to interfering APs	If a valid enterprise client attempts to associate with an AP classified as "interfering", select this field to break the association using a denial of service attack.
Enforce WEP Encryption for all Traffic	Any valid AP not using WEP will be flagged as misconfigured.
Enforce WPA Encryption for all Traffic	Any valid AP not using WPA will be flagged as misconfigured.
Valid Access Point Manufacturers OUI List (OUIs must be entered in the format 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** > **Advanced** > **WLAN Intrusion Protection** > **Policies** > **Weak WEP** as shown in the following figure.



Intrusion Prevention > Policies > **Weak WEP**

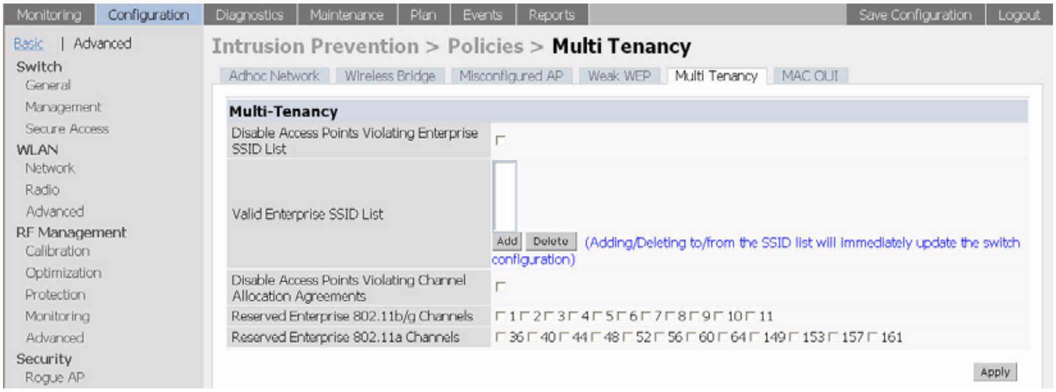
Weak WEP

Detect APs and Clients Using Weak WEP IV □

2. Select the check box for **Detect APs and Clients Using Weak WEP IV** to enable this feature.

Configuring Multi-Tenancy Detection

To configure multi-tenancy policies, navigate to **Configuration** > **Advanced** > **WLAN Intrusion Prevention** > **Policies** > **Multi Tenancy** as shown below.



Intrusion Prevention > Policies > **Multi Tenancy**

Multi-Tenancy

Disable Access Points Violating Enterprise SSID List □

Valid Enterprise SSID List

(Adding/Deleting to/from the SSID list will immediately update the switch configuration)

Disable Access Points Violating Channel Allocation Agreements □

Reserved Enterprise 802.11b/g Channels □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11

Reserved Enterprise 802.11a Channels □ 36 □ 40 □ 44 □ 48 □ 52 □ 56 □ 60 □ 64 □ 149 □ 153 □ 157 □ 161

The table below describes the fields in this section.

Field	Description
Disable Access Points Violating Enterprise SSID List	When an unknown AP is detected advertising a reserved SSID, select this field to disable the AP using a denial of service attack.
Valid Enterprise SSID List	This is a list of all the SSIDs that have been reserved for Multi-Tenancy Protection. This list is empty by default and does not contain any SSIDs configured on the WLAN Switch. Adding to or deleting from the SSID List will immediately update the WLAN Switch. See "Updating the Valid Enterprise SSID List".

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.
Reserved Enterprise 802.11b/g Channels	This is a list of reserved channel numbers for b/g mode.
Reserved Enterprise 802.11a Channels	A list of reserved channel numbers for a mode.

Updating the Valid Enterprise SSID List

SSIDs added to the Valid Enterprise SSID list are known as “Valid SSIDs” or “Reserved SSIDs.” The list is empty by default and does not contain any SSIDs configured on the WLAN Switch. You can add SSIDs to the list using the WebUI or CLI.

To add an SSID to the Valid Enterprise SSID list:

WebUI

1. Navigate to the Configuration > Advanced > WLAN Intrusion Prevention > Policies > Multi Tenancy page (shown previously).
2. Click the **Add** button.
3. Enter the name of the SSID, then click **Add**.

CLI

```
wms valid-ssid ssid_name
```

Use of the Valid Enterprise SSID List

This section describes the use of the Valid Enterprise SSID list with both Multi-Tenancy protection and Misconfigured AP protection.

As part of its function, Multi-Tenancy protection prevents an interfering AP from advertising an SSID that is added to the Valid Enterprise SSID list. This feature protects against honeypot attacks.

Misconfigured AP protection also uses the Valid Enterprise SSID list to classify an AP as misconfigured.

Whether a client can connect to an SSID depends on whether Multi-Tenancy protection or Misconfigured AP protection are enabled or disabled, whether the AP is valid or interfering, and whether the SSID is in the Valid Enterprise SSID list.

Table 1-1 describes client connections to valid and non-valid SSIDs when Multi-Tenancy protection and Misconfigured AP protection are enabled or disabled.

TABLE 1-1 Valid SSIDs with Multi-Tenancy and Misconfigured AP Protection

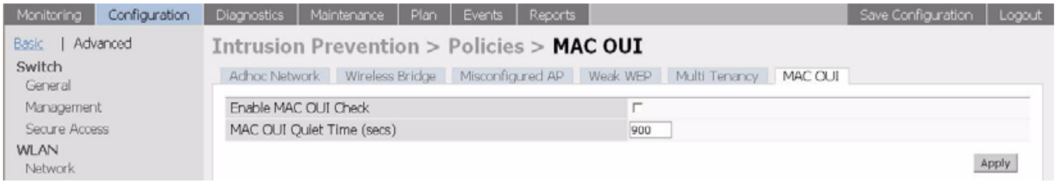
Multi-Tenancy Protection	Misconfigured AP Protection	Client Connections
Enabled	Disabled	If there are entries in the valid SSID list: ■ Clients can connect to valid SSIDs on valid APs. ■ Clients cannot connect to valid SSIDs on interfering APs (including known interfering APs). ■ Clients can connect to SSIDs not in the valid SSID list on valid APs. ■ Clients can connect to SSIDs not in the valid SSID list on interfering APs (including known interfering APs). If the valid SSID list is empty, it is ignored and clients can connect to all SSIDs on both valid APs and interfering APs (including known interfering APs). Not adding an SSID to the valid SSID list exposes that SSID to honeypot attacks.
Enabled	Enabled	If there are entries in the valid SSID list: ■ Clients can connect to valid SSIDs on valid APs. ■ Clients cannot connect to valid SSIDs on interfering APs (including known interfering APs). ■ Clients cannot connect to SSIDs not in the valid SSID list on valid APs. ■ Clients can connect to SSIDs not in the valid SSID list on interfering APs. If the valid SSID list is empty, it is ignored and clients can connect to all SSIDs on both valid APs and interfering APs (including known interfering APs). Not adding an SSID to the valid SSID list exposes that SSID to honeypot attacks.

TABLE 1-1 Valid SSIDs with Multi-Tenancy and Misconfigured AP Protection

Multi-Tenancy Protection	Misconfigured AP Protection	Client Connections
Disabled	Enabled	If there are entries in the valid SSID list: ■ Clients can connect to valid SSIDs on valid APs. ■ Clients can connect to valid SSIDs on interfering APs (including known interfering APs). ■ Clients cannot connect to SSIDs not in the valid SSID list on valid APs. ■ Clients can connect to SSIDs not in the valid SSID list on interfering APs. If the valid SSID list is empty, it is ignored and clients can connect to all SSIDs on both valid APs and interfering APs (including known interfering APs). When Multi-Tenancy protection is disabled, the network is susceptible to honeypot attacks.

Configuring MAC OUI Checking

To enable MAC OUI checking, navigate to **Configuration > Advanced > WLAN Intrusion Protection > Policies > MAC OUI** as shown in the figure below.



Enable MAC OUI Check ☐
MAC OUI Quiet Time (secs) 900

The table below describes the fields in this section.

Field	Description
Enable MAC OUI Check	Enables or disables the MAC OUI Check feature.
MAC OUI Quiet Time (secs)	Allows you to set a minimum amount of time that must pass before identical alarms may be triggered.

Volume 7

Managing the OmniAccess System

AOS-W User Guide

Release 2.5.3

ALCATEL

Copyright

Specifications in this manual are subject to change without notice.

Originated in the USA.

Trademarks

AOS-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 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

This preface includes the following information:

- An overview of the contents of 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

The *AOS-W User Guide* is now in eight separate volumes for easier download and information access. The volumes are as follows:

- Volume 1 contains an overview of the OmniAccess System.
- Volume 2 describes how to install the OmniAccess System in a wired network.
- Volume 3 describes WLAN configuration, including remote Access Points.
- Volume 4 describes wireless encryption and authentication configuration.
- Volume 5 describes configuring multi-WLAN switch environments.
- Volume 6 describes intrusion prevention configuration.
- Volume 7 (this volume) describes managing the OmniAccess System.
- Volume 8 describes configuring advanced services, such as Quality of Service (QoS) for voice and the External Services Interface module.

Related Documents

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

- *AOS-W User Guide*
- *Alcatel Wireless LAN Switch Installation Guides*
- *Alcatel Access Point Installation Guides*
- *Release Notes*

Text Conventions

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

TABLE 1 Text Conventions

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>	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: # **send** *<text message>* 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 | Item B }	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Contacting Alcatel

Contact Center Online		
■	Main Site	http://www.alcatel.com/enterprise
■	Support Site	http://eservice.ind.alcatel.com
■	Email	support@ind.alcatel.com
Sales & Support Contact Center Telephone		
■	North America	1-800-995-2696
■	Latin America	1-877-919-9526
■	Europe	+33 (0) 38 85 56 92 9
■	Asia Pacific	+65 6586 1555
■	Worldwide	1-818-880-3500

Configuring Management Access

1

This chapter describes management utilities for an Alcatel wireless network.

This chapter describes the following topics:

- "Configuring SNMP" on page 2
- "Configuring Logging" on page 14
- "Creating Guest Accounts" on page 17

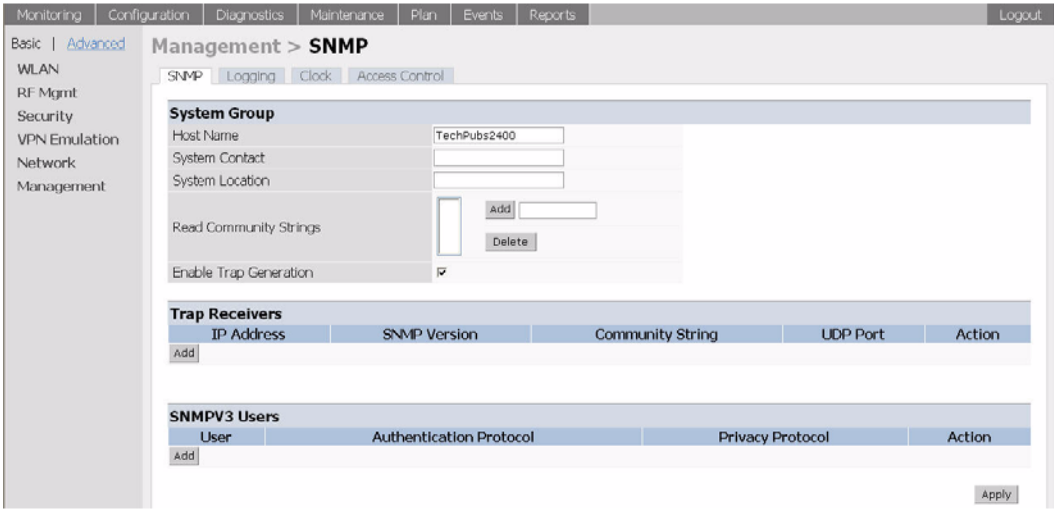
Configuring SNMP

Alcatel WLAN Switches 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.

SNMP for the WLAN Switch

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

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



Management > SNMP

System Group

Host Name	TechPubs2400
System Contact	
System Location	
Read Community Strings	
Enable Trap Generation	☑

Trap Receivers

IP Address	SNMP Version	Community String	UDP Port	Action

SNMPV3 Users

User	Authentication Protocol	Privacy Protocol	Action

Field	Description	Expected/recommended Value
Host Name	Host name of the WLAN Switch.	String to act as the host name for the WLAN Switch being configured.
System Contact	Name of the person who acts as the System Contact or administrator for the WLAN Switch.	System contacts name/ contact information.
System Location	String to describe the location of the WLAN Switch.	Description of the location of the WLAN Switch.

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 WLAN Switch.
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 WLAN Switch.	Select this option and configure the details of the trap receivers to enable generation of traps for various events by the Alcatel WLAN Switch.
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 WLAN Switch	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 the default port number if not modified by the user.

If you are using SNMPv3 for getting the values from the Alcatel WLAN Switch, follow the steps below to configure valid users for SNMPv3:

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

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

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

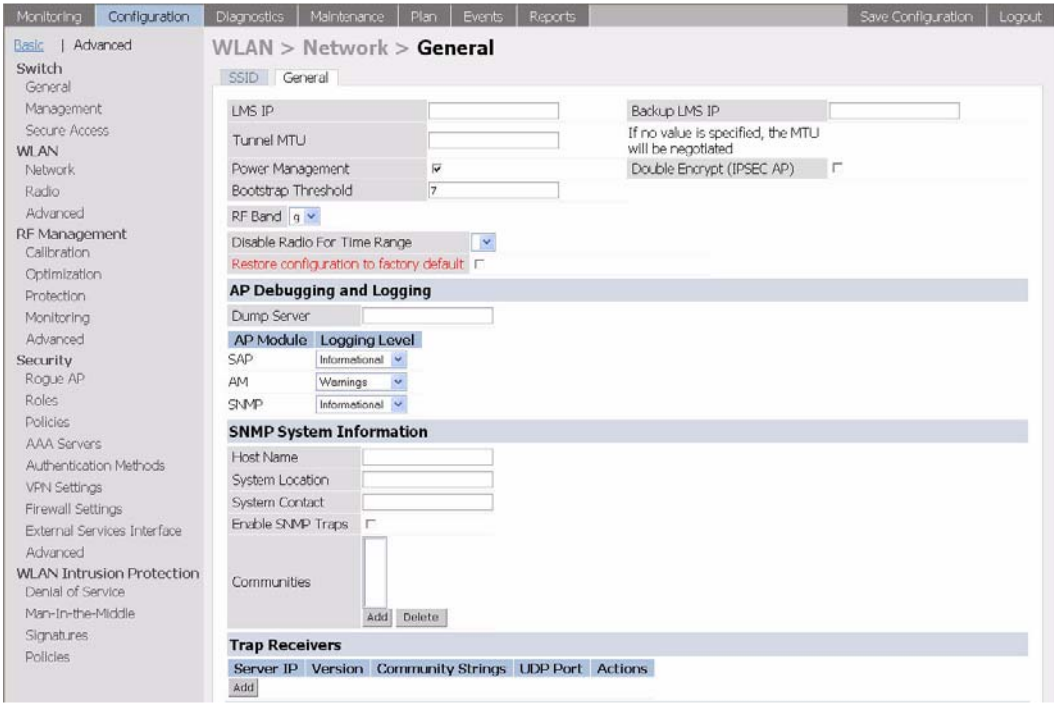
SNMP for Access Points

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 WLAN 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 > Advanced > WLAN > Network > General** page on the WebUI of the Master WLAN Switch. This page includes fields for configuring the SNMP parameters on all Access Points in the network.



WLAN > Network > **General**

LMS IP		Backup LMS IP	
Tunnel MTU		If no value is specified, the MTU will be negotiated	
Power Management	☑	Double Encrypt (IPSEC AP)	□
Bootstrap Threshold	7		
RF Band	g		
Disable Radio For Time Range			
Restore configuration to factory default	□		

AP Debugging and Logging

Dump Server

AP Module	Logging Level
SAP	Informational
AM	Warnings
SNMP	Informational

SNMP System Information

Host Name	
System Location	
System Contact	
Enable SNMP Traps	□
Communities	

Trap Receivers

Server IP	Version	Community Strings	UDP Port	Actions

2. Configure the basic SNMP parameters in the SNMP System Information area. The fields are similar to those for the WLAN Switch and are explained in the table below.

Field	Description	Expected/Recommended Values
Host Name	Host name for all Access Points in the network.	Any name to identify the devices as Alcatel APs.
System Location	Location for Access Points in the network	String to identify the location of the APs.
System Contact	Contact name or information for administrative contact.	String to identify administrative contact for all APs.
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.
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.
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 the default port number if not modified by the user.

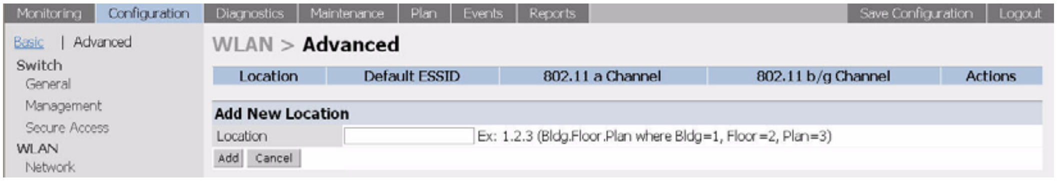
If you are using SNMPv3 for getting the values from the Alcatel WLAN Switch, follow the steps below to configure valid users for SNMPv3.

Field	Description	Expected/Recommended Values
User name	A string representing the name of the user.	A string value for the user name.
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.
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.
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).
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 > Advanced > WLAN > Advanced** page on the WebUI of the Master WLAN Switch.

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.



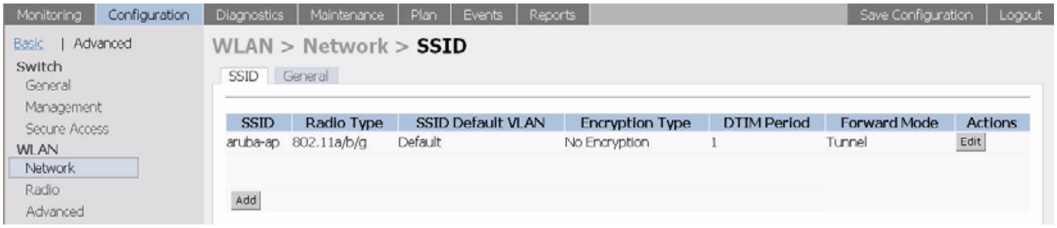
WLAN > Advanced

Location	Default ESSID	802.11 a Channel	802.11 b/g Channel	Actions

Add New Location

Location: Ex: 1.2.3 (Bldg.Floor.Plan where Bldg=1, Floor=2, Plan=3)

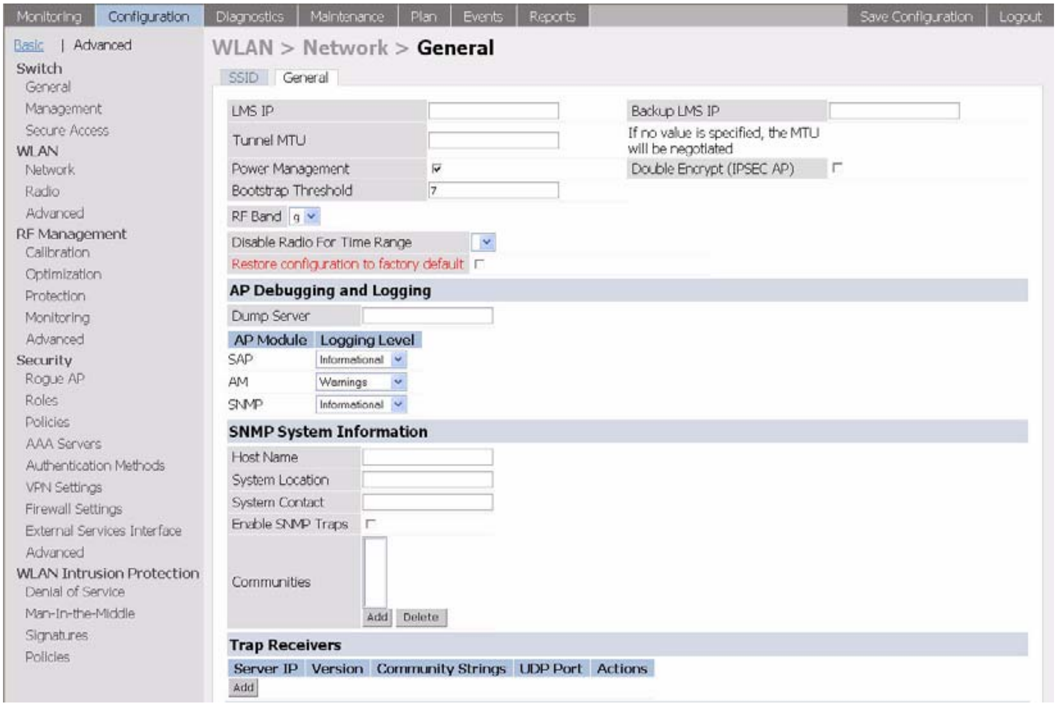
3. Navigate to **Configuration** > **Advanced** > **WLAN** > **Network** > **SSID** to configure the SSID for the Access Point:



WLAN > Network > SSID

SSID	Radio Type	SSID Default VLAN	Encryption Type	DTIM Period	Forward Mode	Actions
aruba-ap	802.11a/b/g	Default	No Encryption	1	Tunnel	Edit

4. Click the **General** tab to configure the SNMP parameters for the set of APs.



WLAN > Network > **General**

LMS IP		Backup LMS IP	
Tunnel MTU		If no value is specified, the MTU will be negotiated	
Power Management	☑	Double Encrypt (IPSEC AP)	□
Bootstrap Threshold	7		
RF Band	g		
Disable Radio For Time Range			
Restore configuration to factory default	□		

AP Debugging and Logging

Dump Server

AP Module	Logging Level
SAP	Informational
AM	Warnings
SNMP	Informational

SNMP System Information

Host Name	
System Location	
System Contact	
Enable SNMP Traps	□
Communities	

Trap Receivers

Server IP	Version	Community Strings	UDP Port	Actions

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

WLAN Switch Traps

The following is a list of key traps generated by the Alcatel WLAN Switch.

1. WLAN Switch IP changed.

Description: This indicates the WLAN Switch IP has been changed. The WLAN 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. WLAN Switch role changed

Description: This indicates that the WLAN Switch has transitioned from being a Master WLAN Switch to a Local WLAN 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 WLAN Switch on which the user event occurs. In other words this is a local event to the WLAN 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 WLAN Switch to the authentication server or some other problem related to the authentication server.

Priority Level: High.

5. Authentication server timed out

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 WLAN 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 WLAN 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 WLAN 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 WLAN 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 WLAN Switch.

Priority Level: Critical

11. Fan failure

Description: As the name indicates, this trap indicates a failure of the fan in the WLAN Switch.

Priority Level: Critical

12. Out of Range Voltage

Description: This trap indicates an out of range voltage being supplied to the WLAN Switch.

Priority Level: Critical

13. Out of Range temperature.

Description: This trap indicates an out of range operating temperature being supplied to the WLAN Switch.

Priority Level: Critical

14. Line card inserted/removed.

Description: These traps indicate that a Line Card has been inserted or removed from the WLAN Switch.

Priority Level: Critical.

15. Supervisor card inserted/removed.

Description: These traps indicate that a Supervisor card has been inserted or removed from the WLAN Switch

Priority Level: Critical

16. Power supply missing

Description: This trap indicates that one of the power supplies is missing.

Priority Level:. Critical.

Access Point/Air Monitor Traps

The following are the key traps that can be generated by the Alcatel Access Point or an Air Monitor:[1]

1. Unsecure AP detected.

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.

[1] For a complete list of traps, refer to the *Alcatel MIB Reference* (0500059).

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 crosses the High Watermark and then will only be triggered if 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

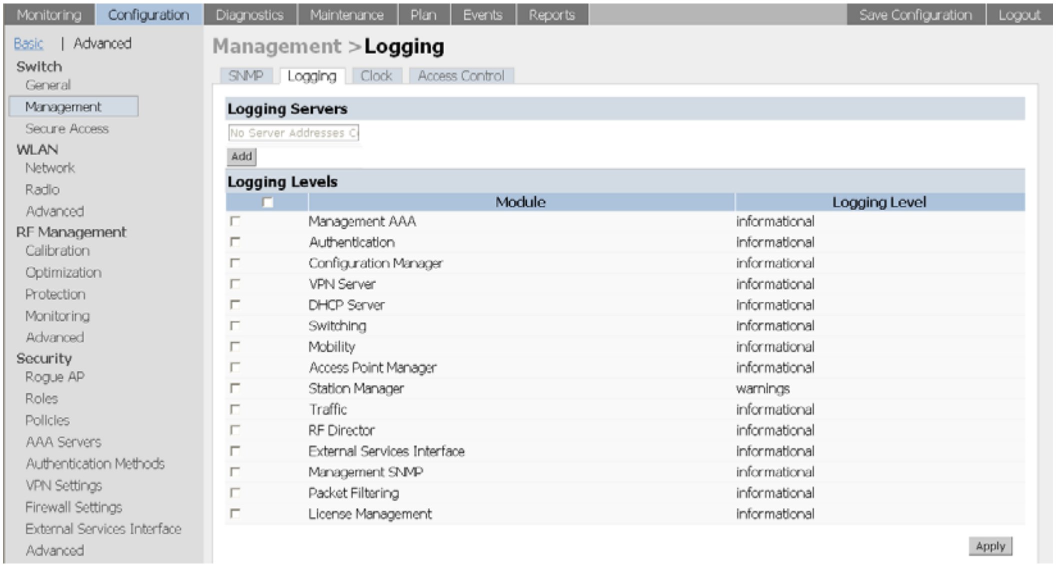
This section outlines the steps required to configure logging on an Alcatel WLAN Switch. The logging level can be set for each of the modules in the software system. The table below summarizes these modules:

Module	**Description**
Management AAA	The module responsible for authentication of management users (telnet/ssh/WebUI).
Authentication	The module responsible for authentication of wireless clients.

Configuration Manager	The module responsible for configuration changes in the Alcatel network and configuration synchronization amongst all Alcatel WLAN Switches.
VPN server	The module responsible for all VPN connections.
DHCP server	The DHCP server in the WLAN Switch.
Switching	The module responsible for all layer 2/3 switching functionality.
Mobility	The module responsible for inter- and intra-WLAN Switch mobility for wireless clients.
User	The module responsible for user state maintenance.
Access Point Manager	The module responsible for managing the Access Points in the network.
Station Manager	The module responsible for all wireless stations at a 802.11 level.
Traffic	A logical module to track traffic patterns to help troubleshooting.
RF Director	The monitor responsible for monitoring the wireless network for any rogues/intrusions etc.

You can configure the logging levels for each of these modules as well as the IP address of a syslog server to which the WLAN Switch can direct these logs. To configure logging:

1. Navigate to the **Configuration > Advanced > Switch > Management > Logging** page on the WebUI.



Management > **Logging**

Logging Servers

No Server Addresses C

Logging Levels

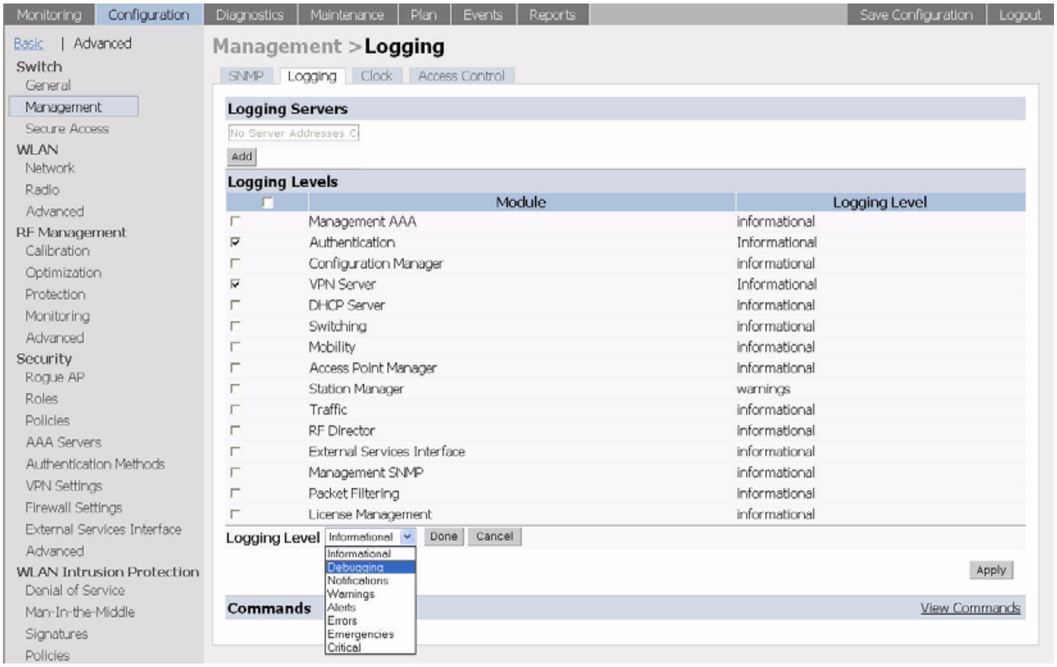
□	Module	Logging Level
□	Management AAA	informational
□	Authentication	informational
□	Configuration Manager	informational
□	VPN Server	informational
□	DHCP Server	informational
□	Switching	informational
□	Mobility	informational
□	Access Point Manager	informational
□	Station Manager	warnings
□	Traffic	informational
□	RF Director	informational
□	External Services Interface	informational
□	Management SNMP	informational
□	Packet Filtering	informational
□	License Management	informational

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.



Management > **Logging**

Logging Servers

Logging Levels

□	Module	Logging Level
□	Management AAA	informational
☑	Authentication	Informational
□	Configuration Manager	informational
☑	VPN Server	Informational
□	DHCP Server	informational
□	Switching	informational
□	Mobility	informational
□	Access Point Manager	informational
□	Station Manager	warnings
□	Traffic	informational
□	RF Director	informational
□	External Services Interface	informational
□	Management SNMP	informational
□	Packet Filtering	informational
□	License Management	informational

Logging Level: Informational

5. Click **Done** to make the modification.

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 *AOS-W System Messages Reference Guide*.

Creating Guest Accounts

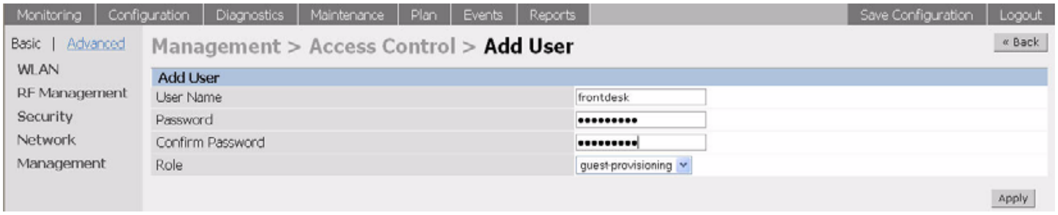
You can create a special administrative login that allows a user, such as a front desk receptionist, to create guest accounts on a WebUI page.

To create the user login:

1. Navigate to the **Configuration > Basic > Management > Access Control** page.

2. Click **Add**.

3. In the **Add User** page, enter the name that the user will log in with to access the guest account page.
4. Enter the password for the user login.
5. For **Role**, select **guest-provisioning** from the drop-down list.

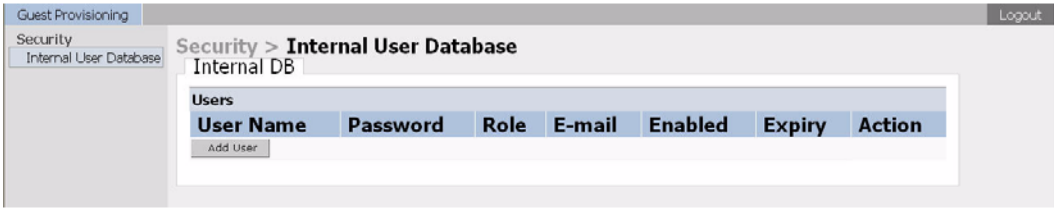


Management > Access Control > Add User

Add User	
User Name	frontdesk
Password	••••••••••
Confirm Password	••••••••••
Role	guest-provisioning

6. Click **Apply**.

When a user logs into the WebUI on the WLAN Switch (in a multi-WLAN Switch system, this must be the master WLAN Switch) using the login and password you just created, a special WebUI page is displayed that allows them to create guest accounts in the WLAN Switch’s internal database.



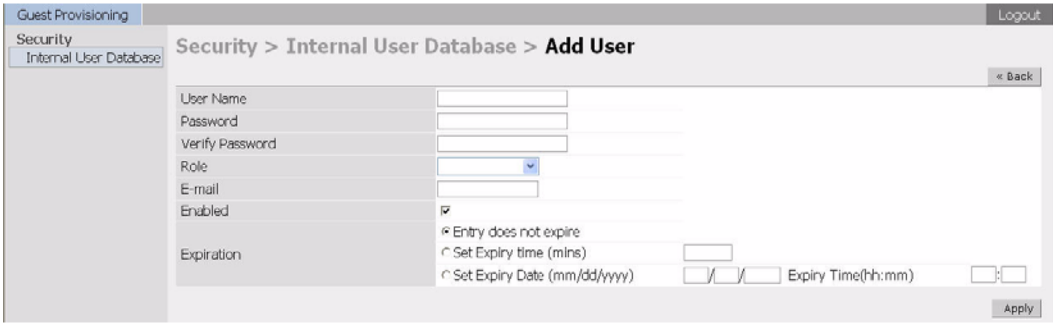
Security > Internal User Database

Internal DB

Users

User Name	Password	Role	E-mail	Enabled	Expiry	Action

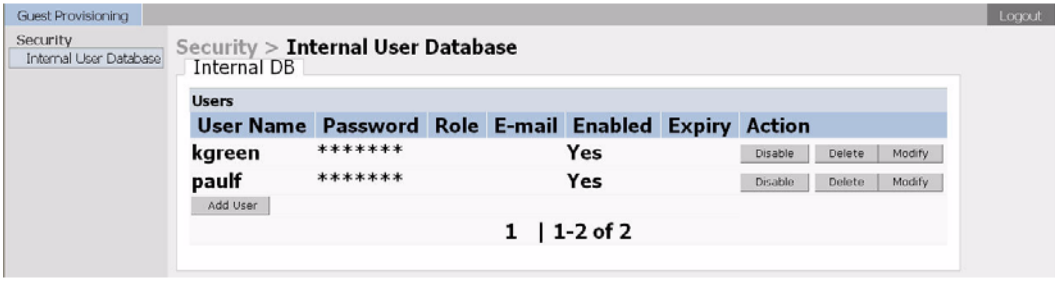
The user clicks **Add** to create a guest account:



Security > Internal User Database > **Add User**

User Name	
Password	
Verify Password	
Role	
E-mail	
Enabled	☑
Expiration	● Entry does not expire ○ Set Expiry time (mins) ○ Set Expiry Date (mm/dd/yyyy) / / Expiry Time(hh:mm) :

The user can then define a user name and password for the guest account and configure the expiration for the account. If the Policy Enforcement Firewall license is installed in the WLAN Switch, the user can also assign a role to the guest account. Clicking **Apply** adds the guest account to the database. The user can then disable, delete, or modify the guest account as needed.



Security > **Internal User Database**

Internal DB

Users

User Name	Password	Role	E-mail	Enabled	Expiry	Action
kgreen	*******			Yes		Disable Delete Modify
paulf	*******			Yes		Disable Delete Modify

1 | 1-2 of 2

NOTE: The special administrative login can assign any configured user role (not just the guest role) to the account. This can be useful for allowing contractors and out-of-town employees to have different network access privileges than other guests.

Managing Software Feature Licenses

2

AOS-W consists of a base software package with optional software modules that you can activate by installing one or more license keys. This chapter describes license types and how to install the licenses on your Alcatel WLAN Switch.

This chapter describes the following topics:

- "Alcatel Software Licenses" on page 21
- "The Software Licensing Process" on page 22
- "Additional Software License Information" on page 25
- "Getting Help with Licenses" on page 28

Alcatel Software Licenses

Alcatel product licenses enable the following software modules:

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

Software License Types

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

- **Permanent license** - This type of license permanently enables the desired software module on a specific Alcatel WLAN Switch. You obtain permanent licenses through the sales order process only. Permanent software license certificates are printed documents that are physically mailed to you; you will also receive the license information in an e-mail confirmation.

- **Evaluation license** - This type of license allows you to evaluate the unrestricted functionality of a software module on a specific WLAN Switch for 90 days (in three 30-day increments) without requiring you to purchase a permanent software license.

At the end of the 90-day period, you must apply a permanent license to re-enable this software module on the WLAN Switch. Evaluation software license certificates are only available in electronic form and are e-mailed to you.

The Software Licensing Process

A software license (permanent or evaluation) is unlocked individually by module type and is applied to each WLAN Switch as a *software license key*. A software license key is a unique alphanumerical string created for an individual WLAN Switch and is only valid for the designated WLAN Switch.

To enable a software license feature on your WLAN Switch:

1. Obtain a valid Alcatel software license certificate for the feature from your sales account manager or authorized reseller.
2. Locate the system serial number (or Supervisor Card serial number) of the WLAN Switch to which you wish to apply the software license.
3. Use the software license certificate ID and the system serial number to obtain a software license key from the Alcatel Software License Management Web site at http://eservice.ind.alcatel.com/oaw.
4. Apply the software license key by using the WebUI to the WLAN Switch on which you wish to apply the license. Log in to the WebUI and navigate to **Maintenance > License Management.** Enter the software license key, and click **Apply**.
5. You must now reboot your WLAN Switch in order for the new feature to become available.

See the following sections for details on each step.

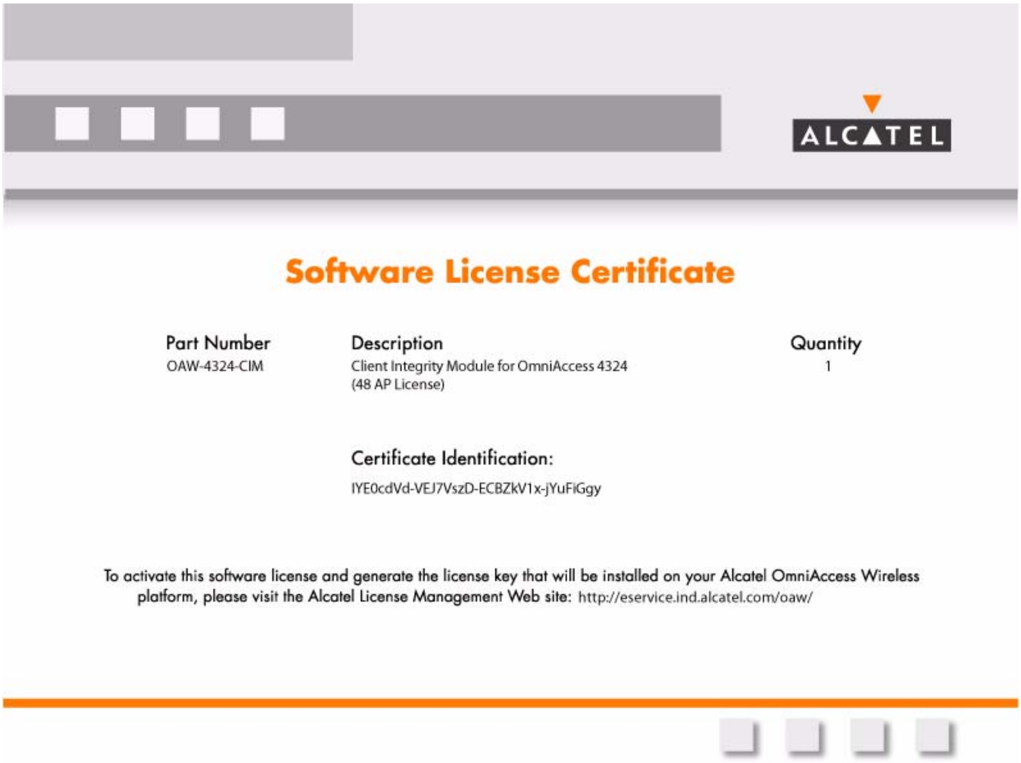
Obtaining a Software License Certificate

To obtain either a permanent or evaluation software license, 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.

Software License Certificates

The software license certificate is a software-module and WLAN Switch-class specific document that states:

- The orderable part number for the license
- A description of the software module type and Alcatel WLAN Switch for which it is valid
- A unique, 32-character alphanumerical string that can be used to access the license management Web site and which, in conjunction with the serial number of an Alcatel WLAN Switch or Supervisor Card, generates a unique software license key



Software License Certificate

Part Number	Description	Quantity
OAW-4324-CIM	Client Integrity Module for OmniAccess 4324 (48 AP License)	1

Certificate Identification:

IYE0cdVd-VEJ7VszD-ECBZkV1x-jYuFiGgy

To activate this software license and generate the license key that will be installed on your Alcatel OmniAccess Wireless platform, please visit the Alcatel License Management Web site: http://eservice.ind.alcatel.com/oaw/

In addition to the printed software license certificate, you will also receive an e-mail confirmation with the certificate ID.

Locating the System Serial Number

The serial number of a WLAN Switch is unique. You can find it as follows:

- System serial number that is specified on the rear of an Alcatel WLAN Switch chassis
- System serial number of the Supervisor Card (*not* the chassis) for an Alcatel modular 6000 series WLAN Switch

You can obtain system serial numbers by physically inspecting the chassis or card or by using the WebUI (by navigating to the **Switch > Inventory** page).

NOTE: To physically inspect the system serial number on a Supervisor Card, you need to remove the card from the WLAN Switch chassis, which can result in network down time.

Obtaining a Software License Key

To obtain a software license key, you must log in to the Alcatel License Management Web site at http://eservice.ind.alcatel.com/oaw.

If you are a first time user of the licensing site, you can use the software license certificate ID number to log in initially and request a user account. If you already have a user account, log in to the site.

Once logged in, you are presented with three options:

- **Activate a Certificate** - to activate a new certificate and create the software license key that you will apply to your WLAN Switch
- **Transfer a Certificate** - to transfer a software license certificate ID from one WLAN Switch to another (for example, transferring licenses to a spare system)
- **List Your Certificates** - to view all currently available and active software license certificates for your account

To create a software license key:

1. Select **Activate a Certificate.**
2. Enter the certificate ID number and the system serial number of the WLAN Switch to which you wish to apply the license.
3. Review the license agreement and select **Yes** to accept the agreement.
4. Click **Activate it**. A copy of the transaction and the software license key will be emailed to you at the e-mail address you entered for your user account.

NOTE: The software license key is *only* valid for the system serial number for which you activated the certificate.

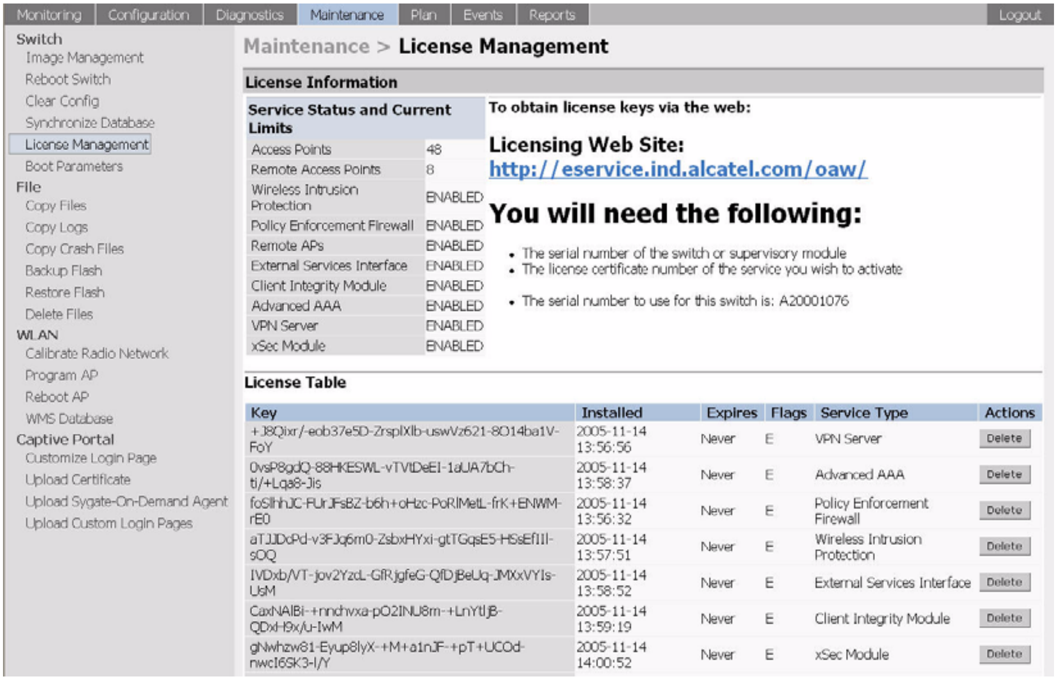
Applying the Software License Key

To enable the software module and functionality, you must now apply the software license key to your Alcatel WLAN Switch:

1. Using the WebUI, log into your WLAN Switch with Administrative access rights.
2. Navigate to **Maintenance > License Management** to display system license information and the License Table.

3. Copy the software license key that was emailed to you, and paste it into the **Add New License Key** field. Click **Add** to apply the license key.

4. You must now reboot your WLAN Switch for the new feature to become available.



Maintenance > License Management

License Information

Service Status and Current Limits	
Access Points	48
Remote Access Points	8
Wireless Intrusion Protection	ENABLED
Policy Enforcement Firewall	ENABLED
Remote APs	ENABLED
External Services Interface	ENABLED
Client Integrity Module	ENABLED
Advanced AAA	ENABLED
VPN Server	ENABLED
xSec Module	ENABLED

To obtain license keys via the web:

Licensing Web Site:
http://eservice.ind.alcatel.com/oaw/

You will need the following:

- The serial number of the switch or supervisory module
- The license certificate number of the service you wish to activate
- The serial number to use for this switch is: A20001076

License Table

Key	Installed	Expires	Flags	Service Type	Actions
+J8Qixr/-eob37e5D-ZrsplXlb-uswVz621-8O14ba1V-FoY	2005-11-14 13:56:56	Never	E	VPN Server	Delete
0vsP8gdQ-88HKESWL-vTVtDeEI-1aUA7bCh-ti/+Lqa8-Jis	2005-11-14 13:58:37	Never	E	Advanced AAA	Delete
foSlhhJC-FUrJFsBZ-b6h+oHzc-PoRlMetL-frK+ENWM-rE0	2005-11-14 13:56:32	Never	E	Policy Enforcement Firewall	Delete
aTJJDdPd-v3FJq6m0-ZsbxHYxi-gtTGqsE5-HSsEfIIl-sOQ	2005-11-14 13:57:51	Never	E	Wireless Intrusion Protection	Delete
IVDxb/VT-jov2YzdL-GfRjgfeG-QfDjBeUq-JMXxVYIs-UsM	2005-11-14 13:58:52	Never	E	External Services Interface	Delete
CaxNAlBi-+nndhvxa-pO2INU8m-+LnYtljB-QDxH9x/u-IwM	2005-11-14 13:59:19	Never	E	Client Integrity Module	Delete
gNwhzw81-Eyup8lyX-+M+a1nJF-+pT+UCOd-nwcI6SK3-l/Y	2005-11-14 14:00:52	Never	E	xSec Module	Delete

CAUTION: When license keys are applied on an Alcatel WLAN Switch, abnormal tampering of the device’s system clock (setting the system clock back by 2 hours or more) results in the disabling of software licensed modules and their supported features. This can affect network services.

Additional Software License Information

This section includes other information about software licenses.

Permanent Licenses

Once installed, permanent software licenses report the software module as **Enabled** in the WebUI for the WLAN Switch. These license types never expire, even when you upgrade the AOS-W software to a newer version.

Evaluation Licenses

Evaluation licenses support the following behavior:

- Evaluation licenses are limited to three 30-day periods. Evaluation licenses time individually; evaluation licenses for various software modules will expire at different times.
- During evaluation, full functionality relating to a specific software module is available to the user.
- During evaluation, the WebUI for the WLAN Switch reports that software licenses are expiring.
- When you log in through the CLI, the time remaining on the licensing term displays as shown below:

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

(alcatel) >
```

NOTE: If multiple evaluation licenses are running concurrently on the same WLAN Switch, the reported expiration time is for the licensed feature with the least amount of time remaining.

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

When an evaluation period expires, the following occurs:

- The WLAN Switch automatically backs up the startup configuration and reboots itself at midnight (according to the system clock).
- All permanent licenses are unaffected. The expired evaluation licensed feature is no longer available and is shown as **Expired** in the WebUI.

You can reapply a software license key to the WLAN Switch only if the 90-day evaluation time for the feature has not been reached. If the maximum time for the evaluation license has been reached, the startup configuration is backed up, however, you can only re-enable the feature by installing a permanent license key.

Deleting a License Key

To remove a license from a system:

1. Navigate to the **Maintenance > License Management** page.
2. Click **Delete** to the right of the feature entry in the License Table.

   If a feature is a fully-licensed feature, deleting the feature results in the feature key being displayed. If a feature is under the trial period of an evaluation license, no key is generated when the feature is deleted.

NOTE: If you are unable to delete a license key on a disabled or damaged system that is subsequently returned to the factory, you can reinstall the license key on another machine. The factory will take the necessary steps to remove the license key from the returned system.

Moving Licenses

It may become necessary to move licenses from one chassis to another or simply delete the license for future use. To move licenses, delete the license from the chassis as described in "Deleting a License Key" on page 27. Then install the license key on the new WLAN Switch as described in "Applying the Software License Key" on page 24.

CAUTION: The ability to move a license from one WLAN Switch to another is provided to allow customers maximum flexibility in managing their organization's network and to minimize the need to contact Alcatel customer support. License fraud detection is monitored and enforced by Alcatel. Abnormally high volumes of license transfers for the same license certificate to multiple WLAN Switches can indicate breach of the Alcatel end user software license agreement and will be investigated.

Resetting the WLAN Switch

The following sections describe the effects of rebooting a WLAN Switch or resetting the configuration on software licenses.

Rebooting a WLAN Switch

Rebooting or resetting a WLAN Switch has no effect on either permanent or evaluation licenses.

Resetting the WLAN Switch Configuration

Issuing the **`write erase`** command on a WLAN Switch running software licenses does *not* affect the license key management database on the WLAN Switch.

Issuing the **`write erase all`** command resets the WLAN Switch to factory defaults, and deletes all databases on the WLAN Switch including the license key management database. You must reinstall all previously-installed license keys.

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://eservice.ind.alcatel.com/oaw.

Volume 8

Configuring Advanced Services

AOS-W User Guide

Release 2.5.3

ALCATEL

Copyright

Specifications in this manual are subject to change without notice.

Originated in the USA.

Trademarks

AOS-W, Alcatel 4308, Alcatel 4324, Alcatel 6000, Alcatel 41, Alcatel 60/61/65, Alcatel 70, and Alcatel 80 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

This preface includes the following information:

- An overview of the contents of 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

The *AOS-W User Guide* is now in eight separate volumes for easier download and information access. The volumes are as follows:

- Volume 1 contains an overview of the OmniAccess System.
- Volume 2 describes how to install the OmniAccess System in a wired network.
- Volume 3 describes WLAN configuration, including remote Access Points.
- Volume 4 describes wireless encryption and authentication configuration.
- Volume 5 describes configuring multi-WLAN switch environments.
- Volume 6 describes intrusion prevention configuration.
- Volume 7 describes managing the OmniAccess System.
- Volume 8 (this volume) describes configuring advanced services, such as Quality of Service (QoS) for voice and the External Services Interface module.

Related Documents

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

- *AOS-W User Guide*
- *Alcatel Wireless LAN Switch Installation Guides*
- *Alcatel Access Point Installation Guides*
- *Release Notes*

Text Conventions

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

TABLE 1 Text Conventions

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>	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: # **send** *<text message>* 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 | Item B }	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Contacting Alcatel

Contact Center Online	
Main Site	http://www.alcatel.com/enterprise
Support Site	http://eservice.ind.alcatel.com
Email	support@ind.alcatel.com

Sales & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
Europe	+33 (0) 38 85 56 92 9
Asia Pacific	+65 6586 1555
Worldwide	1-818-880-3500

Configuring QoS for Voice 1

This chapter outlines the steps required to configure QoS on an Alcatel WLAN Switch 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.

This chapter describes the following topics:

Roles and Policies for Voice Traffic

The central concept of an Alcatel WLAN Switch 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 "Configuring Roles and Policies" in Volume 4 of the *AOS-W User Guide* for more details).

In an Alcatel system, you 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 Roles and Policies" in Volume 4 of the *AOS-W User Guide* 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.

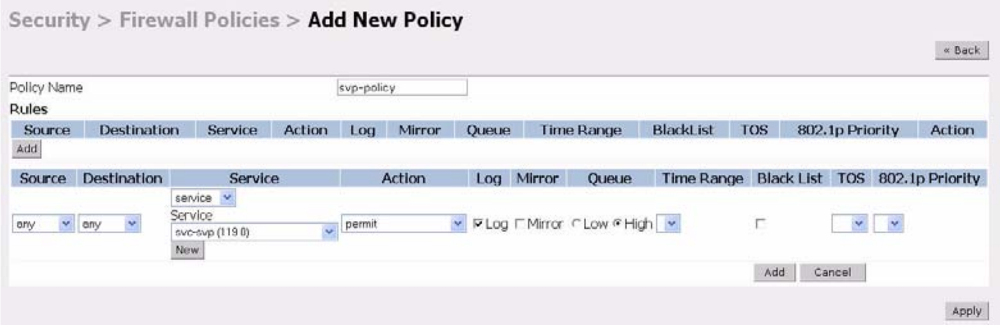
Configuring QoS for SVP

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 "Configuring Roles and Policies" in Volume 4 of the *AOS-W User Guide* 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 WLAN 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 high priority as show below.



Security > Firewall Policies > **Add New Policy**

« Back

Policy Name: svp-policy

Rules

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Action

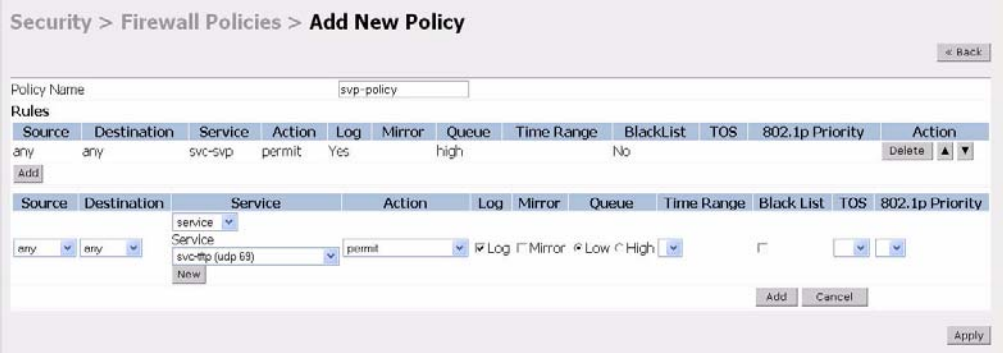
Add

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Black List	TOS	802.1p Priority
any	any	service Service svc-svp (119 0) New	permit	☑ Log	□ Mirror	○ Low ● High		□		

Add Cancel

Apply

3. Create a rule to allow TFTP traffic with low priority to allow for software/firmware upgrades of the SVP phones/devices.



Security > Firewall Policies > **Add New Policy**

« Back

Policy Name: svp-policy

Rules

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Action
any	any	svc-svp	permit	Yes		high		No			Delete ▲ ▼

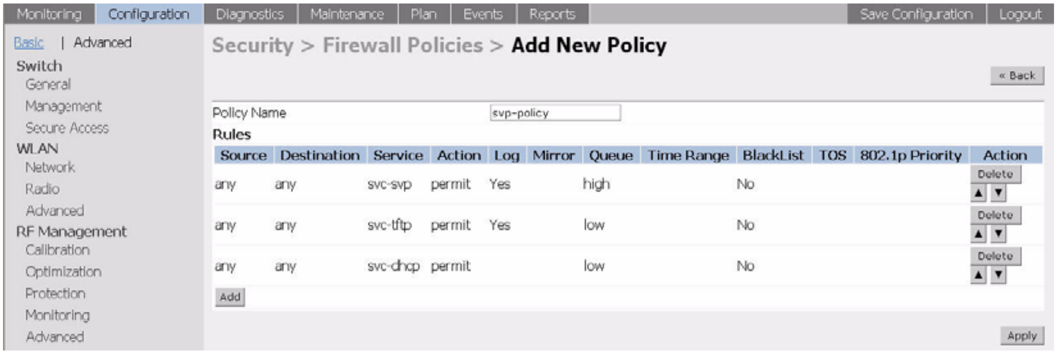
Add

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Black List	TOS	802.1p Priority
any	any	service Service svc-tftp (udp 69) New	permit	☑ Log	□ Mirror	● Low ○ High		□		

Add Cancel

Apply

4. Create a rule to allow DHCP traffic with low priority to allow the phones to use DHCP.



Security > Firewall Policies > **Add New Policy**

« Back

Policy Name: svp-policy

Rules

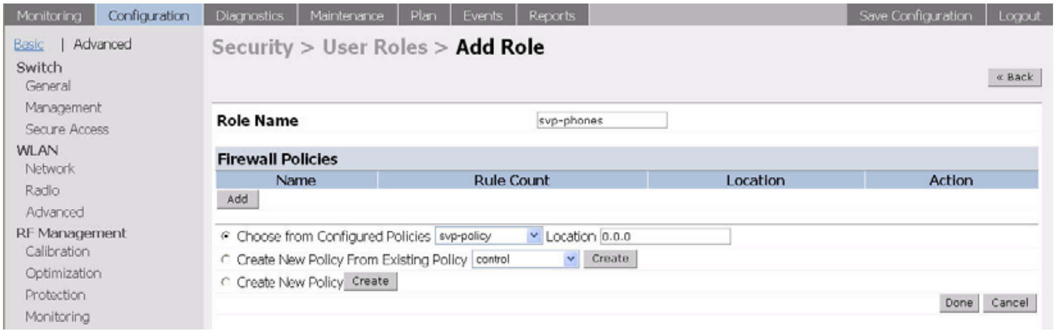
Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Action
any	any	svc-svp	permit	Yes		high		No			Delete ▲ ▼
any	any	svc-tftp	permit	Yes		low		No			Delete ▲ ▼
any	any	svc-dhcp	permit			low		No			Delete ▲ ▼

Add

Apply

5. Create a role for SVP phones called *"svp-phones"* and assign the policy *"svp-policy"* to it. (Refer to "Configuring Roles and Policies" in Volume 4 of the *AOS-W User Guide* for more details on adding and configuring a firewall

role).



Security > User Roles > **Add Role**

Role Name: svp-phones

Firewall Policies

Name	Rule Count	Location	Action

● Choose from Configured Policies: svp-policy Location: 0.0.0

○ Create New Policy From Existing Policy: control

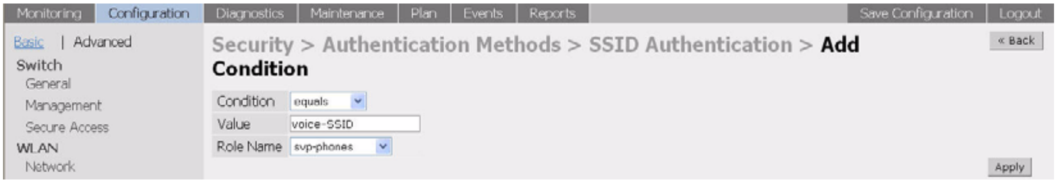
○ Create New Policy

6. 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:

   SSID based role derivation:

   A. Navigate to **Configuration** > **Advanced** > **Security** > **Authentication Methods** > **SSID** page.

   B. 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).



Security > Authentication Methods > SSID Authentication > **Add Condition**

Condition: equals

Value: voice-SSID

Role Name: svp-phones

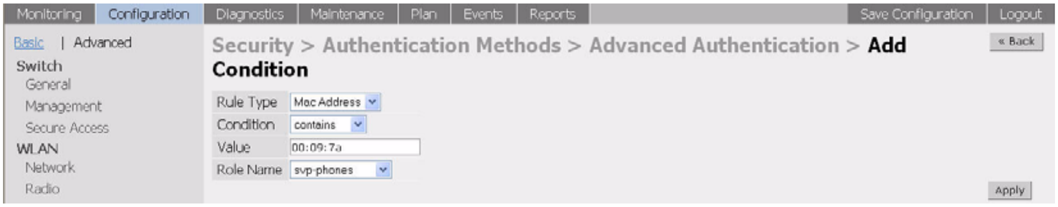
   C. Click **Apply** to apply the configuration.

   NOTE: The changes will not take effect until this step is completed.

   OUI based role derivation:

   A. Navigate to **Configuration** > **Advanced** > **Security** > **Authentication Methods** > **Advanced**.

B. 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.



Security > Authentication Methods > Advanced Authentication > **Add Condition**

Rule Type: Mac Address
Condition: contains
Value: 00:09:7a
Role Name: svp-phones

C. Click **Apply** to apply this configuration.

NOTE: Note: The changes will not take effect until this step is completed.

For deployments where there is expected to be considerable delay between the WLAN 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 WLAN Switch is an optimization that allows AOS-W to take better decisions.)

To do this, access the CLI of the WLAN Switch (using the console connection or by performing a Telnet/SSH into the WLAN Switch) and using the following commands:

```
(WLAN_Switch) (config) #ap location 0.0.0
(WLAN_Switch) (sap-config location 0.0.0) #local-probe-response enable
(WLAN_Switch) (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 temporary lost of connectivity with the Alcatel WLAN Switch.

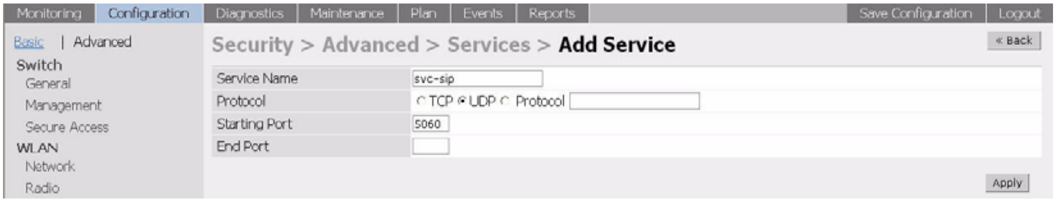
Configuring QoS for SIP

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.

   A. Navigate to **Configuration** > **Advanced** > **Security** > **Advanced**.

B. 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”.



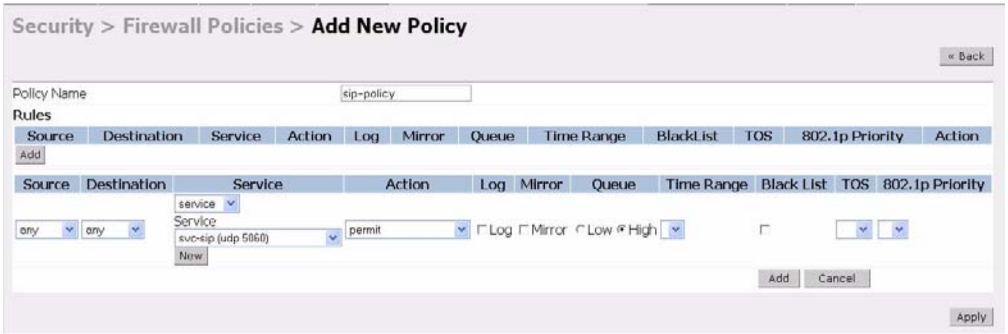
Security > Advanced > Services > Add Service

Service Name	svc-sip
Protocol	○ TCP ● UDP ○ Protocol
Starting Port	5060
End Port	

C. 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 Roles and Policies” in Volume 4 of the *AOS-W User Guide* 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.



Security > Firewall Policies > **Add New Policy**

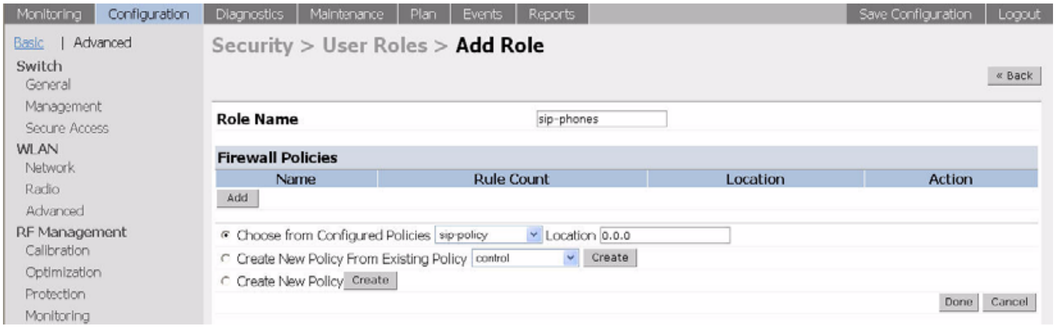
Policy Name: sip-policy

Rules

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Action

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Black List	TOS	802.1p Priority
any	any	service Service svc-sip (udp 5060) New	permit	☐ Log	☐ Mirror	○ Low ● High		☐		

3. Create a role for SIP phones called *"sip-phones"* and assign the policy *"sip-policy"* to it.



Security > User Roles > **Add Role**

Role Name: sip-phones

Firewall Policies

Name	Rule Count	Location	Action

● Choose from Configured Policies: sip-policy — Location: 0.0.0

○ Create New Policy From Existing Policy: control — Create

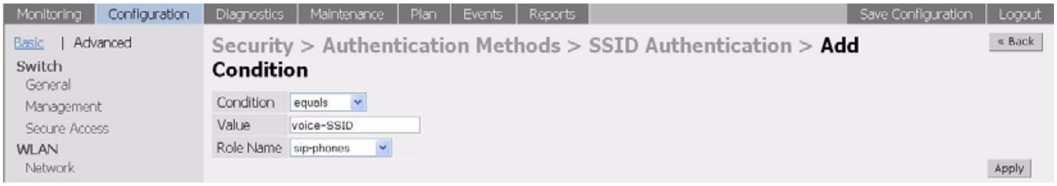
○ Create New Policy — Create

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:

SSID based role derivation:

A. Navigate to **Configuration > Advanced > Security > Authentication Methods > SSID**.

B. 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).



Security > Authentication Methods > SSID Authentication > **Add Condition**

Condition	equals
Value	voice-SSID
Role Name	sip-phones

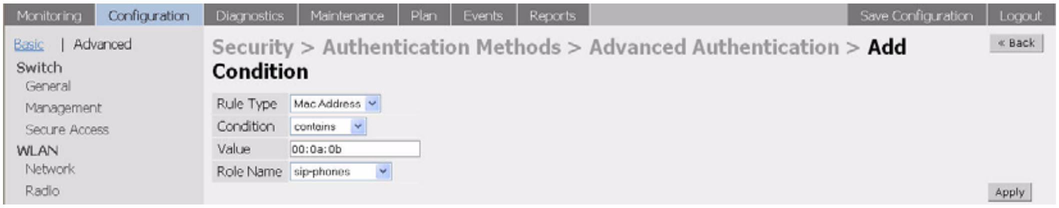
C. Click **Apply** to apply this configuration.

NOTE: The changes will not take effect until this step is completed

OUI based role derivation:

A. Navigate to **Configuration** > **Advanced** > **Security** > **Authentication Methods** > **Advanced**.

B. 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.



Security > Authentication Methods > Advanced Authentication > **Add Condition**

Rule Type	Mac Address
Condition	contains
Value	00:0a:0b
Role Name	sip-phones

C. Click **Apply** to apply this configuration.

NOTE: The changes will not take effect until this step is completed.

External Services Interface 2

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"

This chapter describes the following topics:

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.

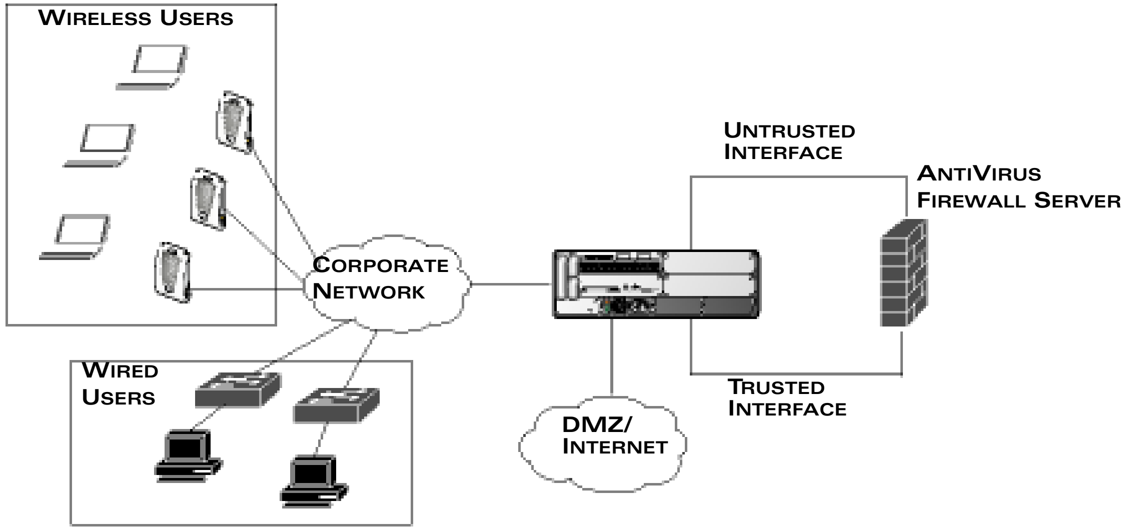


FIGURE 2-1 The Alcatel-Fortinet Topology

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 WLAN Switch over the existing network.

The Alcatel WLAN 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 WLAN Switch and the AntiVirusFirewall (AVF) server device. The Alcatel WLAN 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 WLAN Switch and the AntiVirusFirewall (AVF) server device. The Alcatel WLAN 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.

[1] In AOS-W 2.5, the only AVF server supported is Fortinet.

The Alcatel WLAN 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 (available from Sygate) on Sygate integrated solutions for more details on this solution.

Load Balancing

The Alcatel WLAN 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 WLAN 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.

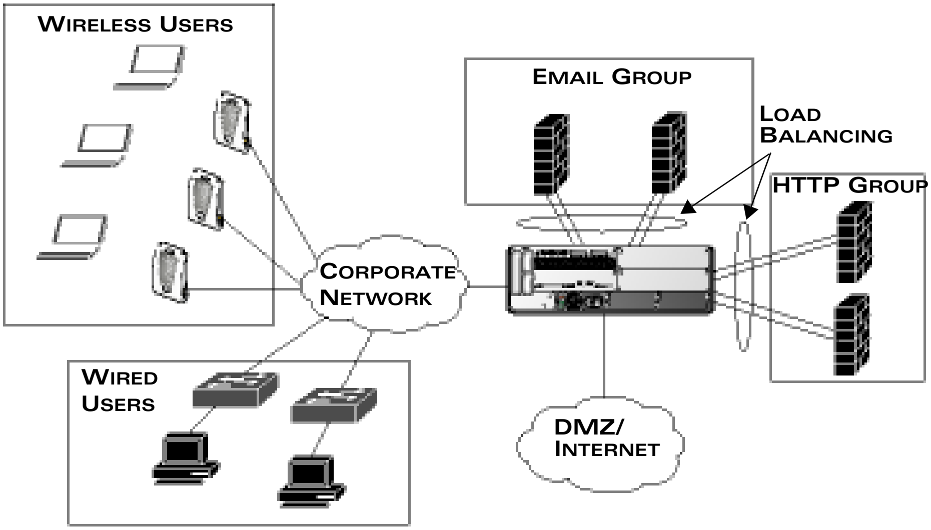


FIGURE 2-2 Load Balancing Groups

Configuring the Alcatel ESI

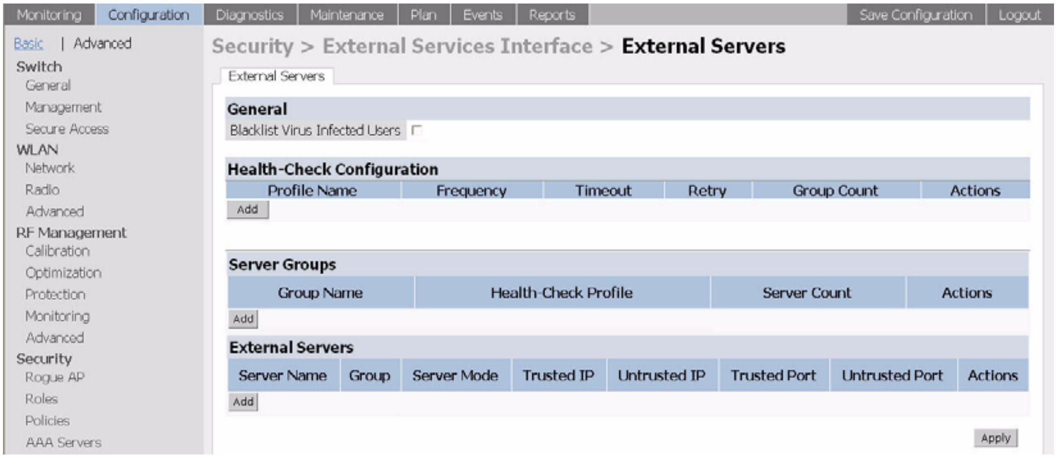
This section describes the relevant configuration required on the Alcatel WLAN Switch to integrate with a AntiVirusFirewall (AVF) server appliance. Refer to the User Guide for more details on configuring the Alcatel WLAN Switch.

There are two sections to configure on the Alcatel WLAN 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 WLAN Switch to redirect the different types of traffic to different “server groups”

Configuring the ESI Servers

To configure the ESI servers on the Alcatel WLAN Switch:

1. Navigate to the **Configuration > Advanced > Security > External Services Interface** page on the WebUI.



Security > External Services Interface > External Servers

General

Blacklist Virus Infected Users □

Health-Check Configuration

Profile Name	Frequency	Timeout	Retry	Group Count	Actions

Server Groups

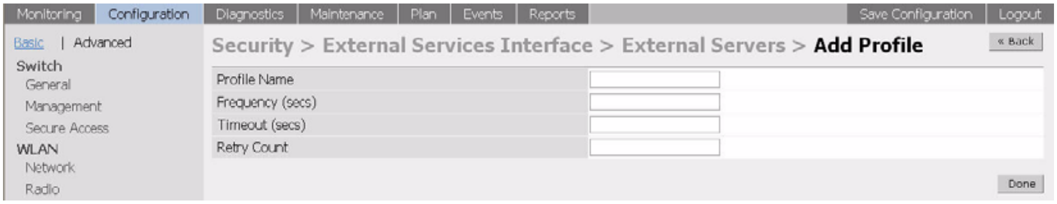
Group Name	Health-Check Profile	Server Count	Actions

External Servers

Server Name	Group	Server Mode	Trusted IP	Untrusted IP	Trusted Port	Untrusted Port	Actions

2. To configure a health check profile, click **Add** in the **Health Check Configuration** section. Enter a **Profile Name**.

To change an existing profile, select it, and click **Edit**.



Security > External Services Interface > External Servers > **Add Profile**

Profile Name
Frequency (secs)
Timeout (secs)
Retry Count

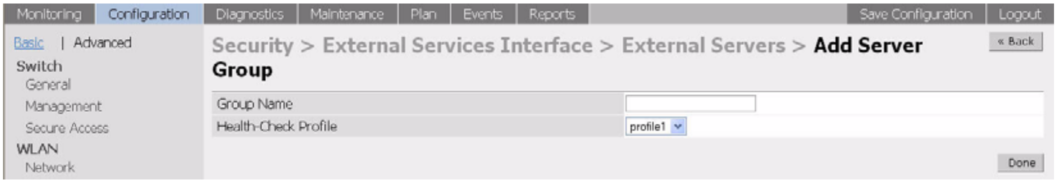
Provide the following details:

- **Frequency (secs)**—Indicates how often the Alcatel WLAN Switch will attempt to monitor to see if the server is up and running.
- **Timeout (secs)**—Indicates the number of seconds the Alcatel WLAN Switch will wait for a response to its health check query before marking the health check as failed.
- **Retry count**—Is the number of failed health checks after which the Alcatel WLAN Switch will mark the server as being down.

3. Click **Done** when you are finished.

4. To configure a server group, click **Add** in the **Server Groups** section. Enter a **Group Name** and specify the required health check profile for this server group.

   To change an existing group, select it, and click **Edit**.



Security > External Services Interface > External Servers > **Add Server Group**

Group Name
Health-Check Profile: profile1

5. Click **Done** when you are finished.

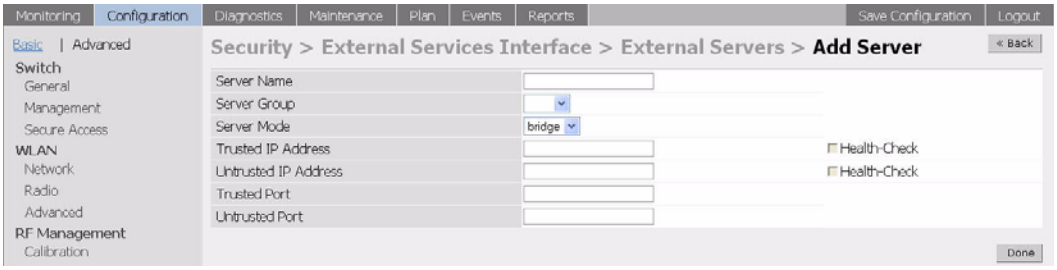
6. To add an AntiVirusFirewall (AVF) server, click **Add** in the **External Servers** section.

   Provide the following details:

   - The device/server name.
   - Assign this server to a group from the existing configured groups.
   - Choose the mode as bridge/route as your topology requires. Refer to the description above to understand the differences between the two modes.
   - For bridge mode, enter the trusted port and un-trusted port as defined earlier.

- For route mode, enter the IP addresses of the trusted and un-trusted interfaces on the AntiVirusFirewall (AVF) server device as defined earlier.

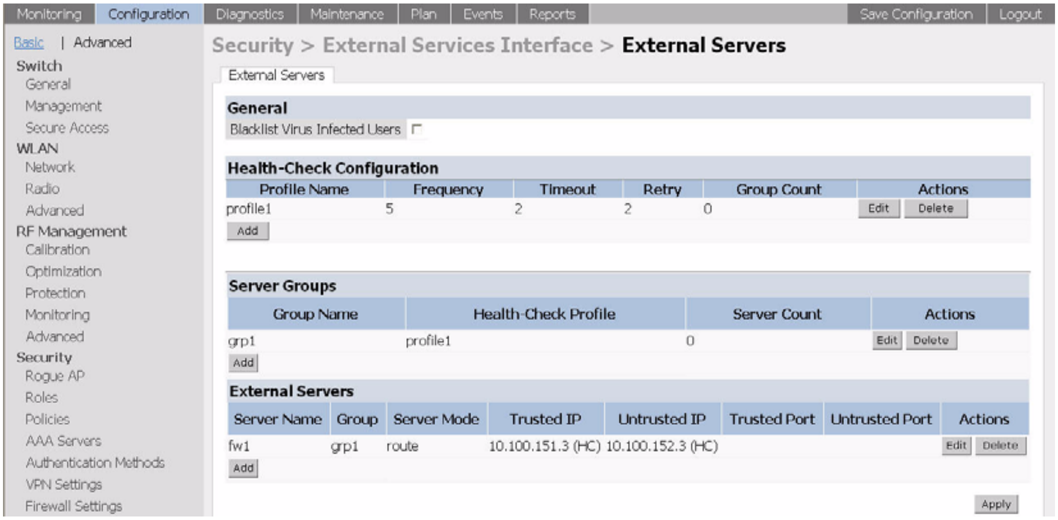
7. Click **Done** when you are finished.



Security > External Services Interface > External Servers > **Add Server**

Server Name		
Server Group		
Server Mode	bridge	
Trusted IP Address		□ Health-Check
Untrusted IP Address		□ Health-Check
Trusted Port		
Untrusted Port		

8. To apply the configuration (changes), click **Apply**. (The configuration will not take effect until you click **Apply**.)



Security > External Services Interface > **External Servers**

General

Blacklist Virus Infected Users □

Health-Check Configuration

Profile Name	Frequency	Timeout	Retry	Group Count	Actions
profile1	5	2	2	0	Edit Delete

Server Groups

Group Name	Health-Check Profile	Server Count	Actions
grp1	profile1	0	Edit Delete

External Servers

Server Name	Group	Server Mode	Trusted IP	Untrusted IP	Trusted Port	Untrusted Port	Actions
fw1	grp1	route	10.100.151.3 (HC)	10.100.152.3 (HC)			Edit Delete

Configuring the User Policy

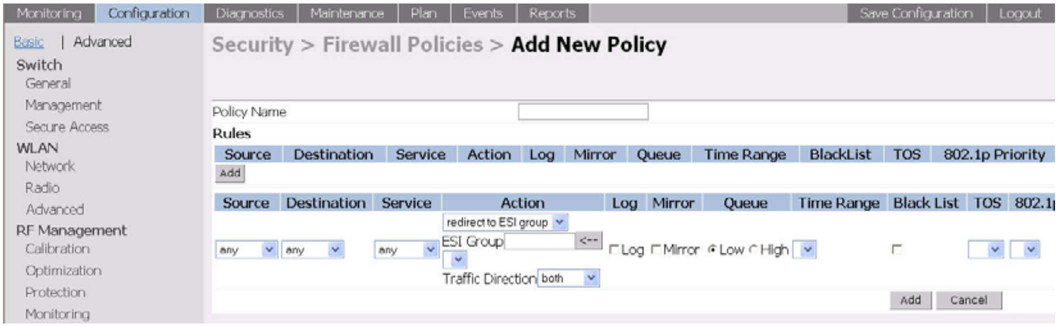
1. To configure user roles to redirect the required traffic to the server(s), navigate to the **Configuration > Advanced > Security > Policies** page.

2. To add a new policy, click **Add**, then enter a name for the policy.

   To change an existing policy, select it, and click **Edit**.

3. To add a new rule, click **Add**.

4. Choose parameters such as source, destination, service in the same way as other firewall policy rules.
   - Select the **redirect to ESI group** option from the drop down list as the **Action**.
   - Select the appropriate ESI-group. (See "Configuring the ESI Servers" on page 12.)
   - Specify the direction of the traffic. **Forward** refers to the direction of traffic from the (untrusted) client or user to the (trusted) server (such as the HTTP server or Email server).



Security > Firewall Policies > **Add New Policy**

Policy Name

Rules

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Black List	TOS	802.1
any	any	any	redirect to ESI group ESI Group <-- Traffic Direction both	□ Log	□ Mirror	● Low ○ High		□		

5. To add this rule to the policy, click **Add**.

6. Repeat the steps to configure the redirection policy for all required services/protocols (HTTP, HTTPS, SMTP, and POP3).

7. To apply the configuration (changes), click **Apply**. (The configuration will not take effect until you click **Apply**.)

8. Refer to "Configuring Roles and Policies" in Volume 4 of the *AOS-W User Guide* for directions on how to apply a policy to a user role.

Example Routed ESI Topology

This section introduces the configuration for a sample route mode topology using the Alcatel WLAN Switch and the Fortinet Anti-Virus gateways. In route mode, the trusted and untrusted interfaces between the WLAN Switch and the Fortinet gateways are on different subnets. An example topology is shown below in Figure 2-3.

NOTE: ESI with Fortinet Anti-Virus gateways is only supported in route mode.

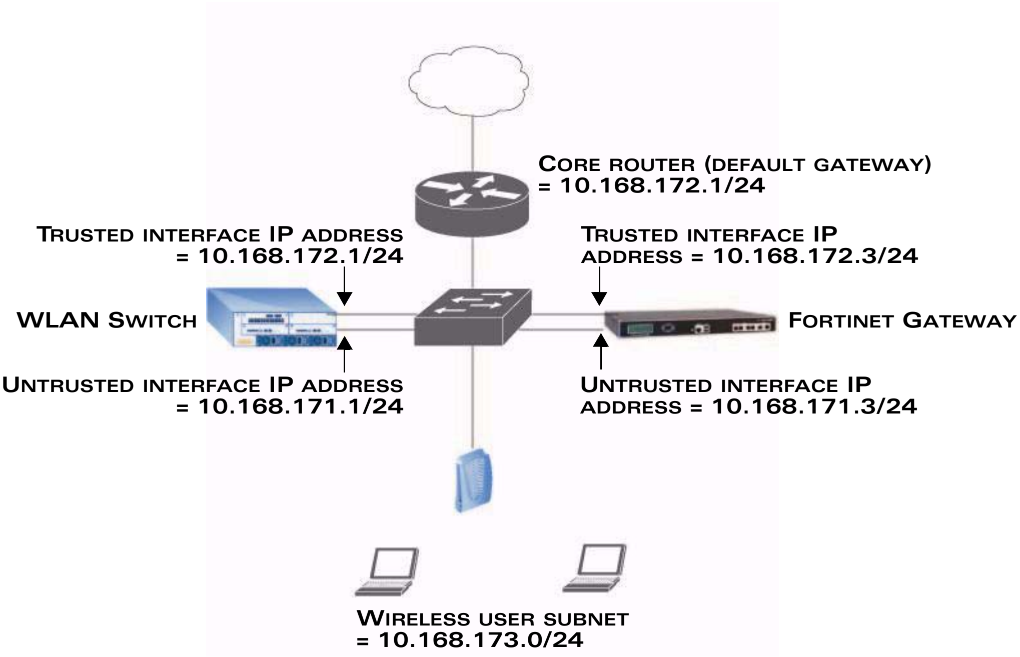

CORE ROUTER (DEFAULT GATEWAY) = 10.168.172.1/24
TRUSTED INTERFACE IP ADDRESS = 10.168.172.1/24
TRUSTED INTERFACE IP ADDRESS = 10.168.172.3/24
WLAN SWITCH
FORTINET GATEWAY
UNTRUSTED INTERFACE IP ADDRESS = 10.168.171.1/24
UNTRUSTED INTERFACE IP ADDRESS = 10.168.171.3/24
WIRELESS USER SUBNET = 10.168.173.0/24

FIGURE 2-3 Example Route Mode Topology

In the topology shown, the following configurations are entered on the WLAN Switch and Fortinet gateway:

ESI Server configuration on WLAN Switch:

- Trusted IP address = 10.168.172.3
- Untrusted IP address = 10.168.171.3
- Mode = route

IP routing configuration on Fortinet Gateway:

- Default gateway (core router) = 10.168.172.1
- Static route for wireless user subnet (10.168.173.0/24) through WLAN Switch (10.168.171.2)