

Aruba Wireless Custom Training

DAY 1-2:

INTRODUCTION TO WIRELESS

Radio Frequency Fundamentals

What Is a Radio Frequency Signal?

Radio Frequency Characteristics

Wavelength

Frequency

Amplitude

Phase

Radio Frequency Behaviors

Wave Propagation

Absorption

Reflection

Scattering

Refraction

Diffraction

Loss (Attenuation)

Free Space Path Loss

Multipath

Gain (Amplification)

Radio Frequency Components, Measurements, and Mathematics

RF Components

Transmitter

Antenna

Receiver

Intentional Radiator (IR)

Equivalent Isotropically Radiated Power

Units of Power and Comparison

Noise Floor

Signal-to-Noise Ratio (SNR)

Received Signal Strength Indicator

Radio Frequency Signal and Antenna Concepts

Beamwidth

Antenna Types

Omnidirectional Antennas

Semidirectional Antennas

Highly Directional Antennas

RF Line of Sight

Fresnel Zone

Earth Bulge

MIMO Antennas

Indoor MIMO Antennas 133

Outdoor MIMO Antennas 133
Antenna Connection and Installation 134
Signal Loss 135
Antenna Mounting 136
Antenna Accessories 141
Attenuators

IEEE 802.11 Standards

802.11b
802.11a
802.11g
802.11r-2008
802.11k-2008
802.11n-2009
802.11ac 177

Wireless Networks and Spread Spectrum Technologies

Industrial, Scientific, and Medical Bands
900 MHz ISM Band
2.4 GHz ISM Band
5.8 GHz ISM Band
Unlicensed National Information Infrastructure Bands
UNII-1 (Lower Band)
UNII-2 (Middle Band)
UNII-2 Extended
UNII-3 (Upper Band)
Frequency Hopping Spread Spectrum
Hopping Sequence
Dwell Time
Hop Time
Modulation
Direct Sequence Spread Spectrum
Adjacent, Nonadjacent, and Overlapping Channels
Throughput vs. Bandwidth

802.11 Medium Access

CSMA/CA vs. CSMA/CD
Collision Detection
Distributed Coordination Function
Interframe Space (IFS)
Duration/ID Field
Carrier Sense
Block Acknowledgment
Wi-Fi Multimedia
Airtime Fairness

802.11 Management Frames

Management Frame Types
Beacon Frame
Probe Request Frame
Probe Response Frame

- Authentication Frame
- Association Request Frame
- Association Response Frame
- Disassociation Frame
- Deauthentication Frame
- Reassociation Request Frame
- Reassociation Response Frame
- Action Frame
- Management Frame Fields
- Management Frame Information Elements
- Action Frames
- Spectrum and Transmit Power Management

802.11 Control Frames

- Understanding Control Frames
- Carrier Sense
- Virtual Carrier Sense
- Physical Carrier Sense
- RTS/CTS Frames
- CTS-to-Self
- Protection Mechanism
- Preventing Collisions
- ERP Information Element
- Triggering Protection Mechanism
- Acknowledgement Frame
- Block Acknowledgement Request
- Block Acknowledgement
- PS-Poll
- Control Wrapper

Data Frames

- Data Subtypes
- QoS and Non-QoS Data Frames
- Data-Carrying vs. Non-Data-Carrying Frames
- Simple Data Frame
- Data Frame Address Fields
- Fragmentation
- Data Frame Aggregation
- Rate Selection
- Multirate Support
- Basic and Supported Rates
- Dynamic Rate Selection

802.11 Security

- Authentication
- Open System Authentication
- Shared Key Authentication
- WLAN Encryption Methods
- WEP
- TKIP

- CCMP
- WPA/WPA2
- Robust Security Network (RSN)
- RSN Information Element
- 802.1X
- Supplicant
- Authenticator
- Authentication Server
- EAP
- Strong EAP Protocols
- EAP-PEAP
- 4-Way Handshake
- Group Key Handshake
- Fast BSS Transition (FT)
- Information Elements
- FT Initial Mobility Domain Association
- Over-the-Air Fast BSS Transition
- Over-the-DS Fast BSS Transition

DAY 3-4:

Introduction to Aruba Controllers and different kinds of deployments

Understanding Basic Deployment and Configuration Tasks

- Fundamentals
- WebUI
- CLI
- Deployment Scenario #1: Controller and APs on Same Subnet
- Deployment Scenario #2: APs All on One Subnet Different from Controller Subnet
- Deployment Scenario #3: APs on Multiple Different Subnets from Controllers
- Configuring the Controller
- Running Initial Setup
- Connecting to the Controller after Initial Setup

Control Plane Security

- Control Plane Security Overview
- Configuring Control Plane Security
- Managing AP Whitelists
- Adding APs to the Campus and Remote AP Whitelists
- Viewing Whitelist Status
- Modifying an AP in the Campus AP Whitelist
- Revoking an AP via the Campus AP Whitelist
- Purging the Campus AP Whitelist
- Offloading a Controller RAP Whitelist to ClearPass Policy Manager
- Managing Whitelists on Master and Local Controllers 1
- Campus AP Whitelist Synchronization
- Viewing and Managing the Master or Local Controller Whitelists
- Working in Environments with Multiple Master Controllers
- Configuring Networks with a Backup Master Controller
- Configuring Networks with Clusters of Master Controllers

- Creating a Cluster Root
- Creating a Cluster Member
- Replacing a Controller on a Multi-Controller Network
- Replacing Controllers in a Single Master Network
- Replacing a Local Controller
- Replacing a Master Controller with No Backup
- Replacing a Redundant Master Controller
- Replacing Controllers in a Multi-Master Network
- Replacing a Local Controller in a Multi-Master Network
- Replacing a Cluster Member Controller with no Backup
- Replacing a Redundant Cluster Member Controller
- Replacing a Cluster Root Controller with no Backup Controller
- Replacing a Redundant Cluster Root Controller
- Troubleshooting Control Plane Security
- Identifying Certificate Problems
- Verifying Certificates
- Disabling Control Plane Security
- Verifying Whitelist Synchronization
- Rogue APs

Software Licenses

- Understanding License Terminology
- Working with Licenses
- Centralized Licensing in a Multi-Controller Network
- Primary and Backup Licensing Servers
- Communication between the License Server and License Clients
- Supported Topologies
- Unsupported Topologies
- Adding and Deleting Licenses
- Replacing a Controller
- Failover Behaviors
- Client is Unreachable
- Server is Unreachable
- Configuring Centralized Licensing
- Pre-configuration Setup in an All-Master Deployment
- Preconfiguration Setup in a Master/Local Topology
- Enabling Centralized Licensing
- Monitoring and Managing Centralized Licenses
- License server Table
- License Client Table
- License Client(s) Usage Table

Network Configuration Parameters

- Configuring VLANs
- Creating and Updating VLANs
- Creating Bulk VLANs
- Creating a VLAN Pool
- Distinguishing Between Even and Hash Assignment Types
- Updating a VLAN Pool
- Deleting a VLAN Pool

- Role Derivation for Named VLAN Pools
- Creating a Named VLAN not in a Pool
- Adding a Bandwidth Contract to the VLAN
- Optimizing VLAN Broadcast and Multicast Traffic
- Configuring Ports
- Classifying Traffic as Trusted or Untrusted
- About Trusted and Untrusted Physical Ports
- About Trusted and Untrusted VLANs
- Configuring Trusted/Untrusted Ports and VLANs
- Configuring Trusted and Untrusted Ports and VLANs in Trunk Mode
- Understanding VLAN Assignments
- VLAN Derivation Priorities for VLAN types
- How a VLAN Obtains an IP Address
- Assigning a Static Address to a VLAN
- Configuring a VLAN to Receive a Dynamic Address
- Configuring Multiple Wired Uplink Interfaces (Active-Standby)
- Enabling the DHCP Client
- Enabling the PPPoE Client
- Default Gateway from DHCP/PPPoE
- Configuring DNS/WINS Server from DHCP/PPPoE
- Configuring Source NAT to Dynamic VLAN Address
- Configuring Source NAT for VLAN Interfaces
- Inter-VLAN Routing
- Configuring Static Routes
- Configuring the Loopback IP Address
- Configuring the Controller IP Address
- Configuring GRE Tunnels
- Important Points to Remember
- Limitations
- Creating a Tunnel Interface
- Directing Traffic into the Tunnel
- Static Routes
- Firewall Policy
- Tunnel Keepalives
- Configuring GRE Tunnel Group
- Creating a Tunnel Group
- Jumbo Frame Support

Link Aggregation Control Protocol (LACP)

- Understanding LACP Best Practices and Exceptions
- Configuring LACP
- LACP Sample Configuration
- Branch Office Topology
- Branch Office Routing Table

Tunneled Nodes

- Understanding Tunneled Node Configuration
- Configuring a Wired Tunneled Node Client
- Configuring an Access Port as a Tunneled Node Port
- Configuring a Trunk Port as a Tunneled Node Port
- Show commands

Authentication Servers

- Understanding Authentication Server Best Practices and Exceptions
- Understanding Servers and Server Groups
- Configuring Authentication Servers
- Configuring a RADIUS Server
- RADIUS Server VSAs
- RADIUS Server Authentication Codes
- RADIUS Server Fully Qualified Domain Names
- DNS Query Intervals
- Managing the Internal Database
- Configuring the Internal Database
- Managing Internal Database Files
- Working with Internal Database Utilities
- Deleting All Users
- Repairing the Internal Database
- Configuring Server Groups
- Configuring Server List Order and Fail-Through
- Configuring Dynamic Server Selection
- Configuring Match FQDN Option
- Trimming Domain Information from Requests
- Configuring Server-Derivation Rules
- Configuring a Role Derivation Rule for the Internal Database
- Assigning Server Groups
- User Authentication
- Management Authentication
- Accounting
- RADIUS Accounting
- RADIUS Accounting on Multiple Servers
- Configuring Authentication Timers
- Setting an Authentication Timer
- Authentication Server Load Balancing
- Enabling Authentication Server Load Balancing Functionality

MAC-based Authentication

- Configuring MAC-Based Authentication
- Configuring the MAC Authentication Profile
- Configuring Clients

802.1X Authentication 252

- Understanding 802.1X Authentication
- Supported EAP Types
- Configuring Authentication with a RADIUS Server
- Configuring Authentication Terminated on Controller
- Configuring 802.1X Authentication
- Configuring and Using Certificates with AAA FastConnect
- Configuring User and Machine Authentication
- Working with Role Assignment with Machine Authentication Enabled
- Enabling 802.1x Supplicant Support on an AP
- Prerequisites
- Provisioning an AP as an 802.1X Supplicant

Sample Configurations

- Configuring Authentication with an 802.1X RADIUS Server
- Configuring Roles and Policies
- Creating the Student Role and Policy
- Creating the Faculty Role and Policy
- Creating the Guest Role and Policy
- Creating Roles and Policies for Sysadmin and Computer
- Creating an Alias for the Internal Network Using the CLI
- Configuring the RADIUS Authentication Server
- Configuring 802.1X Authentication
- Configuring VLANs
- Configuring the WLANs
- Configuring the Guest WLAN
- Configuring the Non-Guest WLANs
- Configuring Authentication with the Controller's Internal Database
- Configuring the Internal Database
- Configuring a Server Rule
- Configuring 802.1x Authentication
- Performing Advanced Configuration Options for 802.1X
- Configuring Reauthentication with Unicast Key Rotation
- Application Single Sign-On Using L2 Authentication
- Important Points to Remember

Certificate Revocation

- Understanding OCSP and CRL
- Configuring a Controller as OCSP and CRL Clients
- Certificate Revocation Checking for SSH Pubkey Authentication

Captive Portal Authentication

- Understanding Captive Portal
- Policy Enforcement Firewall Next Generation (PEFNG) License
- Controller Server Certificate
- Configuring Captive Portal in the Base Operating System
- Using Captive Portal with a PEFNG License
- Sample Authentication with Captive Portal
- Creating a Guest User Role
- Creating an Auth-guest User Role
- Configuring Policies and Roles
- Creating a Time Range
- Creating Aliases
- Creating an Auth-Guest-Access Policy
- Creating an Block-Internal-Access Policy
- Creating a Drop-and-Log Policy
- Creating a Guest Role
- Creating an Auth-Guest Role
- Configuring Policies and Roles in the CLI
- Defining a Time Range
- Creating Aliases
- Creating a Guest-Logon-Access Policy
- Creating an Auth-Guest-Access Policy

- Creating a Block-Internal-Access Policy
- Creating a Drop-and-Log Policy
- Creating a Guest-Logon Role
- Creating an Auth-Guest Role
- Configuring Guest VLANs
- Configuring Captive Portal Authentication Profiles
- Modifying the Initial User Role
- Configuring the AAA Profile
- Configuring the WLAN
- Managing User Accounts
- Configuring Captive Portal Configuration Parameters
- Enabling Optional Captive Portal Configurations
- Uploading Captive Portal Pages by SSID Association
- Changing the Protocol to HTTP
- Configuring Redirection to a Proxy Server
- Redirecting Clients on Different VLANs
- Web Client Configuration with Proxy Script
- Personalizing the Captive Portal Page
- Creating and Installing an Internal Captive Portal
- Creating a New Internal Web Page
- Username Example
- Password Example
- FQDN Example
- Basic HTML Example
- Installing a New Captive Portal Page
- Displaying Authentication Error Messages
- Reverting to the Default Captive Portal
- Configuring Localization
- Customizing the Welcome Page
- Customizing the Pop-Up box
- Customizing the Logged Out Box
- Creating Walled Garden Access
- Enabling Captive Portal Enhancements
- Configuring the Redirect-URL
- Configuring the Login URL
- Defining Netdestination Descriptions
- Configuring a Whitelist
- Configuring the Netdestination for a Whitelist
- Associating a Whitelist to Captive Portal Profile
- Applying a Captive Portal Profile to a User-Role
- Verifying a Whitelist Configuration
- Verifying a Captive Portal Profile Linked to a Whitelist
- Verifying Dynamic ACLs for a Whitelist
- Verifying DNS Resolved IP Addresses for Whitelisted URLs

Virtual Private Networks

- Planning a VPN Configuration
- Selecting an IKE protocol
- Understanding Suite-B Encryption Licensing
- Working with IKEv2 Clients
- Understanding Supported VPN AAA Deployments

- Working with Certificate Groups
- Working with VPN Authentication Profiles
- Configuring a Basic VPN for L2TP/IPsec \
- Defining Authentication Method and Server Addresses
- Defining Address Pools
- RADIUS Framed-IP-Address for VPN Clients
- Enabling Source NAT
- Selecting Certificates
- Defining IKEv1 Shared Keys
- Configuring IKE Policies
- Setting the IPsec Dynamic Map
- Configuring a Basic L2TP VPN in the CLI
- Configuring a VPN for L2TP/IPsec with IKEv2
- Defining Authentication Method and Server Addresses
- Selecting Certificates
- Configuring IKE Policies
- Setting the IPsec Dynamic Map

Roles and Policies

- Configuring Firewall Policies
- Working With Access Control Lists (ACLs)
- Support for Desktop Virtualization Protocols
- Creating a Firewall Policy
- Creating a Network Service Alias
- Creating an ACL White List
- Configuring the White List Bandwidth Contract in the CLI
- User Roles
- Assigning User Roles
- Assigning User Roles in AAA Profiles
- Working with User-Derived VLANs
- Understanding Device Identification
- Configuring a User-derived Role or VLAN
- User-Derived Role Example
- RADIUS Override of User-Derived Roles
- Configuring a Default Role for Authentication Method
- Configuring a Server-Derived Role
- Configuring a VSA-Derived Role
- Understanding Global Firewall Parameters
- Using AppRF 2.0

DAY 5-6:

Continuation for Controller based deployment

ClearPass Policy Manager Integration

- Introduction
- Important Points to Remember
- Enabling Downloadable Role on a Controller
- Sample Configuration
- CPPM Server Configuration

- Adding a Device
- Adding Enforcement Profile
- Advanced Role Configuration Mode
- Adding Enforcement Policy
- Adding Services
- Controller Configuration
- Configuring CPPM Server on Controller
- Configuring Server Group to include CPPM Server
- Configuring 802.1X Profile
- Configuring AAA Profile

Virtual APs

- Virtual AP Profiles
- Configuring the Virtual AP Profile
- Creating and Configuring a Profile
- Selective Multicast Stream
- Associating Other Profiles to the Virtual AP
- Configuring a Virtual AP in the CLI
- Associating a Virtual AP Profile to an AP or AP Group
- Excluding a Virtual AP Profile
- Virtual AP Configuration Workflow
- Radio Resource Management (802.11k)
- Configuring the 802.11k Profile

Understanding ARM

- ARM Support for 802.11n
- Monitoring Your Network with ARM
- Maintaining Channel Quality
- Configuring ARM Scanning
- Understanding ARM Application Awareness
- Client Match
- ARM Coverage and Interference Metrics
- Configuring ARM Profiles
- Creating and Configuring a New ARM Profile
- Modifying an Existing Profile
- Copying an Existing Profile
- Deleting a Profile
- Assigning an ARM Profile to an AP Group
- Using Multi-Band ARM for 802.11a/802.11g Traffic
- Band Steering
- Steering Modes
- Enabling Band Steering
- Enabling Traffic Shaping
- Enabling Traffic Shaping
- Enabling or Disabling the Hard Limit Parameter in Traffic Management Profile
- Spectrum Load Balancing
- Reusing Channels to Control RX Sensitivity Tuning
- Configuring Non-802.11 Noise Interference Immunity
- Troubleshooting ARM
- Too many APs on the Same Channel
- Wireless Clients Report a Low Signal Level
- Transmission Power Levels Change Too Often

APs Detect Errors but Do Not Change Channels
APs Don't Change Channels Due to Channel Noise

Wireless Intrusion Prevention

Understanding Wizard Intrusion Detection
Understanding Wizard Intrusion Protection
Understanding client intrusion protection
Understanding Client Intrusion Detection

Access Points (APs)

Basic Functions and Features
Naming and Grouping APs
Creating an AP group
Assigning APs to an AP Group
Understanding AP Configuration Profiles
AP Profiles
RF Management Profiles
Wireless LAN Profiles
Mesh Profiles
QoS Profiles
IDS Profiles
HA Group profiles
Other Profiles
Profile Hierarchy
Viewing Profile Errors
Before you Deploy an AP
Mesh AP Preconfiguration
Remote AP Preconfiguration
Enable Controller Discovery
Controller Discovery using DNS
Controller Discovery using ADP
Controller discovery using a DHCP Server
Enable DHCP to Provide APs with IP Addresses
AP Provisioning Profiles
Defining an AP Provisioning Profile
Assigning Provisioning Profiles
Configuring Installed APs
Configuring an AP using the Provisioning Wizard
Configuring a Remote AP
Remote Authentication
RAP Configuration
Configuring a Mesh AP
Verifying the Configuration
Optional AP Configuration Settings
AP Installation Mode
Important Points to Remember
AP Redundancy
AP Maintenance Mode
AP LEDs
RF Management
802.11a and 802.11g RF Management Profiles

VHT Support on AP-200 Series, AP-210 Series, AP-220 Series, and AP-270 Series Access Points

Managing 802.11a/802.11g Profiles

Creating or Editing a Profile

Assigning an 802.11a/802.11g Profile to an AP or AP Group

Assigning a High-throughput Profile

Assigning an ARM Profile

Deleting a Profile

Creating or Modifying a Profile

Viewing RF Management Settings

Assigning a 802.11a/802.11g Profile

Deleting a Profile

RF Optimization

RF Event Configuration

Optimizing APs Over Low-Speed Links

Configuring the Bootstrap Threshold

Prioritizing AP heartbeats

Configuring AP Channel Assignments

Channel Switch Announcement (CSA)

Secure Enterprise Mesh

Mesh Overview Information

Mesh Configuration Procedures

Understanding Mesh Access Points

Mesh Portals

Mesh Points

Mesh Clusters

Understanding Mesh Links

Link Metrics

Optimizing Links

Understanding Mesh Profiles

Mesh Cluster Profiles

Mesh Radio Profiles

RF Management (802.11a and 802.11g) Profiles

Adaptive Radio Management Profiles

High-Throughput Radio Profiles

Mesh High-Throughput SSID Profiles

Wired AP Profiles

Mesh Recovery Profiles

Understanding Remote Mesh Portals (RMPs)

Understanding the AP Boot Sequence

Booting the Mesh Portal

Booting the Mesh Point

Air Monitoring and Mesh

Mesh Deployment Solutions

Thin AP Services with Wireless Backhaul Deployment

Point-to-Point Deployment

Point-to-Multipoint Deployment

High-Availability Deployment

Mesh Deployment Planning

Pre-Deployment Considerations

Outdoor-Specific Deployment Considerations

Increasing Network Uptime Through Redundancy and VRRP

- High Availability
- Pre-Deployment Information
- Configuration Procedures
- High Availability Deployment Models
- Master-Redundancy Deployment Model
- AP Communication with Controllers
- Client State Synchronization
- Feature Guidelines and Limitations
- High Availability Inter-Controller Heartbeats
- High Availability Extended Controller Capacity
- Feature Requirements
- Standby Controller Capacity
- AP Failover
- Configuring High Availability
- Pre-Deployment Information
- Configuring High Availability
- Configuring a Master Controller for Redundancy and High Availability
- Migrating from VRRP Redundancy
- Migrating from Backup-LMS Redundancy
- Configuring VRRP Redundancy
- Configuring the Local Controller for Redundancy
- Configuring the LMS IP
- Configuring the Master Controller for Redundancy
- Configuring Database Synchronization
- Enabling Incremental Configuration Synchronization (CLI Only)
- Configuring Master-Local Controller Redundancy
- Default LLDP Configuration
- Configuring LLDP
- Monitoring LLDP Configuration

Remote Access Points

- Configuring the Secure Remote Access Point Service
- Configure a Public IP Address for the Controller
- Configure the NAT Device
- Configure the VPN Server
- Configuring Certificate RAP
- Creating a Remote AP Whitelist
- Configuring PSK RAP
- Add the user to the internal database
- RAP Static Inner IP Address
- Provision the AP
- Deploying a Branch Office/Home Office Solution
- Provisioning the Branch Office AP
- Configuring the Branch Office AP
- Troubleshooting Remote AP
- Local Debugging
- Remote AP Summary
- Multi homing on remote AP (RAP)
- Seamless failover from backup link to primary link on RAP

- Remote AP Connectivity
- Remote AP Diagnostics
- Enabling Remote AP Advanced Configuration Options
- Understanding Remote AP Modes of Operation
- Working in Fallback Mode
- Backup Configuration Behavior for Wired Ports

LAB and Real time troubleshooting scenarios for Controller based networks.

DAY 7-8:

Introduction to Aruba Instant and management with Airwave

About Aruba Instant

- Instant Overview
- Supported Devices
- Instant UI
- Instant CLI

Setting up an IAP

- Setting up Instant Network
- Connecting an IAP
- Assigning an IP address to the IAP
- Connecting to a Provisioning Wi-Fi Network
- IAP Cluster
- Disabling the Provisioning Wi-Fi Network
- Logging in to the Instant UI
- Regulatory Domains
- Applying Configuration Changes
- Using Sequence Sensitive Commands

Instant User Interface

- Main Window
- Networks Tab
- Access Points Tab
- Clients Tab
- Links
- New Version Available
- System
- RF
- Security
- Maintenance
- Under More
- VPN
- IDS
- Wired
- Services
- DHCP Server
- Support
- Help
- Logout

- Monitoring
- Info
- RF Dashboard
- RF Trends
- Usage Trends
- Mobility Trail
- Client Match
- AppRF
- Spectrum
- Alerts
- IDS
- AirGroup
- Configuration
- AirWave Setup
- Aruba Central
- Pause/Resume

Initial Configuration Tasks

- Modifying the IAP Name
- Updating Location Details of an IAP
- Configuring a Preferred Band
- Configuring Virtual Controller IP Address
- Configuring a Timezone
- Configuring an NTP Server
- Enabling AppRF Visibility
- Changing Password
- Additional Configuration Tasks
- Configuring Virtual Controller VLAN
- Configuring Auto Join Mode
- Configuring Terminal Access
- Configuring Console Access
- Configuring LED Display
- Configuring Additional WLAN SSIDs
- Enabling the Extended SSID
- Preventing Inter-user Bridging
- Preventing Local Routing between Clients
- Enabling Dynamic CPU Management 89

Customizing IAP Settings

- Modifying the IAP Hostname
- Configuring Zone Settings on an IAP
- Specifying a Method for Obtaining IP Address
- Configuring External Antenna
- EIRP and Antenna Gain
- Configuring Antenna Gain
- Configuring Radio Profiles for an IAP
- Configuring ARM Assigned Radio Profiles for an IAP
- Configuring Radio Profiles Manually for IAP
- Configuring Uplink VLAN for an IAP
- Master Election and Virtual Controller
- Master Election Protocol
- Preference to an IAP with 3G/4G Card

- Preference to an IAP with Non-Default IP
- Viewing Master Election Details
- Manual Provisioning of Master IAP 96
- Provisioning an IAP as a Master IAP 96
- Adding an IAP to the Network
- Removing an IAP from the Network

VLAN Configuration

- VLAN Pooling
- Uplink VLAN Monitoring and Detection on Upstream Devices

Wireless Network Profiles

- Configuring Wireless Network Profiles
- Network Types
- Configuring WLAN Settings for an SSID Profile
- Configuring VLAN Settings for a WLAN SSID Profile
- Configuring Security Settings for a WLAN SSID Profile
- Configuring Access Rules for a WLAN SSID Profile
- Configuring Fast Roaming for Wireless Clients
- Opportunistic Key Caching
- Editing a WLAN SSID Profile
- Deleting a WLAN SSID Profile

Wired Profiles

- Configuring a Wired Profile
- Configuring Wired Settings
- Configuring VLAN for a Wired Profile
- Configuring Security Settings for a Wired Profile
- Configuring Security Settings for a Wired Employee Network
- Configuring Access Rules for a Wired Profile
- Assigning a Profile to Ethernet Ports
- Link Aggregation Control Protocol
- Understanding Hierarchical Deployment

Captive Portal for Guest Access --

Understanding Captive Portal

- Types of Captive Portal
- Walled Garden
- Configuring a WLAN SSID for Guest Access
- Configuring Wired Profile for Guest Access
- Configuring External Captive Portal for a Guest Network
- External Captive Portal Profiles
- Creating a Captive Portal Profile
- Configuring an SSID or Wired Profile to Use External Captive Portal Authentication
- Configuring External Captive Portal Authentication Using ClearPass Guest
- Creating a Web Login page in ClearPass Guest
- Configuring RADIUS Server in Instant UI
- Configuring Facebook Login
- Setting up a Facebook Page

- Configuring an SSID
- Configuring the Facebook Portal Page
- Accessing the Portal Page
- Configuring Guest Logon Role and Access Rules for Guest Users
- Configuring Captive Portal Roles for an SSID
- Configuring Walled Garden Access
- Disabling Captive Portal Authentication
- Authentication and User Management
- Managing IAP Users
- Configuring Authentication Parameters for Management Users
- Configuring a TACACS+ Server Profile for Management User Authentication
- Configuring Users for Internal Database of an IAP
- Configuring the Read-Only Administrator Credentials
- Adding Guest Users through the Guest Management Interface

Understanding Authentication Methods

- 802.1X authentication
- MAC authentication
- MAC authentication with 802.1X authentication
- Captive Portal Authentication
- MAC authentication with Captive Portal authentication
- 802.1X authentication with Captive Portal Role
- WISPr authentication
- Supported EAP Authentication Frameworks
- Authentication Termination on IAP
- Supported Authentication Servers
- Internal RADIUS Server
- External RADIUS Server
- RADIUS Server Authentication with VSA
- Dynamic Load Balancing between Two Authentication Servers
- Understanding Encryption Types
- WPA and WPA2
- Configuring Authentication Servers
- Configuring an External Server for Authentication
- Configuring Dynamic RADIUS Proxy Parameters
- Configuring Dynamic RADIUS Proxy Parameters for Authentication Servers
- Associate the Authentication Servers with an SSID or Wired Profile
- Configuring 802.1X Authentication for Wired Profiles
- Configuring MAC Authentication for a Network Profile
- Configuring MAC Authentication for Wireless Network Profiles
- Configuring MAC Authentication for Wired Profiles
- Configuring MAC Authentication with 802.1X Authentication
- Configuring MAC and 802.1X Authentication for a Wireless Network Profile
- Configuring MAC and 802.1X Authentication for Wired Profiles
- Configuring MAC Authentication with Captive Portal Authentication
- Blacklisting Clients
- Blacklisting Clients Manually
- Uploading Certificates
- Loading Certificates through Instant UI
- Removing Certificates
- Loading Certificates through AirWave

DAY 9-10:

For Instant based deployment Management with Airwave

Instant Management with AirWave

AirWave Security Options
Intrusion Detection System
Firmware Image Management
Using Aruba Instant with AirWave
Secure Access to AirWave
AMP Pages with Instant-Specific Features
Supported Firmware

Setting up Aruba Instant

Setting up Aruba Instant Manually
Creating your Organization String
Authenticating to the AirWave Server
Shared Key Authentication
Whitelist Authentication
Entering the Organization String and AirWave Information into the IAP
Setting up Aruba Instant Automatically
Verifying the Shared Secret
Completing the Setup

Using Template Configuration

Adding the First Instant Device to AirWave
Updating the Instant Template
Adding Additional Instant APs to AirWave
Adding Multiple Devices from a File
Changing the Mode to Monitor Only for New Instant Devices

Editing Variables

Editing Individual Virtual Controller Values

Bulk Editing of Multiple Virtual Controllers

Using Custom Variables

Applying Changes

Using Instant Config

Enabling Instant Config

Buttons and Icons in Instant Config

Importing Devices for Instant Config

Add Newly Discovered Devices to a Group

The Instant Config UI

Group Focus

Virtual Controller Focus

Network Focus

Where to Get Additional Information

Field-Level Help

Additional Documentation

Other Available Task

Resolving Mismatches

Resolving Mismatches when Instant Config is Disabled

Resolving Mismatches when Instant Config is Enabled

Enabling the IAP Role

Monitoring Devices

Run Commands

Best Practices and Known Issues

Best Practices

Known Issues with the Aruba Instant Integration with AirWave

Controller Configuration in AirWave

Requirements, Restrictions, and ArubaOS Support in AirWave

Requirements

Restrictions

ArubaOS Support in AirWave

Overview of Aruba Configuration in AirWave

Device Setup > Aruba Configuration Page

Groups > Controller Config Page with Global Configuration Enabled

Groups > Controller Config when Global Configuration is Disabled

Support for Editing Multiple Device Settings

Controller Configuration Sections in the Tree View

Aruba AP Groups Section

AP Overrides Section

WLANs Section

Profiles Section

Security Section

Local Config Section

Advanced Services Section

Groups

Additional Concepts and Components

Global Configuration and Scope

Referenced Profile Setup

Save, Save and Apply, and Revert Buttons

Additional Concepts and Benefits

Scheduling Configuration Changes

Auditing and Reviewing Configurations

Licensing and Dependencies in Aruba Configuration

Setting Up Initial Aruba Configuration

Prerequisites

Procedure

Additional Capabilities

Aruba Configuration in Daily Operations

Aruba AP Groups Procedures and Guidelines

Guidelines and Pages for Aruba AP Groups

Selecting Aruba AP Groups

Configuring Aruba AP Groups

General WLAN Guidelines

Guidelines and Pages for WLANs in Aruba Configuration

General Profiles Guidelines

General Controller Procedures and Guidelines

Using Master, Standby Master, and Local Controllers

Pushing Device Configurations to Controllers

Supporting APs with Aruba Configuration

AP Overrides Guidelines

Changing Adaptive Radio Management (ARM) Settings

Changing SSID and Encryption Settings

Changing the Aruba AP Group for an AP Device

Using AMP to Deploy Aruba APs

Using General AMP Device Groups and Folders

Visibility in Aruba Configuration

Visibility Overview

Defining Visibility for Aruba Configuration

Appendix A Controller Configuration Reference

Aruba AP Groups

WLANs

Understanding Aruba Configuration Profiles

Security

Server Groups Page Overview

Supported Servers

Adding a New Server Group 51

Security

Local Config

DAY 15

ADVANCED CLEARPASS

About ClearPass Policy Manager

Services

Live Monitoring

Authentication Methods and Sources

Identity Settings

Posture Policies and Audit Servers

Enforcement Profiles and Policies

Network Access Devices

Scheduling Network and Subnet Scans

Policy Simulation

ClearPass Device Profiler

Administration

Cluster Update and Upgrade

Ingress Events Processing

OnGuard Agents

Insight Report Tool

A: Command Line Interface

B: SNMP MIB & Traps, System Events, Error Codes

C: Use Cases

D: Rules Editing and Namespaces