

Contents

1.1 Revision History 1

2 Demo Topology 2

3 Guest Access Configuration – Bridge Mode 3

3.1 Guest Wireless Configuration..... 3

3.2 ClearPass Guest policy Configuration 5

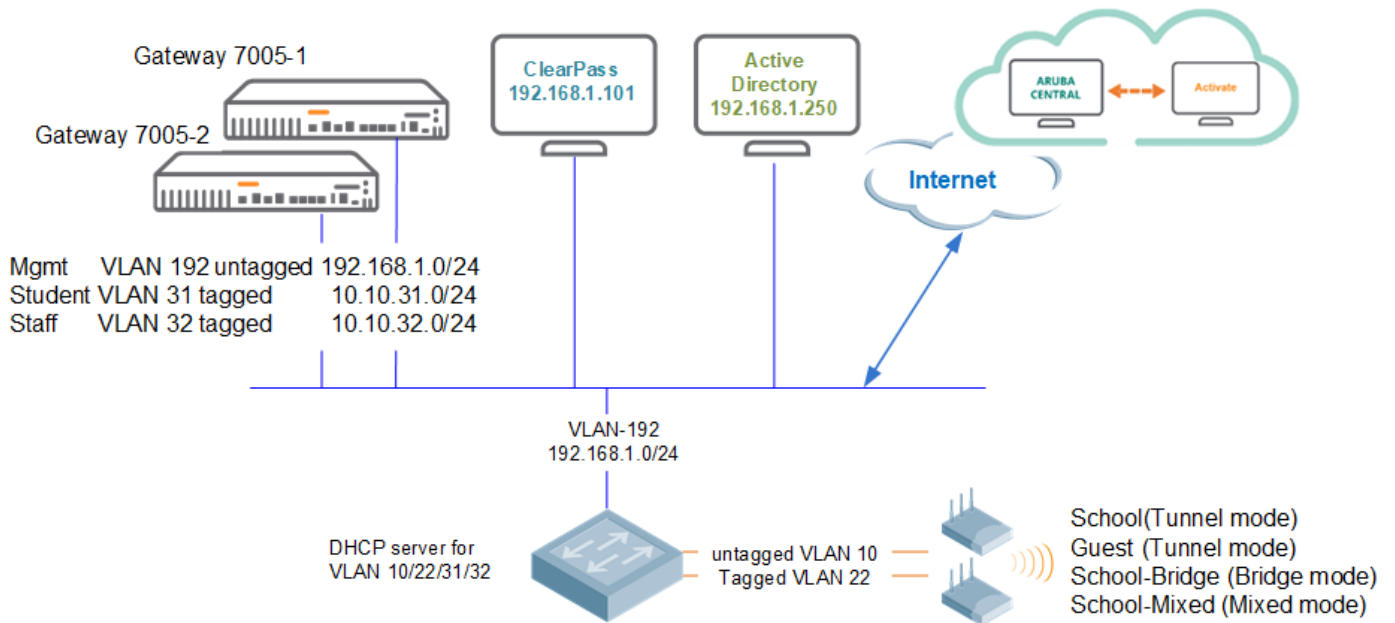
3.3 Guest Testing..... 6

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
04 Jan 2024	0.1	Ariya Parsamanesh	Initial creation
08 Jan 2024	0.2	Ariya Parsamanesh	Guest testing

2 Demo Topology

This is the final part of the 4x parts AOS10.4 Tutorial series where here we demonstrate the Guest WLAN functionality in Bridge mode.



3 Guest Access Configuration – Bridge Mode

Here we'll use the same weblogin page with minor changes to the ClearPass service.

3.1 Guest Wireless Configuration

We'll start with the configuration of External captive portal profile.

The screenshot shows the Aruba web management interface. On the left, the 'Customer: Ariya Publ...' is selected, and the 'AOS10' device is chosen. The 'Security' tab is active, and the 'Authentication Servers' section is expanded. A table lists several authentication servers, with 'guest-redirect-B' highlighted. Below this, the 'Edit Server' dialog is open for 'guest-redirect-B'. The 'Server Type' is set to 'External Captive Portal', and the 'Captive Portal Failure' is set to 'Deny Internet'. The 'Name' is 'guest-redirect-B', the 'IP or Hostname' is 'cp1-611.arubatechs.com', the 'URL' is '/guest/school.php', and the 'Port' is '443'. The 'Use HTTPS' checkbox is checked. The 'Save' button is visible at the bottom right of the dialog.

Name	Type
ClearPass	RADIUS
CP-Guest	External Captive Portal
MPSK-Rego	External Captive Portal
default	External Captive Portal
guest-redirect	External Captive Portal
guest-redirect-B	External Captive Portal

Edit Server

Server Type: External Captive Portal Captive Portal Failure: Deny Internet

Name: guest-redirect-B

IP or Hostname: cp1-611.arubatechs.com Server offload: ☐

URL: /guest/school.php Prevent Frame Overlay: ☐

Port: 443 Use AP IP in Redirect URL: ☐

Redirect URL:

Use HTTPS: ☒

Cancel Save

Followed by the user role guest-redirect-B.

The screenshot shows the Aruba web management interface. On the left, the 'Customer: Ariya Publ...' is selected, and the 'AOS10' device is chosen. The 'Security' tab is active, and the 'Roles' section is expanded. A table lists several roles, with 'guest-redirect-B' highlighted. Below this, the 'Access Rules For Selected Roles' section is visible, showing a list of rules for the selected role. The rules include 'Enforce Captive Portal', 'Allow http on domain cp1-611.arubatechs.com', 'Allow https on domain cp1-611.arubatechs.com', 'Allow dhcp to all destinations', 'Allow dns to all destinations', and 'Allow icmp to all destinations'. The 'Save' button is visible at the bottom right of the rules section.

Role
School-Mixed
Student-Bridge
Student-Devs
Tguest
default_wired_port_profile
guest-redirect
guest-redirect-B

Access Rules For Selected Roles

- Enforce Captive Portal
- Allow http on domain cp1-611.arubatechs.com
- Allow https on domain cp1-611.arubatechs.com
- Allow dhcp to all destinations
- Allow dns to all destinations
- Allow icmp to all destinations

Now we'll start with the configuration of the new guest SSID in bridge mode.

Customer: Ariya Publ...

AOS10

Manage

Overview

Devices

Clients

Guests

Applications

Security

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

IoT

Configuration Audit

Summary

List

Config

Hide Advanced

Create a New Network

1 General

2 VLANs

3 Security

4 Access

5 Summary

Name (SSID):

Bguest

Band:

☒ 2.4 GHz

☒ 5 GHz

☐ 6 GHz

> Advanced Settings

Create a New Network

1 General

2 VLANs

3 Security

4 Access

5 Summary

Traffic forwarding mode:

☒ Bridge

☐ Tunnel

☐ Mixed

Client VLAN Assignment:

☒ Static

☐ Dynamic

VLAN ID:

22

Multiple VLAN IDs or single named VLAN allowed.

> Show Named VLANs

Create a New Network

1 General

2 VLANs

3 Security

4 Access

5 Summary

Security Level:

Enterprise

Personal

Visitors

Open

Access Network

Type:

External Captive Portal

Captive Portal Profile:

guest-redirect-B

+

Primary Server:

ClearPass

+

Secondary Server:

-- Select --

+

Encryption:

Key Management:

Enhanced Open

Advanced Settings

Captive Portal Proxy Server IP:

Captive Portal Proxy Server Port:

MAC Authentication:

Use IP for Calling Station ID:

Delimiter Character:

Called Station ID Type:

MAC Address

Reauth Interval:

0

min

Denylisting:

Max Authentication Failures:

0

Enforce DHCP:

Accounting

Accounting:

Use authentication servers

Accounting Interval:

1

min

Create a New Network

1 General 2 VLANs 3 Security 4 Access 5 Summary

Access rules

Role Based Network Based Unrestricted

Role

Bguest CP-Guest Contractor Employee Executive-Bridge IoT1 IoT2

Access Rules For Selected Roles

Allow any to all destinations

Role Assignment Rules

Default role: Bguest

+ ADD ROLE ASSIGNMENT

Assign Pre-Authentication Role: ☒ guest-redirect-B

Enforce Mac Auth Only Role: ☐

1 Role(s)

3.2 ClearPass Guest policy Configuration

We need two new enforcement profiles.

Enforcement Profiles - gg Aruba guest-redirect-B

Summary

Profile

Attributes

Profile:

Name:	gg Aruba guest-redirect-B
Description:	Captive Portal Role/VLAN enforcement
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= guest-redirect-B

Enforcement Profiles - gg Aruba Bguest access

Summary

Profile

Attributes

Profile:

Name:	gg Aruba Bguest access
Description:	Role/VLAN enforcement for Guest
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Bguest
2. Radius:IETF	User-Name	= %{Endpoint:Username}

And we'll modify our existing services starting with simple MAC auth service.

Services - simple MAC Authentication

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions					
Enforcement Policy:		simple MAC Authentication Enforcement Policy Modify			Add New Enforcement Policy
Enforcement Policy Details					
Description:					
Default Profile:		[Deny Access Profile]			
Rules Evaluation Algorithm:		first-applicable			
Conditions		Enforcement Profiles			
1.	(Tips:Role MATCHES_ALL [MAC Caching] [Guest]) AND (Connection:SSID EQUALS Tguest)	gg Aruba Tguest access, gg MAC Auth Session Timeout			
2.	(Tips:Role MATCHES_ALL [MAC Caching] [Guest]) AND (Connection:SSID EQUALS Bguest)	gg Aruba Bguest access, gg MAC Auth Session Timeout			
3.	(Tips:Role MATCHES_ALL [MAC Caching] [Contractor])	Aruba contractor access, gg MAC Auth Session Timeout			
4.	(Tips:Role MATCHES_ANY [Guest] [Contractor] [Employee]) AND (Connection:SSID EQUALS Tguest)	[Allow Access Profile], gg Aruba guest-redirect			
5.	(Tips:Role MATCHES_ANY [Guest] [Contractor] [Employee]) AND (Connection:SSID EQUALS Bguest)	[Allow Access Profile], gg Aruba guest-redirect-B			

And finally the simple User Authentication with MAC Caching service.

Services - Simple User Authentication with MAC Caching

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy:	simple User Authentication with MAC Caching Enforcement Policy Modify				Add New Enforcement Policy
Enforcement Policy Details					
Description:					
Default Profile:	[Allow Access Profile]				
Rules Evaluation Algorithm:	first-applicable				
Conditions			Enforcement Profiles		
1.	(Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 10) (Tips:Role EQUALS [Contractor])			[Deny Access Profile]	
2.	AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) (Tips:Role EQUALS [Guest])			Aruba contractor access, gg MAC Caching Session Timeout, gg MAC Caching Session Limit, gg Guest MAC Caching, [Update Endpoint Known], gg MAC Caching Do Expire, gg MAC Caching Expire Post Login	
3.	AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) AND (Connection:SSID EQUALS Tguest) (Tips:Role EQUALS [Guest])			gg Aruba Tguest access, gg MAC Caching Session Timeout, gg MAC Caching Session Limit, gg Guest MAC Caching, [Update Endpoint Known], gg MAC Caching Do Expire, gg MAC Caching Expire Post Login	
4.	AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) AND (Connection:SSID EQUALS Bguest)			gg Aruba Bguest access, gg MAC Caching Session Timeout, gg MAC Caching Session Limit, gg Guest MAC Caching, [Update Endpoint Known], gg MAC Caching Do Expire, gg MAC Caching Expire Post Login	

3.3 Guest Testing

The test laptop will connect to Bguest SSID, it gets automatically redirected to guest page, exactly the same as before.

Customer: Ariya Publ...	Clients 3 hours List																																		
AOS10	CLIENTS ALL 54.66 MB (10.16 MB 44.50 MB)																																		
Overview	All 2 Connecting 0 Connected 1 Failed 0 Offline 1 Blocked 0 Wireless 2 Wired 0 Remote 0																																		
Devices	<table> <thead> <tr> <th>CLIENTS</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></tr> <tr> <th>Client Name</th><th>Status</th><th>IP Address</th><th>VLAN</th><th>Connected To</th><th>SSID/Port</th><th>AP Role</th><th>Gateway Role</th><th>Health</th></tr> </thead> <tbody> <tr> <td>02:fd:71:95:4d:e4</td><td>Connected</td><td>10.10.22.29</td><td>22</td><td>bidg-a</td><td>Bguest</td><td>guest-redirect-B</td><td></td><td></td></tr> </tbody> </table>								CLIENTS									Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role	Health	02:fd:71:95:4d:e4	Connected	10.10.22.29	22	bidg-a	Bguest	guest-redirect-B		
CLIENTS																																			
Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role	Health																											
02:fd:71:95:4d:e4	Connected	10.10.22.29	22	bidg-a	Bguest	guest-redirect-B																													
Clients																																			
Guests																																			
Applications																																			

Customer: Ariya Publ...

Summary AI Insights Location Sessions Profile

02fd71954de4

Overview

Applications Security Live Events Events Tools

CLIENT DETAILS

DATA PATH

CLIENT 02fd71954de4 FAILED TO CONNECT

SSID Bguest

AP bldg-a UP

Failure Stage: MACAUTH
Failure Reason: Authentication Server Reject

CLIENT

USERNAME 02fd71954de4

HOSTNAME

IP ADDRESS

CLIENT CATEGORY Computer

CLIENT OS Windows 8/10/11

MANUFACTURER

CLIENT TYPE Wireless

MAC ADDRESS 02fd71954de4

CLIENT FAMILY Windows

CONNECTED SINCE

LAST SEEN Nov 28, 2023, 17:26:00

ENCRYPTION

NETWORK

VLAN

AP ROLE

GATEWAY ROLE

SEGMENTATION

AUTH SERVER 192.168.1.101

TUNNELED

VLAN DERIVATION

AP DERIVATION

SWITCH ROLE

DHCP SERVER

TUNNELED ID

CONNECTION

CHANNEL

BAND

CLIENT CAPABILITIES

CLIENT MAX SPEED

LEDs on ACCESS POINT (bldg-a)

Blink LEDs

Checking the AP's CLI as well.

```
bldg-a# sh clients

Client List
-----
Name          IP Address      MAC Address      OS          ESSID    Access Point  Channel  Type  Role
IPv6 Address  Signal          Speed (mbps)
-----
02fd71954de4  10.10.22.29     02:fd:71:95:4d:e4 Win 10      Bguest    bldg-a        6        GN    guest-redirect-B
fe80::d279:9595:a12f:6105 34(good) 78(ok)
Number of Clients :1
Info timestamp    :27975

bldg-a#
```

and checking the gateway's user table and we don't find the user there.

```
(7005_AOS10_gwy1) #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
IP          MAC          Name Role Age(d:h:m) Auth VPN link Connected To Roaming
Essid/Bssid/Phy Profile Forward mode Type Host Name User Type
-----
User Entries: 0/0
Curr/Cum Alloc:0/6 Free:1/6 Dyn:1 AllocErr:0 FreeErr:0

(7005_AOS10_gwy1) #
(7005_AOS10_gwy1) #
```

Now once again we login with the cpguser credentials

Customer: Ariya Publ...

Summary AI Insights Location Sessions Profile

AOS10

Overview Devices Clients

Guests Applications

CLIENTS

ALL

50.41 MB (9.53 MB)

All 2 Connecting 0 Connected 1 Failed 0 Offline 1 Blocked 0 Wireless 2 Wired 0 Remote 0

CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role
cpguser	Connected	10.10.22.29	22	bldg-a	Bguest	Bguest	

```
bldg-a# sh clients

Client List
-----
Name          IP Address      MAC Address      OS          ESSID    Access Point  Channel  Type  Role  IPv6 Address
Signal          Speed (mbps)
-----
02fd71954de4  10.10.22.29     02:fd:71:95:4d:e4 Win 10      Bguest    bldg-a        6        GN    guest-redirect-B
fe80::d279:9595:a12f:6105 34(good) 78(ok)
Number of Clients :1
Info timestamp    :27975

bldg-a#
```

```

-----
-----
cpguser 10.10.22.29 02:fd:71:95:4d:e4 Win 10 Bguest bldg-a 56E AC Bguest
fe80::d279:9595:a12f:6105 39(good) 526(good)
Number of Clients :1
Info timestamp :28289

bldg-a#

```

checking the access tracker.

#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	
1.	10.10.10.47	CP1-611	RADIUS	cpguser	simple MAC Authentication	ACCEPT	gg Aruba Bguest access, gg MAC Auth Session Timeout	1
2.	10.10.10.47	CP1-611	RADIUS	cpguser	Simple User Authentication with MAC Caching	ACCEPT	gg MAC Caching Session Limit, gg Guest MAC Caching, [Update Endpoint Known], gg MAC Caching Do Expire, gg MAC Caching Expire Post Login, gg Aruba Bguest access, gg MAC Caching Session Timeout	1
3.	10.10.10.47	CP1-611	RADIUS	02fd71954de4	simple MAC Authentication	REJECT	[Deny Access Profile]	1