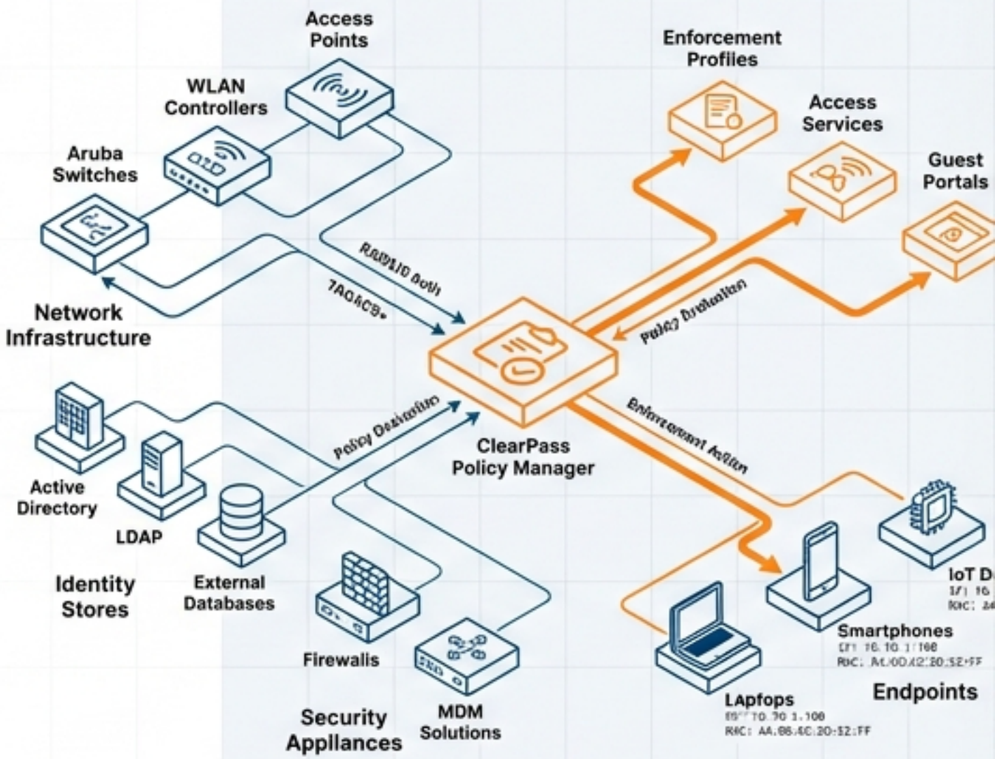
ClearPass Policy Manager: Operational Architecture & Security Policy Analysis

As-Built Documentation and Configuration Review for Environment LAB02

December 2025 | Version 1.0 | Status: Post-Optimization Review



Executive Summary: A Layered Approach to Network Access Control

1. Infrastructure Integrity

Validation of the High Availability (HA) cluster status and replication health between Publisher and Subscriber nodes ensures a stable enforcement engine.

2. Service Logic

Analysis of the linear evaluation models used to differentiate between Wired, Wireless, Guest, and Administrative traffic.

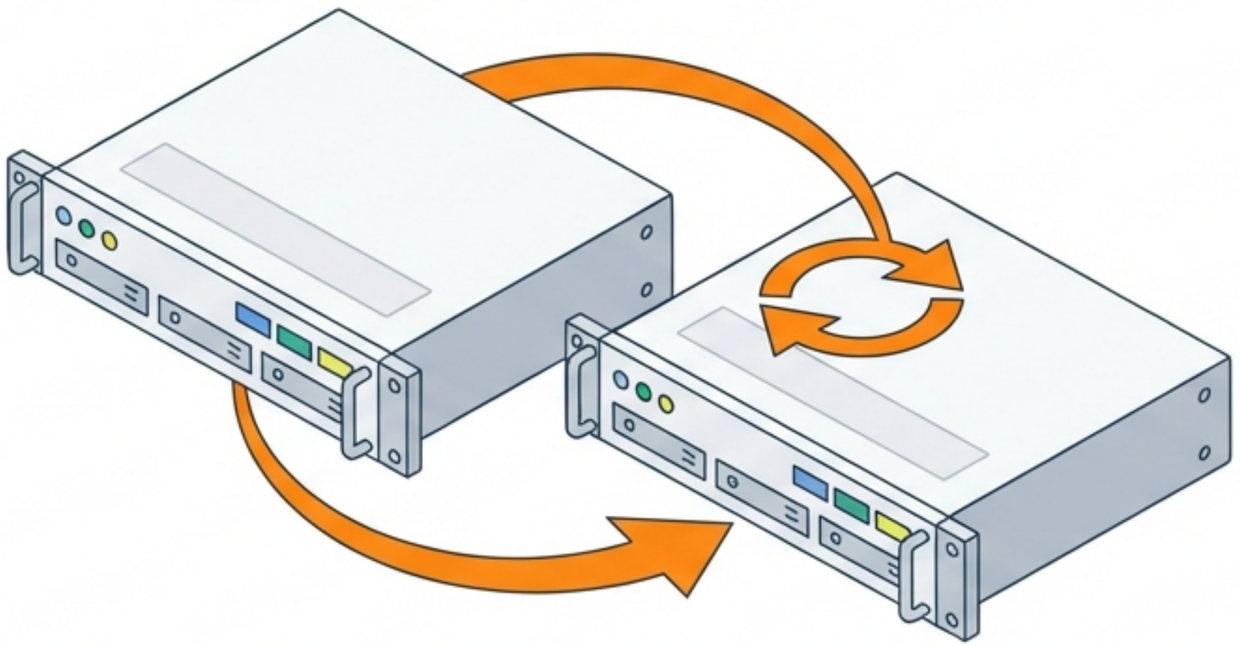
3. Optimization History

A review of the configuration changes from December 6th to December 8th, highlighting the transition from draft policies to a refined production state.

Key Insight: The environment utilizes a ‘First Match’ evaluation logic, requiring precise ordering of services to prevent security gaps. The current configuration reflects a successfully optimized hierarchy.

The Foundation: Infrastructure Health & Redundancy

Before enforcing policy, we must validate the stability of the enforcement engine.



Cluster Status: Active High Availability Confirmed

Status	Host Name	Management IPv4	Server Role	Last Replication	Status Message
✓	cppm	10.0.60.5	Publisher	-	OK
✓	cppm02	10.0.60.2	Subscriber	Dec 08, 2025 11:53:57 UTC	OK

Replication Health

Last Sync: Dec 08, 2025 11:53:57 UTC

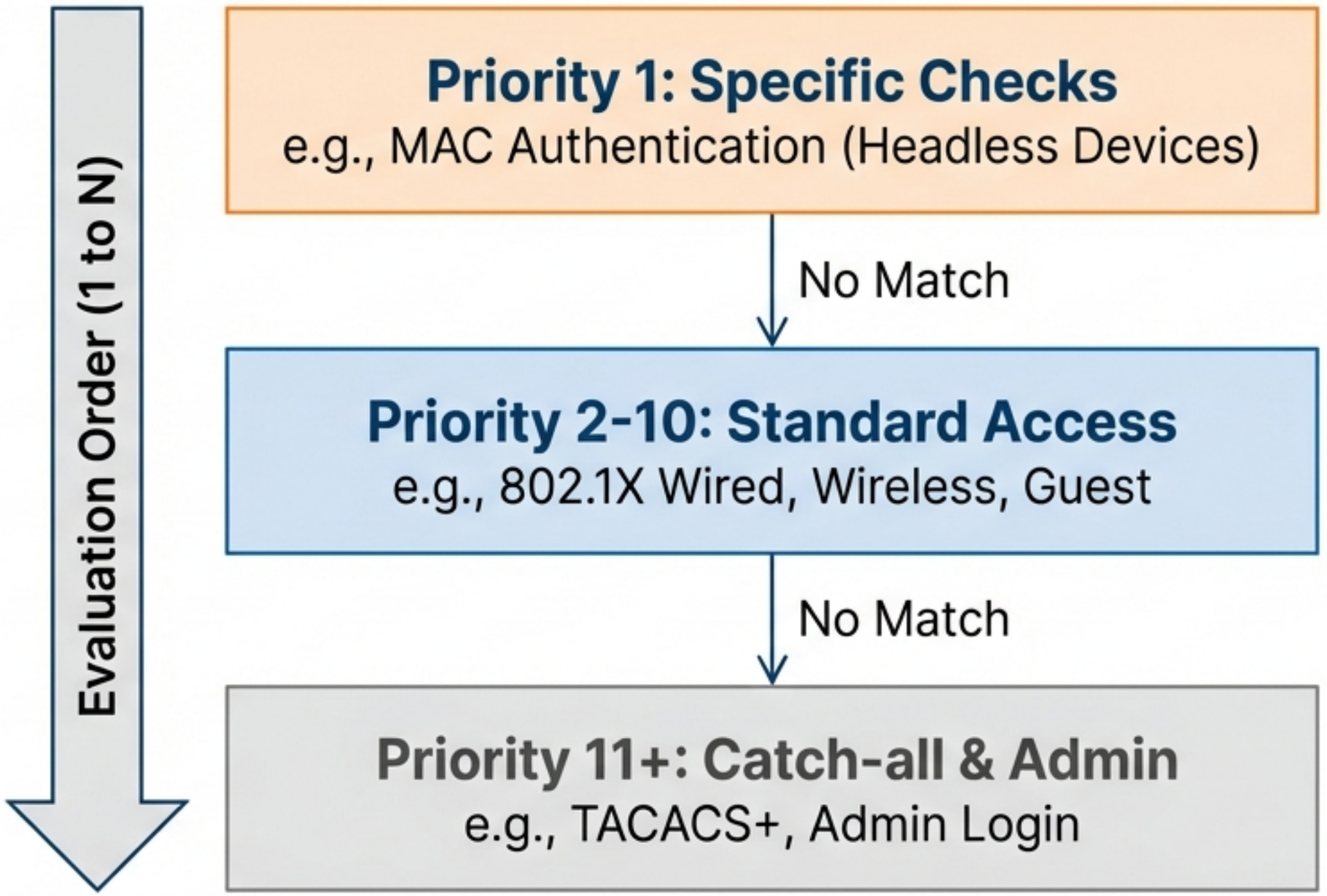
Status: Nominal

The environment is operating in a healthy cluster state. The Subscriber ('cppm02') is successfully replicating data from the Publisher ('cppm'), ensuring no single point of failure for authentication requrests. Both nodes report an 'OK' status with valid RFC1918 internal IP addressing.

The Decision Engine: Service Evaluation Logic

Understanding how ClearPass filters and processes incoming authentication requests.

The “First Match Wins” Evaluation Strategy



Linear Processing:
The Policy Manager evaluates requests linearly from top to bottom. Once a request matches the criteria of a service, processing stops.

Strategic Ordering:
Specific authentication types, such as MAC Authentication for headless devices, are placed at Index 1. This prevents them from failing against stricter 802.1X policies that might be lower in the list.

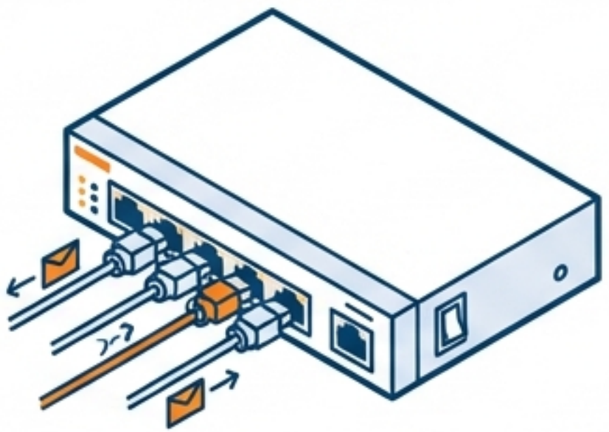
aruba

Use Case Analysis

Categorizing security policies by function: Corporate, Guest, and Administrative.

Corporate

Guest



Administrative

Corporate Network Access (802.1X)

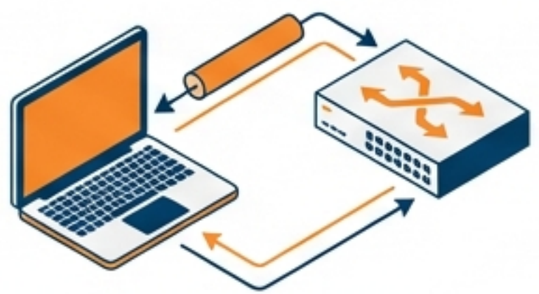
Order	Name	Type	Template
2	LAB-TEAP	RADIUS	802.1X Wired
4	Lab-WIFI-LAB	RADIUS	802.1X Wireless
5	LAB-EAP-DUR	RADIUS	802.1X Wired

TEAP Integration

Utilization of Tunnel Extensible Authentication Protocol (TEAP) suggests a high-security posture for corporate devices, allowing chaining of authentication methods inside a secure tunnel.

DUR (Downloadable User Roles)

The presence of 'DUR' in service names indicates dynamic policy enforcement. Upon authentication, the ClearPass Policy Manager pushes the specific switch configuration (ACLs, VLANs) to the network device, centralizing control.



Guest Access & Web Authentication

Order	Name	Type	Template
3	LAB-WIRED-GUEST	WEBAUTH	Web-based Authentication
7	LAB-Onboard	Application	Aruba Application Authentication
9	LAB-Posture	WEBAUTH	Web-based Health Check Only
13	LAB02-GUEST MAC…	RADIUS	MAC Authentication

Web-Based Authentication

Unlike corporate traffic which uses 802.1X, guest traffic is handled via Captive Portals (WEBAUTH). This allows for self-registration or sponsored access for unmanaged devices.

Health & Posture

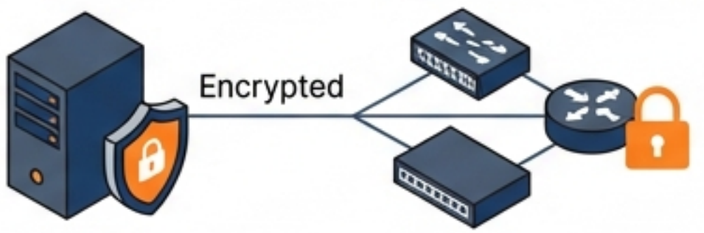
The ‘LAB-Posture’ service functions as a gatekeeper, ensuring devices meet specific health criteria (OS updates, antivirus status) before full network access is granted.

Infrastructure Management & Device Administration

Order	Name	Type	Template
11	LAB-Tacacs+	RADIUS	RADIUS Enforcement (Generic)
15	[Policy Manager Admin...]	TACACS+	TACACS+ Enforcement
17	[Aruba Device Access...]	TACACS+	TACACS+ Enforcement

TACACS+ Enforcement

These services are critical for “Device Administration”—controlling who can log into the switches, routers, and the ClearPass server itself. This separates separates user traffic from management traffic.



Strategic Placement

Placed lower in the evaluation order (Index 11+), these services act as specific enforcers for IT operations. They ensure that administrative credentials are never accidentally processed against a less secure Guest or User policy.

Configuration Evolution

Tracing the optimization of the Policy Manager
from December 6 to December 8.

aruba

Chronological Optimization: Draft vs. Production

Dec 06: The Draft Build

Order	Name
1	LAB-WIRED-GUEST
...	...
14	LAB02-----Tacacs---CPPM-Admin

Inconsistent naming and 'Guest' prioritized over 'MAC Auth'.

Dec 08: The Production Build

Order	Name
1	LAB-MAC Auth
...	...
11	LAB-Tacacs+ (Roboto Mono)

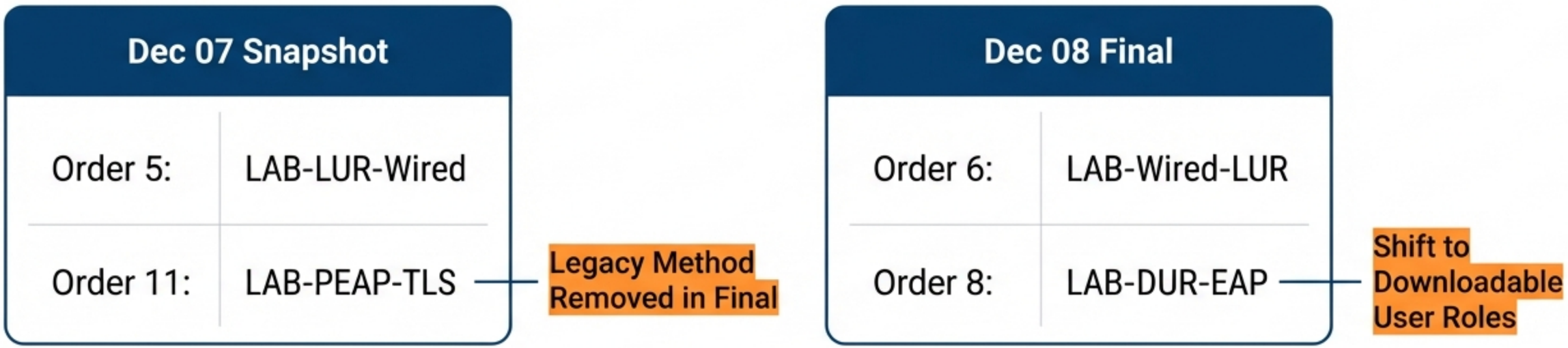
Optimized hierarchy. MAC Auth moved to #1 to prevent timeouts. Naming standardized.

The environment evolved from a functional draft to an optimized hierarchy. Moving MAC Authentication to Order 1 handles headless devices quickly, preventing unnecessary timeouts on 802.1X services.

aruba
Technical Swiss International

Intermediate State Analysis (December 07)

LUR vs DUR Experimentation



This snapshot captures the “Tuning Phase.” We see active experimentation with Local User Roles (LUR) versus Downloadable User Roles (DUR), leading to the final configuration where DUR is prioritized for its centralized management benefits.

aruba

Current Operational State: The Complete Service Table

Snapshot Date: December 08, 2025

Order	Name	Type	Template
1	LAB-MAC Auth	RADIUS	MAC Authentication
2	LAB-TEAP	RADIUS	802.1X Wired
3	LAB-WIRED-GUEST	WEBAUTH	Web-based Authentication
4	Lab-WIFI-LAB	RADIUS	802.1X Wireless
5	LAB-EAP-DUR	RADIUS	802.1X Wired
6	LAB-Wired-LUR	RADIUS	802.1X Wired
7	LAB-Onboard	Application	Aruba Application Authentication
8	LAB-DUR-EAP	RADIUS	802.1X Wired
9	LAB-Posture	WEBAUTH	Web-based Health Check Only
10	Lab-Onboard	Application	Aruba Application Authentication
11	LAB-Tacacs+	RADIUS	RADIUS Enforcement (Generic)
12	LAB-EAP-AD	RADIUS	802.1X Wired
13	LAB02-GUEST MAC…	RADIUS	MAC Authentication
14	LAB02-GUEST User…	RADIUS	RADIUS Enforcement (Generic)
15	[Policy Manager Admin…]	TACACS+	TACACS+ Enforcement
16	[AirGroup Auth…]	RADIUS	RADIUS Enforcement (Generic)
17	[Aruba Device Access…]	TACACS+	TACACS+ Enforcement

aruba

Technical Swiss International

December 08, 2025

Final Assessment

Status: Healthy. The cluster is redundant with confirmed sub-second replication times between `10.0.60.5` and `10.0.60.2`.

Security: Multi-layered. The configuration successfully layers 802.1X (TEAP/PEAP) for employees, WebAuth for guests, and MAC Auth for IoT, ensuring no coverage gaps.

Management: Active. The audit log proves the environment is being actively tuned and reordered for performance.

Recommendation: Continue monitoring the ‘Hit Count’ metrics to identify and decommission any unused legacy services (such as Row 6 ‘`LAB-Wired-LUR`’) in future sprints.