aruba
a Hewlett Packard
Enterprise company

MOBILE FIRST NETWORK

클리어패스 USE CASE

정규태 이사

Ted Jung(ted.jung@hpe.com)

Security Consulting Engineer

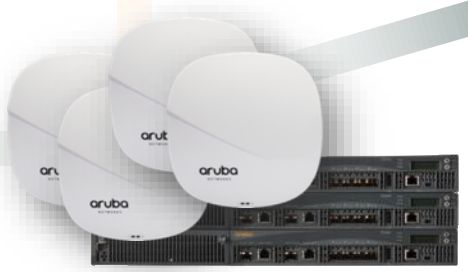
AMFX WW#14

Mobile First Network with ClearPass

Internet of Things (IoT)

Multi-vendor switching

BYOD and corporate owned



Multi-vendor WLANs

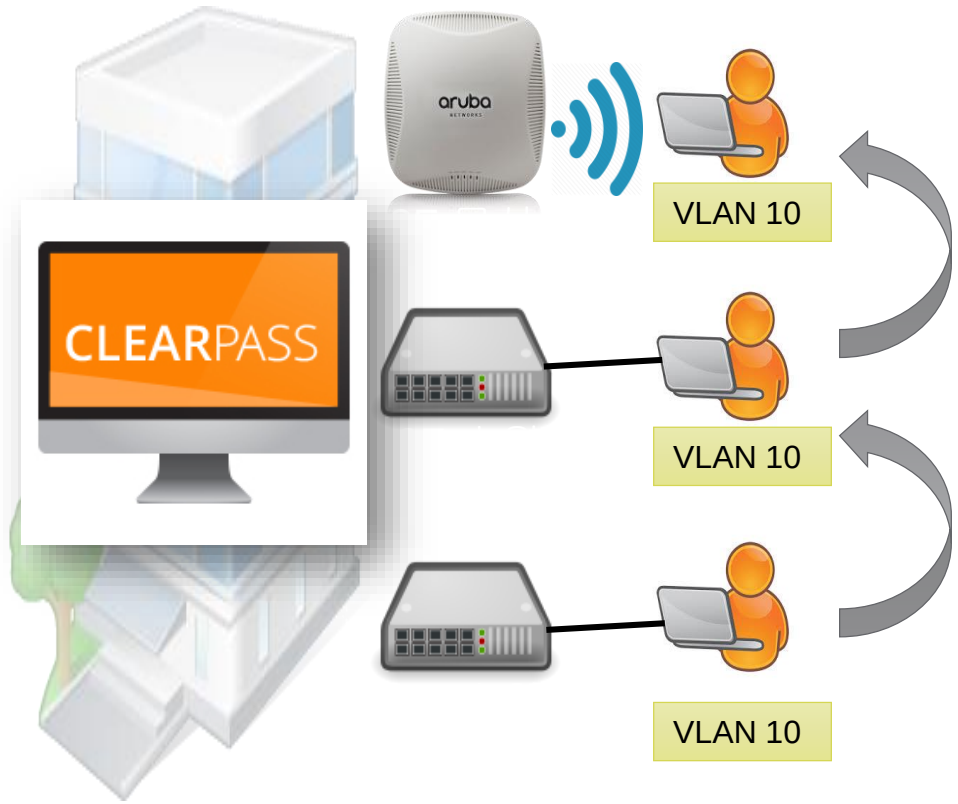
NEW

User/Device Profiling

Who: **Bob**
Group: **Faculty**
Device: **Personal iPad**
Location: **Room 104**
Time: **9am, Monday**
Compliance: **Healthy**
Mac Address: X
IP Address: Y
Airgroup **Permissions**

Aruba ClearPass
- RADIUS
- TACACS+
- 802.1x
- MAC 인증
- OnConnect for IOT

Dynamic Network with Multi-Vendor



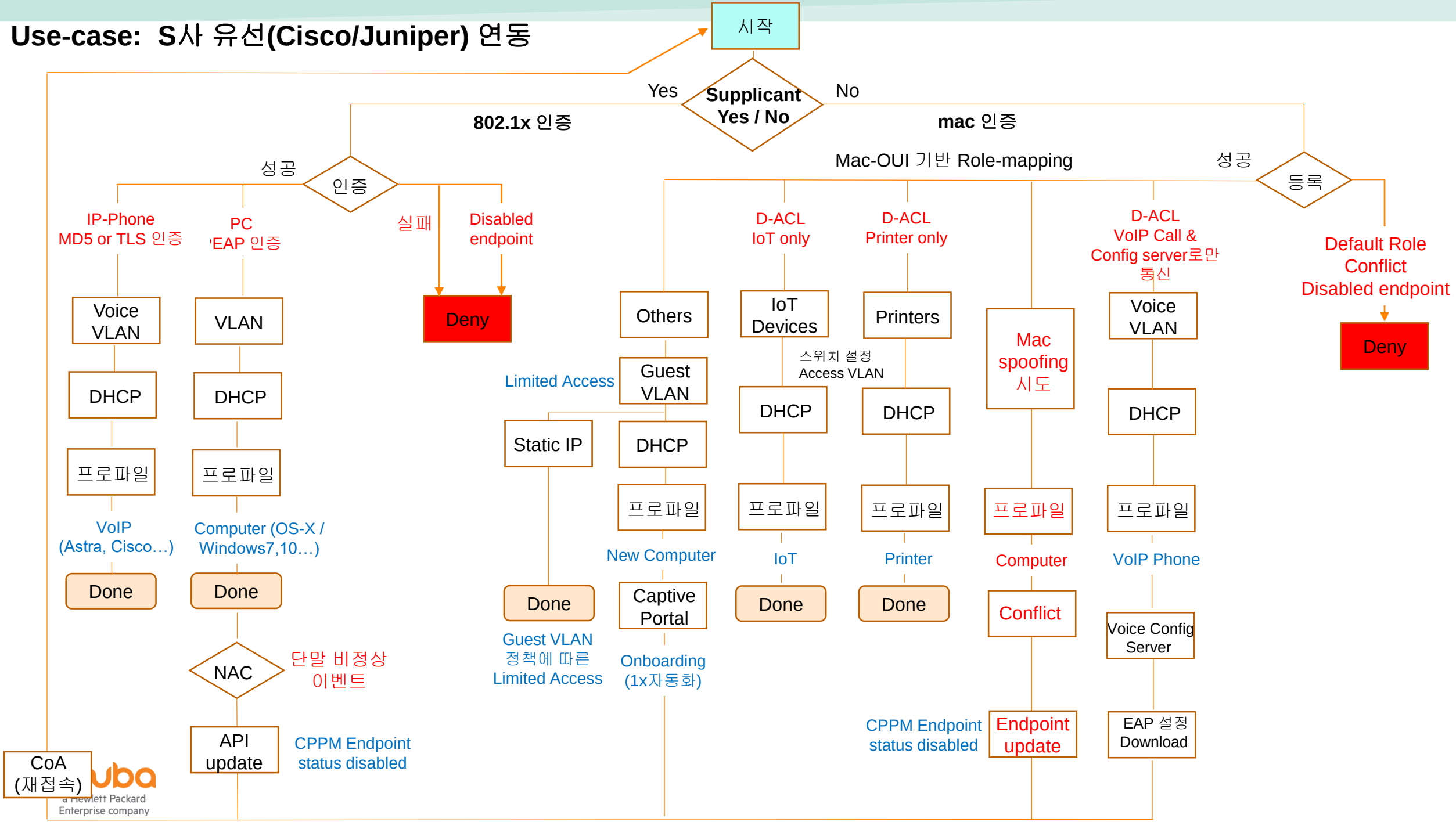
Dynamic VLAN

- HPE Aruba, Brocade, Cisco, Alcatel등 802.1x를 지원하는 모든스위치에 적용 가능
- 사용자 인증 성공시 부서에 따른 VLAN할당
- 매년 최소 1회 이상의 조직 변경

Dynamic ACL

- HPE Aruba, Cisco, Alcatel등의 벤더에서 사용자인증결과에 따라 네트워크 접근권한을 할당 (NAC)
- 사용자 인증 성공시 부서에 따른 ACL할당
- 사용자 세션별 ACL이 적용 되어 보안향상

Use-case: S사 유선(Cisco/Juniper) 연동



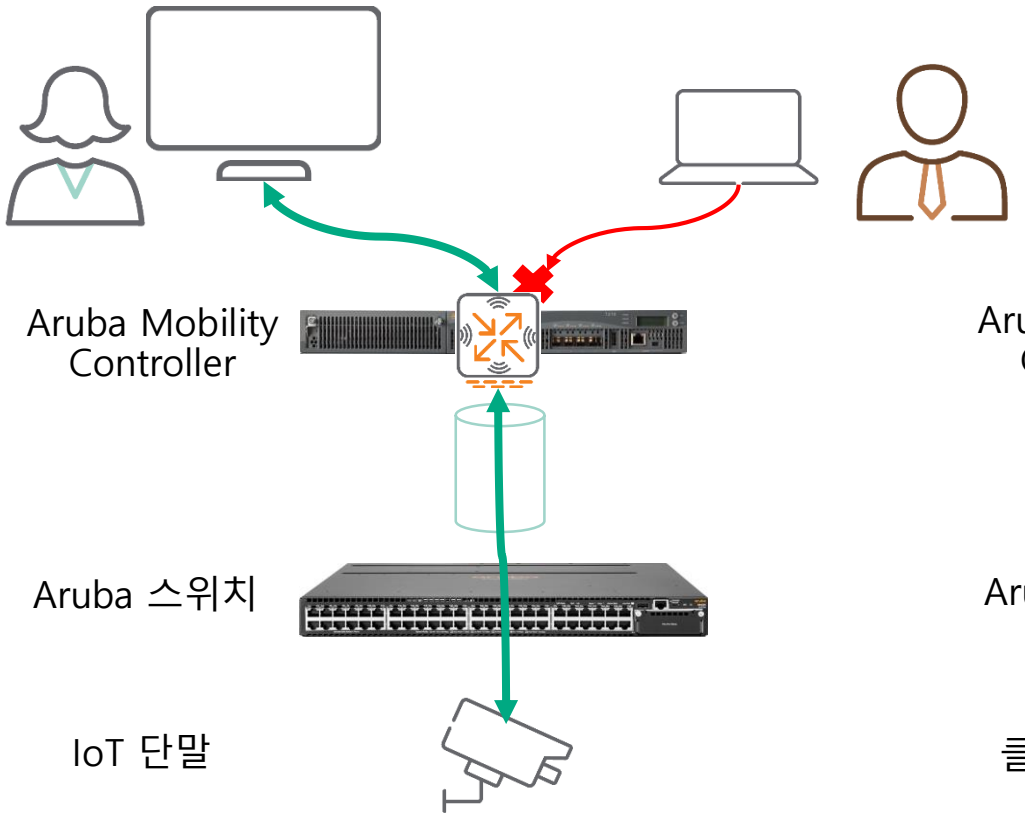
Aruba Mobile First Network

유무선 모빌리티 & 보안 모델

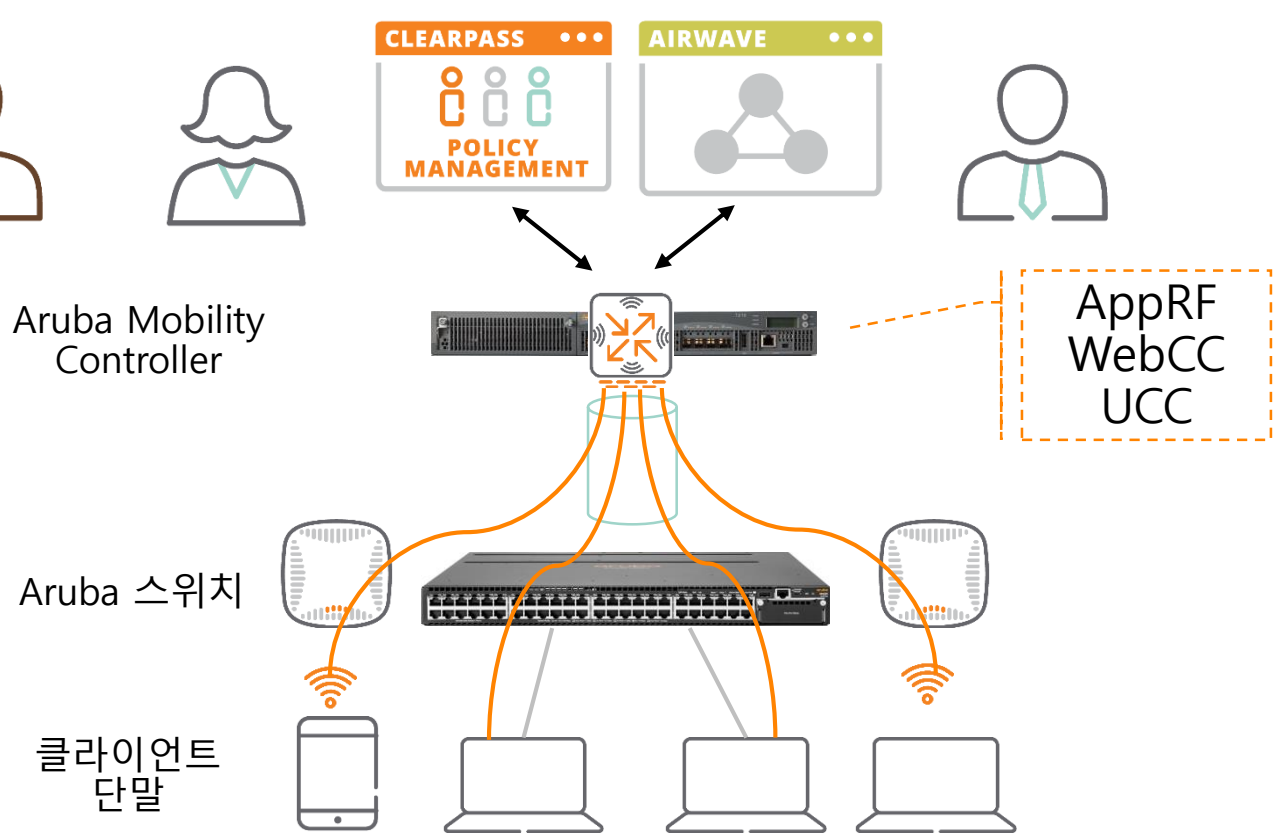
aruba
a Hewlett Packard Enterprise company

Dynamic Segmentation

고객의 주요 자산 보호



통합 정책 및 가시성



aruba
a Hewlett Packard Enterprise company

Downloadable User Roles

단일의 정책 관리 시스템

– ClearPass를 통해서
  단말 인증시 자동으로 정책 적용

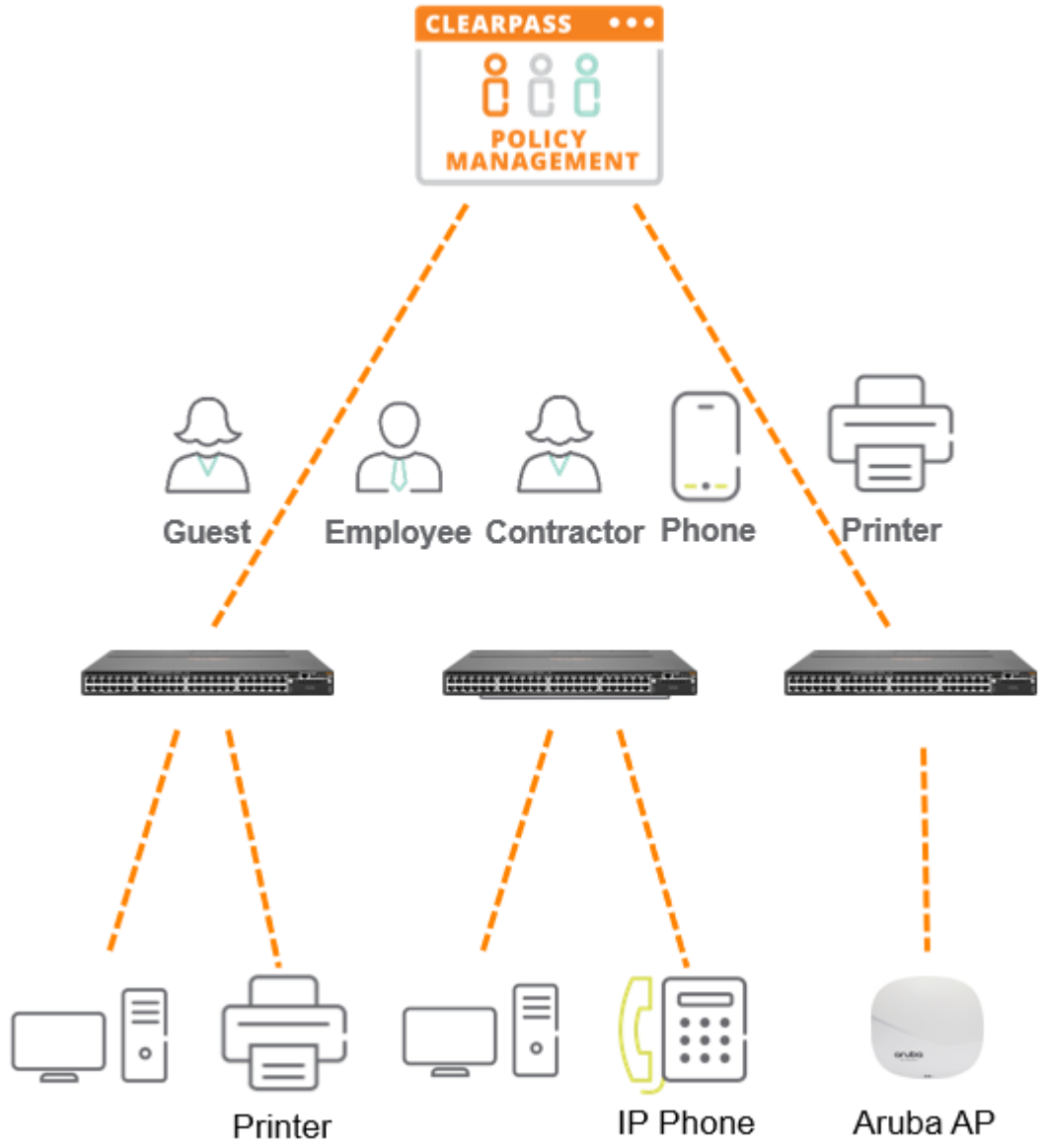
기존 사용자/단말 위에 **Role(역할)** 생성

– 모든 사용자와 단말에 Role을 할당

– Role에 따른 정책(QoS, VLAN, ACL, Rate Limits)
  적용

유무선 통합 정책 관리

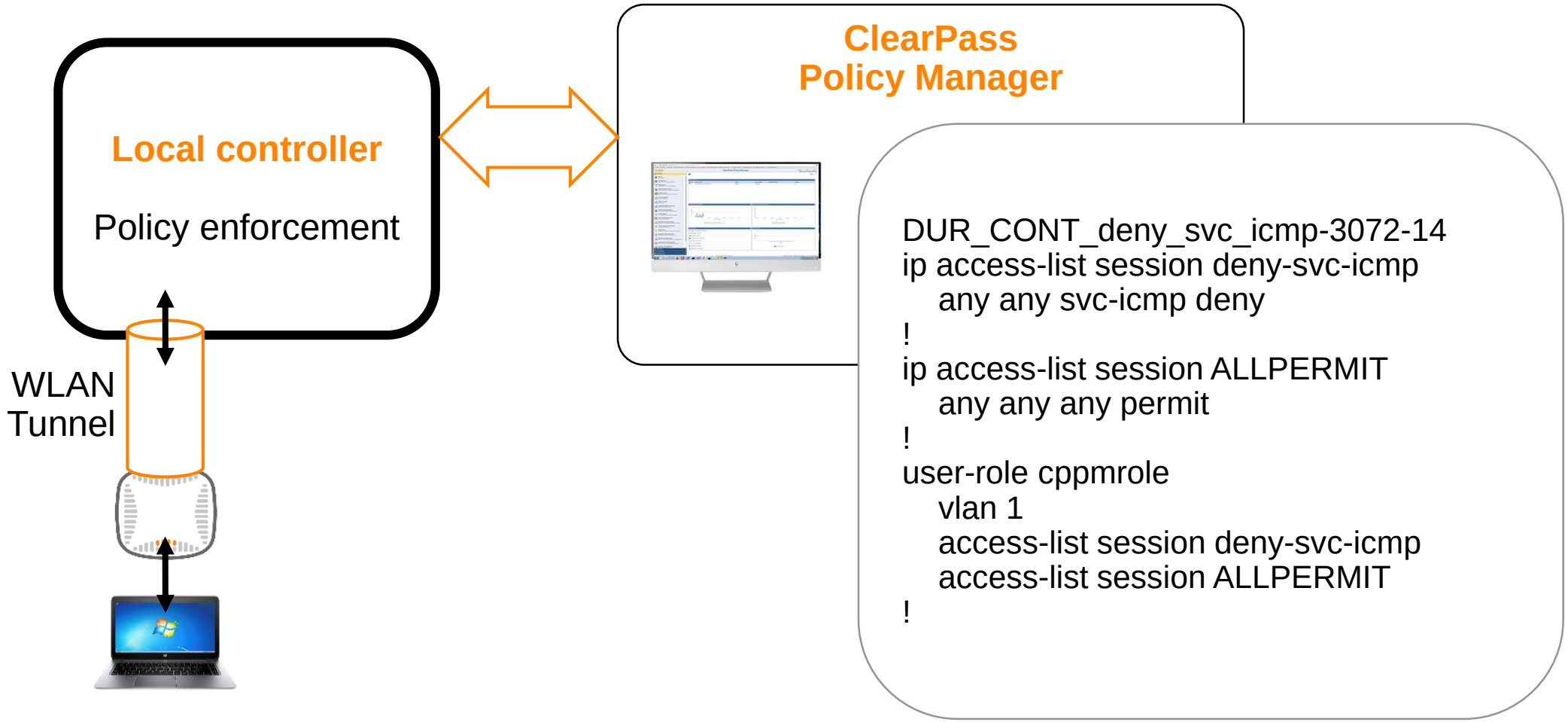
– 무선 AP와 마찬가지로 간단한 정책 구성 및 관리



*ArubaOS-Switch 16.04 이후부터 가능

aruba
a Hewlett Packard Enterprise company

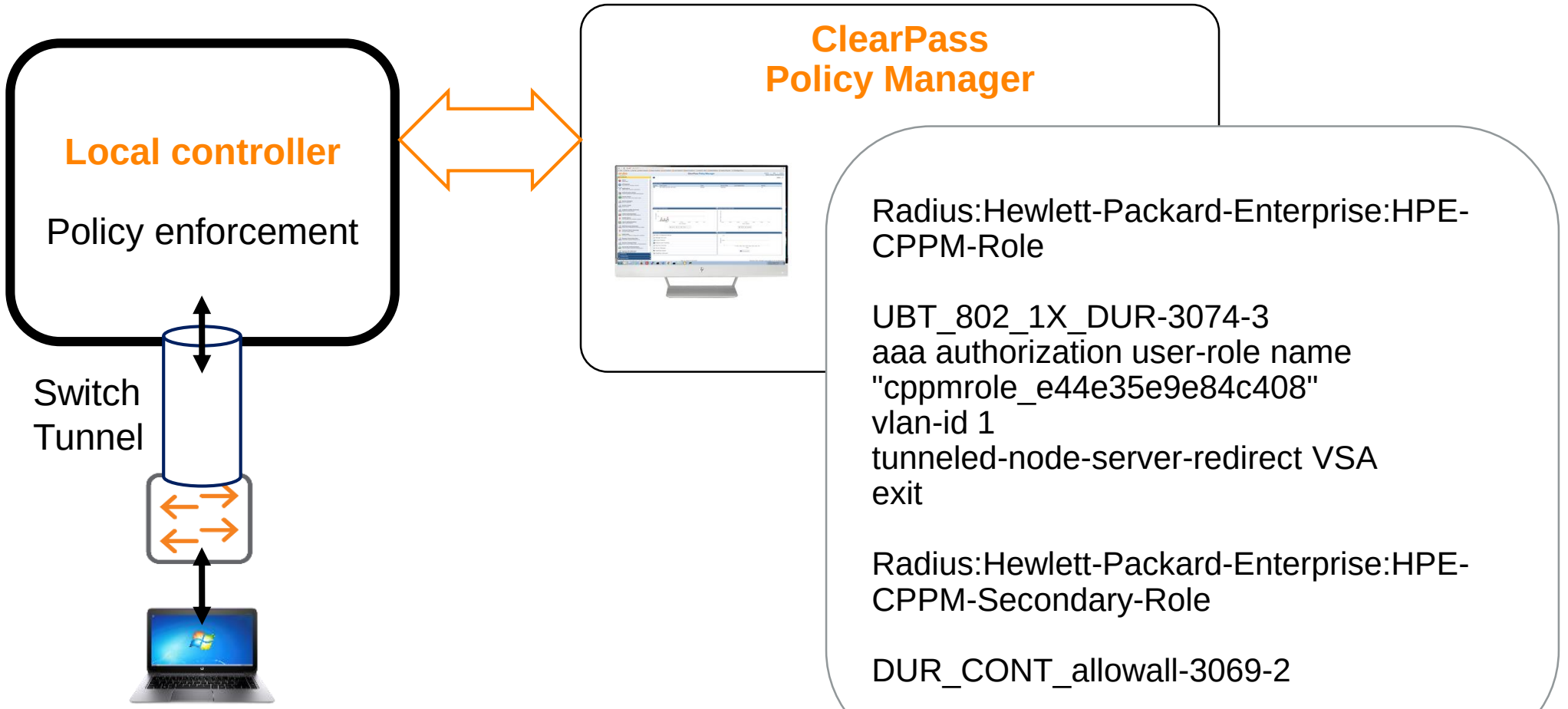
Aruba Controller DUR(Downloadable User Role)



Aruba Controller DUR(Downloadable User Role)

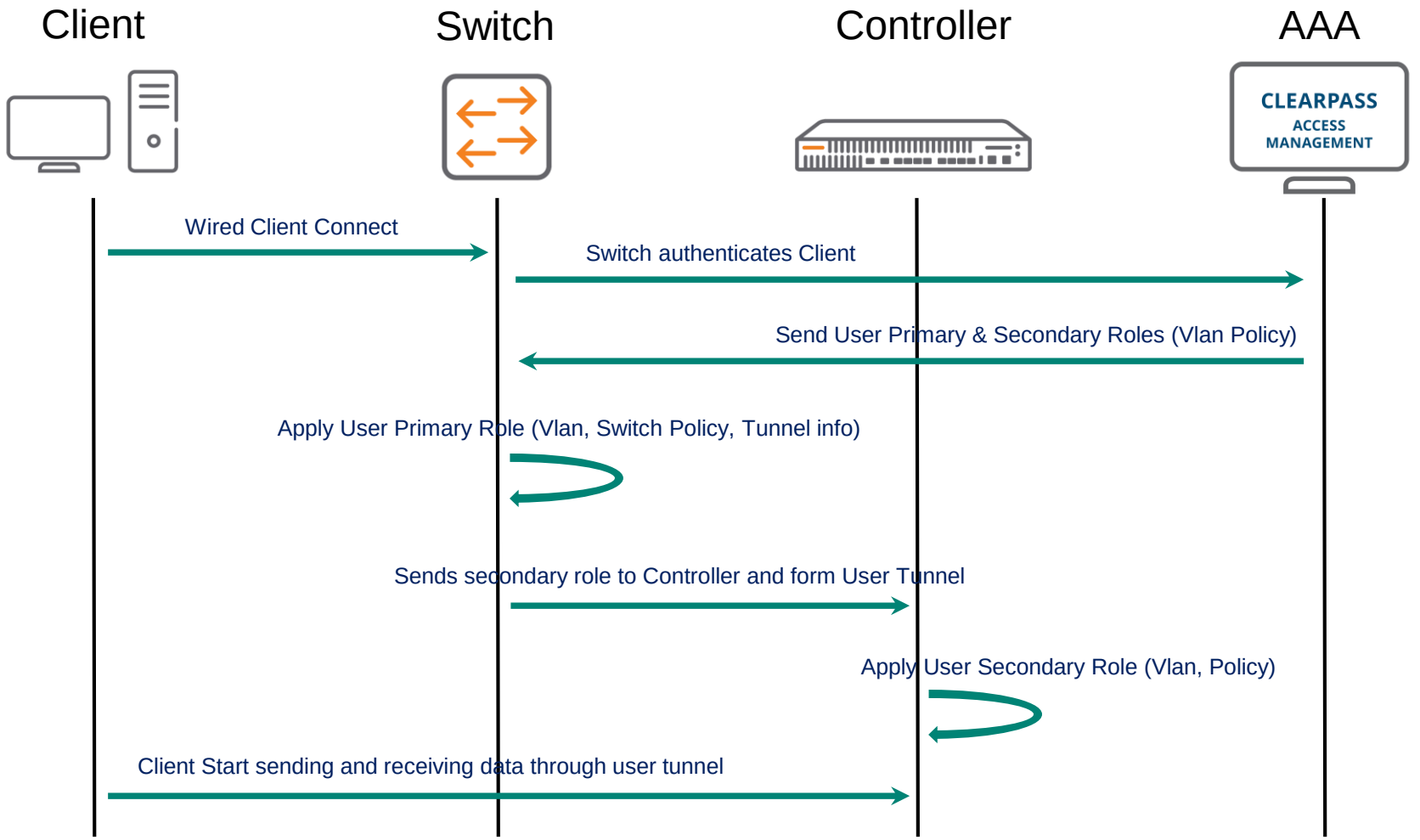
DEMO

Switch Tunnel with DUR(Downloadable User Role)



User-Based Tunneling (UBT)

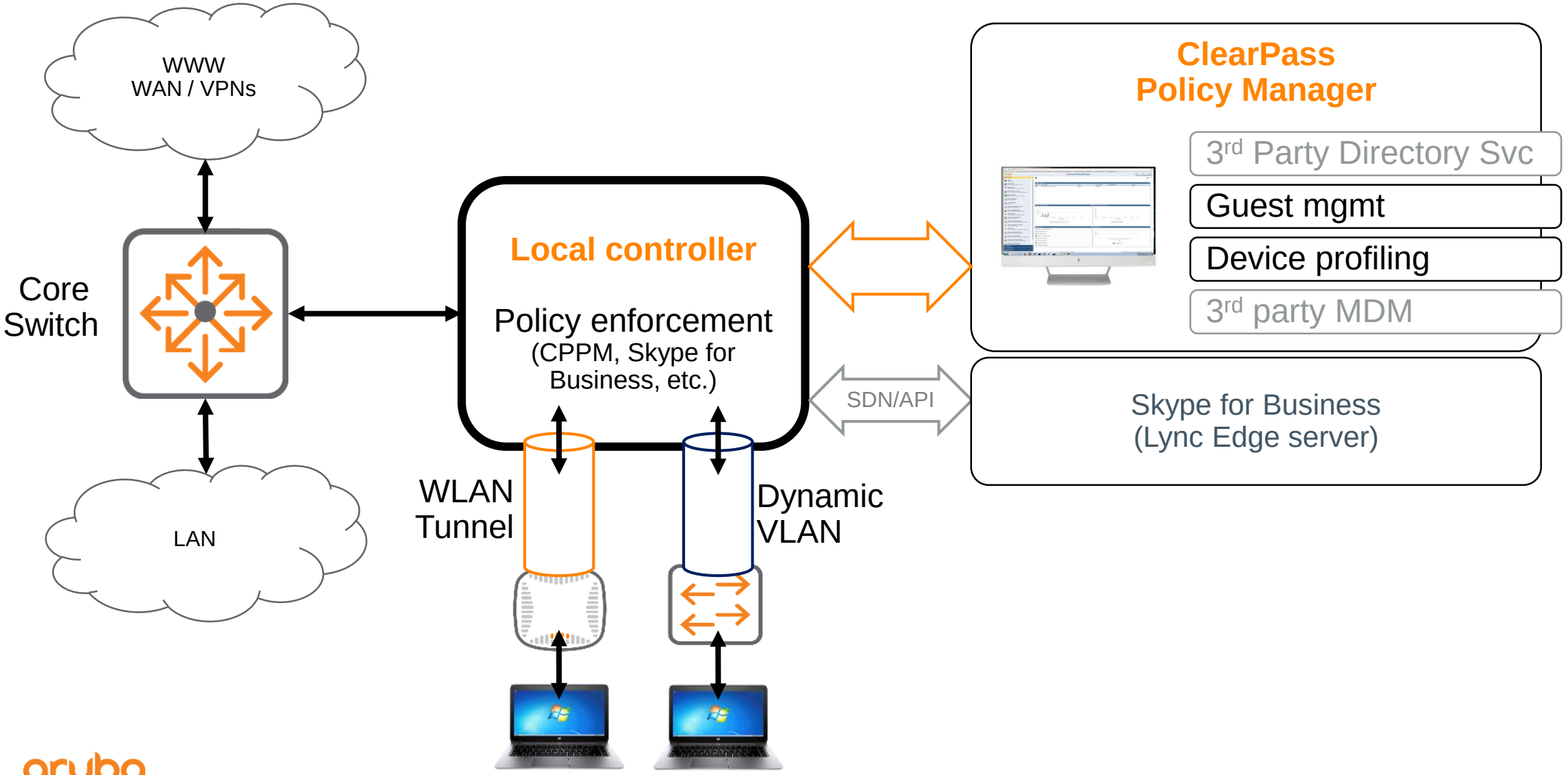
Wired Client Flowchart



Switch Tunnel with DUR(Downloadable User Role)

DEMO

Aruba Mobile First Network



aruba
a Hewlett Packard
Enterprise company

Aruba Mobile First Network

APP-RF & Airwave
DEMO

New Features in ArubaOS/InstantOS 8.4

Common Features

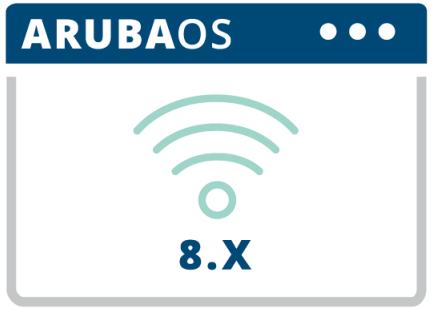
Wi-Fi CERTIFIED WPA3

Wi-Fi CERTIFIED Enhanced Open

Multi-PSK (MPSK)

Support for AP-303P

New 4G Modems



ArubaOS 8.4

IoT management (enhanced)

NetInsight Integration (enhanced)

Dynamic Segmentation (enhanced)

Multi-language support

AP provisioning UI/UX

Simple WAN features (enhanced)

InstantOS 8.4

UI Enhancements

PnP Mesh

Downloadable roles

Aruba Mobility Master – Virtual and Hardware appliance

Aruba Mobility Master Controller-VA

Aruba Mobility Master Controller - HW

Next generation Master controller

- **Centralized management**
- **Hitless failovers** during controller failures
- **Real-time upgrade** with no downtime
- **User and AP load balancing** across controllers
- **Automated RF management** for better network throughput in congested environment
- **Multi-tenant wireless networks** for better network efficiency
- Network intelligence with **NBAPIs**

Aruba Virtual Mobility Controllers

Aruba Mobility Controllers

MM VA/HW which one should I use?
Whatever works best with your operational standards.

aruba
a Hewlett Packard Enterprise company

Mobility Controller options – Virtual and hardware appliance

Virtual Mobility Controllers

Mobility Controller Virtual Appliance

- Ease of moves, changes and use
- 99% feature parity with hardware appliance
- Cost effective if building for redundancy
- Operate as a standalone controller or managed by the Mobility Master

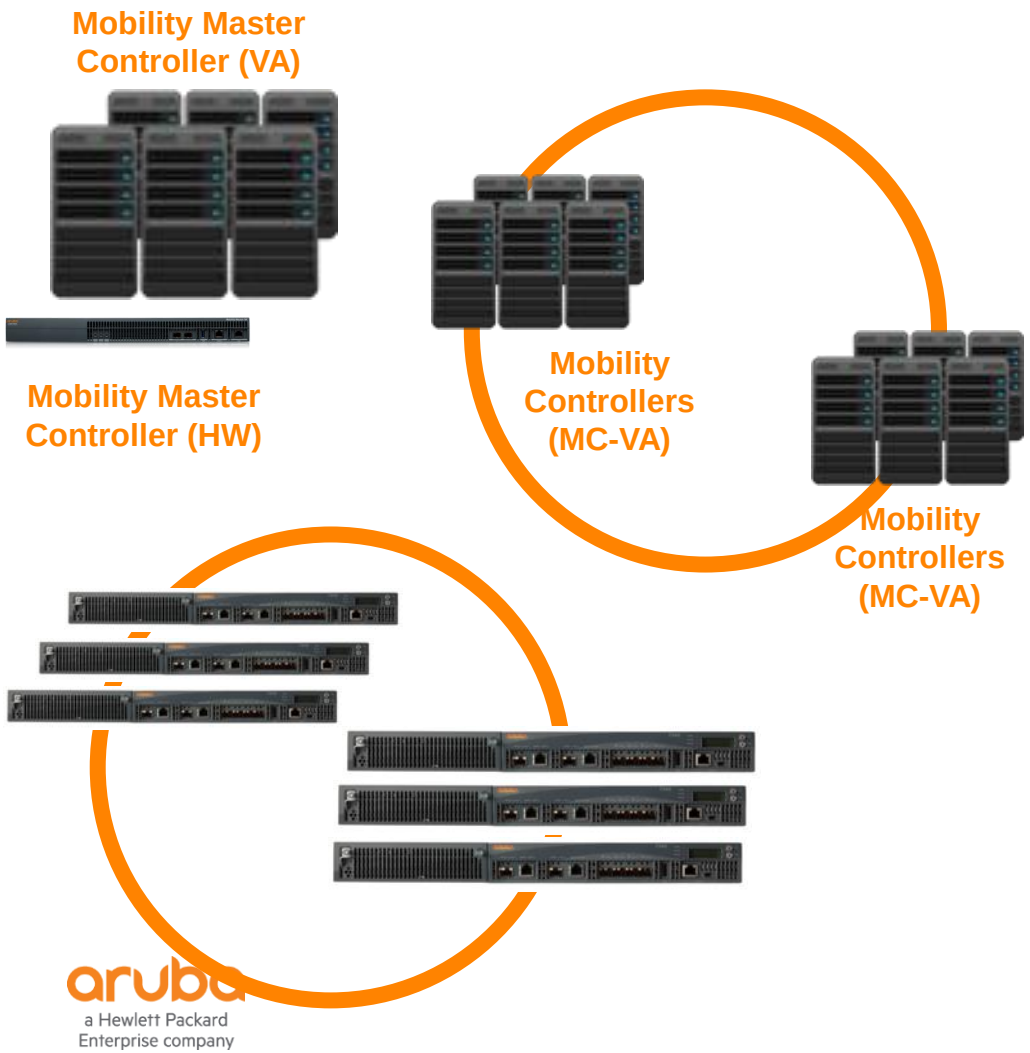
Mobility Controller Hardware

- 70xx and 72xx supported in 8.x
- Simplified support model
- Cost effective for high throughput needs
- Operate as a standalone controller or managed by the Mobility Master

aruba
a Hewlett Packard Enterprise company

컨트롤러 클러스터링 – 완벽한 안정성 제공

New AOS8



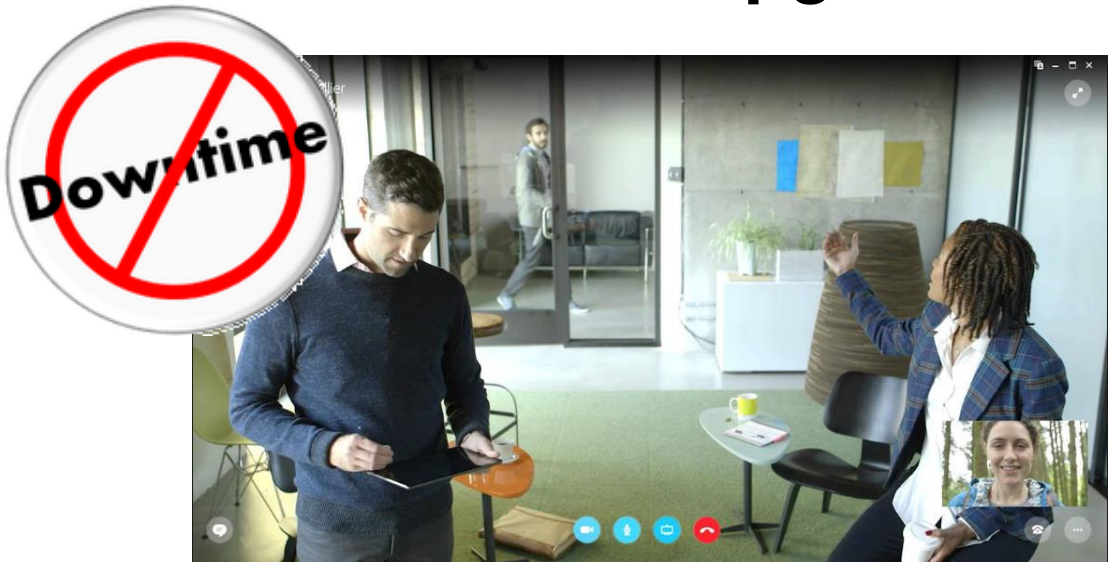
Controller Clustering

- **Seamless 컨트롤러 Failover**
  - 실시간 보이스 또는 비디오에 영향 없음
- 사용자 및 **AP** 로드밸런싱

- 자원의 효율화 및 확장성 제공

- 클러스터 내에서의 완벽한 로밍

Reliable network upgrade



New AOS8

Live Upgrade

Real-time upgrade to the latest OS with min downtime

- No need for through upgrade planning or maintenance window
- Healthcare, Higher Ed and manufacturing cannot afford downtime

In-service Upgrade

- Upgrade major features and functions, such as NB APIs, AirGroup, AppRF, ClientMatch

Multi-OS support

- Run multiple OS on the network- A gradual migration tool to adopt new innovations while minimizing risk.
- Only available on ArubaOS 8.2 +

*The average Fortune 500 company experiences 1.6 hours of downtime per week. That's **$164m in lost productivity every year.***

aruba
a Hewlett Packard Enterprise company

Controller Clustering
컨트롤러 장애시에도 단말 영향 없음

Hit-less failover
Demo

aruba

a Hewlett Packard Enterprise company

SAML

Paul Kim (paul.kim@hpe.com)

4th, April 2019

Who am I?

- **김민혁 (Paul Kim)**
- **2002 ~ 2012 Developer**
  - 웹 서비스 개발(도메인 등록/그룹웨어/모니터링 등)
  - 임베디드 시스템 개발(UTM 장비 개발)
  - CDN/Cloud 시스템 개발 및 REST API 개발
- **2012 ~ 2018 삼성SDS Security Engineer**
  - 빅데이터 기반의 로그 분석 시스템 개발
  - 삼성 그룹 보안 / 모의해킹 / 취약점 분석 등
- **2018.03 ~ Aruba Systems Engineer**
  - FY18Q3 SE Community Contribution Contest Award
  - CISSP / ACCP / ACMP / ACMX

AGENDA

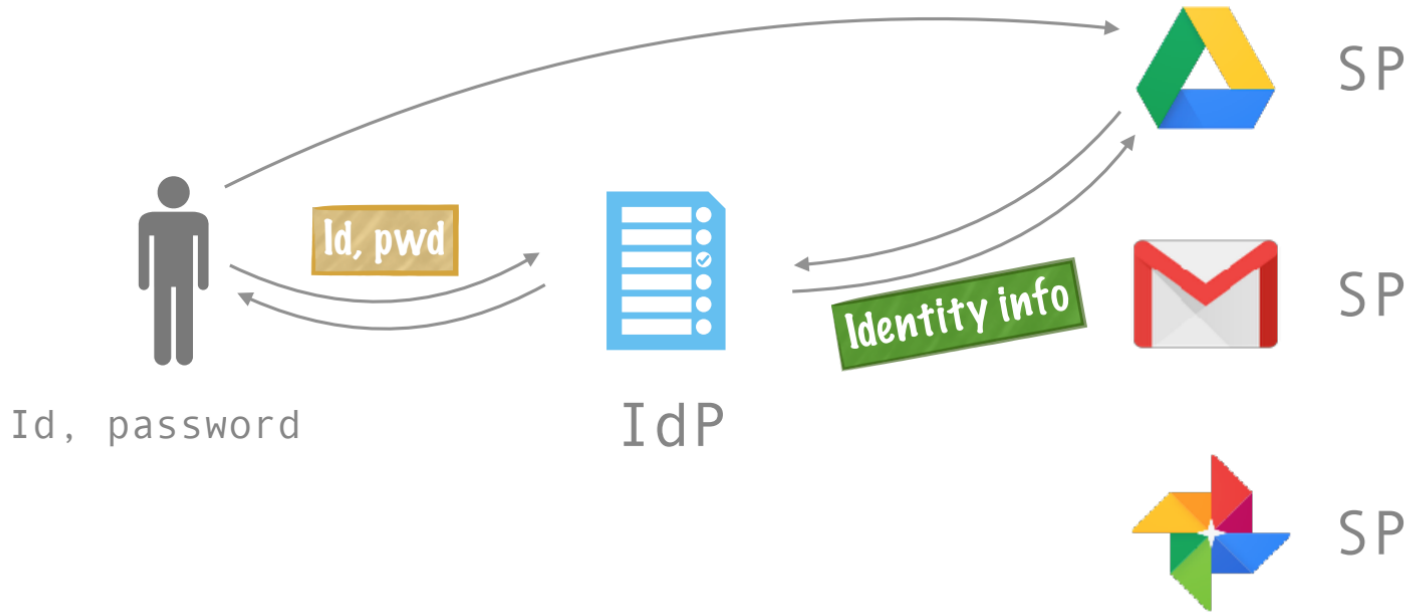
- SAML 개요
- SAML 구성요소
- SAML 동작방식
- SAML와 Clearpass의 연동
- SP로서 CPPM과 SAML 연동 (Demo)
- IdP로서 CPPM과 SAML 연동 (Demo)

SAML 개요

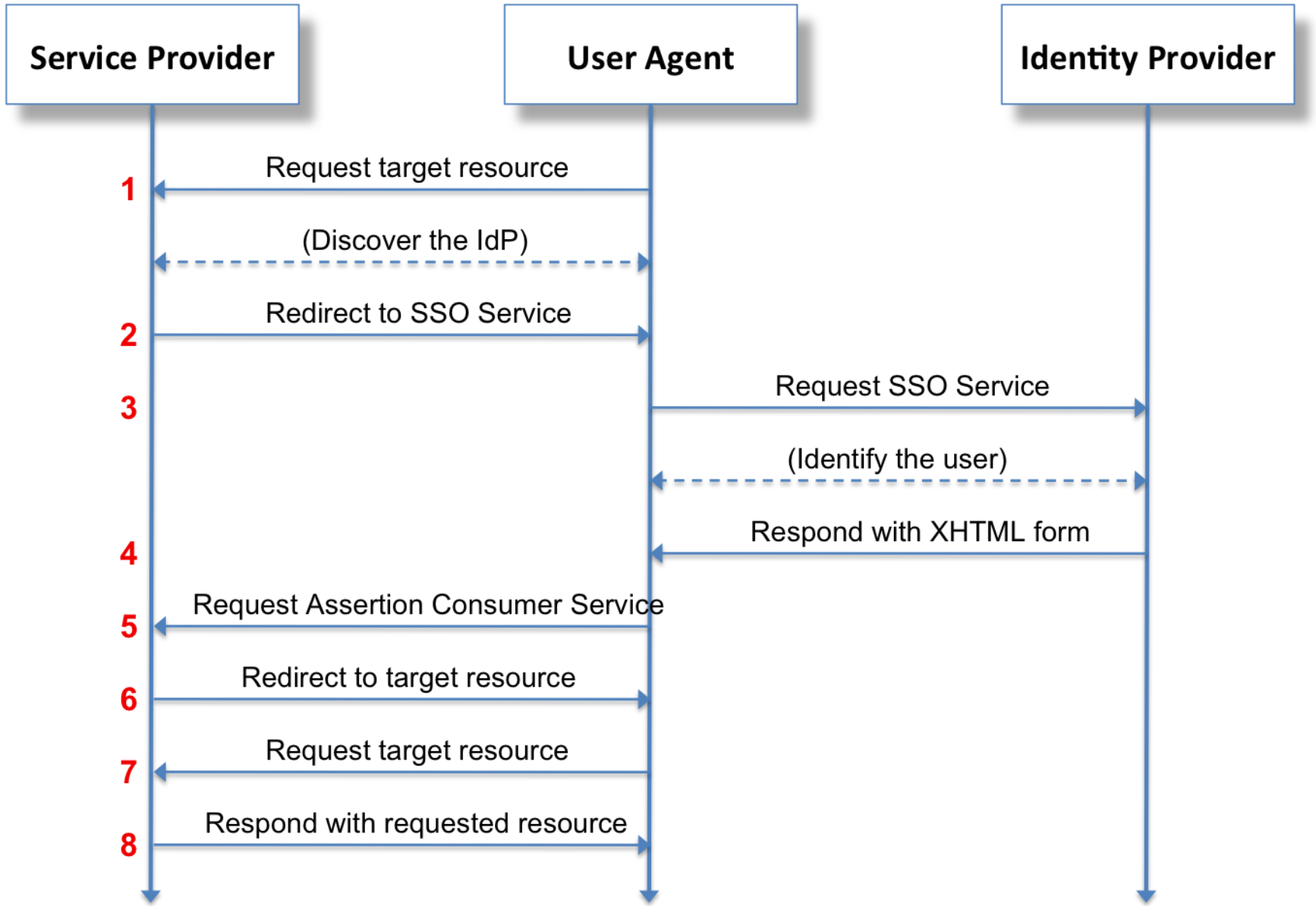
- Security Assertion Markup Language (SAML, "sam-el")
- OASIS의 Security Service Technical Committe에서 정의(2005년)
- 도메인간에 인증(authentication)과 권한부여(authorization)에 관련된 자료를 교환할 수 있는 XML 기반의 표준
- Cross Domain 간 Single Sign On을 지원하기 위한 프로토콜

SAML 구성요소

- User : 서비스를 이용하는 사용자
- SP(Service Provider) : 서비스를 제공하는 주체
- IdP(Identify Provider) : 유저에 대한 인증을 담당하는 주체



SAML 동작방식



aruba
a Hewlett Packard Enterprise company

SAML와 Clearpass의 연동

- Claerpass 6.1부터 SAML 지원.
- Clearpass 는 SP, IdP 으로 모두 사용가능.
- Clearpass as Service Provider
  - Guest / Insight / Onboard / Policy Manager
- Clearpass as Identity Provider
  - Authentication Source

SP로서 CPPM과 SAML 연동

- Clearpass Insight 서비스를 SP으로 SAML으로 연동.
- SAML Idp는 SimpleSAMLphp 사용(idp.apollo89.com)
- Insight 접속 시 idp.apollo89.com 으로 Redirect
- idp.apollo89.com 에서 인증 완료시 Insight 서비스 사용.

Demo : SP로서 CPPM과 SAML 연동

ClearPass - Aruba Networks

https://cppm.apollo89.com/tips/welcome.action

aruba

ClearPass Policy Manager
Role-based Policies, Enterprise-grade AAA with Device Profiling

ClearPass Guest
Guest Management

ClearPass Onboard
Mobile Devices Provisioning

ClearPass Insight
Advanced Analytics, In-depth Reporting, Compliance & Regulation

IdP로서 CPPM과 SAML 연동

- Clearpass Insight 서비스를 SP으로 SAML으로 연동.
- SAML Idp는 Clearpass으로 사용
- Insight 접속 시 Clearpass web login 으로 Redirect
- Clearpass web login 에서 인증 완료시 Insight 서비스 사용.

Demo : IdP로서 CPPM과 SAML 연동

ClearPass - Aruba Networks

https://cppm.apollo89.com/tips/welcome.action

aruba

ClearPass Policy Manager
Role-based Policies, Enterprise-grade AAA with Device Profiling

ClearPass Guest
Guest Management

ClearPass Onboard
Mobile Devices Provisioning

ClearPass Insight
Advanced Analytics, In-depth Reporting, Compliance & Regulation

References

- SAML Configuration Guide v1.5.pdf
- https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language
- https://simplesamlphp.org/
- https://hanee24.github.io/2018/08/04/sso/
- https://stackoverflow.com/questions/2837553/saml-vs-federated-login-with-oauth

AMAZING EXPERIENCES WITH AMAZING SIMPLICITY

a Hewlett Packard
Enterprise company