DATA SHEET

ARUBAOS 8

모바일 업무환경을 위한 스마트 OS

소개

모바일 디바이스, IoT, 비즈니스 크리티컬 애플리케이션들은 모바일 근무자들의 생산성과 효율성을 향상시키는 동시에, 네트워크 요구를 가중시킵니다.

ArubaOS는 Aruba Mobility Controller, Virtual Mobility Controller, Mobility Master, 컨트롤러 매니지드(controller-managed) 무선 AP를 위한 OS입니다. 다양한 기술과 기능이 통합된 ArubaOS 8은 유무선 통합 액세스, 끊김 없는 로밍, 엔터프라이즈급 보안, 그리고 고밀도 환경 지원에 필요한 성능, 사용자 경험, 안정성을 보장하는 올웨이즈 온(always-on) 네트워크를 제공합니다.

모빌리티 마스터(Mobility Master)는 모바일 및 IoT 디바이스로 인한 요구 증가에 따라 네트워크를 확장하고 중앙에서 제어하는데 필요한 고급 기능들을 지원하는 아루바 아키텍처의 새로운 구성요소입니다. 모빌리티 마스터(Mobility Master)는 또한 이전 마스터 컨트롤러의 기능을 대체하며, VM 또는 x86 기반 하드웨어 어플라이언스 형태로 구축 가능합니다. 모빌리티 마스터(Mobility Master)는 자동 RF 최적화를 제공하며, 드물게 컨트롤러 장애가 발생할 경우에 무중단 장애 복구(hitless failover)를 지원합니다.

모빌리티 마스터(Mobility Master)를 사용하는 아루바 기존 고객은 ArubaOS 버전 6에서 버전 8로 업그레이드하여 최신 사양과 기능을 즉시 활용할 수 있습니다. 고객은 타사 통합과 같은 고급 기능들을 활용하기 위해 모빌리티 마스터(Mobility Master)를 기존 인프라에 추가해야 할 것입니다. ArubaOS 8에서 제공되는 기능 상세 목록은 릴리즈 노트에서 확인하기 바랍니다.

다음의 ARUBAOS 8 기술은 모빌리티 마스터(MOBILITY MASTER)에서만 지원됩니다.

기능	이점
AirMatch	아루바는 AirMatch를 통해 ARM(Adaptive Radio Management) 기술을 더욱 향상시킵니다. AirMatch는 새로운 자동 채널 최적화, 전송 출력 조정, 채널 폭 튜닝 시스템으로써 다이나믹 머신러닝 인텔리전스를 활용하여 WLAN 네트워크 전반에 대한 최적의 뷰를 자동 생성합니다.
Controller Clustering	Controller Clustering은 컨트롤러를 최대 12대까지 단일 클러스터화함으로써 대규모 캠퍼스에서 장애가 발생하거나 사용자 밀도가 급증하더라도 끊김 없는 경험을 보장합니다.
MultiZone	모빌리티 마스터(Mobility Master) 내의 최신 MultiZone 기능은 IT 팀이 동일한 물리적 공간에서 동일한 액세스 포인트(AP)를 사용하여 다수의 분리된 보안 네트워크들을 보유할 수 있도록 해줍니다.
NBAPIs	모빌리티 마스터(Mobility Master)는 네트워크에 대한 심층적 가시성을 제공하는 종합적인 노스바운드 API(NBAPI) 세트를 보유하고 있습니다. NBAPI는 RF 상태 통계, 앱 활용, 디바이스 타입, 사용자 데이터 등을 통합하기 쉬운 형태로 제공합니다. 타사 애플리케이션들이 이러한 정보를 컨트롤러로부터 수신하여 분석함으로써 가시성과 모니터링을 향상시킵니다.
In-service module upgrade	모빌리티 마스터(Mobility Master) 상에 탑재된 개별 서비스 모듈(AppRF, AirGroup, ARM, AirMatch, NBAPI, UCM, WebCC, IP Classification)을 전체 시스템 재부팅 필요 없이 다이나믹하게 업데이트할 수 있습니다.

다음은 ARUBAOS의 핵심 기술입니다.	
기능	**이점**
ClientMatch	아루바의 특허 받은 ClientMatch 기술은 스티키 클라이언트(sticky clients) 현상을 제거하여 클라이언트가 항상 최적의 액세스 포인트에 연결되도록 보장함으로써 Wi-Fi 성능을 대폭 향상시킵니다. 또한 MU-MIMO 클라이언트들을 그룹화하여 다수의 디바이스로 동시 전송이 이루어지도록 함으로써 전반적인 WLAN 용량 증대를 실현합니다.
AppRF	AppRF 기술은 ArubaOS PEF(Policy Enforcement Firewall) 모듈의 일부로서, WLAN 상에서 애플리케이션 인식 기능을 제공합니다. 이를 통해 IT팀이 사용자 별로 애플리케이션 우선순위를 설정하고, BYOD 트랜잭션 및 디바이스 밀도에 따라 확장 계획을 수립할 수 있도록 지원합니다.
AirGroup technology	AirGroup은 서브넷 전반에서 Apple TV, 프린터, Google Chromecast, 기타 DNS 알림 디바이스들을 손쉽게 공유할 수 있도록 해줍니다. 간단한 구성 옵션을 통해 모든 디바이스들의 상호 인식을 보장합니다. 이와 동시에 고급 옵션을 통해 물리적 위치, 시간대, 역할, Self-provisioned Sharing Island를 기반으로 공유 범위를 축소할 수 있습니다.
Adaptive Radio Management (ARM)	ARM(Adaptive Radio Management)은 RF 환경을 다이나믹하게 조정하여 Wi-Fi 안정성과 예측가능성을 극대화합니다. 이렇게 함으로써 Microsoft Skype for Business 음성, 비디오, 데스크톱 공유, 채팅 플로우를 비롯한 모든 클라이언트와 앱들에 대해 최적의 성능을 보장합니다.
RFProtect 모듈	ArubaOS 8은 무선 위협으로부터 네트워크 리소스를 보호하고 네트워크 성능을 최적화하기 위해 업계 최강의 AP Containment & Classification 솔루션인 ArubaOS RFProtect 모듈이 통합되어 있습니다. RFProtect 모듈은 별도의 RF 센서와 보안 장비 시스템 필요 없이 네트워크 인프라에 무선 보안을 통합하고, 가버먼트급 WIP(Wireless Intrusion Protection)를 구현합니다. 알림: 라이센스 옵션으로 제공되는 기능입니다.
Advanced cryptography	ArubaOS ACR(Advanced Cryptography) 모듈은 아루바 모빌리티 컨트롤러에 밀리터리급 Suite B 암호화를 제공하여, 민감한 기밀 정보를 다루는 네트워크에서 사용자 모빌리티와 보안 액세스를 지원합니다. 미국 NSA(National Security Agency) 승인을 획득한 Suite B는 성능을 향상시키고, 불필요하게 복잡한 워크플로우와 엄격한 처리 요구사항을 없애줍니다.
Virtual Intranet Access (VIA) 클라이언트	VIA는 무료 하이브리드 IPsec/SSL VPN으로서, 가장 안전한 기업 네트워크 연결을 자동 검색하여 선택합니다. 전통적인 VPN 소프트웨어와 달리, VIA는 제로터치 엔드유저 경험을 제공하고, 클라이언트 디바이스 상에서 자동적으로 WLAN 설정을 구성합니다. VIA는 완벽한 Wi-Fi 인식을 지원합니다.
Clarity	IT 팀은 비(non) RF 지표(RADIUS, DHCP, DNS 서버)를 확인함으로써 무선 사용자 경험에 대한 엔드–투–엔드 가시성을 확보할 뿐만 아니라, 사용자가 불편을 겪기 전에 연결 이슈를 미리 예측할 수 있습니다. Clarity는 네트워크로 들어가는 실제 트래픽에 대한 가시성을 제공할 뿐만 아니라, WLAN 관리자가 트래픽 시뮬레이션을 통해 서비스 장애와 성능 이슈를 사전에 파악할 수 있도록 해줍니다. 이러한 선제적인 워크플로우를 수천여 로케이션 전반에서 온디맨드 또는 예정된 일정에 따라 실행할 수 있습니다. 알림: 라이센스 옵션으로 제공되는 기능입니다.

단순한 운영

글로벌 구성 및 로컬 구성이 포함된 평면적인 구성 모델로 운영되는 ArubaOS 6와 달리, ArubaOS 8은 매니지먼트, 컨트롤, 포워딩 기능의 명확한 분리를 제공하는 최신 UI 하의 중앙화된 멀티티어 아키텍처를 사용합니다. 모빌리티 마스터(Mobility Master)와 관리되는 디바이스들의 전체 구성은 중앙 로케이션에서 이루어집니다. 따라서 구성 프로세스가 간소화, 효율화되고 반복이 최소화될 뿐만 아니라 가시성과 모니터링이 향상됩니다.

ArubaOS 8의 최신 UI는 모던한 디자인과 신속한 워크플로우로 사용이 훨씬 간편해졌습니다. ArubaOS 8은 다음과 같은 기능을 통해 네트워크 운영을 간소화합니다.

중앙 라이센싱 풀: IT 팀은 모빌리티 마스터(Mobility Master) 또는 마스터 컨트롤러에서 중앙화된 라이센싱을 통해 모든 라이센스를 중앙 관리할 수 있습니다. AOS 8에서는 이러한 기능이 더욱 확대되어 풀(Pools)을 통한 중앙 라이센싱이 새로 포함되었습니다. 한 회사 내에서 서로 다른 그룹들이 개별적으로 자금을 운용하는 고객의 경우, 각 그룹별로 라이센스를 할당하여 자체적으로 관리하고 소비하도록 할 수 있습니다.

ZTP(Zero touch provisioning): ZTP는 액세스 포인트와 관리 대상 디바이스들의 구축을 자동화합니다. 플러그 앤 플레이 방식으로 빠르고 간편한 구축과 단순한 운영이 가능하며, 비용과 프로비저닝 에러가 감소됩니다. ZTP는 7xxx 모빌리티 컨트롤러(Mobility Controller)에서 처음 도입되었으며, 이제 ArubaOS 8을 통해 72xx 모빌리티 컨트롤러까지 이 기능이 확장됩니다. 모빌리티 컨트롤러는 마스터 컨트롤러 또는 모빌리티 마스터(Mobility Master)로부터 로컬 구성, 글로벌 구성, 라이센스 기준을 수신하여 자체적인 자동 프로비저닝을 실행합니다.

통합 액세스 지원

아루바는 물리적 위치, 유선 또는 무선에 관계 없이 어떤 사용자든지 엔터프라이즈 네트워크에 안전하게 액세스하여 일관된 상시 연결 경험을 보장받도록 지원합니다. 본사, 브랜치 오피스, 홈 오피스에 있는 사용자와 이동 중인 사용자들에게 일관된 보안 및 액세스 정책이 적용됩니다. 사용자와 디바이스는 간단하고 가벼운 액세스 디바이스 또는 소프트웨어를 통해 네트워크에 들어오고, 이러한 액세스 디바이스 또는 소프트웨어는 안전하게 모빌리티 컨트롤러로 자동 연결됩니다.

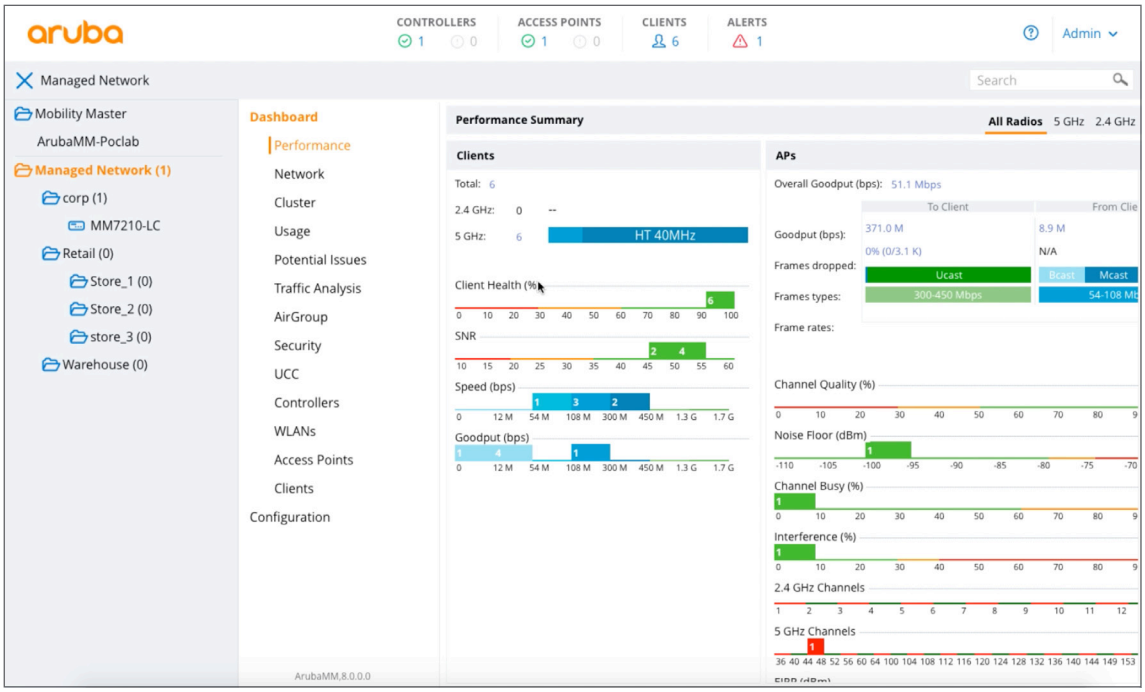


그림 1: ArubaOS 8 최신 UI

통합 액세스(UNIFIED ACCESS) 프레임워크	
사용자 연결 방식	• 안전한 엔터프라이즈급 Wi-Fi • 유선 이더넷 • VPN 리모트 액세스
AP 연결 방식	• 프라이빗 또는 퍼블릭 IP 클라우드 – 이더넷 – 무선 WAN (EVDO, HSDPA) • Wi-Fi 메시 (Point-to-Point 및 Point-to-Multipoint)
트래픽 포워딩	• 중앙화 – 모든 사용자 트래픽을 모빌리티 컨트롤러로 전송 • 정책 라우팅(Policy-routed) – 트래픽 종류와 정책에 따라 선택적으로 사용자 트래픽을 모빌리티 컨트롤러로 전송 또는 로컬에서 브리징.
Wi-Fi 암호화	• 중앙화 – 디바이스와 모빌리티 컨트롤러 사이에서 트래픽이 암호화됨 • 분산 – 디바이스와 AP 사이에서 트래픽이 암호화됨 • 오픈 – 암호화 미실행
기존 네트워크와의 통합	• Layer 2 및 Layer 3 통합 – 모빌리티 컨트롤러가 VLAN 별로 트래픽 스위칭 또는 라우팅 가능 • Rapid Spanning Tree – 고속 Layer 2 컨버전스 구현 • OSPF – 기존 라우팅 토폴로지와의 간단한 통합

ArubaOS 8이 탑재된 모빌리티 컨트롤러(Mobility Controller)는 아루바 액세스 디바이스와 액세스 소프트웨어를 관리합니다. 모빌리티 컨트롤러는 또한 소프트웨어 이미지, 구성, 사용자 연결 상태 및 실행 정책을 관리합니다. 유무선 인프라 전반을 아루바 AirWave로 단일 창을 통해 관리함으로써 IT 팀이 여러 세대로 구성된 멀티벤더 네트워크 전반에서 사용자들의 애플리케이션 및 디바이스 경험을 관리할 수 있습니다. AirWave를 통해 무선 및 모빌리티 SLA(service-level agreements)에 영향을 미치는 모든 것들에 대한 가시성을 확보함으로써 선제적인 용량 계획, 클라이언트 성능 시각화, 그리고 헬프데스크 티켓 생성보다 신속한 애플리케이션 이슈 사전 해결이 가능합니다.

끊김 없는 모빌리티를 위한 아키텍처

기업 사용자들의 이동 중 네트워크 액세스 요구가 증가하고 있습니다. ArubaOS는 사용자들이 네트워크 여기 저기를 이동하는 동안에도 끊김 없는 Wi-Fi 네트워크 연결을 제공합니다. 로밍 핸드오프 (Roaming Handoff) 시간이 2-3 msec에 불과하기 때문에 음성, 비디오 같이 지연에 민감하고 지속적인 애플리케이션들이 끊김 없이 실행됩니다.

ArubaOS는 프록시 모바일 IP 및 프록시 DHCP 기능을 통합하여 사용자들이 서브넷, 포트, AP, 컨트롤러들 사이에서 특정 클라이언트 소프트웨어 없이도 로밍할 수 있도록 해줍니다. 이렇게 함으로써 사용자가 맨 처음 연결된 AP에서 멀리 떨어져 네트워크 내에서 다른 곳으로 이동하더라도 매끄러운 성능을 보장합니다.

VLAN Pooling은 네트워크 설계를 단순화하는 강력한 액세스 엣지 기능입니다. VLAN들을 네트워크 엣지로 풀링(Pulling)하는 대신에 모빌리티 컨트롤러(Mobility Controller) 내에 중앙화하고 AP들까지 터널화합니다. 이렇게 함으로써 네트워크 구성의 복잡성과 Spanning Tree Diameter를 줄이는 이점을 얻을 수 있습니다. VLAN 사용자 멤버쉽 로드밸런싱을 통해 네트워크 내부에서 많은 사람들이 돌아다니는 경우에도 최적의 네트워크 성능을 유지합니다.

아루바의 통합 액세스 방식은 또한 프라이빗 WAN 또는 퍼블릭 인터넷을 통해 엔터프라이즈 네트워크를 리모트 로케이션으로 확장하고, 사용자들에게 위치에 관계없이 동일한 액세스 경험을 제공합니다. 엔터프라이즈 네트워크 인프라에서 멀리 떨어진 사용자들을 연결하기 위해, 모빌리티 컨트롤러가 표준 VPN Concentrator로 작동하여 리모트 사용자들을 다른 엔터프라이즈 사용자들과 동일한 액세스 및 보안 프레임웍을 통해 연결합니다.

모빌리티 마스터(Mobility Master)를 활용할 경우, Controller Clustering을 통해 대규모 캠퍼스 내에서 매끄러운 로밍이 가능합니다. 사용자들은 대형 캠퍼스 내부에서 이동하면서 Skype for Business 통화와 같은 미션 크리티컬 애플리케이션을 사용하더라도 일체의 지연을 느끼지 않습니다. 클러스터 내의 모든 컨트롤러들이 연동되어 사용자들을 관리합니다. IP 주소 갱신, 재인증, 방화벽 상태 정보 손실 없이 10,000여개의 AP사이에서 사용자 로밍이 가능합니다.

네트워크 전반의 무선 보안

엔터프라이즈 네트워크 보안을 위해 ArubaOS 8은 사용자 및 디바이스에 대한 인증, 접근제어, 암호화를 실행합니다. 아루바 아키텍처에서 인증은 기본이며, 유선 및 무선 네트워크에 구축 가능합니다. 무선의 경우, 802.1X가 WPA2의 구성요소이며, 802.11i 프로토콜은 Wi-Fi 보안을 위한 최첨단 기술로 널리 알려져 있습니다.

ArubaOS는 802.1X 인증 교환(Authentication Exchanges)의 암호화된 부분이 모빌리티 컨트롤러에서 종료되도록 하는 AAA FastConnect를 지원합니다. 이렇게 함으로써 RADIUS와 LDAP를 비롯한 다양한 ID 저장소들 간의 통합이 이루어집니다. AAA FastConnect는 PEAP-MSCHAPv2, PEAP-GTC, EAP-TLS를 지원함으로써 외부 인증 서버의 802.1X 실행 필요성을 없앱니다.

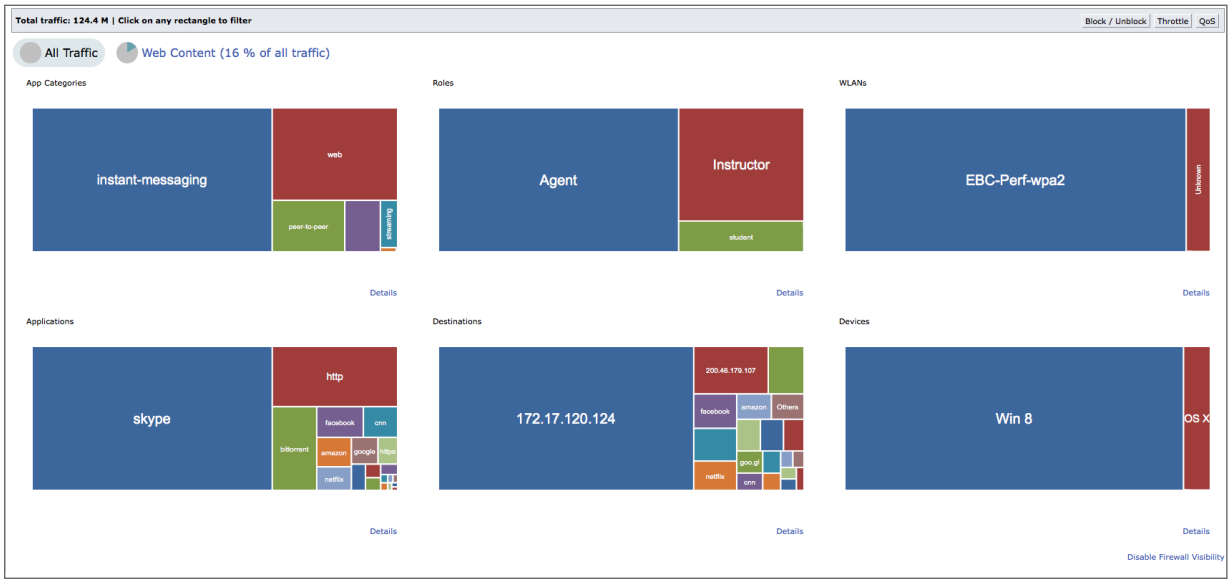
WPA, VPN 또는 다른 보안 소프트웨어가 없는 클라이언트를 위해, 아루바는 안전한 브라우저 기반 인증을 제공하는 웹 기반 캡티브 포털을 지원합니다. 캡티브 포털 인증은 SSL을 사용하여 암호화되며, 패스워드로 로그인한 등록 사용자와 이메일 주소만 입력한 게스트 사용자 양쪽 모두를 지원할 수 있습니다.

허용되지 않은 무선 디바이스들로부터 네트워크를 보호하는 아루바의 악성 AP 분류(Rogue AP Classification) 알고리즘은 시스템이 네트워크에 연결된 악성 AP와 인근의 간섭 AP들을 정확히 구분할 수 있도록 해줍니다. 악성으로 분류된 AP들은 무선 및 유선 네트워크에서 자동적으로 비활성화시킬 수 있습니다. 악성 AP 분류 및 격리는 기본 ArubaOS 내에서 제공되며, 추가적인 모빌리티 컨트롤러 라이센싱은 필요 없습니다.

웹은 필수적인 동시에 위험한 공간이기 때문에, 사용자들이 방문하는 사이트의 유형을 신속하게 파악하고 해당 사이트로 인한 네트워크와 사용자들의 위협 노출 수준을 평가할 수 있어야 합니다. 가장 정확한 최신 방식으로 이를 수행하기 위해, ArubaOS 8에는 적절한 정책에 따라 차단 및 Rate Limit을 실행하는데 사용할 수 있는 URL 필터링, IP 평판조회, 지오로케이션(Geolocation)을 위한 Web Content Policy & Reputation 서브스크립션 옵션이 포함되어 있습니다. 현재 AOS 8은 URL 필터링 및 URL 평판조회만을 지원합니다.

종합적인 WIP(Wireless Intrusion Protection)를 위해, 모빌리티 컨트롤러를 위한 RFProtect 모듈은 애드혹 네트워크(Ad Hoc Network), MITM(Man-in-the-Middle) 공격, DoS(Denial of Service) 공격 등 다양한 위협들에 대한 보호를 제공하며, 무선 침입 시그니처 탐지를 지원합니다.

ARUBAOS 8 엔터프라이즈 보안 프레임워크	
인증 종류	• IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, EAP-POTP,EAP-GTC, EAP-TLV, EAP-AKA, EAP-Experimental, EAP-MD5) • RFC 2548 Microsoft vendor-specific RADIUS attributes • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS authentication • RFC 3579 RADIUS support for EAP • RFC 3580 IEEE 802.1X RADIUS guidelines • RFC 3748 extensible authentication protocol • MAC address authentication • Web-based captive portal authentication
인증 서버	• 내부 데이터베이스 • LDAP/SSL Secure LDAP • RADIUS • TACACS+ • 테스트된 인증 서버 상호운용성: – Microsoft Active Directory (AD) – Microsoft IAS and NPS RADIUS servers – Cisco ACS, ISE servers – Juniper Steel Belted RADIUS, Unified Access servers – RSA ACE/Server – Infoblox – Interlink RADIUS Server – FreeRADIUS
암호화 프로토콜	• CCMP/AES • WEP 64- and 128-bit • TKIP • SSL and TLS: – RC4 128-bit – RSA 1024-bit – RSA 2048-bit • L2TP/IPsec (RFC 3193) • XAUTH/IPsec • PPTP (RFC 2637)
프로그래머블 암호화 엔진	소프트웨어 업데이트를 통한 향후 암호화 표준 지원 가능
웹기반 캡티브 포털 (SSL)	유연한 인증 방식 허용
통합 게스트 액세스 관리	안전한 게스트 액세스 옵션 제공
사이트–투–사이트 VPN	모빌리티 컨트롤러와 IPsec 디바이스 간에 IPsec 터널 생성. X.509 PKI, IKEv2, IKE PSK, IKE Aggressive Mode 인증 지원.



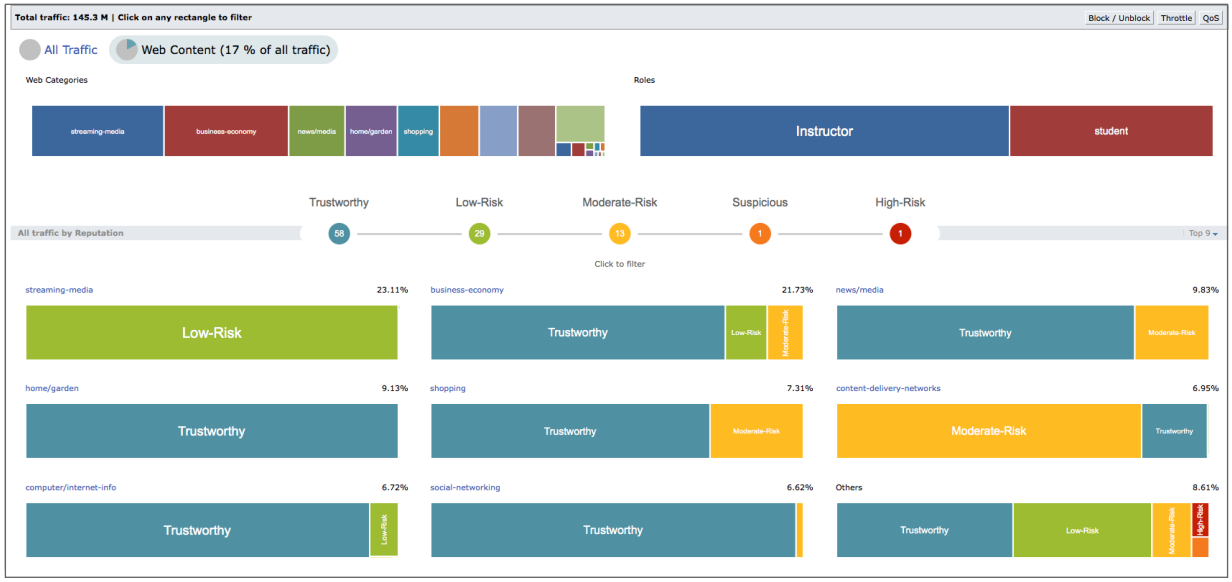


그림 2: WebCC 대시보드

애플리케이션 인식 가시성 및 역할 기반 보안

ArubaOS PEF 라이센스는 사용자 중심 보안, 애플리케이션 가시성, 컨트롤을 향상시킵니다. PEF는 대부분의 사용자 트래픽이 네트워크에서 가장 먼저 진입하게 되는 무선 엣지에서 차세대 모빌리티 방화벽 기능을 제공합니다. PEF는 DPI(Deep Packet Inspection)를 사용하여 트래픽을 분류하고 최적화하며, 단순한 대시보드를 통해 완벽한 트래픽 가시성을 제공합니다.

PEF는 종합적인 아이덴티티 기반 보안을 추가하고 무선 엣지에서 사용자 별 방화벽 컨트롤을 적용함으로써 보안을 향상시키고 단순화합니다. 이렇게 함으로써 ArubaOS는 각 사용자 또는 디바이스 주위에 보안 경계를 생성하고, 해당 사용자 또는 디바이스의 엔터프라이즈 네트워크 리소스 액세스를 철저히 컨트롤합니다.

PEF 라이센스의 일부인 AppRF는 WLAN에 애플리케이션 인식 및 컨트롤을 제공합니다. AppRF는 Wi-Fi 네트워크 상의 트래픽 유형에 대한 가시성을 제공함으로써 관리자가 어떤 사용자 트래픽이 중요한 무선 리소스를 소비하고 있는지 파악하도록 해줍니다. 또한 AppRF는 트래픽에 대한 탁월한 컨트롤을 제공하여 관리자가 2,500여 개 이상의 애플리케이션들에 대해 사용자 및 우선순위에 따라 무선에서 어떤 트래픽을 허용할 것인지 지정할 수 있도록 해줍니다.

ArubaOS 8에는 고객이 커스텀 애플리케이션 및 애플리케이션 카테고리를 설정할 수 있도록 해주는 AppRF Customization 기능이 추가되었습니다. AppRF Customization 기능을 통해 고객은 아루바가 향후 소프트웨어 릴리즈에 맞춤화 기능을 탑재할 때까지 기다릴 필요 없이, 커스텀 카테고리와 해당 카테고리와 관련된 모든 애플리케이션에 정책을 적용하고 커스텀 애플리케이션 트래픽에 우선순위를 적용함으로써 사용자 경험을 향상시킬 수 있게 될 것입니다.

UCC(UNIFIED COMMUNICATIONS COLLABORATION) 사용자 경험 향상

오늘날 업무 공간에서는 모바일 UCC의 자유로움과 협업이 선호됩니다. 아루바 UCC 솔루션은 Apple의 페이스타임, 알카텔 루슨트의 NOE (New Office Environment), 마이크로소프트의 링크 / 스카이프 (Lync/Skype for Business) / 시스코 Jabber, 시스코 SCCP (Skinny Call Control Protocol), SVP(Spectralink Voice Priority), SIP,H.323, Vocera, 그리고 Cellular Wi-Fi Calling과 같은 애플리케이션들을 위해 네트워크 품질을 자동적으로 모니터링하고 분류함으로써 보다 나은 사용자 경험을 제공합니다.

아루바 Skype for Business 솔루션은 SDN과 Microsoft Skype for Business 및 AppRF 기술을 통합하여 QoS를 적용하고, 향상된 가시성을 통해 예측가능한 UC(Unified Communications) 경험을 보장합니다. ArubaOS 8는 UCC 솔루션을 더욱 향상시키며, 다음과 같은 UCC 기능들을 제공합니다.

- Cisco Jabber 지원: Cisco Jabber 클라이언트의 암호화된 버전을 사용하여 음성, 화상 통화, 데스크톱 공유 세션을 위한 QoS와 가시성을 제공합니다.
- Multi-Application Layer Gateway (ALG) 지원: 동일한 클라이언트 디바이스 상에서 동시에 실행되는 다수의 애플리케이션들을 식별하고 우선순위화합니다. 클라이언트 디바이스 한 대에서 동시에 실행되는 애플리케이션들을 최대 10개까지 지원할 수 있습니다.

Wi-Fi Calling이 보편화됨에 따라 이에 대비하여 내부 Wi-Fi 네트워크의 설계, 핸드오프, QoS, RF 커버리지 기준을 재검토할 필요가 있습니다. ArubaOS 8은 실내 Wi-Fi 커버리지 향상, QoS 적용, 통화 차단 또는 제한, 클라이언트 상태에 대한 가시성 제공을 지원하고, 이를 통해 고객에게 캐리어급 음성 경험을 제공합니다. 또한 아루바는 고품질 서비스 향상 외에도 사용자별, 디바이스별, 통신사별 Wi-Fi Calling 가시성을 제공합니다.

APP 인식 가시성 및 역할 기반 보안

기능	이점
글로벌 또는 역할 기반 정책	하나의 명령으로 모든 사용자 트래픽을 컨트롤하는 단순성, 정확히 어떤 사용자가 어떤 앱을 실행할 수 있는지를 컨트롤하는 유연성
2,500 이상의 애플리케이션	고도로 정교한 가시성 및 지원
19개의 애플리케이션 카테고리	다양한 트래픽 유형에 대한 간단한 컨트롤
QoS 태그 실행	어떤 애플리케이션을 다른 애플리케이션들보다 우선적으로 처리
부적절한 애플리케이션 차단	대역폭 보존 및 부적절한 행위 차단
애플리케이션 또는 애플리케이션 카테고리에 대한 속도 조절(Rate Limit)	비필수 트래픽을 허용하긴 하나, 그로 인해 중요한 애플리케이션들의 성능이 저하되지 않도록 방지

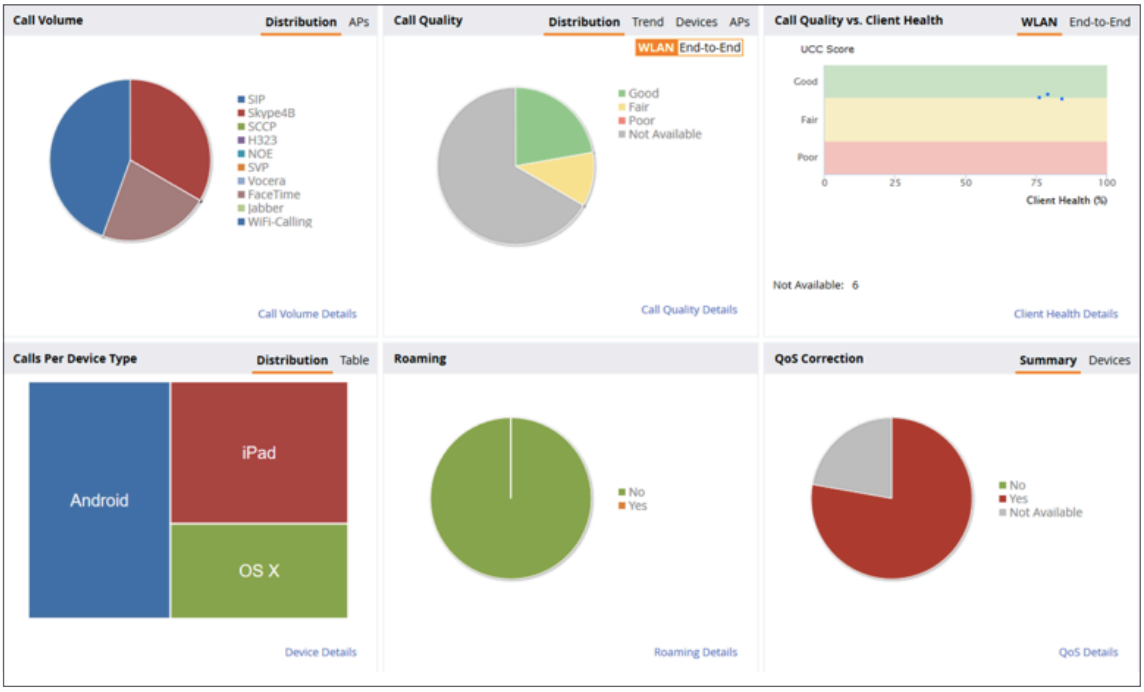


그림 3: AOS 8 UCC 대시보드

엔터프라이즈급 ADAPTIVE WLAN

오늘날 업무 환경에서는 언제 어디서나 모바일 디바이스와 애플리케이션에 액세스할 수 있어야 합니다. 이러한 액세스를 안정적으로 제공하기 위해서는 다이나믹한 모바일 환경에 맞춰 RF 스펙트럼을 능동적으로 관리하는 WLAN이 요구됩니다.

Adaptive Radio Management (ARM) 기술은 자동화된 인프라스트럭처 기반 컨트롤을 사용하여 RF 스펙트럼 전반을 관리하는 특허 받은 기술입니다. ARM은 RF 환경을 다이나믹하게 조정하여 Wi-Fi 안정성과 예측가능성을 극대화하고, 모든 클라이언트와 애플리케이션에 대한 최적의 성능을 보장합니다. 그리고 Microsoft Skype for Business 음성, 비디오, 데스크톱 공유, 챗(chat) 플로우에 대한 개별적인 가시성과 컨트롤을 제공합니다. ARM을 통해 사용자는 IT 개입 없이 일관되고 우수한 사용자 경험을 얻을 수 있습니다.

ArubaOS 8은 새로운 RF 최적화 시스템인 AirMatch를 통해 Adaptive Radio Management (ARM) 기술을 한층 더 향상시킵니다.

모빌리티 마스터 내의 AirMatch는 현대적인 RF 환경을 고려하여 설계되었습니다. AirMatch는 노이즈가 많은 고밀도 환경에 최적화되어 있습니다. AirMatch는 과거 24시간에 대한 RF 통계를 수집하고, 이를 기반으로 익일을 위해 선제적으로 네트워크를 최적화합니다. AirMatch는 자동화된 채널, 채널 폭, 전송 출력 최적화를 통해 고른 채널 사용을 보장하고, 간섭 완화 및 시스템 용량 극대화를 지원합니다.

AIRMATCH 이점	
균등한 채널 할당	가용 채널 전반에 균등하게 라디오를 배포하여 간섭을 완화하고 시스템 용량을 극대화
다이나믹한 채널 폭 조정	고객 환경의 밀도에 맞게 20MHz, 40MHz, 80MHz 사이에서 다이나믹하게 조정
전송 출력(Transmit Power) 자동 조정	전체 WLAN 커버리지를 확인하여 AP들의 전송 출력을 자동 조정함으로써 최고의 커버리지와 사용자 경험을 보장

안정성 및 사용자 경험 향상

모바일 디바이스, IoT, 주요 업무용 애플리케이션들로부터 막대한 네트워크 트래픽이 발생하고 있습니다. 하지만 사용자들은 컨트롤러 장애가 발생하거나 대규모 캠퍼스에서 이동하는 동안에도 여전히 끊김 없는 안정적인 모바일 경험을 기대합니다. ArubaOS 8은 컨트롤러 장애 발생 시에도 다운타임을 최소화하도록 설계된 다음과 같은 강력한 고가용성 기능 세트를 제공합니다.

모빌리티 마스터(Mobility Master)에서 컨트롤러 클러스터링(Mobility Master)은 캠퍼스 WLAN 내에서 컨트롤러들을 최대 12대까지 클러스터로 만들어 무중단 장애 복구(Hitless Failover)를 제공합니다. 사용자는 드물게 컨트롤러 장애가 발생하더라도 전혀 이슈를 눈치채지 못할 것입니다. 음성 통화, 비디오, 데이터 전송 모두가 사용자가 느낄만한 영향 없이 계속해서 유지됩니다. 클러스터 내 컨트롤러들이 사용자 세션 정보를 공유함으로써 어떤 사용자에게도 SPOF(Single Point Of Failure)가 없도록 보장합니다.

지역사무소 및 재택근무자를 위한 리모트 네트워킹

아루바 리모트 및 브랜치 네트워킹 솔루션은 단순하고 안전하며 비용대비 효과적으로 기업 네트워크를 사무실, 클리닉, 매장, 소호, 재택근무자에게 확장할 수 있도록 해줍니다. ArubaOS는 캠퍼스 또는 데이터센터에 구축된 모빌리티 컨트롤러의 VPN Termination, 브랜치 게이트웨이로 구축된 모빌리티 컨트롤러의 WAN 서비스 등의 전용 브랜치 기능을 모빌리티 컨트롤러 상에 통합합니다.

캠퍼스 내의 모빌리티 컨트롤러는 모든 복잡한 구성, 관리, 소프트웨어 업데이트, 인증, 침입 탐지, 리모트 사이트 종료(termination) 작업을 처리합니다. 브랜치에 구축된 모빌리티 컨트롤러는 정책 기반 라우팅, 압축, 로컬 네트워크 기능 등의 작업을 처리합니다. 소규모 브랜치 또는 리모트 유스케이스에서는 경제적인 가격대의 RAP(Remote Access Points) 또는 아루바 VIA(Virtual Intranet Access) VPN 서비스 OTG(on-the-go)를 통해 기업 네트워크를 확장할 수 있습니다.

고가용성 구축 모드	
Active/Active (1:1)	각 모빌리티 컨트롤러가 일반적으로 정격 용량의 50%를 제공합니다. 제 1 컨트롤러가 제 2 컨트롤러에 의해 지원되는 AP들을 위한 스탠바이 역할을 실행하고, 반대도 마찬가지입니다. 한 컨트롤러에 장애가 발생할 경우, 해당 AP들이 다른 컨트롤러로 페일오버되어 모든 AP들에 대한 고가용성이 보장됩니다.
Active/Standby (1+1)	한 대의 모빌리티 컨트롤러가 모든 AP들을 지원하고, 다른 컨트롤러는 스탠바이 역할을 맡습니다. 기본 컨트롤러에 장애 발생 시, AP들이 스탠바이 컨트롤러로 이동합니다.
N+1	다수의 액티브 모빌리티 컨트롤러들을 한 대의 스탠바이 컨트롤러가 백업합니다.

기능	이점
AP가 액티브 및 스탠바이 모빌리티 컨트롤러 양쪽으로 동시에 통신 채널을 생성	제 1 컨트롤러에 장애 발생 시, 스탠바이 모빌리티 컨트롤러로 즉시 페일오버
페일오버 과정에서 AP들이 라디오를 껐다 켜지 않음	SSID 상시 가용
Layer 3 네트워크에서 솔루션 실행	특별한 토폴로지 필요 없음
클라이언트 상태 동기화	크리덴셜을 캐시화함으로써 재인증 및 오버로드 RADIUS 서버의 필요성 제거
N+1 오버서브스크립션	구성을 단순화하고, 필요한 모빌리티 컨트롤러 수를 줄임

재택근무자를 위한 RAP(REMOTE ACCESS POINTS)	
ZTP(Zero-touch provisioning)	관리자가 사전 구성 없이 RAP 구축 가능. 엔드유저에게 바로 배송
유선 및 무선	사용자가 유선 Ethernet, Wi-Fi, 또는 둘 다를 통해 RAP 연결
유연한 인증	802.1X, 캡티브 포털, 포트별/사용자별 MAC 주소 인증
중앙 관리	AP 상에서 로컬 구성 필요 없음. 모빌리티 컨트롤러에 의해 구성 및 관리 실행.
3G/4G LTE WAN 연결	기본 또는 백업 인터넷 연결을 위해 RAP가 USB 무선 WAN 어댑터(EV-DO, HSDPA) 지원
FlexForward 트래픽 포워딩	• 중앙화 – 모든 사용자 트래픽이 모빌리티 컨트롤러로 전송됨 • 로컬 브리징 – 모든 사용자 트래픽이 액세스 디바이스에 의해 로컬 LAN 세그먼트로 브리징됨 • 정책 라우팅 – 트래픽 유형/정책에 따라 사용자 트래픽이 선택적으로 모빌리티 컨트롤러로 포워딩 되거나 로컬에서 브리징됨(PEF 라이센스 필요)
엔터프라이즈급 보안	RAP는 X.509 인증서를 사용하여 모빌리티 컨트롤러를 인증하고, 안전한 IPsec 터널을 생성
UBR(Uplink Bandwidth Reservation)	음성과 같이 손실에 민감한 애플리케이션 프로토콜을 위해 예약된 대역폭 설정
로컬 진단	헬프데스크 콜 발생 시, 로컬 사용자가 사전정의된 URL을 통해 종합적인 RAP 진단을 확인할 수 있음
Remote mesh portal	RAP는 또한 메시 포털 역할을 실행하여 다운스트림 AP들을 위한 무선 링크를 제공
지원되는 AP	RAP-3, RAP-100 시리즈, RAP-155, AP-105, AP-220 시리즈, AP-130 시리즈, AP-110 시리즈, AP-100 시리즈, AP-90 시리즈, AP-175 시리즈
최소 링크 속도	SSID 당 64 kbps
암호화 프로토콜(RAP와 모빌리티 컨트롤러 사이)	AES-CBC-256 (내부 IPsec ESP)

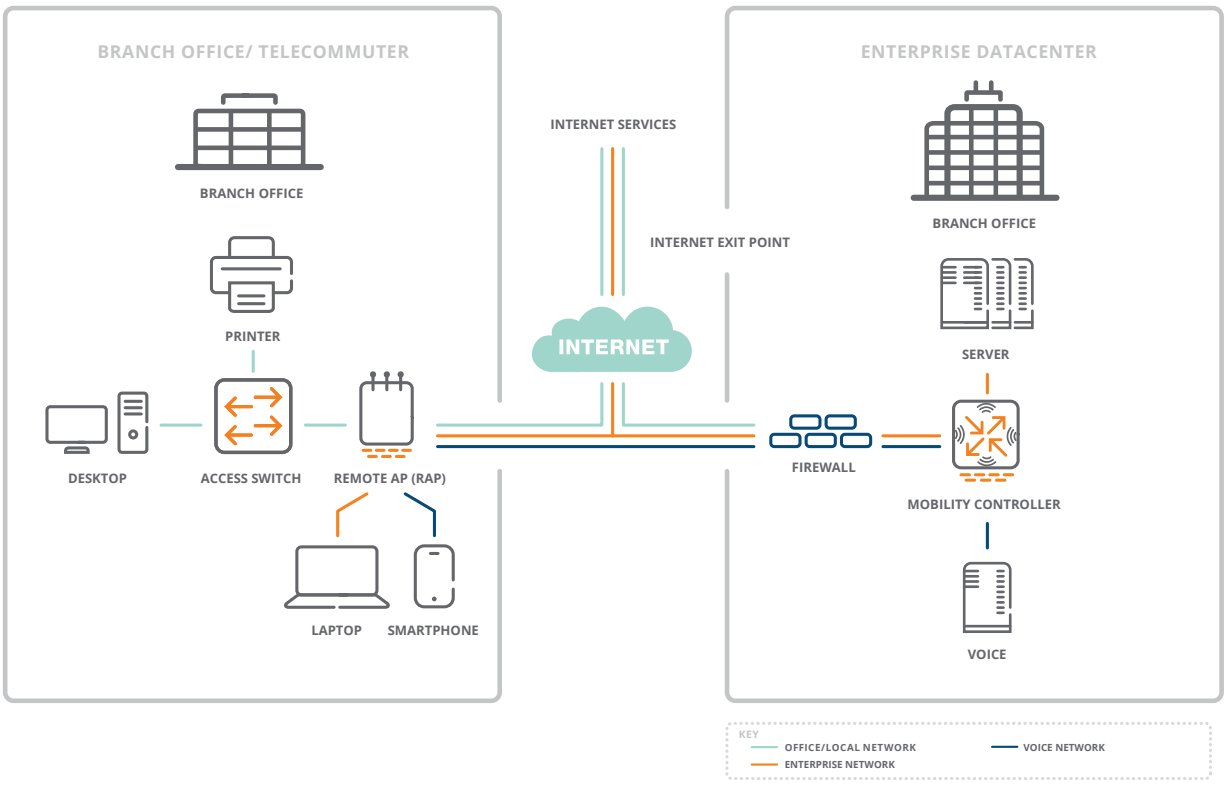


figure 2.8_071614

아루바 RAP는 브랜치 및 홈 오피스에 안전한 모바일 연결을 제공합니다.

출장 근무자를 위한 단순하고 안전한 연결

사용자가 사무실 외부에서 엔터프라이즈 리소스에 액세스해야 할 경우, 일반적으로 VPN 클라이언트 소프트웨어가 사용됩니다.
VPN 클라이언트 소프트웨어는 엔터프라이즈 DMZ에 위치한 VPN Concentrator로 연결됩니다.

아루바 솔루션에서는 리모트 VPN 사용자를 다른 사용자와 동일하게 취급합니다. 본사 또는 브랜치 오피스 RAP 구축에서 사용되는 동일한 액세스 정책과 서비스 정의를 활용합니다. 모빌리티 컨트롤러가 VPN Concentrator 역할을 실행하므로 동일한 중복 액세스 인프라가 필요 없습니다.

ArubaOS는 주요 VPN 클라이언트 및 주요 클라이언트 운영체제에 빌트인된 VPN 클라이언트들과 호환됩니다. ArubaOS는 또한 옵션 VIA 클라이언트를 제공합니다. VIA 클라이언트는 Android, iOS, Mac OS X, Windows 디바이스에 인스톨 가능합니다.

액세스 네트워크들을 통합함으로써 정책과 액세스 구성이 통합되고, 사용자 경험이 향상되며, 헬프데스크 콜이 감소하고, IT 비용이 절감됩니다.

리모트 액세스를 위한 안전한 연결	
클라이언트 지원	• Windows 상의 아루바 VIA 클라이언트 • Cisco 및 Nortel VPN 클라이언트 • OpenVPN, Apple/Windows 네이티브 클라이언트
VPN 프로토콜	• L2TP/IPsec (RFC 3193) • XAUTH/IPsec • PPTP (RFC 2637)
인증	• 유저네임/패스워드 • X.509 PKI • RSA SecurID • Smart Card • Multi-factor

SECURE ENTERPRISE MESH

아루바 Secure Enterprise Mesh 솔루션은 유연한 무선 설계를 제공하여 AP들을 실내 및 실외의 필요한 곳 어디에든 설치할 수 있도록 해줍니다. 화이버 또는 케이블이 없기 때문에 네트워크 설치 비용이 대폭 절감되고, 필요한 이더넷 포트 수도 상대적으로 적습니다.

Secure Enterprise Mesh 솔루션은 아루바 통합 액세스 프레임웍과 완벽히 통합되어 사용자가 어디로 로밍하더라도 단일한 엔터프라이즈 네트워크를 구현합니다. Secure Enterprise Mesh는 프로그래밍이 가능한 소프트웨어를 기반으로 하며, 특정 하드웨어가 필요 없습니다. 아루바 인도어 또는 아웃도어 802.11n 또는 802.11ac AP가 메시 AP 기능을 실행할 수 있습니다.

Secure Enterprise Mesh는 Wi-Fi 액세스, 동시 WIP(Wireless Intrusion Protection), 무선 백홀, LAN 브리징, Point-to-Multipoint 연결 등 모든 엔터프라이즈 무선 니즈를 지원합니다. 이 모든 것이 하나의 공통 인프라를 통해 제공됩니다.

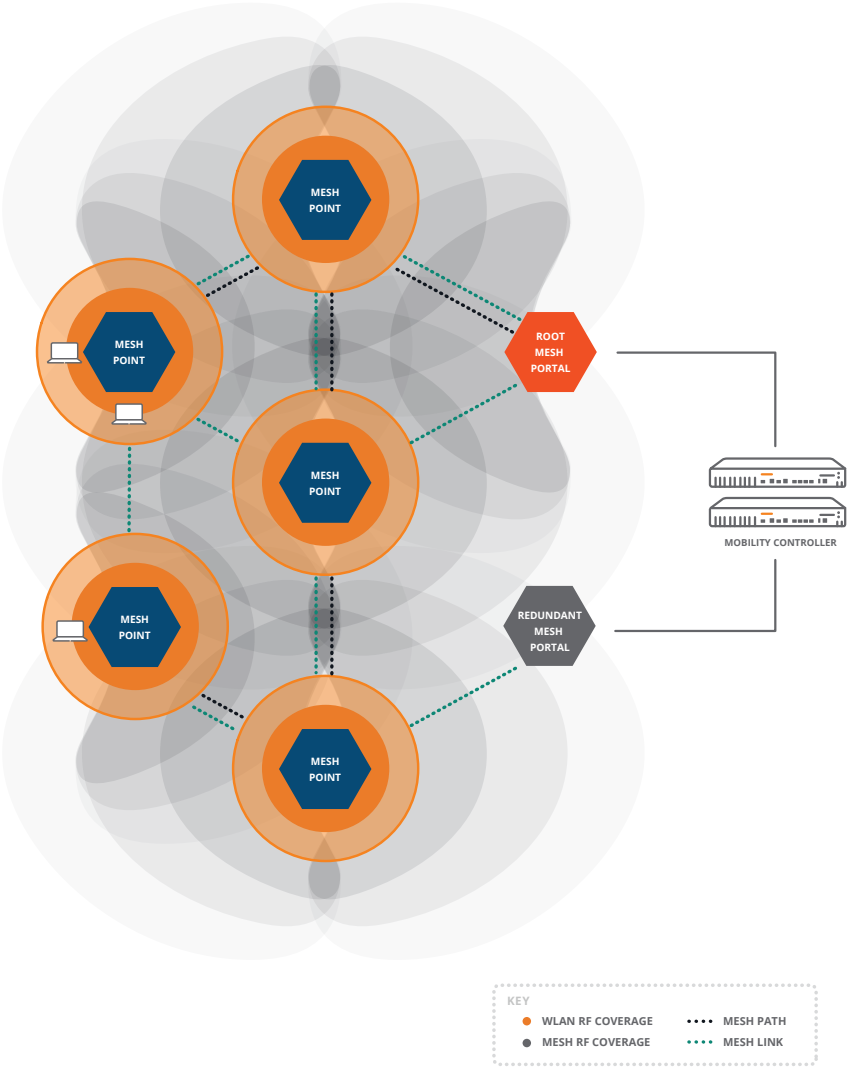
Secure Enterprise Mesh는 건물 간 연결, 아웃도어 캠퍼스 모빌리티, 무선 오피스, 유선 백업, 비디오 및 오디오 모니터링, 알람, 긴급 신호 등의 보안 애플리케이션, 산업용 애플리케이션과 센서 네트워크를 비롯한 연결 애플리케이션들을 위한 뛰어난 솔루션입니다.

아루바는 Cooperative Control 기술을 통한 인텔리전트 링크 관리 알고리즘을 사용하여 트래픽 경로와 링크를 최적화합니다.

메시 AP들은 인근 AP들과 통신하고 RF 및 링크 속성(링크 비용, 경로 비용, 노드 비용, 로딩 등)을 알림으로써 애플리케이션을 위한 최고의 경로를 선택할 수 있습니다.

로드가 많거나 간섭이 있을 경우, 메시 경로와 링크가 자동 조정됩니다. 또한 음성 및 비디오 트래픽에 대한 애플리케이션 태그가 공유되어 지연에 민감한 트래픽이 데이터보다 우선적으로 처리되도록 보장합니다.

Cooperative Control 기술은 또한 경로 단절 또는 AP 장애 시 메시 네트워크를 위한 Self-healing 기능을 제공합니다.



아루바 Secure Enterprise Mesh 솔루션

아루바 SECURE ENTERPRISE MESH 솔루션	
광범위한 애플리케이션 지원	Wi-Fi 액세스, 동시 WIP(Wireless Intrusion Protection), 무선 백홀, LAN 브리징, Point-to-Multipoint 연결
통합 네트워크 액세스	메시 네트워크를 캠퍼스 및 브랜치 오피스 WLAN과 통합. 사용자들이 캠퍼스, 브랜치 Wi-Fi, 메시 네트워크 사이에서 끊김 없이 로밍
Cooperative control	인텔리전트 RF 링크 관리를 통해 최적 성능 경로를 파악하고, 네트워크의 Self-organize 지원
Self-healing	복원력 있는 Self-healing 메시로 경로 단절 또는 AP 장애 해결
Mesh clustering	대규모 메시가 고가용성 클러스터들로 분할될 수 있도록 함으로써 확장성 지원
중앙 암호화	데이터가 클라이언트에서 코어까지 엔드–투–엔드 암호화됨. 메시 AP 도난 시에도 네트워크를 보호
중앙 관리	모든 메시 노드가 중앙에서 모빌리티 컨트롤러에 의해 구성되고 컨트롤됨. 로컬 관리 필요 없음
광범위한 그래픽 지원 툴	커버리지 히트 맵, 자동 Link Budget 계산, 플로어 플랜, 네트워크 토폴로지 맵 등 종합적인 네트워크 시각화
표준기반 설계	IEEE 802.11s 설계 원칙을 기반으로 한 Secure Enterprise Mesh

관리, 구성, 트러블슈팅

모빌리티 컨트롤러 구성, 관리, 트러블슈팅은 브라우저 기반 GUI와 네트워크 관리자에게 익숙한 CLI를 통해 제공됩니다.

ArubaOS는 또한 AirWave와 통합됩니다. AirWave는 계획과 구축에서부터 모니터링, 분석, 트러블슈팅까지 WLAN 라이프사이클의 모든 단계에서 관리를 간소화시킵니다. AirWave는 또한 장기적 트렌딩과 분석, 헬프데스크 통합 툴, 맞춤 리포팅을 제공합니다.

브랜치 또는 지역 사무소에 분산된 모든 AP와 모빌리티 컨트롤러를 중앙의 단일 콘솔에서 구성하고 관리할 수 있습니다. 일반 작업 구성을 간소화하기 위해, 직관적인 작업 기반 마법사가 네트워크 관리자를 단계별 프로세스에 따라 안내합니다.

모빌리티 컨트롤러는 1:1 및 1:n VRRP 기반의 이중화 구성 및 이중화 데이터센터 지원 구성으로 구축할 수 있습니다. Layer 3 토폴로지로 구축할 경우, OSPF 라우팅 프로토콜이 신속한 컨버전스를 위한 자동 경로 Route Learning 및 Route Distribution을 지원합니다.

무선 네트워크 관리 및 구성	
IEEE 802.11s 설계 원칙을 기반으로 한 Secure Enterprise Mesh	웹기반 구성으로 어떤 관리자든 표준 웹 브라우저로 시스템을 관리할 수 있음
Command line	콘솔 및 SSH
Syslog	다수의 서버, 다수의 레벨, 다수의 시설 지원
SNMP v2c	지원
SNMP v3	암호화 보안을 통한 향상된 표준 SNMP
모빌리티 컨트롤러 중앙 구성	지정된 마스터 모빌리티 컨트롤러가 여러 개의 다운스트림 로컬 컨트롤러들을 구성하고 관리할 수 있음
VRRP	다수의 모빌리티 컨트롤러 사이에서 고가용성 지원
이중화 데이터센터 지원	지원 – 백업 컨트롤러 IP 주소로 액세스 디바이스 구성 가능
OSPF	지원 – 디폴트 경로 습득 또는 업스트림 라우터에 로컬 경로 삽입을 위한 stub 모드 지원
Rapid Spanning Tree 프로토콜	지원 – 고속 Layer 2 컨버전스 제공

ARUBAOS의 IPV6 지원

가용 IPv4 주소가 고갈되어 감에 따라 많은 조직이 네트워크 내부에서 IPv6 구축을 계획하고 있거나 이미 시작하였습니다.

IPv4와 IPv6 모두 네트워크 상의 데이터 전송을 정의하나, IPv6가 IPv4에 비해 훨씬 많은 주소 공간을 추가하며 수십억 개의 IP 주소를 지원할 수 있습니다.

조직이 IPv4에서 IPv6로 전환하는 과정에서 네트워크 장비는 IPv4 네트워크 내부에서 IPv6 듀얼스택 상호운용성을 지원하거나 순수한 IPv6 환경 내부의 완전한 구축을 지원해야 합니다.

ArubaOS는 오늘날 IPv6 및 듀얼스택 환경에서 모빌리티 컨트롤러와 AP의 구축을 지원합니다. IPsec을 제외한 거의 모든 기능을 네이티브 IPv6 모드에서 구축할 수 있습니다. 관리, 모니터링, 방화벽의 모든 측면이 완벽하게 IPv6를 인식합니다.

IPV6 지원	
IPV6 IPsec	지원
IPv6 관리	GRE, SSH, Telnet, SCP, Web UI, FTP,TFTP, Syslog, SNMP
IPv6 DHCP 서버	지원
IPv6를 통한 캡티브 포털	지원
모빌리티 컨트롤러 상의 IPv6 VLAN 인터페이스 주소 지원	지원
IPv6를 통한 AP-Mobility Controller 통신 지원	지원
USGv6 인증 방화벽	지원

컨텍스트 인식 컨트롤

802.11e 및 Wi-Fi Multimedia (WMM) 지원으로 WMM 태그 및 내부 하드웨어 큐(queues) 간의 매핑을 통해 지연에 민감한 애플리케이션들을 위한 무선 QoS를 보장합니다. 모빌리티 컨트롤러는 무선 QoS를 위해 802.1p 및 IP DiffServ 태그를 하드웨어 큐로 매핑할 수 있으며, 특정 802.1p 및 IP DiffServ 태그가 각기 다른 애플리케이션에 온디맨드로 적용되도록 할 수 있습니다.

Aruba PEF 모듈 추가와 함께 Lync, SIP(Session Initiation Protocol), SVP(Spectralink Voice Priority), Alcatel NOE(New Office Environment), Vocera, SCCP(Skinny Call Control Protocol) 등의 VoIP 프로토콜들이 아루바 모빌리티 컨트롤러 내에서 지원됩니다. 아루바의 애플리케이션 핑거프린팅 기술은 모빌리티 컨트롤러가 암호화된 시그널링 프로토콜들을 지원할 수 있도록 해줍니다. 이러한 스트림이 식별되면, 아루바 WLAN은 무선 채널 상의 전송 및 음성 관련 기능 실행을 위해 이들을 우선순위화합니다.

이러한 음성 관련 기능들로는 통화 중의 ARM 스캐닝 연기, 통화 중인 클라이언트에 대한 우선적인 로밍 등의 명령이 포함됩니다. 이러한 기능은 Wi-Fi를 통한 엔터프라이즈 음성 커뮤니케이션 대규모 구축 시에 필수적입니다.

또한 ArubaOS는 디바이스 핑거프린팅(Device Fingerprinting) 기술을 통해 네트워크 관리자가 애플리케이션과 사용자뿐 아니라 디바이스 타입 별로도 네트워크 정책을 할당할 수 있도록 해줍니다. 디바이스 핑거프린팅은 어떤 디바이스가 네트워크에 액세스할 수 있으며, 이러한 디바이스들이 어떻게 사용될 수 있는지에 대한 강력한 컨트롤을 제공합니다.

ArubaOS는 Android 또는 BlackBerry 운영체제가 탑재된 디바이스는 물론 Apple iPad, iPhone, iPod 등의 모바일 디바이스들을 정확하게 식별하고 분류할 수 있습니다. 이러한 정보를 AirWave와 공유하여 위치나 모바일 디바이스에 관계없이 모든 네트워크 사용자들에 대한 네트워크 가시성을 향상시킵니다.

컨텍스트 인식 네트워크 컨트롤	
T-SPEC/TCLAS	지원
WMM	지원
WMM priority mapping	지원
U-APSD (Unscheduled Automatic Power-Save Delivery)	지원
효율적인 멀티캐스트 전송을 위한 IGMP Snooping	지원
애플리케이션 및 디바이스 핑거프린팅	지원

인증

- Wi-Fi Alliance 인증 (802.11a/b/g/n/d/h/ac, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM Power Save)
- FIPS 140-2 유효성 검증 (FIPS 모드 작동 시)
- Common Criteria EAL-2
- RSA 인증
- Polycom/Spectralink VIEW 인증
- USGv6 방화벽

표준 지원

일반 스위칭 및 라우팅

- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1519 CIDR
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- RFC 1122 Host Requirements
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 894 IP over Ethernet
- RFC 1027 Proxy ARP
- RFC 2236 IGMPv2
- RFC 2328 OSPFv2

- RFC 2328 OSPFv2
- RFC 2338 VRRP
- RFC 2460 Internet Protocol version 6 (IPv6)
- RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE)
- RFC 3220 IP Mobility Support for IPv4 (partial support)
- RFC 4541 IGMP and MLD Snooping
- IEEE 802.1D-2004 – MAC Bridges
- IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks
- IEEE 802.1w – Rapid Spanning Tree Protocol

QoS 및 정책

- IEEE 802.1D – 2004 (802.1p) Packet Priority
- IEEE 802.11e – QoS Enhancements
- RFC 2474 Differentiated Services

무선

- IEEE 802.11a/b/g/n/ac 5 GHz, 2.4 GHz
- IEEE 802.11d Additional Regulatory Domains
- IEEE 802.11e QoS
- IEEE 802.11h Spectrum and TX Power Extensions for 5 GHz in Europe
- IEEE 802.11i MAC Security Enhancements
- IEEE 802.11k Radio Resource Management
- IEEE 802.11ac Enhancements for Very High Throughput
- IEEE 802.11n Enhancements for Higher Throughput
- IEEE 802.11v Wireless Network Management (partial support)

관리 및 트래픽 분석

- RFC 2030 SNTP, Simple Network Time Protocol v4
- RFC 854 Telnet client and server
- RFC 783 TFTP Protocol (Revision 2)
- RFC 951 Bootstrap Protocol (BOOTP)
- RFC-1542 Clarifications and Extensions for the Bootstrap Protocol
- RFC 2131 Dynamic Host Configuration Protocol
- RFC 1591 DNS (client operation)
- RFC 1155 Structure of Management Information (SMIv1)
- RFC 1157 SNMPv1
- RFC 1212 Concise MIB definitions.
- RFC 1213 MIB Base for Network Management of TCP/IP-based internets - MIB-II
- RFC 1215 Convention for defining traps for use with the SNMP
- RFC 1286 Bridge MIB
- RFC 3414 User-based Security Model (USM) for v.3 of the Simple Network Management
- RFC 1573 Evolution of Interface
- RFC 2011 SNMPv2 Management Information Base for the Internet Protocol using SMIv2
- RFC 2012 SNMPv2 Management Information
- RFC 2013 SNMPv2 Management Information
- RFC 2578 Structure of Management Information Version 2 (SMIv2)
- RFC 2579 Textual Conventions for SMIv2
- RFC 2863 The Interfaces Group MIB
- RFC 3418 Management Information Base (MIB) for SNMP
- RFC 959 File Transfer Protocol (FTP)
- RFC 2660 Secure HyperText Transfer Protocol (HTTPS)
- RFC 1901 1908 SNMP v2c SMIv2 and Revised MIB-II
- RFC 2570, 2575 SNMPv3 user based security, encryption and authentication
- RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 2233 Interface MIB
- RFC 2251 Lightweight Directory Access Protocol (v3)
- RFC 1492 An Access Control Protocol, TACACS+
- RFC 2865 Remote Access Dial In User Service (RADIUS)
- RFC 2866 RADIUS Accounting
- RFC 2869 RADIUS Extensions
- RFC 3576 Dynamic Authorization Extensions to remote RADIUS
- RFC 3579 RADUIS Support For Extensible Authentication Protocol (EAP)
- RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)
- RFC 2548 Microsoft RADUIS Attributes
- RFC 1350 The TFTP Protocol (Revision 2)
- RFC 3164 BSD System Logging Protocol (syslog)
- RFC 2819 Remote Network Monitoring (RMON) MIB

보안 및 암호화

- IEEE 802.1X Port-Based Network Access Control
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 2104 Keyed-Hashing for Message Authentication (HMAC)
- RFC 2246 The TLS Protocol (SSL)
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405 ESP DES-CBC cipher algorithm with explicit IV
- RFC 2406 IP Encapsulating Security Payload (ESP)
- RFC 2407 IP Security Domain of Interpretation for ISAKMP

- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 Internet Key Exchange (IKE) v1
- RFC 2451 The ESP CBC-Mode Cipher Algorithms
- RFC 2661 Layer Two Tunneling Protocol "L2TP"
- RFC 2716 PPP EAP TLS Authentication Protocol
- RFC 3079 Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)
- RFC 3162 Radius over IPv6
- RFC 3193 Securing L2TP using IPsec
- RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3706 Dead Peer Detection (DPD)
- RFC 3736 DHCP Services for IPv6
- RFC 3748, 5247 Extensible Authentication Protocol (EAP)
- RFC 3947 Negotiation of NAT-Traversal in the IKE
- RFC 3948 UDP encapsulation of IPsec packets
- RFC 4017 EAP Method Requirements for Wireless LANs
- RFC 4106 GCM for IPSEC
- RFC 4137 State Machines for EAP Peer and Authenticator
- RFC 4306 Internet Key Exchange (IKE) v2
- RFC 4793 EAP-POTP
- RFC 5246 TLS1.2
- RFC 5247 EAP Key Management Framework
- RFC 5281 EAP-TTLS v0
- RFC 5430 Suite-B profile for TLS
- RFC 6106 IPv6 Router Advertisement Options for DNS Configuration
- IETF Draft RadSec – TLS encryption for RADIUS

a Hewlett Packard Enterprise company

www.arubanetworks.com
www.arubanetworks.co.kr

아루바 휴렛팩커드 엔터프라이즈 컴퍼니
서울특별시 영등포구 의사당대로 83 한국휴렛팩커드 빌딩
제품정보 및 구입안내: 02-2199-0371

M10/2016

DS_ArubaOS8_083016