HOJA DE DATOS

ARUBAOS 8

El sistema operativo más inteligente para el lugar de trabajo móvil de la actualidad

DESCRIPCIÓN GENERAL

Los dispositivos móviles, IoT y las aplicaciones críticas de negocio están permitiendo que los trabajadores móviles sean más productivos y eficientes – pero al mismo tiempo, están aumentando la demanda sobre la red.

ArubaOS es el sistema operativo para todos los Aruba Mobility Controllers, Virtual Mobility Controllers, Mobility Conductor y access points inalámbricos administrados por controlador. Con un conjunto extenso de tecnologías y capacidades integradas, ArubaOS 8 entrega acceso unificado alámbrico e inalámbrico, itinerancia transparente, seguridad de grado empresarial y una red siempre activada con el rendimiento requerido, la experiencia de usuarios y la confiabilidad necesaria para soportar ambientes de alta densidad.

El Mobility Conductor es un nuevo componente de la arquitectura de Aruba que permite que los clientes aprovechen las características avanzadas que requieren coordinación central y para que las redes escalen debido al aumento en la demanda de dispositivos móviles e IoT. También reemplaza las funciones anteriores del controlador maestro y puede ser desplegado como una VM o como un dispositivo de hardware x86. El Mobility Conductor proporciona optimización RF automática y permite hitless failover en el improbable caso de una caída del controlador.

Los clientes actuales de Aruba con Mobility Controllers pueden actualizarse desde ArubaOS versión 6 a la versión 8 y beneficiarse inmediatamente de algunas de las nuevas características y capacidades. Para características más avanzadas, como integración de terceros, los clientes necesitarán agregar un Mobility Conductor en su instalación. Para una lista de características detalladas de ArubaOS 8, refiérase a las release notes disponibles aquí.

LAS SIGUIENTES TECNOLOGÍAS EN ARUBAOS 8 SÓLO ESTÁN SOPORTADAS EN EL MOBILITY CONDUCTOR

Característica	Beneficio
AirMatch	Aruba enriquece aún más la tecnología ARM (Adaptive Radio Management) con AirMatch – el nuevo sistema automatizado de optimización de canales, ajuste de la potencia de transmisión y afinación del ancho de canales que utiliza inteligencia dinámica de aprendizaje de máquina para generar automáticamente la vista óptima de toda la red WLAN.
Live Upgrade*	La actualización a un nuevo sistema operativo puede típicamente resultar en tiempo de caída de toda la red. Sin embargo, cuando usted está corriendo constantemente datos de misión crítica la red, el encontrar una ventana de mantenimiento cada vez se está volviendo más difícil. Con "Live Upgrades", su red completa se puede actualizar al sistema operativo más reciente en tiempo real con cerotiempo de caída y sin afectar a ningún usuario.
Controller Clustering	Al soportar hasta 12 controladores en un cluster, la característica Controller Clustering permite una experiencia transparente a través de campuses gigantes, en el caso de una falla o de una densidad significativa en la multitud.
MultiZone	La nueva característica MultiZone en el Mobility Conductor permite que las organizaciones de TI tengan múltiples redes seguras separadas mientras utilizan el mismo AP en la misma ubicación física.
NBAPIs	El Mobility Conductor tiene un conjunto completo de APIs northbound que permiten visibilidad profunda de la red. Las NBAPIs proporcionan métricas de operación de RF, utilización de apps, tipo de dispositivo y datos y usuario en un formato sencillo de integrar. Aplicaciones de terceros pueden recibir información del controlador y analizar todas estas métricas para obtener mejor visibilidad y monitoreo.
Actualización de módulos en servicio	El Mobility Conductor introduce la capacidad de actualizar dinámicamente los módulos de servicio individuales (AppRF, AirGroup, ARM, AirMatch, NBAPI, UCM, WebCC e IP classification) que residen en el Mobility Conductor, sin requerir una reinicialización completa del sistema.

* Esta característica sólo está disponible en ArubaOS 8.1.

LAS SIGUIENTES TECNOLOGÍAS ESTÁN EN EL CORAZÓN DEL SISTEMA OPERATIVO DE ARUBA	
Característica	**Beneficio**
ClientMatch	La tecnología patentada ClientMatch de Aruba elimina sticky clients e impulsa el rendimiento Wi-Fi, asegurando que los clientes se asocien con el mejor access point. También agrupa juntos a los clientes MU-MIMO para transmisión simultánea múltiples dispositivos, mejorando la capacidad general de la WLAN.
AppRF	La tecnología AppRF, parte del módulo opcional PEF (Policy Enforcement Firewall™) de ArubaOS, integra la concientización de aplicaciones en las WLANs. Permite que TI priorice aplicaciones para cada usuario y escala para transacciones BYOD y densidad de dispositivos.
AirGroup technology	AirGroup facilita compartir Apple TVs, impresoras, Google Chromecast y otros dispositivos anunciados por DNS a través de subredes. Opciones sencillas de configuración aseguran que todos los dispositivos se puedan ver entre sí, mientras que opciones avanzadas reducen el alcance de la capacidad de compartir en base a la ubicación física, horario del día, rol e islas auto aprovisionadas para compartir.
Adaptive Radio Management (ARM)	ARM (Adaptive Radio Management) ajusta dinámicamente el ambiente RF para maximizar la estabilidad y previsibilidad Wi-Fi, asegurando rendimiento óptimo para todos los clientes y apps, incluyendo voz de Microsoft Skype for Business, video, desktop sharing y flujos de chats.
RFProtect module	Para proteger los recursos de la red de amenazas inalámbricas y optimizar el rendimiento de la red, ArubaOS 8 integra la solución de contención y clasificación de APs no autorizados, líder en la industria – el módulo ArubaOS RFProtect. El Módulo RFProtect integra la seguridad inalámbrica en la infraestructura de la red sin requerir un sistema separado o sensores RF o dispositivos de seguridad y permite la Protección en contra de Intrusiones Inalámbricas (Wireless Intrusion Protection) de grado gubernamental. Nota: esta es una característica con licenciamiento opcional.
Advanced cryptography	El módulo ACR (Advanced Cryptography) de Aruba OS contribuye criptografía Suite B de grado militar a los Mobility Controllers de Aruba, permitiendo la movilidad de los usuarios y el acceso seguro a redes que manejan información sensible, confidencial y clasificada. Aprobada por la NSA (National Security Agency) de Estados Unidos, Suite B mejora el rendimiento y elimina flujos de trabajo pesados y requerimientos de manejo estrictos.
Virtual Intranet Access (VIA) client	VIA es una VPN IPsec/SSL híbrida gratuita que automáticamente escanea y selecciona la mejor conexión segura a la red corporativa. A diferencia de software VPN tradicional, VIA ofrece una experiencia sin intervención humana al usuario final y automáticamente configura los valores WLAN en los dispositivos cliente. VIA es completamente consciente de Wi-Fi.
Clarity	Las organizaciones de TI pueden tener visibilidad de métricas que no son de RF (RADIUS, DHCP y DNS), lo cual no tan sólo les otorga visibilidad de la experiencia de un usuario inalámbrico de extremo a extremo, sino también les proporciona la capacidad de preveer problemas de conectividad antes de que los usuarios se vean impactados. En adición a ver el tráfico real que fluye a través de la red, Clarity también permite que los administradores de la WLAN simulen tráfico para identificar caídas en el servicio y problemas de rendimiento antes de que los usuarios los experimenten. Este flujo de trabajo proactivo puede ser bajo demanda o programado a través de miles de ubicaciones. Nota: esta es una característica con licenciamiento opcional.

OPERACIÓN SIMPLIFICADA

En contraste con ArubaOS 6, el cual opera sobre un modelo plano de configuración que contiene la configuración global y local, ArubaOS 8 utiliza una arquitectura centralizada de múltiples niveles bajo una nueva Interface de Usuario que proporciona una clara separación entre las funciones de administración, control y reenvío.
La configuración completa para el Mobility Conductor y para los dispositivos administrados se efectúa desde una ubicación centralizada– proporcionando mejor visibilidad y monitoreo, así como simplificando y optimizando el proceso de configuración y minimizando repeticiones.

La nueva Interface de Usuario (UI) en ArubaOS 8 viene con un aspecto moderno y un flujo de trabajo rápido que es mucho más sencillo de utilizar. Las siguientes características en ArubaOS 8 simplifica las operaciones de la red:

Licenciamiento centralizado con Pools: El equipo de TI puede administrar todas sus licencias desde una ubicación centralizada con licenciamiento centralizado, desde el Mobility Conductor o desde el Conductor Controller. En el nuevo ArubaOS 8, hemos extendido esta capacidad para que incluya el licenciamiento centralizado con Pools. Para algunos clientes que tienen financiamiento separado para diferentes grupos dentro de su corporación, tendrán la opción de simplemente asignar licencias a cada grupo para que las administren y las consuman ellos mismos.

Zero touch provisioning (ZTP): ZTP automatiza el despliegue de APs y dispositivos administrados. Plug-n-play permite el despliegue rápido y sencillo y operaciones simplificadas, reduce el costo y limita los errores de aprovisionamiento. ZTP fue introducido en los Mobility Controllers Serie 7xxx y ahora, en ArubaOS 8 estamos extendiendo la capacidad para que incluya a los Mobility Controllers Serie 72xx. El Mobility Controller reside su configuración local, su configuración global y los límites de licencia del Conductor Controller o del Mobility Conductor y se aprovisiona a sí mismo automáticamente.

HABILITANDO EL ACCESO UNIFICADO

Aruba permite que cualquier usuario, sin importar su ubicación física, alámbrico o inalámbrico, acceda en forma segura a la red empresarial con una experiencia consistente y siempre activada. Seguridad uniforme y políticas de acceso se aplican a los usuarios en las oficinas centrales, en las sucursales, en las oficinas en los hogares y durante viajes. Los usuarios y los dispositivos se unen a la red mediante dispositivos de acceso ligeros y sencillos o software, los cuales se conectan en forma segura y automática a los Mobility Controllers.

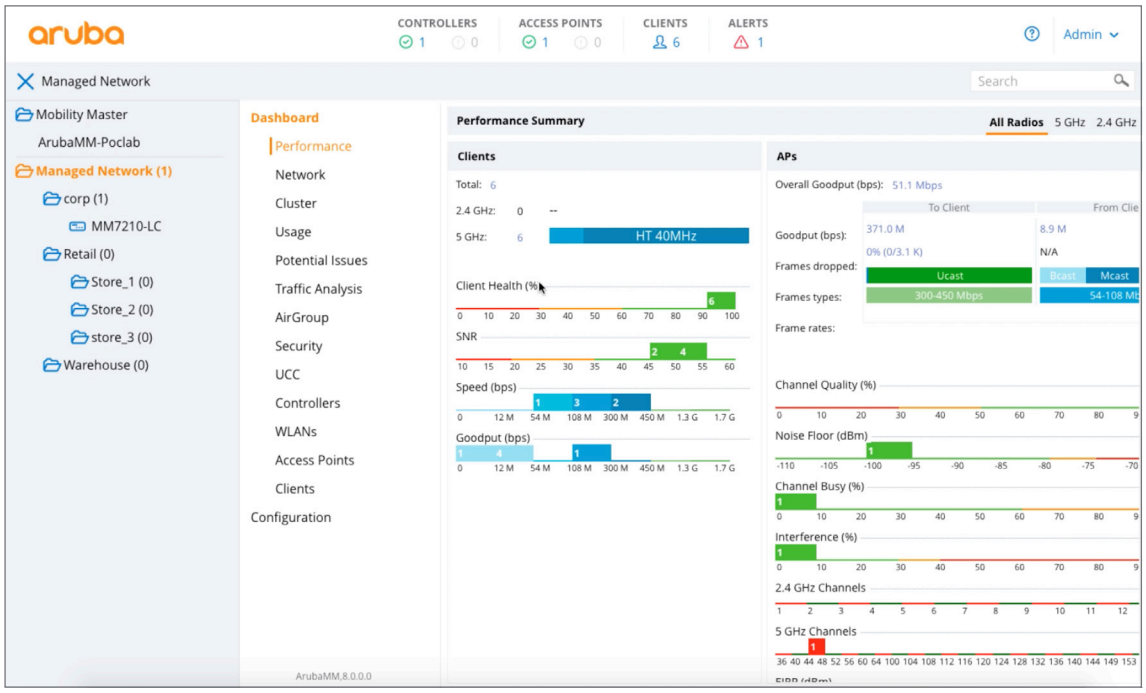


Figura 1: Nueva Interface de Usuario (UI) de ArubaOS 8

MARCO DE TRABAJO DE ACCESO UNIFICADO	
Método de conectividad de usuarios	• Wi-Fi segura de grado empresarial • Ethernet alámbrico • Acceso remoto VPN
Método de conexión de APs	• Nube IP privada o pública - Ethernet - WAN Inalámbrica (EVDO, HSDPA) • Malla Wi-Fi (punto-a-punto y punto-a-multipunto)
Reenvío de tráfico	• Centralizado – Todo el tráfico de usuarios fluye a un Controlador de Movilidad • Enrutado por política – El tráfico de usuarios se reenvía selectivamente a un Controlador de Movilidad o se puentea lógicamente, dependiendo del tipo de tráfico y de política
Cifrado Wi-Fi	• Centralizado – El tráfico se cifra entre dispositivos y el Controlador de Movilidad • Distribuido – El tráfico se cifra entre el dispositivo y el AP • Abierto – Sin cifrado
Integración con redes existentes	• Integración Layer 2 y Layer 3 – Los Controladores de Movilidad pueden conmutar o enrutar tráfico en base a cada VLAN • Rapid Spanning Tree – Permite convergencia rápida Layer 2 • OSPF – Integración simple con topologías de enrutamiento existentes

Impulsados por ArubaOS, los Mobility Controllers administran a los dispositivos de acceso y al software de acceso de Aruba. También administran las imágenes de software, las configuraciones y los estados de conexión de los usuarios y hacen cumplir las políticas. La infraestructura completa – inalámbrica y alámbrica – se controla mediante una sola hoja de vidrio por Aruba AirWave, el cual permite que TI administre las aplicaciones y la experiencia de dispositivos de usuarios a través de varias generaciones de redes de múltiples proveedores. Con visibilidad a todo lo que afecte la comunicación inalámbrica y los contratos de nivel de servicio de movilidad (SLAs), AirWave le permite planificar en forma proactiva la capacidad, visualizar el rendimiento de clientes y localizar y resolver problemas de las aplicaciones antes de que usted reciba un ticket de helpdesk.

ARQUITECTURA DISEÑADA PARA MOVILIDAD TRANSPARENTE

Cada vez más, los usuarios empresariales requieren el acceso a la red mientras se desplazan de un lugar a otro. Para redes Wi-Fi, ArubaOS proporciona conectividad transparente mientras los usuarios se desplazan a través de la red. Con tiempos de handoff durante itinerancia de 2 a 3 milisegundos, aplicaciones persistentes y sensibles a retrasos, como voz y vídeo, experimentan rendimiento ininterrumpido.

ArubaOS integra funciones proxy mobile IP y proxy DHCP permitiendo que los usuarios se desplacen entre subredes, puertos, APs y controladores sin software especial de clientes. Esto asegura rendimiento transparente, aun cuando los usuarios se alejen mucho del AP al cual se conectaron inicialmente conforme se mueven a través de la red efectuando sus trabajos.

VLAN pooling es otra poderosa característica que simplifica el diseño de la red. En lugar de jalar a las VLANs al edge de la red, se centralizan en el Mobility Controller y enviadas por túnel a los APs. Esto tiene enormes ventajas, incluyendo el reducir la complejidad de configuración de la red y el diámetro del spanning tree. La membresía de usuarios de las VLANs se balancea en carga para mantener rendimiento óptimo de la red conforme grandes grupos de usuarios se desplazan a lo largo de la red.

El enfoque de acceso unificado de Aruba también extiende la empresa a ubicaciones remotas, sobre WANs privadas o utilizando el Internet público, otorgándole a los usuarios la misma experiencia de acceso sin importar sus ubicaciones. Para conectar a los usuarios que están alejados de la infraestructura de la red empresarial, los Mobility Controllers operan como concentradores VPN estándar, enlazando a los usuarios remotos a través del mismo marco de trabajo de acceso y seguridad como otros usuarios empresariales.

Al aprovechar el Mobility Conductor, se habilita la itinerancia transparente en grandes campuses mediante Controller Clustering. Los usuarios no experimentan ningún retraso al moverse a través de un campus grande cuando se encuentran en aplicaciones de misión crítica, como llamadas de Skype for Business. Todos los controladores en un cluster trabajan juntos para administrar a los usuarios. Un usuario puede itinerar a través de 10,000 APs sin jamás obtener una nueva dirección IP, sin reautenticarse, ni perder información del estado del firewall.

SEGURIDAD INALÁMBRICA A TRAVÉS DE LA RED Para asegurar la red empresarial, ArubaOS 8 efectúa autenticación, control de acceso y cifrado para usuarios y dispositivos. Con la arquitectura de Aruba, la autenticación es estándar y se puede implementar para redes alámbricas e inalámbricas.

Para redes inalámbricas, 802.1X es un componente de los protocolos WPA2 y 802.11i ampliamente reconocidos como el estado del arte para seguridad Wi-Fi.

ArubaOS soporta en forma singular AAA FastConnect, el cual permite que las porciones cifradas de los intercambios de autenticación 802.1X se terminen en el Mobility Controller, permitiéndole federar entre diferentes almacenes de identidad, incluyendo RADIUS y LDAP. Soportando PEAP-MSCHAPv2, PEAP-GTC y EAP-TLS, AAA FastConnect elimina el requerimiento de que los servidores de autenticación externos sean capaces de manejar el protocolo 802.1X.

Para clientes que no cuenten con WPA, VPN, u otro software de seguridad, Aruba soporta un portal cautivo que proporciona autentificación segura basada en navegador. La autentificación del portal cautivo se cifra utilizando SSL y puede soportar a usuarios registrados con un nombre de usuario y un password o a usuarios visitantes que proporcionen solamente una dirección de correo electrónico.

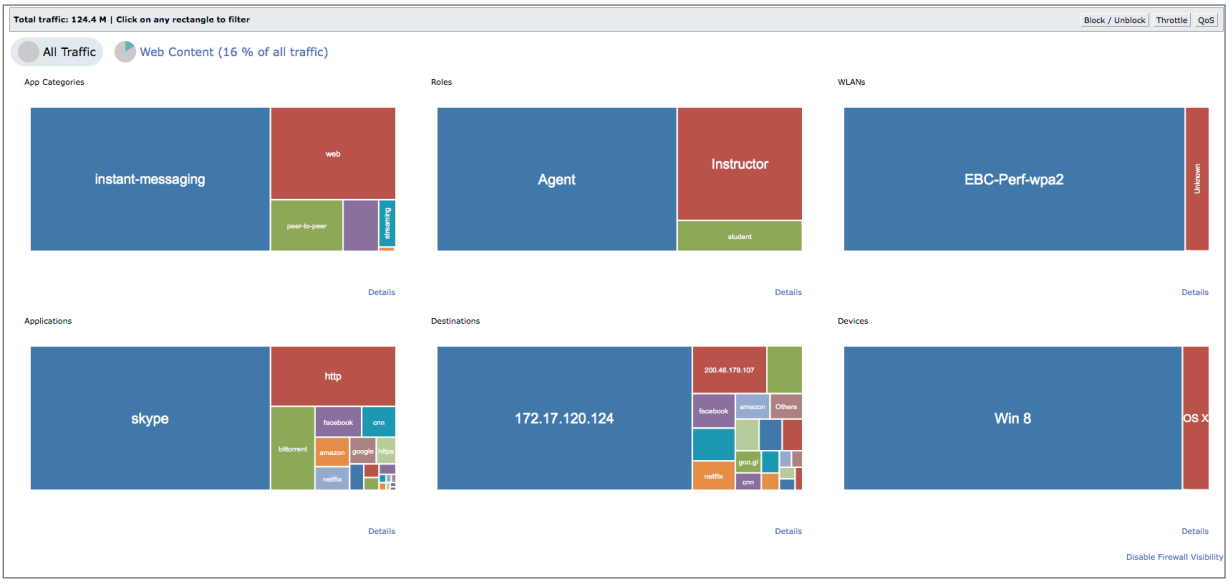
Para protección en contra de dispositivos inalámbricos no autorizados, los algoritmos de clasificación de APs no autorizados de Aruba permiten que el sistema diferencie en forma precisa entre APs no autorizados conectados a la red y APs cercanos que interfieren.

Una vez que se clasifican como no autorizados, estos APs se pueden deshabilitar automáticamente a través de la red alámbrica e inalámbrica. La contención y clasificación de APs no autorizados está disponible dentro de ArubaOS base y no requiere licenciamiento adicional para los Mobility Controllers.

Debido a que la web se ha convertido en un lugar esencial pero peligroso, deseamos ser capaces de determinar rápidamente el tipo de sitios que los usuarios están visitando y medir la amenaza relativa que esos sitios representan para la red y para sus usuarios. Con el objeto de hacer eso de la forma más precisa y actualizada posible, ArubaOS 8 incluye una suscripción opcional a Política de contenido Web y reputación para filtrado URL, IP reputation y geolocalización, los cuales se pueden utilizar para bloquear y limitar en tasas con políticas adecuadas. AOS 8 sólo soporta filtrado URL y reputación URL en este momento.

Para protección completa de intrusiones inalámbricas, el módulo RFProtect para Mobility Controllers habilita la protección en contra de redes ad-hoc, ataques man-in-the-middle, ataques DoS (denial of-service) y muchas otras amenazas, al tiempo que habilita la detección de firmas de intrusiones inalámbricas.

MARCO DE TRABAJO DE SEGURIDAD EMPRESARIAL DE ARUBAOS 8	
Tipos de autenticación	• 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 autenticación RADIUS • RFC 3579 soporte de RADIUS para EAP • RFC 3580 IEEE 802.1X directrices RADIUS • RFC 3748 protocolo de autenticación extensible • Autenticación de direcciones MAC • Autenticación del portal cautivo basado en web
Servidores de autenticación	• Base de datos interna • LDAP/SSL LDAP seguro • RADIUS • TACACS+ • Se probó la interoperabilidad del servidor de autenticación: - Microsoft Active Directory (AD) - Servidores Microsoft IAS y NPS RADIUS - Servidores Cisco ACS, ISE - Servidores Juniper Steel Belted RADIUS, Unified Access - Servidor/ACE RSA - Infoblox - Servidor Interlink RADIUS - FreeRADIUS
Encryption protocols	• CCMP/AES • WEP 64- y 128-bit • TKIP • SSL y TLS: - RC4 128-bit - RSA 1024-bit - RSA 2048-bit • L2TP/IPsec (RFC 3193) • XAUTH/IPsec • PPTP (RFC 2637)
Módulo de cifrado programable	Permite que normas de cifrado futuras se soporten mediante actualizaciones de software
Portal cautivo basado en web (SSL)	Permite flexibilidad en métodos de autenticación
Administración integrada de acceso de visitantes	Proporciona opciones seguras para el acceso de visitantes
VPN Sitio-a-sitio	Un Túnel IPsec se establece entre el Mobility Controller y los dispositivos IPsec. Soporte de autenticación para X.509 PKI, IKEv2, IKE PSK, IKE aggressive mode.



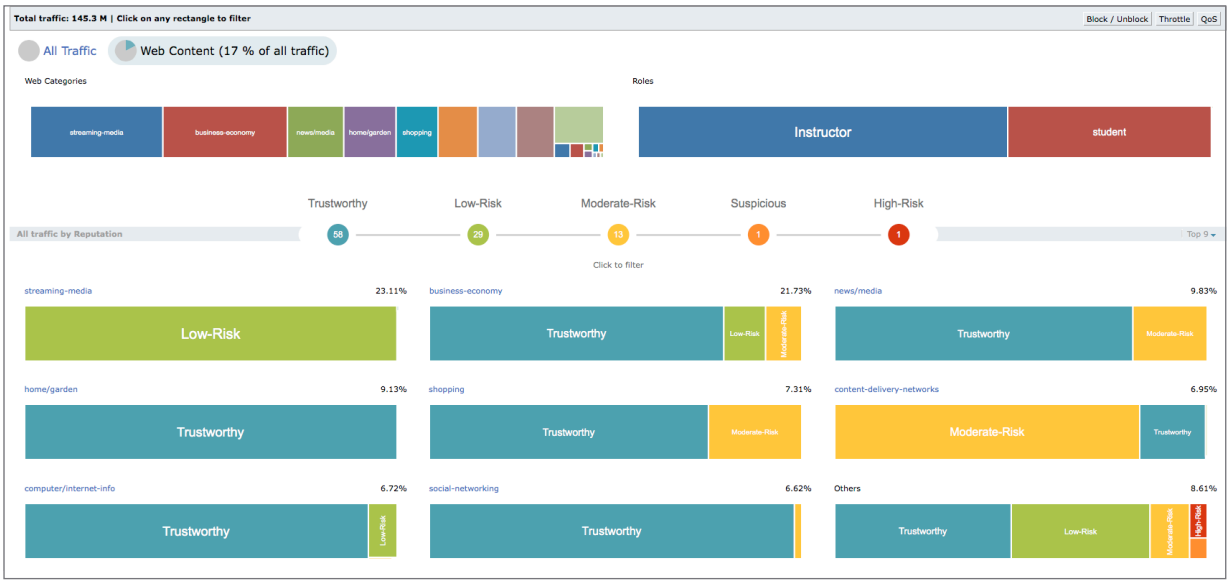


Figura 2: Tablero de Control WebCC

VISIBILIDAD CONSCIENTE DE APLICACIONES Y SEGURIDAD BASADA EN ROLES

La licencia de PEF de ArubaOS enriquece la seguridad centrada en usuarios, la visibilidad de aplicaciones y el control. Implementa el poder de un firewall de movilidad de siguiente generación al edge inalámbrico, en donde la mayoría del tráfico de usuarios toca por primera vez a la red. Utiliza DPI (Deep Packet Inspection) para clasificar y optimizar el tráfico y le proporciona visibilidad completa del tráfico a través de un tablero de control simple.

PEF simplifica y enriquece la seguridad de acceso agregando seguridad completa basada en identidades con controles de firewall integrados aplicados en base a cada usuario en el edge inalámbrico. Esto permite que ArubaOS cree un perímetro de seguridad alrededor de cada usuario o dispositivo, controlando rigurosamente la forma en la cual ese usuario o dispositivo puede acceder a los recursos de la red empresarial.

AppRF, parte de la licencia de PEF, aporta concientización de aplicaciones y control a la WLAN. Al proporcionar visibilidad de los tipos de tráfico que están corriendo en la red Wi-Fi, AppRF permite que los administradores entiendan cuál tráfico de usuarios está consumiendo el recurso vital de aire. AppRF también proporciona control sin precedentes sobre ese tráfico, permitiendo controles flexibles y poderosos que permiten que los administradores elijan cuál tráfico se permite en el aire para más de 2,500 aplicaciones, por cuáles usuarios y con qué prioridad.

Ahora en ArubaOS 8, estamos extendiendo las capacidades de AppRF, agregando la capacidad para que los clientes definan aplicaciones y categorías de aplicaciones – AppRF Customization. Esto permitirá que los clientes apliquen una política para la categoría personalizada y para todas las aplicaciones asociadas con esa categoría y apliquen priorización del tráfico de aplicaciones personalizadas para obtener una mejor experiencia de usuario, sin necesidad de esperar a que Aruba implemente la personalización en una liberación de software futura.

ENRIQUECIENDO LA EXPERIENCIA DE USUARIO PARA UCC (UNIFIED COMMUNICATIONS COLLABORATION)

La fuerza laboral de la actualidad prefiere la libertad y la colaboración de UCC móvil. La solución Aruba UCC proporciona una mejor experiencia de usuario, clasificando y monitoreando automáticamente la calidad de la red para la siguientes aplicaciones: Apple FaceTime, Alcatel Lucent New Office Environment (NOE), Microsoft Lync/Skype for Business, Cisco Jabber, Cisco Skinny Call Control Protocol (SCCP), Spectralink Voice Priority (SVP), SIP, H.323, Vocera y Cellular Wi-Fi Calling.

La solución Aruba Skype for Business aprovecha la integración SDN con Microsoft Skype for Business y con la tecnología AppRF para aplicar calidad de servicio (QoS) y obtener mejor visibilidad para asegurar una experiencia de comunicaciones unificadas predecible. ArubaOS 8 enriquece más aún la solución UCC e introduce las siguientes características de UCC:

- El soporte de Cisco Jabber proporciona QoS y visibilidad para voz, llamadas de vídeo y sesiones de desktop-sharing efectuadas utilizando una versión no cifrada del cliente Cisco Jabber.
- El soporte de ALG (Multi-Application Layer Gateway) permite que múltiples aplicaciones que estén corriendo simultáneamente en el mismo dispositivo cliente se identifiquen y prioricen. Se soporta un máximo de 10 aplicaciones corriendo simultáneamente en un dispositivo cliente.

Conforme las llamadas por Wi-Fi sean más prevalentes, usted necesita prepararse y reevaluar su diseño de red Wi-Fi interna, handoffs, QoS y objetivos de cobertura RF. ArubaOS 8 mejora la cobertura Wi-Fi en interiores y aplica calidad de servicio, bloquea o regula llamadas y proporciona visibilidad acerca del estado de operación de dispositivos cliente, proporcionando una experiencia de voz de categoría carrier para clientes. En adición a enriquecer la alta calidad de servicio, Aruba también ofrece visibilidad en llamadas de Wi-Fi en base a cada usuario, cada dispositivo y cada carrier.

VISIBILIDAD CONSCIENTE DE APPS Y SEGURIDAD BASADA EN ROLES

Característica	Beneficio
Políticas globales o basadas en roles	Simplicidad para controlar todo el tráfico de usuarios con un solo comando, flexibilidad para controlar exactamente cuáles usuarios pueden correr cuales apps.
Más de 2,500 aplicaciones	Visibilidad y control altamente granular.
19 categorías de aplicaciones	Simplifica el control sobre diferentes tipos de tráfico.
Hacer cumplir etiquetas QoS (quality-of-service)	Priorizar una aplicación sobre otra
Bloquear aplicaciones no deseadas	Conservar ancho de banda y detener actividades no deseadas.
Límites de tasas para aplicaciones o para categorías de aplicaciones	Permitir tráfico no esencial, evitando que abrume a aplicaciones de misión crítica.

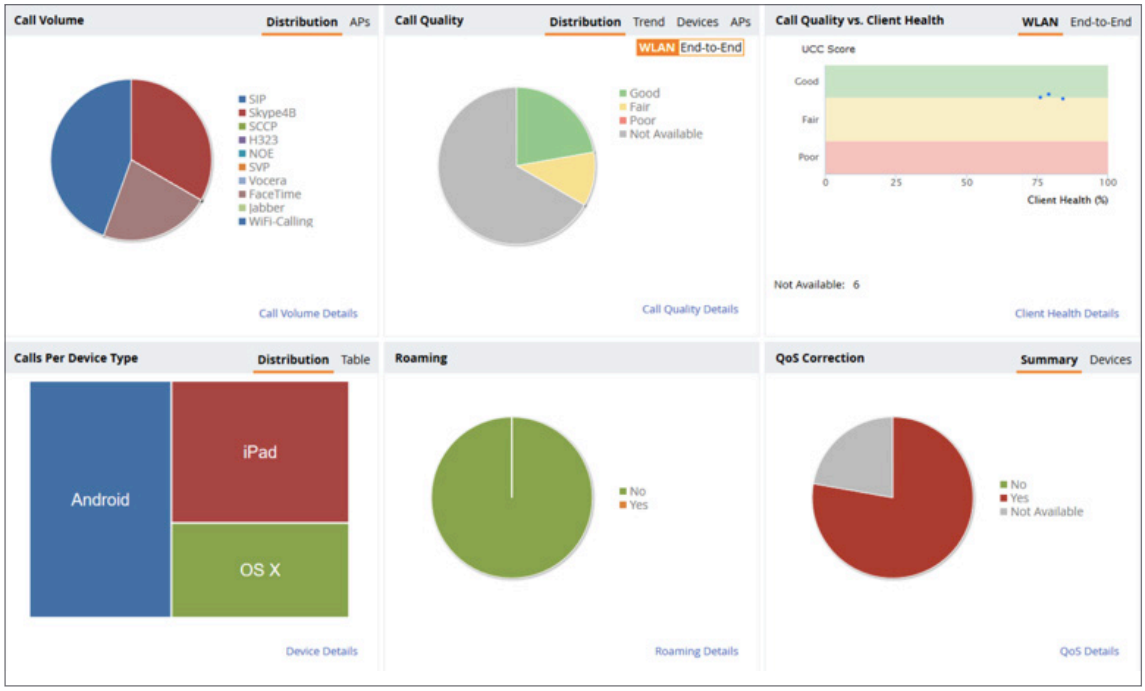


Figura 3: Tablero de control UCC en ArubaOS 8

WLAN ADAPTATIVA DE GRADO EMPRESARIAL

El acceso en cualquier momento y en cualquier lugar para dispositivos móviles y aplicaciones es un requerimiento en el mundo de negocios de hoy. El entregar ese acceso en forma confiable requiere una WLAN que administre activamente el espectro de radiofrecuencia (RF) en sincronía con el ambiente móvil dinámico mismo.

La tecnología ARM (Adaptive Radio Management), es una tecnología patentada y probada que utiliza controles automáticos basados en la infraestructura para administrar el espectro de RF completo. ARM ajusta dinámicamente el ambiente RF para maximizar la estabilidad y previsibilidad Wi-Fi, asegurando rendimiento óptimo para todos los clientes y aplicaciones, incluyendo visibilidad y control de flujos individuales de voz de Microsoft Skype for Business, video, desktop sharing y flujos de chats.

Con ARM, los usuarios obtienen una experiencia de usuario consistentemente positiva – sin intervención de TI.

ArubaOS 8 enriquece más aún la tecnologia Adaptive Radio Management (ARM) con AirMatch – el nuevo sistema de optimización RF.

AirMatch en el Mobility Conductor está diseñado teniendo en mente el ambiente RF moderno. AirMatch está afinado para ambientes ruidosos y de alta densidad, con escaso espacio de aire limpio o libre. Recopila estadísticas RF de las últimas 24 horas y optimiza proactivamente la red para el día siguiente. Con optimización automatizada de canales, ancho de canales y potencia de transmisión, AirMatch asegura uso parejo de canales, asiste en mitigación de interferencias y maximiza la capacidad del sistema.

Beneficios de AirMatch	
Asignación homogénea de canales	Proporciona distribución homogénea de radios a través de canales disponibles, mitiga interferencia y maximiza la capacidad del sistema.
Ajuste dinámico del ancho de canales	Ajusta dinámicamente entre 20MHz, 40MHz y 80MHz para igualar la densidad de su ambiente.
Ajuste automático de la potencia de transmisión	Examina la cobertura completa de la WLAN y ajusta automáticamente la potencia de transmisión de los APs para asegurar la mejor cobertura y experiencia de usuario.

MEJORA EN LA CONFIABILIDAD Y EXPERIENCIA DE USUARIO

Cantidades masivas de tráfico le está pegando a las redes desde dispositivos móviles, IoT y aplicaciones críticas de negocio. Los usuarios esperan no tener interrupciones en su experiencia móvil por falla de controladores o cuando se están desplazando en un campus grande. ArubaOS 8 proporciona un conjunto robusto de capacidades de alta disponibilidad, enlistadas a continuación, diseñadas para minimizar el tiempo de caída en el caso de falla de un controlador.

En el Mobility Conductor, la característica Controller Clustering permite que hasta 12 controladores se configuren en cluster en un despliegue WLAN campus y proporciona hitless failover. Los usuarios no notarán un problema en el remoto caso de la falla de un controlador. Las llamadas de voz, vídeo y transferencias de datos continuarían sin ningún impacto observable. La información de las sesiones de los usuarios se comparte a todos los controladores en el cluster para asegurar que no exista ningún sólo punto de falla para ningún usuario.

NETWORKING REMOTO PARA OFICINAS SUCURSALES Y TRABAJADORES REMOTOS

Las soluciones de networking remoto y para sucursales de Aruba proporciona una forma sencilla, segura y efectiva en costos para extender la red corporativa a oficinas sucursales, clínicas, tiendas, oficinas en el hogar y trabajadores remotos. ArubaOS integra características de sucursal dedicadas en el Mobility Controller, incluyendo terminación VPN en Mobility Controllers basados en el campus con el data center y servicios WAN en Mobility Controllers desplegados como un gateway de sucursal.

Los Mobility Controllers en el campus manejan todas las tareas complejas de configuración, administración, actualizaciones de software, autenticación, detección de intrusiones y terminación de los sitios remotos, mientras que los Mobility Controllers en la sucursal manejan tareas de gateway, como enrutamiento basado en políticas, compresión y funciones de red locales. En pequeñas sucursales o en casos de uso remotos, se pueden extender las redes corporativas con RAPs (Remote Access Points (RAPs) asequibles, o con servicios VPN VIA (Aruba Virtual Intranet Access) para personas que se están desplazando.

Modos de Implementación de Alta Disponibilidad	
Activo/Activo (1:1)	Cada Mobility Controller típicamente sirve al 50% de su capacidad calificada. El primero actúa como un respaldo para APs servidos por el segundo controlador y viceversa. Si uno de los controladores falla, sus APs efectúan failover al otro controlador, asegurando alta disponibilidad para todos los APs.
Activo/Respaldo (1+1)	Un Mobility Controller termina todos los APs, mientras que el otro controlador actúa como respaldo. Si el controlador primario se cae, los APs se mueven al controlador de respaldo.
N+1	Múltiples Mobility Controllers activos son respaldados por un solo controlador de respaldo.

Característica	**Beneficio**
El AP establece canales de comunicación simultáneos con el Mobility Controller activo y de respaldo.	Failover instantáneo al Mobility Controller redundante cuando el primero falla.
Durante un failover, los APs no apagan y prenden sus radios.	SSID siempre disponible.
La solución opera a través de redes Layer 3	No se requieren topologías especiales.
Client state sync	Las credenciales están en caché, eliminando la necesidad de reautenticar y sobrecargar el servidor RADIUS.
Sobresuscripción N+1	Simplifica la configuración y reduce el número de Controladores de Movilidad necesarios.

TRABAJADORES REMOTOS CON ACCESS POINTS REMOTOS	
Aprovisionamiento Zero-touch	Los administradores pueden desplegar RAPs sin ninguna pre configuración. Simplemente se envían al usuario final.
Alámbrico e inalámbrico	Los usuarios se conectan a los RAPs vía Ethernet alámbrico, Wi-Fi o ambos.
Autenticación flexible	802.1X, portal cautivo, autenticación de direcciones MAC por puerto y por usuario.
Administración centralizada	No se efectúa ninguna configuración local en APs – La configuración y la administración se efectúan por el Mobility Controller.
Conexión WAN LTE 3G/4G	Los RAPs soportan adaptadores WAN inalámbricos USB (EV-DO, HSDPA) para conectividad de Internet primaria o de respaldo.
Reenvío de tráfico FlexForward	• Centralizado – Todo el tráfico de usuarios fluye a un Mobility Controller • Puenteado localmente – Todo el tráfico de usuarios se puentea por el dispositivo de acceso al segmento LAN local. • Enrutado por política – El tráfico de usuarios selectivamente reenviado al Mobility Controller o puenteado localmente, dependiendo del tipo de tráfico/política (requiere licencia PEF).
Seguridad de grado empresarial	Los RAPs se autentican a los Mobility Controllers utilizando certificados X.509 y después establecen túneles IPsec seguros.
Reservación de ancho de banda uplink	Define el ancho de banda reservado para protocolos de aplicaciones sensibles a pérdidas, como voz.
Diagnósticos locales	En el caso de una llamada al help desk, los usuarios locales pueden navegar a un URL predefinido para acceder a diagnósticos completos para el RAP.
Portal de malla remoto	Un RAP también puede fungir como un portal de malla, proporcionando enlaces inalámbricos a APs downstream.
APs soportados	RAP-3, RAP Serie 100, RAP-155, AP-105, AP Serie 220, AP Serie 130, AP Serie 110, AP Serie 100, AP Serie 90, AP Serie 175
Velocidad de enlace mínima requerida	64 kbps por SSID
Protocolo de cifrado (RAP a Controlador de Movilidad)	AES-CBC-256 (inside IPsec ESP)

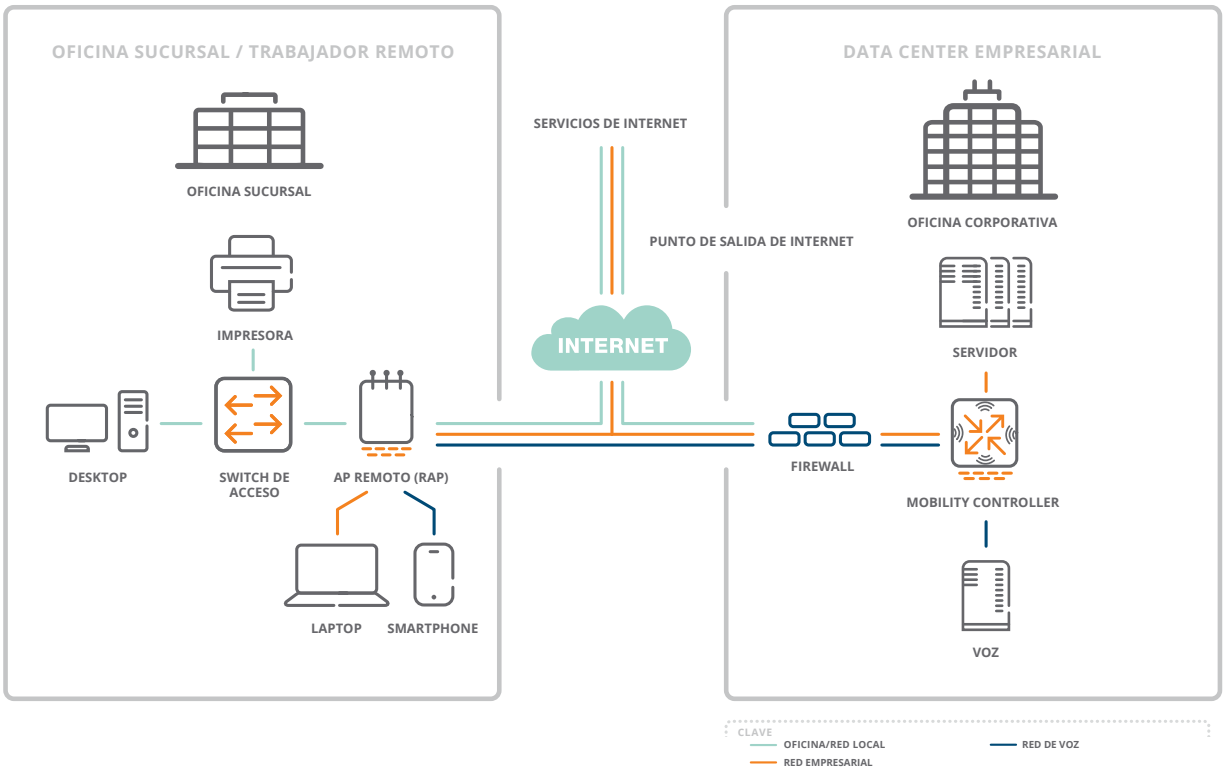


figura 2.8_071614

Los RAPs de Aruba proporcionan conectividad móvil segura a oficinas sucursales y oficinas en el hogar.

CONECTIVIDAD SIMPLE Y SEGURA PARA PROFESIONALES QUE VIAJAN

Los usuarios que requieren acceso a recursos empresariales mientras están alejados de la oficina típicamente dependen de software de cliente VPN, el cual se conecta a un concentrador VPN localizado en una DMZ empresarial.

Con Aruba, los usuarios VPN remotos son tratados como cualquier otro usuario. Aprovechan las mismas políticas de acceso y definiciones de servicio utilizadas en las oficinas centrales o en una implementación de RAP en oficina sucursal.

Los Mobility Controllers actúan como concentradores VPN, eliminando la necesidad de una infraestructura de acceso paralela.
ArubaOS es compatible con varios clientes VPN populares y con clientes VPN interconstruidos en sistemas operativos importantes de clientes. También proporciona el cliente VIA opcional, el cual se puede instalar en dispositivos Android, iOS, Mac OS X y Windows.
Al fusionar las redes de acceso, la política y la configuración de acceso se unifican, la experiencia para los usuarios se mejora, las llamadas al helpdesk se reducen y los gastos de TI disminuyen.

Conectividad Segura para Acceso Remoto	
Soporte a clientes probado	• Cliente Aruba VIA en Windows • Clientes VPN de Cisco y Nortel • OpenVPN, Apple/Windows cliente nativo
Protocolos VPN	• L2TP/IPsec (RFC 3193) • XAUTH/IPsec • PPTP (RFC 2637)
Autenticación	• Nombre de usuario/password • X.509 PKI • RSA SecurID • Smart Card • Multi-factor

MALLA EMPRESARIAL SEGURA

La solución de Malla empresarial segura de Aruba proporciona un diseño flexible, libre de cables, permitiendo que los APs sean colocados en donde se requieran – interiores y exteriores. La ausencia de segmentos de fibra o de cable reduce significativamente los costos de instalación de red y requiere menos puertos Ethernet.

La solución se integra completamente con el marco de trabajo de acceso unificado de Aruba, permitiendo una sola red empresarial en cualquier lugar en donde se encuentren los usuarios. La malla empresarial segura está basada en software programable y no requiere de hardware especializado; cualquier AP 802.11n o 802.11ac de Aruba para interiores o para exteriores puede funcionar como un AP de malla.

La malla empresarial segura puede soportar todas las necesidades inalámbricas empresariales, incluyendo acceso a Wi-Fi, protección concurrente de intrusiones inalámbricas, backhaul inalámbrico, puenteo LAN

y conectividad punto-a-multipunto, todo con una sola infraestructura común.

Esta es una solución excelente para aplicaciones de conectividad, incluyendo conectividad entre edificios, conectividad exterior en campus, oficinas libres de cables y respaldo de wire-line; aplicaciones de seguridad, como monitoreo de vídeo y audio, alarmas y señales de emergencia, aplicaciones industriales y redes de sensores.

A través de la tecnología de control cooperativo, Aruba utiliza un algoritmo inteligente de administración de enlaces para optimizar las rutas de tráfico y los enlaces.

Los APs de malla se comunican con sus vecinos y anuncian un número de atributos de RF y de enlaces – como costo de enlace, costo de ruta, costo de nodo, nivel de carga – que les permite efectuar una selección inteligente de la mejor ruta a tomar para la aplicación.

Las rutas en malla y los enlaces se ajustan automáticamente en el caso de altas cargas o interferencia. Más aún, las etiquetas de aplicaciones para tráfico de voz y de vídeo se comparten para asegurar que el tráfico sensible a latencia tendrá prioridad sobre datos.

La tecnología de control cooperativo también proporciona funcionalidad de auto reparación para la red en malla en el caso de una ruta bloqueada o de la falla de un AP.

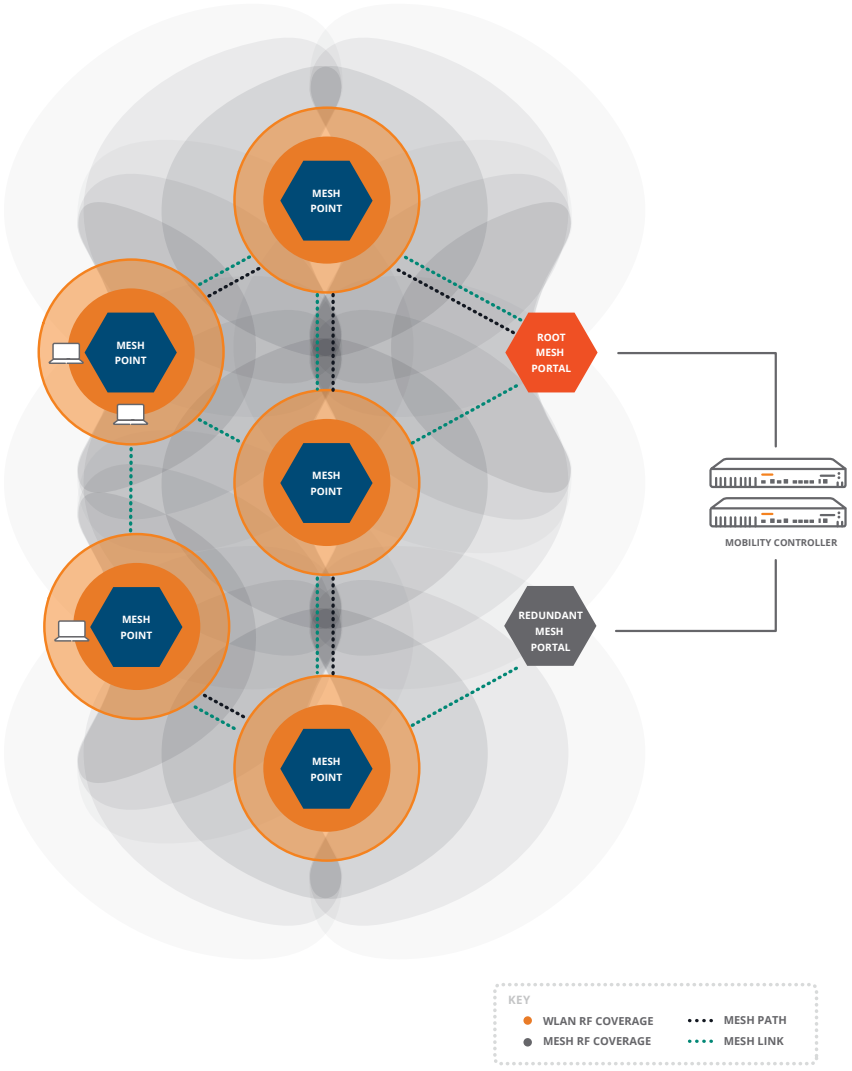


figura 2.9_071614

Solución de Malla Empresarial Segura de Aruba

Solución de Malla Empresarial Segura de Aruba	
Amplio soporte a aplicaciones	Acceso Wi-Fi, protección concurrente para intrusiones inalámbricas, backhaul inalámbrico, puenteo LAN y conectividad punto-a-multipunto.
Acceso unificado la red	Integra redes en malla con WLANs de campus y de oficinas sucursales. Los usuarios se desplazan transparentemente entre las redes Wi-Fi campus y de oficinas sucursales y las redes en malla.
Control Cooperativo	La administración inteligente de enlaces RF determina la ruta de rendimiento óptimo y permite que la red se auto organice.
Auto reparación	La malla resiliente auto reparable se sobrepone a una ruta interrumpida o a la falla de un AP.
Clustering en malla	Soporta escalabilidad, permitiendo que una gran malla sea segmentada en clusters altamente disponibles.
Cifrado centralizado	Datos cifrados de extremo a extremo, desde el cliente al core, protegiendo a la red aún si un AP de malla es robado.
Administración centralizada	Todos los nodos en la malla se configuran y se controlan centralmente por Controladores de Movilidad. No se requiere ninguna administración local.
Herramientas extensas de soporte gráfico	La visualización completa de la red incluye mapas de calor de cobertura, cálculo automático de presupuesto de enlaces, planes de piso y mapas con la topología de la red.
Diseño basado en normas	Secure enterprise mesh based on design principles from IEEE 802.11s.

ADMINISTRACIÓN, CONFIGURACIÓN Y REPARACIÓN DE FALLAS

La configuración, la administración y la localización y resolución de fallas de los Mobility Controlers se proporcionan a través de un GUI basado en navegador y una interface de líneas de comando, con la cual estará familiarizado cualquier administrador de redes.
ArubaOS también se integra con AirWave, lo cual facilita la administración durante todas las etapas del ciclo de vida de la WLAN – desde planificación y despliegue a monitoreo, análisis y localización y resolución de fallas. AirWave también proporciona tendencias a largo plazo y análisis, herramientas integración al helpdesk y reportes personalizados.

Todos los APs y Mobility Controllers, aún aquellos distribuidos en las oficinas sucursales o regionales, se pueden configurar y administrar centralmente desde una sola consola. Para facilitar la configuración de tareas comunes, los asistentes intuitivos basados en tareas guían al administrador de la red a través de cada paso del proceso.

Los Mobility Controllers se pueden desplegar en configuraciones redundantes 1:1 y 1:n basadas en VRRP con soporte redundante del data center. Al desplegarse en topologías Layer 3, el protocolo de enrutamiento OSPF permite el aprendizaje automático de rutas y distribución de rutas para rápida convergencia.

Administración y Configuración de la Red Inalámbrica	
Web-based configuration	Permite que cualquier administrador con un navegador web estándar administre el sistema.
Command line	Consola y SSH
Syslog	Soporta a múltiples servidores, múltiples niveles y múltiples instalaciones
SNMP v2c	Sí
SNMP v3	Enriquece el SNMP estándar con seguridad criptográfica.
Centralized configuration of Mobility Controllers	Un Mobility Controller maestro designado puede configurar y administrar a varios controladores locales downstream.
VRRP	Soporta alta disponibilidad entre múltiples Mobility Controlers.
Redundant data center support	Sí – los dispositivos de acceso se pueden configurar con direcciones IP para controladores de respaldo.
OSPF	Sí – soporte stub mode para aprendizaje de la ruta por omisión o inyectar rutas locales en un ruteador upstream.
Rapid spanning tree protocol	Sí – proporciona convergencia rápida Layer 2.

SOPORTE DE ARUBAOS PARA IPV6

Con el agotamiento de direcciones IPv4 disponibles, las organizaciones están ahora planificando o ya han comenzado implementaciones de IPv6 dentro de sus redes.

Aun cuando IPv4 y IPv6 definen como los datos se transmiten sobre las redes, IPv6 agrega un espacio de direcciones mucho mayor que IPv4 y puede soportar billones de direcciones IP únicas.

Conforme las organizaciones transicionan de IPv4 a IPv6, el equipo de red debe soportar interoperabilidad dual-stack de IPv6 dentro de una red IPv4 o implementaciones completas dentro de un ambiente puro de IPv6.

ArubaOS facilita el despliegue de Mobility Controllers y de APs en ambientes IPv6 y dual-stack de la actualidad. Casi todas las funciones, con la excepción de IPsec, se pueden implementar en modo nativo IPv6. Cada aspecto del administración, monitoreo y firewalls son completamente conscientes de IPv6.

Soporte para IPV6	
IPV6 IPsec	Sí
Administración sobre IPv6	GRE, SSH, Telnet, SCP, Web UI, FTP,TFTP, Syslog, SNMP
Servidor DHCP IPv6	Sí
Portal cautivo sobre IPv6	Sí
Soporta dirección de interface VLAN IPv6 en el Controlador de Movilidad	Sí
Soporta comunicación AP-Controlador de Movilidad sobre IPv6	Sí
Firewall certificado USGv6	Sí

CONTROLES CONSCIENTES DE CONTEXTO

Soporte para 802.11e y Wi-Fi Multimedia (WMM) asegura QoS inalámbrico para aplicaciones sensibles a retrasos con mapeo entre etiquetas WMM y colas de hardware internas.

Los Mobility Controllers permiten el mapeo de etiquetas 802.1p y IP DiffServ a colas de hardware para QoS del lado alámbrico y pueden ser instruidos para aplicar ciertas etiquetas 802.1p y IP DiffServ a diferentes aplicaciones bajo demanda.

Con la adición del módulo Aruba PEF, se les da seguimiento a los protocolos de voz sobre IP – incluyendo Lync, SIP (session initiation protocol), SVP (Spectralink Voice Priority), NOE (Alcatel New Office Environment), Vocera y SCCP (skinny call control protocol) – dentro del Mobility Controller de Aruba. La tecnología de "fingerprinting" de aplicaciones de Aruba permite que los Mobility Controllers den seguimiento a protocolos de señalización cifrados.

Una vez que estos flujos se identifican, las WLANs de Aruba los priorizan para entrega en el canal inalámbrico y disparan características relacionadas con voz.

Estas características relacionadas con voz pueden incluir comandos como posponer el escaneo de ARM por la duración de la llamada y priorizan itinerancia para clientes que están involucrados en una llamada activa. Esto es crítico para habilitar el despliegue a gran escala de comunicaciones de voz empresariales sobre Wi-Fi.

Adicionalmente, ArubaOS ahora incluye tecnología de "fingerprinting" para dispositivos, permitiendo que los administradores asignen políticas de red a tipos de dispositivos, en adición a aplicaciones y a usuarios. Fingerprinting de dispositivos entrega mayor control sobre la forma en la cual se permite a los dispositivos acceder a la red y la forma en la cual estos dispositivos se pueden utilizar.

ArubaOS puede identificar y clasificar en forma precisa a dispositivos móviles, como el Apple iPad, iPhone, o iPod, así como a dispositivos corriendo los sistemas operativos Android o BlackBerry. Esta información se puede compartir con AirWave para visibilidad enriquecida de la red para todos los usuarios de la red, independientemente de sus ubicaciones o dispositivos móviles.

CONTROLES CONSCIENTES DE CONTEXTO	
T-SPEC/TCLAS	Sí
WMM	Sí
Mapeo de prioridad WMM	Sí
U-APSD (Unscheduled Automatic Power-Save Delivery)	Sí
Snooping IGMP para entrega eficiente de multicast	Sí
Fingerprinting de aplicaciones y dispositivos	Sí

CERTIFICACIONES

- Certificado por Wi-Fi Alliance (802.11a/b/g/n/d/h/ac, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM Power Save)
- Validado por FIPS 140-2 (cuando se opera en modo FIPS)
- Common Criteria EAL-2
- Certificado por RSA
- Certificado por Polycom/Spectralink VIEW
- USGv6 firewall

NORMAS SOPORTADAS

Switching y Routing General

- 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 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 y Políticas

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

Inalámbrico

- 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)

Administración y Análisis de Tráfico

- 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

Seguridad y Cifrado

- 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