



Red Aruba centrada en el usuario para sanidad

¿Cuál es su objetivo? ¿Contribuir a que su hospital sea un verdadero centro de excelencia respecto a la atención al paciente? ¿Proporcionar a sus médicos y enfermeras la mejor tecnología, extendiendo la efectividad y eficiencia al lugar de atención médica? ¿Crear una red que verdaderamente sea accesible para todo el personal sanitario, de administración y a los pacientes en cualquier lugar, desde cualquier dispositivo, que se ajuste exactamente a sus necesidades?

Aruba ha elaborado un nuevo enfoque para ayudarle a conseguir su objetivo. Las redes Aruba centradas en el usuario integran LAN inalámbricas adaptativas, seguridad basada en identidad y servicios de continuidad de aplicación en un sistema de alto rendimiento para campus sanitarios, clínicas, consultas médicas y oficinas domésticas. El resultado es una red de gestión centralizada que distribuye las aplicaciones de asistencia sanitaria por la LAN, la WAN e Internet, aumentando la productividad de los usuarios sin ningún impacto negativo sobre la seguridad. A diferencia de otras soluciones, la red Aruba centrada en el usuario se superpone a las redes existentes, preservando las inversiones actuales y evitando cambios de red disruptivos.

Características únicas de Aruba

LA LEY HIPAA DE EE.UU. (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT) Y LA CONFIDENCIALIDAD DE LOS PACIENTES

La HIPAA y otras normativas similares a nivel internacional obligan al personal sanitario a asegurar la confidencialidad de la información del paciente. La seguridad Aruba basada en identidad asegura el cumplimiento de la HIPAA y el acceso a las aplicaciones de asistencia sanitaria desde cualquier lugar y a través de cualquier dispositivo. Con el cortafuegos de Aruba con certificado ICSA integrado, las políticas de seguridad por usuario se aplican dentro del hospital o desde el hospital hasta el consultorio, e incluso en casa o en la oficina. Además, con la seguridad basada en identidad, los dispositivos anteriores (por ejemplo, dispositivos portátiles VoWLAN, escáneres de código de barras que sólo son compatibles con seguridad rudimentaria tipo WEP) pueden integrarse de forma segura en la red sin contravenir la HIPAA.

La normativa HIPAA también requiere mantener sistemas seguros, lo cual incluye la capacidad para detectar e

impedir dispositivos no autorizados (por ejemplo, AP maliciosos) o ataques en el aire (OTA). Aruba ofrece servicios integrados de protección contra intrusiones inalámbricas, en los que los AP de Aruba actúan como supervisores del entorno inalámbrico (AM), eliminando la necesidad de sensores de seguridad de otros fabricantes.

CONTINUIDAD DE APLICACIÓN

La operación ininterrumpida de aplicaciones clínicas móviles, como EMR/EHR y CPOE es vital para el entorno de asistencia sanitaria. Adicionalmente, el uso de una LAN con VOIP inalámbrico (VoWLAN) para aplicaciones de llamadas a personal sanitario y como sustitución de una mala cobertura de red móvil es esencial. Para conseguir la compatibilidad de aplicaciones clínicas y de voz, la red debe ser capaz de implementar QoS por aire y por cable, y ajustar los patrones de tráfico para optimizar el rendimiento.

Aruba ofrece una serie de funciones adaptativas de LAN inalámbricas para optimizar la RF para el funcionamiento de aplicaciones esenciales y sensibles a la latencia, incluso en el entorno con más

La ventaja de Aruba:

- **Conectividad Sígueme:** Ofrece un acceso en cualquier lugar dentro de los hospitales, clínicas, consultorios médicos y oficinas domésticas.
- **Seguridad Sígueme:** Asegura la confidencialidad del paciente y el cumplimiento de las normativas HIPAA.
- **Continuidad de aplicación:** Servicios ininterrumpidos para el entorno de asistencia sanitaria esencial.
- **Menor coste total de propiedad:** Una plataforma integrada de alto rendimiento para la asistencia sanitaria que elimina la necesidad de dispositivos extra.

desafíos. Esto incluye el roaming rápido (<10 ms) durante las transferencias entre AP, detección y corrección automática de huecos de cobertura y reparto de carga en áreas de alta densidad. La solución de Aruba reconoce la voz totalmente, aprovechando un cortafuegos basado en la aplicación que asegura y prioriza la voz. El tráfico de voz se prioriza a través de etiquetas QoS 802.1p y DSCP y esta priorización acompaña a los usuarios de voz en su desplazamiento por la red. Aruba reconoce automáticamente los protocolos de voz más comunes (especialmente SIP, SVC, y SCCP) y aplica una prioridad estricta al tráfico de voz. La priorización de llamadas también puede realizarse a través del control de admisión de llamadas (CAC). CAC establece un máximo de llamadas de voz por AP, moviendo de forma dinámica cualquier llamada por encima de este límite a otros AP vecinos y manteniendo una calidad de la voz excepcionalmente elevada.

Para asegurar los más altos niveles de fiabilidad y rendimiento, Aruba se ha asociado con muchos de los mejores proveedores de soluciones para la asistencia sanitaria, testando y probando cada aplicación antes de ser ofertada. Entre los socios de Aruba se encuentran Welch Allyn y Drager Medical para las soluciones de monitorización del paciente; SpectraLink/Polycom, Avaya, Ascom y Vocera para sistemas de llamada de personal sanitario y de voz; AeroScout, Ekahau e Inner Wireless/Pango para soluciones de seguimiento de dispositivos.

GESTIÓN CENTRALIZADA

Desplegar y gestionar una red eminentemente inalámbrica puede resultar una ardua tarea si no se enfoca correctamente. La red Aruba centralizada y su gestión de políticas está diseñada para facilitar su despliegue y funcionamiento. Con la gestión centralizada Aruba, la

configuración de los datos se propaga de forma automática y segura por toda la red, los puntos de acceso y los controladores locales y remotos. Se proporciona una única interfaz para TI con el fin de implementar y proteger las políticas subyacentes que aseguran la integridad, la seguridad y el funcionamiento de toda la red. La función de control centralizado también incluye perfiles de rendimiento que son utilizados por los puntos de acceso Aruba para optimizar su operación y soportar con garantías las aplicaciones esenciales. El resultado es una red de gran escalabilidad que es lo suficientemente simple como para ser utilizada por usuarios no especializados.

RENDIMIENTO Y ESCALABILIDAD

La LAN inalámbrica debe ser compatible con los requisitos existentes a la vez que es capaz de adaptarse al crecimiento y la adopción de nuevos dispositivos y aplicaciones portátiles. Los retos clave de ampliar una LAN inalámbrica para la asistencia sanitaria están relacionados con la densidad de usuarios y dispositivos, la carga instantánea durante el uso en horas punta, y la movilidad de los usuarios por diferentes áreas a través de la LAN, la WAN e Internet. Aruba Networks ha desarrollado innovaciones para automatizar la configuración RF, descargar los servidores backend AAA y hacer más escalable el diseño de VLAN para adaptarse a diferentes patrones de uso. Adicionalmente, Aruba ofrece plataformas de alto rendimiento específicas, de gran escalabilidad y potente capacidad que implementan las aplicaciones existentes, la infraestructura de TI y los clientes estándar. Diseñados para adaptarse a las necesidades de los usuarios de hoy y de los años venideros, la mayoría de los productos Aruba cuentan con una arquitectura de software modular y actualizable que se puede mejorar fácilmente con el tiempo a medida que estén disponibles nuevas funciones.

La solución de Aruba Networks para sanidad

La solución Aruba está formada por tres componentes clave: puntos de acceso ligeros (AP), controladores de movilidad centralizados y módulos de software para los controladores de movilidad; además de los equipos opcionales de protección frente a amenazas y análisis de la gestión. Los AP proporcionan una conectividad inalámbrica segura a los dispositivos y se conectan mediante sistemas LAN/WAN existentes para conducir todo el tráfico LAN inalámbrico por un túnel GRE o IPsec a un controlador de movilidad instalado en el centro de datos. El controlador de movilidad es el punto central de configuración, gestión, servicios de continuidad de la aplicación y seguridad.

Con los módulos de seguridad para controladores de movilidad, Aruba ofrece la seguridad necesaria de conformidad con la normativa.

A continuación, se incluye la explicación de una red inalámbrica en un entorno sanitario con servicios de TI centralizados:

Centro de datos: Uno o varios controladores de movilidad se encuentran instalados en el centro de datos, que puede ser usado como el punto de gestión y configuración para toda la red internacional. Estos controladores también pueden terminar AP usados para dar conectividad

inalámbrica en el campus de asistencia sanitaria principal y AP remotos usados por teletrabajadores y oficinas domésticas. Un controlador principal puede admitir hasta 500 controladores remotos y también puede respaldar a un controlador en una ubicación remota en caso de caída. Para alcanzar un mayor despliegue, varios controladores principales pueden compartir la tarea de gestionar los controladores locales y AP en ubicaciones remotas, y el sistema de gestión de movilidad (MMS) puede usarse como interfaz única de gestión y configuración.

Ambulatorios, edificios de consultas médicas y grandes clínicas: En función del número de AP que cada ubicación requiera, se instala un modelo diferente de controlador de movilidad Aruba, también conocido como controlador local. Todos los modelos de controladores Aruba operan con el mismo software y tienen la misma funcionalidad, pero difieren en su capacidad de AP, que oscila entre 4 y 512 AP. Cada controlador local obtiene su configuración del controlador principal. La continuidad de aplicación y las políticas de seguridad se aplican a nivel de usuario por el controlador local. Se aplican diferentes roles de usuario mediante una política de grupo definida en la infraestructura de autenticación y los invitados pueden ser redireccionados mediante un túnel fuera de la red para terminar en la zona desmilitarizada

o DMZ. Los controladores también locales ofrecen protección contra intrusiones inalámbricas y pueden proporcionar servicios de autenticación local o enviar peticiones al centro de datos. Cada controlador local calibra automáticamente la cobertura de RF para optimizar el rendimiento de la aplicación y tapar cualquier hueco de cobertura. Además, para extender la cobertura inalámbrica a áreas que sean difíciles o costosas de cablear, los AP de Aruba tienen capacidad de backhaul (red de retorno) sobre Wi-Fi mediante la tecnología galardonada de malla empresarial segura.

Oficinas domésticas y consultorios médicos: Los AP remotos son una solución económica para ofrecer conectividad inalámbrica segura y gestionada centralmente a las ubicaciones que sólo necesitan uno o dos AP. Los AP remotos se pueden conectar directamente vía Ethernet a una conexión de Internet pública o privada o a la LAN. Los AP remotos detectan automáticamente el controlador principal, establecen un túnel VPN al centro de datos y extienden la conectividad inalámbrica segura al usuario. El tráfico de la aplicación se puede dirigir mediante un túnel al centro de datos o bien se puede puentear localmente.

