



## Benutzerorientierte Netzwerke von Aruba für Gesundheitseinrichtungen

Wie gestalten Sie die Zukunft? Sie möchten, dass Ihr Krankenhaus bei der Patientenversorgung durch exzellente Leistungen beeindruckt? Ihre Ärzte und Pflegekräfte sollen modernste Technologien effizient und effektiv auch im direkten Patientenkontakt einsetzen? Sie möchten ein Netzwerk nutzen, das tatsächlich überall verfügbar ist und auf das alle medizinischen Mitarbeiter, Verwaltungsangestellten und Patienten sicher zugreifen können – ortsunabhängig, bedarfsgerecht und mit beliebigen Geräten?

Aruba hat einen neuen Ansatz entwickelt und implementiert, mit dem diese Vision praktisch realisiert werden kann. Die benutzerorientierte Netzwerkarchitektur von Aruba verknüpft adaptive Drahtlosnetzwerkinfrastrukturen mit identitätsorientierten Sicherheitsfunktionen und Application Continuity Services und ermöglicht so integrierte Hochleistungsnetzwerke für Krankenhäuser, Praxen und Heimarbeitsplätze. Innerhalb des zentral verwalteten Netzwerks können die Benutzer produktiver arbeiten, da sie Krankenhausanwendungen über LAN, WAN und Internet ohne Einschränkungen bei der Sicherheit mobil nutzen können. Im Unterschied zu anderen Lösungen kann die benutzerorientierte Netzwerkarchitektur von Aruba in bestehende Netzwerke integriert werden, so dass bereits getätigte Investitionen weiterhin genutzt und radikale Umbauten bestehender Netzwerke vermieden werden.

### Einzigartige Aruba-Funktionen

#### **HIPAA UND VERTRAULICHE BEHANDLUNG VON PATIENTENDATEN**

HIPAA und andere Gesetze in vielen Ländern der Welt verpflichten Gesundheitsdienstleister, die Vertraulichkeit von Patientendaten durch geeignete Maßnahmen zu sichern. Die identitätsorientierten Sicherheitsfunktionen der Aruba-Architektur sorgen für die Einhaltung der HIPAA-Vorschriften und für sicheren Zugriff auf Softwareanwendungen an beliebigen Orten und mit beliebigen Geräten. Die ICSA-zertifizierte Firewall als Bestandteil der Netzwerkarchitektur von Aruba ordnet Sicherheitsrichtlinien Benutzern zu, so dass diese immer in gleicher Weise gelten, auch wenn sich Benutzer innerhalb des Krankenhauses bewegen oder sich in Praxen bzw. ihren Heimbüros aufhalten. Mit identitätsorientierten Sicherheitsfunktionen können Geräte, die nicht auf dem neuesten Stand der Technik sind (z. B. VoWLAN-Telefone oder Barcodescanner, die nur schwache Sicherheitsfunktionen wie WEP unterstützen), sicher in das Netzwerk eingebunden werden, ohne gegen Datenschutzbestimmungen zu verstoßen.

Die HIPAA-Bestimmungen fordern auch den Einsatz von Systemen zur Erkennung und Verhinderung von Angriffen nicht autorisierter

Geräte (z. B. fremder Access Points) auf das WLAN. Die Netzwerkarchitektur von Aruba ist mit Funktionen zum Schutz vor Angreifern ausgestattet (Wireless Intrusion Prevention). Zur Überwachung des Netzwerks werden die Access Points von Aruba als Air Monitors (AMs) eingesetzt, so dass keine zusätzlichen Überwachungsgeräte von Drittanbietern eingesetzt werden müssen.

#### **APPLICATION CONTINUITY**

Der unterbrechungsfreie Betrieb mobiler Anwendungen wie CPOE und der EPA ist eine entscheidende Funktion im Krankenhausbetrieb. Darüber hinaus sind VoIP-over-WLAN-Dienste (VoWLAN) für den Personalruf und als Alternative bei schlechter Mobilfunknetzversorgung wichtig. Damit Klinik- und Sprachanwendungen zuverlässig funktionieren, müssen QoS-Funktionen für drahtlosen und drahtgebundenen Datenverkehr eingesetzt werden, die unterbrechungsfreie Sprachanrufe ermöglichen und Datenverkehrsmuster optimieren.

Die WLAN-Architektur von Aruba optimiert die Funkübertragung für entscheidende und latenzempfindliche Anwendungen auch in schwierigsten Umgebungen. Zu den eingesetzten

Vorteile der Aruba-Lösung:

- **Ortsunabhängiger Netzzugriff:** Ortsunabhängiger Zugriff in Krankenhäusern, Praxen und Heimbüros
- **Ortsunabhängige Sicherheit:** Gewährleistet Sicherheit der Patientendaten und Einhaltung der gesetzlichen Vorschriften
- **Application Continuity:** Unterbrechungsfreier Betrieb entscheidender Anwendungen
- **Geringere Gesamtbetriebskosten:** Integrierte Hochleistungsplattform macht ergänzende Systeme von Drittanbietern überflüssig

Techniken gehören Fast Roaming (<10 ms) bei Handoffs zwischen Access Points, automatische Erkennung und Korrektur von Abdeckungslücken und Lastverteilung in Bereichen mit hoher Gerätedichte. Die Aruba-Architektur ist uneingeschränkt sprachdatenfähig, da zur Sicherung und Priorisierung von Sprachdatenübertragungen die anwendungsorientierte Firewall genutzt werden kann. Sprachdatenverkehr wird mit 802.1p- und DSCP-QoS-Tags priorisiert. Die Priorisierung wird auch dann aufrechterhalten, wenn sich Nutzer von Sprachdiensten im Netzwerk bewegen. Das System erkennt verbreitete Sprachübertragungsprotokolle wie SIP, SVC und SCCP automatisch und weist dem Transport von Sprachdaten höchste Priorität zu. Anrufe können außerdem mit Call Admission Control (CAC) priorisiert werden. Eine Höchstanzahl zulässiger Sprachanrufe pro Access Point kann festgelegt werden, so dass weitere Anrufversuche über benachbarte APs abgewickelt werden und die gewünschte Sprachqualität laufender Gespräche nicht beeinträchtigt wird.

Um beste Ergebnisse bei Zuverlässigkeit und Leistung zu erreichen, kooperiert Aruba mit mehreren führenden Gesundheitsdienstleistern, bei denen alle Anwendungen umfassend getestet und evaluiert werden. Bei Anwendungen für die Patientüberwachung kooperiert Aruba unter anderem mit Welch Allyn und Dräger Medical. Bei Sprach- und Personalarufdiensten arbeiten wir mit SpectraLink/Polycom, Avaya, Ascom und Vocera zusammen. Im Bereich Bestandsverfolgung bestehen Partnerschaften mit AeroScout, Ekahau und Inner Wireless/Pango.

#### **ZENTRALE VERWALTUNG**

Die Bereitstellung und Verwaltung großer Drahtlosnetzwerke kann sich zu einem kritischen Problem auswachsen, wenn schwer handhabbare Ansätze gewählt werden. Die zentralisierte Netzwerk- und Richtlinienverwaltung der Aruba-Architektur ist auf einfache Handhabung bei Bereitstellung

und Betrieb ausgerichtet. In zentral verwalteten Netzwerkinfrastrukturen von Aruba werden Konfigurationsdaten automatisch und sicher im Netzwerk verbreitet und zu lokalen und externen Access Points und Controllern weitergeleitet. IT-Administratoren steht eine einheitliche Benutzeroberfläche zur Verfügung, mit der sie Richtlinien implementieren und schützen können, um Integrität, Sicherheit und Betriebsbereitschaft des Netzwerks sicherzustellen. Zu den Funktionen für zentralisierte Steuerung gehören auch Leistungsprofile, mit denen Access Points von Aruba ihren Betriebsmodus optimieren, um entscheidende Anwendungen zuverlässig unterstützen zu können. Auf diese Weise entsteht ein extrem skalierbares Netzwerk, das auch von technischen Laien mühelos genutzt werden kann.

#### **LEISTUNG UND SKALIERBARKEIT**

Beim Aufbau von WLAN-Systemen muss darauf geachtet werden, dass diese nicht nur aktuell bestehende Anforderungen erfüllen, sondern auch an steigenden Bedarf und zukünftige Geräte und Anwendungen angepasst werden können. Zu den größten Herausforderungen beim Skalieren von Drahtlosnetzwerken in Gesundheitseinrichtungen gehören Benutzer- und Gerätedichte, Lastspitzen während der Hauptnutzungszeiten und die Versorgung mobiler Benutzer über LAN, WAN und Internet. Aruba hat eine Reihe von Innovationen für automatische Funknetzwerkverwaltung, zur Entlastung von AAA-Servern und zur Skalierung von VLANs entwickelt, die flexibles Reagieren auf variable Nutzungsmuster ermöglichen. Darüber hinaus bietet Aruba leistungsstarke, extrem skalierbare optimierte Plattformen mit hohem Durchsatz an, in die bestehende Anwendungen, IT-Infrastrukturen und Standardclients integriert werden können. Damit auch unvorhersehbare Anforderungen erfüllbar sind, werden die meisten Produkte von Aruba mit einer modularen Softwarearchitektur betrieben, die schrittweise erweitert werden kann, sobald neue Funktionen benötigt werden.

### **Die Netzwerklösung von Aruba für Gesundheitseinrichtungen**

Zur Lösung von Aruba gehören drei Hauptkomponenten: Thin Access Points (APs), zentrale Mobility Controller und Softwaremodule für Mobility Controller. Als optionale Komponente können Appliances für Analysen und zum Schutz vor Angriffen eingesetzt werden. Die Access Points sorgen für sichere drahtlose Verbindungen von den Endgeräten zu bestehenden LAN-/WAN-Systemen und leiten den gesamten drahtlosen Datenverkehr über GRE- bzw. IPsec-Tunnel zu einem Mobility Controller im Datenzentrum. Der Mobility Controller ist die zentrale Schaltstelle für Konfiguration, Verwaltung, Application Continuity Services und Sicherheit. Mit Sicherheitsmodulen für Mobility

Controller bietet Aruba die erforderlichen Sicherheitslösungen für die Einhaltung einschlägiger Vorschriften an.

Im Folgenden werden wichtige Merkmale für drahtlose Netzwerke in Gesundheitseinrichtungen mit zentralisierter IT-Administration beschrieben:

**Datenzentrum:** Im Datenzentrum wird mindestens ein Master Mobility Controller installiert, der als zentrale Schaltstelle für Konfiguration und Verwaltung für das gesamte globale Netzwerk genutzt werden kann. Master Controller können auch Gegenstellen für Access Points im Haupthaus der Einrichtung und für Remote Access Points

sein, die von Telearbeitern und in Heimbüros eingesetzt werden. Jeder Master Controller kann bis zu 500 Remote Controller verwalten und außerdem als Ausfallsicherung für Controller an externen Standorten genutzt werden. Bei größeren Installationen kann die Verwaltung lokaler Controller und Access Points an externen Standorten auf mehrere Master Controller verteilt werden. Als Schnittstelle für Verwaltung und Konfiguration kann in diesem Fall ein Mobility Management System (MMS) eingesetzt werden.

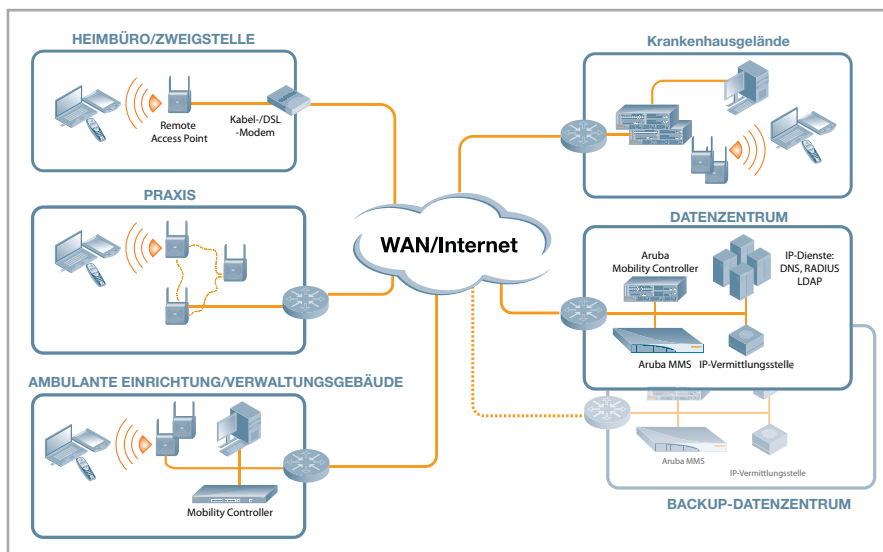
**Ambulante Einrichtungen/  
Verwaltungsgebäude/große Kliniken:**

Welche Aruba Mobility Controller an den einzelnen Standorten installiert werden (lokale Controller) hängt davon ab, wie viele Access Points jeweils verwaltet werden müssen. Alle Controllermodelle von Aruba sind mit der gleichen Software und mit den gleichen Funktionen ausgestattet. Sie unterscheiden sich lediglich in der Anzahl der unterstützten Access Points. Unterstützt werden je nach Modell 4 bis 512 Access Points. Die lokalen Controller erhalten ihre Konfigurationsdaten vom Master Controller. Application Continuity und Sicherheitsrichtlinien werden benutzerorientiert von den lokalen Controllern verwaltet. Die Anwendung von Benutzerrollen erfolgt anhand von Gruppenrichtlinien, die in der Authentifizierungsinfrastruktur definiert sind. Gästedatenverkehr kann am internen Netzwerk vorbei in die DMZ geleitet werden.

Die lokalen Controller bieten außerdem Wireless Intrusion Protection und lokale Authentifizierungsdienste und/oder leiten Anfragen an das Datenzentrum weiter. Jeder einzelne lokale Controller kalibriert automatisch die Funkreichweite, um optimale Anwendungsleistung zu erzielen und Lücken in der Netzabdeckung zu vermeiden. Um die Funknetzwerkversorgung auf Bereiche auszudehnen, in denen das Verlegen von Netzkabel nur schwer oder nur zu hohen Kosten möglich wäre, können Access Points von Aruba auf die innovative Secure Enterprise Mesh-Technik zurückgreifen.

**Niedergelassene Ärzte und Heimbüros:**

Mit Remote Access Points können Bereiche, in denen nur ein oder zwei APs benötigt werden, kostengünstig, sicher und zentral verwaltet mit Drahtlosanbindung versorgt werden. Remote Access Points können direkt an öffentliche/private Internetzugänge oder an LANs angeschlossen werden. Sie finden automatisch den Master Controller und bauen einen VPN-Tunnel zum Datenzentrum auf, so dass externe Benutzer sicher mit drahtloser Anbindung versorgt werden können. Datenverkehr kann je nach Anwendung über das Datenzentrum oder lokal geroutet werden.



[WWW.ARUBANETWORKS.COM](http://WWW.ARUBANETWORKS.COM)

1322 Crossman Avenue, Sunnyvale, CA 94089, USA | Tel.: +1 408.227.4500 | Fax: +1 408.227.4550