



Benutzerorientierte Netzwerke von Aruba für die verarbeitende Industrie

Wie gestalten Sie die Zukunft? Sie wünschen sich schnelleren Überblick bei Abläufen, Projekten und Inventar? Sie möchten die Produktivität steigern, indem Sie Zugriff auf Netzwerkressourcen und Kontakt zwischen Mitarbeitern jederzeit und an jedem Ort ermöglichen? Sie möchten die Fehlerhäufigkeit senken und Fertigungsabläufe weiter automatisieren?

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 Hochleistungssysteme für Produktionsanlagen, Außendienst, Lager und Verwaltung. Sie bietet zuverlässigen drahtlosen Zugang auf dem gesamten Betriebsgelände zu beliebigen mobilen Anwendungen und mit beliebigen Geräten.

Einzigartige Aruba-Funktionen

OPTIMIERT FÜR RAUE PRODUKTIONSUMGEBUNGEN

Anders als klassische Büroräume sind Produktionsanlagen für drahtlose Netzwerke aufgrund vieler variabler Parameter und starker physischer Beanspruchung eine besondere Herausforderung. Aruba hat eine angepasste Lösung für die unterbrechungsfreie drahtlose Netzwerkanbindung entwickelt.

WLANS in anspruchsvollen Umgebungen

können mit dem Aruba AP-85 and anderen robust konstruierten Access Points realisiert werden. Dank Temperaturbeständigkeit über große Temperaturbereiche, verschiedener Stromversorgungsoptionen, leistungsstarker Funkantennen, räumlicher Diversität, IP68 und anderer Merkmale sind unternehmenstaugliche Drahtlosnetzwerke nun auch für die anspruchsvollsten Innen- und Außenbereiche verfügbar.

Außengelände und Bereiche, in denen keine Kabel verlegt werden können, sind jetzt mit der innovativen Secure Enterprise Mesh-Technik von Aruba erreichbar. Alle Access Points von Aruba für Innen- und Außenbereiche, die nicht über Ethernet- oder Glasfaserkabel in das Netzwerk eingebunden werden können, lassen sich untereinander drahtlos verbinden.

ZUVERLÄSSIGE BEREITSTELLUNG ENTSCHEIDENDER MOBILER ANWENDUNGEN

Mobile Anwendungen in Produktionsanlagen sind vielfältig und unverzichtbar für die

Aufrechterhaltung des Produktionsbetriebs. Dazu gehören unter anderem Echtzeitschutz vor Angriffen auf das drahtlose Netzwerk, Bestandsverfolgung, VoIP über WLAN (VoWLAN), Funksensoren und Videoübertragung über IP. Damit mobile Daten-, Sprach- und Videoanwendungen zuverlässig und simultan unterstützt werden können, muss das Netzwerk QoS-Funktionen für drahtlosen und drahtgebundenen Datenverkehr bieten und Datenverkehrsmuster für optimale Anwendungsleistung anpassen.

Die WLAN-Architektur von Aruba optimiert die Funkübertragung für entscheidende und latenzempfindliche Anwendungen auch in schwierigsten Umgebungen. Zu den eingesetzten 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 Architektur ist uneingeschränkt sprachdatenfähig, da zur Sicherung und Priorisierung von Sprachdatenübertragungen die Deep Packet Inspection 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 innerhalb des Netzwerks bewegen.

SICHERHEIT FÜR ANWENDUNGSSPEZIFISCHE GERÄTE

Vorteile der Aruba-Lösung:

- Angepasst für physisch anspruchsvolle Innen- und Außenbereiche
- Zuverlässiger Betrieb dank adaptiver Drahtlosanbindung und Anwendungssensitivität
- Netzwerke und Unternehmenswerte werden durch technologie- und anwendungsspezifische Funktionen für Gerätesicherheit geschützt
- Geringe Gesamtbetriebskosten dank integrierter WLAN-, Sicherheits- und Verwaltungsplattform

(ASDs)

ASDs, die in Produktionsanlagen benutzt werden, sind anders als handelsübliche WLAN-Notebooks meist nur durch schwache Sicherheitsfunktionen wie WEP geschützt. Die identitätsorientierten Sicherheitsfunktionen der Aruba-Architektur sorgen dafür, dass auch ASDs und Geräte, die nicht auf dem neuesten technischen Stand sind, sicher in das Netzwerk eingebunden werden. Angriffe auf WLANs für ASDs und schwach geschützte Geräte werden von den Aruba-Controllern durch benutzerbezogene Firewall- und Intrusion Detection-Funktionen verhindert. Das Sicherheitsniveau wird deshalb nicht mehr durch die eingesetzten Endgeräte begrenzt.

GERINGE GESAMTBETRIEBSKOSTEN

Mit einer integrierten Plattform für Sicherheit (Wireless IPS, ICSA-zertifizierte Stateful Firewall, VPN Concentrator), WLAN und Verwaltung (Funk-Heatmaps, zentrale Verwaltung, Packet Capture-Werkzeuge) werden Kosten für Beschaffung, Schulung

und Wartung separater Systeme zum Sichern und Verwalten drahtloser Netzwerke eingespart.

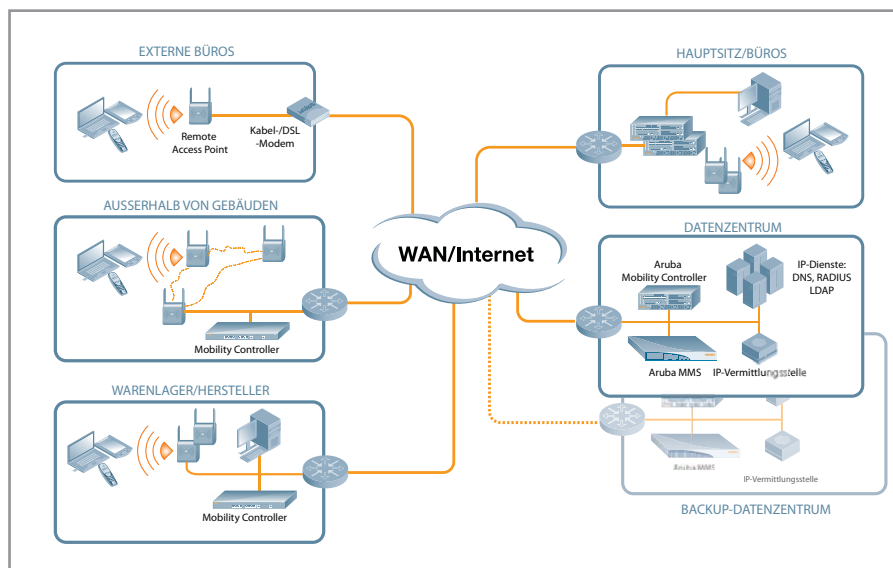
Zentralisierte Verwaltung und einfache Bereitstellung sind unverzichtbar, da in vielen Fällen vor Ort keine IT-Administratoren verfügbar sind. Die zentralisierte Architektur von Aruba reduziert die Kosten für IT-Support sowie Ausfallzeiten mit einer Vielzahl von Werkzeugen für die Fehlerbehebung von einem zentralen Ort aus. Zu den Funktionen gehören die Analyse der WLAN-Umgebung an den einzelnen Remotestandorten, gerätebezogene Fehlererkennung und Remote Packet Capture für die gezielte Fehlersuche. Aruba-Technologie reduziert weitere Kosten auch dadurch, dass WLANs an Remotestandorten ohne Eingriffe von Administratoren eingerichtet werden können. Controller und Access Points an Remotestandorten finden automatisch den Master Controller im Datenzentrum und laden selbsttätig die passenden Konfigurationsdaten

Die Netzwerklösung von Aruba für die verarbeitende Industrie

Zur Lösung von Aruba gehören drei Hauptkomponenten: Thin Access Points (Thin APs), zentrale Mobility Controller und Sicherheitsmodule für Mobility Controller. Als optionale Komponente kann ein Mobility Management System (MMS) 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 zum Schutz der Unternehmenswerte und sensibler Daten.

Im Folgenden werden wichtige Elemente zentral administrierter drahtloser Netzwerke



herunter.

für Produktionsanlagen, Lager, Freigelände und Büros beschrieben:

Datenzentrum: Je nach Anzahl der zu verwaltenden Standorte und Access Points werden ein oder mehrere Master Mobility Controller im Datenzentrum installiert. Diese Controller können auch Gegenstellen für Access Points sein, mit denen drahtloser Netzwerkzugriff in externen oder kurzfristig eingerichteten Büros bereitgestellt wird. Jeder Master Controller kann bis zu 500 Remote Controller verwalten und fungiert als gemeinsame Schnittstelle für Konfiguration und Management. Master Controller können auch 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 gemeinsame Verwaltungsplattform wird in diesem Fall MMS eingesetzt.

In Lagern und Produktionsanlagen:

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 2048 Access Points. Die lokalen Controller erhalten ihre Konfigurationsdaten vom Master Controller. Application Continuity und Sicherheitsrichtlinien werden benutzerorientiert von den lokalen Controllern verwaltet. 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.

Außerhalb von Gebäuden: Für den Außeneinsatz unter widrigen Umgebungsbedingungen sind auch robust konstruierte Access Point-Modelle verfügbar. Wenn in Außenbereichen keine Ethernet- oder Glasfaserkabel verfügbar sind, können mit beliebigen Access Points von Aruba vermaschte Netzwerke aufgebaut werden, die Datenverkehr über Access Points weiterleiten, die an das Hauptnetzwerk angeschlossen sind und für die der Betrieb in vermaschten Netzwerken zugelassen wurde. Die Access Points in den vermaschten Netzwerken verhalten sich wie normale Thin APs, wobei die Verbindung zum Controller über die Access Points realisiert wird, die als Mesh Hop eingebunden sind.

Externe und kurzfristig eingerichtete

Büros: Remote AP ist ein softwaregesteuerter Betriebsmodus, mit dem Aruba Access Points LAN-Anbindung an Remotestandorten bereitstellen. Remote APs können direkt an öffentliche/private Internetzugänge oder an LANs angeschlossen werden. Sie finden automatisch den Master Controller und bauen einen sicheren VPN-Tunnel zum Datenzentrum auf, so dass auch externe Benutzer und Gruppen sicher mit drahtloser Anbindung versorgt werden können. Datenverkehr kann je nach Anwendung über das Datenzentrum oder lokal geroutet werden. Bei Einsatzszenarien, in denen mehrere Access Points am Remotestandort benötigt werden, können zusätzliche Access Points mit eigener Stromversorgung eingesetzt werden. Diese können ein vermaschtes Netzwerk aufbauen und Datenverkehr über den Access Point weiterleiten, der mit dem Hauptnetzwerk verbunden ist.



WWW.ARUBANETWORKS.COM

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