



Benutzerorientierte Netzwerke von Aruba für Hochschulen

Wie gestalten Sie die Zukunft? Sie möchten Technologie zum zentralen Element des Lebens und Lernens auf dem Hochschulgelände machen? Sie möchten alle Kommunikationsanwendungen über ein einziges flexibles Netzwerk unterstützen? Sie wünschen sich ein Netzwerk, auf das alle Studierenden, Lehrkräfte und Verwaltungsmitarbeiter mühelos und sicher zugreifen können – unabhängig davon, wo sie sich gerade aufhalten und welche Geräte sie benutzen?

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 Hochschuleinrichtungen. Die Architektur zeichnet sich dadurch aus, dass sie die hohen Übertragungsraten drahtgebundener Netzwerke mit der Flexibilität von Drahtlosnetzwerken verknüpft, bei zentraler Verwaltung, uneingeschränkter Sicherheit und niedrigen Gesamtbetriebskosten.

Einzigartige Aruba-Funktionen

Aruba ist branchenführend bei Innovationen für mobilen Datenzugriff in Campus-Szenarien. Die angebotene Architektur kann in bereits bestehende Netzwerkinfrastrukturen integriert werden.

ADAPTIVER 802.11N-BETRIEB

Mit den leistungsstarken 802.11n-Produkten von Aruba wird der vollständig drahtlos vernetzte Campus zur praktisch realisierbaren Option. Aruba bietet eine adaptive Lösung, die mit vertretbarem Aufwand in bestehende Infrastrukturen integriert und an das ständig steigende Datenverkehrsaufkommen angepasst werden kann. Mit 3x3-MIMO-Betrieb (Multiple-In/Multiple-Out), skalierbarem Aufbau und vollem Funktionsumfang auch bei Nutzung von 802.3af-PoE (Power over Ethernet) eignen sich 802.11n-Access Points von Aruba für Anwendungen wie drahtlosen Netzwerkzugang, Intrusion Detection Monitoring, Datenverkehrsanalyse, sichere vermaschte Drahtlosnetzwerke und Remote Access Points. Da die Geräte ihre Betriebssoftware über das Netzwerk laden können, sind Umwidmungen und Updates ohne zeit- und kostensintensive Vor-Ort-Wartung möglich.

ZUKUNFTSSICHERES DESIGN

Die Architektur von Aruba ist als Basis für zukünftige netzwerkorientierte

Anwendungen geeignet. Die Schaltkreise der Geräte sind programmierbar und bieten großzügige Leistungsreserven, so dass Upgrades per Software und ohne größere Betriebsunterbrechungen möglich sind. Viele Hochschuleinrichtungen beginnen mit einfachen Drahtlosfunktionen und erweitern diese schrittweise um weitere Merkmale: Wireless Intrusion Protection, Voice over Wi-Fi für Wartungs- und Rettungsdienste, Ausfallsicherung für Glasfaserverbindungen durch vermaschte Drahtlosnetzwerke und Standortverfolgung für Geräte, die an Studenten verliehen wurden. Um derartige Erweiterungen zu aktivieren, sind beim Einsatz von Aruba-Geräten keine Netzwerkumbauten erforderlich. Einfache Softwareupdates sind ausreichend. Auch neue Standards, zum Beispiel veränderte Verschlüsselungs- und Authentifizierungsverfahren, können durch einfache Softwareupdates und ohne störende Unterbrechungen des Netzwerkbetriebs implementiert werden.

IDENTITÄTSORIENTIERTE SICHERHEITSFUNKTIONEN

Wenn sich Studierende, Lehrkräfte und Verwaltungsmitarbeiter auf dem Hochschulgelände bewegen, besteht die Herausforderung darin, ihnen einen unterbrechungsfreien Netzwerkzugang zu gewähren, aber

Vorteile der Aruba-Lösung:

- **Adaptiver 802.11n-Betrieb:** Automatische Netzwerkanpassung zur bedarfsorientierten 802.11n-Bereitstellung
- **Zukunftssicher:** Anpassung an neue Anwendungen durch Softwareupdates
- **Identitätsorientierte Sicherheitsfunktionen:** Sicherheitsmaßnahmen „folgen“ Benutzern, unabhängig von deren Aufenthaltsort auf dem Campus oder auf dem Globus
- **Anwendungssensitiv:** Optimiert für Konvergenz von Daten-, Sprach- und Videoanwendungen in Drahtlosnetzwerken
- **Zentrale Verwaltung:** Einfache und zentralisierte Konfiguration, Überwachung und Fehlerbehebung

gleichzeitig sicherzustellen, dass sie nur auf personenbezogen freigegebene Ressourcen zugreifen können. Herkömmliche Verfahren zur Zugriffssteuerung, die sich an Zugangspunkten orientieren, werden bei mobiler und drahtloser Nutzung obsolet. Kriterien für die Zugriffssteuerung bei mobiler Nutzung sind Benutzeridentität, Rolle, Gerätetyp, Standort, Uhrzeit und weitere relevante Benutzer- und Gerätemerkmale. Mobilität sollte nahtlos in bestehende AAA-Infrastrukturen wie RADIUS, LDAP und Active Directory integriert werden können. Diese Integration gehört zu den entscheidenden Vorteilen der Netzwerkarchitektur von Aruba. Während sich Richtlinien bei anderen Lösungen an SSIDs/VLANs orientieren, um Netzwerke zu sichern und zu segmentieren, setzt Aruba eine Stateful Firewall ein, die Sicherheitsrichtlinien auf Rollen und Benutzer bezieht. Benutzerorientierung bedeutet, dass Sicherheitsrichtlinien unabhängig vom Aufenthaltsort der Benutzer gelten.

APPLICATION CONTINUITY

Hochschulen können ihre Investitionen in Wi-Fi-Technik für zusätzliche Anwendungen auf dem Campus nutzbar machen, zum Beispiel für mobile Sprachdienste, Videoübertragung, Überwachungssysteme und Gebäudesicherung. Die Konzentration auf ein einziges sicheres System kann zu deutlichen Kosteneinsparungen führen. Das System von Aruba ist für Konvergenzfunktionen optimiert, anwendungssensitiv und ermöglicht

den Einsatz spezieller Sicherheits- und Steuerungsfunktionen für spezifische Anwendungstypen, Geräte und Benutzer. Dadurch können Hochschulen die Vorteile von IP-Konvergenz nutzen und isolierte, schwer zu verwaltende Systeme in eine gemeinsame Infrastruktur einbinden.

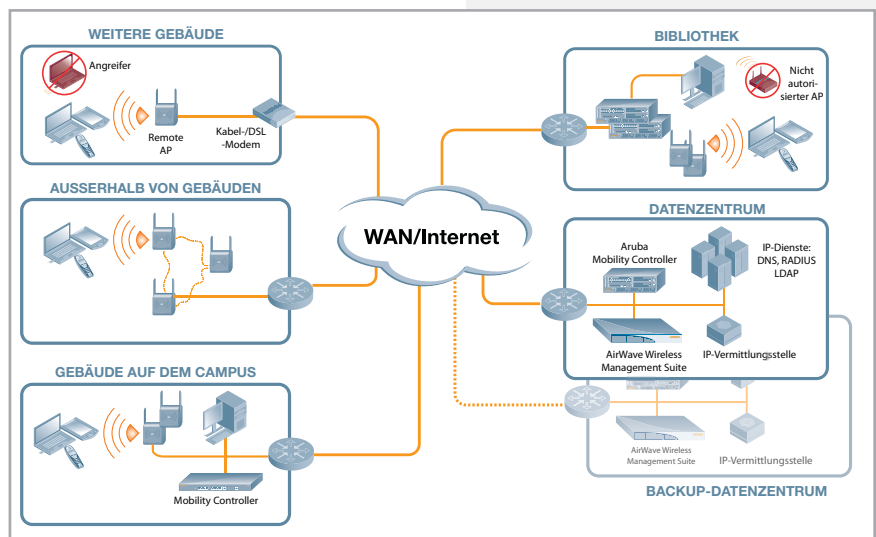
ZENTRALE VERWALTUNG UND STEUERUNG

Die zentralisierte Netzwerkarchitektur von Aruba bietet zentrale Überwachung, Steuerung und Fehlerbehebung, unabhängig davon, ob sich Netzwerke über einen Campus erstrecken oder über Kontinente. Wenn mehrere Institutionen kooperieren, kann es erforderlich sein, die Kompetenzen der IT-Administratoren der beteiligten Einrichtungen abzugrenzen. Für diesen Zweck bietet Aruba eine „Manager of Managers“-Funktion, die den Datenzugriff der zuständigen Administratoren nach einem hierarchischen Schema logisch separiert. Innerhalb der Netzwerkinfrastruktur von Aruba ist Remote Packet Capture möglich, so dass IT-Administratoren Probleme von einem zentralen Standort aus analysieren und beheben können. Darüber hinaus bietet das System Echtzeitanalysen der Funkumgebung aller Gebäude, die an das Campusnetzwerk angeschlossen sind. Alle Wartungs- und Upgradaufgaben können von zentraler Stelle aus bearbeitet werden, Warnungen bei nicht autorisierten Zugriffen und sonstigen sicherheitsrelevanten Ereignissen werden ohne Zeitverzögerung an die zentrale Verwaltung weitergeleitet.

Die Netzwerklösung von Aruba für Hochschulen

Zur Lösung von Aruba gehören drei Hauptkomponenten: Thin Access Points (Thin APs), zentrale Mobility Controller und Softwaremodule für Mobility Controller. Als optionale Komponente kann die AirWave Wireless Management Suite von Aruba eingesetzt werden. Die Access Points ermöglichen sicheres drahtloses Anbinden von Endgeräten an bestehende LAN-/WAN-Systeme und leiten den gesamten drahtlosen Datenverkehr über GRE- bzw. IPsec-Tunnel je nach Datenverkehrsart zu einem Mobility Controller im Datenzentrum oder in einem nahegelegenen Gebäude. Der Mobility Controller ist die zentrale Schaltstelle für Konfiguration, Verwaltung, Application Continuity Services und Sicherheit. Dank des modularen Softwarekonzepts der Mobility Controller kann der Funktionsumfang auf das notwendige Maß beschränkt und bei Bedarf später erweitert werden.

Im Folgenden werden wichtige Merkmale für drahtlose Netzwerke in Hochschulen mit zentralisierter IT-Administration 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 im Gebäude des Datenzentrums bereitgestellt wird, sowie für Remote Access Points, die in kleinen Außenstellen und in Heimbüros betrieben werden. 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 Schnittstelle für Verwaltung und Konfiguration kann in diesem Fall MMS eingesetzt werden.

Gebäude auf dem Campus: 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 6 bis 2048 Access Points. Die lokalen Controller erhalten ihre Konfigurationsdaten vom Master Controller. Application Continuity und PCI-Sicherheitsstufen werden benutzerbezogen von den lokalen Controllern verwaltet. Die lokalen Controller bieten außerdem Wireless Intrusion Protection und 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.

Außerhalb von Gebäuden: Die meisten Access Points von Aruba können in geschützten Außenbereichen genutzt werden, also zum Beispiel für

Anwendungen wie Einzelhandel in Stadien, Überwachungskameras, Notrufsäulen oder schlicht zum Bereitstellen von Netzwerkzugriff für Studenten außerhalb von Gebäuden. Für den Außeneinsatz unter widrigen Umgebungsbedingungen sind auch robust konstruierte Access Point-Modelle verfügbar. Wenn in Außenbereichen keine Ethernet- oder Glasfaserkabel verlegt 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.

Remotebenutzer und kurzfristig eingerichtete Standorte: Mit Remote Access Points können Bereiche, in denen nur wenige 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 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, die ein vermaschtes Netzwerk aufbauen und Datenverkehr über den Access Point mit direkter Verbindung zum Controller weiterleiten. Auf diese Weise können innerhalb kürzester Zeit drahtlos vernetzte Büros in Betrieb genommen werden, ohne dass LAN-Kabel verlegt und ohne dass IT-Administratoren vor Ort aktiv werden müssen.



WWW.ARUBANETWORKS.COM

1344 Crossman Avenue, Sunnyvale, CA 94089, USA | Tel.: +1 408.227.4500 | Fax: +1 408.227.4550