

Lösungsleitfaden |

Enterprise



## **Virtuelle Standortvernetzung**

**ARUBA**<sup>®</sup>  
networks

## Einführung

Niederlassungen, Satelliten Kliniken, Telearbeiter, Zeitarbeiter und Außendienstmitarbeiter benötigen alle einen Netzwerkzugriff auf die geschäftskritischen Daten der Unternehmenszentrale. Herkömmliche Remote Netzwerklösungen setzen auf den Einsatz von VPN Clients (Virtual Privat Network Clients) oder replizieren Routing, Switching, Firewalls und andere Services auf jeden einzelnen Standort. Client VPN Lösungen beziehen sich meist nur auf einzelne Geräte, erfordern eine Revisionskontrolle und ein Management für kompatible Treiber. Zudem werden nicht alle Plattformen unterstützt. Weiterhin erhalten die Remote Nutzer oft nicht die gleiche Performance wie die Kollegen im lokalen Netzwerk, müssen zudem geschult werden und erhöhen den Supportaufwand durch vermehrte Help Desk Anrufe. In den Fällen, in denen die IT-Administration die Netzwerkinfrastruktur auf jeden einzelnen Standort abbilden muss, erhöhen sich die Kosten um ein Vielfaches und die Wartung der Anlage wird zunehmend komplizierter. Die Remote Nutzer müssen zudem oft Abstriche bei den Netzwerkservices wie z.B. dem Drucken, den Sprachdiensten oder bei der generellen Zusammenarbeit, machen. Das zentralisierte Port-Management einiger Hersteller weist oft Lücken in der Sichtbarkeit und den Kontrollmechanismen auf.

Aruba`s virtuelle Standortvernetzung dagegen senkt die Komplexität und die Kosten bei der Einrichtung eines Remote-Netzwerkes, bei einem bis zu hunderten von Nutzern. Die Hochleistungscontroller von Aruba übernehmen in der Datenzentrale die komplexen Konfigurationen, das Management des Netzwerkes, die automatischen Software Updates, das Intrusion Detection und die Umsetzung der einzelnen Aufgaben in den Standorten. Die Services werden durch die Controller in der Datenzentrale virtualisiert und dann im Push Verfahren an die kosteneffektiven, benutzerdefinierten Remote Access Points (RAP`s) und Niederlassungscontroller (BOC`s) verteilt. Die RAP`s und BOC`s bieten eine sichere Verbindung und liefern die zentralisierten Services direkt an den Benutzer weiter. Durch das Layer 3 Tunneling Verfahren zwischen den Controllern und den RAP`s und BOC`s wird sichergestellt, daß alle WAN Netzwerkbereiche - einschließlich dem 3G Mobilfunknetz – ausgenutzt werden können.

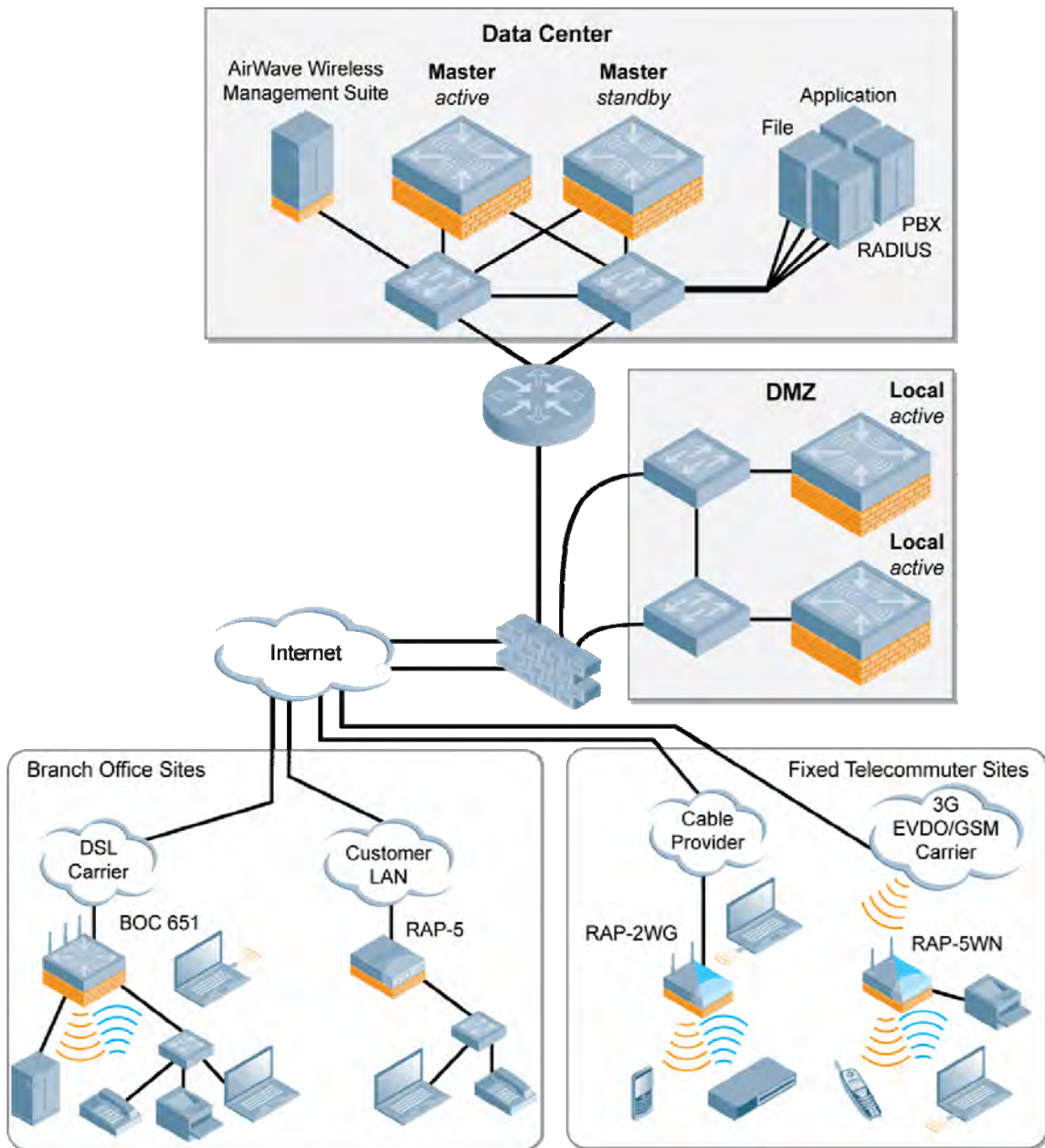
Die VBN Lösung unterscheidet sich zu den traditionellen Lösungen bei der Fokussierung auf die Policing der Routes, der Subnetze und VLAN`s, statt auf die Portverwaltung. Aruba`s verteilte Policy Enforcement Firewall bietet dafür den zentralen Weg die Policies zu managen und zu kontrollieren. Firewall Agents sorgen dabei für die Durchsetzung der Richtlinien bei den Remote Geräten. Die Firewall liefert Policy-basierte Kontrolle, hohe Sicherheit, unterstützt unterschiedliche benutzerdefinierte Services und steht immer unter der Kontrolle des IT Personals. Die Lösung ist widerstandsfähig, einfach zu konfigurieren, erfordert keine Benutzereinweisung und wird als Plug & Play installiert. Das Ergebnis ist ein konformes und sicheres Arbeiten für den Nutzer, unabhängig von wo aus er auf das Netzwerk zugreift.

Im Gegensatz zu den VPN Client Lösungen, wird hier keine spezielle Software für den Zugriff benötigt. Die Benutzer müssen für die Zugriffsprozedur nicht geschult werden, es muss keine Software bereitgestellt werden und keine Token Cards verwendet werden. Die Daten werden wie bei VPN verschlüsselt und authentifiziert, mit dem Unterschied, daß der Nutzer für den Aufbau der Verbindung nicht eingreifen muss. Alle Sicherheitsrichtlinien werden gleichermaßen durchgesetzt, unabhängig von wo aus auf das Netzwerk zugegriffen wird. Somit merkt der Nutzer keinen Performanceunterschied zwischen drahtgebundenem und drahtlosen Netzwerkverbindungen.

Die VBN Lösung wird über die Aruba AirWave Management Platform (AMP) verwaltet, die entsprechende Schnittstellen für den Help Desk, der Netzwerktechnik, den Security und Audit Gruppen, der Unternehmensleitung und den Benutzern, bereitstellt. Im Gegensatz zu herkömmlichen Netzwerkmanagement Lösungen, die sich auf die Problembhebung der Ports, VLAN's und IP Adressen konzentrieren, bietet die AMP eine Sichtbarkeit bis zu den Endnutzern und Geräten.

Die Hauptmerkmale der VBN Lösung setzen bei den Schwachstellen herkömmlicher Remote Netzwerklösungen an:

- Durch das zero-touch IT-Bereitstellungsmodell muss keine zusätzliche Software oder weitere Zugriffslegitimationen zwischen den entfernten Standorten und der Unternehmenszentrale bereitgestellt werden. Benutzer ohne technisches Verständnis können sowohl drahtgebundene als auch drahtlose RAP Büros ohne Hilfe aufsetzen. Die Anwendungen und Geräte arbeiten im out-of-the-box Verfahren ohne zusätzliche Konfiguration;
- Mit einem Klick die Datenerzeugung testen, mit einem Klick die Werkseinstellung wiederherstellen, eine intuitive einfache Benutzerschnittstelle zur Erkennung und Beseitigung von Geschwindigkeitsproblemen;
- Die Referenzen werden alle automatisch vom System zugewiesen – ein entsprechendes IT-Referenzmanagement entfällt dadurch;
- Policy-basiertes Forwarding stellt sicher, daß IP-basierte Geräte (VoIP Telefone, Drucker) und Services von der Ferne aus genauso gut arbeiten wie im lokalen Netzwerk. Eine Trennung der Sprachnetze von der Security-Infrastruktur ist dadurch nicht nötig;
- Es können alle WAN Verkehrswege genutzt werden, an Stelle von teuren privaten Netzen;
- Alle Management- und Kontrollfunktionen befinden sich zentralisiert auf den Aruba Controllern. Diese nutzerfixierte Management Architektur bietet eine Sichtbarkeit von alle Benutzern und Geräten und eine schnelle Reaktion bei einem Gerätausfall. Eine weitere Management Infrastruktur entfällt;
- Durch die zentralisierten Policies- und der User-Zugriffskontrolle ist eine 2. Firewall zur Absicherung des Remote Netzwerkes unnötig.



Die

Aruba Lösung für virtuelle Standortvernetzung

## Spezialgefertigte RAP`s und BOC`s

Aruba verfügt über drei speziell angefertigte RAP und BOC Familien. Alle diese Geräte verfügen über Policy-basiertes lokales und remote Packet Forwarding, sowie über die Adaptive Radio Management (ARM) Technologie zur Optimierung des WiFi-Betriebs. Ein Diagnosetool zeigt den Gerätestatus über ein einfaches User Interface an und unterstützt den ein-Klick Debugging Mode und den ein-Klick Reset zur Werkseinstellung.

Weitere Hauptmerkmale der neuen Produktlinie beinhalten:

- RAP-2 Familie: nicht größer als ein Paket Spielkarten. Ausgelegt für 1–5 Benutzer, ideal für Telearbeiter, Mini-Standorte und SOHO Anwendungen. 802.11 b/g WiFi Frequenz und 2 Ethernet Ports für den Einsatz von drahtgebundenen Geräten, z.B. VoIP Telefone;
- RAP-5 Familie: die in Buchformat erhältliche RAP-5 beinhaltet 5 high-speed Ethernet Ports, einen USB Port für ein Breitband 3G Mobilfunkmodem, Hardware beschleunigte Verschlüsselung und optional einen 802.11n WiFi Frequenzbereich mit integrierten Antennen. Die RAP-5 Familie ist für kleinere Niederlassungen bis zu 50 Benutzer ausgelegt;
- 600 BOC Familie: als „branch-in-a-box“ entwickelte Lösung für Büros mit bis zu 256 Benutzern einsetzbar. Die 600-er Familie bietet: eine großen Bereich an WAN Verbindungsmöglichkeiten, Netzwerkspeicherplatz, integrierten Print Server, Gigabit Ethernet, Power over Ethernet Plus (PoE+), ExpressCard Einschub und USB Optionen. Ein optionaler 802.11n WiFi Frequenzbereich ergänzt das Angebot für ein echtes vollständige Wireless Büro.



*Die Aruba Produkte für virtuelle Standortvernetzung*

RAP`s wurden für kleine Büros, Telearbeitsplätze und SOHO Anwendungen entwickelt. Die sichere ein-Klick Bedienung erlaubt es den Nutzern ohne jegliche Administrationshilfen auszukommen und dadurch die Aufwandskosten für Help Desk und Support zu senken.

Ein-Klick Diagnose Tools und ein-Klick Werkswiederherstellung, minimieren den Aufwand für eventuelle Diagnose und Wartungsarbeiten an den RAP`s.

Die RAP`s beinhalten die Aruba`s Adaptive Radio Management (ARM) Technologie, die zur Optimierung der Wireless Netzwerkperformance eingesetzt wird und somit kein Eingreifen der IT-Administration notwendig ist. Viele der RAP`s unterstützen 3G Mobilfunknetz, das einerseits als Backup WAN Verbindung genutzt, oder für die automatische Verteilung der Software Upgrades und Konfigurationsänderungen an alle RAP`s genutzt werden kann. RAP`s die zu diesem Zeitpunkt offline sind, werden beim nächsten Reconnect upgedatet.

Die Aruba BOC`s wurden für den Einsatz in kleinen bis mittelgroßen Büros mit bis zu 256 Benutzern entwickelt. Es werden drahtgebundenen und drahtlose Verbindungen über high-speed LAN Ports angeboten, sowie Aruba Wireless Access Points und ein optional integrierter 3x3 MIMO 802.11a/b/g/n Access Point. In Büros in denen WiFi genutzt wird, kann der BOC die anderen Aruba Access Points mit integrierte ARM Technologie für beste Wireless Performance, mit verwalten.

BOC`s sind auch in der Lage USB Drucker und Netzwerkspeicherplatz zu hosten. 3G Mobilfunknetze können via USB oder ExpressCard Slots, als Backup WAN Verbindungen genutzt werden. BOC`s beinhaltet einen integrierten Authentifizierungsserver für unabhängige Einstellungen bei kleinen Standorten. Damit können wiederum wichtige Ressourcen in der Datenzentrale eingespart werden.

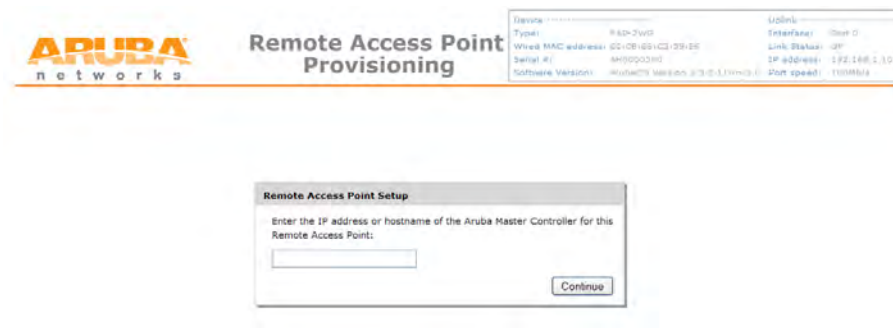
Sichere Gastzugänge können über das Aruba GuestConnect Feature ohne Administrationshilfe selbst eingestellt werden, um z.B. temporäre Nutzeraccounts anzulegen. RAP`s und BOC`s können entweder zentral vom Aruba Controller, oder über die AirWave Management Plattform, verwaltet werden.

## Selbständige IT-Bereitstellung

RAP's können ohne vorherige Gerätekonfiguration durch das IT-Personal bereitgestellt werden. Der Administrator muss lediglich eine Liste der autorisierten RAP's auf dem Controller erstellen.

Sobald sich ein RAP mit dem richtigen digitalen Zertifikat (entsprechend der Liste) am Netz anmeldet, wird er automatisch als Teil des Unternehmensnetzwerkes eingebunden. Der Benutzer muss dann nur noch die URL des Controllers in den RAP Web Browser eingeben. Der Rest erfolgt automatisch. Konfigurations- und Software Updates werden automatisch in Echtzeit bei jeder Veränderung geladen.

Anweisungen für den Benutzer werden automatisch durch den Controller generiert und können als PDF gespeichert werden. Die Anweisungen begleiten den User durch den Bereitstellungsprozess und können per E-Mail oder Ausdruck an weitere User verteilt werden.



*Der RAP Self-Provisioning Bildschirm*

Die selbständige IT-Bereitstellung ist auf folgenden RAP Model verfügbar: RAP-2WG, RAP-5WN, und RAP-5. Die Modelle werden von den Aruba Controllern 3200, 3400, 3600, und 6000 M3 Serien unterstützt

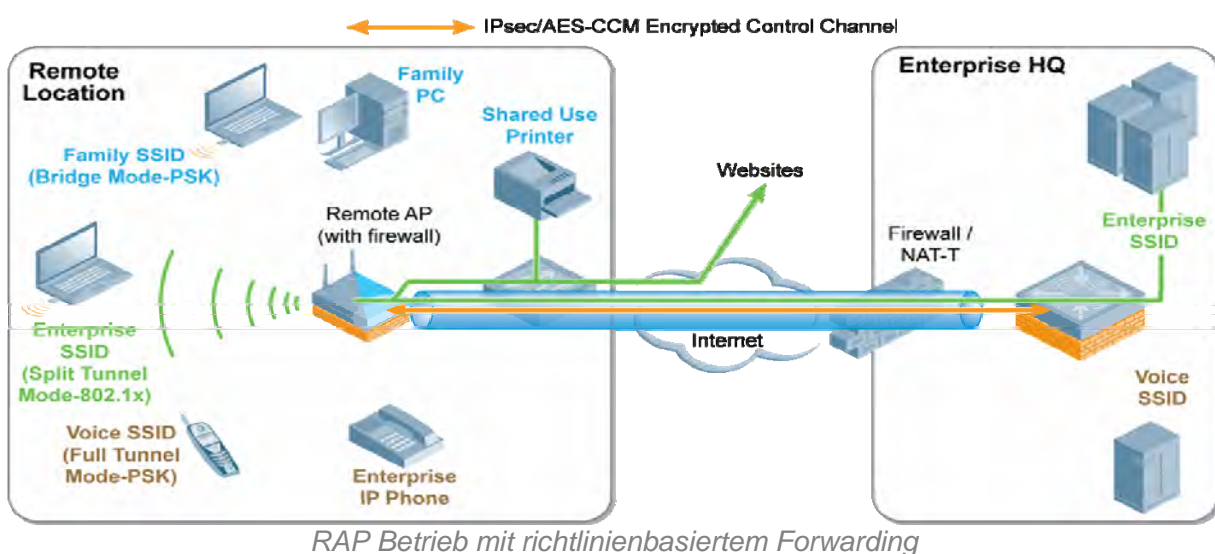
## Richtlinienbasierte Vernetzung

Die Aruba VBN Lösungen setzen auf richtlinienbasierte Konfigurationen anstatt auf Port-basierter Sicherheit wie bei herkömmlichen Lösungen. Die Sicherheitsrichtlinien werden durch die IT-Administration mit Hilfe der Aruba Controller durchgeführt und dann automatisch via Push-Technologie, nahezu in Echtzeit, bei jeder Veränderung an die Geräte bei den verteilten Standorten übertragen.

In den Policies werden u.a. folgende Kriterien definiert: User-Rollen, Port Verhalten, SSID`s, Traffic Forwarding, Authentifizierung und Verschlüsselung. Die User-Rollen werden durch die Firewall Policies nach Traffic Typen und den erlaubten Ressourcenzugriffen für jeden einzelnen User definiert. Dadurch können sich unterschiedliche User auf die gleichen RAP und BOC`s, mit der gleichen Authentifizierungsmethode einwählen und erhalten dabei verschiedene Zugriffsrechte, basierend auf die vorher definierten User-Rollen.

Die LAN Ports können sowohl für allgemeine freie Zugriffe oder für authentifizierte Zugriffskontrolle (NAC) mit unterschiedlichen Authentifizierungstypen konfiguriert werden. Um Mitarbeiter- und Gastzugriffe auf den gleichen LAN Port legen zu können, kann sowohl eine 802.1X Authentifizierung als auch Captive Portal gleichzeitig verwendet werden. Authentifizierten Usern wird dabei der entsprechende Mitarbeiterzugriff gewährt, wogegen Gastuser und nicht 802.1X Geräte auf ein webbasierte Portal geleitet werden, auf dem man die entsprechenden Login-Daten angeben muss, um einen Zugriff zu erhalten. Obwohl sich Mitarbeiter, Gäste und nicht gemanagte Geräte den gleichen Port teilen, verfügen alle über einen unterschiedlichen Zugriffslevel. Dadurch entstehen keine Sicherheitslücken bei uneingeschränkten LAN Ports und der User muss nicht angewiesen werden bestimmte Ports zu nutzen.

Durch die Verwendung von virtuellen AP`s, unterstützen die RAP`s und BOC`s gleichzeitig mehrere Wireless SSID`s auf dem selben Frequenzbereich, wobei Authentifizierung und Verschlüsselung, benutzerdefiniert auf jeder SSID zur Verfügung steht. Beispiel: Autorisierte User erhalten einen vollen WPA2 verschlüsselten Unternehmenslink, Gäste authentifizieren sich über ein offenes WLAN via Captive Portal und VoIP Telefone eine pre-shared key Authentifizierung über eine dritte WLAN Verbindung. Alle drei nutzen dabei aber den gleichen AP Frequenzbereich.



## Universelle Verbindung an allen Standorten

Aruba's VBN Lösung erlaubt eine gemeinsame Konfiguration der Ports und/oder SSID's, die über alle RAP's und BOC's gleichzeitig verbreitet werden, so daß ein neues Firmen LAN oder WAN effektiv auf alle Standorte erweitert werden kann. Auf Grund dieser Eigenschaft können sich Laptops, WiFi Telefone, PDA's und andere Clients, bei Erkennung des Netzwerkes, sofort mit den standardisierten Sicherheitsprotokollen, unabhängig von ihrem Standort, in das Unternehmensnetz einwählen.

Alle Services mit den entsprechenden Zugriffsrestriktion, kontrolliert von den IT-Policies, durchgesetzt von der Aruba Firewall, stehen allen Standorten zur Verfügung. Mobile User genießen von jedem beliebigen Standort aus die gleichen Zugriffsprozeduren und Netzwerkservices, während sich der IT-Manager keine Gedanken mehr darüber machen muss, welcher Service für welchen User bei welcher Standortart, bereitgestellt werden soll. Dabei sind keine Client Software oder Token Cards für den Zugriff notwendig. Die Arbeitsabläufe müssen nicht verändert werden und die Sicherheit bleibt komplett transparent.

Ein weiterer Punkt zur Vereinfachung der Vernetzung: die RAP's können die IP-Adressierung des Unternehmensnetzwerkes so erweitern, daß die verteilten Stationen im selben IP-Adressbereich wie das Firmennetz arbeiten. Dies reduziert oder eliminiert das WAN-Routing, da der Controller in der Datenzentrale den gleichen IP-Adressbereich nutzt.

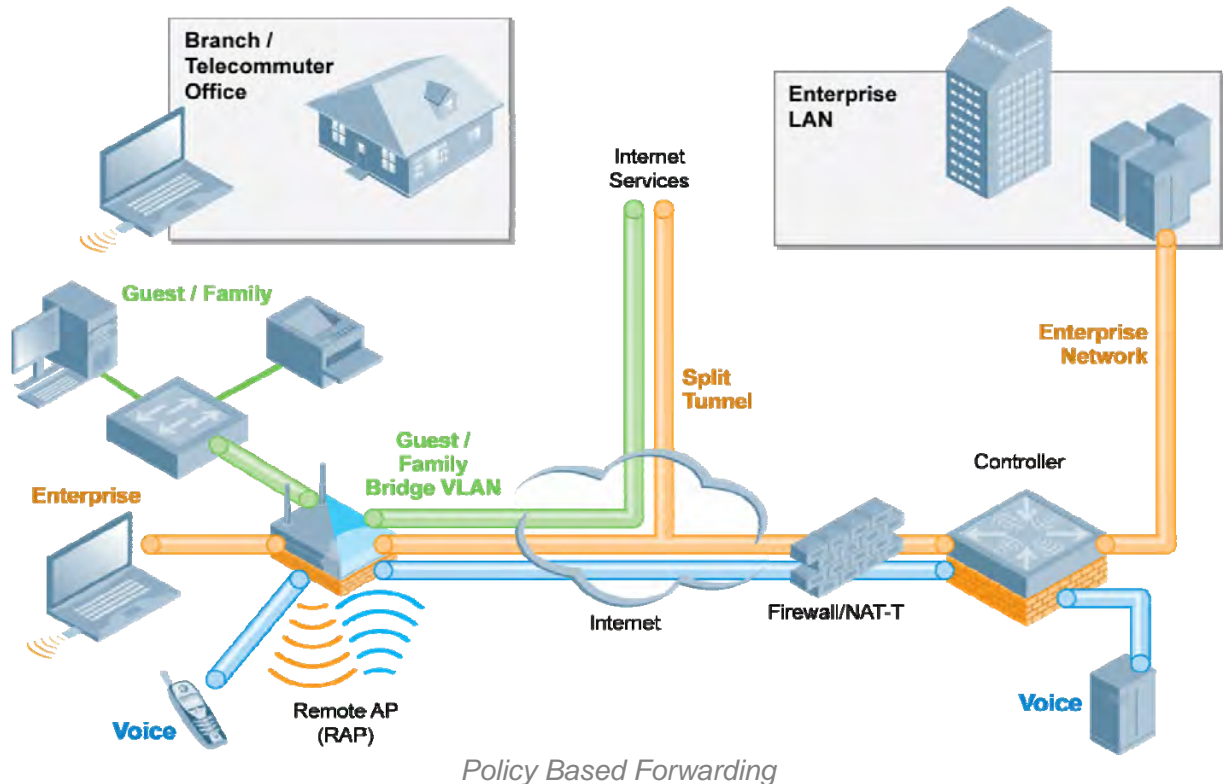
## Verringerung des WAN Traffic Backhaul durch Policy Based Forwarding

Eine Optimierung des WAN Traffics, durch Kapazitätsreduzierung und preiswerteren WAN Verbindungen, führt zu einer besseren Bandbreitennutzung und kann die Betriebskosten senken. Viele traditionelle Lösungen leiten den gesamten Netzwerkverkehr zur Analyse über das WAN in die Datenzentrale. Dadurch muss der Internetverkehr und lokale Druckerservices im Daten Center umgeleitet werden, so daß es zu Zeit- und Bandbreitenproblemen kommen kann.

Aruba's VBN Lösung gibt das Traffic Forwarding in die Kontrolle der IT-Zentrale, in der die dedizierte Hardware mit den entsprechenden definierten Policies läuft. Die Policy Enforcement Firewall (PEF) trifft hierbei die Entscheidungen nach Kriterien wie der IP Adresse, dem Traffic Typ und den dazugehörigen User-Rollen basierten Policies. Dabei kann der Verkehr zwischen den Standorten über einen sicheren Tunnel zur Datenzentrale gelegt werden, während der lokale und Internet Verkehr, über Policy Definitionen lokal gebrückt wird. Das Drucken kann auf lokale Subnetze eingeschränkt werden. Im Gegensatz zu VPN Client „split tunnel“ Konfigurationen, die durch malicious Software manipuliert und zwischen öffentlichen und privaten Schnittstellen weitergeleitet werden kann, garantiert die PEF eine permanente Durchsetzung der Policy Entscheidungen.

Da Router nur den Verkehr zur Ziel IP-Adresse untersuchen erfordert jede Veränderung der Weiterleitung und des Port Verhaltens, eine erneute Konfiguration der komplexen Zugriffskontrolllisten (ACL's). Die PEF dagegen arbeitet nach vorgegebenen Benutzer- bzw. Geräte definierten Sicherheitsregeln für das Traffic Forwarding, so daß die Ports oder VLAN nicht verändert werden müssen. Eine VBN Lösung ist daher wesentlich einfacher zu konfigurieren und zu verändern als eine Router basierende Lösung. Die User basierte Policing entlastet dadurch die IT Administration nicht nur bei der Einrichtung sondern vor allem auch bei allen Änderungen des Netzwerkes.

Der polierte Zugriff auf das lokale Netzwerk oder dem Internet, stört den User in seinen Arbeitsabläufen nicht. Bei traditionellen VPN Client Software Lösungen dagegen, muss der User zunächst die bestehende Verbindung unterbrechen, auf lokale Ressourcen zurückgreifen und dann wieder den Netzwerk Service aufgreifen. Eine massive Störung, die sich daraufhin in vielen unnötigen Help Desk Anrufen widerspiegelt.



## Unterbrechungsfreie Anbindung der Standorte

Aruba unterstützt 2 Arten, um die Niederlassungen während einer WAN Verbindungsunterbrechung oder einer Service-Unterbrechung mit der Datenzentrale weiterarbeiten zu lassen: 3G Mobilfunknetz Backup und den sog. Mode für lokale „Überlebensfähigkeit“. Sollte ein drahtgebundener WAN Link zusammenbrechen, können vorher definierte RAP und BOC Modelle automatisch auf ein 3G Mobilfunkmodem als Backupverbindung umschalten. Das Mobilfunkmodem wird in die RAP und BOC's via USB oder ExpressCard Slots betrieben. Aruba stellt dafür eine umfassende Kompatibilitätsliste der Anbieter zur Verfügung.

Der sog. lokale „Überlebens-Mode“ hält die lokalen LAN und Wireless LAN Zugriffe während einer Serviceunterbrechung der Datenzentrale, aufrecht. Durch dieses Merkmal kann je nach WAN Status und IT-Policy, die Standort-Kommunikation und die Internetverbindung aufrecht erhalten werden.

Die Aruba Controller im Daten Center können zur Hochverfügbarkeit geclustert werden. Über DNS basierte Techniken kann auch die Datenzentrale zusätzlich redundant aufgebaut werden.

## **Vereinfachende und sichere drahtlose Standortvernetzung**

VBN fügt sich nahtlos in Aruba's drahtlose end-to-end Sicherheit und Verwaltbarkeit ein. Die Errichtung von drahtlosen Standorten wird durch die RAP und BOC Unterstützung des Wireless Intrusion Prevention Systems (WIPS) und der Adaptive Radio Management (ARM) Software, stark vereinfacht.

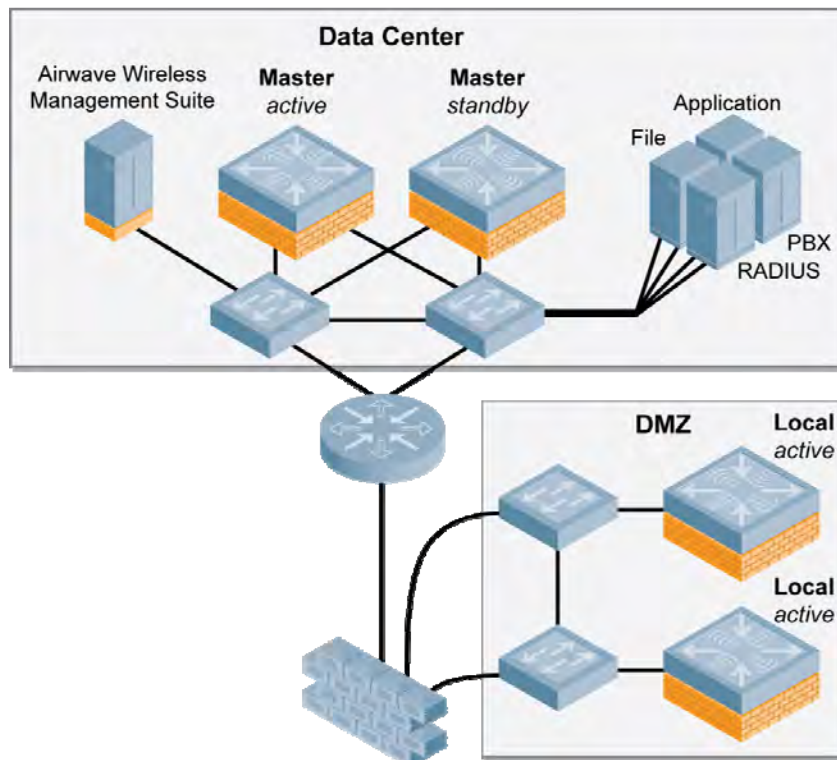
WIPS erkennt, meldet und entschärft drahtlose Bedrohungen auf Niederlassungen, bei defekten Access Points und falsch konfigurierten Client Geräten. Es schützt auch gegen falsche Übertragungen bei defekten Access Points, sowie gegen bekannte Angriffssignaturen. Falls ein Angriff oder eine Schwachstelle erkannt wird, alarmiert das System den Administrator und unterstützt die vorgeschlagenen Korrekturen. Dieses Merkmal ist besonders bei PCI (Payment Card Industry)-Unternehmen und anderen Compliance-konformen Firmen wichtig.

Aruba löst das Problem des Frequenzbereichmanagements durch seine Erfahrung in sehr großen Unternehmensinstallationen und durch die Zentralisierung des Controllings und des Managements. Mit dem Adaptive Radio Management (ARM) kann Aruba auch die Problematik der RF Channel und des Power Settings lösen.

## **Verringerung der Komplexität durch die Zentralisierung von Konfiguration, Management und Problemlösung**

VBN zentralisiert das Management von Remote-Netzwerken und erlaubt dem IT-Personal die gesamte Verwaltung und Problemlösung über eine einfache Plattform zu bewältigen. Zum Beispiel bei der Nachverfolgung der Verbindungen zu den Controllern im Daten Center, wenn ein RAP automatisch seine Konfigurationsdateien und Software Updates über einen sicheren Link herunter lädt. Diese Merkmal ersetzt das manuell Update von hunderten oder tausenden Standortgeräten. Die Konfigurationen und die Software sind auf den Controller in der Datenzentrale abgelegt und obliegen zu jeder Zeit der Kontrolle des IT-Managements.

Die Problemlösung und die Berichterstattung können über die AirWave Management Plattform (AMP) oder den Controllern abgebildet werden. Das AMP sorgt für die Sichtbarkeit der LAN Seite jedes Standortes und enthält alle Informationen über die Nutzer und die Geräte. AMP kann zu anderen IT Management Lösungen verlinken, unterstützt ein umfassendes Reporting und liefert spezielle Einsichten für den Help Desk, der Security/Audit Gruppe, sowie der Unternehmensführung.



*Datenzentrale mit der Airwave Management Plattform*

Sowohl das AMP als auch die Controller ermöglichen den Netzwerktechnikern auf den Status der Geräte und der Verbindungen, sowie den erforderlichen Policy Konfigurationen und Endgeräten, zuzugreifen. AMP liefert viele schnelle Troubleshooting- und Diagnose-Tools, die direkt zum Help Desk verlinken, um dort eine schnelle Lösung für das Problem zu finden.

AMP kann auch mehrere Konfigurationsdateien abspeichern um eine Synchronisation von weiteren WLAN's oder Niederlassungen mit identischen Policies, zu vereinfachen.

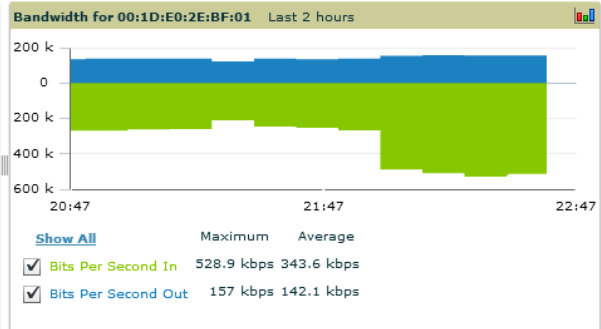
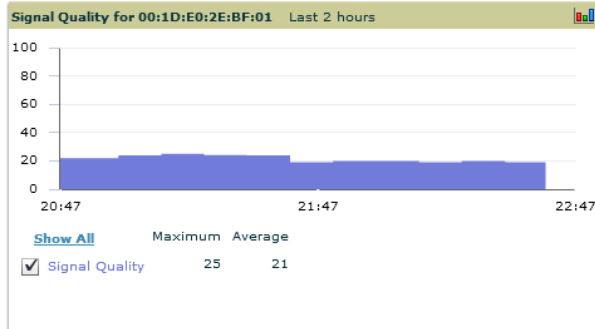
Detail for 00:1D:E0:2E:BF:01

**Device Information**

Username: -  
 Vendor: Intel Corporate  
 First Seen: 4/23/2009 1:02 PM on 00:0b:86:c3:5e:27 for 1 hr 5 mins  
 Last Seen: 4/28/2009 10:46 PM on 00:0b:86:c3:5e:27 for 3 hrs 16 mins  
 Classification: Unclassified

**Alert Summary at 4/28/2009 10:46 PM**

Type	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	0	-
Incidents	0	0	0	-
RADIUS Authentication Issues	0	0	0	-



AMP Benutzbildschirm

Um das Remote Troubleshooting zu vereinfachen, besitzt der RAP einen Diagnosebildschirm, der lokal vom Benutzer angesteuert werden kann. Falls ein RAP keine Verbindung mehr zum Daten Center aufbauen kann, erleichtert dieses Feature die Lösung des Problems aus der Ferne.

RAP Console



SUMMARY Connectivity Diagnostics

Connection Status: Connected Basic Advanced Last updated: 10:48:43 PM [Refresh](#) | [Generate & save support file](#)

**Wired Ports**

Port	Status
0 (uplink)	<span>Connected</span>
1	<span>Disabled</span>

**Wireless SSIDs**

SSID	Status	Band
rn-demo-employee	<span>Up</span>	2.4GHz
rn-demo-guest	<span>Up</span>	2.4GHz
rn-demo-voice	<span>Up</span>	2.4GHz

**Wired User**

Mac Address	IP Address

**Wireless User**

MAC Address	IP Address
00:21:5c:50:01:91	172.16.0.231

**Device Info**

Type: RAP-2WG  
 Name: 00:0b:86:c3:59:e6  
 Wired MAC address: 00:0b:86:c3:59:e6  
 Serial #: AH0000580  
 Tunnel IP address: 192.168.253.111  
 Software Version: ArubaOS Version 3.3.2.11-rn-3.0.0

Up time: 7 min  
 Master: 63.82.214.195  
 lms: 172.16.0.254

**Uplink Info**

Port 0 (active)  
 Port Speed: 100Mb/s  
 IP address: 192.168.1.103

RAP Console für Remote Troubleshooting

## **Vorgehensweise beim Aufbau von Aruba`s virtueller Standortvernetzung**

Es sind 4 Schritte nötig um eine virtuelle Standortvernetzung von Aruba zu errichten: (1) Implementierung der preiswerten RAP`s und BOC`s an den Standorten; (2) Ausnutzung von handelsüblichen WAN Verbindungen, an Stelle von teuren privaten WAN Clouds; (3) Zentralisierung des Managements und des Controllings mit Hilfe der Aruba Controller in der Datenzentrale und (4) Einrichtung des User orientierten Managements über die AirWave Management Plattform, um eine durchgängige Sichtbarkeit aller Nutzer und Geräte im Netzwerk zu erreichen.

In der Einrichtungsphase können die Aruba RAP`s und BOC`s mit minimaler oder sogar ohne Voreinstellung an die Standorte verschickt werden. Der Benutzer kann die Geräte auf Grund der Einfachheit selbständig installieren.

Während der Designphase muss erörtert werden, welchen Level an WAN Verbindungen die einzelnen Standorte erhalten sollen. In den meisten Fällen sind bereits ausreichende DSL- und Kabelverbindungen vorhanden, die bei den Standorten genutzt werden können.

Die Aruba Controller werden am Frontend des Remote Netzwerkes in der Datenzentrale eingerichtet. Alle RAP`s und BOC`s werden sich an diese Controller ankoppeln, die dann als Systemkontrollpunkt und als Management Plattform für die Standorte agieren werden.

Das AMP liefert die detaillierten Reports und das netzwerkweite Troubleshooting. Die detaillierten Statistiken, Echtzeit-Bilder und die erweiterten Help Desk Anwendungen machen das AMP zu einem unverzichtbaren Tool für die Remote Netzwerkanwendungen.

## **Reduzierung der Kosten und der Komplexität bei der Standortvernetzung**

Durch die Umstellung zu immer mehr verteilten Arbeitsplätzen steigt die Nachfrage nach Standortvernetzungen, im gleichen Zuge soll aber auch eine Reduzierung der Kosten erreicht werden. Mit diesen Anforderungen stellt sich die Aruba Lösung als eine der besten Lösungen dafür auf. Aruba`s VBN Lösung bietet dazu sichere one-touch Installationen durch den Benutzer, Unterstützung verschiedenster preiswerter und handelsüblicher WAN Verbindungen, zentrales Management und Controlling in der Datenzentrale, den Einsatz der AirWave Management Plattform für eine durchgängige Sichtbarkeit aller Nutzer und Geräte im Netzwerk. Die Summe all dieser Merkmale liefert eine starke, sichere Niederlassungslösung, zu geringen Kosten und einem minimalen IT Overhead.

Anstatt teure und komplexe Produkte auf jeden Standort replizieren zu müssen, zeichnet Aruba eine Seite der Virtualisierungstechnik auf, in der komplexe Aufgaben in der Datenzentrale konsolidiert werden und die Services zu den preiswerten Standortgeräten hin virtualisiert werden. Letztendlich macht VBN bei der Standortvernetzung und Sicherheit das Gleiche, wie es die Datenzentrale zur Virtualisierung der Desktop Anwendungen umsetzt.

## Typische Anwendungen

Die Verfügbarkeit einer preiswerten, ständig erreichbaren, einfach zu installierenden Niederlassungslösung macht es wirtschaftlich sinnvoll, diese Lösung auch für eine breite Palette an neuen Anwendungen einzurichten.

### Die Niederlassung

Unabhängig von der Größe der Filiale, ob ein oder hunderte von Mitarbeitern, jeder der heutigen Filialmitarbeiter benötigt einen Zugriff zu lokalen Ressourcen (Server oder Drucker), eine drahtgebundene und drahtlose Netzwerkverbindung mit entsprechender Verschlüsselung und ein Intrusion Protection System das die Integrität der Unternehmensdaten sicherstellt.

### Einzelhandels Vernetzung

Läden, Lagerhäuser, Handelsketten und Büros benötigen heute eine Remote Netzwerklösung, die ohne IT-Fachpersonal installiert werden kann, eine robuste Verbindung zu drahtlosen Scannern und VoIP Telefonen liefert, sowie mit hochsicheren Merkmalen versehen ist, die einer PCI Compliance entsprechen kann.

### Telearbeitsplätze und Home Offices

Festangestellte Mitarbeiter, die von Zuhause aus arbeiten, benötigen den gleichen Zugang zu den Unternehmensressourcen, wie Ihre Kollegen in der Firmenzentrale. Die RAP's liefern ein hoch performantes WiFi, einen sicheren drahtgebundenen Zugriff zu drahtlosen Laptops, sowie drahtgebundene VoIP Telefone und Netzwerkdrucker. Durch das Policy-basierte Forwarding, wird den IT-Managern ein weiter Spielraum gegeben, lokale Zugriffsrechte einschließlich Internet Zugriffen zu konfigurieren.

### Das virtuelle Call Center

Call Center benötigen sehr daten- und sprachintensive Anwendungen. Selbst der kostengünstigste RAP bietet für VoIP Telefone und PC eine sichere Verbindung in die Datenzentrale, über handelsübliche DSL- oder Kabelverbindungen, an. VBN ist eine sehr kostengünstige Lösung und ermöglicht sowohl den Zeitarbeitern, als auch den Vollzeit Mitarbeitern effizient von Zuhause oder über Satelliten Büros zu arbeiten

### Telemedizin

Der weitgefächerte Einsatz bei der Telemedizin hängt von der Verfügbarkeit preiswerter, sich selbst installierender Netzwerke ab, die Daten zuverlässig und ohne Kompromittierung der Privatsphäre austauschen müssen. VBN ist eine kostengünstige Lösung für eine sichere Übertragung der Telemetrie, der Diagnostik, der Patientenaufzeichnungen, digitaler Bilder und weiteren Anwendungen zwischen den Kliniken und den entfernten Standorten.

## **Die virtuelle Universität**

Immer mehr Universitäten bieten ihren Studenten virtuelle Lehrbereiche oder Fernzugangstudien an. Auch hier steigt der Bedarf an kostengünstigen Zugriffsmöglichkeiten auf die Universitätsressourcen. VBN ist hierbei die ideale Lösung für diese Anwendungen, da über die billigen RAP`s jeder drahtlose PC, jedes iPhone oder ein anderes technisches Hilfsmittel der Studenten, unterstützt werden kann. Zusätzlich wird dadurch die Netzwerkintegrität bewahrt sowie die Zusammenarbeit und Innovation gefördert.

## **Notfallplanung und Disaster Recovery**

Im Falle einer natürlichen Katastrophe, menschlichem Versagen oder einer Pandemie, bietet VBN einfache und effektive Mittel, um das Unternehmen weiter am Laufen zu halten, indem einfach den Mitarbeitern die Zugänge zum Unternehmensnetz von anderen Standorten, z.B. von Zuhause aus zur Verfügung gestellt werden. VBN erlaubt es, das Notfallpersonal über weite Entfernungen hinweg, mit den kritischen Notfallressourcen in Kontakt zu halten. Die 3G Mobilfunkunterstützung kann ohne vorherige Planung sofort eingesetzt werden. Somit ist VBN auch für schnelle Einsatzoperationen geeignet.



1344 Crossman Ave. Sunnyvale, CA 94089-1113  
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | [info@arubanetworks.com](mailto:info@arubanetworks.com)  
<http://www.arubanetworks.com>