

Technologie White Paper

Alcatel-Lucent Remote Access Point Lösung - die einfache Verlängerung des Unternehmensnetzwerkes in kleine Außenstellen und Home Offices.

In diesen Dokument wird der Anwendungsbereich der Alcatel-Lucent Remote VPN Lösung beschrieben. Es wird die unkomplizierte Installation der Lösung am Standort des Nutzers und die einfache Administration durch die verantwortlichen Mitarbeiter oder zentrale IT Abteilungen dargestellt. Ferner geht das Dokument auf die zusätzlichen Möglichkeiten und die erhöhte Sicherheit während der Nutzung ein.

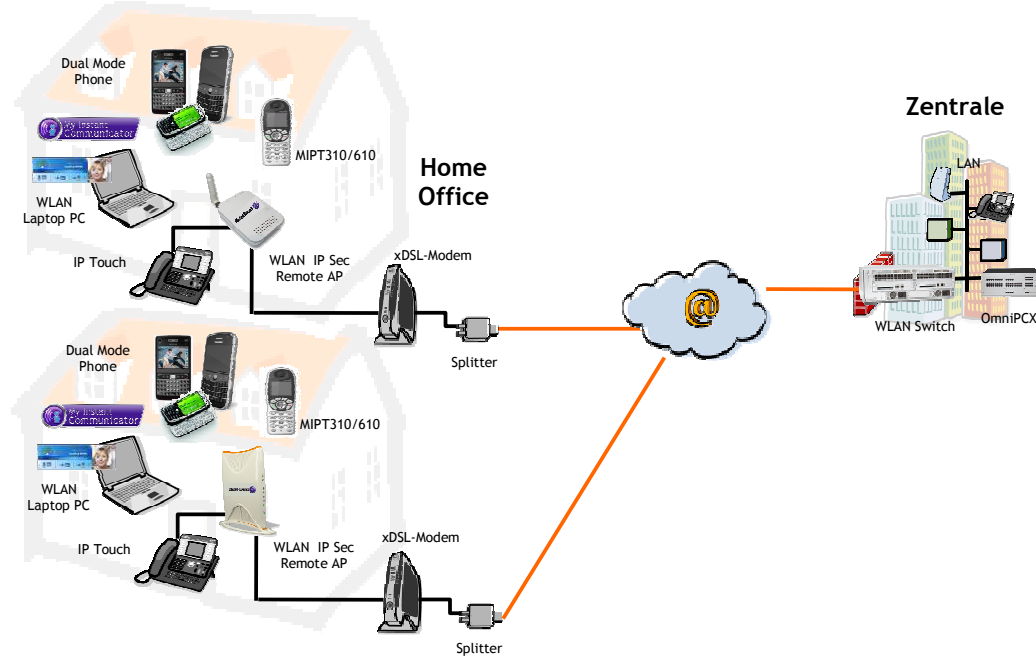
Neben Umwelt- sprechen auch viele ökonomische Gesichtspunkte für die Nutzung von Home Offices und kleineren dezentralen Büros. Für die Mitarbeiter in diesen Büros ist die Nutzung derartiger Möglichkeiten meist mit einem erhöhten Aufwand und geringerem Komfort bei der Kommunikation erkaufte. In der Regel wird zum Beispiel auf den vollen Funktionsumfang von Systemtelefonen, wie sie in den zentralen Standorten von Unternehmen eingesetzt werden, verzichtet. Typischer Weise eingesetzte Geräte bieten nur eingeschränkte Funktionen und erlauben keinen Zugriff auf zentrale Daten wie Adressbücher. Andererseits ist eine verschlüsselte Datenkommunikation in vielen Fällen zwingend notwendig. Der Aufbau einer verschlüsselten Verbindung wird in der Regel mit Token- oder One-Time-Password-Systemen umgesetzt, die die Eingabe von Daten durch den Nutzer erfordern. Da diese Systeme aus Sicherheitsgründen mit Time-Out Mechanismen ausgestattet sind, muss der verschlüsselte Verbindungsaufbau häufiger durchgeführt werden.

Eine Kommunikation zu direkten Nachbarn (z.B. LAN-Druckern) ist in der Regel aus Sicherheitsgründen ausgeschlossen, da dies für mobile Nutzer in Hot Spot und anderen öffentlich zugänglichen Umgebungen außerhalb der eigenen Home Office Umgebung ein Eindringen von extern auf den eigenen Notebook ermöglichen könnte.

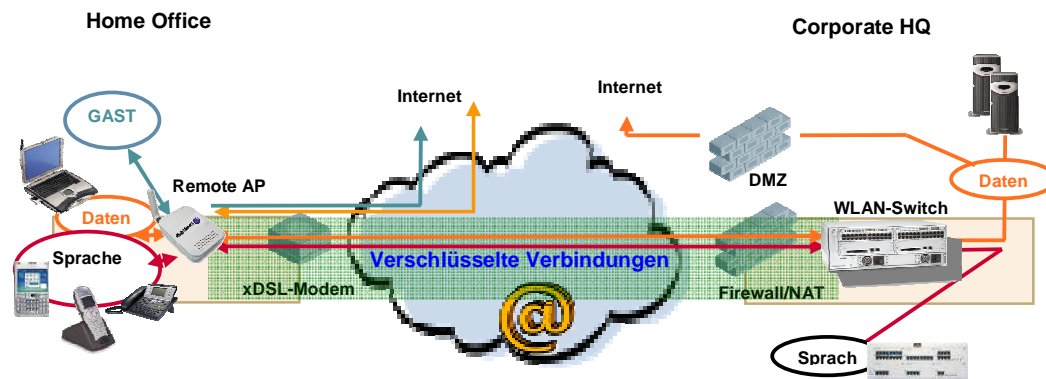
Erhöhter Aufwand tritt aber auch auf der administrativen Seite auf. Die Mitarbeiter müssen bei der Einrichtung der IT-Komponenten in den dezentralen Büros unterstützt werden. Sollte auch WLAN verwendet werden, so werden vielfach unterschiedliche WLAN-Einstellungen in der Zentrale bzw. in den Remote Offices genutzt. Dies muss auf den Endgeräten administriert werden. Auch muss für die zentrale Überwachung und Administration ein erhöhter Aufwand betrieben werden. Man denke hier nur an ein zentrales Logging oder Software-Updates.

Die Alcatel-Lucent Lösung macht den Unterschied

Die Alcatel-Lucent Remote Access Point Lösung ist vom Design her zentralistisch aufgebaut.

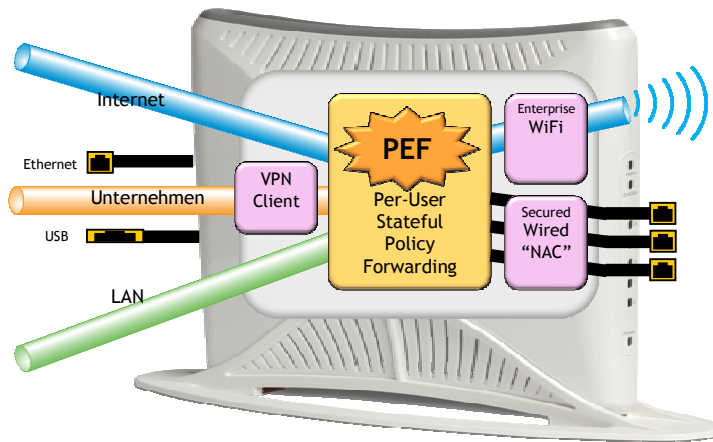


In der Zentrale wird ein WLAN-Switch implementiert. Dieser übernimmt die gesamte Verwaltung der Remote Access Point Lösung. In den dezentralen Büros werden Remote Access Points implementiert. Diese werden vom Nutzer ausschließlich mit dem Internet-Anschluss (xDSL-Modem) verbunden. Sofern der Access Point über einen USB-Anschluss verfügt, ist dies auch über UMTS möglich. Weitere Installationsarbeiten sind nicht notwendig.



Nach der Hardware-Installation baut der Remote Access Point eine verschlüsselte Verbindung zum zentralen WLAN-Switch auf und lädt sich dort die aktuelle Software und Konfiguration.

Der Remote Access Point lädt sich mit der Konfiguration auch ein optionales Firewall Regelwerk, welches mögliche Kommunikationsbeziehungen überwacht und ggf. unterbindet.



Über die Firewall Funktion lässt sich ein Gast-Zugang direkt in Richtung Internet ermöglichen. Somit wird der Verkehr des Gastes in Richtung Internet nicht durch das Unternehmensnetzwerk geleitet. Auch eine Zugangskontrolle auf den LAN-Ports ist konfigurierbar. Somit wird ein unberechtigter Zugang zum Firmennetzwerk ausgeschlossen, der gerade in Home Office Umgebungen vor Ort schwer kontrollierbar wäre.

Vorteile für den Nutzer im Home Office oder kleinen Außenstellen

- **Verschlüsselte Verbindung** - Die verschlüsselte Verbindung in die Firmenzentrale wird durch den Remote Access Point realisiert. Über LAN angeschlossene Endgeräte wie PC's oder IP Phones brauchen selbst keine verschlüsselte Verbindung mehr aufbauen. Die Eingabe von Passwort-Informationen für den Verbindungsaufbau durch den Nutzer im Endgerät entfällt.
- **Dauerhafte Verbindung zur Firmenzentrale** - Der Remote Access Point stellt eine dauerhafte Verbindung in die Firmenzentrale her. Damit entfällt der manuelle Aufbau von verschlüsselten Verbindungen.
- **WLAN-Nutzung** - Es können die gleichen WLAN-Zugangsmechanismen wie für das WLAN in der Unternehmenszentrale genutzt werden. Zusätzliche Profile auf Endgeräten für den WLAN-Zugang entfallen. Mobile Geräte, wie WLAN-Phones verbinden sich automatisch zum WLAN, egal ob diese im Einzugsbereich des WLANs in der Unternehmenszentrale oder im Home Office sich befinden.
- **System-Telefone** - Über die verschlüsselte Verbindung ist es auch möglich, IP-System-Telefone wie auch im Firmen-LAN zu betreiben. Somit werden die gleichen Funktionen wie auf dem Telefon in der Firmenzentrale geboten. Es ist in der Konfiguration zu beachten, dass die Access Points kein PoE liefern. Wenn somit ein schnurgebundenen IP Phone angeschlossen werden soll, so ist für die Stromversorgung zu sorgen.
- **USB-UMTS** - Ausgewählte Access Points verfügen über einen USB-Port, der auch mit einem UMTS Stick bestückt werden kann. So kann ein kleines Büro mit mehreren Endgeräten auch kabellos, bequem und sicher an die Unternehmenszentrale angebunden werden.

Vorteile für die zentrale IT

- **Zentrale Konfiguration** - Alle Remote Access Points können leicht mit einer einheitlichen Konfiguration ausgestattet werden. Hierzu wird eine virtuelle Access Point Konfiguration erstellt und diese dann den realen Access Points zugewiesen.
- **Konfigurationsänderungen** - Konfigurationsänderungen werden in den zentralen virtuellen Access Point Konfigurationen vorgenommen. Alle realen Access Points, die dieser virtuellen Konfiguration zugewiesen sind, erhalten die geänderte Konfiguration.
- **Keine dezentrale Konfiguration** - Die Remote Access Points erlauben keine lokale Administration über eine Konsol-Schnittstelle. Die Konfiguration erfolgt ausschließlich über den zentralen WLAN-Switch.
- **Software-Updates** - Eine neue Software wird auf dem zentralen WLAN-Switch hinterlegt und die Remote Access Points werden über einen zentral angestoßenen Reboot mit neuer Software versorgt.
- **Firewall-Updates** - Die dezentral auf den Remote Access Points notwendigen Firewall Regeln werden zentral auf dem WLAN-Switch verwaltet.
- **Quality of Service und Bandbreitenbegrenzung** - Neben der Zugangskontrolle sorgt die Firewall-Lizenz im WLAN-Switch auch für die Umsetzung von Quality of Service. So können Applikationen priorisiert werden. Zusätzlich können mit der Connection Admission Control die Anzahl der Nutzer einer Applikation beschränkt werden (z.B. Anzahl der VoIP Nutzer). Somit wird verhindert, dass sich gerade bei schmalen Bandbreiten Nutzer mit gleichen QOS-Merkmalen gegenseitig die Bandbreite wegnehmen.
- **Zentrale Nutzerverwaltung** - Die Nutzerdaten (User Name und Passwort) liegen zentral in einer Datenbank auf dem WLAN-Switch oder auf einem zentralen Radius-Server und sind damit Hardware-unabhängig. Auch ist ein zentrales Black-Listing möglich.
- **Zentrale Überwachung** - Wichtige Informationen wie zum Beispiel Angriffe auf die WLAN-Funktion des Remote Access Points werden durch den Remote Access Point an den zentralen WLAN-Switch geschickt und dort zentral dargestellt. Sie können durch den Administrator effizient bearbeitet werden bzw. schnell Sicherheitsvorkehrungen getroffen werden.
- **Einfaches Hardware-Replacement** - Durch die Entkopplung der Software-Konfiguration von der Hardware, ist im Fehlerfall ein einfacherer Austauschprozess möglich. Auf einem Remote Access Point müssen ausschließlich die Internet-Zugangsparameter konfiguriert werden, welche nicht zwingend standortspezifisch sind. Weitere Prüfungen (SW-Release, Konfigurations-Stand u.ä.) entfallen.

Somit ergeben sich zusammengefasst folgende Vorteile.

- Die Nutzung von Remote Anbindungen wird für den Nutzer wesentlich vereinfacht. Dies erhöht die Arbeitseffizienz.
- Der Remote-Nutzer kann IP-basierte Dienste nutzen, die sonst nur in der Firmenzentrale nutzbar waren. Dies sind zum Beispiel
 - IP Phones
 - Zentrale Print Services
- Die Software-Konfiguration wird von der Hardware entkoppelt. Im Fehlerfall wird eine neue Hardware zum Nutzer versendet.

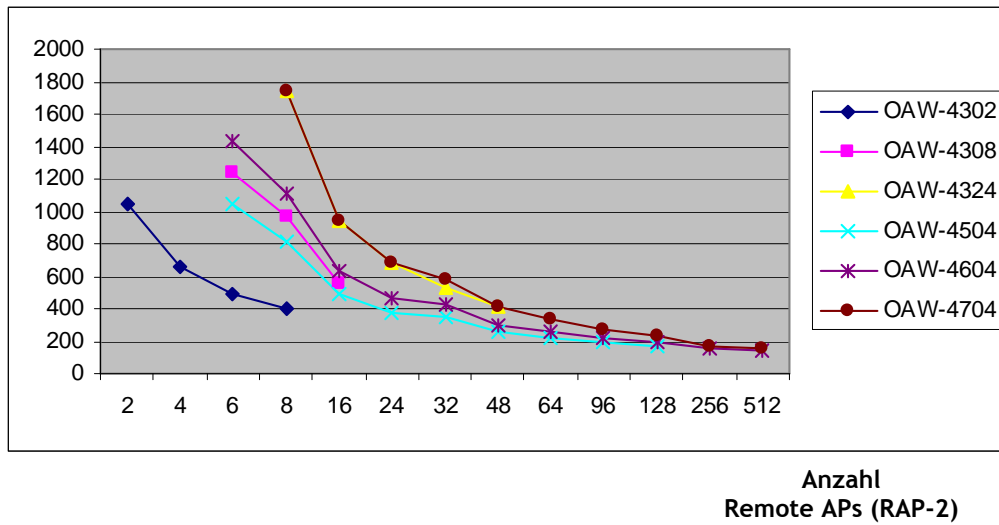
- Durch die zentrale Administration erhöht sich die Effizienz in der Verwaltung derartiger Konfigurationen erheblich.

Kostenstruktur

Nachfolgend ist die Kostenstruktur für Remote Access Point Konfigurationen einmal exemplarisch dargestellt. In den Konfigurationen wurden unterschiedliche zentrale WLAN Switches in exemplarischen Ausbaustufen mit Remote Access Points (RAP-2) betrachtet.

Neben der Hardware und den Remote Access Point Lizenzen wurden ebenfalls noch die Firewall und Voice-Lizenzen im zentralen WLAN Switch mit eingerechnet. Die Firewall-Lizenzen sind für den Gast-Zugang (direkten Ausstieg ins Internet) und für die Priorisierung von Datenapplikationen notwendig. Die Voice-Lizenz sorgt zum Beispiel für die Überwachung der Anzahl der Gespräche auch im Zusammenhang mit der für andere Applikationen zur Verfügung stehenden Bandbreite. Für eine einfache Anbindung von Daten-Endgeräten können zum Beispiel aber auch beide kostenpflichtige Lizenzen entfallen.

Stückkosten in Euro
(Listenpreis)



Folgende Komponenten stehen für eine Konfiguration zur Verfügung.

Dedizierte Remote Access Points:

RAP-2WG

- 802.11b/g Single Radio Access Point
- 2 Fast Ethernet Interfaces
- Extrem kleiner Formfaktor
- Dedizierter Remote Access Point
- Externes Netzteil inklusive



RAP-5WG

- Single-Radio pre-802.11n (a/n oder b/g/n)
- 3x3 MIMO 300Mbps per radio
- 1x GigabitEthernet (RJ-45) und 4x FastEthernet (RJ-45)
- 1x USB 2.0 port
- WAN Support via EVDO/HSDPA, Ethernet
- Dedizierter Remote Access Point für bis zu 50 Nutzer
- Externes Netzteil inklusive



Access Points, die auch als Remote Access Point verwendet werden können:

AP60/61

- Single Radio (per Software konfigurierbar) 802.11a oder b/g
- 1 Fast Ethernet Interface
- Interne (AP61) oder externe (AP60) Antenne
- Ext. Netzteil oder PoE notwendig



AP65

- Dual Radio 802.11a und b/g
- 1 Fast Ethernet Interface
- Interne Antenne für beide Frequenzbereiche
- Ext. Netzteil oder PoE notwendig



AP70

- Dual Radio 802.11a und b/g
- 2 Fast Ethernet Interfaces
- Interne Antennen für beide Frequenzbereiche
- 2 externe Anschlüsse je Frequenzbereich
- 1 USB Port
- Ext. Netzteil oder PoE notwendig



AP85

- Outdoor Einsatz
- Dual Radio 802.11a und b/g
- 1 Fast Ethernet Interfaces (TX, FX,LX)
- 2 externe Anschlüsse je Frequenzbereich
- Ext. Netzteil oder PoE notwendig













AP12x

- AP120/121 - Single-Radio pre-802.11n (a/n oder b/g/n SW-konfigurierbar)
- AP124/125 - Dual-Radio pre-802.11n (a/n und b/g/n)
- 3x3 MIMO 300Mbps per radio
- 2 Gigabit Ethernet Interfaces
- AP120 /124 3 externe Antennenanschlüsse
- AP121/125 3 interne, ausklappbare Antennen
- Ext. Netzteil oder PoE notwendig



Zentrale WLAN Switches:

Für alle nachfolgend genannten WLAN Switches ist pro Remote Access Point eine Remote Access Point Lizenz zu konfigurieren.

Typ		Max. Anzahl Remote APs	Durchsatz mit AES	Anzahl Interfaces Gigabit/FastEthernet
OAW4302		8	0,2GBit/s	1/1
OAW4304		4	0,2GBit/s	1/8
OAW4308		16	0,2GBit/s	1/8
OAW4324		48	0,4GBit/s	2/24
OAW4504		128	0,8GBit/s	4/0
OAW4604		256	2GBit/s	4/0
OAW4704		512	4GBit/s	4/0
OAW-SUP-1		128	2GBit/s	Über ext. Interface-Karten
OAW-SUP-2		256	2GBit/s	Über ext. Interface-Karten
OAW-SUP-3		2048	4GBit/s	10 zuzgl. 2x10GE

www.alcatel-lucent.com Alcatel, Lucent, Alcatel-Lucent und das Alcatel-Lucent-Logo sind Marken von Alcatel-Lucent. Alle anderen Marken sind Eigentum ihrer jeweiligen Besitzer. Änderungen der hier enthaltenen Informationen behalten wir uns ohne Ankündigung vor. Alcatel-Lucent übernimmt keine Verantwortung für die Richtigkeit der hier enthaltenen Informationen.

Rev. A 10/2009

© 2009 Alcatel-Lucent. Alle Rechte vorbehalten.