A wireless office yes

Powerful, open, flexible Wi-Fi for the new Mobile-Cloud world.

Key Benefits

- **Security without complexity**

  With mobile devices, BYOD, guest access, and internet-of-things (IoT) devices, security is of paramount importance. The solution allows access control policies to be set and enforced using programmable network infrastructure to offload much of the responsibility to end users and automate the orchestration of security processes, saving time and operational costs.

- **Unified communications**

  To realise the full productivity benefits of unified communication and collaboration using applications such as Microsoft's Skype for Business, the mobile network has to support business grade voice and video. The solution has proven capability in this area in many large organisations throughout the world.

- **Cost savings**

  Fewer wired desktops and desk phones means the need for edge switches is lessened. PBXs and specialised conferencing systems can be eliminated. Moves and changes are easier. Network access control and security policy management can be automated. If BYOD is adopted, there is no need to supply corporate laptops or phones. These can translate into significant operational and capital savings.

The growing adoption of mobile devices (smartphones, tablets and laptops), increasing number of personal and corporate applications running on those devices, and changing work practices (such as Activity Based Working) all present challenges for organisations. In this environment, organisations look to:

- Reliably and securely connect mobile devices to apps in public and private clouds and on-premise with ubiquitous Wi-Fi.
- Prioritise these apps to ensure adequate response for corporate apps and support business grade voice and video over Wi-Fi.
- Securely connect different classes of user (employees, contractors, guests) using different types of devices, including bring-your-own device (BYOD), without imposing an additional load on IT resources.

The Aruba Wi-Fi Managed Service from Optus is designed for large enterprises and government agencies that are moving to a wireless office and facing the above challenges. The ICT paradigm is increasingly one of securely and efficiently connecting mobile devices to apps in public and private clouds. Using Aruba's flexible and open architecture Optus can cater for the needs of large organisations with tailored solutions encompassing headquarters/campus, branch office, and remote access, and with global scale.

These solutions use the appropriate blend of technology (on-premise, cloud, controller based and controller-less) suited to the needs of your organisation. Solutions that are open, and incorporate best-of-breed multi-vendor components and leverage your existing network investments.

With the Aruba Wi-Fi Managed Service, security is paramount, embracing network access control, BYOD and guest access. Security workflows are automated, reducing management complexity. The latest technologies, such as 802.11ac 2nd wave and software-defined networking (SDN), are exploited.

The solution is ideal for supporting mobile unified communications (UC) such as Microsoft's Skype for Business (SfB) with the required Quality of Service (QoS) to enable business grade voice and video.

Optus can manage the solution as a service, provide it as a turnkey implementation, or simply provide you with the products and maintenance.

Solution Features

Security

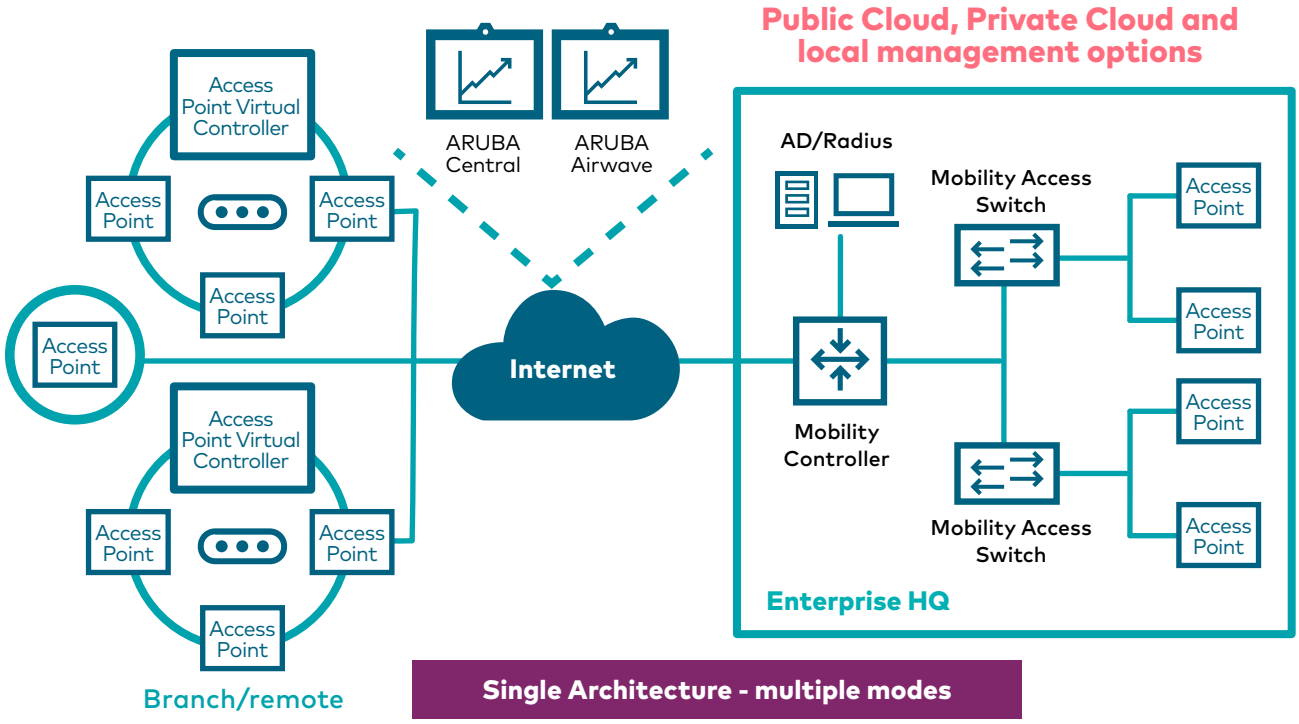
In the new world of mobility with BYOD and guest access, security is a number one priority. No longer can the physical security of ports be relied on, nor can locked down corporate devices with standard operating environments and software be assumed. Security policies for network access control need to be set by user, device, app, location and time and enforced irrespective of the method of connection. Also, given this increased complexity, security workflows and integration with other network security components such as firewalls, mobile device management products and anti-virus/malware software need to be orchestrated automatically in real time. This is what Aruba's ClearPass does, reducing costs by minimising the need for manual intervention.

ClearPass provides automated login for single sign on (SSO) and also detects insecure devices and blocks their access to network resources.

ClearPass helps to ensure security of network access (wireless, wired, remote), managing multi-vendor networks from a single point with a simplified IT and user experience:

- Authentication, authorisation and accounting (AAA) /policy management
- Device on-boarding
- Visitor management
- Device health

Strong encryption (up to Suite B classified/military) and automated intrusion prevention and detection of rogue devices at the access point/controller level complete the security story.



Guest Access

Guest access is managed by ClearPass. With little IT involvement, guest sponsors such as receptionists, event coordinators and other non-IT staff can create temporary accounts for guest Wi-Fi access.

- Guest self registration
- Sponsor privileges with access verification
- Per session controls
- Automated SMS/email credential delivery
- Social logins with Facebook, Google+, Twitter and Linkedin

Mobile-friendly login pages displayed to visitors can be customised with your company logo, custom welcome messages, terms and conditions, backgrounds, colors, and images.

Managed Services

Optus' Wi-Fi managed services cover site survey, design, product procurement, installation, maintenance and management. These services can be tailored to your needs and integrated with other services from Optus such as core networking, internet connection, and applications including SfB to provide complete networking and communications capability based on ITIL style service level agreements.

Support for Microsoft SfB and other mobile UC solutions

Aruba has a long history of engagement with Microsoft and joint research and development to make business grade voice and video over Wi-Fi possible. Aruba was the first Wi-Fi vendor to be certified for SfB (then called Lync). In 2013, Aruba was again the first vendor to adopt Microsoft's SDN application programming interface . Microsoft itself uses Aruba globally to deliver mobile UC to 80,000 employees. There are a large number of references all over the world deploying SfB over Aruba Wi-Fi. Aruba also supports most common UC solutions.

There are three things essential for voice and video support over Wi-Fi:

- **Make best use of the air** – Aruba's Adaptive Radio Management technology optimises Wi-Fi network behavior and automatically ensures that the access points stay clear of RF interference. Aruba's Airtime Fairness provides every client with an equal opportunity to utilise network bandwidth. High throughput clients do not get penalised because of slower clients. Aruba's ClientMatch eliminates sticky client behavior while enabling call admission control.
- **Prioritise applications** – Aruba leverages SDN integration with Microsoft SfB and Aruba's AppRF technology to prioritise voice and video traffic to enable a predictable mobile UC experience. This means fewer dropped calls and higher quality video.
- **UC dashboard** – Aruba offers end-to-end diagnostic visibility correlated across the mobility network and SfB server which simplifies operations for the network administrator. Issues are promptly isolated and fixed giving users confidence in using SfB for mobile UC.

Get started today

For organisations moving to the new world of mobile-cloud computing Optus' Aruba Wi-Fi solution offers unparalleled security without complexity, support for mobile UC, and significant potential cost savings. Contact us today to get started.

GMO_N 0376 0716MZ