SOLUTION OVERVIEW

aruba
a Hewlett Packard Enterprise company

THE ARUBA MOBILE FIRST ARCHITECTURE

March 2018

Table of Contents

Introduction

The Aruba networking architecture for the software-defined enterprise is designed to be mobile first, and it delivers a network that is open, secure, and autonomous. The velocity, variety, and volume of users and things connecting to networks have forced IT to change the way they build and operate next-generation networks.

- Mobile First—Allows users and things to connect to the network and receive the same policy and permissions regardless of how they connect, wired or wireless, making them truly mobile. Purposefully designed to deliver a non-stop networking experience for environments where mobile, IoT, and cloud are mission critical.

- Open—Networks are multi-vendor and need to be open. This means not only supporting open standards but providing rich API support in order to enable easy integration and automation end-to-end in the network by IT, line of business, and even users. Organizations need to be able to innovate at their pace and not be locked-in and limited by a single vendor's architecture.

- Secure—Security at all layers in the network is critical. Aruba secures the wired and wireless infrastructure with signed code, secure boot, and cryptographic hardware protection. User data is protected with strong encryption and per-user level policy, both granting appropriate access and protecting devices from threats. Analytics-driven security, market leading policy management, and an extensive ecosystem of trusted security partners enables IT to design and operate their network.

- Autonomous—Machine learning uses massive amounts of analytics data in order to understand the operational and security state of the network. Automated systems optimize performance and alert administrators of changes or highlight potential changes that require acceptance via on-premise and cloud-managed network operations.

Traditional networks have become a mess of VLANs and ACLs because organizations have enforced policy and security on an infrastructure never designed to handle policy based on applications. Switch ports have static configurations and VLAN interfaces have hundreds, sometimes thousands of ACLs—leading to network designs that are fragile and that IT is afraid to touch.

Design

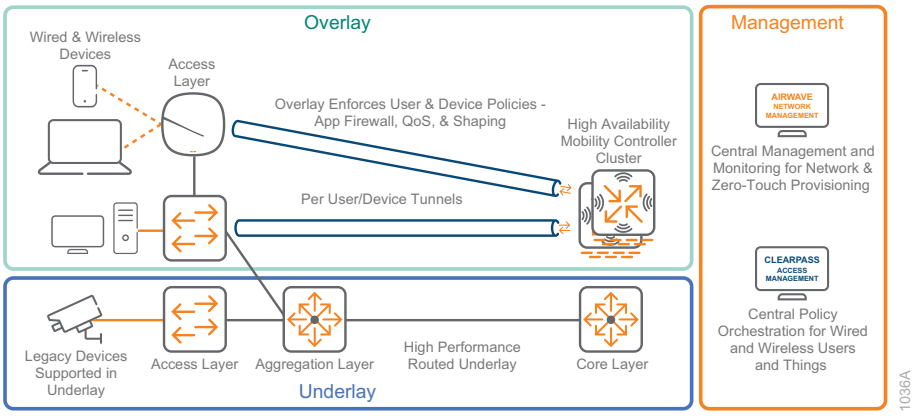
There is not one network in the future; there are thousands, and Aruba is delivering infrastructure with a model to support the diversity and complexity required in next-generation software-defined networks. In the software defined enterprise, IT runs the infrastructure and underlay network and gives the users and line of business the ability to self-provision overlay networks.

USE CASES

- **Temporary guest access to network resources**—Users can create temporary guest accounts and give permission to access network resources such as conference room video systems, printers, and Internet via an ephemeral secured overlay.
- **Facilities needs to allow vendor access to building IoT systems**—The building manager can create a secure IoT overlay for the building control systems and provision VPN service for the vendor so they can access and monitor equipment.
- **Users have devices and want own personal network**—Users with multiple wired and wireless devices need to be able to securely onboard their devices and allow them to communicate with each other regardless of how they connect to the organization's network.

Delivering the network as a service to users is the core of software defined enterprise. BYOD and its normalization has shown that IT needs to be able to support a wide range of user devices and the avalanche of IoT devices means the scale of what needs to be supported is beyond what an IT group in front of an IT management system by themselves can handle. Tools that allow IT to delegate service creation to users based on defined privileges are necessary to enable the enterprise and prevent a whole new wave of shadow IT.

Figure 1 *Aruba Mobile First Architecture*



UNDERLAY

Enterprise networks need to support the current endpoints, including many legacy systems, while they transition into a software defined model. Designs that require a full network redesign, including hardware and network protocol stack, can cause serious interruption and risk-compatibility issues, especially with legacy systems. Mobile First maintains the existing routed network, using a standard interior gateway protocol (IGP), such as OSPF, as an underlay, allowing IT to continue to run and operate existing hardware when new network is rolled out. Legacy devices can continue to operate on the underlay, and enhancements to policy allow for additional security and control on the network underlay beyond what is commonly deployed in traditional networks.

OVERLAY

The overlay allows organizations to safely tunnel Layer 2 or Layer 3 traffic over the top of the existing network. Aruba has been delivering wireless networks with an overlay model since the beginning, enabling IT to deliver service that would not be secure or stable otherwise across multi-vendor networks. Aruba is extending this functionality to wired networks, allowing the access layer switch to act as a "wired access point." Network traffic from wired and wireless users and devices is tunneled to centralized mobility controller clusters. All user and device level policy can be enforced in the overlay using the mobility controller firewall, QoS, and traffic shaping and user context is easily shared to other domains. Existing VLAN and IP addresses structures can be maintained, but because policy is enforced at the user and group levels, VLAN and IP address are not tied to policy.

DYNAMIC SEGMENTATION

The Aruba Mobile First Architecture does not rely on static port configurations, VLANs, or access lists on access points—or access switches in the network—to apply policy to users and devices.

- Tunnel node—Allows an access switch to act like a "wired access point." Users who connect to the switch can be tunneled to the mobility controller to give the same policy and user experience as when connected to the wireless network. For high availability, multiple tunnels are created, and if a controller needs to be taken offline for maintenance or an unplanned outage occurs, the user seamlessly fails over to a standby controller.
- Downloadable roles—If users or legacy devices connect to the wired network and need direct connectivity to the underlay, downloadable roles allow for the access port configuration to loaded dynamically based on the user and device posture and policy.
- Centralized policy—Aruba ClearPass handles all users and devices connected to the network. Devices can be profiled upon connection to the network, posture checked, and then the appropriate policy downloaded to the access port.

- Adaptive trust—After devices are granted access to the network, their behavior is continually monitored by behavioral analytics tools, firewall, and IPS systems. If the security posture of the device changes, a security analyst can take a number of manual or automated actions such as reauthentication to verify the user, quarantining the device with limited access to network resources to allow for easy remediation, or fully isolating the device on the network while any incidents are investigated. If everything is found to be ok or the device is remediated the security analyst can quickly restore standard access.

Aruba's dynamic segmentation allows organizations to connect users and devices to wired ports and tunnel them to a controller or connect them to the appropriate VLAN and subnet and to download a dynamic policy (with security and QoS settings) to the port to which they are connected. This extends the functionality of traditional wired 802.1X to workflows that were typically deployed only in wireless networks, such as easy onboarding by users of unknown devices (BYOD), wired guest access with the same captive portal on the wireless network, and automated support and remediation for devices failing policy or posture checks with captive portal.

NON-STOP NETWORKING

Wireless is viewed as a utility level service in enterprise networks today, meaning users expect it to be always available and perform at its best. The Aruba architecture delivers a number of wired and wireless features to support wireless networks deployed as a non-stop service with high availability an inherent part of the design.

- Controller Clustering—Up to 12 Aruba mobility controllers can form a high availability load-sharing cluster that scales to hundreds of Gbps of traffic and tens of thousands of users.
- In-Service Upgrades—With Aruba OS 8, the wireless network is able to upgrade software on access points and controllers in a manner that is transparent to users on the wireless network. Users are gracefully steered off select APs and controllers while they are upgraded and then seamlessly added back into the network.
- Seamless Failover—Access points connect to multiple controllers in a cluster, and in the event of a failure with the primary controller, the access points switch to the secondary with no noticeable interruption to the user.
- Non-Stop Switching—Aruba OS-CX in the core and aggregation layers of the network delivers high availability and hitless upgrades, allowing IT to service the network without taking an outage.

Together these features allow an Aruba network to deliver wireless that can run non-stop in an organization's network. The network can be upgraded while users are connected, with no interruption. And because of best-in-class high availability, the network can handle access point and controller failures without users experiencing interruption.

Summary

The Aruba Mobile First Architecture allows organizations to gracefully transition their existing network to a software-defined enterprise, enabling new features and functionality while supporting legacy systems. An open, multi-vendor network infrastructure allows organizations to innovate at their pace and not become locked-in to a single vendor solution but also leverage their existing investments. Security built in at all layers in the network protects infrastructure, users, and devices from existing and emerging threats from the outside and inside. Intelligent use of analytics by administrators and machine-learning based automation provides network assurance and begins the shift to a "self driving" network where IT maintains the infrastructure and policy and users provision services dynamically.

You can use the feedback form to send suggestions and comments about this solution overview.

a Hewlett Packard Enterprise company

B-000110A-1 03/18