Tech Brief |

Enterprise

The Aruba S3500 Mobility Access Switch

ARUBA® networks

Tech Brief: The Aruba S3500 Mobility Access Switch

Table of Contents

Introducing the Aruba S3500 Mobility Access Switch

The Aruba Networks™ S3500 Mobility Access Switch brings the role-based access model of Aruba wireless LANs (WLANs) to the wired network infrastructure. The S3500 is an integral part of the Aruba Mobile Virtual Enterprise (MOVE) architecture, which centralizes network access policies, security, traffic forwarding and management using a consistent set of services for wired and wireless, regardless of location, user, device or connection type.

The S3500 makes network operations more efficient while providing users with the seamless connectivity that they expect wherever they work or roam. It is designed for network access deployments in building wiring closets and connects:

- Wired Ethernet devices such as virtual desktops, IP phones or videophones, classroom peripherals, medical devices, point-of-sale devices, or security cameras.
- 802.11 access points (APs) from any vendor.

With its user-centric, role-based network access and flexible deployment options, the Aruba S3500:

- Secures the network, delivering visibility into user behavior, device types, and locations without new hardware or additional expenses.
- Simplifies access by centralizing user and device authentication across wired and wireless networks.
- Drives operational efficiency for IT staff via zero-touch provisioning and centralized configuration.
- Reduces capital and operational expenditures through rightsizing.

Aruba MOVE

The Aruba MOVE architecture provides a common set of network services for:

- Identity management
- Guest access
- Role-based policy enforcement
- Application traffic management
- Content security
- Device and network configuration
- RF and spectrum management
- Compliance

Flexible deployment modes

The S3500 uniquely supports three flexible deployment modes. As a *wired access point*, all ports on the S3500 are configured to tunnel traffic to a centralized Aruba Mobility Controller where the access network services, including authentication and policy enforcement, reside.

When tunneling traffic to a Mobility Controller, the S3500 operates in a manner identical to Aruba wireless APs.

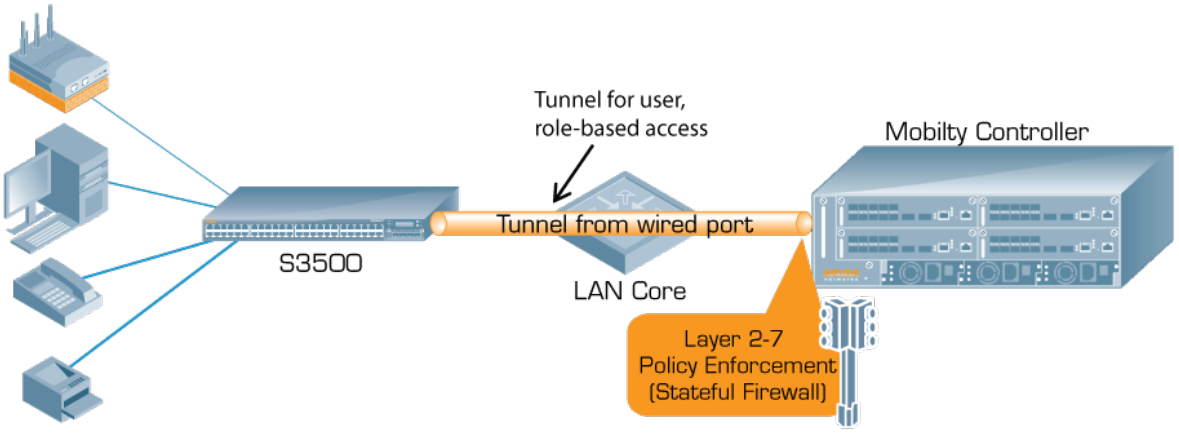

Figure 1. Wired AP deployment mode.

Optionally, the S3500 supports a full complement of Layer 2 and Layer 3* (roadmap) forwarding protocols, and ports may be configured for local forwarding. Deployment modes are configured on a port-by-port basis. Some ports may tunnel traffic back to a Mobility Controller while others are set for local forwarding. As a result, network administrators make individual decisions on which traffic is sent to the Mobility Controller's stateful firewall.

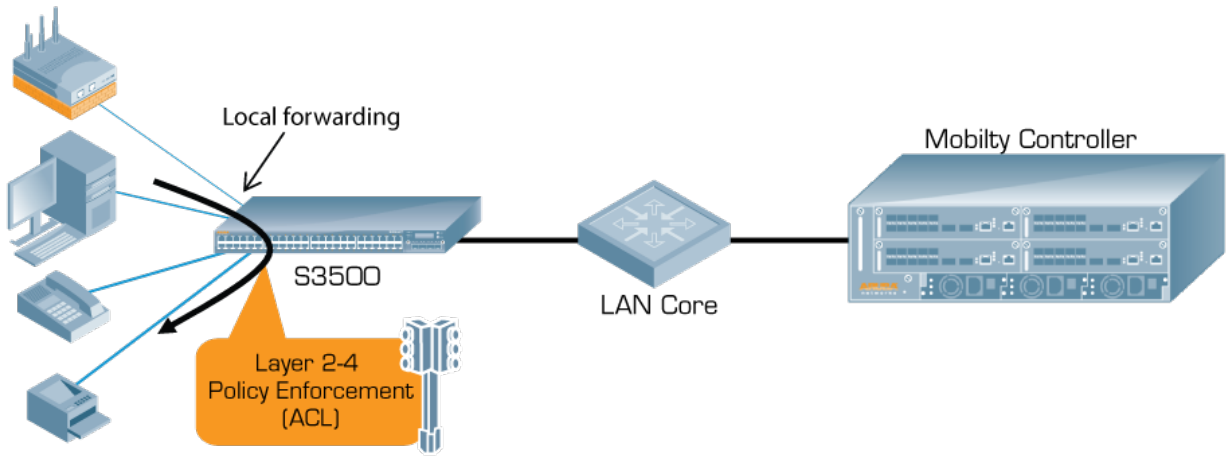

Figure 2. Local forwarding using Layer 2 and Layer 3 protocols.

Finally, the S3500 may act as a Mobility Controller* for up to eight Aruba wireless APs operating on campuses or in remote offices. In this case, the S3500 would be configured as a local controller residing at the aggregation layer of the Aruba architecture. Local controllers handle AP termination, user authentication and policy enforcement.

Configuration of the local controller occurs on a master Mobility Controller, as well as user troubleshooting, RF planning, and real-time RF visualization. In addition, the master Mobility Controller makes Adaptive Radio Management (ARM) decisions for all local controllers and is responsible for radio power and channel settings at the wireless access layer.

** Roadmap feature*

Role-based network access improves security and eliminates expenses and hassles

Wired networks based on the legacy architecture of the last 20 years have control and visibility only to the port. When connecting to that port, the user is assigned a role based on that port's virtual LAN (VLAN). The VLAN then defines policy for that physical location.

However, users are more mobile; their lives no longer revolve around an office, cubicle or any other single location. They use multiple devices to get their work done, from laptops to tablet PCs to smartphones.

In this environment, the legacy port and VLAN model does not provide adequate visibility or control over network access. And it does not scale because multiple VLANs need to be configured across ports in wiring closets, buildings, and remote locations for various employee, contractor, and guest user populations.

Ironically, in order to add mobility to a legacy wired network, IT is required to determine where users and devices are going to go before they get there!

In contrast, Aruba's MOVE architecture assigns each user a predefined role based on the user, device, application and location, and enforces that role via the firewall in the Aruba Mobility Controller. Each role may have its own firewall ACLs and other policies such as time-of-day or bandwidth limits, which are applied at wire speed.

This centralized role and enforcement model provides true mobility, allowing users and devices freedom of access without the complexity and hassle of defining VLANs and policies at many locations, including switches, routers and firewalls. Eliminating the need to configure VLANs at the network access layer saves IT an extraordinary amount of time.

MOVE supports authentication via 802.1X, MAC and captive portal without requiring a separate appliance to configure and manage. For organizations with Aruba WLANs in place, the S3500 enables access for wired and wireless users.

Rather than operating separate wired and wireless networks, Aruba integrates both into a single, efficient access infrastructure. The common network services treat users and devices as users and devices, not as extensions of a port or VLAN.

As a result, users get more consistent network access while IT eliminates complexity. In addition, the S3500 offers unprecedented granular visibility into user identity and behavior, device types, and applications. The result is faster troubleshooting, improved service quality across the network, and optimized quality of service (QoS) for business-critical applications.

In addition to network access security, the S3500 supports data encryption via IEEE 802.1AE Media Access Control Security (MACSec). MACSec provides connectionless data confidentiality between MACSec enabled devices, for example between the S3500 and Aruba's AP-130 series 802.11n wireless APs.

Zero-touch configuration saves time

Similar to Aruba's wireless APs, the S3500 is self-installing and self-configuring via pre-defined templates created in the Aruba Mobility Controller. Just plug in the device, plug in the uplink, and Aruba does the rest. This zero-touch configuration eliminates hours of tedious work configuring access switch parameters such as VLANs, ACLs, spanning tree and quality of service.

It also makes it much easier to support remote locations without onsite IT staff because it is no longer necessary to touch every device that is deployed. With up to 30 minutes of time saved in every wiring closet, the advantages of the S3500 provide new opportunities to focus on more strategic work.

The Aruba architecture provides an abstraction layer between the physical settings of the system and the conceptual goals of the network architect using configuration profiles and AP groups. This abstraction layer allows the Aruba administrator to create reusable groups of settings – called *profiles* – that can be applied in a mix-and-match fashion with extremely fine granularity – further simplifying network management and eliminating tedious work.

A flexible architecture powers network rightsizing

For the first time ever, the S3500 breaks the network's dependence on its physical wiring closets. Its ArubaStack™ feature can interconnect up to eight S3500 wired APs across multiple wiring closets and manage them as a single logical device. Accommodating a wide range of optics, the ArubaStack spans a 10-kilometer radius.

Instead of constraining access network design to accommodate individual wiring closets, IT can focus on optimizing service to where the users are – in buildings and on campuses. This flexible approach simplifies management tasks and rightsizes the network by requiring fewer uplinks to the core and fewer managed devices. The results are lower capital and operating expenses.

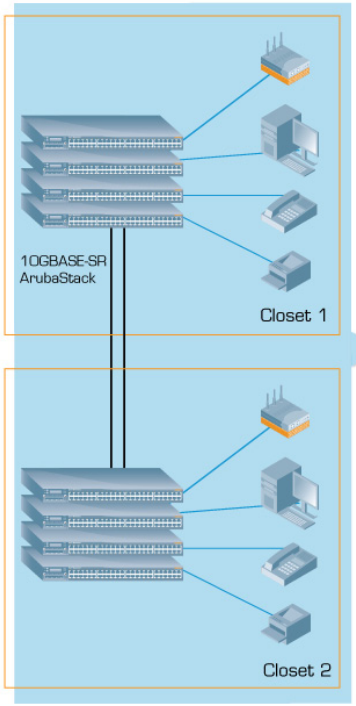

Figure 3. ArubaStack

Network Rightsizing with ArubaStack

With the legacy architecture defined by the wiring closet, every closet typically requires a minimum of two ports for redundancy. In many cases, the bandwidth provided greatly exceeds what would be required to meet performance standards – leading to an over-engineered network.

Because ArubaStack can connect multiple closets together within a building or across buildings, IT has the flexibility to engineer to performance requirements, not to an antiquated design.

ArubaStack provides another example of network rightsizing. It maintains redundancy while reducing the number of uplinks to the core by more than 80 percent. This reduces the number of ports in the aggregation layer, yielding capital expenditure savings of 10 percent.

In some cases, IT can eliminate the aggregation layer entirely by collapsing it into the core. This approach reduces capital expenditures by more than 30 percent in campus LAN deployments. Finally, IT can drive operational efficiencies with fewer devices and a simplified logical architecture with fewer instances of spanning tree and routing.

Better rogue detection and mitigation makes the WLAN more secure

Augmenting Aruba WLANs with the S3500 makes it easier to correlate potential wireless rogues with data from the wired network and mitigate threats. The Aruba AirWave® management system and Aruba RFProtect™ Wireless Intrusion Protection software can utilize data from the S3500 to determine whether potential rogues are physically connected to the network.

If a threat is identified, the S3500 can automatically shut off the affected port instead of simply containing the device through de-authentication or tarpitting. This reduces business risk and enables the IT security team to focus its efforts on the real threats.

In addition, when a user tries to authenticate to a rogue AP that has been contained, the S3500 can gracefully remediate the situation by directing the user to a page that provides instructions for authenticating to a valid AP. In doing so, it eliminates calls to the help desk.

Smart design supports the availability requirements of a 24x7 world

With the massive increases in users, mobile devices, and bandwidth requirements brought on by the demand for video content, the access network must be robust enough to continue operation in the event of any network component failure. For wired users and devices, which are typically attached to the network via a single 10/100/100BASE-T connection, the S3500 has been designed so that IT can easily fix the most common problems before they affect users.

The S3500 features dual load-sharing and hot-swappable power supplies that provide seamless failover in the event of a power failure. Multi-blower fan trays keep the S3500 in full operation in the event of a fan failure. All major components – power supplies, fans and uplink modules – are field-replaceable to cut down on repair times.

Additionally, the ArubaStack architecture enables resilient WLANs. Today's WLAN already has some levels of resiliency:

- They are deployed for full coverage within a building while providing some overlap. When a Wi-Fi device detects two APs, it will attach to the strongest signal.
- Aruba's ARM also provides for band-steering and spectrum load-sharing distribute users and devices across bands and channels.

The S3500 delivers a new level of resiliency to WLANs. Typically, network designers connect all APs to a single wiring closet switch. In the event that the switch fails, users lose all Wi-Fi access.

However, the ability of ArubaStack to extend across multiple wiring closets makes it practical to build multiple wired access rings. Some APs may be tied to one ring and others to a second ring, essentially distributing the APs across multiple S3500s.

In the event of a failure of a single device in the wiring closet, the remaining WLAN APs will automatically increase signal strength using ARM and provide RF coverage for the WLAN gaps created by the failure.

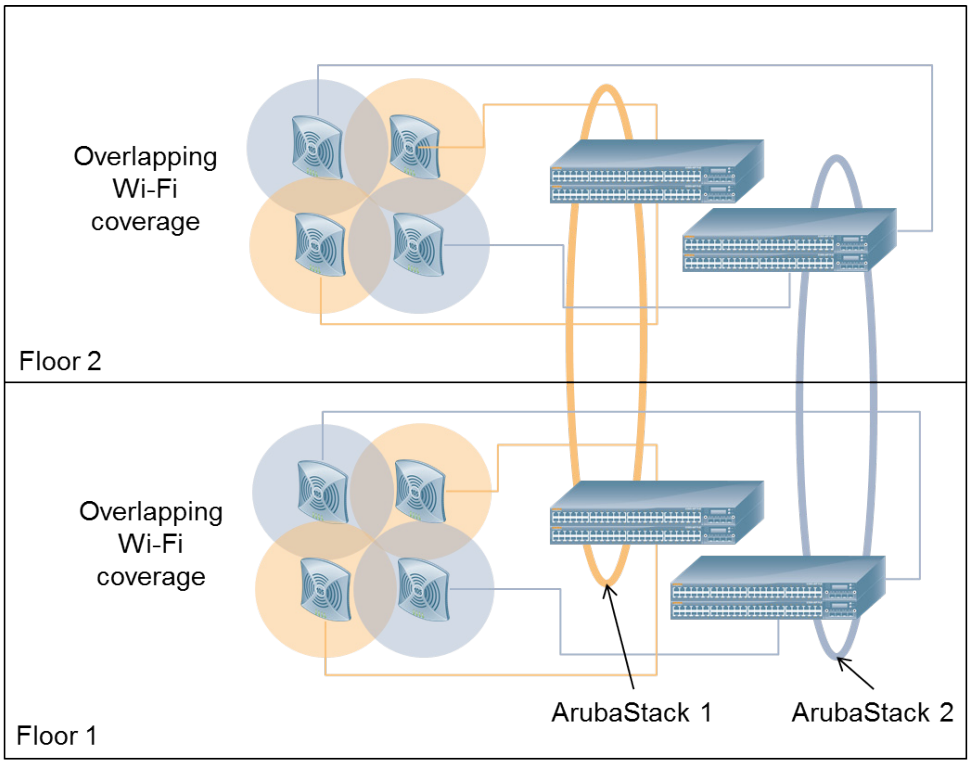

Figure 4. ArubaStack enables redundant access rings

Energy-efficient features save money and benefit the environment

Aruba is concerned about the financial and environmental impacts of the always-on mobile Internet. Consequently, the S3500 takes advantage of a variety of Aruba *green* features that reduce power usage across the network.

For example, the S3500 can cut network power usage by reducing WLAN coverage at non-peak hours when fewer people are working. In this case, IT can configure the network to shut off specific APs connected to the S3500 during non-peak time windows.

Aruba's ARM technology automatically assigns channel and power settings for all wireless APs in the network and adjusts those settings during ongoing operation as the level of Wi-Fi interference and RF noise change. Late-night users will automatically associate with remaining APs.

By deploying the S3500 in conjunction with the Aruba AirWave management system, IT can monitor the power-over-Ethernet (PoE) that is consumed on attached devices. These baseline

statistics give IT the information it needs to further optimize the network for greater energy efficiency.

Summary

The Aruba S3500 Mobility Access Switch brings the role-based access model of Aruba WLANs to the wired enterprise network infrastructure and provides flexible deployment options to support smart, rightsized network designs. Taking advantage of the common enterprise network services at the core of the Aruba MOVE architecture, the S3500 reduces capital expenditures, makes network operations more efficient, and provides users with the seamless connectivity that they expect wherever they work or roam.

About Aruba Networks

Aruba is the global leader in distributed enterprise networks. Its award-winning portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to all corporate applications and services - regardless of the user's device, location, or network. This dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter, Facebook, or the Green Island News Blog.

Aruba Networks

1344 Crossman Ave.
Sunnyvale, CA 94089-1113
Phone: +1-408-227-4500
Fax: +1-408-227-4550
Get Directions »

General Inquiries:
info@arubanetworks.com