INTEROPERABILITY TEST RESULTS: ARUBA MOBILITY ACCESS SWITCH AND ARISTA 7050S

ARUBA networks

Table of Contents

Executive summary	3
Scope and methodology	3
Interface connectivity	4
Port channels and link aggregation control protocol (LACP)	4
VLAN trunking	4
Spanning tree protocol	5
Hot standby link	5
Link layer discovery protocol (LLDP)	6
Cisco discovery protocol (CDP)	6
Quality of service (DSCP and 802.1p)	7
802.1X authentication	7
MAC authentication	8
Captive access portal	8
Tunneled node authentication	8
Internet group management protocol (IGMP) snooping	9
Internet protocol version 4 (IPv4)	10
Aruba AirGroup integration (L2GRE)	10
About Aruba Networks, Inc.	11

Executive summary

Aruba Networks has conducted key network protocol tests to assess interoperability between its Mobility Access Switches and the Arista Networks 7050S multilayer switch. This test included the validation of data, voice and security protocols commonly used in enterprise networks.

The Aruba and Arista devices exchanged traffic using every protocol tested demonstrating complete interoperability.

Test results validating complete interoperability are summarized in the following table.

Aruba Networks Mobility Access Switch (S3500 and S2500) and Arista Networks 7050S Interoperability			
Interface Connectivity	✓	Port Channels and LACP	✓
VLAN Trunking	✓	Spanning Tree Protocol	✓
Hot Standby Link	✓	LLDP	✓
CDP	✓	DSCP	✓
802.1p	✓	802.1X	✓
MAC	✓	Captive Portal	✓
Tunneled Node	✓	IGMP	✓
IPv4	✓	Aruba Airgroup	✓

Scope and methodology

The illustration below demonstrates the test bed used for the interoperability tests.

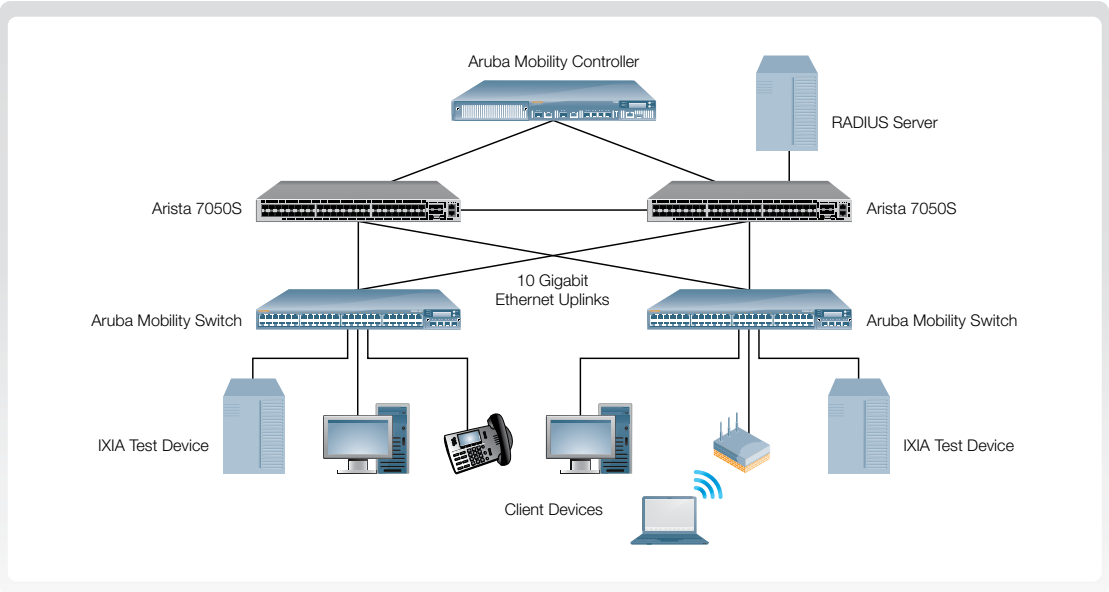

Figure 1. Aruba-Arista interoperability test bed

Interface connectivity

Aruba verified the following 10 Gigabit Ethernet connectivity between the Aruba and Arista switches.

Aruba and Arista 7050S Interface Connectivity	
SFP-10GE-DAC	10 Gigabit Ethernet SFP+ direct attach cable (DAC) with copper Twinax connectors on both ends for ArubaStack or interconnect between servers and switch
SFP-10GE-SR	10GBASE-SR SFP+; 850 nm pluggable 10 Gigabit Ethernet optic; LC connector; up to 300 meters over multimode fiber (Type OM3)
SFP-10GE-LR	10GBASE-LR SFP+; 1,310 nm pluggable 10 Gigabit Ethernet optic; LC connector; up to 10,000 meters over single-mode fiber

Note: Arista 7050S must use Arista-validated fiber optics only. Aruba allows the use of any vendor optics, but will only provide technical assistance for Aruba-validated optics.

Port channels and link aggregation control protocol (LACP)

Aruba tested the ability of Aruba and Arista devices to bundle multiple physical ports into one logical port using the IEEE 802.3ad LACP, using 10 gigabit links.

As shown in Figure 2 below, engineers configured the Aruba and Arista switches to set up dynamic link aggregation groups across multiple physical ports. The Aruba Mobility Access switch used two 10 Gigabit Ethernet links to form a dynamic link aggregation group (LAG) with the Arista 7050S.

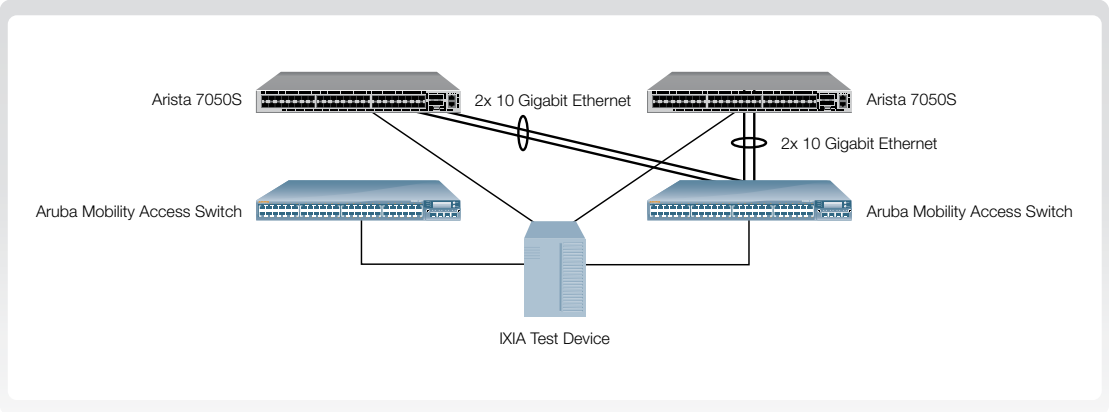

Figure 2. Link aggregation test bed

IXIA offered bidirectional traffic across each dynamic link aggregation group. In all cases, the Aruba and Arista switches correctly forwarded traffic using link aggregation.

VLAN trunking

Aruba tested IEEE 802.1Q VLAN trunking interoperability in three ways: forwarding of allowed tagged traffic; forwarding of allowed untagged (native) traffic; and blocking of disallowed untagged traffic.

Engineers configured eight VLANs on each switch, and configured trunk ports between switches to allow traffic from six VLANs as tagged frames and a seventh VLAN as untagged frames. To determine whether switches would correctly block disallowed traffic, engineers did not include the eighth VLAN ID in the list of VLANs allowed across trunk ports.

IXIA then offered untagged traffic in all VLANs to each Aruba and Arista switch, destined for all other switches. In all cases, traffic counters verified that Aruba and Arista switches correctly forwarded VLAN traffic that was intended to be forwarded, and did not carry VLAN traffic that was not intended to be forwarded. Engineers also captured traffic from a trunk port to verify that all switches forwarded tagged and untagged traffic as expected.

Spanning tree protocol

The spanning tree protocol serves as a key loop prevention and redundancy mechanism in enterprise networks. Over the years it has been refined with updates such as multiple spanning tree (MSTP) to form a separate spanning tree instance for each VLAN.

In addition to the standards-based protocols, Arista switches use proprietary variants called Per-VLAN spanning tree plus (PVST+) and Rapid PVST+.

Engineers verified interoperability using three variations of spanning tree:

Arista 7050S	Aruba Mobility Access Switch
MSTP	MSTP
RSTP	MSTP
Rapid PVST+	MSTP
MSTP	PVST+
RSTP	PVST+
Rapid PVST+	PVST+

In the cases involving PVST+ and Rapid PVST+, VLAN 1 was configured on the Arista switches, while the Aruba Mobility Access Switch was configured with multiple VLANs.

For each variation, engineers set up redundant connections between all switches, and configured spanning tree so that the Arista 7050S would act as the root bridge. Engineers then offered traffic to each switch using IXIA. The results verified spanning tree interoperability by demonstrating that traffic was received from, and only from, the intended ports in forwarding state. Ports placed in blocking state by spanning tree did not forward traffic.

For each combination of spanning tree variants, engineers configured the Aruba Mobility Access Switch to act as the root bridge. This forced the network to converge around new spanning trees (one per VLAN). By examining the command-line interface (CLI) output on each device, engineers verified that all switches agreed that the Mobility Access Switch now acted as root. In all spanning tree test cases, all switches ensured loop-free operation and seamless convergence following configuration changes.

Hot standby link (HSL)

Aruba's HSL technology offers an alternative to spanning tree without the latter protocol's configuration complexity. With HSL, network managers simply define primary and secondary physical ports between switches. If the primary link fails, the switches then redirect traffic onto the secondary port (the hot standby link). Aruba verified that HSL would work between Aruba and Arista switches with no additional configuration needed.

As shown in Figure 3, engineers set up HSL by redundantly connecting the Aruba Mobility Access Switch to the Arista 7050S.

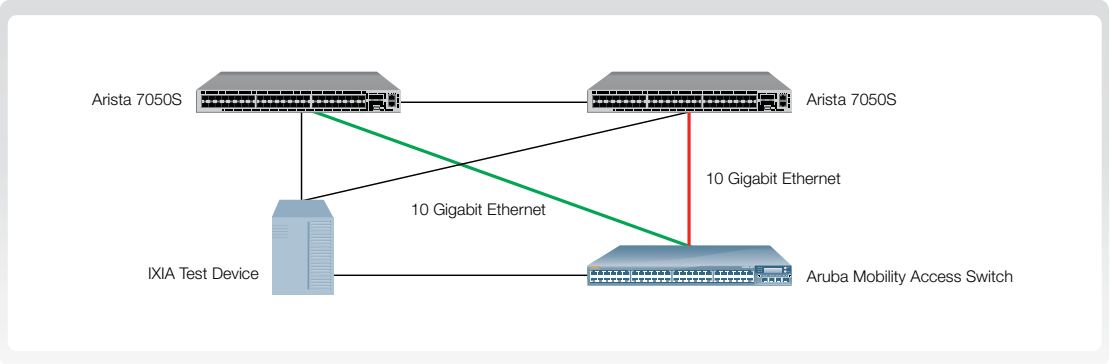

Figure 3. Hot standby link test bed

Engineers then offered traffic between Aruba and Arista switches, and observed traffic being forwarded only on primary links. Next, they physically disconnected the primary link on the Aruba switch, and verified that the switches continued to forward traffic on the secondary links. No extra configuration was needed on the Arista switches. HSL correctly forwarded traffic both before and after a link failure. Engineers then repeated this exercise with a primary link to an Arista switch. Again, HSL failed over from primary to secondary links, allowing traffic to continue to flow.

Link layer discovery protocol (LLDP)

Link Layer Discovery Protocol (LLDP), defined in the IEEE 802.1AB standard, is a Layer 2 protocol that allows network devices to advertise their identity and capabilities on a LAN. The Mobility Access Switch supports a simple one-way neighbor discovery protocol with periodic transmissions of LLDP PDU.

Aruba validated the following LLDP TLVs (type-length-value).

Verified LLDP TLVs	
Chassis Subtype	Capabilities
Port Subtype	Management Address
Time to Live	Port Description
System Name	Port VLAN ID
System Description	VLAN Name

Aruba Mobility Access Switch can also recognize Arista 7050S as a neighbor.

Cisco discovery protocol (CDP)

The proprietary Cisco Discovery Protocol (CDP) allows sharing of information, such as IP address, model number and power requirements, among connected Cisco devices.

Aruba verified the ability of the Aruba Mobility Access Switch and Arista 7050S switches to pass-through CDP data between two connected Cisco devices. Transport of this information was validated by connecting CDP on two Aruba Mobility Switches and locally attaching Cisco VoIP phones.

Quality of service (DSCP and 802.1p)

Voice, video, and other delay-sensitive applications make heavy use of quality-of-service (QoS) mechanisms such as the Differentiated Services Code Point (DSCP) and 802.1p (for non-IP tagged frames) to ensure timely traffic delivery. Switches can change the DSCP/802.1p field in the IP header of incoming packets, ensuring these packets will receive special treatment as they pass through upstream devices. For example, a switch might change the value for incoming voice packets to ensure high-priority forwarding, which in turn keeps latency low.

To verify the ability of the Aruba Mobility Access Switch to remark DSCP/802.1p values, engineers set up separate VLANs for voice and data, and also configured the Aruba switch to mark all voice traffic with a DSCP value of 46 (which represents expedited forwarding, a common high-priority treatment) and a value of 5 in the case of 802.1p. The IXIA test instrument then offered traffic to both VLANs, in both cases with a value of 0. Engineers then captured traffic on the destination ports to determine if the Aruba switch had remarked the field.

The Aruba switch correctly remarked voice traffic with the expected DSCP and 802.1p values. As expected, the Aruba switch did not remark traffic in the data VLAN.

802.1X authentication

Network access control (NAC) introduces a new concept in enterprise network security. With NAC, the identity of a user, and not that of a machine or switch port, governs what resources the user can reach. NAC greatly enhances mobility within the enterprise by allowing users to attach anywhere within the network and still enjoy the same access rights.

A fundamental building block of NAC is the IEEE 802.1X protocol, in which supplicants (clients) supply login credentials to an authenticator (such as an access switch), which in turn relays these credentials to an authentication server (typically a RADIUS server, which may be tied to a user database such as Microsoft Active Directory).

As shown in Figure 4 below, Aruba validated 802.1X interoperability using a configuration commonly found in enterprise networks running Microsoft Windows. A Windows 2003 server acted as Active Directory (AD) domain controller and also ran Internet Authentication Services (IAS) to tie AD credentials to RADIUS requests. On the client side, a PC running Windows 7 Ultimate Edition sent an 802.1X authentication request to gain access to the network. The client attached to an 802.1X-enabled Aruba Mobility Access Switch, which linked to an Arista switch, which in turn connected to the Windows server.

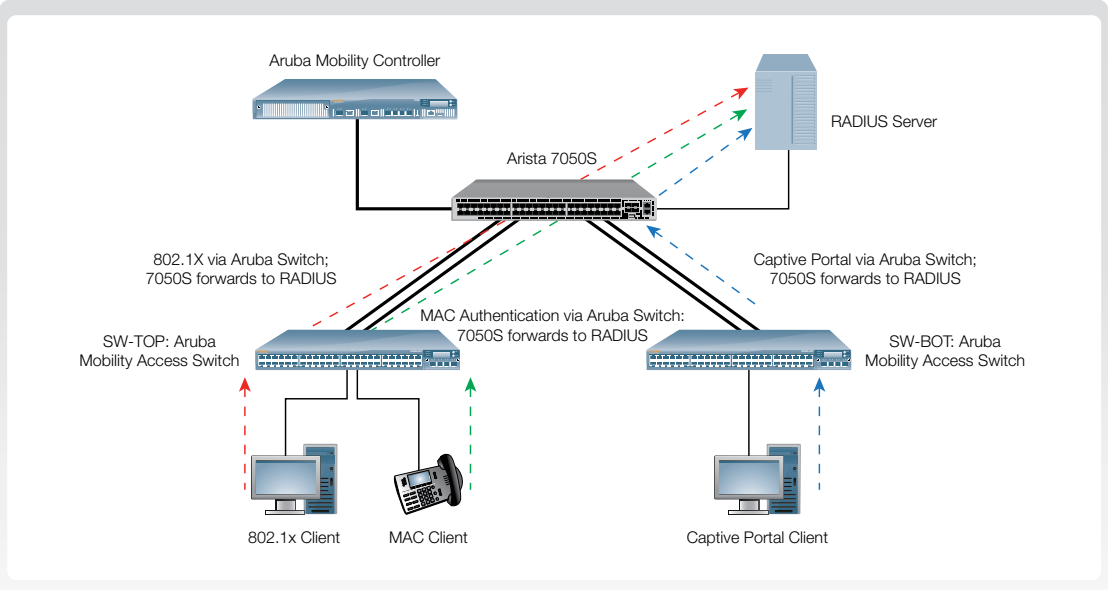

Figure 4. 802.1X, MAC authentication, and captive portal test bed

In all test cases, the Aruba Mobility Access Switch and Arista switch worked together to process a valid 802.1X request from a user. The user was then able to reach network resources as defined by the Windows server's group policy. The engineers also conducted negative tests with invalid user password credentials; here, the Aruba switch correctly relayed RADIUS rejection messages. .

MAC authentication

MAC authentication provides a way for clients to reach enterprise network resources based on source MAC address. This allows networked printers, web cameras, and legacy devices that may lack 802.1X authentication capabilities to take part in a NAC-enabled network.

To validate MAC authentication, engineers disabled 802.1X support on the client PC running Windows 7, and then reconfigured the RADIUS server to use the PC's MAC address for authentication.

The Aruba Mobility Access Switch was able to authenticate the attached client via MAC authentication through a core network comprised of Arista 7050S switches.

Captive access portal

Since Network Access Control (NAC) is based on user identity, different classes of users may reach different resources. Aruba validated support for this capability during tests of tunneled node with role-based authentication. Engineers defined authenticated and guest user roles, with different VLANs and access rights for each. In particular, engineers configured guest access requests to be redirected to a captive-portal web page running on the Aruba controller.

Engineers then attempted to authenticate authorized and guest users via the same switch port. The system correctly granted full access to authenticated users, and redirected guest users to a captive-access portal running on the Aruba controller. The system correctly placed authenticated and guest users in different VLANs.

Tunneled node authentication

One possible drawback of NAC is that it requires 802.1X support on the authenticator, requiring configuration of every access switch (or even replacement of access switches if they lack 802.1X capability). Aruba offers an alternative: Tunneled node with role-based authentication.

As shown in Figure 5, a single Aruba Mobility Controller can act as authenticator for an entire enterprise. The Aruba controller sets up tunneled node using generic routing encapsulation (GRE) between itself and the Aruba Mobility Access Switch, with no requirement for 802.1X awareness on the Aruba Switch.

With tunneled node in place, devices along the path between authenticator (the controller) and supplicant (the client) do not require any 802.1X awareness or support. Tunneled node with role-based authentication enhances the ability to scale up 802.1X authentication without the requirement to support 802.1X on every access switch.

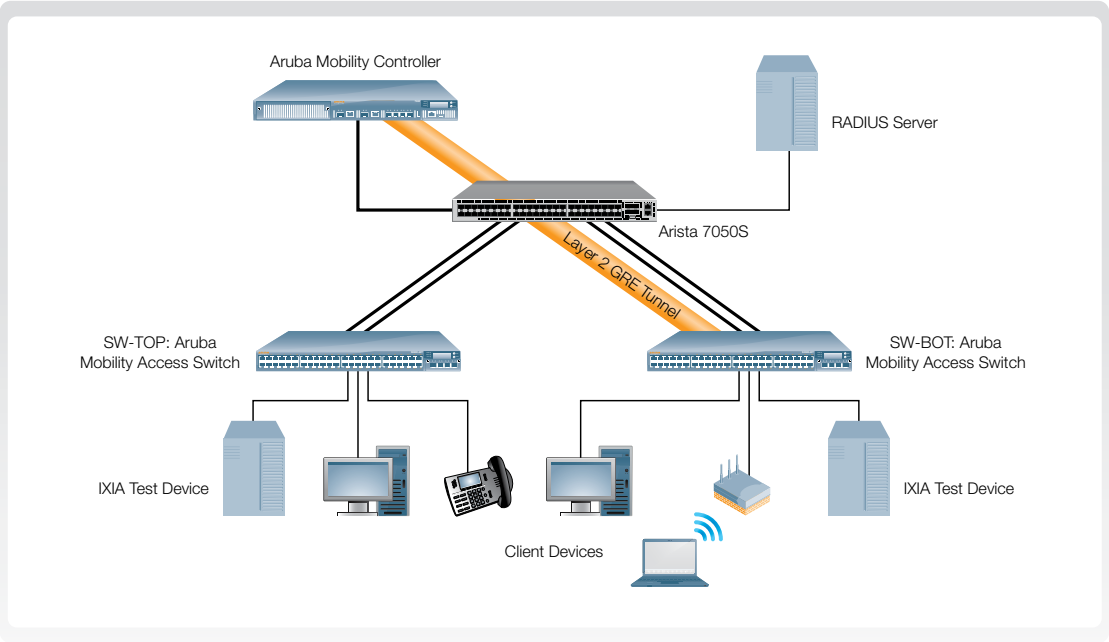

Figure 5. Tunneled node authentication test bed

To validate tunnel-node authentication, engineers set up a tunneled node between an Aruba controller and a Mobility Access Switch with an Arista 7050S inline between the Aruba devices.

In all test cases, tunneled node with role-based authentication correctly granted access via 802.1X authentication across a network made up of Aruba and Arista switches. No 802.1X or GRE configuration was required on any of the Arista switches.

Internet group management protocol (IGMP) snooping

With enterprises making ever-greater use of IP multicast for everything from videoconferencing to routing protocol updates, IGMP snooping has become a critical feature in enterprise switching. Aruba engineers validated the ability of Aruba and Arista switches to share information about multicast topology in a hybrid switched/routed multicast environment.

In this scenario, engineers configured the Aruba Mobility Access Switch in layer-2 switching mode, with IGMP snooping enabled. Engineers then configured the Arista switch in layer-3 routing mode, running the Protocol Independent Multicast-Sparse Mode (PIM-SM) routing protocol.

This setup represents a common design in enterprise networks: One access switch (Aruba Mobility Access Switch) receives multicast traffic from multiple routers (Arista switches), and then uses IGMP snooping to determine where the multicast traffic should be forwarded.

An IXIA port attached to each Arista switch offered traffic destined to 10 multicast groups, while other test ports emulated multicast subscribers on the Aruba Mobility Access Switch. Engineers also attached an additional monitor port to the Aruba switch to verify it did not flood multicast frames to non-subscriber ports.

The Aruba and Arista devices correctly delivered multicast traffic to subscribers in all groups, and did not flood traffic to non-subscriber ports.

Internet protocol version 4 (IPv4)

IPv4 is a protocol for relaying packets across connected networks where network devises are assigned 32-bit addresses. For the interoperability test with Arista 7050S, Aruba connected the uplink module on the Mobility Access Switch, and created a Layer 3 adjacency between the Arista switch and enabled Open Shortest Path First (OSPF) on both the switches.

Aruba Networks validated OSPF adjacency between the Aruba Mobility Access Switch and the Arista 7050S in the following areas: Backbone, normal, stub, totally stubby, and not-so-stubby area (NSSA). Additionally, MD5 authentication tested between the two switches was also validated.

Aruba AirGroup integration (L2GRE)

Aruba AirGroup is a unique enterprise-class capability that leverages zero configuration networking to allow mobile devices to use services like the Apple AirPrint wireless printer service and the Apple AirPlay streaming service. These services use multicast DNS (mDNS) packets to locate devices and the services that those devices offer.

Ensuring that wired and wireless AirPrint- and AirPlay-enabled devices could communicate with one another previously required all devices to be on the same Layer 2 network which may not be desirable. AirGroup avoids that need by enabling the Aruba Mobility Access Switch to redirect mDNS traffic to an Aruba Mobility Controller regardless of VLAN. A simple rule on the Mobility Access Switch is used to redirect all incoming mDNS packets on a port to a Layer 2 GRE tunnel, which is then terminated on a Mobility Controller. This allows the Mobility Controller to handle the rest of the AirGroup functionality.

Aruba verified that the mDNS traffic was forwarded from the Mobility Switch through Arista 7050S switches in the core directly to a Mobility Controller.

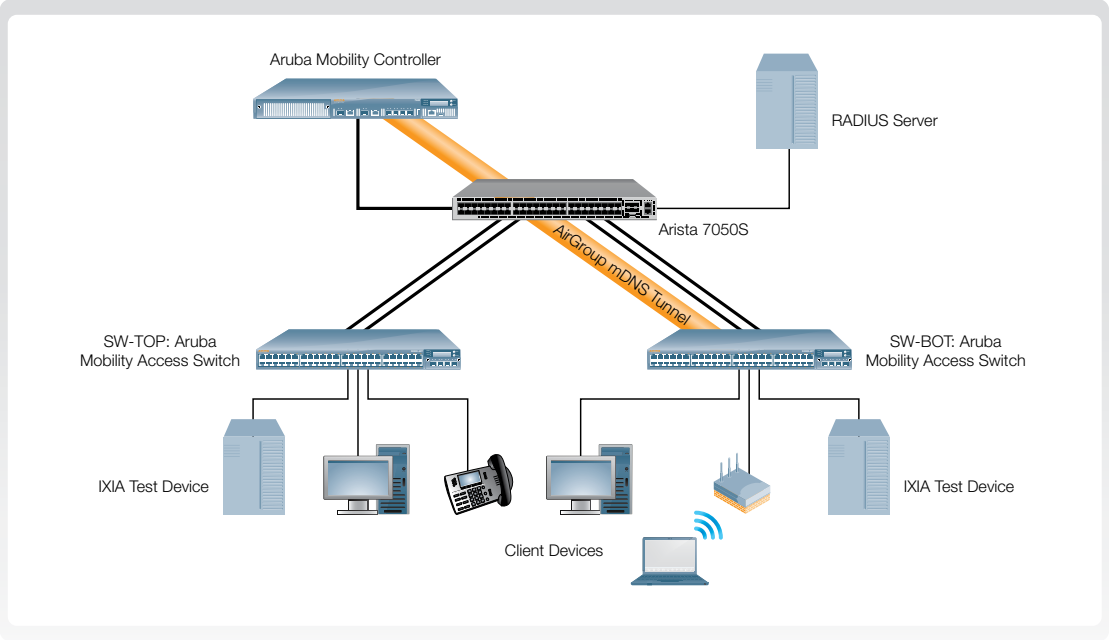

Figure 6. Aruba AirGroup – layer 2 GRE integration test bed

Conclusion

These tests validated interoperability in every case where both Aruba and Arista devices supported a given protocol. Some test cases, such as those involving two spanning tree variants, also demonstrated interoperability between standards-based and proprietary protocols.

Successful interoperability testing provides assurance to network professionals considering design or deployment of networks comprised of a mix of Aruba and Arista devices.

About Aruba Networks, Inc.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company's Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks enables IT organizations and users to securely address the Bring Your Own Device (BYOD) phenomenon, dramatically improving productivity and lowering 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, Africa and Asia Pacific regions. To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com.

ARUBA networks

www.arubanetworks.com

1344 Crossman Avenue. Sunnyvale, CA 94089

1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com