
networktest

Aruba S3500/Cisco Catalyst Interoperability Test Results

September 2011

Aruba/Cisco Interoperability Test Results

Executive Summary

Aruba Networks commissioned Network Test to assess interoperability between its S3500 Mobility Access Switch and switches from Cisco Systems. Working with a test bed that included core-, distribution-, and access-layer switches, Network Test validated the interoperability of 13 data, voice, and security protocols commonly used in enterprise networks.

The Aruba and Cisco devices exchanged traffic using every protocol tested. In other words, testing demonstrated complete interoperability.

The following table summarizes the results of interoperability tests.

| Aruba Networks / Cisco Systems Protocol Interoperability | | | |
|--|---------------------------|---|---|
| Aruba S3500 Mobility Access Switch | | Aruba S3500 Mobility Access Switch | |
| VLAN trunking | | Diff-serv codepoint remarking | |
| Cisco Catalyst 3750 | ✓ | Cisco Catalyst 3750 | ✓ |
| Cisco Catalyst 4506 | ✓ | Cisco Catalyst 4506 | ✓ |
| Cisco Catalyst 6506 | ✓ | Cisco Catalyst 6506 | ✓ |
| Multiple spanning tree protocol (MSTP) | | Link aggregation | |
| Cisco Catalyst 3750 | ✓ | Cisco Catalyst 3750 | ✓ |
| Cisco Catalyst 4506 | ✓ | Cisco Catalyst 4506 | ✓ |
| Cisco Catalyst 6506 | ✓ | Cisco Catalyst 6506 | ✓ |
| MSTP (Aruba) / PVST+ (Cisco on VLAN 1) | | VoIP using LLDP-MED | |
| Cisco Catalyst 3750 | ✓ | Cisco Catalyst 3750 | ✓ |
| Cisco Catalyst 4506 | ✓ | Cisco Catalyst 4506 | ✓ |
| Cisco Catalyst 6506 | ✓ | Cisco Catalyst 6506 | ✓ |
| MSTP (Aruba) / Rapid PVST+ (Cisco on VLAN 1) | | 802.1X authentication (S3500 as authenticator) | |
| Cisco Catalyst 3750 | ✓ | Cisco Catalyst 3750 | ✓ |
| Cisco Catalyst 4506 | ✓ | Cisco Catalyst 4506 | ✓ |
| Cisco Catalyst 6506 | ✓ | Cisco Catalyst 6506 | ✓ |
| Aruba Hot Standby Link (HSL) | | Tunneled node with role-based authentication | |
| Cisco Catalyst 3750 | ✓ | Cisco Catalyst 3750 | ✓ |
| Cisco Catalyst 4506 | ✓ | Cisco Catalyst 4506 | ✓ |
| Cisco Catalyst 6506 | ✓ | Cisco Catalyst 6506 | ✓ |
| IGMP snooping | | MAC authentication | |
| Cisco Catalyst 3750 | ✓ | Cisco 7942G phone | ✓ |
| Cisco Catalyst 4506 | ✓ | Aruba AP-105 access point | ✓ |
| Cisco Catalyst 6506 | ✓ | Aruba AP-135 access point | ✓ |
| Power over Ethernet (PoE)/PoE+ | | | |
| | Cisco 7942G IP phone | ✓ | |
| | Aruba AP-135 access point | ✓ | |
| | Aruba AP-135 access point | ✓ | |

Methodology and Results

Figure 1 below illustrates the test bed used to validate interoperability for most tests.

The interoperability test bed used a three-tier design commonly found in enterprise campus networks, with separate devices at the core (Catalyst 6506), distribution (Catalyst 4506), and access layers (Cisco Catalyst 3750 and Aruba S3500 Mobility Access Switch). A Spirent TestCenter traffic generator/analyzer emulated clients and servers, and externally verified interoperability of the various protocols.

Except where otherwise noted, tests involved connections between each layer of the network, validating interoperability of each protocol using every device on the test bed. Aruba Networks supplied all Aruba and Cisco equipment for this project.

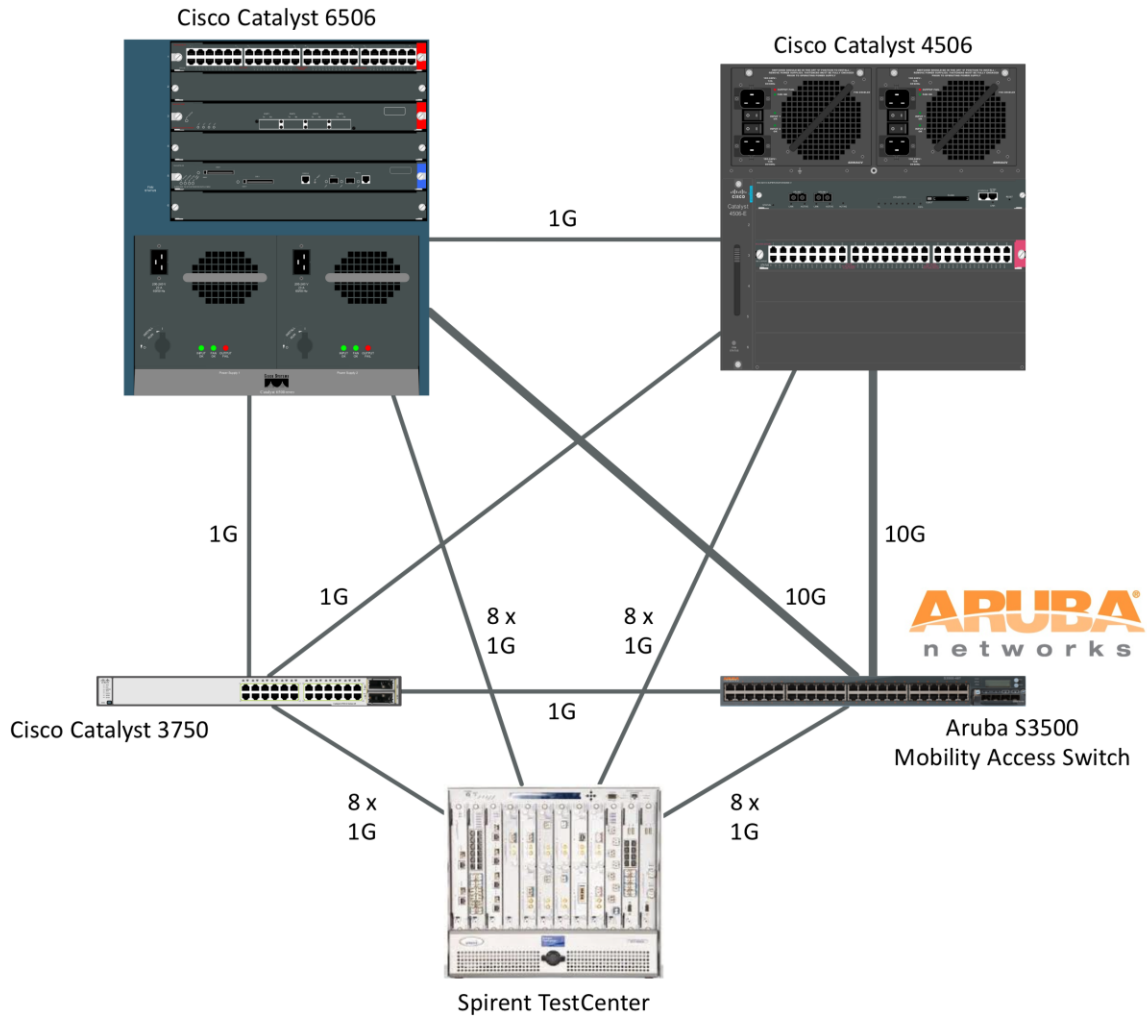


Figure 1: The Aruba-Cisco Interoperability Test Bed

Aruba/Cisco Interoperability Test Results

VLAN Trunking

Network Test evaluated 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.

Spirent TestCenter then offered untagged traffic in all VLANs to each Aruba and Cisco switch, destined for all other switches. In all cases, traffic counters on the Spirent test instrument verified that **Aruba and Cisco 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.**

Multiple Spanning Tree Protocol (MSTP)

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, Cisco switches use proprietary variants called per-VLAN spanning tree plus (PVST+) and Rapid PVST+.

Network Test verified interoperability using three variations of spanning tree:

1. MSTP (Aruba and Cisco, using the IEEE 802.1s specification)
2. MSTP (Aruba) / PVST+ (Cisco)
3. MSTP (Aruba) / Rapid PVST+ (Cisco)

In the cases involving PVST+ and Rapid PVST+, VLAN 1 was configured on the Cisco switches, while the Aruba S3500 was configured with multiple VLANs.

For each variation, engineers set up redundant connections between all switches, and configured spanning tree so that the Cisco Catalyst 6506 would act as the root bridge. Engineers then offered traffic to each switch using Spirent TestCenter. **The results verified spanning tree interoperability by demonstrating that 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 then configured the Aruba S3500 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

Aruba/Cisco Interoperability Test Results

Network Test then offered traffic between Aruba and Cisco switches, and observed traffic being forwarded only on primary links. Next, engineers physically disconnected the primary link on the Aruba switch, and Network Test verified that the switches continued to forward traffic on the secondary links. **No extra configuration was needed on the Cisco switches. HSL correctly forwarded traffic both before and after a link failure.** Network Test then repeated this exercise with a primary link to a Catalyst 3750 switch. Again, HSL failed over from primary to secondary links, allowing traffic to continue to flow

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. Network Test validated the ability of Aruba and Cisco switches to share information about multicast topology in a hybrid switched/routed multicast environment.

In this scenario, engineers configured the Aruba S3500 Mobility Access Switch in layer-2 switching mode, with IGMP snooping enabled. Engineers then configured the three Cisco switches 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 (the Aruba device) receives multicast traffic from multiple routers (the Cisco devices), and then uses IGMP snooping to determine where the multicast traffic should be forwarded.

A Spirent TestCenter port attached to each Cisco device offered traffic destined to 10 multicast groups, while other test ports emulated multicast subscribers on the Aruba S3500 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 Cisco devices correctly delivered multicast traffic to subscribers in all groups, and did not flood traffic to non-subscriber ports.

Diff-Serv Codepoint Remarking

Voice, video, and other delay-sensitive applications make heavy use of quality-of-service mechanisms such as the diff-serv codepoint (DSCP) to ensure timely traffic delivery. Switches can change the DSCP field in the IP header of incoming packets, ensuring these packets will receive special treatment as they pass through upstream devices¹. For example, a switch might change the DSCP value for incoming voice packets to ensure high-priority forwarding, which in turn keeps latency low.

To verify the ability of the Aruba S3500 Mobility Access Switch to remark DSCP values, engineers set up separate VLANs for voice and data, and also configured the Aruba switch to mark all voice traffic with a

¹ [RFCs 2474](#) and [2475](#) define DSCP. [RFC 3246](#) defines Expedited Forwarding.

Aruba/Cisco Interoperability Test Results

DSCP value of 46 (which represents Expedited Forwarding, a common high-priority treatment). The Spirent TestCenter test instrument then offered traffic to both VLANs, in both cases with a DSCP value of 0. Engineers then captured traffic on the destination ports to determine if the Aruba switch had remarked the DSCP field in voice packets using a value of 46.

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

Link Aggregation

Network Test evaluated the ability of Aruba and Cisco devices to bundle multiple physical ports into one logical port using the IEEE 802.3ad link aggregation protocol, both on gigabit and 10-gigabit links.

As shown in Figure 3 below, engineers configured the Aruba and Cisco switches to set up link aggregation groups (LAGs) across multiple physical ports. The Aruba S3500 Mobility Access switch used two 10-gigabit Ethernet links to form a single link aggregation group (LAG) with the Cisco Catalyst 6506. The Aruba switch also established LAGs using two gigabit Ethernet links apiece with each of the three Cisco switches.

Spirent TestCenter offered bidirectional traffic across each LAG. **In all cases, the Aruba and Cisco switches correctly forwarded traffic using link aggregation.**

Aruba/Cisco Interoperability Test Results

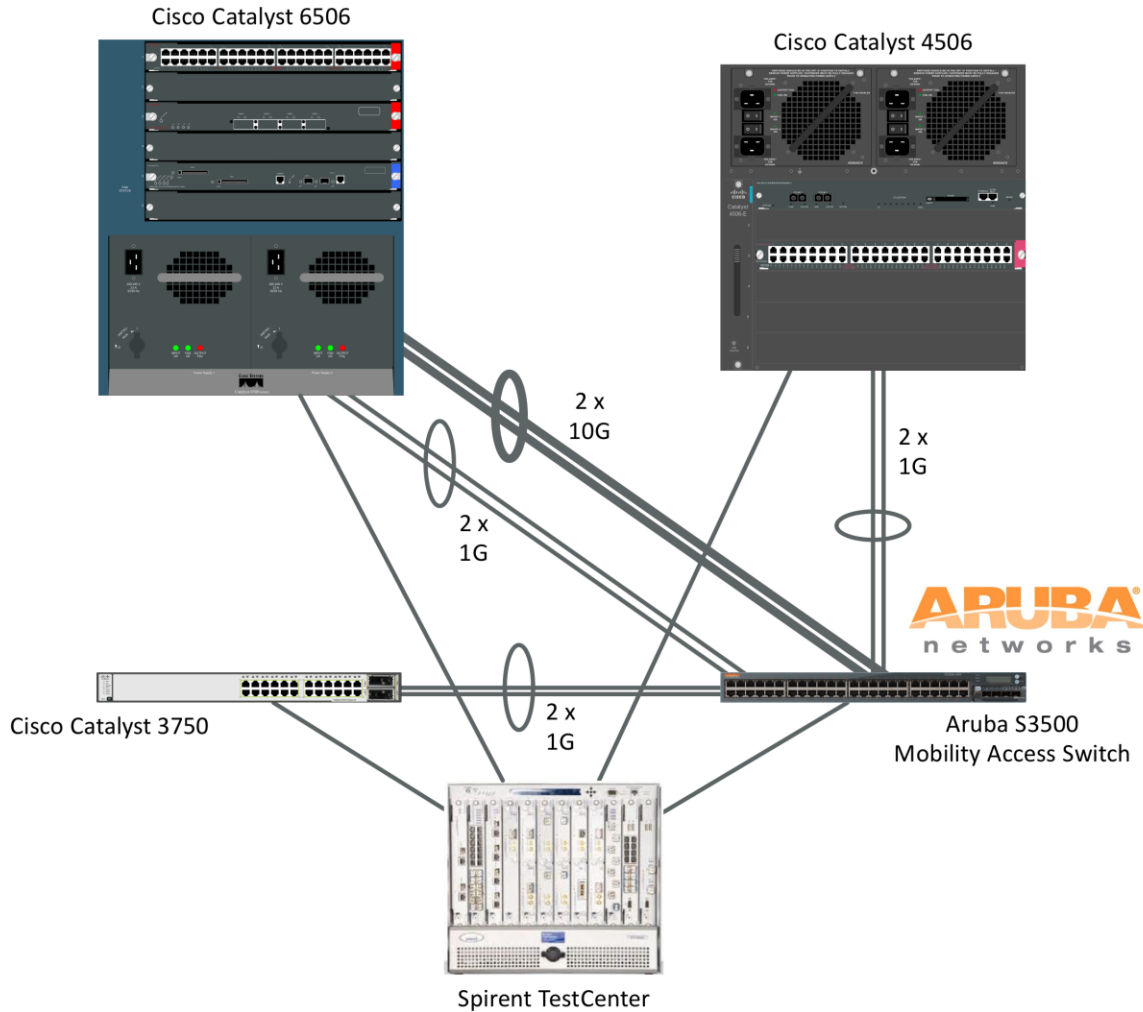


Figure 3: Link Aggregation Test Bed

VoIP Using LLDP-MED

The Media Endpoint Discovery extensions to the logical-link discovery protocol (LLDP-MED) offer a means by which end-stations can automatically learn configuration and policy settings. A common use case for LLDP-MED in enterprise settings is voice over IP: When IP phones attach to a network, they can use LLDP-MED to learn VLAN IDs and other networking parameters.

Network Test validated the ability of an Aruba switch and Cisco phones to exchange LLDP-MED messages using Cisco IP phones and a Cisco PBX, as shown in Figure 4 below. In each test, engineers attached two Cisco 7942G IP phones to an Aruba S3500 Mobility Access Switch. **The Cisco phones obtained network policy such as voice VLAN information via LLDP-MED exchanges with the Aruba switch**, which in turn allowed the phones to register with a Cisco Unified Communication Manager

Aruba/Cisco Interoperability Test Results

Express (CUCME) feature running on a Cisco 2901 Integrated Services Router. After the phones had registered with the PBX, engineers verified correct operation of LLDP-MED by using the port-mirroring functionality of the Aruba S3500 switch, and also by placing a call between phones.

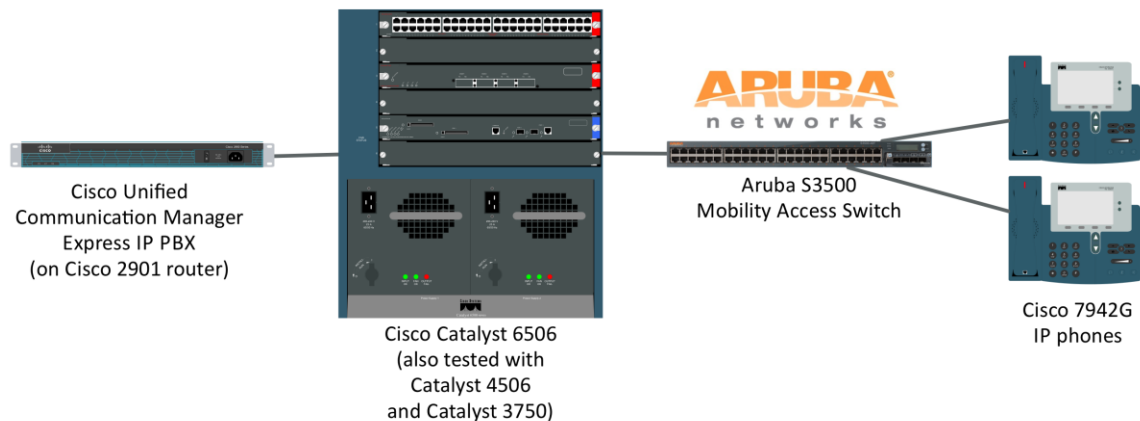


Figure 4: VoIP Interoperability Using LLDP-MED

Engineers repeated the test three times, swapping in the Catalyst 6506, Catalyst 4506, and Catalyst 3750 as the device linking the Aruba switch and the Cisco 2901 equipped with CUCME. **In all test cases, the Aruba switch and Cisco IP phones successfully used LLDP-MED to establish connectivity.**

802.1X Authentication (S3500 as Authenticator)

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 5 below, Network Test 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/Cisco Interoperability Test Results

Aruba S3500 Mobility Access switch, which linked to a Cisco switch, which in turn connected to the Windows Server. (Engineers reran this test with Cisco Catalyst 6506, Catalyst 4506, and Catalyst 3750 switches between the Aruba switch and the Windows server).

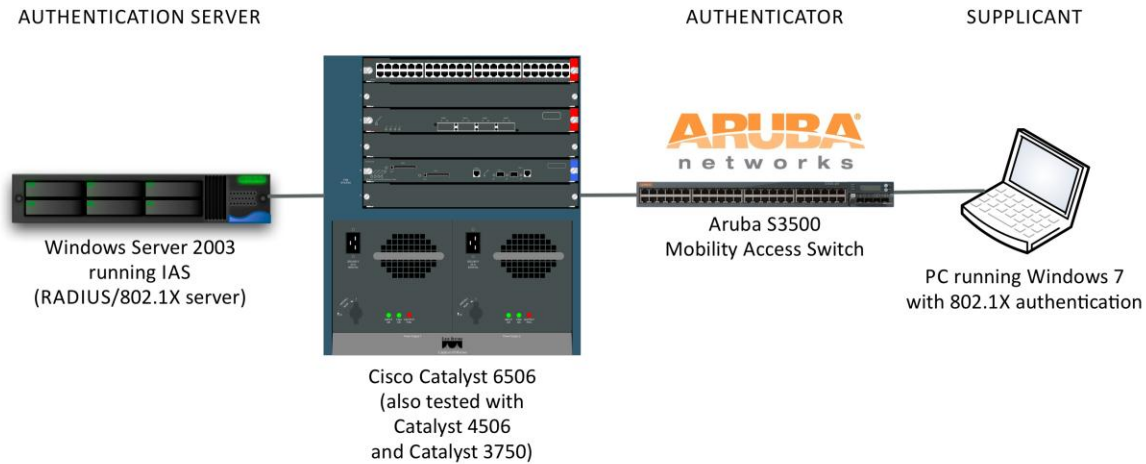


Figure 5: The 802.1X Test Bed

In all test cases, the Aruba S3500 Mobility Access Controller and Cisco switches 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. Network Test also conducted negative tests with invalid user password credentials; here, the Aruba switch correctly relayed RADIUS rejection messages.

Tunneled Node With Role-Based 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 Networks offers an alternative: **tunneled node with role-based authentication**. As shown in Figure 6 below, a single Aruba 3600 Mobility Controller can act as authenticator for an entire enterprise. The Aruba 3600 sets up tunneled node using generic routing encapsulation (GRE) between itself and the Aruba S3500, with no requirement for 802.1X awareness on the S3500.

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.

Aruba/Cisco Interoperability Test Results

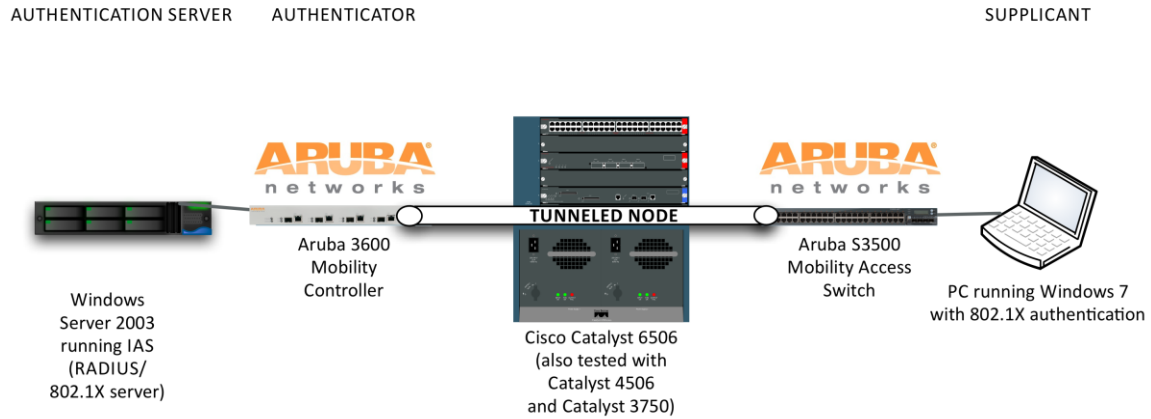


Figure 6: Tunnelled-Node Authentication

To validate tunnel-node authentication, engineers set up a tunneled node between an Aruba 3600 controller and S3500 switch with a Cisco switch inline between the Aruba devices. Network Test repeated this exercise three times, swapping in the Catalyst 6506, Catalyst 4506, and Catalyst 3750 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 Cisco switches. No 802.1X or GRE configuration was required on any of the Cisco switches.

Because NAC is based on user identity, different classes of users may reach different resources. Network Test 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 3600 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.**

MAC Authentication

Just as tunneled node with role-based authentication removes the requirement for 802.1X support on every access switch, MAC authentication provides a way for supplicants (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.

Aruba/Cisco Interoperability Test Results

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.

MAC authentication correctly granted access to a client with no 802.1X support. In a negative test case, MAC authentication did not grant access to a client supplying the wrong MAC address.

Power Over Ethernet/PoE+

The IEEE power over Ethernet (PoE) and PoE+ standards describe a method for supplying power as well as data via Ethernet ports. The standards, which supply up to 15.4 and 30 watts per port respectively², offer an ideal method for connecting Wi-Fi access points, IP phones, and other devices that might otherwise require separate power infrastructure.

Aruba asked Network Test to verify this functionality by attaching multiple PoE and PoE+ devices to an Aruba S3500 Mobility Access Switch. These devices included an Aruba AP-105 access point and two Cisco 7942G IP phones, both PoE-capable; and an Aruba AP-135 access point, which supports both PoE and the newer PoE+ specification. (The AP-135 requires PoE+ mode only when it uses both gigabit Ethernet interfaces.) **In all test cases, the Aruba switch correctly supplied power to attached access points and IP phones.**

Conclusion

These tests achieved interoperability in every case where both Aruba and Cisco 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 Cisco devices.

² IEEE specifications 802.3af-2003 and 802.3at-2009 describe PoE and PoE+ respectively. The 15.4- and 30-watt limits describe power at the source (in this case, the access switch); the maximum power supplied to devices is 12.95 and 25.5 watts for PoE and PoE+ devices, respectively, to account for power attenuation in the cable plant.

Appendix A: About Network Test

Network Test is an independent third-party test lab and engineering services consultancy. Our core competencies are performance, security, and conformance assessment of networking equipment and live networks. Our clients include equipment manufacturers, large enterprises, service providers, industry consortia, and trade publications.

Appendix B: Software Releases Tested

This appendix describes the software versions used on the test bed. All tests were conducted in August and September 2011 at Network Test's facility in Westlake Village, CA, USA. Aruba Networks supplied all Aruba and Cisco devices used in testing.

| Component | Version |
|---------------------------------------|-----------------------------|
| Aruba S3500 Mobility Access Switch | ArubaOS 7.0.2.0 build 29560 |
| Aruba 3600 Mobility Controller | ArubaOS 6.1.2.2 build 29487 |
| Aruba AP-105 | ArubaOS 6.1.2.2 build 29487 |
| Aruba AP-135 | ArubaOS 6.1.2.2 build 29487 |
| Cisco Catalyst 6506 | 12.2(33)SXJ |
| Cisco Catalyst 4506 | 12.2(54)SG |
| Cisco Catalyst 3750 | 12.2(55)SE1 |
| Cisco 2901 Integrated Services Router | 15.0(1)M5 |
| Cisco 7942G | 8.3(3)SR2S |
| Spirent TestCenter | 3.62.0686.0000 |

Appendix C: Disclaimer

Network Test Inc. has made every attempt to ensure that all test procedures were conducted with the utmost precision and accuracy, but acknowledges that errors do occur. Network Test Inc. shall not be held liable for damages, which may result for the use of information contained in this document. All trademarks mentioned in this document are property of their respective owners.



Version 2011092600. Copyright 2011 Network Test Inc. All rights reserved.

Network Test Inc.

31324 Via Colinas, Suite 113
Westlake Village, CA 91362-6761
USA
+1-818-889-0011
<http://networktest.com>
info@networktest.com