Voice Over IP and Wireless Data Coexistence in a WLAN Switch Deployment

Introduction

Wireless technology is becoming increasingly integrated into the world's networks. Recent innovations, such as offloading processing to wireless local area network (WLAN) switches at the network's edge, have cleared the way for large-scale enterprise deployments. However, despite improved maintenance and administration tools, switched WLAN networks are vulnerable to issues arising from the heterogeneous network environment, especially the integration of services such as voice over IP (VoIP). Because VoIP services are in demand in professional settings, it is imperative to enterprise adoption that wireless data and sensitive VoIP streams can coexist in a WLAN switch system.

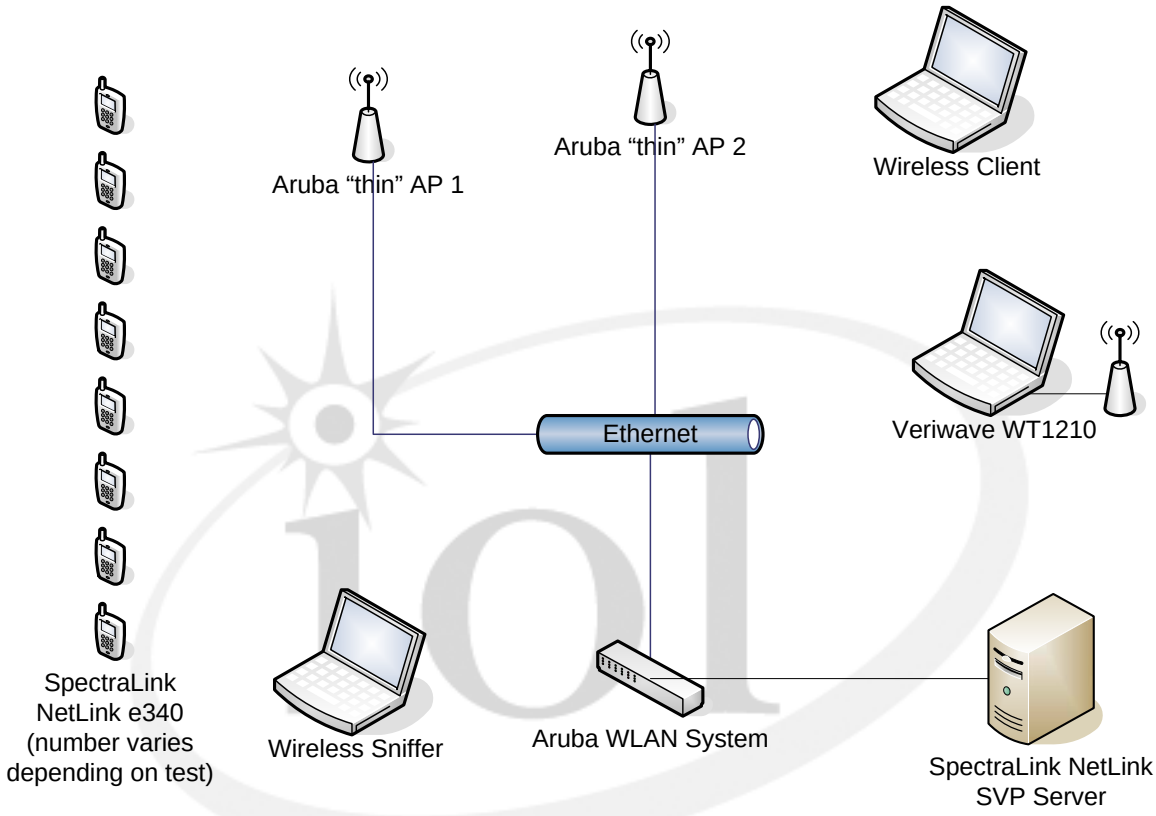
Wireless companies are working to solve these and other professional deployment issues and including new solutions in their WLAN switch implementations. An open-industry enterprise services and security test event held from March 21 to March 25, 2005 at the University of New Hampshire InterOperability Laboratory (UNH-IOL) provided a backdrop for testing these solutions. This test brought VoIP and wireless companies to the UNH-IOL facility in Durham, N.H. to build a deployment-style, multi-vendor network that foregrounded VoIP and wireless data coexistence issues arising from the combination of these two powerful networking mediums.

Overview

All of the tests in this report employ the network topology depicted on the following page, which was designed to verify that the participating companies' wireless solutions would perform optimally in a real-world environment. For the testing, the UNH-IOL used a variety of equipment supplied by participating vendors including Aruba Networks' mobility controllers (Aruba's 2400 and 5000 systems) and 802.11a/b/g access points (Aruba AP 61), Veriwave's WT1210 WaveTest 802.11a,g,g traffic generator / Performance Analyzer, SpectraLink NetLink e340 wireless telephones, and a SpectraLink NetLink SVP Server. As with most WLAN switch setups, the Aruba APs are "ultra thin" APs that interacted with wireless and VoIP devices as any AP would, but also forwarded all traffic over a secure GRE tunnel to the Aruba mobility controller for processing. The wireless testing device allowed testers to perform certain tests by doing special tasks such as simulating a wireless client, generating different types of traffic, and measuring throughput values for both VoIP and wireless devices. The March 2005 test event included devices implementing all of the following solutions to wireless/VoIP integration.

Various wireless companies have broached the problem of the coexistence of voice streams and wireless data in WLAN switch systems with the ability to distinguish the different traffic types in VoIP and regular wireless data. Devices with this feature are referred to as "session aware." These session aware switches keep the actual state of each

connection, tracking what TCP/UDP port that is being being used. They are also able to distinguish between different traffic types such as VoIP from regular wireless data, keeping the two separate to ensure no crossover between them. Session awareness also prevents VoIP clients from accessing data streams and data devices from accessing VoIP streams. Aruba's session-aware system, for example, is able to allow only certain traffic types, such as SIP or H.323, across a discrete SSID. Other traffic is denied and the device trying to access the SSID can be automatically blacklisted.



Most WLAN switching systems employ a solution known as "application aware" functionality. This allows the WLAN switch to monitor all ports in the network. The WLAN switch can then turn on/off certain ports as they are needed. This capability enhances security, and greatly decreases the chance of unwanted access through open ports.

The application aware and session aware functionalities are general networking solutions that help optimize network performance at many levels in various ways. The session aware functionality, for example, can be used in WLAN switch implementations to provide an enhanced radio frequency (RF) scanning feature. Routine RF scanning is a method whereby an AP in a WLAN switch implementation will enter into listening mode long enough for the network to scan the RF spectrum for clearer channels, identify traffic abmormalities or protect against rogue devices. However, going "off-channel" even for a moment, can cause a noticeable drop in voice quality. Therefore, many WLAN switch

implementations disable RF scanning when integrating VoIP devices. This, in turn, compromises overall network efficiency and security.

Advanced systems can enable adaptive RF management to detect which light APs are engaged in VoIP data transmission. This "voice-aware scanning" allows the WLAN switch to postpone the scanning operations on these APs while the other APs on the system will enter the monitoring / scanning mode as per the AP's schedule. This preserves the integrity of VoIP traffic without compromising network maintenance and security.

Session awareness is also used to solve additional issues with VoIP/wireless coexistence. Typically wireless data and VoIP traffic are kept on separate APs/SSIDs for ease of administration. However, there are scenarios (eg. Soft phones on laptops or Wi-Fi enabled cellular phone) when VoIP and wireless devices will be together on the same AP/SSID. This is commonly referred to as the "converged network." This type of network must give VoIP traffic priority to maintain sufficient voice quality. The session aware functionality allows the WLAN switch to distinguish VoIP traffic from wireless data and give it priority. Thus, again, coexistence is achieved without sacrificing voice quality.

Because VoIP traffic streams are so sensitive, many devices incorporate a setting that limits the maximum number of allowable VoIP devices and calls. "Call load balancing" features built into these next generation WLAN systems automatically force a VoIP device to roam to another AP within the WLAN domain if a maximum pre-defined threshold is reached.

Similarly, client blacklisting furthers protect sensitive VoIP traffic streams by not allowing clients that violate the policy of a certain AP/SSID access to the WLAN. Thus, as previously mentioned, any client configured only for VoIP traffic that attempts to send wireless data traffic or any data client trying to spoof a voice device with be blacklisted and denied access to the network. The client will remain blacklisted until an administrator removes it.

The UNH-IOL submitted these solutions to a battery of tests designed to verify their functionality in the field. These tests were divided into four sections: Call Performance and Call Load Capacity, Voice Aware Features, Voice Quality of Service, and Voice Security. Each section consisted of multiple tests that verified different aspects of each solution.

1. Call Performance and Call Load Capacity

The Call Performance and Call Load Capacity section consisted of three tests. The first test was a Call Capacity test, which tested the maximum number of calls allowed per AP for both the SIP and SVP protocols.

The second and third tests were Call Performance tests that verified if the WLAN system prioritized VoIP traffic when both VoIP and wireless data were being transmitted

through the system. This test only verified prioritization on the wired network; a subsequent test verified wireless prioritization. In the first Call Performance test, the voice servers and APs were plugged directly into its WLAN system. In the second Call Performance test, they were connected with the switch via a bridge/routed network.

Note: The UNH-IOL was unable to perform this testing at the March 2005 event due to the large number of phones required. The laboratory plans to test full load performance and capacity testing at a future date.

2. Voice Aware Features

The Voice Aware Features section also consisted of three tests. The first test verified that the Voice Aware RF scanning didn't compromise VoIP quality. The laboratory ran three different setups: a control test, testing VoIP quality with RF scanning turned off; a VoIP quality test with regular RF scanning turned on, and a VoIP quality test incorporating voice aware RF scanning.

The second test in this section, the Call Admission Control test, verified the WLAN system's ability to detect VoIP devices connected to the network whether or not they were engaged in a call (referred to as "on hook" if not engaged and "off hook" if engaged), and to balance and control the number of calls per AP based on the number of active voice calls.

The last portion of this testing, Voice Application Awareness, verified that WLAN switches could both successfully distinguish the different VoIP protocols (SIP, SVP) and open the ports that were needed, as they were needed.

3. Voice Quality of Service

Voice Quality of Service tests verified the prioritized queuing of VoIP data. The tests ensured that the VoIP traffic was prioritized over wireless data being streamed at the same time. This test verified VoIP prioritization in the wireless medium only. A separate Call Performance test (detailed in the first section) verified wired VoIP prioritization.

An additional test for QoS checked 802.1p and DSCP tags on packets moving to and from the AP. Finally, a bandwidth control test ensured that data could be limited to a certain throughput amount, so that the VoIP traffic was guaranteed the bandwidth it required.

4. Voice Security

The Voice Security sectioned verified voice stream access and blacklisting functionalities. The first test in the section, the Limiting Network Access for Voice Users test, verified that VoIP devices were not allowed to access anything but the voice relevant portions of the network.

The second and final test in this section, the Blacklisting Client test, ensured that any device on the VoIP network that violated the voice policies was blacklisted from the network and kept there until cleared by an administrator.

Results from Section 2: Voice Aware Feature Tests

Aruba's WLAN System (Device Under Test or DUT) first underwent the Voice Aware RF Management tests. The DUT had 14 phones connected to it, and they engaged in 7 calls. For each part of this test, the wireless testing device measured an "R-Value" for each phone call. An R-Value is the quantitative measurement of VoIP quality in a network, and the preferred measurement of VoIP quality. The first part of the test ran with RF scanning disabled on the DUT. This provided a control value that represented the DUT's performance when unencumbered. The table following provides the values garnered in this test.

Table 1

Test Label	1st Test Run	2nd Test Run
R-Value of VoIP flow 1	77.9	77.3
R-Value of VoIP flow 2	77.9	77.8
R-Value of VoIP flow 3	78.0	77.9
R-Value of VoIP flow 4	Error – value not present	Error – value not present
R-Value of VoIP flow 5	77.8	77.8
R-Value of VoIP flow 6	77.9	77.8
R-Value of VoIP flow 7	77.9	77.9

The second part of this test ran with the RF scanning enabled on the DUT, but with no voice-sensitive features. This showed a significant drop in voice quality, which caused broken voice output. Depending on the scanning time, some of the calls were dropped and the R-value falls to around 60. This is clear proof that the AP's off channel scan time can affect the quality of the call. The quality of the calls dropped significantly even with a small increase in the scan time.

The final portion of this test ran with voice sensitive RF scanning enabled on the DUT. As evidenced by the table below, the voice sensitive RF scanning features successfully preserved the integrity of the voice traffic stream. The R-Values are comparable to the first test without RF scanning; in this test however, RF scanning provided maintenance and security without sacrificing VoIP quality.

Table 2

Test Label	1st Test Run	2nd Test Run
R-Value of VoIP flow 1	77.9	77.9
R-Value of VoIP flow 2	77.8	77.9
R-Value of VoIP flow 3	77.8	77.9
R-Value of VoIP flow 4	Error – value not present	Error – value not present
R-Value of VoIP flow 5	77.9	77.8
R-Value of VoIP flow 6	77.3	77.8
R-Value of VoIP flow 7	77.5	77.9

The Call Admission Control test was the next test performed in this section. Call admission control and Call load balancing were enabled on the DUT. The test began with 12 VoIP devices connected to a light AP (AP 1) controlled by the DUT. Another light AP (AP 2) with no VoIP devices connected to it was brought up with the same settings. This test used the SVP protocol, with a maximum number of 4 SVP calls allowed. The following output from the DUT's command line interface (CLI) displayed the status of the phones at the beginning of the test.

Figure 1

```
VoIP Client Table (Flags: C = call in progress)
-----------------
MAC Address       Location BSSID              ESSID VLAN   Protocol     Flags
-----------       -------- -----              ----- ----   ---          -----
00:90:7a:02:4a:09 AP 1     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:15:d2 AP 1     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:36:42 AP 1     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:38:a5 AP 1     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:49:af AP 1     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:19:31 AP 1     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:4a:03 AP 1     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:49:f5 AP 1     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:2f:85 AP 1     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:2b:82 AP 1     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:0e:d6 AP 1     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:24:b8 AP 1     00:0b:86:c0:f9:60  voip  1      svp
Number of Clients:12
```

The four VoIP devices placed phone calls after this setup was verified. This was the maximum number of calls allowed per AP, and therefore the DUT was expected to correctly balance the system, by moving all of the "on hook" (not engaged in phone calls) devices to a neighboring light AP (AP 2).

Figure 2

```
VoIP Client Table (Flags: C = call in progress)
-----------------
MAC Address       Location BSSID              ESSID VLAN   Protocol     Flags
-----------       -------- -----              ----- ----   ---          -----
00:90:7a:02:4a:09 AP 2     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:15:d2 AP 2     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:36:42 AP 2     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:38:a5 AP 2     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:49:af AP 2     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:19:31 AP 2     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:4a:03 AP 2     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:49:f5 AP 2     00:0b:86:c0:f9:60  voip  1      svp
00:90:7a:02:2f:85 AP 1     00:0b:86:c0:f9:60  voip  1      svp          C
00:90:7a:02:2b:82 AP 1     00:0b:86:c0:f9:60  voip  1      svp          C
00:90:7a:02:0e:d6 AP 1     00:0b:86:c0:f9:60  voip  1      svp          C
00:90:7a:02:24:b8 AP 1     00:0b:86:c0:f9:60  voip  1      svp          C
Number of Clients:12
```

The DUT correctly detected the call status of a connected VoIP device, as evidenced by the CLI output. The DUT proactively moved all "on hook" VoIP devices to AP2, which correctly balanced out the system when the maximum number of calls was reached.

The Voice Application Awareness test, the final test of this section, ran with voice application awareness enabled on the DUT. This solution ensured that specified ports were only opened when VoIP calls of various protocols were engaged (SIP, SVP, Cisco SCCP). All other ports should have remained closed. Successful phone calls made using the SIP, SVP, and SCCP protocols verified that this solution worked properly. The DUT properly detected and opened ports for specific VoIP traffic protocols, thereby passing the test.

Results from Section 3: Voice Quality of Service Tests

The third section of tests focused on the ability of the DUT to prioritize Voice traffic. The Prioritized Queuing test, the first test in this section, ran with prioritized queuing enabled on the DUT. Eight devices connected to the DUT engaged in four VoIP phone calls. A wireless testing device also transmitted traffic through the system at 4 Mbps. A wireless trace verified that the DUT correctly prioritized the VoIP traffic over the wireless data. In 10000 frames captured, only 867 of these frames were data frames from the wireless testing device; 3970 data frames were sent to and from the VoIP clients. The DUT used the bandwidth mainly for exchanging VoIP data, and allowed the wireless testing device to transmit data when there was an opening.

The Traffic Tagging test checked the ability of the DUT to tag packets in both 802.1p and DCSP formats. The test ran with the traffic tagging option enabled in the DUT, and an Ethernet trace was taken. This trace verified that the DUT was tagging the packets as specified.

The Bandwidth Control test, the last test in this section, ran with the Bandwidth Control option enabled in the DUT, and set to allow only 1 Mbps of throughput. This option was designed to limit the amount of wireless data, and reserve the medium for throughput sensitive VoIP traffic. A wireless testing device transmitted data at 4 Mbps through the DUT for a specified amount of time. At the end of the test, the wireless test tool verified that only 1 Mbps of wireless throughput was received. The DUT correctly limited bandwidth for wireless data users and preserved the quality of the VoIP traffic streams.

Results from Section 4: Voice Security Tests

The final section tested the security features of the VoIP network. The first test ensured the ability of the DUT to limit the access for voice devices. This test ran with a feature enabled that kept data networks secure from relatively unsecured voice networks. This feature worked by limiting the access for devices on a voice SSID to only voice ports and other voice devices. A wireless data client connected to the limited voice SSID, and all ICMP traffic sourced to a non-VoIP device failed. The DUT denied all attempted access to a non-VoIP device or port, which verified the functionality of the limited voice network access feature.

The Blacklisting Clients test, the second and final test of the section, ensured that devices on a voice network that attempted to access non-voice devices or use non-voice

data protocols would be placed on a blacklist, wherein all network access would be prohibited. First, a wireless data client connected to the voice SSID where blacklisting has been enabled. Second, the wireless client attempted to access the data network via a web browser. The DUT correctly denied all access to the data network. The DUT also added the wireless data client to the Blacklist. This is evidenced by the DUT CLI output seen below. The device highlighted in bold letters is the data client.

Figure 3

MAC Address	Location	BSSID	ESSID	Role	Age(d:h:m)
00:0d:28:2e:8f:9d	AP1	00:0b:86:c0:fa:60	voip	cisco	00:01:07
00:90:7a:02:15:d2	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:06
00:0e:38:50:26:ff	AP1	00:0b:86:c0:fa:60	voip	cisco	00:01:07
00:90:7a:02:4a:03	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:07
00:90:7a:02:49:af	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:07
00:90:7a:02:36:42	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:07
00:90:7a:02:38:a5	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:07
00:90:7a:02:24:b8	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:07
00:90:7a:02:19:31	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:07
00:90:7a:02:2b:82	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:07
00:90:7a:02:4a:09	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:07
00:90:7a:02:49:f5	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:07
00:90:7a:02:2f:85	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:07
00:90:7a:02:0e:d6	AP1	00:0b:86:c0:fa:60	voip	phones	00:01:07
00-05-4E-44-20-3B	**AP1**	**00:0b:86:c0:fa:60**	**voip**	**phones**	**00:00:10**

The wireless client appeared on the blacklist after it attempted to access the data network.

Figure 4

DoS STA List

STA	reason	block-time(sec)
00:05:4E:44:20:3B	**session-blacklist**	**60**

The DUT denied all attempts to communicate on the network after the wireless data client was blacklisted, until an Administrator manually removed the client from the blacklist.

Summary

These results provide a positive outlook for those looking to combine the power of VoIP protocols with the versatility of a wireless network. Prioritized queuing, bandwidth control, and voice sensitive RF scanning all protected sensitive VoIP streams and preserved their quality. Both assigning roles and limiting access based on these roles provided security for data networks that could have contained private information; the Blacklisting feature provided additional protection from devices that attempted to break these rules. The results of this test event indicate that the major problems of integrating the two network mediums have solutions that can be implemented. These tests also further promote interoperability not only in a test environment, but also in a real world environment.