

Motorola WiNG5 Wireless LAN Architecture Advantages

Lab Evaluation vs. Traditional Hub-and-Spoke WLAN Solutions

Tolly Report #211114
Commissioned by
Motorola Solutions, Inc.

May 2011





**Motorola
Solutions, Inc.**

**WiNG5 WLAN
Architecture**

**Distributed vs.
Traditional
Hub-and-spoke
WLAN
Architecture**



*April
2011*

THE BOTTOM LINE

The Motorola WiNG 5 solution delivered unique differentiation in the following areas in comparison to the other solutions tested:

- 1 Provided significantly greater distributed functionality with authentication, local bridging, fast roaming, firewall enforcement, and RF interference remediation at the AP
- 2 Demonstrated site & services survivability when the link to the controller was removed and also demonstrated controller-less deployment operation
- 3 Exhibited greater scalability, simulated a deployment of 10,000 APs, 4,000 RF domains, and 100,000 clients - all being managed by a single controller
- 4 Delivered lower setup and installation times ultimately resulting in lower costs

Executive Summary

Enterprise-class wireless LAN (WLAN) installations can range from dozens to potentially thousands of wireless access points (APs) serving large communities of corporate users across a global network. The inherent complexity of Enterprise WLAN led to early-generation hierarchical, hub-and-spoke architectures that centralized intelligence in a system controller that connected to “thin” wireless LAN APs that contained little functionality besides the essential function of transmitting and receiving wireless signals. The Cisco Systems WLAN solution is built on just such an architecture.

Unfortunately, the fundamental flaws in traditional, hierarchical solutions become readily apparent when WLAN solutions need to be deployed to geographically disparate locations. Consider a situation where a WLAN controller in Atlanta manages 10 APs in a single Los Angeles office. With a traditional Cisco solution configured for central switching, all traffic between APs in LA, must travel via the controller in Atlanta. This not only slows down the communication between the two LA-based devices, but loads the wide-area network (WAN) unnecessarily, likely degrading the performance of other applications sharing the Atlanta-LA WAN link. Furthermore, as Wi-Fi transmission speeds increase and device counts increase, the WAN burden in the hub-and-spoke model will likely increase.

Because the central switching approach was inherently not scalable, Cisco introduced a more intelligent AP solution (known as the Hybrid Remote Edge AP or H-REAP) that allowed traffic between devices at a remote location to be switched locally without traversing the WAN.

Still, this is essentially a retrofit for what remains a centralized, hub-and-spoke architecture. While session traffic is no longer forced to traverse the WAN, the central controller still provides significant services on behalf of each remote AP. The branch-office AP's reliance on the centralized controller becomes problematic in situations where the connection between the controller and the AP is lost because of WAN problems. In such cases the remote APs, though still able to bridge traffic locally, lose considerable functionality until such time as the link to the controller is restored. In fact, because the Cisco remote APs are unable to process any new users via RADIUS without connectivity to the central controller, once current users become inactive or time out, the Cisco remote AP effectively shuts itself down until the WAN link, and the connection to the controller, is once again available¹.

Motorola's WiNG5 architecture was designed to deal with the challenges of higher bandwidth 802.11n wireless networks and scale efficiently from small to large, geographically dispersed deployments. In the WiNG5 architecture, the controller function is distributed throughout the network. In fact, each AP has much of the same capability as the main system controller.

¹ Cisco H-REAP Design and Deployment Guide, http://www.cisco.com/en/US/products/ps6087/products_tech_note09186a0080736123.shtml#intro



Because system intelligence exists local to each access point, local WLAN traffic always stays local - removing a significant burden on WAN resources. Furthermore, in situations where the APs are unable to communicate with the main system controller, no loss of function is experienced at the local WLAN and users are not impacted.

Motorola Solutions commissioned Tolly to benchmark the performance and system behavior of products built on Motorola's new WiNG5 architecture and compare those results with solutions from Cisco and another leading vendor² that are based on traditional, controller-based architectures. Testing was conducted in April 2011.

Efficiency of Distributed Architecture with Site Survivability

Tolly testing found that the Motorola products built on the WiNG5 architecture were dramatically more efficient with respect to WAN bandwidth usage than the traditional offerings configured for centralized switching. Testing confirmed that Motorola APs could provide full functionality and, thus, site survivability to local WLAN clients when the network connection to the system controller was unavailable. This contrasted with the traditional solutions where loss of the controller connection results in loss of significant functionality such as stateful firewall enforcement, client roaming & authentication, intrusion detection and protection and RF interference remediation.

Branch-Office Controller Performance

For those customers that want to take an "integrated services" approach to branch office connectivity, Motorola offers a branch office controller that combines wireless LAN access point functionality with wired Ethernet ports. This unit was benchmarked against a comparable unit from Vendor X.

Tolly engineers used WLAN test equipment from VeriWave, Inc. to determine the maximum WLAN throughput of the device. Testing was carried out using various settings detailed later in this report. When tested with a data frame size of 512 bytes, the maximum throughput for Vendor X was 60.27 Mbps where Motorola delivered 192.22 or more than 3X the throughput of the competitor.

Similarly, when tested with a data frame size 1500 bytes, the maximum throughput for Vendor X was 182.75 Mbps where Motorola delivered 232.73 Mbps or over 25% greater throughput.

Installation & Management

As businesses grow, the number of deployed APs will grow as well. When a new Motorola AP is deployed, the Motorola system will automatically identify its location, dynamically apply the AP configuration policies running at that location, and bring it online for use - all without any manual configuration. Conversely, the Cisco solution requires 8 manual configuration steps at the controller before a new AP is operational and usable. Similarly, the Vendor X solution requires 6 manual configuration steps.

² The second vendor will be referred to generically as Vendor X throughout this document.



Motorola leverages its distributed model to optimize software updates for APs. Where Cisco's approach is to transmit a duplicate copy of the new code to each remote AP, Motorola transmits a single copy to one AP which then serves as a local distribution point to any and all other APs at the same physical location. This functionality is also exploited when applying policy updates and statistics collection, further reducing unnecessary loading of the WAN link.

In short, the Motorola solution is more WAN-friendly than the hub-and-spoke solutions offered by Cisco and Vendor X.

Scalability

Ultimately, the distributed nature of the Motorola solution results in greater system scalability. Tolly witnessed a Motorola simulated deployment that consisted of over 10,000 APs, in more than 4,000 radio frequency (RF) domains, communicating with over 100,000 simulated clients managed by a Motorola NX 9000 Integrated Services Controller.³

Conversely, the Cisco solution claims to support up to 512 managed APs and 7,000 clients - even though the Cisco WLAN controller provides only 8 GbE ports. The Vendor X solution claims up to 4,096 APs and 32,768 clients connected simultaneously.

In summary, products implementing Motorola's WiNG5 distributed architecture deliver a solution that is more resource-efficient and more robust, while being easier to manage and maintain than a traditional solution from Cisco Systems or Vendor X.

³ Exact numbers are provided in the Test Results section.



Test Results

Tolly evaluated three enterprise WLAN solutions. Each solution included an enterprise WLAN controller and access points. Two solutions also provided an alternative WLAN controller suitable for providing integrated services (LAN/WAN/WLAN) at branch office locations. See Table 1 for system information. Tests included bandwidth efficiency, system performance, functionality, site survivability, and scalability.

WLAN Solutions Evaluated

Vendor	Enterprise Controller	Branch Office Controller	Access Point
Motorola Solutions, Inc.	RFS 6000 Wireless LAN Switch (RFS 6010-100-WR Code: V5.1.0.0-046B) NX 9000 Integrated Services Controller (for scalability test)	RFS 4000 802.11n Integrated Services Controller (Code: V5.1.0.0-046B)	AP 7131 Wireless Access Point (AP 7131N-66S00-US Code: V5.1.0.0-046B)
Cisco Systems, Inc.	5508 Wireless Controller (Code: V7.0.98.0)	Not offered	Aironet 1042i (LAP1042N-A-K9) Aironet 3502e (CAP3502E-A-K9)
Vendor X	Enterprise Controller	Branch-Office Controller	Access Point

Note: As the WLAN test tool used in this evaluation required direct connections to access point, testers used APs with internal antennas as well as APs with connections for external antennas. Cisco Systems was invited to participate in the evaluation. Cisco representatives did not respond to the invitation from Tolly.

Source: Tolly, April 2011

Table 1

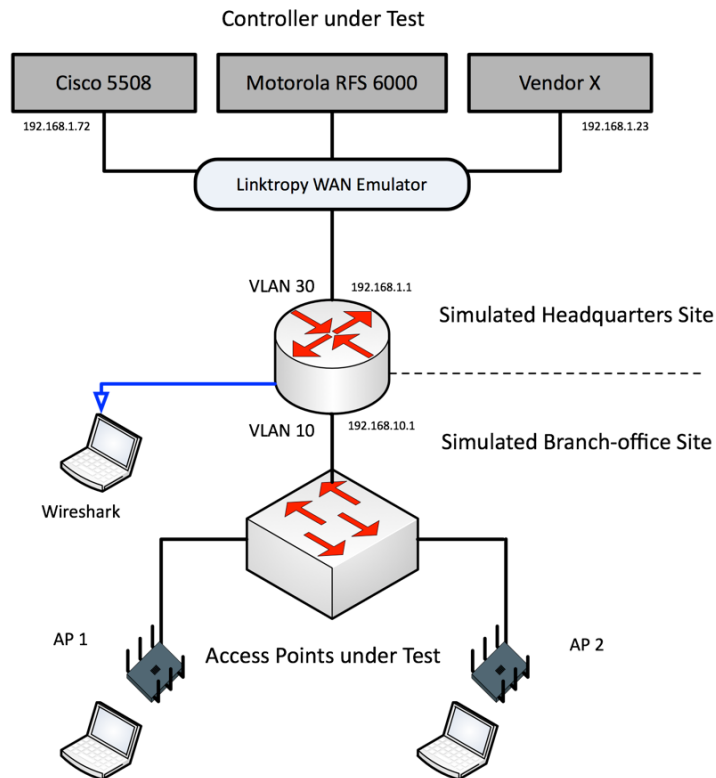
Engineers built a test environment that was a microcosm of an enterprise WLAN deployment with a main location (“hub”) and a remote office (“spoke”). Engineers were, thus, able to trace the flow of traffic as well create scenarios where the remote office to main office link would be deliberately severed to evaluate the site survivability characteristics of the “spoke” sites. See Figure 1.

Efficiency & Availability

Traditional hub-and-spoke WLAN systems centralize intelligence in such a way that control traffic needs to transit the WAN to/from the branch office.

The reliance on the intelligent controller located across the WAN by Cisco and Vendor X becomes a major issues, as will be seen shortly, when the WAN link is unavailable.

Enterprise Wireless LAN Test Environment



Source: Tolly, April 2011

Figure 1

Less widely known, and equally important, is that the requirement for control traffic to transit the WAN even when the Cisco solution is configured for local bridging/switching. This requirement can affect the stability of the branch office WLAN even when the WAN link is connected. In fact, Cisco warns that, because of this requirement, an additional WAN quality-of-service solution might be required to assure a reliable connection between the controller and the APs it controls at each branch office.

According to Cisco's H-REAP Design and Deployment Guide (Doc ID: 71250): "Roundtrip latency must not exceed 300 milliseconds (ms) for data and 100 ms for voice and data between the access point and the controller, and CAPWAP⁴ control packets must be prioritized over all other traffic."

If the CAPWAP packets cannot reach the AP in a timely fashion, the systems can (incorrectly) think the WAN connection has gone offline and then, moments later re-establish the connection. This situation is known as "H-REAP flapping." In the same document, Cisco notes that: "Frequent H-REAP flapping causes serious connectivity

⁴ CAPWAP: Control and provisioning of wireless access points.



issues. Without proper network prioritization in place, it is prudent to place controllers at remote sites to ensure consistent and stable wireless access." It should be noted that the least expensive configuration of Cisco 5508 WLAN controller available at the CDW website in April 2011 is \$7,863.99.

Because Motorola provides intelligence in each AP, no such requirement for quality-of-service and/or local controllers exists.

Traffic Flow

Tolly engineers configured each system according to manufacturer's instructions. Once the systems were operational, engineers initiated a session between two WLAN clients that were co-located in the same simulated branch office but were associated with different APs.

Engineers verified the traffic flow by connecting a network trace tool at the central location. As expected, the Motorola intelligent APs were able to provide a traffic path between the clients on the different, co-located APs that kept all traffic locally. No traffic traversed the WAN.

With Cisco's APs configured to the local switching mode (provided by the Cisco hybrid remote edge AP), traffic between local clients on the same or different APs also remains local to the branch office.

Conversely, the Vendor X solutions natively conducted all inter-AP communications via the controller deployed in the central location. In fact, in the hub-and-spoke scenarios, all traffic traverses the WAN twice - once as the source AP tunnels the traffic to the "hub" and again when the "hub" directs the traffic back to the target AP at the same branch location. With Vendor X, its branch-office WLAN controller would need to be deployed at each and every branch office to provide the WAN efficiency of the Motorola solution.

As noted, this causes the session traffic, which both originates and terminates in the remote office, to traverse the WAN two times - out and back - before being delivered. Not only does this waste precious WAN resource for no good reason but it introduces latency - delay - into the communication. The amount of delay will depend on the speed of the WAN link as well as how congested that link is. With latency-sensitive applications like VoIP and interactive video, the delay alone could be an issue.

Site Survivability and Motorola's Distributed Intelligence

As noted earlier, the controller in traditional, hub-and-spoke implementations provides key management and operations functions for the APs in the system. In situations where the WAN link connecting a given "spoke" to the "hub" becomes unavailable, the WLAN users at the branch office can experience degraded communications even within the branch office.

Tolly engineers evaluated the availability to branch-office WLAN clients of several key functions when the WAN link between the remote branch and the main location was unavailable. Table 2 summarizes the results.



Security Authentication

In a typical enterprise environment, a wired or WLAN client connecting to the network would be authenticated via a dedicated security authentication server. (That is, a RADIUS server that is not integrated into in the WLAN controller.) Authentication requests for branch-office WLAN users are typically relayed to the central site where they are processed.

When the WAN is offline, neither Cisco nor Vendor X can authenticate any new users until the link to the controller is available. (Cisco does allow the user to provide for a backup RADIUS server located at each branch office site.) Furthermore, should existing users reach time-out periods for their credentials, they can no longer access protected resources.

Because the Motorola system supports a RADIUS server on-board its access points, new users can be authenticated even in situations where the APs have no link to the controller. (This feature requires configuration.)

Local Bridging/Switching

Both Cisco and Vendor X solutions support local bridging/switching mode, and in the event of a controller failure, can be configured to switch data locally, operating

Site Survivability WLAN Functionality Available at Disconnected Branch Office

Feature	Motorola	Cisco Systems	Vendor X
Authentication	✓ ₁	✗	✗
Local Bridging	✓	✓ ₂	✓ ₂
Fast Roaming	✓	✗	✗
Firewall Enforcement	✓	✗	✗
RF Interference Remediation	✓	✗	✗

Notes: 1. Motorola caches RADIUS credentials of existing clients. 2. Must be configured

Source: Tolly, April 2011

Table 2



independent of the hub. Cisco's H-REAP (Hybrid Remote Edge Access Point) mode allows the AP to continue to operate with existing users in the event that WAN communication is lost. For Vendor X, local bridging/switching must be configured manually as a failover option, before the WAN outage occurs.

The Motorola solution provides local bridging/switching as part of its normal operation and, thus, continues to function should the link to the controller become unavailable. This provides a significant benefit especially for large scale deployments where manual reconfiguration of access points for local bridging is simply not a viable solution.

Fast Roaming

In office environments with multiple APs, it is desirable for a given WLAN client to communicate using the strongest signal available at a given time. As users move throughout the office with their laptop and/or mobile devices, the devices will monitor the availability and signal strength of APs and "roam" or migrate to a different AP if doing so will provide a better connection.

The traditional solutions manage the roaming process by caching the Pairwise Master Key (PMK), allowing clients to roam between access points without needing to completely re-authenticate with the RADIUS server, a process that can take longer than 150 ms. While this would seem to be a non-issue, latency-sensitive applications such as VoIP and Video streaming would see a noticeable degradation in quality. With the controller connected, Cisco was able to complete the client authentication in 157 ms with the caching off, once enabled, that time dropped to 42 ms. When the controller was disconnected, the clients connected to either Cisco or Vendor X were unable to roam, since the controller is needed for key caching to enable fast roaming.

Motorola, however, was able to perform OPMK (Opportunistic PMK) caching without connectivity to the centralized controller and connected clients were able to roam in just 28.4 ms.⁵

Firewall Enforcement

The traditional WLAN solution can be thought of as a subnetwork within the corporate LAN, the controller acting as the point-of-egress for the connected clients. While certain firewall and content filtering policies may exist at the edge and on LAN connected machines, the wireless network is left unmanaged, since it is independently administered by the controller. Thus, a necessary component of a comprehensive WLAN solution is the firewall, which has traditionally been enforced at the controller.

When the controller is no longer in the data path, such as in a WAN outage or local-bridging configuration, Cisco and Vendor X are not able to enforce the firewall policies, leaving the local network open to unauthorized access. With the Motorola WiNG5 solution, the distributed intelligence architecture incorporates a stateful firewall to each node of the wireless network, providing widespread, synchronized network security, while easing the congestion of the network.

⁵ As Vendor X does not have detachable antennas, engineers were unable to run this test.



RF Interference Remediation

At the branch office, a company’s wireless solution will often be deployed within range of multiple other APs such that the wireless spectrum becomes quite crowded, and, depending on usage, some channels may have so much contention that no users of the channel will receive for consistent performance. Furthermore, interference present (e.g., cordless phones, Bluetooth devices, radio jammers) could potentially completely disrupt client connectivity to the AP.

To mitigate such situations, it is an accepted practice to run frequent scans of every channel for noise, dynamically switching between them if a more suitable one is found. However, in the hub-and-spoke architecture, the decision to switch channels resides solely with the controller, which collect the scan data from the APs and update the policy to use a different channel. Without the controller present, individual APs lose the capability and can be rendered effectively unusable by traffic congestion and/or interference.

Tolly testing showed that regardless of whether or not the controller was present, the Motorola solution was able to detect and mitigate wireless interference, synchronized across multiple APs, in under 30 seconds.

The Cisco and Vendor X solutions were not able to provide this functionality while disconnected from the controller.

Branch Office Performance

There are some branch-office scenarios where a local integrated services controller may be preferable to the customer. Both Motorola and Vendor X supply a branch office controller, acting as a standalone AP, firewall, and gateway, while managing other local APs, providing an end-to-end managed network.

These platforms may be similar in functionality and form, the performance cannot be considered static. Testing showed that Motorola’s solution consistently outperformed

Branch-Office WLAN Performance

Frame Size (Bytes)	Vendor X Radio Management Disabled	Vendor X Radio Management Enabled	Motorola WiNG5 Radio Management Disabled
88	X	X	51.47 Mbps
512	16.86 Mbps	60.27 Mbps	192.22 Mbps
1500	182.75 Mbps	100.40 Mbps	232.73 Mbps

Note: 88-byte tests were not able to be run successfully on Vendor X solution. With radio management enabled, the Vendor X solution selected a lower throughput 20MHz channel. Testers then manually selected an optimal channel to illustrate maximum throughput.

Source: Tolly, April 2011

Table 3



the competition. With radio management functionality disabled, Vendor X was only able to achieve 17 Mbps for 512-byte frames, and 183 Mbps for 1500-byte frames. When radio management was enabled (allowing the APs to choose the best operating parameters dynamically), the 512-byte throughput rose to 60 Mbps. The throughput at the larger frame size, however, dropped to 100 Mbps, due to the APs selecting a channel with a narrower 20MHz bandwidth⁶. Motorola, conversely, was able to provide 192 Mbps with 512-byte frames, and nearly 233 Mbps with 1500-byte frames. See Table 3.

Installation & Management

When building out a traditional WLAN solution or even adding to an existing one, the most time consuming part is provisioning each and every access point for use on the system. Dealing with a large deployment, that equates to hours if not days of configuration, as each AP cannot be assigned a policy until it is online, not taking into account the switching configuration that must occur to ensure connectivity back to the controller.

While Cisco and Vendor X both support the grouping of APs, this is done by assignment, not inherited from a global configuration. Motorola introduced the idea of RF Domains, or sites, which are all provisioned with the same policy. In fact, a Motorola AP will actually discover its local network upon first boot (either through CDP, LLDP, DNS, etc.) and supply that identifying information to the controller, which then initializes and provisions the AP with the same RF Domain policy, providing touch-less AP Adoption to organizations of any size.

Having multiple APs in an RF Domain also exposed another unique property of the WiNG5 solution. Typically, in the event of a policy update or firmware upgrade, the controller would push the configuration to each and every AP individually, multiplying the WAN usage over a period of time. With the WiNG5 architecture, multiple APs in the same physical location hold an election for Site Manager, an AP which communicates directly with the controller to receive configurations, distributing copies to each local AP as another means of WAN optimization. This is true as well for statistics collection and reporting.

Motorola's solution provided the most efficient AP provisioning with respect both to time and WAN bandwidth usage.

Scalability

CIOs are unwilling to invest in a solution that is not "future-proof", whether the company grows internally or externally, creating branches and franchises, one must be certain that any newly implemented technologies are able to stand the test of time. The most fundamental difference about the Motorola WiNG5 architecture when compared to the traditional method is the capability of switching traffic locally, ensuring that only the traffic that is destined for the cloud, traverses the WAN. More so, this local and Internet

⁶ With radio management enabled, the Vendor X solution selected a lower throughput 20MHz channel. Testers then manually selected an optimal channel to illustrate maximum throughput.



traffic is no longer forced through the controller, eliminating the most significant potential bottleneck that exists in Enterprise Wi-Fi. Because of this, the scalability of the WiNG5 architecture is unmatched by the other solutions tested.

As the controller is no longer responsible for terminating and routing traffic, its switching backplane does not need to increase with the deployment size, and it is freed up to perform the task for which it was originally intended, to manage, monitor, and delegate tasks to all the APs and clients within its global domain. For the Motorola controller platform, Tolly witnessed a lab environment where custom software was used to generate the stateful traffic generated by 10,201 APs, in 4,001 RF Domains, with 117,360 active, connected clients. Vendor X claims to support 4,096 APs and up to 32,768 connected clients, while Cisco claims support for up to 512 managed APs, and 7,000 clients.



Test Bed & Test Methodology

Engineers deployed each vendor's WLAN solution to provide a simulated headquarters location as well as a simulated remote, branch-office location. The two environments were connected using a Linktropy 4500 WAN emulator from Apposite Technologies.

At the branch-office site, two APs were connected to switch VLAN 10. At the HQ site, each solution's controller was connected to a different switch port inVLAN 30. Each AP was configured to have two SSIDs, one "local" was mapped to the local VLAN 10, while "central" was mapped to VLAN 30, with no switch on the branch office side mapped to VLAN 30.

See Table 1 for the details of the solutions under test.

Ixia's IxChariot was used to generate traffic for the traffic flow test.

A VeriWave WaveTest system was used for the branch-office performance tests. A Wireshark network analyzer was connected, as appropriate, to the network to verify traffic flow.

A Wi-Spy DBx Pro, paired with Chanalyzer Pro, both made by MetaGeek, LLC, was used for the interference tests. A Fluke AirCheck was used to monitor the WLAN traffic.

See Table 4 for test tool details.

Test Tools

Vendor	System
Fluke Corporation	AirCheck Wi-Fi Tester
VeriWave, Inc	WaveTest 90 Chassis outfitted with 1x WBE1000 WaveBlade Ethernet Card and 2x WBW2000 WaveBlade 802.11n Card WaveAPP Release 4.3.2-WT-3.9.5 (2010.12.15.08)
Apposite Technologies	Linktropy 4500 WAN Emulator, Hardware Revision: N2
Ixia	IxChariot 7.1 EA SP2 Performance Endpoint
MetaGeek, LLC	Wi-Spy DBx Spectrum Analyzer and Chanalyzer 3.4
Wireshark Foundation	Wireshark 1.4.x

Source: Tolly, April 2011

Table 4



Traffic Flow

To demonstrate the main architectural difference of WiNG5 versus the traditional hub-and-spoke architecture, engineers configured one client on each local AP at the branch office, and began passing traffic using Ixia's IxChariot. Monitoring the utilization of the WAN link, engineers were able to determine the traffic path.

Site Survivability

Several tests were conducted to determine the functionality available when the branch-office site was disconnected from the controller residing at the HQ site. The simulated WAN link between the sites was "failed" by disconnecting the WAN emulation device.

Authentication

Since the WiNG5 APs incorporate a centrally-updated RADIUS server, clients can still authenticate to the network at the branch office, even when the controller is unreachable. To demonstrate this, engineers configured the policy for the Motorola RF domain to perform local authentication, caching the centralized RADIUS server. Disconnecting the branch office from the WAN, engineers attempted to authenticate clients to the network.

Fast Roaming

Engineers connected both APs of a given solution to the VeriWave traffic generator/performance analyzer, and simulated a client on one AP, with the controller connected. Engineers then disconnected the controller and induced a roaming event, in which the client will connect to the second AP while maintaining its session. Metrics were reported by WaveAPP 4.3.2.

Stateful firewall

For this test, engineers connected two clients to the same AP, setting up a streaming media server on the local network. One client machine was also configured to stream a video clip over the network, while the other was used to view both media streams simultaneously. For each Vendor, engineers connected the clients, applied a firewall policy to disallow all media originating on the WLAN, and then failed the WAN link, placing Vendor X and Cisco into Local switching mode. If the unauthorized stream ceased while the valid one was not impacted, then the firewall enforcement is at the AP.

Interference Remediation

Engineers configured each solution for dynamic RF management, and connected two clients to the same AP. Then, engineers disconnected the controller, and using a MetaGeek Wi-Spy Spectrum Analyzer and Chanalyzer, introduced interference on the same channel as the AP. Timing was recorded from the number of lost pings between the two connected clients.



Branch Office Performance

Using the VeriWave system, engineers connected the Motorola Branch Office Controller RFS4011, as well as the Vendor X SMB controller radios to the chassis, using the WaveAPP 4.3.2 program to perform a throughput test for each system for 88, 512, and 1500-byte packets. While the factory default was used for Motorola, two tests were done with Vendor X, one with dynamic RF management enabled (Which picked a 20MHz channel) and one disabled, manually configured for a 40MHz channel.

AP Adoption

To test the AP adoption for each solution, engineers took an AP out of the box, connected it to a preexisting branch office environment with other APs deployed, and recorded time/steps needed to bring the AP online and provision it with the correct policy.

Scalability

To view the scalability of the WiNG5 Architecture, Tolly engineers witnessed an active test bed consisting of software-emulated access points, generating all the management traffic of RF Domains and connected clients, each one of which could be individually managed. For the reported Cisco and Vendor X scalability metrics, data was taken from each Vendor's data sheet as to the maximum number of supported clients/APs on each system.



About Tolly...

The Tolly Group companies have been delivering world-class IT services for 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by email at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
<http://www.tolly.com>

Interaction with Competitors

In accordance with Tolly's Fair Testing Charter, Tolly personnel invited representatives from the competing companies to review the testing. Neither firm responded to the invitation.

For more information on the Tolly Fair Testing Charter, visit:

<http://www.tolly.com/FTC.aspx>



Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.