Miercom

Lab Testing Summary Report

April 2011

Report 110411

Product Category:

Wireless Controller

Vendor Tested:

CISCO

Products Tested:

Cisco Flex 7500
Motorola WiNG
Aruba VBN

Miercom PERFORMANCE VERIFIED

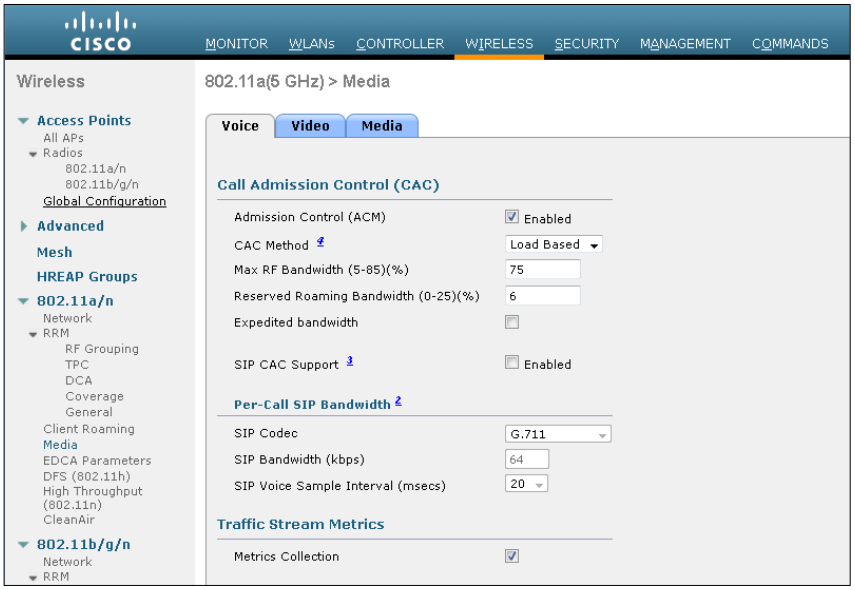
Key findings and conclusions:

- **Cisco FlexConnect architecture allows branch offices to continue operation when the WAN link is down or the controller is unavailable**
- **Port-based 802.1x authentication protects against installation of rogue access points**
- **Fast Roam with Cisco Centralized Key Management (CCKM) does not require keys to be exchanged, permits roaming even if the controller is down**
- **Provides Voice dynamic over-the air CAC (Call Admission Control) support to manage limited bandwidth, latency issues and protect existing voice calls**
- **FlexConnect architecture provides authentication flexibility — APs can perform 802.1x authentication**

Cisco engaged Miercom to perform an independent validation of their FlexConnect architecture featured in the Flex 7500 WLAN controller, with a focus on resiliency as it applies to branch office deployments. For comparison purposes, we also looked at solutions from Motorola and Aruba, specifically Motorola WiNG v5.0 and Aruba Virtual Branch Networking 2.0.

As wireless branch deployments are expanded to larger branch applications, several interrelated factors are of concern: continuity of business operations at the branch when WAN connectivity to the datacenter is lost, and deployment cost. Miercom selected several

Figure 1: Cisco Voice CAC



Source: Miercom, April 2011

Cisco Voice CAC manages bandwidth usages when the wireless link is congested to protect existing voice conversations. Administrators can select Load Based or Bandwidth Based limiting.

metrics to evaluate how well each solution addressed these concerns. We examined the ability to authenticate new clients when the controller fails, and/or the WAN link is down, as well as how the solution avoids Extensible Authentication Protocol (EAP) session timeouts over high latency WAN links. Finally, how does each solution deal with the authentication when the Radius server is down?

Branch survivability during a WAN failure includes the ability to continue mobile voice calls. We looked at the ability to continue roaming voice calls within the branch when the WAN is down. To evaluate the situation where bandwidth may be limited, or there are latency issues, we examined the CAC support offered by each product. In addition, how does each solution protect against the threat of rogue access points being installed in the branch?

In each of these situations, the Cisco FlexConnect solution clearly demonstrated its advantages in providing Mobile Branch Survivability and cost containment of wireless branch deployments by eliminating controllers in each branch.

Local Authentication/ Distributed Client Authentication

Does the Cisco FlexConnect continue to provide operations when the controller fails or the WAN link is down? A baseline was established by successfully associating laptop and VoIP clients with each vendor's APs and verifying successful authentication to the ACS server through each controller. The link to the controller at the datacenter was then purposefully brought down to simulate an outage. VoIP calls and FTP download sessions running on the laptops were monitored for any drops.

Cisco FlexConnect did not experience any service outage when the controller was unavailable. FTP downloads continued, and VoIP calls remained up. The Cisco AP is capable of authenticating with the ACS server directly, bypassing the controller. Not only are existing users able to remain connected but new users may authenticate with the ACS server and pass traffic successfully. Users do not experience any down time during a controller outage. We verified that the AP was authenticating with the ACS directly by generating the authentication log reports for the last 30 minutes on the ACS. This indicated that the AP was operating in "standalone" mode. When the controller was brought back online, we observed that the AP went into "connected" mode, indicating that authentication would now take place with the controller.

There was a difference with the Motorola WiNG v5.0. Motorola APs are entirely dependent on the controller. During the simulated controller outage, the entire branch loses wireless functionality. All APs are down, and do not broadcast an SSID. Existing clients lose connections, and new clients cannot join. An added headache from a network management perspective is that when the controller is brought back up, each access point at each branch must be rebooted in order for wireless functionality to be restored to end users.

For Aruba VBN 2.0, when the controller was brought down, existing users kept their connections. VoIP calls remained up, and FTP sessions continued to download. However, new users were unable to authenticate using 802.1x as the APs were unable to authenticate on the controllers behalf, with or without ACS available.

Wireless Resiliency

What happens when both primary and backup ACS RADIUS servers are down at the datacenter? FTP sessions were established between existing clients accessing server resources. Next, the port was shut down on the switch which provided WAN access to the Radius server. We attempted to add new clients to the branch AP. The AP console was monitored for successful authentication of the clients.

With both the Cisco Flex 7500 controller and the primary and backup RADIUS servers unavailable, the existing clients remained up and FTP transfers were not interrupted. New clients were able to join successfully by authenticating directly with the access point. FlexConnect allows the AP to function as a backup branch RADIUS server. The authentication process took slightly longer compared to baseline since the system stepped through the alternate methods of authentication. Branch communications in the data plane remained up and the branch was able to operate autonomously in the absence of

both the controller and the RADIUS server. As expected, there was no visibility between the APs and the controller, as the management and control planes were down.

The Motorola system requires a controller in order for the access points to remain functional. Once that link was broken, it was impossible to perform a test using only the Radius server to authenticate with communication down in the entire branch.

The Aruba VBN successfully maintained FTP downloads to existing clients when the ACS was unavailable. However, new clients were unable to associate with an AP as the Aruba access points are unable to authenticate without a controller. In addition, existing clients whose authentication timers expired were unable to re-authenticate as long as the controller was unavailable.

Voice Fast Roam and Wireless Resiliency

A key factor in wireless resiliency is the ability of wireless clients to roam within the branch during a WAN link failure. A client was associated with the first branch access point, AP-1. A voice call was initiated from the wireless phone to a wired handset. The WAN link was then brought down. Next, we forced a roam by walking from the Branch AP-1 to Branch AP-2. The voice call was monitored for any drops.

Cisco FlexConnect uses both 802.1x and distributed keys which are cached at the access point. With distributed keys in the event that the controller is unavailable, the keys are still valid and wireless clients can still authenticate. Fast Roam does not require the clients to re-authenticate. A wireless voice client successfully roamed between the branch access points without any interruption to the call. There is essentially no resiliency of branch communications with the competing solutions.

The Motorola WiNG v5.0 requires the controller to be available for the access points to function. Once the WAN link is brought down, wireless clients cannot roam within the branch.

Aruba VBN 2.0 maintained the voice call as long as the client remained associated with the initial access point. If the client roams to another access point, the call is lost and the client is unable to associate with the new access point. The client is also unable to re-associate with the original AP, so communication within the branch is effectively lost. Aruba requires re-authentication of the client with the access point when roaming occurs, and is unable to authenticate clients locally to the AP without a controller available.

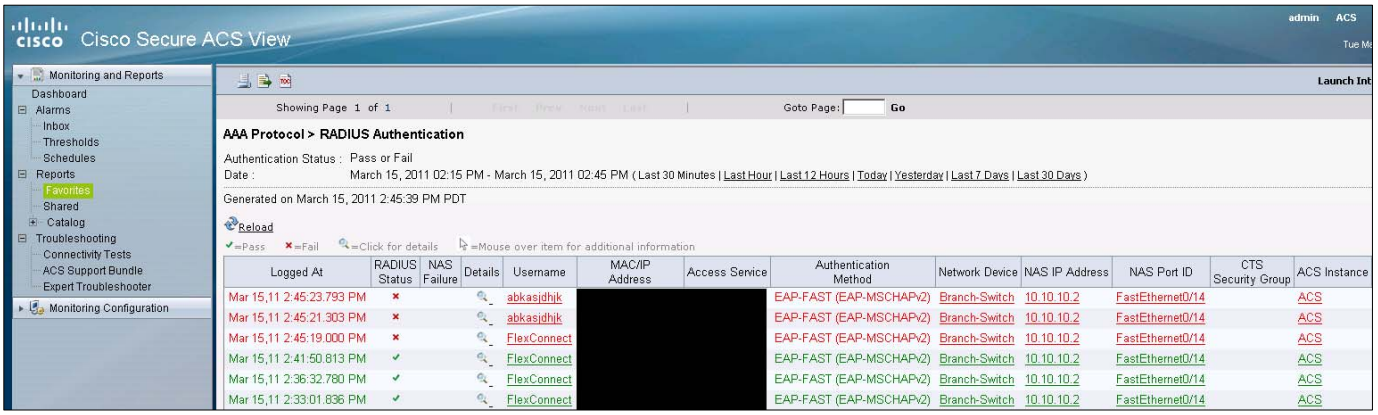
Voice CAC

How are load-based and static CAC options supported by each vendor? CAC at the branch is crucial to preserving the call quality of existing calls with limited WAN bandwidth or when latency issues limit the addition of new client voice calls.

On the Cisco Flex 7500 controller, CAC was set to a static value of 5% bandwidth. A voice call was placed between a pair of wireless handsets. When we attempted to initiate another voice call, the client received a “Network Busy” message, indicating that CAC was limiting the number of clients on the network. We observed that out of a bandwidth available of 6,250 kbps, 1,072 kbps were being used. Next, we changed the CAC to 20% of bandwidth. This time, the additional wireless client was able to make a call successfully. The bandwidth being used was reported as 3,184 kbps out of 6,250 kbps available. CAC functionality is only supported when the access points are connected to the wireless controller. See *Figure 1* on page 1.

Motorola WiNG v5.0 also supports CAC, and can limit based on amount of airtime and by number of wireless clients. The settings are somewhat confusing, for example the setting for Maximum Airtime specifies a range of 0-150, but it is unclear what the unit of measurement is. We began with Maximum Airtime set to 5. A call was successfully established between a wireless phone to a wired phone. Next we associated a second wireless phone with the AP and attempted a call. This phone received a “Network Busy” message, and no call could be made. A successful call was made after increasing the Maximum Airtime to 20, however a radio reboot was needed to implement the setting change. A second call was successfully established between two more wireless clients. This demonstrated that Motorola was effectively limiting the number of clients based on amount of

Figure 2: Failed Port Authentication



Source: Miercom, April 2011

When the incorrect 802.1x authentication credentials are supplied, devices cannot authenticate with the ACS 5.2 server. Failed authentications are displayed above in red. This prevents installation of rogue devices.

bandwidth available. As with Cisco, CAC functionality is only supported as long as WAN access to the controller is available.

Aruba VBN 2.0 supports CAC in tunnel mode, but does not support CAC in bridged mode. In branch deployments, the bridged mode is used for the operation of CAC.

Port-based AP 802.1x Authentication

Wireless branch deployments have a greater threat of rogue devices being installed, which could compromise the security of the network. Port-based 802.1x authentication on the wired network provides increased security by requiring that proper credentials are entered. These are checked against the ACS/Radius server before the access point can join the network. We evaluated each solution for the provisioning of network security.

Cisco FlexConnect uses the branch switch as a proxy for authentication. Port security was enabled on the branch switch. The AP was provisioned with the proper 802.1x credentials, connected to the switch port and verified that it successfully joined the controller. The ACS uses Radius and a shared secret, and the AP supports the 802.1x supplicant which is required to authenticate the AP to the edge switch. Rogue APs will not authenticate and will not receive an IP address. See *Figure 2*.

Neither Motorola nor Aruba support 802.1x supplicant at the access point. The Motorola RFS 4000 controller features an area for 802.1x authentication, but the Enable check box is grayed out and the option cannot be selected.

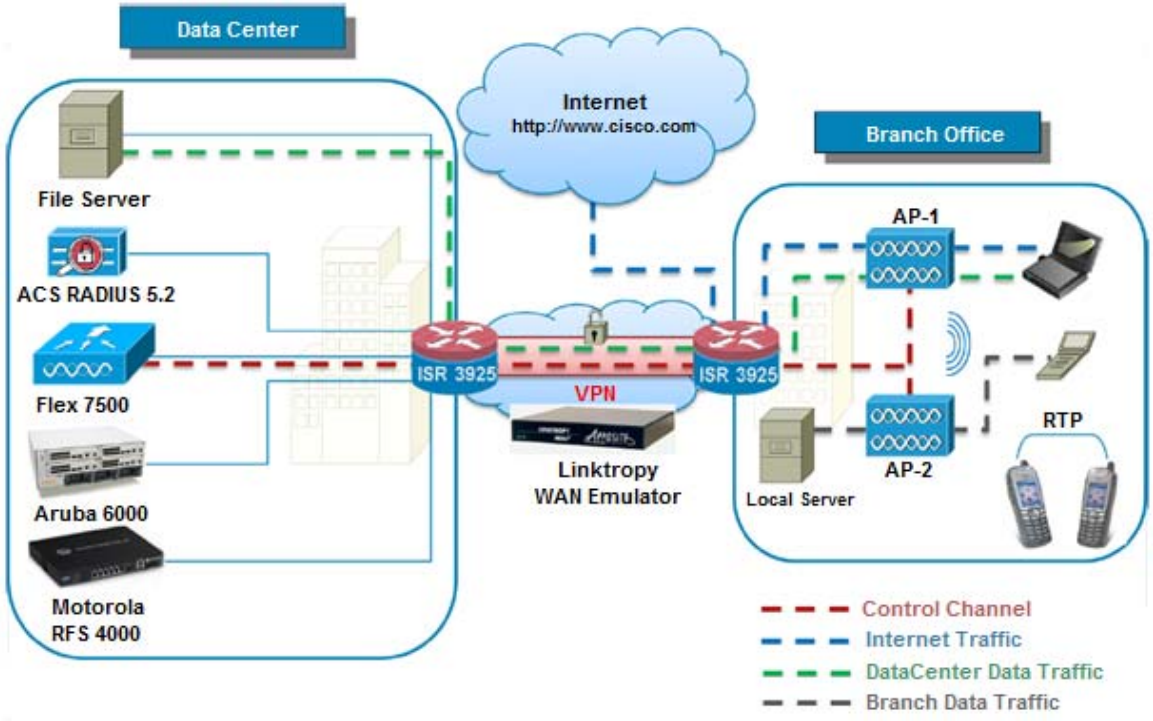
Bottom Line

For a large customer with deployments using a wireless strategy to branches, resiliency of the branch architecture and cost containment of deployment are key considerations. The FlexConnect architecture featured in the Cisco Flex 7500 Wireless Controller was the only solution in this test which thoroughly satisfied these metrics.

FlexConnect architecture provides the ability to authenticate clients locally with the AP when central authentication is unavailable due to a controller or WAN link failure. Roaming continued within the branch when the WAN link was down. To provide the same level of resiliency, other solutions would require primary and backup controllers for each branch location, increasing the cost of branch deployment. Cisco FlexConnect uses 802.1x authentication to prevent rogue access points from being installed in the branch, increasing network security.

Cisco FlexConnect featuring the Flex 7500 Wireless Controller is a well-executed solution for providing Wireless Branch Survivability.

Test Bed Diagram



How We Did It

The network architecture at the data center consisted of the Cisco Flex 7500-Series Wireless Controller, Aruba 6000 Controller v6.0.0.1, Motorola RFS 4000 v5.0.3.0-001R, Cisco ISR 3925 providing a Site-to-Site VPN, a file server (Windows Server 2008 R2) and Cisco ACS 5.2 authentication server running in VMware ESX. At the branch office, we had Cisco Aironet 3500-Series and 1040-Series Access Points configured in FlexConnect mode, also known as HREAP (Hybrid Remote Edge Access Point), Aruba AP 105 in Remote AP mode, Motorola AP 650, Cisco 3925 (providing VPN and Call Manager functions), and wireless clients (laptops and Cisco 7921G IP phones). The data center was linked to the branch office via a WAN connection through a VPN, throttled down to a T1 with an Apposite WAN emulator. The branch office contains two APs from each vendor, a wireless PC client, two wireless Cisco VoIP clients and a wired Cisco VoIP phone.

Each controller is configured specifically for a branch site. This allows wireless users at branch sites to access the Internet directly instead of going back to the data center then to the Internet. Internal traffic stays local and Internet and data center is forwarded out a different path based on an access rule in the router. This branch deployment saves WAN bandwidth and increases speeds for branch users. The two APs are located approximately 30 feet away from each other with the lowest signal strength configured. The low signal strength on the APs ensure that the signals don't overlap, making it easier for roaming testing.

The Apposite Linktropy WAN Emulator www.apposite-tech.com was used to simulate the T1 WAN link between the data center environment and the branch site. The bandwidth between the two sites was limited to a 1.44 Mbps link, latency was set to 40ms on both ends and packet loss set to .1%.

Each vendor controller holds the same configurations to guarantee fair testing. The testing environment is unchanged during each vendors testing.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Current or prospective customers interesting in repeating these results may contact reviews@miercom.com for additional details on the configurations applied to the System Under Test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a selection.

Miercom Performance Verified

Based on our testing and observations, the Cisco Flex 7500 wireless LAN controller is awarded Performance Verified for its survivability and branch office resiliency when compared to similar products.

Miercom tested authentication processes when the controller or WAN link failed, observed roaming voice calls during a WAN failure, examined the CAC support for limited bandwidth situations, and analyzed how FlexConnect architecture protected against rogue access points.

In each of these cases, the Cisco FlexConnect solution clearly demonstrated its advantages in providing mobile branch survivability, while also containing the cost of wireless branch deployments by not requiring a controller be installed in each branch.

Cisco Flex 7500

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
1-800-553-6387
www.cisco.com

About Miercom's Product Testing Services

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including Network World, Business Communications Review - NoJitter, Communications News, xchange, Internet Telephony and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the NetWORKS As Advertised program, the industry's most thorough and trusted assessment for product usability and performance.