Center for Convergence and
Emerging Networking Technologies

Network Technology Performance Evaluation
Cisco Wireless High Availability

July 31, 2013

School of Information Studies
SYRACUSE UNIVERSITY

Executive Summary

Dramatic improvements in wireless networking combined with an increasingly important role for mobile devices is driving a trend towards Wi-Fi as the primary network access mechanism in many networks. An increasing number of enterprise networks and especially mission critical networks like healthcare cannot afford to have application sessions drop at any cost. These trends are driving CIO's and network managers to demand increasing levels of service resiliency. Wireless network vendors are addressing these needs by implementing new capabilities, more intelligent wireless networks, that are able to prioritize mission critical traffic and dynamically recover from component failures. High availability (HA) services are not new. Vendors have long supported key HA capabilities, including dynamic RF management to mitigate AP failures or interference as well as dynamic failover of AP's to backup controllers, should a primary controller fail. However, while these first-generation failover services have decreased the duration of service outages from hours to minutes, they have failed to meet the test of user transparency. Applications often time out and users are usually forced to reauthenticate once an AP has failed over to its backup controller. To meet service standards, enterprises and other vertical industries need more sophisticated failover services that are stateful in nature, presenting themselves as a nearly imperceptible delay in network access for users and complete restoration of application sessions.

Cisco approached Syracuse University's Center for Convergence of Emerging Networking Technologies (CCENT), an applied technology research lab with 15 years of experience testing Wi-Fi products, to perform a systematic beta test, including before/after benchmarking of several applications, of their newest Wireless LAN Controller (WLC) Software (code version 7.5), which includes a new controller failover feature called Client Stateful Switchover (Client SSO). We tested this new service offering on our wireless testbed that included Cisco 5508 Wireless LAN controllers and the Cisco AIR-2602i access point. Client SSO represents an evolution in HA services for Cisco's Unified Wireless Network Access architecture. For many years, Cisco supported stateless failover of AP's to a backup controller. In August 2012, they introduced stateful AP failover capabilities to speed up the failover process, and while most applications would recover in 3 to 4 seconds, client state was not maintained and re-association was required. The release of v7.5 builds on this by promising stateful failover of not just AP's but client state as well. This new Client SSO service copies AP and client state information from the primary controller to the secondary controller's memory on a constant basis in the background. The promise is imperceptible application downtime on the client side in event of a primary controller failure. What previously took 3-4 seconds to occur now takes place in milliseconds.

Key Findings:

1. Time sensitive applications like Microsoft Lync, Citrix VDI and Adobe Connect experienced **imperceptible application downtime** in the event of a controller failover event
2. The failover time in **v7.5 is 98% less than that in v7.4** which only supported AP Stateful Switchover.
3. The failover time in **v7.5 is 99% less than that in v7.2** which supported only state-less failover.

Test Methodology

A team of 3 graduate students, with supervision from a faculty member responsible for the CCENT wireless testing projects, worked with technical representatives from Cisco's Wireless Networking Group (WNG) to configure Cisco's new failover services on the wireless test-bed in our lab. The testbed consisted of Cisco's failover-enabled wireless network infrastructure and a range of typical enterprise application services that we used to evaluate failover services. We focused our efforts on three commonly deployed enterprise applications - Citrix XenDesktop 5.6 VDI, Microsoft Lync 2010, and Windows file sharing using Common Internet File System (CIFS). We also used Adobe Connect to assess an educational application and a Cisco 7921G phone to assess the experience for a VoIP phone. To measure the application downtime, we used online time meter, which allowed us to measure application response time in milliseconds. The timer was started once we detected that an application stopped working and the timer was stopped once applications started to work again. In addition, we also used a ping utility to record exact times when client sessions were dropped and subsequently restored. To get granular measurement for Client SSO, the delay between each ping packets was set to 100 milliseconds so we were able to measure system recovery time by counting the number of dropped pings and multiplying times 100 milliseconds.

In order to ensure accurate measurements, the testbed was isolated from the University's wired and wireless systems. A Cisco 2911 Router configured for NAT services was used to provide access to testbed devices, when necessary, from the University network. Our network testbed included a Cisco 3750 Catalyst Switch, a Cisco UCS C210 server running VMware ESXi 5.0 that hosted all our Virtual machines, including an Active Directory Domain Controller, Lync 2010 Server, Citrix XenDesktop controller and VMs (see Figure 1 below). For tests involving Adobe connect, we accessed those services from Syracuse University's network, through which we established and tested video collaboration sessions between two wireless clients on our testbed. All testing was performed with both Macbook Pro and Dell laptops Latitude E6430 equipped with 3-stream capable 802.11n network adapters. In our preliminary testing, we were not able to detect any differences between these two client types. The network was configured using WPA2-Enterprise authentication and PEAP authentication on the backend RADIUS server. All reported test results are based on the Dell laptops. All performance testing took place on the second floor of Hinds Hall, home to SU's School of Information Studies, in a typical enterprise cube office (inside the CCENT Lab).

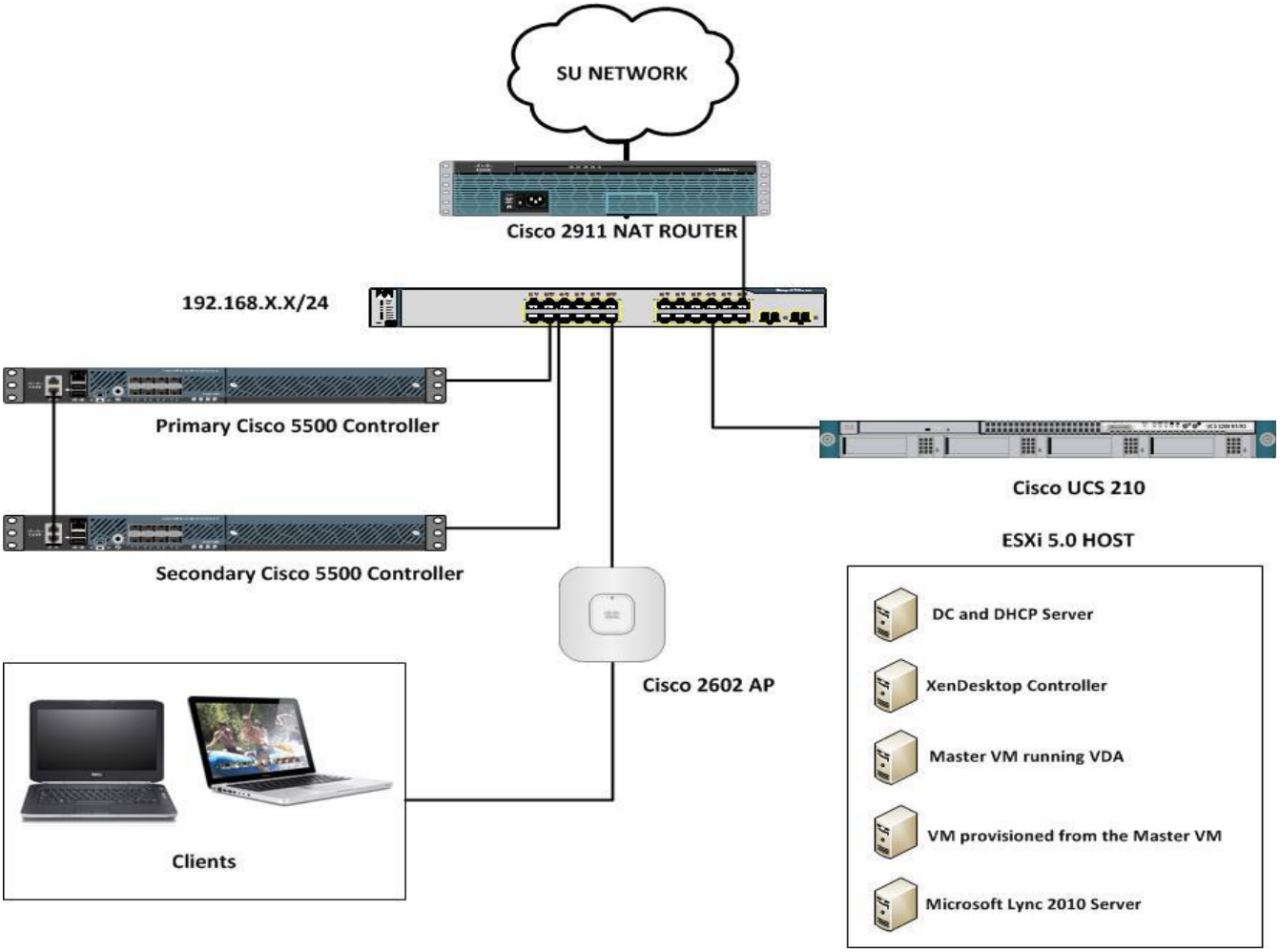

Figure 1 Network Testbed Diagram

Applications Tested

PING

PING is stateless traffic that provided a basic indication of how long the network is down for. All of the other applications are stateful, therefore we record how long each application resumes the session in our test. To obtain a granular view on Ping traffic in milliseconds, we implemented the Fping Utility which run on the command prompt, allows the user to fine-tune options on the delay time between pings, length of data on the ICMP packet and much more. We had modified the utility to display continuous ping traffic with a delay time of 100 milliseconds between ping intervals to the gateway, to have a precise measure of the failover seen in the network traffic.

```
Syntax: >Fping.exe <Gateway IP address> -t 100(milliseconds) -c (continuous)
```

Microsoft Lync 2010

To evaluate a typical enterprise unified communications system, we chose Microsoft Lync 2010 as our target application for SSO testing. This included Microsoft Lync voice and video calls.

Cisco VoIP Phone

Rather than the traditional PBX system, enterprise industries trend to invest in a more flexible and cost effective Voice over IP system as their means of communications within and outside their network. After Installing the Call Manager Express version 4.1 on the Cisco ISR 2811 router and integrating it to the network, we connected a Cisco 7960 IP phone on SCCP Firmware file Version 7.x on the wired network and the Cisco 7921G wireless IP phone on SCCP Firmware file Version 8.x through the Wireless network using the PEAP authentication protocol. We then initiated a call between the two phones to test the effects of the failover.

Citrix XenDesktop

Citrix XenDesktop has achieved increasing popularity within enterprises in recent years as a mechanism for remotely delivering application services. XenDesktop provides location and device independent secure virtual desktop and application services to users. As a network-intensive service, it is highly sensitive to performance issues. To test failover with this application, we configured one wireless client to stream HD 1080p video through the Citrix VDI session.

Windows File Transfer

File Transfer between two Windows PCs happens every day in enterprise wireless networks. In this test, we configured one client to copy a 40 GB shared folder from the vCenter Server (connected to the switch through wire). Continuous file transfer was taking place between a wireless client on the same network.

For each application, to test the result failover on application performance, we simulated failover by pulling the plug off of the primary controller while the applications were running.

Results

The following tables and graphs show the application downtime as well as ping drops experienced by the clients in the event of primary controller failure for three WLC software code versions that feature different types of failover mechanisms.

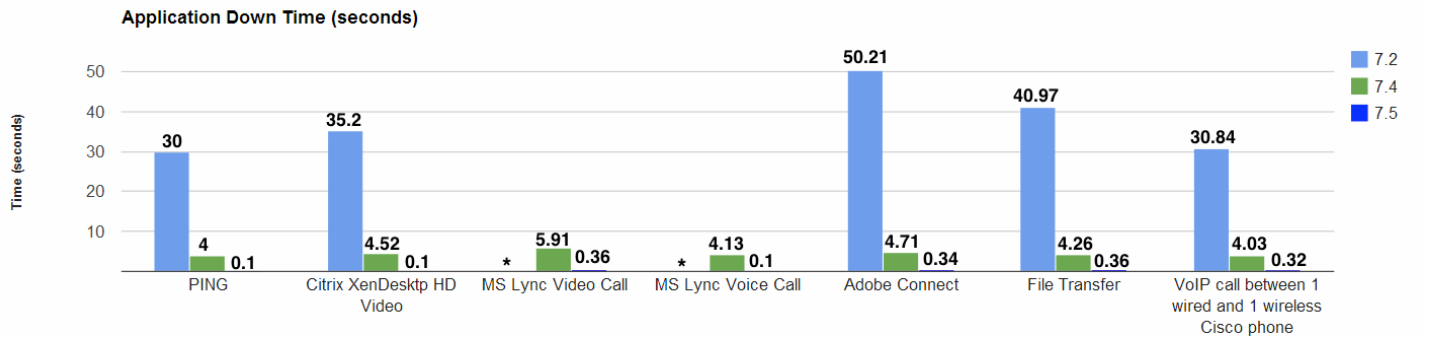

Figure 2
Application Downtime Performance of Cisco WLC Code Versions

Application Down Time (seconds)			
	7.2	7.4	7.5
PING	30.00	4.00	0.10
Citrix XenDesktp HD Video	35.20	4.52	0.10
MS Lync Video Call	- *	5.91	0.36
MS Lync Voice Call	- *	4.13	0.10
Adobe Connect	50.21	4.71	0.34
File Transfer	40.97	4.26	0.36
VoIP call between 1 wired and 1 wireless Cisco phone	30.84	4.03	0.32

*** The calls were dropped and session never resumed**

Table 1
Application Downtime Performance of Cisco WLC Code Versions

Conclusion

Our performance testing, while not exhaustive, verifies that Cisco's Stateful Switchover (SSO) is effective in rapidly restoring wireless LAN services in the event of a controller failover. We measured reductions in application downtime of between **92 and 98 percent** compared to earlier product offerings. Measurable application downtime was always less than a second, a marked improvement from earlier failover services.

Delta between 7.4 and 7.5			
	7.4	7.5	Delta
PING	4	0.1	Decreased by 98%
Citrix XenDesktp HD Video	4.52	0.10	Decreased by 98%
MS Lync Video Call	5.91	0.36	Decreased by 94%
MS Lync Voice Call	4.13	0.10	Decreased by 98%
Adobe Connect	4.71	0.34	Decreased by 93%
File Transfer	4.26	0.36	Decreased by 92%
VoIP call between 1 wired and 1 wireless Cisco phone	4.03	0.32	Decreased by 92%

As Enterprise Wi-Fi systems continue to mature and improve, employing more sophisticated architectures that improve security, management, performance, and resiliency. Cisco's focus on improving application failover through its newly enhanced SSO offerings represents a behind-the-scenes improvements that most network managers hope they never need to take advantage of. This is indicative of the evolution of wireless network services. The easiest problems have already been solved, allowing Cisco and other vendors to concentrate on more subtle enhancements that allow enterprises to approach availability levels traditionally associated with wired networks.