TEST REPORT

Tolly.

#212116

May 2012

Commissioned by Alcatel-Lucent

Alcatel-Lucent Converged Network Solution

High-Quality User Experience with an Application Fluent Network

EXECUTIVE SUMMARY

With the increased adoption of multimedia applications such as video, Unified Communications, collaboration suites, and the rapid adoption of next-generation devices and mobility, it is imperative to have a robust LAN infrastructure that is always-on and provides sufficient bandwidth, switching capacity and automatic adjustments to support unpredictable traffic patterns. The Alcatel-Lucent Converged Network Solution provides a reliable and high-quality end-user experience with an intelligent network that can automatically adjust its behavior based on the context of the users, devices, and applications involved in what Alcatel-Lucent terms a "conversation".

Tolly measured failover time and its effect on multimedia applications in the event of possible failures in the network - including power supply, core switch, and link failures. Tolly found the Alcatel-Lucent Converged Network Solution provides a sustained, high-quality user experience for video and voice, recovering from failures within 55ms, on average, when deploying the OS6900 and OS6450. Tolly also verified the network's capability to adjust automatically based on the context of the user or device connected, as well as possessing functionality which facilitates operations, management and administration. See Figure 1.

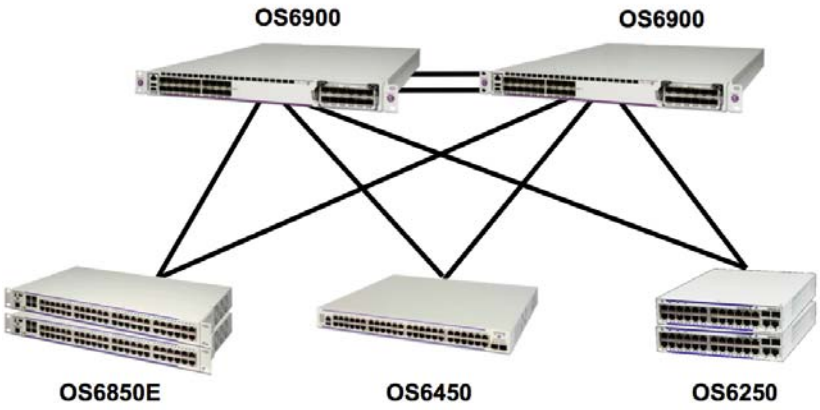
Tests were conducted using the Alcatel-Lucent Compact Core Architecture, featuring a selection of the recently-launched OmniSwitch™ LAN Switch Series.

THE BOTTOM LINE

The Alcatel-Lucent Converged Network Solution:

1. Provides sustained high-quality telephony and video during network failures
2. Is able to enforce security, quality and bandwidth policies based on the context of users and devices connected
3. Simplifies deployment of a network by the use of automated provisioning
4. Recovers from failures within 55 ms, on average, when deploying the new generation OmniSwitch™ 6900 at the core and OmniSwitch™6450 at the access layer

Quality of User Experience with OmniSwitch™ Network Infrastructure



FAILURE EVENT	VOICE CALLS	STREAMING VIDEO
POWER SUPPLY	SUSTAINED HIGH-QUALITY	SUSTAINED HIGH-QUALITY
CORE SWITCH	SUSTAINED HIGH-QUALITY	SUSTAINED HIGH-QUALITY
NETWORK LINK	SUSTAINED HIGH-QUALITY	SUSTAINED HIGH-QUALITY

Source: Tolly, April 2012

Figure 1

Background

Introduction

A robust and highly-available network infrastructure is critical to provide end-users with a high-quality experience, especially when accessing demanding multimedia applications such as voice and video.

Engineers built a network that conforms to the Alcatel-Lucent Compact Core blueprint of the Converged Network Solution featuring the OmniSwitch™ 6900 at the core and the entire OmniSwitch™ access switch series at the access layer, including the new OmniSwitch™ 6450. Along with data traffic, test traffic also included real-time applications such as VoIP telephony and IP multicast video streams.

Tests aimed to evaluate multiple aspects of the Alcatel-Lucent Application Fluency approach (See Alcatel-Lucent sidebar). First, Tolly verified the ability of the Alcatel-Lucent implementation of Multi-Chassis Link Aggregation (MC-LAG) and Link Aggregation (LAG) to offer superior resiliency to link or switch failures in comparison to conventional deployment using IEEE STP-based networks. During the test, Tolly evaluated the impact of these failures on voice and video applications.

Tolly audited the solution's ability to automatically adjust network behavior based on the context of the user or device using a functionality known as the User Network Profile (uNP).

Tolly also verified functional capabilities intended to simplify operations, including automatic provisioning and alerts by the Network Management System (Omnivista™ 2500 NMS) to warn operators of network failures.

Test Results

Resilient Architecture

Core Switching Failures

The core of the converged network solution consists of two OmniSwitch 6900 10GbE switches that are set up to act as peers in a Multi-Chassis Group (See Figure 3). By using a Virtual Fabric Link (VFL) in between peers, the Multi-Chassis Group is able to act as a single chassis and connect to other switches and/or servers using standard link aggregation. This provides a highly-available network core with all links

Alcatel-Lucent Converged Network Solution

User Quality Experience Evaluation

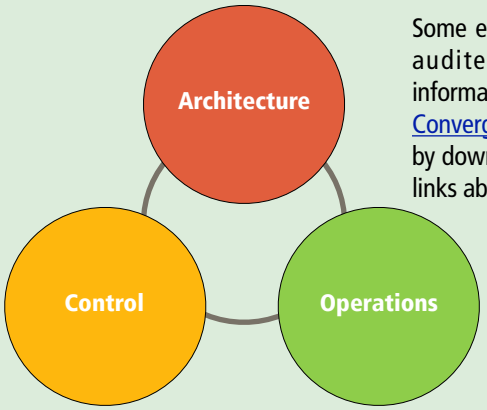
Tested April 2012

Alcatel-Lucent Application Fluent Network

An Application Fluent Network is Alcatel-Lucent's vision for network infrastructures that understand the context of users, devices and applications involved in a conversation and adapt to ensure a high quality user experience.

The Converged Network Solution follows the application fluency principles, which are realized by considering three pillars:

- **Resilient Architecture:** Simplified architecture, fast re-convergence on failures, secure, etc.
- **Automatic Control:** Network automatically adjusts behavior based on the context of user, device or application
- **Streamlined Operations:** Less IT intervention, low-touch provisioning, simplified operation & reduced operational cost



Some elements of each of these pillars are audited in this test report. More information on Application Fluency and Converged Network Solution can be found by downloading documents available at the links above.

Source: Alcatel-Lucent. Content not verified by Tolly.

Specific System Failures and Impact on Application Quality

Average Traffic Interruption Time and Subjective User-Quality Impact on Voice and Video

Unsolicited Events (Failures) Effects				
Event	Traffic Interruption In Milliseconds (ms)	Audio Quality	Video Quality	Notes
OS6900 VFL Link Failure	0 ms	No Impact	No Impact	0 ms on all flows
OS6900 Single Power Supply Failure	0 ms	No Impact	No Impact	0 ms on all flows
OS6900 Core Switch Failure	54 ms	No Impact	No Impact	Multiple flows with range between 0 and 238 ms
OS6850E Stack Uplink Failure	80 ms	No Impact	No Impact	Multiple flows with range between 0 and 204 ms
OS6450 Uplink Failure	55 ms	No Impact	No Impact	Multiple flows with range between 0 and 203 ms
OS6250 Stack Uplink Failure	107 ms	No Impact	No Impact	Multiple flows with range between 0 and 236 ms

Note: Audio and video quality are subjective measures and thus in this case, "no impact" means that the session was uninterrupted by the link or switch failure.

Source: Tolly, April 2012 Table 1

active during normal operation for full bandwidth availability. This is referred to as "Core Switching".

Tolly engineers initiated multiple core switching failures, including power supply failure of a peer switch, a link failure on the VFL aggregate, peer switch failure, and failure of link between core switching and access switching.

During these failures, Tolly engineers recorded subjective opinion (visual and audible human perception - no measurement via equipment) of the impact these failures had on the performance of real-time, multimedia applications such as IP telephony and multicast video streams. Times were recorded in milliseconds (ms).

Overall, Tolly engineers found that the network recovered from an uplink (between a core and access switch) failure in under 110 ms, on average. In all failure cases, the audio and video quality were not impacted. See Table 1.

Furthermore, a network with only the OS6900 and OS6450 switches experienced an interruption of only ~55 ms, on average.

For both the VFL link and single power supply failure on the OS6900 peer switches at the core, the average traffic interruption was 0 ms (no interruption) on all flows, and did not affect the subjective voice or video quality adversely.

A complete peer switch failure on the OS6900 core switches resulted in a traffic interruption of just 54 ms on average. The failure had no detectable impact on continuity of video or voice sessions, or their quality.

The failure of an uplink between the OS6850E switch stack and the OS6900 core switches resulted in an average 81 ms of traffic interruption. The failure of these links did not cause any detectable impact on the video or voice quality.

Similarly, the failure of an uplink between the OS6450 switch and the OS6900 core switches caused 56 ms of traffic interruption. The link failure did not cause any detectible impact on the video or voice quality.

Finally, the failure of an uplink between the OS6250 switch stack and the OS6900 core switches resulted in 108 ms of traffic interruption. The failure did not cause any detectible impact on the video or voice quality.

Conversations Managed in Context

User Network Profile (uNP)

Network conversations can be managed in proper context by leveraging the networks' ability to recognize users and devices and bind them to a User Network Profile (uNP) that dynamically sets up VLAN, ACL and QoS policies based on who or what is connected to the switch port. This recognition of users and devices is achieved

by monitoring the traffic on a specific switch port.

The Alcatel-Lucent switches can analyze MAC address or use authentication methods such as 802.1X or Captive Portal to determine the nature of the user or device attempting to access the network. This allows the network to understand the context of each conversation and automatically adjust the configuration of VLAN, QoS, ACL, bandwidth restriction policies and even enforce a Host Integrity Check (HIC).

Tolly engineers tested this functionality by using a laptop shared by two types of users, "tolly" - a low-privilege user, and "engineering" - an administrator-level user, connecting to the same switch port. Engineers defined "Deny FTP", "Deny Telnet" and "DSCP 46" policies. See Table 2.

Depending on the profile of the user, the switch assigned different Quality of Service (QoS) policies and/or Access Control Lists (ACL) to the traffic.

When user "tolly" (a basic-level user) logged in, the uNP profile configured for the user was returned from the RADIUS authentication server, and the uNP was assigned to the switch port. The associated QoS and Authentication, Authorization and Accounting (AAA) policies were then applied on the port. When the user "tolly" tried to access FTP and Telnet services, the switch blocked the attempts and logged the hits against the AAA rules blocking these actions. Tolly engineers then verified the switch interface to show the rule-match incidents.

When the user "engineering" (administrator-level user) logged in, the uNP profile configured for the user was returned from the RADIUS authentication server, and the uNP was assigned to the switch port. The associated QoS and AAA policies were then applied to the port and the switch port was placed in a VLAN 72, as specified by the uNP configuration.

In addition to managing access and permissions based on the user, the Converged Network Solution is able to identify devices and adjust the switch port configuration accordingly to the uNP associated with that device. In this case, an IP telephone set was associated with the uNP profile "phone". The VLAN on the switch port changed automatically to the voice VLAN (ID 75, as defined in the uNP) when the telephone was connected. See Figure 3.

The capabilities of the uNP feature allow the network to dynamically adjust its configuration based upon the context of a particular conversation, to deliver the optimal level of service to the end-user or application.

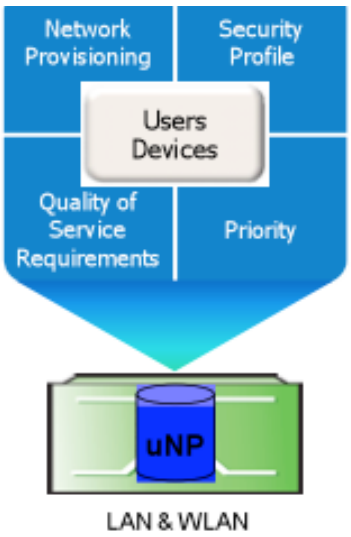
Streamlined Operations

Tolly engineers verified the capabilities of the Converged Network Solution to streamline the administrative and maintenance operations like software/firmware updates, endpoint provisioning, event monitoring, etc.

Remote Configuration Load

The OmniSwitch series of switches implement a feature called "Remote Configuration Load" (RCL), which enables an OmniSwitch to automatically download switch configuration instructions and software/firmware updates from a network server at boot time. RCL was demonstrated on the OmniSwitch 6450 switch to trigger at boot up based on an installation file or using a script file. Engineers also verified that an administrator could abort an RCL process in progress by simply logging into the switch.

User Network Profile (uNP) Diagram



Source: Tolly, April 2012 Figure 2

Automatic Endpoint Provisioning

Tolly engineers also verified the capability of the OmniSwitch switches to automatically provision an endpoint based on its LLDP-MED profile (the standard for multimedia endpoint discovery). This feature was demonstrated on an OmniSwitch 6450. When a multimedia endpoint such as an IP telephone was plugged into the switch, engineers verified that the telephone automatically downloaded an available firmware update or software configuration during the boot-up process. As part of this provisioning process, engineers verified that the phone registered with the call server, obtained an extension number, and that the switch port was reassigned from a regular VLAN to a dedicated voice VLAN.

RADIUS Server Configuration

RADIUS Server		
User	Password	Role
tolly	****	"basic-level user"
engineering	****	"administrator"
<IP Phone MAC Address>	N/A	"phone"

User Network Profile (uNP) Configuration and Policy List in the OmniSwitch

uNP Profiles			
Profile Name	VLAN ID	HIC (Enabled/Disabled)	Policy List Name
"basic-level user"	71	Disabled	"Block-FTP-Telnet"
"administrator"	72	Disabled	"High-Priority QoS"
"phone"	75	Disabled	No Policy List Assigned

Policy List	
List Name	Policies
"Block-FTP-Telnet"	DenyFTP, Deny Telnet
"High-Priority-QoS"	DSCP 46

Source: Tolly, April 2012

Table 2

OmniVista 2500 NMS

Tolly engineers examined the OmniVista 2500 Network Management System (NMS) for its capability to provide a centralized interface to monitor and manage alarms, warnings, and event notifications across the entire network.

The OmniVista interface showed a detailed list of granular network link and node-level events, as well as a detailed topological view of all the network links and devices. (See Table 3 and Figure 4.)This level of detail on the state of the network facilitates operations and allows network administrators to take appropriate actions to ensure quality network availability and service.

Test Bed Setup & Methodology

Test Bed Setup

The test bed centered around Alcatel-Lucent's OmniSwitch family of core and access layer switches. Engineers set up a microcosm of an enterprise-scale LAN consisting of distinct access and core switches, "Compact Core", and data center components as depicted in Figure 3.

The data center network consisted of a pair of OmniSwitch 6900 switches, along with Alcatel-Lucent's OXE Call Server to handle the VoIP calls, a multicast video server, and associated servers for network services such as RADIUS authentication server, DNS and DHCP servers. The data center switches were connected to the "Compact Core" network using two 10Gigabit Ethernet (10GbE) links. The tests focused solely on the Compact Core. The data center network was used to provide the applications needed to run these tests.

The Compact Core network consisted of a simplified two-layer architecture. At the core were two OmniSwitch 6900 switches, connected to each other using two Virtual Fabric Links (VFLs) utilizing 10GbE links.

At the access layer, three types of OmniSwitch switches were used. First, two OmniSwitch 6850E Stackable Gigabit LAN switches (the 24-port OS6850E models) were used in a stacked configuration. Two OS6250 Fast Ethernet Stackable LAN switches (the 24-port, PoE-capable

OS6250-P24 models) were used in a stacked configuration. Finally, the recently-launched OmniSwitch 6450 Gigabit Ethernet Stackable LAN switch supporting PoE.

Each of the access switches were connected to the core using two uplinks (10GbE links for OS6850E and OS6450 switches, and GbE links for the OS6250 switch). The core used Multi-Chassis Link Aggregation (MC-LAG) technology providing virtualized link aggregation connection to the access switches that were configured with standard link aggregation (LAG) on the uplinks. This solution is designed to maximize the active paths and bandwidth in the network, as well as minimize re-convergence time in the event of switch/link failure.

The OS6900 switches in the core were configured to perform bridging, Layer 3 VLAN routing using OSPF, prioritized IP multicast and VoIP traffic.

The test endpoints consisted of Alcatel-Lucent IP Touch 4028 EE and 4038 EE IP phones and three laptops used to access IP multicast video streams.

In order to be able to receive messages about topology changes and to test downloads of new software into switches, OmniVista 2500 Network Management System (NMS) was appropriately set up and connected to the network infrastructure.

To generate an average load on the network, test traffic was generated using 24 GbE ports from an Ixia Optixia XM-12 traffic generator.

Table of Events Report for OmniVista 2500

Unsolicited Traffic Events (Failures) Report on OnmiVista 2500		
Event	Alarm Properly Reported	Topology Change Displayed
OS6900 VFL Link Failure	YES	YES
OS6900 Single Power Supply Failure	YES	N/A
OS6900 Switch Failure	YES	YES
Link Failure to OS6850E Stack	YES	YES
Link Failure to OS6450	YES	YES
Link Failure to OS6250 Stack	YES	YES

Maintenance/Repair of Failure Report on OnmiVista 2500		
Event	Alarm Properly Reported	Topology Change Displayed
OS6900 VFL Link Failure	YES	YES
OS6900 Single Power Supply Failure	YES	N/A
OS6900 Switch Failure	YES	YES
Link Failure to OS6850E Stack	YES	YES
Link Failure to OS6450	YES	YES
Link Failure to OS6250 Stack	YES	YES

Source: Tolly, April 2012 Table 3

Test Methodology

Resilient Architecture

To measure the recovery times of the network infrastructure topology due to failures on the switches and links, engineers used the Ixia IxNetwork application to generate Layer 2 and Layer 3 traffic consisting of 1,518-byte frames in separate VLANs at the rate of 10,000 frames/packets per second.

In addition, VoIP calls between IP Touch phones in dedicated voice VLANs and IP multicast video streams were accessed from the three laptops. This multimedia traffic traversed the access, core and the data center switches.

The OS6900 switches in the core were configured to perform IP routing using OSPF, prioritized VoIP and IP multicast video streams between endpoints on different VLANs spanning the multiple switches in the data center and the Compact Core Network.

Network link and switch failures were introduced to force the network to re-converge the data and multimedia traffic on to alternative paths with minimum disruption. Re-convergence from failures was calculated by the time the network took to re-converge from disruptions when the links and switches failed as well as when they were restored. Link down disruptions were simulated by unplugging the link(s) from the switch port(s), and link up disruptions were simulated by plugging the link(s) back into the switch port(s). Similarly, the switch failures were simulated by powering down the switch, and switch restores were simulated by powering up the switch.

The re-convergence time is calculated from the number of packets lost while the

network finds an alternative path when a link/switch goes down or comes back up. Since test traffic was transmitted at the rate of 10,000 packets/sec, re-convergence time in seconds was calculated using the formula:

(number of packets lost) ÷ 10,000

Since the network consisted of multiple active data streams across the links and switches, re-convergence time for a particular link or switch disruption only considered the loss on traffic streams that actually traversed those links/switches. On the data streams that were selected on this criteria, engineers noted the maximum re-convergence time among the individual traffic streams, as well as an average of the re-convergence times of all the traffic streams impacted by the particular link/switch failure.

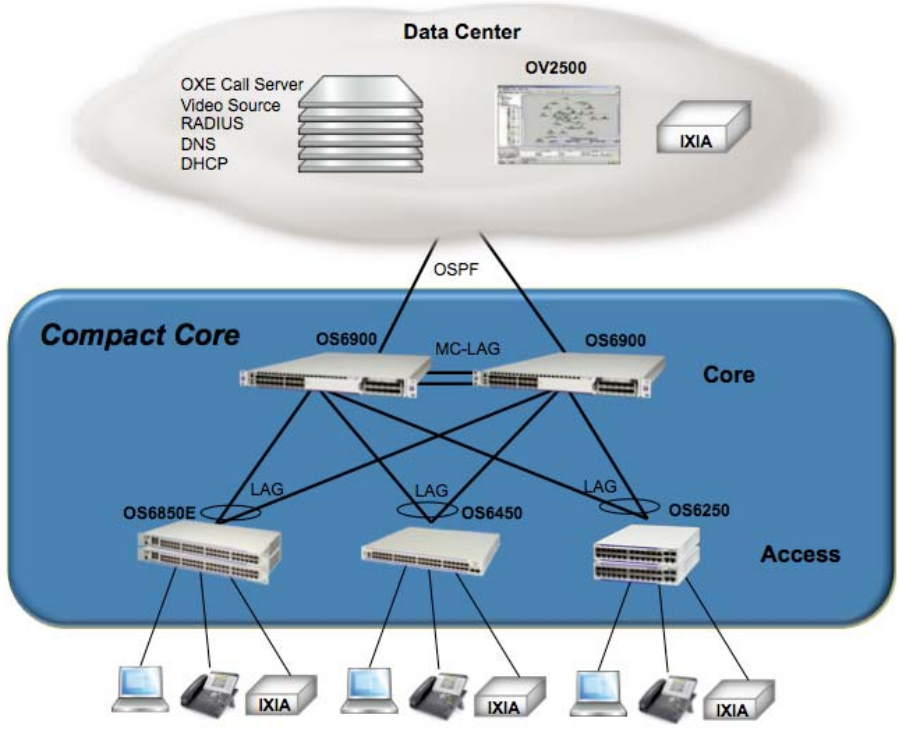
Engineers ran each test three times and reported the average and maximum from the three runs.

Conversations Managed in Context

For this test, engineers configured the User Network Profile (uNP) capability of the OmniSwitch series of switches. The switch can associate a user or endpoint to a particular uNP based on the user credentials using a captive portal, MAC address or 802.1x authentication.

In the scenario using a captive portal, engineers configured two uNP profiles - one for a normal-level user (basic-level user), and one for an administrator-level user (administrator). Each of these profiles were assigned unique QoS policies and ACL rules to the particular switch port based on the authenticated user's group privileges. Specifically, the normal user was assigned a uNP profile that specifies a VLAN ID 71, and ACL rules to deny FTP and Telnet services.

Test Bed Topology



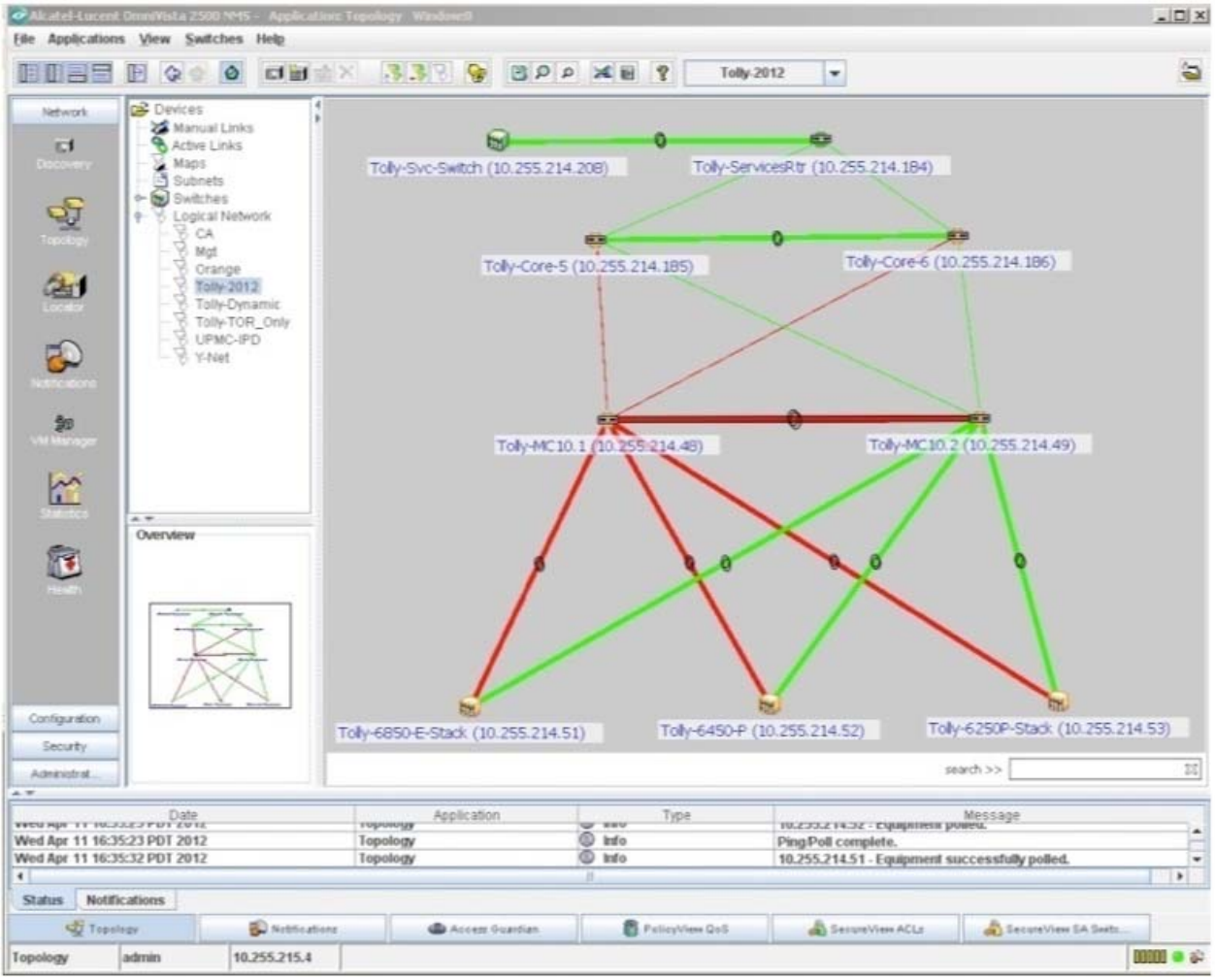
Source: Tolly, April 2012 Figure 3

The administrator-level user was assigned a uNP profile to assign a VLAN ID 72 on the switch port, a DSCP value of 46 to traffic generated by the user and no restrictions on services like FTP or Telnet.

When a laptop was plugged into an appropriately configured OmniSwitch, a user browser session was directed to a captive portal for authentication and assignment of a uNP profile. Tolly engineers verified that a normal user when authenticated was assigned a uNP profile that accordingly prevented access to FTP and Telnet services and assigned a VLAN ID 71 to the switch port. On the other hand, an administrator-level user was assigned the appropriate uNP profile that assigned a VLAN ID 72 on the switch port, and no restrictions on accessing services like FTP and Telnet.

For the scenario of assigning a uNP profile based on MAC address authentication, engineers configured the OmniSwitch to recognize an endpoint like an IP phone and associate a uNP profile (phone), which assigned a dedicated VLAN (ID 75) for VoIP. Engineers then verified this by plugging in an IP phone, and observed that the switch port belonged to one VLAN prior to plugging in the phone, but was then assigned a different VLAN ID (75) when the phone was recognized as a IP phone based on its MAC address.

Snapshot of Topology on OV2500 when a Core OS6900 is Down



Snapshot of Alarm Window on OV2500

Source: Tolly, April 2012

Figure 4

Streamlined Operations

Engineers demonstrated that the OmniSwitch series can help streamline provisioning and maintenance operations through features such as Remote Configuration Load (RCL) and automatic provisioning of multimedia endpoints using LLDP.

To demonstrate the RCL feature, engineers plugged in an OmniSwitch 6450 into the OmniSwitch 6900 core switch.

Tolly engineers verified that when an OmniSwitch 6450 without a configuration file was powered on, a dhcp-client was created on the switch, a dhcp address was acquired from the network and then a file (inst.alu) was automatically executed. The inst.alu file contains a list of commands instructing the switch to download the firmware, configuration files and script files from a network location such as a TFTP server. As part of the DHCP response, it acquires the address of a TFTP/FTP server. The switch downloaded the firmware, or a configuration file, wrote the configuration to memory and then rebooted.

Tolly verified that the inst.alu on the OmniSwitch 6450 could be instructed to bypass the boot.cfg file download and instead execute a script file (script.txt) containing a series of configuration commands, and then write it to the memory as an updated boot.cfg file.

Finally, Tolly engineers verified that a multimedia endpoint, such as an IP phone, could be configured automatically, based on its LLDP profile when plugged into the OmniSwitch 6450. Tolly engineers configured the IP phone to use LLDP-MED to convey its identity and capabilities to the switch. Engineers verified that a switch port belonging to a particular VLAN ID was then assigned to a unique voice VLAN when the IP phone was plugged in. Tolly engineers also verified that the IP phone automatically downloaded an updated firmware and configuration file as part of the boot up process when plugged into the switch.

During all these tests, engineers verified that appropriate SNMP traps for the various network link and switch level events (link/switch failure/restore, LinkAggPortJoin, LinkAggPortLeave, etc.) were displayed in the OmniVista 2500 NMS interface. Furthermore, changes in network topology were represented graphically in the interface.

About Tolly…

The Tolly Group companies have been delivering world-class IT services for more than 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

Test Equipment Summary

The Tolly Group gratefully acknowledges the providers of test equipment/software used in this project.

Vendor	Product	Web
Ixia	**Ixia XM12 with IxOS 5.70.600.13** **10/100/1000-LSM XMVDC16 and 10G-MSM Line Cards.** **IxNetwork 5.60.301.30.**	http://www.ixiacom.com

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.

212116-bsc-mt-kk-wt-23May12-verL