THE TOLLY GROUP

No. 207179 February 2007

Nortel

Nortel Application Switch 2424/3408

Evaluation of Security, Resiliency and Load Balancing on a Network Supporting Microsoft Live Communications Server 2005 and Nortel Multimedia Communication Server 5100

Tolly Up to Spec Certified — Test Summary

Premise: *The convergence of voice, data and video services onto the enterprise LAN demands that the underlying infrastructure deliver load balancing and resiliency for servers that support converged services like enterprise instant messaging, voice, video and other real-time services.*

Nortel commissioned The Tolly Group to evaluate a converged network infrastructure for Enterprise users to illustrate the load balancing capabilities of its Nortel Application Switch 2424/3408.

Telephony and video services were built on the Microsoft Live Communications Server 2005 Enterprise Edition (referred to as "LCS", hereafter) or Nortel Multimedia Communication Server 5100 (referred to as "MCS" hereafter) servers running in a resilient, multi-site network with each site consisting of a Nortel Application Switch 2424 or 3408 and multiple Nortel Ethernet Routing Switches (ERS) 8600 units at the core communicating with ERS 8300 and ERS 5520 switches at the network edge. Users placed voice and video calls across the test network.

Tests attempted to show Nortel Application Switch support for Server Load Balancing for servers running Nortel MCS or Microsoft LCS - either locally, or across the network. Tests also illustrated the ability of the Nortel Application Switch to detect and block security attacks like Distributed Denial of Service (DDoS) attacks.

Tests were conducted in November 2006.

Test Highlights

- Nortel Application Switch 2424/3408 successfully detects and blocks Distributed Denial of Service (DDoS) security attacks
- Nortel's Global Server Load Balancing solution operating on the Nortel Application Switch delivers uninterrupted service to Microsoft Live Communications Server 2005 (LCS) and Nortel Multimedia Communication Server (MCS) 5100
- Microsoft LCS and Nortel MCS servers can be load balanced for faster response, increased reliability, and to maintain user sessions seamlessly in the event of an outage to other LCS and MCS servers in the network
- User voice and video sessions migrate gracefully during failover of the Application Switch or when the local LCS or MCS server managing those sessions failed

Global and Local Server Load Balancing on Nortel Application Switches Supporting Microsoft Live Communications Server 2005 and Nortel Multimedia Communication Server 5100

	Global Server Load Balancing (GSLB) *	Local Server Load Balancing (SLB) *
Resiliency with uninterrupted user voice and video sessions	☑	☑
User session load balancing	Across the network	Local (On site)

* **Note:** GSLB support was tested for both Microsoft LCS and Nortel MCS, while Local SLB was tested only on Microsoft LCS. GSLB resiliency was tested by failing the Application Switch controlling the MCS or LCS server to induce transfer of user sessions to other active MCS or LCS servers network wide. SLB resiliency was tested similarly, though sessions transferred to LCS servers on site.

Source: The Tolly Group,November 2006

Figure 1

Executive Summary

Nortel Application Switches successfully provided a high level of network resiliency while load balancing Nortel's Multimedia Communication Server (MCS) and/or Microsoft Live Communications Server 2005 (LCS) servers.

Tests show that Nortel's load-balancing features of the Nortel Application Switch are capable of managing and balancing user sessions shared between Nortel Multimedia Communication Server (MCS) or Microsoft LCS servers in a network, locally and/or network wide.

Active voice and video calls handled by an MCS or LCS server in the test network continued uninterrupted even when the primary link to the network core from an Application Switch supporting MCS or LCS server was failed — effectively isolating the Application Switch, and thereby the MCS or LCS Servers connected to it, from the network.

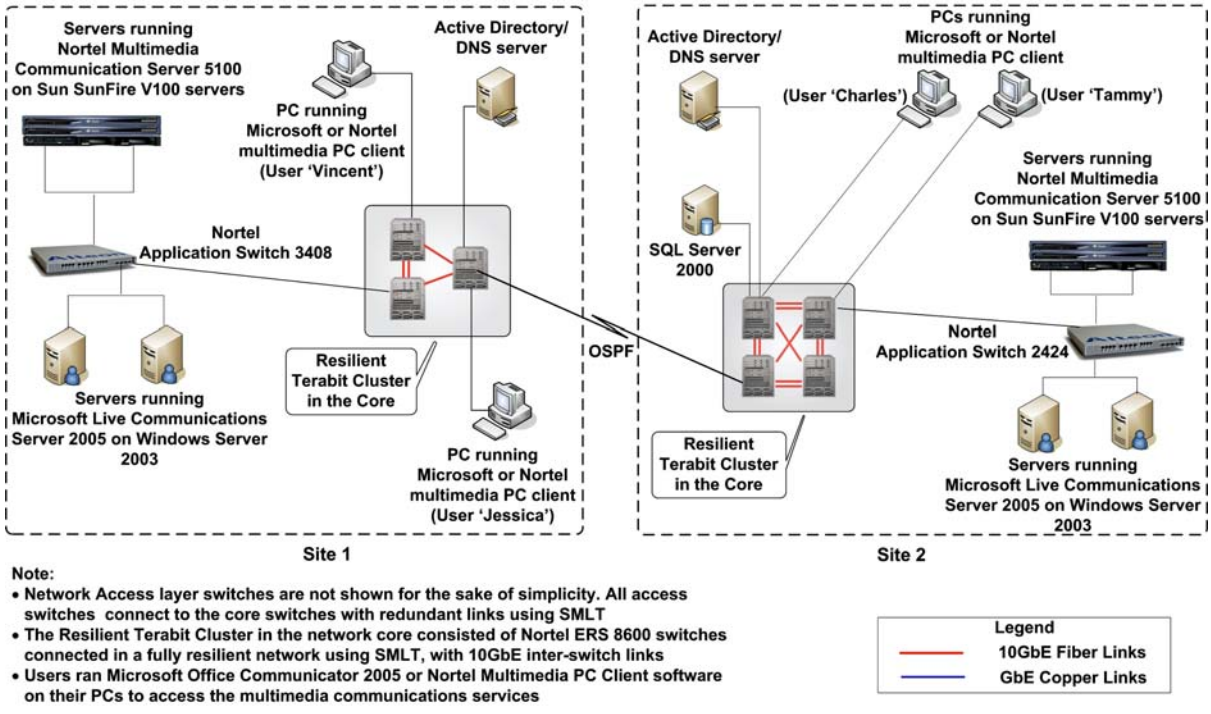
Resiliency was tested repeatedly by failing the Application Switch in each site alternately, but the results remained the same as the user sessions associated with the isolated MCS or LCS servers were migrated to other MCS or LCS servers elsewhere in the network. New user sessions initiated from a site — after its Application Switch and MCS or LCS Servers failed — were observed to be associated with the remaining available MCS or LCS servers in the network.

This demonstrated the resiliency offered by Nortel's Global Server Load Balancing working with the Nortel MCS or Microsoft LCS solutions using Nortel Application Switches.

Test Setup & Methodology

The test bed was constructed to create a microcosm of an enterprise network consisting of two sites. Each site had its own core routing network consisting of multiple Nortel Ethernet Routing Switch 8600 switches connected in a fully resilient network using Split Multi-Link Trunking (SMLT). (See Figure 2.)

Each site had a Nortel Application Switch 2424/3408 connected to a pair of Microsoft LCS or Nortel MCS servers that provided multimedia communication services.



Source: The Tolly Group. November 2006

Figure 2

Note, only Nortel MCS servers or only Microsoft LCS servers were tested at any given time in the test bed. Each site also had several user terminals like PCs with Web cameras and equipped with the appropriate client software — Microsoft Office Communicator client while testing LCS servers, and Nortel Multimedia Communication Server PC Client (referred to as MCS PC client, hereafter) while testing Nortel MCS servers — that provided multimedia communication services.

While testing with LCS servers, user database and authentication services were handled by servers on each site, running the Microsoft Active Directory with Microsoft SQL Sever 2000 database along with DNS services.

The two network sites communicated with each other using an OSPF (Open Shortest Path First) routed link. The two Application Switches monitored each others' health using Distributed Site Selection Protocol (DSSP).

The objective of the test was to verify that the Application Switch on each site load balanced the user sessions across the multiple LCS servers on-site (using Server Load Balancing — SLB) or the MCS or LCS servers throughout the network (using Global Sever Load Balancing — GSLB).

The tests also verified that Nortel's Application Switch provides resiliency by seamlessly taking over active and new user sessions from other sites in the network, in the event of the failure of the available Application Switch or the active MCS or LCS servers of the other sites.

Global Server Load Balancing (GSLB)

This feature of the Nortel Application Switch was tested separately with both Nortel MCS and Microsoft LCS servers.

Each site was configured with two PCs, each running the appropriate client software — Microsoft Office Communicator 2005 client while testing LCS servers, and Nortel MCS PC client software while testing MCS servers.

Each client was configured with a unique user account. Users "Vincent" and "Jessica" were located in site 1, and users "Tammy" and "Charles" were located in site 2. It was made sure that the two MCS or LCS servers on each site were active. Then, each user was signed in on the clients using their authentication credentials.

The Application Switch on each site directed users to the available MCS or LCS servers within a pool once user credentials were authenticated and verified by the Active Directory in conjunction with the SQL Server 2000 database.

The MCS or LCS server interface was checked to note the particular user sessions associated with that server. It was verified that the two user sessions on each site were load balanced between the MCS or LCS servers on that site.

Voice and video calls were placed between the users across the two sites (e.g. Tammy with Vincent, Jessica with Charles, and so on).

While the voice and video calls were in progress, the Application Switch (and the MCS or LCS servers connected to it) on one of the sites (say, site 1) was isolated from the network by failing its uplink to the network core.

It was verified that the active voice and video calls were uninterrupted and the user sessions from site 1 were associated with the available MCS or LCS servers in site 2, indicating a seamless failover to the Application Switch on site 2.

Nortel Application Switch 2424/3408

Load Balancing and Resiliency

New user sessions from the site 1 were then verified to be associated to the MCS or LCS servers on site 2 through the Application Switch on site 2.

The test was repeated by alternatively failing each Application Switch, and it was verified that active user sessions remained uninterrupted with the available Application Switch in the network assuming control of the MCS or LCS servers and user sessions in the network.

Local Server Load Balancing (SLB)

The network topology was identical to the GSLB scenario, but this time, GSLB was not enabled. This test was performed only on the Microsoft LCS server.

Similar to the GSLB scenario described earlier, two users were configured on each site, and voice and video sessions were initiated between the users on the two sites.

It was verified that new user sessions were distributed ("load balanced") between the LCS servers on-site, and in the event of failure of one of the LCS servers, the user sessions were redirected to the other available LCS server(s) on-site without interrupting active user sessions.

New user sessions were verified to be registered with the available LCS server.

Security using Nortel Application Switch

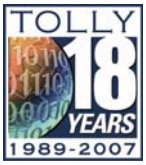
Engineers also tested the security functionality built into the Nortel Application Switch 2424/3408 by subjecting it to security attacks while handling active voice and video calls.

For this testing, the Nortel MCS 5100 server was handling voice and video calls between two MCS PC clients, when a Distributed Denial of Service (DDoS) attack was launched against the Nortel Application Switch at the rate of 1,000 frames per second, using an Ixia 1600T traffic generator and IxLoad 3.10 application. The Application Switch recognized the attack, and blocked it automatically, without dropping the active voice and video calls.

Note: The Nortel Application Switch provides functions not tested for this report but worth noting. Features include DoS prevention, intrusion detection, and the ability to identify and shape traffic by application. The latter lets LCS administrators identify and block rogue applications, such as non-approved VoIP, or consumer instant messaging traffic, according to Nortel.

Test Bed Equipment Summary

Product	Version
Nortel Ethernet Routing Switch 8600	SW Ver. 4.1.1, Boot Monitor Ver. 4.1.1
Nortel Application Switch 3408	SW Ver. 23.0
Nortel Application Switch 2424	SW Ver. 23.0
Nortel Multimedia Communication Server 5100	SW Ver. 3.5, running on Sun SunFire V100 servers
Nortel Multimedia PC Client	SW Ver. 3.5.208
Microsoft Live Communications Server 2005 Enterprise Edition	Ver. SP1 running on Windows Server 2003 Enterprise Edition
Microsoft SQL Server 2000	Ver. SP3
Microsoft Office Communicator 2005	Ver. 1.0.559



207179-opsufmu-CDB-02FEB07