Special Advertising Section

TOLLY
Benchmarks

Volume 6, Issue 4

THE TOLLY GROUP

ABOUT

Tolly Benchmarks is a regular advertising supplement that highlights innovative and compelling technology research conducted by The Tolly Group, the industry's leading independent testing and strategic consulting organization based in Boca Raton, FL. **For more information** on any of the products or technologies covered here, visit The Tolly Group's Web site at ***http://www.tolly.com***.

info@tolly.com	phone (561) 391-5610	fax (561) 391-5810

Study finds 3Com's OSN delivers an innovative new approach to building networks

Sponsor: **3Com Corporation**
Document number: **207186**
Product class: **Network applications platform**
Products under test:
3Com Open Services Networking (OSN)
Testing window: **January 2007**
For more info on this test, visit:
http://www.3com.com/OSN

An in-depth Tolly Group examination of 3Com Corp.'s Open Services Networking (OSN) revealed that the solution enables enterprises, service providers and systems integrators to deliver innovative, flexible solutions; develop and deploy services faster; simplify network management; and achieve lasting investment protection.

OSN is a communications infrastructure that enables applications to run inside the network and address a range of issues that confront CIOs and network designers. OSN makes it possible for 3Com router and switching platforms to run a variety of open source and best-of-breed commercial applications to enable a range of network services.

Tests demonstrated OSN's ability to support best-of-breed applications or open source-based applications on the hardware, giving users a critical choice in how they wish to deploy their application base and manage software costs. Moreover, tests showed that the OSN module itself is based on a recent, up-to-date, secure Linux operating system, that it is ready to host mission-critical applications such as voice over IP (VoIP) and that it supports standard IP when interfacing with its host router.

OSN saves on capital expenses by eliminating the need for additional appliances and reducing power consumption. From an operational expense viewpoint, OSN enables remote deployment and management of applications, eliminating on-site technical support.

3Com also has focused OSN on serviceability and control to reduce the cost and complexity of servicing network applications. This was evident by the tight integration between the module and the router or switch platform, enabling administrators to control applications as needed.

Additionally, tests show that 3Com has created OSN with security in mind, ensuring the applications hosted on an OSN platform are protected behind multiple hardware and software components. Testing validated this when access control lists (ACLs), network address translation (NAT) and firewall connections were tested.

Testing also demonstrated that OSN is capable of running enhanced applications that required advanced disk, traffic and CPU resources. Additionally, testing proved that OSN is easy to use and to deploy. Simply mounting the OSN software and bringing up the OSN modules on a 3Com router required a matter of just a few minutes. And testing also demonstrated that OSN "auto-interfaces" with its host router and 3Com has furnished simplified administration via a Webmin Open Source Web portal interface.

Finally, tests demonstrated that OSN modules inside the router or switch deliver near wire-speed performance, even when transmitting data to clients behind firewall connections.

Average Throughput of 3Com OSN Module to Switch-Attached Laptop Across Fast Ethernet

(TCP Stream Test with Mixed Packet Sizes)

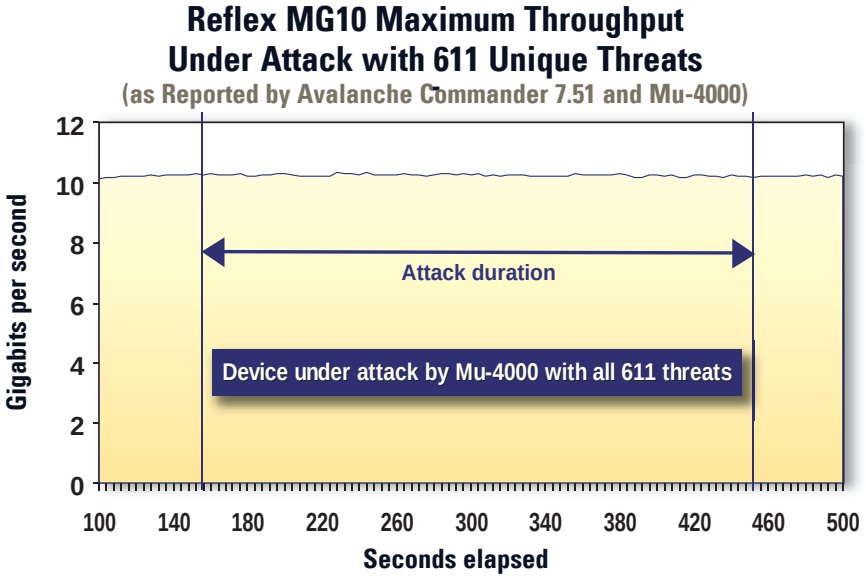
Duration	Avg. Throughput (Mbps)	Bytes Transmitted (MB)
10 seconds	94.15	123.4
30 seconds	94.13	370.2
5 minutes	94.12	3700

- **Achieves near wire-speed performance over Fast Ethernet connections**
- **Delivers the flexibility for management to deploy best-of-breed or open source applications, or mix and match to curb costs**
- **Fosters secure applications by enabling administrators to specify rules for NAT and firewall operations**
- **Supports multiple monitoring applications, and interoperability with SNMP-enabled products so users can deploy multiple types of service monitoring, tailored to a specific business need**

View the full report at:
http://www.tolly.com/DocDetail.aspx?DocNumber=207186

Reflex MG10 Network Security Switch repels severe attacks, maintains traffic performance

- Maintains average maximum throughput of 10.25 Gbps even when device is processing 611 unique threats — the maximum attacks supported by the Mu-4000 Security Analyzer with Version 2.3.28 attack library
- Blocks 611 security threats out of 611 generated
- Sustains throughput, with zero failed transactions, during random blade failure
- Supports almost 5.8 million steady-state TCP connections over two 10GbE and eight GbE ports



Tests show that a network security switch from Reflex Security can successfully thwart a heavy barrage of attack traffic while simultaneously processing normal application traffic without sacrificing performance.

Reflex Security, Inc. commissioned The Tolly Group to examine the performance of the Reflex MG10, a network switch that employs a blade-based Distributed Security Architecture™ (DSA) that provides scalable throughput from 10 Mbps to 10 Gigabits per second (Gbps). The aim was to understand how the MG10 can handle normal application traffic while also handling a serious load of security threats.

Engineers also measured the number of open TCP connections sustained across the MG10, and examined how the unit responds during an invoked failure.

Throughput tests show that the MG10 delivers 10.25 Gbps of throughput while its deep packet inspection detected and prevented the complete library of attacks generated by a Mu Security Mu-4000 Security Analyzer. The Reflex MG10 also delivered uninterrupted performance and zero transaction loss during simulated failures of Reflex MG chassis security blades. In fact, engineers, simulated a failure by pulling a system blade for 60 seconds. This represented a serious hardware failure on the device. However, the MG10 continued to deliver 6.3 Gbps of throughput even with the loss of a single blade. Engineers noted that the reinsertion of the MG10 blade did not result in the loss of any transactions.

Engineers measured the ability of the MG10 to perform a SYN-SYN ACK process to open a connection with another device and then maintain that open TCP connection. Tests of TCP connections shows that the security switch can sustain 5.8 million open TCP connections over the device backplane.

View the full white paper at:
http://www.tolly.com/DocDetail.aspx?DocNumber=207219

Sponsor: **Reflex Technology, Inc.**
Document number: **207219**
Product class: **Network security switch**
Products under test:

- Reflex MG10 supporting Reflex MG V 6.1 threat signature and Reflex Command Center V 6.1 management software

Testing window: **June 2007**
For more info on this test, visit: ***http://www.reflexsecurity.com***

- Accurately identifies all traffic types tested from a stream of 1.6 Gbps of aggregate throughput across the device backplane
- Maintains at least 1.6 Gbps of throughput and 100% detection accuracy even as the number of rules scales from 0 to 20,000
- Generates less than 1 millisecond of one-way average latency while performing Layer 7 Deep Flow Inspection (DFI) at the of 1.6 Gbps with 20,000 rules enabled
- Deploys in just four basic steps into an existing network

Tests reveal speed, accuracy and scalability of Procera Networks PacketLogic 7600 for broadband ISPs

Broadband Internet service providers (ISPs) intent on improving Quality of Service (QoS) and managing applications that hog bandwidth could benefit from the findings of a Tolly Group test on the Procera Networks PacketLogic 7600 traffic and service management system.

Tolly Group tests confirm that the Procera PacketLogic 7600 offers high accuracy in traffic identification, extremely low latency, ease of installation and the ability to scale to accommodate changing network traffic loads.

The PL7600 typically is deployed by broadband service providers to manage and control network and service usage and traffic, to provide tiered service levels and assure agreed-upon throughputs (SLAs), and to conform to the technical assistance requirements of lawful intercept regulations such as CALEA (Communications Assistance for Law Enforcement Act) in the U.S.

The Procera PacketLogic 7600's traffic identification capabilities, which allow service providers and others to manage applications such as BitTorrent and file sharing, achieved 100% accuracy in identifying all 50 traffic types tested, even as traffic scaled from 0.2 to 1.6 Gbps. Further, the PacketLogic 7600 generated less than 1 millisecond average latency across all throughput rates, with up to 20,000 traffic management rules enabled — proving the system's high performance and ability to easily scale without introducing undue latency and network delays. And finally, Tolly Group engineers affirmed the system's ease of use and installation by documenting the steps needed for initial deployment in an existing network.

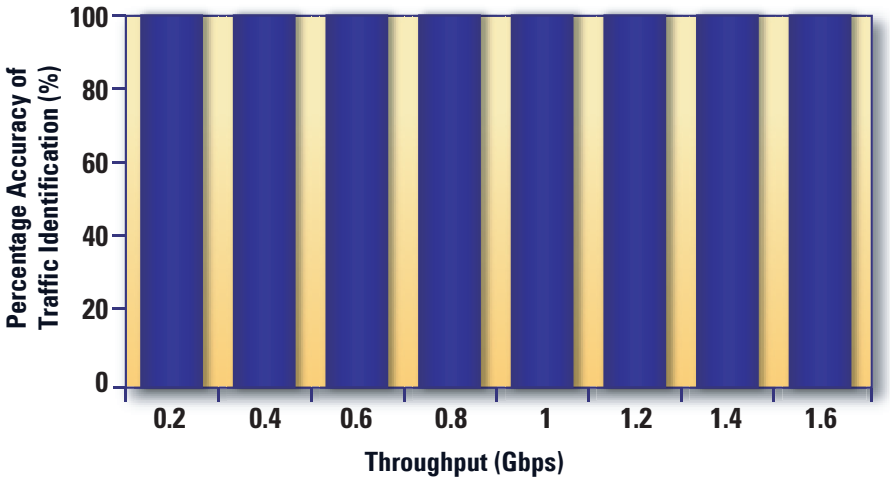
On the scalability front, engineers verified that the PacketLogic 7600 does not degrade the throughput and latency performance up to 20,000 rules tested by sustaining 1.6 Gbps throughput and less than 1 ms of average latency. Maximum latency measurements did not exceed 3 ms.

From an ease-of-use perspective, Tolly Group engineers verified that just four basic steps are needed to deploy a PacketLogic 7600 appliance into an existing network. Since the PacketLogic 7600 runs transparent in the network at Layer 2, it starts gathering Layer 7 traffic information by being inserted into the existing network inline or as a tap. By default, the 7600 is equipped with 300+ signatures to identify common services used by applications. However, like typical users, Tolly Group engineers changed IP information, enabled the statistics, created new objects and associated the objects with rules/policies.

View the full report at:
http://www.tolly.com/DocDetail.aspx?DocNumber=207173

Traffic Identification Accuracy at Various Throughput Rates

(Simulation of 50 Well-Known Applications)



Note: Engineers used Shenick's "TCP Replay" feature to replay PCAP files which contained the behaviors of 50 well-known applications and generated up to 1.6 Gbps of stateful throughput. While the PacketLogic 7600 is rated at up to 2 Gbps of bidirectional throughput, the test tool used only generated up to 1.6 Gbps.

Sponsor: **Procera Networks, Inc.**
Document number: **207173**

Products under test:
- Procera Networks PacketLogic 7600 running protocol version 10 and build version 324

Testing window: **April 2007**

For more info on this test, visit:
- ***http://www.proceranetworks.com***

Nortel proves price/performance lead over Cisco and HP in Ethernet switch tests

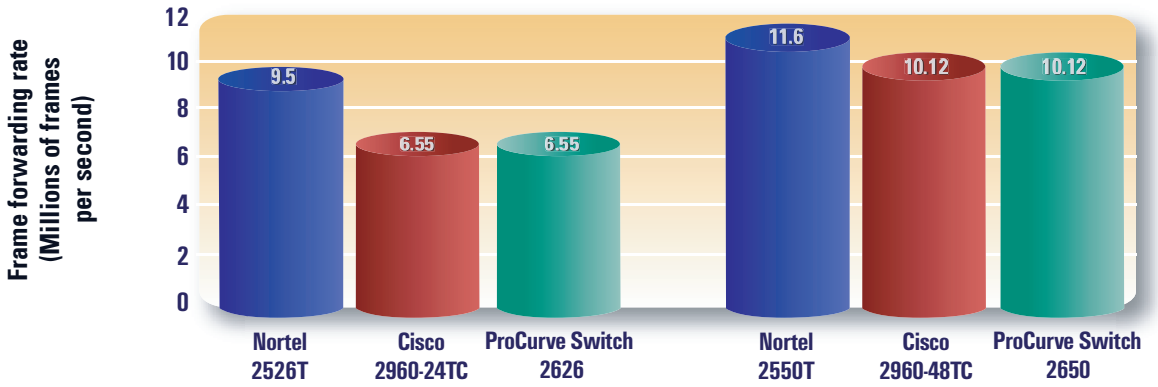
In two separate tests conducted for Nortel, the company's Ethernet Routing Switches exceeded the price perfomance of comparable switches from Cisco Systems and ProCurve Networking by HP.

A May 2007 test of Nortel's ERS 2526T and ERS 2550T shows that the Nortel switches delivered superior performance of up to 9.52 and 11.6 million frames per second for 64-byte frames, surpassing the Cisco Catalyst 2960-24T and 48T and ProCurve Networking 2626 and 2650. The Nortel switches also offered a lower cost-per-Gbps of throughput — $109/$153 for 24/48 ports, versus ProCurve at $143/$159 and Cisco at $567/$661.

A September 2007 Tolly Group report found that Nortel's ERS 4548GT-PWR achieved 48 Gbps of throughput vs 26 to 30 Gbps for Cisco Catalyst 3560-48PS and 3750-48PS switches tested. Again, Nortel offered the lowest cost-per-Gbps of throughput at $70, vs. $250 for the Catalyst 3750G-48PS and $153 for the Catalyst 3560-48PS.

Layer 2 Bidirectional Frame Forwarding Rate of Nortel ERS, Cisco Catalyst and HP ProCurve using 64-Byte Frames

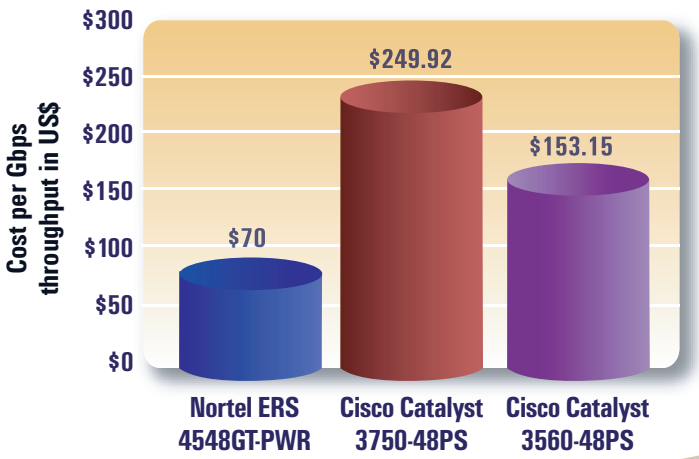
as Reported by Spirent SmartFlow 5.5



Note: 1.) All switches tested with maximum available GbE uplink ports 2.) The frame forwarding rate was measured in Layer 2 switching mode- and bidirectional traffic was generated in a full-mesh configuration where ports of the same type were grouped together.

View the full ERS 2526/2550T report at:
http://www.tolly.com/DocDetail.aspx?DocNumber=207178

Cost-per-Gbps of Throughput in a Standalone Switch Configuration



Sponsor: **Nortel**

Document numbers:

207178 and 207237

For more info on this test, visit:

http://www.nortel.com

View the full 4548GT-PWR report at:
http://www.tolly.com/DocDetail.aspx?DocNumber=207237

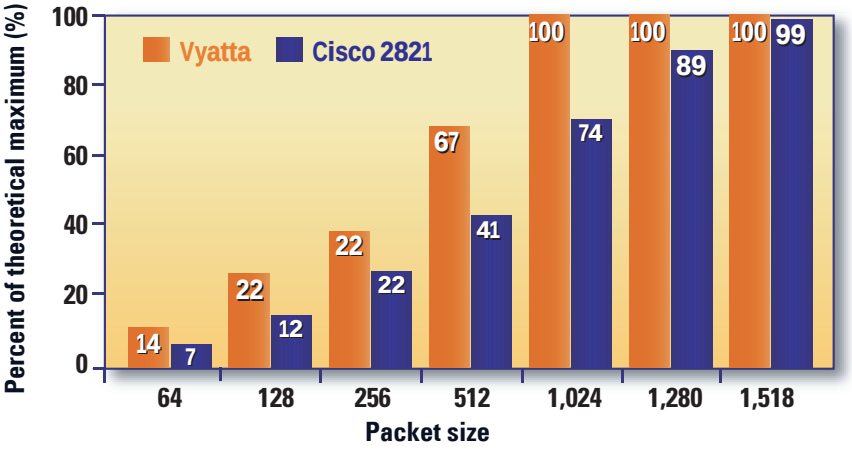
Sponsor: **Vyatta**
Document number: **207190**
Product class:
- **Open-source software-based router**

Products under test:
- Vyatta 1.1.2 running on Dell PowerEdge 860 Server system (Single Celeron D 2.80 GHz, 256K cache, 512 MB DDR-2 SDRAM, OS: Linux Kernel Ver. 2.6.16)
- Cisco 2821 Integrated Services Router, software version 12.3(14) T4

Testing window: **February 2007**
For more info on this test, visit:
- ***http://www.vyatta.com***

Vyatta open-source router doubles performance over Cisco 2821 in head-to-head test

Bidirectional Zero-loss (£ 0.001%) Routing Throughput
(as Reported by Spirent SmartFlow 5.5)



There is a myth that proprietary hardware products are always better choices over standard x86-based systems for enterprises and small- to medium-sized business (SMB) networking needs. As the networks become more complex and diverse, network managers have to pay more attention to upfront investments, ongoing maintenance costs and costs to scale for future growth. For the majority of SMB and enterprise branch office managers, open software on standard hardware is the answer to performance and cost-effective growth needs.

Tolly Group tests show that a Vyatta open-source, software-based routing and security solution on an x86 processor-based system (Dell PowerEdge 860) delivered twice the performance for half the price of a Cisco router tested during a Gigabit Ethernet-to-Gigabit Ethernet (GbE) scenario with all packet sizes tested.

The Vyatta software achieved Layer 3 wire-speed throughput (2 Gbps of aggregate throughput) for 1,024 bytes or higher, while a Cisco 2821 Integrated Services Router never achieved wire-speed performance in any tests. For the 64-byte bidirectional throughput test, Vyatta offered double the throughput of the Cisco device —282 Mbps while the Cisco 2821 attained 138 Mbps.

Engineers also proved that the Vyatta software router delivered lower frame loss than the Cisco 2821 for all packet sizes and achieved zero frame loss with 1,024-byte packets and higher.

Tolly Group engineers also computed a cost-per-Mbps of throughput value to assess the the price/routing throughput performance. With a retail price of $1,797 for bundled hardware/software/support, Vyatta delivers price/performance from a low of 90 cents per Mbps (1,024 byte packets or higher) to a high of $6.37 (64-byte packets). The base system Cisco 2821, with a retail price of $3,334.98, has a cost-per-Mbps ranging from a low of $1.69 (1,518-byte packets) to a high of $24.17 (64-byte packets). WAN interfaces were not factored into pricing.

When users want to add an additional Layer 3 Fast Ethernet routing port, Cisco users pay $1,009.99 (CDW.COM) to add one Fast Ethernet Layer 3 port (Cisco 1-port HWIC, MFG# HWIC-1FE). Vyatta users, by contrast, pay only $65 for a GbE port since they can leverage the structural cost benefits of the x86 system.

- **Outperforms the Cisco 2821 router consistently in Layer 3 Ethernet bidirectional zero-loss throughput, achieving up to twice the performance at half the price**
- **Operates at Layer 3 wire-speed across two onboard Gigabit Ethernet ports when forwarding 1,024-byte packets or higher**
- **Delivers lower packet loss than the Cisco 2821 for all packet sizes and achieves zero packet loss with 1,024-byte packets and higher**
- **Leverages standard hardware and the structural cost benefits of the x86 ecosystem to offer a flexible, extensible and faster solution at attractive price points**

View the full report at:
http://www.tolly.com/DocDetail.aspx?DocNumber=206190

NAC test reveals Mirage Endpoint Control secures networks with real-world applications

- Protects customer networks from infected, out-of-policy, and unknown endpoints
- Stops behavioral threats, preventing malware from propagating throughout a network
- Detects and stops unauthorized applications such as instant messaging and peer-to-peer file sharing
- Stops unknown/rogue devices such as gaming consoles, personal routers and servers until they are registered
- Protects wireless networks from unauthorized mobile devices such as iPhones and Windows Mobile devices

Features/Functions of Mirage Endpoint Control
Validated by The Tolly Group

Compliance and Monitoring	Requires authentication and host posture check for Windows, Linux and Macintosh devices, restricting access when devices are not compliant	✓
	Monitors behavior of all devices on the network, restricting access when policies are broken	✓
P2P File Sharing Control	Detects P2P packets and alerts network admins	✓
	Stops flow of P2P traffic	✓
	Revokes network access to offending applications or endpoints	✓
Instant Messaging Checks	Detects IM traffic from AOL, Yahoo!, MSN Messenger and Trillian	✓
	Stops flow of IM traffic	✓
	Blocks network access of offending applicatoins or endpoints	✓
Rogue Device Registration	Detects unregistered devices such as personal routers, servers, Xbox and PlayStation	✓
	Allows devices to register for network access	✓
WLAN Access Control	Detects and blocks Apple iPhones and Windows Mobile devices from accessing wireless LANs	✓

Mirage Networks Endpoint Control appliance provides security that controls or revokes network access to devices that are unknown, out-of-policy, or threat-infected, according to a recent Tolly Group hands-on evaluation.

Tests show that the Endpoint Control appliance restricted access of Windows XP, Windows Vista, Linux and Macintosh clients until each user successfully entered authentication credentials, completed a system scan to validate OS patches, anti-virus and anti-spyware versions and personal firewall versions/status, and, lastly, that the clients followed predefined behavioral guidelines. When endpoints were granted access, Mirage stopped a range of threats from propagating throughout the network.

The Tolly Group validated that Mirage's Endpoint Control appliance effectively deals with applications such as Peer-to-Peer (P2P) and Instant Messaging (IM), and can also identify and isolate rogue devices seeking access to the network, and preclude nuisance devices, such as gaming consoles from commandeering network resources without authorization. Engineers also validated the ability to isolate Apple iPhones from joining wireless networks where they could be the root cause of broadcast storms.

On the P2P side, the appliance also blocked a Windows XP client's network access when it attempted to use P2P, and issued an SNMP alert and E-mail notification to network personnel.

Additionally, the Mirage appliance detected IM traffic from services such as Yahoo Instant Messenger, AOL Instant Messenger, MSN Messenger and Trillian and proceeded to stop the flow of IM traffic, blocked the endpoint client's network access, and issued an SNMP alert and E-mail notification to network personnel.

Tests also show the the Endpoint Control appliance detected rogue routers, servers, and Microsoft Xbox and Sony PlayStation gaming consoles. Further, it blocked network access until the devices were registered.

Finally, engineers also validated that the Endpoint Control appliance detected an iPhone and a Windows Mobile device connecting to the wireless network and blocked network access until the devices were authenticated.

The upshot is that while many NAC devices offer some level of access control, Mirage Networks has proven that its Endpoint Control appliance enables tangible customer applications to utilize endpoint access control that is above and beyond general endpoint security.

Sponsor: **Mirage Networks, Inc.**
Document number: **207252**
Product class: **Network access control appliance**
Products under test:

- **Mirage Networks Endpoint Control, version 3.1**

Testing window: **September 2007**
For more info on this test, visit:

- ***http://www.miragenetworks.com***

For more info on this test, visit:
http://www.tolly.com/DocDetail.aspx?DocNumber=207252

NETGEAR Gigabit Stackable Smart Switches demo blazing speed, security, QoS, resiliency and management

NETGEAR ProSafe 24- and 48-Port Gigabit Stackable Smart Switches Feature Validation		
Resiliency	Automatic master fail-over	✓
	Redundant stacking architecture	✓
	Hot-swappable switches	✓
Management	Stack manageable via single IP address	✓
	Web-based management interface	✓
	SNMP-based management software support	✓
Security	802.1x via RADIUS	✓
	MAC-based Access Control List (ACL)	✓
QoS	Rate limiting	✓
	Layer 2 (802.1p) prioritization	✓
	Layer 3 (DSCP) prioritization	✓

Note: Figure shows only features validated by The Tolly Group, not entire spectrum of ProSafe GS748TS and GS724TS Gigabit Stackable Smart Switch features.

- **Delivers wire-speed performance for all frame sizes tested in a full-mesh configuration for 48-port and 24-port switches**
- **Offers comparable security and QoS features to managed switches**
- **Manages the stack easily with a single IP address and intuitive Web-based management**
- **Demonstrates redundant stacking architecture via a pair of bidirectional stacking ports per switch, which provide 20 Gbps aggregate throughput in stacking ring topology**
- **Integrates key stackable switch features into SMB domain in a cost-effective way**

Recent Tolly Group tests show that the NETGEAR ProSafe GS748TS and GS724TS stackable smart switches support advanced network features that are important to SMB and branch office users while also delivering robust performance and functionality.

In a feature evaluation, engineers ran various tests under the categories of resiliency, management, security and QoS to validate capabilities. Engineers proved that the ProSafe GS748TS and GS724TS support advanced security and management features normally offered in more expensive products.

In a Layer 2 Gigabit Ethernet switch performance test, the NETGEAR stackable switches achieved wire-speed throughput in 48-port and 24-port, full-mesh configurations for all frame sizes tested. This equates to 48 Gbps and 24 Gbps aggregate throughput for the GS748TS and GS724TS, respectively. What this means is that the ProSafe GS748TS and the GS724TS have ample headroom for growth and embrace high-bandwidth applications.

Tests also proved that each high-speed stacking port supports 5 Gbps of traffic in each direction. Engineers also witnessed sub-second fail-over when one of the active switches in the stack was failed. Tests also validated that the NETGEAR switches support rate limiting and Layer 2/3 prioritization.

From a management angle, engineers verified that the stack can be managed via a single IP address and also verified that users can manage the NETGEAR stack via a Web browser and SNMP-based management software.

On the security front, Tolly Group engineers verified that the ProSafe GS748TS and GS724TS authenticate users via 802.1x and refer to a RADIUS server to verify user credentials. They also proved that the switches enable administrators to allow or deny access based on MAC addresses.

Sponsor: **NETGEAR, Inc.**
Document number: **207206**
Product class:
- **Gigabit Stackable Smart Switches**

Products under test:
- **NETGEAR ProSafe GS724TS and GS748TS GbE stackable smart switches running firmware version 1.0.1.4**

Testing window: **July 2007**

For more info on this test, visit:
- ***http://www.netgear.com***

View the full test summary at:
http://www.tolly.com/DocDetail.aspx?DocNumber=207206