Document # 207186

Open Services Networking:

3Com Harnesses Router and LAN Switching Platforms to Address Network Pain Points

THE TOLLY GROUP

A white paper commissioned by 3Com Corp.

White Paper

January 2007

THE TOLLY GROUP

Table of Contents

Before using this document you must agree to the terms of usage.
These terms are listed on the final page.

Table of Contents

Before using this document you must agree to the terms of usage.
These terms are listed on the final page.

Executive Summary

Enterprise network planners, and carriers alike, are faced with one of two choices when deploying network infrastructures — they can opt for a best-of-breed application approach and deploy a patchwork quilt of network appliances, or they can opt to deploy a single vendor network solution to ensure integration of components which lacks the robustness of best-of-breed applications. What network designers really need is a network model that enables them to address specific business needs by controlling how, and when, to scale their networks, saving human resources and protecting capital investments. Moreover, they need a network infrastructure that fosters deployment of applications from a variety of possible sources: from independent software vendors (ISVs), from a single vendor, or from the open source development community. 3Com Corp. is delivering such an environment with the introduction of its Open Services Networking (OSN) initiative. The goal is to enable implementors of OSN to tie network solutions close to business needs and technology opportunities and empower organizations to deploy such solutions rapidly, at low cost and with significant flexibility.

3Com commissioned The Tolly Group to evaluate the company's Open Services Networking (OSN) initiative. OSN is a communications infrastructure that can host strategic network applications to solve specific business problems and address a host of issues that confront CIOs and network designers.

3Com's OSN harnesses the company's family of routers and switches to host a wide array of network services and applications that represent the spectrum of products from Open Source to best-of-breed Linux applications.

Initially, 3Com has focused OSN on key areas such as network and application visibility, application performance, network complexity, compliance (HIPPA, PCI, CALEA and more) and security. Ultimately, though, OSN creates a platform to support any network services or network-centric applications that are critical to business operations.

OSN enables 3Com router and switching platforms to run a variety of open, Linux applications to enable a range of network services. Moreover, the openness of OSN enables users to leverage best-of-breed commercial applications on OSN platforms as well, so users are not locked into a single application direction.

From a hardware perspective, Linux-based OSN|M modules integrate into existing 3Com router and switching systems and operate independently of the host's CPU. 3Com also will be working with third-party ISVs, the Open Source community, and customers who develop "homegrown" applications.

This underscores one of several key underpinnings of the OSN strategy — openness. The goal of OSN is to furnish users with an open infrastructure that gives them a wide array of choices with regards to addressing business needs. Testing repeatedly showed that OSN is open to both commercial and Open Source applications, giving users the option of curbing costs via Open Source tools, or going the best-of-breed software route and deploying strategic applications. Moreover, tests showed that OSN itself is based on a recent, up-to-date 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.

3Com also has focused OSN on serviceability and control to reduce the cost and complexity of servicing network applications. This was evident by the flexible service channel to OSN|M modules, enabling administrators to control applications as needed.

Additionally, 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.

Testing also demonstrated that OSN|M modules deliver near wire-speed performance, even when transmitting data to clients behind firewall connections.

Hardware Review

An OSN-enabled infrastructure consists of a robust enterprise network with routing and switching devices coupled tightly to Open Services Modules (OSN|M) that can run a variety of Linux-based applications. Initial OSN solutions are in the form of “modules” to deliver applications. Over time, it is likely that 3Com will “virtualize” the OSN|M technology to further reduce costs.

Critical to the OSN architecture is a set of comprehensive provisioning management, security and control tools all embedded inside the OSN Con-

3Com

Open Services Networking

Functionality and Performance Evaluation

TOLLY Up to Spec CERTIFIED

Product Specifications

Vendor-supplied information not necessarily verified by The Tolly Group

3Com Corporation
Open Services Networking Module for 3Com Router 6040

Key Benefits

- *Open and flexible services platform*
- *Comprehensive application support*
- *Secure hardware/software integration*
- *Easy to deploy and manage*
- *Reduced capital/operating costs*

OSNIM Module Specifications

- *Processor: Intel Pentium M, 1.4GHz, 2MB L2 Cache*
- *Operating system: OSN|OS Hardened Linux with kernel version 2.6.9*
- *Storage: Hard Drive: 80 GB*
- *Memory: 512 MB DDR SDRAM*
- *Flash: 256 MB*
- *Boot ROM: 2 MB*
- *Ports: One internal 10/100/1000 Ethernet and one external 10/100/1000 Ethernet; Two USB 1.1 (Host mode only)*

For more information contact:

3Com Corporation
350 Campus Drive
Marlborough, MA 01752
Phone: (508) 323-5000
Fax: (508) 323-1111
http://www.3com.com

trol Agent (OSN|CA). The OSN|CA) ensures efficient distribution and management of applications, secure access to the network's switching and routing features, and advanced failover and fault tolerance.

In any router or switch chassis, one or more OSNIM modules may populate the chassis to support multiple applications, or for scalability or redundancy reasons.

Each OSN|M module is a self-contained server capable of supporting multiple applications. The OSN|M is designed with a 1.4-GHz Pentium processor, 512MB of SDRAM memory and an 80-GB hard drive.

In the hardware phase of OSN testing, Tolly Group personnel observed the openness, flexibility, security, ease-of-use and performance characteristics of the OSNIM inserted into a 3Com Router 6040.

Engineers started with the Router 6040, outfitted with a Router Processing Unit (RPU) that enabled full-featured IP and IPX routing. In addition, the Router 6040 was configured with an enhanced serial module providing a T1 interface such as those commonly used for branch office environments. The Router 6040 was connected via Fast Ethernet to a NIST Net network traffic simulator, which was connected to a 3Com Router 5012 branch office device that supported a local IP telephone. (See FIgure 4, page 19.)

Getting Started

For this portion of the hardware review, engineers stepped through some basic steps to bring the OSN functionality online and to validate certain features/functions. Engineers started by powering on the Router 6040 and then hot inserting an OSN|M into the router. The hot-swappable OSN|M occupies a standard interface slot in the Router 6040 chassis and connects to the internal backplane. Once the OSN module was inserted, engineers entered the necessary configuration commands via a management console to bring up the OSN services and dynamically configure them for operation on the host router. Installation will be

a snap to any Linux fan, since OSN|M is based on CentOS — an Enterprise-class Linux distribution derived from sources freely provided to the public.

What is interesting to note here is that when the OSN module came on-line, it dynamically created an additional Ethernet interface separate from the router's interface. A separate Ethernet interface is important because it demonstrates that the module can communicate with external devices separate from the host router — meaning access to onboard services will not be affected by the performance of the host router's Ethernet connection.

Verification of Boot Message

Engineers verified the OSN|M module's ability to boot up in response to a message via a console command. Here, engineers input the OSN boot commands into the existing router CLI interface via an attached management console and the OSN module in the Router 6040 rebooted cleanly. The integrated OSN management console furnishes administrators with basic commands to control an OSN|M, such as: shutdown, reboot, etc. This integrated console guarantees service connectivity to the OSN|M and allows administrators access via Telnet, SSH or serial connectivity.

Verification of IP Connectivity

Engineers verified that the OSN|M module was logically connected to the IP network. Next, they decommissioned the OSN|M and issued SNMP traps to the module's IP address which confirmed that the module had been removed. Once the module was reinserted, the traps showed that slot 3 on the Router 6040 was again filled and an IP address was automatically created.

Hardware Review Observations

One of the first points observers will notice is the openness of the OSN|M design. The device utilizes standard IP communications with the surrounding network infrastructure, and its 1.4-GHz OSN|M is based upon a standard Intel platform with Gigabit Ethernet connectivity and a 256MB compact flash memory. This standard platform provides an open platform for application development and enables users to quickly load applications.

Moreover, the module's support for a Linux-based OS makes it an open and fertile platform for application development, or for deployment of Open Source applications.

Next up, security clearly has been carefully built into the OSN|M design. Administrators can peruse Syslog messages, trap notifications or dig into OSN activity via the device's management console. During installation, testers observed that once the OSN|M module was installed, administrators began receiving notification of what devices were "pulled" out of service or "added." This demonstrates a high degree of maintenance control.

In addition to security, testers found that OSN was easy to use, as well. The device auto-interfaces with the host Router 6040, and once the OSN|M module is installed, users have anytime access to its operation via the management CLI — with control over everything from a BIOS boot to network services running on the module.

From an operational expense (OPEX) viewpoint, OSN|M is efficient. Instead of deploying a separate application server, the OSNIM piggybacks onto the back of its host router so users manage a single power supply for both. Moreover, redundancies built into the router can be used for the OSN|M module.

With one customer premises device to deploy and manage, users can add application services onto the OSN|M via Dynamic Service Provi-

sioning — meaning the router continues to hum along and perform its core duties, while the OSN|M is configured to deliver various application services across the network. In essence, new services can be added onto the OSN|M inside the router added, versus other approaches where users would be forced to deploy additional server boxes and add significant hardware investment.

Operating System Review

In this test phase, Tolly Group personnel witnessed the OSN boot procedure, verified access to OSN operating system services via a Webmin interface, verified various security options via the host router and verified OS performance metrics.

OSN Boot Procedure

Tolly Group personnel examined the options available to users during the boot procedure for an OSN|M module. The exercise was meant to determine what flexibility users have when starting up the blade's OS.

Looking closely at the OS on startup, users will find the Standard Lilo (Linux Loader) bootloader which offers the capability to load and run the CentOS-based operating system - which 3Com calls OSN|OS - either from flash only or with full hard disk mounted.

To install the OSN|OS, 3Com uses a PXE (Pre-Execution Environment) bootstrapper to re-image hard disk and compact flash across the network. Both of these options can be used to boot the CentOS operating system that is at the heart of the OSN|M.

The use of a CentOS-based operating system underscores 3Com's commitment to openness with the OSN platform. CentOS exists to provide a free enterprise-class computing platform to anyone who wishes to use it. CentOS 2, 3, and 4 are built from publicly available open source code provided by a prominent North American Enterprise Linux vendor. CentOS is designed for users who need an enterprise-class OS without

the cost or support of a commercial product.

For this test phase, Tolly Group observers witnessed a remote imaging of the OSN|OS software. A user on a laptop computer connected to a port on a 3Com Switch 4200, which also connected over the Internet to the Router 6040 housing the OSN|M. DHCP and TFTP were both started on the laptop and the user issued a “reboot” command from the laptop to the OSN module in slot 3 of the router. The laptop user then connected to slot 3 of the router and intentionally interrupted the reboot. The laptop user then installed Linux with Ethernet and obtained an IP address for the OSN|M module from the DHCP server on the laptop.

The OSN module proceeded to load the supplied filename which then loaded a small version of Linux on the OSN|M. The laptop user then issued a command to install PXE and the OSN|M software was loaded and installed within 20 minutes.

Managing the OS with Webmin

3Com’s commitment to openness with the OSN architecture extends into how the operating system is managed. Instead of designing and deploying yet another vendor tool, 3Com employs a third-party Open Source tool called Webmin.(http://www.webmin.com)

Webmin is a Web-based portal interface for system administration for Unix. Using any browser that supports tables and forms (and Java for the File Manager module), users can set up user accounts, Apache, DNS, file sharing and so on. Webmin consists of a simple Web server, and a number of CGI programs which directly update system files like /etc/inetd.conf and /etc/passwd. The Web server and all CGI programs are written in Perl version 5, and use no non-standard Perl modules.

During testing, Tolly Group personnel witnessed access to a variety of OSN|M applications and user accounts via the Webmin interface.

Verification of Security Functions

Tolly Group observers verified that the OSN|M management interface allows administrators to set security options via the host router. User were able to specify rules for NAT and firewall operations. In one exercise, NAT was set to block traffic from outside the corporate network (meaning block Internet feeds). Observers noted that the Webmin access was terminated because the router guards access to the OSN|M via NAT.

Operating System Performance

Testers measured the throughput sustained by the OSN|M when handling TCP stream traffic from the module across a Fast Ethernet connection to the Router 6040 RPU. MIxed packet sizes, ranging from 64 bytes to 1,518 bytes, were used. Engineers measured the throughput across three test scenarios: a 10-second test, a 30-second test and a five-minute test. In all three scenarios, three test iterations were run and the results were averaged.

Average Throughput OSN|M 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

Source: The Tolly Group, December 2006 *Figure 1*

Across all three test durations, averaged throughput remained consistent, delivering near wire-speed throughput ranging from 94.12 Mbps to 94.15 Mbps. (See Figure 1.)

Next, engineers measured throughput across the Fast Ethernet switched network across a firewall to a remote laptop. Again, throughput

Average Throughput OSN|M Module to Remote Laptop Across Fast Ethernet Firewall Connection (TCP Stream Test with Mixed Packet Sizes)		
Duration	Avg. Throughput (Mbps)	Bytes Transmitted (MB)
10 seconds	94.07	118.2
30 seconds	94.15	367
5 minutes	94.15	3702

Source: The Tolly Group, December 2006 *Figure 2*

was measured with the same three test scenarios, with three iterations taken and results were averaged.

Again, the OSN|M delivered near wire-speed throughput ranging from 94.07 Mbps to 94.15 Mbps (See Figure 2.)

OS Review Observations

One of the primary messages 3Com delivers with OSN is openness and that is clearly evident with the operating system. Use of a CentOS-based operating system as a standards-based open software platform affirms 3Com's pledge to openness; it also guarantees that third-party developers can write or port best-of-breed applications to OSN, or users can deploy Open Source freeware tools where appropriate.

The flexibility of the OS is evident in the multiple boot options provided by 3Com. Users can boot with or without hard disk support.

From a security standpoint, OSN offers protection via the host router by way of NAT and firewall support. Administrators are able to protect access to specific ports on the OSN or block entire traffic types if preferable.

Access to OS features is made easy via the Webmin portal, which provides an open portal environment to managed operating system functions/features, as well as to manage boot operations.

Lastly, from an OPEX perspective, the high performance offered by OSN assures users that they do not need to worry about the OS. Moreover, support for CentOS and its openness assures users they have the option of choosing between best-of-breed applications or more economical Open Source options.

Network Service Monitoring

This test phase sought to prove that OSN|M is capable of collecting critical network service metrics and has the ability to act on service exceptions.

Network service monitoring has become essential to the delivery of enterprise and carrier service provisioning. One of the strategic values of the OSN|M is that it collects traffic statistics (latency, packet loss and jitter) and offers a service-based view into the network.

To demonstrate OSN|M's service monitoring capabilities, testers first deployed a Network Quality Analyzer (NQA) Agent onto the Router 6040 hosting the OSN|M module. Next they started capturing service measurements.

From there, Tolly Group observers witnessed testers logging onto the OSN OS where they next loaded MRTG — Multi Router Traffic Grapher, a freeware tool used to monitor the load on network links. MRTG consists of a Perl script which uses SNMP to read the traffic counters of routers (or other devices) and a fast C program which logs the traffic data and creates colorful graphs representing the traffic on the monitored network connection. These graphs are embedded into Web pages which can be viewed from any Web-browser.

Using MRTG, testers were able to gather statistics from the router network interfaces, including delay, packet loss and Mean Opinion Score (MOS), which is used for determining the perceived quality of a voice over IP (VoIP) connection.

When testers ran traffic through the network, MRTG collected the statistics and displayed them for administrators. In fact, when a 10% packet loss delay was removed from the test traffic, the MOS score jumped from 3.35 (dissatisfied users) to 4.1 (satisfied users). The maximum score attainable

for MOS is 4.4, though any score above 4.0 is considered toll quality by The Tolly Group.

Tolly Group observers also noted that testers loaded 3Com's Enterprise Management Suite (EMS), an umbrella manager used to manage SNMP-based switches, routers, security devices, telephony servers and more. For the test, EMS clients connected to the OSN|M module, which fed the traffic management data to the EMS client.

In fact, at one point during testing, the connection for the Router 6040 was pulled and the EMS client running on the OSN|M module caught the anomaly and reported it.

Network Service Monitoring Observations

Here, again the 3Com message of openness comes through loud and clear. tests show that the OSN|M is capable of supporting multiple monitoring applications (EMS, MRTG), as well as deliver interoperability with SNMP-enabled products. This means users can deploy multiple types of service monitoring, each tailored to a specific business need.

From a flexibility viewpoint, the capability to deploy multiple service monitoring tools gives users increased freedom to choose different tools to meet divergent needs. Further, by deploying monitoring at the network edge, in the edge router, administrators can gain a better understanding of the conditions that users see when they are utilizing the services.

The ease-of-use factor with service monitoring focuses on set up — both MRTG and EMS require just about 15 minutes total for set up.

On the security front, deploying SLA monitoring tools at the network's edge translates into a reduction in the amount of management traffic piped upstream to the data center. Instead, service monitoring tools track events locally and feed back only summary data.

With regards to performance, testing shows that the OSN|M exhibits more than enough power to load and sustain multiple applications.

Looking at service monitoring from an OPEX viewpoint, OSN results in faster problem resolution by handling problems locally and tying only exceptions to E-mails that get sent to administrators for immediate notification.

Traffic & Application Visibility

Knowing who, and/or what, is accessing IT resources is vital in today's enterprise networks. Just as important though is how those resources are being utilized and how to better manage them for business gain.

OSN was architected to help users gain a window into network and application utilization. To gain visibility of network and application activity, 3Com utilizes ntop, as well as third-party applications such as AdventNet, Inc. NetFlow Analyzer.

Ntop is a network traffic probe that displays the network usage, similar to what the popular top Unix command does. Ntop users can make use of a Web browser (e.g. Netscape) to navigate through ntop (which acts as a Web server) traffic information and get a dump of the network status.

Improving Visibility

For this scenario, testers enabled NetStream (3Com's version of NetFlow on its routers) and logged into the OSN|M. Testers then loaded ntop and AdventNet's NetFlow Analyzer 5.5, a commercial bandwidth monitoring and reporting tool that analyzes NetFlow data.

With those applications loaded, testers then gathered statistics on traffic flows from all router interfaces on the test network and reviewed the statistics. Tolly Group observers noted that both applications enabled OSN to discover what devices and applications were communicating with the OSN|M.

Traffic & Application Visibility Observations

OSN delivers a level of traffic analysis, integration and visibility into traffic flows and applications that typically can be achieved only by costly

network probe deployments. From an openness standpoint, 3Com has done well to foster tight integration between its NetStream solution and various flow analysis tools.

Moreover, OSN delivers great flexibility —administrators can choose to run Open Source applications, like ntop, or commercial applications like NetFlow Analyzer. Or, they can run them all at the same time with minimal impact on processor utilization; tests show that the OSN processor is utilized just about 10% with NetStream, ntop and NetFlow Analyzer all running.

Moreover, support for such applications is a security boon, since the traffic and application analysis provided by such applications can help reveal potential unsecure hosts or traffic connections and enable administrators to take remedial action.

In the ease-of-use category, both ntop and NetFlow Analyzer load in just 15 minutes or less and offer a Web interface that is easy to navigate.

In the OPEX area, visibility provided by these applications fosters traffic optimization to make more efficient use of network connections, while reengineering brought about by traffic analysis could also reduce operational costs.

Systems Element Manager Review

Beyond network monitoring and traffic flow analysis, administrators need to keep close tabs on switch activity. One way to do so is through port mirroring of all switch activity so companies can capture data and perform traffic pattern analysis.

This becomes especially critical as companies support latency-sensitive applications, like VoIP and video. As these applications proliferate, it becomes essential that enterprises and service providers alike maintain a close watch on VoIP quality, RTP traffic and even HTML data.

One way to maintain such control is through remote support of critical systems elements by enabling OSN|M to support applications that police these traffic types.

Taming Traffic with TShark

For this test, Tolly Group observers enabled traffic mirroring from the switch to the OSN|M front GbE port. Testers then logged into the OSN console and captured multiple traffic patterns of RTP and VoIP using TShark, an Open Source network analyzer available at wireshark.org.

TShark enables users to capture packet data from a live network, or read packets from a previously saved capture file, either printing a decoded form of those packets to the standard output or writing the packets to a file. TShark's native capture file format is libpcap format, which is also the format used by tcpdump and various other tools.

Engineers used TShark to analyze the captured VoIP and RTP streams. In essence, TShark provides deep packet analysis while running on the OSN|M with no need for additional management probes.

By focusing the packet analysis in the OSN|M module, administrators can solve problems without the need for on-site visits.

During the test scenario, Tolly Group observers watched as engineers placed a VoIP call from one IP phone attached to the network, across the test bed to another IP phone. Both the caller and the call recipient spoke for a few seconds before terminating the call.

TShark captured the call duration, and testers were able to isolate the call from the captured packets and replay the entire call with acceptable call quality and clarity.

Packet Capture Performance

Engineers measured the rate at which TShark and OSN|M can capture traffic across a Fast Ethernet link. As in previous tests, mixed packet sizes (64 bytes to 1,518 bytes) were used and three test iterations were run for each test duration and the results were averaged.

Tests show that the OSN|M with TShark can capture traffic at near line-rate, capturing data at a rate of 94.07 Mbps on average.

OSN | M Module Average Packet Capture Rate over Fast Ethernet (Router Bypassed)
TCP Stream Test with Mixed Packet Sizes

Duration	Avg. Throughput	Packets sent	Packets dropped
10 seconds	94.01	121,345	926
30 seconds	94.09	359,177	2,450
5 minute	94.12	2.98M	636,597

Source: The Tolly Group, December 2006 *Figure 3*

Systems Element Manager Observations

The TShark test scenario demonstrated that OSNIM, along with the Open Source TShark application, are able to collect a variety of traffic types — including VoIP, RTP and HTML data.

Detailed Results

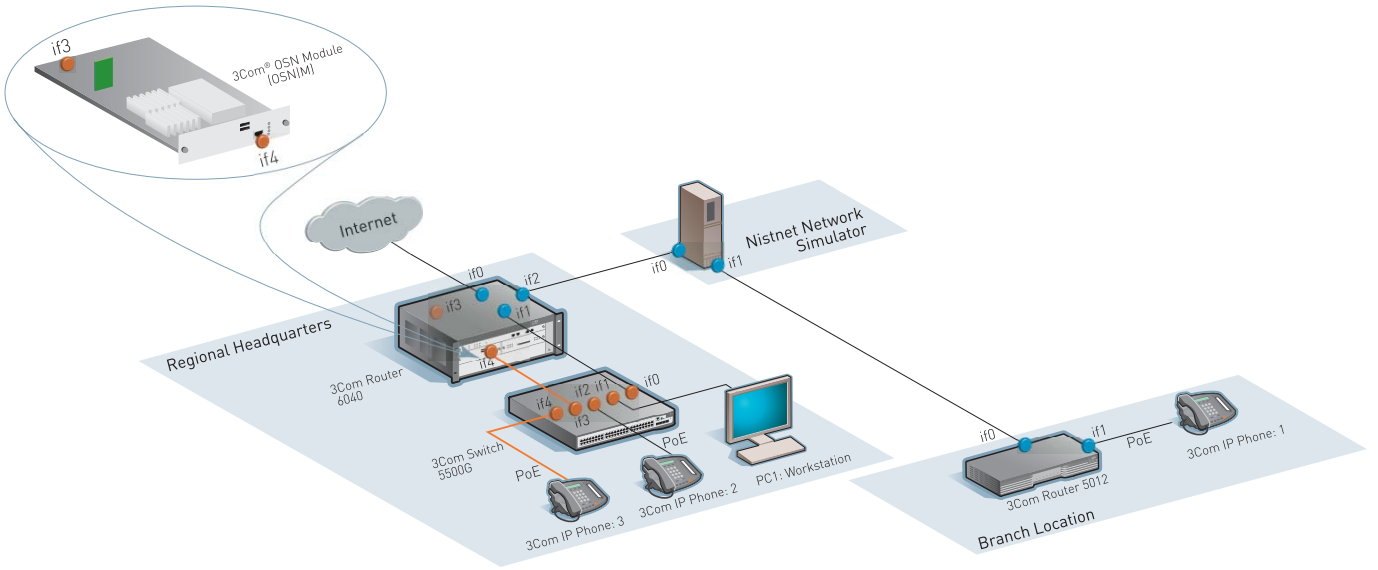
Solutions Under Test

3Com® Router 6040 OSN|M Module

- Processor: 1.4-GHz Intel Pentium M, 400 MHz system bus
- Memory: 512MB/200-MHz RAM DDR DIMM
- Storage: 80-GB EIDE hard disk, 256MB compact flash
- Networking: Two Gigabit Ethernet ports (One external, one connected to internal backplane)
- Serial console redirected to router
- BIOS support: PXE, Boot from CF and extended test

Test Environment

Test Bed — General setup



6040 Interfaces
if0 : NAT enabled connection to Internet connected Subnet
if1 : HQ Subnet
if2 : Connection via simulator to branch Subnet
if3 : OSN|M Internal Backplane GE connection
if4 : OSN|M External GE connection

5500G Interfaces
if0 : Uplink to Router
if1, 2, 4 : Access Ports
if3 : Mirroring / analyzer port

5012 Interfaces
if0 : Uplink to Regional HQ
if1 : Access Port

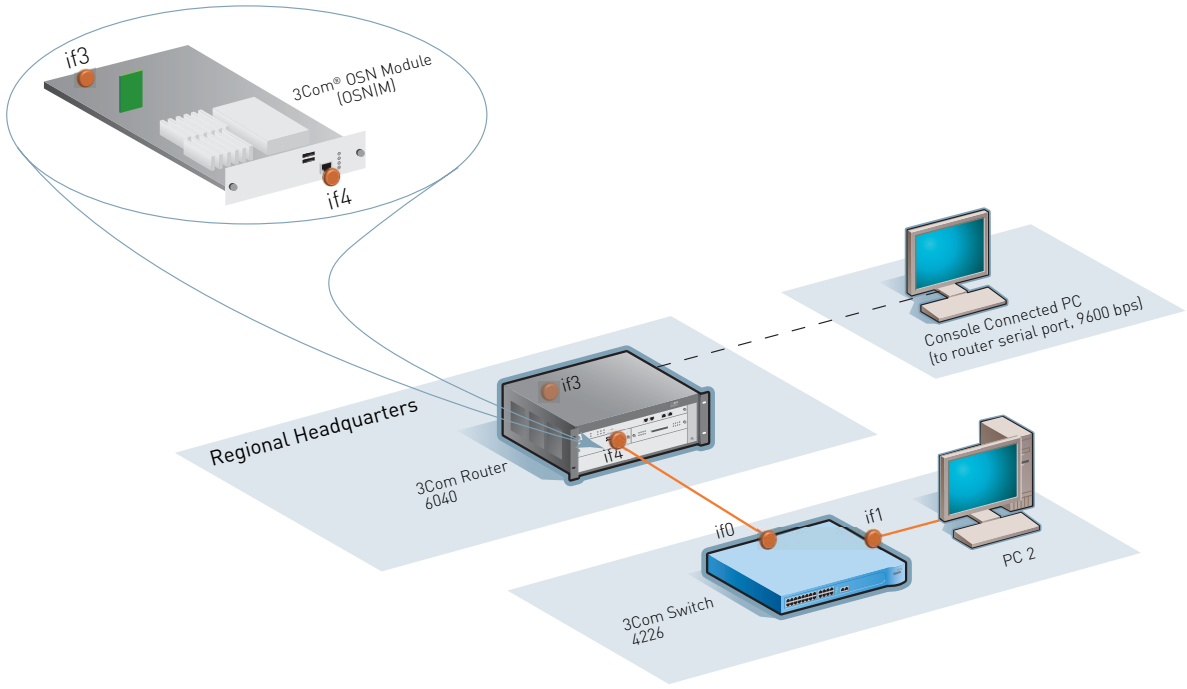
Phone 1, 2, 3 : SIP Phones (G.711)
PC1 : Workstation

10/100 Mbps Interface
10/100/1000 Mbps Interface
100 Mbps Connection
1 Gbps Connection

Source: The Tolly Group, December 2006

Figure 4

Test Bed setup — Bootstrap OS test



6040 Interfaces
if3 : OSNIM Internal Backplane GE connection
if4 : OSNIM External GE connection

4200G Interfaces
if0, 1 : Bridged GE ports

PC 2 : PXE Server (DHCP, TFTP)

10/100 Mbps Interface
10/100/1000 Mbps Interface
100 Mbps Connection
1 Gbps Connection

Test tools

The following tools are supported on the 3Com OSNIM:

Open Source Tools:

- mrtg 2.14.7
  Web:http://oss.oetiker.ch/mrtg/
- ntop 3.2.0
  Web: http://www.ntop.org/

- tshark (wireshark) 0.99.2
  Web:http://www.wireshark.org/
- netperf 2.4.2 (traffic generation tool)
  Web: http://www.netperf.org/netperf/
- squid (web proxy) 2.5
  Web: http://www.squid-cache.org/
- Sarg1.4.1 (Squid analysis report generator)
  Web: http://www.sarg.sourceforge.net/
- Webmin 1.3
  Web: http://www.webmin.com/
- Snort 2.3.3
  Web: http:www.snort.org/
- Hdparm 5.7 (hard disk performance test tool)
  Web: http://www.sourceforge.net/projects/hdparm/
- Nistnet 2.0.12
  Web: http://www-antd.nist.gov/nistnet/

Third-party commercial tools

- Adventnet Netflow Analyzer 5.5 free edition
  Web: http://www.adventnet.com/

3Com tools

- EMS (Enterprise Management Suite) V2.3

Terms of Usage

USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

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 must be based on your own assessment of suitability.

This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and 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. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental and consequentlal damages which may result from the use of information contained in this document

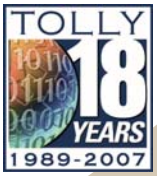
The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers.

When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.

All trademarks are the property of their respective owners.

The Tolly Group is a leading global provider of third-party validation services for vendors of IT products, components and services.

The company is based in Boca Raton, FL and can be reached by phone at (561) 391-5610, or via the Internet at http://www.tolly.com, sales@tolly.com



THE TOLLY GROUP