Miercom

Lab Testing Summary Report

April 2012

Report SR120412

Product Category:

Carrier Class SBC

Vendor Tested:

GENBAND

Products Tested:

S3 on 2U
S3 on GENiUS

Miercom PERFORMANCE VERIFIED™

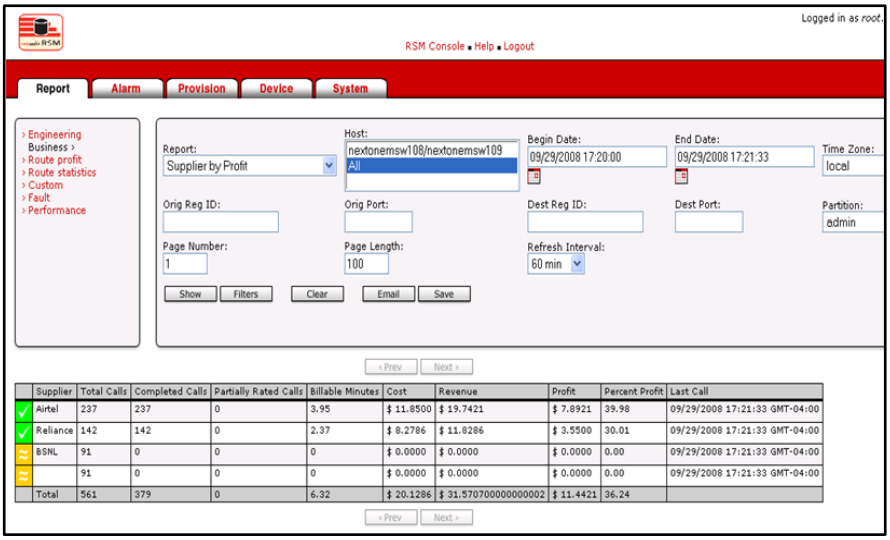
Key findings and conclusions:

- **S3 on 2U Rack Mount Server processes 50,000 concurrent calls at 330 cps**
- **S3 on GENiUS successfully registered 600,000 IADS in 23 minutes, and processed 300,000 concurrent calls at 2,000 cps**
- **GENBAND S3 was resilient to security attacks, such as registration, spoof and call flood attacks, DoS and rogue RTP attacks**
- **Processed 20 million calls while under a 17 hour DoS attack without any performance and quality impact**
- **S3 RSM provides NOC management of performance, configuration, SIP header manipulation, call routing, licensing and backup**

GENBAND engaged Miercom to validate the performance of S3 Session Border Controller (SBC), 2U Server platform and GENiUS blade chassis platform. The GENBAND S3 is a carrier class SBC that is designed to provide intelligent session management, quality assurance, and adaptive security in order to deliver the highest quality service to meet the critical demands of service providers. These platforms do not require customized ASICS or proprietary hardware, which reduces cost and increases flexibility.

The 2U Server platform is intended for small or medium deployments, while the GENiUS platform provides massive scalability with up to six fully redundant blade pairs. Testing was conducted to evaluate the overall performance, scalability, resiliency, and robustness of the

Figure 1: RSM Business Process Reporting



Source: Miercom, April 2012

GENView RSM provides real-time reports that can show call routing prioritized by profit, revenue or minutes.

platforms in both peering and access mode configurations. We also examined the S3s with GENView RSM, which provides NOC management of the entire network, including quality and performance monitoring, configuration management, SIP header manipulation, transcoding, licensing, backup, call routing statistics, alerting and reporting, and CDR generation.

Registration Avalanche

To fully stress the S3 on 2U and S3 on GENiUS and test their robustness, the systems were individually subjected to a registration avalanche or blackout scenario. A registration avalanche can occur in the real world when there are failures or outages in service provider networks. Once the power is restored, all affected SIP devices attempt to reconnect to the network and register to the SBC simultaneously, causing a flood of registration messages. The ability of the SBC to successfully process registration requests from all SIP devices and forward it to the core application server in a reasonable amount of time is a good indicator of the robustness of the platform. These SIP devices can consist of residential endpoints, IADs, as well as IP-PBXs.

Simulation of a registration avalanche was performed on the S3 on 2U platform by first registering 105,600 SIP devices. At the same time, we placed 38,000 concurrent calls though S3 at a rate of 105 calls per second. A firewall rule that blocked all traffic to the SBC was enabled. Within eight minutes, all registered subscribers were dropped from the system.

The S3 recovered from the network failure and reregistered all 100K SIP devices to the network core in under 11 minutes, recording a peak registration rate of 580 rps. Peak CPU utilization was 48.8% and memory usage was constant at 5.3GB.

The S3 on GENiUS was subjected to a larger registration avalanche with endpoints totaling 600,000. At the same time, we directed a total of 228,000 SIP calls through S3 on GENiUS at a call rate of 630 cps.

All endpoints were unregistered, using the firewall rule, from the SBC by monitoring the S3 CLI. Once the firewall rule was disabled, S3 on GENiUS recovered from the network failure and registrations began to occur at a rate of 580 registrations per second (rps). It took 23 minutes to reregister all 600,000 endpoints with a peak of 3,480 rps for the total system.

Peering and Interconnect Call Capacity

Having the capability to achieve high call rates between different carriers in the ever growing SBC space is essential. An SBC needs to achieve high call rates and successfully reach high capacities while utilizing low system resources with high availability and 99.999% uptime.

To verify the call capacity of the 2U Server, we configured the test using six ports of the SBC with call rates of 55 cps per port and a call hold time of 150 seconds. In this configuration, the device achieved a call rate of 330 cps and 50,000 concurrent calls. While under this load, only 28.5% of the CPU and 29% of memory was used. Call quality was good, as metrics recorded during this test included a MOS score of 4, an R-Factor of 78, and call setup latency of 12 msec. The codec used during the capacity test was G.723.1 at 6.3 kbps.

Before the test was initiated, we captured the CPU and memory utilization to determine a baseline when the system was idle. The system resources at idle were relatively low with CPU at 9% and memory of 145MB out of 8.2GB.

The S3 on GENiUS platform was also tested for call capacity. Each redundant blade pair was able to successfully achieve 330 cps, concurrently

Table 1: GENBAND S3 on 2U Performance during Response Flood

Call Metric	Performance
Connected	562,906
Failed Attempted	0
Received	562,907
Answered	562,907
Failed Received	0
End Calls Initiated	518,798
End Calls Received	518,709
End Calls Completed	1,037,445
Transferred	0
Busy	0
Active	50,000
System Resource Usage	
CPU	32%
Memory	2.2GB (27%)

Call performance metrics and resource usage during a SIP Response Flood attack on the S3 on 2U.

processing 1,980 cps across all six blade pairs. A concurrent call rate of 300,000 was maintained for an 11-hour period. Of the 78,600,000 calls placed, only 1,544 calls failed, achieving 99.999% uptime. CPU reached a maximum of 33% and memory was 2.5GB per blade.

S3 on 2U Base Load and Attack

The S3 on 2U product employs a nested security hierarchy that includes IP Rate Limiting (IPRL) as well as Dynamic Blacklisting (DBL). This multilayered approach provides protection against attacks intended to disrupt IP networks.

The S3 implements security features at multiple stages to protect the system from disruption by misbehaving endpoints. Rate limiting is employed in conjunction with dynamic blacklisting. Inbound traffic to the system is first checked against a configurable blacklist policy. The blacklist monitors for malformed or invalid SIP messages, as well as traffic flows which are in excess of the S3 Session Layer Rate Limits (SLRL). Traffic from a blacklist is dropped or rejected gracefully, and the system generates Call Detail Records (CDRs) for tracking purposes.

IP Rate Limiting is performed at multiple levels including endpoint, subnet, realm, and system level. This granularity of security allows identification and isolation of malicious endpoints.

A baseline was established using a G.723.1 codec at 6.3kbps. The base load was 330 cps, call hold time of 150 seconds for a total load of 50,000 concurrent calls. The system used 28.5% CPU and 29% memory. MOS of 4, R-Factor of 78 and latency of 12 msec was recorded. This baseline was used to determine the effects of flood attacks on the product.

SIP INVITE Flood

The S3 on 2U Server was subjected to a SIP INVITE flood and spoofed INVITE flood DoS attack to prove legitimate calls remained connected and new calls could be connected. A SIP INVITE flood attempts to disrupt normal operation of the SBC by sending a flood of INVITEs from random invalid IPs that causes the system to stop processing legitimate calls. The INVITE floods sent 140,000 messages per second for 30 minutes.

The INVITE flood attack had no impact on the MOS and R-Factor. However, the call setup latency increased to 13 msec. This is considered minimal, since it does not impact voice quality.

The CPU and memory utilization were lightly stressed, with CPU reaching 34.6% and memory at a constant 32%. All calls remained connected with 50,000 concurrent calls at 330 cps.

During the spoofed INVITE flood attack, the S3 successfully identified the spoofed endpoint and immediately dynamically blacklisted it to avoid any disruptions to traffic from other legitimate endpoints. Approximately 17% drop was observed, as expected, in concurrent calls, representing traffic blocked from the spoofed endpoint. The MOS, R-Factor and call setup latency were unchanged from the baseline test run. CPU utilization was 29% and memory usage was constant at 2.2GB (27%). Once the attack subsided, the legitimate call processing rates returned to the baseline numbers of 50,000 concurrent calls at 330 cps.

Registration Flood

Overloading an SBC with false registrations from random endpoints causes the SBC to deny registrations from legitimate SIP endpoints. This attack sent 140,000 messages per second for 30 minutes. The attack did not impact the performance of the S3 on 2U Server. All legitimate SIP calls remained connected and illegitimate SIP registrations were dropped. Peak CPU utilization was 35% while memory was constant at 27%. MOS was 4.0, R-Factor 78, and call setup latency increased to 14 msec.

SIP Response Flood

The SIP Response flood was run to ensure legitimate calls remained connected and new calls could be processed during this attack. A spoofed Response flood was also run to determine whether the SBC could distinguish between legitimate responses and responses coming from spoofed IPs. The Response flood attack was configured to send “180 ringing” messages at a rate of 140,000 messages per second for 30 minutes.

The Response flood did not have any impact on call processing for the S3 on 2U. Peak CPU utilization of 32.3% and memory was 27%. Call quality was unaffected. MOS remained stable at 4, R-Factor was 78 and call setup latency was 13 msec.

During the spoofed Response flood attack, the S3 successfully identified the spoofed endpoint and

Table 2: Call Statistics - Calls per Second, R-Factor and Call Setup Latency

	Time Intervals in Minutes:Seconds					
Time Stamp	**28:28**	**28:30**	**28:32**	**28:34**	**28:36**	**28:38**
Calls per Second						
Attempted Calls/Sec	333	328	334	330	334	329
Connected Calls/Sec	333	329	333	330	330	334
R-Factor						
R-Factor Instant (Avg)	78	78	78	78	78	78
R-Factor Instant (Best)	78	78	78	78	78	78
Call Setup Latency						
Call Setup Time (Avg – ms)	12	12	12	12	12	12
Talk Time (Avg – ms)	151,538	151,538	151,538	151,538	151,538	151,538
End Call Time (Avg – ms)	9	9	9	9	9	9
Total Call Duration (Avg – ms)	151,559	151,559	151,559	151,559	151,559	151,559

A ten-minute glimpse of metrics observed for calls per second, R-Factor and call setup latency.

immediately dynamically blacklisted it to avoid any disruptions to traffic from other legitimate endpoints. An approximate 17% drop was observed, as expected, in the number of concurrent calls representing traffic blocked from a spoofed endpoint. CPU, memory, latency, MOS and R-Factor remained stable.

Rogue RTP

Rogue RTP are attempts to inject extraneous IP packets to impact network service quality, deny service, and overload network resources. To prevent rogue packets in media streams, S3 assures that only media streams with authorized packet data are accepted and routed.

A media processor card determines the source IP from signaling information, rather than from media packets, as they arrive and are filtered. The attack traffic was configured to send 140,000 messages per second for 30 minutes.

The rogue RTP attack did not have any impact on connected calls and the S3 maintained the high call processing rate and concurrent calls. Both S3 implementations maintained excellent call quality during the attacks with MOS of 4 and R-Factor of 78-80. System resource utilization remained low. Peak CPU utilization recorded was 35.4% and memory remained at a constant 27%. Call quality of established calls remained unaffected and we recorded MOS of 4 and R-Factor of 78. The call setup latency also remained virtually unchanged.

INVITE Attack Soak Test

A longer duration INVITE attack was initiated against the S3 on 2U to evaluate long-term stability and resiliency of the system. Legitimate SIP calls were connected at a rate of 330 cps with 50,000 concurrent calls for a 17-hour period. The INVITE flood was configured to send 140,000 messages per second using TCP Replay. A resilient solution will maintain call quality and calls.

With over 20 million calls processed, we observed no call failures. Call processing rate and concurrency was maintained with CPU utilization peaking to 30% and memory consistently at 30%. Observed MOS and R-Factor values remained unchanged from the baseline readings, indicating call quality was unaffected. Call setup latency was 14 msec, compared to the baseline of 12 msec.

Survivability Test

In addition to flood attacks and capacity tests, a survivability assessment was performed against the S3 on GENiUS platform with an industry standard SIP fuzz test, SIP torture test and ping of death. These tests would verify the ability of the S3 to withstand attacks and continue normal operation without failure.

SIP fuzz test used PROTOS consisting of 5,400 different fuzzed SIP messages. Throughout the duration of the PROTOS test, the S3 GENiUS SBC maintained system availability.

A SIP torture test was also run against the SBC using Codenomicon's RFC 4475 SIP torture test suite. The SIP torture test consisted of 50 test cases. There was no impact on the S3, the system completely immune to the attack.

Additionally a ping of death was run against the GENiUS platform for ten minutes at 100,000 pps. The ping of death attempts to crash an SBC by

sending large packets at the device under test. The S3 was unaffected by this attack and maintained normal system operation.

GENView RSM Demo

GENBAND provided a demonstration of their GENView RSM. This tool, combined with the S3, provided NOC-level management of the entire network. Quality and performance of the network can be monitored, with real-time analysis available to meet SLA requirements.

Configuration management with the ability to upgrade software on an active SBC can be performed without impacting current call processing. This is possible because the S3 maintains two software images at any given time. GENView also manages image file backups, and restoring from older images.

SIP header manipulation, performed in real-time, can be managed through the same interface, to support real-time interworking with various SIP devices.

GENView RSM provides rich reporting options, including canned and customizable reports for specific needs. In addition to CDR generation, engineering reports can be created showing Average call Success Rates (ASR), Network Effectiveness Ratio (NER), and QoS. Reports supporting business policies can be created, showing calls, minutes, revenue or profit. See *Figure 1* on *page 1*. The reports allow NOC managers to compare rates among peering or billing partners, and adjust alternative routing, as appropriate.

Network alerts and alarms are provided. A unique feature permits proactive decisions based on network traffic performance, allowing the S3 to reroute traffic due to network congestion.

Bottom Line

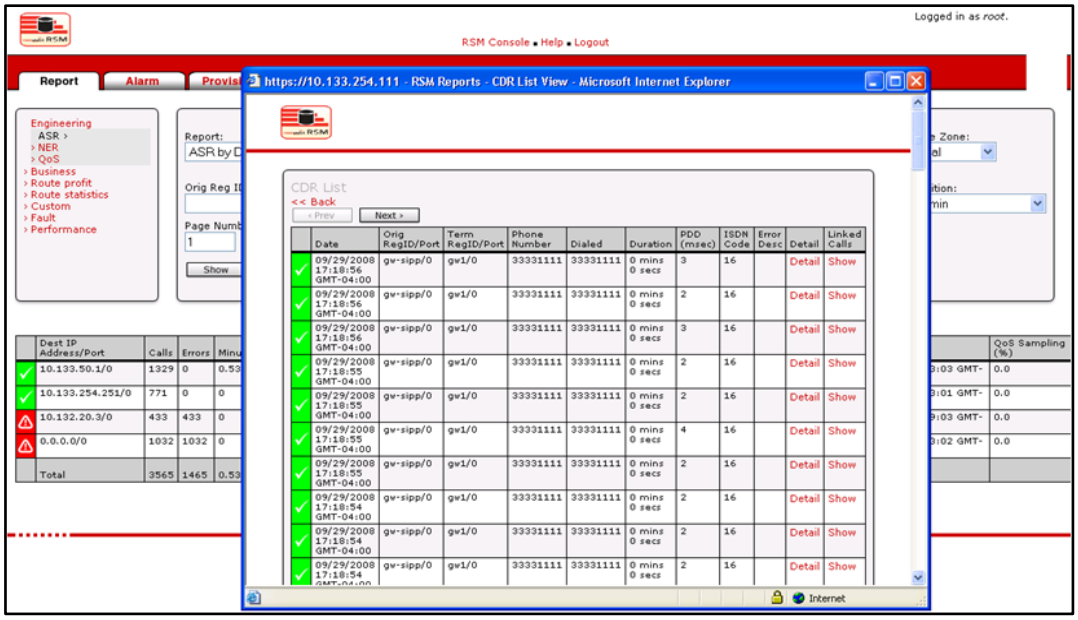
The GENBAND S3 on 2U Server for small and medium deployments provides up to 330 cps and up to 50,000 simultaneous calls.

The S3 on GENiUS chassis provides scalability and high call processing performance, supporting up to 600,000 endpoints and 300,000 concurrent calls at 2,000 cps using six blades.

GENView RSM provides a NOC-holistic view of the entire network, enabling management, monitoring, and reporting functions to support business processes and SLA compliance.

S3 is robust and resilient, maintaining call processing even when subjected to various SIP-based attacks.

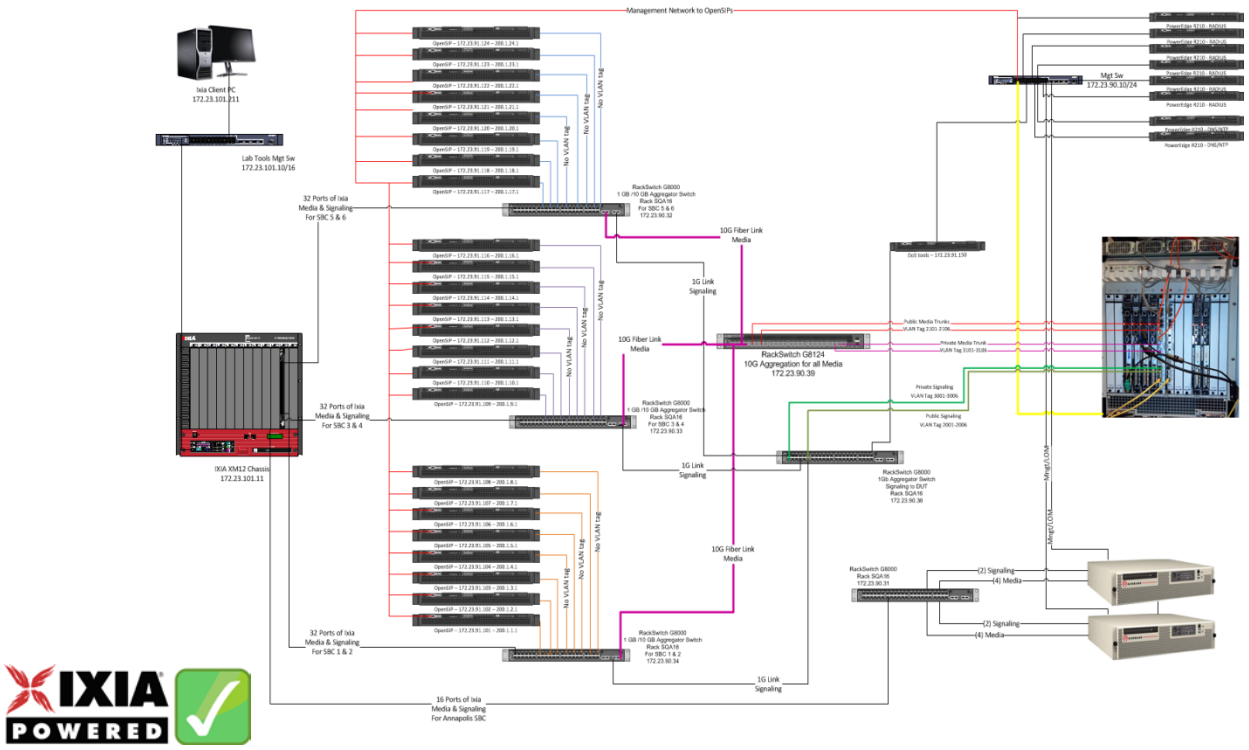
Figure 2: RSM Average Success Rate with CDR List



Source: Miercom, April 2012

GENView RSM displays the average success rate of calls to user-specified destinations. It also provides a list of CDRs for diagnostic and troubleshooting purposes.

Test Bed Diagram



How We Did It

The S3 on 2U server was deployed as an HA pair. The S3 on GENiUS was deployed as a chassis with six redundant blade pairs. Both S3 SBCs ran GENBAND software version 8.0.1.0.

Thirty Dell servers running OpenSIP open-source SIP proxy version 1.7.2 were used to provide registration for 44,500 endpoints.

Five IBM BNT RackSwitch G8000 switches and one RackSwitch G8124 switch with software version 6.7.3 provided aggregation for all signaling and media traffic.

Legitimate baseline call traffic load was provided using IxLoad releases 5.15.168.205 and 5.40.214.37 and Ixia XM12 chassis with 7 Ultra-NP blades.

Baseline registration and call traffic was delivered to the S3 using the Ixia XM12 IP traffic generator. Ixia's (www.ixiacom.com) IxLoad application was used with the XM12 to generate the SIP call loads to the GENBAND S3 SBC. IxLoad is a scalable solution for testing converged multiplay services and application delivery platforms. IxLoad emulates data, voice, and video subscribers and associated protocols for performance testing.

SIP floods from invalid endpoints, spoofed IP flood traffic and Rogue RTP attacks were provided using TCP Replay.

Survivability tests consisting of SIP malformed packet tests, RFC 4475 SIP Torture Test, and Ping of Death attacks were run using PROTOS Test-Suite: c07-sip and Codenomicon Defensics.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Current or prospective customers interested in repeating these results may contact reviews@miercom.com for details on the configurations applied to the Device Under Test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a product selection.

Miercom Performance Verified

The performance of GENBAND S3 on 2U and S3 on GENiUS was verified by Miercom. In hands-on testing, GENBAND demonstrated advanced performance capabilities such as:

- S3 on 2U server processing 50,000 concurrent calls at a rate of 330 cps
- Resiliency to security attacks, such as registration, spoof and call flood attacks, DoS and rogue RTP attacks
- S3 on GENiUS successfully registering 600,000 IADS in 23 minutes and processing 300,000 concurrent calls at 2,000 cps on six blades
- S3 RSM providing NOC management of entire network, including performance, call routing, business metrics, licensing and backup

S3 on 2U and S3 on GENiUS

GENBAND
2801 Network Boulevard,
Suite 300
Frisco, TX 75034
+1.972.521.5800
www.genband.com

About Miercom's Product Testing Services

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including Network World, Business Communications Review, Tech Web - NoJitter, Communications News, xchange, Internet Telephony and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the NetWORKS As Advertised program, the industry's most thorough and trusted assessment for product usability and performance.