Competitive Performance Testing Results
Carrier Class Ethernet Services Routers

Cisco Aggregation Services Router 9000 Series
v
Juniper MX 960 Ethernet Services Router

27 August 2009
Table of Contents

Overview 3
Key Findings and Conclusions 3
How We Did It 4
Quality of Service (QoS) 6
Figure 1: Fabric QoS during Stressful Congestion 7
Figure 2: Fabric QoS with 35% oversubscription of Best Effort Traffic 8
Table 1: Class of Service 9
Scenario A 9
Figure 3: Expected/Unexpected Packet Drop for VLAN Services 10
Scenario B 11
Figure 4: Packet Drop for VLAN Services - with 1500Mbps of Internet Class Traffic 11
Figure 5: Packet Drop for VLAN Services - with 1500Mbps of Internet Class Traffic 12
Scenario C 13
Figure 6: Packet Drop for VLAN Services - with 1500Mbps of Business-1 Class Traffic - Cisco 13
Figure 7: Packet Drop for VLAN Services - with 1500Mbps of Business-1 Class Traffic – Juniper 14
Multicast – Video Resiliency 15
Scenario A 15
Figure 8: Multicast Traffic drops during unrelated hardware event via graceful CLI command 16
Scenario B 17
Figure 9: Multicast Traffic drops caused by physical card removal 17
Figure 10: Multicast Traffic - Packet Drop on Interfaces - Cisco 18
Figure 11: Multicast Traffic - Packet Drop on Interfaces – Juniper 19
Figure 12: Juniper MX 960 Packet Loss for Multicast Return Traffic 20
Resiliency and High Availability 21
Table 2: Service Scale Summary 21
Figure 13: Controlled CLI Initiated Failure Packet Loss - Cisco 22
Figure 14: Controlled CLI Initiated Failure Packet Loss - Juniper 23
Figure 15: Controlled CLI Initiated Failure Packet Loss- Per Port - Juniper 23
Figure 16: Controlled CLI Initiated Failure Packet Loss- Per Port – Juniper 24
Figure 17: Physical Removal Initiated Failure Packet Loss - Per Port - Cisco 25
Figure 18: Physical Removal Initiated Failure Packet Loss - Per Port - Juniper 26
Figure 19: Physical Removal Initiated Failure Packet Loss -PPS rate received - Cisco 26
Figure 20: Physical Removal Initiated Failure Packet Loss- PPS rate received Juniper 27
Figure 21: Packet Loss summary during Simulated Hardware Failure 27
Figure 22: OSPF routing via Graceful Restart – Packet Loss 28
Path Failure Convergence 29
Figure 23: Single Member Link Failure - Cisco 29
Figure 24: Single Member Link Failure - Juniper 30
Figure 25: Bundle Link Failure – resulting in IGP Convergence - Cisco 31
Figure 26: Bundle Link Failure – resulting in IGP Convergence - Juniper 32
Throughput/Capacity Testing 33
Figure 27: Test Topology 33
Figure 28: 160G Live Traffic 34
Modular Power Architecture 35
Other Notes and Comments 36
Overview

The Cisco ASR 9000 Series router proved capable of protecting high priority traffic, while achieving High Availability, and providing superior scalability to meet customers’ future needs.

During testing, the Cisco ASR 9000 Series router outperformed the Juniper MX 960 in the areas of Quality of Service, Multicast for Video Distribution and Streaming services, High Availability and Resiliency.

The Cisco ASR 9000 operates efficiently, providing redundant hardware components such as Route Switch Processors (RSPs), switching fabric, fans and power supplies. Additionally, the platform design allows customers to add power supply modules on an as-needed basis, a “Pay-as-you Grow” approach.

The Cisco ASR 9000 optimizes transport infrastructure due to its service flexibility, resiliency, and High Availability, focusing on Carrier Ethernet as the foundation for service delivery. These attributes allow the ASR 9000 to provide advanced performance in Service Provider environments, where strict Service Level Agreements (SLAs) must be maintained.

Key Findings and Conclusions

- Cisco ASR 9000 hardware architecture protected high priority traffic under all congestion conditions tested. The Juniper MX 960 failed to maintain high priority traffic under the same conditions.
- Fabric-based multicast replication of the Cisco ASR 9000 architecture, proved to be more scalable and resilient than the Distributed Tree Replication (DTR) multicast replication scheme from Juniper. The Cisco ASR 9000 protected both IP Video and Video on Demand (VoD) traffic at all times regardless of the type of failure.
- Cisco ASR 9000 achieved zero packet loss for all services during High Availability testing. The Juniper MX 960 demonstrated unpredictable and severe packet loss depending on the type of failure, under moderate service scale.
- During link failures, the Cisco ASR 9000 converged up to sixty times faster than the Juniper MX 960, protecting services and reducing service outage to a minimum, under moderate service scale.
How We Did It

The Systems Under Test (SUT) included:

- **Cisco ASR 9000 Series Aggregation Services Router (IOS XR version 3.7.2)** included: Two Route Switch Processor Cards (ASR9K-RSP-4G), 4 Port Line Cards: 4 x 10GE (ASR9K-4T-E), 8 Port Line Cards: 8 x 10GE (ASR9K-8T/4-E).
  
- **Juniper MX 960 Ethernet Services Router (JUNOS 9.5 R1.8)** included: Three System Controller Boards (SCB-MX960), with two Routing Engines (RE-S-2000-4096), 4 Port Line Cards: 4 x10GE L2/L3 with Enhanced Queuing (DPCE-R-Q-4XGE-XFP), 4 x10GE L2/L3 capable (DPCE-R-4XGE-XFP) and 4 x10GE L2/L3 capable (DPC-R-4XGE-XFP).
  
- **The Cisco CRS-1 router was configured as a core (P) node with four 2 x 10GE redundant link bundles (a total of 8 x 10GE ports) to provide load balancing and scaling.**

The test equipment was used to create a simulated topology that combines different types of Layer 2 and Layer 3 based services towards the SUT.

30 x 10GE interfaces on the SUT were configured as customer facing UNI interfaces to handle the mixed services with the distribution of services per 10GE interface described below. Each service interface was configured through a single VLAN using IEEE 802.1Q.

Please note: This test was conducted with the most up to date and Generally Available (G.A.) software release from both vendors.

### VPLS (Business VPN):

- 67 x VPLS service interfaces/10G using LDP Signaling
- 67 x VPLS service interfaces/10G using BGP Signaling
- **Total 30 *(67+67) = 4020 VPLS based interfaces with 50/50 distribution between LDP and BGP**

### EoMPLS (Business VPN)

- 134 x EoMPLS service interfaces / 10G (using Martini)
- **Total 30*134 = 4020 x EoMPLS based service interfaces**
L3VPN (Business VPN)
- 10 x L3 VPN service interfaces / 10G
- Total 30*10 = 300 x L3 VPN interfaces

Video Broadcast / Video On Demand
- Shared single L3 based interface/10G for L3 VoD unicast and L3 multicast for video broadcast
- Shared single L2 based multicast interface/10G for L2 multicast broadcast video distribution

High Speed Internet (HSI) / Voice over IP (VoIP):
- Shared Single L2 UNI /10G for Pseudowire-based backhaul of HSI and VoIP traffic to BRAS/BNG

The test equipment simulated 27 separate remote Provider Edges (PEs) connected through the CRS-1 core (P) node simulating all services.
- Each EoMPLS service interface on the SUT was configured to connect point-to-point to one simulated PE.
- Each Virtual Private LAN Service (VPLS) interface represented a unique VPLS domain connected to three remote simulated PEs. The SUT had 4020 VPLS service interfaces, 2010 BGP signaled VPLS domains and 2010 LDP signaled VPLS domains.
- Each Layer 3 VPN service interface was connected to one of three simulated PEs with an equal distribution. Each simulated PE had 100 Layer 3 VPN interfaces.
- Layer 3 based multicast testing consisted of one 10GE interface, connected directly from the test equipment, feeding IP-based multicast traffic into the SUT. This test port was configured to run PIM-SM on the source side, while all UNI interfaces ran IGMPv3.
- The Layer 2 based multicast SUT testing contained a single 10GE interface that was connected from the test system to the SUT, and acted as the source for the multicast traffic. A single VPLS domain was configured in the SUT which spanned across all UNI interfaces, and the source interface. A single VLAN was used on each interface.

The test system used in this evaluation was the SpirentTestCenter ver. 2.32, by Spirent (www.spirent.com). We used three SpirentTestCenter sessions with six links per session between Spirent and the Cisco CRS-1 and ten links per session between the Spirent and SUT. The SpirentTestCenter was used to drive traffic streams, representing High Speed Internet, Video on Demand, Voice, Layer 2 and Layer 3 VPNs.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Contact reviews@miercom.com for additional details on the configurations applied to the System 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 selection.
Quality of Service (QoS)  
**Oversubscription and Preservation of Priority Traffic**

With today’s high end routers, the hardware architecture’s QoS capability is essential when delivering high value services, at the speeds and densities required by service providers. These QoS capabilities include Ingress interface, Fabric QoS and Priority-aware Fabric Scheduling. The Cisco ASR 9000 hardware architecture implements all aspects of QoS and deploys differentiated services with strict SLAs, providing true customer traffic protection.

Networks may over-provision “Best Effort” traffic, incorporating over-subscription in their operating procedures. It is critical for the network system to preserve High Priority traffic during high usage. Since Video and Voice applications are sensitive to traffic loss, and therefore, cannot sustain packet loss, differentiation between the High Priority and Low Priority traffic is essential and required.

Two key tests were performed when it came to QoS:

- **Test 1: Fabric QoS Test**
- **Test 2: Interface Hierarchal-QoS (H-QoS) Test**

**Test 1: Fabric QoS**

We compared the Cisco ASR 9000 to the Juniper MX 960 under congestion conditions where the egress forwarding engine’s fabric connection was congested.

To test the egress forwarding engine’s fabric connection a 3:1 oversubscription setup was used. A 3:1 10GE based oversubscription burst is considered common with today’s networks considering the 10GE port densities and the ratios of upstream to downstream capacities deployed. Each ingress 10GE port was sent a mix of traffic which was comprised of 66% Best Effort (BE), 16% Priority-1 Queue (PQ1) and 17% Priority-2 Queue (PQ2) traffic. The expected result was that the egress 10GE port would transmit 48% PQ1, 51% PQ2 and 1% BE traffic preserving the PQ traffic and dropping almost all the BE traffic.

As shown in Figure 1, the Cisco ASR 9000 dropped more than 99% of “Best Effort” traffic, while 0% of Priority-1 Queue (PQ1) and Priority-2 Queue (PQ2) traffic was dropped thus preserving high priority traffic across the board. In contrast, the Juniper MX 960 dropped anywhere from 97.7% to 98.2% of Best Effort traffic as well as 10.37% of PQ1 traffic and 7.2% of PQ2 traffic. On the Juniper MX 960 all priority level drops were observed in the toward fabric class of service statistics via the Command Line Interface (CLI).

When the rate of oversubscription was reduced by lowering “Best Effort” traffic rate to 35% oversubscription, the Cisco ASR 9000 maintained its protection of priority traffic as before. Juniper’s MX 960 continued to drop all classes of traffic, with 96% of Best Effort traffic dropped, 8.63% of PQ1 traffic dropped and 8.23% of PQ2 traffic dropped, as shown in Figure 2.

We confirmed that all PQ1 and PQ2 traffic generated from Spirent was transmitted by the Cisco ASR 9000, demonstrating that high priority queues were present at both ingress towards the fabric queuing, and on the egress interface port queuing. Evaluating the Juniper MX 960 test results, it appeared the MX 960 supports bandwidth fairness only across the fabric, which gives all ingress streams an equal allocation of bandwidth irrespective of priority. The MX 960 also appeared not to have a strict high priority queue towards the fabric and therefore, BE traffic was transmitted to the egress-forwarding engine effectively blocking PQ traffic during the fabric congestion bursts. On the other hand, the Cisco ASR 9000 priority aware switch fabric and multi-priority toward fabric queuing with strict priorities allowed end-to-end QoS to be maintained.
 carriers retrieve

Carrier Class Routers: Cisco ASR 9000 Series v Juniper MX 960
Copyright Miercom 2009 Page 7 August 2009

Figure 1: Fabric QoS during Stressful Congestion

Cisco ASR 9000 – shows Zero Packet Drop for PQ1 and PQ2 service

![Chart showing packet drop](chart1.png)

Juniper MX 960 – 10.35% and 7.91% Packet Drop on all PQ1 and PQ2 services

![Chart showing packet drop](chart2.png)

In this test scenario, measuring loss during periods of fabric congestion, the Cisco ASR 9000 Series protects high priority traffic during periods of congestion while the Juniper MX 960 experienced packet loss for all services.
In summary, the Cisco ASR 9000 had zero packet loss for any high priority traffic PQ1 and PQ2, based on its advanced system architecture with consistent back pressure and flow control, providing end to end system QoS. In the same test, the Juniper MX 960 resulted in a 10.35% and 7.19% traffic loss for PQ1 and PQ2 respectively during stressful congestion bursts.

Note: This test was performed on the Juniper MX 960 using the DPCE-R-Q-4XGE-XFP line cards.
Test 2: Interface Hierarchical-QoS (H-QoS) Test

We compared the ability of the two platforms to deliver strict SLAs. A three-level H-QoS profile was used under various congestion conditions. This test was performed using the DPCE-R-Q-4XGE-XFP line cards on the Juniper MX 960.

The egress port was configured with 9 VLANs each shaped at 1Gbps. Each VLAN was configured with a 6 class Service Policy as shown in Table 1 below:

Table 1: Class of Service

<table>
<thead>
<tr>
<th>CoS</th>
<th>Service</th>
<th>BW Guarantee (Mbps)</th>
<th>Packet Size</th>
<th>97% of contract to transmit (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Internet</td>
<td>200</td>
<td>1500</td>
<td>194</td>
</tr>
<tr>
<td>1</td>
<td>Business 3</td>
<td>300</td>
<td>1500</td>
<td>291</td>
</tr>
<tr>
<td>2</td>
<td>Business 2</td>
<td>100</td>
<td>1500</td>
<td>97</td>
</tr>
<tr>
<td>3</td>
<td>Business 1</td>
<td>100</td>
<td>1500</td>
<td>97</td>
</tr>
<tr>
<td>4</td>
<td>VoD</td>
<td>250 (policed)</td>
<td>1280</td>
<td>42.5</td>
</tr>
<tr>
<td></td>
<td>Multicast</td>
<td></td>
<td></td>
<td>200</td>
</tr>
<tr>
<td>5</td>
<td>Voice</td>
<td>50 (policed)</td>
<td>128</td>
<td>48.5</td>
</tr>
</tbody>
</table>

Traffic was generated at 97% of contract; i.e., not oversubscribed. We performed three different scenarios within this test. These included:

- **Scenario A:** An additional 500Mbps of multicast stream was sent to all VLANs.
- **Scenario B:** An additional 1500Mbps Internet class traffic was sent on the first three customer VLANs.
- **Scenario C:** An additional 1500Mbps of Business 1 class traffic was sent on the first three customer VLANs.

**Scenario A**

The additional 500Mbps of multicast traffic sent should be policed to 250Mbps, including the Video on Demand (VoD) service which shares the same queue as the multicast service.

The Cisco ASR 9000 performed as expected, dropping only Video on Demand and Multicast packets. No packet loss was seen for any other service.

The Juniper MX 960 dropped Video on Demand and Multicast traffic as expected, but also dropped approximately 600Mbps of Business-3 class traffic across all VLANs. This result highlighted a class isolation issue on the Juniper MX 960, due to its inability to guarantee minimum bandwidth reservations across multiple classes of traffic on the same VLAN interface. Figure 3 shows the resulting packet drops for the ASR 9000 and the Juniper MX 960 for test Scenario A.
With an additional 500Mbps of Multicast Class traffic, the percentage of packets dropped for congested “Best Effort” traffic according to policing policy is indicated in green. The red bar indicates the percentage of packets dropped for non-congested traffic classes. Cisco’s superior QoS architecture in the ASR 9000 protects non-congested classes of traffic according to SLAs, while the Juniper MX 960 shows clear class isolation issues in violation of SLAs.
Scenario B

An additional 1500Mbps of Internet class traffic was sent on the first three customer VLANs only for this test scenario.

The Cisco ASR 9000 performed as expected, dropping only the Internet class traffic on the VLANs that experienced the additional 1500Mbps traffic burst. All the other service classes on all customer VLANs were protected.

The Juniper MX 960, however, dropped Internet class traffic on all VLANs and not just the first three customer VLANs. Investigating the MX 960 drops revealed that all packet drops occurred at the physical interface chassis queue and not the individual VLAN queues. It appears that all the same class traffic have a shared fate across the chassis queue irrespective of which VLAN they belong to. This indicates VLAN or customer isolation issues across the chassis queues. Figures 4 and 5 show the resulting packet drops on the ASR 9000 and MX 960 for Scenario B.

Figure 4: Packet Drop for VLAN Services - with 1500Mbps of Internet Class Traffic

Cisco ASR 9000
Figure 5: Packet Drop for VLAN Services - with 1500Mbps of Internet Class Traffic

Juniper MX 960

VLAN Queue Isolation Problem

Tested VLAN interfaces (Green = expected drops / Red = unexpected drops)
Scenario C

In this scenario, an additional 1500Mbps of Business-1 class traffic was sent on the first three customer VLANs.

The Cisco ASR 9000 performed as expected and dropped only the Business-1 class traffic on just the first three customer VLANs. All other traffic classes and customer VLANs were protected.

The Juniper MX 960 also dropped Business-1 class traffic on the first three VLANs, but also dropped other non-oversubscribed, in-contract classes of traffic on all VLANs (Business-3 and Internet class traffic). Upon further investigation, all Business-3 and Internet class traffic drops occurred at the physical interface chassis queue and not the individual VLAN queues. This indicates not only VLAN or customer isolation issues but also traffic class isolation issues across the chassis queues. Figure 6 and Figure 7 show the results for packet drops on the ASR 9000 and MX 960 for this scenario.

Figure 6: Packet Drop for VLAN Services - with 1500Mbps of Business-1 Class Traffic- Cisco

Cisco ASR 9000

![VLAN Isolation works for Priority Traffic](image)
In summary, the results from these three scenarios highlight a difference in the architectural approaches taken by Cisco and Juniper for Interface QoS. The Juniper MX 960 proved that it cannot maintain minimum bandwidth reservation within the congested customer VLANs nor protect other customer VLANs that were within the contracted bandwidth guarantees. The Cisco ASR 9000, on the other hand, performed efficiently and handled traffic based on defined policies, while protecting customer VLAN traffic.
Multicast – Video Resiliency

The Cisco ASR 9000 router utilizes an intelligent fabric to replicate multicast traffic between forwarding engines/line cards. On the ASR 9000 multicast traffic has separate queue structures across the fabric from those available for unicast traffic. The MX 960 utilizes a multicast replication scheme that Juniper refers to as “Distributed Tree Replication (DTR)” which requires forwarding engines to replicate multicast traffic across the fabric. Furthermore, the Juniper MX 960 multicast traffic shares the same queues as unicast traffic.

In this particular case we again conducted three different tests to demonstrate the various methods of ensuring video resiliency with multicast traffic. These include:

- **Test 1: Unrelated events to Multicast failures**
- **Test 2: Multicast Receiver (customer) side failure event**
- **Test 3: Impact on Video services due to Unicast-based services**

**Test 1: Unrelated events to Multicast failures**

Our test simulated a POP aggregation router providing multicast video distribution and other unicast/MPLS based Layer 2 and Layer 3 services. This test utilized a single Spirent session whereby all 30 UNI links were simultaneously managed in order to properly assess any impact to multicast video distribution when unrelated events to multicast occur on the SUT.

Each UNI link generated 24% of 10GE unicast traffic towards the CRS-1 core (P) router and received 20% (2Gbps) of multicast traffic. The 2Gbps multicast traffic was sourced from a separate link and not one of the 30 UNI or 8 NNI (trunk) links.

This test comprised of two failure scenarios:

- **Scenario A: Induced failure on a trunk link**
- **Scenario B: Induced Route Processor/Switch Fabric hardware failure**

**Scenario A**

In Scenario A, a failure was induced on a core facing line card via a graceful Command Line Interface (CLI) reload command resulting in a 50% reduction in core bandwidth capacity between the CRS-1 core (P) router and the SUT.

The Cisco ASR 9000 was able to protect the multicast streams 100% when the core facing line card supporting 50% of the unicast bandwidth was failed via a graceful restart CLI command.

The Juniper MX 960 experienced a 2%-15% loss of the 2Gbps Multicast streams on 28 out of the 30 customer facing UNI ports. Figure 8 highlights these results.

The Cisco ASR 9000 performed fabric based multicast replication, maximized total switch capacity and guaranteed service availability, compared to the Juniper MX 960 router. The Juniper MX 960 DTR multicast replication architecture was unable to deal with events unrelated to multicast, causing critical service outage.
Figure 8: Multicast Traffic drops during unrelated hardware event via graceful CLI command

Cisco ASR 9000

Juniper MX 960
Scenario B

In Scenario B, we physically removed the active Route Processor / Switch Fabric module and observed that the Juniper MX 960 experienced a 2% to 24% loss of the total 2Gbps multicast streams on all 30 customer facing UNI ports. The Cisco ASR 9000 was able to protect 100% of multicast streams when the active Route Switch Processor (RSP) was “failed”, via physical removal. See Figure 9 for the results of this scenario.

Figure 9: Multicast Traffic drops caused by physical card removal

In summary, the Juniper MX 960 architecture was not capable of protecting multicast streams during hardware outage events, causing critical service outage. The resilient Cisco ASR 9000 architecture protects against hardware related failures and in turn, protects multicast video based services.
**Test 2: Multicast Receiver (customer side) Failure Event**

We tested the ability of the SUT to protect multicast streams when an unpredictable traffic disruption occurs for multicast services. This was simulated when a line card supporting four customer facing UNI (10GEs) ports was failed via a graceful restart CLI command. This test was further simplified by removing unicast traffic and reducing the total multicast traffic to 1Gbps. Again, the multicast traffic was sourced from a separate link and not one of the 30 UNI or 8 NNI links. All 30 UNI links received the 1Gbps multicast traffic.

The Cisco ASR 9000 was able to protect the multicast streams. The only multicast traffic lost on the ASR 9000 was on the specific failed line card, as expected.

The Juniper MX 960 experienced an average of 5.18% packet loss of the total 1Gbps multicast streams, over the test duration of 5 minutes on the majority of the 30 customer facing UNI ports. As shown in Figures 10 and 11, there is a period of approximately 30 seconds when the affected receiving ports lost 100% of the traffic.

**Figure 10: Multicast Traffic - Packet Drop on Interfaces - Cisco**

*Cisco ASR 9000*
The graph above and on the previous page, illustrate the duration of impact on traffic experienced, when four customer-facing UNI ports are failed via a CLI graceful restart command.

The Juniper MX 960 DTR multicast architecture led to unpredictable traffic disruption for multicast services caused by hardware outages unrelated to multicast source. The Cisco ASR 9000 protected multicast traffic against the hardware related failures, providing an efficient delivery of multicast video based services. The ASR 9000 provides a resilient fabric architecture, which does not depend on other system components for multicast replication.
**Test 3: Impact on Video Services due to Unicast-based Services**

This final test investigated how the SUT would behave with a high volume of multicast traffic simulating a scaled HDTV broadcast service. We used the same set up as in Test 2 but with 6.5Gbps of multicast traffic instead of 1Gbps replicated to all 30 UNI ports transmitting broadcast HDTV services. We also introduced, gradually increasing, unicast-based service traffic originating from one of the 10GE customer facing UNI ports.

The Cisco ASR 9000 correctly forwarded all unicast and multicast based services.

The Juniper MX 960 experienced an average of 0.14% packet loss on 15 of the 30 UNI ports once the unicast traffic rate from the customer 10GE UNI port reached 6.7Gbps. All unicast traffic from the customer 10GE UNI port above 6.7Gbps was also dropped. This indicates that the Juniper DTR multicast architecture has bandwidth and scale inefficiencies. The challenge in this case would be to predict every customer (UNI) link bandwidth requirements in order to safely protect the multicast HDTV service. See Figure 12 below for detailed results.

Figure 12: Juniper MX 960 Packet Loss for Multicast Return Traffic

In summary, the fact that unicast-based services traffic impacts the multicast streams, leading to unpredictable traffic disruption for unicast and multicast based services, the Juniper MX 960 proved it could not provide customer/service isolation. The Cisco ASR 9000 correctly forwarded all injected traffic and provided predictable delivery of multiple real-time based services, proving efficient architecture design.
Resiliency and High Availability

Offering continuous network operations for all applications/services is a basic requirement for all Service Providers. Residential customers require access to data, voice, and video services at all times. Enterprise business customers depend on 24-hour network operations with strong service-level agreements (SLAs) for mission-critical applications. Mobile phone subscribers expect to be able to make calls and access data services at all times.

All resiliency and system availability tests were performed with a moderately scaled configuration as described in Table 2 below:

Table 2: Service Scale Summary

<table>
<thead>
<tr>
<th>Services</th>
<th>Transport Protocols</th>
<th>Number of Connections Configured in Test</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSI / Voice</td>
<td>MPLS P2P pseudowire (PW)</td>
<td>30 PWs</td>
<td>Shared VLAN / Port Per UNI Interface Traffic 512Mbps 8K subscribers per UNI port 64 Kbps bandwidth per subscriber 240K total Subscribers 15.4Gbps Aggregate Traffic</td>
</tr>
<tr>
<td></td>
<td>Backhaul</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoD</td>
<td>L3 IP Unicast</td>
<td>30 Sub-interfaces</td>
<td>3K VoD subscribers (100/UNI port), 2.5Mbps each (250Mbps/UNI port) 7.5Gbps of Aggregate Traffic for 30 UNI ports.</td>
</tr>
<tr>
<td>Video Broadcast</td>
<td>L3 IP Multicast / L2 Multicast</td>
<td>30 L3 sub-interfaces (Shared with VoD) / 30 sub-interfaces for L2 Multicast</td>
<td>1.25Gbps L2 Multicast per UNI port 1.25Gbps L3 Multicast per UNI port 75Gbps Aggregate multicast Replication</td>
</tr>
<tr>
<td>Business</td>
<td>MPLS P2P PW</td>
<td>4020 PWs</td>
<td>134 sub-interfaces per UNI Port 512Kbps per service (sub-interface) 67Mbps per UNI Port 2.01Gbps Aggregate Traffic</td>
</tr>
<tr>
<td>Business L2 VPN</td>
<td>VPLS PW 50% BGP signaled</td>
<td>12K PWs for 4020 domains</td>
<td>134 sub-interfaces per UNI Port 512Kbps per VPLS domain (sub-interface) 67Mbps per UNI Port 2.01Gbps Aggregate Traffic</td>
</tr>
<tr>
<td>P2P</td>
<td>50% LDP signaled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business L3 VPN</td>
<td>MPLS / IP</td>
<td>300 L3 VRFs</td>
<td>VRF per sub-interface, 10 per UNI port 1Mbps per sub-interface 10Mbps per UNI port 300Mbps Aggregate Traffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The failover of a Route Processor/Switch Fabric, without traffic impact, is critical to a Service Provider for providing High Availability (HA) to their customers who in turn depend on 24-hour network operations for data, voice, mobile phone and video services, with strong SLAs.
In this particular test, we conducted three different scenarios whereby we tested the impact to services when we initiated different failover events. These included:

- **Scenario A:** Route Processor/switch Fabric failover using a graceful CLI command
- **Scenario B:** Physical removal of Route Processor/switch Fabric failover with a hardware failure
- **Scenario C:** Restarting OSPF via a CLI command.

**Scenario A: Route Processor/switch Fabric failover using a graceful CLI**

A resilient architecture should failover from the primary control plane to the standby control plane, without incurring packet loss, thereby preserving traffic for all services.

Figure 13, Figure 14, Figure 15 and Figure 16 illustrate the results for the command line initiated failover. The Cisco ASR 9000 experienced 0% packet loss, while the Juniper MX 960 experienced a 31% packet loss.

An investigation into the unexpected severe packet drops demonstrated by the Juniper MX 960 revealed that it did not send a graceful re-start Link State Advertisement (LSA) to the neighboring core (P) router resulting in an OSPF timeout. However, even if we only consider the packet loss before the OSPF timeout for one of the three Spirent sessions, the Juniper MX 960 still exhibited significantly higher packet loss than that of the Cisco ASR 9000.

**Figure13: Controlled CLI Initiated Failure Packet Loss - Cisco**

Cisco ASR 9000 - Zero Packets dropped across all services
**Figure 14: Controlled CLI Initiated Failure Packet Loss - Juniper**

Juniper MX 960 Packets dropped across all services

![Graph showing packets dropped across all services.]

**Figure 15: Controlled CLI Initiated Failure Packet Loss- Per Port - Juniper**

Juniper MX 960 (Ignoring OSPF Timeout)

![Graph showing packets dropped per port.]

The graph above shows the Packets Per Second (PPS) rate received when the actual switchover occurred between 10:28:28 and 10:28:56. During that period a total of 267140 packets were dropped on the Juniper MX-960.
Figure 16: Controlled CLI Initiated Failure Packet Loss - Per Port – Juniper

Juniper MX 960

Packets lost during RE failover only

Session 1 Test Results

Packets dropped by Juniper MX 960 on a per port basis. No packet drops were observed for Cisco ASR 9000
**Scenario B: Physical removal of Route Processor/Switch Fabric failover with a (hardware failure)**

Figures 17 and Figure 18 illustrate the results for the hardware simulated failure. The Cisco ASR 9000 experienced 0.0017% packet loss and the Juniper MX 960 a 15.6% (17762641 packets) packet loss. The Cisco ASR 9000 dropped an insignificant number of packets using IOS XR version 3.7.2 during failover of the Route Switch Processor/Switch Fabric, compared to the Juniper MX 960 which demonstrated significant performance degradation. A pre-release version of IOS XR version 3.9 proved even better performance, with zero packet loss on the ASR 9000.

An investigation into the unexpected severe packet drops by the Juniper MX 960 revealed that it did not send a graceful re-start Link State Advertisement (LSA) to the neighboring core (P) router resulting in an OSPF timeout. Considering only the packet loss before the OSPF timeout for one of the three Spirent sessions, the Juniper MX 960 still exhibited significantly higher packet loss than that of the Cisco ASR 9000. Please refer to Figure 19, Figure 20 and Figure 21 for more test details.

**Figure 17: Physical Removal Initiated Failure Packet Loss- Per Port - Cisco**

Cisco ASR 9000 - 0.0017% Packet Loss

During the switchover period, 0.0017% packet loss was seen across all services for the Cisco ASR 9000
During the switchover period, packet loss was seen across all services and a total of 17,752,641 packets were dropped on the Juniper MX-960.

This graph shows the PPS rate received on the ASR 9000 when the Route Processor/Switch Fabric failover occurred. As we can see, the packet loss on the ASR 9000 was 0.0017%.
Figure 20: Physical Removal Initiated Failure Packet Loss- PPS rate received Juniper

Juniper MX 960 –15.62% Packet Loss (Ignoring OSPF Timeout)

The graph above shows the PPS rate received on the Juniper MX 960 when the Route Processor/Switch Fabric switchover occurred. Packet loss was seen across all services and in some cases, severe packet loss was observed.

Figure 21: Packet Loss summary during Simulated Hardware Failure

(Ignoring OSPF Timeout for Juniper MX 960)
**Scenario C: Restarting OSPF via a CLI command.**

Figure 22 illustrates the results for the OSPF process restart via CLI command. On the Juniper MX 960 all routing protocols had to be restarted as they all run in one process. The Cisco ASR 9000 experienced 0% packet loss while the Juniper MX 960 experienced a 0.067% packet loss. For this process restart test, an OSPF graceful restart LSA was successfully generated, ruling out the possibility of erroneous system configuration issues.

**Figure 22: OSPF routing via Graceful Restart – Packet Loss**

- **Cisco ASR 9000 – Zero Packet Loss**

  ![Cisco ASR 9000 Packet Loss Graph](image)

- **Juniper MX 960 - 0.067% Packet Loss**

  ![Juniper MX 960 Packet Loss Graph](image)

Compared to Juniper MX 960, the Cisco ASR 9000 had zero packet loss when restarting a routing protocol like OSPF using a graceful CLI command. The Juniper MX 960 showed a 0.067% packet loss.

To summarize the previous three test scenarios, the Juniper MX 960 allowed critical traffic flows to drop across all services, even during a routing process graceful restart. The Cisco ASR 9000 preserved traffic flows for all services during system failover. The Cisco ASR 9000 has been designed from its inception to support service scale with High Availability, ensuring Non Stop Service Availability.
Path Failure Convergence

Service providers are focusing on the migration of their networks to a single, converged infrastructure, supporting all services, which results in reduced costs and operating expenses. We measured the packet loss during convergence time for each SUT using two different scenarios:

- **Scenario A:** Single link member failure within a bundle
- **Scenario B:** Entire bundle failure

This test was performed with a moderately scaled configuration as described in Table 2 on page 21. The physical topology included a total of four bundle groups; i.e., four ECMP paths between the SUT and the core (P) router. The link failures were simulated by disconnecting the physical Transmit (Tx) and Receive (Rx) links through an Optical Cross Connect (OCC) used to establish all the links between the SUT and core (P) router and Spirent Testcenter.

**Scenario A: Single link member failure within a bundle**

The failure of a single link does not fail an IGP path and therefore only a switch over of traffic to the remaining links in the link bundle is required. Cisco ASR 9000 was able to switch traffic to the active link with only 0.02% traffic loss. Juniper MX 960 demonstrated a more significant loss; i.e. 0.36% traffic loss. See Figure 23 and Figure 24 for more details.

**Figure 23: Single Member Link Failure - Cisco**

Cisco ASR 9000 Minimal Impact on Services- 0.02% packet loss
The Cisco ASR 9000 was able to switch over from one link to another within the same bundle, much faster than the Juniper MX 960, which resulted in fewer packet drops, critical for meeting strict SLAs.
**Scenario B: Entire bundle failure**

The failure of a link bundle does result in the loss of one of the four bundles/ECMP paths resulting in an IGP path recalculation. The Cisco ASR 9000 was able to switch traffic as a result of the bundle failure to the remaining three active bundles with only 0.01% traffic loss. The Juniper MX 960 demonstrated a much more significant loss of 2.18%. The outage on the Juniper MX 960 lasted more than a minute, which in some cases can be considered very serious for Service Providers who offer SLAs, particularly to financial customers. Please see Figure 25 and Figure 26 for more details.

**Figure 25: Bundle Link Failure – resulting in IGP Convergence - Cisco**

---

**Cisco ASR 9000 0.01% Packet Loss**

![Packet Loss Graph](image-url)
Figure 26: Bundle Link Failure – resulting in IGP Convergence - Juniper

Juniper MX 960 – Larger impact on Services- 2.18% Packet Drop

Cisco ASR 9000 was able to switch over traffic across the ECMP paths in approximately the same time as it did for a single link member failure. Juniper MX 960 was significantly slower than its single link member failure time, indicating that it is greatly impacted when an IGP path recalculation is required. The Cisco ASR 9000 was able to failover, with approximately 155 times less traffic loss.

In summary, the Cisco ASR 9000 was able to switch over from one link to another within the same bundle or across ECMP paths in approximately the same time with only 0.01-0.02% packet loss. The Juniper MX 960 was significantly slower for the ECMP link bundle failure recovery than its single link member failure recovery time indicating that there is a greater impact when an IGP path recalculation is required. The MX 960 with the IGP path recalculation demonstrated 155 times more packet loss than the Cisco ASR 9000.
Throughput/Capacity Testing

We evaluated the throughput and scalability of the Cisco ASR 9000 to verify that it can indeed support in excess of 100 Gbps throughput per slot and be the industry’s first vendor to support such a capability. With the new 16-port 10GE card (A9K-16T/8) the Cisco ASR 9000 can support 160 Gbps per slot as shown in Figure 28.

We could not run a similar test on the Juniper MX 960 as the platform supports a 4-port 10GE card and a 40 Gbps forwarding engine, thus allowing for a total of 44 x 10GE ports total per chassis and 440 Gbps maximum system capacity. While the Cisco ASR 9000 supports a 4-port 10GE and an 8-port 10GE cards as well, the new 16 port-10GE card we tested allows for a total of 128 10GE ports per system.

The ASR 9000 was able to demonstrate:

- The 16-port 10GE card is capable of forwarding 160Gbps Unicast and Multicast traffic (100% line rate for all ports)
- Zero packet loss during Route Switch Processor failover, ensuring industry’s highest availability at 160 Gbps per slot

Figure 27: Test Topology

The diagram above shows the test topology that was configured, demonstrating the Throughput/Capacity validation of the 16-port 10GE card.
Figure 28: 160G Live Traffic

This diagram above shows the line rate traffic (10 Gbps) received on each of the ports for the 16 x 10GE card. Each port is identified by a unique color. The traffic received is a combination of unicast and multicast traffic.


Modular Power Architecture

The modular power supply architecture of the Cisco ASR 9000 Series offers advantages by scaling to match port density requirements quickly and easily.

Customers can benefit from the “Pay-as-you-Grow” model, by only consuming the power needed to support the density of the installed ports or line cards.

The efficient power modules provide one to one load-sharing ability, with no down time, providing system flexibility and High Availability. The power supplies are housed in serviceable Power Entry Modules (PEMs), in AC (3KW (AC) or two different DC (2.1KW (DC) or 1.5KW (DC) configurations. Each PEM can hold up to three modules of its corresponding type, with no power zones or placement restrictions. Note that AC and DC power combination is not supported.

We evaluated the insertion and removal of power supply modules on the Cisco ASR 9000 Series to determine the impact on the traffic flow. We observed no impact to traffic or services during removal and insertion of power supply modules, and router statistics reflected the current load sharing status. It should be noted, you don’t need to disconnect/connect additional power sources when inserting or removing power supplies, making this a very simple procedure. Offering a modular architecture, the Cisco ASR 9000 Series allows customers to add power supplies as needed, with no impact to traffic flow and avoids “day one” maximum system power consumption. The current thermal infrastructure design of the Cisco ASR 9000 Series routers supports the cooling needs for future higher capacity line cards.

Though the Juniper MX 960 offers redundant power supplies, by contrast, the fixed power supply configuration does not offer the flexibility to scale power consumption to port density needs.
Other Notes and Comments

Information contained in this report is based upon results observed at a Cisco facility in San Jose, CA. Test cases were based on parameters set by Cisco.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Contact reviews@miercom.com for additional details on the configurations applied to the System 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 selection.

Product names or services mentioned in this report are registered trademarks of their respective owners. Miercom makes every effort to ensure that information contained within our reports is accurate and complete, but is not liable for any errors, inaccuracies or omissions. Miercom is not liable for damages arising out of or related to the information contained within this report.