

JUNIPER NETWORKS: QUALITY OF EXPERIENCE VALIDATION

Report for Microsoft Lync

Introduction

Now more than ever, the corporate network is a strategic business tool. Unfortunately, many networks today can't keep pace with the escalating demands and risks that compromise their effectiveness. With unified communications (UC) becoming an essential way of conducting business, successful deployments of applications such as Microsoft® Lync™ rely on a super powerful networking infrastructure to satisfy unique requirements presented by UC – the ultimate combination of presence, messaging, video, conferencing, and voice. These stringent requirements include:

- Assured low latency, low jitter, and packet loss, while providing adequate bandwidth to guarantee predictable high-definition video and audio traffic
- Continuous network availability throughout all locations at all times
- High degree of scalability, ease of deployment, and visibility
- Superior network security to ensure that mobile and remote users gain LAN-like quality over the WAN across all locations

As a Lync network technology partner, Juniper recently conducted a series of network performance tests to demonstrate its ability to meet these stringent requirements, and validate compliance against specified performance criteria for Microsoft's UC platform. This document describes the network configuration and presents the successful result of the network testing that was run by Microsoft and Juniper personnel.

At the completion of testing, Microsoft validated that the Juniper networking products fully met, and even exceeded, the end-to-end performance requirements for Lync application traffic.

Overall Network Design

For validation purposes, Microsoft provides a target network design consisting of a headquarters and three branch office locations, interconnected via a simulated WAN. For purposes of this test and simplicity, Juniper configured all network connections using 1 Gbps Ethernet. A Shunra Virtual Enterprise STA latency/packet loss generator appliance was connected inline to simulate network degradation between sites. A Spirent traffic generator was used to provide background traffic and validate the injected latency and packet loss.

Transport mode IPsec VPN tunnels using AES-128 encryption were defined from each branch office to HQ and the other branch offices in a fully meshed configuration, to provide full privacy and authenticity. Juniper's focus on high-performance networking also allowed for a design with high security that more accurately reflects the real-world conditions into which a Lync environment would typically be installed.

Quality of service (QoS) using DiffServ code point (DSCP), was configured end to end. Where supported, six queues were used to separate and prioritize the media and signaling traffic from the normal data traffic. Traffic was classified on ingress to the network and assigned to the appropriate queue. On egress, queued traffic was marked for priority treatment by the next device. Due to Juniper Networks' focus on high-performance networking, prioritization of real-time traffic can be reliably performed without impacting network performance.

See *Figure 1 Microsoft Lync case study designated profile*

Headquarters – Boston

The headquarters network consisted of a simulated data center and end user networks. The network Windows Domain Controller, SQL Server, front end servers, and QoE Monitoring Server were located within this simulated data center. End user terminals (IP phones and soft clients) were attached to a separate subnet in HQ. The HQ network was comprised of a Juniper Networks® EX8208 Ethernet Switch with separate VLANs for the data center and end user connections. Data center servers were connected directly to the EX8208.

Individual end user connections included workstations (running Microsoft Windows 7 and Microsoft® Lync™ Server 2010 with attached Microsoft Web camera and Polycom Blackwire C220 Headset) and Polycom CX600 IP phones. These end user stations were connected to a Juniper Networks EX4200 Ethernet Switch with Virtual Chassis technology, which was then connected to the EX8208. Security and VPN tunnel termination for the HQ site was provided by a Juniper Networks SRX3600 Service Gateway, which connected between the EX8208 and a Juniper Networks M7i Multiservice Edge Router used for WAN connectivity.

Branch Offices

Three branch offices were configured as part of the test network. Each of the branch networks used a Juniper Networks SRX Series Services Gateways device for security and WAN access. Two branches (each designated as medium sized) used a Juniper Networks EX4200 Ethernet Switch with Virtual Chassis for local connectivity and to provide Power over Ethernet (PoE). The remaining branch (designated small) used an SRX210 Services Gateway for security, WAN access, local connectivity, and PoE. Figure 2 represents the entire Juniper test topology.

Quality of Service

Quality of service (QoS) was configured on all network infrastructure devices. For devices that supported it, six traffic queues were used in this demonstration: “best-effort,” “expedited-forwarding,” “assured-forwarding,” “network-content,” “voice-rtp,” and “voice-sip.” For these test scenarios, simple traffic filters were used on the SRX210 ingress ports to categorize traffic. Any traffic going to or from any of the data center-based servers was assigned to the “voice-sip” queue. Any traffic originating from the local Lync Server 2010 clients and destined for any of the remote Lync Server 2010 clients was assigned to the “voice-rtp” queue. In a production deployment, more restrictive filters that limit prioritization to just media and signaling would be defined. These filters could be based on a rich mix of source/destination IP addresses, protocol ports, packet size, or many other criteria that

could uniquely identify the VoIP traffic. In addition, the Juniper Networks EX Series Ethernet Switches and SRX Series Services Gateways support Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED), which automatically places the phone into the correct voice VLAN and QoS queue.

On egress, traffic shapers were defined to ensure that client signaling and media traffic were transmitted ahead of other, less delay sensitive traffic. Real-Time Transport Protocol (RTP) and Session Initiation Protocol (SIP) were each allocated 10 percent of the buffer. Best-effort traffic was given the remainder.

Quality of Experience

The best method of determining the quality of a VoIP system is to have end users rate the sound quality of the calls they make. The sound quality of an audio call is very subjective. An end user’s determination of a good vs. poor quality call is influenced by a number of factors, including (but not limited to) background noise, subject of the call, current mood, hearing impairment, etc. In addition, the audio system itself affects the perceived quality by limiting audio response and/or using compressors/decompressors (codecs) to reduce bandwidth requirements.

The International Telecommunications Union (ITU) has a standardized procedure (P.800) that utilizes a panel of listeners and certain phrases to determine call quality. Each panel member listens to the predefined phrases read over the audio system being evaluated. The panel member rates each phrase with a numeral

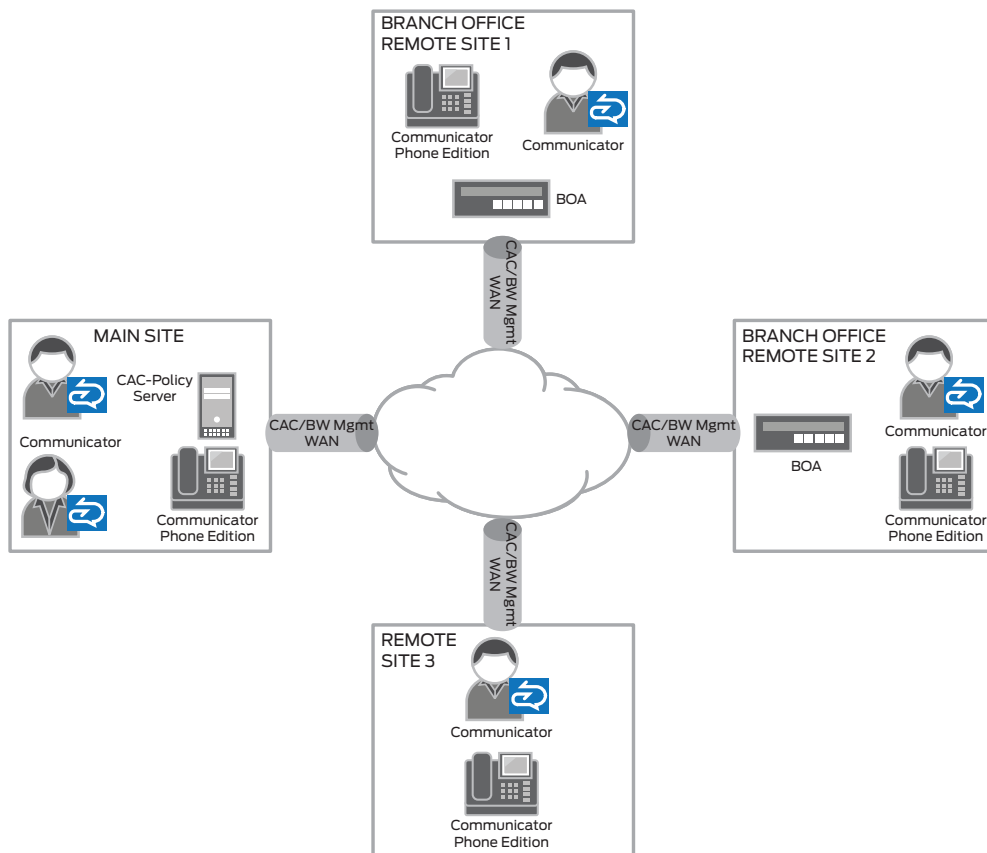


Figure 1: Microsoft Lync case study designated profile

between 1 (Impossible to communicate) and 5 (Clear – like the person was next to the listener). All values are averaged together to give a final Mean Opinion Score (MOS). Since it is impractical to seat a panel of listeners anytime you want to evaluate an IP phone system, mathematical approximations have been developed that take into account network packet loss, jitter, the codec used, and other measurements to calculate an approximate MOS value.

Video content is much more complex than audio, requiring higher bandwidth for acceptable signal quality and making the content much more affected by network impairments such as bandwidth restrictions, packet loss, jitter, and delay.

For historical and technical reasons, measurement of video experience has trailed measurement of audio experience. Work is progressing in the area of video quality evaluation methodologies and several solutions are becoming available. The primary focus of these solutions is to derive a video MOS that quantifies the overall perceived quality of a video transmission and the effect network impairments have on the perceived quality of transmitted video.

Microsoft Quality of Experience Monitor

As part of the Lync installation, a Quality of Experience (QoE) monitor was installed. The QoE monitor receives real-time quality metrics from the user endpoints, correlates the data, and calculates Mean Opinion Scores (MOS) for each audio or video conversation. The server provides real-time updates, alerts, and detailed analysis of network performance to accurately reflect users' experience based on the endpoint they're using. QoE monitor reports were used to capture call metrics and report on test case call quality.

Network Impairment and Latency

A Shunra Virtual Enterprise STA appliance was inserted inline between the branch offices to emulate real-world network latency and packet loss. During various test cases, latency and packet loss were programmed into the link to simulate network degradation.

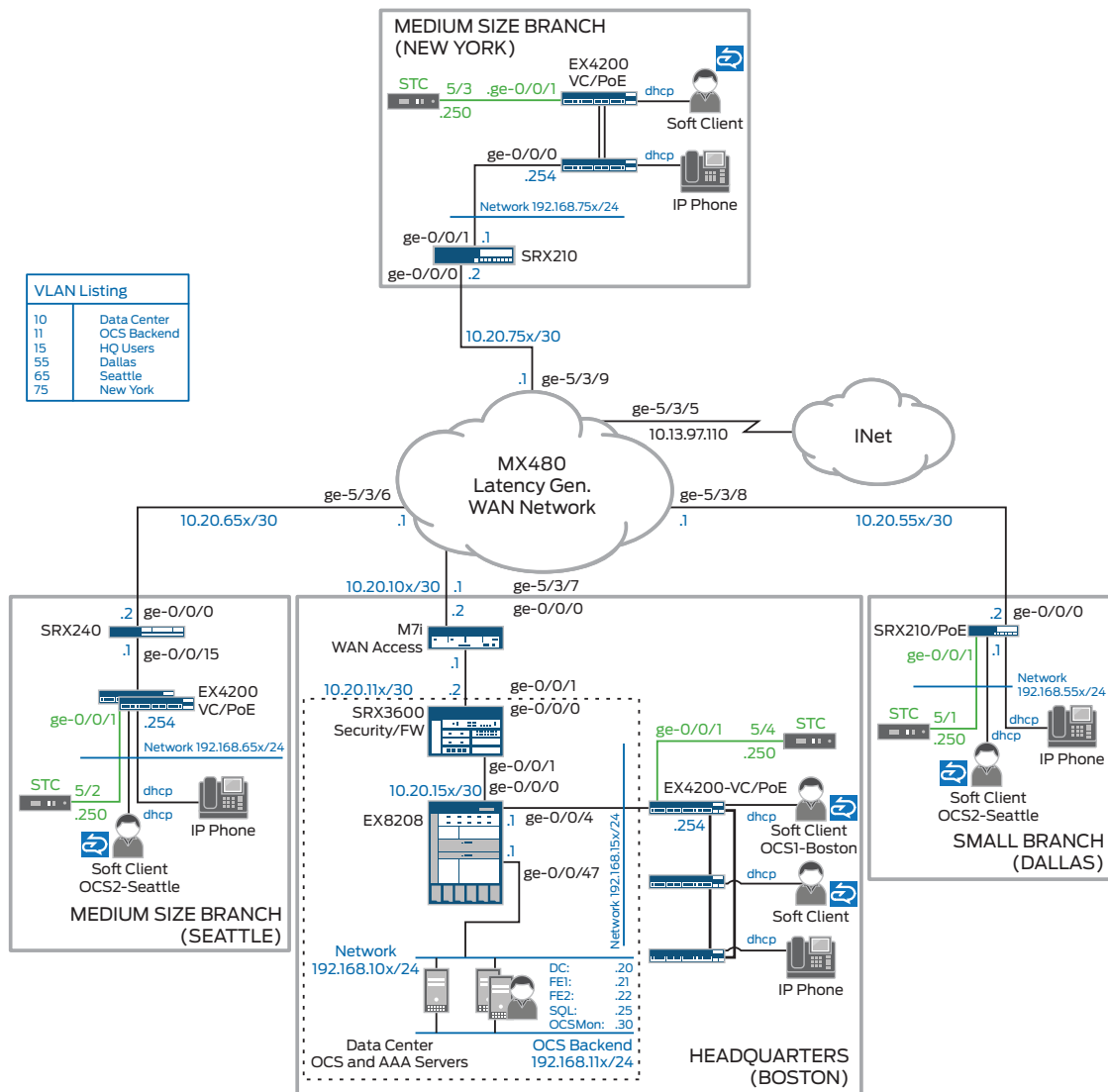


Figure 2: Juniper Networks Lync test network

Test Cases

The network was configured and connectivity between all sites was verified. Endpoints (hard phones and/or soft clients) were connected and upgraded to the latest available Lync Server 2010 beta software. Calls between sites were made to ensure connectivity, prior to the start of formal testing.

Latency and packet loss were programmed into the network, and test calls were made between sites. Live users on each end ensured that call quality was sufficient to have a normal conversation. In

addition to audio calls, video was used between the soft clients with video cameras. After the test call was completed, call metrics were captured from the QoE monitor reports.

It is important to note that in *all* test cases, IPsec encryption was turned ON. The strong results indicate high performance in the midst of enabling security across the network.

Detailed configuration for all network elements are available upon request. Please contact your Juniper Account Team for further information.

Results

Following is a table of the test cases and quality results:

CALLING FROM	CALLING TO	USING	NETWORK IMPAIRMENT	LATENCY (MSEC)	AVG. JITTER (MSEC)	AVG. MOS
HQ	All Sites	Polycom CX600	No packet loss	0	0.83	4.16
			10% packet loss	35	0.25	3.85
			15% packet loss	35	0.25	3.42
			25% packet loss	48	1.53	3.80
HQ	All Sites	Soft Client	No packet loss	0	0.86	4.24
			10% packet loss	35	0	3.81
			15% packet loss	35	0	3.66
			25% packet loss	48	1.22	4.13
New York	All Sites	Polycom CX600	No packet loss	0	1	4.17
			10% packet loss	55	0.5	3.62
			15% packet loss	55	0.5	3.62
			25% packet loss	55	1.6	3.40
New York	All Sites	Soft Client	No packet loss	0	0.5	4.24
			10% packet loss	55	0.5	3.91
			15% packet loss	55	0	3.60
			25% packet loss	55	1.5	3.80
Seattle	All Sites	Polycom CX600	No packet loss	0	0.5	4.04
			10% packet loss	80	1	3.68
			15% packet loss	80	0.5	3.44
			25% packet loss	85	2	3.20
Seattle	All Sites	Soft Client	No packet loss	0	0.5	4.27
			10% packet loss	80	0	3.84
			15% packet loss	80	0	3.49
			25% packet loss	85	1.5	3.98
Boston	Seattle	Soft Client with Video	5% packet loss	75	4.83	3.96
Seattle	New York	Soft Client with Video	5% packet loss	85	3.5	3.80

Conclusions

Juniper Networks' focus on high-performance, secure networking components gives customers the ability to design and build networks that are able to securely transport audio and video signals with minimal performance degradation under the most challenging network conditions. Throughout all test cases described in this paper, voice and video quality were found to be highly acceptable, in spite of some very severe network impairments. Even with IPsec encryption and forced packet loss and high latency, the network carried voice and video signals without causing excessive jitter or additional delay. The testing described in this paper demonstrates the superiority and value of using Juniper Networks' equipment to transport traffic generated by the Lync communication suite.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Appendix A - Equipment List

LOCATION	DEVICE	SOFTWARE VERSION
Boston/HQ	EX-4200 VC	10.2R2.11
	EX-8208	10.2R2.11
	SRX-3600	10.2R2.11
	M7i	10.2R2.11
WAN	MX-480	10.2R2.11
Seattle	EX-4200 VC	10.2R2.11
	SRX-240	10.2R2.11
New York	EX-4200 VC	10.2R2.11
	SRX-210	10.2R2.11
Dallas	SRX-210	10.2R2.11
DATA CENTER	DOMAIN CONTROLLER	WINDOWS 2008 R2 SERVER
	SQL Server	Windows 2008 R2 Server SQL Server 2008 R2 Microsoft Lync Server 2010 2010Beta Software, Build 7400
	FE One	Windows 2008 R2 Server Microsoft Lync Server 2010 2010Beta Software, Build 7400
	FE Two	Windows 2008 R2 Server Microsoft Lync Server 2010 2010Beta Software, Build 7400
	Monitor Server	Windows 2008 R2 Server Microsoft Lync Server 2010 2010Beta Software, Build 7400

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.