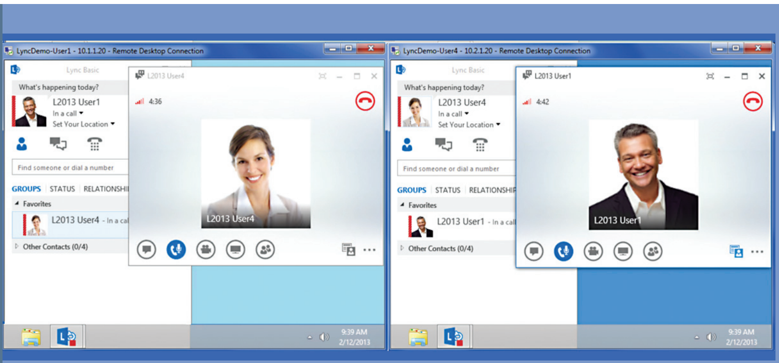
NetSocket

White Paper

A Real-world Demonstration of NetSocket Cloud Experience Manager for Microsoft Lync



Introduction

Microsoft Lync connects people everywhere as part of their everyday productivity experience. When issues in the underlying IP network affect a user's Lync experience, unified communications (UC) managers need to solve those problems immediately. The solution to these issues lies in the tight integration with Lync services that captures all the data responsible for identifying the root cause behind Lync-specific UC problems. Unfortunately, many service assurance solutions on the market today fall short and do not capture all the information necessary or automatically correlate related issues back to these root causes. In addition, the number of costly third-party probes required at each endpoint in a Lync UC routed network can exceed what many companies can afford. Only NetSocket's Cloud Experience Manager (CEM) provides comprehensive insight into Lync UC network issues for fast problem resolution without expensive probes, lowers the total cost of ownership (TCO) and increases the quality of Lync user experience.

This paper will discuss how CEM's unique integration with the Microsoft Lync Network Diagnostics API can provide the insight required to anticipate, isolate and remediate voice, video and data issues in Lync and hybrid UC environments. It also describes a demonstration of how CEM resolves Lync issues in a real-world scenario.

The Business Problem

According to Microsoft Lync customer experiences, the majority of issues related to Lync UC problems occur within the client routed network. Most commonly, there is configuration drift — when client locations change or applications expand, QoS settings on the routers become obsolete. Traditional UC network service assurance monitoring solutions use an element monitoring or probe approach to identify the root cause of service degradations. This approach does not accurately provide insight into what the user experiences during that event, nor does it automatically correlate the disparate data into actionable insight for root cause and trending analysis.

Why Probe-based Solutions Don't Work

Even when using traditional probe-based monitoring methods, most IT operations managers are plagued with the following issues when trying to resolve Lync UC service problems:

- There is no visibility of the routed network
- Most solutions require expensive probes in multiple locations
- Lync media and signaling data is encrypted and cannot be seen
- Issue triage and correlation are done manually
- Lack of proper "bracketing" of the source of the problem leads to constant misleading finger-pointing

- Post-event averages of call quality metrics don't present an accurate, real-time picture of the call
- Poor end-user experience cannot be resolved quickly, or in some cases, at all

Without an effective means of quickly identifying and correlating network issues to the session and content events of a specific call, fault isolation and remediation are unpredictable. This unpredictability translates to high Lync user service-case counts, lengthy time per case and root cause misdiagnosis. The subsequent avalanche of data from multiple sources requires highly skilled technicians to manually filter and correlate "haystacks" of forensic data from disparate components. Fault isolation also depends on the hope that the same root cause event will happen while the after-the-fact diagnostics traces are enabled. After days or weeks of hunting, the root cause "needle" is rarely found.

The NetSocket Solution

NetSocket's CEM UC service assurance solution for Microsoft Lync 2013 and 2010 is more than just monitoring; it provides complete IP network information correlation for Lync environments. CEM automatically correlates, in real time, all session, content and IP topology data to each user call, enabling managers to quickly anticipate, isolate and remediate the root causes of network-based UC problems. CEM delivers immediate insight into underlying IP networks without costly probes at each endpoint and without burdening the performance of all Lync elements with post-event diagnostic traces.

Empowering Microsoft Lync users with the enhanced optimizations that CEM provides begins with NetSocket incorporating support for the new and powerful Microsoft Lync Network Diagnostics (LND) API into its patented IP Correlation Engine® (ICE). This API enables CEM to provide real-time, hop-by-hop IP topology path identification and recording of all media streams for all Lync voice and video calls down to the Lync user endpoint. The identification of specific route paths in real time for each call allows support personnel to correlate a user's complaint to the likely root cause of service degradation within a few clicks, significantly reducing the time to resolve issues and the TCO of Lync operations and support.

Integration with Microsoft's LND API gives NetSocket's CEM UC service assurance solution a unique view into content, session and IP topology-level data throughout a Lync network.

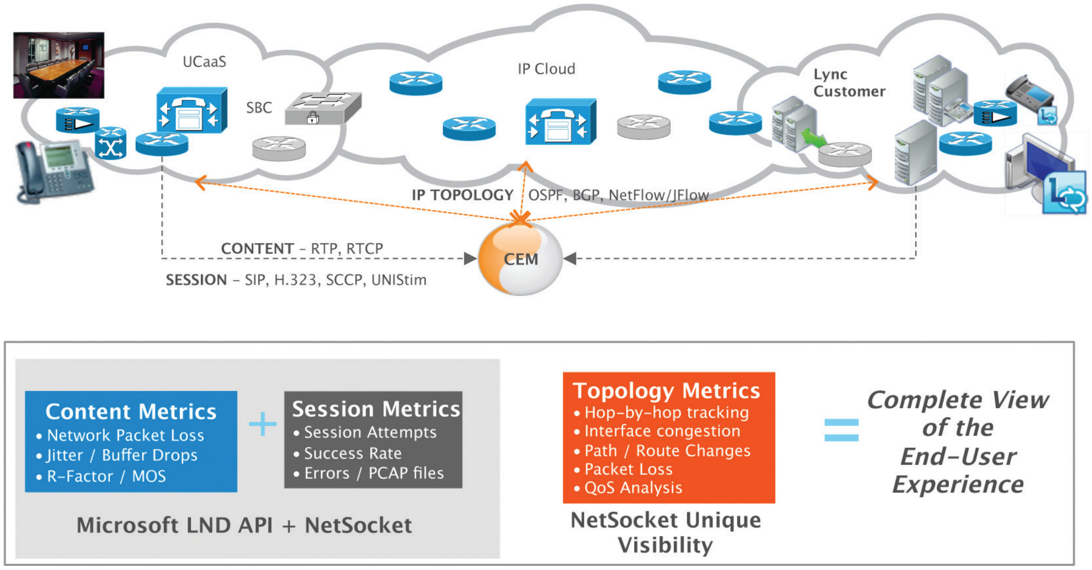
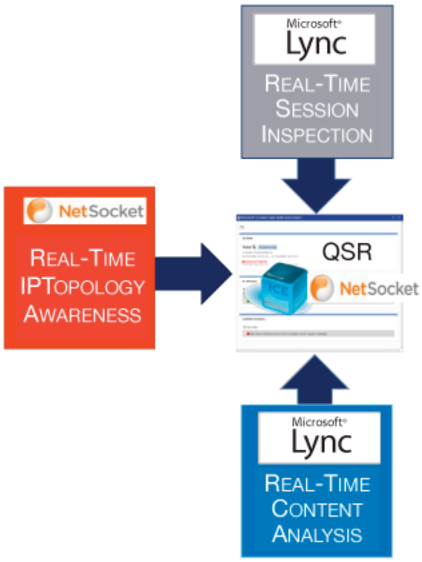


Figure 1. CEM for Lync correlates content, session and topology metrics in real time for a complete view of the end-user experience

CEM reports on each Lync endpoint without probes to provide network administrators with a unique comprehensive visibility into the Lync environment, including:

- Viewing Lync's encrypted signaling and media traffic without compromising security
- Capturing session-level information throughout the Lync network
- Tracking calls throughout the network in real time from start to finish
- Delivering real-time analytics on the signaling and media throughout the life of each call to calculate the actual quality of the call, something no other vendor can do with post-call average-quality metrics
- Correlating the quality of the call with what is happening throughout the route taken by the call
- Isolating where the problem is actually occurring (data center, branch office, cloud, etc.) by peering with nearest router and correlating the information across the network; probes need to poll each endpoint
- Bracketing issues throughout the network more cost-effectively, providing a minimal footprint to deliver the most in-depth visibility
- Tying the problem back to the root cause through real-time content, session and topology correlation

CEM's tight integration with Microsoft's LND API enables CEM to facilitate Microsoft Lync event root cause analysis, identification and resolution in just a few clicks, minimizing the manual efforts of IT operations and support personnel. CEM produces a quality of session record (QSR) for each call, which is a real-time correlation of the Lync session, content and IP topology information. The QSR reports can be generated via the CEM graphic user interface (GUI) and identify the root cause and allow you to take appropriate action to remediate the service-affecting issue.

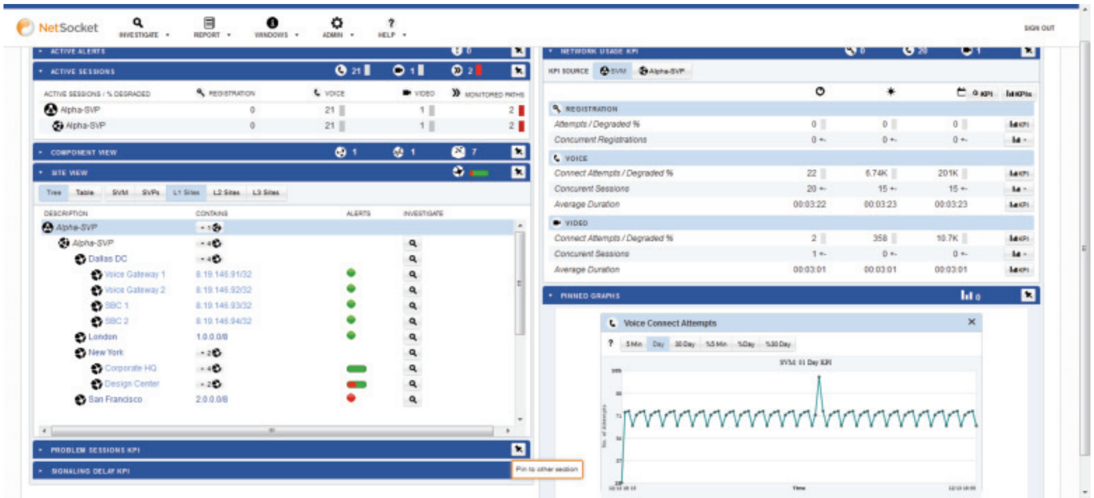

Microsoft Lync
REAL-TIME SESSION INSPECTION
NetSocket
REAL-TIME IPTOPOLOGY AWARENESS
QSR
NetSocket
Microsoft Lync
REAL-TIME CONTENT ANALYSIS

- **Multi-dimensional, auto-correlated record**
- **Insight into customer experience**
- **Isolates root cause of alerts and problems**
- **Dramatically reduces MTTI/MTTR**

Figure 2. CEM's QSR reports identify the root causes behind Lync UC issues

Reduced Complexity in Managing the Lync and Hybrid UC Network

CEM provides a comprehensive, well-organized, single pane of glass web-based GUI and workflow structure that allows a much greater percentage of UC service cases to be quickly managed at help desks without requiring expert resources. Ample forensic data is supplied if escalation to higher skill-set agents is required. CEM also supports manager-of-manager applications such as Microsoft System Center — delivering KPI threshold-crossing alerts and other service-related data to unified management solutions.



ACTIVE SESSIONS / % DEGRADED	REGISTRATION	VOICE	VIDEO	MONITORED PATHS
Alpha-SVP	0	21	1	2
Alpha-SVP	0	21	1	2

DESCRIPTION	CONTAINS	ALERTS	INVESTIGATE
Alpha-SVP	1		
Alpha-SVP	4		
Dallas DC	4		
Voice Gateway 1	8.19.146.91/32	●	
Voice Gateway 2	8.19.146.92/32	●	
SBC 1	8.19.146.93/32	●	
SBC 2	8.19.146.94/32	●	
London	1.0.0.0/8	●	
New York	2		
Corporate HQ	4		
Design Center	2		
San Francisco	2.0.0.0/8	●	

REGISTRATION			
Attempts / Degraded %	0	0	0
Concurrent Registrations	0	0	0
VOICE			
Connect Attempts / Degraded %	22	6.74K	201K
Concurrent Sessions	20	15	15
Average Duration	00:03:22	00:03:23	00:03:23
VIDEO			
Connect Attempts / Degraded %	2	358	10.7K
Concurrent Sessions	1	0	0
Average Duration	00:03:01	00:03:01	00:03:01

Figure 3. CEM GUI and Performance Management Dashboard

Accurate Forensics and Correlation

CEM's forensic data is derived from all calls – including those affected by service disruptions. After-the-fact, hunt-and-peck trace enabling and analysis are not required, nor are costly probes at every endpoint. CEM's tight integration with Microsoft Lync Network Diagnostics API provides real-time, hop-by-hop path identification across Microsoft Lync as well as heterogeneous UC and network environments, eliminating other network elements from the hunt for the root cause.

Quicker Root Cause Analysis and Time to Resolution

CEM's deep visibility and correlation of UC session, content and IP topology layers yield up to a 70% reduction in mean time to repair (MTTR) UC service degradations and reduces false diagnoses. CEM QSRs help IT managers understand how severely the voice call was impacted at a particular hop and provide the correlated detail behind the congestion, facilitating the identification of the root cause and reducing the problem resolution time. CEM provides complete end-to-end visibility and root cause identification from the data center out to the farthest edges of the network. CEM enables IT managers to perform "site grouping" to segregate calls from remote sites and accurately isolate faults for fast remediation in highly distributed enterprise networks.

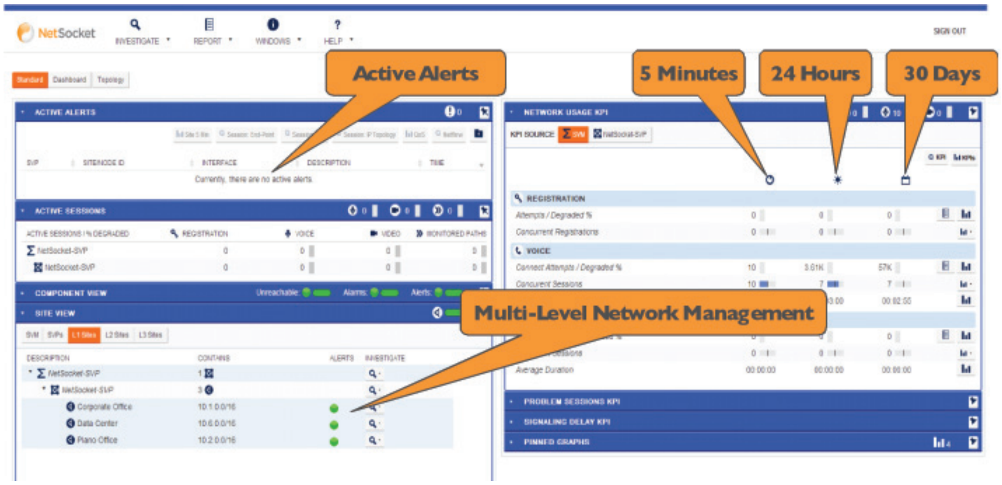


Figure 4. Dashboard overview

Trend Analysis and Reporting

CEM historical reports and key performance indicators (KPIs) identify mid- and long-term trends for predicting capacity and performance actions, enabling administrators to anticipate caseload peaks and take action through proactive alerting. CEM provides IT managers over 50 different KPIs — half of which can be set for specific thresholds (e.g., MOS Factor, Packet Loss, Jitter, One-Way Audio, Signal Noise Ratio and Call Attempt Counter). CEM also features over 35 standard reports along with the ability to customize reports and graphs that quantify the overall health of the network. Executive summaries of the reports can then be customized to highlight key metrics and attributes. The enhanced visibility afforded by CEM provides both a reduction in TCO and a greater predictability for managing Microsoft Lync operations and meeting service level agreements.

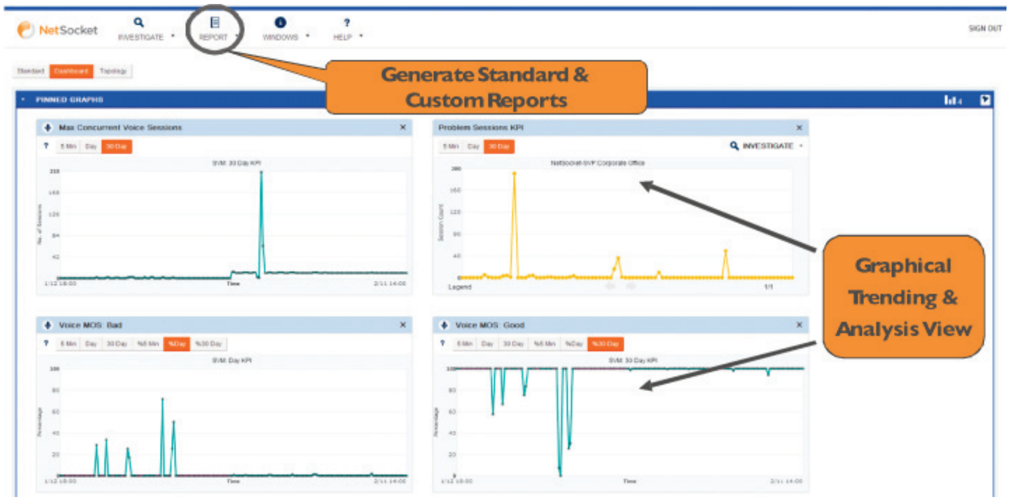


Figure 5. Reporting and graphical trending analysis

The NetSocket CEM and Microsoft Lync Demonstration

The following demonstration illustrates some of the ways that NetSocket's CEM can be used to monitor and troubleshoot a Microsoft Lync deployment. The topology map in Figure 6 shows the network that is being monitored by NetSocket's CEM. In order for the corporate office to call the branch office, the traffic must pass through the five routers in three locations: the corporate data center (C1, C2, CE1), an MPLS network (CE2) and a router at the remote branch site (R1).

This comprehensive insight into the network traffic is provided by CEM without using probes at each of the endpoints. NetSocket's CEM SVP monitors the routers to provide a hop-by-hop view of the complete network path for each call and to detect network events in real time. The Microsoft Lync server sends the session quality information for the Lync endpoints to the CEM SVP when the call terminates. CEM also monitors session quality as it passes through the network. In this demonstration, we are analyzing traffic as it passes through the two routers (CE1 and R1) on the edges of the corporate network and tracking a network event along that path.

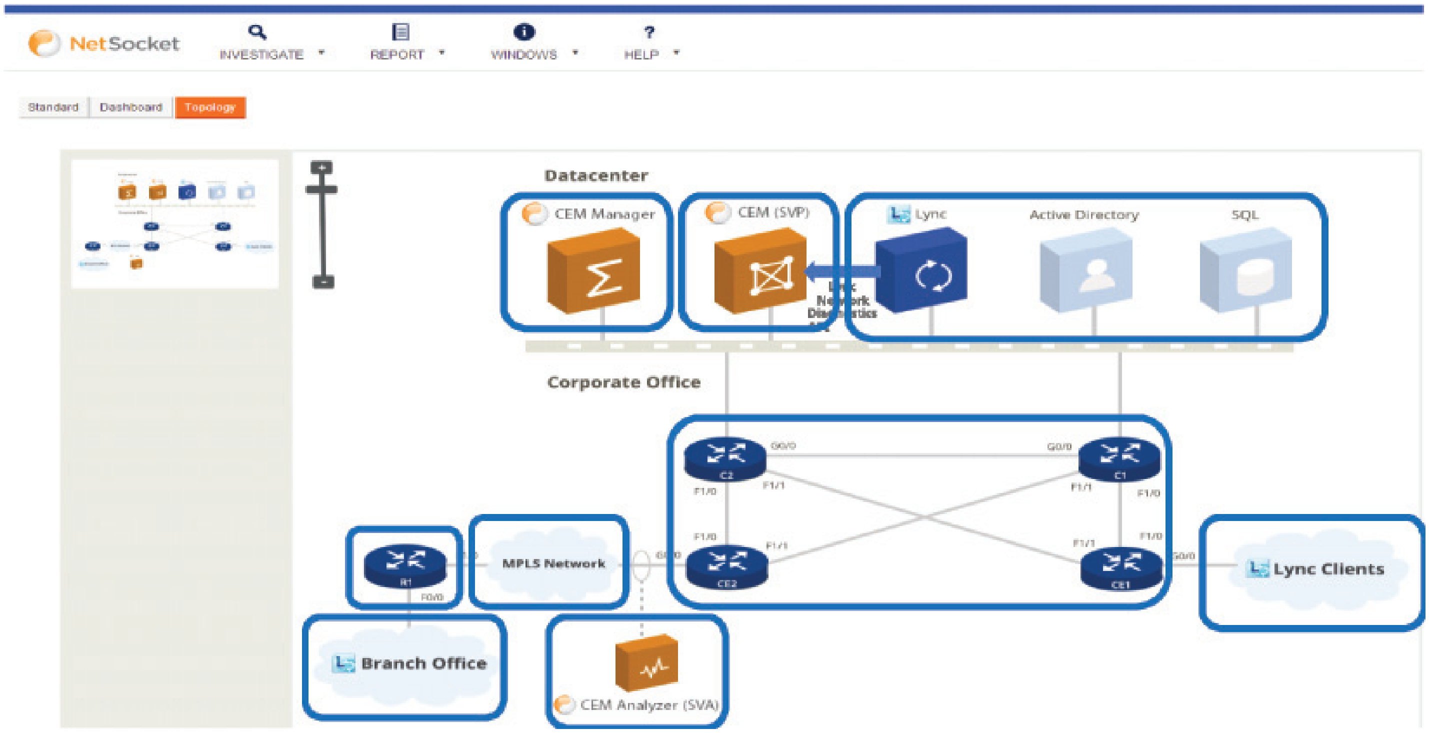


Figure 6. Topology map

A female user (User 1) in the corporate office calls a male user (User 4) in the remote branch site. The audio of a phone call is breaking up and the female user cannot be understood.

Figure 7. Lync user dashboard

The voice call was impacted by the network link going down between CE1 and C2 and there was a moment of silence while the traffic was rerouted from CE1 to C1.

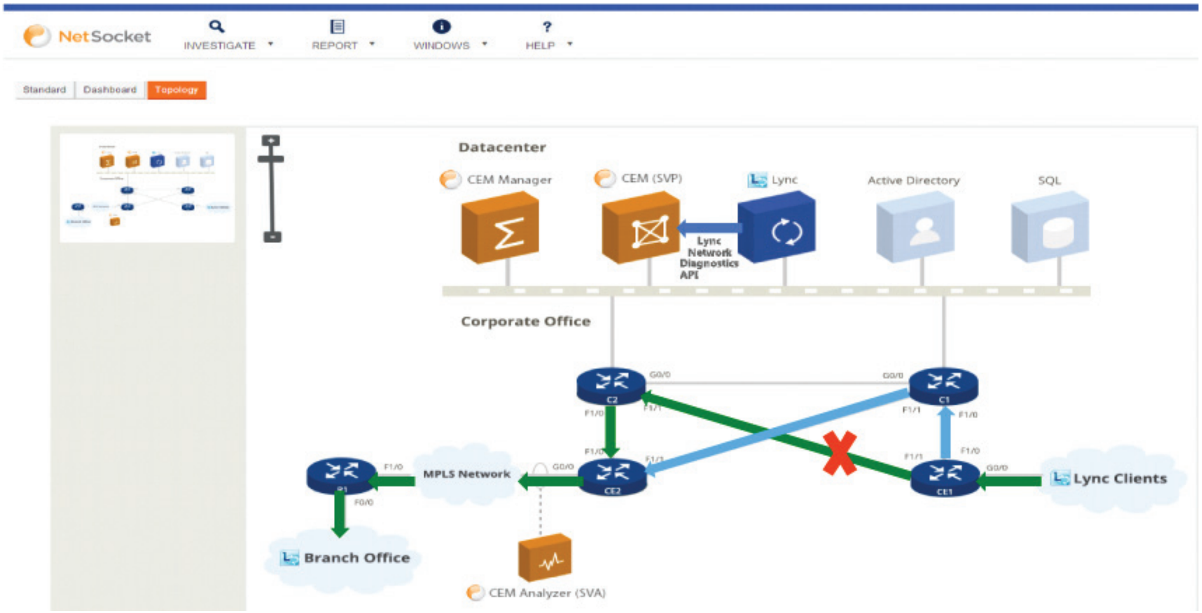
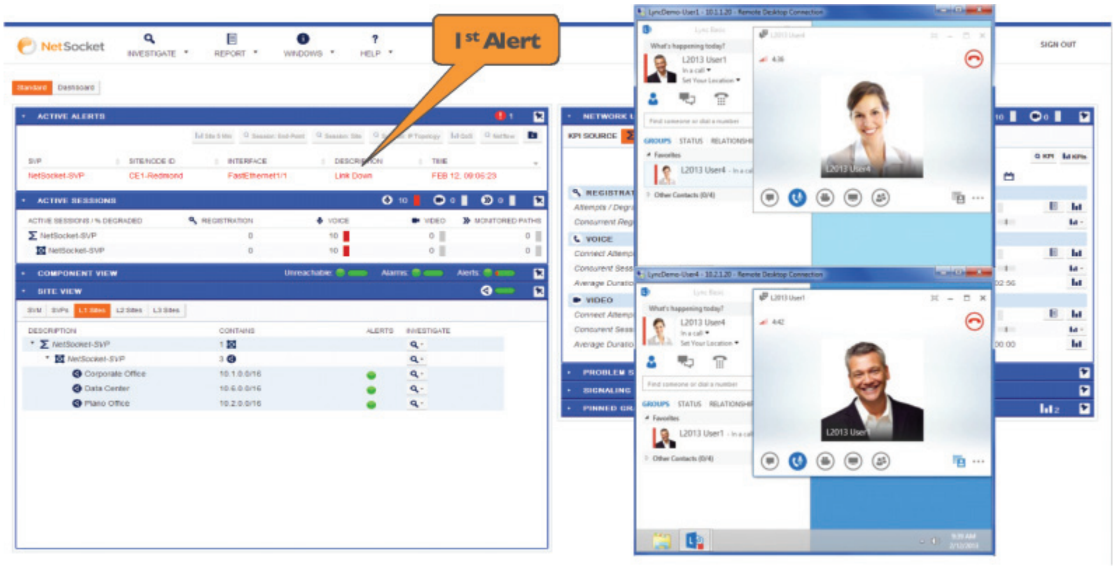


Figure 8. Topology map with the network rerouting

As the network rerouting occurs, a “priority queue alert” appears on the CEM dashboard.



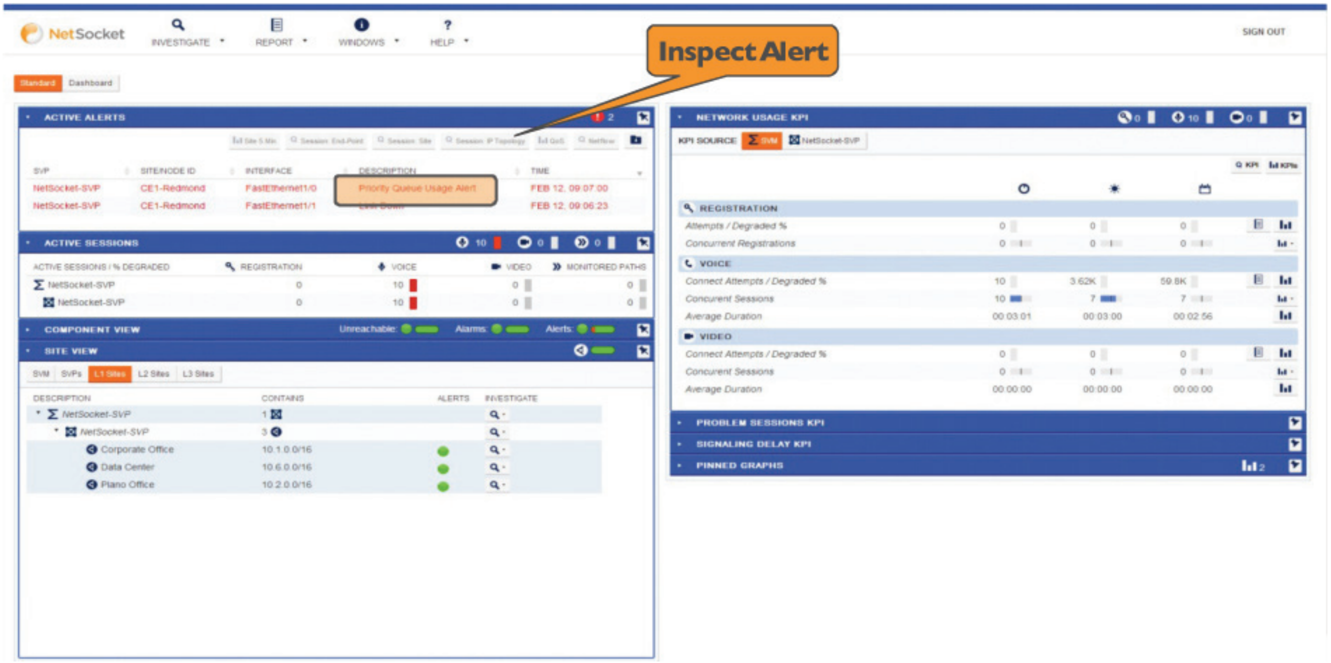
SVP	SITE/NODE ID	INTERFACE	DESCRIPTION	TIME
NetSocket-SVP	CE1-Redmond	FastEthernet1/1	Link Down	FEB 12, 09:06:23

ACTIVE SESSIONS / % DEGRADED	REGISTRATION	VOICE	VIDEO	MONITORED PATHS
NetSocket-SVP	0	10	0	0
NetSocket-SVP	0	10	0	0

DESCRIPTION	CONTAINS	ALERTS	INVESTIGATE
NetSocket-SVP	1		
NetSocket-SVP	3		
Corporate Office	10.1.0.0/16	●	
Data Center	10.6.0.0/16	●	
Plano Office	10.2.0.0/16	●	

Figure 9. Priority queue alert of the network link going down

By clicking on the alert and performing a session query, you’ll find information on sessions that were going through the link while it was congested.



SVP	SITE/NODE ID	INTERFACE	DESCRIPTION	TIME
NetSocket-SVP	CE1-Redmond	FastEthernet1/0	Priority Queue Usage Alert	FEB 12, 09:07:00
NetSocket-SVP	CE1-Redmond	FastEthernet1/1	Link Down	FEB 12, 09:06:23

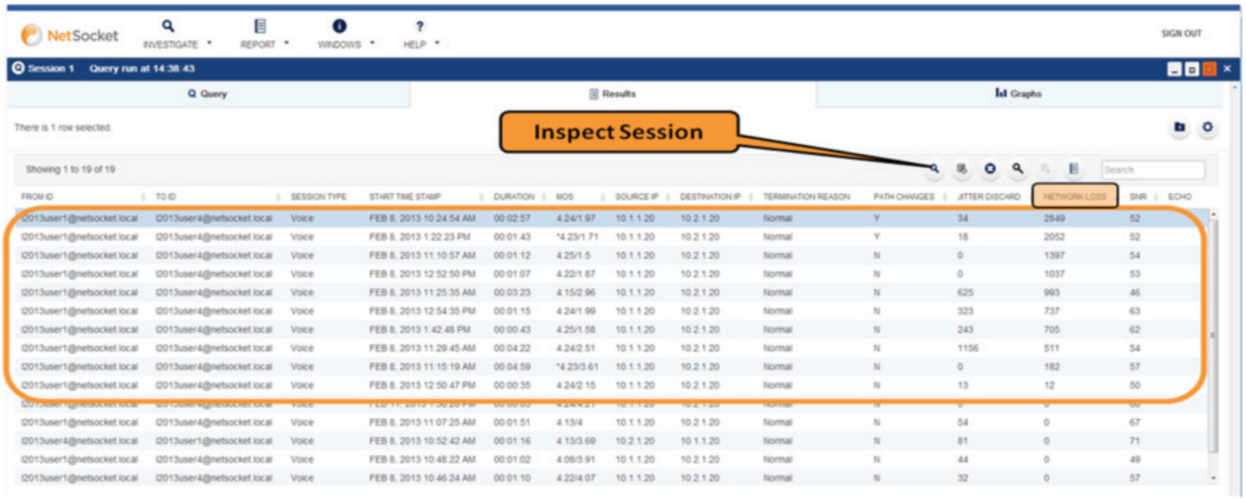
ACTIVE SESSIONS / % DEGRADED	REGISTRATION	VOICE	VIDEO	MONITORED PATHS
NetSocket-SVP	0	10	0	0
NetSocket-SVP	0	10	0	0

DESCRIPTION	CONTAINS	ALERTS	INVESTIGATE
NetSocket-SVP	1		
NetSocket-SVP	3		
Corporate Office	10.1.0.0/16	●	
Data Center	10.6.0.0/16	●	
Plano Office	10.2.0.0/16	●	

REGISTRATION			
Attempts / Degraded %	0	0	0
Concurrent Registrations	0	0	0
VOICE			
Connect Attempts / Degraded %	10	3.62K	59.8K
Concurent Sessions	10	7	7
Average Duration	00:03:01	00:03:00	00:02:56
VIDEO			
Connect Attempts / Degraded %	0	0	0
Concurent Sessions	0	0	0
Average Duration	00:00:00	00:00:00	00:00:00

Figure 10. Alert details show network congestion on the link that went down

If you sort on the network loss column, you'll find that the session with the most packet loss was between User 1 and User 4.



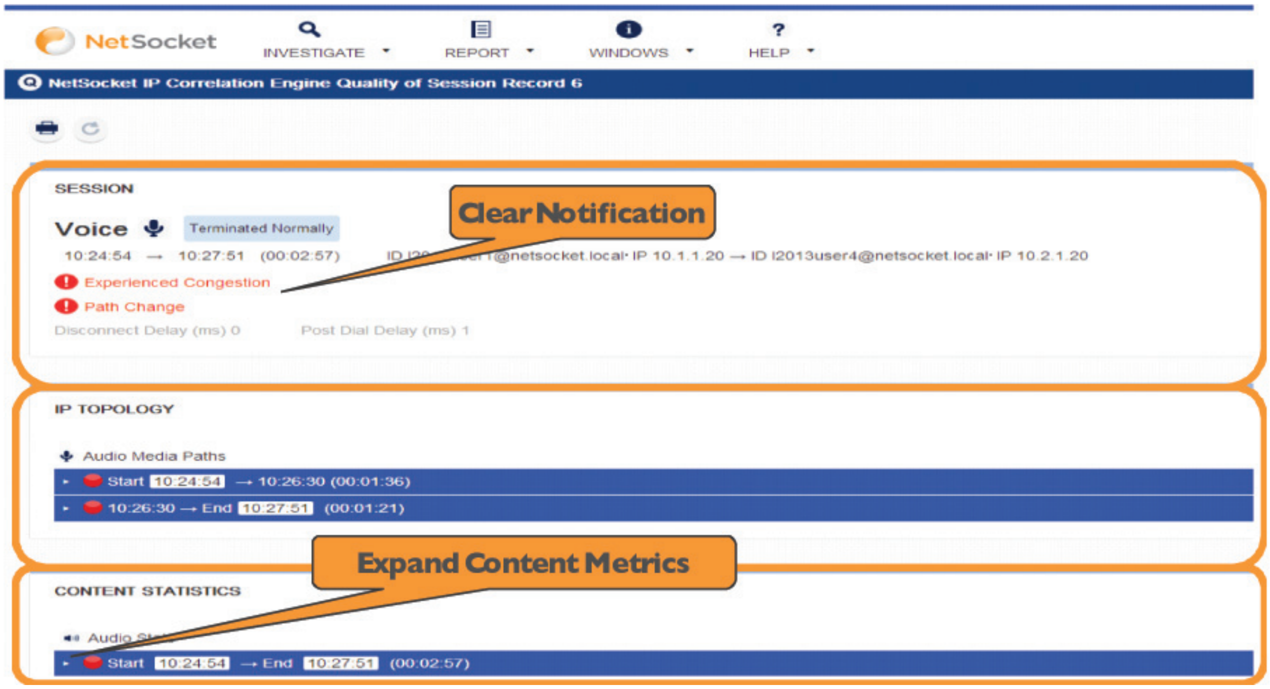
There is 1 row selected

Showing 1 to 19 of 19

FROM ID	TO ID	SESSION TYPE	START TIME STAMP	DURATION	MOS	SOURCE IP	DESTINATION IP	TERMINATION REASON	PATH CHANGES	JITTER DISCARD	NETWORK LOSS	SNR	ECHO
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 10:24:54 AM	00:02:57	4.24/1.97	10.1.1.20	10.2.1.20	Normal	Y	34	2849	52	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 1:22:23 PM	00:01:43	*4.23/1.71	10.1.1.20	10.2.1.20	Normal	Y	18	2052	52	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 11:10:57 AM	00:01:12	4.25/1.5	10.1.1.20	10.2.1.20	Normal	N	0	1397	54	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 12:52:50 PM	00:01:07	4.22/1.87	10.1.1.20	10.2.1.20	Normal	N	0	1037	53	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 11:25:35 AM	00:03:23	4.15/2.96	10.1.1.20	10.2.1.20	Normal	N	625	993	46	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 12:54:35 PM	00:01:15	4.24/1.99	10.1.1.20	10.2.1.20	Normal	N	323	737	63	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 1:42:48 PM	00:00:43	4.25/1.58	10.1.1.20	10.2.1.20	Normal	N	243	705	62	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 11:29:45 AM	00:04:22	4.24/2.51	10.1.1.20	10.2.1.20	Normal	N	1156	511	54	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 11:15:19 AM	00:04:59	*4.23/3.61	10.1.1.20	10.2.1.20	Normal	N	0	182	57	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 12:50:47 PM	00:00:35	4.24/2.15	10.1.1.20	10.2.1.20	Normal	N	13	12	50	
[illegible]	[illegible]	Voice	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Normal	N	0	0	[illegible]	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 11:07:25 AM	00:01:51	4.13/4	10.1.1.20	10.2.1.20	Normal	N	54	0	67	
I2013user4@netsocket.local	I2013user1@netsocket.local	Voice	FEB 8, 2013 10:52:42 AM	00:01:16	4.13/3.69	10.2.1.20	10.1.1.20	Normal	N	81	0	71	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 10:48:22 AM	00:01:02	4.08/3.91	10.1.1.20	10.2.1.20	Normal	N	44	0	49	
I2013user1@netsocket.local	I2013user4@netsocket.local	Voice	FEB 8, 2013 10:46:24 AM	00:01:10	4.22/4.07	10.1.1.20	10.2.1.20	Normal	N	32	0	57	

Figure 11. QSR details the quality of the call

To see detailed call information, open the quality of session record, or QSR, for this session. The top section of the QSR contains basic session information such as the time the call was established and terminated. It also flags that the audio stream experienced a path change and went through a congested interface.



NetSocket IP Correlation Engine Quality of Session Record 6

SESSION

Voice Terminated Normally

10:24:54 → 10:27:51 (00:02:57) ID I20[illegible]r1@netsocket.local· IP 10.1.1.20 → ID I2013user4@netsocket.local· IP 10.2.1.20

Experienced Congestion

Path Change

Disconnect Delay (ms) 0 Post Dial Delay (ms) 1

IP TOPOLOGY

Audio Media Paths

- Start 10:24:54 → 10:26:30 (00:01:36)
- 10:26:30 → End 10:27:51 (00:01:21)

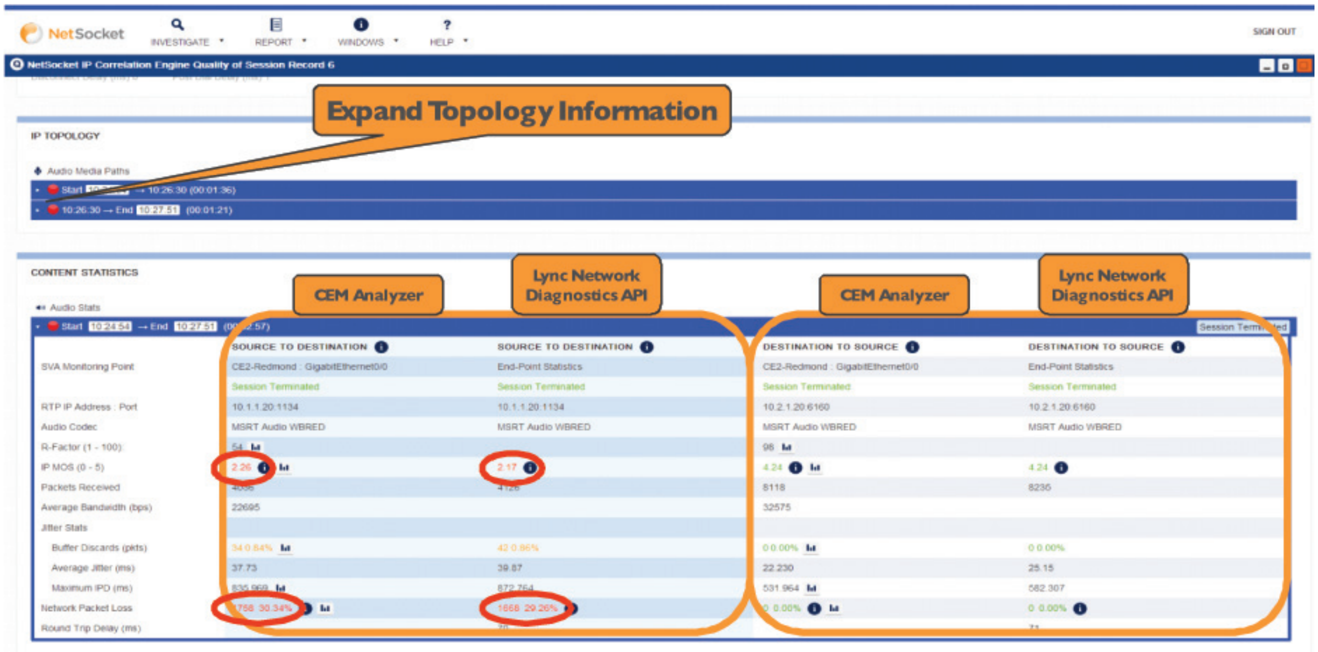
CONTENT STATISTICS

Audio St[illegible]

- Start 10:24:54 → End 10:27:51 (00:02:57)

Figure 12. QSR shows congestion and network path change notification

The content statistics section of the QSR reports session quality information for both the source to destination and destination to source real-time transport protocol (RTP) streams. Each section contains three columns; the first two from the NetSocket CEM monitoring points and the third from endpoint information provided by Microsoft Lync. The first CEM monitoring point saw a call with no issues; however, the second CEM monitoring point and the Lync endpoint statistics both report a significantly reduced mean opinion score (MOS) and significant network packet loss — approximately 30%. It is CEM's full support of the Microsoft Lync Network Diagnostics API that provides this detailed level of information on the Lync endpoints.


NetSocket
INVESTIGATE
REPORT
WINDOWS
HELP
SIGN OUT
Expand Topology Information
CEM Analyzer
Lync Network Diagnostics API
CEM Analyzer
Lync Network Diagnostics API

NetSocket IP Correlation Engine Quality of Session Record 6

IP TOPOLOGY

Audio Media Paths

- Start [illegible] → 10:26:30 (00:01:36)
- 10:26:30 → End 10:27:51 (00:01:21)

CONTENT STATISTICS

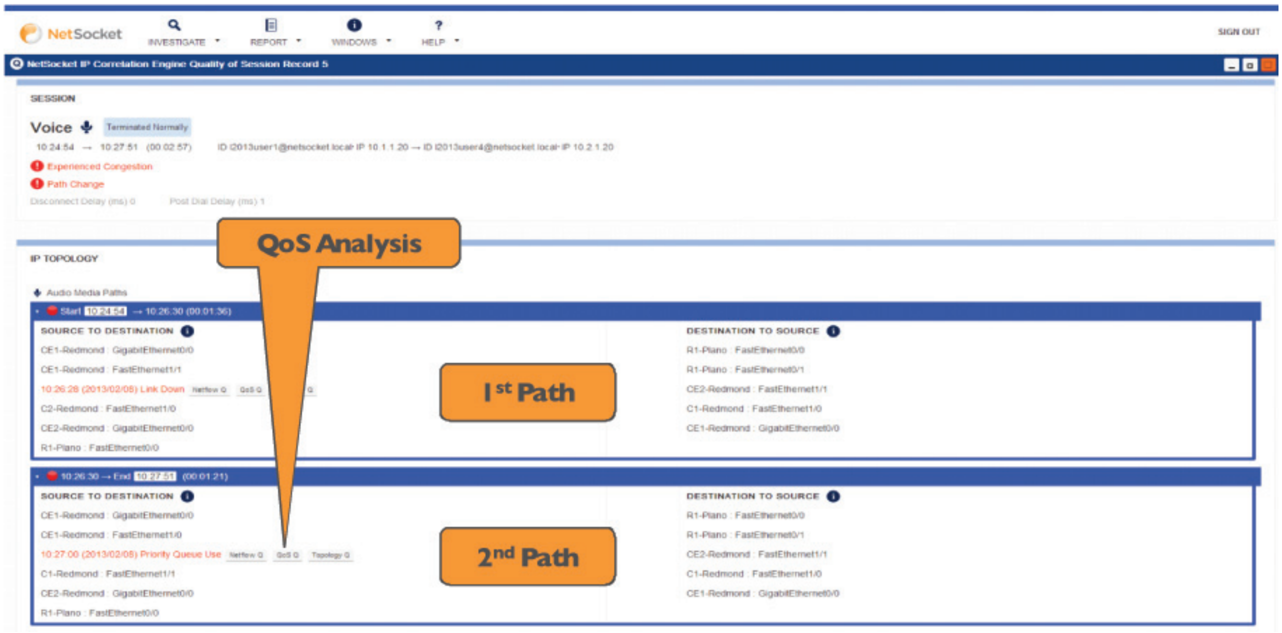
Audio Stats

- Start 10:24:54 → End 10:27:51 (00:02:57) Session Terminated

	SOURCE TO DESTINATION	SOURCE TO DESTINATION	DESTINATION TO SOURCE	DESTINATION TO SOURCE
SVA Monitoring Point	CE2-Redmond : GigabitEthernet0/0	End-Point Statistics	CE2-Redmond : GigabitEthernet0/0	End-Point Statistics
	Session Terminated	Session Terminated	Session Terminated	Session Terminated
RTP IP Address : Port	10.1.1.20:1134	10.1.1.20:1134	10.2.1.20:6160	10.2.1.20:6160
Audio Codec	MSRT Audio WBRED	MSRT Audio WBRED	MSRT Audio WBRED	MSRT Audio WBRED
R-Factor (1 - 100):	54		98	
IP MOS (0 - 5)	2.26	2.17	4.24	4.24
Packets Received	4036	4126	8118	8236
Average Bandwidth (bps)	22695		32575	
Jitter Stats				
Buffer Discards (pkts)	34 0.84%	42 0.86%	0 0.00%	0 0.00%
Average Jitter (ms)	37.73	39.87	22.230	25.15
Maximum IPD (ms)	835.969	872.764	531.964	582.307
Network Packet Loss	1758 30.34%	1668 29.26%	0 0.00%	0 0.00%
Round Trip Delay (ms)		70		71

Figure 13. QSR shows low MOS score and high network packet loss

The IP topology section of the QSR shows the network path the RTP stream took through the network. In this case, there were two paths because of the network reroute. The upper section shows the hops prior to the link going down, and the lower section shows the hops taken after the link went down. You can see that this interface went down, causing a network reroute. The reroute caused additional network congestion on the interface highlighted here, resulting in a priority queue alert.



NetSocket IP Correlation Engine Quality of Session Record 5

SESSION

Voice — Terminated Normally

10:24:54 → 10:27:51 (00:02:57) ID l2013user1@netsocket.local IP 10.1.1.20 → ID l2013user4@netsocket.local IP 10.2.1.20

Experienced Congestion

Path Change

Disconnect Delay (ms) 0 Post Dial Delay (ms) 1

IP TOPOLOGY

Audio Media Paths

Start 10:24:54 → 10:26:30 (00:01:36)

SOURCE TO DESTINATION	DESTINATION TO SOURCE
CE1-Redmond : GigabitEthernet0/0	R1-Plano : FastEthernet0/0
CE1-Redmond : FastEthernet1/1	R1-Plano : FastEthernet0/1
10:26:28 (2013/02/08) Link Down Netflow Q QoS Q Q	CE2-Redmond : FastEthernet1/1
C2-Redmond : FastEthernet1/0	C1-Redmond : FastEthernet1/0
CE2-Redmond : GigabitEthernet0/0	CE1-Redmond : GigabitEthernet0/0
R1-Plano : FastEthernet0/0	

10:26:30 → End 10:27:51 (00:01:21)

SOURCE TO DESTINATION	DESTINATION TO SOURCE
CE1-Redmond : GigabitEthernet0/0	R1-Plano : FastEthernet0/0
CE1-Redmond : FastEthernet1/0	R1-Plano : FastEthernet0/1
10:27:00 (2013/02/08) Priority Queue Use Netflow Q QoS Q Topology Q	CE2-Redmond : FastEthernet1/1
C1-Redmond : FastEthernet1/1	C1-Redmond : FastEthernet1/0
CE2-Redmond : GigabitEthernet0/0	CE1-Redmond : GigabitEthernet0/0
R1-Plano : FastEthernet0/0	

Figure 14. IP topology section of QSR shows the network paths before and after the link was rerouted

This information can also be displayed on the topology map. Here, the path the audio stream took through the network is displayed. The red line shows the interface that went down, while the red circle shows the outbound interface that was congested.

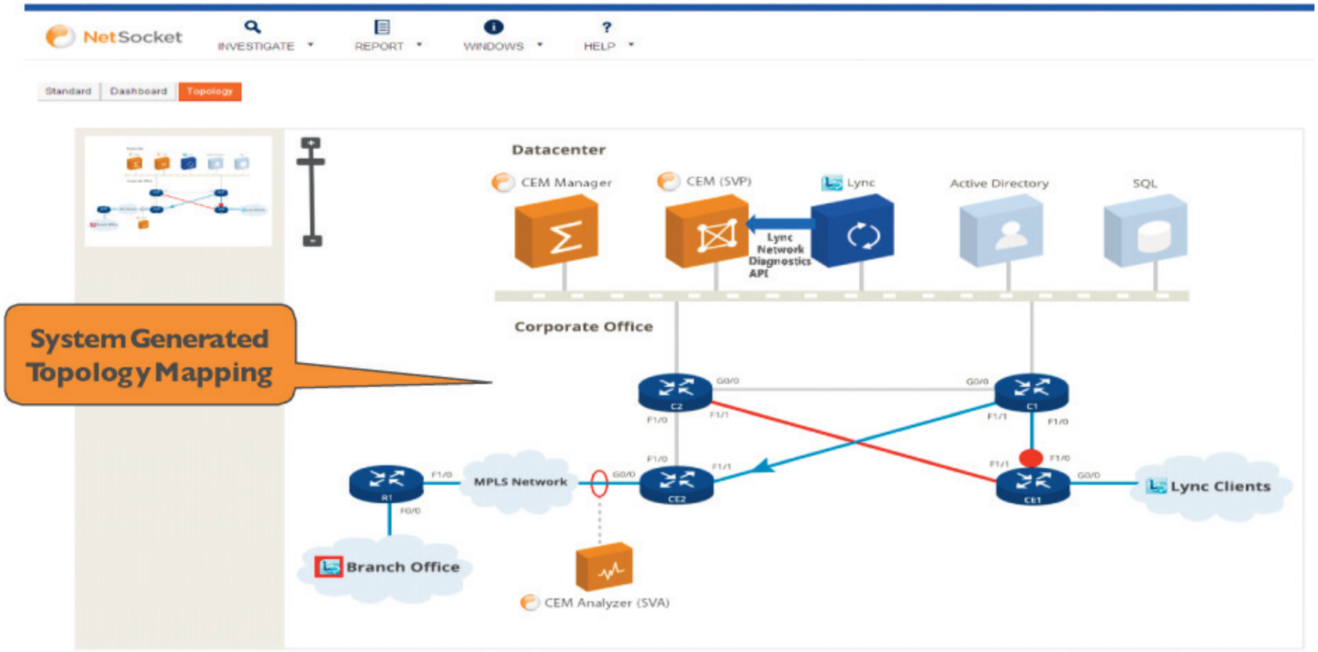
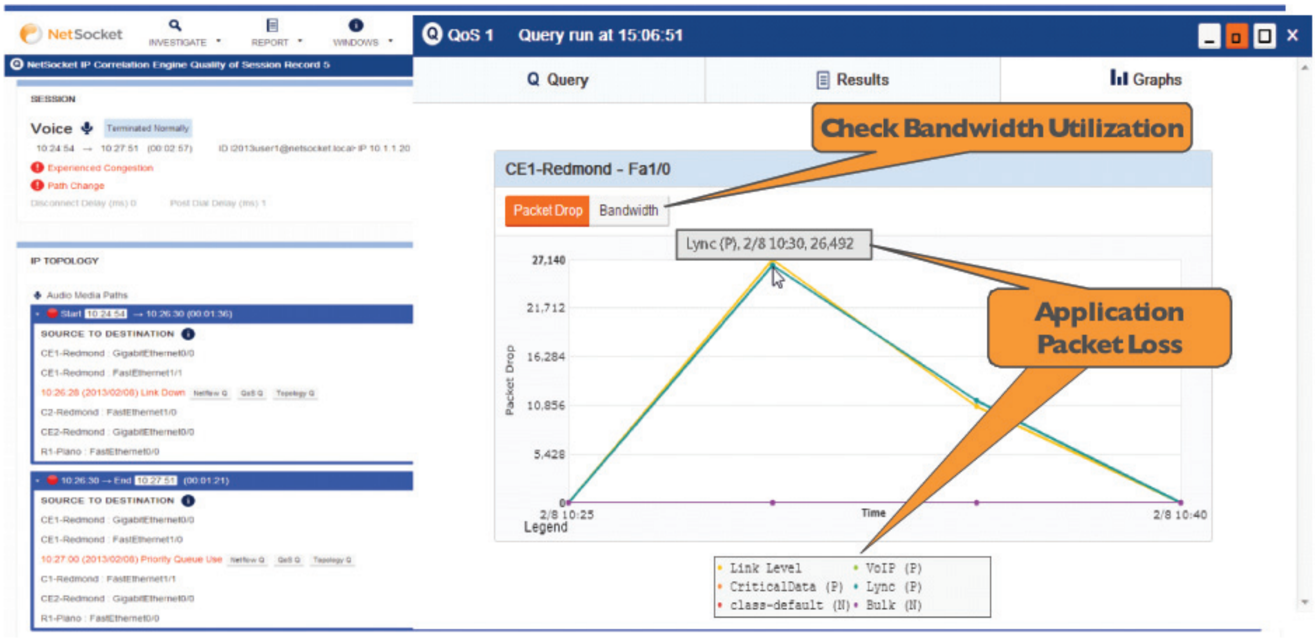


Figure 15. Topology map shows the interface that went down and the congested interface

You can see the impact of this by clicking on the QSR query button. It returns two graphs; the first is packet drop. You can see from the legend that there is Lync-level information as well as information for five classes. While the call was active, there was significant packet loss out of the Lync class.



NetSocket IP Correlation Engine Quality of Session Record 5

SESSION

Voice Terminated Normally

10:24:54 → 10:27:51 (00:02:57) ID i2013user1@netsocket.local· IP 10.1.1.20

Experienced Congestion

Path Change

Disconnect Delay (ms) 0 Post Dial Delay (ms) 1

IP TOPOLOGY

Audio Media Paths

Start 10:24:54 → 10:26:30 (00:01:36)

SOURCE TO DESTINATION

CE1-Redmond : GigabitEthernet0/0
CE1-Redmond : FastEthernet1/1
10:26:28 (2013/02/08) Link Down Netflow Q QoS Q Topology Q
C2-Redmond : FastEthernet1/0
CE2-Redmond : GigabitEthernet0/0
R1-Plano : FastEthernet0/0

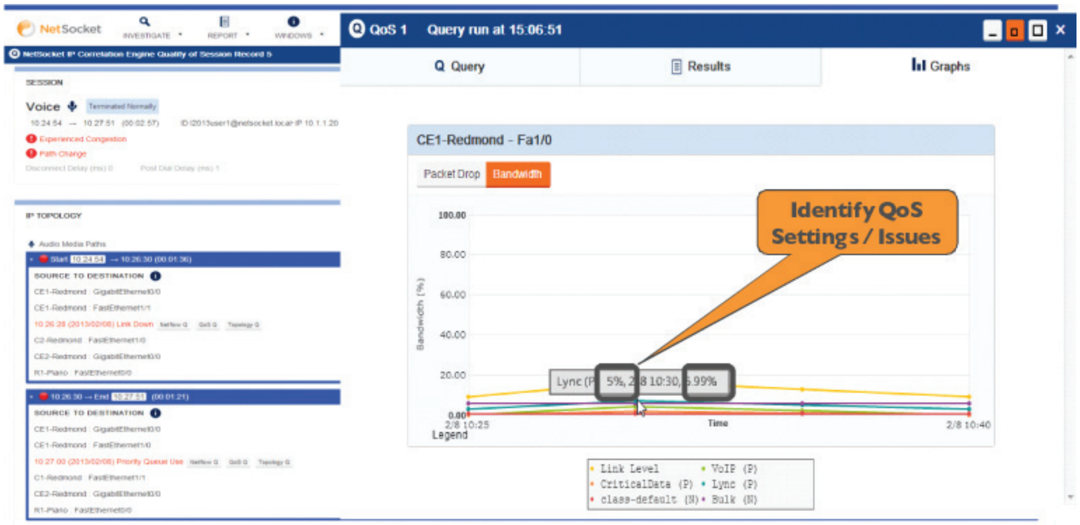
10:26:30 → End 10:27:51 (00:01:21)

SOURCE TO DESTINATION

CE1-Redmond : GigabitEthernet0/0
CE1-Redmond : FastEthernet1/0
10:27:00 (2013/02/08) Priority Queue Use Netflow Q QoS Q Topology Q
C1-Redmond : FastEthernet1/1
CE2-Redmond : GigabitEthernet0/0
R1-Plano : FastEthernet0/0

Figure 16. Packet loss during the Lync call

The second graph is bandwidth, which shows both the configured bandwidth for each queue and amount of traffic that was classified into that queue. The Lync class was provisioned for 5%, but more than 7% was attempting to get through. This caused the network packet loss and points to a QoS configuration issue.



NetSocket IP Correlation Engine Quality of Session Record 5

SESSION

Voice Terminated Normally

10:24:54 → 10:27:51 (00:02:57) ID i2013user1@netsocket.local· IP 10.1.1.20

Experienced Congestion

Path Change

Disconnect Delay (ms) 0 Post Dial Delay (ms) 1

IP TOPOLOGY

Audio Media Paths

Start 10:24:54 → 10:26:30 (00:01:36)

SOURCE TO DESTINATION

CE1-Redmond : GigabitEthernet0/0
CE1-Redmond : FastEthernet1/1
10:26:28 (2013/02/08) Link Down Netflow Q QoS Q Topology Q
C2-Redmond : FastEthernet1/0
CE2-Redmond : GigabitEthernet0/0
R1-Plano : FastEthernet0/0

10:26:30 → End 10:27:51 (00:01:21)

SOURCE TO DESTINATION

CE1-Redmond : GigabitEthernet0/0
CE1-Redmond : FastEthernet1/0
10:27:00 (2013/02/08) Priority Queue Use Netflow Q QoS Q Topology Q
C1-Redmond : FastEthernet1/1
CE2-Redmond : GigabitEthernet0/0
R1-Plano : FastEthernet0/0

Figure 17. Bandwidth utilization during the Lync call

This demonstration illustrates that it is CEM's comprehensive view and automatic correlation of the IP network content, session and topology layers, in addition to its access to Microsoft Lync session information that provides fast root cause identification, analysis and remediation in just a matter of clicks.

NetSocket: Because Correlation Matters

NetSocket's CEM automatically provides a complete view of the content, session and network quality for each Lync session on a hop-by-hop basis. CEM's unique ability to peer with the routed network provides immediate end-to-end visibility into Lync network events and issues. CEM with the new Lync Network Diagnostics API uniquely enables network deployment without costly probes.

CEM enables an end-to-end superior user experience by optimizing Microsoft Lync UC service management with:

- Immediate insight into network issues that affect Microsoft Lync performance
- Session-level integration with Microsoft Lync for real-time visibility without costly probes
- Automatic correlation of all IP network session, content and topology data with the user experience to see the "whole" Microsoft Lync end-user experience picture
- Accurate root cause analysis to find the "needle in the haystack" in just a few clicks
- Real-time and historic trending and reporting for greater predictability
- More than 70% reduction in problem resolution for a lower TCO

You may view the NetSocket CEM and Microsoft Lync demonstration by going to **www.netsocket.com**, or contact NetSocket for a live demonstration at **info@netsocket.com**.

NetSocket

3701 W. Plano Pkwy, Suite 140, Plano TX 75075
Phone: +1 214.427.7300 Fax: +1 972.596.7943
info@netsocket.com www.netsocket.com