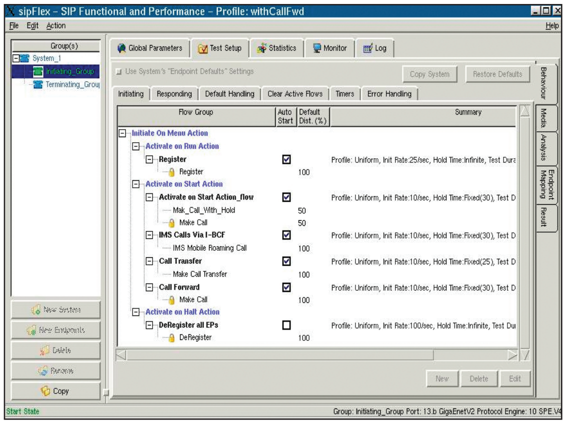
IP-to-IP Gateway Test Suite

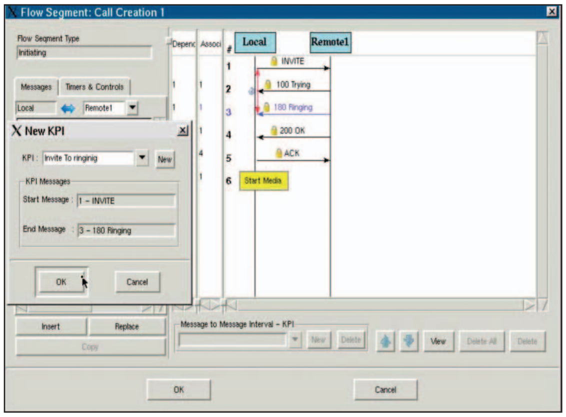


□ Use System's "Endpoint Defaults" Settings

Flow Group	Auto Start	Default Dist. (%)	Summary
Initiate On Menu Action			
Activate on Run Action			
Register	☑		Profile: Uniform, Init Rate:25/sec, Hold Time:Infinite, Test Dura
Register		100	
Activate on Start Action			
Activate on Start Action_flow	☑		Profile: Uniform, Init Rate:10/sec, Hold Time:Fixed(30), Test D
Mak_Call_With_Hold		50	
Make Call		50	
IMS Calls Via I-BCF	☑		Profile: Uniform, Init Rate:10/sec, Hold Time:Fixed(30), Test D
IMS Mobile Roaming Call		100	
Call Transfer	☑		Profile: Uniform, Init Rate:10/sec, Hold Time:Fixed(25), Test D
Make Call Transfer		100	
Call Forward	☑		Profile: Uniform, Init Rate:10/sec, Hold Time:Fixed(30), Test D
Make Call		100	
Activate on Halt Action			
DeRegister all EPs	□		Profile: Uniform, Init Rate:100/sec, Hold Time:Infinite, Test Du
DeRegister		100	

Start State

Group: Initiating_Group Port: 13.b GigaEnetV2 Protocol Engine: 10 SPE.V4



Flow Segment Type: Initiating

KPI : Invite To ringinig

KPI Messages

Start Message : 1 – INVITE

End Message : 3 – 180 Ringing

Message to Message Interval – KPI

Highlights

- 320 000 RTP streams
- 2 560 000 endpoints
- 4250 sessions per second with RTP
- Theft of service (ToS) and session policing tests
- Media-pinhole opening and closing tests
- Generation and analysis of voice, video and DTMF services
- Quality of service (QoS) and VQT testing
- Video quality assessment with MDI
- Extensive list of codecs
- Comprehensive statistics
- Transport layer security (TLS)
- IPSec
- IKEv1, IKEv2
- SIP, H.323 and H.248
- SRTP/SRTCP

Next-Generation Network Assessment

EXFO
EXPERTISE REACHING OUT

Overview

IP-to-IP gateways such as session border controllers, H.248 border gateways, security gateways and firewalls, play a critical role in enabling and protecting the new generation of multimedia services, which are driving the deployment of VoIP and fixed mobile converged (IMS) networks.

VoIP and IMS IP-to-IP gateways support a number of core functions such as security against theft of service and malicious attacks using SIP flood/DoS and rogue media, per-session policing, QoS monitoring and reporting as well as secure access to services. These functions are critical to ensure the viability of VoIP and IMS services. This IP-to-IP Gateway Test Suite focuses on testing these functions as well as performance, scalability and reliability of the IP-to-IP gateways.

Large-Scale and High Performance Signaling Solution

This solution can simulate 4250 sessions per second with signaling and RTP. It offers a large-scale test solution, which can emulate up to 2 560 000 endpoints (distributed over ten groups of endpoints) in subscriber and/or gateway modes with each subscriber supporting a unique IP address.

Comprehensive Media Generation and Analysis

The IP-to-IP Gateway Test Suite can generate and terminate up to 320 000 RTP/SRTP streams on a single chassis, providing the ability to emulate up to 160 000 active sessions while generating RTP for the entire duration of each session.

Each session is unique and can support its own media characteristics such as codec type and packetization interval and wave file. RTP and path verification analysis can be performed on every established session to verify the integrity of the RTP packets that are received.

RTP/SRTP (voice, video and DTMF) analysis (VQT, QoS, MDI) can be performed on up to 320 000 simultaneous sessions in real time for the duration of the sessions. The results of the analysis are displayed in real time and updated on a one-second interval.

Tightly-Coupled Signaling and Media

In real-world deployments, signaling and the associated RTP stream for each session is tightly coupled. The media will start only after signaling has been successfully established and will stop as soon as the session has been terminated from a signaling perspective.

The IP-to-IP Gateway Test Suite emulates real world implementations by guaranteeing a tight coupling between the signaling and media for each session, regardless of the session characteristics.

The time between signaling establishment and media generation and between signaling termination and media termination is of the order of milliseconds, guaranteeing that the device under test will not terminate the sessions because of inactivity after the sessions are successfully established.

The media start and stop times relative to session establishment and tear down can be configured.

Real-World Traffic Characteristics

In order to emulate real world traffic, the IP-to-IP Gateway Test Suite allows users to easily define the following traffic characteristics for up to eight independent groups of endpoints:

- Session establishment rate and distribution
- Session duration
- Media mix in terms of percentage of certain media types (audio, video and DTMF) and codecs where applicable
- Percentage of sessions with media—rest of sessions will be placed on hold
- Call flow and signaling messages content

QoS, VQT and DTMF Analysis

The IP-to-IP Gateway Test Suite provides the ability to measure the quality of the end-user experience by performing voice, video and DTMF analysis in real time on up to 320 000 simultaneous RTP/SRTP streams on a single platform.

Thresholds can be configured for a number of parameters. If the threshold conditions are not met, the session is declared failed and detailed information is provided at the endpoint group, media type (voice, video and DTMF), codecs and session levels.

The following media quality measurements are provided and updated in real time:

- QoS: packet loss, delay and jitter
- Voice quality: mean opinion score (MOS) and R-factor
- Video quality: media delivery index (MDI)

The application also supports generation and analysis of DTMF in-band and out-of-band using signaling (SIP info and H.248 notify/modify messages) and RFC 2833.

Session Policing and Protection Against Service Theft

A core function of IP-to-IP Gateway Test Suite is to perform per-session inspection to ensure that each session complies to the negotiated bandwidth. This function is critical not only to protect against theft of services (session negotiating audio but generating video for example), but also to ensure that sessions that comply to their negotiated contract are not impacted by non-conforming sessions.

A single non-compliant video stream of 10 Mbit/s could consume the required bandwidth of 156 G.711 64 kbit/s audio calls and if these calls are starved of their required bandwidth, the quality of the user experience will be significantly degraded.

The IP-to-IP Gateway Test Suite provides the ability to easily test this core function of IP-to-IP gateways. Users can simulate theft of services by selecting different media/codec types for negotiation and transmission.

The application will detect theft-of-service activities and provide detailed statistics in real time so that the user can verify whether the gateway detected and penalized the non-conforming media streams while the streams that conformed to their negotiated contract were not impacted.

Media Integrity and Routing Verification

Under load an IP-to-IP gateway could route packets to unintended subscribers, which could result in crosstalk.

The path and media verification tests of the IP-to-IP Gateway Test Suite can detect misrouted packets, mislabeled ToS and DSCP headers, unexpected media types and inactivity after call establishment.

Pinhole Opening and Closing Verification

IP-to-IP gateways provide access to the network by opening a media path typically referred to as a pinhole for each established session. Resources (memory, processing cycles, etc.) are allocated to each pinhole and the associated media stream. On termination of each session, the IP-to-IP Gateway Test Suite should deallocate the resources and close the pinhole.

Failure to close the pinhole and deallocate the resources will result in a resource-leak, which will eventually cause the gateway to run out of resources and crash. In addition, open pinholes that are not associated with an active session are security loopholes, which can be exploited by hackers to steal services and attack the network with rogue media.

The IP-to-IP Gateway Test Suite supports canned test scenarios to verify that pinholes are successfully opened when sessions are established and closed once the sessions are terminated. The solution also supports the ability to generate media through a pinhole after the session has been terminated and detect whether the media was forwarded by the gateway.

TLS Security

Each emulated SIP endpoint in the SIP IP-to-IP Gateway Test Suite can be TLS enabled providing the ability to emulate up to 320 000 unique security associations. The endpoints can emulate both client and server modes and support the following cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA

Media Security

Secure real-time transport protocol (SRTP) and secure real-time transport control protocol (SRTCP) can be enabled on any media stream to provide security. Up to 320 000 secure media connections (SRTP and SRTCP) are generated and analyzed at full line rate. Encryption keys are exchanged using the SDP security description (RFC 4568).

Media security can also be enabled on any of the 320 000 media streams using IPSec with IKEv2 negotiating the keys while at the same time providing real-time generation and analysis on all streams. Signaling and media can share the same IPSec tunnel or have their own dedicated tunnels as per the network topology.

Bandwidth Thresholds Configuration

In a deployed network, the bandwidth utilization is a complex calculation which depends on the session establishment rates and hold-time and mix of media/codecs. This computation can be very complex especially in scenarios where the traffic patterns are non-constant, contain a number of different traffic types (mix of codecs) and the session hold-time is variable.

To generate RTP traffic within certain minimum and maximum bandwidth thresholds, the IP-to-IP Gateway Test Suite allows users to configure the upper and lower bounds of the bandwidth utilization for each Gigabit Ethernet interface. Once the upper threshold is reached, the application can be configured to generate signaling-only sessions, or pause call generation until the lower bandwidth threshold is achieved.

ToS and DSCP Remapping Verification

IP-to-IP gateways will need to remap ToS/DSCP values for one value on the incoming stream to another on the outgoing stream.

ToS remapping is required to maintain quality of service guarantees especially when media streams cross service providers' network boundaries. The IP-to-IP Gateway Test Suite supports a canned test scenario to test the ToS and DSCP remapping functions of the gateway. Endpoints can be configured to generate and detect particular ToS and DSCP values within the RTP media stream. When an incorrect ToS or DSCP value is received by an endpoint, a detailed call record with very detailed media information is created.

Troubleshooting Capabilities

To aid in troubleshooting, a comprehensive set of statistics, protocol message information and troubleshooting logs captured by the application are available in real-time. All protocol errors observed by the application protocol stack and other detailed protocol information that are required to identify the root cause of the errors are logged.

Integrated Ethereal

The application supports a built-in signaling monitor and integrated Ethereal. Up to ten independent Ethereal monitors (one for each group of endpoints) can be launched. The Ethereal monitors will only display the signaling traffic for the endpoint-group for which it is launched.

Statistics

A comprehensive list of signaling and media statistics are available to aid in the identification of stability, reliability, performance and scalability issues that could arise during the tests. All statistics including QoS measurements and threshold violations are updated in real-time at a one-second interval and are available in tabular and time-based histograms and graphs. The statistics views can be fully customized—allowing focused statistics from any category in a convenient single view—and all statistics can be exported to comma-separated files for post analysis.

Three levels of statistics are available to expedite the identification and resolution problem of areas:

- Global Summary Statistics

  The global summary view provides a high-level summary of the signaling and media statistics for all endpoint-groups in a single screen. From this view, endpoint-groups with signaling protocol errors and or QoS, MOS, MDI, DTMF, service theft, rogue media and other media related issues can be easily identified.

- Endpoint-Group Statistics

  Detailed signaling and media statistics are available for each endpoint-group. The media statistics are collected and displayed on a per media/codec type in a single screen. Up to 15 unique media types can be monitored and analyzed in real-time for bandwidth utilization, packet loss, delay, jitter, MOS, MDI and DTMF. Voice/video and DTMF quality as well as other media related thresholds violation are highlighted per media type.

- Detailed Session Statistics

  Call records are provided for each session that fails user-defined thresholds for:

  - Path/media verification, ToS/DSCP remapping, theft of service, misrouted packets
  - QoS/VQT, MDI, MOS, delay, loss, jitter, R-factor
  - DTMF digit verification and inter-digit gaps
  - Signaling errors during the session establishment and tear-down phases

Within each call record, detailed information is provided for a comprehensive list of session characteristics such as the calling and called parties, signaling and media start and stop times, negotiated, transmitted and received codecs, QoS (delay, loss and jitter), MOS, R-factor, MDI and DTMF analysis.

Up to ten time-stamped periods during which the user-defined thresholds were not met are captured.

Automation

A TCL command line interface (CLI) is available to automate the key features of the IP-to-IP Gateway Test Suite.

Interface Support

10/100/1000 Ethernet

Transport

- TCP, UDP, SCTP

Network

- IPv4, IPv6

SIP Signaling Protocol

- RFC 3261, RFC 3262, RFC 3265, RFC 2976, RFC 3515, RFC 311, RFC 3263, RFC 2327, RFC 3264

H.248 Signaling Protocol

- ITU-T H.248.1 v3, ETSI TS 283 018 v.1.1.1, ETSI TS 102 333 v.1.1.2

Audio Codecs

- ITU-T G.711 A-law
- ITU-T G.711 U-law
- ITU-T G.721
- ITU-T G.722
- ITU-T G.723
- ITU-T G.726
- ITU-T G.728
- ITU-T G.729
- ILBC
- GSM-EFR, GSM-FR, GSM-HR
- AMR wideband and narrowband
- EVRC, EVRC-B

Audio Quality Measurements

- ITU-T G.107 E-model

Video Codecs

- H.263
- H.264

Video Quality Measurements

- RFC 4445 (MDI)

DTMF

- In-band
- RFC 2833
- SIP info and H.248 modify/notify methods

Security Protocols

- Transport layer security: RFC 2246, RFC 2459, RFC 3546 and RFC 3268
- IPSec
- IKEv1, IKEv2
- SRTP

ORDERING INFORMATION

For ordering information, please contact **isales@EXFO.com**

EXFO Corporate Headquarters > 400 Godin Avenue, Quebec City (Quebec) G1M 2K2 CANADA | Tel.: +1 418 683-0211 | Fax: +1 418 683-2170 | info@EXFO.com

Toll-free: +1 800 663-3936 (USA and Canada) | **www.EXFO.com**

EXFO America	3701 Plano Parkway, Suite 160	Plano, TX 75075 USA	Tel.: +1 800 663-3936	Fax: +1 972 836-0164
EXFO Asia	151 Chin Swee Road, #03-29 Manhattan House	SINGAPORE 169876	Tel.: +65 6333 8241	Fax: +65 6333 8242
EXFO China	36 North, 3rd Ring Road East, Dongcheng District Room 1207, Tower C, Global Trade Center	Beijing 100013 P. R. CHINA	Tel.: + 86 10 5825 7755	Fax: +86 10 5825 7722
EXFO Europe	Omega Enterprise Park, Electron Way	Chandlers Ford, Hampshire S053 4SE ENGLAND	Tel.: +44 2380 246810	Fax: +44 2380 246801
EXFO NetHawk	Elektroniikkatie 2	FI-90590 Oulu, FINLAND	Tel.: +358 (0)403 010 300	Fax: +358 (0)8 564 5203
EXFO Service Assurance	270 Billerica Road	Chelmsford, MA 01824 USA	Tel.: +1 978 367-5600	Fax: +1 978 367-5700

EXFO is certified ISO 9001 and attests to the quality of these products. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. EXFO has made every effort to ensure that the information contained in this specification sheet is accurate. However, we accept no responsibility for any errors or omissions, and we reserve the right to modify design, characteristics and products at any time without obligation. Units of measurement in this document conform to SI standards and practices. In addition, all of EXFO's manufactured products are compliant with the European Union's WEEE directive. For more information, please visit **www.EXFO.com/recycle**. **Contact EXFO for prices and availability or to obtain the phone number of your local EXFO distributor**.

For the most recent version of this spec sheet, please go to the EXFO website at **http://www.EXFO.com/specs**

In case of discrepancy, the Web version takes precedence over any printed literature.

EXFO

EXPERTISE REACHING OUT

CE ISO 9001 2008

Printed in Canada 10/07