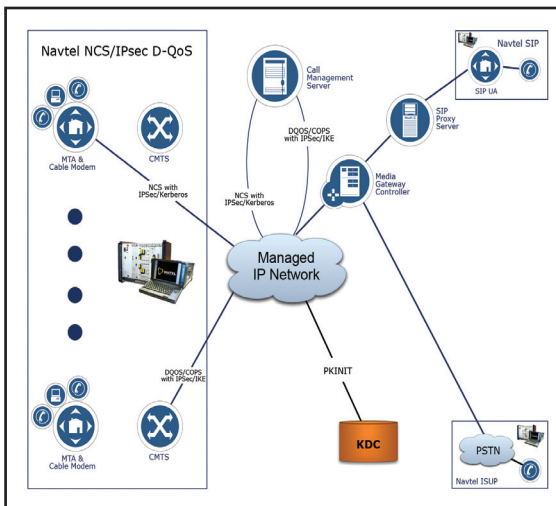


PacketCable™ CMS Performance Test Suite



Highlights

- Generation and termination of hundreds of calls per second for each Ethernet port (up to ten ports per chassis)
- Various NCS traffic characteristics (uniform, step and burst) simultaneous emulation with or without IPSec and D-QoS
- Up to 32 000 MTAs, 200 CMTS and 32 000 endpoints emulation per chassis
- Up to 80 000 security associations with the CMS per chassis
- User-definable NCS messages and call flow
- IPSec support with dynamic key exchange (Kerberos, PKINIT, IKE) or with pre-shared keys
- D-QoS (COPS) support
- Extensive call statistics and troubleshooting logs
- SIP, ISUP, PacketCable™ (NCS, IPSec and D-QoS) and Megaco support in a single chassis



Global award for technology innovation
in 1 and 10 Gigabit Ethernet testing

Overview

VoIP popularity is growing and cable operators are well positioned to play a major role as VoIP providers thanks to the PacketCable™ project, which leverages the existing cable infrastructure by building the VoIP architecture on top of the established DOCSIS cable network. This new network introduces challenges that network operators and network equipment manufacturers will face in order to ensure network readiness for planned traffic volume, security, quality of service and interoperability. The call management server (CMS), the heart of the new network infrastructure, will be responsible for traffic security and QoS management and will play a crucial role in PacketCable™ VoIP network.

The PacketCable CMS Performance Test Suite is an advanced solution that emulates hundreds of thousands of PacketCable™ access network devices (MTAs), hundreds of CMTSes and generates high volumes of network call signaling (NCS), IP security (IPSec) and dynamic quality of service (D-QoS) traffic. It emulates real-world network conditions so that network equipment manufacturers and network operators can perform stability, performance benchmarking, reliability and scalability tests on the call management server (CMS).

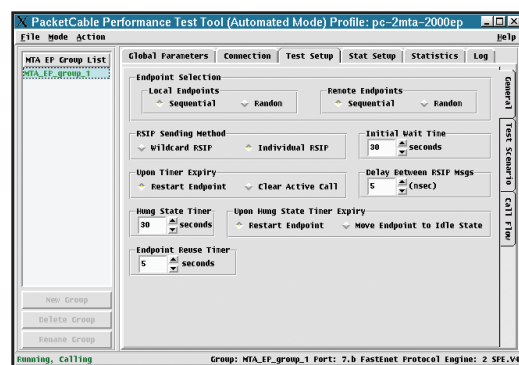
The CMS Performance Test Suite is part of the High-Performance VoIP Test Solution, which also includes SIP, Megaco and ISUP.

Large-Scale and High-Performance Solution

This test suite can generate and respond to thousands of calls per second. It offers a large-scale test solution that can emulate 32 000 MTAs, 20 CMTS and 32 000 endpoints per Ethernet port. Users can configure various test profiles within a single test to replicate real-world signaling traffic scenarios.

Emulated MTAs can be configured into groups, each with its own NCS traffic characteristics as defined below:

- Traffic profile (uniform, step and burst)
- Call rate and call rate variation during the life of the test (initial call rate, final call rate and increment/decrement call/rate)
- Call hold time (infinite, fixed and random)
- NCS messages and call flow



Characterizing IPSec Impact on CMS Performance

When IPSec is enabled, the CMS needs to verify certificates and exchange keys in order to establish security associations for every MTA. The increase in protocol traffic and the need to decrypt and encrypt every NCS and D-QoS message received and transmitted by the CMS, could have a significant negative impact on the performance of the CMS, which could be degraded by as much as 30 %.

The PacketCable CMS Performance Test Suite supports encapsulating security payload (ESP) IPSec operations between the CMS and emulated devices (MTAs, CMTSes). It supports IPSec with dynamic key exchange (Kerberos/PKINIT, IKE) and pre-shared keys. Each emulated device (MTA, CMTS) will have its own unique security association, thus allowing complete and large scale load-test of the CMS.

Characterizing D-QoS Impact on CMS Performance

Dynamic quality of service is required in the PacketCable™ network to provide quality of service guarantees to the end user. Part of the QoS mechanism involves the use of a gate control protocol using COPS. Gates are dynamically allocated, opened, closed and de-allocated as calls are initiated and torn down. Without an open gate, an NCS call supporting D-QoS may fail to get the required QoS. Gates that are not closed/deallocated after calls are torn down, will remain in the hung state and will not be available for re-use by other NCS calls. If the gate allocation/deallocation mechanism fails, it is possible that the CMS will exhaust the limited number of gates that are supported by the CMTS and then the network will not be able to deliver the QoS necessary to ensure high-quality voice over the PacketCable™ network.

The PacketCable CMS Performance Test Suite supports D-QoS through the use of the COPS protocol supported on TCP. Groups of MTAs can be configured to use D-QoS in which case the CMS will need to exchange D-QoS information with the emulated CMTS every time a call is initiated or terminated by an MTA. The D-QoS information exchanged between the CMS and the CMTS must be consistent with the state of the NCS call; hence, there needs to be state-synchronization among the MTAs, CMTS and CMS for every NCS call.

Using this test suite, users can configure a large number of D-QoS enabled MTAs and then generate increasing NCS loads to the CMS. This increase in NCS traffic will also trigger an equivalent increase in D-QoS traffic between the CMS and the CMTS. As traffic rates increase beyond the normal operating level of the CMS, the operations of the D-QoS mechanisms could be impacted by the large volume of traffic that the CMS will experience.

By leveraging the capabilities of this test suite to emulate a large number of MTAs generating high call rates with various call generation profiles, in combination with the detailed statistics and troubleshooting logs provided by the application, network equipment manufacturers and network operators can get a clear indication of how the QoS of voice traffic will be impacted when the CMS is subjected to large amounts of NCS calls at high rates.

Characterizing CMS Fault Tolerant and Recovery Mechanisms

The failover mechanisms of the CMS can be triggered by the detection of a hardware or software fault in the CMS or during standard hardware or software upgrades of the primary and secondary (redundant) CMSs in production networks. In both cases the secondary CMS will take over the responsibilities of the primary CMS and all active calls should be maintained while calls that are in progress but are not active will be dropped until the failover is complete.

Software faults could occur in the CMS system software or in the following protocols:

- NCS
- D-QoS
- IPSec

In the above scenarios, it is extremely important that the failover and fault tolerant mechanisms of the CMS work flawlessly and expeditiously in order to avoid any catastrophic network failure or temporary loss of service.

The PacketCable CMS Performance Test Suite enables users to characterize the stability and efficiency of the CMS failover, fault-tolerance and recovery mechanisms under various network conditions. Users can induce failover in the CMS while it is subjected to various network loads and then utilize the extensive statistics and troubleshooting logs of the test suite to characterize the behavior of the CMS before, during and after a failover has occurred. It also supports failover at the NCS, D-QoS and IPSec protocol layers and in some cases, makes use of domain name server (DNS) as per the protocol(s) specification.

Defining and Generating User-Defined Messages

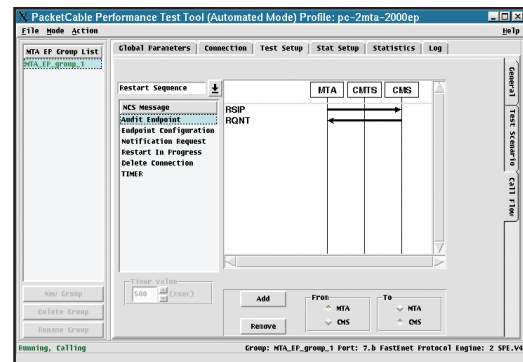
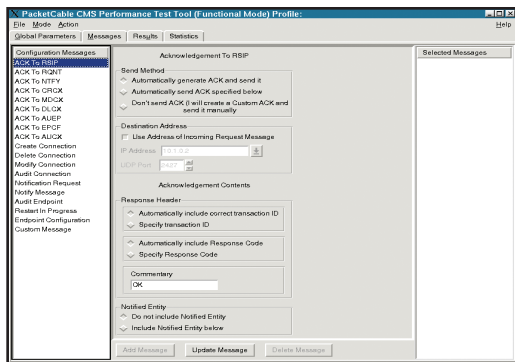
The PacketCable CMS Performance Test Suite enables users to define any NCS message and then generate this message to the device under test. This feature allows users to perform negative and positive testing of the CMS under load. The contents of the generated message and the response of the device under test can be viewed in the message display window.

Functional/Positive Testing

The core functions of the CMS can be tested using the Functional mode of the PacketCable CMS Performance Test Suite.

In this mode users can define:

- NCS messages content
- Automatic response to incoming NCS messages with either the standard or user define NCS message
- Call flow—generate NCS messages or respond to incoming messages based on a standard or user-defined call flow
- Predefined or on-the-fly user-definable call flow



Negative Testing

In order to verify proper protocol implementation and characterize CMS behavior when subjected to protocol errors, the CMS Performance Test Suite allows users to:

- Ignore incoming messages
- Generate incorrect responses
- Specify a delay before responding to incoming messages
- Define compliant and non-compliant NCS messages and call flow

Statistics

The PacketCable CMS Performance Test Suite provides a comprehensive list of statistics and troubleshooting logs to aid in the identification of stability, reliability, performance and scalability issues that could arise during the tests. The statistics are provided in real-time and are also stored in a comma-separated file for post analysis.

Global and Group Cumulative Statistics

NCS Statistics

Incoming statistics

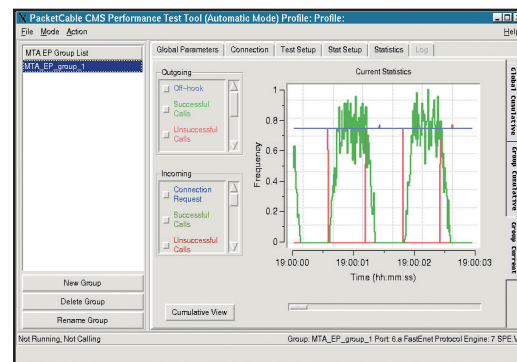
- Successful/unsuccessful CRCX
- Successful/unsuccessful MDCX
- Successful/unsuccessful DLCX
- Successful/unsuccessful AUCX
- Successful/unsuccessful AUEP
- Successful/unsuccessful RQNT

Outgoing statistics

- Successful/unsuccessful NTFY
- Successful/unsuccessful RSIP
- Resent RSIP

Errors are grouped based on:

- Transient errors
- MTA/CMTS related errors
- Protocol errors
- CMS related errors



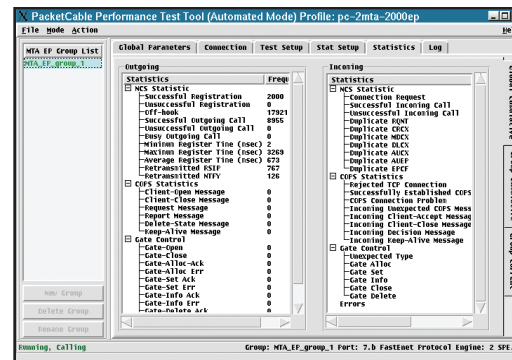
Security Statistics

CMTS statistics

- Successful/unsuccessful SA establishment
- Dynamic IPsec (IKE operations)
- Successful/unsuccessful IKE authentications
- Successful/unsuccessful CMTS certificates validated

MTA statistics

- Successful/unsuccessful SA establishment



Dynamic IPsec (Kerberos/PKINIT)

- Successful/unsuccessful Kerberos authentication
- Successful/unsuccessful service tickets requests from KDC
- Successful/unsuccessful authentication with CMS
- Successful/unsuccessful MTA certificates generated
- Successful/unsuccessful new (after ticket expiry) acquisition
- KDC communication errors
- Re-key messages
- Wake-up messages

D-QoS STATISTICS

COPS Statistics

Incoming statistics

- Successful/unsuccessful client accept
- Successful/unsuccessful client close
- Successful/unsuccessful decision to CMTS request
- Successful/unsuccessful unsolicited decision

Outgoing statistics

- Successful/unsuccessful client open
- Successful/unsuccessful request
- Successful/unsuccessful report state
- Successful/unsuccessful request state

Gate Controller Statistics

Incoming messages

- Successful/unsuccessful gate alloc
- Successful/unsuccessful gate set
- Successful/unsuccessful gate info
- Successful/unsuccessful gate delete

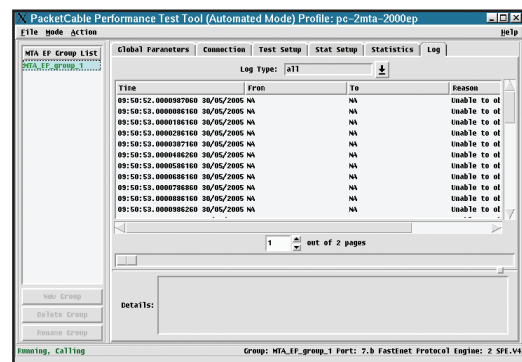
Outgoing messages

- Gate-Alloc Ack
- Gate-Alloc Err
- Gate-Set Ack
- Gate-Set Err
- Gate-Info Ack
- Gate-Info Err
- Gate Close
- Gate Delete

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 are logged to a file with a timestamp and other detailed protocol information that can be used to identify the root cause of the error.

All the statistics, protocol messages and troubleshooting data can be saved to a file for post analysis.



Test CMS Interworking with Other Voice Networks

The PacketCable™ CMS Performance Test Suite when used in conjunction with the ISUP, SIP and Megaco Performance Test Suites enables users to test the interworking capabilities of a CMS with other networks. In addition, users can emulate different call traffic mixes to recreate real-world call scenarios where calls are either initiated or terminated outside of the PacketCable™ network.

All performance test suites provide an extensive list of call statistics and protocol error logs for real-time troubleshooting. The statistics and logs are saved to a comma separated file format for offline/post-test analysis.

ISUP Performance Test Suite (ISUP PTS)

The ISUP Performance Test Suite enables the user to benchmark CMS functions and performance under heavy ISUP loads and characterize its response to SS7 network congestion and failure. It emulates four SS7 signaling points (SSP/STP) 16384/8192 CIC, 32 000 endpoints (telephone numbers), and generates 500 calls/sec for each T1/E1 port.

The functional mode enables the user to configure messages and call-flows, sending any ISUP message on-the-fly to reproduce real-world scenarios and perform negative testing.

SIP Flex Test Suite

This test suite enables the user to benchmark the CMS under heavy SIP traffic loads. It emulates up to 32 000 user agents/terminations and up to 250 calls per second on each port.

Specifications PacketCable™ (Protocol Compliance)

- PacketCable™ 1.0 Architecture Framework Technical Report, PKT-TR-ARCHV01-991201, December 1, 1999, Cable Television Laboratories, Inc.
- PacketCable™ Network-Based Call Signaling Protocol Specification, PKT-SP-EC-MGCP-I10-040402, Cable Television Laboratories, Inc.
- PacketCable™ Dynamic Quality-of-Service Specification, PKT-SP-DQOS-I11040723, Cable Television Laboratories, Inc.
- PacketCable™ Security Specification, PKT-SP-SEC-I11-040730, July 30, 2004, Cable Television Laboratories, Inc.

ISUP

- ANSI T1.113/T1.111 and ITU-T Q.761-764, Q.730 and Q.700

SIP

- RFC 3261

Megaco

- RFC 3015
- ITU-T H.248

Interface Support

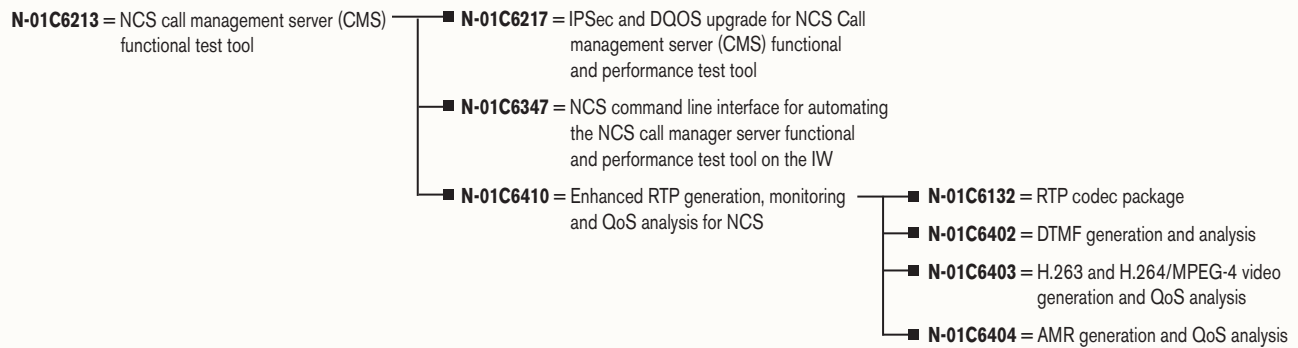
- 10/100/1000 Ethernet

Target Users

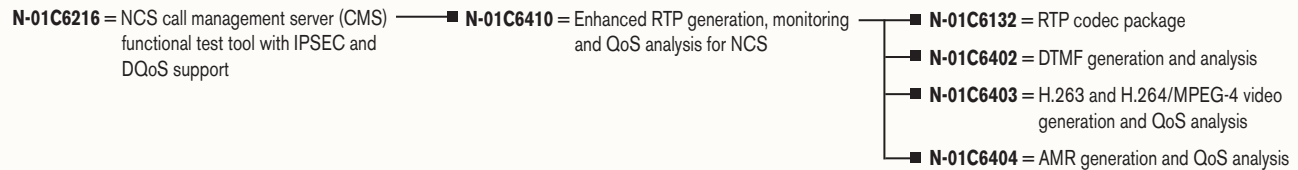
Equipment manufacturers: to verify the proper NCS protocol implementation, analyze CMS performance, stability, reliability, interoperability and scalability with IPsec and D-QoS enabled.

Network operators: to evaluate network equipment before they are deployed and to perform regression testing of new versions of network devices before upgrading their existing network.

ORDERING INFORMATION



Hardware requirements: InterWatch R14 platform or InterWatch M7 platform, a Gigabit Ethernet Interface and a secondary protocol engine version 4.0 (SPEv4).
Platform software requirements: Contact customer service department.



Hardware requirements: InterWatch R14 platform or InterWatch M7 platform, a Gigabit Ethernet Interface and a secondary protocol engine version 4.0 (SPEv4).
Platform software requirements: Contact customer service department.

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	No. 88 Fuhua First Road Central Tower, Room 801, Futian District	Shenzhen 518048 P. R. CHINA	Tel: +86 (755) 8203 2300	Fax: +86 (755) 8203 2306
	Beijing New Century Hotel Office Tower, Room 1754-1755 No. 6 Southern Capital Gym Road	Beijing 100044 P. R. CHINA	Tel: +86 (10) 6849 2738	Fax: +86 (10) 6849 2662
EXFO Europe	Omega Enterprise Park, Electron Way	Chandlers Ford, Hampshire S053 4SE ENGLAND	Tel: +44 2380 246810	Fax: +44 2380 246801
EXFO Service Assurance	285 Mill Road	Chelmsford, MA 01824 USA	Tel: +1 978 367-5600	Fax: +1 978 367-5700