Ensuring quality of service: IMS Testing

Uvaiz Ahmed, Product Manager–Navtel Business Unit

IP Multimedia Subsystem (IMS) has been defined as the technology that will merge the Internet with the cellular world. It combines the delivery of Internet-friendly services such as e-mail, web browsing, presence and instant messaging (IM) with the advantage of cellular technology, providing seamless handover, across any access type. The utopian goal of IMS is to enable the delivery of a common set of converged services across any access network, as put forth by its mantra: any service, across any access or device, anywhere.

The immediate advantage of IMS is for network service providers (NSPs) who are moving towards offering triple- and quadruple-play services. Not only can they benefit from offering a common set of services, which avoids the present quagmire of service duplication across various access networks, but they can also reclaim revenues by offering services that are presently being offered by third-party providers over the existing NSP infrastructure–no wonder the IMS architecture is being promoted by the NSPs!

For consumers, in the short term, IMS may not seem to be a major advantage, although it does come with some hidden benefits, such as the ability to configure services centrally and having access to these same services across any access network or device. Imagine configuring your channel preferences, presence information, find me/follow me preferences in one place and having access to the same content, regardless of whether you are at home on your laptop/PC/TV or on the road and on your cell phone or personal digital assistant (PDA). All this is indeed possible, and with the added convenience of dealing with only one provider and a single account number and bill.

Network equipment manufacturers (NEMs) developing IMS network elements and NSPs deploying IMS networks need to validate that the subsystem works the way it is designed to and that it provides the benefits expected from an investment in such an infrastructure. IMS defines a set of functions and interfaces, and it uses various protocols. Some of these protocols are already defined by the IETF and other standards bodies (e.g., SIP, RTP, SDP, etc.), while others are enhancements to existing standards (such as enhancing the diameter protocol to add the Cx/Dx interface). Developing and deploying an IMS network presents significant challenges for NEMs and NSPs, and there needs to be an extensive testing and validation cycle to ensure the reliability and quality of IMS networks.

In a previous application note entitled Ensuring Reliability of the IMS Core Network, some of the pre-deployment test activities that ensure the quality of the IMS network were discussed. This application note will discuss how some of these pre-deployment testing activities can be performed with equipment such as EXFO's QualityAssurer.

1. TESTING TOPOLOGIES THROUGHOUT THE ENTIRE LIFECYCLE

There are various test-cycle stages during the development of a network element and, at each stage, there are different testing objectives. For example, development test engineers are focused on testing product features, validating adherence to various specifications, checking for device stability and testing against negative scenarios. Performance and scale is not their focus, as this falls under the domain of quality assurance (QA) teams, who are responsible for testing the product not only in isolation, but also end to end from the end user's perspective.

NSPs focus on end-to-end and interoperability testing, as their network is typically a multivendor environment. They are concerned about the effects the introduction of new services will have on the existing network infrastructure and, typically, they will have a QA lab that will mimic the real production network for testing and trial purposes. Prior to the introduction of a new service or a software or hardware upgrade, NSPs will perform regression testing in their QA labs.

NEMs and NSPs can use a stress and emulation testing solution throughout their entire testing lifecycle–from feature testing through to performance, load, regression and capacity testing. The next few sections will outline some of the testing topologies that are supported by the unit.

1.1 Network element testing

When network elements are being designed and developed, NEMs are interested in testing each device by surrounding it with a test bed that can emulate the rest of the network. The types of tests that are carried out at this stage include feature, load, regression, performance, scale and conformance testing. In addition, NSPs may perform these kinds of tests at their evaluation and regression labs. Figure 2 depicts how a stress and emulation testing solution, such as the QualityAssurer, can be used to surround a device under test (DUT) with the rest of the network to perform network-element testing.

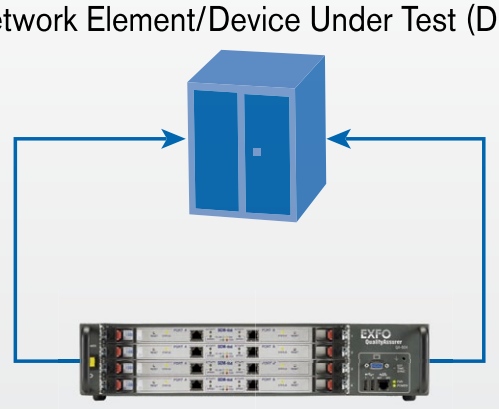


Figure 2: Network element testing

As an example, when testing the IMS S-CSCF, I-CSCF or the AS, this test solution can emulate the IMS subscribers (UEs) and the P-CSCF on one port, and the HSS on the other port, generating IMS test traffic towards the DUT.

Similarly, when testing the P-CSCF, one port of the unit can be used to emulate the IMS subscribers, and the other can emulate the I-CSCF and S-CSCF.

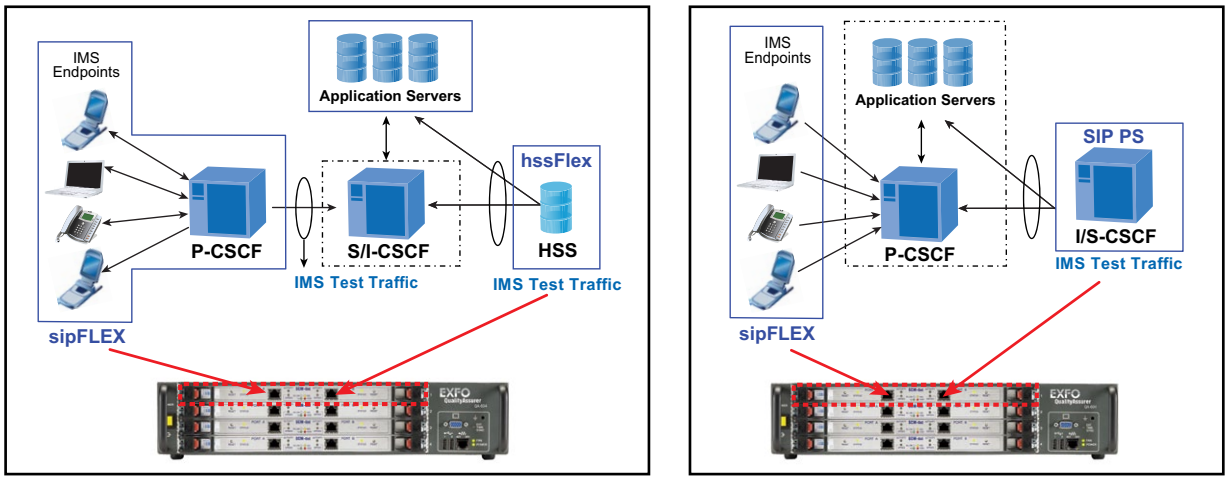


Figure 3. Testing the I-CSCF, S-CSCF and the AS using a test solution such as the QualityAssurer to emulate IMS subscribers (UE's) and HSS on each port

With these test topologies, various IMS test traffic, from both the subscribers perspective (Gm interface) and the HSS perspective (Cx, Dx, Sh,Dh), can be generated towards the DUT.

1.2 Network segment testing

Today's networks are a combination of network elements from different vendors, which must interoperate to provide the complete solution. NEMs need to perform interoperability testing with other devices in their proof of concept and system test labs. They may partner up with their preferred vendors to demonstrate their device and highlight how it interconnects and interoperates with their partners. They need a test bed that will emulate the other parts of the network as they conduct interoperability testing. NSPs will also invite different vendors into their evaluation labs and will require a test tool that can surround the network segment and test it from the various interfaces. Those tests include load, performance and scalability testing against the different network elements within the network segment.

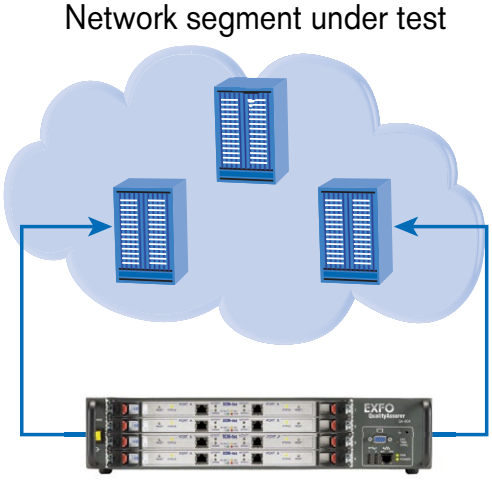


Figure 4. Network segment testing

An example of a network segment is an IMS core. To test the IMS core, it needs to be surrounded by the IMS subscribers at one end and the HSS at the other end. This can be achieved by using one port of the test equipment to emulate the IMS subscribers, generating traffic from the Gm interface, and the other port to emulate the HSS/SLF generating traffic from the Cx, Dx, Sh, Dh interfaces.

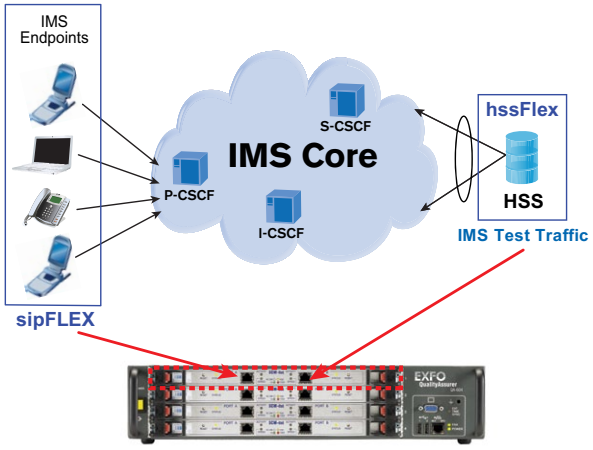


Figure 5. Testing the IMS core using a test solution such as the QualityAssurer by emualting the IMS subscribers (UEs) and HSS (one from each port)

Using the test topology shown above, various types of IMS test traffic can be generated towards the IMS core, from both the subscribers and the HSS. The ability of the IMS core to handle these different types of traffic can be tested and validated.

1.3 End-to-end testing

The quality of customer experience (QoE) is a key metric that will determine the success of the deployed IMS network. QoE can be measured by performing end-to-end testing of the IMS network. This is typically done at NSP evaluation and QA labs, as well as NEM proof-of-concept labs. The test bed is used to test the end-to-end QoE by generating traffic towards the IMS network from a user's perspective. Apart from the user experience, end-to-end testing is very useful for testing the capacity, load and performance of the IMS network.

The following figure shows how two ports on the QualityAssurer can be used to surround the IMS network and perform end-to-end testing. Each port can simulate different IMS network blocks consisting of thousands of IMS subscribers along with their traffic and behavior pattern.

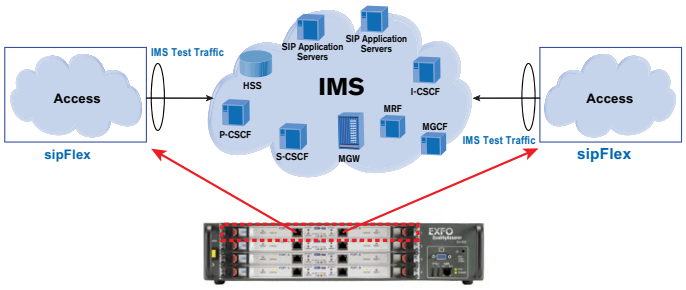
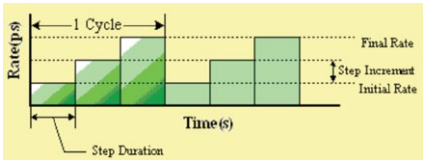


Figure 6. End-to-end testing of the IMS network

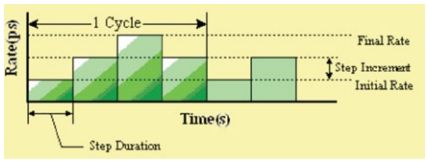
2. VALIDATION OF VARIOUS TRAFFIC SCENARIOS

A deployed network will be subjected to different types of network traffic, depending on the services being offered, subscriber behavior, time of day and geographic location. The traffic in a network that offers multiple services is much more complicated than in a single-service network. The traffic in a city center is different from the traffic that is in a residential neighborhood; the city center will see a lot of conference-calling and Class 5 features (call hold, call transfer, etc.), whereas a residential neighborhood will have simple basic calls with three-way calling and maybe presence and IM traffic. The traffic in a city center will be heavy during business hours, whereas the traffic in a residential neighborhood will increase in the evenings.

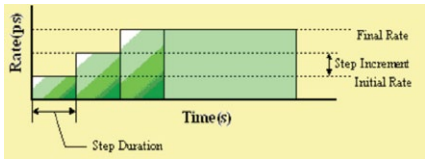
The IMS network must cater to all these different types of network loads and traffic patterns, and these must be validated prior to deployment. In order to test against real-world traffic, stress and emulation test solutions, such as the QualityAssurer, can simulate the following subscriber behavior and traffic patterns towards the network:



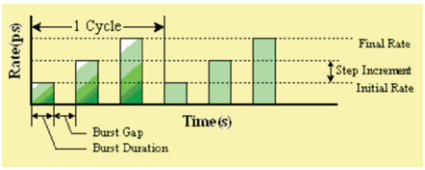
Uniform step up



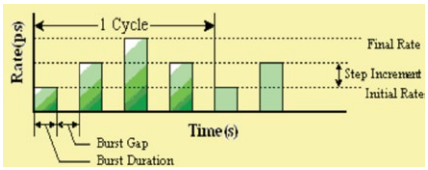
Uniform step up and down



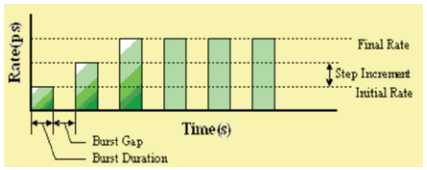
Uniform step up and hold



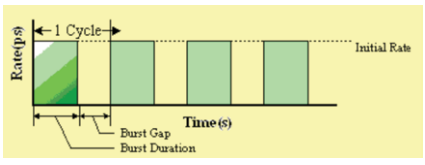
Burst step up



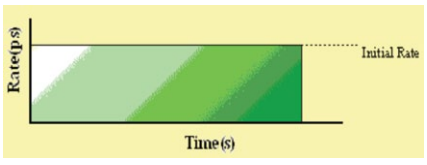
Burst step up and down



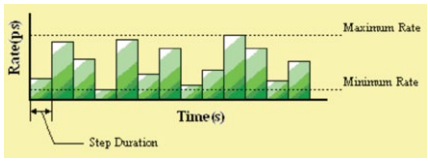
Burst step up and hold



Burst



Uniform Distribution



Random

Figure 7. Different types of traffic patterns

2.1 Registration and authentication

Registration is a key process of any IMS network. If users are not registered, then they cannot access services from the network. In an IMS network, there will be various registration types at any given time. Some of the registrations will be first-time registrations (with authentication using AKA), while others will be re-registrations and de-registrations. Testing the IMS network with various registration distributions is crucial to ensure that the subscribers are granted or denied the services based on their registration states. The different types of registrations must be tested, not only in isolation, but also in combination with each other. Apart from the normal registration traffic, there may be registration avalanches due to normal or abnormal conditions; e.g., after a power outage, upon the restoration of power, there will be a flood of registrations that will be directed towards the network. There can also be denial of service (DoS) attacks in terms of registration floods, and the IMS network will need to be resilient against such attacks. Therefore, it is critical that the network be tested against these real-world scenarios. Some stress and emulation testing solution such as the QualityAssurer can generate tens of thousands of registrations per second.

Figure 8 illustrates an example of how test equipment can be used to assess these different registration scenarios. One port emulates the IMS network subscribers, and the other port emulates the HSS, thereby surrounding the IMS core. The registrations originate from the endpoints towards the IMS network, and the HSS aids in the registration process. In this example, there is a mixture of registration traffic that is generated towards the IMS network, i.e., 50% registration without authentication, 20% registration with 401, 15% with AKA and 15% de-registering from the network. In the background, there is a registration flood that is generated to emulate DoS attacks. The QualityAssurer applications provide latency measurements that can be plotted in real time to study the effect of the DoS attack on the registration process. The applications are packaged with all the registration flows, and these can be generated towards the network in any distribution and load characteristic. The step up option in the traffic profile can be used to gradually increase the registration rate to determine the maximum registration rate that the network can handle.

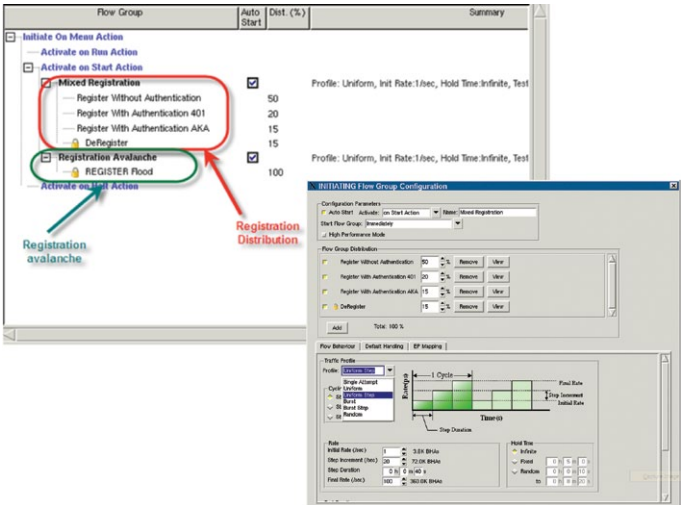


Figure 8. Simualtion of a mix of registration traffic using the QualityAssurer

The impact of de-registration from the HSS (operator-assisted de-registration) can also be studied by generating de-registrations from the HSS, as can be seen from the following screenshot.

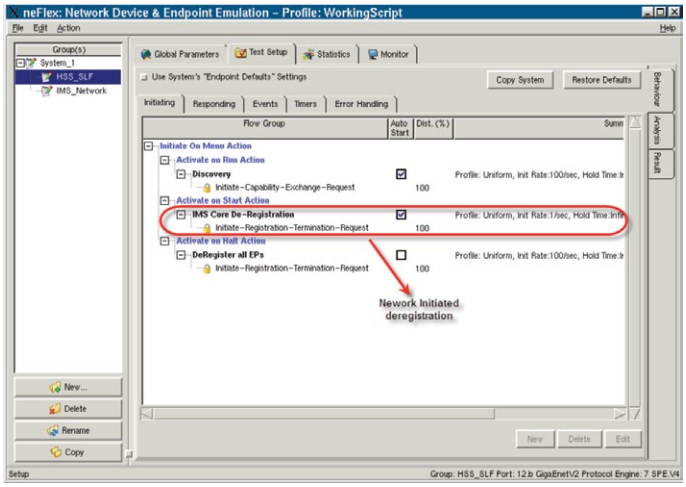


Figure 9. Simulation of de-registration traffic from the HSS using the QualityAssurer

2.2 Mix of services

One of the main drivers for IMS is its ability to allow NSPs to easily introduce new services. As the service delivery platform is independent of the access and the control plane, applications can be accessed by any device that is IMS-enabled. Application servers from third-party vendors can be used to introduce new services faster and cheaper. NSPs may want to evaluate various vendor solutions prior to rolling out a new service. Evaluation of the vendors with some benchmark mix of service is essential for selecting the best products in order for the NSPs to offer services that are competitive and faster to market.

As these new services are introduced, they must also be tested, not only to validate that the service works the way it should, but also to understand the impact of this new service on previously offered services. If, by adding new services, the existing services are negatively affected, then it will lead to dissatisfied customers, thereby increasing customer churn. Operators need to simulate, as close as possible, the varying mix of services that their customers will access–keeping in mind that this mix will change over time.

Some stress and emulation test solutions, such as the QualityAssurer, can be used to simulate a number of IMS services. These include normal calls, Class 5 services (call hold, call transfer, three-way calling, etc.), presence, and IM. It also provides the ability to create custom call flows using the flexible message and flow editor. The various traffic profiles such as uniform, burst, random with step up and down options allow the operator to simulate realistic scenarios and validate all the services that are being offered prior to deployment. The application also allows for the definition of response behavior so as to simulate actual subscriber responses to incoming sessions. In a real-world IMS deployment, not all calls will be answered; for example, some calls will be answered, a few of them will be busy and some of the subscribers will have moved to a new number.

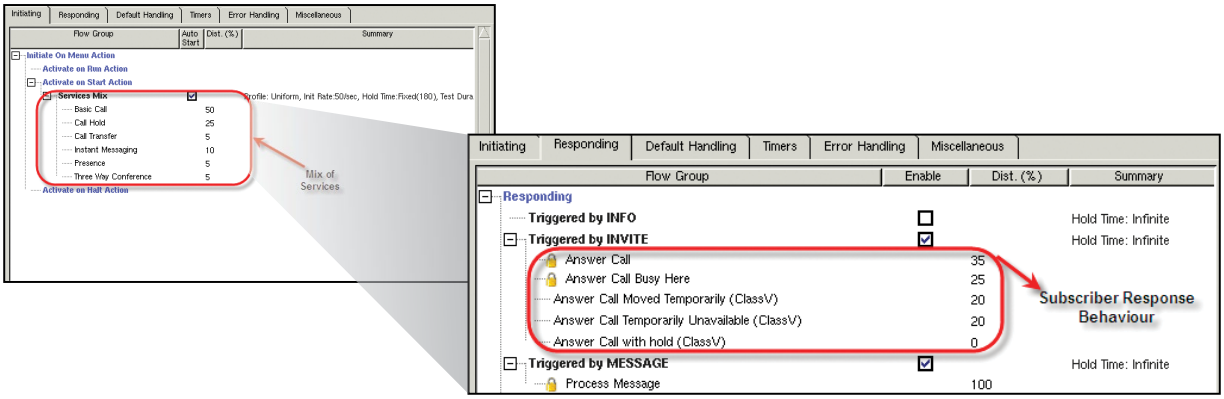


Figure 10. Simualting a mix of services and response behaviors using the QualityAssurer

2.3 Modification of flows and messages

As mentioned above, IMS is an evolving technology consisting of various interfaces and protocols. With any evolving technology, there may be implementations that differ from specifications and could cause problems in the deployed network. NSPs need to ensure that as their network is exposed to different types of implementations, it will be robust and not crash. NEMs developing the network elements need to quickly make changes that reflect a new standard or proprietary implementation. The test tool cannot become the bottleneck in the test cycle; e.g., it cannot have dependencies on professional services (of the test vendor) or complicated scripting for every message and flow manipulation.

With the QualityAssurer test solution, changing a message or a flow is quite simple. All the flows are represented by an easy-to-use ladder diagram. Any message in the flow can be double-clicked to launch a WYSIWYG editor; changes to the messages can be made and previewed immediately. The following screenshot shows an example of the flexible message and flow editor:

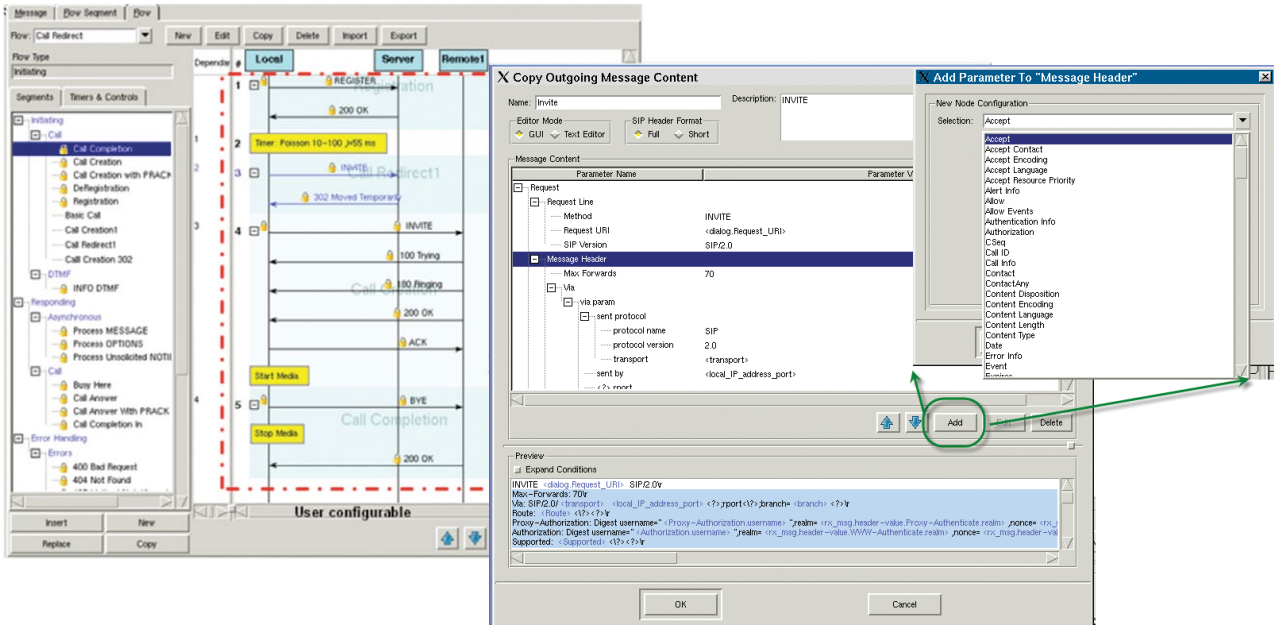


Figure 11. Message or flows manipulation using the QualityAssurer

2.4 DoS attacks

DoS attacks are the most common security threat to NSP networks. It is critical that the network be protected against these attacks so as to prevent the network from being overloaded, as this could result in the denial of service for legitimate requests. Some stress and emulation test solutions, can be used to generate tens of thousands of messages per second, to simulate DoS attacks and analyze the effect of these attacks on legitimate subscriber services. These attacks can be generated from the subscribers' or HSS perspective. As an example, the application can monitor the time it takes to set up a basic call, introduce a DoS attack and then study the effect of the DoS attack on call setup time. This is done by plotting the session latency measurements in real time and observing any degradation in network response. These latency measurements are user-defined and can be measured across any set of messages.

Figure 12 shows an example of how the application can simulate legitimate sessions and flood attacks towards the network. Figure 13 shows the plot of the session setup latency as the network is subjected to a DoS attack; the latency degradation after the DoS attack can be observed.

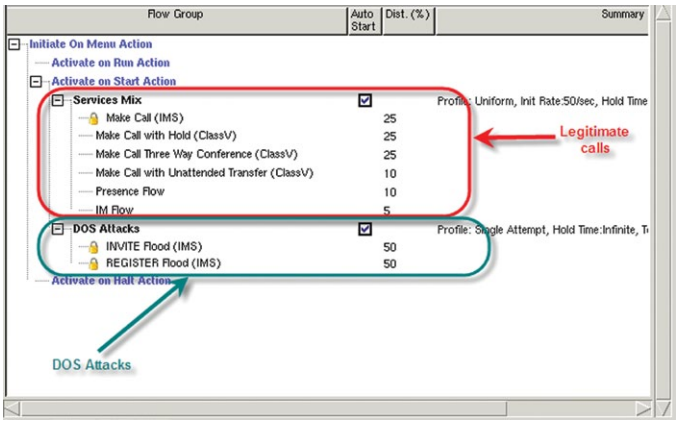


Figure 12: DoS flood attacks along with normal traffic load simulation

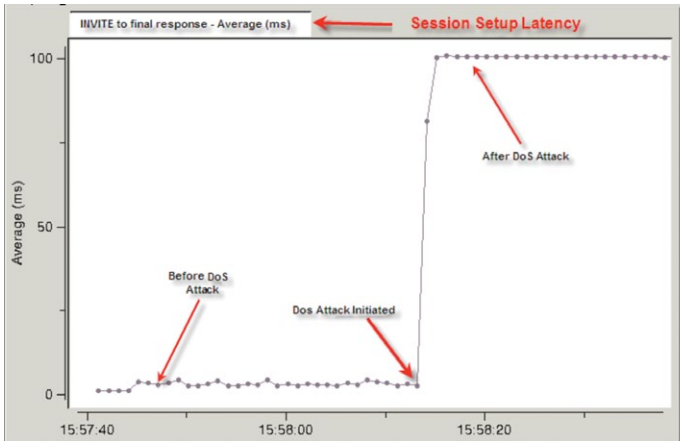


Figure 13. Real-time plot of the session setup latency measurement. This shows the effect of the DoS attack on the session setup latency.

2.5 Scale and Capacity

Scale and capacity of the IMS network elements are key aspects that need to be determined before, during and after the deployment of IMS networks. NEMs and NSPs are interested in knowing what their devices and networks are capable of supporting in terms of the number of subscribers and the sessions established per second. A scalable and high-performance solution, when fully populated, can generate tens of thousands of sessions per second, supporting millions of subscribers. The platform scales by adding hardware modules, each of which supports two ports. As each port has its own dedicated processor and memory, there is no degradation in capacity and scale as the platform is expanded.

Another important requirement is a multi-user and multi-application platform, that allows each port to be used to emulate subscribers, network elements or network segments. The following table lists the capacity and performance of a typical stress and emulation IMS testing solution.

As shown in Figure 14, each set of modules can be used independently by test engineers to create their own test bed, or they can be combined to test for higher capacity and scale.

Capacity	Up to 2 048 000 subscribers
Performance	15 200 SIP registrations per second 3200 SIP calls per second 35 200 SIP message floods per second

Table 1: Typical capacity and performance for IMS testing.

3. CONCLUSION

This application note highlighted how stress and emulation testing solutions can assist NEMs and NSPs in validating IMS networks prior

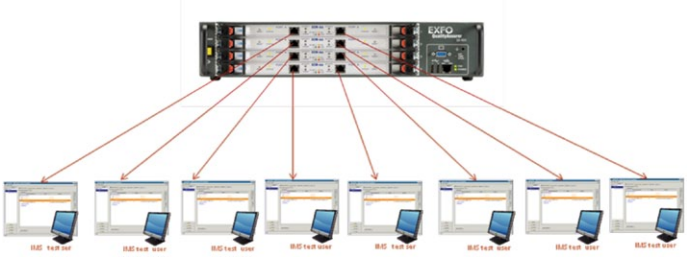


Figure 14. Multi-user and multi-application platform; each port can represent a test bed.

to deployment. Powerful, flexible, and easy-to-use test applications are a must to help perform network element, network segment and end-to-end testing. With such a solution, real-world network traffic scenarios can be generated towards the IMS core so as to ensure the reliability of the network and guaranteegood-quality customer experience.

For a sample list of generic IMS testing uses, please click here to view a table of test cases.

EXFO Headquarters > Tel.: +1 418 683-0211 | Toll-free: +1 800 663-3936 (USA and Canada) | Fax: +1 418 683-2170 | info@EXFO.com | **www.EXFO.com**

EXFO serves over 2000 customers in more than 100 countries. To find your local office contact details, please go to **www.EXFO.com/contact**.