



**Quality of Service (QoS) and Congestion
Test Cases**

MSF-P-IOT-SCN-001-FINAL

MultiService Forum Contribution

Contribution Number: **msf2010.107.03**

Last Saved: 29 July 2010

Working Group: **Network Robustness**

Title: **Quality of Service (QoS) and Congestion Test Cases**

Source: **National Communications System (NCS)**

Richard Kaczmarek (rkaczmarek@csc.com)

Frank Suraci (frank.suraci@dhs.gov)

Arye Ephrath (arye.r.ephrath@saic.com)

John Wullert (jwullert@telcordia.com)

Abstract:

Network Robustness is a new work area for the MSF that includes the following topics / work items: congestion and overload control, disruption testing, network feedback and instabilities, prioritization, and QoS in general, and QoS over the Network-to-Network (NNI) in particular.

To accomplish its mission of providing priority communications during times of network congestion, the NCS is conducting tests which will examine the above work items. Previous Global MSF Interoperability (GMI) testing demonstrated that prioritization of Emergency Telecommunications Services (ETS) traffic was feasible across multiple IMS cores using various access technologies. Current testing will build upon these results in terms of network feedback of QoS and congestion and overload control.

This document describes the Performance Management Reporting Interoperability Test (P-1OT) 2010 Network Robustness Scenarios and Test Cases. These tests focus on the ability of Session Border Gateways (SBGs) to report voice QoS statistics back to a Network Operations Center (NOC) under various network congestion scenarios.

By submitting this contribution, the representatives of the source companies acknowledge reading and agree to the MSF IPR Policy Statement.

The MultiService Forum (MSF) is responsible for developing Implementation Agreements or Architectural Frameworks which can be used by developers and network operators to ensure interoperability between components from different vendors. MSF Implementation Agreements are formally ratified via a Straw Ballot and then a Principal Member Ballot.

Draft MSF Implementation Agreements or Architectural Framework may be published before formal ratification via Straw or Principal Member Ballot. In order for this to take place, the MSF Technical Committee must formally agree that a draft Implementation Agreement or Architectural Framework should be progressed through the balloting process. A Draft MSF Implementation Agreement or Architectural Framework is given a document number in the same manner as an Implementation Agreement.

Draft Implementation Agreements may be revised before or during the full balloting process. The revised document is allocated a new major or minor number and is published. The original Draft Implementation Agreement or Architectural Framework remains published until the Technical Committee votes to withdraw it.

After being ratified by a Principal Member Ballot, the Draft Implementation Agreement or Architectural Framework becomes final. Earlier Draft Implementation Agreements or Architectural Frameworks remain published until the Technical Committee votes to withdraw them.

DISCLAIMER

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and the MultiService Forum is not responsible for any errors or omissions. The MultiService Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything to the contrary, neither the MultiService Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind whether based on theories of tort, contract, strict liability or otherwise, shall be assumed or incurred by the MultiService Forum, its member companies, or the publisher as a result of reliance or use by any party upon any information contained in this publication. All liability for any implied or express warranty of merchantability or fitness for a particular purpose is hereby disclaimed.

The receipt or any use of this document or its contents does not in any way create by implication or otherwise:

Any express or implied license or right to or under any MultiService Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

Any warranty or representation that any MultiService Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

Any commitment by a MultiService Forum company to purchase or otherwise procure any product(s) and/or service(s) that embody any or all of the ideas, technologies, or concepts contained herein; nor

Any form of relationship between any MultiService Forum member companies and the recipient or user of this document.

Implementation or use of specific MultiService Forum Implementation Agreements, Architectural Frameworks or recommendations and MultiService Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in the MultiService Forum.

For addition information contact:

MultiService Forum

39355 California Street, Suite 307, Fremont, CA 94538

(510) 608-5922

(510) 608-5917 (fax)

info@msforum.org

WWW.MSFORUM.ORG

© MultiService Forum 2010

Table of Contents

MULTISERVICE FORUM CONTRIBUTION	1
1 SCOPE.....	5
2 REFERENCES	6
3 NETWORK CONFIGURATION	6
4 SCENARIO 1 TEST CASES – SINGLE DOMAIN PERFORMANCE MANAGEMENT MEASUREMENT	8
4.1 TEST CONFIGURATION	8
4.2 SCENARIO 1.1 – ACCESS SESSION BORDER GATEWAY TESTING.....	9
4.2.1 SBG Voice Performance Reporting Testing	9
4.2.2 SBG Voice Performance Testing	11
4.3 SCENARIO 1.2 – PRIORITY VIDEO TESTING.....	15
4.3.1 SBG Video Performance Reporting Testing	15
4.3.2 SBG Video Performance Testing	17
4.4 SCENARIO 1.3 – I3 FORUM QoS KPI TESTING	21
4.4.1 Scenario 1.3.1 – SBCs Ability to Support i3 Forum Performance KPIs.....	21
5 SCENARIO 2 TEST CASES – MULTI-DOMAIN PERFORMANCE MANAGEMENT MEASUREMENT	22
5.1 TEST CONFIGURATION	22
5.2 SCENARIO 2.1 – NETWORK-TO-NETWORK INTERFACE PROVISIONING	23
5.2.1 SBG NNI Provisioning.....	23
5.3 SCENARIO 2.2 – SBG NNI TESTING	25
5.3.1 SBG NNI Performance Reporting Testing	25
5.3.2 SBG NNI Performance Testing.....	28
5.4 SCENARIO 2.3 – PRIORITY DATA TESTING.....	33
5.4.1 Test Configuration.....	33
5.4.2 Scenario 2.3.1 – Dynamic Provisioning of the Data Border Gateway (DBG) to Support Priority Data	34
5.4.3 DBG Performance Reporting Testing.....	36
5.5 SCENARIO 2.4 – I3 FORUM QoS KPI TESTING	37
5.5.1 Scenario 2.4.1 – SBGs Ability to Support i3 Forum Performance KPIs	37
6 FUTURE TESTS	38

Table of Figures

Figure 3-1 – Basic XTE Configuration	7
Figure 3-2 – XTE Equipment Available for P-IOT 2010 Testing	8
Figure 4-1 – Scenario 1 Test Configuration	9
Figure 4-2. SBG to NOC Message Flows	10
Figure 4-3 – Session Request Rejected	13
Figure 4-4. SBG to NOC Message Flows	16
Figure 4-5 – Session Request Rejected	19
Figure 5-1 – Scenario 2 Test Configuration	23
Figure 5-2 – Normal Call and ETS Call INVITES	24
Figure 5-3 – SBG to NOC Message Flows.....	26
Figure 5-4 – Session Request Rejected	30
Figure 5-5 – Scenario 2.3 Test Configuration	34
Figure 5-6 – NOC to DBG Messaging	35
Figure 5-7 – Bearer Packet Marking	35

1 Scope

Network Robustness is a new work area for the MSF that includes the following topics / work items:

- Congestion and overload control
- Disruption testing
- Network feedback and instabilities
- Prioritization
- QoS in general and QoS over the Network-to-Network interface (NNI) in particular.

To accomplish its mission of providing priority communications during times of network congestion, the NCS is conducting tests which will examine the above work items. Previous Global MSF Interoperability (GMI) testing demonstrated that prioritization of Emergency Telecommunications Services (ETS) traffic was feasible across multiple IMS cores using various access technologies. Current testing will build upon these results in terms of network feedback of QoS and congestion and overload control.

This document describes the Performance Management Reporting Interoperability Test (P-IOT) 2010 Network Robustness Scenarios and Test Cases. These tests focus on the ability of Session Border Gateways (SBGs) to report voice QoS statistics back to a Network Operations Center (NOC) under various network congestion scenarios.

The specific scenarios and test cases discussed in this document are:

- Scenario 1 – Single Domain Performance Management Measurement
 - Scenario 1.1 – Access Session Border Gateway Testing
 - Scenario 1.1.1 – SBG Voice Performance Reporting Under “No Traffic Load”
 - Scenario 1.1.2 – SBG Voice Performance Reporting Under Link Traffic Congestion
 - Scenario 1.1.3 –SBG Voice Session Establishment Congestion
 - Scenario 1.1.4 –SBG Voice Bearer Throughput Congestion
 - Scenario 1.2 – Priority Video Testing
 - Scenario 1.2.1 –SBG Video Performance Reporting Under “No Traffic Load”
 - Scenario 1.2.2 –SBG Video Performance Reporting Under Link Traffic Congestion
 - Scenario 1.2.3 –SBG Video Session Establishment Congestion
 - Scenario 1.2.4 –SBG Video Bearer Throughput Congestion
 - Scenario 1.3 – International Internet Protocol (IP) Interconnection Forum (i3 Forum) Quality of Service (QoS) Key Performance Indicators (KPIs) Testing
 - Scenario 1.3.1 – SBGs Ability to Support i3 Forum Performance KPIs
- Scenario 2 – Multi-Domain Performance Management Measurement
 - Scenario 2.1 – Network-to-Network Interface Provisioning
 - Scenario 2.1.1 – SBG NNI Provisioning with “Encrypted” IPsec Tunnel
 - Scenario 2.2 – SBG NNI Testing
 - Scenario 2.2.1 –SBG NNI Voice and Video Performance Reporting Under “No Traffic Load”
 - Scenario 2.2.2 –SBG NNI Voice and Video Performance Reporting For IPsec Tunnels Where the Link Supporting the IPsec Tunnel is Congested
 - Scenario 2.2.3 –SBG NNI Voice and Video Session Establishment Congestion

- Scenario 2.2.4 –SBG NNI Voice and Video Bearer Throughput Congestion
- Scenario 2.3 – Priority Data Testing
- Scenario 2.3.1 – Dynamic Provisioning of the Data Border Gateway (DBG) to Support Priority Data
 - Scenario 2.3.2 – DBG Performance Reporting Under “No Traffic Load”
 - Scenario 2.3.3 – DBG Performance Reporting Under Internet Traffic Congestion
- Scenario 2.4 – i3 Forum QoS KPIs Testing
- Scenario 2.4.1 – SBGs Ability to Support i3 Forum Performance KPIs

This Network Robustness Interoperability Test is an extension of previous interoperability events, which focused on the validation of Implementation Agreements (IAs) between vendor equipment. This Network Robustness event includes exploratory experiments to determine the capabilities of existing vendor interfaces and their potential for interoperation. These experiments will form the basis for subsequent specification of interfaces and IAs, and the more traditional interoperability testing.

2 References

msf2010.064.03 PRD for MSF Performance Management Reporting IOT event

msf2010.065.06 Test Scenarios for MSF Performance Management Reporting IOT event

msf2010.104.00 i3 Forum Service value and process of measuring QoS KPIs (Release 1.0) May 2010

3 Network Configuration

The NCS' eXperimental Testbed Environment (XTE) will be the host site for the Performance IOT event. The XTE has 20u of available rack space for vendor equipment for the IOT, as well as floor, power (110 VAC and -48 VDC) and cooling space for two to three mobile racks of equipment provided by vendors. The XTE can also establish Virtual Private Network (VPN) connections with vendor and carrier facilities over the Internet for the IOT.

The basic configuration of the XTE is shown in Figure 3-1. The lower portion of the Figure shows the Virtual Local Area Network (VLAN) configuration supporting equipment in the XTE racks. Typically:

- VLANs 110 is used to connect devices for traffic origination
- VLAN 140 is used for IMS and non-IMS components associated with network origination
- VLANs 6xx are used for core network routing and for NNI testing
- VLAN 240 is used for IMS and non-IMS components associated with network termination
- VLANs 210 is used for devices for traffic termination

The upper portion of the Figure shows the XTE's Mobile Demonstration Unit configuration. VLANs 115 and 215 are used for end devices, while VLAN 540 is used for IMS and non-IMS components. The MDU can be used as a standalone demonstration device, or can be connected to the XTE via the Internet for more complex testing and demonstrations.

The XTE configuration allows the provisioning of components to reflect both single domain and multi-domain cores. The high-level scenarios to be tested require slight modifications to the overall architecture; therefore a network configuration diagram is detailed at the beginning of each Scenario under test.

The tests presented in this document assume that only equipment currently available in the XTE will be used for the IOT. The tests will be modified and extended to support other equipment and facilities as they are identified.

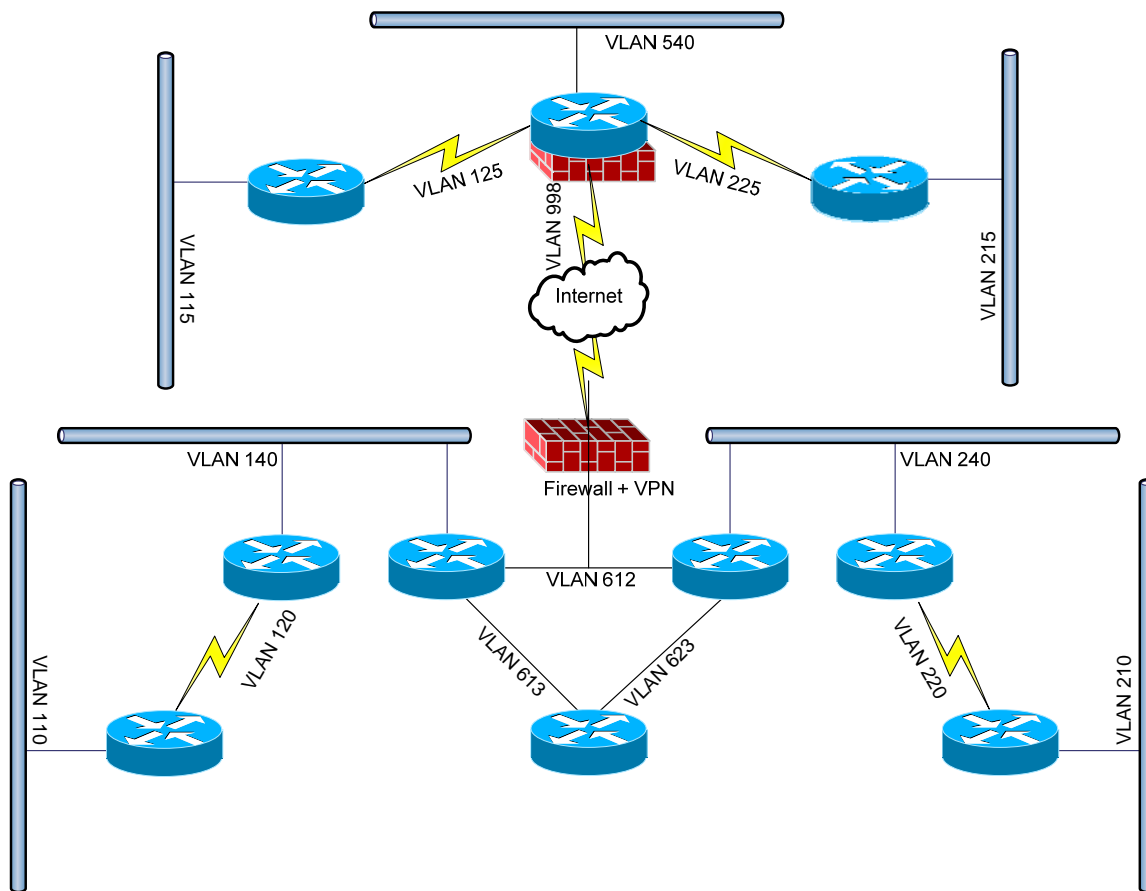


Figure 3-1 – Basic XTE Configuration

Figure 3-2 shows the equipment in the XTE available for P-IOT 2010 testing.

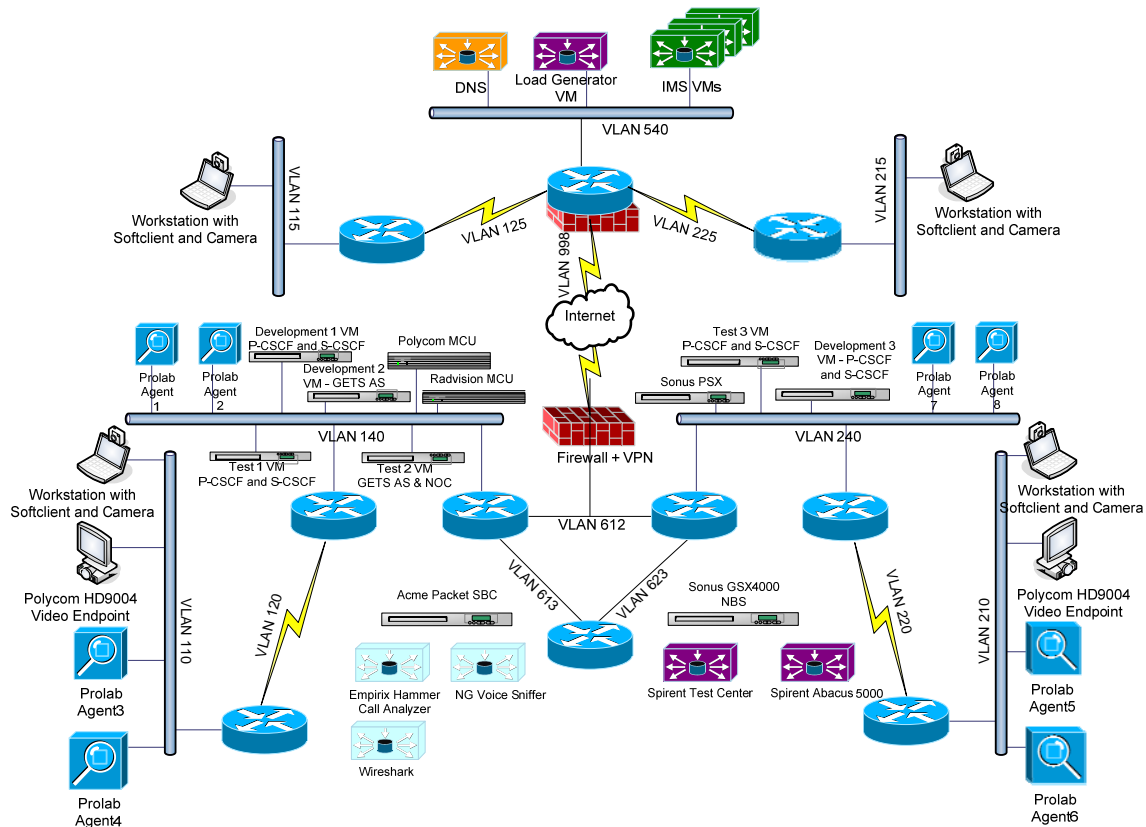


Figure 3-2 – XTE Equipment Available for P-IOT 2010 Testing

4 Scenario 1 Test Cases – Single Domain Performance Management Measurement

4.1 Test Configuration

The network configuration for the Scenario 1 tests is shown in Figure 4-1. Scenario 1 testing requires:

- Endpoints which can establish Voice over Internet Protocol (VoIP) and Video calls
- Traffic Generators to congest various links and Functional Entities (FEs)
- SBGs which generate alarms, call detail records (CDRs) and management information blocks (MIBs)
- Other FEs which generate alarms and MIBs
- A NOC which can view and act on alarms, CDRs and MIBs. In general, the NOC will use an Element Management System (EMS) and / or Network Management System (NMS) for this capability
- Other network analysis equipment (e.g., Sniffer, Wireshark)

Note that the Session Border Gateways (SBGs) used in the XTE are integrated devices that support both signaling and bearer traffic. For this scenario, the SBGs replace the access routers connecting VLAN 120 to VLAN 140 and VLAN 220 to VLAN 240.

Also note that the Proxy (P-) and Serving (S-) Call Session Control Functions (CSCF) are on separate Virtual Machines (VMs) within the test architecture. The SBGs are not acting as P-CSCFs in these tests, but are communicating with the P-CSCFs in the IMS core.

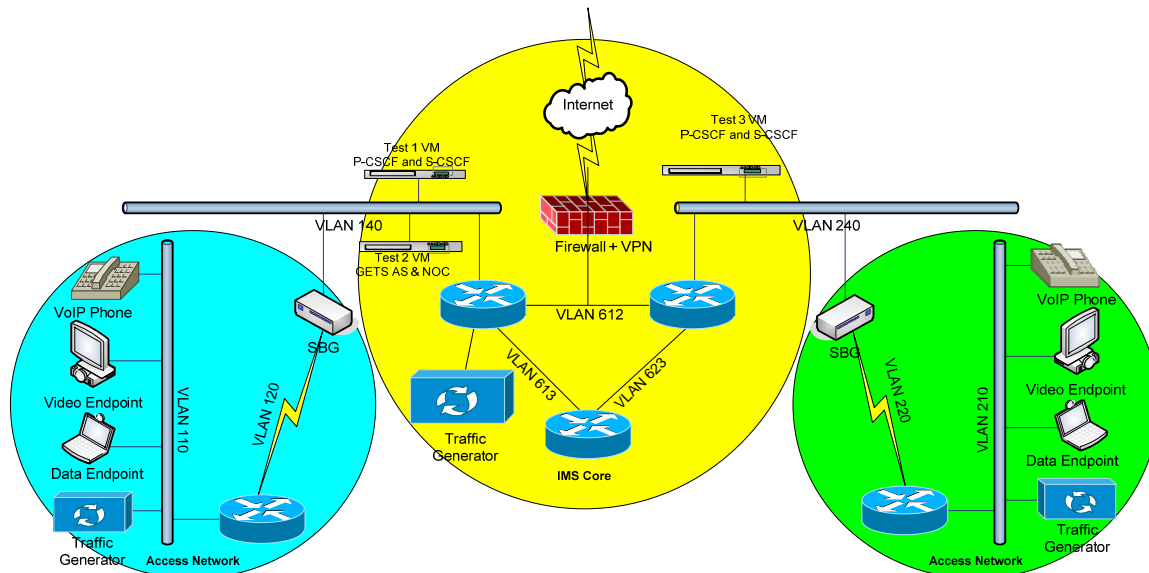


Figure 4-1 – Scenario 1 Test Configuration

4.2 Scenario 1.1 – Access Session Border Gateway Testing

This scenario consists of four tests:

- Scenario 1.1.1 – SBG Voice Performance Reporting Under “No Traffic Load”
- Scenario 1.1.2 – SBG Voice Performance Reporting Under Link Traffic Congestion
- Scenario 1.1.3 –SBG Voice Session Establishment Congestion
- Scenario 1.1.4 –SBG Voice Bearer Throughput Congestion

4.2.1 SBG Voice Performance Reporting Testing

4.2.1.1 Purpose

These test cases demonstrate the ability of an SBG to report the performance of a VoIP call traversing the SBG. SBGs typically generate delay, jitter and loss statistics for each call leg that traverses the SBGs. In addition, some SBGs capture delay, jitter and loss statistics for the call from the RTCP stream traversing the SBG. The Scenario 1.1.1 and 1.1.2 tests are to determine if there is a way to correlate the end-to-end performance presented in the RTCP stream with the performance reported by the SBGs for each call leg. This is done for both “no traffic load” cases, where one hopes to find a high degree of correlation, and for “traffic congestion” cases, where correlation may be more problematic.

4.2.1.2 Scenario 1.1.1 – SBG Voice Performance Reporting Under “No Traffic Load”

4.2.1.2.1 Test Setup and Procedure

- Test configuration as per Section 4.1.
- Traffic Generators turned off.
- Place a VoIP call between endpoints.

- Capture RTCP stream at both endpoints. Capture VoIP performance statistics generated by SBGs and reported to the NOC.
- Note that an SBG typically generates delay, jitter and loss statistics for each call leg that traverses the SBG.

4.2.1.2.2 Observable Results

The message formats and protocols used to transmit data will be captured and analyzed.

There should be minimal delay, jitter and loss for the VoIP call as reported by the RTCP streams by the two endpoints. The delay, jitter and loss statistics from the RTCP streams shall be captured at the end of the call.

The delay, jitter and loss statistics generated by the SBGs for each call leg shall be captured and accumulated into “end-to-end” values. These “end-to-end” values shall be compared with the values captured in the RTCP streams. If the SBG reports delay, jitter and loss statistics captured from the RTCP stream traversing the SBC, these values shall be compared against the statistics reported by the endpoints.

4.2.1.2.2.1 Pass/Fail Criteria

The SBG statistics should closely track the RTCP statistics reported by the endpoints.

4.2.1.2.2.2 Message Flows

The SBG will periodically push Management Information Base (MIB) operational measurements to the NOC using the Simple Network Management Protocol (SNMP). Alerts are immediately pushed to the NOC via SNMP. CDR records may be pushed immediately to the NOC, or may be batched and sent to the NOC. The protocol used depends on the type of push. If the SBGs can be provisioned to support the MSF MI-6 IA (<http://www.msforum.org/techinfo/approved/MSF-IA-RTCP.003-FINAL.pdf>), the tests will be repeated using this IA.

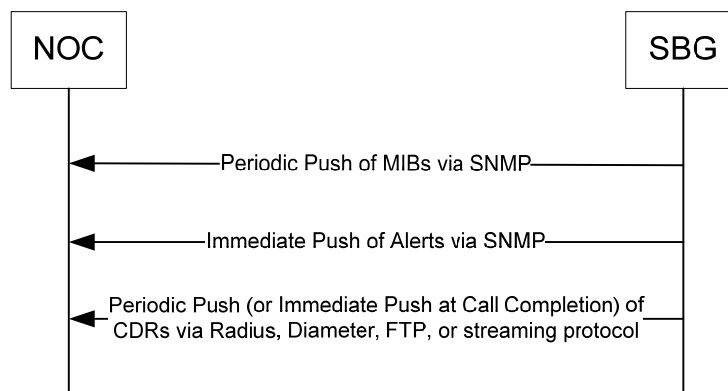


Figure 4-2. SBG to NOC Message Flows

4.2.1.2.3 Trace Capture

Capture the RTCP streams on VLANs 110, 140, 210 and 240. Capture the CDRs and / or MIBs generated by the SBGs and sent to the NOC.

4.2.1.2.4 Known Issues

None.

4.2.1.3 Scenario 1.1.2 – SBG Voice Performance Reporting Under Link Traffic Congestion

4.2.1.3.1 Test Setup and Procedure

- Test configuration as per Section 4.1.

Scenario 1.1.2a – Originating Access Link Congestion

- Traffic Generator set to congest VLAN 120.
- Place a VoIP call between endpoints.
- Capture RTCP stream at both endpoints. Capture VoIP performance statistics generated by SBGs and reported to the NOC.

Scenario 1.1.2b –Core Network Congestion

- Traffic Generator set to congest VLANs 612 and 613.
- Place a VoIP call between endpoints.
- Capture RTCP stream at both endpoints. Capture VoIP performance statistics generated by SBGs and reported to the NOC.

Scenario 1.1.2c – Terminating Access Link Congestion

- Traffic Generator set to congest VLAN 210.
- Place a VoIP call between endpoints.
- Capture RTCP stream at both endpoints. Capture VoIP performance statistics generated by SBGs and reported to the NOC.

4.2.1.3.2 Observable Results

There should be appreciable delay, jitter and loss for the VoIP call as reported by the RTCP streams by the two endpoints. The delay, jitter and loss statistics from the RTCP streams shall be captured at the end of the call.

The delay, jitter and loss statistics generated by the SBG for each call leg shall be captured and accumulated into “end-to-end” values. These “end-to-end” values shall be compared with the values captured in the RTCP streams. If the SBG reports delay, jitter and loss statistics captured from the RTCP stream traversing the SBC, these values shall be compared against the statistics reported by the endpoints.

4.2.1.3.2.1 Pass/Fail Criteria

The SBG statistics should closely track the RTCP statistics reported by the endpoints.

4.2.1.3.2.2 Message Flows

Message flows between the SBG and NOC are defined in Scenario 1.1.1.

4.2.1.3.3 Trace Capture

Capture the RTCP streams on VLANs 110, 140, 210 and 240. Capture the CDRs and / or MIBs generated by the SBGs and sent to the NOC.

4.2.1.3.4 Known Issues

None.

4.2.2 SBG Voice Performance Testing

4.2.2.1 Purpose

These test cases demonstrate the ability of an SBG to impact the performance of a VoIP call traversing the SBG.

4.2.2.2 Scenario 1.1.3 –SBG Voice Session Establishment Congestion

4.2.2.2.1 Purpose

This test is designed to exercise the load-management capabilities of the SBGs, prioritization within those management operations and the ability of SBGs to report the results of such management. The SBGs will be configured with the maximum number of sessions that they can support. The test will exceed that number, and verify that the SBGs reject or shed sessions, based on session priority and on their defined behaviors, and that they accurately report the statistics describing these actions.

4.2.2.2.2 Test Setup and Procedure

- Test configuration as per Section 4.1.

Scenario 1.1.3a – Attempt to Establish More Sessions than Provisioned Maximum

- Provision Originating Access Network SBG to support X1 (TBD) normal sessions and “X1 + 1” ETS sessions.
- Provision Originating Access Network Traffic Generator to generate “X1 - 1” sessions.
- Attempt to place a VoIP call between endpoints. Call should complete.
- Capture VoIP endpoint signaling with SBG. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End the VoIP call.
- Attempt to place a VoIP call between endpoints. Call should complete.
- Attempt to place a second VoIP call between endpoints while first call is active. Since this call exceeds the limit allowed by the SBG, it should be rejected.
- Capture VoIP endpoint signaling with SBG. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active VoIP calls.
- Attempt to place three ETS VoIP calls between endpoints. Two calls should complete and one call should be rejected, since ETS calls should be exempt from the normal session limit but be subject to the ETS session limit.
- Capture VoIP endpoint signaling with SBG. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active VoIP calls.

Scenario 1.1.3b – Attempt to Establish Sessions when SBG is Throttling Sessions

- Pre-test
 - Provision Originating Access Network SBG to support X2 (TBD) sessions. Determine resources used for these sessions (e.g., 25% CPU utilization).
 - Provision the SBG’s lowest congestion level (e.g., throttling mechanism) to kick-in using a lower resource value. Provision SBG highest congestion level to kick-in at the resource utilization for X2 calls.
- Provision Originating Access Network Traffic Generator to generate “X2 - 1” sessions. Verify that not all sessions are being established.
- Attempt to place a normal VoIP call between endpoints. Call should be rejected.
- Capture VoIP endpoint signaling with SBG. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC.
- Attempt to place multiple ETS VoIP calls between VoIP endpoints. Some calls should complete and some calls should be rejected, depending on the SBG’s congestion level.
- Capture VoIP endpoint signaling with SBG. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active VoIP calls.

4.2.2.2.3 Observable Results

Normal session requests that exceed the allowable maximum for simultaneous sessions should be rejected. ETS session requests will be recognized by the SBG via digits analysis of the “710” area code or via an RPH: ets.0 field in the SIP INVITE. ETS calls will be exempted from the maximum limit for normal calls, but will be subject to the maximum limit for ETS calls.

SBGs typically have multiple congestion levels. At each level, the SBGs apply congestion control mechanisms (e.g., shedding call requests) to ensure the SBGs can continue to function. At the lower congestion levels, normal session requests are shed while ETS calls are exempt from shedding. At the highest congestion level, both normal and ETS session requests are shed.

Reports to the NOC should accurately reflect the number of session attempts that were affected by the overload management.

4.2.2.2.3.1 Pass/Fail Criteria

The SBG should reject non-priority calls that would exceed the defined capacity for normal calls. The SBG should allow priority calls, as long as they do not exceed the defined capacity for ETS calls. The statistics reported to the NOC should accurately reflect the number of sessions that were rejected.

4.2.2.2.3.2 Message Flows

A session that cannot be established should receive a 486 response, as shown in Figure 4-3.

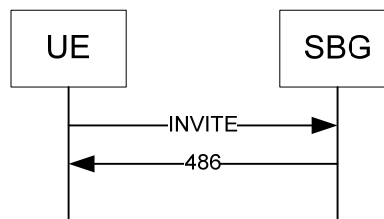


Figure 4-3 – Session Request Rejected

Message flows between the SBG and NOC are defined in Scenario 1.1.1.

4.2.2.2.4 Trace Capture

Capture the endpoint signaling on VLANs 110. Capture the alarms, CDRs and / or MIBs generated by the Originating Access Network SBG and sent to the NOC.

4.2.2.2.5 Known Issues

None.

4.2.2.3 Scenario 1.1.4 –SBG Voice Bearer Throughput Congestion

4.2.2.3.1 Purpose

This test is designed to exercise the load-management capabilities of the SBGs, prioritization within those management operations and the ability of SBGs to report the results of such management. The SBGs will be configured with a maximum bearer throughput for normal calls that they can support (e.g., in bytes per second). For ETS calls, the SBGs may either calculate a higher maximum value (based on the maximum for normal calls), or may allow a higher maximum value to be provisioned. The test will exceed that capacity, and verify that the SBGs reject or shed sessions, based on session priority and on their defined behaviors, and that they accurately report the statistics describing these actions.

4.2.2.3.2 Test Setup and Procedure

- Test configuration as per Section 4.1.

Scenario 1.1.4a – Attempt to Transmit More Traffic than Provisioned Maximum for Normal Calls

- Pre-test
 - Provision Originating Access Network SBG to support X3 (TBD) kbps bearer throughput for normal traffic.
 - Provision Originating Access Network Traffic Generator to generate calls with 100 kbps bearer traffic.
 - Provision Originating Access Network Traffic Generator to generate “(X3/100) – 1” sessions.
- Attempt to place a normal VoIP call between endpoints. Call should complete.
- Capture VoIP endpoint signaling with SBG. Capture RTCP stream at both endpoints. Capture VoIP performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End the VoIP call.
- Attempt to place a normal VoIP call between endpoints. Call should complete.
- Attempt to place a second normal VoIP call between endpoints while first call is active. Since this call exceeds the bearer throughput limit allowed by the SBG, it should be rejected.
- Capture VoIP endpoint signaling with SBG. Capture RTCP stream at both endpoints. Capture VoIP performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active VoIP calls.

Scenario 1.1.4b – Attempt to Transmit ETS Traffic when Normal Traffic is at Provisioned Maximum

- Pre-test
 - Provision Originating Access Network SBG to support X3 (TBD) kbps throughput for normal traffic.
 - Either calculate the maximum throughput for ETS traffic or provision Originating Access Network SBG to support X4 (TBD) kbps throughput for ETS traffic.
 - Provision Originating Access Network Traffic Generator to generate “X3/100” sessions.
- Attempt to place multiple ETS VoIP calls between endpoints so that ETS maximum bearer throughput is exceeded. Some calls should complete and some should be rejected.
- Capture VoIP endpoint signaling with SBG. Capture RTCP stream at both endpoints. Capture VoIP performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active VoIP calls.

4.2.2.3.3 Observable Results

The SBG should reject session requests that exceed the maximum bearer thresholds.

The delay, jitter and loss statistics generated by the SBG for each call leg shall be captured and accumulated into “end-to-end” values. These “end-to-end” values shall be compared with the values captured in the RTCP streams. These values should provide an acceptable call QoS.

The delay, jitter and loss statistics for calls occurring when the SBC is supporting more throughput than the maximum throughput for normal calls should be worse than the statistics when the SBC is only supporting the maximum throughput for normal calls. However, these “worse” values should still provide an acceptable call QoS.

4.2.2.3.3.1 Pass/Fail Criteria

The SBG should demonstrate the observable results.

4.2.2.3.3.2 Message Flows

Message flows between the SBG and NOC are defined in Scenario 1.1.1.

4.2.2.3.3.3 Trace Capture

Capture the RTCP streams on VLANs 110, 140, 210 and 240. Capture the alarms, CDRs and / or MIBs generated by the SBGs and sent to the NOC.

4.2.2.3.4 Known Issues

None.

4.3 Scenario 1.2 – Priority Video Testing

The Scenario 1.2 tests repeat the Scenario 1.1 tests for video sessions. Of interest is whether the SBG provides statistics only for the delay, jitter and loss of the audio “channel” or provides separate statistics for both the audio and video “channels” or provides one set of statistics combining both the audio and video channels. These tests will allow analysis of the implications of the SBC approach taken on evaluating network performance.

This scenario consists of four tests:

- Scenario 1.2.1 –SBG Video Performance Reporting Under “No Traffic Load”
- Scenario 1.2.2 –SBG Video Performance Reporting Under Link Traffic Congestion
- Scenario 1.2.3 –SBG Video Session Establishment Congestion
- Scenario 1.2.4 –SBG Video Bearer Throughput Congestion

4.3.1 SBG Video Performance Reporting Testing

4.3.1.1 Purpose

These test cases demonstrate the ability of an SBG to report the performance of a video call traversing the SBG.

4.3.1.2 Scenario 1.1.1 – Video SBG Performance Reporting Under “No Traffic Load”

4.3.1.2.1 Test Setup and Procedure

- Test configuration as per Section 4.1.
- Traffic Generators turned off.
- Place a video call between endpoints.
- Capture RTCP stream at both endpoints. Capture video performance statistics generated by SBGs and reported to the NOC.
- Note that an SBG typically generates delay, jitter and loss statistics for each call leg that traverses the SBG.

4.3.1.2.2 Observable Results

The message formats and protocols used to transmit data will be captured and analyzed.

There should be minimal delay, jitter and loss for the video call as reported by the RTCP streams by the two endpoints. The delay, jitter and loss statistics from the RTCP streams shall be captured at the end of the call.

The delay, jitter and loss statistics generated by the SBG for each call leg shall be captured and accumulated into “end-to-end” values. These “end-to-end” values shall be compared with the values captured in the RTCP streams. If the SBG reports delay, jitter and loss statistics captured from the RTCP stream traversing the SBC, these values shall be compared against the statistics reported by the endpoints.

4.3.1.2.2.1 Pass/Fail Criteria

The SBG statistics should closely track the RTCP statistics reported by the endpoints.

4.3.1.2.2.2 Message Flows

The SBG will periodically push MIB operational measurements to the NOC using SNMP. Alerts are immediately pushed to the NOC via SNMP. CDR records may be pushed immediately to the NOC, or may be batched and sent to the NOC. The protocol used depends on the type of push. If the SBGs can be provisioned to support the MSF MI-6 IA, the tests will be repeated using this IA.

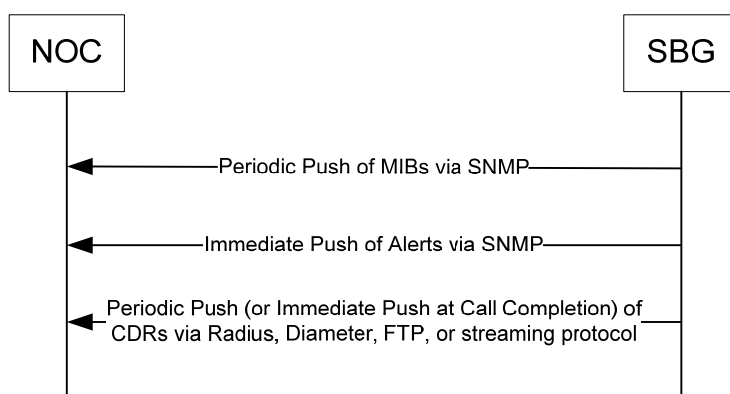


Figure 4-4. SBG to NOC Message Flows

4.3.1.2.3 Trace Capture

Capture the RTCP streams on VLANs 110, 140, 210 and 240. Capture the CDRs and / or MIBs generated by the SBGs and sent to the NOC.

4.3.1.2.4 Known Issues

None.

4.3.1.3 Scenario 1.2.2 –SBG Video Performance Reporting Under Link Traffic Congestion

4.3.1.3.1 Test Setup and Procedure

- Test configuration as per Section 4.1.

Scenario 1.2.2a – Originating Access Link Congestion

- Traffic Generator set to congest VLAN 120.
- Place a video call between endpoints.
- Capture RTCP stream at both endpoints. Capture video performance statistics generated by SBGs and reported to the NOC.

Scenario 1.2.2b –Core Network Congestion

- Traffic Generator set to congest VLANs 612 and 613.
- Place a video call between endpoints.

- Capture RTCP stream at both endpoints. Capture video performance statistics generated by SBGs and reported to the NOC.

Scenario 1.2.2c – Terminating Access Link Congestion

- Traffic Generator set to congest VLAN 210.
- Place a video call between endpoints.
- Capture RTCP stream at both endpoints. Capture video performance statistics generated by SBGs and reported to the NOC.

4.3.1.3.2 Observable Results

There should be appreciable delay, jitter and loss for the video call as reported by the RTCP streams by the two endpoints. The delay, jitter and loss statistics from the RTCP streams shall be captured at the end of the call.

The delay, jitter and loss statistics generated by the SBG for each call leg shall be captured and accumulated into “end-to-end” values. These “end-to-end” values shall be compared with the values captured in the RTCP streams. If the SBG reports delay, jitter and loss statistics captured from the RTCP stream traversing the SBC, these values shall be compared against the statistics reported by the endpoints.

4.3.1.3.2.1 Pass/Fail Criteria

The SBG statistics should closely track the RTCP statistics reported by the endpoints.

4.3.1.3.2.2 Message Flows

Message flows between the SBG and NOC are defined in Scenario 1.2.1.

4.3.1.3.3 Trace Capture

Capture the RTCP streams on VLANs 110, 140, 210 and 240. Capture the CDRs and / or MIBs generated by the SBGs and sent to the NOC.

4.3.1.3.4 Known Issues

None.

4.3.2 SBG Video Performance Testing

4.3.2.1 Purpose

These test cases demonstrate the ability of an SBG to impact the performance of a video call traversing the SBG.

4.3.2.2 Scenario 1.2.3 –SBG Video Session Establishment Congestion

4.3.2.2.1 Purpose

This test is designed to exercise the load-management capabilities of the SBGs, prioritization within those management operations and the ability of SBGs to report the results of such management. The SBGs will be configured with a maximum number of sessions that they can support. The test will exceed that number, and verify that the SBGs reject or shed sessions, based on session priority and on their defined behaviours, and that they accurately report the statistics describing these actions.

4.3.2.2.2 Test Setup and Procedure

- Test configuration as per Section 4.1.

Scenario 1.2.3a – Attempt to Establish More Sessions than Provisioned Maximum

- Provision Originating Access Network SBG to support X5 (TBD) normal sessions and “X5 + 1” ETS sessions.
- Provision Originating Access Network Traffic Generator to generate “X5 – 1” sessions.
- Attempt to place a video call between endpoints, Call should complete.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End the video call.
- Attempt to place a video call between endpoints. Call should complete.
- Attempt to place a second video call between endpoints while first call is active. Since this call exceeds the limit allowed by the SBG, it should be rejected.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active video call.
- Attempt to place three ETS video calls between endpoints. Two calls should complete and one call should be rejected, since ETS calls should be exempt from the normal session limit but be subject to the ETS session limit.
- Capture endpoint signaling with SBG. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active video calls.

Scenario 1.2.3b – Attempt to Establish Sessions when SBG is Throttling Sessions

- Pre-test
 - Provision Originating Access Network SBG to support X6 (TBD) sessions. Determine resources used for these sessions (e.g., 25% CPU utilization).
 - Provision the SBG’s lowest congestion level (e.g., throttling mechanism) to kick-in using a lower resource value. Provision SBG highest congestion level to kick-in at the resource utilization for X6 sessions.
- Provision Originating Access Network Traffic Generator to generate “X6 – 1” sessions. Verify that not all sessions are being established
- Attempt to place a normal video call between endpoints. Call should be rejected.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC.
- Attempt to place multiple ETS video calls between endpoints. Some calls should complete and some calls should be rejected, depending on the SBG’s congestion level.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active video calls.

4.3.2.2.3 Observable Results

Session requests that exceed the allowable maximum for simultaneous sessions should be rejected. ETS calls will be exempted from the maximum limit for normal calls, but will be subject to the maximum limit for ETS calls.

SBGs typically have multiple congestion levels. At each level, the SBGs apply congestion control mechanisms (e.g., shedding call requests) to ensure the SBGs can continue to function. At the lower congestion levels, normal session requests are shed while ETS calls are exempt from shedding. At the highest congestion level, both normal and ETS session requests are shed.

4.3.2.2.3.1 Pass/Fail Criteria

The SBG should demonstrate the observable results.

4.3.2.2.3.2 Message Flows

A session that cannot be established should receive a 486 response, as shown in Figure 4-5.

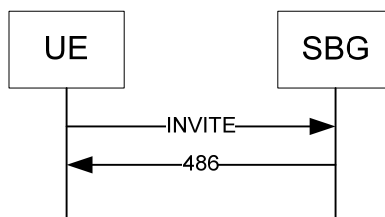


Figure 4-5 – Session Request Rejected

Message flows between the SBG and NOC are defined in Scenario 1.2.1.

4.3.2.2.4 Trace Capture

Capture the endpoint signaling on VLANs 110. Capture the alarms, CDRs and / or MIBs generated by the Originating Access Network SBG and sent to the NOC.

4.3.2.2.5 Known Issues

None.

4.3.2.3 Scenario 1.2.4 –SBG Video Bearer Throughput Congestion

4.3.2.3.1 Purpose

This test is designed to exercise the load-management capabilities of the SBGs, prioritization within those management operations and the ability of SBGs to report the results of such management. The SBGs will be configured with a maximum bearer throughput for normal calls that they can support (e.g., in bytes per second). For ETS calls, the SBGs may either calculate a higher maximum value (based on the maximum for normal calls), or may allow a higher maximum value to be provisioned. The test will exceed that capacity, and verify that the SBGs reject or shed sessions, based on session priority and on their defined behaviors, and that they accurately report the statistics describing these actions.

4.3.2.3.2 Test Setup and Procedure

- Test configuration as per Section 4.1.

Scenario 1.2.4a – Attempt to Transmit More Traffic than Provisioned Maximum for Normal Calls

- Pre-test
 - Provision Originating Access Network SBG to support X7 (TBD) kbps bearer throughput for normal traffic.
 - Provision Originating Access Network Traffic Generator to generate calls with B1 kbps bearer traffic.
 - Provision Originating Access Network Traffic Generator to generate “(X7/B1) – 1” sessions.
- Attempt to place a normal video call between endpoints. Call should complete.
- Capture endpoint signaling with SBG. Capture RTCP stream at both endpoints. Capture performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End the video call.
- Attempt to place a normal video call between endpoints. Call should complete.

- Attempt to place a second normal video call between endpoints while first call is active. Since this call exceeds the bearer throughput limit allowed by the SBG, it should be rejected.
- Capture endpoint signaling with SBG. Capture RTCP stream at both endpoints. Capture performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active video calls.

Scenario 1.2.4b – Attempt to Transmit ETS Traffic when Normal Traffic is at Provisioned Maximum

- Pre-test
 - Provision Originating Access Network SBG to support X7 (TBD) kbps throughput for normal traffic.
 - Either calculate the maximum throughput for ETS traffic or provision Originating Access Network SBG to support X8 (TBD) kbps throughput for ETS traffic.
 - Provision Originating Access Network Traffic Generator to generate “X7/B1” sessions.
- Attempt to place multiple ETS video calls between endpoints so that ETS maximum bearer throughput is exceeded. Some calls should complete and some should be rejected.
- Capture endpoint signaling with SBG. Capture RTCP stream at both endpoints. Capture performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active video calls.

4.3.2.3.3 *Observable Results*

The SBG should reject session requests that exceed the maximum bearer thresholds.

The delay, jitter and loss statistics generated by the SBG for each call leg shall be captured and accumulated into “end-to-end” values. These “end-to-end” values shall be compared with the values captured in the RTCP streams. These values should provide an acceptable call QoS.

The delay, jitter and loss statistics for calls occurring when the SBC is supporting more throughput than the maximum throughput for normal calls should be worse than the statistics when the SBC is only supporting the maximum throughput for normal calls. However, these “worse” values should still provide an acceptable call QoS.

4.3.2.3.3.1 *Pass/Fail Criteria*

The SBG should demonstrate the observable results.

4.3.2.3.3.2 *Message Flows*

Message flows between the SBG and NOC are defined in Scenario 1.2.1.

4.3.2.3.3.4 *Trace Capture*

Capture the RTCP streams on VLANs 110, 140, 210 and 240. Capture the alarms, CDRs and / or MIBs generated by the SBGs and sent to the NOC.

4.3.2.3.3.5 *Known Issues*

None.

4.4 Scenario 1.3 – i3 Forum QoS KPI Testing

This scenario consists of one test:

- Scenario 1.3.1 – SBGs Ability to Support i3 Forum Performance KPIs

4.4.1 Scenario 1.3.1 – SBCs Ability to Support i3 Forum Performance KPIs

4.4.1.1 Purpose

The i3 Forum, in its document *Service value and process of measuring QoS KPIs (Release 1.0) May 2010* defines the following measurements:

- Service Parameters
 - Network Efficiency Ratio (NER) – Call Establishment
 - Answer Seizures Ratio (ASR) – Called Party Answers
 - Average Length of Call (ALOC)
 - Post Gateway Ringing Delay (PGRD)
 - Mean Opinion Score (MOSCQE) / R-factor
- Call Attributes
 - Calling Line Identification (CLI) Transparency – Transmission of received CLI across network
- Transport Parameters
 - Round-Trip Delay
 - Jitter
 - Packet Loss

The Service Parameters are calculated from information found in CDRs. The Call Attribute KPI is measured by a probe, while the Transport Parameters can be obtained from both CDRs and probes.

The SBGs used for testing incorporate call handling functions analogous to a Proxy – Call Session Control Function (P-CSCF) and generate CDRs.

The purposes of Scenario 1.3 are:

- To determine if the SBCs' CDR contain sufficient information to calculate the i3 Forum Service Parameters and Transport Parameters,
- To determine if the information in the CDRs is sufficient to determine if an “error condition” was received from a downstream network or was generated by the functional entity creating the CDR,
- To determine how the CDR information tracks with the information generated by end-to-end probes under various congestion scenarios.

4.4.1.2 Test Setup and Procedures

For each of the Scenario 1 tests, capture the CDRs and probe information. Run the calculations identified in the i3 Forum document. Identify discrepancies and missing elements.

4.4.1.3 Observable Results

Identify what values are included in each SBG. Identify parameters that can be used to correlate CDRs from different SBGs.

4.4.1.4 Pass/Fail Criteria

The statistics necessary to support the i3 Forum KPIs can be successfully collected by the SBG and transmitted to the NOC.

4.4.1.5 Message Flows

Message flows between the SBG and NOC are defined in Scenarios 1.1.1 and 1.2.1.

4.4.1.6 Trace Captures

Trace captures are covered under Scenario 1 tests.

4.4.1.7 Known Issues

CDRs typically have more information than is of interest to a Service Provider. Service Providers and vendors create proprietary filter applications to strip “unwanted” information from CDRs before the CDRs are passed to “back end” systems. Thus successful demonstration of the i3 Forum KPIs does not mean Service Providers’ systems are currently capable of generating these KPIs.

Some information that may be useful for analysis of errors is not captured in CDRs, but in Operational Measurements (OMs).

Service Providers may not share CDRs, but only select information from (filtered) billing records to aid in reconciliation.

5 Scenario 2 Test Cases – Multi-Domain Performance Management Measurement

5.1 Test Configuration

The network configuration for the Scenario 2 tests is shown in Figure 5-1. Scenario 2 testing requires:

- Endpoints which can establish Voice over Internet Protocol (VoIP) and Video calls
- Traffic Generators to congest various links and Functional Entities (FEs)
- SBGs which generate alarms, call detail records (CDRs) and management information blocks (MIBs)
- Other FEs which generate alarms and MIBs
- A NOC which can view and act on alarms, CDRs and MIBs. In general, the NOC will use an Element Management System (EMS) and / or Network Management System (NMS) for this capability
- Other network analysis equipment (e.g., Sniffer, Wireshark)

Note that access routers are used to connect the endpoints on VLAN 110 to the P-CSCF on VLAN 140, and to connect the endpoints on VLAN 210 to the P-CSCF on VLAN 240. The SBGs are configured to pass traffic between VLANs 140 and 613 and between VLANs 240 and 623. An IPsec tunnel connects the two SBGs.

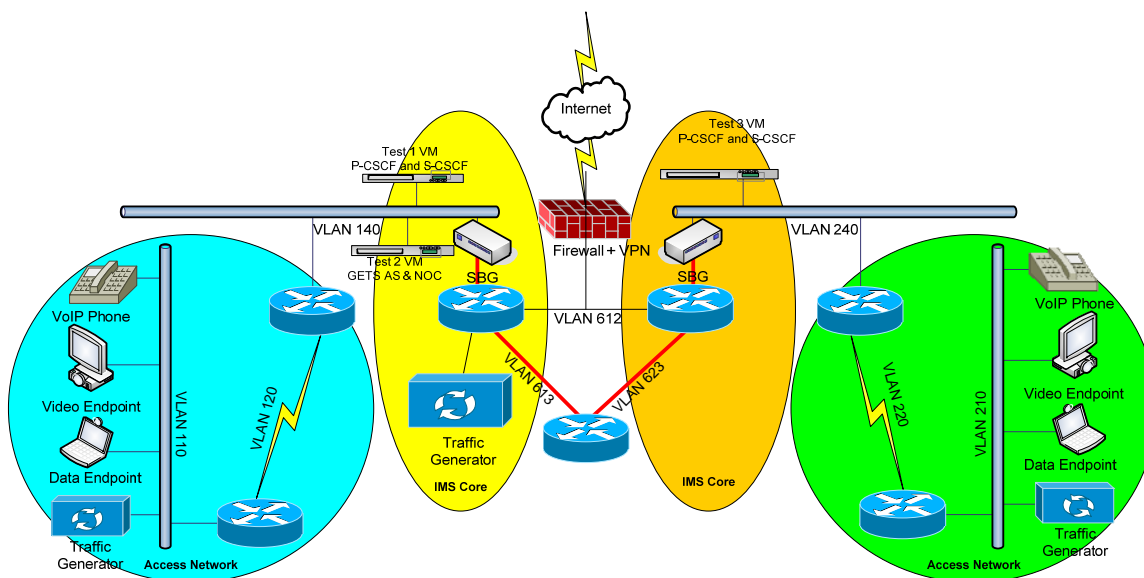


Figure 5-1 – Scenario 2 Test Configuration

5.2 Scenario 2.1 – Network-to-Network Interface Provisioning

This scenario consists of one test:

- Scenario 2.1.1 – SBG NNI Provisioning with “Encrypted” IPsec Tunnel

Service Providers may place both ETS and normal traffic on a single IPsec tunnel, or may place ETS traffic and normal traffic on separate IPsec tunnels. The following tests assume a single IPsec tunnel for all traffic.

5.2.1 SBG NNI Provisioning

5.2.1.1 Purpose

This case tests the SBG-to-SBG interface, including encryption capabilities and RPH handling.

5.2.1.2 Scenario 2.1.1 – SBG NNI Provisioning with “Encrypted” IPsec Tunnel

5.2.1.2.1 Test Setup and Procedure

- Test configuration as per Section 5.1.
- Pre-test
 - Configure SBGs to transmit both normal and ETS traffic across the same IPsec tunnel.
 - Configure Core domain of each SBG to recognize ETS traffic. Configure SBGs to strip the “Require: RPH” parameter from the ETS INVITE messages received from the Core and sent to the NNI, and to insert the “Require: RPH” parameter to the ETS INVITE messages received from the NNI and sent to their Core.¹

¹ If the “Require: RPH” parameter is left in the INVITE and the receiving SBG does not support the RPH parameter, then the receiving SBG will reject the SIP INVITE with a 420 (Bad Extension) response. If the receiving SBG supports the RPH parameter but does not understand the ets namespace, then the receiving SBG will reject the SIP INVITE with a 417 (Unknown Resource Priority) response. If there is no “Require: RPH” parameter in the SIP INVITE, then according to the normal rules of RFC 3261, Section 8.2.2, if the

- “Configure” IPsec tunnel to encrypt traffic across the tunnel.
- Validate Encryption is working
 - Wireshark is not provisioned with IPsec tunnel keys.
 - Traffic Generators turned off.
 - Place a normal VoIP call between one pair of endpoints.
 - Place an ETS VoIP call between another pair of endpoints
 - Capture signaling on VLANs 140, 240 and 613.
- Analyze IPsec traffic
 - Wireshark is provisioned with IPsec tunnel keys.
 - Traffic Generators turned off.
 - Place a normal VoIP call between one pair of endpoints.
 - Place an ETS VoIP call between another pair of endpoints
 - Capture signaling on VLANs 140, 240 and 613.

5.2.1.2.2 Observable Results

Both normal and ETS signaling should be using the same IPsec tunnel.
 The SBGs should be stripping Require:RPH from ETS INVITEs sent across the IPsec tunnel.
 The SBGs should be inserting Require:RPH to ETS INVITEs received from the IPsec tunnel.

5.2.1.2.2.1 Pass/Fail Criteria

The observable results should be met.

5.2.1.2.2.2 Message Flows

Figure 5.2 shows the flows for INVITEs for normal and ETS calls.

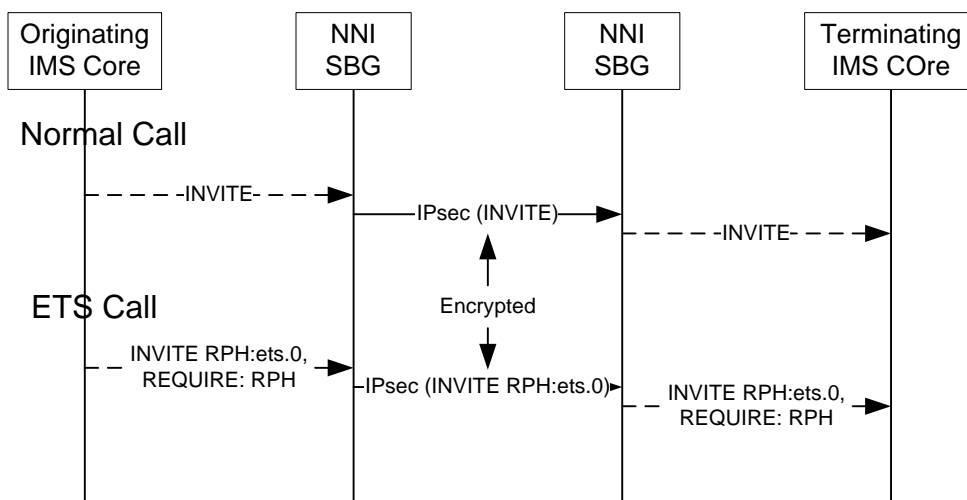


Figure 5-2 – Normal Call and ETS Call INVITEs

SBG does not understand the RPH header field, it will ignore the RPH header field, continue processing the SIP INVITE, and propagate the RPH header field downstream unchanged.

5.2.1.2.3 *Trace Capture*

Capture the signaling on VLANs 140, 240 and 613.

5.2.1.2.4 *Known Issues*

There are no known protocol issues.

5.3 Scenario 2.2 – SBG NNI Testing

This scenario consists of four tests:

- Scenario 2.2.1 –SBG NNI Voice and Video Performance Reporting Under “No Traffic Load”
- Scenario 2.2.2 –SBG NNI Voice and Video Performance Reporting For IPsec Tunnels Where the Link Supporting the IPsec Tunnel is Congested
- Scenario 2.2.3 –SBG NNI Voice and Video Session Establishment Congestion
- Scenario 2.2.4 –SBG NNI Voice and Video Bearer Throughput Congestion

5.3.1 SBG NNI Performance Reporting Testing

5.3.1.1 *Purpose*

These test cases demonstrate the ability of an SBG to report the performance of a video call traversing the NNI.

5.3.1.2 *Scenario 2.2.1 –SBG NNI Voice and Video Performance Reporting Under “No Traffic Load”*

5.3.1.2.1 *Test Setup and Procedure*

- Test configuration as per Section 5.1.
- Pre-test
 - Configure SBGs to transmit both normal and ETS traffic across the same IPsec tunnel.
 - Configure Core domain of each SBG to recognize ETS traffic. Configure SBGs to strip the “Require: RPH” parameter from the ETS INVITE messages received from the Core and sent to the NNI, and to insert the “Require: RPH” parameter to the ETS INVITE messages received from the NNI and sent to their Core.
 - “Configure” IPsec tunnel to encrypt traffic across the tunnel.
- Traffic Generators turned off.

Scenario 2.2.1a – Placing a Voice Call Under No Traffic Load

- Place a voice call between endpoints.
- Capture RTCP stream at both endpoints. Capture voice performance statistics generated by SBGs and reported to the NOC, focusing on the statistics associated with the NNI.
- Note that an SBG typically generates delay, loss and jitter statistics for each call leg that traverses the SBG.

Scenario 2.2.1b – Placing a Video Call Under No Traffic Load

- Place a video call between endpoints.

- Capture RTCP stream at both endpoints. Capture video performance statistics generated by SBGs and reported to the NOC, focusing on the statistics associated with the NNI.
- Note that an SBG typically generates delay, loss and jitter statistics for each call leg that traverses the SBG.

5.3.1.2.2 Observable Results

The message formats and protocols used to transmit data will be captured and analyzed.

There should be minimal delay, jitter and loss for the voice and video calls as reported by the RTCP streams by the two endpoints. The delay, jitter and loss statistics from the RTCP streams shall be captured at the end of the call.

The delay, jitter and loss statistics generated by the SBGs for each call leg shall be captured and accumulated into “end-to-end” values. These “end-to-end” values shall be compared with the values captured in the RTCP streams. If the SBG reports delay, jitter and loss statistics captured from the RTCP stream traversing the SBC, these values shall be compared against the statistics reported by the endpoints. Finally, check the statistics generated for the NNI leg to see if they are meaningful.

5.3.1.2.2.1 Pass/Fail Criteria

The SBG statistics should closely track the RTCP statistics reported by the endpoints.

5.3.1.2.2.2 Message Flows

The SBG will periodically push MIB operational measurements to the NOC using SNMP. Alerts are immediately pushed to the NOC via SNMP. CDR records may be pushed immediately to the NOC, or may be batched and sent to the NOC. The protocol used depends on the type of push. If the SBGs can be provisioned to support the MSF MI-6 IA, the tests will be repeated using this IA.

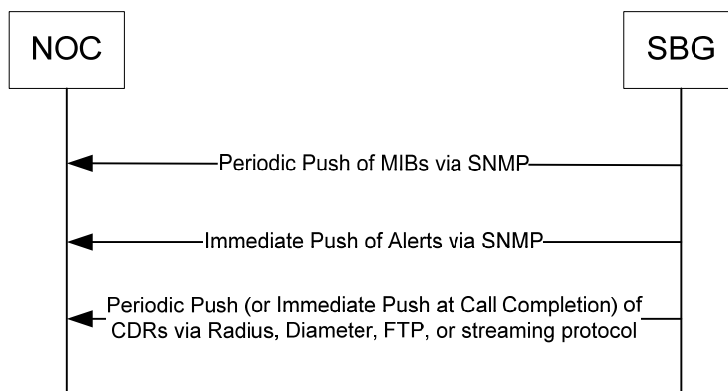


Figure 5-3 – SBG to NOC Message Flows

5.3.1.2.3 Trace Capture

Capture the RTCP streams on VLANs 140 and 240. Capture the CDRs and / or MIBs generated by the SBGs and sent to the NOC.

5.3.1.2.4 Known Issues

None.

5.3.1.3 Scenario 2.2.2 –SBG NNI Voice and Video Performance Reporting for IPsec Tunnels Where the Link Supporting the IPsec Tunnel is Congested

If routers are not configured to provide sufficient assured bandwidth to an IPsec tunnel traversing the router, then all traffic in the IPsec tunnel can be impacted by link congestion. This is demonstrated in the following case.

5.3.1.3.1 *Test Setup and Procedure*

- Test configuration as per Section 5.1.
- Pre-test
 - Configure SBGs to transmit both normal and ETS traffic across the same IPsec tunnel.
 - Configure Core domain of each SBG to recognize ETS traffic. Configure SBGs to strip the “Require: RPH” parameter from the ETS INVITE messages received from the Core and sent to the NNI, and to insert the “Require: RPH” parameter to the ETS INVITE messages received from the NNI and sent to their Core.
 - “Configure” IPsec tunnel to encrypt traffic across the tunnel.

Scenario 2.2.2a – Normal Voice Call

- Traffic Generator set to congest a link supporting the IPsec tunnel.
- Place a normal voice call between endpoints.
- Capture RTCP stream at both endpoints. Capture voice performance statistics generated by SBGs and reported to the NOC.

Scenario 2.2.2b – ETS Voice Call

- Traffic Generator set to congest a link supporting the IPsec tunnel.
- Place an ETS voice call between endpoints.
- Capture RTCP stream at both endpoints. Capture voice performance statistics generated by SBGs and reported to the NOC.

Scenario 2.2.2c – Normal Video Call

- Traffic Generator set to congest a link supporting the IPsec tunnel.
- Place a normal video call between endpoints.
- Capture RTCP stream at both endpoints. Capture video performance statistics generated by SBGs and reported to the NOC.

Scenario 2.2.2d – ETS Video Call

- Traffic Generator set to congest a link supporting the IPsec tunnel.
- Place an ETS video call between endpoints.
- Capture RTCP stream at both endpoints. Capture video performance statistics generated by SBGs and reported to the NOC.

5.3.1.3.2 *Observable Results*

The message formats and protocols used to transmit data will be captured and analyzed. The delay, jitter and loss statistics from the RTCP streams shall be captured at the end of the call.

The delay, jitter and loss statistics generated by the SBGs for each call leg shall be captured and accumulated into “end-to-end” values. These “end-to-end” values shall be compared with the values captured in the RTCP streams.

There should be appreciable delay, jitter and loss for both normal and ETS calls as reported by the RTCP streams by the two endpoints.

5.3.1.3.2.1 *Pass/Fail Criteria*

The SBG statistics should closely track the RTCP statistics reported by the endpoints.

5.3.1.3.2.2 Message Flows

Message flows between the SBG and NOC are defined in Scenario 2.2.1.

5.3.1.3.3 Trace Capture

Capture the RTCP streams on VLANs 140 and 240. Capture the CDRs and / or MIBs generated by the SBGs and sent to the NOC.

5.3.1.3.4 Known Issues

None.

5.3.2 SBG NNI Performance Testing

5.3.2.1 Purpose

These test cases demonstrate the ability of an SBG to impact the performance of a video call traversing the NNI.

5.3.2.2 Scenario 2.2.3 –SBG NNI Voice and Video Session Establishment Congestion

5.3.2.2.1 Purpose

This test is designed to exercise the load-management capabilities of the SBGs, prioritization within those management operations and the ability of SBGs to report the results of such management, specifically in the case where the SBG is using IPsec for NNI communications. The SBGs will be configured with a maximum number of sessions. The test will exceed that number, and verify that the SBGs reject or shed sessions, based on session priority and on their defined behaviors, and that they accurately report the statistics describing these actions. The purpose of this test is to determine how these parameters are impacted by creation of an IPsec tunnel between the SBGs.

5.3.2.2.2 Test Setup and Procedure

- Test configuration as per Section 5.1.
- Pre-test
 - Configure SBGs to transmit both normal and ETS traffic across the same IPsec tunnel.
 - Configure Core domain of each SBG to recognize ETS traffic. Configure SBGs to strip the “Require: RPH” parameter from the ETS INVITE messages received from the Core and sent to the NNI, and to insert the “Require: RPH” parameter to the ETS INVITE messages received from the NNI and sent to their Core.
 - “Configure” IPsec tunnel to encrypt traffic across the tunnel.

Scenario 2.2.3a – Attempt to Establish More Voice Sessions than Provisioned Maximum

- Provision SBGs to support X9 (TBD) normal sessions and “X9 + 1” ETS sessions across the NNI.
- Provision Originating Access Network Traffic Generator to generate “X9 – 1” sessions.
- Attempt to place a voice call between endpoints. Call should complete.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End the voice call.
- Attempt to place a voice call between endpoints. Call should complete.
- Attempt to place a second voice call between endpoints while first call is active. Since this call exceeds the limit allowed by the SBG, it should be rejected.

- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End active voice call.
- Attempt to place three ETS voice calls between endpoints. Two calls should complete and one call should be rejected, since ETS calls should be exempt from the normal session limit but be subject to the ETS session limit.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active voice calls.

Scenario 2.2.3b – Attempt to Establish Voice Sessions when SBG is Throttling Sessions

- Pre-test
 - Provision Originating Access Network SBG to support X10 (TBD) sessions across NNI. Determine resources used for these sessions (e.g., 25% CPU utilization).
 - Provision the SBG's lowest congestion level (e.g., throttling mechanism) to kick-in using a lower resource value. Provision SBG highest congestion level to kick-in at the resource utilization for X10 sessions.
- Provision Originating Access Network Traffic Generator to generate "X10 – 1" sessions. Verify that not all sessions are being established
- Attempt to place a normal voice call between endpoints. Call should be rejected.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC.
- Attempt to place multiple ETS voice calls between endpoints. Some calls should complete and some calls should be rejected, depending on the SBG's congestion level.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End active voice calls.

Scenario 2.2.3c – Attempt to Establish More Video Sessions than Provisioned Maximum

- Provision SBGs to support X11 (TBD) normal sessions and "X11 + 1" ETS sessions across the NNI.
- Provision Originating Access Network Traffic Generator to generate "X11 – 1" sessions.
- Attempt to place a video call between endpoints. Call should complete.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End the video call.
- Attempt to place a video call between endpoints. Call should complete.
- Attempt to place a second video call between endpoints while first call is active. Since this call exceeds the limit allowed by the SBG, it should be rejected.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End active video call.
- Attempt to place three ETS video calls between endpoints. Two calls should complete and one call should be rejected, since ETS calls should be exempt from the normal session limit but be subject to the ETS session limit.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the Originating Access Network SBG and reported to the NOC. End active video calls.

Scenario 2.2.3d – Attempt to Establish Video Sessions when SBG is Throttling Sessions

- Pre-test
 - Provision Originating Access Network SBG to support X12 (TBD) sessions across NNI. Determine resources used for these sessions (e.g., 25% CPU utilization).
 - Provision the SBG’s lowest congestion level (e.g., throttling mechanism) to kick-in using a lower resource value. Provision SBG highest congestion level to kick-in at the resource utilization for X12 sessions.
- Provision Originating Access Network Traffic Generator to generate “X12 – 1” sessions. Verify that not all sessions are being established
- Attempt to place a normal video call between endpoints. Call should be rejected.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC.
- Attempt to place multiple ETS video calls between endpoints. Some calls should complete and some calls should be rejected, depending on the SBG’s congestion level.
- Capture endpoint signaling with SBGs. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End active video calls.

5.3.2.2.3 Observable Results

Session requests that exceed the allowable maximum for simultaneous sessions should be rejected. ETS calls will be exempted from the maximum limit for normal calls, but will be subject to the maximum limit for ETS calls.

SBGs typically have multiple congestion levels. At each level, the SBGs apply congestion control mechanisms (e.g., shedding call requests) to ensure the SBGs can continue to function. At the lower congestion levels, normal session requests are shed while ETS calls are exempt from shedding. At the highest congestion level, both normal and ETS session requests are shed.

5.3.2.2.3.1 Pass/Fail Criteria

The SBG should demonstrate the observable results.

5.3.2.2.3.2 Message Flows

A session that cannot be established should receive a 486 response, as shown in Figure 5-4.

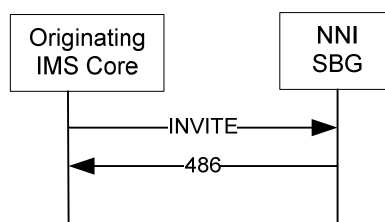


Figure 5-4 – Session Request Rejected

5.3.2.2.4 Trace Capture

Capture the endpoint signaling on VLANs 140. Capture the alarms, CDRs and / or MIBs generated by the SBGs and sent to the NOC.

5.3.2.2.5 Known Issues

None.

5.3.2.3 Scenario 2.2.4 –SBG NNI Voice and Video Bearer Throughput Congestion

5.3.2.3.1 Purpose

Many SBGs can be provisioned with a maximum throughput between domains that ensures that the SBG does not go into resource overload. If an SBG can support multiple priority queues feeding an IPsec tunnel, then the following test can be run. In this case, the SBGs will be configured with a maximum bearer throughput for normal calls that they can support (e.g., in bytes per second). For ETS calls, the SBGs may either calculate a higher maximum value (based on the maximum for normal calls), or may allow a higher maximum value to be provisioned. The test will exceed that capacity, and verify that the SBGs reject or shed sessions, based on session priority and on their defined behaviors, and that they accurately report the statistics describing these actions.

5.3.2.3.2 Test Setup and Procedure

- Test configuration as per Section 5.1.
- Pre-test
 - Configure SBGs to transmit both normal and ETS traffic across the same IPsec tunnel.
 - Configure Core domain of each SBG to recognize ETS traffic. Configure SBGs to strip the “Require: RPH” parameter from the ETS INVITE messages received from the Core and sent to the NNI, and to insert the “Require: RPH” parameter to the ETS INVITE messages received from the NNI and sent to their Core.
 - “Configure” IPsec tunnel to encrypt traffic across the tunnel.

Scenario 1.2.4a – Attempt to Transmit More Traffic than Provisioned Maximum for Normal Voice Calls

- Pre-test
 - Provision Originating Access Network SBG to support X13 (TBD) kbps bearer throughput for normal traffic.
 - Provision Originating Access Network Traffic Generator to generate calls with B1 kbps bearer traffic.
 - Provision Originating Access Network Traffic Generator to generate “(X13/B1) – 1” sessions.
- Attempt to place a normal voice call between video endpoints. Call should complete
- Capture endpoint signaling with SBGs. Capture RTCP stream at both endpoints. Capture performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End the voice call.
- Attempt to place a normal voice call between endpoints. Call should complete.
- Attempt to place a second normal voice call between endpoints while first call is active. Since this call exceeds the bearer throughput limit allowed by the SBG, it should be rejected.
- Capture endpoint signaling with SBGs. Capture RTCP stream at both endpoints. Capture performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End active voice calls.

Scenario 1.2.4b – Attempt to Transmit ETS Voice Traffic when Normal Voice Traffic is at Provisioned Maximum

- Pre-test
 - Provision Originating Access Network SBG to support X13 (TBD) kbps throughput for normal traffic.
 - Either calculate the maximum throughput for ETS traffic or provision SBG to support X14 (TBD) kbps throughput for ETS traffic.
 - Provision Originating Access Network Traffic Generator to generate more than “X13/B1” sessions.
- Attempt to place multiple ETS voice calls between endpoints so that ETS maximum bearer throughput is exceeded. Some calls should complete and some should be rejected.
- Capture endpoint signaling with SBGs. Capture RTCP stream at both endpoints. Capture performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End active voice calls.

Scenario 1.2.4c – Attempt to Transmit More Traffic than Provisioned Maximum for Normal Video Calls

- Pre-test
 - Provision Originating Access Network SBG to support X14 (TBD) kbps bearer throughput for normal traffic.
 - Provision Originating Access Network Traffic Generator to generate calls with B2 kbps bearer traffic.
 - Provision Originating Access Network Traffic Generator to generate “(X14/B2) – 1” sessions.
- Attempt to place a normal video call between video endpoints. Call should complete
- Capture endpoint signaling with SBGs. Capture RTCP stream at both endpoints. Capture performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End the video call.
- Attempt to place a normal video call between endpoints. Call should complete.
- Attempt to place a second normal video call between endpoints while first call is active. Since this call exceeds the bearer throughput limit allowed by the SBG, it should be rejected.
- Capture endpoint signaling with SBGs. Capture RTCP stream at both endpoints. Capture performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End active video calls.

Scenario 1.2.4d – Attempt to Transmit ETS Traffic when Normal Video Traffic is at Provisioned Maximum

- Pre-test
 - Provision Originating Access Network SBG to support X14 (TBD) kbps throughput for normal traffic.
 - Either calculate the maximum throughput for ETS traffic or provision SBG to support X15 (TBD) kbps throughput for ETS traffic.
 - Provision Originating Access Network Traffic Generator to generate more than “X14/B2” sessions.

- Attempt to place multiple ETS video calls between endpoints so that ETS maximum bearer throughput is exceeded. Some calls should complete and some should be rejected.
- Capture endpoint signaling with SBGs. Capture RTCP stream at both endpoints. Capture performance statistics generated by SBGs and reported to the NOC. Capture alarms, CDRs and MIBs generated by the SBGs and reported to the NOC. End active video calls.

5.3.2.3.3 Observable Results

The SBG should reject session requests that exceed the maximum bearer thresholds.

The delay, jitter and loss statistics generated by the SBG for each call leg shall be captured and accumulated into “end-to-end” values. These “end-to-end” values shall be compared with the values captured in the RTCP streams. These values should provide an acceptable call QoS.

The delay, jitter and loss statistics for calls occurring when the SBC is supporting more throughput than the maximum throughput for normal calls should be worse than the statistics when the SBC is only supporting the maximum throughput for normal calls. However, these “worse” values should still provide an acceptable call QoS.

5.3.2.3.3.1 Pass/Fail Criteria

The SBG should demonstrate the observable results.

5.3.2.3.3.2 Message Flows

Message flows between the SBG and NOC are defined in Scenario 2.2.1.

5.3.2.3.3.4 Trace Capture

Capture the RTCP streams on VLANs 140 and 240. Capture the alarms, CDRs and / or MIBs generated by the SBGs and sent to the NOC.

5.3.2.3.3.5 Known Issues

None.

5.4 Scenario 2.3 – Priority Data Testing

All packets do not traverse SBGs when going between networks (e.g., hypertext transfer protocol (HTTP) packets across a firewall). However, there is a need to provide ETS processing at all functional elements found at network boundaries. This scenario focuses on the capabilities of Data Border Gateways (DBGs), such as firewalls.

This scenario consists of three tests:

- Scenario 2.3.1 – Dynamic Provisioning of the Data Border Gateway (DBG) to Support Priority Data
- Scenario 2.3.2 – DBG Performance Reporting Under “No Traffic Load”
- Scenario 2.3.3 – DBG Performance Reporting Under Internet Traffic Congestion

5.4.1 Test Configuration

The network configuration for the Scenario 2.3 tests is shown in Figure 5-5. Scenario 2.3 testing requires:

- Endpoints which can establish data transactions, such as web browsing and file transfers
- Traffic Generators to congest various links and Functional Entities (FEs)
- Data Border Gateways (DBGs) which generate alarms and management information blocks (MIBs)
- Other FEs which generate alarms and MIBs

- A NOC which can view and act on alarms and MIBs. In general, the NOC will use an Element Management System (EMS) and / or Network Management System (NMS) for this capability
- An ETS Application Server, which can set policy in the DBGs
- Other network analysis equipment (e.g., Sniffer, Wireshark)

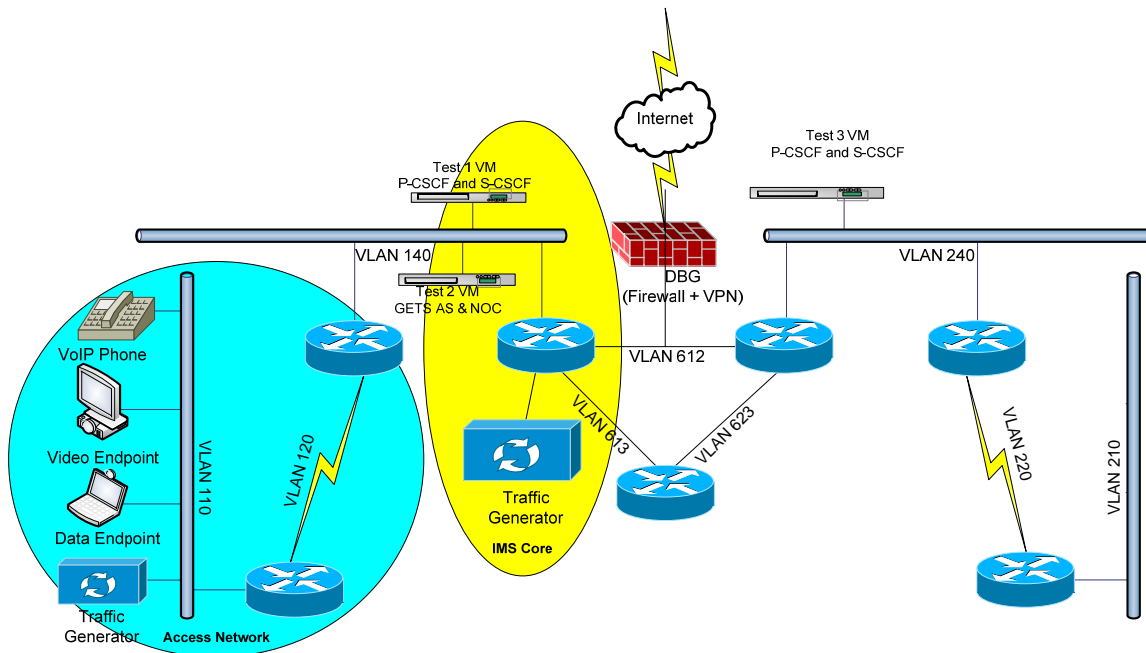


Figure 5-5 – Scenario 2.3 Test Configuration

5.4.2 Scenario 2.3.1 – Dynamic Provisioning of the Data Border Gateway (DBG) to Support Priority Data

5.4.2.1 Purpose

This test case demonstrates the ability of a DBG to manipulate normal and ETS traffic differently.

5.4.2.2 Test Setup and Procedure

- Test configuration as per Section 5.4.1.
- Traffic Generators turned off.
- One endpoint establishes an HTTPS session with ETS Application Server to request priority browsing with servers on the Internet.²
- ETS Application Server pushes policy to DBG to have packets received from the Internet destined to Endpoint A to have a DSCP value of AF41.
- A second endpoint browses the Internet.
- Capture packets on VLAN 612.

² For this test case, the ETS Application Server (AS) recognizes the endpoint as an ETS endpoint and provides priority. However, mechanisms have been defined to allow any endpoint send a “best effort” request to the ETS AS. The ETS AS will set up an https session (with priority communications) to the endpoint to collect identification and security information. After authenticating the endpoint, the ETS AS would push policy to the appropriate network devices to provide priority data transport.

5.4.2.3 Observable Results

Packets destined to the second endpoint should be marked with a BE DSCP value. Packets destined to the first endpoint should be marked with an AF41 DSCP value.

5.4.2.4 Pass/Fail Criteria

The observable results should be met.

5.4.2.5 Message Flows

The NOC will push policy to the DBG at the beginning and end of a data “session.” The DBG will periodically push MIB operational measurements to the NOC using SNMP. Alerts are immediately pushed to the NOC via SNMP. Alerts are immediately pushed to the NOC via SNMP. CDRs are periodically pushed (or immediately pushed at call completion) to the NOC via Radius, Diameter, FTP, or streaming protocol.

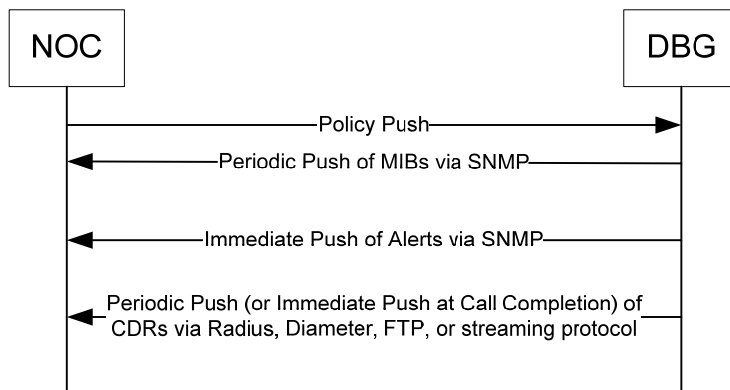


Figure 5-6 – NOC to DBG Messaging

The DBG will change the DSCP markings on ETS packets going into the Internet and received from the Internet, as shown in Figure 5-7.

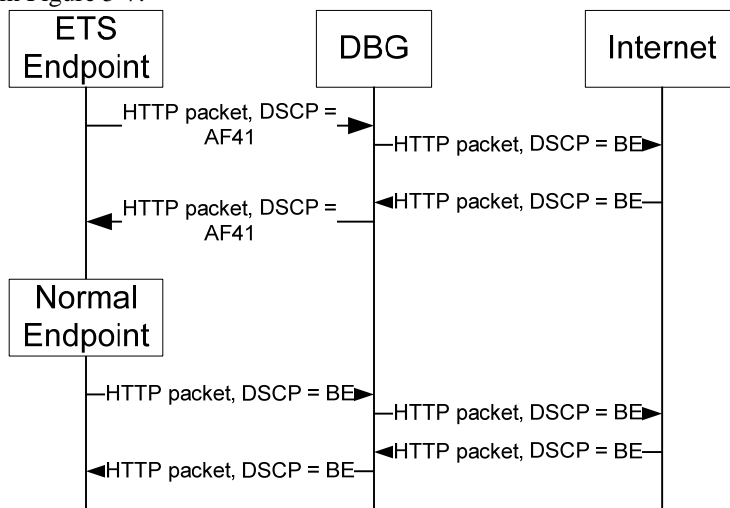


Figure 5-7 – Bearer Packet Marking

5.4.2.6 Trace Capture

Capture packets on VLAN 612.

5.4.2.7 Known Issues

None.

5.4.3 DBG Performance Reporting Testing

5.4.3.1 Purpose

These test cases demonstrate the ability of a DBG to report the performance of a “data session” traversing the DBG.

5.4.3.2 Scenario 2.3.2 – DBG Performance Reporting Under “No Traffic Load”

5.4.3.2.1 Test Setup and Procedure

- Test configuration as per Section 5.4.1.
- Traffic Generators turned off.
- Establish a “data session” between Endpoint A and a server on the Internet.
- Capture data packets on VLAN 612. Capture performance statistics generated by DBGs and reported to the NOC. It is desirable that the DBG capture statistics for each “call leg” (i.e., VLAN 612 and the Internet connection to the DBG).

5.4.3.2.2 Observable Results

DBG statistics.

5.4.3.2.2.1 Pass/Fail Criteria

The DBG is able to report on packets sent, packets received, and packets dropped for each “call leg.”

5.4.3.2.2.2 Message Flows

Not applicable.

5.4.3.2.3 Trace Capture

Capture packets on VLAN 612. Capture the MIBs generated by the DBG and sent to the NOC.

5.4.3.2.4 Known Issues

None.

5.4.3.3 Scenario 2.3.3 – DBG Performance Reporting Under Link Traffic Congestion

5.4.3.3.1 Test Setup and Procedure

- Test configuration as per Section 5.4.1.
- Traffic Generator set to congest VLAN 612.
- Establish a “data session” between Endpoint A and a server on the Internet.
- Capture data packets on VLAN 612 filtered by Endpoint’s A IP address. Capture performance statistics generated by DBGs and reported to the NOC. It is desirable that the DBG capture statistics for each “call leg” (i.e., VLAN 612 and the Internet connection to the DBG).

5.4.3.3.2 Observable Results

DBG statistics.

5.4.3.3.2.1 Pass/Fail Criteria

The DBG is able to report on packets sent, packets received, and packets dropped for each “call leg.”

5.4.3.3.2 Message Flows

Not applicable.

5.4.3.3.3 Trace Capture

Capture data packets on VLAN 612 filtered by Endpoint's A IP address. Capture the MIBs generated by the DBG and sent to the NOC.

5.4.3.3.4 Known Issues

None.

5.5 Scenario 2.4 – i3 Forum QoS KPI Testing

Whereas Scenario 1.3 focused on the reporting of statistics from a single access router, Scenario 2.4 focuses on the reporting of statistics between two network side SBGs. The measurements between the pair of network SBGs will be compared to see if they are consistent.

Scenario 2.4 consists of one test:

- Scenario 2.4.1 – SBGs Ability to Support i3 Forum Performance KPIs

5.5.1 Scenario 2.4.1 – SBGs Ability to Support i3 Forum Performance KPIs

5.5.1.1 Purpose

The i3 Forum, in its document *Service value and process of measuring QoS KPIs (Release 1.0) May 2010* defines the following measurements:

- Service Parameters
 - Network Efficiency Ration (NER) – Call Establishment
 - Answer Seizures Ratio (ASR) – Called Party Answers
 - Average Length of Call (ALOC)
 - Post Gateway Ringing Delay (PGRD)
 - Mean Opinion Score (MOSCQE) / R-factor
- Call Attributes
 - Calling Line Identification (CLI) Transparency – Transmission of received CLI across network
- Transport Parameters
 - Round-Trip Delay
 - Jitter
 - Packet Loss

The Service Parameters are calculated from information found in CDRs. The Call Attribute KPI is measured by a probe, while the Transport Parameters can be obtained from both CDRs and probes.

The SBGs used for testing incorporate call handling functions analogous to a Proxy – Call Session Control Function (P-CSCF) and generate CDRs.

The purposes of Scenario 2.4 are:

- To determine if the SBCs' CDR contain sufficient information to calculate the i3 Forum Service Parameters and Transport Parameters

- To determine if the information in the CDRs is sufficient to determine if an “error condition” was received from a downstream network or was generated by the functional entity creating the CDR
- To determine how the CDR information tracks with the information generated by end-to-end probes under various congestion scenarios.
- To determine if the two network SBGs provide consistent metrics for the NNI they are supporting.

5.5.1.2 Test Setup and Procedures

For each of the Scenario 2.2 tests, capture the CDRs and probe information. Run the calculations identified in the i3 Forum document. Identify discrepancies and missing elements. Compare the results of the two SBGs for each test to see if the metrics are consistent across the NNI.

5.5.1.3 Observable Results

Identify what values are included in each SBG. Identify parameters that can be used to correlate CDRs from different SBGs.

5.5.1.4 Pass/Fail Criteria

The statistics necessary to support the i3 Forum KPIs can be successfully collected by the SBG and transmitted to the NOC. If the SBG supports the MI-6 IA specification, the statistics necessary to support the i3 Forum KPIs can be successfully collected by the SBG and transmitted to the NOC using this specification. The metrics produced by each SBG supporting the NNI are consistent for each test case.

5.5.1.5 Message Flows

Message flows between the SBG and NOC are defined in Scenario 2.2.1.

5.5.1.6 Trace Captures

Trace captures are covered under Scenario 2 tests.

5.5.1.7 Known Issues

CDRs typically have more information than is of interest to a Service Provider. Service Providers and vendors create proprietary filter applications to strip “unwanted” information from CDRs before the CDRs are passed to “back end” systems. Thus successful demonstration of the i3 Forum KPIs does not mean Service Providers’ systems are currently capable of generating these KPIs.

Some information that may be useful for analysis of errors is not captured in CDRs, but in Operational Measurements (OMs).

Service Providers may not share CDRs, but only select information from (filtered) billing records to aid in reconciliation.

6 Future Tests

As equipment for testing becomes available, the NCS is interested in conducting the following Network Robustness tests:

- Disruption testing of virtual machines and cloud computing environments, since this represents the direction of future application processing.
- Policy and Charging Rules Function (PCRF) testing. How knowledgeable is the PCRF about the state of the access network? Is this information timely? Can this information be used by a NOC to make better decisions about handling ETS calls?