Network Working Group
INTERNET-DRAFT
Expires in: October 2005

Scott Poretsky
Reef Point Systems

Shankar Rao
Qwest Communications

July 2005

Methodology for Benchmarking Accelerated Stress with Operational Security <draft-ietf-bmwg-acc-bench-meth-opsec-00.txt>

Status of this Memo

ABSTRACT
Routers in an operational network are simultaneously configured with multiple protocols and security policies while forwarding traffic and being managed. To accurately benchmark a router for deployment it is necessary that the router be tested in these simultaneous operational conditions, which is known as Stress Testing. This document provides the Methodology for performing Stress Benchmarking of networking devices when subjected to instability as described in [7].

Descriptions of test topology, benchmarks and reporting format are provided in addition to procedures for conducting various test cases. This methodology is based upon the accelerated stress methodology guidelines [6] and is to be used with the companion terminology document [4].

Table of Contents

1. Introduction

Routers in an operational network are simultaneously configured with multiple protocols and security policies while forwarding traffic and being managed. To accurately benchmark a router for deployment it is necessary that the router be tested in these simultaneous operational conditions, which is known as Stress Testing. This document provides the Methodology for performing Stress Benchmarking of networking devices when subjected to instability as described in the OpSec Requirements for Service Providers [7]. Descriptions of Test Topology, Benchmarks and Reporting Format are provided in addition to procedures for conducting various test cases. This methodology is based upon the accelerated stress methodology guidelines [6] and is to be used with the companion terminology document [4].

2. Existing definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [8]. RFC 2119 defines the use of these key words to help make the intent of standards track documents as clear as possible. While this document uses these keywords, this document is not a standards track document.

Terms related to Accelerated Stress Benchmarking are defined in [4].

3. Test Setup

Test Setup, Test Topologies, Considerations, and Reporting Format MUST be as described in [6].

4. Test Cases

4.1 Restart Under Load

Objective
The purpose of this test is to benchmark the performance of the DUT during restart when stress conditions are applied.

Procedure
1. Report Configuration Set
2. Begin Startup Conditions with the DUT
3. Establish Configuration Sets with the DUT
4. Report benchmarks (for stability)
5. Restart DUT. This marks the beginning on the recovery period.
6. Report benchmarks (for recovery)
7. Optional - Change Configuration Set and/or Instability Conditions for next iteration

NOTE 1: Restart via the DUT's Command Line Interface rather than power cycle is typically more stressful than power cycle since hardware can maintain state.
NOTE 2: Instability Conditions are not applied for this test case.

Results
DUT should re-establish all control protocol sessions and have a Recovery Time [4] that is not infinite.

4.2 Destination Control Processor

Objective
The purpose of this test is to benchmark the performance of the DUT during stress conditions when traffic is destined for the Control Processor of the DUT.

Procedure
1. Report Configuration Set
2. Begin Startup Conditions with the DUT
3. Start Configuration Sets with the DUT, except Data Plane Configuration Set
4. Report benchmarks (for stability)
5. Apply Instability Conditions
6. Send offered load at maximum forwarding rate of DUT interfaces to all DUT interfaces. Traffic MUST be configured so that the offered load has a destination address that is the DUT's central control processor
7. Report benchmarks (for instability)
8. Stop applying all Instability Conditions, including data traffic
9. Report benchmarks (for recovery)
10. Optional - Change Configuration Set and/or Instability Conditions for next iteration

Results
Results will vary with specific vendor implementations.
It is possible that significant session loss is observed.

4.3 Destination Control Processor with Rate-Limiting

Objective
The purpose of this test is to benchmark the performance of the DUT during stress conditions when traffic is destined for the Control processor of the DUT.

Procedure
1. Report Configuration Set
2. Apply policy filter to rate-limit traffic arriving at the Central Processor to be only 1% of the offered load.
3. Begin Startup Conditions with the DUT
4. Start Configuration Sets with the DUT, except Data Plane Configuration Set
5. Report benchmarks (for stability)
6. Apply Instability Conditions
7. Send offered load at maximum forwarding rate of DUT interfaces to all DUT interfaces. Traffic MUST be configured so that the offered load has a destination address that is the DUT's central control processor
8. Report benchmarks (for instability)
9. Stop applying all Instability Conditions, including data traffic
10. Report benchmarks (for recovery)

11. Optional - Change Configuration Set and/or Instability
    Conditions for next iteration

Results
Results will vary with specific vendor implementations. There should b
no session loss observed.

4.4 Destination Interfaces

Objective
The purpose of this test is to benchmark the performance
of the DUT during stress conditions when traffic is destined for
the interfaces of the DUT.

Procedure
1. Report Configuration Set
2. Begin Startup Conditions with the DUT
3. Start Configuration Sets with the DUT, except Data Plane
   Configuration Set
4. Report benchmarks (for stability)
5. Apply Instability Conditions
6. Send offered load at maximum forwarding rate of DUT interfaces
   to all DUT interfaces. Traffic MUST be configured so that the
   offered load has destination addresses of the interfaces receiving
   traffic.
7. Report benchmarks (for instability)
8. Stop applying all Instability Conditions, including data traffic
9. Report benchmarks (for recovery)
10. Optional - Change Configuration Set and/or Instability
    Conditions for next iteration

Results
Results will vary with specific vendor implementations.
There should be no session loss observed.

4.5 DoS Attack

Objective
The purpose of this test is to benchmark the performance of the
DUT during stress conditions while experiencing a DoS attack.

Procedure
1. Report Configuration Set
2. Begin Startup Conditions with the DUT
3. Establish Configuration Sets with the DUT
4. Report benchmarks (for stability)

5. Apply Instability Conditions
6. Initiate DoS Attack against DUT. It is RECOMMENDED that the SYN Flood attack be used for the DoS attack.
7. Report benchmarks (for instability)
8. Stop applying all Instability Conditions
9. Report benchmarks (for recovery)
10. Optional - Change Configuration Set and/or Instability Conditions for next iteration

Results
DUT should be able to defend against DoS attack without additional packet loss or session loss.

5. Security Considerations

Documents of this type do not directly affect the security of the Internet or of corporate networks as long as benchmarking is not performed on devices or systems connected to operating networks.

6. Normative References

[1] Bradner, S., Editor, "Benchmarking Terminology for Network Interconnection Devices", RFC 1242, July 1991.

[2] Mandeville, R., "Benchmarking Terminology for LAN Switching Devices", RFC 2285, June 1998.

[3] Bradner, S. and McQuaid, J., "Benchmarking Methodology for Network Interconnect Devices", RFC 2544, March 1999.

[4] Poretsky, S. and Rao, S., "Terminology for Accelerated Stress Benchmarking", draft-ietf-bmwg-acc-bench-term-05, work in progress, July 2005.

[5] Poretsky, S., "Benchmarking Terminology for IGP Data Plane Route Convergence", draft-ietf-bmwg-igp-dataplane-conv-term-05, work in progress, July 2005.

[6] Poretsky, S. and Rao, S., "Methodology Guidelines for Accelerated Stress Benchmarking", draft-ietf-bmwg-acc-bench-meth-03, work in progress, July 2005.

[7] RFC 3871 "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure. G. Jones, Ed.. IETF, September 2004.

[8] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

7. Informative References

[NANOG25] "Core Router Evaluation for Higher Availability", Scott Poretsky, NANOG 25, June 8, 2002, Toronto, CA.

[IEEECQR] "Router Stress Testing to Validate Readiness for Network Deployment", Scott Poretsky, IEEE CQR 2003.

[CONVMETH] Poretsky, S., "Benchmarking Methodology for IGP Data Plane Route Convergence", draft-ietf-bmwg-igp-dataplane-conv-meth-05, work in progress, July 2005.

8. Author's Address

Scott Poretsky
Reef Point Systems
8 New England Executive Park
Burlington, MA 01803
USA

Phone: + 1 781 395 5090
EMail: sporetsky@reefpoint.com

Shankar Rao
1801 California Street
8th Floor
Qwest Communications
Denver, CO 80202
USA
Phone: + 1 303 437 6643
Email: shankar.rao@qwest.com

Intellectual Property Statement

Disclaimer of Warranty

Copyright Statement