Network Working Group
INTERNET-DRAFT
Expires in: October 2005

Scott Poretsky
Quarry Technologies

Shankar Rao
Qwest Communications

February 2005

Methodology for Accelerated Stress Benchmarking

<draft-ietf-bmwg-acc-bench-meth-02.txt>

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. Descriptions of Test Topology, Benchmarks and Reporting Format are provided in addition to procedures for

conducting various test cases. The methodology is to be used with the companion terminology document [4].

Table of Contents

1. Introduction

Router testing benchmarks have consistently been made in a monolithic fashion wherein a single protocol or behavior is measured in an isolated environment. It is important to know the limits for a networking device's behavior for each protocol in isolation, however this does not produce a reliable benchmark of the device's behavior in an operational network.

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 to test that router in operational conditions by simultaneously configuring and scaling network protocols and security policies, forwarding traffic, and managing the device. It is helpful to accelerate these network operational conditions with Instability Conditions [4] so that the networking devices are stress tested.

This document provides the Methodology for performing Stress Benchmarking of networking devices. Descriptions of Test Topology, Benchmarks and Reporting Format are provided in addition to procedures for conducting various test cases. The methodology is to be used with the companion terminology document [4].

Stress Testing of networking devices provides the following benefits:

1. Evaluation of multiple protocols enabled simultaneously as configured in deployed networks
2. Evaluation of System and Software Stability
3. Evaluation of Manageability under stressful conditions
4. Identification of Buffer Overflow conditions
5. Identification of Software Coding bugs such as:
    a. Memory Leaks
    b. Suboptimal CPU Utilization
    c. Coding Logic

These benefits produce significant advantages for network operations:

1. Increased stability of routers and protocols
2. Hardened routers to DoS attacks
3. Verified manageability under stress
4. Planning router resources for growth and scale

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 [Br97]. 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

3.1 Test Topologies

Figure 1 shows the physical configuration to be used for the methodologies provided in this document. The number of interfaces between the tester and DUT will scale depending upon the number of control protocol sessions and traffic forwarding interfaces. A separate device may be required to externally manage the device in the case that the test equipment does not support such functionality. Figure 2 shows the logical configuration for the stress test methodologies. Each plane may be emulated by single or multiple test equipment.

3.2 Test Considerations

The Accelerated Stress Benchmarking test can be applied in service provider test environments to benchmark DUTs under stress in an environment that is reflective of an operational network. A particular Configuration Set is defined and the DUT is benchmarked using this configuration set and the Instability Conditions. Varying Configuration Sets and/or Instability Conditions applied in an iterative fashion can

provide an accurate characterization of the DUT
to help determine future network deployments.

```
                                 ___________
                                |   DUT     |
                             ___|Management |
                            |   |           |
                            |    -----------
                           \/
                      ___________
                     |           |
                     |    DUT    |
                |--->|           |<---|
         xN     |     -----------     |    xN
     interfaces |                     | interfaces
                |     ___________     |
                |    |           |    |
                |--->|   Tester  |<---|
                     |           |
                      -----------

                Figure 1. Physical Configuration



         ___________             ___________
        |  Control  |           | Management|
        |   Plane   |___     ___|   Plane   |
        |           |   |   |   |           |
         -----------    |   |    -----------
                       \/  \/
                      ___________               ___________
                     |           |             | Security  |
                     |           |<------------|   Plane   |
                     |    DUT    |             |           |
                |--->|           |<---|         -----------
                |     -----------     |
                |                     |
                |     ___________     |
                |    |   Data    |    |
                |--->|   Plane   |<---|
                     |           |
                      -----------

                Figure 2. Logical Configuration
```

3.3 Reporting Format

Each methodology requires reporting of information for test repeatability when benchmarking the same or different devices. The information that are the Configuration Sets, Instability Conditions, and Benchmarks, as defined in [4]. Example reporting formats for each are provided below.

3.3.1 Configuration Sets

Example Routing Protocol Configuration Set-

PARAMETER	UNITS
BGP	Enabled/Disabled
Number of EBGP Peers	Peers
Number of IBGP Peers	Peers
Number of BGP Route Instances	Routes
Number of BGP Installed Routes	Routes
MBGP	Enabled/Disabled
Number of MBGP Route Instances	Routes
Number of MBGP Installed Routes	Routes
IGP	Enabled/Disabled
IGP-TE	Enabled/Disabled
Number of IGP Adjacencies	Adjacencies
Number of IGP Routes	Routes
Number of Nodes per Area	Nodes

Example MPLS Protocol Configuration Set-

PARAMETER	UNITS
MPLS-TE	
Number of Ingress Tunnels	Tunnels
Number of Mid-Point Tunnels	Tunnels
Number of Egress Tunnels	Tunnels
LDP	
Number of Sessions	Sessions
Number of FECs	FECs

Example Multicast Protocol Configuration Set-

PARAMETER	UNITS
PIM-SM	Enabled/Disabled
RP	Enabled/Disabled
Number of Multicast Groups	Groups
MSDP	Enabled/Disabled

Example Data Plane Configuration Set-

PARAMETER	UNITS
Traffic Forwarding	Enabled/Disabled
Aggregate Offered Load	bps (or pps)
Number of Ingress Interfaces	number
Number of Egress Interfaces	number
TRAFFIC PROFILE	
Packet Size(s)	bytes
Packet Rate(interface)	array of packets per second

Number of Flows	number
Encapsulation(flow)	array of encapsulation type

Management Configuration Set-

PARAMETER	UNITS
SNMP GET Rate	SNMP Gets/minute
Logging	Enabled/Disabled
Protocol Debug	Enabled/Disabled
Telnet Rate	Sessions/Hour
FTP Rate	Sessions/Hour
Concurrent Telnet Sessions	Sessions
Concurrent FTP Session	Sessions
Packet Statistics Collector	Enabled/Disabled
Statistics Sampling Rate	X:1 packets

Security Configuration Set -

PARAMETER	UNITS
Packet Filters	Enabled/Disabled
Number of Filters For-Me	number
Number of Filter Rules For-Me	number
Number of Traffic Filters	number
Number of Traffic Filter Rules	number
SSH	Enabled/Disabled
Number of simultaneous SSH sessions	number
RADIUS	Enabled/Disabled
TACACS	Enabled/Disabled

3.3.2 Instability Conditions

PARAMETER	UNITS
Interface Shutdown Cycling Rate	interfaces per minute
BGP Session Flap Rate	sessions per minute
BGP Route Flap Rate	routes per minutes
IGP Route Flap Rate	routes per minutes
LSP Reroute Rate	LSP per minute
Overloaded Links	number
Amount Links Overloaded	% of bandwidth
FTP Rate	Mb/minute
IPsec Session Loss	sessions per minute
Filter Policy Changes	policies per hour
SSH Session Restart	SSH sessions per hour
Telnet Session Restart	Telnet session per hour

3.3.3 Benchmarks

PARAMETER	UNITS	PHASE
Stable Aggregate Forwarding Rate	pps	Startup
Stable Latency	seconds	Startup
Stable Session Count	sessions	Startup
Unstable Aggregate Forwarding Rate	pps	Instability
Degraded Aggregate Forwarding Rate	pps	Instability
Ave. Degraded Aggregate Forwarding Rate	pps	Instability
Unstable Latency	seconds	Instability
Unstable Uncontrolled Sessions Lost	sessions	Instability

Recovered Aggregate Forwarding Rate	pps	Recovery
Recovered Latency	seconds	Recovery
Recovery Time	seconds	Recovery
Recovered Uncontrolled Sessions Lost	sessions	Recovery

It is RECOMMENDED that Aggregate Forwarding Rates, Latencies, and Session Losses be measured at one-second intervals. These same benchmarks can also be used as Variability Benchmarks reported as the differences between the Benchmarks for multiple iterations with the same DUT. For the purpose of the Variability Benchmarks, A more complete characterization of the DUT would be to apply multiple test iterations for the same Configuration Sets and Instability Conditions, measure the Variability Benchmarks, and then vary the Configuration Set and/or Instability Conditions.

4. Test Cases

4.1 Failed Primary EBGP Peer

Objective
The purpose of this test is to benchmark the performance of the DUT during stress conditions when losing an EBGP Peer from which most FIB routes have been learned.

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. Remove link to EBGP peer with most FIB routes. This SHOULD be achieved by losing physical layer connectivity with a local fiber pull. Loss of the peering session SHOULD cause the DUT to withdraw 100,000 or greater routes.
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
It is expected that there will be significant packet loss until the DUT converges from the lost EBGP link. Other DUT operation should be stable without session loss or sustained packet loss. Recovery time should not be infinite.

4.2 Establish New EBGP Peer

Objective
The purpose of this test is to benchmark the performance of the DUT during stress conditions when establishing a new EBGP Peer from which routes are learned.

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. Configure a new EBGP peering session at DUT and peering router. Physical and Data Link Layer connectivity SHOULD already exist to perform this step. Establishment of the peering session MUST result in the DUT learning 100,000 or greater routes from the BGP peer and advertising 100,000 or greater routes to the BGP peer
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
It is expected that there will be zero packet loss as the DUT learns the new routes. Other DUT operation should be stable without session loss or sustained packet loss.

4.3 BGP Route Explosion

Objective
The purpose of this test is to benchmark the performance of the DUT during stress conditions when there is BGP Route Explosion experienced in the network.

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. Advertise 1M BGP routes to the DUT from a single EBGP neighbor.
7. Report benchmarks (for instability)
8. Stop applying all Instability Conditions, including BGP route advertisement.
9. Report benchmarks (for recovery)

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

Results
It is expected that there will be no additional packet loss from the advertisement of routes from the BGP neighbor. Other DUT operation should be stable without session loss.

4.4 BGP Policy Configuration

Objective
The purpose of this test is to benchmark the performance of the DUT during stress conditions when there is continuous reconfiguration of BGP Policy at the DUT.

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. Configure BGP Policy on the DUT for each established neighbor. The BGP Policy SHOULD filter 25% of the routes learned from that neighbor. Note that the specific policy configuration to achieve the filtering may be device specific.
7. Every 30 minutes remove the BGP Policy configuration and then configure it gain so that it is reapplied.
8. Report benchmarks (for instability)
9. Stop applying all Instability Conditions, including Policy changes
10. Report benchmarks (for recovery)
11. Optional - Change Configuration Set and/or Instability Conditions for next iteration

Results
It is expected that there will be no packet loss resulting from the continuous configuration and removal of BGP Policy for BGP neighbors. Other DUT operation should be stable without session loss.

4.5 Persistent BGP Flapping

Objective
The purpose of this test is to benchmark the performance of the DUT during stress conditions when flapping BGP Peering sessions for an infinite period.

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. Repeatedly flap an IBGP and an EBGP peering session.
   This SHOULD be achieved by losing physical layer connectivity via a local interface shutdown/no shutdown every 180 seconds with a delay of 10 seconds between the shut and no shut.
   The loss of the EBGP peering session MUST cause the DUT to withdraw 100,000 or greater routes that are re-learned when the session re-establishes.   Route Flap Dampening SHOULD NOT be enabled.
7. Report benchmarks (for instability)
8. Stop applying all Instability Conditions, including flapping
9. Report benchmarks (for recovery)
10. Optional - Change Configuration Set and/or Instability Conditions for next iteration

Results
It is expected that there will be significant packet loss from repeated Convergence Events. Other DUT operation should be stable without session loss. Recovery time should not be infinite.

4.6 BGP Route Flap Dampening

Objective
The purpose of this test is to benchmark the performance of the DUT during stress conditions when flapping BGP Peering sessions for an infinite period and route flap dampening is enabled.

Procedure
1. Report Configuration Set
2. Configure Route Flap Dampening on the DUT with DEFAULT parameter values.
3. Begin Startup Conditions with the DUT
4. Establish Configuration Sets with the DUT
5. Report benchmarks (for stability)
6. Apply Instability Conditions
7. Repeatedly flap an IBGP and an EBGP peering session.
   This SHOULD be achieved by losing physical layer connectivity via a local interface shutdown/no shutdown every 180 seconds with a delay of 10 seconds between the shut and no shut.
   The loss of the EBGP peering session MUST cause the DUT to withdraw 100,000 or greater routes that are re-learned when the session re-establishes.
8. Report benchmarks (for instability)
9. Stop applying all Instability Conditions
10. Report benchmarks (for recovery)
11. Optional - Change Route Flap Dampening parameter values
12. Optional - Change Configuration Set and/or Instability Conditions for next iteration

Results
It is expected that there will be significant packet loss from repeated Convergence Events and flap dampening. Other DUT operation should be stable without session loss. Recovery time should not be infinite.

4.7 Nested Convergence Events [5]

Objective
The purpose of this test is to benchmark the performance of the DUT during stress conditions when flapping BGP Peering sessions causes Nested Convergence Events.

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. Repeatedly flap an IBGP and an EBGP peering session. This SHOULD be achieved by losing physical layer connectivity via a local interface shutdown/no shutdown every 10 seconds with a delay of 1 second between the shut and no shut. The loss of the EBGP peering session MUST cause the DUT to withdraw 100,000 or greater routes that are re-learned when the session re-establishes. Route Flap Dampening SHOULD NOT be enabled.
7. Report benchmarks (for instability)
8. Stop applying all Instability Conditions, including flapping
9. Report benchmarks (for recovery)
10. Optional - Change Configuration Set and/or Instability Conditions for next iteration

Results
It is expected that there will be significant packet loss from Nested Convergence Events. New Other DUT operation should be stable without session loss. Recovery time should not be infinite.

4.8 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.

4.9 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.

4.10 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 be
no session loss observed.

4.11 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.

4.12 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, February 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, February 2005.

[5] Poretsky, S., "Benchmarking Terminology for IGP Data Plane

Route Convergence", draft-ietf-bmwg-igp-dataplane-conv-term-05,
work in progress, February 2005.

7. Informative References

[RFC3871] RFC 3871 "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure. G. Jones, Ed.. IETF, September 2004.

[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, February 2005.

8. Author's Address

Scott Poretsky
Quarry Technologies
8 New England Executive Park
Burlington, MA 01803
USA

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

Shankar Rao
950 17th Street
Suite 1900
Qwest Communications
Denver, CO 80210
USA
Phone: + 1 303 437 6643
Email: shankar.rao@qwest.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.