Network Working Group
INTERNET-DRAFT
Expires in: January 2005

Scott Poretsky
Quarry Technologies

Shankar Rao
Qwest Communications

July 2004

Methodology for Accelerated Stress Benchmarking
<draft-ietf-bmwg-acc-bench-meth-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. 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 [6].

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 [6] so that the networking devices are stress tested.

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 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

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 [6].

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 RFC 2119.

Terms related to Accelerated Stress Benchmarking are defined in [6].

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.

```
                             ___________
                            |   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

3.2 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.

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 [6]. 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 minute
SSH Session Re-Start	SSH sessions per minute

3.3.3 Benchmarks

PARAMETER	UNITS
Stable Aggregate Forwarding Rate	pps
Stable Session Count	sessions
Unstable Aggregate Forwarding Rate	pps
Degraded Aggregate Forwarding Rate	pps
Average Degraded Aggregate Forwarding Rate	pps
Unstable Uncontrolled Sessions Lost	sessions
Recovered Aggregate Forwarding Rate	pps
Recovery Time	seconds
Recovered Uncontrolled Sessions Lost	sessions

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
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 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 from a single EBGP 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 no additional packet loss from the advertisement of duplicate routes from a single peer. Other DUT operation should be stable without session loss. Recovery time should not be infinite.

4.3 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
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 from repeated convergence events. Other DUT operation should be stable without session loss. Recovery time should not be infinite.

4.4 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
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. Recovery time should be immediate. Open issue is definition of DoS Attack for the purpose of this test. COuld any DoS Attack be used? Should DoS Attack be defined?

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

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

[6] Poretsky, S. and Rao, S., "Terminology for Accelerated Stress Benchmarking", draft-ietf-bmwg-acc-bench-term-03, work in progress, July 2004.

7. 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.

Disclaimer of Warranty

Copyright Statement