Methodology Guidelines for
Accelerated Stress Benchmarking
<draft-ietf-bmwg-acc-bench-meth-09.txt>

Intellectual Property Rights (IPR) statement:
    By submitting this Internet-Draft, each author represents that any
    applicable patent or other IPR claims of which he or she is aware
    have been or will be disclosed, and any of which he or she becomes
    aware will be disclosed, in accordance with Section 6 of BCP 79.

ABSTRACT
    Routers in an operational network are configured with multiple
    protocols and security policies while simultaneously forwarding
    traffic and being managed. To accurately benchmark a router for
    deployment it is necessary to test the router in a lab environment
    under accelerated conditions, which is known as Stress Testing.
    This document provides the Methodology Guidelines for performing
    Accelerated Stress Benchmarking of networking devices.
    The methodology is to be used with the companion terminology
    document [4]. These guidelines can be used as the basis for
    additional methodology documents that benchmark stress conditions
    for specific network technologies.

   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
   configured with multiple protocols and security policies while
   simultaneously 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
   [5]. 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 reflects conditions found in
   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.

   For the management plane SNMP Gets SHOULD be performed
   continuously. Management sessions SHOULD be open
   simultaneously and be repeatedly open and closed using
   access protocols such as telnet and SSH. Open management
   sessions SHOULD have valid and invalid configuration and

show commands entered. For the security plane, tunnels
for protocols such as IPsec SHOULD be established and
flapped. Policies for Firewalls and ACLs SHOULD be
repeatedly added and removed via management sessions.

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

Figure 1. Physical Configuration


```
    _____         _____
   |  Control  |       | Management|
   |   Plane   |___   ___|  Plane   |
   |          |   |  |  |          |
    ----------    |  |   -----------
              \/   \/
             _____         _____
            |           |<----------| Security  |
            |    DUT    |           |   Plane   |
        |-->|           |<---|      |           |
            |   -----------     |    -----------
            |               |
            |               |
            |    _____     |
            |   |   Data    |    |
        |-->|   |   Plane   |<---|
            |           |
             -----------
```
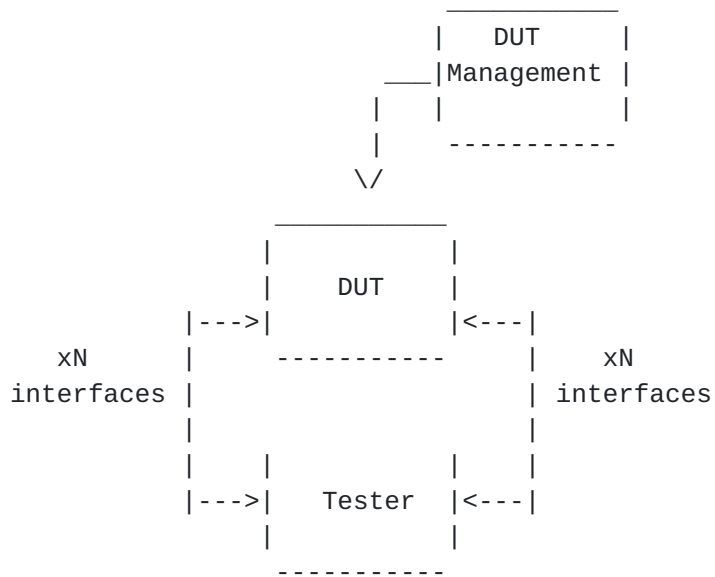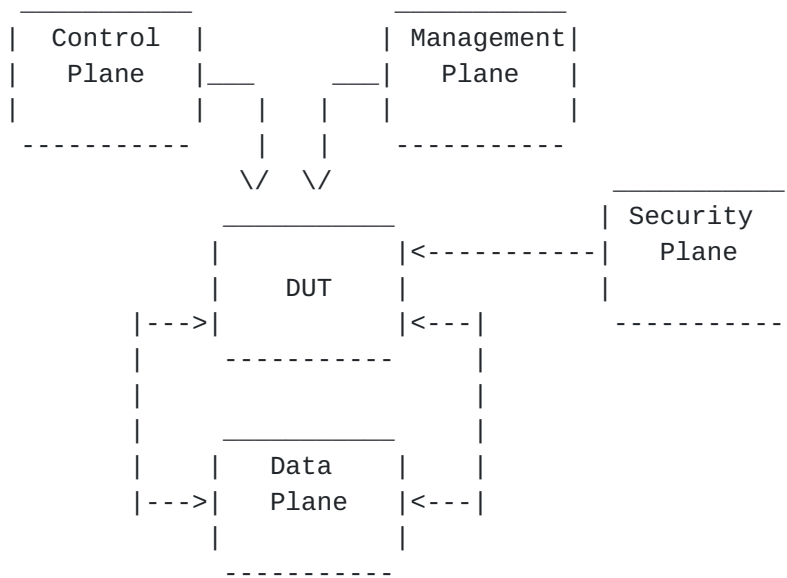
Figure 2. Logical Configuration

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. Benchmarks
MUST be reported as provided below.

3.3.1 Configuration Sets

The minimum Configuration Set that MUST be used is as follows:

       PARAMETER   UNITS
       Number of IGP Adjacencies   Adjacencies
       Number of IGP Routes   Routes
       Number of Nodes per Area   Nodes
       Number of Areas per Node   Areas
       SNMP GET Rate   SNMP Gets/minute
       Telnet Establishment Rate   Sessions/Hour
       Concurrent Telnet Sessions   Sessions
       FTP Establishment Rate   Sessions/Hour
       Concurrent FTP Session   Sessions
       SSH Establishment Rate   Sessions/Hour
       Concurrent SSH sessions   Sessions
       DATA TRAFFIC
          Traffic Forwarding   Enabled/Disabled
          Aggregate Offered Load   bps (or pps)
          Number of Ingress Interfaces interfaces
          Number of Egress Interfaces   interfaces
          Packet Size(s)   bytes
          Offered Load (interface)   array of bps
          Number of Flows   flows
          Encapsulation(flow)   array of encapsulation types

Configuration Sets MAY include and are not limited to the
following examples.
 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
         Number of Areas per Node   Areas

  Example MPLS Protocol Configuration Set-
         PARAMETER   UNITS
         MPLS-TE   Enabled/Disabled
         Number of Tunnels as Ingress   Tunnels

```
         Number of Tunnels as Mid-Point      Tunnels
         Number of Tunnels as Egress         Tunnels
         LDP                                 Enabled/Disabled
         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
        Number of Ingress Interfaces   interfaces
        Number of Egress Interfaces   interfaces

        TRAFFIC PROFILE
        Packet Size(s)   bytes
        Packet Rate(interface)   array of packets per second
        Aggregate Offered Load   pps
        Number of Flows   number of flows
        Traffic Type   array of (RTP, UDP, TCP, other)
        Encapsulation(flow)   array of encapsulation type
        Mirroring   enabled/disabled

   Example Management Configuration Set-
        PARAMETER   UNITS
        SNMP GET Rate   SNMP Gets/minute
        Logging   Enabled/Disabled
        Protocol Debug   Enabled/Disabled
        Telnet Establishment Rate   Sessions/Hour
        Concurrent Telnet Sessions   Sessions
        FTP Establishment Rate   Sessions/Hour
        Concurrent FTP Session   Sessions
        SSH Establishment Rate   Sessions/Hour
        Concurrent SSH sessions   Sessions
        Packet Statistics Collector   Enabled/Disabled
        Statistics Sampling Rate   X:1 packets

   Example Security Configuration Set -
        PARAMETER   UNITS
        Packet Filters   Enabled/Disabled
        Number of Filters For-Me   filters
        Number of Filter Rules For-Me   rules
        Number of Traffic Filters   filters
        Number of Traffic Filter Rules   rules
        IPsec tunnels   tunnels
        RADIUS   Enabled/Disabled
        TACACS   Enabled/Disabled

   Example SIP Configuration Set -

PARAMETER	UNITS
Session Rate	Sessions per Second
Media Streams per Session	Streams per session
Total Sessions	Sessions

   3.3.2 Startup Conditions
   Startup Conditions MAY include and are not limited to the following
   examples:
         PARAMETER   UNITS
         EBGP peering sessions negotiated   Total EBGP Sessions
         IBGP peering sessions negotiated   Total IBGP Sessions
         ISIS adjacencies established   Total ISIS Adjacencies
         ISIS routes learned rate   ISIS Routes per Second
         IPsec tunnels negotiated   Total IPsec Tunnels
         IPsec tunnel establishment rate   IPsec tunnels per second

   3.3.3 Instability Conditions
   Instability Conditions MAY include and are not limited to the
   following examples:
         PARAMETER   UNITS
         Interface Shutdown Cycling Rate   interfaces per minute
         ISIS 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 Tunnel Flap Rate   tunnels per minute
         Filter Policy Changes   policies per hour
         SSH Session Rate   SSH sessions per hour
         Telnet Session Rate   Telnet session per hour
         Command Entry Rate   Commands per Hour
         Message Flood Rate   Messages

   3.3.4 Benchmarks

   Benchmarks are as defined in [4] and MUST be reported as follow:
         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   sessions Recovery

[4]. Stress Test Procedure

   4.1 General Methodology with Multiple Instability Conditions

   Objective
   To benchmark the DUT under accelerated stress when there are
   multiple instability conditions.

   Procedure

        1. Report Configuration Set
        2. Begin Startup Conditions with the DUT
        3. Establish Configuration Sets with the DUT
        4. Report Stability Benchmarks
        5. Apply Instability Conditions
        6. Apply Instability Condition specific to test case.
        7. Report Instability Benchmarks
        8. Stop applying all Instability Conditions
        9. Report Recovery Benchmarks
        10. Optional - Change Configuration Set and/or Instability
             Conditions for next iteration

   Expected Results
   Ideally the Forwarding Rates, Latencies, and Session Counts will
   be measured to be the same at each phase. If no packet or
   session loss occurs then the Instability Conditions MAY be
   increased for a repeated iteration (step 10 of the procedure).

   Example Procedure

        1. Report Configuration Set

           BGP Enabled
           10 EBGP Peers
           30 IBGP Peers
           500K BGP Route Instances
           160K BGP FIB Routes

           ISIS Enabled
           ISIS-TE Disabled
           30 ISIS Adjacencies
           10K ISIS Level-1 Routes
           250 ISIS Nodes per Area

           MPLS Disabled
           IP Multicast Disabled

           IPsec Enabled
           10K IPsec tunnels

```
            640 Firewall Policies
            100 Firewall Rules per Policy
```

          Traffic Forwarding Enabled
          Aggregate Offered Load 10Gbps
          30 Ingress Interfaces
          30 Egress Interfaces
          Packet Size(s) = 64, 128, 256, 512, 1024, 1280, 1518 bytes
          Forwarding Rate[1..30] = 1Gbps
          10000 Flows
          Encapsulation[1..5000] = IPv4
          Encapsulation[5001.10000] = IPsec
          Logging Enabled
          Protocol Debug Disabled
          SNMP Enabled
          SSH Enabled
                10 Concurrent SSH Sessions
          FTP Enabled
          RADIUS Enabled
          TACACS Disabled
          Packet Statistics Collector Enabled

   2. Begin Startup Conditions with the DUT

      10 EBGP peering sessions negotiated
      30 EBGP peering sessions negotiated
      1K BGP routes learned per second
      30 ISIS Adjacencies
      1K ISIS routes learned per second
      10K IPsec tunnels negotiated

   3. Establish Configuration Sets with the DUT

   4. Report Stability Benchmarks as follow:

      Stable Aggregate Forwarding Rate
      Stable Latency
      Stable Session Count

      It is RECOMMENDED that the benchmarks be measured and
      recorded at one-second intervals.

   5. Apply Instability Conditions

      Interface Shutdown Cycling Rate = 1 interface every 5
                                        minutes
      BGP Session Flap Rate = 1 session every 10 minutes
      BGP Route Flap Rate = 100 routes per minute
      ISIS Route Flap Rate = 100 routes per minute
      IPsec Tunnel Flap Rate = 1 tunnel per minute
      Overloaded Links = 5 of 30

```
         Amount Links Overloaded = 20%
         SNMP GETs = 1 per sec
         SSH Session Rate = 6 sessions per hour
         SSH Session Duration = 10 minutes
         Command Rate via SSH = 20 commands per minute
```

            FTP Restart Rate = 10 continuous transfers (Puts/Gets)
                            per hour
            FTP Transfer Rate = 100 Mbps
            Statistics Sampling Rate = 1:1 packets
            RADIUS Server Loss Rate = 1 per Hour
            RADIUS Server Loss Duration = 3 seconds

      6. Apply Instability Condition specific to test case.

      7. Report Instability Benchmarks as follow:
         Unstable Aggregate Forwarding Rate
         Degraded Aggregate Forwarding Rate
         Ave. Degraded Aggregate Forwarding Rate
         Unstable Latency
         Unstable Uncontrolled Sessions Lost

         It is RECOMMENDED that the benchmarks be measured and
         recorded at one-second intervals.

      8. Stop applying all Instability Conditions

      9. Report Recovery Benchmarks as follow:

         Recovered Aggregate Forwarding Rate
         Recovered Latency
         Recovery Time
         Recovered Uncontrolled Sessions Lost

         It is RECOMMENDED that the benchmarks be measured and
         recorded at one-second intervals.

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

   4.2 General Methodology with a Single Instability Condition

   Objective
   To benchmark the DUT under accelerated stress when there is a
   single instability conditions.

   Procedure

      1. Report Configuration Set
      2. Begin Startup Conditions with the DUT
      3. Establish Configuration Sets with the DUT
      4. Report Stability Benchmarks
      5. Apply single Instability Condition
      6. Report Instability Benchmarks
      7. Stop applying all Instability Condition

```
   8. Report Recovery Benchmarks
   9. Optional - Change Configuration Set and/or Instability
      Conditions for next iteration
```

Expected Results
Ideally the Forwarding Rates, Latencies, and Session Counts will
be measured to be the same at each phase. If no packet or session
loss occurs then the Instability Conditions MAY be increased
for a repeated iteration (step 10 of the procedure).

5. IANA Considerations
This document requires no IANA considerations.

6. 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.

7. Normative References

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

[2]   Mandeville, R., "Benchmarking Terminology for LAN Switching
       Devices", RFC 2285, October 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-13,
       work in progress, February 2008.

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

8. 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, October 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-15, work in
           progress, February 2008.

9. Author's Address

      Scott Poretsky
      NextPoint Networks
      3 Federal Street
      Billerica, MA 01821
      USA
      Phone: + 1 508 439 9008
      EMail: sporetsky@nextpointnetworks.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

    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.