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.

Status of this Memo

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Copyright Notice
Copyright (C) The IETF Trust (2008).

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.
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.
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:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of IGP Adjacencies</td>
<td>Adjacencies</td>
</tr>
<tr>
<td>Number of IGP Routes</td>
<td>Routes</td>
</tr>
<tr>
<td>Number of Nodes per Area</td>
<td>Nodes</td>
</tr>
<tr>
<td>Number of Areas per Node</td>
<td>Areas</td>
</tr>
<tr>
<td>SNMP GET Rate</td>
<td>SNMP Gets/minute</td>
</tr>
<tr>
<td>Telnet Establishment Rate</td>
<td>Sessions/Hour</td>
</tr>
<tr>
<td>Concurrent Telnet Sessions</td>
<td>Sessions</td>
</tr>
<tr>
<td>FTP Establishment Rate</td>
<td>Sessions/Hour</td>
</tr>
<tr>
<td>Concurrent FTP Session</td>
<td>Sessions</td>
</tr>
<tr>
<td>SSH Establishment Rate</td>
<td>Sessions/Hour</td>
</tr>
<tr>
<td>Concurrent SSH sessions</td>
<td>Sessions</td>
</tr>
</tbody>
</table>

DATA TRAFFIC

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Forwarding</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Aggregate Offered Load</td>
<td>bps (or pps)</td>
</tr>
<tr>
<td>Number of Ingress Interfaces</td>
<td>interfaces</td>
</tr>
<tr>
<td>Number of Egress Interfaces</td>
<td>interfaces</td>
</tr>
<tr>
<td>Packet Size(s)</td>
<td>bytes</td>
</tr>
<tr>
<td>Offered Load (interface)</td>
<td>array of bps</td>
</tr>
<tr>
<td>Number of Flows</td>
<td>flows</td>
</tr>
<tr>
<td>Encapsulation(flow)</td>
<td>array of encapsulation types</td>
</tr>
</tbody>
</table>

Configuration Sets MAY include and are not limited to the following examples.

Example Routing Protocol Configuration Set-

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Number of EBGP Peers</td>
<td>Peers</td>
</tr>
<tr>
<td>Number of IBGP Peers</td>
<td>Peers</td>
</tr>
<tr>
<td>Number of BGP Route Instances</td>
<td>Routes</td>
</tr>
<tr>
<td>Number of BGP Installed Routes</td>
<td>Routes</td>
</tr>
<tr>
<td>MBGP</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Number of MBGP Route Instances</td>
<td>Routes</td>
</tr>
<tr>
<td>Number of MBGP Installed Routes</td>
<td>Routes</td>
</tr>
<tr>
<td>IGP</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>IGP-TE</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Number of IGP Adjacencies</td>
<td>Adjacencies</td>
</tr>
<tr>
<td>Number of IGP Routes</td>
<td>Routes</td>
</tr>
<tr>
<td>Number of Nodes per Area</td>
<td>Nodes</td>
</tr>
<tr>
<td>Number of Areas per Node</td>
<td>Areas</td>
</tr>
</tbody>
</table>

Example MPLS Protocol Configuration Set-

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS-TE</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Number of Tunnels as Ingress</td>
<td>Tunnels</td>
</tr>
<tr>
<td>Number of Tunnels as Mid-Point</td>
<td>Tunnels</td>
</tr>
<tr>
<td>Number of Tunnels as Egress</td>
<td>Tunnels</td>
</tr>
<tr>
<td>LDP</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Number of Sessions</td>
<td>Sessions</td>
</tr>
<tr>
<td>Number of FECs</td>
<td>FECs</td>
</tr>
</tbody>
</table>
Example Multicast Protocol Configuration Set-

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM-SM</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>RP</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Number of Multicast Groups</td>
<td>Groups</td>
</tr>
<tr>
<td>MSDP</td>
<td>Enabled/Disabled</td>
</tr>
</tbody>
</table>

Example Data Plane Configuration Set-

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Forwarding</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Number of Ingress Interfaces</td>
<td>interfaces</td>
</tr>
<tr>
<td>Number of Egress Interfaces</td>
<td>interfaces</td>
</tr>
</tbody>
</table>

TRAFFIC PROFILE

<table>
<thead>
<tr>
<th>Packet Size(s)</th>
<th>bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Rate(interface)</td>
<td>array of packets per second</td>
</tr>
<tr>
<td>Aggregate Offered Load</td>
<td>pps</td>
</tr>
<tr>
<td>Number of Flows</td>
<td>number of flows</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>array of (RTP, UDP, TCP, other)</td>
</tr>
<tr>
<td>Encapsulation(flow)</td>
<td>array of encapsulation type</td>
</tr>
<tr>
<td>Mirroring</td>
<td>enabled/disabled</td>
</tr>
</tbody>
</table>

Example Management Configuration Set-

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP GET Rate</td>
<td>SNMP Gets/minute</td>
</tr>
<tr>
<td>Logging</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Protocol Debug</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Telnet Establishment Rate</td>
<td>Sessions/Hour</td>
</tr>
<tr>
<td>Concurrent Telnet Sessions</td>
<td>Sessions</td>
</tr>
<tr>
<td>FTP Establishment Rate</td>
<td>Sessions/Hour</td>
</tr>
<tr>
<td>Concurrent FTP Session</td>
<td>Sessions</td>
</tr>
<tr>
<td>SSH Establishment Rate</td>
<td>Sessions/Hour</td>
</tr>
<tr>
<td>Concurrent SSH sessions</td>
<td>Sessions</td>
</tr>
<tr>
<td>Packet Statistics Collector</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Statistics Sampling Rate</td>
<td>X:1 packets</td>
</tr>
</tbody>
</table>

Example Security Configuration Set -

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Filters</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Number of Filters For-Me</td>
<td>filters</td>
</tr>
<tr>
<td>Number of Filter Rules For-Me</td>
<td>rules</td>
</tr>
<tr>
<td>Number of Traffic Filters</td>
<td>filters</td>
</tr>
<tr>
<td>Number of Traffic Filter Rules</td>
<td>rules</td>
</tr>
<tr>
<td>IPsec tunnels</td>
<td>tunnels</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>TACACS</td>
<td>Enabled/Disabled</td>
</tr>
</tbody>
</table>

Example SIP Configuration Set -

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Rate</td>
<td>Sessions per Second</td>
</tr>
<tr>
<td>Media Streams per Session</td>
<td>Streams per session</td>
</tr>
<tr>
<td>Total Sessions</td>
<td>Sessions</td>
</tr>
</tbody>
</table>

Poretsky and Rao
3.3.2 Startup Conditions
Startup Conditions MAY include and are not limited to the following examples:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>EBGP peering sessions negotiated</td>
<td>Total EBGP Sessions</td>
</tr>
<tr>
<td>IBGP peering sessions negotiated</td>
<td>Total IBGP Sessions</td>
</tr>
<tr>
<td>ISIS adjacencies established</td>
<td>Total ISIS Adjacencies</td>
</tr>
<tr>
<td>ISIS routes learned rate</td>
<td>ISIS Routes per Second</td>
</tr>
<tr>
<td>IPsec tunnels negotiated</td>
<td>Total IPsec Tunnels</td>
</tr>
<tr>
<td>IPsec tunnel establishment rate</td>
<td>IPsec tunnels per second</td>
</tr>
</tbody>
</table>

3.3.3 Instability Conditions
Instability Conditions MAY include and are not limited to the following examples:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Shutdown Cycling Rate</td>
<td>interfaces per minute</td>
</tr>
<tr>
<td>ISIS Route Flap Rate</td>
<td>routes per minutes</td>
</tr>
<tr>
<td>LSP Reroute Rate</td>
<td>LSP per minute</td>
</tr>
<tr>
<td>Overloaded Links</td>
<td>number</td>
</tr>
<tr>
<td>Amount Links Overloaded</td>
<td>% of bandwidth</td>
</tr>
<tr>
<td>FTP Rate</td>
<td>Mb/minute</td>
</tr>
<tr>
<td>IPsec Tunnel Flap Rate</td>
<td>tunnels per minute</td>
</tr>
<tr>
<td>Filter Policy Changes</td>
<td>policies per hour</td>
</tr>
<tr>
<td>SSH Session Rate</td>
<td>SSH sessions per hour</td>
</tr>
<tr>
<td>Telnet Session Rate</td>
<td>Telnet session per hour</td>
</tr>
<tr>
<td>Command Entry Rate</td>
<td>Commands per Hour</td>
</tr>
<tr>
<td>Message Flood Rate</td>
<td>Messages</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>UNITS</th>
<th>PHASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stable Aggregate Forwarding Rate</td>
<td>pps</td>
<td>Startup</td>
</tr>
<tr>
<td>Stable Latency</td>
<td>seconds</td>
<td>Startup</td>
</tr>
<tr>
<td>Stable Session Count</td>
<td>sessions</td>
<td>Startup</td>
</tr>
<tr>
<td>Unstable Aggregate Forwarding Rate</td>
<td>pps</td>
<td>Instability</td>
</tr>
<tr>
<td>Degraded Aggregate Forwarding Rate</td>
<td>pps</td>
<td>Instability</td>
</tr>
<tr>
<td>Ave. Degraded Aggregate Forwarding Rate</td>
<td>pps</td>
<td>Instability</td>
</tr>
<tr>
<td>Unstable Latency</td>
<td>seconds</td>
<td>Instability</td>
</tr>
<tr>
<td>Unstable Uncontrolled Sessions Lost</td>
<td>sessions</td>
<td>Instability</td>
</tr>
<tr>
<td>Recovered Aggregate Forwarding Rate</td>
<td>pps</td>
<td>Recovery</td>
</tr>
<tr>
<td>Recovered Latency</td>
<td>seconds</td>
<td>Recovery</td>
</tr>
<tr>
<td>Recovery Time</td>
<td>seconds</td>
<td>Recovery</td>
</tr>
<tr>
<td>Recovered Uncontrolled Sessions</td>
<td>sessions</td>
<td>Recovery</td>
</tr>
</tbody>
</table>
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


8. Informative References


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
Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.