Resource Unavailability (RU) Per Domain Behavior
draft-karagiannis-ru-pdb-01.txt

Status of this Memo

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.

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.

This Internet-Draft will expire on September 6, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).
Abstract

This draft specifies a Per Domain Behavior that provides the ability to Diffserv nodes located at the border or outside Diffserv domain(s) to detect when the resources provided by the Diffserv domain(s) are not available. This PDB is used when the negotiated SLS is associated to throughput (or bandwidth) and when the SLS agreed throughput bound is not statically but loosely defined in order to allow a more efficient utilization of the Diffserv domain(s) and a more simple network management operation. This PDB can be applied in association with either a single Diffserv domain or multiple neighboring Diffserv domains. This specification is denoted as Resource Unavailability (RU) PDB and it follows the guidelines given in RFC 3086.

Table of Contents

1. Introduction. .................................................. 3
2. Applicability .................................................. 3
3. TCS and PHB configurations ..................................... 3
4. Attributes of this PDB ......................................... 9
5. Parameters ..................................................... 9
6. Assumptions ................................................... 9
7. Example uses .................................................. 10
8. Environmental concerns ....................................... 15
9. Security considerations ....................................... 15
10. IANA considerations .......................................... 15
11. Acknowledgments ............................................. 15
12. Normative References ....................................... 16
13. Informative References ..................................... 17
1. Introduction

The RU PDB can be applied in the situation where Diffserv nodes located at the border or outside Diffserv domain(s) must detect when the resources provided by the Diffserv domain(s) are not available.

This PDB is used when the negotiated SLS is associated to throughput (or bandwidth) and when the SLS agreed throughput bound is not statically but loosely defined. The main purpose of loosely defining the SLS throughput bound is to allow a more efficient utilization of the Diffserv domain(s) and a more simple network management operation. This PDB can be applied in association with either a single Diffserv domain or multiple neighboring Diffserv domains.

The resource unavailability on the Diffserv nodes within the Diffserv domain(s) can be detected using a DSCP remarking approach where the remarking is proportional to the amount of unavailable resources.

The Diffserv nodes located at the border or outside the Diffserv domain(s) can then use the remarked DSCP packets to calculate the percentage of throughput (or bandwidth) that does exceed the loosely agreed SLS throughput bound.

These nodes can then, in combination with the sender of the traffic and support by the Diffserv domain(s), reduce the generated throughput until the loosely agreed SLS throughput bound is satisfied. Possible applicability areas on using the remarked DSCP packets/bytes are related to the support of final handling decisions on the admission control and/or severe congestion handling process.

2. Terminology

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 [RFC2119].

3. TCS and PHB Configuration

Packets using any PHB can receive the RU PDB treatment. Furthermore, the RU PDB can be used in combination with any other defined PDB.
3.1. Diffserv End System or Ingress Edge Router Configuration

The Diffserv source end systems or the ingress edges, which support the RU PDB, ensure that the packets are being marked with the right PHB. Note that the process of marking can be specified by another PDB. In this text, for simplicity reasons, the PDB that is defining the PHB marking is denoted as another_PDB. For each of the chosen PHB, the TCS and PHB configurations associated with the RU PDB are following the rules defined by another_PDB, which MAY use the specifications provided in [RFC2474], [RFC2475], [RFC3246], [RFC2597] and [RFC3290].

3.2 Common Diffserv end system, edge and interior router configurations

The Diffserv nodes, which are supporting the RU PDB, ensure that for each of the chosen PHB, the TCS and PHB configurations are following the rules that are defined by the another_PDB, see above.

The classification of packets SHOULD be based on either the DSCP or on a combination of IP header fields including the DSCP.

In addition, the edge and interior routers MUST support the DSCP remarking feature that is remarking the original DSCP into one or more locally specified DSCPs, which SHOULD be associated with the same PHB. In the following text, the original DSCP is denoted as original_DSCP and the locally specified DSCPs that receive the same PHB are denoted as locali_DSCP, where i= 1, 2, 3.

In order to provide this feature the Diffserv nodes SHOULD support the following functions that can be implemented in a similar way as specified in [RFC3290]:

Classify: The Diffserv node SHOULD be configured to consider that the packets marked either with the original_DSCP or with the locali_DSCPs SHOULD receive the same per hop behavior treatment. However, packets that are marked with the different DSCPs, i.e., original_DSCP, local1_DSCP, local2_DSCP, local3_DSCP MAY be classified to enter a different queue per DSCP. This classification can be accomplished by the Classify function.

The classification of packets SHOULD be based on either the DSCP or on a combination of IP header fields including the DSCP.
Meter + Action: Each Diffserv node SHOULD maintain a metering function (Meter) that measures/counts the bandwidth used by packets belonging to a certain DSCP, e.g., original_DSCP, local1_DSCP, local2_DSCP, local3_DSCP. In addition to that, either one preconfigured loosely agreed SLS throughput (bandwidth) threshold or two preconfigured loosely agreed SLS throughput (bandwidth) thresholds SHOULD be maintained by the Diffserv node. The exact definition of how these throughput (bandwidth) thresholds are communicated from the location of where the SLS parameters are maintained up to the Diffserv nodes it is outside the scope of this draft. In the following text we denote the above mentioned thresholds as Threshold1 and Threshold2. Note that if both thresholds are maintained by a Diffserv node then the following inequality SHOULD be valid:

Threshold2 > Threshold1.

If only one bandwidth threshold is maintained by the Diffserv node, then this bandwidth threshold can be used either for resource unavailability or for an overload situation detection. When this threshold is used for resource unavailability detection then this threshold is denoted in this text as Threshold1. Otherwise, this bandwidth threshold is used for overload situation detection and is denoted in this text as Threshold2.

3.2.1 Resource unavailability detection threshold

If the Meter detects that the measured/count throughput (bandwidth) exceeds the resource unavailability detection threshold (Threshold1) then this exceeded throughput (bandwidth) (packets/bytes) SHOULD be remarked accordingly ( remarking whole exceeded bandwidth) by the Action functionality block into a locally predefined DSCP, e.g., local1_DSCP.

3.2.2 Overload situation detection threshold

If the Meter detects that the measured/count throughput (bandwidth) exceeds the overload situation detection threshold (Threshold2) then this exceeded bandwidth (packets/bytes) SHOULD be proportionally remarked by the Action functionality block into two locally predefined DSCP, e.g., local2_DSCP and local3_DSCP. The exact definition of this is outside the scope of this draft. However, the following text describes an example of the meter and action functionality specification.
The Diffserv node estimates the average amount of incoming throughput (bandwidth) by counting the number of bytes $N$ that arrive during a measurement interval of $T$ seconds and dividing $N$ by $T$. If this value is higher than the pre-configured threshold, i.e., $\text{Threshold}_2$, the Diffserv node knows that an overload situation has occurred and estimates the overload $O$ as $O = \frac{N}{T} - \text{Threshold}_2$, which is the amount of incoming traffic above the $\text{Threshold}_2$. Using the encoded DSCP (local2_DSCP), the Diffserv node encodes the value of $O$ into the outgoing packets as follows.

Firstly, at the end of each measurement period of $T$ seconds the estimated overload $O$ of that period is converted to an equivalent number of bytes $B$ using the following formula: $B = O \times T$.

Secondly, the Diffserv node re-marks the DSCP field of a certain number of packets with the encoded DSCP (local2_DSCP) such that the total sum of packet sizes of all the packets with an encoded DSCP (local2_DSCP) is equal to $B$. The rest of the outgoing packets are marked with the affected DSCP (local3_DSCP). In this way, when an egress node receives a packet with a re-marked DSCP field (local2_DSCP or local3_DSCP), it knows that there is an overloaded node on the path the packet followed.

Note that the packets that are used as input for the above described remarking procedure have been marked with either the original_DSCP or local1_DSCP.

Note that this procedure can be applied on more than one neighboring Diffserv domains. Therefore, it is possible that a marked packet can be received by the edge router of a new neighboring Diffserv domain (and thus new domain operator). The new Diffserv domain may use another type of Diffserv remarking scheme. Thus the original_DSCP, local1_DSCP, local2_DSCP and local3_DSCP may be remarked to other DSCP. However, the semantics and relations between these DSCPs MUST remain. In the following text we assume that the same DSCP names are kept.

If a Diffserv node receives marked packets, with one of the locali_DSCPs, it means that another Diffserv node, located upstream, on the same communication path remarked packets. Consider that the remarking of the local2_DSCP and local3_DSCP proportion is accomplished as above. Furthermore, consider that the total number of bytes, $B$, that represent the percentage of overload above $\text{Threshold}_2$ and have to be remarked with the encoded DSCP (local2_DSCP) is calculated as explained above. Moreover, consider that the number of bytes that are received by the current Diffserv node and marked as encoded DSCP (local2_DSCP) are denoted as IR. Note that these IR remarked bytes SHOULD be transmitted over the output link of the current Diffserv node.
Furthermore, consider that the number of bytes that have to be remarked by the current Diffserv node using the encoded DSCP (local2_DSCP) are denoted as CR, which can be calculated as follows:

\[
\text{IF } (B > IR) \\
\text{THEN} \\
\quad CR = B - IR \\
\text{ELSE} \\
\quad CR = 0
\]

The rest of the outgoing packets are marked with the affected DSCP (local3_DSCP).

3.3 Diffserv nodes supporting final handling decisions on resource unavailability and/or overload situation handling process

When a Diffserv node located at the boundary or outside Diffserv domain(s) is used to provide final decisions on the resource unavailability and/or overload handling process then the following steps SHOULD be followed by this Diffserv node. Note that the Diffserv node that provides final decisions on resource unavailability is denoted in this text as Resource Unavailability Handling Diffserv node. Furthermore, the Diffserv node that provides final decisions on overload situation handling process is denoted in this text as Overload Situation Handling Diffserv node.

3.3.1 Resource unavailability handling

When the Diffserv node that is located at the border or outside the Diffserv domain(s) provides final handling decisions on the resource unavailability functionality, then the amount of the original (original_DSCP) and remarked (local1_DSCP) packets is counted by this node to provide the basis of call acceptance for new flows. If this Resource Unavailability Handling Diffserv node supports a QoS agent, then this QoS agent can be informed when a new request has to be accepted or rejected.

The downstream packets marked with the local1_DSCP are remarked back to the original_DSCP by the Admission control Diffserv node.
3.3.2 Overload situation handling

When the Diffserv node located at the boundary or outside the Diffserv domain(s) provides final handling decisions on the overload situation handling process, then the following steps must be followed.

When the first packet with a re-marked DSCP field (encoded (local2_DSCP) or affected (local3_DSCP) is received by this node, it starts two counters that count the number of received packets with encoded (local2_DSCP) and affected (local3_DSCP) DSCPs, respectively. The counting interval of these counters is set to the same length as the measurement periods used on the other Diffserv nodes (T). At the end of the counting interval, the Overload Situation Handling Diffserv node calculates an overload value by summing the packet sizes of all the received encoded (local2_DSCP) packets and dividing this sum by the length of the counting interval. Based on this overload value, the Overload Situation Handling Diffserv node can then decide whether flow termination is necessary. If flow termination is needed, the Overload Situation Handling Diffserv node using information provided by the QoS agent or a local policy, it can select flows to terminate from the flows that received packets with the encoded (local2_DSCP) or affected (local3_DSCP) DSCP, since these are the flows that experienced overload situation.

By giving preference to lower priority flows during the selection procedure, higher priority flows such as emergency calls can be protected. This is done by first trying to clear all overload by terminating only affected flows from the lowest priority class. If this is not sufficient, affected flows from the next priority class will be terminated, etc. The flows to be selected from a certain priority class are chosen in such a way, that the total number of flows to be terminated is kept as low as possible. This is accomplished by using the well-known "best-fit first" heuristic. For example, if the overload to be cleared is 200 Kbps and the choice is between three flows with reserved bandwidths of respectively 60, 180 and 210 Kbps, then the 180 Kbps flow will be selected first. Once the flows that are to be terminated have been selected, then the QoS agent is notified of which flows can be terminated.

The downstream packets marked with the local2_DSCP and local3_DSCP are remarked back to the original_DSCP by this egress edge.
4. Attributes of this PDB

The new attributes that are related to this PDB are related to the agreed SLS throughput (bandwidth) bound (threshold).

Different agreed SLS throughput thresholds, see Section 3, might be used. Each of these throughput (bandwidth) thresholds are compared to the measure throughput.

5. Parameters

The used parameter is the SLS throughput (or bandwidth).

6. Assumptions

The negotiated SLA may include either one preconfigured loosely agreed SLS throughput (bandwidth) threshold or two preconfigured loosely agreed SLS throughput (bandwidth) thresholds (bound). It is assumed that the network operator communicates these throughput (bandwidth) thresholds from the location of where the SLS parameters are maintained up to the Diffserv nodes within the Diffserv domain(s).

The RU PDB can be applied on more than one neighboring Diffserv domains. Therefore, it is possible that that a marked packet can be received by the edge router of a new neighboring Diffserv domain (and thus new domain operator). The new Diffserv domain may use another type of Diffserv remarking scheme. Thus the original DSCP, local1 DSCP, local2 DSCP and local3 DSCP may be remarked to other DSCP. However, the network operator MUST configure the Diffserv remarking scheme such that the semantics and relations between the original DSCP, local1 DSCP, local2 DSCP and local3 DSCP remain even when packets using the RU PDB are passing via multiple neighboring Diffserv domains.

Furthermore, a network operator may configure Diffserv nodes located at the boundary or outside Diffserv domain(s) to provide final handling decisions on the resource unavailability and/or overload situation process, see Section 3.3.

A network operator may configure the QoS Agent functionality (see e.g., [RFC3290]) that may be used by the Diffserv nodes located at the boundary or outside Diffserv domain(s) to provide final handling decisions on the resource unavailability and/or overload situation process. The QoS Agent functionality can support a signaling protocol, e.g., RSVP [RFC2205], or NSIS [RFC4080].
7. Example uses

7.1 Single Diffserv domain admission control based on probing: controlled by egress

In this scenario the RU PDB is applied only within one Diffserv domain.

The ingress router supports the RU PDB functionality specified in Section 3.1. The interior router supports the RU PDB functionality as specified in Section 3.2.1 and the egress edge supports the functionality as specified in Section 3.3.1. In addition to this it is considered that each edge MAY maintain a QoS agent.

In this example, see Figure 1, a simple measurement-based admission control within a Diffserv domain can be realised. In the interior nodes along the data path a threshold (Threshold1) is set in the measurement-based admission control function for the traffic belonging to different PHBs.

When a probe packet (note that this packet MAY be sent by the QoS Agent available at the Ingress as a signaling message), which is marked with the original_DSCP arrives at the congested Interior node (C), i.e., measured bandwidth is higher than Threshold2, then this probe packet will be remarked to local1_DSCP.

When the egress receives this marked probe packet then it decides to deny the request of the probe packet. If a QoS Agent is available at the ingress and egress, then the QoS Agent at the egress SHOULD send a notify alike message, to the QoS Agent available at the ingress edge to inform it about the denial of the probe packet request.

The downstream packets marked with the local1_DSCP are remarked back to the original_DSCP by this egress edge.

Karagiannis, et al.
7.2 Multiple Diffserv domains admission control based on probing: controlled by egress

In this scenario the RU PDB is applied within multiple neighboring Diffserv domains. The operation of this scenario is similar to the scenario described in Section 7.1. The main difference is related to the fact that only the egress edge, which is located within the last downstream Diffserv domain provides the final handling decision on the admission control specified in Section 3.3.1. All the other end systems, ingress and egress edges operate according to the specification given in Section 3.2.1. Furthermore, the ingress edge of the first downstream Diffserv domain supports the RU PDB functionality specified in Section 3.1.

Note that also other ingress edges MAY support the RU PDB functionality specified in Section 3.1. In addition to this it is considered that each edge MAY maintain a QoS agent. Note that if the egress edge located within the last downstream Diffserv domain maintains a QoS Agent, then the QoS Agent at this egress SHOULD send a notify like message to the QoS Agent available at an intermediate ingress edge to inform him about the denial of the probe packet request.

The downstream packets marked with the local1_DSCP are remarked back to the original_DSCP by the egress edge, which is located within the last downstream Diffserv domain.
7.3 Single Diffserv domain admission control based on probing: controlled by receiving end system

This scenario is very much similar to the scenario described in Section 7.1.

The main difference is related to the fact that in this scenario the egress node does not support the functionality specified in Section 3.3.1, while the Diffserv receiving end system is supporting this functionality, see Figure 2. In addition to this, it is considered that the end systems (Source and Receiver) are also supporting the functionality specified in 3.2.1 and MAY maintain a QoS agent. The downstream packets marked with the local1_DSCP are remarked back to the original_DSCP by the receiver and not by the Diffserv egress.

![Diagram of admission control based on probing within one Diffserv domain controlled by receiver](image)

Figure: 2 Admission control based on probing within one Diffserv domain: controlled by receiver
### 7.4 Multiple Diffserv domains admission control based on probing: controlled by receiving end system

This scenario is very much similar to the scenario described in Section 7.2.

The main difference is related to the fact that in this scenario the egress node does not support the functionality specified in Section 3.3.1, while the Diffserv receiving end system (Receiver) is supporting this functionality. In addition to this it is considered that the end systems (Source and Receiver) are also supporting the functionality specified in 3.2.1 and MAY maintain a QoS agent. The downstream packets marked with the local1_DSCP are remarked back to the original_DSCP by the receiver and not by the Diffserv egress.

### 7.5 Single Diffserv domain severe congestion handling: controlled by egress

In this scenario the RU PDB is applied only within one Diffserv domain.

The ingress router supports the RU PDB functionality specified in Section 3.1. The interior router supports the RU PDB functionality as specified in Section 3.2.2 and the egress edge supports the functionality as specified in Section 3.3.2. In addition to this it is considered that each edge MAY maintain a QoS agent.

In this example, see Figure 3, a severe congestion detection procedure is shown.

When a failure in a communication path, e.g. router or link failure, occurs, the routing algorithms will adapt to these failures by changing the routing decisions to reflect changes in the topology and traffic volume. As a result, the re-routed traffic will follow a new path, which may result in overloaded nodes as they need to support more traffic. This may cause severe congestion in the communication path. In this situation the available resources, are not enough to meet the required QoS for all the flows along the new path.

This severe congestion is detected in this example by using the RU PDB.
When an Interior node becomes severe congested (S), i.e., measured bandwidth is higher than Threshold2, then the remarking procedure explained in Section 3.2.2 will be used. Note that the # marked bytes, in Figure 2, represent the local2_DSCP and local3_DSCP bytes, while the # unmarked bytes represent the original_DSCP bytes.

If a QoS Agent is available at the ingress and egress, then the QoS Agent at the egress SHOULD send for each selected flow (that should be terminated) a notify like message to the QoS Agent available at the ingress edge to inform him that the flow has to be terminated.

The downstream packets marked with the local2_DSCP and local3_DSCP are remarked back to the original_DSCP by this egress edge.

<table>
<thead>
<tr>
<th>Ingress</th>
<th>Interior</th>
<th>Interior</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td>user data</td>
<td>user data</td>
<td>user data</td>
<td>user data</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>-----&gt;</td>
<td>------------</td>
<td>-------</td>
<td>S(# marked bytes)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S(# unmarked bytes)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Term.</td>
<td></td>
</tr>
<tr>
<td>Notification S</td>
<td></td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure: 3 Severe congestion detection within one Diffserv domain: controlled by egress

7.6 Multiple Diffserv domains severe congestion handling: controlled by egress

In this scenario the RU PDB is applied within multiple neighboring Diffserv domains. The operation of this scenario is similar to the scenario described in Section 7.5. The main difference is related to the fact that only the egress edge, which is located within the last downstream Diffserv domain maintains the admission control functionality specified in Section 3.3.2. All the other ingress and egress edges operate according to the specification given in Section 3.2.2. Furthermore, the ingress edge of the first downstream Diffserv domain supports the RU PDB functionality specified in Section 3.1.

Karagiannis, et al. [Page 14]
Note that also other ingress edges MAY support the RU PDB functionality specified in Section 3.1. In addition to this it is considered that each edge MAY maintain a QoS agent. Note that if the egress edge located within the last downstream Diffserv domain maintains a QoS Agent, then the QoS Agent at this egress SHOULD send a notify like message to the QoS Agent available at an intermediate ingress edge to inform him that the flow should be terminated.

The downstream packets marked with the local2_DSCP and local3_DSCP are remarked back to the original_DSCP by the egress edge, which is located within the last downstream Diffserv domain.

8. Environmental concerns

There are no environmental concerns specific to this PDB. However, depending on the the area wherein the RU PDB is applied (one Diffserv domain or multiple neighboring domains), different requirements have to be fulfilled by the network operators, see Section 6.

9. Security considerations for RU PDB

There are no specific security exposures for this PDB. See the general security considerations in [RFC2474] and [RFC2475].

10. IANA Considerations

[Editor’s Note: A future version of this document will provide instructions to IANA.]

11. Acknowledgements

We thank Kathie Nichols for reviewing this draft and providing useful comments.

Karagiannis, et al. [Page 15]
12. Normative References


13 Informative References


Authors’ Addresses

Georgios Karagiannis
University of Twente
P.O. BOX 217
7500 AE Enschede, The Netherlands
EMail: g.karagiannis@ewi.utwente.nl

Lars Westberg
Ericsson Research
Kistagangen 26
SE-164 80 Stockholm
Sweden
EMail: Lars.Westberg@ericsson.com

Attila Bader
Ericsson Research
Ericsson Hungary Ltd.
Laborc 1, Budapest, H-1037
Hungary
EMail: Attila.Bader@ericsson.com

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany
EMail: Hannes.Tschofenig@siemens.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 Validity

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 AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Copyright (C) The Internet Society (2006).

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.