DNA Working Group
Internet-Draft
Expires: December 8, 2006

S. Narayanan
G. Daley
Panasonic
N. Montavont
GET - ENST Bretagne

June 6, 2006

Detecting Network Attachment in IPv6 - Network Deployment Considerations

draft-ietf-dna-network-00.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 December 8, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

Hosts experiencing rapid link-layer changes may require to do configuration change detection procedures more frequently than traditional fixed hosts. This document describes practices available to network deployers in order to support such hosts in Detecting Network Attachment in IPv6 networks.

Requirements Language

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 [2].

Table of Contents

1. Introduction

Hosts on the Internet may be connected by various media. It has become common that hosts have access through wireless media and are mobile. The frequency of configuration change for wireless and nomadic devices are elevated, due to the vagaries of wireless propagation or the motion of the hosts themselves.

Such hosts need to determine if they have moved to a new IPv6 link rapidly, in order that configuration procedures may be run and application packet delivery services restored. Detecting Network Attachment (DNA) is a strategy to assist such configuration changes by rapidly determining whether they are required.

Several network-side factors may impact the effectiveness and speed of DNA procedures. This document provides guidelines embodying the best current practice for network deployers wishing to support detection of network attachment by IPv6 hosts.

It should be noted that many already deployed routers will not support these recommendations, and that hosts SHOULD NOT rely on their being in place, unless they have particular reason to do so.

1.1 Terms and Abbreviations

Access network: A network where hosts are present. Especially, a network used for the support of visiting wireless hosts.

Link: A link is the range across which communications can pass without being forwarded through a router [1].

Link-Change: Link-Change occurs when a host moves from a point-of-attachment on a link, to another point-of-attachment where it is unable to reach devices belonging to the previous link, without being forwarded through a router.

Point-of-Attachment: A link-layer base-station, VLAN or port through which a device attempts to reach the network. Changes to a host's point-of-attachment may cause link-change.

Reachability Detection: Determination that a device (such as a router) is currently reachable, over both a wireless medium, and any attached fixed network. This is typically achieved using Neighbor Unreachability Detection procedure [1].

Wireless Medium: A physical layer which incorporates free space electromagnetic or optical propagation. Such media are susceptible to mobility and interference effects, potentially resulting in high packet loss probabilities.

1.2 Relevant Host Issues

Hosts attempting to discover link change are likely to send Router Solicitations (RSs) in order to identify the routers and prefixes available on a link. Additionally, they may wish to send Neighbour Solicitations (NSs) to known routers for reachability detection purposes.

The following is a list of critical issues for hosts undertaking link change detection in IPv6:

Hosts require Router Advertisements (RAs) rapidly in order to minimize reconfiguration latencies in the case of link change or link failure.

Hosts need to identify if their current prefix is still valid on a link before the prefix expires. Existing IPv6 Neighbour Discovery procedures make this difficult. If the host can determine that the target router is still reachable through a NS/NA exchange, it does not mean that the prefix is still valid on that link. This is because link-local addresses are used for the NS/NA exchange. Conversely, if host sends an RS, the RA received in response may not contain the prefix of interest for the hosts.

Hosts wish to detect if a particular router is reachable in order to use it for routing.

Hosts may require some assurance that a device is actually present, and is authorized to act as a router.

Consideration for these issues underlie the practices recommended in this document.

1.3 Relevant Router Issues

The IPv6 Neighbour Discovery RFC [1] provides mechanisms where hosts can send Router Solicitations and receive Router Advertisements, from each of the routers on a link.

Responses may either be unicast or multicast, but in all cases, a random delay of between 0 and 500 milliseconds is required before responses are sent. This is to prevent multiple routers

responding at the same time, and also may mitigate the effects of simultaneous solicitations. This results in a basic time delay incurred by hosts receiving response RAs, which cannot be avoided within current standards [1].

As described in Section 2.1, additional delays may occur if multicast responses are required.

Routers should also be careful not to increase the network overhead by frequently transmitting router advertisements (see Section 2.4).

Multiple prefixes advertised in different RAs by a single router may lead to host configurations errors. It may generate erroneous movement detection and/or delay hosts to detect that a prefix is not valid anymore.

1.4 Applicability statement

The practices embodied in this document are considered to provide minimal support for hosts wishing to detect network attachment. Current work within the DNA working group aims to provide substantially improved performance for link change detection.

Existing limitations in base protocols such as IPv6 Neighbour Discovery preclude support of real-time applications in some environments. Future deployers and implementers are encouraged to consider the protocols under development at this time in order to provide a generic service to support hosts detecting change.

2. Configuration Practices for DNAv6 Routers

Routers which are being deployed to aid hosts' change detection procedures should attempt to use appropriate configurations, which limit advertisement latency, and provide appropriate service considering the constraints of the deployed access network technology.

This section describes several configuration parameters which may exist on IPv6 routers, and how their tuning may affect DNA hosts.

2.1 Multicast and Unicast RA Responses

While IPv6 Neighbour Discovery assumes that responses to solicitations will be sent multicast, the specification allows any router to respond to RS message with a unicast RA [1]. Note that the delay between 0 and MAX_RA_DELAY_TIME is still applicable when a

router responds to a RS with a unicast RA.

The advantage in responding with an unicast RA message is to allow the IP host to conclusively infer bi-directional reachability from the RS-RA exchange. Neighbour Discovery does not provide any mechanism to match multicast RA responses with their solicitation, and therefore it is not possible for the hosts to find out whether at least one of its RS messages was received and processed by the router. Since unicast RAs are only sent in response to solicitation, a host can infer that at least one of its Router Solicitations reached the router.

The dis-advantage in sending unicast RA is that the router will not be able to aggregate its response for multiple RS messages from multiple hosts received during the waiting period before RA transmission. Moreover, using unicast RA to respond to RS disables routers' ability to limit the rate of unicast RA.

For multicast Router Advertisements, a minimum separating delay exists so that these RAs may not be scheduled close to each other. When a host solicits and attempts to schedule a multicast RA within MIN_DELAY_BETWEEN_RAS (or MinDelayBetweenRAs from Mobile IPv6 [3]) of the previous multicast Router Advertisement, the scheduling of a response will be deferred until the minimum separation expires.

This separation delay does not affect unicast Router Advertisement responses. Routers MAY choose to respond to RS messages with a unicast RA response to avoid the delay introduced by the MIN_DELAY_BETWEEN_RAS restriction [1].

Where many unicast responses are scheduled awaiting transmission, Routers MAY consider aggregating them into a single multicast response if a multicast advertisement may be sent before the advertisements' scheduled transmission time.

It is noted that computational requirements for SEND may preclude this subsequent aggregation in some environments.

Where multiple unicast transmissions for the same destination await transmission, routers MAY remove all transmissions after the first without ill-effect, if a multicast RA is scheduled for the next possible response time.

In some cases it is not possible to provide unicast responses, since solicitations may be sent with an unspecified address, or solicitations do not provide enough link-layer addressing information to send an unicast response without neighbour discovery exchange. In these cases, a router may need to send multicast responses, even if

the expected delay is greater.

2.1.1 Recommendations

Routers SHOULD respond to a RS message with unicast RA message.

Routers SHOULD aggregate RA messages into a multi-cast RA message if more than 3 unicast RA messages are queued for transmission.

Where multiple unicast transmissions for the same destination await transmission, routers MAY remove all transmissions after the first without ill-effect.

2.2 Router Advertisement Parameters

Where hosts often change their link attachment (e.g., because they are mobile), there may be a number of prefixes or routers stored in the host's memory, which are no longer directly reachable. This additional storage may make movement detection slower where hosts rapidly pass through networks, or pass through networks which have very long advertised timeouts.

Routers SHOULD be configured to advertise non-default Valid and Preferred lifetimes in order to provide DNA hosts with link-specific address lifetime information.

Administrators are advised to set the advertised Preferred and Valid timers of prefixes to the maximum duration for which any host may be required to continue functioning without receiving a particular advertised prefix.

Where hosts with long-lifetime communications, or well known services (such as DNS) are present on a network, the preferred lifetime SHOULD be greater than the maximum expected outage time (For example, if the maximum router outage is 8.72 hours (for 0.999 uptime), the preferred lifetime could be set to 9 hours, which would be sufficient to support existing and allow new communications across the failure).

Upon links where fixed hosts are unlikely to be present, administrators SHOULD reduce the Router Lifetime, and Prefix Valid and Preferred Lifetimes on routers used to support DNA.

One potential configuration heuristic would be to configure lifetimes to be a low number (for example: 15) of times the MaxRtrAdvInterval, or greater than the lower quartile cell residence time of hosts on the network (if known). This allows reuse of configuration in the case where hosts are moving back and forth rapidly between links, but

allows rapid timeouts of old configurations.

The Router Lifetime MUST NOT be advertised as less than the MaxRtrAdvInterval unless the router is not to be used as a default [1].

Routers MUST NOT be configured with Valid or Preferred lifetime values lower than the MaxRtrAdvInterval. These minima ensure that lifetimes do not expire in between periodic Router Advertisements.

2.2.1 Recommendations

Routers SHOULD be configured to advertise non-default Valid and Preferred lifetimes in order to provide DNA hosts with link-specific address lifetime information.

Upon links where fixed hosts are unlikely to be present, administrators SHOULD reduce the Router Lifetime, and Prefix Valid and Preferred Lifetimes on routers used to support DNA.

The Router Lifetime MUST NOT be advertised as less than the MaxRtrAdvInterval unless the router is not to be used as a default [1].

Routers MUST NOT be configured with Valid or Preferred lifetime values lower than the MaxRtrAdvInterval.

2.3 Router Advertisement Options

When receiving a Router Advertisement from a particular router for the first time, a host needs to determine if the information contained in the RA indicates link change or that the transmitting router is part of the same link as another router it has already seen. It is not possible to do this unless global prefix information is included in the advertisement.

Routers SHOULD include at least one global Prefix Information Option in every Router Advertisement.

Mobile IPv6 introduced a new option for Router Advertisements, which indicates the current MaxRtrAdvInterval of router [3]. Reception of this option allows hosts to estimate whether they have missed Router Advertisements, and allows them to check reachability or discover new routers.

Routers SHOULD include Advertisement Interval options in Router Advertisements.

Mobile IPv6 adds the Router Address 'R' Flag to Prefix Information options [3]. This flag, when set indicates that the router's entire global address is configured and sent in the prefix information option. Bits beyond those specified in the prefix length field identify the router's Interface Identifier [5].

Hosts which are detecting network attachment can use a global router address to uniquely identify the router and link, rather than using link-local source addresses, which may be present on multiple links.

Routers SHOULD advertise at least one global address consistently in a Prefix Information Option, by setting the Router Address 'R' Flag.

2.3.1 Recommendations

Routers SHOULD include at least one global Prefix Information Option in every Router Advertisement.

Routers SHOULD include Advertisement Interval options in Router Advertisements.

Routers SHOULD advertise at least one global address consistently in a Prefix Information Option, by setting the Router Address 'R' Flag.

2.4 Triggered Router Advertisements

There are proposals for IPv6 Router Advertisements to be sent to hosts based on network side link-layer information.

Where these mechanisms exist they can provide Router Advertisements in the quickest possible time without need for Router Solicitation. These systems rely upon link-layer facilities are not available in all environments. Therefore, interested readers are referred to the individual methods' documentation [10].

2.5 Split Advertisements

A router may choose to split the options in the RA and send multiple RAs to reduce bandwidth overhead or to reduce the size of the RA to below the link MTU (section 6.2.3 of [1]).

If such a choice is made, average multicast RA time discussed in Appendix B increases for each subset of the prefixes included in the split RA messages.

Routers SHOULD consistently include one prefix in both sets of its RA

messages. This provide the host with a unique identifier based on the combination of link-local address and the constant prefix, to identify the router every time a RA message is received.

2.6 Router Configurations

Each router can have its own configuration with respect to sending RAs, and the treatment of router and neighbour solicitations. Different timers and constants might be used by different routers, such as the delay between Router Advertisements or delay before replying to a multicast RS. If a host is changing its IPv6 link, a newly seen router on that link may have a different configuration and may introduce more delay than the previous default router of the host.

While transitions between links under different administrative control are considered to be common, it is RECOMMENDED that network deployers adopt uniform configuration practices across routers on different links within the same logical domain, in order to provide consistent performance.

3. Topological Practices for DNAv6 Networks

IPv6 does not prefer one particular network topology over another and allows multiple routers and subnet prefixes to exist on one link. Different deployments of network elements and their configuration may impact on link change detection though. Effects and recommended practices for dealing with different network topologies are presented below.

3.1 Link Extent and Composition

Most of today's access networks deploy link-layer bridging technologies in order to extend their logical range beyond a single Medium Access Control domain.

Consequently, while many routers will come with traditional wired or optic-fibre interfaces, packets travelling within the same link may have been bridged across from a wired segment to a wireless segment.

In many of cases, the router will not have accurate information about the transmission rates or media of particular segments on the link. When defining the frequency at which RA will be sent over a link, Routers with interfaces whose technology is bridgeable SHOULD NOT assume that all segments and devices on the link have the same bandwidth available.

3.2 Multiple Router Links

IPv6 Neighbour Discovery allows multiple routers to be advertising on the same link [1]. These routers are not required to advertise the same prefixes as each other. This section provides some guidelines for deploying multiple routers on the same link.

While many routers may exist on a link, it is preferable to limit the number of advertising routers. There SHOULD NOT be more than three (3) routers advertising on a link. This will provide robustness in the case of RA packet loss, but provides a bound for bandwidth consumption.

Multiple routers responding to Router Solicitation will reduce the mean delay for solicitation, at the cost of additional traffic. For unicast responses, the delays may be halved for three responding routers.

Num advertising routers	1	2	3
Expected Unicast Delay	0.250s	0.167s	0.125s

If using advertising intervals lower than those specified in IPv6 Neighbour Discovery, only one router MAY advertise at the elevated rate. Other routers beyond the first SHOULD NOT have MinDelayBetweenRAs, MinRtrAdvInterval or MaxRtrAdvInterval less than the minima specified in IPv6 Neighbour Discovery [1][3].

Where it is possible, routers SHOULD include at least one common prefix in all of their Router Advertisement messages. This allows hosts to immediately see that both routers are on the same link.

3.3 Point-to-point Links

IPv6 Router Discovery mandates the delay of RA responses by stating (in section 6.2.6 of [1]):

> "In all cases, Router Advertisements sent in response to a
> Router Solicitation MUST be delayed by a random time
> between 0 and MAX_RA_DELAY_TIME seconds."

Cases where the router is on a point-to-point link, this restriction is too stringent as the router in question will be the only router on the link. Routers on such point-to-point links MAY avoid the delay by not waiting for the prescribed random time before responding for the Router Solicitation message [7] [9].

4. IANA Considerations

No action is required by IANA for this document

5. Security Considerations

When operating a network in support of hosts performing link change detection, both the operational security of the hosts and network infrastructure are important. DNA procedures rely upon rapid delivery of information to hosts using IPv6 Neighbour Discovery. Neighbour Discovery as a critical service in IPv6 networks is subject to various attacks as described in [6].

The following sections describe issues and practices to provide additional functional security for operators.

5.1 Providing Router Authorization

In DNA, some hosts will begin configuration procedures based on a single message transmitted by a router. As such the ability of routing infrastructure to prove its authenticity and authorization is important to support correct operation of hosts. Authentication and authorization mechanisms exist which allow hosts to check security of routers when they receive Router Advertisements indicating link change.

Today these mechanisms require additional message exchanges and public key operations to check the authorization chain back to a trusted root. Considering the computational cost for verifying certificates, it will be useful for administrators to attempt to minimize the length of these authorization chains.

Where a Router Advertisement is sent by a router, it SHOULD contain sufficient information to prove that the router is on the same link as previously seen advertisers, or is indeed the same router. This may prevent expensive checks by hosts which will not need to immediately test the authenticity of the router through signature verification, or additional transmissions. As described in section Section 3.2, advertising common prefixes achieves this goal.

Hosts which wish to have secured exchanges with neighbours and on-link routers may use Secured Neighbour Discovery (SEND) [4]. SEND provides authenticity as well as response matching, using nonces copied from solicitations into advertisements.

6. References

6.1 Normative References

[1] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[4] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

6.2 Informative References

[5] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

[6] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[7] Haskin, D. and E. Allen, "IP Version 6 over PPP", RFC 2472, December 1998.

[8] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[9] "3GPP TS 29.061 V5.5.0 (2003-03) Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) (Release 5)", TS 29.061, March 2003.

[10] Choi, J., "Fast Router Discovery with L2 support", draft-ietf-dna-frd-00 (work in progress), October 2005.

Authors' Addresses

Sathya Narayanan
Panasonic Princeton Lab
Two Research Way, 3rd Floor
Princeton, NJ 08536
USA

Phone: 609 734 7599
Email: sathya@Research.Panasonic.COM
URI:

Greg Daley
Panasonic Princeton Lab
Two Research Way, 3rd Floor
Princeton, NJ 08536
USA

Phone: 609 734 7334
Email: gregd@Research.Panasonic.COM
URI:

Nicolas Montavont
GET - ENST Bretagne
Departement RSM
2, rue de la chataigneraie
Cesson-Sevigne 35576
FRANCE

Phone: (33) 2 99 12 70 23
Email: nicolas.montavont@enst-bretagne.fr
URI: http://www.rennes.enst-bretagne.fr/~montavont/

Appendix A. Summary of Recommendations

It should be noted that many already deployed routers will not support these recommendations, and that hosts SHOULD NOT rely on their being in place, unless they have particular reason to do so.

Where many unicast responses are scheduled awaiting transmission, Routers MAY consider aggregating them into a single multicast response if a multicast advertisement may be sent before the advertisements' scheduled transmission time.

Where multiple unicast transmissions for the same destination await transmission, routers MAY remove all transmissions after the first

without ill-effect, if a multicast RA is scheduled for the next possible response time.

Routers MAY choose to respond to RS messages with a unicast RA response to avoid the delay introduced by the MIN_DELAY_BETWEEN_RAS restriction [1].

Routers SHOULD be configured to advertise non-default Valid and Preferred lifetimes in order to provide DNA hosts with link-specific address lifetime information.

Where hosts with ongoing transactions, or well known services are present on a network, this duration SHOULD be greater than the maximum expected outage time.

Upon links where fixed hosts are unlikely to be present, administrators SHOULD reduce the Router Lifetime, and Prefix Valid and Preferred Lifetimes on routers used to support DNA.

The Router Lifetime MUST NOT be advertised as less than the MaxRtrAdvInterval unless the router is not to be used as a default [1].

Routers MUST NOT be configured with Valid or Preferred lifetime values lower than the MaxRtrAdvInterval.

Routers SHOULD include at least one global Prefix Information Option in every Router Advertisement.

Routers SHOULD include Advertisement Interval options in Router Advertisements.

Routers SHOULD advertise at least one global address consistently in a Prefix Information Option, by setting the Router Address 'R' Flag.

A router MAY choose to split the options in the RA and send multiple RAs to reduce bandwidth overhead or to reduce the size of the RA to below the link MTU (see section 6.2.3 of [1]).

While transitions between links under different administrative control are considered to be common, it is RECOMMENDED that network deployers adopt uniform configuration practices across routers on different links within the same logical domain, in order to provide consistent performance.

Routers with interfaces whose technology is bridgeable SHOULD NOT assume that all segments and devices on the link have the same bandwidth available.

There SHOULD NOT be more than three (3) routers advertising on a link.

If using advertising intervals lower than those specified in IPv6 Neighbour Discovery, only one router MAY advertise at the elevated rate. Other routers beyond the first SHOULD NOT have MinDelayBetweenRAs, MinRtrAdvInterval or MaxRtrAdvInterval less than the minima specified in IPv6 Neighbour Discovery [1][3].

Where it is possible, routers SHOULD include at least one common prefix in all of their Router Advertisement messages.

Routers on point-to-point links MAY avoid delay by not waiting for the prescribed random time before responding for the Router Solicitation message [7] [9].

Considering the computational cost for verifying certificates, administrators SHOULD attempt to minimize the length of authorization chains.

Where a Router Advertisement is sent by a router, it SHOULD contain sufficient information to prove that the router is on the same link as previously seen advertisers, or is indeed the same router.

Routers supporting DNA SHOULD provide secured router discovery services using SEND [4].

On access networks supporting Detecting Network Attachment, administrators SHOULD configure routers to advertise at the shortest safe intervals.

Appendix B. Router Advertisement Rates

Unsolicited Router Advertisements are scheduled to be transmitted at a time between MinRtrAdvInterval and MaxRtrAdvInterval after the last multicast Router Advertisement. These parameters may be configured in the way which best suits the network. The table below summarizes the parameters as described by IPv6 Neighbour Discovery [1].

Timer	Maximum	Default	Minimum
MaxRtrAdvInterval	1800	600	4
MinRtrAdvInterval	594	198	3
Avg. Multicast RA time	1197	399	3.5

The load on the network, and the timeliness of any received information updates are therefore influenced by the router's advertisement parameters.

On access networks supporting Detecting Network Attachment, administrators SHOULD configure routers to advertise at the shortest safe intervals. Determination of the shortest safe intervals depends on topology, and the composition of the link, as described in Section 3.1.

Mobile IPv6 attempts to address the delays associated with hosts' movement and change detection by reducing the minimum settings for MinRtrAdvInterval to 30ms and MaxRtrAdvInterval to 70ms. Not all IPv6 routers support these configuration values today. Where hosts have no reactive way of detecting change, and do not solicit for Router Advertisements, these intervals may allow change detection sufficiently fast to support real-time applications.

The effect of these timers are summarized in the table below.

Timer	Maximum	Default	Minimum
MaxRtrAdvInterval	1800	600	0.07
MinRtrAdvInterval	594	198	0.03
Avg. Multicast RA time	1197	399	0.05

Where Mobile IPv6 is supported, the minimum values change, but the default timers are unmodified. If administrators wish to take advantage of shorter intervals between unsolicited RAs, explicit configuration is required. This is because the elevated rate of multicast RA transmission can have detrimental effects on some constrained links [3].

The minimum average for un-solicited Router Advertisements would be 20 messages per second. Assuming the minimum packet size for an RA with one prefix as 88 bytes, the bandwidth used will be 14 kbps. With SEND Options, and (somewhat weak) 1024-bit RSA keys, a single RA could be around 432 octets. This would consume approximately 69 kbps without considering link-layer overheads [4].

As described in Section 2.1, parameters may be chosen to optimize solicited behaviour in a way which limits the mean bandwidth overhead for unsolicited RAs.

A good example would be setting a MinRtrAdvInterval (along with MinDelayBetweenRAs) as 0.5 s, and the MaxRtrAdvInterval to 4s. This makes the mean delay before receiving an unsolicited RA 2.25 seconds, and limits the bandwidth utilization for unsolicited RAs (using the SEND example above) to 1.5 kbps, and the maximum multicast solicited rate to 6.9 kbps (one multicast RA each 0.5s).

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 Statement

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.

Acknowledgment

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