TOC

IPv6 Operations	T. Chown
Internet-Draft	University of Southampton
Intended status: Informational	S. Venaas
Expires: January 15, 2009	UNINETT
	July 14, 2008

Rogue IPv6 Router Advertisement Problem Statement
draft-chown-v6ops-rogue-ra-01

Status of this Memo

Abstract

When deploying IPv6 networks, whether IPv6-only or dual-stack, routers are configured to use IPv6 Router Advertisements to convey information to on link nodes that enable them to autoconfigure on the network. This information includes the implied default router address taken from the observed source address of the Router Advertisement (RA) message. However, in some networks 'bogus' RAs are observed, which may be present due to misconfigurations or possibly malicious attacks on the network. In this draft we summarise the scenarios in which rogue RAs may be observed, and we present a list of possible solutions to the problem. The goal of this draft is to present a framework around which solutions can be proposed and discussed.

Table of Contents

1. Introduction

TOC

The Neighbor Discovery protocol (Narten, T., Nordmark, E., Simpson, W., and H. Soliman, “Neighbor Discovery for IP version 6 (IPv6),” September 2007.) [RFC4861] describes the operation of IPv6 Router Advertisements (RAs), which are used during the IPv6 autoconfiguration process, whether stateful (via DHCPv6 (Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” July 2003.) [RFC3315] or DHCPv6 Light (Droms, R., “Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6,” April 2004.) [RFC3736]) or stateless (as per RFC4862 (Thomson, S., Narten, T., and T. Jinmei, “IPv6 Stateless Address Autoconfiguration,” September 2007.) [RFC4862]). In either case, the default router address is drawn directly from the source address of the RA message. In contrast to IPv4, there is no DHCPv6 option to configure a default gateway address.

In observing the operation of deployed IPv6 networks, it is apparent that there is a problem with undesired or 'bogus' IPv6 Router Advertisements (RAs) appearing on network links or subnets. By 'bogus' we mean RAs that were not the intended configured RAs, rather RAs that have appeared for some other reason.

The problem with rogue RAs is that they can cause partial or complete failure of operation on an IPv6 link. As such they are an operational issue for which solution(s) are required, and for which best practice needs to be conveyed.

In the next section, we discuss the scenarios that may give rise to rogue RAs being present. In the following section we present some candidate solutions for the problem, some of which may be more practical to deploy than others.

2. Bogus RA Scenarios

TOC

There are three broad classes of scenario in which bogus RAs may be introduced to an IPv6 network.

2.1. Administrator misconfiguration

TOC

Here an administrator incorrectly configures RAs on a router interface, causing incorrect RAs to appear on links and hosts to generate incorrect IPv6 address or other information. In this case the default gateway may be correct, but a host might for example become multi-addressed, possibly with a correct and incorrect address based on a correct and incorrect prefix. There is also the possibility of bad lifetime information being configured.

In the case of a Layer 2 VLAN misconfiguration, RAs may 'flood' to unintended links, causing hosts or more than one link to potentially become incorrectly multiaddressed, with possibly two different default routers available.

2.2. User misconfiguration

TOC

In this case a user's device 'accidentally' transmits RAs onto the local link, adding an addition default gateway and prefix information. This is typically seen on wireless (though sometimes wired) networks where a laptop has been used as a home gateway (e.g. a 6to4 gateway) and has then been attached to another network with the gateway configuration still active. A not infrequent cause here is the Windows Internet Connection Sharing service (ICS) which turns a host into a 6to4 gateway; this can be a useful feature, unless it is run when not intended. We have had reports that hosts may not see the genuine RAs on

link due to host firewalls, and then turning on a connection sharing service and 6to4 as a result.
There are also reported incidents in enterprise networks of users physically plugging Ethernet cables into the wrong sockets and bridging two subnets together, causing an problem similar to VLAN flooding.

2.3. Malicious misconfiguration

TOC

Here an attacker is deliberately generating RAs on the local network in an attempt to perform some form of denial of service or man-in-the-middle attack.

3. Methods to Mitigate against Rogue RAs

TOC

In this section we present a summary of methods suggested to date for reducing or removing the possibility of rogue RAs being seen on a network.

3.1. Manual configuration

TOC

The default gateway can usually be manually configured on a device. This is of course a resource intensive solution, and also prone to mistakes in itself.

3.2. Secure Neighbor Discovery

TOC

The SEND (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.) [RFC3971] protocol provides a method for hosts and routers to perform secure Neighbor Discovery. At present there are very few SEND implementations available, and SEND is perceived as a complex protocol to deploy. It is also likely that not all scenarios will be able to use SeND, for various reasons.

TOC

3.3. Introduce RA snooping

It should be possible to implement 'RA snooping' in Layer 2 switches in a similar way to DHCP snooping, such that RAs observed from incorrect sources are blocked or dropped, and not propagated through a subnet. One candidate solution in this space called RA-Guard [ra-guard] (Van de Velde, G., Levy-Abegnoli, E., Popoviciu, C., and J. Mohacsi, “IPv6 RA-Guard (draft-ietf-v6ops-ra-guard-00),” July 2008.) has recently been proposed. This type of solution has appeal because it is a familiar model for enterprise network managers, but it can also be used to complement SeND.
It is interesting to note that the Windows ICS that runs a 6to4 gateway also starts an IPv4 DHCP service, so any snooping solution is mitigating against both these issues.
This type of solution may not be applicable everywhere, e.g. in environments where there are not centrally controlled switches.

3.4. Use the Router Preference Option

TOC

RFC4191 (Draves, R. and D. Thaler, “Default Router Preferences and More-Specific Routes,” November 2005.) [RFC4191] introduced router preference options, such that an RA could carry one of three router preference values: High, Medium (default) or Low. Thus an administrator could use High settings for managed RAs, and hope that 'accidental' RAs would be medium priority, and that hosts implemented this optional protocol.

3.5. Rely on Layer 2 admission control

TOC

In principle, if a technology such as IEEE 802.1x is used, devices would first need to authenticate to the network before being able to send or receive IPv6 traffic. Ideally authentication would be mutual. This may mitigate against a malicious attacker, but doesn't address the misconfiguration issues.

3.6. Use host-based packet filters

TOC

In a managed environment hosts could be configured via their 'personal firewall' to only accept RAs from trusted sources. However, the problem is then pushed to keeping this configuration maintained and correct. If a router fails and is replaced, possibly with a new Layer 2 interface address, the link local source address in the filter may be incorrect and no network exists to push the new information to the host. Also, hosts could potentially be configured to discard 6to4-based RAs in a managed enterprise environment.

3.7. Use an 'intelligent' deprecation tool

TOC

It could be possible to run a daemon on a link (perhaps on the router on the link) to watch for incorrect RAs and to send a deprecating RA with router lifetime of zero when such an RA is observed. The KAME rafixd is an example of such a tool, which has been used at IETF meetings with some success. Whether or not such a tool is the preferred method, monitoring a link for observed RAs seems prudent from a network management perspective. Some such tools exist already, e.g. ndpmon.

3.8. Wait before using new advertisements

TOC

It might be possible, in generally static networks, to configure an option such that any new RAs that are seen are not acted upon for a certain period, e.g. 2 hours. This might allow time for a misconfiguration or accidental RA to be detected and stopped, before hosts use the data in the RA. Of course this would add delays where genuine new RAs are required, while new hosts appearing on a network would still be vulnerable (or be unable to configure at all).

3.9. Add a Default Gateway Option to DHCPv6

TOC

It may be possible to define a new Default Gateway Option for DHCPv6 that would allow network administrators to only have hosts use DHCPv6 for default gateway configuration in managed networks. While such an option could be defined, its ramifications remain unclear. In the absence of RAs, other configuration information would also be missing, e.g. on-link prefix information. Of course, it may be that an RA is still required to inform the host to use DHCPv6, and that may introduce a Catch-22 unless hosts are configured directly to only use DHCPv6. An advantage of DHCPv6 is that should an error be introduced, only hosts that have refreshed their DHCP information since that time are affected, while a rogue RA will most likely affect all hosts immediately. DHCPv6 also allows different answers to be given to different hosts.

One objection to introducing such an option is that DHCPv6 in itself is not a secure protocol, and it is also of course subject to misconfigurations, accidental or otherwise. Comparing the threat model for rogue RAs and rogue DHCPv6 servers is an interesting exercise in itself. Use of Authenticated DHCP is currently minimal and thus the (lack of) security is just pushed to another place, albeit one that site administrators are more familiar and (rightly or wrongly) comfortable with.

4. Other considerations

TOC

There are other general observations that have been made.
One is that it would generally be prudent for network monitoring or management platforms to be able to observe and report on observed RAs, and whether unintended RAs (possibly from unintended sources) are present on a network. Further, it may be useful for individual hosts to be able to report their address status, e.g. this could be useful during an IPv6 renumbering phased process as described in RFC4192 (Baker, F., Lear, E., and R. Droms, “Procedures for Renumbering an IPv6 Network without a Flag Day,” September 2005.) [RFC4192].
The second is how readily a host can recover from bad configuration information, e.g. considering the '2 hour rule' of Section 5.5.3 of RFC4862 (though this applies to the prefix lifetime not the router lifetime). We should ensure that methods exist for a network administrator to correct bad configuration information on a link or subnet, and that OS platforms support these methods. At least if the problem can be detected, and corrected promptly, the impact is minimised.
A comment has been made that in the case of 6to4 being run by a host on a subnet that is not administratively configured with IPv6, some OSes or applications may begin using IPv6 to the 6to4 host (router) rather than IPv4 to the intended default IPv4 router. Mitigating against this condition can also be seen to be important.

5. Conclusions

TOC

In this text we have described scenarios via which rogue Router Advertisements (RAs) may appear on a network, and some measures that could be used to mitigate against these.
While SEND perhaps offers the most robust solution, implementations are not widely available, and the solution is perceived as complex (parallels can possibly be drawn with Authenticated DHCP in terms of likely deployment). Adding a new DHCPv6 Default Gateway Option would allow configuration by DHCP, and be a method that IPv4 administrators

are comfortable with (for better or worse), but such an option would have significant impacts elsewhere, and in any event one must recognise that the security risk is then simply shifted elsewhere.

Further feedback on the solutions is certainly welcome. In the meantime, perhaps the simplest initial step would be for RA snooping to be defined and deployed for Layer 2 devices, in such a way that can address (shared) wireless as well as wired networks. One draft proposal in this space, RA-Guard, has recently been published [ra-guard] (Van de Velde, G., Levy-Abegnoli, E., Popoviciu, C., and J. Mohacsi, “IPv6 RA-Guard (draft-ietf-v6ops-ra-guard-00),” July 2008.). Alternatively, certain switch platforms can already implement a form of snooping by the administrator configuring Access Control Lists (ACLs) that block RA ICMP messages that might be inbound on 'user' ports. A cleaner solution is desirable though.

This topic has also highlighted that some DHCPv6 on-link prefix option may be useful for some scenarios, caused in part by the change of the 'default on-link' rule. This should be seen as independent of whether DHCPv6 is extended to add a Default Gateway Option, which is another open question at this time.

The material presented here is relevant to the IETF dhc and v6ops working groups, but the text is labeled as v6ops due to its operational issue focus. Should new DHCP features be defined as a result, we assume these would be presented within the dhc working group.

6. Security Considerations

TOC

There are no extra Security consideration for this document.

7. IANA Considerations

TOC

There are no extra IANA consideration for this document.

8. Acknowledgments

TOC

Thanks are due to members of the IETF IPv6 Operations and DHCP WGs for their inputs on this topic, including but not limited to Iljitsch van Beijnum, David Malone, Tony Hain, Christian Huitema, Remi Denis-Courmant, Chip Popoviciu, Dave Thaler and Tatuya Jinmei.

9. Informative References

TOC

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” RFC 3315, July 2003 (TXT).

[RFC3736] Droms, R., “Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6,” RFC 3736, April 2004 (TXT).

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” RFC 3971, March 2005 (TXT).

[RFC4191] Draves, R. and D. Thaler, “Default Router Preferences and More-Specific Routes,” RFC 4191, November 2005 (TXT).

[RFC4192] Baker, F., Lear, E., and R. Droms, “Procedures for Renumbering an IPv6 Network without a Flag Day,” RFC 4192, September 2005 (TXT).

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, “Neighbor Discovery for IP version 6 (IPv6),” RFC 4861, September 2007 (TXT).

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, “IPv6 Stateless Address Autoconfiguration,” RFC 4862, September 2007 (TXT).

[ra-guard] Van de Velde, G., Levy-Abegnoli, E., Popoviciu, C., and J. Mohacsi, “IPv6 RA-Guard (draft-ietf-v6ops-ra-guard-00),” July 2008.

Authors' Addresses

TOC

Tim Chown
University of Southampton
Southampton, Hampshire SO17 1BJ
United Kingdom
Email: tjc@ecs.soton.ac.uk

Stig Venaas
UNINETT
Trondheim NO 7465
Norway
Email: venaas@uninett.no

Full Copyright Statement

TOC

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 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.

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.