Rogue IPv6 Router Advertisement Problem Statement

Abstract

   When deploying IPv6, whether IPv6-only or dual-stack, routers are
   configured to send IPv6 Router Advertisements (RAs) to convey
   information to 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 RA message, as
   well as on-link prefix information. However, unintended
   misconfigurations by users or administrators, or possibly malicious
   attacks on the network, may lead to bogus RAs being present, which in
   turn can cause operational problems for hosts on the network. In
   this document, we summarise the scenarios in which rogue RAs may be
   observed and present a list of possible solutions to the problem. We
   focus on the unintended causes of rogue RAs in the text. The goal of
   this text is to be Informational, and as such to present a framework
   around which solutions can be proposed and discussed.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Not all documents
   approved by the IESG are a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6104.

Table of Contents

1. Introduction

   The Neighbor Discovery protocol [RFC4861] describes the operation of
   IPv6 Router Advertisements (RAs) that are used to determine node
   configuration information during the IPv6 autoconfiguration process,
   whether that node's configuration is stateful, via the Dynamic Host
   Configuration Protocol for IPv6 (DHCPv6) [RFC3315] or stateless, as
   per [RFC4862], possibly in combination with DHCPv6 Light [RFC3736].

   In observing the operation of deployed IPv6 networks, it is apparent
   that there is a problem with undesired or "bogus" IPv6 RAs appearing
   on network links or subnets. By "bogus" we mean RAs that were not
   the intended configured RAs, but rather RAs that have appeared for
   some other reason. While the problem appears more common in shared
   wireless environments, it is also seen on wired enterprise networks.

   The problem with rogue RAs is that they can cause partial or complete
   failure of operation of hosts on an IPv6 link. For example, the
   default router address is drawn directly from the source address of
   the RA message. In addition, rogue RAs can cause hosts to assume
   wrong prefixes to be used for stateless address autoconfiguration.
   In a case where there may be mixing of "good" and "bad" RAs, a host
   might keep on using the "good" default gateway, but pick a wrong
   source address, leading to egress filtering problems. As such, rogue
   RAs are an operational issue for which solution(s) are required, and
   for which best practice needs to be conveyed. This not only includes
   preventing or detecting rogue RAs, but also where necessary ensuring
   the network (and hosts on the network) have the ability to quickly
   recover from a state where host configuration is incorrect as a
   result of processing such an RA.

   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. This document focuses on
   "accidental" rogue RAs; while malicious RAs are of course also
   possible, the common problem today lies with unintended RAs. In
   addition, a network experiencing malicious attack of this kind is
   likely to also experience malicious Neighbor Advertisement (NA) and
   related messages.

2. Bogus RA Scenarios

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

2.1. Administrator Misconfiguration

   Here an administrator incorrectly configures RAs on a router
   interface, causing incorrect RAs to appear on links and causing hosts
   to generate incorrect or unintended IPv6 address, gateway, or other
   information. In such a case, the default gateway may be correct, but
   a host might for example become multiaddressed, possibly with a
   correct and incorrect address based on a correct and incorrect
   prefix. There is also the possibility of other configuration
   information being misconfigured, such as the lifetime option.

   In the case of a Layer 2 IEEE 802.1Q Virtual LAN (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

   In this case, a user's device "accidentally" transmits RAs onto the
   local link, potentially adding an additional default gateway and
   associated prefix information.

   This seems to typically be seen on wireless (though sometimes wired)
   networks where a laptop has enabled the Windows Internet Connection
   Sharing (ICS) service, which can turn a host into a 6to4 [RFC3056]
   gateway; this can be a useful feature, unless of course it is run
   when not intended. This service can also cause IPv4 problems, as it
   will typically start a "rogue" DHCPv4 server on the host.

   We have also had reports that hosts may not see genuine IPv6 RAs on a
   link due to host firewalls, causing them to turn on a connection-
   sharing service and 6to4 as a result. In some cases, more technical
   users may also use a laptop as a home gateway (e.g., again a 6to4
   gateway) and then connect to another network, forgetting their
   previous gateway configuration is still active.

   There are also reported incidents in enterprise networks of users
   physically plugging Ethernet cables into the wrong sockets and
   bridging two subnets together, causing a problem similar to VLAN
   flooding.

2.3. Malicious Misconfiguration

   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.

As stated above, while this is a genuine concern for network
administrators, there have been few if any reports of such activity,
while in contrast reports of accidental rogue RAs are very
commonplace. In writing this text, and with the feedback of the
v6ops working group, we came to the conclusion that the issue of
malicious attack, due to the other complementary attacks that are
likely to be launched using rogue NA and similar messages, are best
considered by further work and document(s). As a result, this text
intends to provide informational guidance for operators looking for
practical measures to take to avoid "accidental" rogue RAs on their
own networks.

3. Methods to Mitigate against Rogue RAs

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

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

Manual configuration implies that RA processing is disabled. Most
operating systems allow RA messages to be ignored, such that if an
IPv6 address is manually configured on a system, an additional global
autoconfigured address will not be added should an unexpected RA
appear on the link.

3.2. Introducing 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"
[RFC6105], has 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 SEcure Neighbor Discovery (SEND)
[RFC3971], by a switch acting as a SEND proxy for hosts.

This type of solution may not be applicable everywhere, e.g., in
environments where there are not centrally controlled or manageable
switches.

3.3. Using ACLs on Managed Switches

   Certain switch platforms can already implement some level of rogue RA
   filtering by the administrator configuring Access Control Lists
   (ACLs) that block RA ICMP messages that might be inbound on "user"
   ports. Again this type of "solution" depends on the presence of such
   configurable switches.

   A recent document describes the RA message format(s) for filtering
   [IPv6-AUTOCFG-FILTER]. The document also notes requirements for
   DHCPv6 snooping, which can then be implemented similarly to DHCPv4
   snooping.

3.4. SEcure Neighbor Discovery (SEND)

   The SEcure Neighbor Discovery (SEND) [RFC3971] protocol provides a
   method for hosts and routers to perform secure Neighbor Discovery.
   Thus, it can in principle protect a network against rogue RAs.

   SEND is not yet widely used at the time of writing, in part because
   there are very few implementations of the protocol. Some other
   deployment issues have been raised, though these are likely to be
   resolved in due course. For example, routers probably don't want to
   use autogenerated addresses (which might need to be protected by
   ACLs), so SEND needs to be shown to work with non-autogenerated
   addresses. Also, it has been argued that there are "bootstrapping"
   issues, in that hosts wanting to validate router credentials (e.g.,
   to a certificate server or Network Time Protocol (NTP) server) are
   likely to need to communicate via the router for that information.

   Further, it's not wholly clear how widely adopted SEND could or would
   be in site networks with "lightweight" security (e.g., many campus
   networks), especially where hosts are managed by users and not
   administratively. Public or conference wireless networks may face
   similar challenges. There may also be networks, like perhaps sensor
   networks, where use of SEND is less practical. These networks still
   require rogue RA protection.

   While SEND clearly can provide a good, longer-term solution,
   especially in networks where malicious activity is a significant
   concern, there is a requirement today for practical solutions, and/or
   solutions more readily applicable in more "relaxed" environments. In
   the latter case, solutions like "RA snooping" or applied ACLs are
   more attractive now.

3.5. Router Preference Option

   [RFC4191] introduced a Router Preference option, 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. This of course would only work in some scenarios -- if the
   user who accidentally sends out a rogue RA on the network has
   configured their device with "High" precedence for their own intended
   usage, the priorities would clash. But for accidental rogue RAs
   caused by software like Windows ICS and 6to4, which would use the
   default precedence, it could be useful. Obviously this solution
   would also rely on clients (and routers) having implementations of
   the Router Preference option.

3.6. Relying on Layer 2 Admission Control

   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. Deployment of 802.1x, with mutual authentication, may
   however be seen as somewhat "heavyweight", akin to SEND, for some
   deployments.

   Improving Layer 2 security may help to mitigate against an attacker's
   capability to join the network to send RAs, but it doesn't prevent
   misconfiguration issues. A user can happily authenticate and still
   launch a Windows ICS service, for example.

3.7. Using Host-Based Packet Filters

   In a managed environment, hosts could be configured via their
   "personal firewall" to only accept RAs from trusted sources. Hosts
   could also potentially be configured to discard 6to4-based RAs in a
   managed enterprise environment.

   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 become incorrect, and thus no method would be
   available to push the new information to the host over the network.

3.8. Using an "Intelligent" Deprecation Tool

   It is 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 a 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. A slightly enhanced tool called RAMOND
has since been developed from this code, and is now available as a
Sourceforge project. As with host-based firewalling, the daemon
would need to somehow know what "good" and "bad" RAs are, from some
combination of known good sources and/or link prefixes. In an
environment with native IPv6, though, 6to4-based RAs would certainly
be known to be rogue.

Whether or not use of 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, which can
also detect other undesirable behaviour.

3.9. Using Layer 2 Partitioning

If each system or user on a network is partitioned into a different
Layer 2 medium, then the impact of rogue RAs can be limited. In
broadband networks, bridging [RFC2684] may be available, for example.
The benefit may be scenario-specific, e.g., whether a given user or
customer has their own network prefix or whether the provisioning is
in a shared subnet or link. It is certainly desirable that any given
user or customer's system(s) are unable to see RAs that may be
generated by other users or customers.

However, such partitioning would probably increase address space
consumption significantly if applied in enterprise networks, and in
many cases, hardware costs and software licensing costs to enable
routing to the edge can be quite significant.

3.10. Adding Default Gateway/Prefix Options to DHCPv6

Adding Default Gateway and Prefix options for DHCPv6 would allow
network administrators to configure hosts to only use DHCPv6 for
default gateway and prefix configuration in managed networks, where
RAs would be required today. A new document has proposed such a
default router option, along with prefix advertisement options for
DHCPv6 [DHCPv6-DEFAULT-RTR]. Even with such options added to DHCPv6,
an RA is in principle still required to inform hosts to 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 multicast rogue RA will most likely affect all
hosts immediately. DHCPv6 also allows different answers to be given
to different hosts.

While making host configuration possible via DHCPv6 alone is a viable
option that would allow IPv6 configuration to be done in a way
similar to IPv4 today, the problem has only been shifted: rather than

rogue RAs being the problem, rogue DHCPv6 servers would be an
equivalent issue. As with IPv4, a network would then still require
use of Authenticated DHCP, or DHCP(v6) snooping, as suggested in
[IPv6-AUTOCFG-FILTER].

There is certainly some demand in the community for DHCPv6-only host
configuration. While this may mitigate the rogue RA issue, it simply
moves the trust problem elsewhere, albeit to a place administrators
are familiar with today.

4. Scenarios and Mitigations

In this section, we summarise the error/misconfiguration scenarios
and practical mitigation methods described above in a matrix format.
We consider, for the case of a rogue multicast RA, which of the
mitigation methods helps protect against administrator and user
errors. For the administrator error, we discount an error in
configuring the countermeasure itself; rather, we consider an
administrator error to be an error in configuration elsewhere in the
network.

Mitigation Method	Scenario	
	Admin Error	User Error
Manual configuration	Y	Y
SEND	Y	Y
RA snooping	Y	Y
Use switch ACLs	Y	Y
Router preference	N	Y
Layer 2 admission	N	N
Host firewall	Y	Y
Deprecation daemon	Y	Y
Layer 2 partition	N	Y
DHCPv6 gateway option	Partly	If Auth

   What the above summary does not consider is the practicality of
   deploying the measure. An easy-to-deploy method that buys improved
   resilience to rogue RAs without significant administrative overhead
   is attractive. On that basis, the RA snooping proposal, e.g.,
   RA-Guard, has merit, while approaches like manual configuration are
   less appealing. However, RA-Guard is not yet fully defined or
   available, while only certain managed switch equipment may support
   the required ACLs.

5. Other Related Considerations

   There are a number of related issues that have come out of
   discussions on the rogue RA topic, which the authors believe are
   worth capturing in this document.

5.1. Unicast RAs

   The above discussion was initially held on the assumption that rogue
   multicast RAs were the cause of problems on a shared network subnet.
   However, the specifications for Router Advertisements allow them to
   be sent unicast to a host, as per Section 6.2.6 of RFC 4861. If a
   host sending rogue RAs sends them unicast to the soliciting host,
   that RA may not be seen by other hosts on the shared medium, e.g., by
   a monitoring daemon. In most cases, though, an accidental rogue RA
   is likely to be multicast.

5.2. The DHCP versus RA Threat Model

   Comparing the threat model for rogue RAs and rogue DHCPv6 servers is
   an interesting exercise. In the case of Windows ICS causing rogue
   6to4-based RAs to appear on a network, it is very likely that the
   same host is also acting as a rogue IPv4 DHCP server. The rogue
   DHCPv4 server can allocate a default gateway and an address to hosts,
   just as a rogue RA can lead hosts to learning of a new (additional)
   default gateway, prefix(es), and address. In the case of multicast
   rogue RAs, however, the impact is potentially immediate to all hosts,
   while the rogue DHCP server's impact will depend on lease timers for
   hosts.

   In principle, Authenticated DHCP can be used to protect against rogue
   DHCPv4 (and DHCPv6) servers, just as SEND could be used to protect
   against rogue IPv6 RAs. However, actual use of Authenticated DHCP in
   typical networks is currently minimal. Were new DHCPv6 default
   gateway and prefix options to be standardised as described above,
   then without Authenticated DHCP the (lack of) security is just pushed
   to another place.

   The RA-Guard approach is essentially using a similar model to DHCP
   message snooping to protect against rogue RAs in network (switch)
   equipment. As noted above, DHCPv6 message snooping would also be
   very desirable in IPv6 networks.

5.3. IPv4-Only Networks

   The rogue RA problem should also be considered by administrators and
   operators of IPv4-only networks, where IPv6 monitoring, firewalling,
   and other related mechanisms may not be in place.

   For example, 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,
   because they have IPv6 enabled by default and some applications
   prefer IPv6 by default. Technically aware users may also
   deliberately choose to use IPv6, possibly for subversive reasons.
   Mitigating against this condition can also be seen to be important.

5.4. Network Monitoring Tools

   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 (assuming their configuration
   status allowed it, of course), e.g., this could be useful during an
   IPv6 renumbering phased process as described in RFC 4192 [RFC4192].

   The above assumes, of course, that what defines a "good" (or "bad")
   RA can be configured in a trustworthy manner within the network's
   management framework.

5.5. Recovering from Bad Configuration State

   After a host receives and processes a rogue RA, it may have multiple
   default gateways, global addresses, and potentially clashing RA
   options (e.g., M/O bits [RFC4861]). The host's behaviour may then be
   unpredictable, in terms of the default router that is used, and the
   (source) address(es) used in communications. A host that is aware of
   protocols such as Shim6 [RFC5533] may believe it is genuinely
   multihomed.

   An important issue is how readily a host can recover from receiving
   and processing bad configuration information, e.g., considering the
   "2 hour rule" mentioned in Section 5.5.3 of RFC 4862 (though this
   applies to the valid address lifetime and 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.

5.6. Isolating the Offending Rogue RA Source

   In addition to issuing a deprecating RA, it would be desirable to
   isolate the offending source of the rogue RA from the network. It
   may be possible to use Network Access Control methods to quarantine
   the offending host, or rather the network point of attachment or port
   that it is using.

6. Conclusions

   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. We have also noted some
   related issues that have arisen in the rogue RA discussions. Our
   discussion is generally focused on the assumption that rogue RAs are
   appearing as a result of accidental misconfiguration on the network,
   by a user or administrator.

   While SEND perhaps offers the most robust solution, implementations
   and deployment guidelines are not yet widely available. SEND is very
   likely to be a good, longer-term solution, but many administrators
   are seeking solutions today. Such administrators are also often in
   networks with security models for which SEND is a "heavyweight"
   solution, e.g., campus networks, or wireless conference or public
   networks. For such scenarios, simpler measures are desirable.

   Adding new DHCPv6 Default Gateway and Prefix options would allow IPv6
   host configuration by DHCP only and would be a method that IPv4
   administrators are comfortable with (for better or worse), but this
   simply shifts the robustness issue elsewhere.

   While a number of the mitigations described above have their appeal,
   the simplest solutions probably lie in switch-based ACLs and
   RA-Guard-style approaches. Where managed switches are not available,
   use of the Router Preference option and (more so in managed desktop
   environments) host firewalls may be appropriate.

   In the longer term, wider experience of SEND will be beneficial,
   while the use of RA snooping will remain useful either to complement
   SEND (where a switch running RA-Guard can potentially be a SEND
   proxy) or to assist in scenarios for which SEND is not deployed.

7. Security Considerations

   This Informational document is focused on discussing solutions to
   operational problems caused by rogue RAs resulting from unintended
   misconfiguration by users or administrators. Earlier versions of
   this text included some analysis of rogue RAs introduced maliciously;
   e.g., the text included an extra column in the matrix in Section 4.
   However, the consensus of the v6ops working group feedback was to
   instead focus on the common operational problem of "accidental" rogue
   RAs seen today.

   Thus, the final version of this text does not address attacks on a
   network where rogue RAs are intentionally introduced as part of a
   broader attack, e.g., including malicious NA messages. On the wire,
   malicious rogue RAs will generally look the same as "accidental"
   ones, though they are more likely, for example, to spoof the Media
   Access Control (MAC) or IPv6 source address of the genuine router, or
   to use a "High" Router Preference option. It is also likely that
   malicious rogue RAs will be accompanied by other attacks on the IPv6
   infrastructure, making discussion of mitigations more complex.
   Administrators may be able to detect such activity by the use of
   tools such as NDPMon.

   It is worth noting that the deprecation daemon could be used as part
   of a denial-of-service attack, should the tool be used to deprecate
   the genuine RA.

8. Acknowledgments

   Thanks are due to members of the IETF IPv6 Operations and DHCP
   working groups for their inputs on this topic, as well as some
   comments from various operational mailing lists, and private
   comments, including but not limited to: Iljitsch van Beijnum, Dale
   Carder, Remi Denis-Courmont, Tony Hain, Bob Hinden, Christian
   Huitema, Tatuya Jinmei, Eric Levy-Abegnoli, David Malone, Thomas
   Narten, Chip Popoviciu, Dave Thaler, Gunter Van de Velde, Goeran
   Weinholt, and Dan White.

9. Informative References

   [RFC2684] Grossman, D. and J. Heinanen, "Multiprotocol Encapsulation
              over ATM Adaptation Layer 5", RFC 2684, September 1999.

   [RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains
              via IPv4 Clouds", RFC 3056, February 2001.

   [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.

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

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

   [RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and
              More-Specific Routes", RFC 4191, November 2005.

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

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

   [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless
              Address Autoconfiguration", RFC 4862, September 2007.

   [RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming
              Shim Protocol for IPv6", RFC 5533, June 2009.

   [RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J.
              Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105,
              February 2011.

   [IPv6-AUTOCFG-FILTER]
              Ward, N., "IPv6 Autoconfig Filtering on Ethernet
              Switches", Work in Progress, March 2009.

   [DHCPv6-DEFAULT-RTR]
              Droms, R. and T. Narten, "Default Router and Prefix
              Advertisement Options for DHCPv6", Work in Progress,
              March 2009.

Authors' Addresses

   Tim Chown
   University of Southampton
   Highfield
   Southampton, Hampshire SO17 1BJ
   United Kingdom

   EMail: tjc@ecs.soton.ac.uk

   Stig Venaas
   Cisco Systems
   Tasman Drive
   San Jose, CA 95134
   USA

   EMail: stig@cisco.com