OPsec Working Group
Internet-Draft
Intended status: Informational
Expires: January 24, 2015

M. Behringer
E. Vyncke
Cisco

July 23, 2014

Using Only Link-Local Addressing Inside an IPv6 Network
draft-ietf-opsec-lla-only-09

Abstract

In an IPv6 network it is possible to use only link-local addresses on infrastructure links between routers. This document discusses the advantages and disadvantages of this approach to help the decision process for a given network.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 24, 2015.

Table of Contents

1. Introduction

An infrastructure link between a set of routers typically does not require global or unique local addresses [RFC4193]. Using only link-local addressing on such links has a number of advantages. For example, that routing tables do not need to carry link addressing, and can therefore be significantly smaller. This helps to decrease failover times in certain routing convergence events. An interface of a router is also not reachable beyond the link boundaries, therefore reducing the attack horizon.

This document discusses the advantages and caveats of this approach.

Note that some traditionally used techniques to operate a network such as pinging interfaces, or seeing interface information in a traceroute do not work with this approach. Details are discussed below.

During IESG review the technical correctness and completeness of the document has been fully reviewed and verified, However, IESG noted that there was no full consensus within the working group on whether to recommend this technique.

2. Using Link-Local Addressing on Infrastructure Links

This document discusses the approach of using only link-local addresses (LLA) on all router interfaces on infrastructure links. Routers don't typically need to receive packets from hosts or nodes outside the network. For a network operator, there may be reasons to use greater than link-local scope addresses on infrastructure interfaces for certain operational tasks, such as pings to an interface or traceroutes across the network. This document discusses such cases and proposes alternative procedures.

2.1. The Approach

In this approach neither globally routed IPv6 addresses nor unique local addresses are configured on infrastructure links. In the absence of specific global or unique local address definitions, the default behavior of routers is to use link-local addresses notably for routing protocols.

The sending of ICMPv6 [RFC4443] error messages (packet-too-big, time-exceeded...) is required for routers. Therefore, another interface must be configured with an IPv6 address with a greater scope than link-local. This address will usually be a loopback interface with a global scope address belonging to the operator and part of an announced prefix (with a suitable prefix length) to avoid being dropped by other routers implementing [RFC3704]. This is implementation dependent. For the remainder of this document we will refer to this interface as a "loopback interface".

[RFC6724] recommends that greater than link-local scope IPv6 addresses are used as the source IPv6 address for all generated ICMPv6 messages sent to a non-link-local address, with the exception of ICMPv6 redirect messages, as defined in [RFC4861] section 4.5.

The effect on specific traffic types is as follows:

- Most control plane protocols, such as BGP [RFC4271], ISIS [IS-IS], OSPFv3 [RFC5340], RIPng [RFC2080], PIM [RFC4609] work by default or can be configured to work with link-local addresses. Exceptions are explained in the caveats section (Section 2.3).

- Management plane traffic, such as SSH [RFC4251], Telnet [RFC0495], SNMP [RFC1157], and ICMPv6 echo request [RFC4443], can use the address of the router loopback interface as the destination address. Router management can also be done over out-of-band channels.

- ICMP error messages are usually sourced from a loopback interface with a greater than link-local address scope. [RFC4861] section 4.5 explains one exception: ICMP redirect messages can also be sourced from a link-local address.

- Data plane traffic is forwarded independently of the link address type.

- Neighbor discovery (neighbor solicitation and neighbor advertisement) is done by using link-local unicast and multicast addresses. Therefore neighbor discovery is not affected.

We therefore conclude that it is possible to construct a working network in this way.

2.2. Advantages

The following list of advantages is in no particular order.

Smaller routing tables: Since the routing protocol only needs to carry one global address (the loopback interface) per router, it is smaller than the traditional approach where every infrastructure link address is carried in the routing protocol. This reduces memory consumption, and increases the convergence speed in some routing failover cases. Because the Forwarding Information Base to be downloaded to line cards is smaller and there are fewer prefixes in the Routing Information Base, the routing algorithm is accelerated. Note: smaller routing tables can also be achieved by putting interfaces in passive mode for the Interior Gateway Protocol (IGP).

Simpler address management: Only loopback interface addresses need to be considered in an addressing plan. This also allows for easier renumbering.

Lower configuration complexity: link-local addresses require no specific configuration, thereby lowering the complexity and size of router configurations. This also reduces the likelihood of configuration mistakes.

Simpler DNS: Less routable address space in use also means less reverse and forward mapping DNS resource records to maintain. Of course, if the operator selects not to enter any global interface addresses in the DNS anyway, then this is less of an advantage.

Reduced attack surface: Every routable address on a router constitutes a potential attack point: a remote attacker can send traffic to that address. Examples are a TCP SYN flood (see [RFC4987]) and SSH brute force password attacks. If a network only uses the addresses of the router loopback interface(s), only those addresses need to be protected from outside the network. This may ease protection measures, such as infrastructure access control lists (iACL).

Without using link-local addresses, it is still possible to achieve the simple iACL if the network addressing scheme is set up such that all link and loopback interfaces have greater than link-local addresses and are aggregatable, and if the infrastructure access list covers that entire aggregated space. See also [RFC6752] for further discussion on this topic.

[RFC6860] describes another approach to hide addressing on infrastructure links for OSPFv2 and OSPFv3, by modifying the existing protocols. This document does not modify any protocol, however it works only for IPv6.

2.3. Caveats

The caveats listed in this section are in no particular order.

Interface ping: if an interface doesn't have a routable address, it can only be pinged from a node on the same link. Therefore, it is not possible to ping a specific link interface remotely. A possible workaround is to ping the loopback address of a router instead. In most cases today, it is not possible to see which link the packet was received on; however, [RFC5837] suggests including the interface identifier of the interface a packet was received on in the ICMPv6 response; it must be noted that there are few implementations of this ICMPv6 extension. With this approach it would be possible to ping a router on the addresses of loopback interfaces, yet see which interface the packet was received on. To check liveliness of a specific interface, it may be necessary to use other methods, such as connecting to the router via SSH and checking locally or using SNMP.

Traceroute: similar to the ping case, a reply to a traceroute packet would come from the address of a loopback interface, and current implementations do not display the specific interface the packets came in on. Also here, [RFC5837] provides a solution. As in the ping case above, it is not possible to traceroute to a particular interface if it only has a link-local address.

Hardware dependency: LLAs are usually EUI-64 based, hence, they change when the MAC address is changed. This could pose problem in a case where the routing neighbor must be configured explicitly (e.g. BGP) and a line card needs to be physically replaced hence changing the EUI-64 LLA and breaking the routing neighborship. LLAs can be statically configured such as fe80::1 and fe80::2 which can be used to configure any required static routing neighborship. However, this static LLA configuration may be more complex to operate than statically configured greater than link-local scope addresses, because LLAs are inherently ambiguous for a multi-link node such as a router; to deal with the ambiguity, the link zone index must also be considered explicitly, e.g., using the extended textual notation described in [RFC4007] as in this example: 'BGP neighbor fe80::1%eth0 is down'.

Network Management System (NMS) toolkits: if there is any NMS tool that makes use of interface IP address of a router to carry out any of its NMS functions, then it would no longer work if the interface

does not have a routable address. A possible workaround for such tools is to use the routable address of the router loopback interface instead. Most vendor implementations allow the specification of loopback interface addresses for SYSLOG, IPfix, and SNMP. The protocol LLDP (IEEE 802.1AB-2009) runs directly over Ethernet and does not require any IPv6 address, so dynamic network discovery is not hindered when using LLDP. But, network discovery based on NDP cache content will only display the link-local addresses and not the addresses of the loopback interfaces; therefore, network discovery should rather be based on the Route Information Base to detect adjacent nodes.

MPLS and RSVP-TE [RFC3209] allow establishing a MPLS LSP on a path that is explicitly identified by a strict sequence of IP prefixes or addresses (each pertaining to an interface or a router on the path). This is commonly used for Fast Re-Route (FRR). However, if an interface uses only a link-local address, then such LSPs cannot be established. At the time of writing this document, there is no workaround for this case; therefore, where RSVP-TE is being used, the approach described in this document does not work.

2.4. Internet Exchange Points

Internet Exchange Points (IXPs) have a special importance in the global Internet, because they connect a high number of networks in a single location, and because a significant part of Internet traffic passes through at least one IXP. An IXP requires therefore a very high level of security. The address space used on an IXP is generally known, as it is registered in the global Internet Route Registry, or it is easily discoverable through traceroute. The IXP prefix is especially critical, because practically all addresses on this prefix are critical systems in the Internet.

Apart from general device security guidelines, there are generally two additional ways to raise security (see also [I-D.ietf-opsec-bgp-security]):

1. Not to announce the prefix in question, and

2. To drop all traffic from remote locations destined to the IXP prefixes.

Not announcing the prefix of the IXP would frequently result in traceroute and similar packets (required for PMTUd) to be dropped due to uRPF checks. Given that PMTUd is critical, this is generally not acceptable. Dropping all external traffic to the IXP prefix is hard to implement, because if only one service provider connected to an

IXP does not filter correctly, then all IXP routers are reachable from at least that service provider network.

As the prefix used in the IXP is usually longer than a /48, it is frequently dropped by route filters on the Internet having the same net effect as not announcing the prefix.

Using link-local addresses on the IXP may help in this scenario. In this case, the generated ICMPv6 packets would be generated from loopback interfaces or from any other interface with a globally routable address without any configuration. However in this case, each service provider would use his own address space, making a generic attack against all devices on the IXP harder. All of an IXP's loopback interface addresses can be discovered by a potential attacker with a simple traceroute; a generic attack is therefore still possible, but it would require more work.

In some cases service providers carry the IXP addresses in their IGP for certain forms of traffic engineering across multiple exit points. Link-local addresses cannot be used for this purpose; in this case, the service provider would have to employ other methods of traffic engineering.

If an Internet Exchange Point is using a global prefix registered for this purpose, a traceroute will indicate whether the trace crosses an IXP rather than a private interconnect. If link local addressing is used instead, a traceroute will not provide this distinction.

2.5. Summary

Using exclusively link-local addressing on infrastructure links has a number of advantages and disadvantages, which are both described in detail in this document. A network operator can use this document to evaluate whether using link-local addressing on infrastructure links is a good idea in the context of his/her network or not. This document makes no particular recommendation either in favour or against.

3. Security Considerations

Using LLAs only on infrastructure links reduces the attack surface of a router: loopback interfaces with routed addresses are still reachable and must be secured, but infrastructure links can only be attacked from the local link. This simplifies security of control and management planes. The approach does not impact the security of the data plane. The link-local-only approach does not address control plane [RFC6192] attacks generated by data plane packets (such

as hop-limit expiration or packets containing a hop-by-hop extension header).

4. IANA Considerations

There are no IANA considerations or implications that arise from this document.

5. Acknowledgements

The authors would like to thank Salman Asadullah, Brian Carpenter, Bill Cerveny, Benoit Claise, Rama Darbha, Simon Eng, Wes George, Fernando Gont, Jen Linkova, Harald Michl, Janos Mohacsi, Ivan Pepelnjak, Alvaro Retana, Jinmei Tatuya and Peter Yee for their useful comments about this work.

6. Informative References

[I-D.ietf-opsec-bgp-security] Durand, J., Pepelnjak, I., and G. Doering, "BGP operations and security", draft-ietf-opsec-bgp-security-03 (work in progress), April 2014.

[IS-IS] ISO/IEC 10589, , "Intermediate System to Intermediate System Intra-Domain Routing Exchange Protocol for use in Conjunction with the Protocol for Providing the Connectionless-mode Network Service (ISO 8473)", June 1992.

[RFC0495] McKenzie, A., "Telnet Protocol specifications", RFC 495, May 1973.

[RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol (SNMP)", STD 15, RFC 1157, May 1990.

[RFC2080] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC4007] Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "IPv6 Scoped Address Architecture", RFC 4007, March 2005.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC4251] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC4609] Savola, P., Lehtonen, R., and D. Meyer, "Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements", RFC 4609, October 2006.

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

[RFC4987] Eddy, W., "TCP SYN Flooding Attacks and Common Mitigations", RFC 4987, August 2007.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.

[RFC5837] Atlas, A., Bonica, R., Pignataro, C., Shen, N., and JR. Rivers, "Extending ICMP for Interface and Next-Hop Identification", RFC 5837, April 2010.

[RFC6192] Dugal, D., Pignataro, C., and R. Dunn, "Protecting the Router Control Plane", RFC 6192, March 2011.

[RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, September 2012.

[RFC6752] Kirkham, A., "Issues with Private IP Addressing in the Internet", RFC 6752, September 2012.

[RFC6860] Yang, Y., Retana, A., and A. Roy, "Hiding Transit-Only Networks in OSPF", RFC 6860, January 2013.

Authors' Addresses

Michael Behringer
Cisco
Building D, 45 Allee des Ormes
Mougins 06250
France

Email: mbehring@cisco.com

Eric Vyncke
Cisco
De Kleetlaan, 6A
Diegem 1831
Belgium

Email: evyncke@cisco.com