Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 01, 2014

F.J. Baker
Cisco Systems

August 28, 2013

Using IS-IS with Token-based Access Control
draft-baker-ipv6-isis-dst-flowlabel-routing-01

Abstract

This note describes the changes necessary for IS-IS to route IPv6 traffic specified prefix if and only if the packet contains an authorization token.

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 March 01, 2014.

Copyright Notice

Table of Contents

1. Introduction

This specification builds on IS-IS for IPv6 [RFC5308] and its extensible TLV. This note defines the sub-TLV for an IPv6 [RFC2460] Flow Label, to define routes from to a destination prefix qualified by an authorization token.

The approach may be combined with other qualifying attributes, such as routing "to that destination AND from a specified source". The obvious application is data center inter-tenant routing using a form of token-based access control. If the sender doesn't know the value to insert in the flow label or hop-by-hop option (the receiver's tenant ID), he in effect has no route to that destination.

1.1. 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 [RFC2119].

2. Theory of Routing

Both IS-IS and OSPF perform their calculations by building a lattice of routers and links from the router performing the calculation to each router, and then use routes (sequences in the lattice) to get to destinations that those routes advertise connectivity to. Following the SPF algorithm, calculation starts by selecting a starting point (typically the router doing the calculation), and successively adding {link, router} pairs until one has calculated a route to every router in the network. As each router is added, including the original router, destinations that it is directly connected to are turned into

routes in the route table: "to get to 2001:db8::/32, route traffic to {interface, list of next hop routers}". For immediate neighbors to the originating router, of course, there is no next hop router; traffic is handled locally.

In this context, the route is qualified by an authorization token, carried in the flow label or a hop-by-hop option; It is installed into the FIB with the destination prefix, and the FIB applies the route if and only if the token in the packet matches the token in the route. Of course, there may be multiple LSPs in the RIB with the same destination and differing authorization tokens; these may also have the same or differing next hop lists. The intended forwarding action is to forward matching traffic to one of the next hop routers associated with this destination and authorization tokens, or to discard non-matching traffic as "destination unreachable".

LSAs that lack an authorization tokens sub-TLV match any token that may be present, by definition.

2.1. Dealing with ambiguity

In any routing protocol, there is the possibility of ambiguity. For example, one router might advertise a fairly general prefix - a default route, a discard prefix (which consumes all traffic that is not directed to an instantiated subnet), or simply an aggregated prefix while another router advertises a more specific one. In source/destination routing, potentially ambiguous cases include cases in which the link state database contains two routes A->B' and A'->B, in which A' is a more specific prefix within the prefix A and B' is a more specific prefix within the prefix B. Traditionally, we have dealt with ambiguous destination routes using a "longest match first" rule. If the same datagram matches more than one destination prefix advertised within an area, we follow the route with the longest matching prefix.

In this case, we follow a similar but slightly different rule; the FIB lookup MUST yield the route with the longest matching destination prefix that also matches the authorization token. A FIB route with no such token matches any authorization token.

2.2. Interactions with other constraints

In the event that there are other constraints on routing, such as proposed in [I-D.baker-ipv6-isis-dst-src-routing], the effect is a logical AND. The FIB lookup must yield the route with the longest matching destination prefix that also matches each of the constraints.

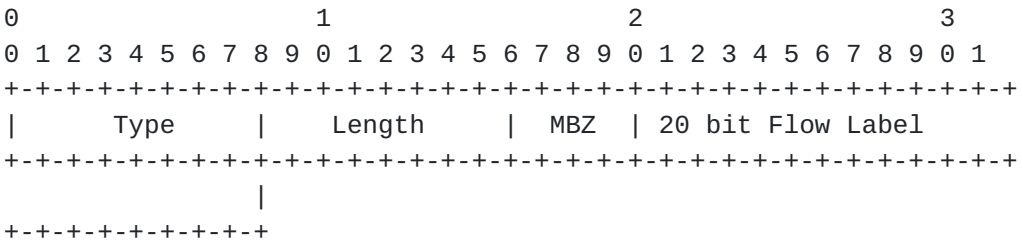
3. Extensions necessary for IPv6 Authenticated Routing in IS-IS

Section 2 of [RFC5308] defines the "IPv6 Reachability TLV", and carries in it destination prefix advertisements. It has the capability of extension, using sub-TLVs.

In this model, the flow label is used to prove that the datagram's sender has specific knowledge of its intended receiver. No proof is requested; this is left for higher layer exchanges such as IPSec or TLS. However, if the information is distributed privately, such as through DHCP/DHCPv6, the network can presume that a system that marks traffic with the right flow label has a good chance of being authorized to communicate with its peer.

The key consideration, in this context, is that the flow label is a 20 bit number. As such, an advertised route requiring a given flow label value is calling for an exact match of all 20 bits of the label value.

3.1. Authorization Token sub-TLV



Source Prefix Sub-TLV

Source Prefix Type: assigned by IANA

TLV Length: Length of the sub-TLV in octets

Flow Label: Flow Label value (20 bits)

4. IANA Considerations

The source prefix type mentioned in Section 3 must be defined.

5. Security Considerations

Network layer Token-based Access Control is part of a security solution. It is not, in itself, a complete solution. It acts as a pervasive network layer firewall, preventing unauthorized traffic from arriving at a destination. However, as in any network, a host is its own last bastion of defense; it needs IPsec or TLS-style

authorization and authorization of its peers, and must refuse traffic that contains the authorization token but is in fact malicious.

6. Acknowledgements

7. References

7.1. Normative References

[ISO.10589.1992]
International Organization for Standardization, "Intermediate system to intermediate system intra-domain-routing routine information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)", ISO Standard 10589, 1992.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S.E. and R.M. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC5308] Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, October 2008.

7.2. Informative References

[I-D.baker-ipv6-isis-dst-src-routing]
Baker, F., "IPv6 Source/Destination Routing using IS-IS", draft-baker-ipv6-isis-dst-src-routing-00 (work in progress), February 2013.

Appendix A. Change Log

Initial Version: February 2013

updated Version: August 2013

Author's Address

Fred Baker
Cisco Systems
Santa Barbara, California 93117
USA

Email: fred@cisco.com