                 LISP Transport for Policy Distribution
                 draft-kowal-lisp-policy-distribution-00

Abstract

   This document describes the use of the Locator/ID Separation Protocol
   (LISP) to encode and transport data models for the configuration of
   LISP ITRs.

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].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

When LISP ITRs are deployed with enough configuration to build a LISP
overlay, they may require additional configurations such as security,
QoS, and/or traffic forwarding policies. As networks continue to
grow, it can be challenging to ensure these configurations are
distributed to many ITRs and kept in sync. LISP network operators
may wish to re-use their existing LISP architecture to distribute
these configurations as opposed to configuring them by hand, using a
script, or investing in a configuration management system. The
configurations can be distributed via a mapping system that the
network operator manages or is managed by a third-party as part of a
managed service offering.

2. Definition of Terms

LISP related terms are defined as part of the LISP specification
[RFC6830], notably EID, RLOC, Map-Request, Map- Reply, Map-Notify,
Ingress Tunnel Router (ITR), Egress Tunnel Router (ETR), Map- Server
(MS) and Map-Resolver (MR).

[3]. Policy Distribution Use Cases

The ITR could use the mapping system to receive configuration policies for use cases such as:

o The RLOC interfaces of an ITR may be connected to WAN links that are policed at sub-line rate by its upstream provider. Using the mapping system, the ITR could receive and apply the QoS policies that would shape traffic to the correct rate on each ITR RLOC interface.

o ITRs use the mapping system to receive access-list (ACL) configuration(s) that would allow them to restrict traffic from authorized sources to authorized services.

o ITRs receive configurations that determine local forwarding policies, such as specifying ITR RLOCs to be used for egress forwarding on a per-application basis or RLOCs on different ITRs within the same LISP site to maintain application symmetry.

o Baseline configurations for common services (e.g., DNS, SSH, Syslog) can be maintained in a mapping system and distributed across multiple ITRs.

Policy distribution is not meant to provide zero-touch provisioning for ITRs within a LISP network. At a minimum, the ITR must have a map resolver defined, IP connectivity to the map resolver, and one or more distinguished names defined for receiving specific policies from the mapping system.

[4]. Policy Distribution: Packet Flow Description

The following figure illustrates a reference system used to support packet flow descriptions in this section.

```
            +----------+           +-+---+
            |controller|----------|MS/MR|
            +----------+           +-----+
                                      |
            _..-._.--._...._,.-|_.,--._.-_._.-..._
          .-.'                                '.-.
          (                RLOC SPACE            )
          (                                      )
           '..'.-._.'--'._.'.-._.'.-._.'.-._.'.--.'
                  /                       \
              (ifaceA)                  (ifaceB)
             +-+--+--+                  +-+--+--+
            .| xTR A |.-.              .| xTR B |.-.
            ( +-+--+--+   )            ( +-+--+--+   )
            .'   Site A   )            .'   Site B   )
            (          .               (          .
            '--'._.'.     )            '--'._.'.     )
                  '--'                       '--'
```
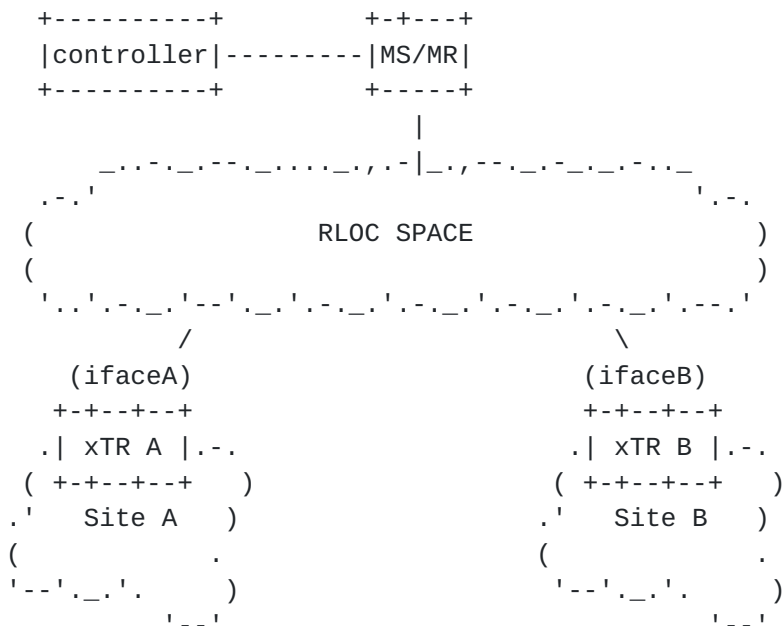
                Figure 1: Reference system for policy distribution

   The reference system contains two sites, site A and site B, with
   corresponding xTR-A and xTR-B providing encapsulation and
   decapsulation services for the overlay traffic. xTR-A uses
   interface-A to forward and receive encapsulated traffic through the
   RLOC space; and xTR-B uses interface-B for it.

   For packet flow purposes the reference system assumes that a network
   controller provides the policies to a map-server.

   When an ITR comes up, it requests it's designated policies with it's
   map-server. The MS may have this policy configured by the
   administrator via a network controller.

4.1. Policy Distribution

   The following is an illustration of the sequence to distribute a
   policy registered by the controller with the mapping system, down to
   an ITR that requests its designated policies. In the example <ITR-A>
   represents the hostname of the ITR that learns a policy using this
   mechanism.

   o The Mapping-System is either configured by an operator or learns a
      mapping sent by a controller though a Map-Register. The Mapping
      System learns the mapping: EID="policy-<ITR-A>" --> RLOC= "{
      "shape":{ "interface":"ifaceA", "direction":"outbound",
      "value":100Mbps }}". The EID is encoded as a Distinguished Name
      and the RLOC as a JSON string.

   o ITR-A is configured to dynamically learn policies from the Mapping
      System with the name "policy-ITR-A" (policy followed by its
      hostname).

   o ITR-A sends a Map-Request to the Mapping System with EID="policy-
      <ITR-A>" encoded as a Distinguished Name. The Map-Request is sent
      with the N-bit set.

   o The Mapping System forwards the request to the appropriate Map-
      Server. The Map-Server adds ITR-A to the subscription list of
      EID="policy-<ITR-A>" and sends back a Map-Notify with the mapping
      that the controller has registered.

   o When ITR-A receives the Map-Notify installs the received policy
      locally, to shape traffic sent over the RLOC facing interface.

   o Note that when the map-server has multiple policies associated
      with this ITR, it can send each one of the policies as an
      additional locator record (following the same JSON format) in the
      mapping. The locator count in the Map-Notify reflects the number
      of policies distributed with the mapping.

4.2. Policy Updates

   Policy distribution takes advantage of the LISP pubsub model to
   ensure that router updates are properly distributed when policies
   change. In such a case, and using the same reference sytem as above,
   the information exchange is as follows:

   o The controller sends a Map-Register to the Mapping System,
      updating the policy mapping with: EID="policy-<ITR-A>" --> RLOC=
      "{ "shape":{ "interface":"ifaceA", "direction":"outbound",
      "value":200Mbps }}".

   o When the corresponding Map-Server receives this update it checks
      the list of ITRs subscribed for updates of EID="policy-<ITR-A>"
      and finds out that ITR-A is subscribed.

   o The Map-Server sends a Map-Notify to ITR-A with the updated
      mapping information that has been registered.

   o When ITR-A receives and validates the Map-Notify, it updates the
      local policy, changing the shaping rate as specified in the new
      JSON description. Note that if the JSON specifies the same policy
      that is currently applied the notification is ignored.

5. **Mapping System Operations**

   The mapping system that is used for distributing policy
   configurations can be managed by either the administrator who owns
   and operates their own LISP sites or a third-party administrator who
   offers LISP mapping system functionality as a managed service. A
   controller or orchestrator could be used to update and optimize
   policies within the mapping system based on network or ITR telemetry.

   Within the mapping system, the administrator must define a
   distinguished name that is specific to an ITR. The distinguished
   name is associated with the specific policy configurations that the
   ITR is to receive. Each ITR is configured with the minimal
   requirements to perform a mapping request procedure as well as a
   distinguished name that can be matched upon in the mapping system.

   Map-Servers should be able to receive policy registrations through
   the Map-Registration process. The Map-Registration must encode the
   policy following the specification in the policy distribution
   encoding section.

6. **Policy Distribution Process**

   The ITR subscribes to its policy via the Map-Request procedure
   defined in section 5 of [I-D.ietf-lisp-pubsub]. The PubSub procedure
   is used to ensure that policies can be updated or audited after an
   ITR has received them. Policies are published to the ITR from the
   mapping system using the mapping notification procedure defined in
   section 6 of [I-D.ietf-lisp-pubsub].

   EID-to-RLOC mappings used for policy distribution are of the type EID
   <Distinguished Name> to RLOC <JSON policy specification>. The EID is
   a distinguished name uniquely identifying a router in the system,
   while each RLOC record uses JSON encoding to specify the particular
   policy (or policies) that this router needs to implement.

7. **Policy Distribution Encoding**

   When the ITR is configured to receive a policy using a distinguished
   name, the ITR sends a subscription for the EID record encoded as this
   Distinguished Name. When a policy has been registered with the
   Mapping System for this Distinguished Name, the ITR receives a
   publication with a list of policies as RLOC records and encoded as
   JSON strings (as defined in section 5.4 of [RFC8060].

   Example encoding for QoS policy that shapes traffic to 50 percent of
   the line-rate: EID-Record encoded as distinguished name "policy-ce-
   router1" RLOC-Record record encoded as JSON string "{ "shape":{

   "interface":"ethernet1", "direction":"outbound", "unit":"percent",
   "value":50 }}"

   Example encoding for setting the ITR's NTP server to 1.1.1.1: EID-
   Record encoded as distinguished name "policy-ce-router" RLOC-Record
   record encoded as JSON string "{ "NTP-address" : "1.1.1.1" }"

   Multiple ITRs can be configured to use multiple distinguished names
   for receiving multiple sets policies. This allows for an ITR to
   receive specific policies and many ITRs to receive policies that can
   be broadly applied. Referring to the two examples above, an ITR can
   be configured to use a distinguished name of "policy-ce-router1" to
   receive a QoS configuration that is specific to that node while also
   using a distinguished name of "policy-ce-router" to receive
   configurations that are common to each ITR in the LISP network (e.g.,
   NTP configuration). The use of multiple distinguished names per ITR
   reduces the amount of configuration within the mapping system.

8. IANA Considerations

   This memo includes no request to IANA.

9. Acknowledgements

   Thanks to James Stankiewicz for his thorough comments and
   suggestions.

10. References

10.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <https://www.rfc-editor.org/info/rfc2119>.

   [RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The
              Locator/ID Separation Protocol (LISP)", RFC 6830,
              DOI 10.17487/RFC6830, January 2013,
              <https://www.rfc-editor.org/info/rfc6830>.

   [RFC8060] Farinacci, D., Meyer, D., and J. Snijders, "LISP Canonical
              Address Format (LCAF)", RFC 8060, DOI 10.17487/RFC8060,
              February 2017, <https://www.rfc-editor.org/info/rfc8060>.

10.2. Informative References

   [I-D.ietf-lisp-pubsub]
              Rodriguez-Natal, A., Ermagan, V., Cabellos-Aparicio, A.,
              Barkai, S., and M. Boucadair, "Publish/Subscribe
              Functionality for LISP", draft-ietf-lisp-pubsub-07 (work
              in progress), January 2021.

Authors' Addresses

   Michael Kowal
   Cisco Systems
   111 Wood Ave. South
   Iselin, NJ 08830
   USA

   Email: mikowal@cisco.com

   Marc Portoles Comeras
   Cisco Systems
   170 Tasman Drive
   San Jose, CA 95134
   USA

   Email: mportole@cisco.com

   Amit Jain
   Juniper Networks
   1133 Innovation Way
   Sunnyvale, CA 94089
   USA

   Email: atjain@juniper.net

   Dino Farinacci
   lispers.net
   San Jose, CA
   USA

   Email: farinacci@gmail.com