draft-ietf-rps-tunnels-00.txt
Category: Standards Track
David Meyer
University of Oregon
November 1996

Representing Tunnels in RPSL

Status of this Memo

This document provides extensions to the Routing Policy Specification Language [RPSL] to provide support for tunnels of various types.

Internet Drafts

Abstract

This document specifies the language and set of semantics describing tunnels in the Routing Policy Specification Language (RPSL). It defines a new tunnel class, inet-tunnel, and a set of extensions to the inet-rtr class. An instance of the inet-tunnel class specifies endpoints for tunnels of various encapsulation types, including DVMRP [DVMRP], GRE [GRE], and IPv6 [IPV6].

This memo is a product of the Routing Policy System Working Group (RPS) in the Operational Requirements area of the Internet Engineering Task Force. Submit comments to <rps@isi.edu> or the author.

Introduction

Tunneling is a fundamental networking technology that is used in a variety circumstances. A common use of tunneling is to incrementally deploy a new network layer protocol. The approach is to encapsulate ("tunnel") the new protocol through the existing network layer protocol, usually IP. Examples of this approach include include the multicast backbone [MBONE], where multicast packets are encapsulated in IP packets using protocol 4 (IP in IP), and IPv6 backbone [6BONE], where IPv6 packets are encapsulated in IP packets using IP protocol 41 [V6TRNS].

Another use of tunneling is to force congruence between the existing (IP unicast) topology and some new topology. Due the special requirements of IP multicast routing, the MBONE is also an example of this use of tunneling.

This document describes extensions to RPSL to support general tunneling mechanisms. The extensions support point to point and point to multipoint tunnels of encapsulation types, including DVMRP, GRE, and IPv6. In addition to the encapsulation, a protocol to run inside the tunnel can also be specified.

Extensions to the inet-rtr class

The inet-rtr class' peer attribute is extended to describe tunnels by assigning a new peer type (tunnel). The tunnel peer attribute has the following fields:

```
inet-rtr: <name>
 ...
peer: tunnel <dest-IP1> source=<source-IP1>
             encap=<encapsulation type>
             name=<name1>
 ...
peer: tunnel <dest-IP2> source=<source-IP2>
             encap=<encapsulation type>
             name=<name2>
```

The type clause of then tunnel peer attribute describes the encapsulation on the tunnel. The defined encapsulation types are DVMRP [DVMRP], GRE [GRE], or IPv6 [IPV6]. The name clause refers to a tunnel object (see below). If there are multiple tunnel peer attributes with the same name attribute, then the tunnel is a point to multipoint tunnel. Note that a router can be the source of multiple tunnels.

Each inet-rtr tunnel peer instance has a mandatory name, source, and destination attributes. The tunnel source attribute must correspond to an ifaddr attribute for the inet-rtr instance.

The inet-rtr instance below describes a DVMRP tunnel with source 204.70.32.6 and destination 204.70.158.61. The tag MBONE-TUNNEL-EUG refers to a tunnel instance (see below). The same router has a GRE tunnel.

```
inet-rtr: eugene-isp.nero.net
loacalas: AS4600
ifaddr:   204.70.32.6 masklen 30
 ...
peer: tunnel encap=DVMRP name=MBONE-TUNNEL-EUG 204.70.32.6 204.70.158.61
peer: tunnel encap=GRE name=GRE-TUNNEL-EUG 204.70.32.6  206.42.19.240
 ...
```

The inet-tunnel Class

A tunnel is specified by an instance of the inet-tunnel class. The attributes of the inet-tunnel class are described below.

```
inet-tunnel:     <name>
tunnel-source:   <inet-router key>
tunnel-sink:     <inet-router key 1>
 ...
tunnel-sink:     <inet-router key n>
tunnel-protocol: <protocol>
tunnel-in: from  <inet-router key1> accept <input-filter-spec1>
tunnel-in: from  <inet-router key2> accept <input-filter-spec2>
 ...
tunnel-in:  from <inet-router keyn> accept <input-filter-specn>
```

```
tunnel-out: to   <inet-router key1>
                 [action
                   [scope=<ttl1>;]
                   [boundary=<prefixn/masklen1>;]
                   [dvmrp-metric=<n>;]]
                 announce <output-filter-spec1>
tunnel-out: to   <inet-router key2>
                 [action
                   [scope=<ttl2>;]
                   [boundary=<prefixn/masklen2>;]
                   [dvmrp-metric=<n>;]]
                 announce <output-filter-spec2>
 ...
tunnel-out: to   <inet-router keyn>
                 [action
                   [scope=<ttln>;]
                   [boundary=<prefixn/masklenn>;]
                   [dvmrp-metric=<n>;]]
                 announce <output-filter-specn>
```

inet-tunnel Class Attributes

```
inet-tunnel:     mandatory, single valued
tunnel-source:   mandatory, single valued, class key
tunnel-sink:     mandatory, single valued, class key
tunnel-protocol: mandatory, single valued
tunnel-in:       mandatory, multi-valued
tunnel-out:      mandatory, multi-valued
```

An instance of the inet-tunnel class describes a single tunnel (although the tunnel-source may be the source of multiple tunnels). The name attribute is a key that is used in an inet-rtr object to reference the tunnel object. The tunnel may be point to point or point to multipoint. A multipoint tunnel will have more than one tunnel-sink value. Each tunnel-sink must have corresponding tunnel-in and tunnel-out attributes. The tunnel-protocol is the protocol to run "inside" the tunnel. The values for tunnel-protocol include BGP, RIPv6, DVMRP, PIM-DM, and PIM-SM. See [SSMMC] for an application that uses BGP tunneled in GRE.

The inet-tunnel class's tunnel-out attribute includes an action clause for which the currently defined actions include: (i). The minimum IP time-to-live required for a packet to be forwarded to the specified endpoint (in the case of multipoint tunnels, there may be per endpoint scopes), (ii). A boundary attribute describes a class of packets that will not be forwarded through the tunnel, and (iii). A DVMRP metric. These attributes are particularly relevant to multicast routing.

The inet-tunnel class also has routing filter specifications which describe filters that are appropriate for the tunnel's routing protocol. In the case of DVMRP, the filter specification can be the list of network prefixes accepted or advertised.

Finally, an instance of the inet-tunnel class also has all of the administrative fields present in an aut-num class, including guardian, admin-c, tech-c, notify, mnt-by, changed, and source.

Example

In this example, the inet-rtr eugene-isp.nero.net has a DVMRP tunnel with the sink on the inet-rtr dec3800-2-fddi-0.SanFrancisco.mci.net. The tunnel object is called MBONE-TUNNEL-EUG. eugene-isp.nero.net will accept any routes. eugene-isp.nero.net will forward packets to the DVMRP tunnel if the packet's time-to-live is greater than or equal to 64. In addition, eugene-isp.nero.net will not pass any packets that match the administrative scope boundary filter (in this case, 239.254.0.0/16).

In addition, the inet-rtr eugene-isp.nero.net has a GRE tunnel represented by GRE-TUNNEL-EUG.

```
   inet-tunnel:     MBONE-TUNNEL-EUG
   tunnel-source:   eugene-isp.nero.net
   tunnel-sink:     dec3800-2-fddi-0.SanFrancisco.mci.net
   tunnel-protocol: DVMRP
   tunnel-in:       from 204.70.158.61 accept ANY
   tunnel-out:      to 204.70.158.61
                    action
                       scope=64;
                       boundary={239.254.0.0/16};
                       dvmrp-metric=1;
                    announce AS-NERO-TRANSIT
   guardian:    meyer@ns.uoregon.edu
   admin-c:     DMM65
   tech-c:      DMM65
   notify:      nethelp@ns.uoregon.edu
   mnt-by:      MAINT-AS3582
   changed:     meyer@ns.uoregon.edu 961104
   source:      RADB

   inet-tunnel:     GRE-TUNNEL-EUG
   tunnel-source:   eugene-isp.nero.net
   tunnel-sink:     ogre.prognet.com
   tunnel-protocol: PIM-DM
   tunnel-in:       from 204.70.158.61 accept ANY
   tunnel-out:      to 206.42.19.240
                    action
                      scope=64;
                    announce ANY
   guardian:    meyer@ns.uoregon.edu
   admin-c:     DMM65
   tech-c:      DMM65
   notify:      nethelp@ns.uoregon.edu
   mnt-by:      MAINT-AS3582
   changed:     meyer@ns.uoregon.edu 961104
   source:      RADB
```

Security Considerations

Security considerations are not discussed in this memo.

References

[6BONE] See http://www-6bone.lbl.gov/6bone/

[DVMRP] T. Pusateri, "Distance Vector Multicast Routing Protocol", draft-ietf-idmr-dvmrp-v3-03, September, 1996.

[GRE] S. Hanks, T. Li, D. Farinacci, and P. Traina, "Generic Routing Encapsulation (GRE)", RFC1701, October, 1994.

[IPV6] A. Conta and S. Deering, "Generic Packet Tunneling in IPv6", draft-ietf-ipngwg-ipv6-tunnel-04.txt, October, 1996

[MBONE] See http://www.best.com/~prince/techinfo/misc.html

[RPSL] C. Alaettinoglu, et. al., "Routing Policy Specification Language (RPSL)", draft-ietf-rps-rpsl-00.txt, October, 1996.

[SSMMC] Y. Rekhter, "Auto route injection with tunnelling", NANOG, October, 1996. For additional information, see http://www.academ.com/nanog/oct1996/multihome.html

[V6TRNS] R. Gilligan and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 1933, April 1996.

Author's Address

David Meyer
University of Oregon
1225 Kincaid St.
Eugene, OR 97403

phone: +1 541.346.1747

email: meyer@ns.uoregon.edu