Network Working Group   Ping Pan
Internet Draft   (Juniper Networks)
Expiration Date: May 2002   Jim Murphy
Network Working Group   (Juniper Networks)

A Network Architecture for Simplified Signaling Protocol
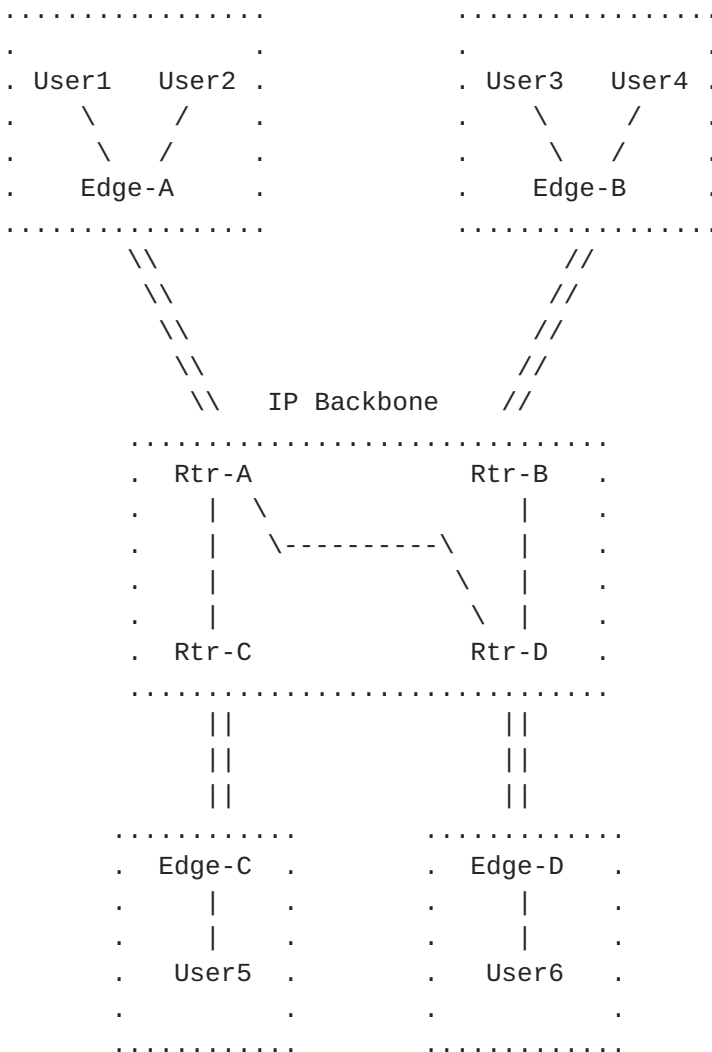

draft-pan-signal-req-00.txt

Abstract

This memo describes a network architecture where a simplified signaling
protocol is required on network routers. We list some of the assumptions
and requirements for the signaling protocol.

1. Introduction

RSVP has been designed as the signaling protocol that is responsible
for setting up reservations for end-to-end user flows in the
Internet. However, over the years, people have been debating over
its usefulness, applicability, and scalability,

In this memo, we describe a network architecture where a protocol to
signal between users and network routers is definitely required.
Moreover, the signaling protocol needs to be simpler than what had
been proposed in RSVP. We illustrate the architecture in Figure-1.

Figure 1: Example Network Topology

```
     ................              ................
     .              .             .              .
     . User1   User2 .            . User3   User4 .
     .    \     /    .            .    \     /    .
     .     \   /     .            .     \   /     .
     .    Edge-A     .            .    Edge-B     .
     ................              ................
          \\                             //
           \\                           //
            \\                         //
             \\                       //
              \\    IP Backbone     //
          ................................
          .  Rtr-A           Rtr-B   .
          .    |  \             |     .
          .    |   \----------\  |     .
          .    |            \  |     .
          .    |             \ |     .
          .  Rtr-C           Rtr-D   .
          ................................
              ||                ||
              ||                ||
              ||                ||
          ............      ............
          . Edge-C  .       . Edge-D   .
          .    |    .       .    |     .
          .    |    .       .    |     .
          .  User5  .       .  User6   .
          .        .       .          .
          ............      ............
```

As shown in the figure, network users need to communicate among each
other over the Internet backbone. There are four types of users that
we need to consider:

 1. Wireless users: They communicate with some base-stations using
    whatever the protocols they desire. The base-stations in turn
    send user traffic over the Internet. It is likely that the
    network providers need to be able to keep track of traffic usage
    on per-user basis, and guarantee some level of service to the
    wireless users. Here, we refer the equipment that is used to
deliver
    user traffic into the Internet as an edge device.

 2. Traditional phone users: Telephone users may choose whatever
    the signaling protocol to negotiate and setup call sessions.
    And the phone providers may want to use the Internet to transfer
    voice traffic. Between phone network edge and the Internet edge,
    it is necessary to have a per-call signaling protocol that is
    responsible for admission control.

 3. High speed end-users: Cable modem and DSL users should have
    the option to demand service guarantees such as bandwidth from
    the Internet providers. To access the backbone, the edge devices
    from the regional providers need to communicate with the backbone
    routers for admission control.

 4. VPN users: For edge devices that support non-IP traffic into the
    backbone, they need to have an IP signaling protocol to
    communicate with the backbone to setup CoS-aware VPN tunnels.

As shown in the figure, Edge A, B, C and D are responsible for
signaling and sending IP packets to the backbone. The backbone edge
routers (Rtr A, B, C and D) are responsible for admission control,
traffic classification and possible traffic aggregation, and sending
packets through the backbone. Here, we make no assumption on the
exact mechanisms (over-provisioning or MPLS, etc) that network
providers must use to satisfy the CoS/QoS requirements.

By the way, there could exist routers between the edge devices and
the backbone edge routers. These routers have the option to process
the signaling messages and make resource reservation for each
individual data flow.

To provide end-to-end signaling requirement, the routers need to
"tunnel" the signaling messages through the backbone.

2. Assumptions

   Under the architecture, we have the following assumptions:

     - User network and IP backbone could manage their own network
       resources, and must satisfy CoS/QoS requirements once packets are
       inside their network. More importantly, it is not required to
       have a signal and unified resource management technique
       in all networks.

     - Though, in theory, the only type of application that requires
       CoS/QoS guarantees is inter-active real-time streaming traffic,
       such as voice data in both wired or wireless networks, the
       signaling described here is independent from the application type.

     - The edge devices have the option to encapsulate user data in
       any transport layer protocol (TCP, RTP, GRE or IP-IP). Thus the
       signaling protocol must be generic.

     - In case of traditional phone users, there could be a very large
       volume of voice traffic arriving at phone and IP network edge,
       we cannot make the assumption that the edge devices will always
       apply some adaptive schemes during packet transmission. Some level
       of resource reservation is always required for such users.

     - We cannot make the assumption that each user flow will last
       for long period of time. In other words, the signaling messages
       can be very dynamic in nature. This can cause heavy processing
       overhead on routers. Thus, while the signaling needs to be
       designed to be as efficient as possible, the signaling messages
       must not be processed inside the backbone.

     - Multicast support causes heavy processing overhead on routers,
       and it is not clear it will be used for the users we described
       here. We leave multicast support for future studies.

3. Signaling Protocol Requirements

   The signaling protocol needs to be processed at edge devices,
   backbone routers and possibly the intermediate routers.

   The edge devices need to notify backbone routers regarding
   arriving/departure of data flows. Since the edge devices are
   responsible for potentially delivering a large number of data flows
   (including those of non-IP sessions) into the Internet, the signaling
   overhead on edge devices must be small. It is not clear that
   receiver-initiated reservation technique emphasis in RSVP is a
   suitable solution for the applications we are addressing here.

   The backbone routers must process each and every signaling message,
   run admission control procedure, and initiate rejection messages in
   case of admission control failure. We always assume that network
   providers have a way to create and manage a set of traffic-class
   specific "bandwidth trunks" across the backbone. Thus, it is possible
   for the backbone routers to follow some classification procedure and
   aggregate the incoming data flows into one of the pre-established
   "bandwidth trunks". To process a large number of flows at backbone
   routers, the signaling needs to be efficient. In addition, the
   signaling protocol must have enough security features that can
   prevent DoS attacks at backbone routers.

   For the intermediate routers between the edge device and the backbone
   routers, processing signal messages should be an option. This is
   because network resources may not be a constraint in many access
   networks. Running admission control at each router here may not be
   necessary but to add more overhead in resource management. However,
   for the edge devices that request very large amount of network
   resources that may cause resource constraint in the access networks,
   the intermediate routers must process the signaling messages and
   reject resource requests at early in the network as possible.

3.1. Processing overhead considerations

   One important factor that we need to consider is the short-lived user
   flows. For example, the average voice phone-call is only 3-4 minutes,
   as oppose to video conferencing sessions may last for hours. This
   requirement alters some of the design decisions for signaling
   protocols. In case of RSVP, routers can apply various techniques
   [RSVP-REFRESH], such as control message compression, to improve
   signaling efficiency. Unfortunately, this can only be effective if
   the user session is long.

   Given users must gain Internet access within a short period of time,

the signaling messages must be delivered reliably. When there are
reservations on the intermediate routers, the user-flows must be able
to adjust to routing changes quickly. Thus, the signaling protocol
needs to be the combination of both "hard-state" and "soft-state".

3.2. Error handling and redundancy considerations

Edge devices and backbone routers must be able to notify the users if
there is an error inside the network. There are two types of network
errors:

 - Recoverable errors: this type error can be locally repaired by the
   network nodes. The network nodes do not have to notify such errors
   to the users immediately.

 - Unrecoverable errors: the network nodes cannot handle this type of
   error, and have to notify the users as soon as possible.

For example, when there is a network failure inside the backbone, if
the backbone routers can utilize redundancy functionality to protect
effected user flows, the routers have the option to notify or not
notify the users about the failure. On the other hand, if the network
failure is so severe that backbone routers have to terminate some of
the user flows, the routers must notify the users immediately on the
network failure. Upon receiving the error messages, the users may
have to rely on their own redundancy function to redirect user flows.

Thus, the distinction of recoverable and unrecoverable errors is
fairly important in signaling protocol design. This can impact the
overall signaling process overhead.

3.3. Security considerations

When users signal network for flow, network resources will be
consumed. Thus all signaling messages must be authenticated.

4. References

   [RSVP] R. Braden, Ed., et al, "Resource ReSerVation protocol (RSVP)
   -- version 1 functional specification," RFC2205.

   [RFC2961] L. Berger, et al, "RFC 2961: RSVP Refresh Overhead
   Reduction Extensions", RFC2961.

5. Author Information

Ping Pan
Juniper Networks
1194 N.Mathilda Ave
Sunnyvale, CA 94089
e-mail: pingpan@juniper.net

Jim Murphy
Juniper Networks
1194 N.Mathilda Ave
Sunnyvale, CA 94089
e-mail: murphy@juniper.net