Service Awareness Network

Daniel Huang,
Liwei Ma,
Dongyu Yuan,
Fenlin Zhou,
Bin Tan, ZTE Corporation
Dong Yang – Beijing Jiaotong University
Cloud topology shifts and service demands more than “best effort” networking quality

1. Cloud deployment pattern shifts and the impacts upon service provisioning:
   - Cloud migrates to edge and super-edge sites and the resulting topology changes dramatically;
   - Services be deployed in multiple and distributed edge sites rather than designated sites;

2. Aggregated coarse-grained traffic routing versus service-centered fine-grained traffic treatment
   - Emerging interactive services could be networking-sensitive with disparate requirements;
   - Routing layer alone can not distinguish service as well as its SLA requirements under the current scheme.
1. Service Identification Label: a unique entity employed to be interfaces between service and underlying network, cloud and network.

2. Service traffic steering under SAN:
   - Computing/Networking sensitive: service awareness-based traffic treatments at SAN nodes;
   - Otherwise (C/N non-sensitive): transmit as it is through ongoing URL-DNS-GSLB-IP BE process.
SAN Control plane consideration

1. Awareness of service requirements:
   - SIL as well as its designated requirements (bandwidth, latency, jitter etc) would be provisioned by SAN system as public and guaranteed service profiles
   - SIL functions as an interface between service and underlying network which would compute and execute SIL-indexed networking policies for the corresponding service traffic
   - Centralized control plane should be employed for awareness of service requirements

2. Awareness of service-related networking and computing resources:
   - GSRS (Global service resource status) and LSRS (Local service resource status) maintained at SAN ingress and egress respectively
   - Both centralized and distributed control plane could be employed for GSRS notification and maitenence, while LSRS would always be handled at local site between SAN egress and Cloud site.
SAN data plane consideration

1, SIL location options in IPv6 header
   • Dedicated encapsulation in IPv6 extension headers, comprehensive meta data could be indicated and flexible SIL length could be possible
   • Leverage the existing header fields to indicate the service identification, such as resource / destination address and flow label

2, SIL-based routing
   • SIL at SAN ingress: extracted from the designated header field and mapped with the SIL-indexed policy as well as GSRS – the SIL-marked traffic would be routed accordingly
   • SIL at SAN egress: extracted from the header field and mapped with LSRS, the SIL-marked traffic would be steered accordingly
   • SIL at cloud site: SIL could be treated as an explicit service residing at the site which could leverage it to make SIL specific forwarding and scheduling such as load balancing.
Dedicated SAN header and encapsulation consideration

1, Dedicated SAN header

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------+</td>
<td>+-------------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SANID Indicator</td>
<td>S</td>
<td>R</td>
</tr>
<tr>
<td>+-------------------------------------------------+</td>
<td>+-------------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SANID(Service ID)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stream ID (optional)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reserved</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-------------------------------------------------+</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- SANID indicator: SAN identification metadata including the length of SANID
- S: indicates the presence of stream ID
- R: indicates the presence of optional reserved part.

2, SAN header encapsulation

| +-------------------------------------------------+ | +-------------------------------------------------+ |
| | Next Header | Hdr Ext Len | Opt Type-TBA1 | Opt Data Len |
| +-------------------------------------------------+ | +-------------------------------------------------+ | +-------------------------------------------------+ | +-------------------------------------------------+ |
| | Type-TBA2 | Length | D | RESERVED |
| +-------------------------------------------------+ | +-------------------------------------------------+ | +-------------------------------------------------+ |

SAN header in HBH/DoH

SAN header in SRH
SAN hierarchical service routing

Service resource status:
- Infrequent updated status: notified to and maintained by remote SAN nodes as GSRS
- Frequent updated status: resides only at the local SAN nodes as LSRS

Two segment service routing:
- SAN ingress routes the service traffic to the SAN egress close to the selected cloud site in terms of GSRS without specific service instance selection at this segment.
- SAN egress forwards the service traffic to the specific service instance in terms of LSRS
DB-based service resource status awareness

Why DB-based resource status awareness?

- Reduce the overwhelmed utilization of L3 protocols and improve the compatibility of the network.
- Simplify the perception and advertisement process and optimize the learning procedure of updated status.
Example demonstration of DB-based service status awareness

The description of service status may include:

(A Service ID to represent a globally unique service semantic identification and its location should be configured as the key for the extracted data model.)
How service routing table coordinates with IP routing table

Service Routing Table & IP Routing Table

- After the current computing status is obtained, a proper resource pool can be selected to satisfy the service SLA requirements, so as to quickly and accurately guide data forwarding.
- Together with path metrics in the network, a specific service routing table is formulated.
- With the service gateway determined, an Interface IP or an SRv6 policy can be indexed.

Service Routing & IP Routing Table

Since the service routing table is generated additionally, it is completely decoupled from the conventional IP routing table.

- For services with requirements for computing resources, the service routing table maps to the IP routing table to complete a forwarding operation.
- For conventional services which are not sensitive to computing resources, a forwarding operation can be implemented simply in the native IP way.
Computing segment for SAN service routing

In order to describe and standardize a service routing behaviour, a new **Computing Segment** is proposed.

Computing Segment is the identifier of packets in which a corresponding SAN header should be identified and further being forwarded via the matched service routing table entity, indicating the following operations:

- Identify the **SAN ID encapsulated in DOH, HBH**.
- Query the forwarding table entry indexed by SAN ID.
- Forward the packet to the new destination.

In the case of SRv6, a new behavior **End.C for Computing Segment** is defined. An instance of a Computing SID is associated with a service routing table and a source address.
Suppose the Endpoint behaviour of END.C is configured at Ingress PE and Egress PE, namely SID 1 and SID 2 respectively. SID1 and SID2 are advertised in the network by IGP.

- SID1 is configured as DA by the client. The packet carrying the SAN header as the option of the DOH is forwarded to Ingress PE.
- When Ingress PE receives the packet, it queries the local routing table in accordance with DA and identifies that DA is a Computing SID(SID1).
- When Egress PE receives the packet, it queries the local routing table in accordance with DA and identifies that DA is a Computing SID(SID2).
- When an intra-cloud LB receives the packet, the packet can be forwarded in accordance with the Endpoint behaviour or be processed as a native IPv6 packet, depending on the practical circumstances.
Next step:
• refine the drafts with both more solution details as well as testing results.
• Comments, suggestions and contributions would be appreciated
• Thanks for your time!