MicroTap Segment

https://www.ietf.org/archive/id/draft-zzhang-spring-microtap-segment-03.txt

Zhaohui Zhang, Ryan Hoffman, Gurminderjit Bajwa, Daniel Voyer, Shay Zadok, Aijun Wang, Luay Jalil, Shengtao Li, Siva Sivabalan

IETF120, Vancouver
Background Refresh

- A MicroTap SID instructs a node to make a copy of a packet & send the copy to a particular destination for packet analysis
  - The original packet continues to the destination
- Strategic placement of one or more microTap SIDs within a SID-list results in traffic tapping at targeted points within the network
  - W/o the need for configuring/unconfiguring firewalls on tapping nodes to start/stop the tapping of certain packets
  - Word “micro” means “micro control” - unrelated to SRv6 “Micro SID”
Example: Traffic tapping at router B

- The traffic path is from client A to server B through Router A, B & C
- The goal is to capture the traffic at router B for packet analysis
- On Router A, microTap SID is placed after the Node SID for router B in the SID-list
- Router A classifies the traffic of interest and pushes the SID-list to the packets
- When microTap SID becomes active on Router B, it replicates the packet and sends the copy to the remote monitor by imposing router D’s Node SID
- Router B also pops the microTap SID off the original packet and continues forwarding to router C
- When microTap SID becomes active on Router D, it sends the packet to monitor

<table>
<thead>
<tr>
<th>Router</th>
<th>Node SID</th>
<th>MicroTap SID</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>B</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>D</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

The diagram shows the traffic path and the insertion of the segment routing header including the micro tap SID. The table lists the routers, node SIDs, and micro tap SIDs.
Changes in Revision -03

- SRv6 Optimization
- Support for tapping by a monitor node
Allocation from Global ID Block

- The SRv6 C-SID specification says:
  In order to efficiently manage the C-SID numbering space, a deployment may divide it into two non-overlapping sub-spaces: a Global Identifiers Block (GIB) and a Local Identifiers Block (LIB).
  ... 
  A global C-SID identifies a segment defined at the Locator-Block level. The tuple (Locator-Block, C-SID) identifies the same segment across all nodes of the SR domain. A typical example is a prefix segment bound to the End behavior.

- We extend this GIB/LIB concept to uncompressed/full SIDs as well
- A monitor node allocates an ID from the GIB and advertises it
  - With the semantics “micro-tapping to the advertising monitor node”
  - Referred to as Tapping ID (TID)
  - Used as a C-SID or FUNC bits of a full SID
Signaling & Operation 1/2

- The monitor node advertises an End SID with the End.TAP behavior
  - With the LB:LN:FUNC:ARG structure where the FUNC bits encode the TID
  - It installs a corresponding LB:LN:FUNC:: IPv6 route to send received tapped traffic to its monitor
    - A tapping node sends the tapped traffic using LB:LN:FUNC::/
    - E.g., LB:00D0:1000::/ where 00D0 identifies D and 1000 is the GIB TID for “tapping to D”
- A tapping-capable node sets a new T-flag bit in its Locator TLV
  - Indicating that it is capable of tapping packets received with this locator
  - For each locator that it advertises with the T-flag and a TID received from a monitor node, it installs a route for tapping to that monitor node
    - E.g., Node B installs LB:00B0:1000::/ route to tap LB:00B0:1000:: packets to Node D
Signaling & Operation

- When an ingress receives D’s LB:00D0:1000:: End SID and B’s LB:00B0:: Locator that has the T-flag set,
- It knows B is capable of tapping and it can use LB:00B0:1000:: to instruct B to tap to node D
- This is optimized for both full SID and NEXT-C-SID Flavor C-SID
  - Because of the LPM match on the combined LB:00B0:1000:: route
  - In the C-SID case, 00B0 and 1000 are all C-SIDs
Tapping by A Monitor Node

- A monitor node may be on the normal forwarding path and may need to tap a packet to its monitor.
- The previously described GIB TID is not enough for this:
  - The LB:LN:GIB-TID:: route on the monitor is to send the received tapped packet to its monitor, not to tap a received packet.
- A separate LIB TID is allocated and advertised for tapping locally:
  - In an End.TAP.X End SID.
  - A LB:LN:LIB-TID:: route is installed to tap to a local monitor.
  - An ingress uses the received SID to instruct the monitor node to tap locally:
    - E.g., LB:00D0:9999::
Summary

• Extend C-SID’s GIB/LIB concepts to the FUNC space of full SIDs
• A monitor node advertises a GIB Tapping ID for “tapping to me”
  • As FUNC part of an End.TAP End SID
  • A local forwarding route is installed to send tapped packets to its monitor
• A tapping node combines the received GIB TID with its own locator
  • Installed as a local forwarding route to do tapping
• An ingress node combines a tapping node’s locator and the GIB TID
  • Used a full SID in the SID list, or
  • The TID is used as a C-SID after the tapping node’s node C-SID
• A monitor node advertises a LIB Tapping ID for “ask me to tap locally”
  • As part of an End.TAP.X End SID
Next Steps

- Continue to seek WG comments and suggestions
- Continue to finish/polish the draft
- Seek adoption afterwards