MicroTap Segment

https://www.ietf.org/archive/id/draft-zzhang-spring-microtap-segment-00.txt

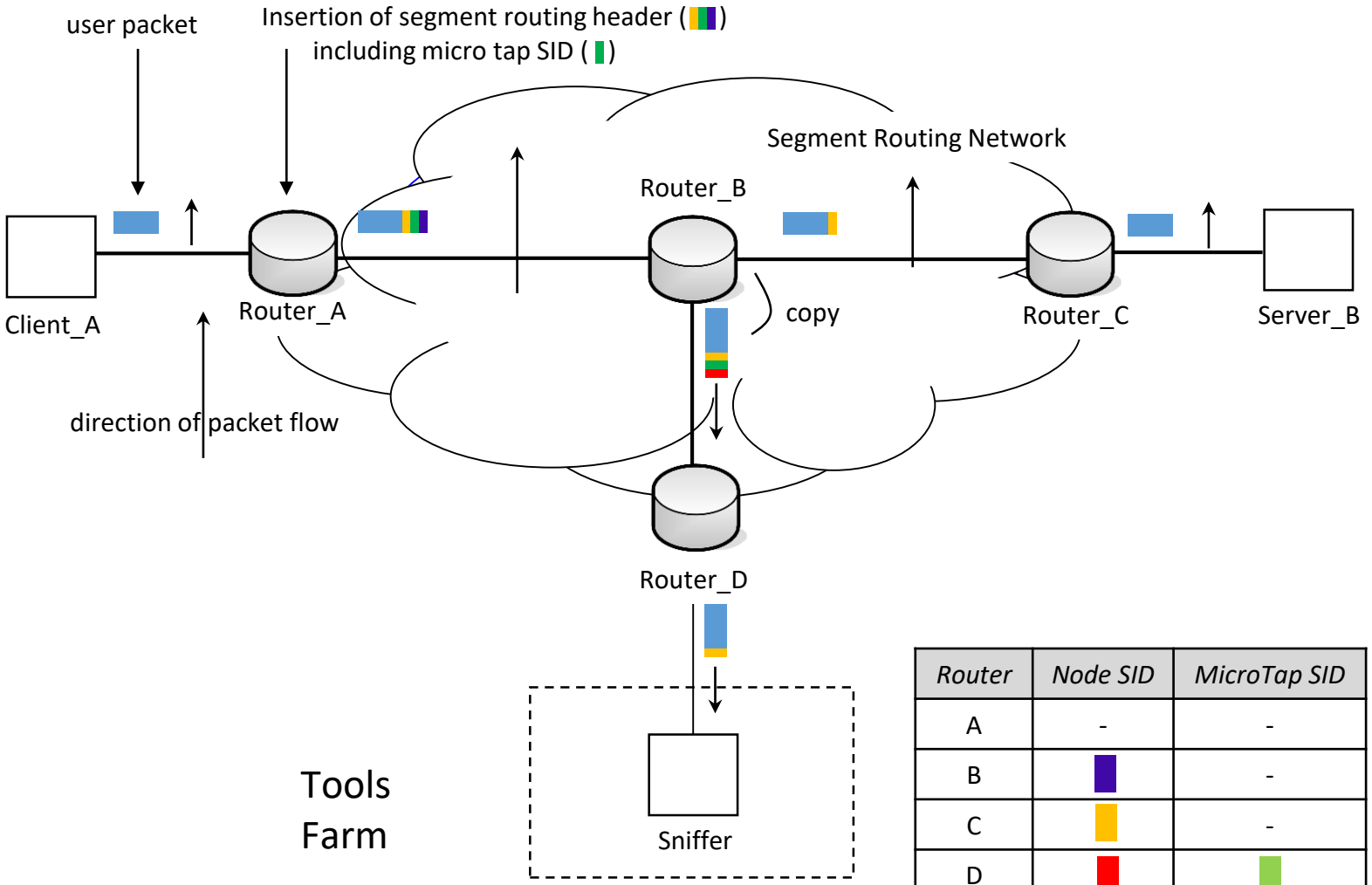
Authors: Zhaohui Zhang, Juniper Networks
Ryan Hoffman, TELUS
Gurminderjit Bajwa, TELUS
Daniel Voyer, Bell Canada
Shay Zadok, Broadcom

Basic intention of the draft

- Defines a new type of segment called microTap segment, used for capturing traffic from a transit router for performance and packet analysis
- Instruction that a MicroTap SID represents: make a copy of the packet & send the copy to a destination for packet analysis
- Strategic placement of one or more microTap SIDs within a SID-list results in traffic tapping at targeted points within the network
  - A router encountering the microTap SID makes a copy of the packet and sends it to the router connected to monitoring tool
  - The original frame continues on to the destination

Example: Traffic capture 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



Router	*Node SID*	*MicroTap SID*
A	-	-
B		-
C		-
D		

Signaling

MicroTap capability: A node supporting microTap function advertises its capability to other nodes and PCE.

For all relevant protocols (ISIS, OSPF & BGP-LS), the new flag T in the Flags field of the Prefix/Adjacency-SID TLV or Sub-TLV indicates that a MicroTap SID is allowed to follow the prefix/adjacency SID in a packet.

MicroTap SID: A node hosting a monitor is provisioned with a microTap SID allocated from the SRGB. The microTap SID is advertised to other nodes and PCE.

A new MicroTap-SID TLV or sub-TLV is defined for all the relevant protocols (ISIS, OSPF & BGP-LS) to advertise a microTap SID.

Benefits vs existing ways of remote mirroring

- **High level of granularity**
  - Offers the ability to capture the traffic of interest with precision especially on transit routers
  - Saves the network capacity needed to tunnel the traffic to tools
  - No excessive consumption of packet replication resources
  - No need for complex packet filtering on packet brokers
- **Use of standard technology**
  - Unifies the way the traffic is tunneled to the tool farm
  - Achieves vendor interoperability
- **Non-invasive**
  - No need to push or change configuration on the transit routers (P or LER)
- **Less resource intensive**
  - Alleviates the need for sophisticated chipsets to look deep into the packet

Next Steps

- Complete the draft
- Solicit comments/reviews and refine the draft accordingly

Thank You!