Intra-domain SAV Support via IGP
Intra-domain SAV Support via BGP

[1]draft-cheng-savnet-intra-domain-sav-igp-01
[2]draft-cheng-savnet-intra-domain-sav-bgp-00

Presenter ： Shengnan Yue (China Mobile)

Co-authors: Weiqiang Cheng (China Mobile)[1][2]
Dan Li (Tsinghua University)[1]
Changwang Lin (New H3C Technologies)[1][2]
Shengnan Yue (China Mobile) [1][2]

IETF119

Background

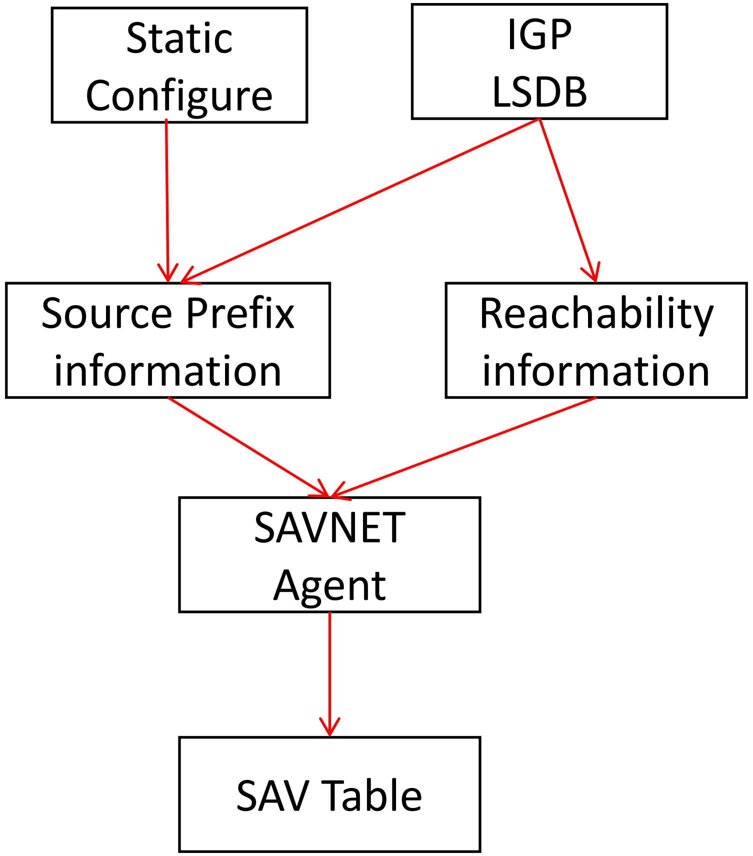
□ Source address validation (SAV) is important for defending against source address spoofing attacks, such as reflection attack

Existing mechanism	disadvantage
ACL-based ingress filtering[RFC2827]	Not Automation
Strict uRPF [RFC3704]	The validation is overly strict, which may lead to packet loss.
Loose uRPF [RFC3704]	The validation is permissive

□Our focus: Compute SAVNET rules based on intra-domain connectivity. SAVNET rules can be dynamically adjusted to the changes of network topology, apply interface-specific filtering, and prevent improper packet loss.

The overall IGP process framework

- The source prefix can be statically configured, or distributed within the domain via the IGP.
- Connectivity calculation is based on the existing IGP LSDB information. During connectivity calculation, it is required to perform two-way neighbor check for validation.
- Based on the source prefix information and reachability information, the SAVNET Agent utilizes connectivity algorithms to calculate the source port information of the source prefix, and generates the SAV rule table.



The principle of connectivity calculation

- □ Step 1: Before initiating the SAVNET rule calculation, save the existing SAVNET rule table to facilitate the identification of changes in SAVNET rule table entries.
- □ Step 2: Traverse all interfaces of the starting node and perform SAVNET rule calculation for each interface.
- □ Step 3:Clear the visited flag for all nodes and mark the starting node as visited to initialize the BFS (Breadth-First Search) traversal.
- □ Step 4: Add the neighboring nodes of the calculated interface to the queue and mark them as visited.
- □ Step 5: Retrieve the first node from the queue.
- □ Step 6: Process current node, add all adjacent unvisited nodes to the queue, and mark them as visited.
- □ Step 7: Generate SAVNET rules for the calculated interface based on the source prefixes of current node.
- □ Step 8: Repeat steps 5 to 7 until the queue is empty.
- □ Step 9: Repeat steps 2 to 8 until SAVNET rules for each interface are individually calculated.
- □ Step 10: Merge the SAVNET rule entries obtained by all interfaces, combining entries with the same prefix into a single entry and consolidating the interfaces from each entry into the interface list of the merged entry.

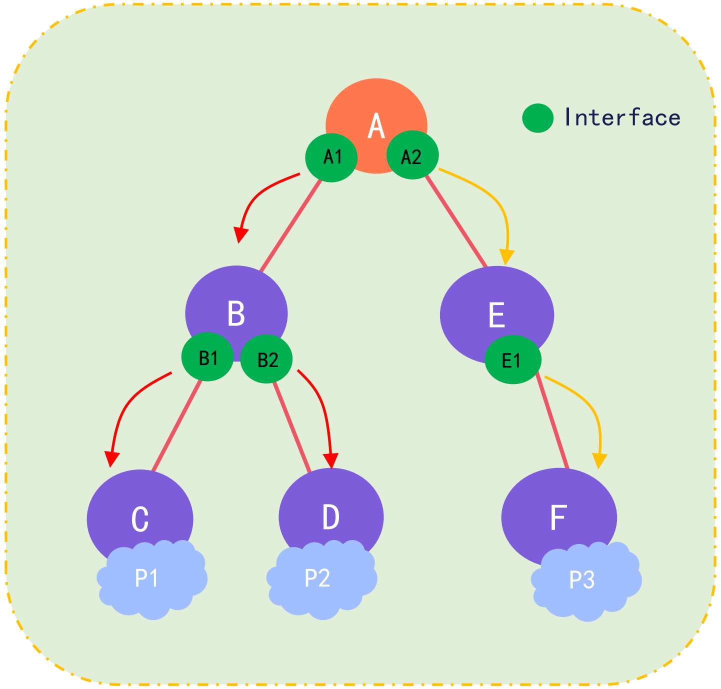
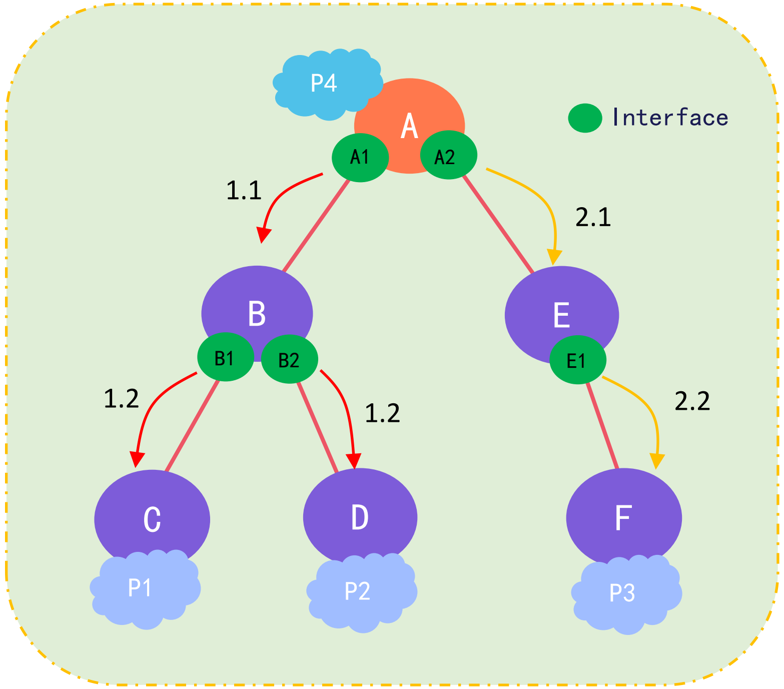
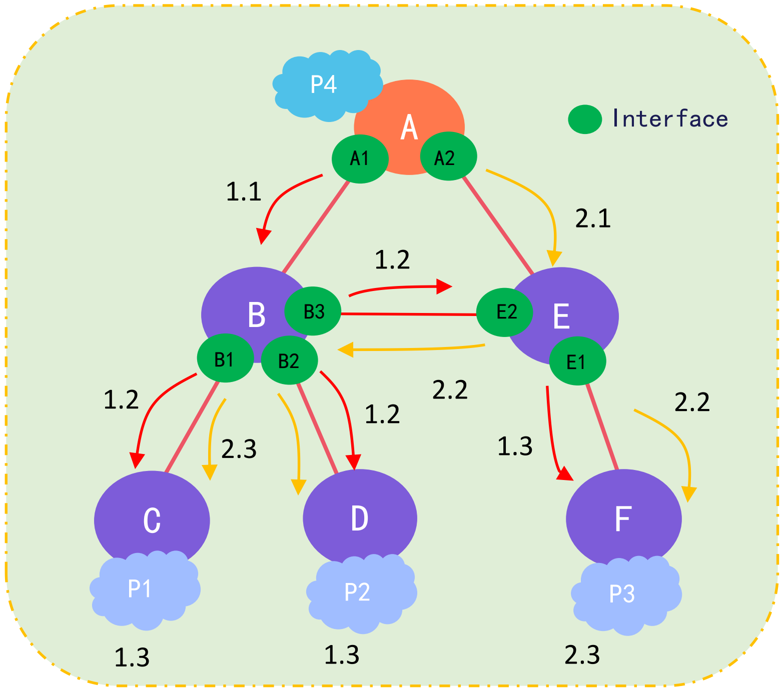
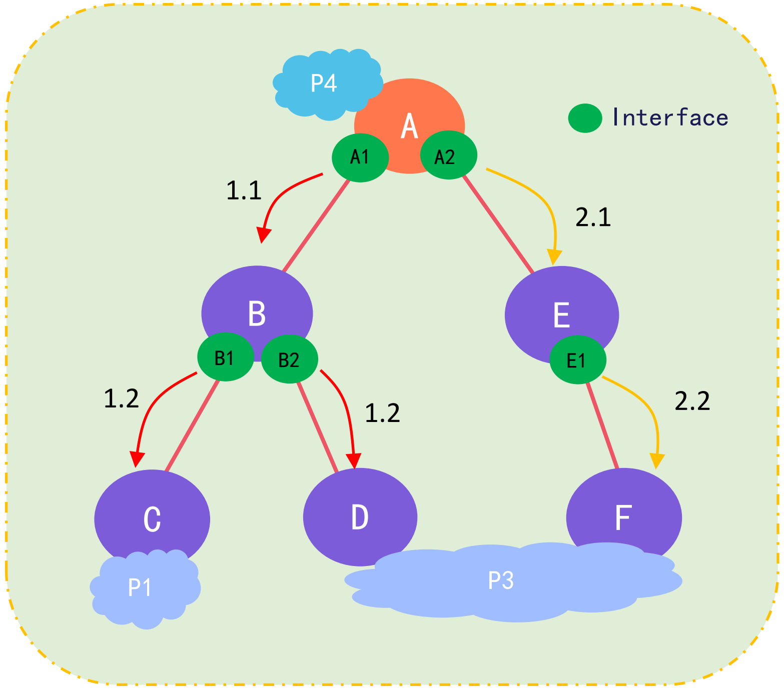


Diagram of IGP protocol calculating SAVNET rules.







Scenario 1

1.1: A1->B; 1.2: B1->C, B2->D;

2.1: A2->E; 2.2: E1->F

□ (P1, A1), (P2, A1)
(P3, A2)

Scenario 2

1.1:A1->B; 1.2:B1->C,B2->D,B3->E;

1.3: E1->F;

2.1:A2->E; 2.2:E1->F,E2->B;

2.3: B1->C, B2->D;

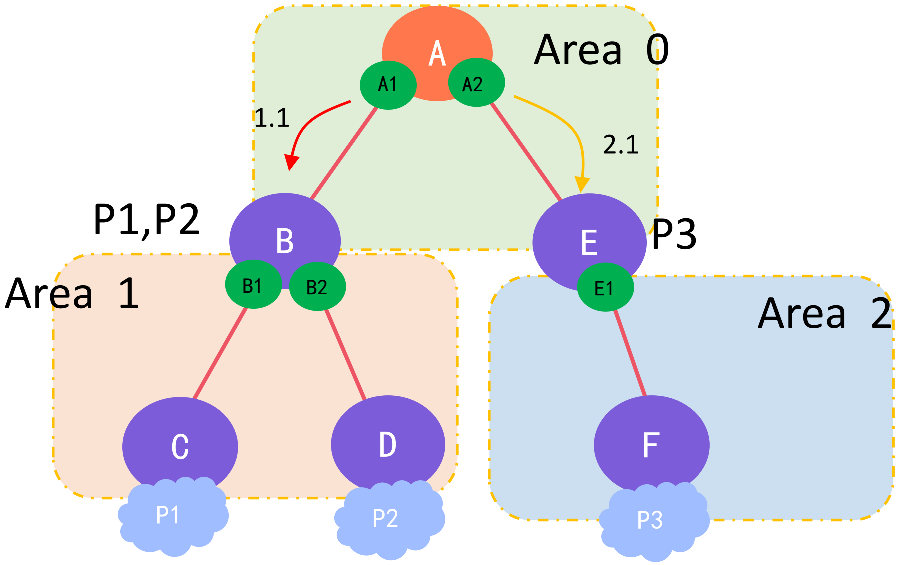
□ (P1, A1), (P2, A1), (P3,A1)
(P3, A2),(P1,A2),(P2,A2)

Scenario 3

1.1: A1->B; 1.2: B1->C, B2->D;

2.1: A2->E; 2.2: E1->F

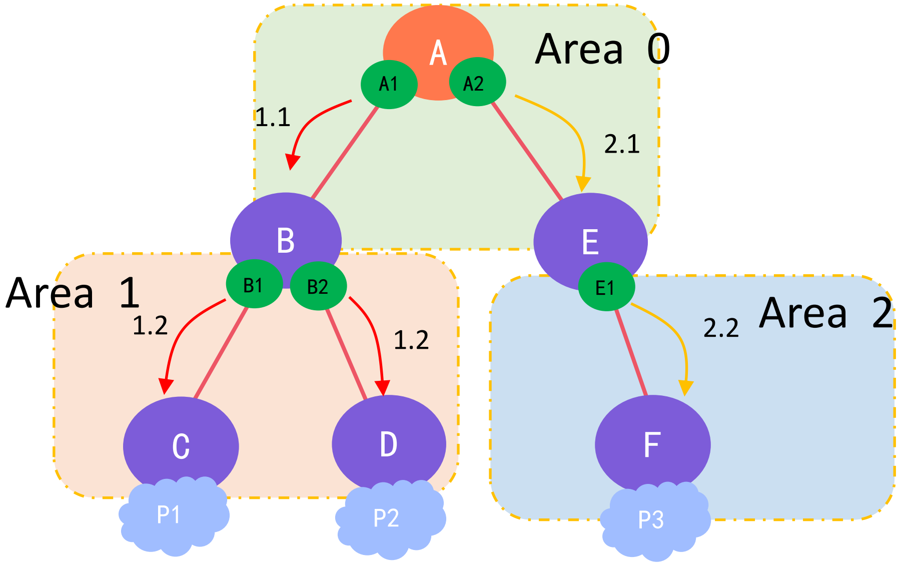
□ (P1, A1), (P3, A1)
(P3, A2)



Internal prefix

Scenario 4
In the case of inter-area internal prefix:
A1->B(ABR)
A2->E(ABR)

□ (P1, A1), (P2, A1)
(P3, A2)



External prefix

Scenario 5
In the case of inter-area external prefix:
A1->B(ABR)->C(ASBR),D(ASBR)
A2->E(ABR)->F(ASBR)

□ (P1, A1), (P2, A1)
(P3, A2)

Optional IGP Extension

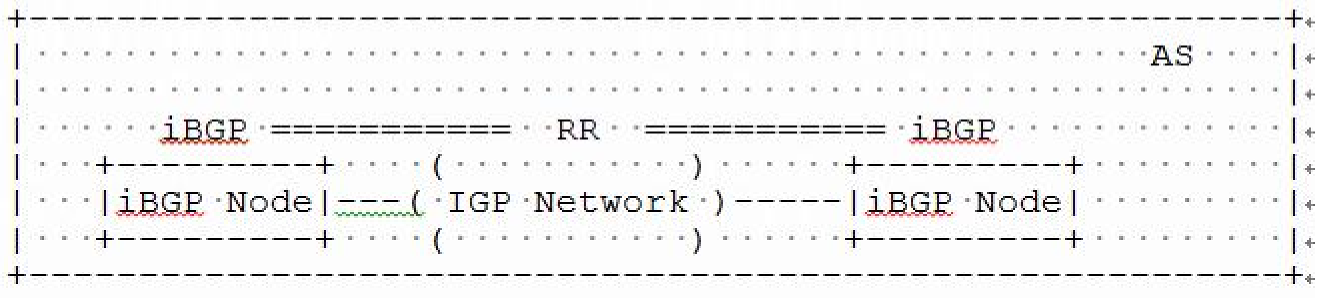
- ISIS: IPv4 SAVNET source prefixes are advertised using "IP Extended Reach TLV" (type 135), while IPv6 SAVNET source prefixes are advertised using "IPv6 Reachability TLV" (type 236, RFC5308). With Source Prefix Flag

- OSPF: SAVNET source prefixes are advertised using “OSPFv2 Extended Prefix Opaque LSA”[RFC7684]. With Source Prefix Flag

- OSPFv3: SAVNET source prefixes are advertised using “OSPFv3 Extended LSA”, including “E-Intra-Area-Prefix-LSA”, " E-Inter-Area-Prefix-LSA" and "E-AS-External-LSA"[RFC8362]. With Source Prefix Flag

Scenario: Propagating Source Prefixes via iBGP

- Propagating Source Prefixes via iBGP over IGP-Based Neighbor Establishment practical networks, it is common to propagate source prefixes via iBGP, which establishes neighbors using the underlying IGP network. All iBGP neighbors exchange source prefix information through a Route Reflector (RR).

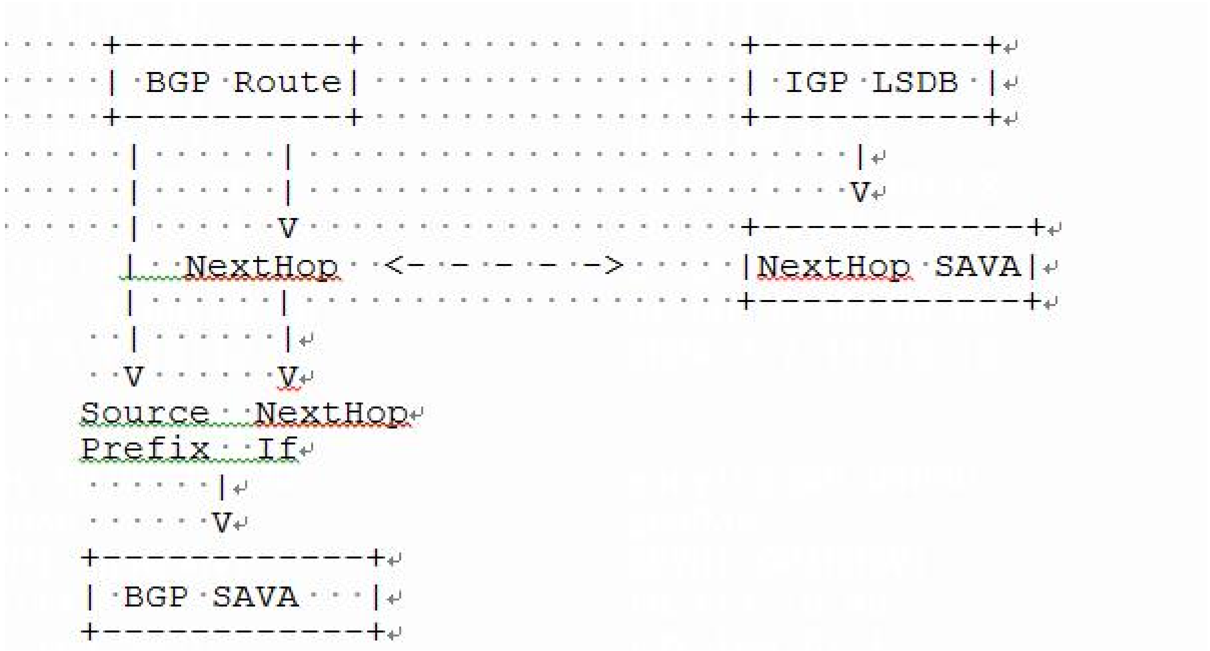


```
+----------------------------------------------------------+
|                                                   AS     |
|                                                          |
|      iBGP ===========  RR  =========== iBGP              |
|   +---------+    (           )      +---------+          |
|   |iBGP Node|---( IGP Network )-----|iBGP Node|          |
|   +---------+    (           )      +---------+          |
+----------------------------------------------------------+
```

iBGP Computation for Intra-Domain SAV Architecture

□Step 1: Calculate the SAV Rule-1 via IGP, using the process before, which are related to the BGP next hop.

□Step 2: Obtain the source prefixes published by the BGP neighbor and fetch the SAV Rule-1 table corresponding to the next hop of the BGP neighbor. Then, inherit the source interface list from the neighbor's SAV Rule-1 table to generate the BGP SAV rule table.

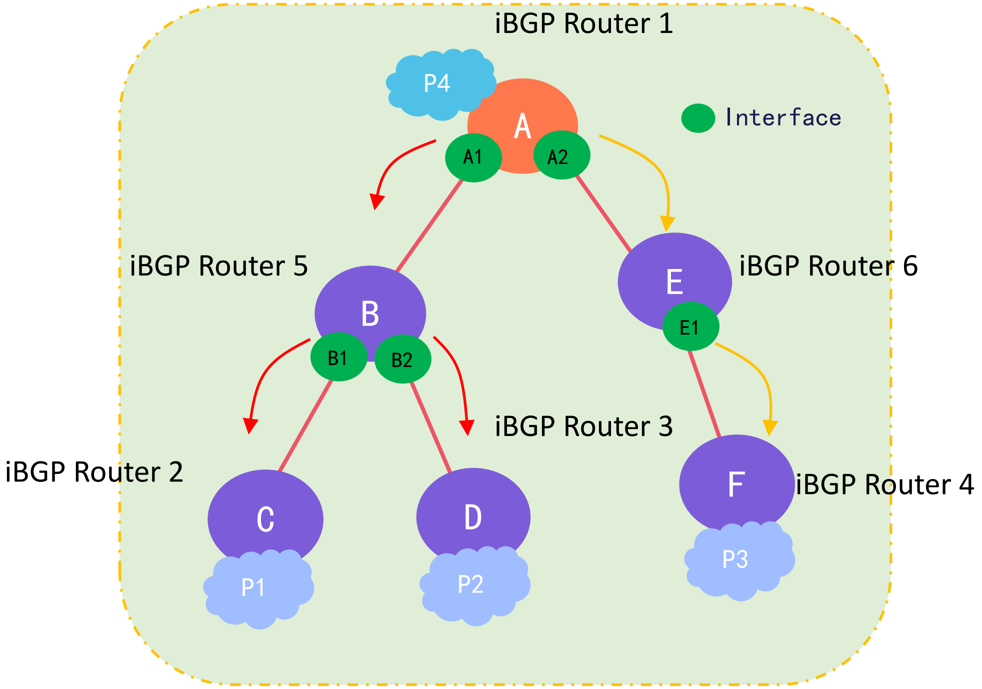


Calculation Process of Intra-Domain SAV Rules in BGP Protocol

Example: Generating SAV Rules for NodeA

- □ Step 1: Calculate the intra-domain next hop SAV Rule-1 table through the IGP protocol. (Router5, A-1), (Router2, A-1), (Router3, A-1); (Router6, A-2), (Router4, A-2).

- □ Step 2: Iterate through the BGP neighbor's next hops. If the neighbor has published source prefixes, use the next hop to search the next hop SAV Rule-1 table and inherit its source interfaces to generate the BGP SAV rule table.(Prefix1, A-1), (Prefix2, A-1), (Prefix3, A-2).



- □ (Router5, A-1), (Router2, A-1),(Router3, A-1)
  (Router6, A-2), (Router4, A-2)
- □ (P1, A1), (P2, A1)
  (P3, A2)

Summary: Intra-domain solutions

Mechanism	Comparative Analysis
ACL-based ingress filtering[RFC2827]	Not Automation
Strict uRPF [RFC3704]	The inspection is overly strict, which may lead to packet loss.
Loose uRPF [RFC3704]	The inspection is permissive
Reverse SPF Calc	Complex calculations required, difficult to calculate backup ingress interface for routers with primary and backup paths
BGP-based SPA/SPD path probing	Requires network-wide upgrade, path probing-based solutions may result in delayed routing convergence
This draft： Based on reached topology	Simplified computation for quick convergence, can be fully deployed incrementally

Next Step

□Add multi-homed subnet scenario

□Add restrictions to minimize traversal of interfaces belonging to the same group, ensuring a more accurate determination of the ingress interface.

SAVNET Use Cases

draft-ys-savnet-use-cases-00

Presenter ： Shengnan Yue (China Mobile)

Co-authors: Shengnan Yue (China Mobile)

Xueyan Song(ZTE Corporation)
Changwang Lin (New H3C Technologies)

Nan Geng (Huawei Technologies)

IETF119

Use case: Mobile Transport Network

□Implementation:

In NG (R)AN network there are optional connection links between CSG and Edge Node (between Access Network and Aggregation Network) which use IP or Ethernet technology.

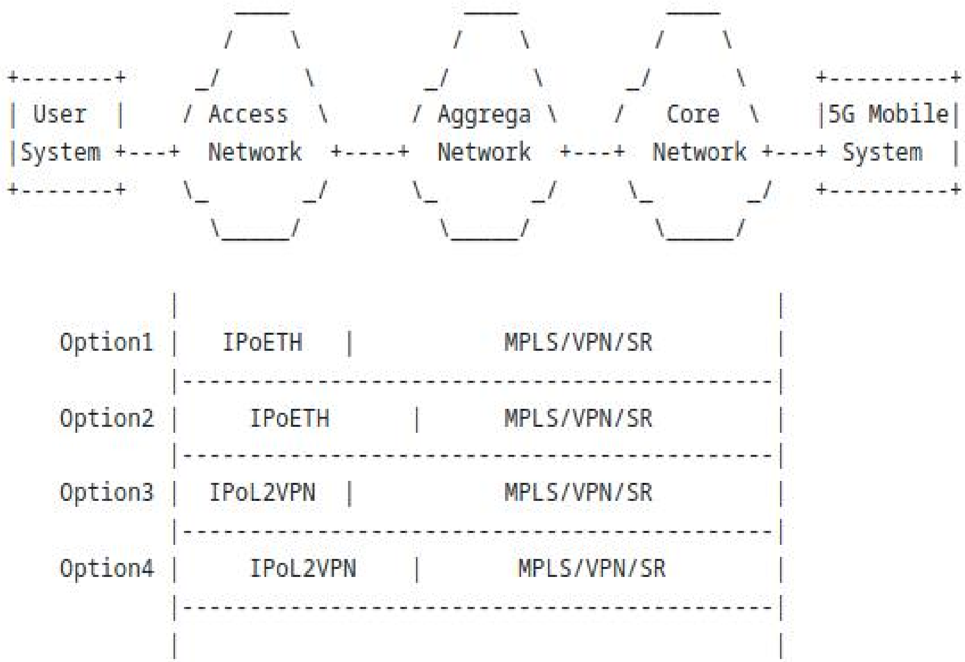
The more common deployment is to use MPLS/VPN as overlay technology.

The validation of label packets with MPLS/VPN deployments is out of the scope of the SAVNET.

□Possible improvements for SAV:

Only location for SAVNET is in Access Network, but SAVI function MAY be enough

In cross-domain network between different Service Providers, EBGP protocol SHOULD support SAVNET.



```
                 ___             ___            ___
                /   \           /   \          /   \
+-------+     _/     \        _/     \       _/     \      +---------+
| User  |    / Access \      / Aggrega \    /  Core  \     |5G Mobile|
|System +---+ Network  +----+ Network  +---+ Network +---+ System  |
+-------+    \_       _/     \_       _/    \_       _/    +---------+
               \_____/         \_____/        \_____/

          |                                         |
  Option1 |   IPoETH   |          MPLS/VPN/SR       |
          |-----------------------------------------|
  Option2 |      IPoETH      |     MPLS/VPN/SR      |
          |-----------------------------------------|
  Option3 |  IPoL2VPN  |          MPLS/VPN/SR       |
          |-----------------------------------------|
  Option4 |      IPoL2VPN    |      MPLS/VPN/SR     |
          |-----------------------------------------|
          |                                         |
```

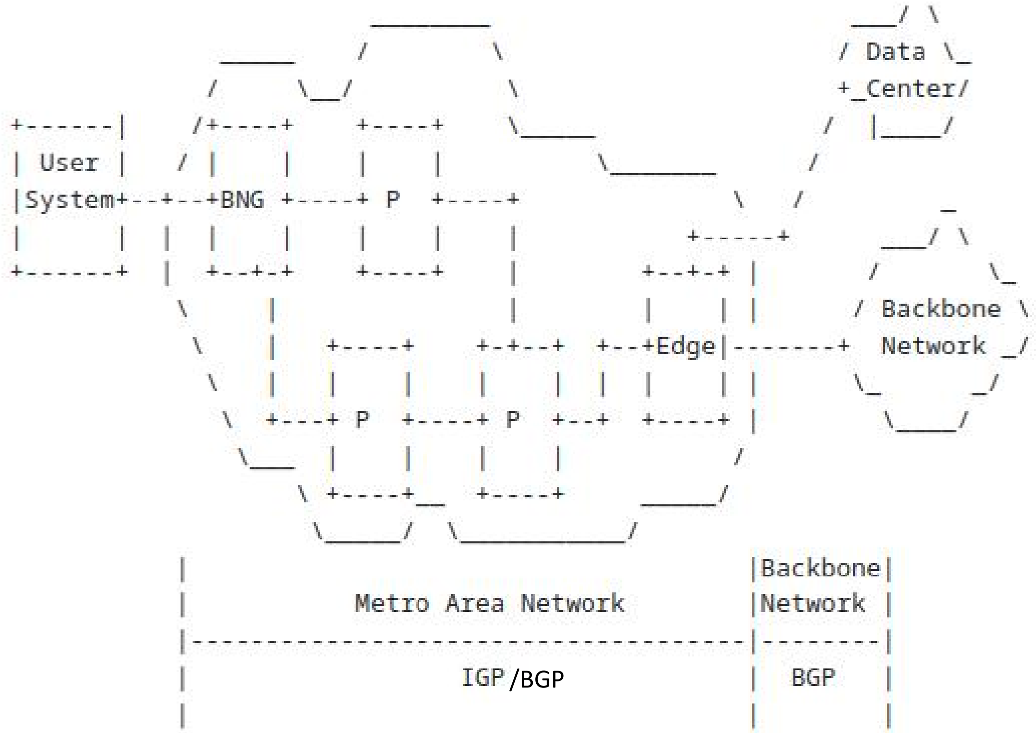
Use case: Fixed Transport Network

□Implementation:

- Access Network： there are optical connection links between fixed user and broadband network gateway (BNG) nodes which use IP or Ethernet technology.

- Metro Area Network：
  IGP (i.e., ISIS, OSPF) for the path connection or user traffic
  BGP for user traffic
  MPLS/VPN for service traffic as overlay.

- Backbone Network：
  BGP (i.e., eBGP) for the path connection



Use case: Fixed Transport Network

□Possible improvements for SAV:

The most feasible way for packets validation is at the location closest to the traffic.

- For the upstream traffic: the BNG
- For the downstream traffic： 1.the edge routers of BN network 2.MAN network nodes.

□For the SAV function used at BNG

- For the upstream traffic

the BNG applies the SAV function to determine whether the source address of the packet belongs to the legitimate user and the inbound port.

- For the downstream traffic

1. BNG advertises the source route prefix of broadband users to the upstream routers and receives the reachable route from the upstream router.
2. After receiving the traffic from the server, the BNG applies the SAV function to check whether the source address of the packet is valid and whether it matches the expected inbound port.

The detailed SAV policy and function is out of the scope of this document. There optional ways described at [I-D.cheng-savnet-intra-domain-sav-igp] or [I-D.cheng-savnet-intra-domain-sav-bgp].

- □Any questions and comments are welcome

THANKS