Reliability Framework for SRv6 SFC

draft-yang-rtgwg-srv6-sfc-reliability-framework

Feng Yang (China Mobile) (**Presenter**)

Xiaoqiu Zhang (China Mobile)

Changwang Lin (New H3C Technologies)

Yuanxiang Qiu (New H3C Technologies)

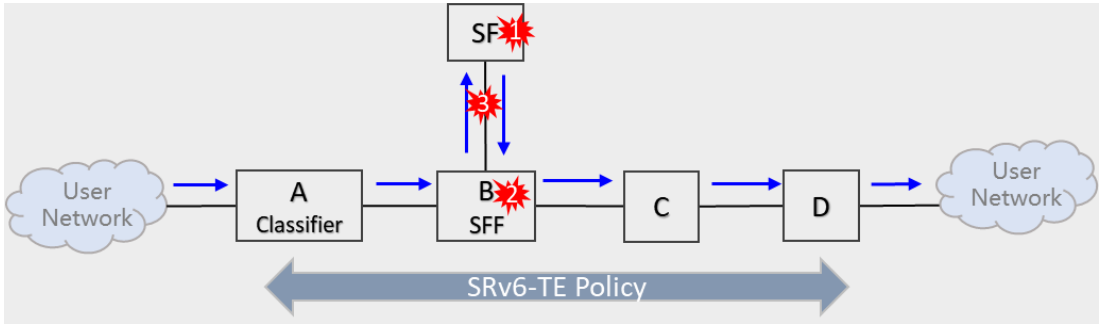
IETF-118

Background & Proposal

In SRv6 networks, the stateless SRv6 Service Function Chain (SFC) solution is implemented by sequentially arranging the specified Service Function (SF) into the SRv6 path.

During the deployment, we found that the SFC solution still has some reliability issues:

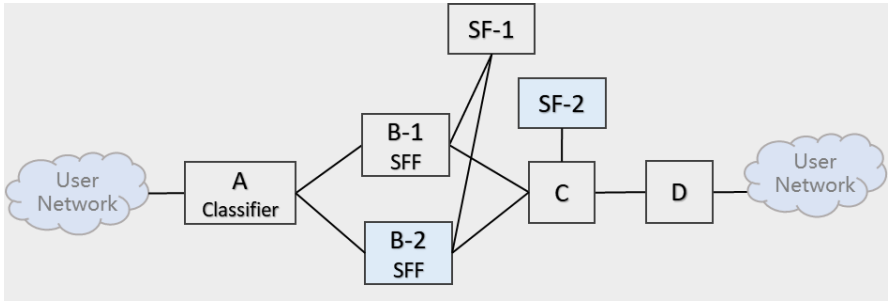
- Fault 1: SF fault
- Fault 2: SFF fault
- Fault 3: Link failure or unreachable routing between SFF and SF



Any of the above faults will cause the service message to be discarded.

How to improve the reliability of SFC?

- **SFF redundant backup**. Can solve Fault 2 and 3.
- **SF redundant backup**. Can solve Fault 1 and 3.
- **SF bypass forwarding**. Can solve Fault 1 and 3.

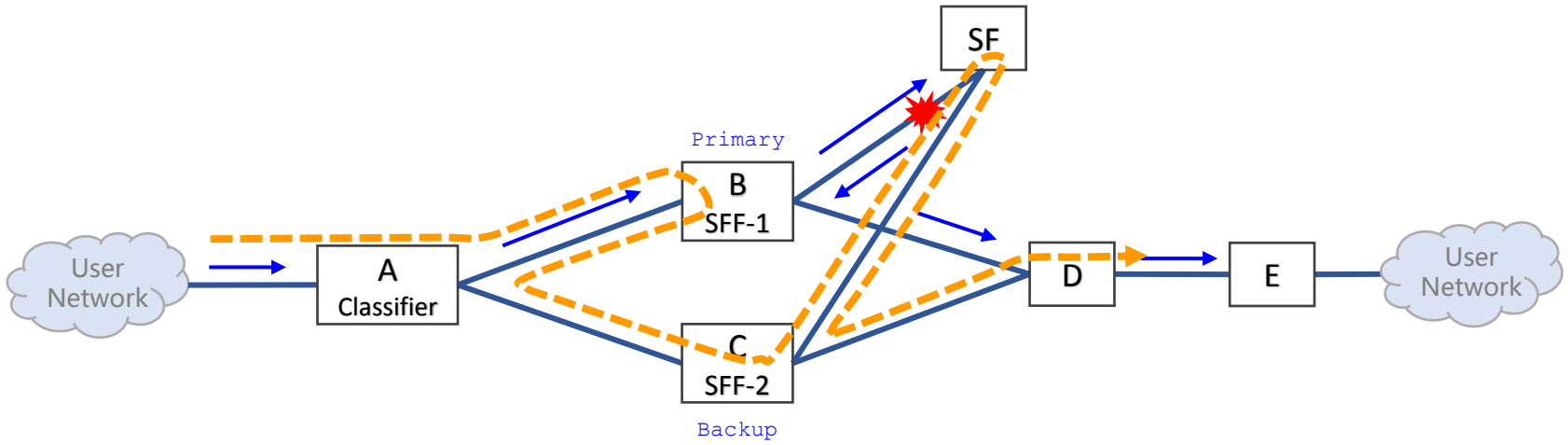


SFF Redundant Backup Protection Method

◆ Overview

- Deploy primary and backup SFFs for SF. SF is connected to both SFFs simultaneously..
- Normally, the messages are forwarded through the primary SFF (SFF-1) along path A->B->SF->B->D->E.
- When there is a fault between SFF-1 and SF, SFF-1 forwards the message to backup SFF (SFF-2), which then forwards the message to SF.

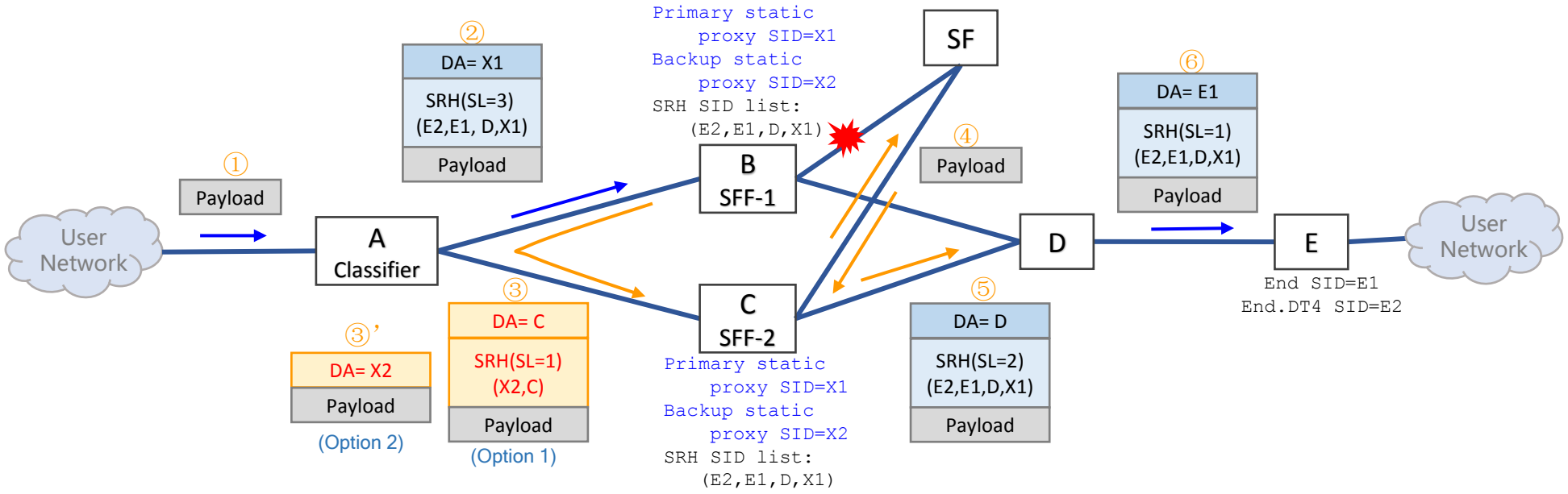
  The new forwarding path is A->B->C->SF->C->D->E.



SFF Redundant Backup Protection Method

◆ Static SR Proxy

- Configuration on SFF-1 and SFF-2
  - The mapping relationship cache entries for SRH and virtual interface.
  - The primary static proxy SID (X1) and backup static proxy SID (X2).
- Process flow
  - When SFF1 detects the fault between SFF-1 and SF, SFF-1 first removes the SRv6 header of the message, then encapsulates a new SRv6 header, and finally forwards the updated message to SFF-2.
    - Option 1: Through the SRv6 TE path to SFF-2, SID[0] is backup static proxy SID.
    - Option 2: Through the SRv6 BE path to SFF-2, the IPv6 DA is backup static proxy SID.
  - After receiving the message, SFF-2 removes the outer IPv6 header and SRH, and forwards the payload to SF.

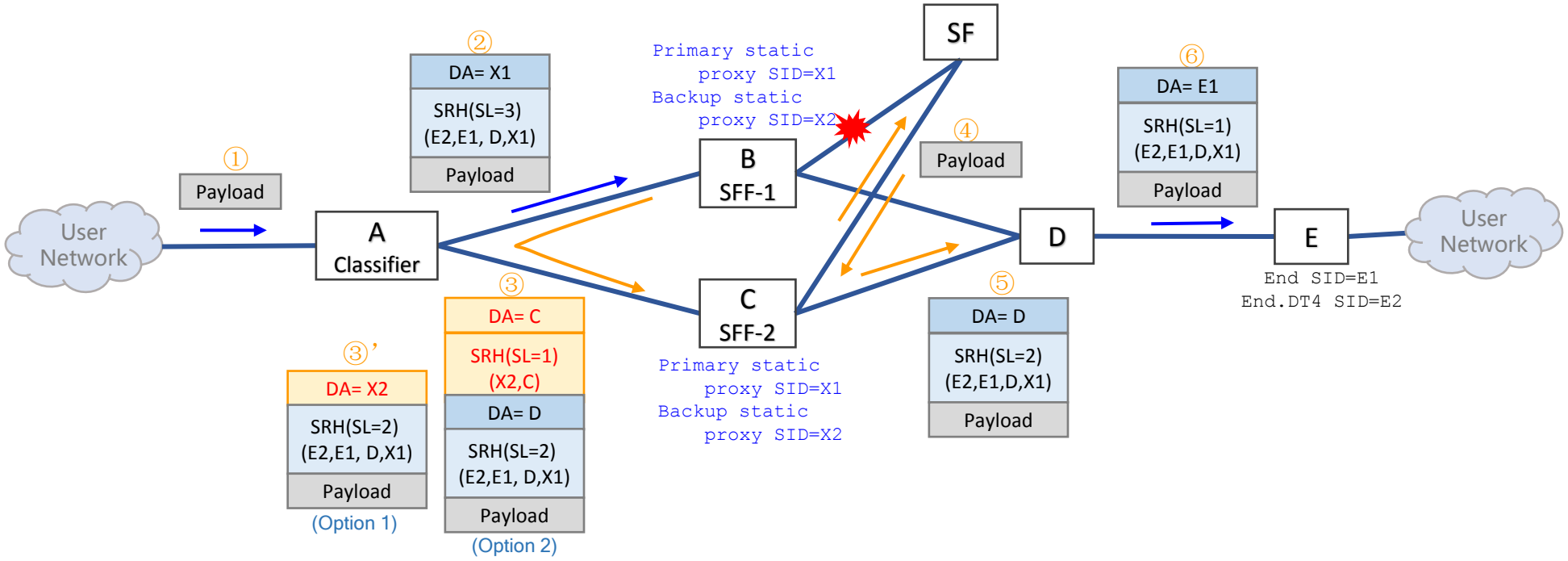


SFF Redundant Backup Protection Method

◆ Dynamic SR Proxy

Because the mapping relationship cache is dynamically generated based on the SRH of the message, SFF-1 cannot remove the SRH and needs to send it to SFF-2.

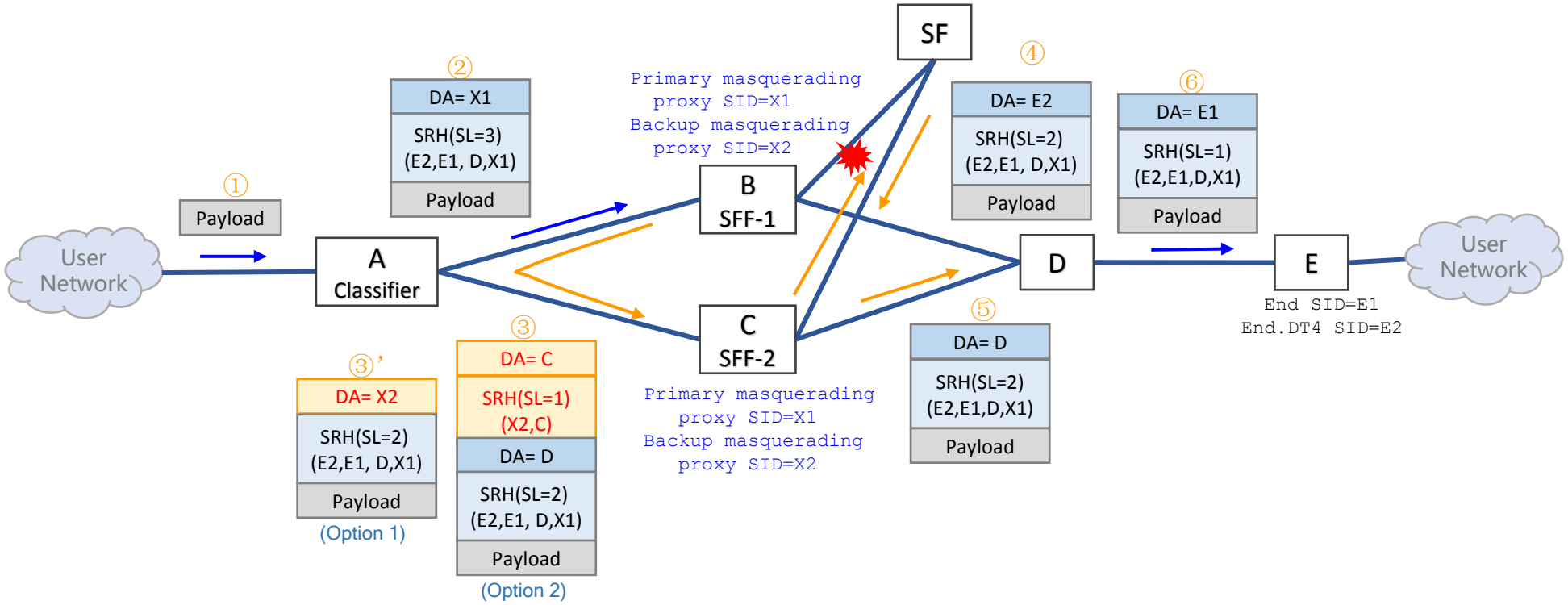
- When SFF1 detects that the route from SFF1 to SF is unreachable,
  - Option 1: SFF-1 replaces the IPv6 DA to backup dynamic proxy SID.
  - Option 2: SFF-1 adds another SRv6 header to the message. The SID[0] is backup dynamic proxy SID.
- After receiving the message, SFF-2 removes the outer IPv6 header(s), sends the payload to SF, and records the mapping relationship between SRH and the interface connecting SF.



SFF Redundant Backup Protection Method

◆ Masquerading SR Proxy

- When SFF1 detects that the route from SFF1 to SF is unreachable,
  - Option 1: SFF-1 replaces the IPv6 DA with the backup masquerading proxy SID.
  - Option 2: SFF-1 adds another SRv6 header to the message. The SID[0] is backup masquerading proxy SID.
- After receiving the message, SFF-2 removes the outer IPv6 header(s), changes the DA to SID[0], sends the payload to SF, and records the mapping relationship between the inner SRH and the interface connecting SF.



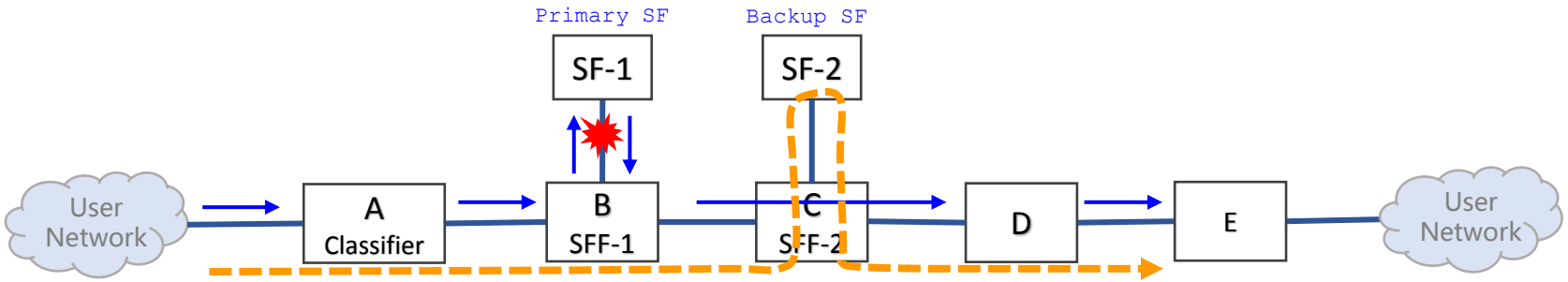
SF Redundant Backup Protection Method

Overview

- There are primary and backup SFs connected to SFF(s).
- Normally, service messages are processed by the primary SF (SF-1), and the forwarding path is A->B->SF-1->B->D->E.
- When there is a fault between SFF-1 and SF-1, SFF-1 will bypass SF-1 and forwards the message to backup SF (SF-2) connected to SFF-2 for service processing.

The bypass forwarding path is A->B->C->SF-2->C->D->E.

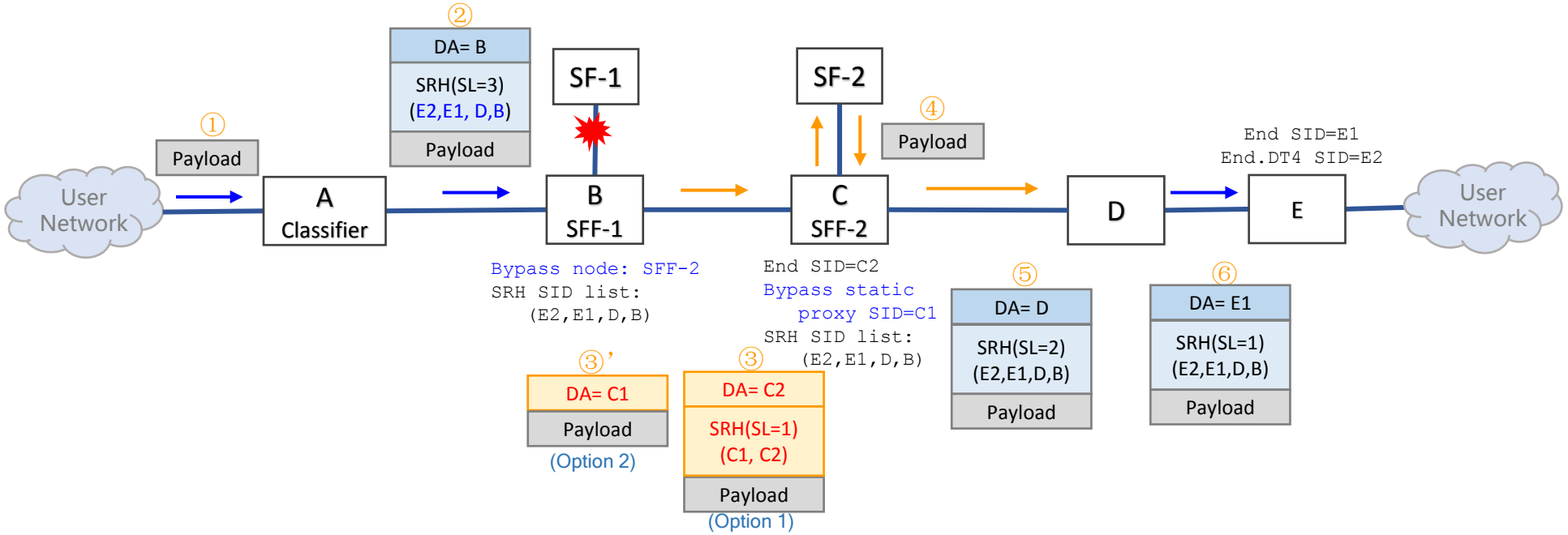
SFF-1 and SFF-2 can be the same device or two devices.



SF Redundant Backup Protection Method

◆ Static SR Proxy

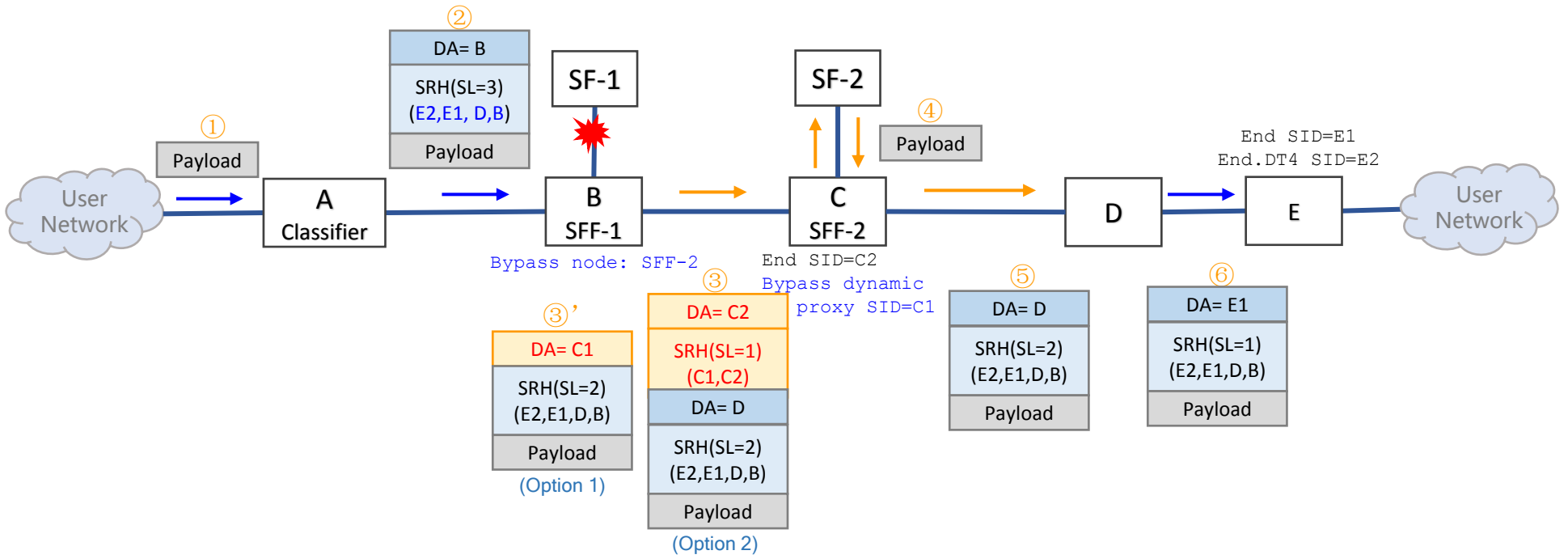
- Configuration
  - Config the mapping relationship cache entries for SRH and virtual interface on SFF-1 and SFF-2.
  - Specify SFF-2 as the bypass protection node on SFF-1.
  - Configure the bypass static proxy SID corresponding to the backup SF on SFF-2.
- Process flow
  - When SFF1 detects that the route from SFF-1 to SF-1 is unreachable, SFF-1 first removes the SRv6 header of the message, then encapsulates new SRv6 header, and finally forwards the updated message to SFF-2.
    - Option 1: Through the SRv6 TE path to SFF-2, SID[0] is bypass static proxy SID.
    - Option 2: Through the SRv6 BE path to SFF-2, the IPv6 DA is bypass static proxy SID.
  - After receiving the message, SFF-2 removes the IPv6 header, and sends the payload to SF-2.



SF Redundant Backup Protection Method

◆ Dynamic SR Proxy

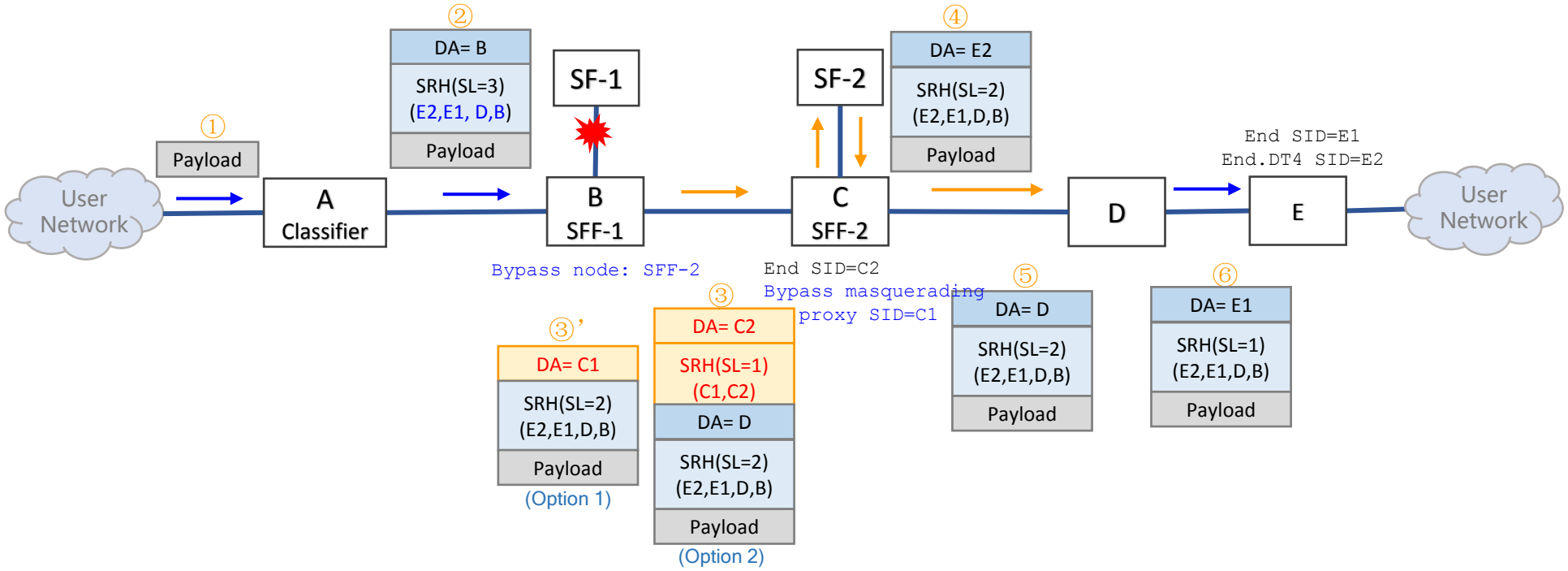
- When SFF1 detects that the route from SFF-1 to SF-1 is unreachable,
  - Option 1: SFF-1 replaces the IPv6 DA to bypass dynamic proxy SID.
  - Option 2: SFF-1 adds another SRv6 header to the message. The SID[0] is the bypass dynamic proxy SID.
- After receiving the message, SFF-2 removes the outer IPv6 header(s), and sends the payload to SF-2.



SF Redundant Backup Protection Method

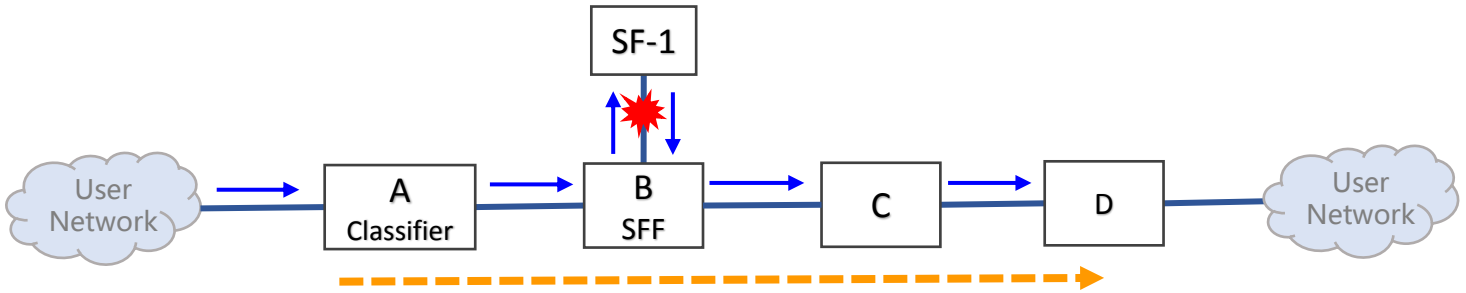
◆ Masquerading SR Proxy

- When SFF1 detects that the route from SFF-1 to SF-1 is unreachable,
  - Option 1: SFF-1 replaces the IPv6 DA to bypass masquerading proxy SID.
  - Option 2: SFF-1 adds another SRv6 header to the message. The SID[0] is the bypass masquerading proxy SID.
- After receiving the message, SFF-2 removes the outer IPv6 header(s), changes the DA to SID[0], and sends the payload to SF-2.



SF Bypass forwarding Method

When SFF detects that the route from SFF to SF is unreachable, it skips the service function processing and directly forwards packets to downstream nodes according to SRH SID list.



Next Steps

- Any questions or comments are welcomed
- Seeking for feedback