

NSF-Triggered Traffic Steering Framework (draft-hyun-i2nsf-nsf-triggered-steering-02)



IETF 98, Chicago, US

Mar. 27, 2017

**Sangwon Hyun, Jaehoon Paul Jeong, SangUk Woo,
YunSuk Yeo, and Jung-Soo Park**

Contents

I Introduction

II Packet Forwarding with SFC

III Our Proposal

IV Update of Version

V Next Step



Introduction

- This document describes an architecture of the I2NSF framework to enable packet forwarding between NSFs.
- Such traffic steering enables composite inspection of network traffic through various types of NSFs.
- It can also provide load balancing over NSF instances combined with dynamic NSF instantiation with NFV.

Packet Forwarding with SFC

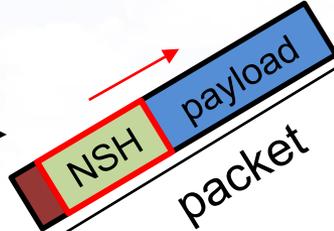
- Determination of the NSF path of a packet
- Re-classification for changing the existing path

Classifier

SFF

- Interpretation of the NSF path information
- Identification of the next NSF on the path
- Steering of the packet through the NSF path

NSH includes
- Path Identifier
- Service Index



NSF₁

NSF₂

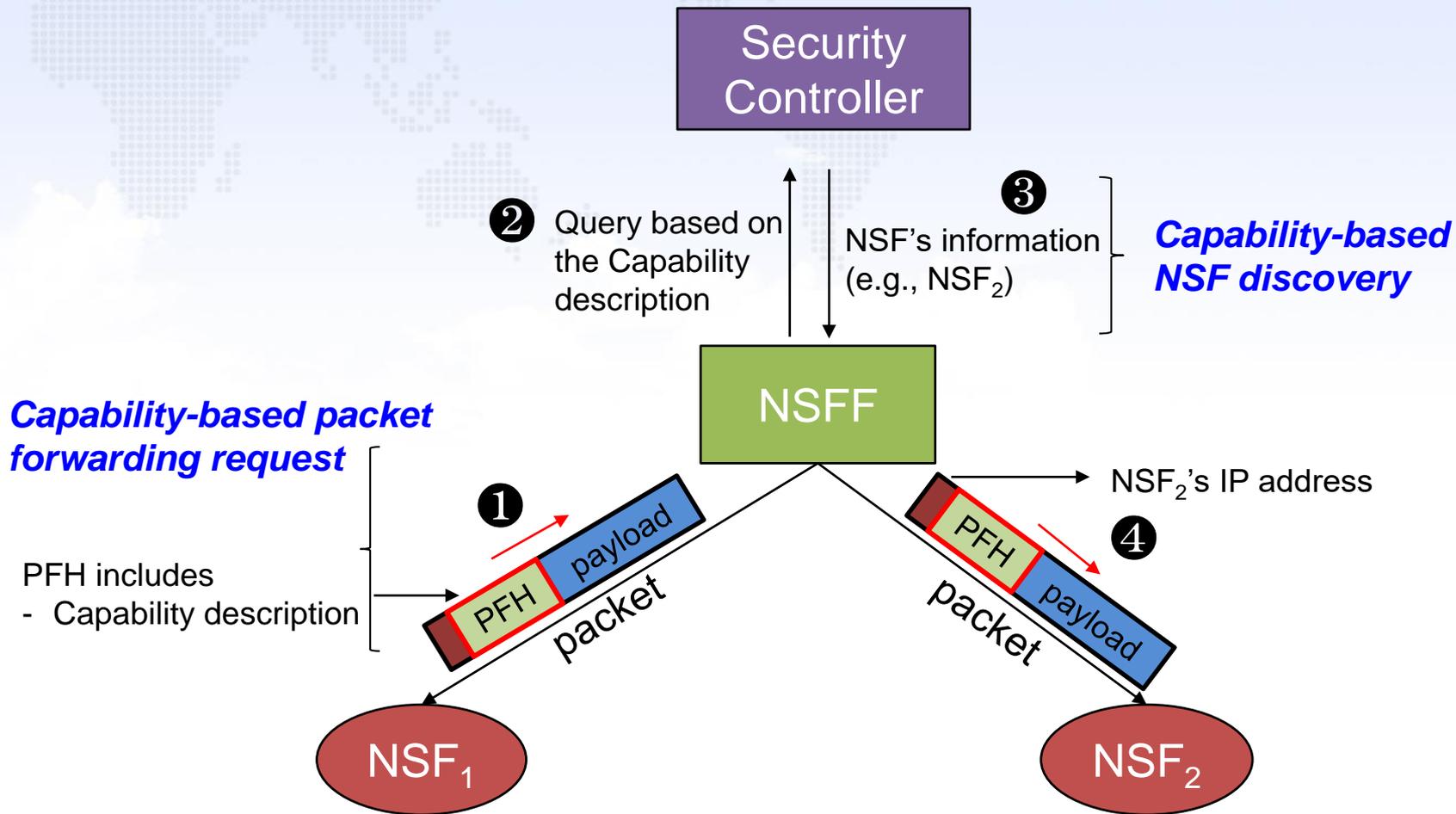
SFC for I2NSF: Pros & Cons

- In I2NSF, the NSF path for a packet is dynamically constructed, not pre-determined.

Pros	Cons
<ul style="list-style-type: none">✓ Existing standard✓ Good for enforcing a static service function path	<ul style="list-style-type: none">✓ <u>Re-classification overhead</u> under the circumstance of <i>dynamic</i> and <i>frequent</i> change of NSF path

Our Proposal:

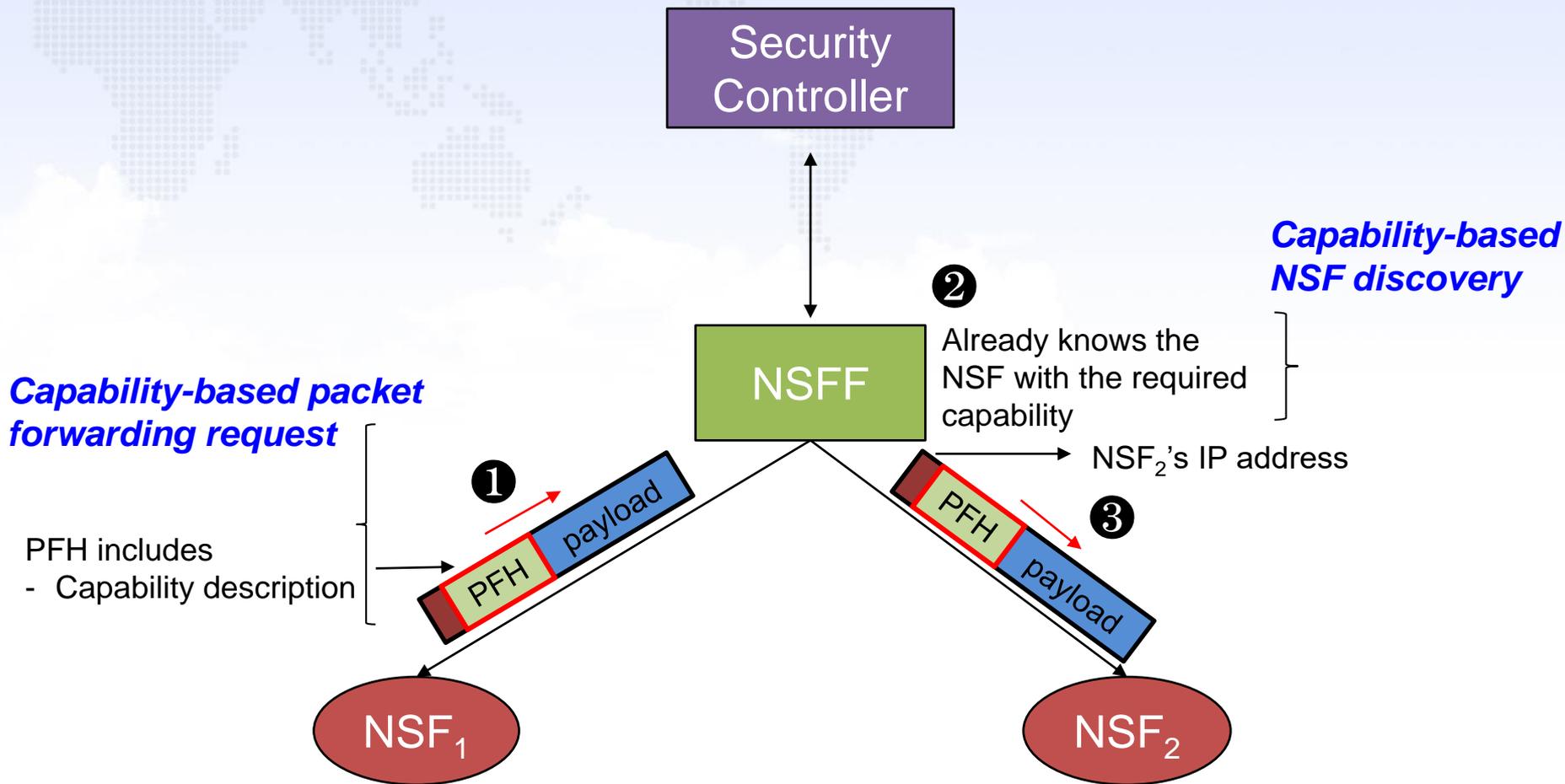
Case 1 (Non-Caching in NSFF)



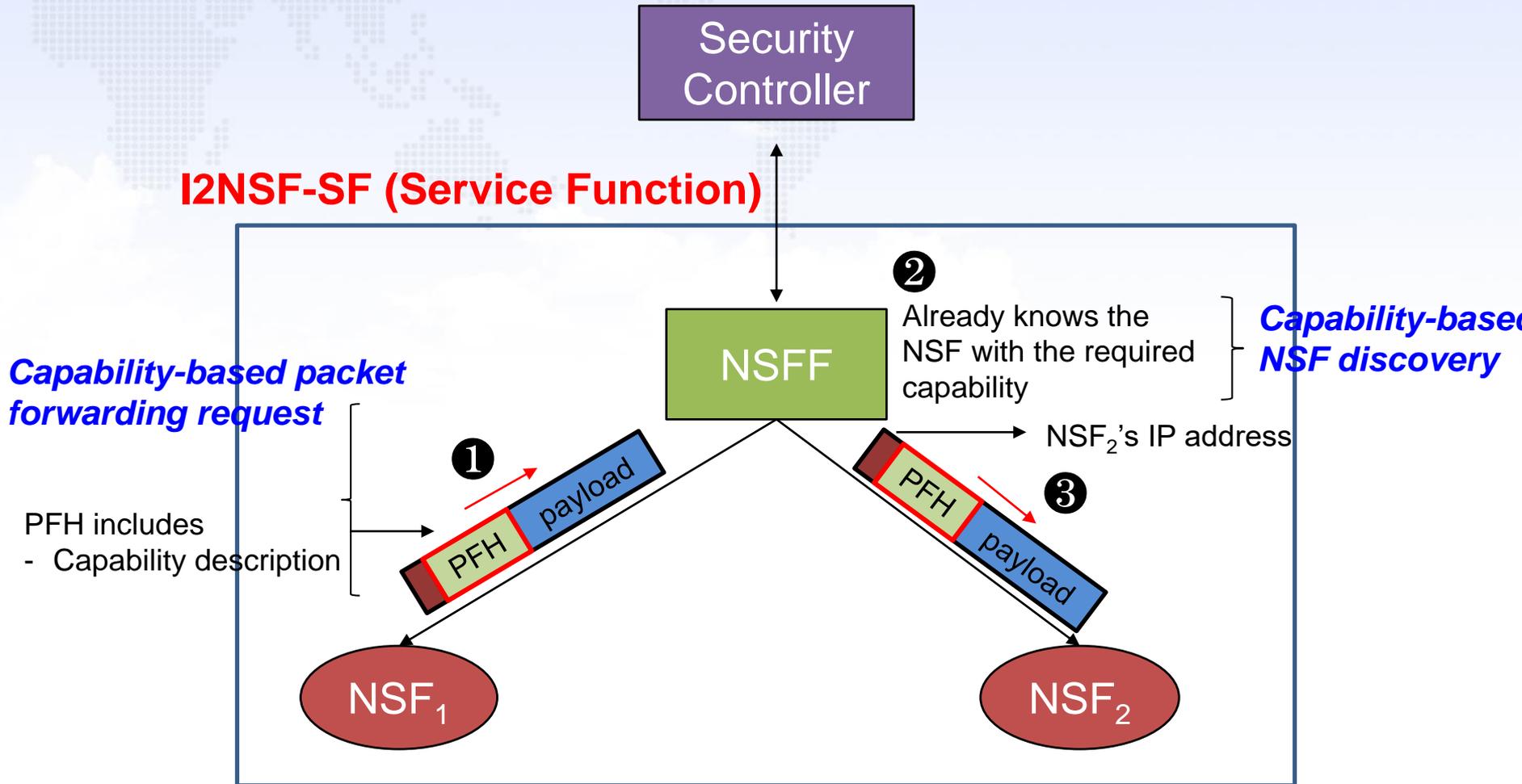
PFH: Packet Forwarding Header
NSFF: NSF Forwarder

Our Proposal:

Case 2 (Caching in NSFF)



Our Proposal: Conformance with SFC Architecture



Our Proposal

- Traffic Steering by only the next hop-by-hop NSF's identifier instead of the whole NSF path information
- Capability-based Packet Forwarding Request
 - Each NSF can trigger an advanced security action for a suspicious packet.
 - The NSF adds the description of the capabilities required for the advanced action to the suspicious packet.
- Capability-based NSF Discovery
 - The NSFF sends a query of an NSF with the required security capabilities to the Security Controller.
 - The Security Controller finds a matching NSF and informs the NSFF of the found NSF.

Update of Version

- The changes from draft-hyun-i2nsf-triggered-steering-in-i2nsf-01:
 - Explanation of **Packet Forwarding Header** is polished concretely.
 - We specified the details of **NSF Forwarding Information** for capability-based NSF discovery.

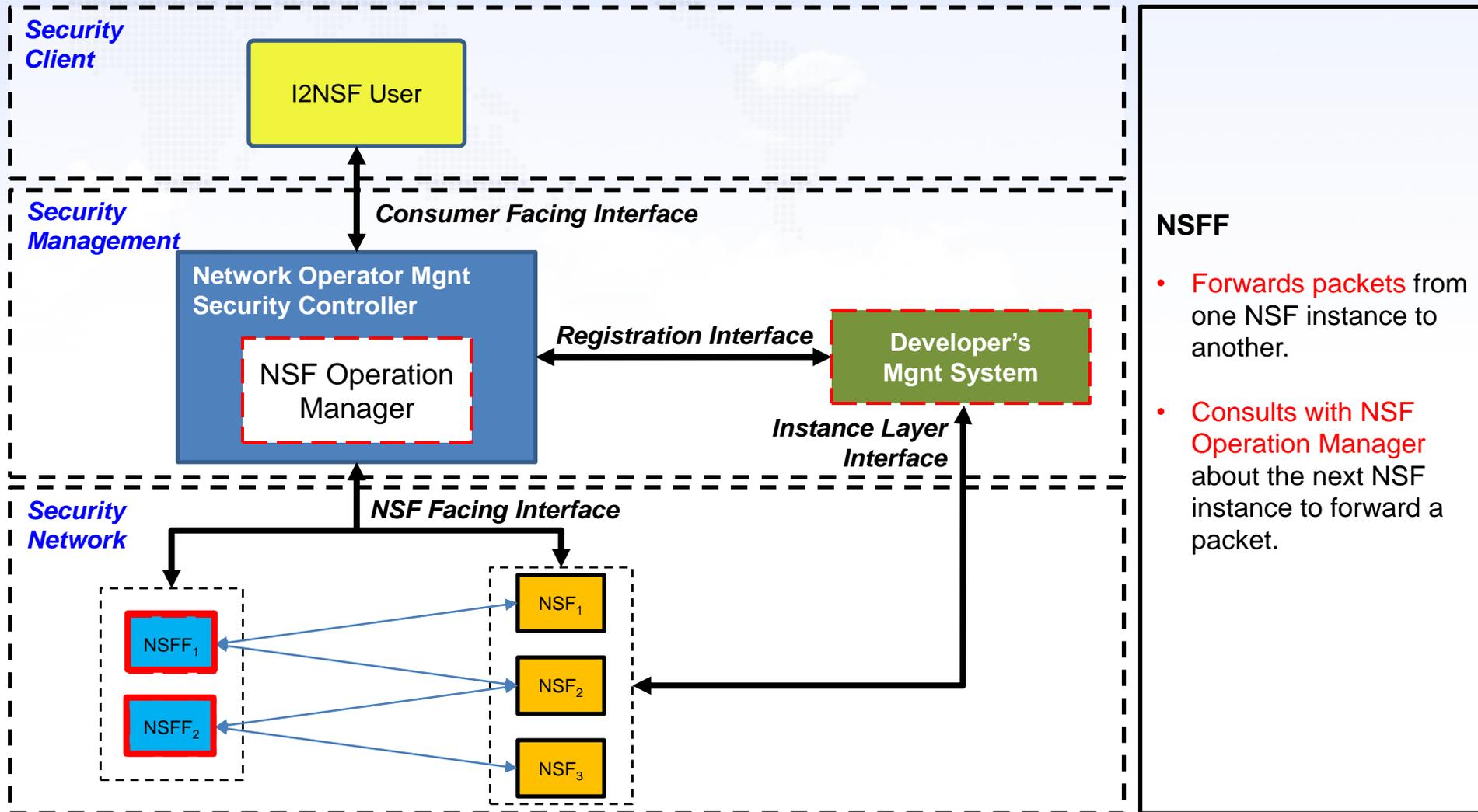
Next Step

- Clarification of our Traffic Steering scheme under SFC Architecture
- Design of **PFH Format** to specify the capability of the next-hop SF
- Design and Implementation of a **YANG Data Model** for NSFF's query of the next-hop SF toward the Security Controller with a given capability

Appendix



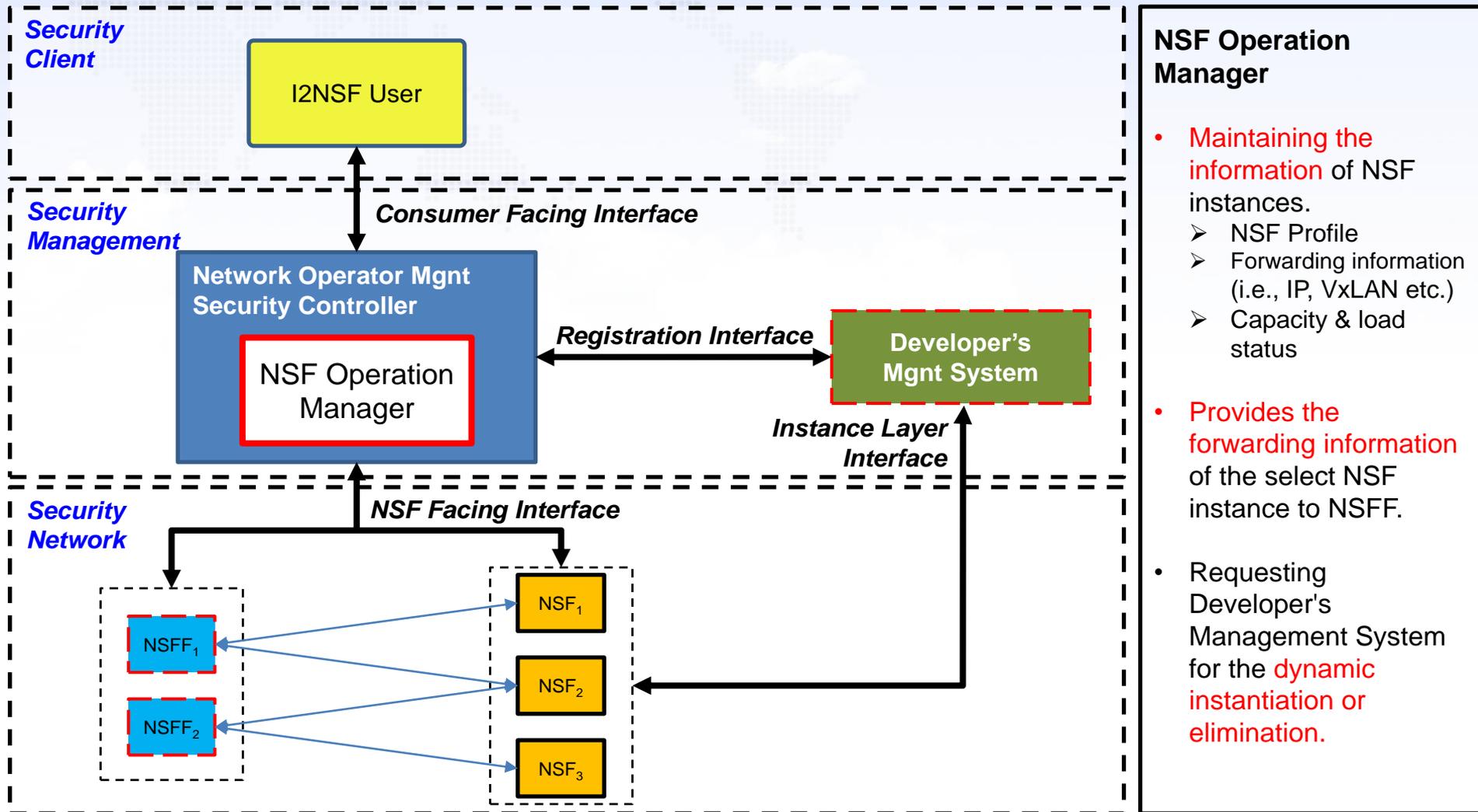
Architecture & Components



NSFF

- **Forwards packets** from one NSF instance to another.
- **Consults with NSF Operation Manager** about the next NSF instance to forward a packet.

Architecture & Components

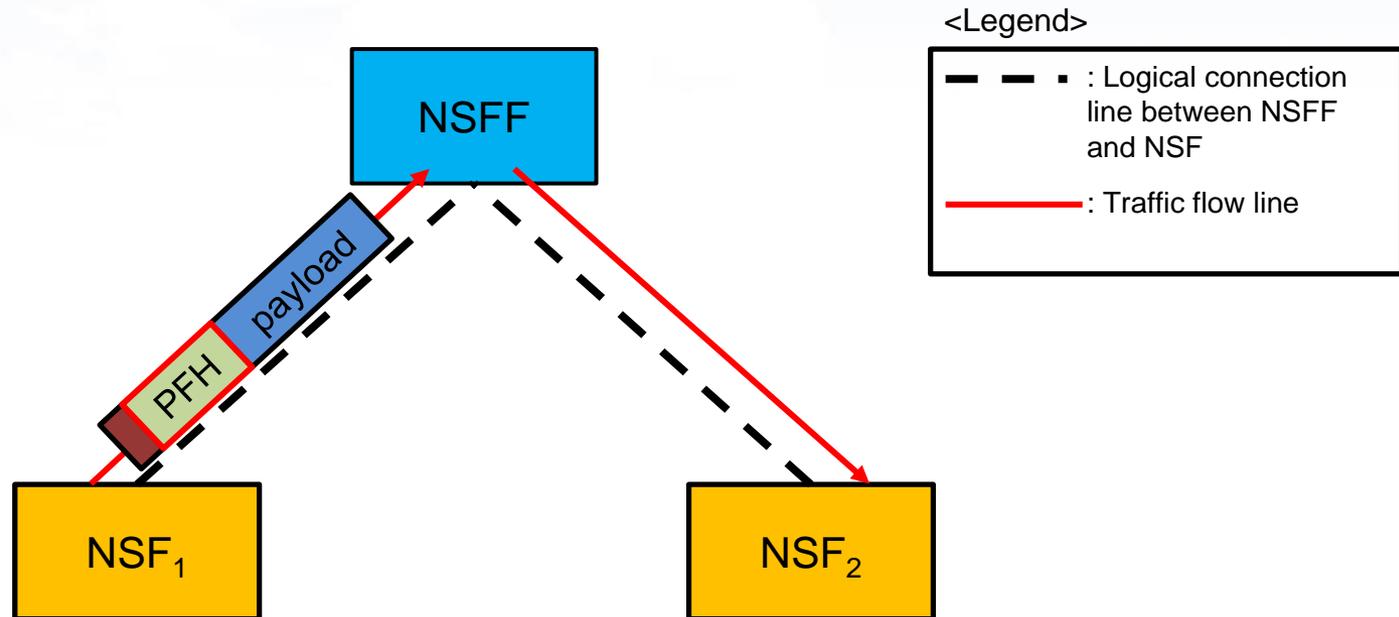


NSF Operation Manager

- **Maintaining the information** of NSF instances.
 - NSF Profile
 - Forwarding information (i.e., IP, VxLAN etc.)
 - Capacity & load status
- **Provides the forwarding information** of the select NSF instance to NSFF.
- Requesting Developer's Management System for the **dynamic instantiation or elimination**.

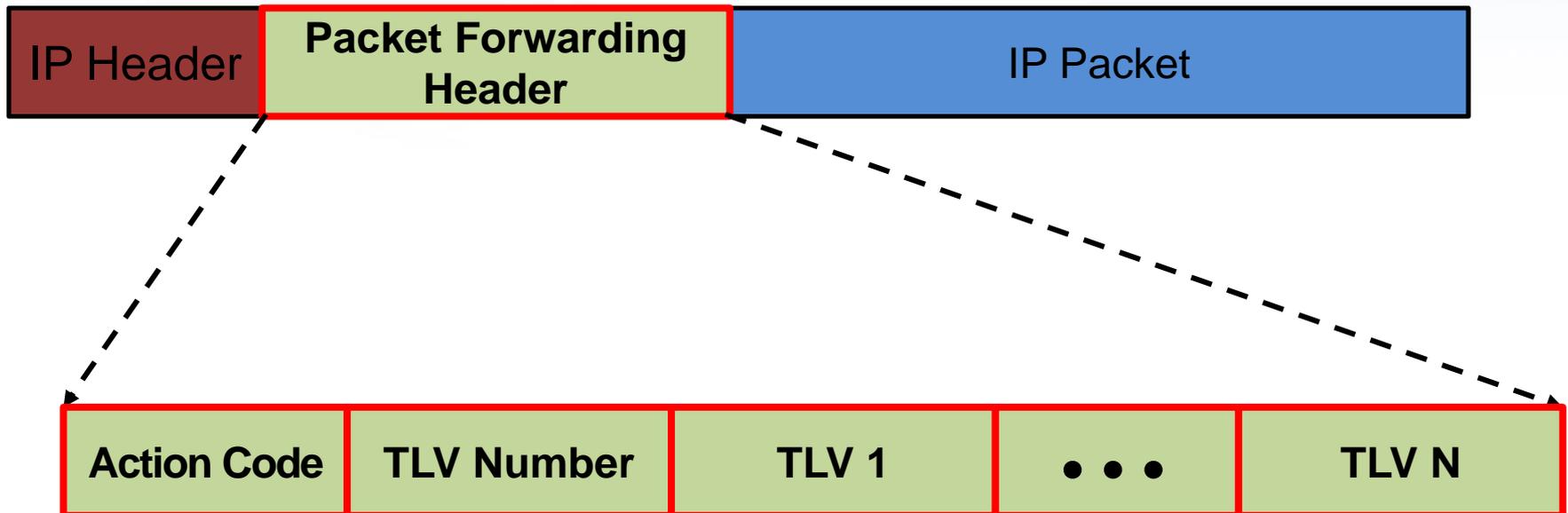
Packet Forwarding Header (1)

- **Packet Forwarding Header** is used to forward a packet from one NSF to another for further inspection.

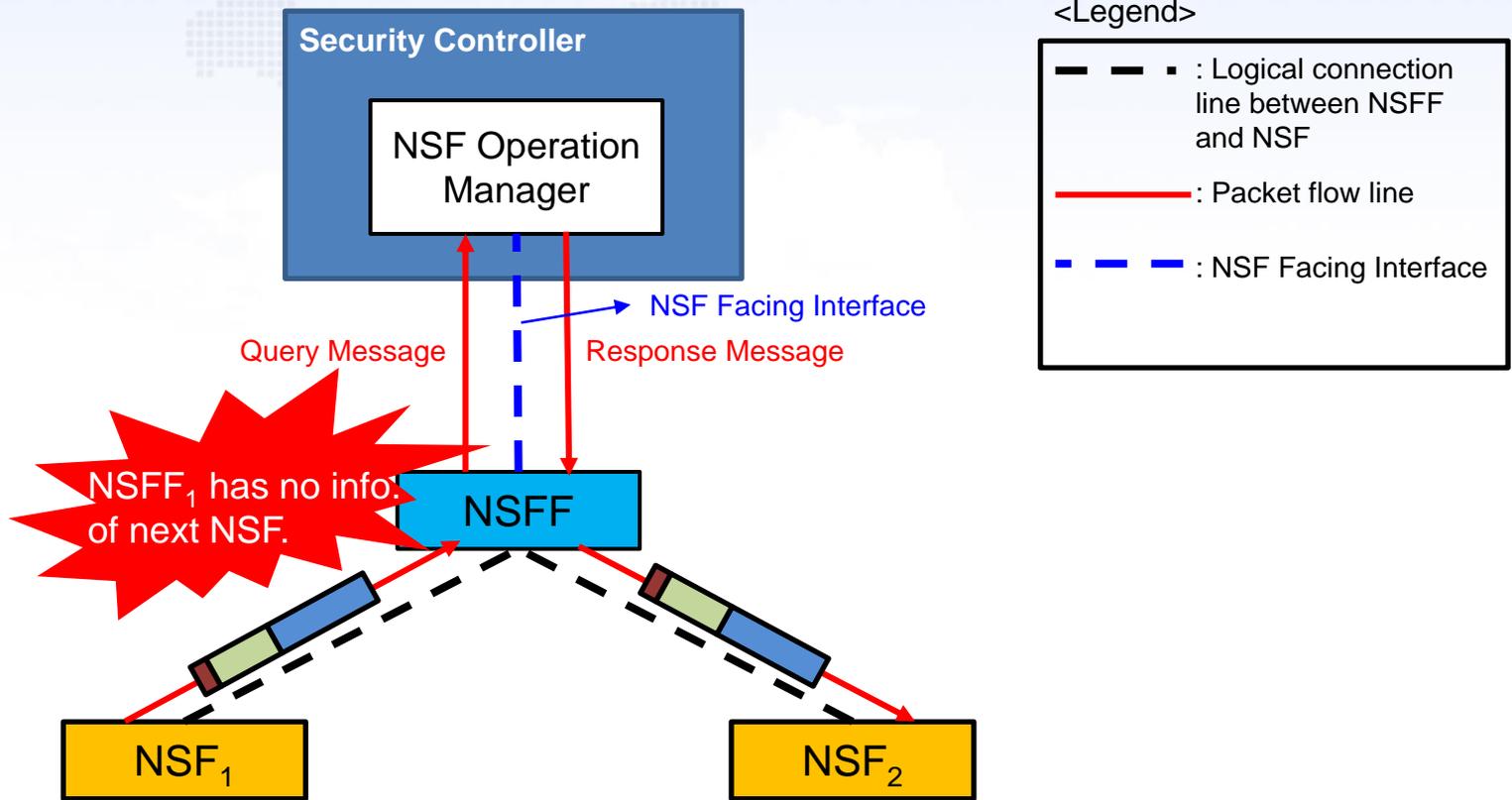


Packet Forwarding Header (2)

- **Packet Forwarding Header** is inserted between IP Header and IP Payload.



NSF Forwarding Information (1)



NSF Forwarding Information (2)

- The **NSF Forwarding Information** consists of IPv4 address, IPv6 address, supported transport protocols, and location information.

