A Service-Inferred, Deterministic Traffic Forwarding Scheme

C. Jacquenet
christian.jacquenet@orange.com

Conseil Scientifique AFNIC – 9 juillet 2013

Outline

- New challenges
- Basic issue and typical use case
- Introducing Network Located Function Chaining (NLFC)
- NLFC operation
- Pending questions

Challenges

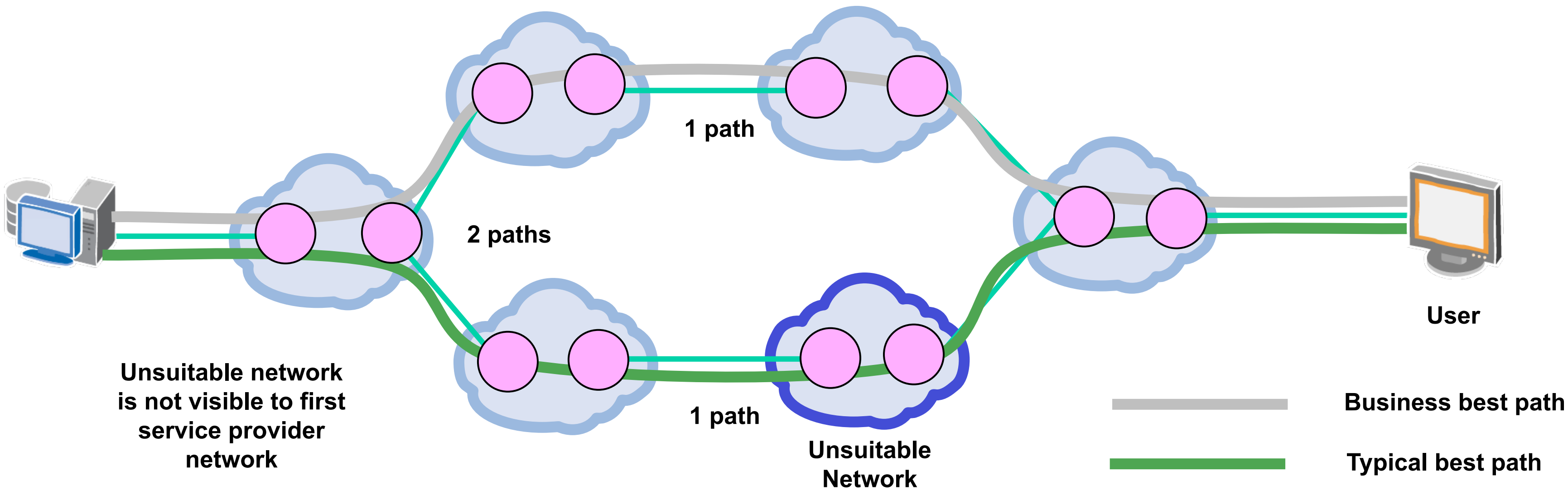
- Network service design and operation now assume the combined and sometimes ordered activation of elementary capabilities
  - Forwarding and routing, firewall, QoS, DPI, *etc*.
  - Function chaining may be conditioned by traffic directionality
- These Network-Located Functions (NLF) may be activated on the same I/F or network segment
  - *E.g.*, the (s)Gi I/F of mobile networks
- Inferred complexity suggests robust mastering of chained NLF activation
  - For the sake of optimized service delivery and efficient forwarding scheme

Core Issue

- IP network operation now assumes the complex chaining of various elementary capabilities
  - Besides basic routing and forwarding functions
- How to efficiently forward traffic entering a network that supports these functions?
  - Differentiation is ensured by tweaking the set of network functions to be invoked
- Packet processing decisions become service-inferred and policy-derived

Business-Driven Forwarding Use Case

- Best path is now computed and selected based upon network service orchestration
  - May differ from typical hop-by-hop path computation and forwarding schemes



NLFC Objectives

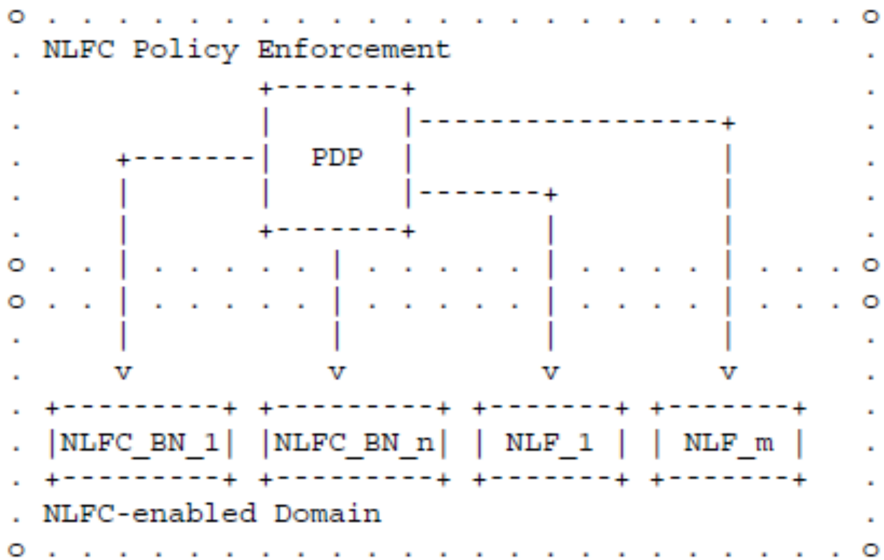
- Compute and establish service-inferred data paths
  - For the sake of optimized traffic flow forwarding
- Master NLF chaining regardless of the underlying topology and routing policies
  - Yielding a NLF-based differentiated forwarding paradigm
- Facilitate NLF operation while avoiding any major topology upgrade
  - Adapt chronology of NLF activation according to the required service and associated parameters
- Contribute to the automation of dynamic resource allocation and policy enforcement procedures

Rationale

- Dynamic NLF provisioning is separated from packet processing
- NLF functions are seen as black boxes
- NLF chaining varies as a function of the service and the traffic directionality
  - Chaining is described by an information processed by devices that participate to the delivery of a given service
  - Such information is signaled by the packets themselves

NLFC Environment

- Policy Decision Point (PDP) *makes* decisions according to policies documented in NLFC Policy Tables
  - PDP decisions are applied by NLF (boundary) nodes which process traffic accordingly



The Intelligence Resides In The PDP

- PDP-maintained NLFC Policy Tables describe the NLF-specific policy to be enforced
- NLF nodes are provisioned with:
  – Local NLF Identifier(s) so that the node can position itself in the NLFC Map
  – NLFC Maps and Locators
- Boundary nodes are also provisioned with Classification Rules
  – A Rule is bound to one NLFC Map
  – (Packet) Classifier relies upon various packet header fields (DA, SA, DS, *etc.*)

NLFC Processing

- Assign NLF Identifiers
  - NLF functions are listed and identified in a repository maintained by the NLFC administrative entity (ISP)
    - Identifier is a case-sensitive string
- Assign NLF Locators
  - Meant to locate a NLF which can be supported by several devices
    - Locator is typically an IP address (could be a FQDN)
    - One or multiple Locators can be configured for each NLF
- Build NLFC Maps
  - Detail the list of NLFs to be invoked in a specific order
  - Maps are identified by an Index and are specific to traffic directionality

NLF Node Operation

- Check whether the incoming packet conveys a NLFC Map Index
  – If not, proceed with typical forwarding rules
- If so, packet is subject to NLFC according to:
  – The NLFC Map
  – The number of NLF functions supported by the node
- If node is not the last in the Map, node forwards packet to the next NLF node as described in the Map
  – Proceeds with typical forwarding rules otherwise

Example

- A node supports NLF function a
  - Function a must be invoked only for packets matching Rules 1 and 3, as per NLFC Maps
  - Next NLF functions to be invoked for such packets are c (Map Index 1) and h (Map Index 3), respectively

```
+-----------------------------------------------+
|              NLFC Policy Table                |
+-----------------------------------------------+
|Local NLF Identifier: NLFa                     |
+-----------------------------------------------+
|Classification Rules                           |
| Rule 1: If DEST=IP1; then NLFC_MAP_INDEX1     |
| Rule 2: If DEST=IP2; then NLFC_MAP_INDEX2     |
| Rule 3: IF DEST=IP3; then NLFC_MAP_INDEX3     |
+-----------------------------------------------+
|NLFC Maps                                      |
| {NLFC_MAP_INDEX1, {NLFa, NLFc}                |
| {NLFC_MAP_INDEX2, {NLFd, NLFb}                |
| {NLFC_MAP_INDEX3, {NLFa, NLFh}                |
+-----------------------------------------------+
```

At NLFC Domain Boundaries

- Ingress Node
  - Strips any existing NLFC Map Index
  - Checks whether received packet matches any existing classification rule
    - If not, proceed with typical forwarding rules
  - If so, retrieves the locator of the first NLF as per the corresponding Map entry
    - If next NLF node is not the next hop, packet is encapsulated (*e.g.*, GRE) and forwarded to next NLF node
- Egress Node
  - Strips any existing NLFC Map Index
  - Proceeds with typical forwarding rules

Pending Questions

- NLC Map Index encoding
  - 8-bit is probably enough, 16-bit is comfortable
- Where to store NLFC Map Index?
  - DS field, Flow Label, new IPv6 extension header, new IP option, L2 field, TCP option, define a new shim, *etc*.
- NLFC forwarding suggests encapsulation
  - When next NLF node is not the next hop as per IGP/BGP machinery
  - GRE, IP-in-IP, LISP, *etc*., are candidate options
- Security issues at NLFC domain boundaries
  - Means to protect against DDoS or illegitimate invocation of resources must be supported

Reading Material

- Problem statement
  - http://tools.ietf.org/html/draft-quinn-nsc-problem-statement-00
- Global framework
  - http://tools.ietf.org/html/draft-boucadair-network-function-chaining-01
- Network Service Header (as a means to encapsulate information that describes a service path)
  - http://tools.ietf.org/html/draft-quinn-nsh-00

Thank You!