

Network Working Group
Internet-Draft
Intended status: Informational
Expires: February 16, 2014

M. Boucadair
C. Jacquenet
France Telecom
R. Parker
Affirmed Networks
August 15, 2013

Requirements for Network Function Chaining draft-boucadair-chaining-requirements-00

Abstract

This document identifies the requirements for the Network Function Chaining. This effort is a companion document to the Network Chaining Framework defined in [\[I-D.boucadair-network-function-chaining\]](#).

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 16, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	2
3.	Detailed Requirements List	2
4.	Deployment-specific Requirements	6
5.	IANA Considerations	7
6.	Security Considerations	7
7.	Acknowledgements	7
8.	References	7
8.1.	Normative References	7
8.2.	Informative References	7
	Authors' Addresses	7

[1.](#) Introduction

This document identifies the requirements for the Network Function Chaining. This document is a companion document to the Network Chaining Framework defined in [[I-D.boucadair-network-function-chaining](#)].

The overall problem space is described in [[I-D.quinn-nsc-problem-statement](#)].

[2.](#) Terminology

The reader should be familiar with the terms defined in [[I-D.boucadair-network-function-chaining](#)].

[3.](#) Detailed Requirements List

The following set of functional requirements should be considered for the design of the Network Function Chaining mechanism:

- REQ#1: The solution MUST NOT make any assumption on whether Network Functions are deployed directly on physical hardware, as one or more Virtual Machines, or any combination thereof.
- REQ#2: The solution MUST NOT make any assumption on whether Network Functions each reside on a separate addressable Network

Element, are co-resident on a single addressable Network Element, or any combination thereof.

REQ#3: The solution MUST NOT require any IANA registry to store the list of Network Functions.

REQ#4: The solution MUST NOT assume predefined chains of particular Network Functions. In particular, the solution MUST NOT require any IANA registry to store typical network function chain logics.

REQ#5: The solution MUST allow a Network Function to be embedded in multiple devices (e.g., servers).

a. This is used for load-balancing, load-sharing, prevent from failures (e.g., hot or cold standby protection mechanism), accommodate planned maintenance operations, etc.

b. How these multiple devices are involved in the service delivery is deployment-specific.

REQ#6: The solution MUST allow for multiple chaining logics to be simultaneously enforced within an administrative domain.

REQ#7: The solution MUST support multiple NFC-enabled domains be deployed within the same administrative domain.

REQ#8: The solution MUST NOT make any assumption on how the traffic is to be bound to a given chaining policy. In other words, classification rules are deployment-specific and policy-based.

REQ#9: The solution MUST be able to dynamically enforce Network Function chains. In particular, the solution MUST allow the update or the withdrawal of existing chains, the definition of a new chain, the addition of new Network Functions without having any impact on existing Network Functions.

REQ#10: Network Function Chaining logic and related policies SHOULD NOT be exposed outside a given administrative domain.

REQ#11: The solution SHOULD minimize fragmentation; in particular a minimal set of NFC-specific information should be conveyed in the packet.

REQ#12: The solution MUST NOT make any assumption on how RIB and FIBs are populated.

REQ#13: The solution MUST NOT make any assumption on the underlying transport technologies used to interconnect involved Network Functions.

- a. In particular, the solution can be used whatever the switching technologies deployed in the underlying transport infrastructure.
- b. Techniques such as MPLS are neither required nor excluded.

REQ#14: The solution MUST allow for chaining logics where involved Network Functions are not within the same layer 3 subnet.

REQ#15: The solution MUST NOT exclude Network Functions to be within the same IP subnet (this is deployment-specific). An administrative entity, grouping its Network Functions within the same IP subnet, SHOULD be able to get rid of any overhead (e.g., encapsulation).

REQ#16: The solution MAY allow (but doesn't require) reclassification at the Network Functions (i.e., a Network Function can also be a classifier).

- a. Given the risk to jeopardize the overall consistency of the Differentiated Forwarding policy enforced for a specific traffic flow or a set thereof, the administrative entity must configure coherent classification rules.
- b. The configuration of classification rules in such context are the responsibility of the administrative entity managing that NFC-enabled domain.

REQ#17: The solution MUST support the ability to invoke differentiated sets of policies for a Network Functions (called Profiles). A profile denotes a set of policies configured to a local Network Function (e.g., content-filter-child, content-filter-adult).

- a. Few profiles should be assumed per Network Function to accommodate the need for scalable solutions.
- b. Finer-grained definition of policies belonging to a Network Function should not be driven by the chaining marking.

- c. Finer-grained of policies should be configured directly to each Network Function; no need to overload the design of Network Function chains with policies of low-level granularity.

REQ#18: The solution MUST provide means to ensure the overall consistency of the procedure. For example:

- a. Ensure the completion of the forwarding actions derived from the contents of the NFC Map until the border node is reached.
- b. Coherent classification rules are installed to all classifiers.
- c. The correlation between the classification policies and forwarding actions should be verified.

REQ#19: The solution MUST prevent the same Network Function to be invoked several times in the context of the same chain (at the risk of generating Network Function Loop).

REQ#20: The solution MUST allow for load-balancing:

- a. Load-balancing may be provided by legacy technologies or protocols (e.g., make use of load-balancers)
- b. Load-balancing may be part of the Network Function itself.
- c. Load-balancer may be considered as a Network Function element.
- d. Because of the possible complications, load balancing SHOULD NOT be handled at the classifier. This logic should be embedded in the entity which is responsible for ensuring the overall consistency of the solution (i.e., Policy Decision Point).

REQ#21: The solution MUST separate provisioning-related aspects from the actual handling of packets (including forwarding decisions).

REQ#22: The solution MUST NOT exclude means to detect the liveliness of involved Network Functions; nevertheless these means are not considered as a mandatory component of the solution.

- REQ#23: Means to dynamically discover Network Functions SHOULD be supported. This feature is not required for the core chaining functionality, but its support is of high interest for operators.
- REQ#24: A Classifier MAY be co-located with other Network Functions.
- REQ#25: The solution MUST NOT require every Network Function be co-located with a Classifier; this is a deployment-specific decision.
- REQ#26: A Classifier MAY be considered as a Network Function in its own.
- REQ#27: The identification of instantiated Network Function chains is local to each administrative domain; it is policy-based and deployment-specific.
- REQ#28: Network Functions may be reachable using IPv4 and/or IPv6. The administrative domain entity MUST be able to define and enforce policies with regards to the address family to be used when invoking a Network Function.
- a. A Network Function Chain may be composed of IPv4 addresses, IPv6 addresses, or a mix of both IPv4 and IPv6 addresses.
 - b. Multiple Network Functions can be reachable using the same IP address.
- REQ#29: The solution MUST allow for gradual deployment in legacy infrastructures, and therefore coexist with legacy technologies that cannot support NFC-specific capabilities, such as NFC Map interpretation and processing.
- REQ#30: The solution MUST be able to work in a domain that may be partly composed of opaque elements, i.e., elements that do not support NFC-specific capabilities.

4. Deployment-specific Requirements

The following deployment considerations should be taken into account:

- o Avoid inducing severe path stretch compared to the path followed if no Network Function is involved.

- o Minimize path computation delays: due to the enforcement of classification rules in all participating nodes, misconception of Network Function chaining, inappropriate choice of nodes elected to embed network-located functions, etc., must be avoided.
- o Avoid Network Function invocation loops: the design of Network Function chaining should minimize as much as possible Network Function invocation loops. Note that means to prevent Network Function loops may be enabled in each Network Function Node.

5. IANA Considerations

This document does not require any action from IANA.

6. Security Considerations

Security considerations related to network function chaining are discussed in [[I-D.boucadair-network-function-chaining](#)].

7. Acknowledgements

TBC.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

8.2. Informative References

[I-D.boucadair-network-function-chaining]
Boucadair, M., Jacquenet, C., Parker, R., Lopez, D., Yegani, P., Guichard, J., and P. Quinn, "Differentiated Network-Located Function Chaining Framework", [draft-boucadair-network-function-chaining-02](#) (work in progress), July 2013.

[I-D.quinn-nsc-problem-statement]
Quinn, P., Guichard, J., Surendra, S., Agarwal, P., Manur, R., Chauhan, A., Leymann, N., Boucadair, M., Jacquenet, C., Smith, M., Yadav, N., Nadeau, T., Gray, K., and B. McConnell, "Network Service Chaining Problem Statement", [draft-quinn-nsc-problem-statement-02](#) (work in progress), July 2013.

Authors' Addresses

Mohamed Boucadair
France Telecom
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Christian Jacquenet
France Telecom
Rennes 35000
France

Email: christian.jacquenet@orange.com

Ron Parker
Affirmed Networks
Acton, MA
USA

Email: Ron_Parker@affirmednetworks.com

