

RTGWG
Internet-Draft
Intended status: Informational
Expires: 27 October 2022

D. King
Lancaster University
A. Farrel
Old Dog Consulting
C. Jacquenet
Orange
25 April 2022

Challenges for the Internet Routing Systems Introduced by Semantic
Routing
draft-king-irtf-challenges-in-routing-08

Abstract

Historically, the meaning of an IP address has been to identify an interface on a network device. Routing protocols were developed based on the assumption that a destination address had this semantic.

Over time, routing decisions have been enhanced to determine paths on which packets could be forwarded according to additional information carried principally within the packet headers, and dependent on policy coded in, configured at, or signaled to the routers.

Many proposals have been made to add semantics to IP packets by placing additional information into existing fields, by adding semantics to IP addresses, or by adding fields to the packets. The intent is always to facilitate routing decisions based on these additional semantics in order to provide differentiated paths to enable forwarding of different packet flows on paths that may be distinct from those derived by shortest path first or path vector routing. We call this approach "Semantic Routing".

This document describes the challenges to the existing routing system that are introduced by Semantic Routing. It then summarizes the opportunities for research into new or modified routing and forwarding approaches that make use of additional semantics.

This document is presented as a study to support further research into clarifying and understanding the issues. It does not pass comment on the advisability or practicality of any of the proposals and does not define any technical solutions.

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 <https://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 27 October 2022.

Copyright Notice

Copyright (c) 2022 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 (<https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
2. Current Challenges to IP Routing	4
3. What is Semantic Routing?	7
3.1. Architectural Considerations	9
4. Challenges for Internet Routing Research	10
4.1. Research Principles	10
4.2. Routing Research Questions to be Addressed	11
5. Security and Privacy Considerations	15
6. IANA Considerations	16
7. Acknowledgements	16
8. Contributors	16
9. Informative References	16
Authors' Addresses	17

1. Introduction

Historically, the meaning of an IP address has been to identify an interface on a network device. Routing protocols were to compute, establish, and maintain paths through networks toward destination prefixes until IP packets eventually reach their destination, and were based on the assumption that a destination address had this semantic. Anycast and multicast addresses were also defined, and those address semantics sometimes required variations to the routing protocols or even encouraged the development of new protocols.

Over time, the mechanisms that enabled routing decisions were enhanced to determine paths on which packets could be forwarded according to additional information carried principally within the packets headers or within 'shim' headers, and dependent on policy coded in, configured at, or signaled to the routers. Perhaps one of the most iconic examples is Equal-Cost Multipath (ECMP) where a router makes a choice about how to forward a packet over a number of parallel links or paths based on the values of a set of fields in the packet header.

Many proposals have been made to add semantics to IP packets by placing additional information into existing fields, by adding semantics to IP addresses, or by adding fields to the packets. The intent is always to facilitate routing decisions based on these additional semantics in order to provide differentiated paths to enable forwarding of different packet flows on paths that may be distinct from those derived by shortest path first or path vector routing. We call this approach "Semantic Routing"
[I-D.farrel-irtf-introduction-to-semantic-routing].

There are many approaches to adding semantics to packet headers: the additional information may be derived from the destination addresses, from other fields in the packet header, or the packet itself. Mechanisms for using the destination address range from assigning an address prefix to have a special purpose and meaning (such as is done for multicast addressing) through allowing the owner of a prefix to use the low-order bits of an address for specific purposes (e.g., to provide an indication of the nature of the service that is associated with these packets). Some proposals suggest variable address lengths, others offer new hierarchical address formats, and some introduce a structure to addresses so that they can carry additional information in a common way. Alternatively, forwarding decisions can be performed based on fields in the packet header (such as the IPv6 Flow Label, or the Traffic Class field), overloading of existing packet fields, or new fields added to the packet headers.

A survey of ways in which routing and forwarding decisions have been made based on additional information carried in packets can be found in [I-D.king-irtf-semantic-routing-survey].

Some Semantic Routing proposals are intended to be deployed in administratively scoped IP domains whose network components (routers, switches, etc.) are operated by a single administrative entity (sometimes referred to as 'limited domains' [RFC8799]), while other proposals are intended for use across the Internet. The impact the proposals have on routing systems may require clean-slate solutions, hybrid solutions, extensions to existing routing protocols, or potentially no changes at all.

This document describes some of the key challenges to the routing system that are already present in today's IP networks. It then briefly outlines the concept of "Semantic Routing" with reference to [I-D.farrel-irtf-introduction-to-semantic-routing] and presents some of the additional challenges to the existing routing system that Semantic Routing may introduce. Finally, this document presents a list of research questions that offer opportunities for future research into new or modified routing protocols and forwarding systems that make use of Semantic Routing.

In this document, the focus is on routing and forwarding at the IP layer. A variety of overlay mechanisms exists to perform service or path routing at higher layers, and those approaches may be based on similar extensions to packet semantics, but that is out of scope for this document. Similarly, it is possible that Semantic Routing can be applied in a number of underlay network technologies, and that, too, is out of scope for this document.

This document is presented as a study to support further research into clarifying and understanding the issues. It does not pass comment on the advisability or practicality of any of the proposals and does not define any technical solutions.

2. Current Challenges to IP Routing

Today's IP routing faces several significant challenges which are a consequence of architectural design decisions and the continued exponential growth in traffic. These challenges include mobility, multihoming, programmable paths, scalability, and security, and were not the focus of the original design of the Internet. Nevertheless, IP networks have, in general, coped well in an incremental manner whenever a new challenge has arisen. The following list is presented to give context to the continuing requirements that routing protocols must meet as new semantics are applied to the routing process.

- * Mobility - Mobility introduces several challenges, including maintaining a relationship between a sender and a receiver in cases where the sender or receiver changes their point of network attachment. The network must always be informed about the mobile node's current location, to allow continuity of services. Mobile users may also consume network resources, while in motion. The mobile user's service instances and attachments will also change due to varying load or latency, e.g., in Multi-access Edge Computing (MEC) environments.
- * Multihoming - Multihomed stations or multihomed networks are connected to the Internet via more than one access circuit or access network and, therefore, may be assigned multiple IP addresses or prefixes from different pools. There are challenges concerning how traffic is forwarded back to the source if the source has originated its traffic using the wrong source address for a particular connection, or if one of the connections to the Internet is degraded.
- * Multi-path - The Internet was initially designed to find the single, "best" path to a destination using a distributed routing algorithm. Current IP network topologies can provide multiple paths to reach a destination, each with different characteristics and with different failure likelihoods. It may be beneficial to send traffic over multiple paths to achieve reliability and enhance throughput, and it may be desirable to select one path or another because of QoS or security considerations for example, or to avoid transiting specific areas of an IP network, based (for example) on the reputation of transit provider for example. However, how packets are forwarded by using the shortest path means that distinguishing these alternate paths and directing traffic to them can be hard. Further, problems concerning scalability, commercial agreements among Service Providers, and the design of BGP make the utilization of multi-path techniques difficult for inter-domain routing. (Note that this discussion is distinct from Equal Cost Multi-path (ECMP) where packets are directed onto several "parallel" paths of identical least cost using a hash algorithm operated on some of the packets' header fields.)
- * Multicast - Delivering the same packet to multiple destinations can place considerable load on a network. Solutions that replicate the packet at the source or at the network edge may obviously cause multiple copies of the packet to flow along the same network links. Solutions that move deterministic replication into the network to make more optimal use of the network resources can be complex to set up and manage since multicast network designs often assume dynamic tree computation where the multicast

distribution tree can be rooted at the source or in the multicast network, thereby leading to specific routing tables whose entries denote the tree structure. More complicated hardware that can replicate packets may also be required within the network. In order that packets can be addressed to a group of destinations and not be forwarded by means of unicast transmission, parts of the addressing space (that is, address prefixes) have been reserved for multicast addressing.

- * Programmable Paths - The ability to decouple IP paths from routing protocols and agreements between Service Providers could allow users and applications to select network paths themselves, based on the required path characteristics. Another option is to let the route computation logic select, establish, and maintain paths on behalf of the user or the application and as a function of their requirements so that Service Providers can participate in the route computation "service". Currently, user and application packets follow the path selected by routing protocols and the way traffic is forwarded through a network is under the control of the Service Provider that operates the said network. The corresponding traffic forwarding policies enforced by the service provider usually comply with the requirements expressed by the user or the application. These requirements may have triggered a dynamic service parameter negotiation cycle that eventually leads to proper (network, CPU, storage) resource allocation.
- * Endpoint Selection - As compute resources and content storage move closer to the edge of the network, there are often multiple points in the network that can satisfy user requests. In order to make the best use of these distributed resources and so as to not overload parts of the network, user traffic needs to be steered to appropriate servers or data centres. In many cases, this function may be achieved in the application layer (such as through DNS [RFC3467]) or in the transport layer (such as using ALTO [RFC5693]). The challenge is to balance higher-layer decisions about which application layer resources to use with information from the lower layers about the availability and load of network resources.
- * Scalability - There are many scaling concerns that pose critical challenges to the Internet. Not least among these challenges is the size of the routing tables that routers in an IP network must maintain. As the number of devices attached to the network grows, so the number of addresses in use also grows, and because of the schemes used to assign address prefixes, the mobility of devices, and the various connectivity options between networks, the routing table sizes also grow, even more so when prefixes are not always amenable to aggregation. This problem is exacerbated by some

services (such as those supported by the IoT where several thousands of objects/sensors may be networked), where, as more devices are added to the network, the size of the routing table may affect the operation of certain routing protocols. It may be noted that scaling issues are also exacerbated by multihoming practices if a host that is multihomed is allocated a different address for each point of attachment.

- * Manageability, Maintainability, and Extensibility - Operational manageability is a key requirement for network technologies: network operators must be able to determine the status of their network and understand the causes of any disruptions or problems. Further, it must be possible to maintain the networks and the technologies running in them without disrupting the services being delivered by the networks. Additionally, the network technologies developed and deployed need to be extensible so that new features can be added and new services supported without the need to invent whole new technologies.
- * Security - Issues of security and privacy have been largely overlooked by the routing systems. However, there is increasing concern that attacks on routing systems can not only be disruptive (for example, causing traffic to be dropped), but may cause traffic to be redirected to inspection points that can breach the security or privacy of the payloads.

Some of the challenges outlined here were previously considered within the IETF by the IAB's "Routing and Addressing Workshop" held in Amsterdam, The Netherlands on October 18-19, 2006 [RFC4984]. Several architectures and protocols have since been developed and worked on within and outside the IETF, and these are examined in [I-D.king-irtf-semantic-routing-survey].

3. What is Semantic Routing?

Semantic Routing is the term applied to routing in an IP network that relies upon additional information to feed the route computation process, to enhance route selection decisions, and to direct the forwarding process. In addition to the routable part of the destination IP address (the prefix), such information may be present in other fields in the packet (chiefly the packet header) and configured or programmed into the routers/forwarders. Semantic Routing includes mechanisms such as "Preferential Routing", "Policy-based Routing", and "Flow steering".

In Semantic Routing, a packet forwarding engine may examine a variety of fields in a packet and match them against forwarding instructions. Those forwarding instructions may be installed by routing protocols,

configured through management protocols or a software defined networking (SDN) controller, or derived by a software component on the router that considers network conditions and traffic loads. The packet fields concerned may be the fields of an IP header, those same fields but with additional semantics, elements of the packet payload, or new fields defined for inclusion in the packet header or as a "shim" between the header and payload. In the case of additional semantics included in existing packet header fields, the approach implies some "overloading" of those fields to include meaning beyond the original definition. In all cases, a well-known definition of the encoding of the additional information is required to enable consistent interpretation within the network.

A more detailed description of Semantic routing can be found in [I-D.farrel-irtf-introduction-to-semantic-routing] and a survey of Semantic Routing proposals and research projects can be found in [I-D.king-irtf-semantic-routing-survey].

Many technical challenges exist for Semantic Routing in IP networks depending on which approach is taken. These challenges include (but are not limited to):

- * The continual growth of routing tables.
- * Convergence times for large networks.
- * Granularity of routing decisions.
- * Address consumption caused by lower address utility rate. The wastage mainly comes from aligning finite allocation for semantic address blocks.
- * Encoding too many semantics into prefixes will require evaluation of which to prioritize.
- * Risk of privacy/information leakage.
- * Lack of visibility of the Semantic Routing information when end-to-end or edge-to-edge encryption is used.
- * Burdening the user, application, or prefix assignment node.
- * Source address spoofing prevention mechanisms are required.
- * Overloading of routing protocols causing stability and scaling problems.

- * Depending on encoding mechanisms, there may be challenges for data planes to scale the processes of finding, reading, and looking up semantic data in order to forward packets at line speed.
- * Backwards compatibility with existing IP networking and routing protocols.
- * Extensibility to support additional functions in the future.
- * Manageability and network diagnostics to be able to determine how the network is functioning and to isolate the causes of any problems.

3.1. Architectural Considerations

Semantic data may be taken into account to integrate with existing routing architectures. An overlay can be built such that Semantic Routing is used to forward traffic between nodes in the overlay, but regular IP is used in the underlay. The application of semantics may also be constrained to within a limited domain. In some cases, such a domain will use IP, but be disconnected from the Internet. In other cases, traffic from within the domain is exchanged with other domains that are connected together across an IP network using tunnels or via application gateways. And in still another case traffic from the domain is forwarded across the Internet to other nodes and this requires backward-compatible routing approaches.

Isolated Domains: Some IP network domains are entirely isolated from the Internet and other IP networks. In these cases, packets cannot "escape" from the isolated domain into external networks and so the Semantic Routing schemes applied within the domain can have no detrimental effects on external domains. Thus, the challenges are limited to enabling the desired function within the domain.

Bridged Domains: In some deployments, it will be desirable to connect together multiple isolated domains to build a larger network. These domains may be connected (or bridged) over an IP network or even over the Internet, possibly using tunnels. An alternative to tunneling is achieved using gateway functionality where packets from a domain are mapped at the domain boundary to produce regular IP packets that are sent across the IP network.

Semantic Prefix Domains: A semantic prefix domain is a portion of the Internet over which a consistent set of semantic-based policies are administered in a coordinated fashion. This is achieved by assigning a routable address prefix (or a set of prefixes) for use with Semantic Routing so that packets may be

forwarded through the regular IP network (or the Internet). Once delivered to the semantic prefix domain, a packet can be subjected to whatever Semantic Routing is enabled in the domain.

Further discussion of architectures for Semantic Routing can be found in [I-D.farrel-irtf-introduction-to-semantic-routing].

4. Challenges for Internet Routing Research

It may not be possible to embrace all emerging scenarios with a single approach or solution. Requirements such as 5G mobility, near-space-networking, and networking for outer-space (inter-planetary networking), may need to be handled using different network technologies. Improving IP network capabilities and capacity to scale, and address a set of growing requirements presents significant research challenges, and will require contributions from the networking research community. Solutions need to be both economically feasible and have the support of the networking equipment vendors as well as the network operators.

4.1. Research Principles

Research into Semantic Routing should be founded on regular scientific research principles [royalsoc]. Given the importance of the Internet today, it is critical that research is targeted, rigorous, and reproducible.

The most valuable research will go beyond an initial hypothesis, a report of the work done, and the results observed. Although that is a required foundation, networking research needs to be independently reproducible so that claims can be verified or falsified. Further, the networks on which the research is carried out need to both reflect the characteristics that are being explicitly tested, and reproduce the variety of real networks that constitute the Internet.

Thus, when conducting experiments and research to address the questions in Section 4.2, attention should be given to how the work is documented and how meaningful the test environment is, with a strong emphasis on making it possible for others to reproduce and validate the work.

4.2. Routing Research Questions to be Addressed

As research into the scenarios and possible uses of Semantic Routing progresses, a number of questions need to be answered. These questions go beyond "Why do we need this function?" and "What could we achieve by carrying additional semantics in an IP address?" The questions are also distinct from issues of how the additional semantics can be encoded within an IP address. All of those issues are, of course, important considerations in the debate about Semantic Routing, but they form only part of the essential groundwork of research into Semantic Routing itself.

This section sets out some of the concerns about how the wider the use of Semantic Routing might impact a routing system. These questions need to be answered in separate research work or folded into the discussion of each Semantic Routing proposal.

1. What is the scope of the Semantic Routing proposal? This question may lead to various answers:

Global: It is intended to apply to all uses of IP.

Backbone: It is intended to apply to IP network connectivity.

Overlay: It is to be used as an overlay network using tunneling over IP or other underlay technologies.

Gateway: The Semantic Routing will be used within a specific domain, and communications with the wider Internet will be handled by IP and probably application gateways.

Domain: The use of the Semantic Routing is strictly limited to within a domain or private network.

Underlying this question is a broader question about the boundaries of the use of IP, and the limit of "the Internet". If a limited domain is used, is it a semantic prefix domain [RFC8799] where a part of the IP address space identifies the domain so that an address is routable to the domain, but the additional semantics are used only within the domain, or is the address used exclusively within the domain so that the external impact of the routability of the address and the additional semantics is not important?

2. What will be the impact on existing routing systems? What would happen if a packet carrying additional semantics was subjected to normal routing operations? How would the existing routing systems react if such a packet escaped (accidentally or

maliciously) from the planned scope of the proposal? For example: how are the semantic parts of an address distinguished from the routable parts (if, indeed, they are separable)?; is there an impact on the size and maintenance of routing tables due to the addition of semantics?; how are cryptographically generated addresses (such as [RFC3972]) made routable and kept simple enough for management?.

3. What path characteristics are needed to describe the desired paths and as input to route computation? Since one of the implications of adding semantics to IP packets is to cause special processing by routers, it is important to understand what behaviors are wanted. Such path characteristics include (but are not limited to):

Quality: Expressed in terms of throughput, latency, jitter, drop precedence, etc.

Resilience: Expressed in terms of survival of network failures and delivery guarantees.

Destination: How is a destination address to be interpreted if it encodes a choice of actual destinations? Can traffic be forwarded over multiple distinct paths if multiple destination addresses are encoded?

Security: What choices of path reduce the vulnerability of the traffic to security or privacy attacks?

In these cases, how do the routers utilize the additional semantics to determine the desired characteristics? Or are such characteristics used to feed the route computation logic, for example, by means of metrics? What additional information about the network do the routing protocols need to gather? What changes to the routing algorithm are needed to deliver packets according to the desired characteristics? How can routes be computed with characteristics that accommodate traffic patterns, requirements, and constraints?

4. Can we solve these routing challenges with existing routing tools and methods? We can break this question into a set of more detailed questions.

- * Is new hardware needed? Existing deployed hardware has certain assumptions about how forwarding is carried out based on IP addresses and routing tables. But hardware is increasingly programmable so that it may be possible to instruct the forwarding components to act on a variety of elements of the packets.
- * Do we need new routing protocols? We might ask some subsidiary questions:
 - Can we make do with existing protocols, possibly by tuning configuration parameters or using them out of the box?
 - Can we make backwards-compatible modifications to existing protocols such that they work equally for today's IP addresses or addresses with extra semantics?
 - Do we need entirely new protocols or radical evolutions of existing protocols in order to enforce advanced Semantic Routing policies?
 - Should we focus on the benefits of routing solutions that are optimized for specific environments (network topologies, technologies, use cases), or should we attempt to generalize to enable wider applicability?
- 5. Do we need new management tools and techniques? How practical is it to debug and operate the routing system? Management of the routing system (especially diagnostic management) is a crucial and often neglected part of the problem space. A critical part of this issue is how packets within the network can be inspected by diagnostic tools (or human operators) and mapped to the routing and forwarding decisions that were made within the network in order to understand the actions made at and by upstream routers.
- 6. What is the impact of Semantic Routing on the security of the routing system?
 - * Does the introduction of Semantic Routing provide a greater attack surface?
 - * Can Semantic Routing provide greater opportunities for security by fine-grain forwarding of flows to be inspected by different security functions?

- * Can Semantic Routing improve security and privacy by obscuring information in the packets, or does the inclusion of additional information risk compromising security and privacy?
 - * To what extent does deployment within a limited domain strengthen security or make it less of a concern?
 - * Does the use of Semantic Routing make it easier or harder to impose censorship, prohibit access to the Internet by specific parties, or block access to certain resources or types of service?
7. What is the scalability impact of Semantic Routing on routing systems? Scalability can be measured as:
- * Routing table size. How many entries need to be maintained in the routing tables by different routers serving different roles in the network? Some approaches to Semantic Routing may be explicitly intended to address this problem.
 - * Forwarding table size. The size of the forwarding table may be less of an issue considering modern hardware, however the more granular the routing/forwarding decisions made in a router, the greater the size of this table. The size of the forwarding table has implications for memory in the forwarding engine, but also for the lookup time for forwarding each packet.
 - * Routing performance. Routing performance may be considered in terms of the volume of data that has to be exchanged both to construct and maintain the routing tables at the participating routers. It may also be measured in terms of how much processing is required to compute new routes when there is a change in the network.
 - * Routing convergence. This is the time that it takes for a routing protocol to discover changes (especially faults) in the network, to distribute the information about any changes to its peers, and to reach a stable state across the network such that packets are forwarded consistently.

For all questions about routing scalability, research that presents figures based on credible example networks is highly desirable. Similar questions may be asked about the amount of forwarding state that has to be maintained in the routers.

8. To what extent can Semantic Routing be applied to multicast transmission schemes:
 - * Can Semantic Routing facilitate the computation and the establishment of (service-inferred) multicast distribution trees?
 - * Can specific semantics be carried in multicast addresses?
9. Is the approach extensible and maintainable? Can new features be added without increasing the complexity and in a backward compatible way? Could the approach be modified to handle evolutions in the rest of the networking infrastructure? Considerations might include the ability to encode additional options or variants within protocol fields, and the ability to add new fields. Such considerations must be actively traded against the processing overhead associated with certain encoding types.
10. What aspects need to be standardized? It is important to understand the necessity of standardization within this research. What degree of interoperability is expected between devices and networks? Is a given domain so constrained (for example, to a single equipment vendor) that standardization would be meaningless? Is the application so narrow (for example, in niche hardware environments) such that interoperability is best handled by agreements among small groups of vendors such as in industry consortia?

5. Security and Privacy Considerations

Research into Semantic Routing must give full consideration to the security and privacy issues that are introduced by these mechanisms. Placing additional information into packet header fields might reveal details of what the packet is for, what function the user is performing, who the user is, etc. Furthermore, in-flight modification of the additional information might not directly change the destination of the packet, but might change how the packet is handled within the network and at the destination.

It should also be considered how packet encryption techniques that are increasingly popular for end-to-end or edge-to-edge security may obscure the semantic information carried in some fields of the packet header or found deeper in the packet. This may render some semantic routing techniques impractical and may dictate other methods of carrying the necessary information to enable Semantic Routing.

6. IANA Considerations

This document makes no requests for IANA action.

7. Acknowledgements

Thanks to Stewart Bryant for useful conversations. Luigi Iannone, Robert Raszuk, Dirk Trossen, Ron Bonica, Marie-Jose Montpetit, Yizhou Li, Toerless Eckert, Tony Li, Joel Halpern, Stephen Farrell, Carsten Bormann, David Hutchison, Jeffery He, Dino Farinacci, Greg Mirsky, and Jeff Haas made helpful suggestions.

This work is partially supported by the European Commission under Horizon 2020 grant agreement number 101015857 Secured autonomic traffic management for a Tera of SDN flows (Teraflow).

8. Contributors

Joanna Dang
Email: dangjuanna@huawei.com

9. Informative References

- [I-D.farrel-irtf-introduction-to-semantic-routing]
Farrel, A. and D. King, "An Introduction to Semantic Routing", Work in Progress, Internet-Draft, draft-farrel-irtf-introduction-to-semantic-routing-03, 22 January 2022, <<https://www.ietf.org/archive/id/draft-farrel-irtf-introduction-to-semantic-routing-03.txt>>.
- [I-D.king-irtf-semantic-routing-survey]
King, D. and A. Farrel, "A Survey of Semantic Internet Routing Techniques", Work in Progress, Internet-Draft, draft-king-irtf-semantic-routing-survey-03, 26 November 2021, <<https://www.ietf.org/archive/id/draft-king-irtf-semantic-routing-survey-03.txt>>.
- [RFC3467] Klensin, J., "Role of the Domain Name System (DNS)", RFC 3467, DOI 10.17487/RFC3467, February 2003, <<https://www.rfc-editor.org/info/rfc3467>>.
- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <<https://www.rfc-editor.org/info/rfc3972>>.

- [RFC4984] Meyer, D., Ed., Zhang, L., Ed., and K. Fall, Ed., "Report from the IAB Workshop on Routing and Addressing", RFC 4984, DOI 10.17487/RFC4984, September 2007, <<https://www.rfc-editor.org/info/rfc4984>>.
- [RFC5693] Seedorf, J. and E. Burger, "Application-Layer Traffic Optimization (ALTO) Problem Statement", RFC 5693, DOI 10.17487/RFC5693, October 2009, <<https://www.rfc-editor.org/info/rfc5693>>.
- [RFC8799] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <<https://www.rfc-editor.org/info/rfc8799>>.
- [royalsoc] The Royal Society, "Evidence synthesis : Principles", Web page, Principles for good evidence synthesis, 19 September 2018, <<https://royalsociety.org/topics-policy/projects/evidence-synthesis/principles/>>.

Authors' Addresses

Daniel King
Lancaster University
United Kingdom
Email: d.king@lancaster.ac.uk

Adrian Farrel
Old Dog Consulting
United Kingdom
Email: adrian@olddog.co.uk

Christian Jacquenet
Orange
Rennes
France
Email: christian.jacquenet@orange.com

Network Working Group
Internet-Draft
Intended status: Informational
Expires: 8 September 2022

S. Peng
Z. Li
Huawei Technologies
G. Mishra
Verizon Inc.
7 March 2022

APN Scope and Gap Analysis
draft-peng-apn-scope-gap-analysis-04

Abstract

The APN work in IETF is focused on developing a framework and set of mechanisms to derive, convey and use an attribute allowing the implementation of fine-grain user group-level and application group-level requirements in the network layer. APN aims to apply various policies in different nodes along a network path onto a traffic flow altogether, for example, at the headend to steer into corresponding path, at the midpoint to collect corresponding performance measurement data, and at the service function to execute particular policies. Currently there is still no way to efficiently realize this composite network service provisioning along the path. This document further clarifies the scope of the APN work and describes the solution gap analysis.

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 <https://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 8 September 2022.

Copyright Notice

Copyright (c) 2022 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 (<https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
2. Requirements Language	3
3. Terminologies	3
4. APN Framework and Scope	3
5. Example Use Case and Existing Issues	4
6. Basic Solution and Benefits	5
7. Solution Gap Analysis	7
7.1. IPv6/MPLS Flow Label	7
7.2. SFC ServiceID	7
7.3. IOAM Flow ID	8
7.4. Binding SID	9
7.5. FlowSpec Label	9
7.6. Group Policy ID	9
7.7. Detnet Flow Identification	9
7.8. Network Slicing Resource ID	10
7.9. Service Path ID	10
7.10. Summary	10
8. IANA Considerations	11
9. Acknowledgements	11
10. Informative References	11
Authors' Addresses	15

1. Introduction

Application-aware Networking (APN) is introduced in [I-D.li-apn-framework] and [I-D.li-apn-problem-statement-usecases]. APN conveys an attribute along with data packets into network and makes the network aware about data flow requirements at different granularity levels.

Such an attribute is acquired, constructed in a structured value, and then encapsulated in the packet. Such structured value is treated as an opaque object in the network to which the network operator applies policies in various nodes/service functions along the path and provides corresponding services.

This structured attribute can be encapsulated in various data planes adopted within a Network Operator controlled limited domain, e.g. MPLS, VXLAN, SR/SRv6 and other tunnel technologies, which waits to be further specified.

With APN, it becomes possible to apply various policies in different nodes along a network path onto a traffic flow altogether in a more efficient way, e.g., at the headend to steer into corresponding path, at the midpoint to collect corresponding performance measurement data, and at the service function to execute particular policies. Currently there is still no way to realize this composite network service provisioning along the path very efficiently. It may be possible to stack those various policies in a list of TLVs at the headend. However, this approach would introduce great complexities and impose big challenges on the hardware processing and forwarding.

The example use-case presented in this draft further expands on the rationale for such an attribute and how it can be derived and used in that specific context.

This document further clarifies the scope of the APN work and describes the solution gap analysis.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 RFC 2119 [RFC2119] RFC 8174 [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Terminologies

APN: Application-aware Networking

CPE: Customer Premises Equipment

DPI: Deep Packet Inspection

OS: Operating System

4. APN Framework and Scope

The APN framework is introduced in [I-D.li-apn-framework], as shown in the Figure 1.

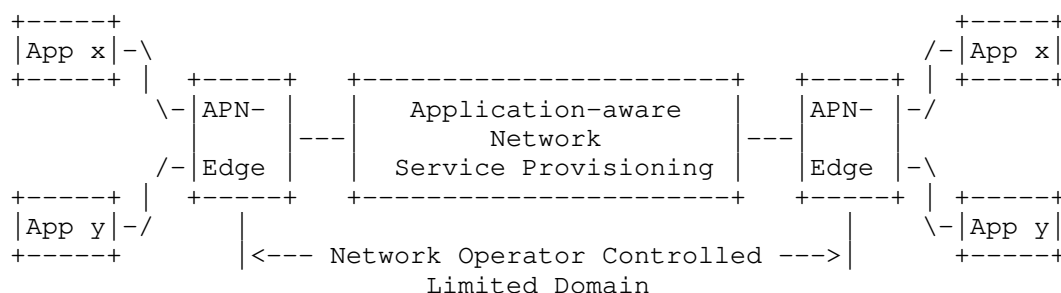


Figure 1. APN Framework and Scope

APN is only applied to an edge-to-edge tunnel encapsulation within a limited trusted domain. It means that the source and destination addresses of the packet are the endpoints of the tunnel (i.e. the domain edges), and nothing about the payload source and destination can be deduced, which substantially reduces the privacy concerns. Typically, an APN domain is defined as a Network Operator controlled limited domain (see Figure 1), in which MPLS, VXLAN, SR/SRv6 and other tunnel technologies are adopted to provide network services.

With APN, the attribute is acquired based on the existing information in the packet header (i.e. source and destination addresses, incoming L2 (or) MPLS encapsulation, incoming physical/virtual port information, the other fields of the 5-tuple if they are not encrypted) at the edge devices of the APN domain, added to the data packets along with the tunnel encapsulation, and delivered to the network, wherein, according to this attribute, corresponding network services are provisioned. When the packets leave the APN domain, the attribute is removed together with the tunnel encapsulation header.

5. Example Use Case and Existing Issues

To be more specific and more concrete, here we use SD-WAN as an example use case to further expand on the rationale for such attribute and how it can be derived and used in that specific context.

In the case of SD-WAN, an enterprise obtains WAN services from an SD-WAN provider so that its employees have access to the applications in the Cloud, and then the SD-WAN provider may buy WAN lines from a Network Operator. The enterprise may know what applications will use the SD-WAN services, but it will only provide the 5 tuples (i.e. source IP address, source port, destination IP address, destination port, transport protocol) of those applications to the SD-WAN

provider. So, the SD-WAN provider does not know what applications it is serving, and will only provide 5 tuples to the Network Operator and the service performance requirements for steering their customer's traffic. In this way, the Network Operator does not know anything else about the traffic except the 5 tuples and requirements. Nowadays, SD-WAN is usually using 5-tuple to steer the traffic into corresponding WAN lines across the Network Operator's network [SD-WAN].

However, there are two main issues in the current SD-WAN deployments.

1) It is complicated to resolve the 5 tuples. Even worse, as the traffic is encrypted, it becomes impossible to obtain any transport layer information. Moreover, in the IPv6 data plane, with the extension headers being added before the upper layer, in some implementations it becomes very difficult and even impossible to obtain transport layer information because that information is located deep in the packet. So, there is no 5 tuples anymore, and maybe only 2 tuples are available.

2) Currently there is still no way to apply various policies in different nodes along the network path onto a traffic flow altogether, that is, at the headend to steer into corresponding path, at the midpoint to collect corresponding performance measurement data, and at the service function to execute particular policies. It may be possible to stack those various policies in a list of TLVs at the headend. However, this approach would introduce great complexities and impose big challenges on the hardware processing and forwarding.

6. Basic Solution and Benefits

With APN, at the edge node, i.e. CPE, of the SD-WAN (see Figure 2), the 5-tuple, plus information related to user or application group-level requirements is constructed into a structured value, called APN attribute. This attribute is only meaningful for the network operators to apply various policies in different nodes/service functions, which can be enforced from the Controllers.

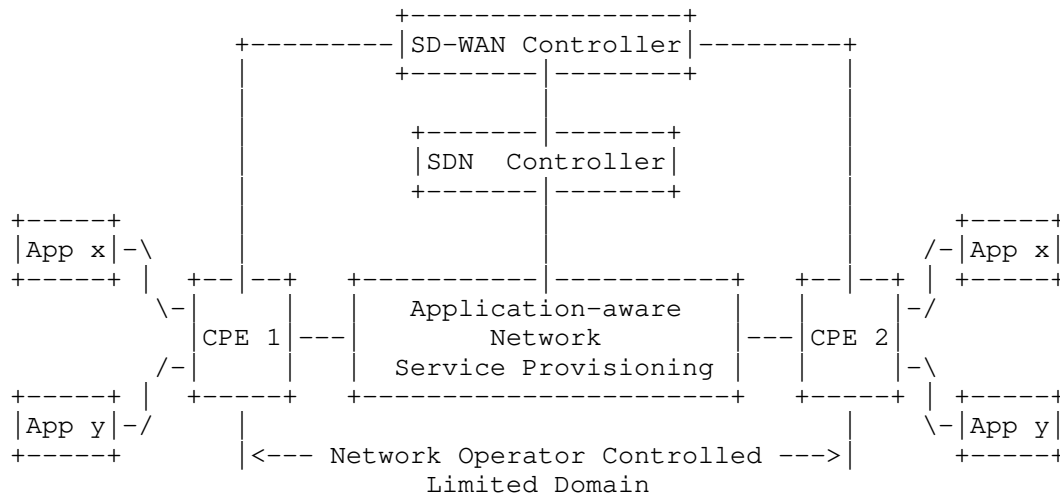


Figure 2. SD-WAN using the APN Framework

With such an attribute in the network, we can easily solve the two issues above-mentioned. For example, when the packet is sent from the CPE1 and the attribute is added along with the tunnel encapsulation, then it is not necessary to resolve the 5-tuple and perform the deep inspection in every node along the path. This attribute is encapsulated in the network layer and can be easily read by the routers and service functions. If the tunnel is based on the IPv6 data plane, for example, such an attribute can be encapsulated in an option of IPv6 hop-by-hop options header.

Since this attribute is taken as an object to the network, the network operators will simply place the policies in the nodes/service functions where this indicated traffic will go through, and the corresponding node/service function will just apply policies for this object. This can be easily done by utilizing this attribute, which is not possible with any current existing mechanism.

Such attribute will also bring other benefits, for example,

- * Improve the forwarding performance since it will only use 1 field in the IP layer instead of resolving 5 tuples, which will also improve the scalability.
- * Very flexible policy enforcement in various nodes and service functions along the network path.

Furthermore, with such attribute, more new services could be enabled, for example,

- * Even more fine-granularity performance measurement could be achieved and the granularity to be monitored and visualized can be controllable, which is able to relieve the processing pressure on the controller when it is facing the massive monitoring data.
- * The policy execution on the service function can be based only on this value and not based on 5-tuple, which can eliminate the need of deep packet inspection.
- * The underlay performance guarantee could be achieved for SD-WAN overlay services, such as explicit traffic engineering path satisfying SLA and selective visualized accurate performance measurement.

7. Solution Gap Analysis

There are already some solutions specified in IETF, which use identifier to perform traffic steering and service provisioning. However, the existing solutions are specific to a particular scenario or data plane. None of them is the same as APN and able to achieve the same effects.

7.1. IPv6/MPLS Flow Label

[RFC6437] specifies the IPv6 flow label which enables the IPv6 flow classification. However, the IPv6 flow label is mainly used for Equal Cost Multipath Routing (ECMP) and Link Aggregation [RFC6438].

Similarly, [RFC6391] describes a method of adding an additional Label Stack Entry (LSE) at the bottom of the stack in order to facilitate the load balancing of the flows within a pseudowire (PW) over the available ECMPs. A similar design for general MPLS use has also been proposed in [RFC6790] using the concept of Entropy Label.

7.2. SFC ServiceID

Subscriber Identifier and Performance Policy Identifier are specified in [RFC8979]. These identifiers are carried only in the Network Service Header (NSH) [RFC8300] Context Header, as shown in Figure 3, while the APN attribute can be carried in various data plane encapsulations.

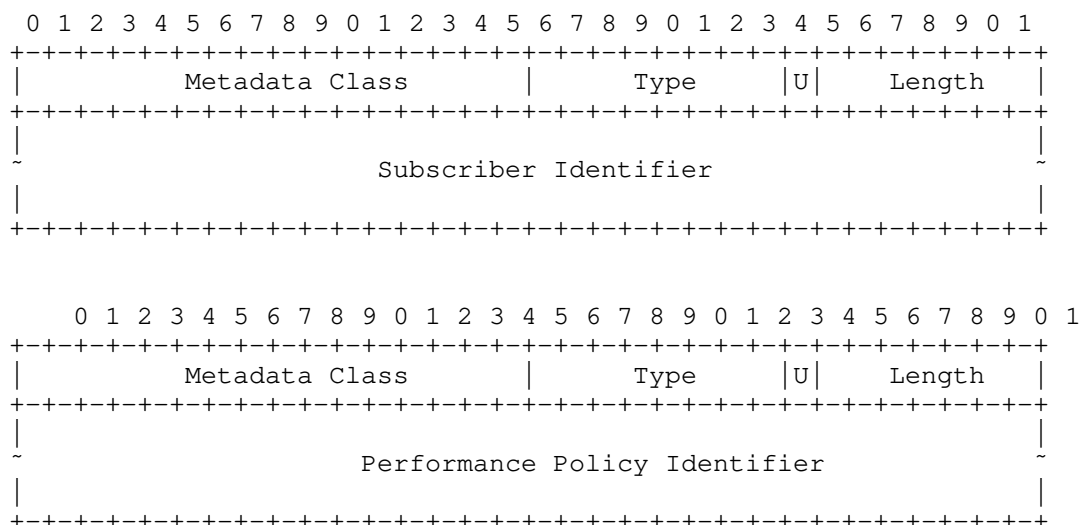


Figure 3. Subscriber Identifier and Performance Policy Identifier

In this draft [RFC8979], the Subscriber Identifier carries an opaque local identifier that is assigned to a subscriber by a network operator, and the Performance Policy Identifier represents an opaque value pointing to specific performance policy to be enforced. In this way, in order to apply various policies in different nodes along the network path onto a traffic flow altogether, e.g., at the headend to steer into corresponding path, at the midpoint to collect corresponding performance measurement data, and at the service function to execute particular policies, those various policies would have to be stacked in a list of TLVs at the headend, introducing great complexities and big challenges on the hardware processing and forwarding.

The APN attribute is treated as an opaque object in the network, to which the network operator applies policies in various nodes/service functions along the path and provide corresponding services.

7.3. IOAM Flow ID

A 32-bit Flow ID is specified in [I-D.ietf-ippm-ioam-direct-export], which is used to correlate the exported data of the same flow from multiple nodes and from multiple packets, while the APN attribute can serve more various purposes.

7.4. Binding SID

The Binding SID (BSID) [RFC8402] is bound to an SR Policy, instantiation of which may involve a list of SIDs. Any packets received with an active segment equal to BSID are steered onto the bound SR Policy. A BSID may be either a local or a global SID. While the APN attribute is not bound to SR only, and it can be carried in various data plane encapsulations.

7.5. FlowSpec Label

The flow specification (FlowSpec) [RFC5575] is actually an n-tuple consisting of several matching criteria that can be applied to IP traffic, which include elements such as source and destination address prefixes, IP protocol, and transport protocol port numbers. In BGP VPN/MPLS networks, BGP FlowSpec can be extended to identify and change (push/swap/pop) the label(s) for traffic that matches a particular FlowSpec rule in [I-D.ietf-idr-flowspec-mpls-match] and [I-D.ietf-idr-bgp-flowspec-label]. In [I-D.liang-idr-bgp-flowspec-route], BGP is used to distribute the FlowSpec rule bound with label(s). While the APN attribute is not bound to MPLS only, and it can be carried in various data plane encapsulations.

7.6. Group Policy ID

The capabilities of the VXLAN-GPE protocol can be extended by defining next protocol "shim" headers that are used to implement new data plane functions. For example, Group Policy ID is carried in the Group-Based Policy (GBP) Shim header [I-D.lemon-vxlan-lisp-gpe-gbp]. GENEVE has similar ability as VXLAN-GPE to carry metadata.

7.7. Detnet Flow Identification

Identification and Specification of DetNet Flows is specified in [RFC9016]. DetNet MPLS flows can be identified and specified by the SLabel and the FLabelStack. The IP 6-tuple is used for DetNet IP flow identification, which consists of SourceIpAddress, DestinationIpAddress, Dscp, Protocol, SourcePort, and DestinationPort. IPv6FlowLabel and IPsecSpi are additional attributes that can be used for DetNet flow identification in addition to the 6-tuple. Therefore, the Detnet IP Flow ID is logical and there is no such Flow ID carried for Detnet, but only the 6-tuple is directly used to identify the Detnet flows.

Only one exceptional case, in [I-D.ietf-spring-sr-redundancy-protection], the 32-bit flow identification (FID) identifies one specific Detnet flow of

redundancy protection. This FID is usually allocated from centralized controller to the SR ingress node or redundancy node in SR network.

7.8. Network Slicing Resource ID

In [I-D.dong-6man-enhanced-vpn-vtn-id], VTN Resource ID is a 4-octet identifier which uniquely identifies the set of network resources allocated to a VTN. For network slicing, the ID is used to indicate the network resources to be allocated to the network slices and it is not bound to any traffic flow.

APN is for traffic steering, while network slicing is about resource partition [I-D.ietf-teas-rfc3272bis].

7.9. Service Path ID

In [RFC8300], Service Path Identifier (SPI) uniquely identifies a Service Function Path (SFP). Participating nodes MUST use this identifier for SFP selection. The initial Classifier MUST set the appropriate SPI for a given classification result. For SFC, the ID is used to indicate a SF path and it is not bound to any traffic flow.

7.10. Summary

The comparison of the identifiers for the typical network services (incl. iOAM, Detnet, Network Slicing (NS), and Service Function Chaining (SFC)) is shown in the following Table from different aspects (incl. ID, Identification Object, Source (for generating the ID), Configuration (Conf.) node, and Size).

	ID	Identification Object	Source	Conf. node	Size
APN	APN ID	The flow that needs fine-granular services	5-tuple Layer 2	Controller	32bits 128b
iOAM	Flow ID	The flow that needs performance monitoring	-	Controller Ingress	32bits
Detnet	Flow ID (6-tuple)	The flow that needs Detnet services	-	Controller	-
Detnet	Flow ID	The redundant protection flow	-	Detnet Controller	32bits
NS	Resource ID	The network resources that are allocated to network slices	-	Controller	32bits
SFC	SPI	The SF Path	-	Controller	24bits
SFC	Performance Policy ID	The performance policy	-	Controller	-

Table 1. Comparison of the Identifiers

As driven by ever-emerging new 5G services, fine-granularity service provisioning becomes urgent. The existing solutions are either specific to a particular scenario or data plane. While APN aims to define a generalized attribute used for fine-granularity service provisioning, and can be carried in various data plane encapsulations.

8. IANA Considerations

There are no IANA considerations in this document.

9. Acknowledgements

The authors would like to acknowledge Martin Vigoureux, Alvaro Retana, Barry Leiba, Stefano Previdi, Adrian Farrel, and Daniel King for their valuable review and comments.

10. Informative References

[I-D.brockners-ippm-ioam-vxlan-gpe]

Brockners, F., Bhandari, S., Govindan, V. P., Pignataro, C., Gredler, H., Leddy, J., Youell, S., Mizrahi, T., Kfir, A., Gafni, B., Lapukhov, P., and M. Spiegel, "VXLAN-GPE Encapsulation for In-situ OAM Data", Work in Progress, Internet-Draft, draft-brockners-ippm-ioam-vxlan-gpe-03, 4 November 2019, <<https://www.ietf.org/archive/id/draft-brockners-ippm-ioam-vxlan-gpe-03.txt>>.

[I-D.dong-6man-enhanced-vpn-vtn-id]

Dong, J., Li, Z., Xie, C., Ma, C., and G. Mishra, "Carrying Virtual Transport Network (VTN) Identifier in IPv6 Extension Header", Work in Progress, Internet-Draft, draft-dong-6man-enhanced-vpn-vtn-id-06, 24 October 2021, <<https://www.ietf.org/archive/id/draft-dong-6man-enhanced-vpn-vtn-id-06.txt>>.

[I-D.ietf-idr-bgp-flowspec-label]

Liang, Q., Hares, S., You, J., Raszuk, R., and D. Ma, "Carrying Label Information for BGP FlowSpec", Work in Progress, Internet-Draft, draft-ietf-idr-bgp-flowspec-label-01, 6 December 2016, <<https://www.ietf.org/archive/id/draft-ietf-idr-bgp-flowspec-label-01.txt>>.

[I-D.ietf-idr-flowspec-mpls-match]

Yong, L., Hares, S., Liang, Q., and J. You, "BGP Flow Specification Filter for MPLS Label", Work in Progress, Internet-Draft, draft-ietf-idr-flowspec-mpls-match-01, 6 December 2016, <<https://www.ietf.org/archive/id/draft-ietf-idr-flowspec-mpls-match-01.txt>>.

[I-D.ietf-ippm-ioam-direct-export]

Song, H., Gafni, B., Zhou, T., Li, Z., Brockners, F., Bhandari, S., Sivakolundu, R., and T. Mizrahi, "In-situ OAM Direct Exporting", Work in Progress, Internet-Draft, draft-ietf-ippm-ioam-direct-export-07, 13 October 2021, <<https://www.ietf.org/archive/id/draft-ietf-ippm-ioam-direct-export-07.txt>>.

[I-D.ietf-sfc-serviceid-header]

Sarikaya, B., Hugo, D. V., and M. Boucadair, "Subscriber and Performance Policy Identifier Context Headers in the Network Service Header (NSH)", Work in Progress, Internet-Draft, draft-ietf-sfc-serviceid-header-14, 11 December 2020, <<https://www.ietf.org/archive/id/draft-ietf-sfc-serviceid-header-14.txt>>.

- [I-D.ietf-spring-sr-redundancy-protection]
Geng, X., Chen, M., Yang, F., Garvia, P. C., and G. Mishra, "SRv6 for Redundancy Protection", Work in Progress, Internet-Draft, draft-ietf-spring-sr-redundancy-protection-01, 15 February 2022, <<https://www.ietf.org/archive/id/draft-ietf-spring-sr-redundancy-protection-01.txt>>.
- [I-D.ietf-teas-rfc3272bis]
Farrel, A., "Overview and Principles of Internet Traffic Engineering", Work in Progress, Internet-Draft, draft-ietf-teas-rfc3272bis-15, 24 February 2022, <<https://www.ietf.org/archive/id/draft-ietf-teas-rfc3272bis-15.txt>>.
- [I-D.lemon-vxlan-lisp-gpe-gbp]
Lemon, J., Maino, F., Smith, M., and A. Isaac, "Group Policy Encoding with VXLAN-GPE and LISP-GPE", Work in Progress, Internet-Draft, draft-lemon-vxlan-lisp-gpe-gbp-02, 30 April 2019, <<https://www.ietf.org/archive/id/draft-lemon-vxlan-lisp-gpe-gbp-02.txt>>.
- [I-D.li-6man-app-aware-ipv6-network]
Li, Z., Peng, S., Li, C., Xie, C., Voyer, D., Li, X., Liu, P., Cao, C., and K. Ebisawa, "Application-aware IPv6 Networking (APN6) Encapsulation", Work in Progress, Internet-Draft, draft-li-6man-app-aware-ipv6-network-03, 22 February 2021, <<https://www.ietf.org/archive/id/draft-li-6man-app-aware-ipv6-network-03.txt>>.
- [I-D.li-apn-framework]
Li, Z., Peng, S., Voyer, D., Li, C., Liu, P., Cao, C., Mishra, G., Ebisawa, K., Previdi, S., and J. N. Guichard, "Application-aware Networking (APN) Framework", Work in Progress, Internet-Draft, draft-li-apn-framework-04, 25 October 2021, <<https://www.ietf.org/archive/id/draft-li-apn-framework-04.txt>>.
- [I-D.li-apn-problem-statement-usecases]
Li, Z., Peng, S., Voyer, D., Xie, C., Liu, P., Qin, Z., Mishra, G., Ebisawa, K., Previdi, S., and J. N. Guichard, "Problem Statement and Use Cases of Application-aware Networking (APN)", Work in Progress, Internet-Draft, draft-li-apn-problem-statement-usecases-05, 20 December 2021, <<https://www.ietf.org/archive/id/draft-li-apn-problem-statement-usecases-05.txt>>.

- [I-D.liang-idr-bgp-flowspec-route]
Liang, Q. and J. You, "BGP FlowSpec based Multi-dimensional Route Distribution", Work in Progress, Internet-Draft, draft-liang-idr-bgp-flowspec-route-00, 20 October 2014, <<https://www.ietf.org/archive/id/draft-liang-idr-bgp-flowspec-route-00.txt>>.
- [I-D.peng-apn-security-privacy-consideration]
Peng, S., Li, Z., Voyer, D., Li, C., Liu, P., and C. Cao, "APN Security and Privacy Considerations", Work in Progress, Internet-Draft, draft-peng-apn-security-privacy-consideration-02, 16 June 2021, <<https://www.ietf.org/archive/id/draft-peng-apn-security-privacy-consideration-02.txt>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <<https://www.rfc-editor.org/info/rfc5575>>.
- [RFC6391] Bryant, S., Ed., Filsfils, C., Drafz, U., Kompella, V., Regan, J., and S. Amante, "Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network", RFC 6391, DOI 10.17487/RFC6391, November 2011, <<https://www.rfc-editor.org/info/rfc6391>>.
- [RFC6437] Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "IPv6 Flow Label Specification", RFC 6437, DOI 10.17487/RFC6437, November 2011, <<https://www.rfc-editor.org/info/rfc6437>>.
- [RFC6438] Carpenter, B. and S. Amante, "Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels", RFC 6438, DOI 10.17487/RFC6438, November 2011, <<https://www.rfc-editor.org/info/rfc6438>>.
- [RFC6790] Kompella, K., Drake, J., Amante, S., Henderickx, W., and L. Yong, "The Use of Entropy Labels in MPLS Forwarding", RFC 6790, DOI 10.17487/RFC6790, November 2012, <<https://www.rfc-editor.org/info/rfc6790>>.

- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8300] Quinn, P., Ed., Elzur, U., Ed., and C. Pignataro, Ed., "Network Service Header (NSH)", RFC 8300, DOI 10.17487/RFC8300, January 2018, <<https://www.rfc-editor.org/info/rfc8300>>.
- [RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <<https://www.rfc-editor.org/info/rfc8402>>.
- [RFC8979] Sarikaya, B., von Hugo, D., and M. Boucadair, "Subscriber and Performance Policy Identifier Context Headers in the Network Service Header (NSH)", RFC 8979, DOI 10.17487/RFC8979, February 2021, <<https://www.rfc-editor.org/info/rfc8979>>.
- [RFC9016] Varga, B., Farkas, J., Cummings, R., Jiang, Y., and D. Fedyk, "Flow and Service Information Model for Deterministic Networking (DetNet)", RFC 9016, DOI 10.17487/RFC9016, March 2021, <<https://www.rfc-editor.org/info/rfc9016>>.
- [SD-WAN] MEF 70.1 Draft (R1), available at <https://www.mef.net/wp-content/uploads/2020/08/MEF-70-1-Draft-R1.pdf>, "SD-WAN Service Attributes and Service Framework", August 2020.

Authors' Addresses

Shuping Peng
Huawei Technologies
Beijing
China
Email: pengshuping@huawei.com

Zhenbin Li
Huawei Technologies
Beijing
China
Email: lizhenbin@huawei.com

Gyan Mishra
Verizon Inc.
United States of America
Email: gyan.s.mishra@verizon.com