Challenges for the Internet Routing Infrastructure Introduced by Semantic Routing
draft-king-irtf-challenges-in-routing-04

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 were enhanced to route packets according to additional information carried within the packets 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 existing fields, by adding semantics to IP addresses, or by adding fields to the packets. The intent is to facilitate enhanced routing decisions based on these additional semantics in order to provide differentiated paths for different packet flows distinct from simple shortest path first 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 protocols to make use of new or additional semantics.

This document is presented as 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/.
1. Introduction

Historically, the meaning of an IP address has been to identify an interface on a network device. Routing protocols were developed to determine paths through the network toward destination addresses so that IP packets with a common destination address converged on that destination. Anycast and multicast addresses were also defined and those address semantics necessitated variations to the routing protocols and the development of new protocols.
Over time, routing decisions were enhanced to route packets according to additional information carried within the packets and dependent on policy coded in, configured at, or signaled to the routers. Perhaps the most obvious example is Equal-Cost Multipath (ECMP) where a router makes a consistent choice for forwarding packets 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 existing fields, by adding semantics to IP addresses, or by adding fields to the packets. The intent is to facilitate enhanced routing decisions based on these additional semantics in order to provide differentiated paths for different packet flows distinct from simple shortest path first routing. We call this approach "Semantic Routing".

There are many approaches to adding semantics to packet headers. These 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 their own purposes. Some proposals suggest variable address lengths, others offer hierarchical addresses, and some introduce a structure to addresses so that they can carry additional information in a common way. Other approaches perform routing decisions on fields in the packet header (such as the IPv6 Flow Label, or the Traffic Class field), overload packet fields, or add new information to packet headers.

A survey of ways in which routing 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 limited domains [RFC8799] (networks) that are IP-based, 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 routing that are present in today’s IP networks. It then defines the concept of "Semantic Routing" and presents some of the challenges to the existing routing system that Semantic Routing may present. Finally, this document presents a list of related research questions that offer opportunities for future research into new or modified routing protocols that make use of Semantic Routing.
In this document, the focus is on routing and forwarding at the IP layer. It is possible that a variety of overlay mechanisms exist to perform service or path routing at higher layers, and that 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 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. These challenges include mobility, multihoming, programmable paths, scalability, and security, and were not the focus of the original design of the Internet. Nevertheless, IP-based networks have, in general, coped well in an incremental manner as each new challenge has evolved. This 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. Mobility users may also consume network resources, while physically moving. 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) scenarios.

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 from different pools of addresses. There are challenges concerning how traffic is routed back to the source if the source has originated its traffic using the wrong 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-based network topologies facilitate
multiple paths each with different characteristics and with
different failure likelihods. 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
in order to provide delivery qualities or to avoid transiting
specific areas of an IP-based network. However, the way in which
packets are routed using the best or 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 two "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 replication into the
network to make more optimal use of the network resources can be
complex to set up and manage requiring sophisticated protocols
that can determine the best multicast delivery topologies, as well
as hardware that can replicate packets within the network. In
order that packets can be addressed to a group of destinations and
not be routed using the normal unicast approaches, parts of the
addressing space (that is, address prefixes) have been reserved to
indicate multicast.

Programmable Paths - The ability to decouple IP-based network
paths from routing protocols and agreements between Service
Providers could allow users and applications to configure and
select network paths themselves, based on the required path (that
is, traffic-delivery) characteristics. Currently, user and
application packets follow the path selected by routing protocols
and the way traffic is routed through a network is under the
exclusive control of the Service Provider that owns the network.

End-Point 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 best use of these distributed services 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) or
in the transport layer (such as using ALTO). 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-based network must maintain and exchange with their peers. As the number of devices attached to the network grows, so the number of addresses in use also grows, and because of the address allocation schemes, the mobility of devices, and the various connectivity options between networks, the routing table sizes also grow and are not amenable to aggregation. This problem exists even in limited domains (such as IoT), where, as more devices are added to the network, the size of the routing table may be a gating factor in the applicability of certain routing protocols. It may be noted that scaling issues are exacerbated by multihoming practices if a host that is multihomed is allocated a different address for each point of attachment.

Security - Issues of security and privacy have been largely overlooked within 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 routed via 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-based network that enhances decisions by considering information present in the packet and configured or programmed into the routers in addition to the routable part of the destination IP address (the prefix). 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 as part of a software defined networking (SDN) system, or derived by a software component on the router that considers network conditions and traffic loads.
The packet fields concerned may be the normal fields of the IP header, those same fields but with additional semantics, elements of the packet payload, or new fields defined for inclusion in the packet header. 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].

Several technical challenges exist for semantic routing in IP-based network depending on which approach is taken. These include:

- 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 preventing mechanisms may be 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-based networking.

3.1. Architectural Considerations

Semantic data may be applied in a number of ways to integrate with existing routing architectures. An overlay can be built such that semantic routing is used to route 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 Internet. In other cases, traffic from within the domain is exchanged with other domains that are connected together across an IP-based network using tunnels or via application gateways. And in still another case traffic from the domain is routed 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-based networks. In these cases, there is no risk to external networks from any semantic routing schemes carried out within the domain. 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 a number of 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 [RFC8799] 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 routed 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, may need to be handled using separate network technologies. Improving IP-based 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 semantic 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 routing system might be impacted by the use of semantic routing. 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 be answered as:

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

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

   Overlay: It is to be used as an overlay network over previous uses of IP or other underlay technologies using tunneling.
Gateway: The semantic routing will be used within a limited domain, and communications with the wider Internet will be handled by a protocol or application gateway.

Domain: The use of the semantic routing is entirely 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 cryptographically generated addresses made routable; how are the semantic parts of an address distinguished from the routable parts; is there an impact on the size and maintenance of routing tables due to the addition of semantics?

3. What path characteristics are needed for the routed paths? Since one of the purposes of adding semantics to the 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?

   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? What additional information about the network do the routing protocols...
need to gather? What changes to the routing algorithm is needed to deliver packets according to the desired characteristics?

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 simple backward-compatible modifications to existing protocols such that they work for today's IP addresses as well as enhanced-semantics?

  + Do we need entirely new protocols or radical evolutions of existing protocols in order to deliver the functions that we need?

  + Should we focus on the benefits of optimized routing solutions, or should we attempt to generalize to enable wider applicability?

Do we need new management tools and techniques? Management of the routing system (especially diagnostic management) is a crucial and often neglected part of the problem space.

5. What is the scalability impact for routing systems? Scalability can be measured as:

* Routing table size. How many entries need to be maintained in the routing table? Some approaches to semantic routing may be explicitly intended to address this problem.

* Routing performance. Routing performance may be considered in terms of the volume of data that has to be exchanged both to establish and to maintain the routing tables at the participating routers. It may also be measured in terms of
how much processing is required to derive new routes when there is a change in the network routing information.

* Routing convergence 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 the network, and to reach a stable state across the network such that packets are routed consistently.

For all questions of routing scalability, research that presents real numbers 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.

6. To what extent can multicast be developed:

* To support programmable SDN systems such as P4 [P4]?
* To satisfy end-to-end applications?
* To apply per-packet multicasting to develop new services?
* As a separate network layer distinct from IP or by encoding group destinations into IP addresses?

7. What aspects need to be standardized? It is really important to understand the necessity of standardization within this research. What degree of interoperability is expected between devices and networks? Is the limited 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 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, and Greg Mirsky 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]

[I-D.king-irtf-semantic-routing-survey]


Authors’ Addresses

Daniel King
Lancaster University
UK

Email: d.king@lancaster.ac.uk

Adrian Farrel
Old Dog Consulting
UK

Email: adrian@olddog.co.uk
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.

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 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 28 April 2022.
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. Terminologies

APN: Application-aware Networking

CPE: Customer Premises Equipment

DPI: Deep Packet Inspection

OS: Operating System

3. APN Framework and Scope

The APN framework is introduced in [I-D.li-apn-framework], as shown in the Figure 1.
APN works within a limited trusted domain. 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 such as 5-tuple and QinQ (S-VLAN and C-VLAN) 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.

4. 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.

5. 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.
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.

6. 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.

6.1. 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.

6.2. 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.
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.

6.3. 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.
6.4. 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.

6.5. 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.

6.6. 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.

6.7. 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.

6.8. 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.

6.9. 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.

6.10. 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).
Table 1. Comparison of the Identifiers

<table>
<thead>
<tr>
<th>Identifier</th>
<th>ID</th>
<th>Identification Object</th>
<th>Source</th>
<th>Conf. node</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>APN</td>
<td>APN ID</td>
<td>The flow that needs fine-granular services</td>
<td>Layer 2</td>
<td>Controller</td>
<td>128b</td>
</tr>
<tr>
<td>iOAM</td>
<td>Flow ID</td>
<td>The flow that needs performance monitoring</td>
<td>-</td>
<td>Controller</td>
<td>32bits</td>
</tr>
<tr>
<td>Detnet</td>
<td>Flow ID</td>
<td>The flow that needs Detnet services</td>
<td>-</td>
<td>Controller</td>
<td>-</td>
</tr>
<tr>
<td>Detnet</td>
<td>Flow ID</td>
<td>The redundant protection flow</td>
<td>-</td>
<td>Detnet</td>
<td>32bits</td>
</tr>
<tr>
<td>NS</td>
<td>Resource ID</td>
<td>The network resources that are allocated to network slices</td>
<td>-</td>
<td>Controller</td>
<td>32bits</td>
</tr>
<tr>
<td>SFC</td>
<td>SPI</td>
<td>The SF Path</td>
<td>-</td>
<td>Controller</td>
<td>24bits</td>
</tr>
<tr>
<td>SFC</td>
<td>Performance Policy ID</td>
<td>The performance policy</td>
<td>-</td>
<td>Controller</td>
<td>-</td>
</tr>
</tbody>
</table>

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.

7. IANA Considerations

There are no IANA considerations in this document.

8. 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.

9. Informative References


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