Path Aware Networking RG
Internet-Draft
Intended status: Informational
Expires: April 20, 2019

B. Trammell
ETH Zurich

October 17, 2018

# Open Questions in Path Aware Networking
## draft-irtf-panrg-questions-01

Abstract

This document poses open questions in path-aware networking, as a background for framing discussions in the Path Aware Networking proposed Research Group (PANRG). These are split into ~~making~~exposing properties of available Internet paths ~~available~~ to endpoints/applications, and allowing endpoints/applications to select paths through the ~~Internet~~ connectivity infrastructure for their traffic.





**Commentaire [Med1]:** This is odd given that networking is by essence about manipulating paths!

Application-enabled Networking or Collaborative Networking would be more appropriate.

I know this is not specific to this draft, but the terminology needs to be fixed somewhere, IMHO.

**Commentaire [Med2]:** This sentence is to be elaborated/reworded because “path-aware networking” is not a well-established concept. I would expand first what is meant because otherwise, it is difficult to understand what is meant.

**Commentaire [Med3]:** The same concept can be valid for a single network, Intranets, etc. I would not restrict to “Internet”.

**Commentaire [Med4]:** Given the distributed nature of networking, I would not expect a model in which an endpoint specifies the full path to be a viable option.

Strict source routing may be OK in some very specific contexts.

I guess what is meant here is more: “infer the selection of the paths” or “contribute to the selection of a portion of the path”. If that is the intent, please reword accordingly.

Table of Contents



## 1. Introduction to Path-Aware Networking

In the current Internet architecture, the inter-domain network layer provides an unverifiable, best-effort service: an application can assume that a packet with a given destination address will eventually be forwarded toward that destination, but little else. A transport layer protocol such as TCP can provide reliability over this best-effort service, and a protocol above the network layer such as IPsec AH [RFC4302] or TLS [RFC5246] can authenticate the remote endpoint. However, no explicit information about the path is available, and assumptions about that path sometimes do not hold, sometimes with serious impacts on the application, as in the case with BGP hijacking attacks.

By contrast, in a path-aware internetworking architecture, endpoints would have the ability to select or influence the path(s) through the network used by any given packet, and the network/transport layer explicitly exposes information about the path or paths available between two endpoints to those endpoints so that they can make this selection. Path control at the packet level enables new transport protocols that can leverage multipath connectivity across maximally-disjoint paths through the Internet, even over a single physical interface. It also provides transparency and control for applications and end-users to specify constraints on the paths that traffic should traverse, for instance to confound pervasive passive surveillance in the network core.

We note that this property of "path awareness" already exists in many Internet-connected networks in an intradomain context. Indeed, much of the practice of network engineering using encapsulation at layer 3

**Commentaire [Med5]:** What is an interdomain network layer?

**Commentaire [Med6]:** Do you assume that paths only expose connectivity matters or you include also service matters (https://tools.ietf.org/html/rfc7665, https://tools.ietf.org/html/rfc8517)?

**Commentaire [Med7]:** « Some » explicit information is available using specific protocols such as RTCP (once the connection is established, though) or PCE (https://tools.ietf.org/html/rfc4655).

**Mis en forme :** Surlignage

**Commentaire [Med8]:** or a segment of those paths?

**Commentaire [Med9]:** Assuming a valid route exists in the network and successful access control validation.

**Commentaire [Med10]:** Why restrict how the information is exposed?

**Commentaire [Med11]:** Because of the asymmetry nature of the routing architecture, I guess this information is per direction?

**Commentaire [Med12]:** I don't parse this.

**Commentaire [Med13]:** Why the information should be bound to specific two endpoints?

This would assume that exposed data will be per-connection/session and no aggregate data can be used.

**Commentaire [Med14]:** This is only possible if the paths are fully specified.

This is too ambitious (and not viable).

**Commentaire [Med15]:** This is too early to assess at this stage. Providing pointers to sections where this is discussed would be valuable.

**Commentaire [Med16]:** Not sure to understand the subtlety here.

Why not say "intra domain context" or "within single domains"?

can be said to be "path aware", in that it explicitly assigns traffic at tunnel endpoints to a given path within the network. Path-aware internetworking seeks to extend this awareness across domain boundaries without resorting to overlays, except as a transition technology.

## 2. Questions

Realizing path-aware networking requires answers to a set of open research questions. This document poses these questions, as a starting point for discussions about how to realize path awareness in the Internet, and to direct future research efforts within the Path Aware Networking Research Group.

### 2.1. A Vocabulary of Path Properties

In order for information about paths to be exposed to ~~the~~ an endpoint~~s~~, and for ~~those~~ an endpoint~~s~~ to be able to use that information, it is necessary to define a common vocabulary for path properties. The elements of this vocabulary could include relatively static properties, such as the presence of a given node or a service function on the path; as well as relatively dynamic properties, such as the current values of metrics such as loss and latency.

This vocabulary must be defined carefully, as its design will have impacts on the expressiveness of a given path-aware internetworking architecture. This expressiveness also exhibits tradeoffs. For example, a system that exposes node-level information for the topology through each network would maximize information about the individual components of the path at the endpoints at the expense of making internal network topology universally public, which may be in conflict with the business goals of each network's operator.

The first question: how are path properties defined and represented?

### 2.2. Discovery, Distribution, and Trustworthiness of Path Properties

Once endpoints and networks have a shared vocabulary for expressing path properties, the network must have some method for distributing those path properties to the endpoint. Regardless of how path property information is distributed to the endpoints, the endpoints require a method to authenticate the properties - to determine that they originated from and pertain to the path that they purport to.

Choices in distribution and authentication methods will have impacts on the scalability of a path-aware architecture. Possible dimensions in the space of distribution methods include in-band versus out-of-band, push versus pull versus publish-subscribe, and so on. There



**Commentaire [Med17]:** I'm not sure this text is helpful here to define the scope of PANRG/differentiate PAN. Inbound/outbound traffic engineering is used to governed how traffic is handle in an inter-domain context.

Also, extensions such as https://tools.ietf.org/html/draft-ietf-idr-performance-routing-01 were defined to help selecting paths that optimize some traffic performance metrics.

**Commentaire [Med18]:** The question is not actually about the vocabulary, but about the identification and characterization of information that need to be exposed.

**Commentaire [Med19]:** Please note that sharing some performance metrics may lead to what we called "QARush" in https://tools.ietf.org/html/rfc5160: that is basically, the deterioration of a path due to better exposed performance metrics.

The solution should prevent that.

**Commentaire [Med20]:** Do you assume that all involved endpoints in a communication (let it be unicast, multicast or whatever "n:m" communication scheme) should be pan-aware to benefit from the solution ?

**Commentaire [Med21]:** This may be dynamic, too!

**Commentaire [Med22]:** The questions are IMHO:
• Why and how an application/endpoint needs to know some QoS parameters reflecting the capabilities of a path/network?
•How an application will identify equivalent set of parameters?
•How to select a path when multiple criteria are used?
•How to select among paths if distinct metrics are exposed for each path?
•How an application knows what is acceptable?

**Commentaire [Med23]:** It is the data model which needs to be defined carefully.

**Commentaire [Med24]:** The first question is : Why?

Then, comes "what" and "how"!

Does an endpoint need the full characterization of a given path, only the access segment, etc.?

**Commentaire [Med25]:** data model?

**Commentaire [Med26]:** sharing?

are temporal issues with path property dissemination as well, especially with dynamic properties, since the measurement or elicitation of dynamic properties may be outdated by the time that information is available at the endpoints, and interactions between the measurement and dissemination delay may exhibit pathological behavior for unlucky points in the parameter space.

The second question: how do endpoints get access to trustworthy path properties?

## 2.3. Supporting Path Selection

Access to trustworthy path properties is only half of the challenge in establishing a path-aware architecture. Endpoints must be able to use this information in order to infer the selection of paths (segments) for some traffic they send.

As with path property distribution/sharing, choices made in path selection methods will also have an impact on the scalability and expressiveness of a path-aware architecture, and dimensions included in-band versus out-of-band, as well. Paths may also be selected on multiple levels of granularity - per packet, per flow, per aggregate - and this choice also has impacts on the scalability ~~scalabilty~~/expressiveness tradeoff. Path selection must, like path property information, be trustworthy, such that the result of a path selection at an endpoint is predictable.

The third question: how can endpoints select paths to use for traffic in a way that can be trusted by both the network and the endpoints?

## 2.4. Interfaces for Path Awareness

In order for applications to make effective use of a path-aware networking architecture, the communication interfaces presented by the network and transport layers must also expose path properties to the application in a useful way, and provide a useful set of paths among which the application can select. Path selection must be possible based not only on the preferences and policies of the application developer, but of end-users as well. Also, the path selection interfaces presented to applications and end users will need to support multiple levels of granularity. Most applications' requirements can be satisfied with the expression path selection policies in terms of properties of the paths, while some applications may need finer-grained, per-path control.

The fourth question: how can interfaces to the transport and application layers support the use of path awareness?

**Commentaire [Med27]:** The solution may be reserved a subset of the traffic.

**Commentaire [Med28]:** Why and how this will be assessed?

•Two applications to which the same set of metrics are exposed, may have distinct decisions.
• The same application may alter its selection to adjust the conditions indicated by a remote peer.

**Commentaire [Med29]:** or applications ?

**Commentaire [Med30]:** I don't understand this.

**Mis en forme :** Surlignage

**Commentaire [Med31]:** Please align this wording with the one above « by the network and transport layers must also expose path properties to the application"

## 2.5. Implications of Path Awareness for the Data Plane

In the current Internet, the basic assumption that at a given time ~~t~~ all traffic for a given flow will traverse a single path, for some definition of path, generally holds. In a path aware network, this assumption no longer holds. The absence of this assumption has implications for the design of protocols above any path-aware network layer.

For example, one advantage of multipath communication is that a given end-to-end flow can be "sprayed" along multiple paths in order to confound attempts to collect data or metadata from those flows for pervasive surveillance purposes [RFC7624]. However, the benefits of this approach are reduced if the upper-layer protocols use linkable identifiers on packets belonging to the same flow across different paths. Clients may mitigate linkability by opting to not re-use cleartext connection identifiers, such as TLS session IDs or tickets, on separate paths. The privacy-conscious strategies required for effective privacy in a path-aware Internet are only possible if higher-layer protocols such as TLS permit clients to obtain unlinkable identifiers.

The fifth question: how should transport-layer and higher layer protocols be redesigned to work most effectively over a path-aware networking layer?

## 2.6. What is an Endpoint?

The vision of path-aware networking articulated so far makes an assumption that path properties will be disseminated to endpoints on which applications are running (terminals with user agents, servers, and so on). However, incremental deployment may require that a path-aware network "core" be used to interconnect islands of legacy protocol networks. In these cases, it is the gateways, not the application endpoints, that receive path properties and make path selections for that traffic. The interfaces provided by this gateway are necessarily different than those a path-aware networking layer provides to its transport and application layers, and the path property information the gateway needs and makes available over those interfaces may also be different.

The sixth question: how is path awareness (in terms of vocabulary and interfaces) different when applied to tunnel and overlay endpoints?

**Commentaire [Med32]:** This is not true. Differentiated paths are used in the network for various reasons (load-balancing, invocation of service functions, etc.).

**Commentaire [Med33]:** This is already possible with current architectures.

An advantage I see with pan is that a consent can be provided to solicit a specific function at the upstream networks (e.g., terminal multipath connections because the remote peer is not MP-capable, terminate a pan-aware connection because the remote peer does not support pan features, etc.).

**Commentaire [Med34]:** This is too generic, IMO.

**Commentaire [Med35]:** I would start with this one.

## 2.7. Operating a Path Aware Network

The network operations model in the current Internet architecture assumes that traffic flows are controlled by the decisions and policies made by network operators, as expressed in interdomain routing protocols. In a network providing path selection to the endpoints, however, this assumption no longer holds, as endpoints may react to path properties by selecting alternate paths. Competing control inputs from path-aware endpoints and the interdomain routing control plane may lead to more difficult traffic engineering or nonconvergent ~~routing~~forwarding, especially if the endpoints' and operators'
notion of the "best" path for given traffic diverges significantly.

A concept for path aware network operations will need to have clear methods for the resolution of apparent (if not actual) conflicts of intent between the network's operator and the path selection at an endpoint. It will also need set of safety principles to ensure that increasing path control does not lead to decreasing connectivity; one such safety principle could be "the existence of at least one path between two endpoints guarantees the selection of at least one path between those endpoints."

The seventh question: how can a path aware network in a path aware internetwork be effectively operated, given control inputs from the network administrator as well as from the endpoints?

## 2.8. Deploying a Path Aware Network

The vision presented in the introduction discusses path aware networking from the point of view of the benefits accruing at the endpoints, to designers of transport protocols and applications as well as to the end users of those applications. However, this vision requires action not only at the endpoints but within the interconnected networks offering path aware connectivity. While the specific actions required are a matter of the design and implementation of a specific realization of a path aware protocol stack, it is clear than any path aware architecture will require network operators to give up some control of their networks over to endpoint-driven control inputs.

Here the question of apparent versus actual conflicts of intent arises again: certain network operations requirements may appear essential, but are merely accidents of the interfaces provided by current routing and management protocols. Incentives for deployment must show how existing network operations requirements are met through new path selection and property dissemination mechanisms.

**Commentaire [Med36]:** Some policies are not expressed in BGP. These are local to ASes.

**Commentaire [Med37]:** Not sure to understand this as the alternate paths assumes existing physical interconnections that are known and made available by a network.

**Commentaire [Med38]:** There is a first tension between inbound and outbound policies from the participating endpoints.

**Commentaire [Med39]:** This depends on the span of the path properties shared with endpoints.

**Commentaire [Med40]:** I'm afraid this is an unsolvable problem because it requires the involvement of transit providers which do not have any actual benefit if the full path is to be controlled by leaf networks/endpoints.

**Commentaire [Med41]:** That is?

**Commentaire [Med42]:** Do you assume that all paths are pre-established?

**Commentaire [Med43]:** This is too generic.

The incentives for network operators and equipment vendors to do provide be made clear, in terms of a plan to transition [RFC8170] an internetwork to path-aware operation, one network and facility at a time.

The eighth question: how can the incentives of network operators and end-users be aligned to realize the vision of path aware networking?

**Commentaire [Med44]:** A key issue is more on transit providers. This is the same issue as with https://tools.ietf.org/html/draft-narten-radir-problem-statement-05#section-3.3

## 3. Acknowledgments

Many thanks to Adrian Perrig, Jean-Pierre Smith, Mirja Kuehlewind, Olivier Bonaventure, Martin Thomson, Shwetha Bhandari, Chris Wood, and Lee Howard, for discussions leading to questions in this document.

This work is partially supported by the European Commission under Horizon 2020 grant agreement no. 688421 Measurement and Architecture for a Middleboxed Internet (MAMI), and by the Swiss State Secretariat for Education, Research, and Innovation under contract no. 15.0268. This support does not imply endorsement.

## 4. References

### 4.1. Normative References

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

### 4.2. Informative References

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <https://www.rfc-editor.org/info/rfc7624>.

[RFC8170] Thaler, D., Ed., "Planning for Protocol Adoption and Subsequent Transitions", RFC 8170, DOI 10.17487/RFC8170, May 2017, <https://www.rfc-editor.org/info/rfc8170>.

Author's Address

Brian Trammell
ETH Zurich
Gloriastrasse 35
8092 Zurich
Switzerland

Email: ietf@trammell.ch