Path Aware Networking: Obstacles to Deployment

(A Bestiary of Roads Not Taken)

(draft-irtf-panrg-what-not-to-do-03)

and what STILL won't work!

Spencer Dawkins

What's new since draft-irtf-panrg-what-not-to-do-01

- C.M Heard, Joe Touch, Joeri de Ruiter, and Wes Eddy sent new comments (thanks!)
- I'm getting careful reads, but not lots of new material. We might be finished. RGLC?
- We can certainly use -03 to guide our research and to discuss with the IETF
- My suggestion is to review Lessons Learned and **see what's still true** - **things change**
- ***^^ This is what I want to focus on, during this talk ^^***
- ***We're not wordsmithing - we have a mailing list and Github for that***
- ***This is the "are you out of your mind?!?" review by the Research Group***

I have suggested answers for whether each Lesson Learned is still true.
These are in blue boxes like this one, and are only Spencer's opinion.
I hope to capture your answers here (and on the mailing list) in a -04 revision

Un-summarized and Annotated "Summary of Lessons Learned" in -03

Overcoming Entropy for Already-Deployed Devices

- The benefit of Path Awareness must be great enough to overcome entropy for already-deployed devices. The colloquial American English expression, “If it ain’t broke, don’t fix it” is a “best current practice” on today’s Internet. (See Section 4.3, Section 4.5, and Section 4.4).

I think this one will always be true for Path Aware Networking
And probably for everything else

Providing Benefits for Early Adopters

- Providing benefits for early adopters can be key - if everyone must deploy a technology in order for the technology to provide benefits, or even to work at all, the technology is unlikely to be adopted. (See Section 4.2 and Section 4.3).

I think this one will always be true for Path Aware Networking
And probably for everything else

End-to-end Mechanisms That Work "Well Enough"

- Adaptive end-to-end protocol mechanisms may respond to feedback quickly enough that the additional realizable benefit from a new Path Aware mechanism may be much smaller than anticipated (see Section 4.3 and Section 4.5).

This one is worth talking about.
It's one of the key debating points in the LOOPS BOF we held Monday morning
A great deal has to do with whether there is more than one long path segment

"Follow the Money"

- “Follow the money.” If operators can’t charge for a Path Aware technology to recover the costs of deploying it, the benefits to the operator must be really significant. (See Section 4.5, Section 4.1, and Section 4.2).

I think this one will always be true for Path Aware Networking
And probably for everything else

Operational Practices Can Be Show-stoppers

- Impact of a Path Aware technology requiring changes to operational practices can prevent deployment of promising technology. (See Section 4.6, including Section 4.6.3).

This one is worth discussing, not because operator motivations have changed, but because we keep developing new ways to mask protocol mechanisms from analysis by middleboxes. See "Version-Independent Properties of QUIC" for perspective.

Per-connection State

- Per-connection state in intermediate devices can be an impediment to adoption and deployment. (See Section 4.1 and Section 4.2).

This one is worth discussing, because access routers and smaller/enterprise routers may be able to handle in-band mechanisms Just Fine.

In-band Mechanisms Can Fall Off The "Fast Path"

- Many modern routers, especially high-end routers, have not been designed to make heavy use of in-band mechanisms such as IPv4 and IPv6 Router Alert Options (RAO), so operators can be reluctant to deploy technologies that rely on these mechanisms. (See Section 4.7).

This one is worth discussing, because access routers and smaller/enterprise routers may be able to handle in-band mechanisms Just Fine.

Can the Network Path Trust Endpoints?

- If the endpoints do not have any trust relationship with the intermediate devices along a path, operators can be reluctant to deploy technologies that rely on endpoints sending unauthenticated control signals to routers. (See Section 4.2 and Section 4.7. We also note this still remains a factor hindering deployment of DiffServ).

We ABSOLUTELY need to talk about this!

Can Endpoints Trust the Network Path?

- If intermediate devices along the path can't be trusted, it's unlikely that endpoints will rely on signals from intermediate devices to drive changes to endpoint behaviors. (See Section 4.5, Section 4.4). The lowest level of trust is sufficient for a device issuing a message to confirm that it has visibility of the packets on the path it is seeking to control [RFC8085] (e.g., an ICMP message included a quoted packet from the source). A higher level of trust can arise when a network device could have a long or short term trust relationship with the sender it controls.

Can Endpoints Trust the Network Path?

- If intermediate devices along the path can't be trusted, it's unlikely that endpoints will rely on signals from intermediate devices to drive changes to endpoint behaviors. (See Section 4.5, Section 4.4). The lowest level of trust is sufficient for a device issuing a message to confirm that it has visibility of the packets on the path it is seeking to control [RFC8085] (e.g., an ICMP message included a quoted packet

We ABSOLUTELY need to talk about this!

Can the Network Provide Actionable Information?

- Because the Internet is a distributed system, if the distance that information from distant hosts and routers travels to a Path Aware host or router is sufficiently large, the information may no longer represent the state and situation at the distant host or router when it is received. In this case, the benefit that a Path Aware technology provides likely decreases. (See Section 4.3).

I think this one will always be true for Path Aware Networking
And probably for everything else

Do Endpoints Know What The Path Needs to Know?

- Providing a new feature/signal does not mean that it will be used. Endpoint stacks may not know how to effectively utilize Path-Aware transport protocol technologies, because the technology may require information from applications to permit them to work effectively, but applications may not a-priori know that information. (See Section 4.1 and Section 4.2).

I think this one will always be true for Path Aware Networking
And probably for everything else

Can the Endpoint Tell The Path What It Knows?

- Even if the application does know that information, the de-facto API has no way of signaling the expectations of applications for the network path. Providing this awareness requires an API that signals more than the packets to be sent. TAPS is exploring such an API [TAPS-WG], yet even with such an API, policy is needed to bind the application expectations to the network characteristics.

I suggest that we let TAPS run for a bit, and then return to this one. We have enough to do now :-)

Assuming this has gone well, so far ...

- We still have questions about some of the Lessons Learned
- We can investigate those questions
- We can use the Lessons we've Learned to guide our research
- (See relevant sections in draft-irtf-panrg-questions)
- We might talk about how the IETF hears about our Lessons Learned

Please Discuss