Path Aware Networking: Obstacles to Deployment (A Bestiary of Roads Not Taken) (draft-irtf-panrg-what-not-to-do-01)

Spencer Dawkins

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

- Gorry Fairhurst provided contributions on ST, ICMP Source Quench, and Flow Labels
- Gorry also performed a significant review of -00. All comments have been addressed
- Significant rewrite of Section 2 ("Summary of Lessons Learned")
- ***^^ 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***
  -

Un-summarized "Summary of Lessons Learned"

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).

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).

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).

"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).

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).

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).

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).

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).

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 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).

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).

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.

Assuming this has gone well, so far ...

- What other experiences should we capture, to add Lessons Learned?
- ... new contributions in -01 have been from INT
- ... we keep talking about reaching out to RTG - is that next?
- ... perhaps we don't have far to go, before declaring victory?
- Are we ready to start using this draft?
- ... perhaps filtering draft-irtf-panrg-questions and looking for gaps
- ... perhaps filtering IETF protocol work and looking for known snares

(At some point, the chairs should probably tell me to sit down!)