Position Paper for IAB SEMI Workshop

Brandon Williams *brandon.williams@akamai.com*

October 31, 2014

Within the IETF, there are widely divergent views on the role and value of middleboxes. Behaviors that are seen as obviously bad within one area of discussion might be seen as critical functionality not to be tampered with in another area. For example, recent discussions about the impact of NAT devices have focused on both the negative impact of breaking end-to-end semantics for addresses and port numbers, and on the positive impact hiding host identities from pervasive monitoring systems. Participants at once look forward to seeing these devices disappear from the internet and defend their existence as critical functionality not to be tampered with.

This mixed view of middleboxes is a pretty good representation of their role on the Internet today. They exist because they help to solve, or at least mitigate, recognized problems, but they frequently do so in ways that break functionality that falls outside their primary area of focus. The trouble they cause comes partially from a failure on the part of some middlebox designers to engage in discussions around protocol design and evolution, and partially from a failure on the part of some protocol designers to offer guidance to cooperative middelbox designers on the question of how to adequately support protocol evolution within their systems.

Due to the role they play, middleboxes will continue to be used on the Internet, and I suspect that their use will only increase. Likewise, it will continue to be the case that some middlebox designers will be slow to react to protocol evolution due to a lack of incentives, financial or otherwise, to support such evolution in their devices. Internet paths will continue to be heterogeneous in this regard. Attempts to find ways to circumvent the functioning of middleboxes in protocol designs or to find paths around them are reasonable approaches for limited experimentation, but not for broad adoption.

Instead, I think it's important to focus on capability detection for the Internet paths that are being used for transport. Paths can change over time, and resilience in the face of such changes is difficult to achieve through out-of-band monitoring. For this reason, capability detection and monitoring is something that I think is most effectively done in-band within the transport protocols themselves, with protocols of varying types (e.g. connection oriented vs datagram oriented) requiring different mechanisms.

I hope that one of the outcomes of this workshop can be a set of recommendations, perhaps in the form of BCP documentation, for how to do this type of capability detection within the transport protocols themselves. Such detection will often be passive, in that the middleboxes will not directly participate, but for the cooperative middlebox designers, I think it would be useful to develop methods for middleboxes to use to explicitly signal levels of protocol support when new or unrecognized features are encountered.