IETF 105 side meeting minutes – APN6

**Time**: Thursday, July 25, 2019, 8:30-9:45

**Location**: Notre Dame room

Note Well applies covering IPR etc.

Chairs: Zhenbin (Robin) Li and Daniel King

Facilitators: Shuping Peng

Minutes: Adrian Farrel

Slides are available through a link to GitHub on the Side Meeting wiki page:

<https://github.com/shupingpeng/IETF105-Side-Meeting-APN6>

<https://trac.ietf.org/trac/ietf/meeting/wiki/105sidemeetings>

**Agenda**

1. Admin (Chairs)
2. Problem Statement and Requirements (Zhenbin Li)
3. Application-aware Information Conveying
   1. Framework of App-aware IPv6 Networking (Shuping Peng)
   2. Firewall and Service Tickets (Tom Herbert)
   3. SRH Metadata for Simplified Firewall (Jim Guichard)
4. App-aware Services
   1. IPv6-based DetNet (Yongqing Zhu)
   2. SRv6 Path Segment (Fengwei Qin)
   3. IPv6-based IFIT (In-situ Flow Information Telemetry) (Tianran Zhou)
5. Shaping Our Discussion (Chairs and Room)
6. Wrap Up (Chairs)

**Minutes**

**2. Problem Statement and Requirements (Zhenbin Li)**

No comments

**3a a. Framework of App-aware IPv6 Networking (Shuping Peng)**

Harald Alvastrom - What is the security model? How to protect the network from users?

Shuping Peng – We have two solutions. For the host-side solution, it will require network authentication of the information encapsulated by the applications, while for the network-side solution, it will be under control of the network.

Qian Wu - TCP may use different algorithms for congestion control. Is this in scope?

Time limited, so it will be discussed offline.

**3b Firewall and Service Tickets (Tom Herbert)**

Aijun Wang - Ticket in EH option. This option is put in IPv6 header. Is there space to put this ticket in application layer (or UDP/TCP)?

Tom - We can do this in the operating system, as to minimize the work at the server side.

**3c SRH Metadata for Simplified Firewall (Jim Guichard)**

**4a IPv6-based DetNet (Yongqing Zhu)**

**4b SRv6 Path Segment (Fengwei Qin)**

**4c IPv6-based IFIT (In-situ Flow Information Telemetry) (Tianran Zhou)**

General comment from Chair (Robin), there are also many other example use case. These were just three.

**5. Shaping Our Discussion (Chairs and Room)**

- Chairs show the discussion slide

- Dan notes issues already raised: Security, congestion control conflicts

Spencer Dawkins - Points to PANRG draft on mistakes made on path-aware networking and technologies produced that have not been deployed. There is a section called "lessons learned" - an application may not know what information the network needs to know, and the API might not provide a mechanism to pass any information anyway. Recommends talking with PANRG.

Tom Herbert - Clarifying the problem will need to be a first step. TE and OAM can be separated out quite easily. That's the back-end and we have lots of work on this. The real new problem is "how do we map what the application wants to what the network is going to do?". It is opposite to the problems in PANRG.

Jim Guichard - Need to do a better job of framing the problems. The fact that PANRG was mentioned shows we haven't got this right. This is really about policy enforcement.

Frank Brockners - +1

As application developer, I don't care about how this is delivered by the network, but I do care about how I talk to the network. How do you provide a vehicle so people can use instrumentation at the application layer. How to make the application visible in the network?

Tall Mizrahi - ideas here are at the network layer, but need to be at the application layer. Security is really important and needs more than just a mention. Consider work in QUIC to minimize bits processed by middleboxes.

Brian Carpenter - missing from scope is "how much is supposed to operate across the internet and how much is supposed to be within a domain with a trust/security boundary?"

Jim Guichard - Yes that was my question to Tom. Bidirectional is hard to solve in the Internet because you can't guarantee return path uses same infrastructure as outbound path.

Tom Herbert - I don't like building protocols that only work in limited domains. But there are benefits in limited domains. If packets are confined to limited domains the security model is different and operator may be willing to expose more information. It is a use-case question. We have different use-case models and we should be able to adapt to any of them. In any case, security is important. How do you get a trust relationship such that information given to a 3rd party can be trusted.

**Charis Wrap Up with a poll to the room:**

- Who thinks "interesting area we should be working on in the IETF?"

- Good majority of the room (50+)

**Next Steps**

Chairs, we will set up an email list to continue the discussions.

**Attendees:**

1. Spencer Dawkins
2. Tom Herbert
3. John Kaippallimalil
4. Stewart Bryant
5. Brian Carpenter
6. Dhruv Dhody
7. Sri Gundavelli
8. Harald Alvestrand
9. Mike Ackermann
10. Nils Warnken
11. Qian Wu
12. Rakesh Gandhi
13. Tal Mizrahi
14. James Guichard
15. Xing Li
16. Adrian Farrel
17. Daniel King
18. Zhenbin Li
19. Shuping Peng
20. David Lou
21. Tianran Zhou
22. Sonum Mathm
23. Jeff Tantsura
24. Lin He
25. Dawei Fan
26. Miya Icohno
27. Remy Liu
28. Cheng Li
29. Lijuan Chen
30. Zle Chen
31. Guangpeng Li
32. Fengwei Qin
33. Peng Liu
34. Xuesong Geng
35. Hui Tian
36. Jianglong Wang
37. Bing (Leo) Liu
38. Sri Mohanna
39. Fenghua Zhao
40. Kentaro Ebisawa
41. (Google)
42. Jorge Rabadan
43. Mach Chen
44. Takuya Miyasaka
45. Jie Dong
46. Georgios Karagiannis
47. Satoru Matsushima
48. Hewu Li
49. Aijun Wang
50. Frank Brockners
51. Shwetha Bhandari
52. Shuai Zhao