IETF Hackathon

Secure Hybrid Network

IETF 122

15–16 March 2025

Bangkok, Thailand

Yutaka Oiwa and Hiro Nakanishi
Secure Hybrid Networking team

Motivation

- Use of hybrid clouds or hybrid network is now common
  - Connect multiple instances of networks and/or cloud services to compose a single system
    - e.g. Use an on-premise cloud for secure data vault, a public cloud for Web frontend
  - Connected by various means of interconnection paths, like VPN-secured path, VLAN/MPLS layer, overlay networks or leased line
- For system integrity, assurance of real-world "properties" of such interconnection paths are important
  - E.g. nodes on such a path are managed only by contracted operators
  - The path is going through the domestic country (legal region)

Our purpose, and benefit on our technology (1/3)

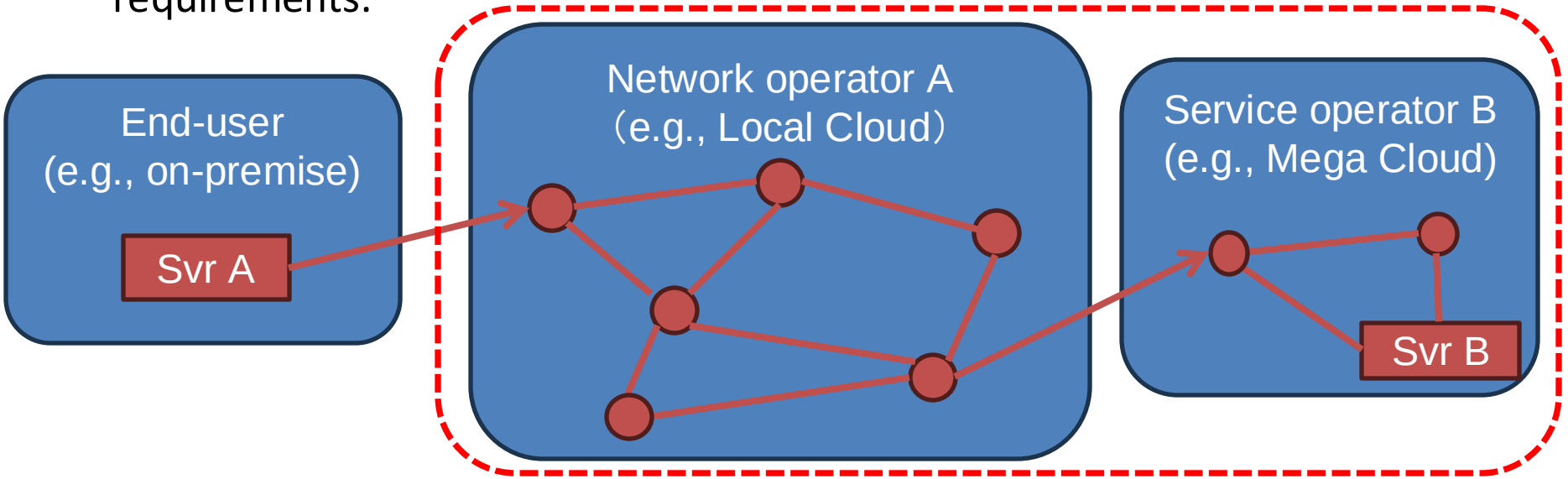
- Purpose
  - This technology supports **the monitoring of certain characteristics of communication paths** resulting from routing.
    - Examples of these characteristics include
      - Communication managed by a particular operator
        - » Communication restricted to a specific country (geographically constrained routing).
      - Communication routed through a designated VPN.

Our purpose, and benefit on our technology (2/3)

- Problem Statement
  - The modern Internet's complexity is currently addressed primarily through manual interventions.
    - Sources of complexity include diverse network environments, such as on-premise, private cloud, and public cloud deployments.
  - Achieving these communication path characteristics requires collaboration between multiple operators, necessitating a standardized and universally accessible protocol.

Complexity Example: Connectibity across diverse network environments, (on-premise, private cloud, and public cloud)

- The end-user has a service agreement only with Network Operator A, but requires assurance that the path properties to Service B meet their requirements.



Our purpose, and benefit on our technology (3/3)

- Design guideline
  - Minimize impact on existing protocols, devices and deployments.
    - This can be achieved through a monitoring-based approach.
  - Support multi-layer environments such as VPNs or overlays that might otherwise be "black boxes" (=> through monitoring).
    - This can be achieved through recursive application of the monitoring technique, enabling verification of characteristics even within nested environments (e.g., VPNs).
- Design
  - The design employs path-centric monitoring, focusing on the routing information associated along the communication path.

Wrap Up

Champions:

- Yutaka OIWA
  y.oiwa@aist.go.jp
- Hiro Nakanishi
- Satoru Kanno

First timers @ IETF/Hackathon:

- Hiro Nakanishi

For more details

Internet Draft

- Securing hybrid network - criteria and requirements

https://datatracker.ietf.org/doc/draft-oiwa-secure-hybrid-network/