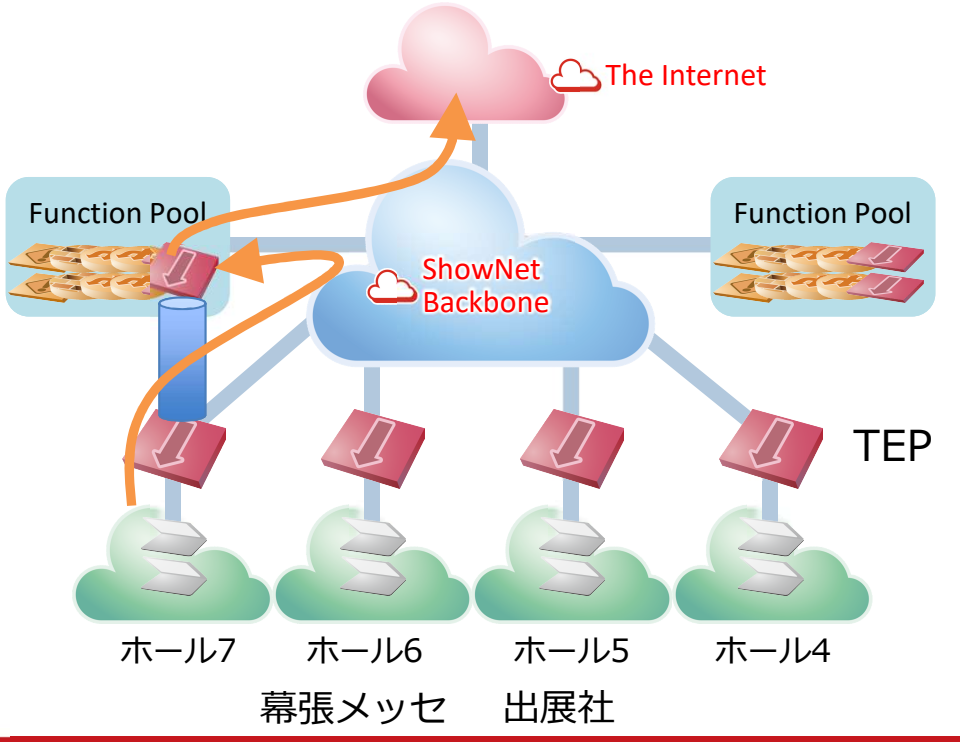
Interop Tokyo 2017
ShowNetにおける
サービスチェイニングの実装と運用

Interop Tokyo 2017
ShowNet NOC Team 大久保 修一

SHOWNET
INHERIT THE INTENTION

ShowNet2017 サービスチェイニング

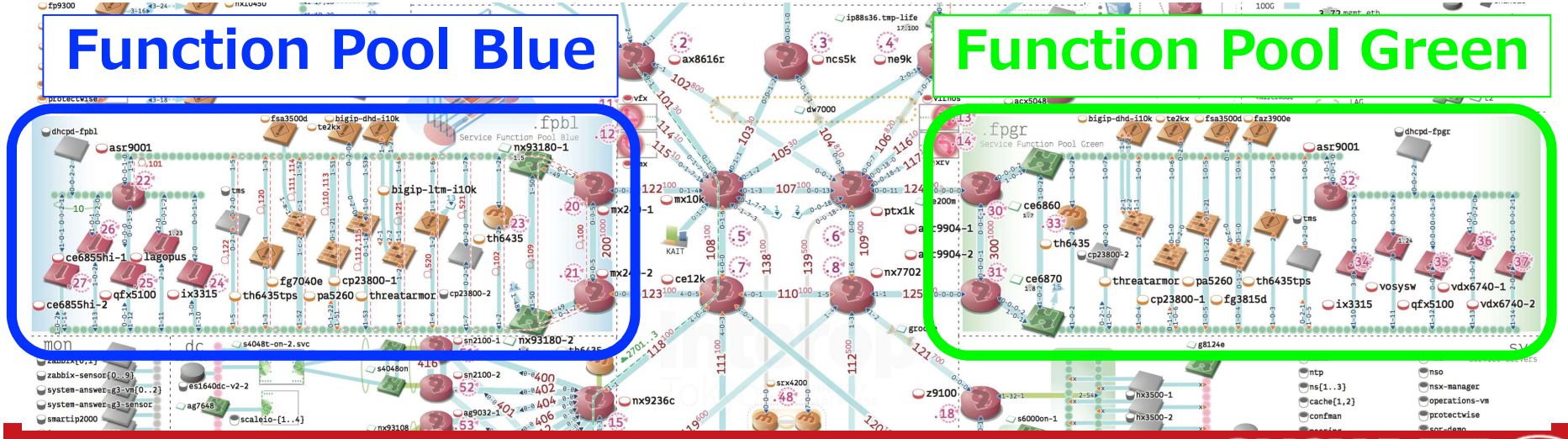
- 出展社に提供するインターネット回線において、セキュリティなどのネットワークファンクションを柔軟に選択可能に
- BGP FlowspecやEVPN/VXLANなど標準技術を用いて、マルチベンダによる構築
- ソフトウェアによる柔軟な制御、コアネットワークのシンプル化を実現



SHOWNET
INHERIT THE INTENTION

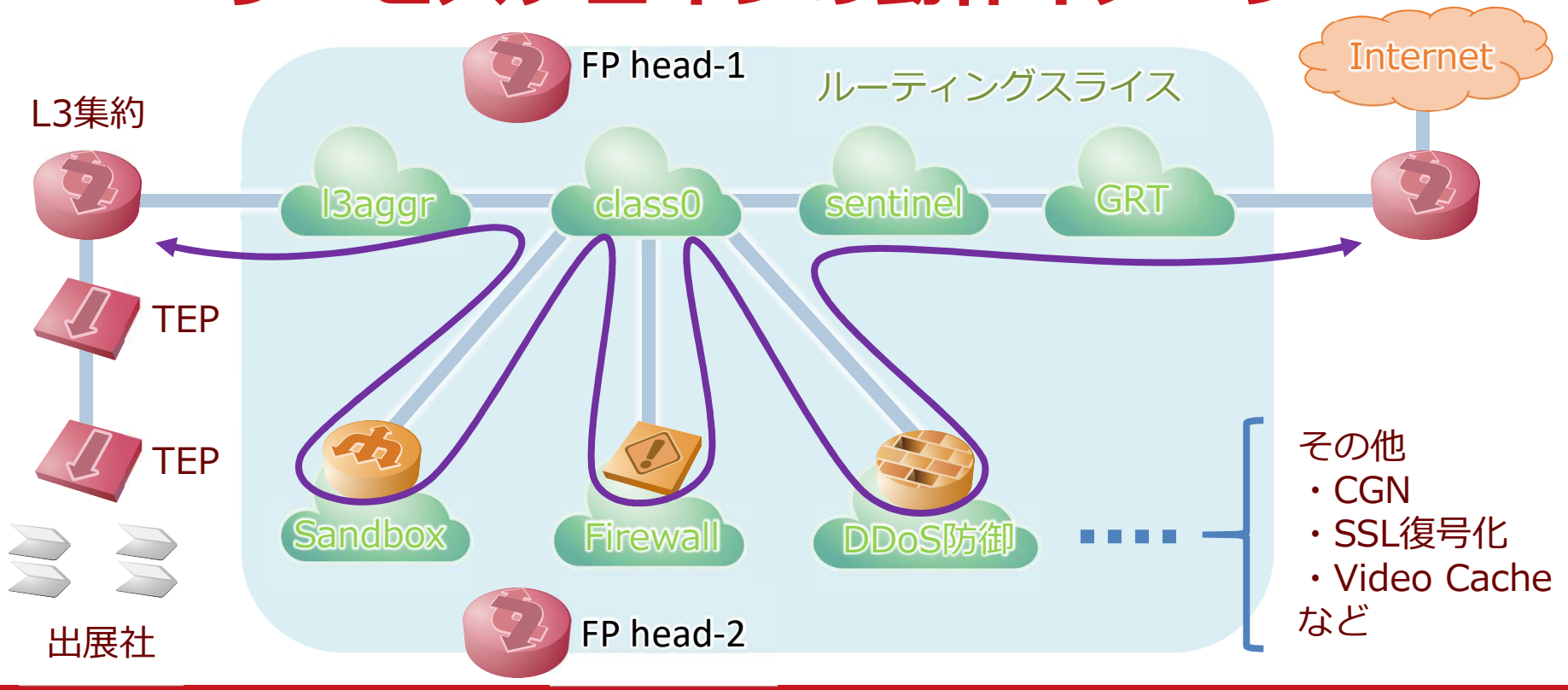
Function Poolとは

- Network Functionを集約したプール
- ShowNetでは冗長のため２つのFunction Poolを構築
  左右のFunction PoolをそれぞれBlue/Greenとし切り替え

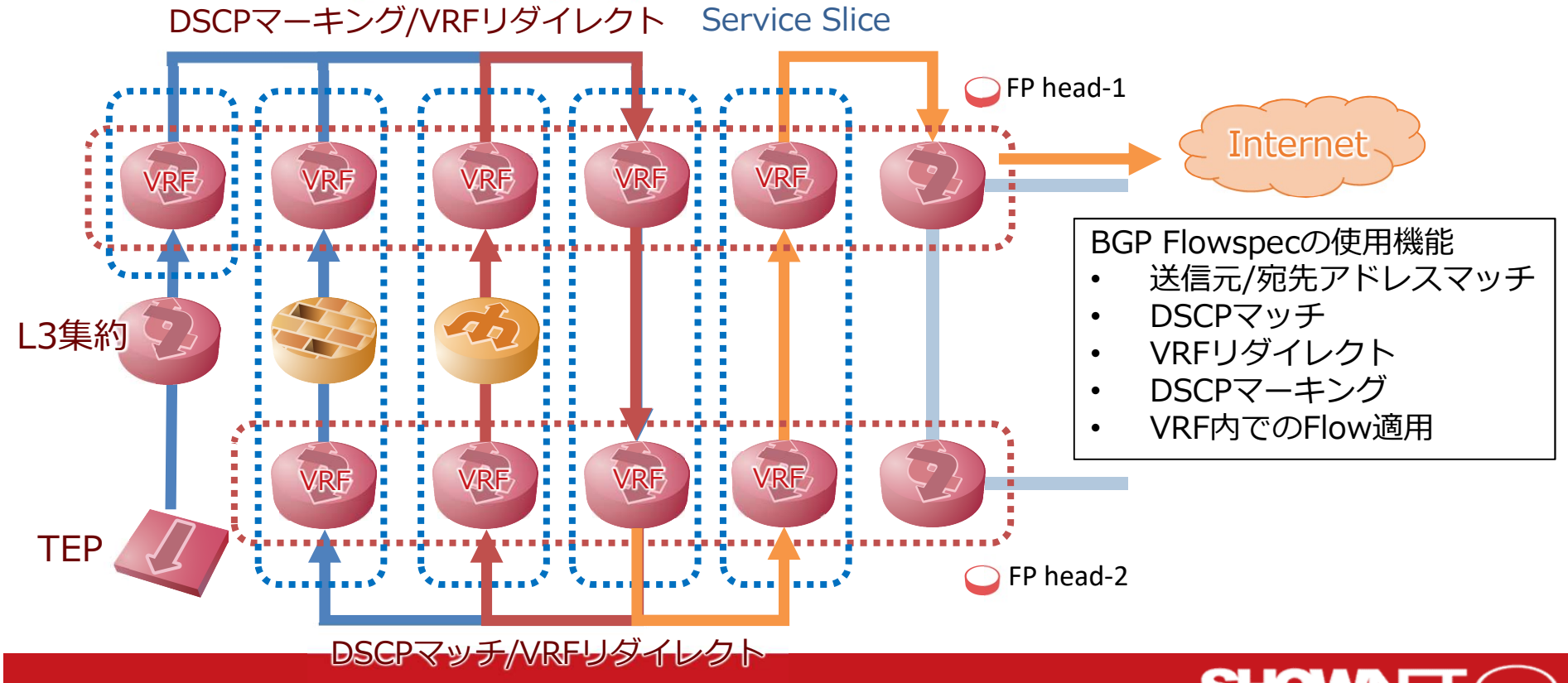


SHOWNET
INHERIT THE INTENTION

サービスチェインの動作イメージ



サービスチェインの動作概要

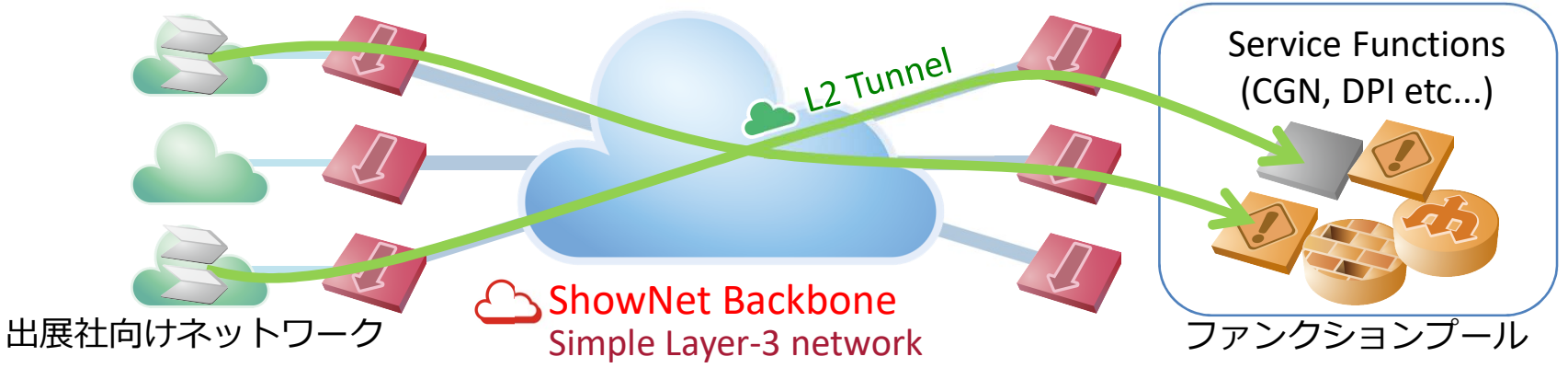


BGP Flowspecの使用機能
- 送信元/宛先アドレスマッチ
- DSCPマッチ
- VRFリダイレクト
- DSCPマーキング
- VRF内でのFlow適用

SHOWNET INHERIT THE INTENTION

出展社収容ネットワークのL2延伸

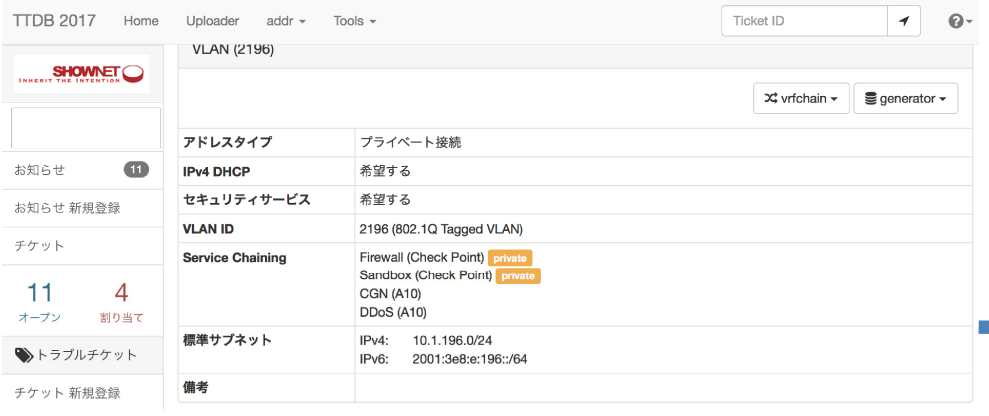
L2オーバレイ技術を用いて、出展社トラフィックをファンクションプールに集約

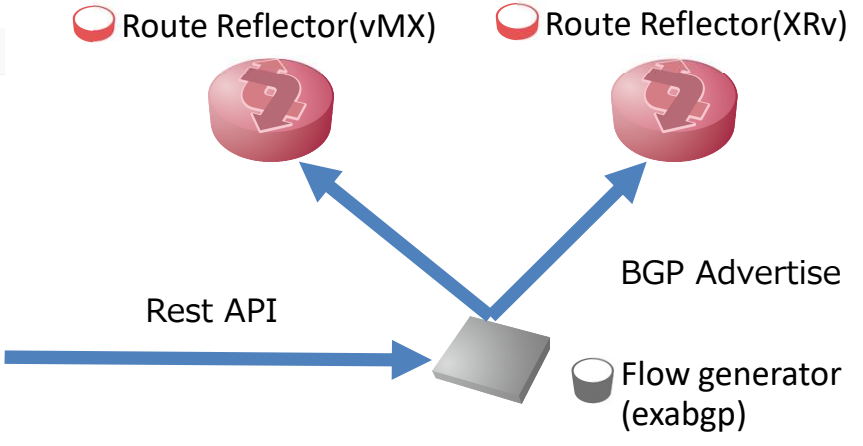


- EVPN/VXLAN – VLAN-Based方式
  - CE6855, VDX6740, NX9372, OCNOS
- Ethernet over GRE
  - Lagopus, VOS
- EVPN/VXLAN – VLAN-Aware Bundle方式
  - QFX5100, FX1
- EtherIP
  - IX3315

チェイン構成の自動化

- ShowNetの機器情報、出展社向け回線情報などを一元管理するデータベース(TTDB)とREST APIにより連携
- オーダーに合わせたBGP Flowspec経路を自動投入

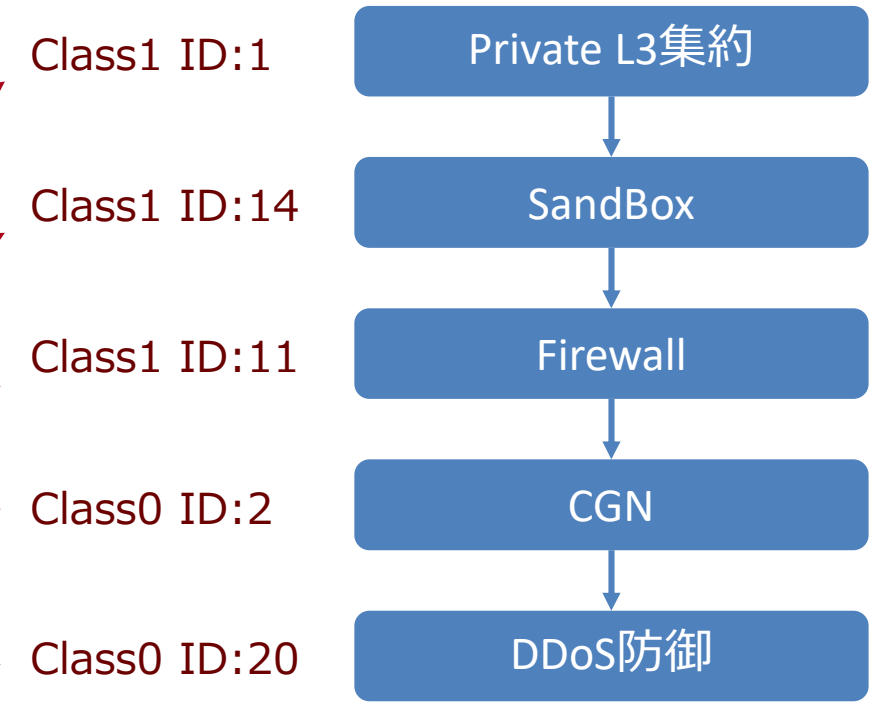




SHOWNET INHERIT THE INTENTION

REST APIリクエストボディの例

```
{
    "2058": {
        "prefix": {
            "class1": [
                "10.1.58.0/24",
                "2001:3e8:e:58::/64"
            ],
            "class0": [
                "130.128.255.58/32",
                "130.128.254.58/32",
                "2001:3e8:e:58::/64"
            ]
        },
        "command": "announce",
        "id": 2058,
        "functions": [
            {
                "class": 1,
                "id": 1
            },
            {
                "class": 1,
                "id": 14
            },
            {
                "class": 1,
                "id": 11
            },
            {
                "class": 0,
                "id": 2
            },
            {
                "class": 0,
                "id": 20
            }
        ]
    },
```



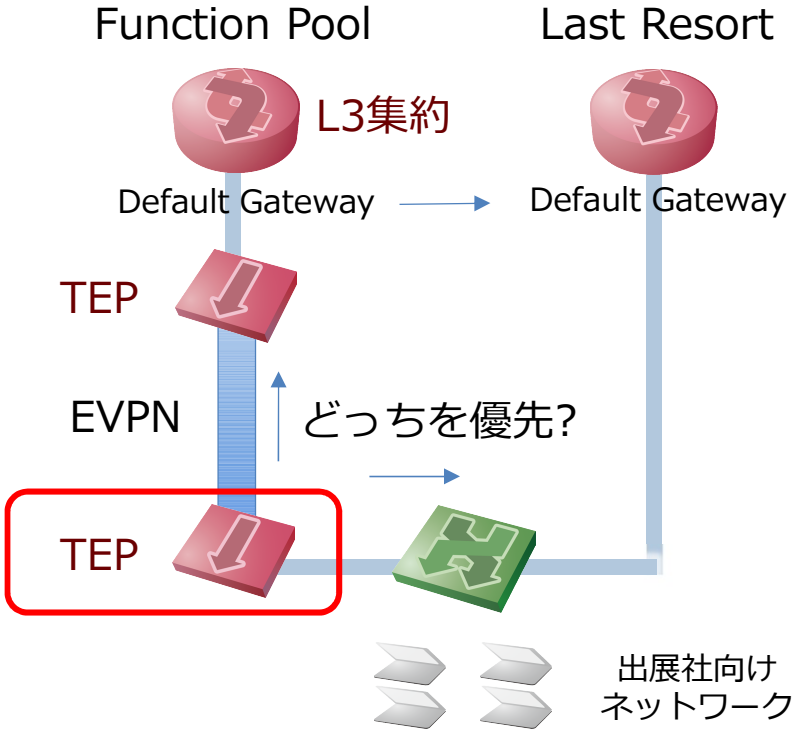
サービスチェイン動作の検証

```
My traceroute  [v0.86]
Host                                                    Loss%   Snt   Last   Avg  Best  Wrst StDev
<snip>
 4. 10.0.2.137
 5. 10.0.2.42
 6. 10.0.2.161
 7. 10.0.2.42
 8. 10.0.2.61                                           0.0%    10    1.8   1.9   1.7   2.1   0.0
 9. vrf-cgn.class0.mx240-1.fpbl.interop-tokyo.net       0.0%    10    2.1   2.0   1.7   2.3   0.0
10. vrf-redirect.class0.mx240-2.fpbl.interop-tokyo.net  0.0%    10    2.0   5.9   1.9  37.9  11.3
11. vrf-ddosmg-a10.class0.mx240-1.fpbl.interop-tokyo.net 0.0%   10    3.2   2.3   1.8   3.2   0.0
12. vrf-redirect.class0.mx240-2.fpbl.interop-tokyo.net  0.0%    10    2.2   8.5   2.0  40.5  13.8
13. vrf-sentinel.class0.mx240-1.fpbl.interop-tokyo.net  0.0%    10    3.2   2.4   2.0   3.2   0.0
14. 45.0.1.89                                           0.0%    10    2.4   4.6   2.3  16.8   4.8
15. 45.0.1.5                                            0.0%    10    3.6   3.6   3.1   4.2   0.0
16. 218.100.6.173                                       0.0%    10    3.2   3.2   3.0   3.6   0.0
17. 108.170.242.193                                     0.0%     9    3.6   3.7   3.5   4.2   0.0
18. 216.239.54.21                                       0.0%     9    3.6   3.6   3.4   3.7   0.0
19. google-public-dns-a.google.com                      0.0%     9    3.6   3.2   3.0   3.6   0.0
```

各VRFのIPアドレスの逆引きにFunction名を記載
疎通確認の際にチェインの確認を容易に

EVPN Remote/Local MACの注意

- 最終フォールバック先として”Last Resort”を準備
- 通常時は閉塞状態にしておく
- Last Resort側に倒すと、Default GatewayのMACがEVPN経由とLocal側の両方に見える
- Local側を優先する実装がほとんどのため、Last Resort側に倒すとすんなり戻せない



まとめ

- レイヤ3でのサービスチェイニングを「いま動く」仕組みを用いて実装
- 枯れた標準技術のみを使用することで安定性の確保、および障害時の自動フォールバックによる高可用性を実現

special thanks

- Router(VRF + BGP Flowspec)
  - **Juniper** MX240
  - **Cisco** ASR9904
- Switches
  - **Cisco** Nexus 93180
  - **Huawei** Cloud Engine 6860, Cloud Engine 6870
- Tunnel End Points
  - **Huawei** Cloud Engine 6855hi
  - **Brocade** VDX6740
  - **Juniper** QFX5100
  - **NEC** IX3315
  - **日本電信電話** Lagopus
  - **Virtual Open Systems** ARMv8 CPE
- Tunnel End Points(cont.)
  - **古河電気工業株式会社** FX1
  - **Cisco** Nexus 9372
  - **Dell** S4048-ON
  - **IP Infusion** OCNOS
- Network Functions
  - **A10 Networks** Thunder 6435
  - **NEC** Traffic Management System
  - **Cisco** ASR9001
- Security Functions
  - **Fortinet** FortiGate-7040e, 3815d, FortiSandbox3500d
  - **PaloAlto Networks** PA5260, WildFire
  - **Checkpoint** 23800, TE2000X
  - **IXIA** ThreatARMOR
  - **NTT-AT** Herculon DHD i10800, BIG-IP LTM i10800
  - **A10 Networks** Thunder 6435 TPS

ご清聴ありがとうございました