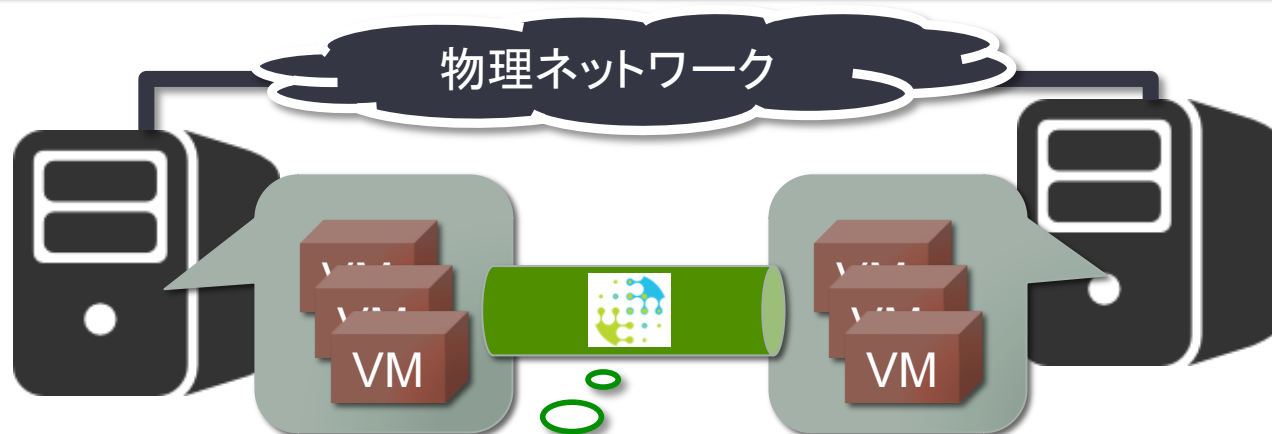


クラウドネットワーク屋の 悩み

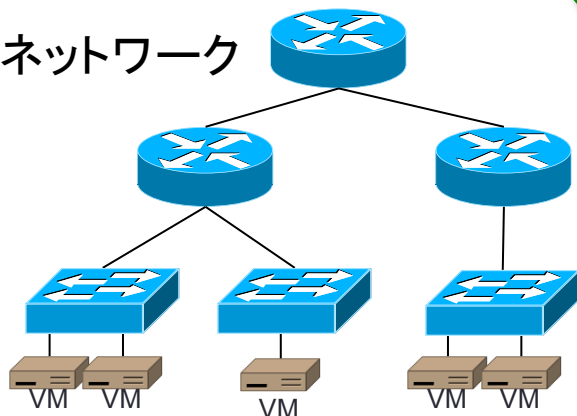
ミドクラジャパン株式会社
高嶋隆一

現在のお仕事

クラウドネットワークの仮想化



論理ネットワーク



VMとVMを繋げる
簡単なお仕事

どんなネット ワーク?

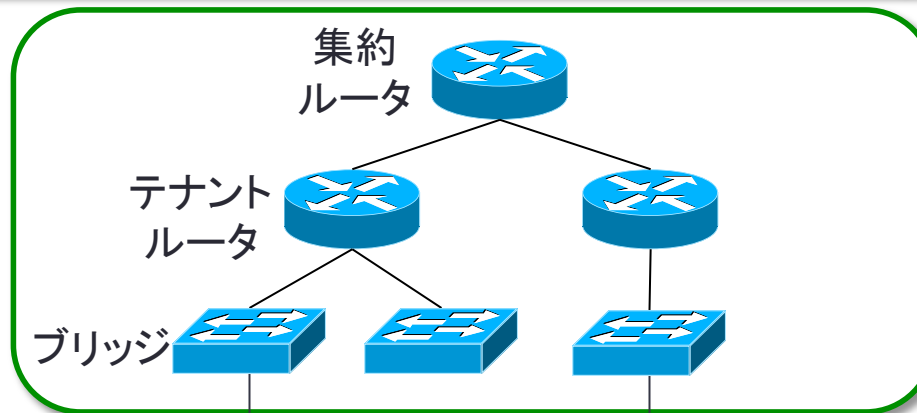


Edge Overlay

物理トポロジ



VMの仮想ポートを境界として物理ネットワーク上に仮想ネットワークを構築 (Overlay)

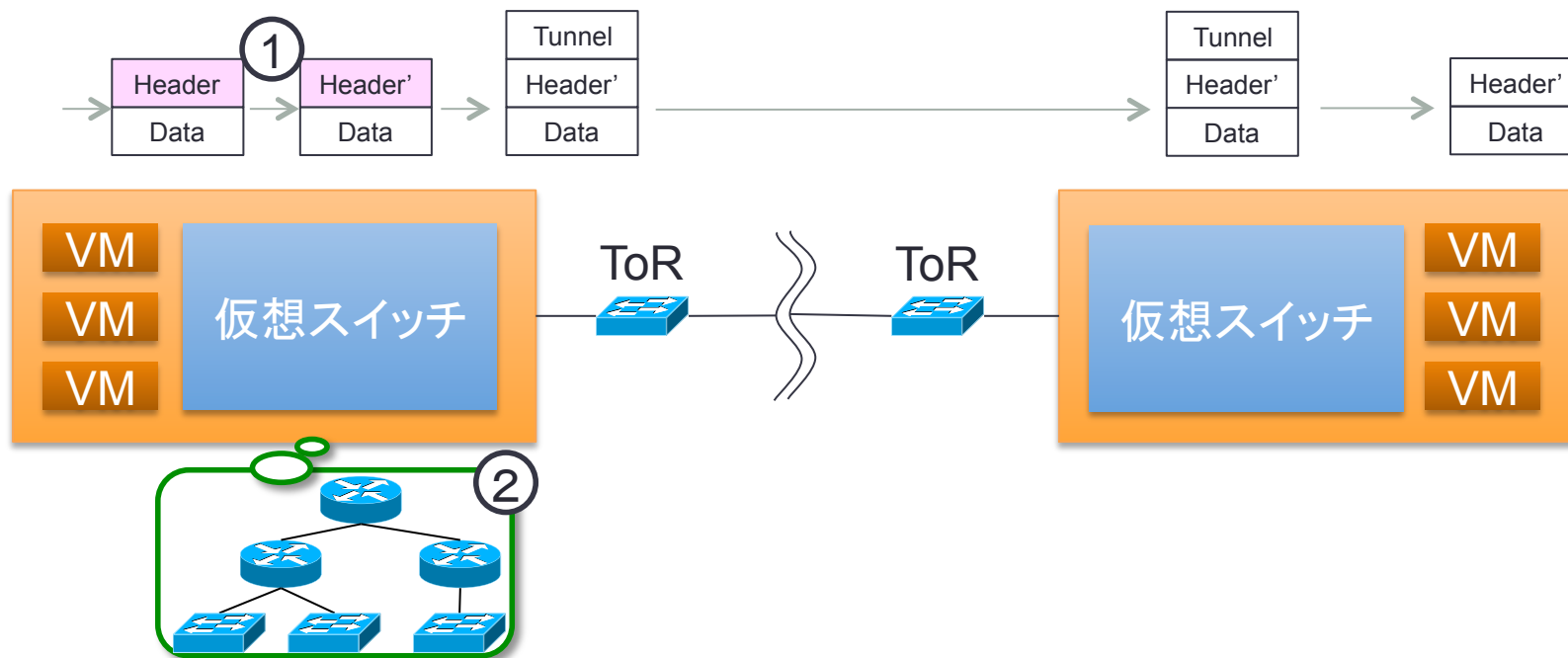


VM

VM

仮想トポロジ

ややこしいところ



① ヘッダの書き換えが生じる ※

② 「経由したこと」にしている仮想トポロジ上のデバイスはヘッダ書き換えの材料であり、VMとしても存在しない

※ L3跨ぎによる MAC Address, IP TTL の書き換えや
NAT, LB による IP Address 書き換え等



新たな悩み

Photo Credit: [ixos](#) via [Compfight cc](#)

課題1. 対話的OAMツール

従来の障害対応

エンド、ネットワーク機器を含め、Hop-by-Hop で確認

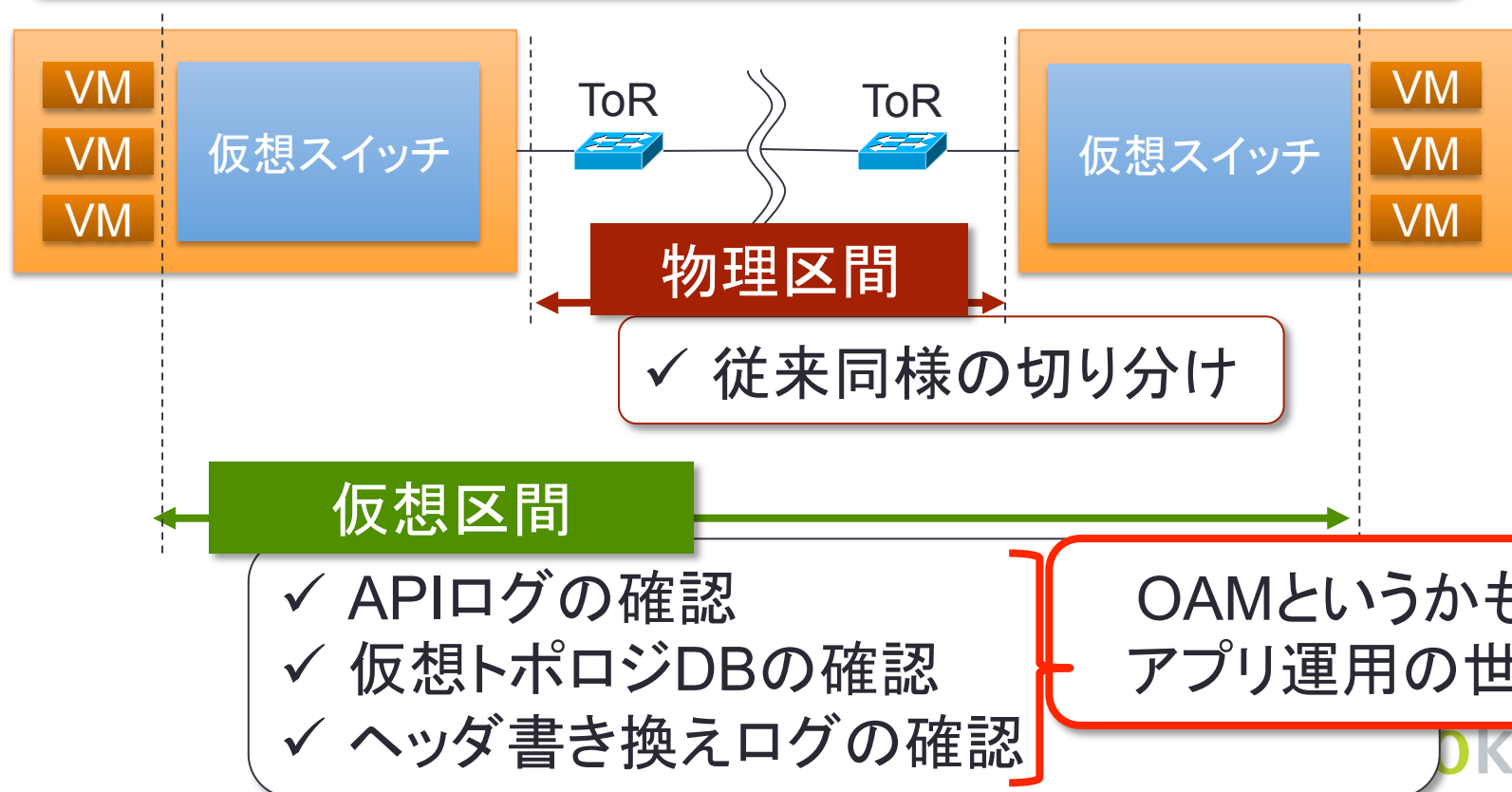
OAMツール

- ✓ Ping
- ✓ Traceroute
- ✓ Router CLI (show ip route 等)
- ✓ パケットキャプチャ

課題1. 対話的OAMツール

Server-side Edge Overlay

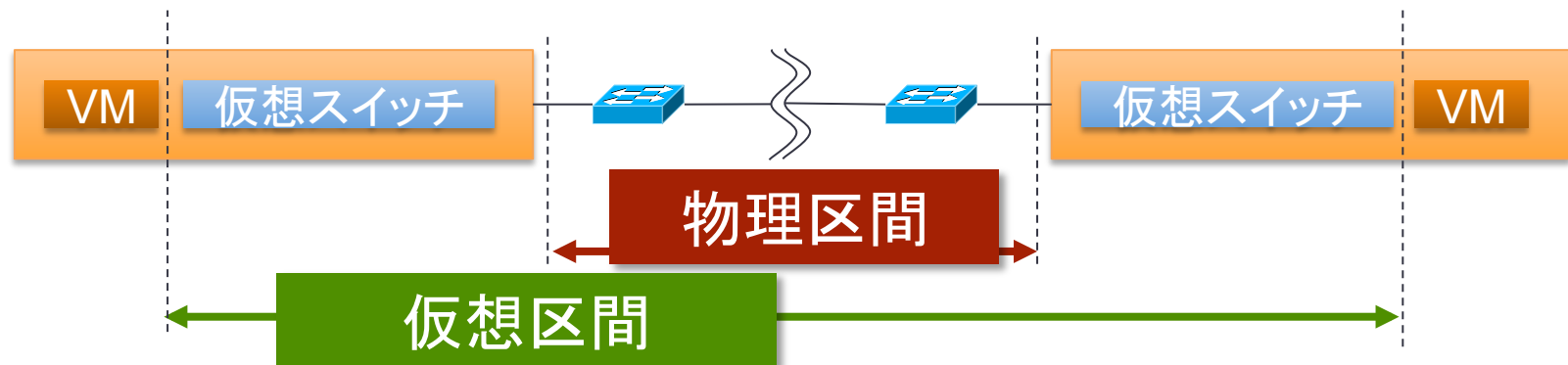
物理区間に加え、仮想区間固有の切り分けが必要



課題2. 定常監視

定常監視の問題点

- ✓ 物理区間と仮想区間どちらが壊れているか
- ✓ 影響範囲の特定



課題2. 定常監視

対応案

Ether-OAM ?

- 階層化の概念がある
- × L3跨ぎやヘッダ書き換えに対応できない

ICMP ?

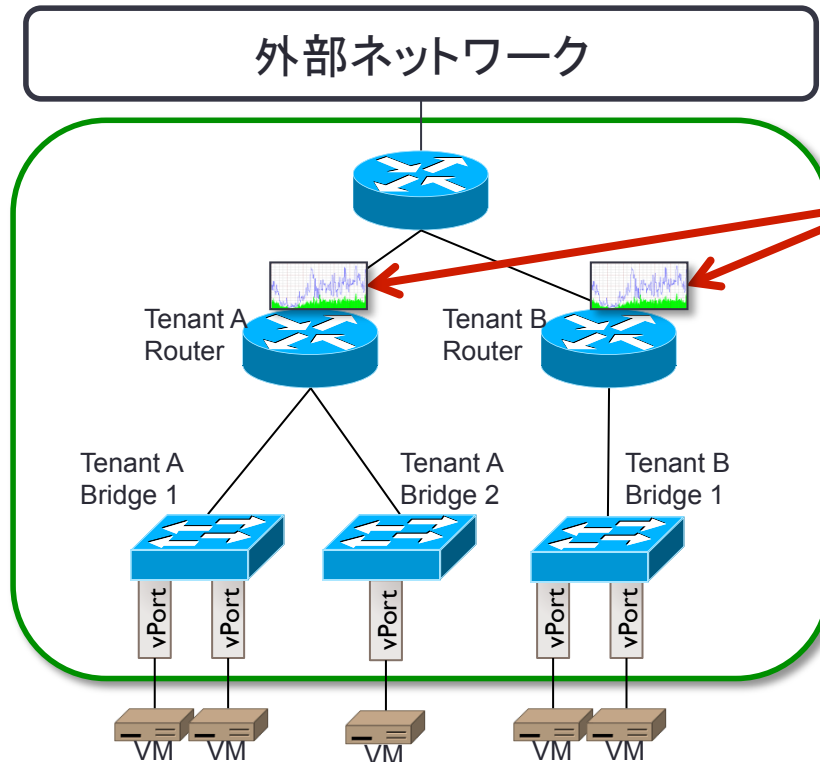
- × 階層化の概念がない
- × 監視の source, destination の定義が難しく、メッシュ監視になってしまう
- 外部接続等、特定区間ならよいかも?

- ✓ 結局の所、監視サーバから全て polling する位しか現実的な手段がない
- 接続性の監視や故障箇所特定には不十分

課題3. 統計情報の可視化

要求

課金やキャパシティ管理の為、
顧客ごとにトラフィック情報を取得したい



従来

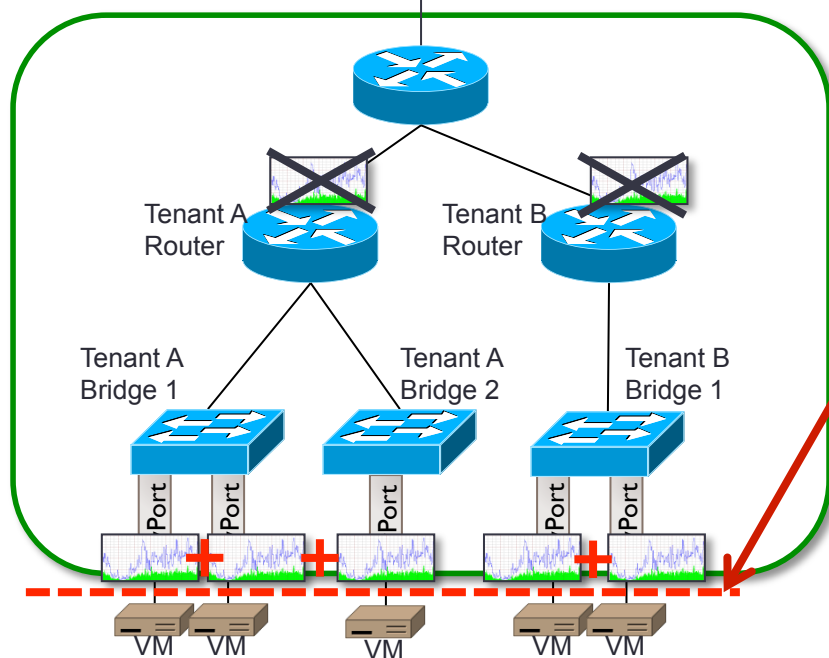
ルータの Uplink の
統計情報を取得

課題3. 統計情報の可視化

Server-side Edge Overlay

ルータは実際には存在しない為、同じ手段が使えない

外部ネットワーク



対応例

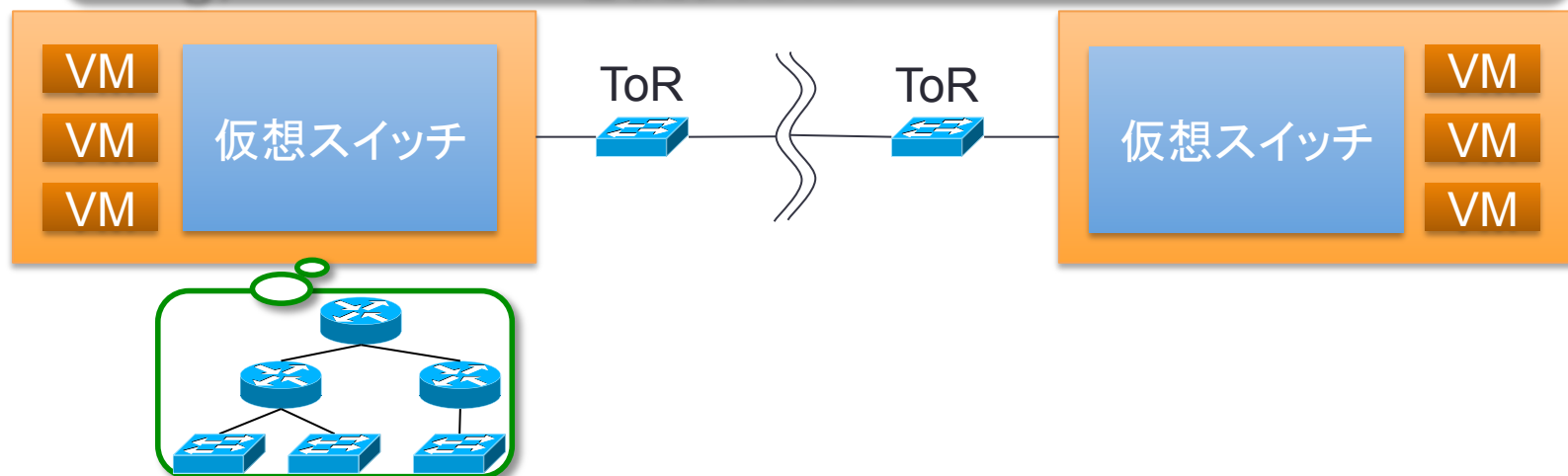
VM を收容する tap interface
の統計情報の集計

- ✓ 集計処理が必要
- ✓ テナント内折り返しも集計されてしまう

課題4. 従来との互換性

要求

エンドユーザの VM へは従来通りに
Ping, Traceroute を提供したい



- 「経由したこと」にしている仮想トポロジ上のデバイスはヘッダ書き換えの材料であり、VMとしても存在しない
- Ingress の仮想スイッチが Ping , Traceroute を処理する事はできるが、意味はあるのか ... ?

結論はありませんが...

- ✓ Server-side Edge Overlay でなくても IaaS や仮想化をとりいれたシステムは大なり小なりおなじ課題を抱えてるはず

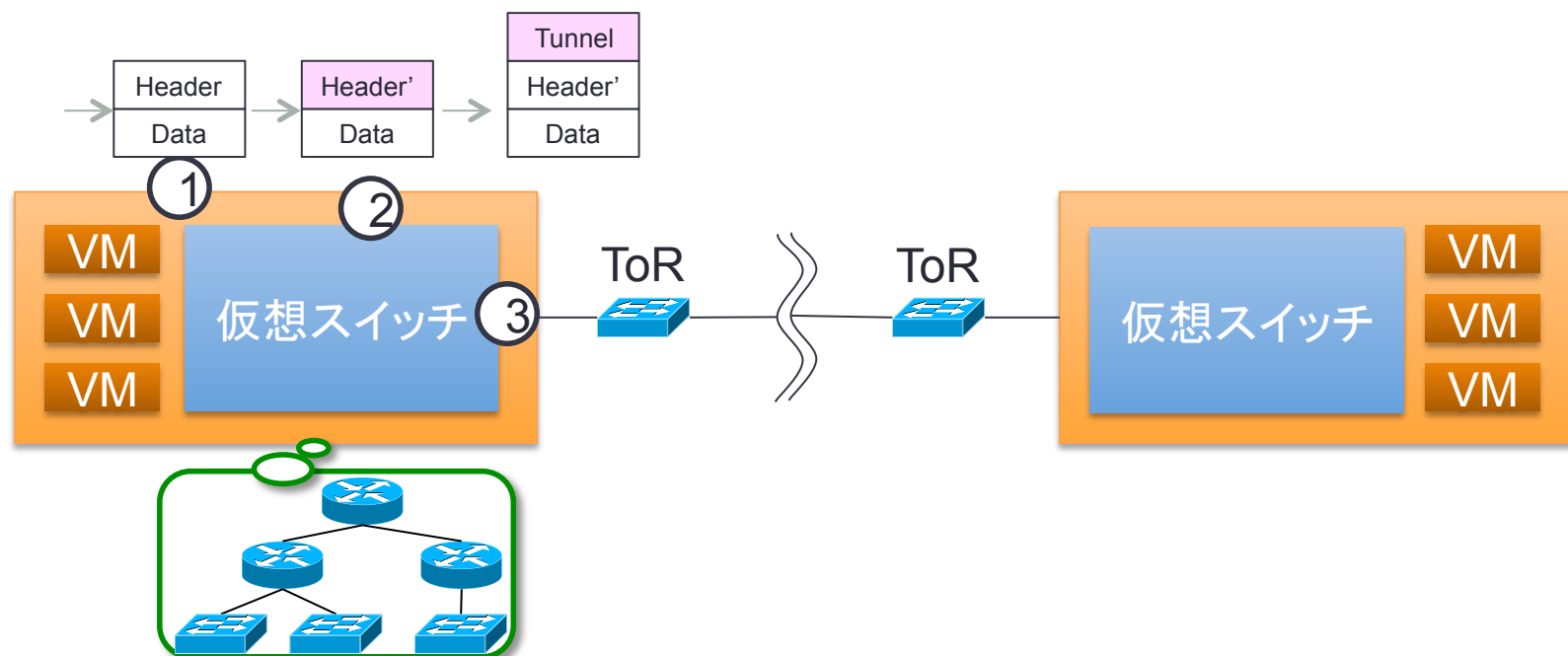
みなさん、
どうしてですか？

NEXT: 大山さん



APPENDIX

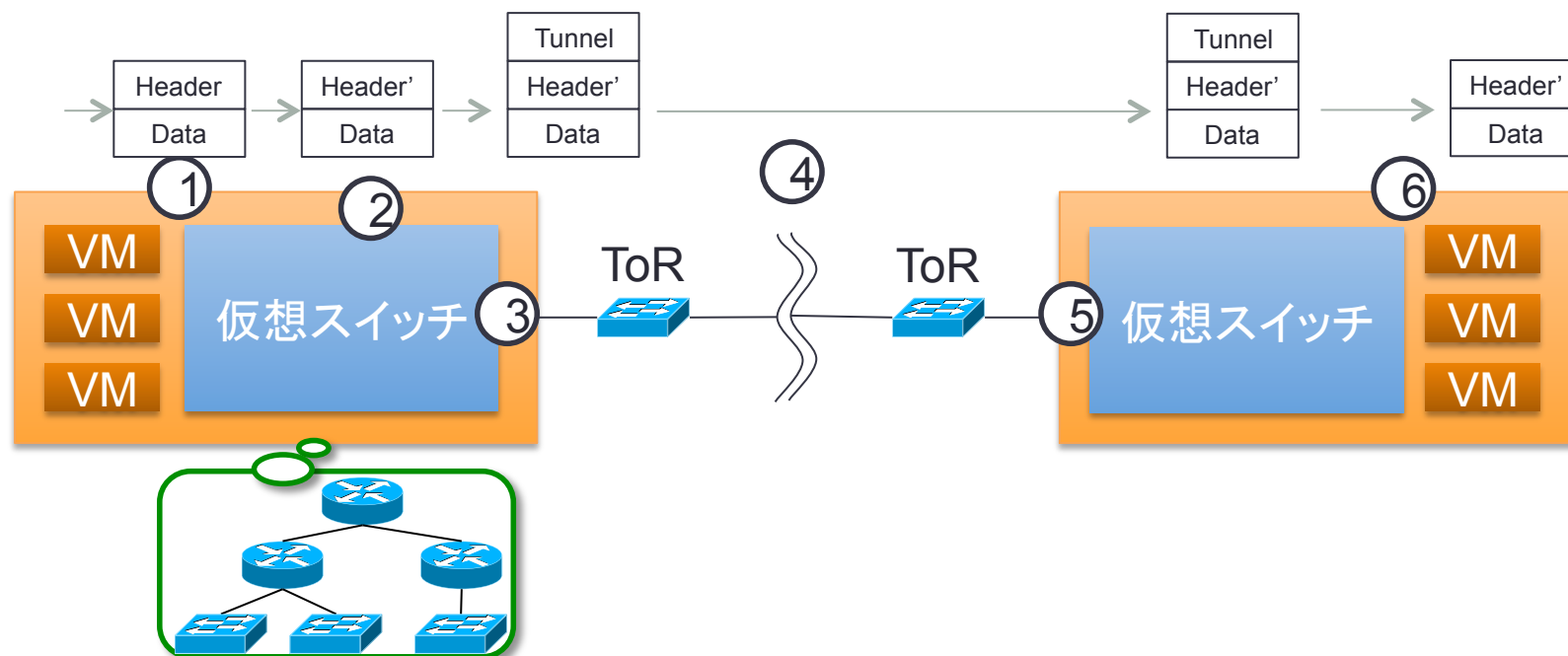
Server-side Edge Overlayの動作



- ① VMがパケットを送信
- ② 仮想スイッチが「こういうネットワークがある」ことにしてヘッダを書き換え ※
- ③ トンネルヘッダを付与して物理ネットワークに送信

※ ルータ越えによる MAC Address, IP TTL や NAT, LB による IP Address 書き換え等

Server-side Edge Overlayの動作



- ④ トンネルヘッダに従い物理ネットワークを配送
- ⑤ 仮想スイッチがトンネルヘッダ付きの packets を受信
- ⑥ 仮想スイッチがトンネルヘッダを除去してVMに送信

VM間では物理ネットワークの制約は受けず、
仮想ネットワークを経由した様に見える