Stratosphere

IRS23発表資料

SDNのセキュリティ

株式会社ストラトスフィア
石黒 邦宏 <ishiguro@stratosphere.co.jp>
永尾 禎啓 <nagao@stratosphere.co.jp>

2012.08.22

株式会社ストラトスフィア

Stratosphere

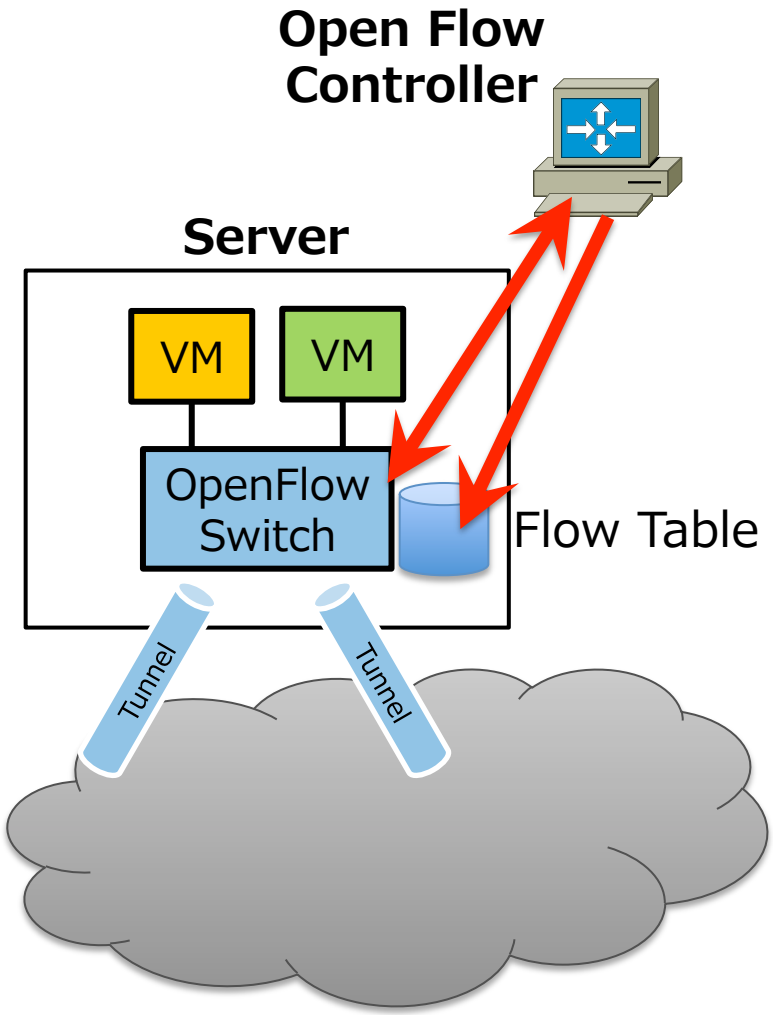
フローテーブルの爆発

フローテーブルの爆発

Stratosphere

OpenFlowスイッチの
(ありそうな)動作モデル

1. 仮想スイッチが未知のパケットを受信
2. OpenFlow コントローラに問い合わせ
3. 転送先ポートをコントローラが計算
4. 仮想スイッチにフローを投入
   - フロー = L2~L4のヘッダ情報(アドレス、プロトコル種別、ポート番号、…)によるマッチングルールとアクションの組
   - 今後同じパケットを素早く処理するため



フローテーブルの爆発

Stratosphere

このモデルの懸念点

- DDoS や spoofing 等で大量のパケットを投げ込まれた場合
- 投入するフローのマッチング部が詳細(下位～上位レイヤのヘッダフィールドまで広く覗く)すぎると…
  - どれもこれも初見のパケット
  - スイッチのフローテーブルに大量のエントリ投入

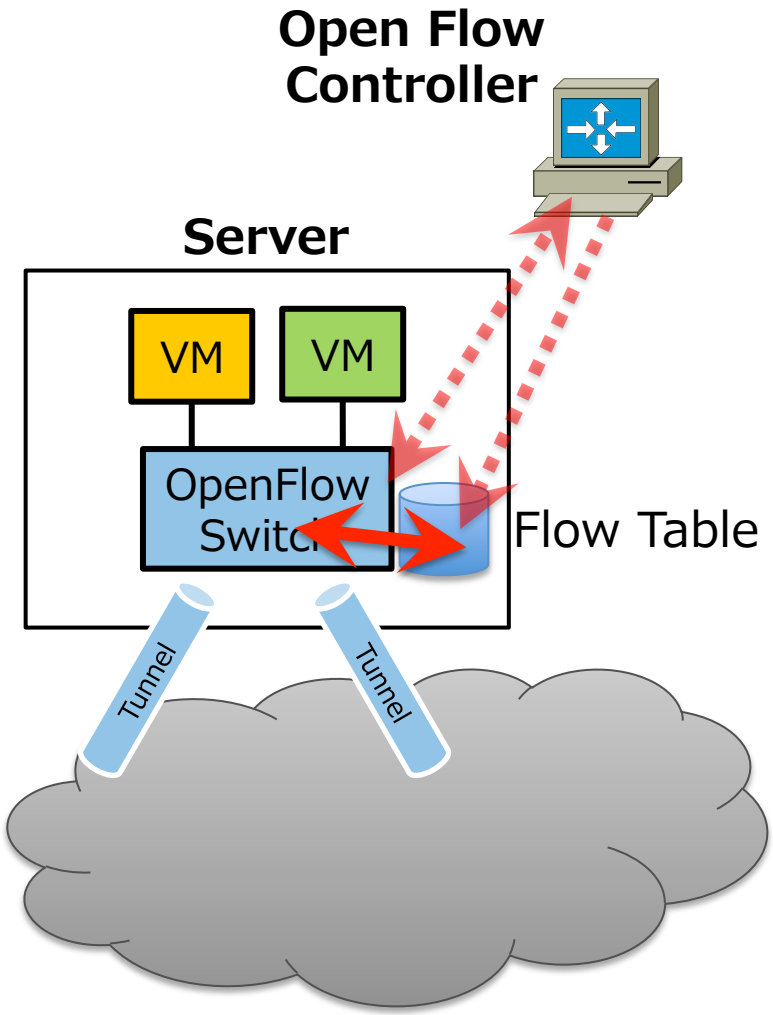
スイッチ動作の性能低下
コントローラの過負荷

フローテーブルの爆発

Stratosphere

Stratosphere の動作モデル

1. 仮想スイッチにあらかじめ static なフローを登録
   - 物理スイッチ相当の動作をルール化
2. 仮想スイッチが「MACアドレス学習」として自律的にフロー追加(timeout付き)※
3. OpenFlow コントローラへの転送は ARP ブロードキャストなど少数のケースのみ



(※ Open vSwitch における Nicira 拡張)

フローテーブルの爆発

Stratosphere

Stratosphere のモデル

- 基本的にMACアドレス学習によるフロー追加のみ
- 投入するフローのマッチング部はL2ヘッダレベルまで

- **VMにMACアドレス詐称を許さないフィルタを入れる運用なら、そもそも爆発しない**
  - 予備試験で、100万フロー登録した状態でもスループットに目に見える影響あらわれず
- コントローラの負荷低減
  - コントローラが暇であれば、そのぶん冗長構成での切り替え時間にも余裕が出てくる

フローテーブルの爆発

Stratosphere

ポイント

- できるだけフローを増やさない
  - static なフローの活用
  - 動的に追加する場合でも、あまり多くのヘッダフィールドをマッチ対象にしない
    - フィールドが多ければ、それだけフローのバリエーション増える
  - アドレス詐称防止の導入を検討
    - 流れるパケットに制限を加えることで、バリエーションが抑制される

OpenFlow Controller

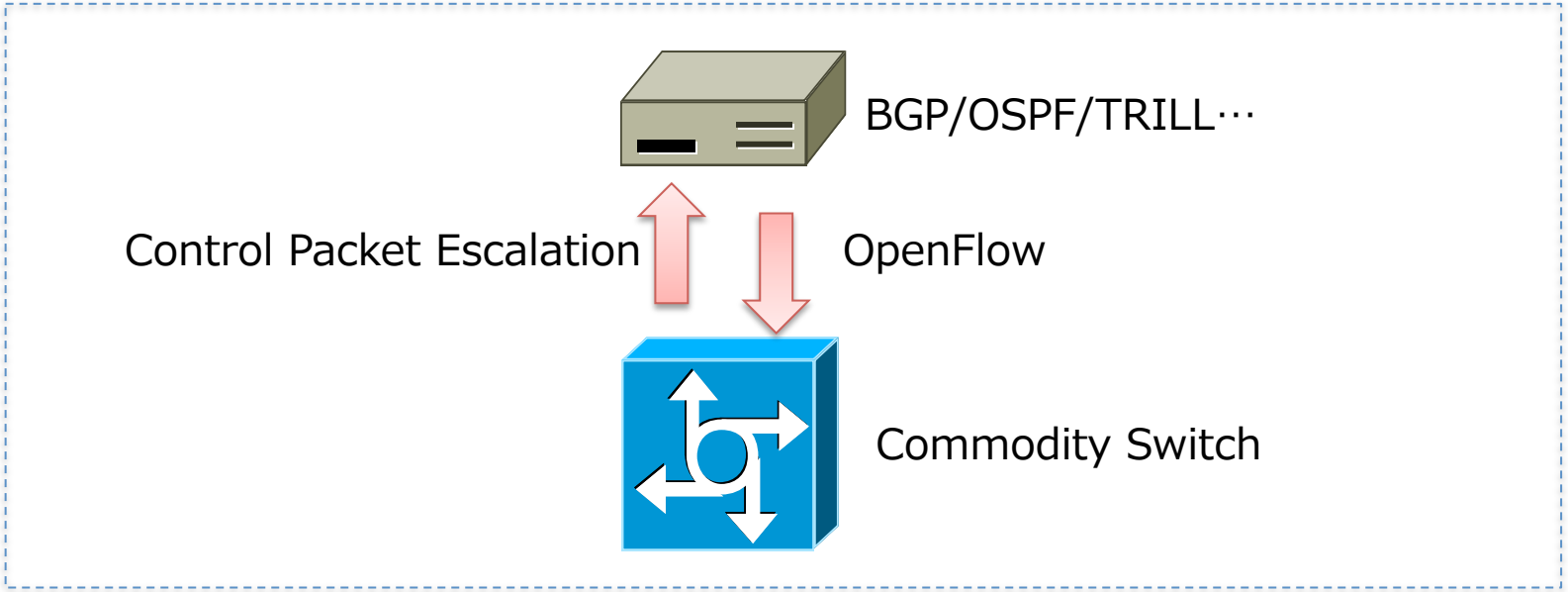
Stratosphere

- スペック上は生TCPかTLS
- たいていPort6633番で待っている
- 油断して、生TCPでControllerを上げていると。。。。。

SDN Fabric

Stratosphere

- OpenFlowを使用したFabric Switch/Router
  - BGP/OSPF/TRILL等のコントロールパケットをサーバーへエスカレーション
  - 生成されたFIB等をOpenFlowでCommodity Switchへインストール
  - OpenFlow接続をハイジャックされると。。。



SDNでの障害検知の課題

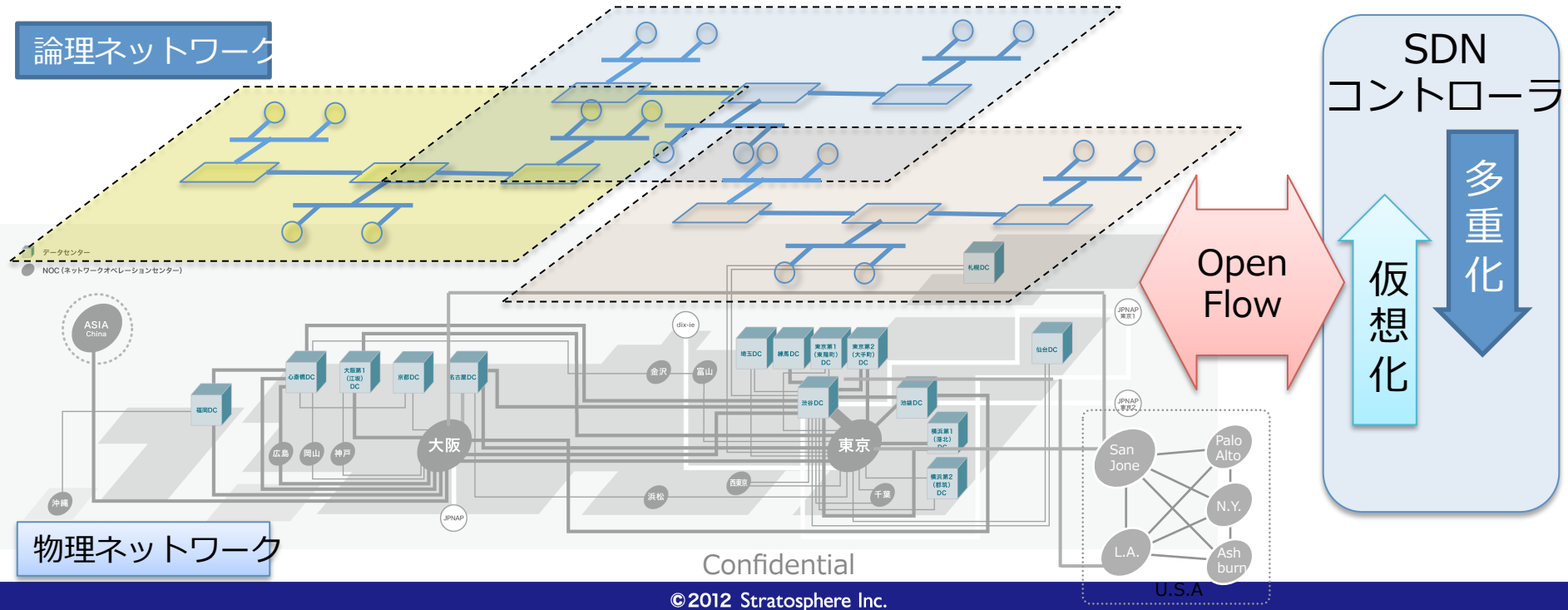
Stratosphere

- 仮想化に伴う障害検知の課題
  - 物理レイヤーと仮想レイヤーのマッピング
  - ネットワーク記述をするためのオブジェクトモデル
- 既存IP網とSDN網両方を統一的に管理する必要が出てくる可能性がある
  - IP Prefix
  - MPLS
  - VLAN
  - Flow
- VXLAN等のトンネル
  - コネクションレストンネル
  - 自動学習をすると時系列で設定が変化

物理ネットワークと論理ネットワーク

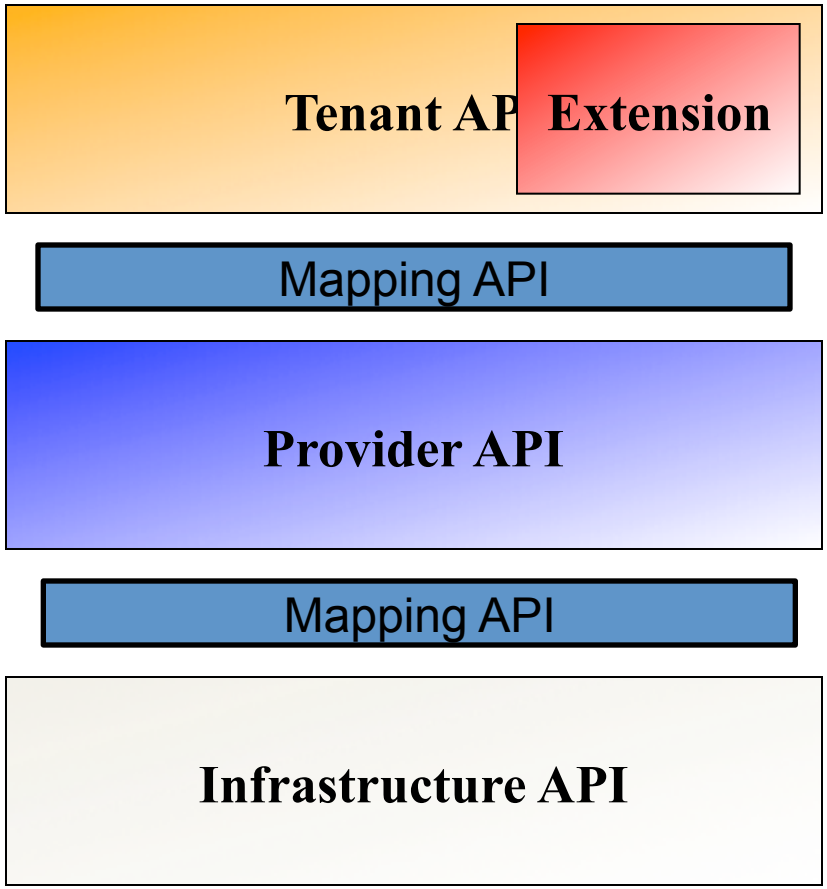
Stratosphere

- 障害時に物理と論理のマッピングの必要がある
- VXLANの場合コネクションレス
- OAMを入れるか？Ethernet OAM, BFD…



3層APIモデル

Stratosphere



- テナントユーザ向け
- テナントネットワークの構築
- Amazon EC2ライク
- 拡張API

- 2次プロバイダ向け
- マルチテナント対応プロバイダネットワークの構築
- QoS / TEを考慮
- ゾーニング

- クラウド/DC事業者向け
- DCネットワークの構築
- 物理ホスト／ネットワーク設定

時系列での変化

Stratosphere

- VXLAN/NVGRE
  - コネクションレストンネル
  - 自動学習するケースもある
  - 時系列でパケットフローが変化する
- 何月何時何分にどうなっていたか？
  - 時系列でのネットワーク設定の再現
  - Net Objectsでのネットワークトポロジーの録画