



CloudStack環境における ネットワーク要件と実装その現状と今後

MPLS Japan 2012

Technology Evangelist

Shinichi MURAKAMI

Sr. Manager Enterprise Sales

Citrix Systems Japan K.K

October, 2012

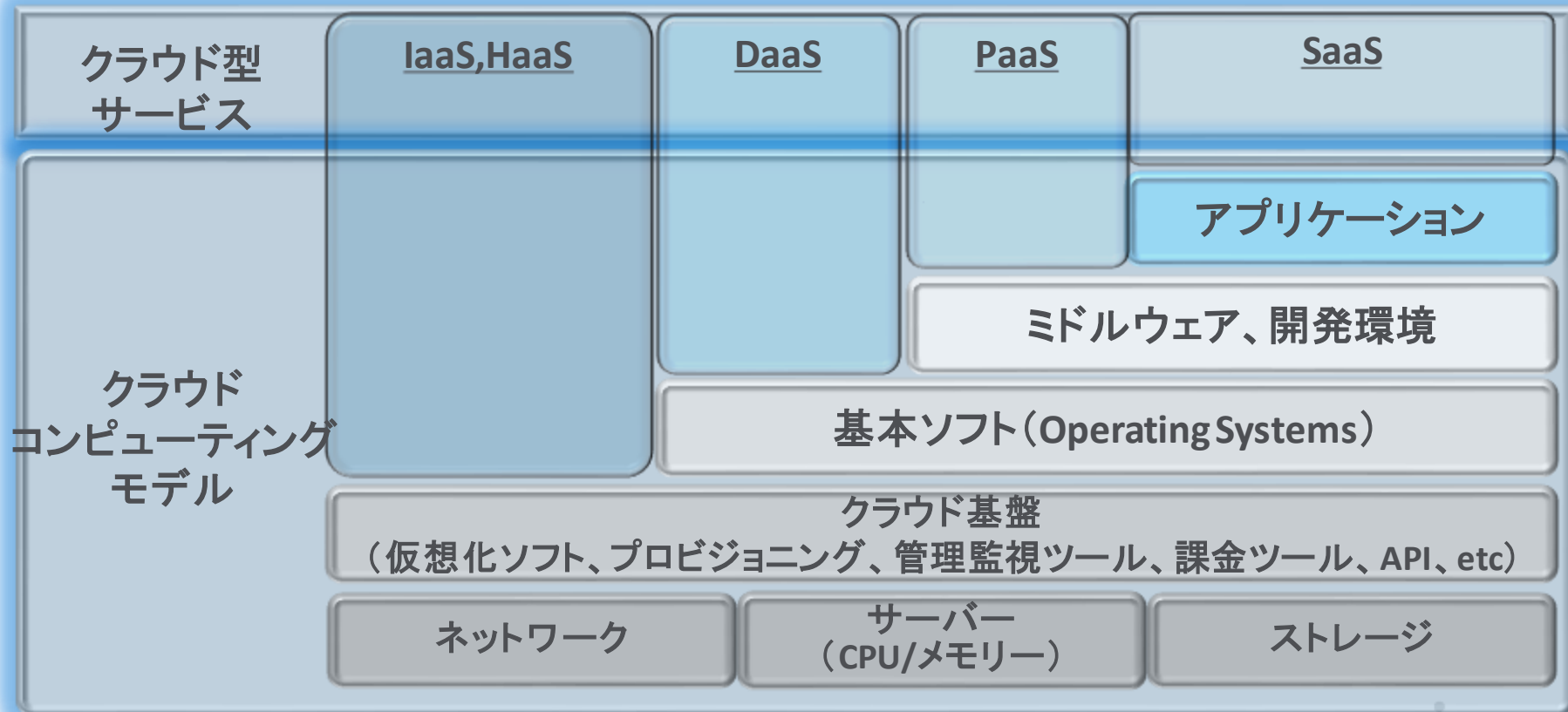


アジェンダ

1. CloudStack/IaaSとは？
2. IaaS基盤のネットワーク抽象化手法
3. 今後の予定 – OpenFlowとの融合

What is IaaS and CloudStack?

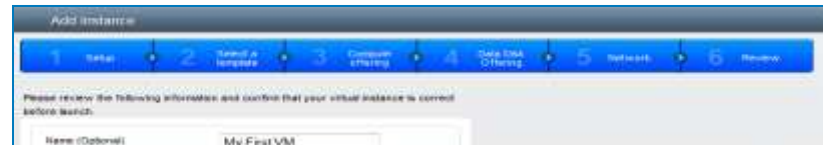
クラウドサービスって？



クラウド・コンピューティング？

キーワード(NISTの定義から)

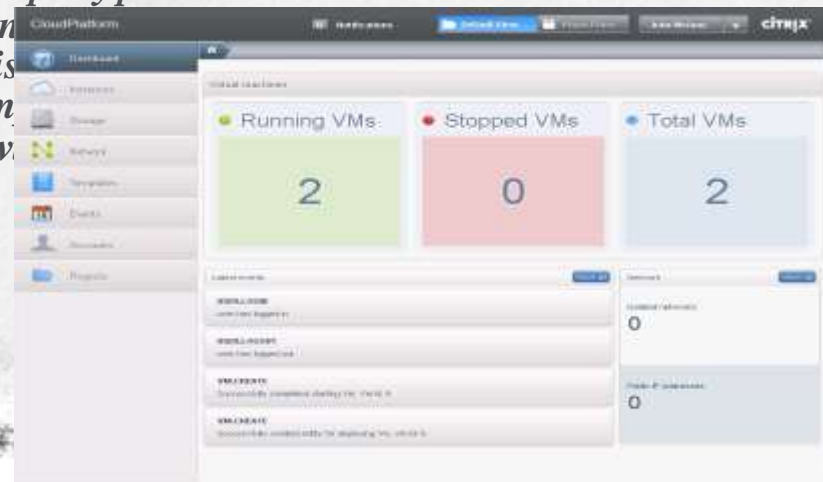
1. オンデマンドセルフサービス
2. ネットワークアクセス
3. 共有リソース
4. 迅速かつ柔軟なプロビジョニング
5. 測定可能なサービス



クラウド・コンピューティングの定義

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal

*man
This
com
serv*



What is CloudStack?

cloudstack

The Cloud Platform of the
Apache Software
Foundation



- セキ
する

- IaaS

- 複数

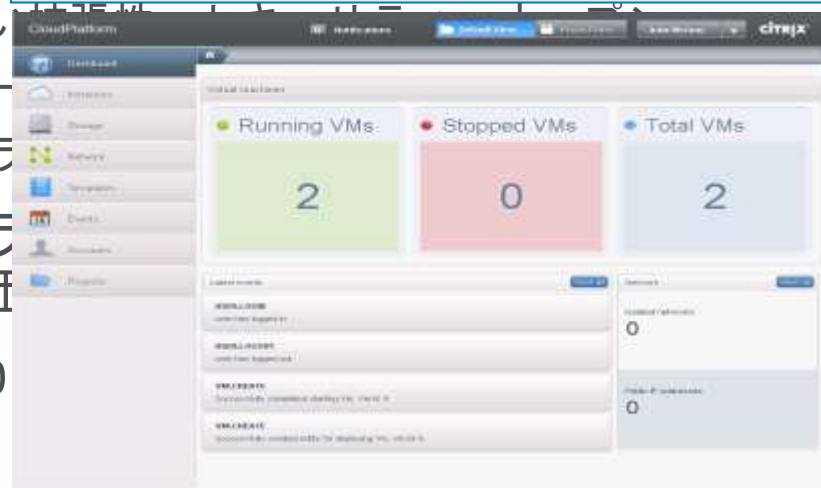
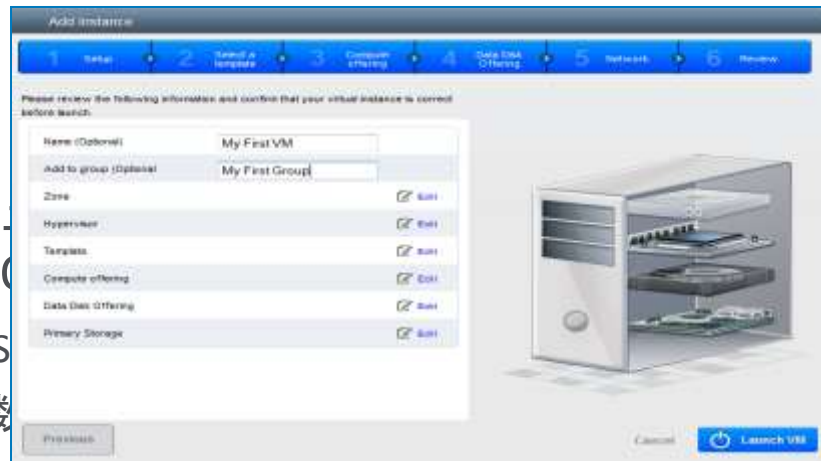
- 高い

- オ

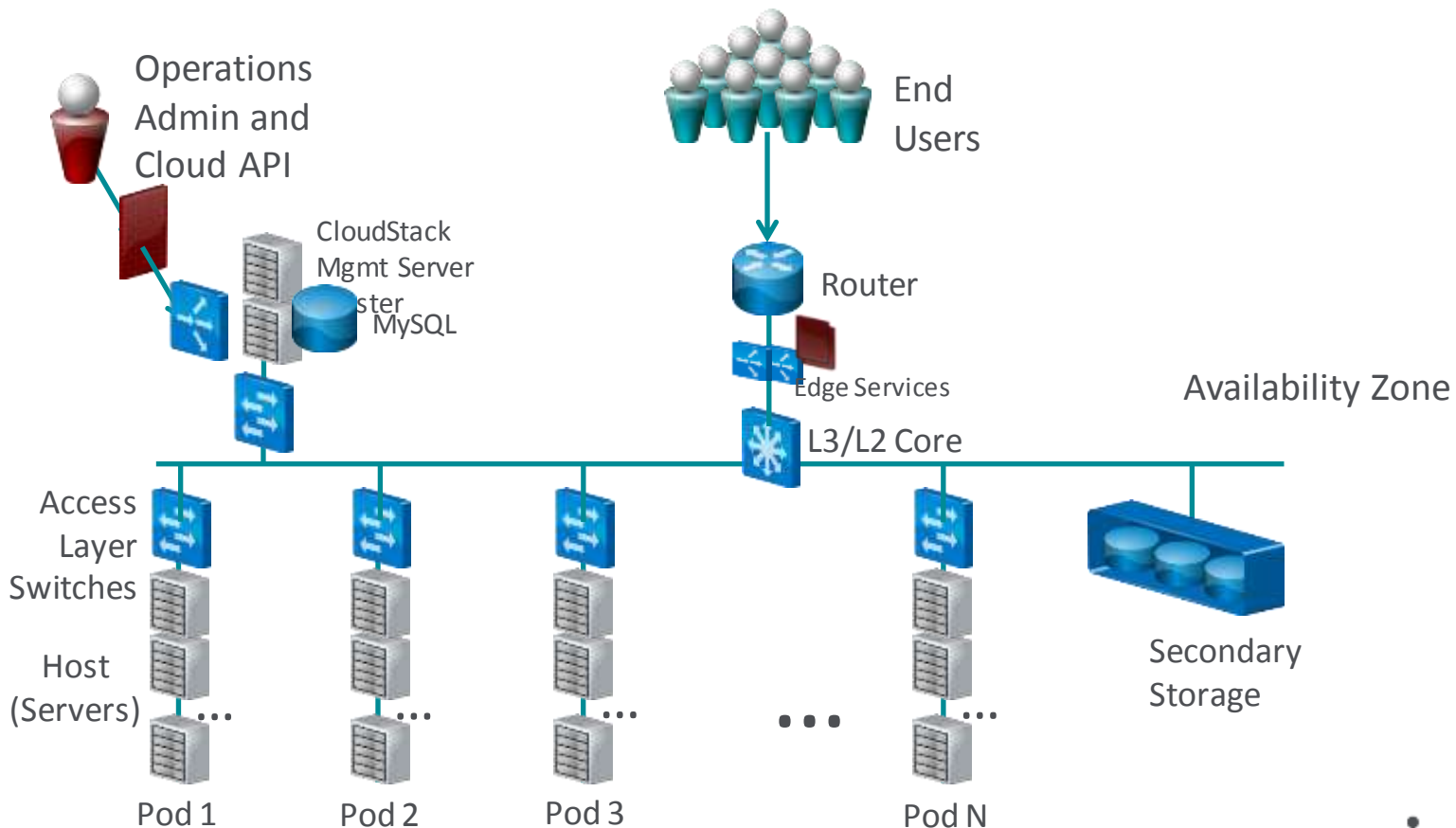
- プ

- クラ
安

- 100



クラウド環境の基本構成



IaaS基盤のネットワーク抽象化手法

- CloudStack Network Offering for Multi-tenancy

クラウド基盤におけるネットワーク形態

ベーシックネットワーク

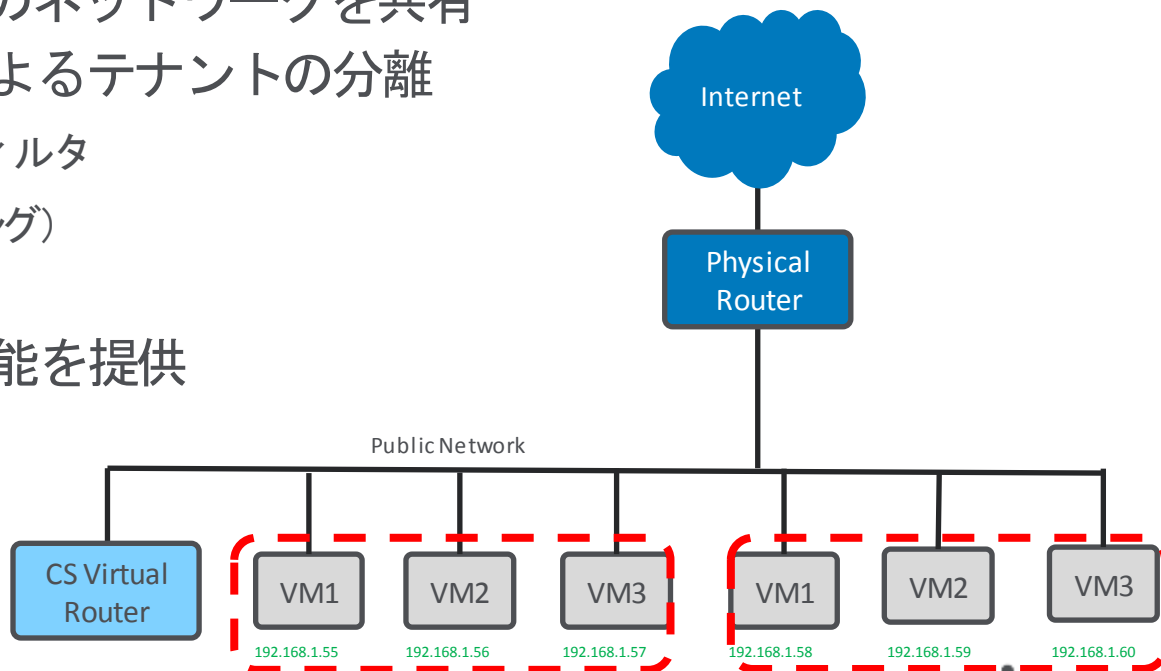
- テナントの分離(抽象化)はセキュリティグループ
- VLANはサポートしない
- パブリッククラウド(IaaS)で利用
- プライベートクラウドでも利用
- IPアドレスの付与はクラウドサービス
- サービスのElastic性を担保

アドバンスネットワーク

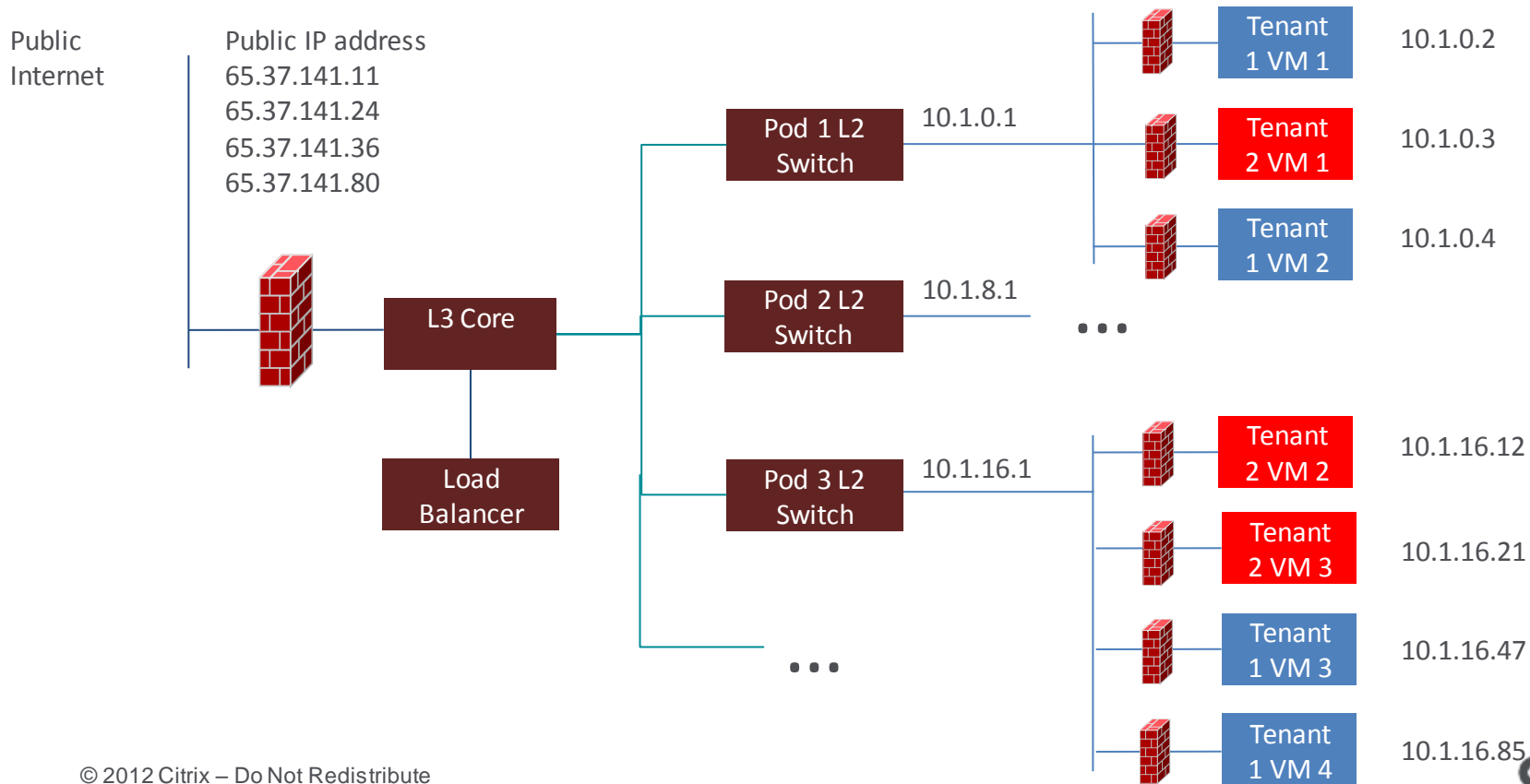
- テナントの分離(抽象化)はVLAN
- VLANをサポート
- VPN, Load Balancing, Firewallsなどをネットワーク機器サポート
- 透過的なネットワークアクセス
- 拡張性が課題

Cloud Infrastructure – ベーシックネットワーク

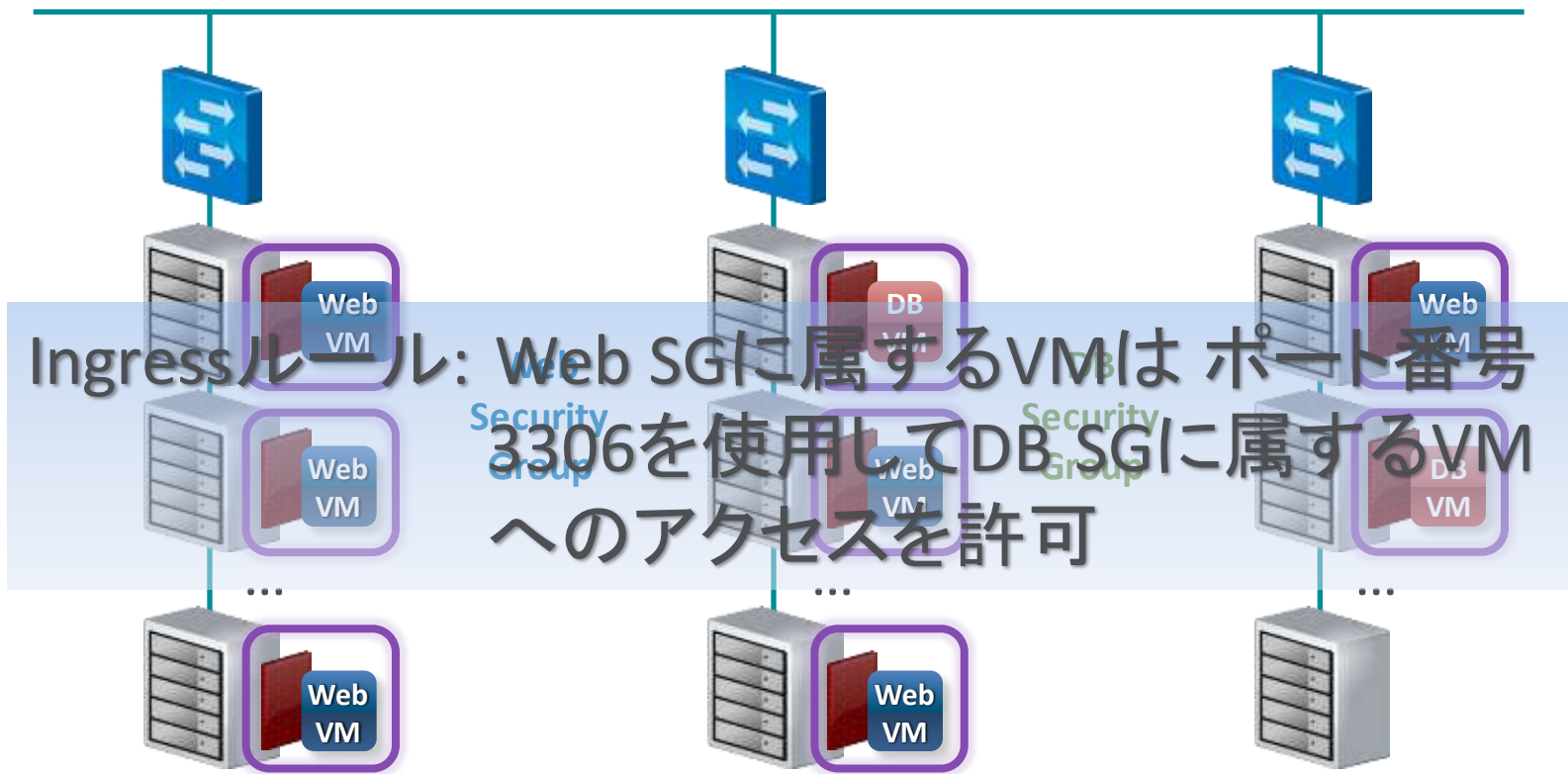
- Basic Shared Public Network:
 - すべてのテナントは単一のネットワークを共有
 - セキュリティグループによるテナントの分離
 - HypervisorによるIPアドレスフィルタ
 - レイヤー3での隔離(フィルタリング)
 - 優れた拡張性
- CloudStackが仮想ルータ機能を提供
 - DHCP
 - DNS



ベーシックネットワークの物理構成

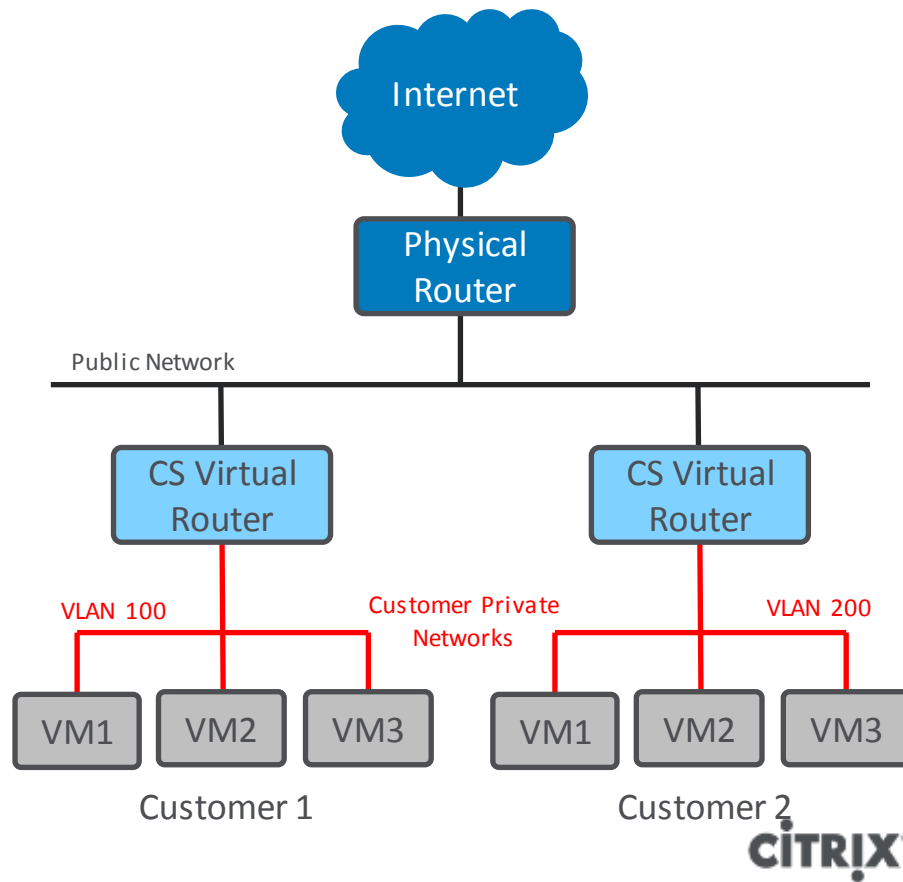


ベーシックネットワーク

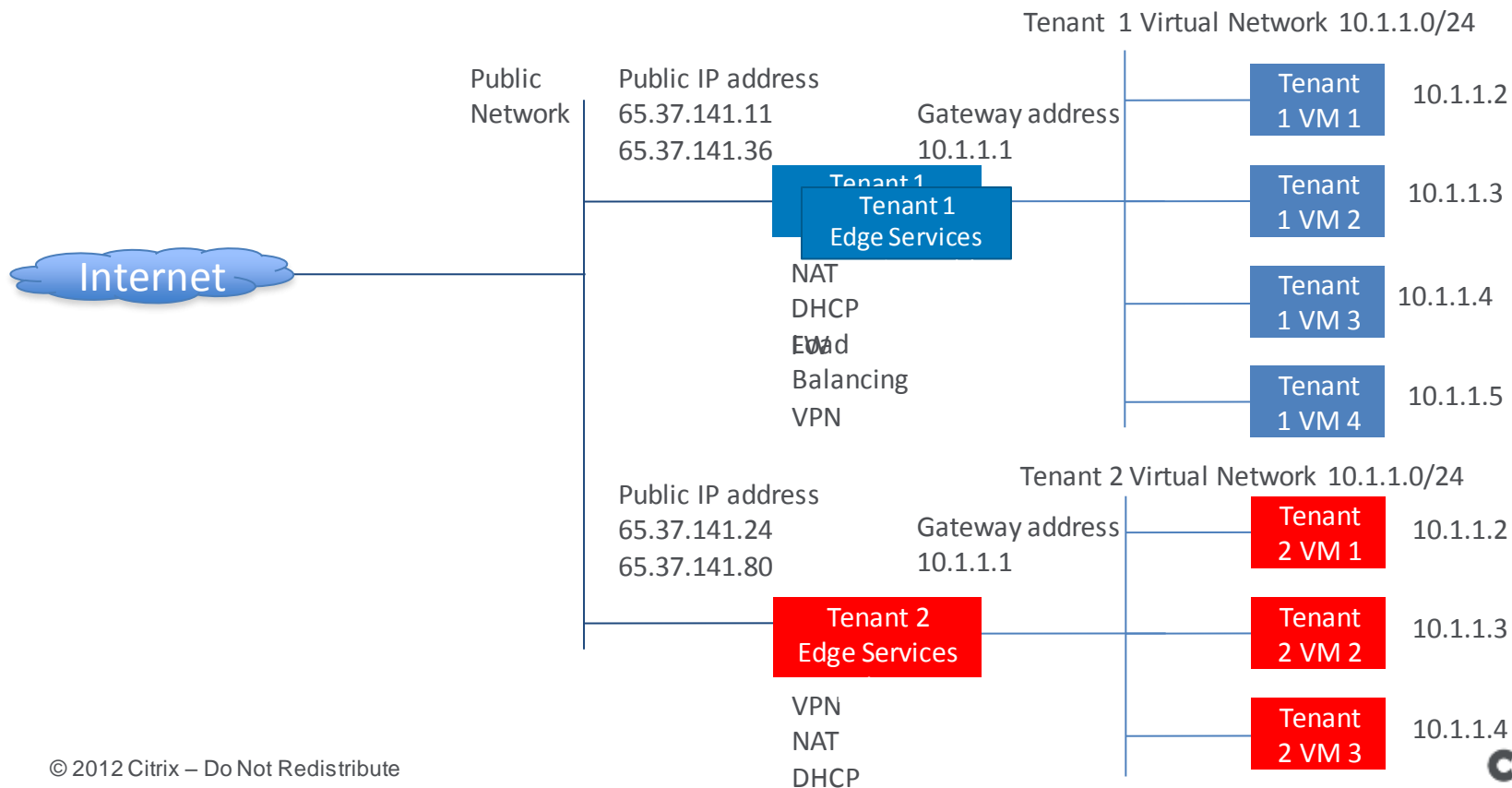


Cloud Infrastructure – アドバンスネットワーク

- Advanced networking :
 - ・ VLANによるネットワーク分離
 - ・ L2TP VPNによるトンネル機能
 - ・ 仮想ルータがゲートウェイ
 - ・ 個別ネットワークサービスが利用可能
 - ・ 1:1のNAT



アドバンスネットワークの物理構成



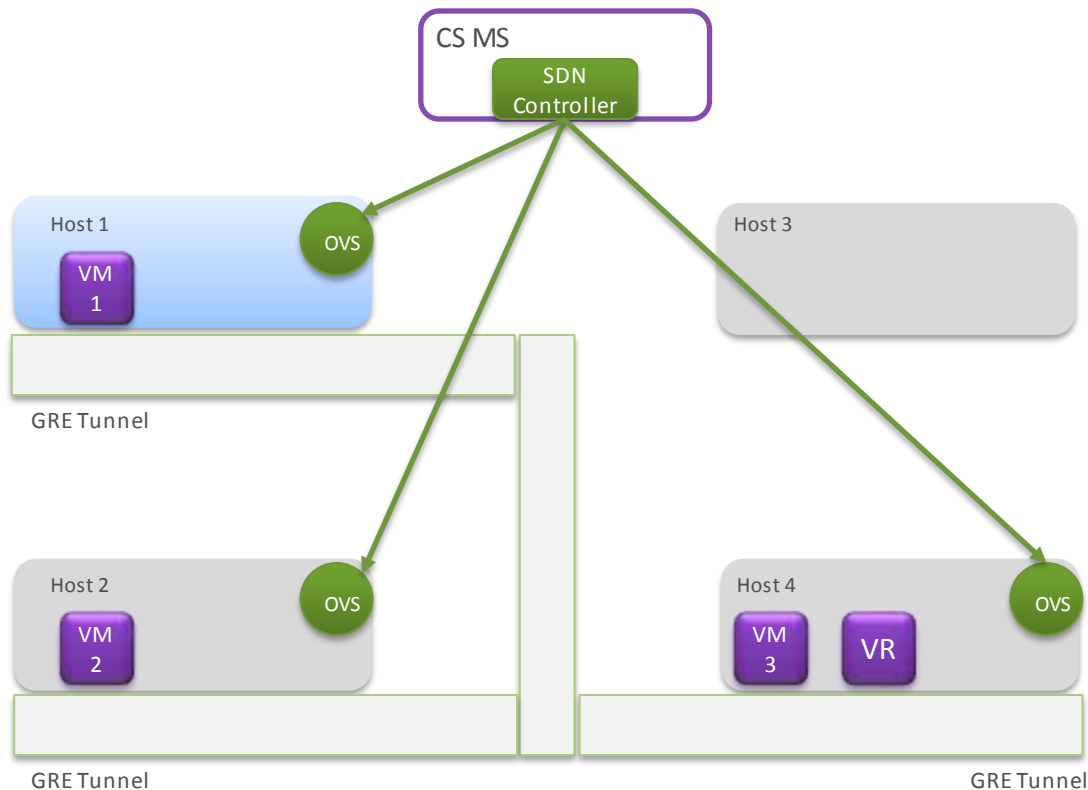
今後の予定

- OpenFlowとの連携

既存環境での課題

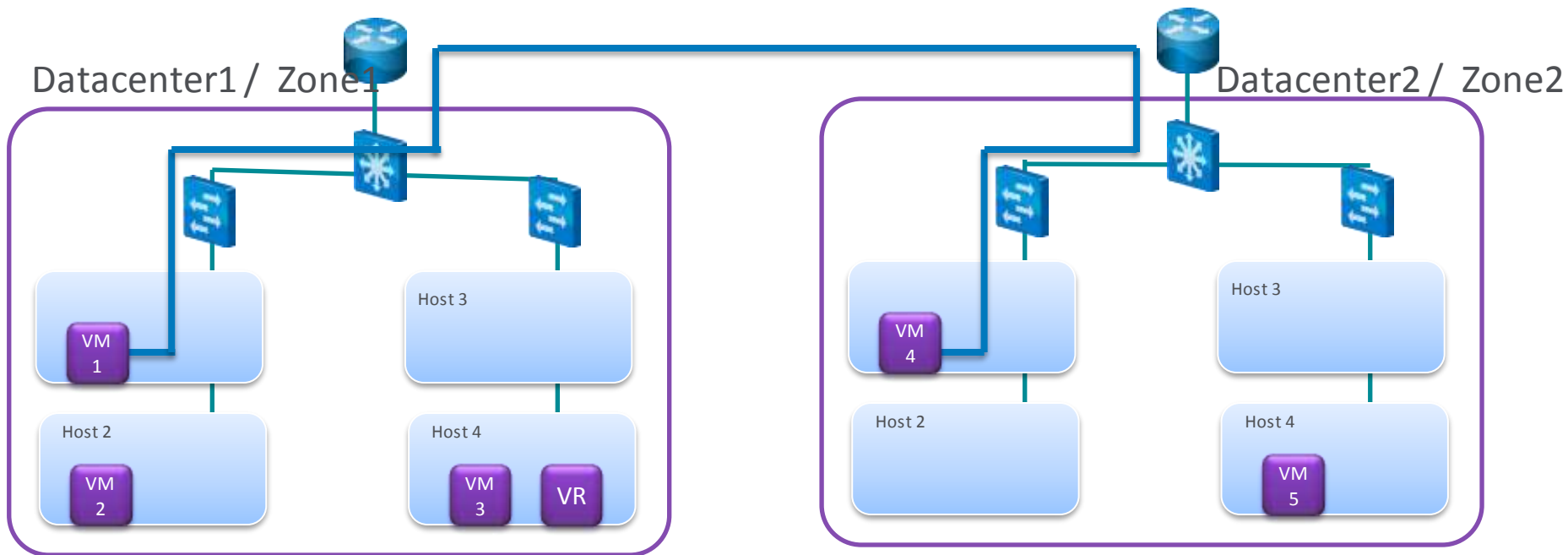
ベーシックネットワーク	アドバンスネットワーク
共通インターフェースの欠如	
<ul style="list-style-type: none">ハイパーバイザー毎に異なる実装	<ul style="list-style-type: none">スイッチ毎に異なる実装ハイパーバイザー毎に異なる実装
拡張性の欠如	
<ul style="list-style-type: none">個別フィルターの管理ハイパーバイザー毎に異なる実装	<ul style="list-style-type: none">VLAN 4Kの壁
サイト間接続時の柔軟性、透過性の欠如	

L2ネットワークのオーバーレイ



- すべての干すとは単一のL2ネットワーク上で展開
- CloudStackのSDNコントローラがOpen vSwitchのGREトンネル設定を実施
- GREトンネルをホスト上のvSwitch間に作成

L3越えの透過接続



L3をまたがるサイト（データセンター）間通信でGREトンネルを使用することにより、テナント内の通信が透過的に実施することが可能

まとめ

- CloudStackにおけるネットワークの抽象化実装
 - ベーシックネットワーク – Security Group (ACL) で分離
 - アドバンスネットワーク – VLAN で分離
- 課題
 - 共通インターフェースの欠如
 - 拡張性の欠如
 - サイト間接続における柔軟性、透過性の欠如
- 今後の展開
 - 抽象化の実現 – OpenFlow / Open vSwitch 活用したオーバーレイ
 - SDNへの取り組み – OpenFlow SDNコントローラーベンダーとの連携

CITRIX[®]

Work better. Live better.