



# マイクロソフトの SDN と ネットワークの仮想化のすべて ～机上の知識からの脱却～

日本マイクロソフト株式会社  
エバンジェリスト  
高添 修

<http://blogs.technet.com/b/osamut>

# 本日の時間割



時間	内容
13:00 - 13:05	はじめに
13:05 - 13:35	『あらためて Microsoft の SDN とネットワークの仮想化』 日本マイクロソフト エバンジェリスト 高添
13:35 - 13:50	休憩
13:50 - 16:20	『今わかっている NVGRE のすべて見せます。～デモ付き～』 三井情報株式会社 後藤 諭史様
16:20 - 16:35	休憩
16:35 - 17:30	『SDN ベースのクラウド構築例と気になるポイント』 日本マイクロソフト エバンジェリスト 高添
17:30 - 19:00	Q&A を兼ねた (その場)懇親会

特別ゲストあり



# 会場のご案内

## その他・ご注意事項

### ● 喫煙について

セミナー会場内は禁煙です。  
喫煙は当ビル B1F 喫煙所をご利用ください。

### ● 飲食について

セミナー会場内でご飲食していただけますが、ほかの方のご迷惑にならないようにご協力をお願いいたします。

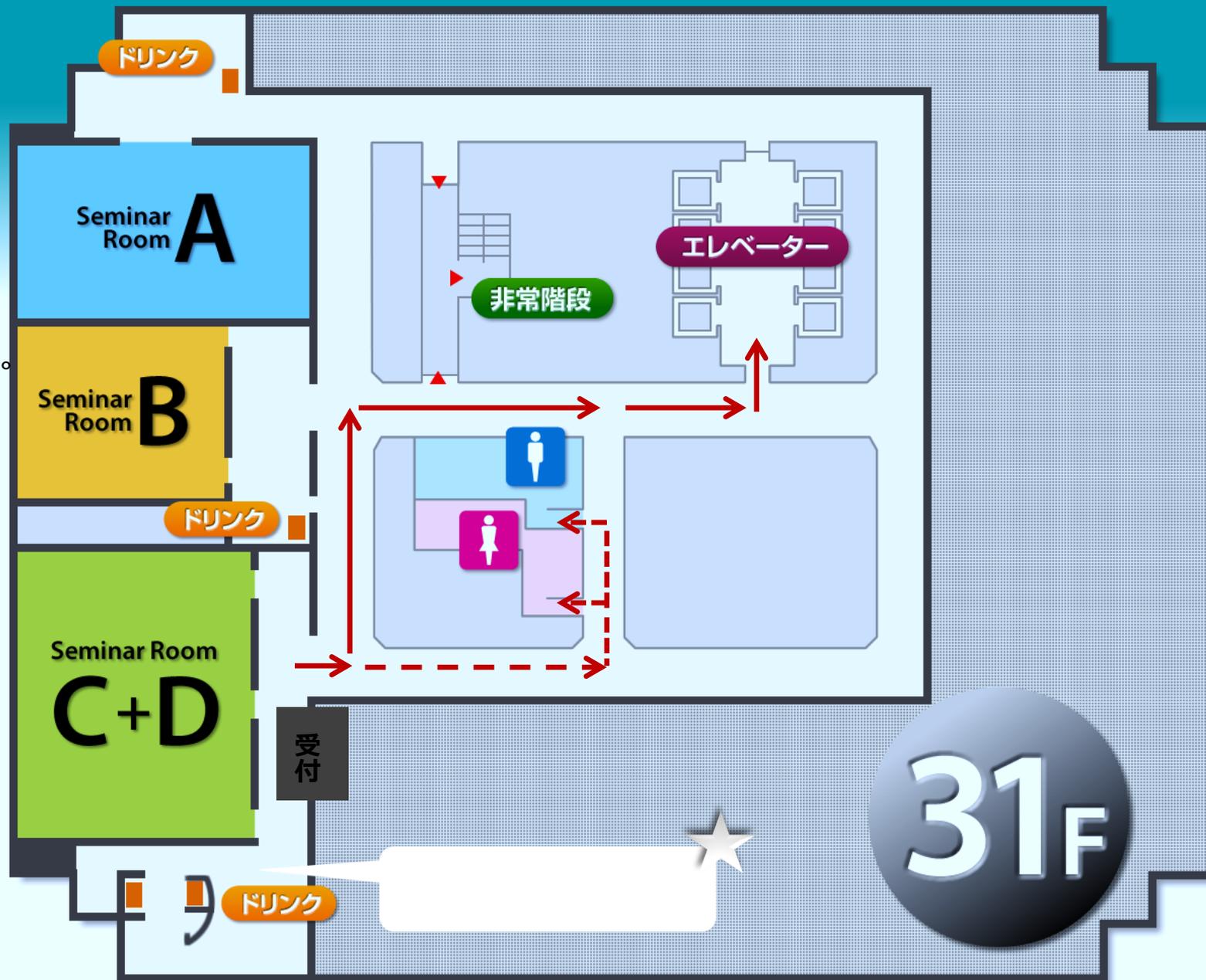
### ● 入館証

会場内では、受付時に発行された入館証が必要となります。

常に確認できるよう携帯をお願いいたします。

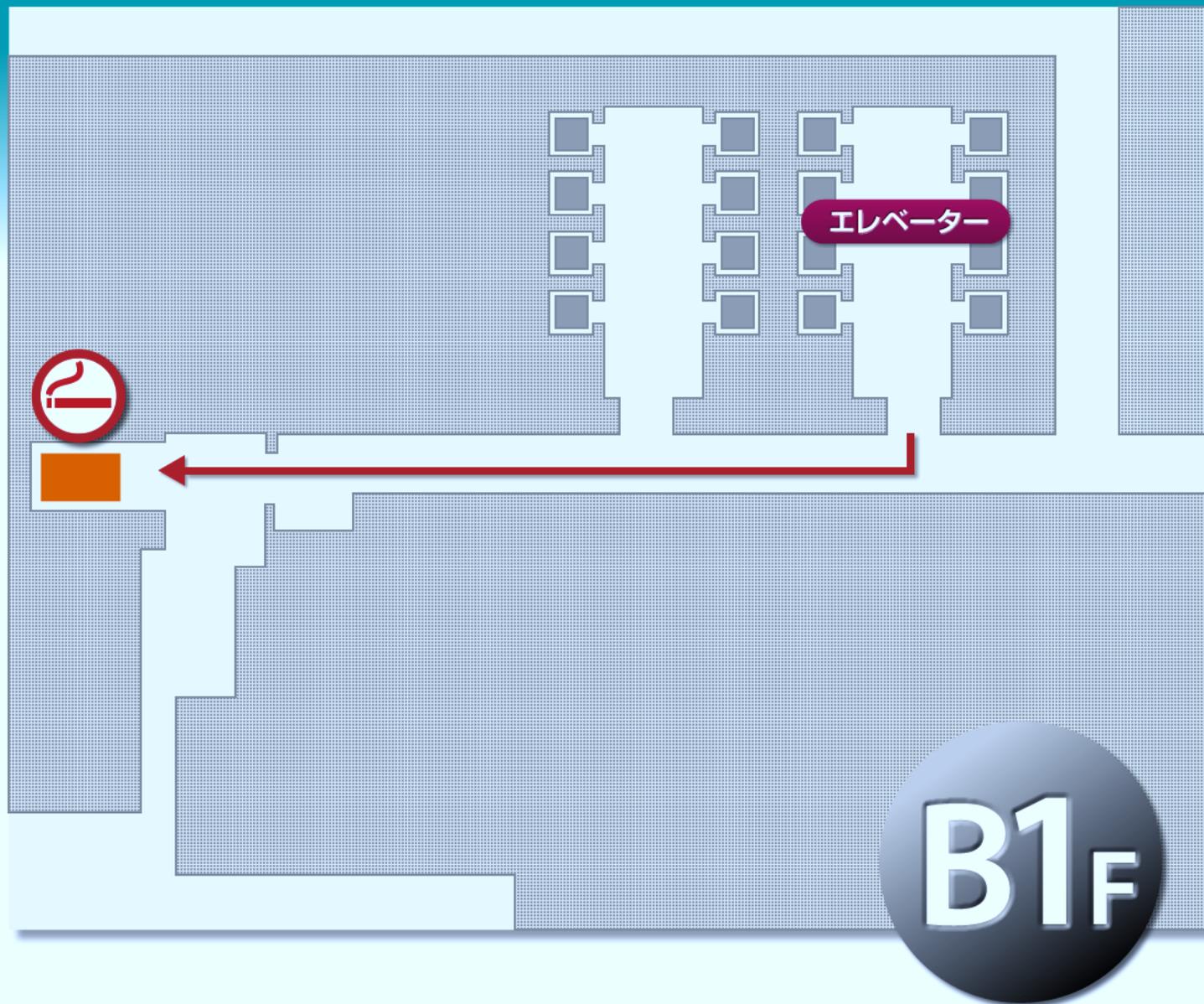
### ● 携帯電話

セッション会場では、他のお客様のご迷惑になりますので、電源をお切りいただくかマナーモードなどの設定にご協力ください。



# 会場のご案内

喫煙所 は B1F にございます。  
エレベーターで B1F へ  
お降りください。



# セミナー終了後のお願い

## 1. アンケートへの回答のお願い

- セミナー終了後～懇親会前にご提出ください。

## 2. 懇親会

- 部屋を出て右側のスペースで実施します。
- 何かのヒントがあるはずですが、是非ご参加ください。
- 貴重品だけは手元で管理をお願いします。

## 3. 退館時

- 入館証を 2F の返却ボックスへ必ずお戻しくください。
  - 入館証返却前に必ず忘れ物チェックをお願いします。



# あらためて Microsoft の SDN と ネットワークの仮想化

日本マイクロソフト株式会社  
エバンジェリスト  
高添 修  
<http://blogs.technet.com/b/osamut>

# ネットワークの進化を軽く整理

Software Defined Network  
(ソフトウェアによる制御)

※ 製品や実装の話



ネットワーク仮想化  
(オーバーレイ ネットワーク)

※ トンネリング プロトコルの話

ハードからソフトへ  
時代の流れ



パフォーマンス向上  
ソフトからハードへ

# ネットワークの仮想化



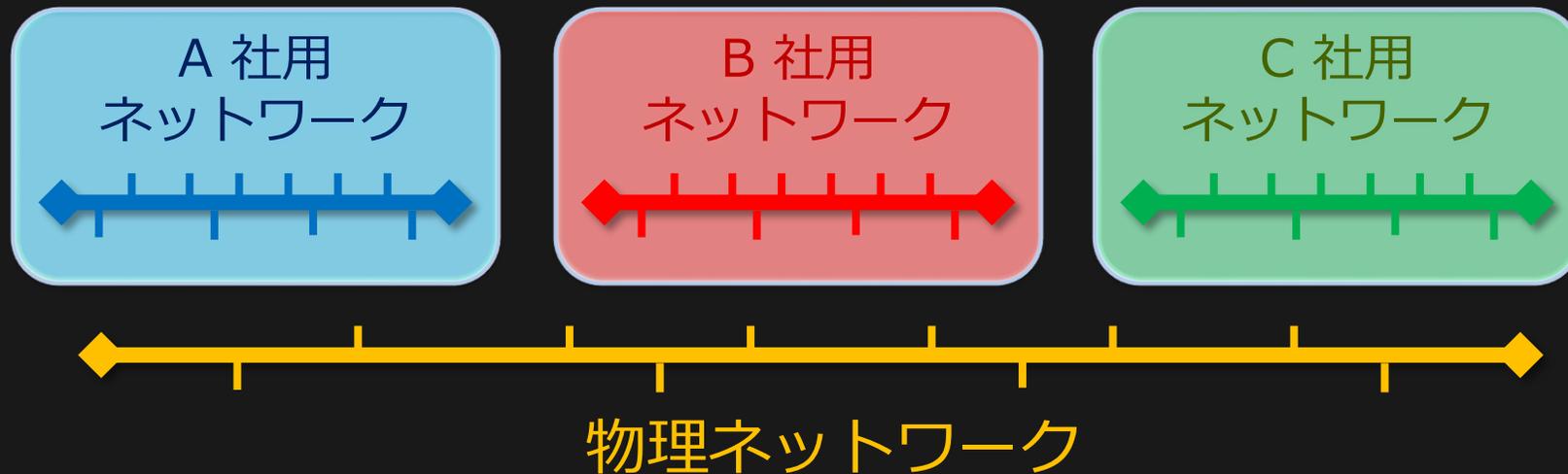
# あたかも x x のように見せる技術

## ●サーバーの仮想化は

- あたかも物理サーバーがたくさんあるように見せる技術

## ●ネットワークの仮想化は

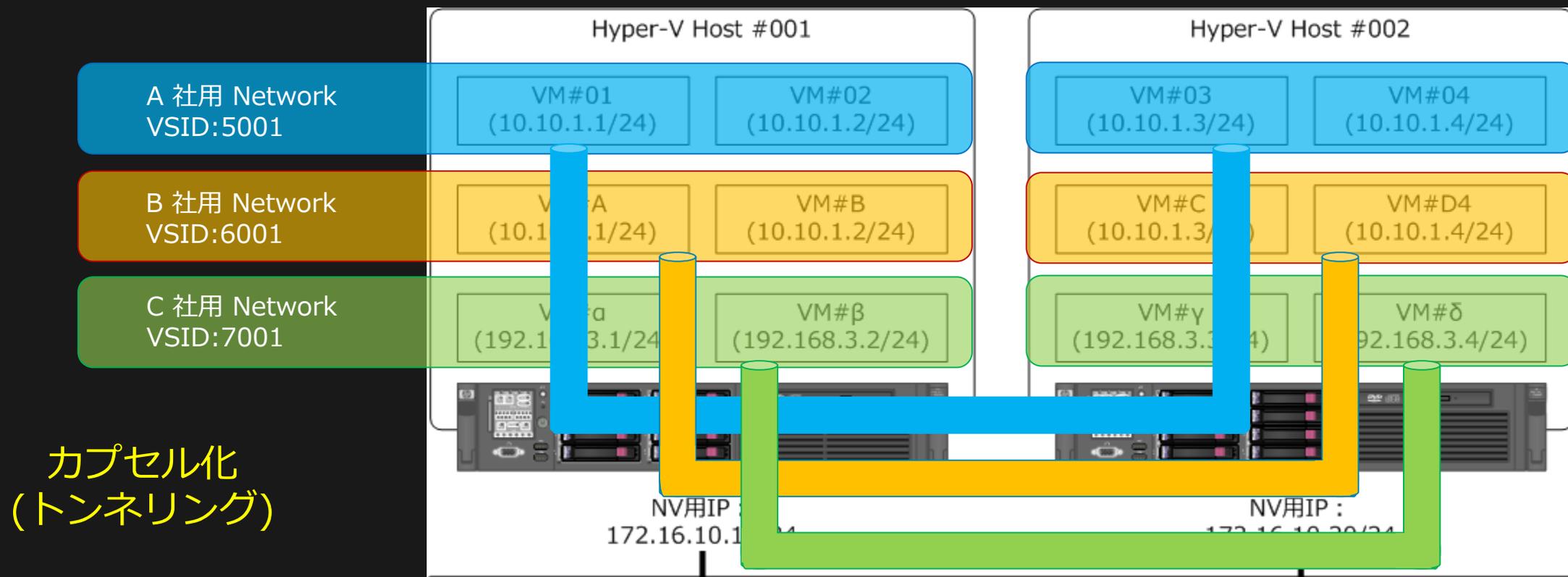
- あたかも物理ネットワークがたくさんあるように見せる技術
- 物理ネットワークとは関係なく自由に IP サブネットを利用可



System Center の  
設定画面は  
このイメージの  
通りにできている

# もう少し具体的に (後藤さん資料から)

- 物理ネットワーク上に、もうひとつのネットワーク (仮想ネットワーク) を上からかぶせるように構築 (オーバーレイ) し、ネットワークの物理構成 / 論理構成 (トポロジー) を切り離してしまおう、技術 / 思想。



# トンネリングの技術

今日はこちら

- NVGRE ( Network Virtualization using Generic Routing Encapsulation )

- GRE でカプセル化 ( 42bytes のオーバーヘッド )
- → Microsoft, Intel, Dell, HP, Broadcom, Arista, Emulex

- VXLAN ( Virtual eXtensible Local Area Network )

- UDP でカプセル化 ( 50bytes のオーバーヘッド )
- → VMware, Cisco, Arista, Broadcom, Citrix, Red Hat

- STT ( Stateless Transport Tunneling Protocol )

- TCP ライクな構造を持つ、ステートレストンネリングプロトコル。
- → Nicira ( VMware )

- IP Rewrite

- IP NAT

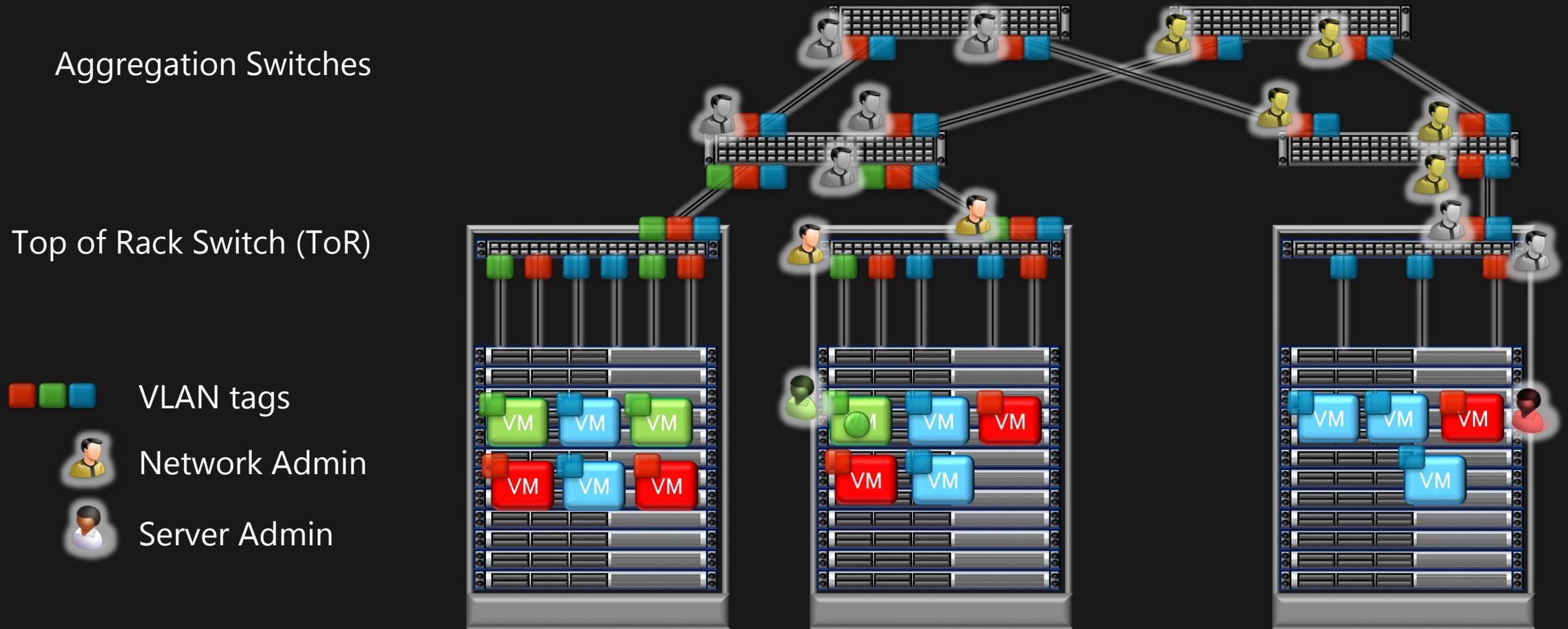
**Windows Server 2012  
Network Virtualizationでは、  
の2方式が使用可能**



<http://www.amazon.co.jp/exec/obidos/ASIN/4844395750/p2ptodwsl-22>

最後まで読んでくださいね！

# Using VLANs to isolate VM traffic



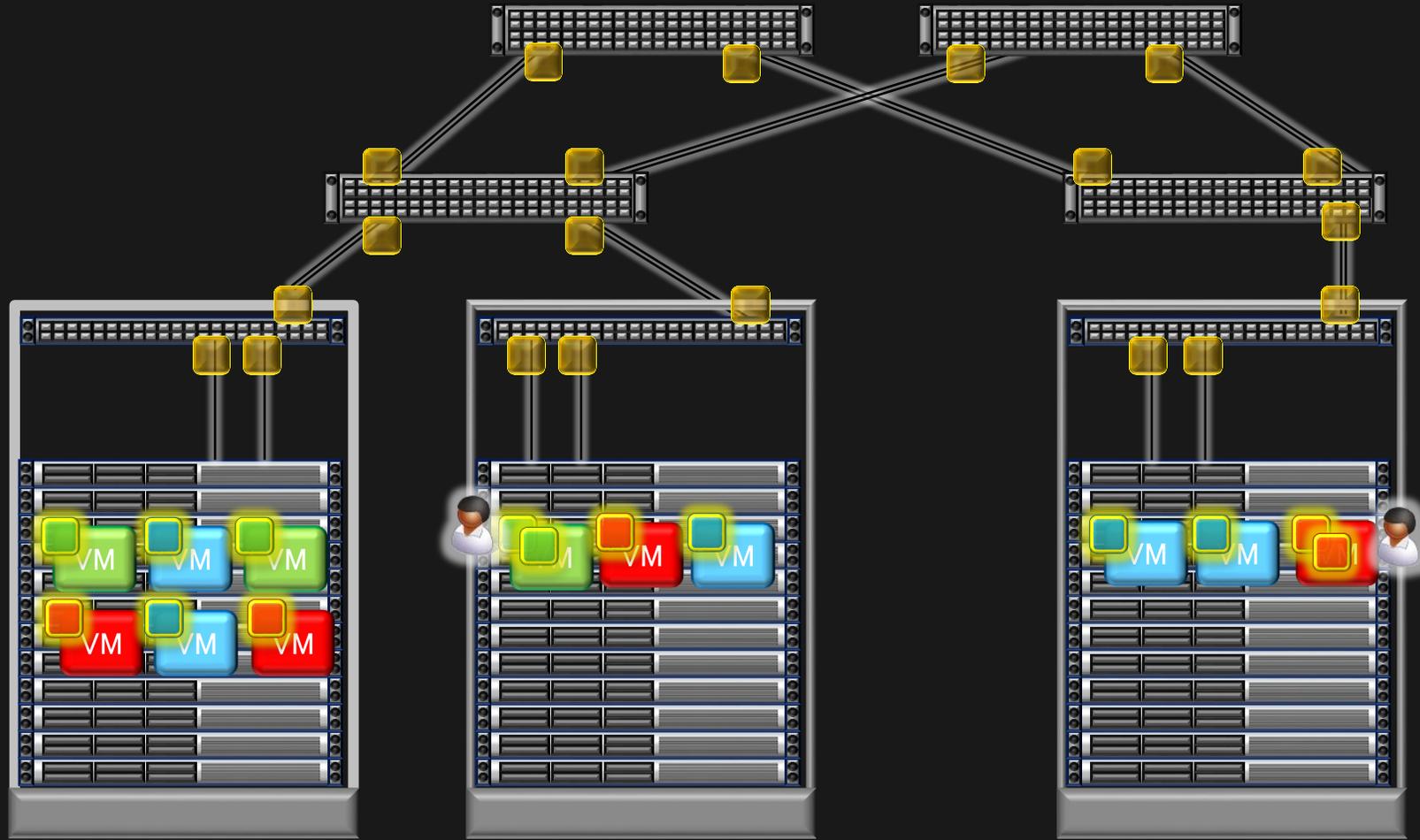
Requires Network Admins to configure VLANs and Subnets

# Using NVGRE for network virtualization

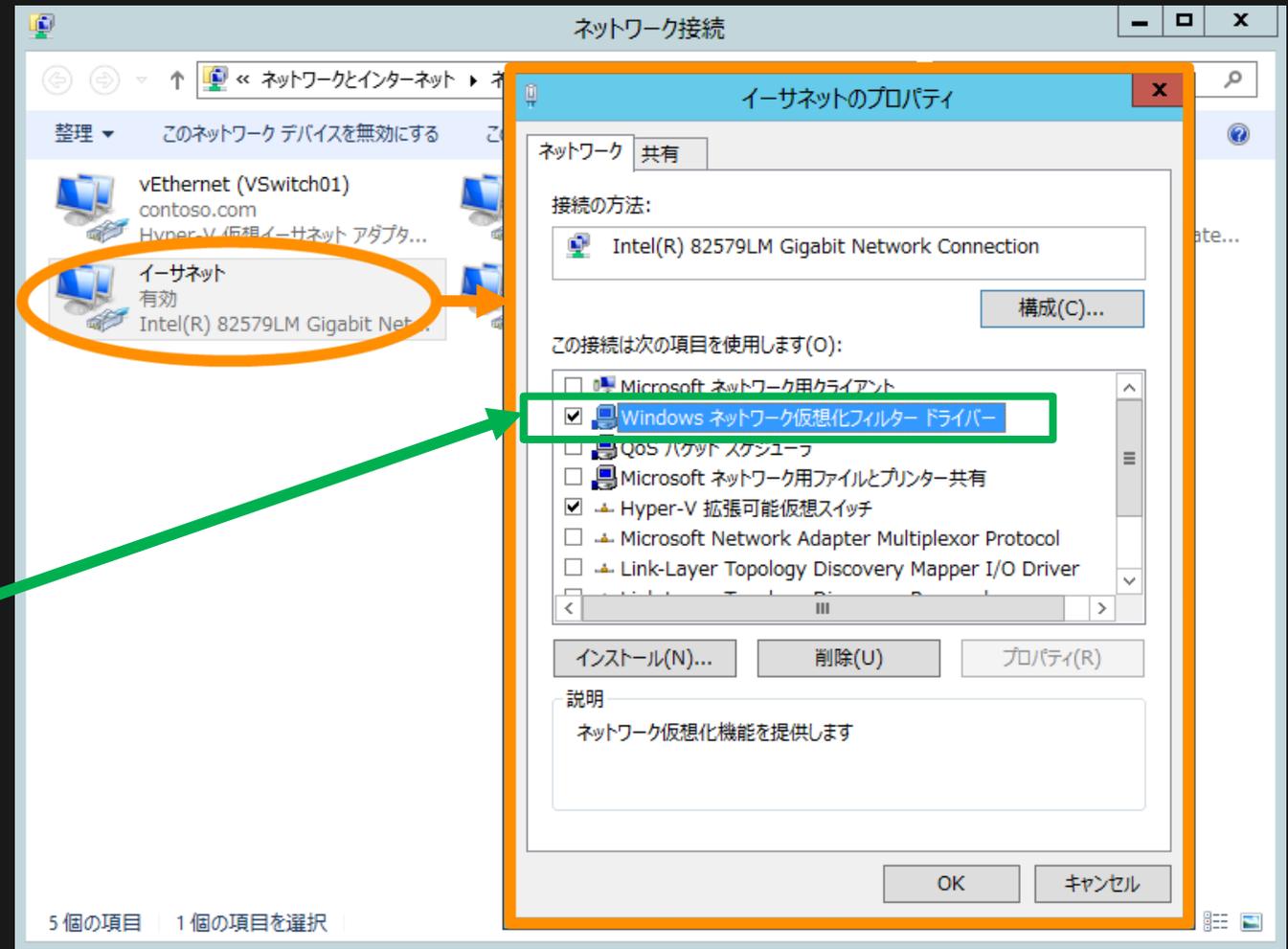
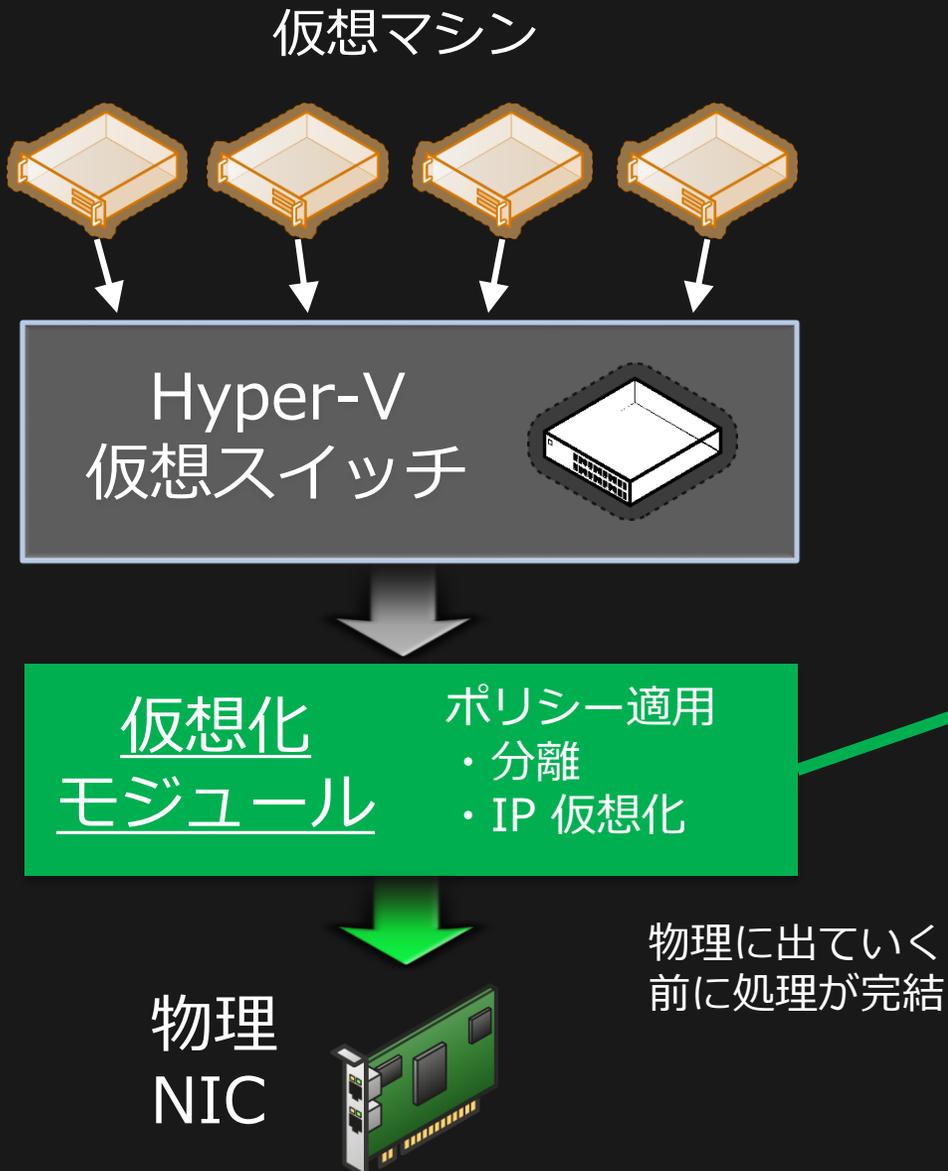
 Provider Network  
   Encapsulated Traffic

## datacenter Policy

-  **Blue**
  - VM<sub>1</sub>: MAC<sub>1</sub>, CA<sub>1</sub>, PA<sub>1</sub>
  - VM<sub>2</sub>: MAC<sub>2</sub>, CA<sub>2</sub>, PA<sub>3</sub>
  - VM<sub>3</sub>: MAC<sub>3</sub>, CA<sub>3</sub>, PA<sub>5</sub>
  - VM<sub>4</sub>: MAC<sub>1</sub>, CA<sub>4</sub>, PA<sub>7</sub>
  - VM<sub>5</sub>: MAC<sub>2</sub>, CA<sub>5</sub>, PA<sub>8</sub>
-  **Red**
  - VM<sub>1</sub>: MAC<sub>x</sub>, CA<sub>1</sub>, PA<sub>2</sub>
  - VM<sub>2</sub>: MAC<sub>y</sub>, CA<sub>2</sub>, PA<sub>4</sub>
  - VM<sub>3</sub>: MAC<sub>z</sub>, CA<sub>3</sub>, PA<sub>6</sub>
  - VM<sub>4</sub>: MAC<sub>z</sub>, CA<sub>3</sub>, PA<sub>9</sub>
-  **Green**
  - VM<sub>1</sub>: MAC<sub>a</sub>, CA<sub>1</sub>, PA<sub>1</sub>
  - VM<sub>2</sub>: MAC<sub>b</sub>, CA<sub>2</sub>, PA<sub>2</sub>
  - VM<sub>3</sub>: MAC<sub>c</sub>, CA<sub>3</sub>, PA<sub>5</sub>



# Windows Server 2012 の何が処理をしているのか

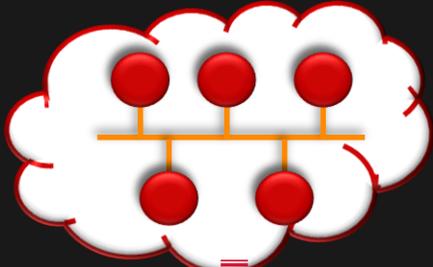
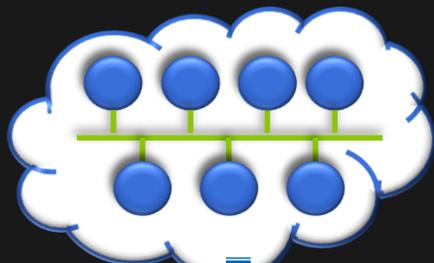


# Hyper-V がルーティングテーブルを持つ

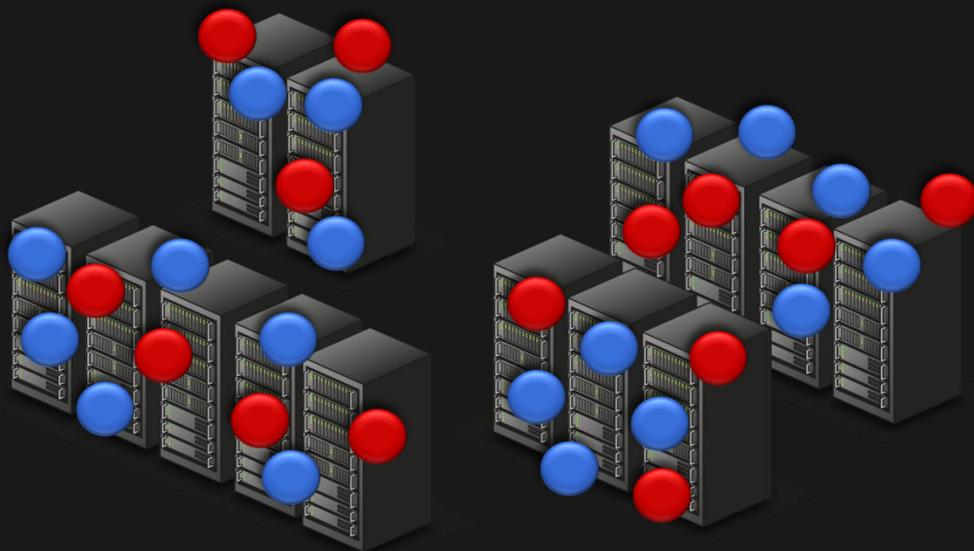
管理用 PowerShell  
コマンドあり

Blue 社

Red 社



ネットワークの仮想化技術



マルチテナント データセンター

## ルーティングテーブル概念

BlueVM01 : 10.1.1.1  
VSID : 30  
Host01 : 192.168.1.11

BlueVM02 : 10.1.1.2  
VSID : 30  
Host02 : 192.168.1.12

RedVM01 : 10.1.1.1  
VSID : 20  
Host01 : 192.168.1.11

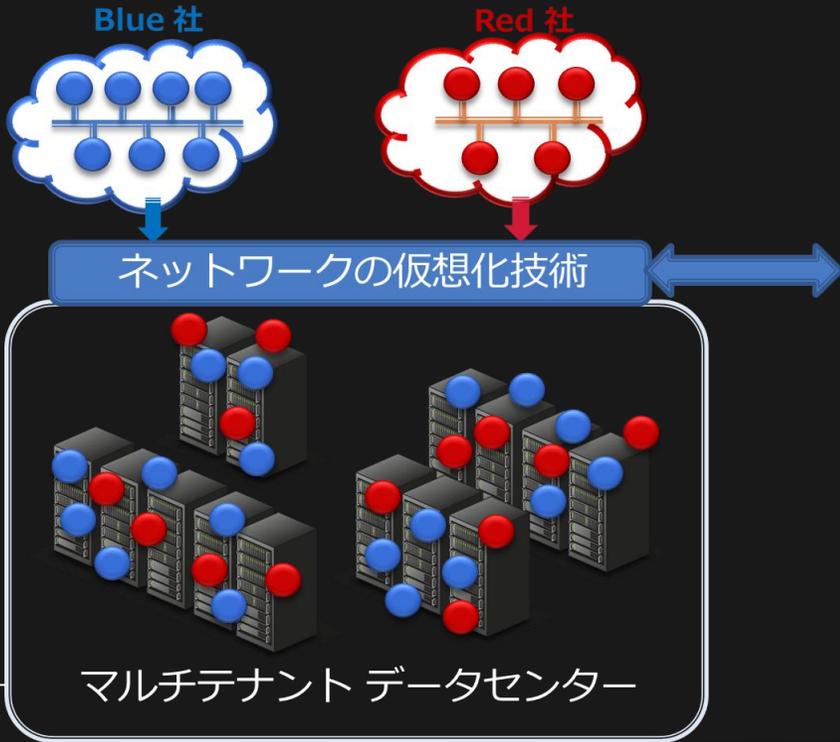
RedVM02 : 10.1.1.2  
VSID : 20  
Host02 : 192.168.1.12

# SDN として

～ Software Defined Network ～



# System Center による集中管理



## ルーティングテーブル概念

- BlueVM01 : 10.1.1.1  
Host01 : 192.168.1.11  
VSID : 30
- BlueVM02 : 10.1.1.2  
Host02 : 192.168.1.12  
VSID : 30
- RedVM01 : 10.1.1.1  
Host01 : 192.168.1.11  
VSID : 20
- RedVM02 : 10.1.1.2  
Host02 : 192.168.1.12  
VSID : 20

## System Center Virtual Machine Manager の出番



- ソフトウェア的に定義
- ソフトウェアで制御

Hyper-V 1

Hyper-V 2

Hyper-V 3

Hyper-V 4

Hyper-V 5



今わかっている NVGRE のすべて見せます。  
～デモ付き～

三井情報株式会社 後藤 諭史様  
よろしくお願ひします。

～ 16:20

Windows Server 2012 & Windows Server 2012 R2



# SDN ベースのクラウド構築例と 気になるポイント

日本マイクロソフト株式会社

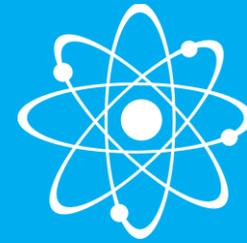
エバンジェリスト

高添 修

<http://blogs.technet.com/b/osamut>

Microsoft

ネットワークが  
サービスになる  
～ オーバーレイのもう1つの価値 ～



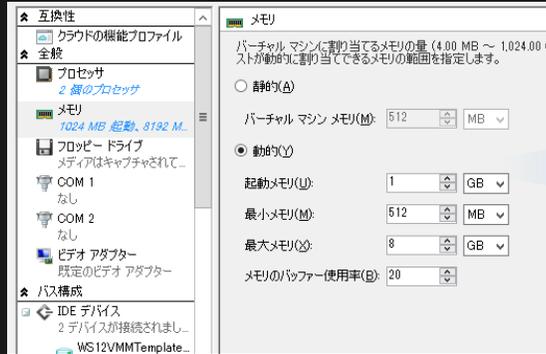
# サーバー仮想化に寄り添うネットワークの仮想化

ネットワーク  
事前定義  
(IPプール化)



ネットワーク仮想化の強制  
SDN としての制御

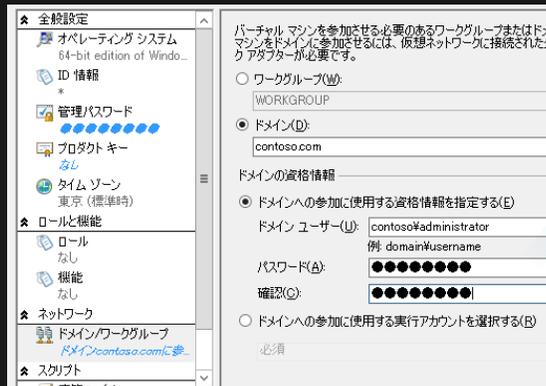
HW スペック  
事前定義  
(SS,S,M,L,XL)



Windows & Linux

テンプレート  
作成

OS 環境  
事前定義  
(管理パスワードや  
ドメイン参加等)



ホスト名設定、IP アドレス設定、ドメイン参加、  
ローカル管理者パスワード設定などを自動化

# SC2012 VMM SP1 とネットワークの関係 (2段階の設定)

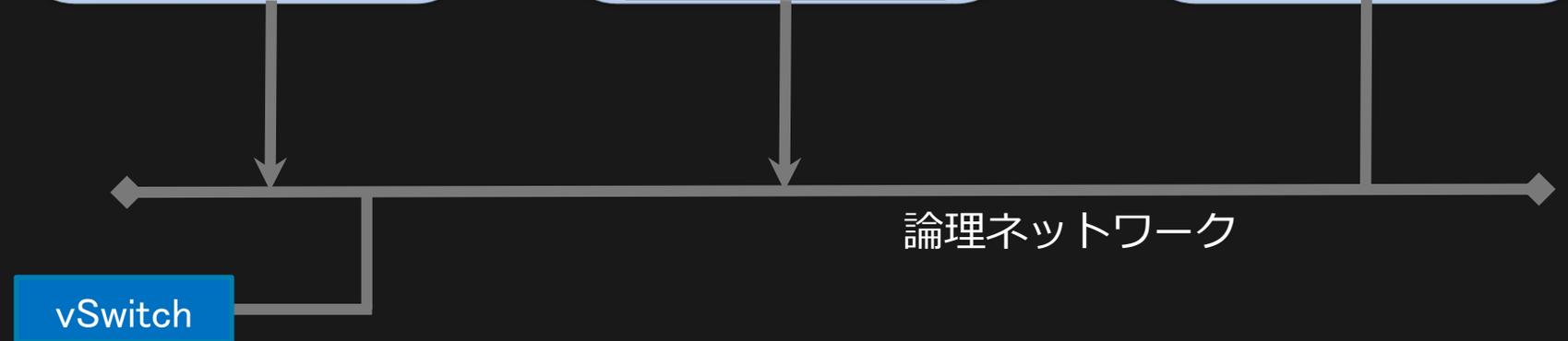
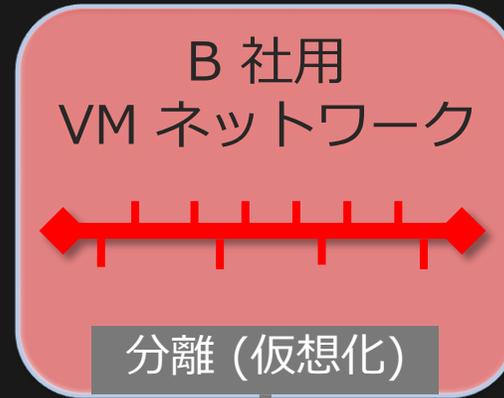
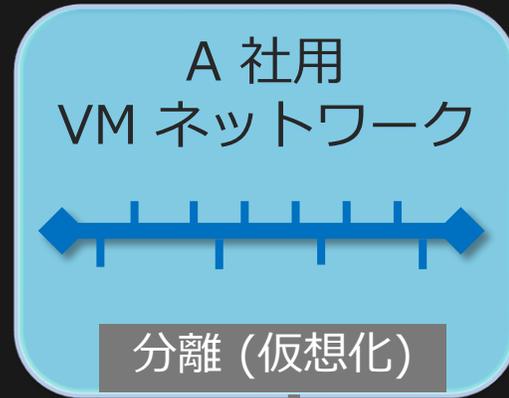
ここをサービスとして活用



「VMとサービス」  
の  
VM ネットワーク



「ファブリック」  
の  
論理ネットワーク



# ネットワークがサービスに

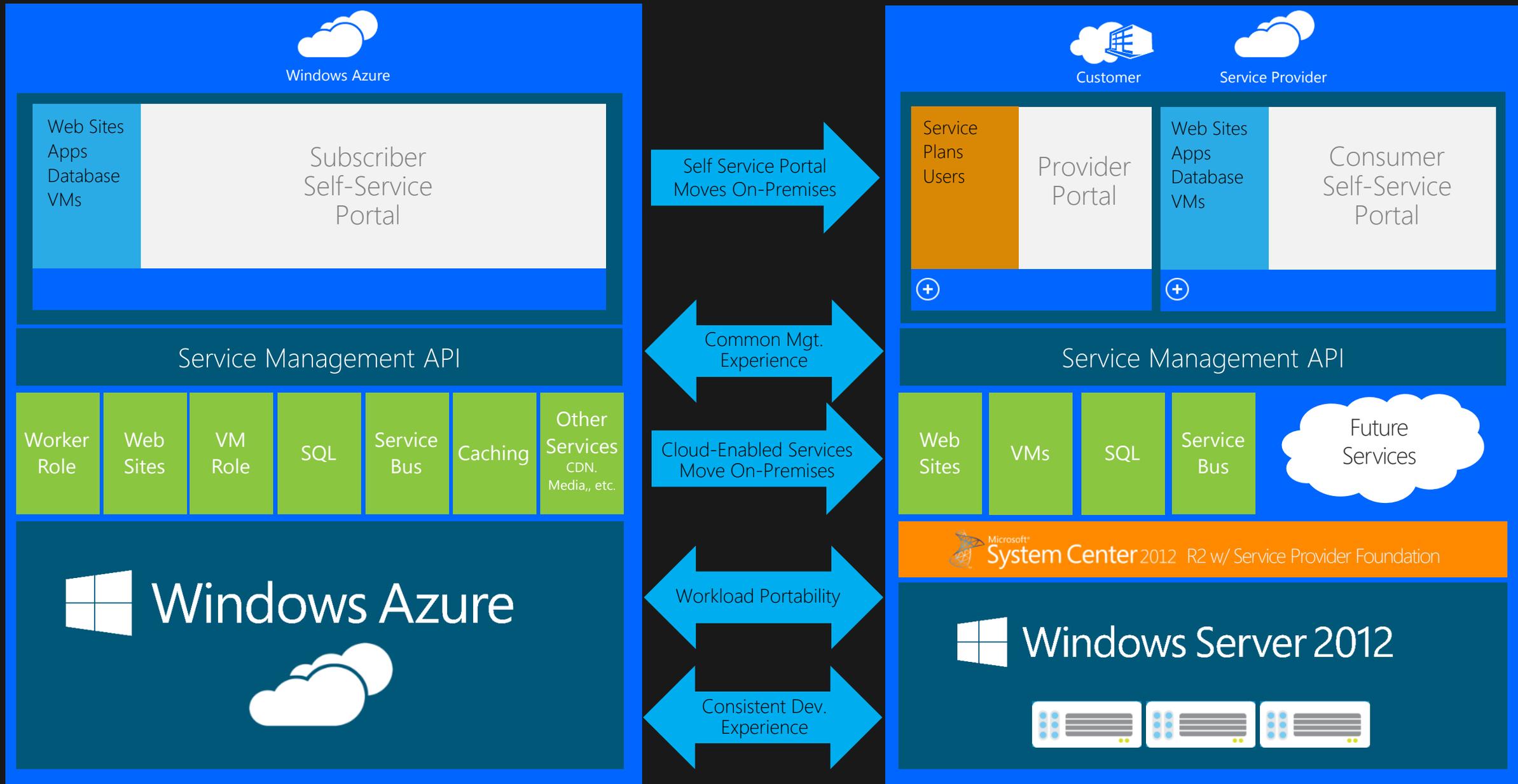
サービスの利用者が  
ネットワークを作成  
(BYOIP)

The screenshot displays the Windows Azure portal interface for creating a virtual network. The left sidebar shows various service categories, with 'ネットワーク' (Network) highlighted and a '+ 新規' (New) button. The main content area shows a table of existing virtual networks, with 'osamutvm001' selected. A modal window for creating a new virtual network is open, showing the following configuration:

- 名前 (Name): TakazoeNet
- アドレス空間 (Address Space): 10.0.0.0/20 (selected from a dropdown menu)
- 最大 VM 数 (Maximum VM Count): 4096 [CIDR: /20]
- DNS サーバー (DNS Server): ADDNS (selected from a dropdown menu)

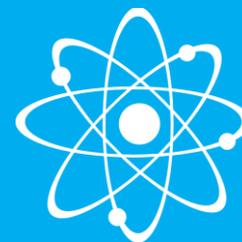
The '仮想ネットワークを作成する' (Create Virtual Network) button is visible at the bottom right of the modal window.

# Windows Azure Pack – 自分で作る疑似 Azure



# Next Stage

～ オーバーレイの更なる進化 ～



# TechEd North America 2013 (New Orleans)

The screenshot shows the event page for TechEd North America 2013, held from June 3-6 in New Orleans. The page features a navigation bar with 'Channel 9', 'BROWSE', 'FORUMS', 'CODING4FUN', and 'EVENTS'. A search bar is present with a Bing logo. The main header includes the 'TechEd North America 2013' logo and the Microsoft logo. Below the header, there are links for 'Events | TechEd | TechEd North America' and a 'Subscribe to this event' button. The event details section shows 'New Orleans | June 3 - 6, 2013' and social media sharing options for Reddit, Twitter (347), Facebook (536), and LinkedIn. A 'Featured' section highlights a 'Keynote Presentation' by Brad Anderson, titled 'Despite sea changes in cloud computing, device proliferation, and the explosion of data, IT pros and developers still live for one simple thing: to deliver amazing experiences for their customers and end-users. In this keynote, Brad Anderson will unveil a broad set of new capabilities across the full...'. Below this, there are buttons for 'List', 'Schedule', 'Most Viewed', and 'All'. A partial view of another session, 'Building Your Lab, Dev, and Test Scenarios in Windows Azure Infrastructure Services (IaaS)', is visible at the bottom.

## Keynote & Breakout Session

- Video
- PPT Slide (ほぼ公開済み)

- Windows Server 2012 R2
- System Center 2012 R2

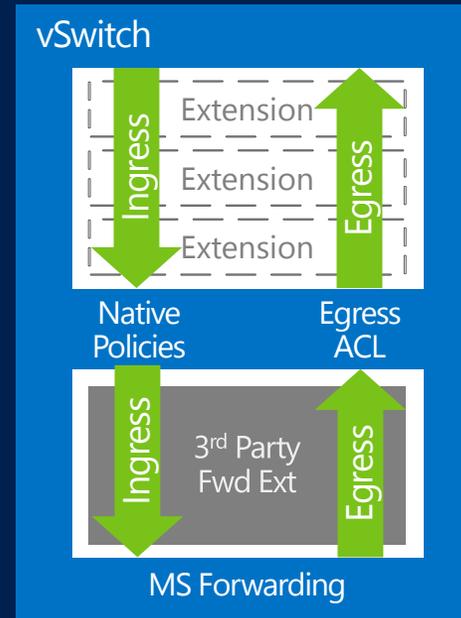
<http://channel9.msdn.com/Events/TechEd/NorthAmerica/2013?sort=sequential&direction=desc&page=10&r%5B0%5D=Modern%20Datacenter#fbid=jiYTnAsR9e0>

# Hyper-V Switch extension co-existence with Hyper-V Network Virtualization

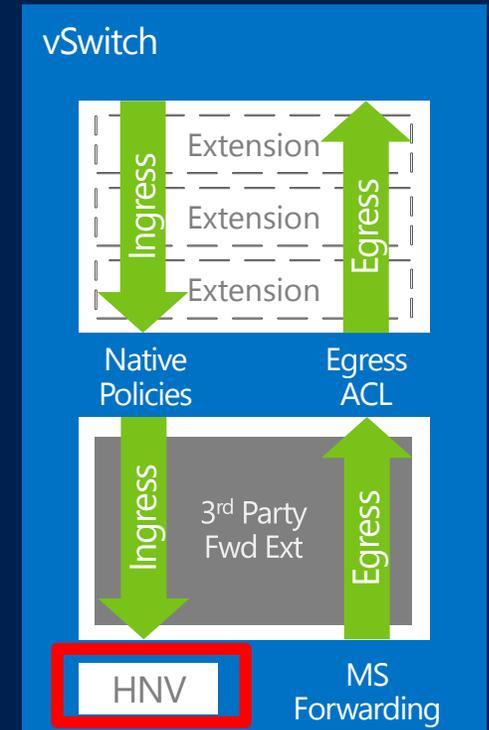
Introduces new hybrid forwarding  
HNV forwards HNV traffic  
Forwarding Extension forwards non-HNV traffic

Richer switch extensions  
Extensions can view CA and PA packets

Enables 3<sup>rd</sup> party network virtualization  
Forwarding extensions can modify packet headers on both ingress and egress



Windows Server 2012



Windows Server 2012 R2

# NVGRE Gateway

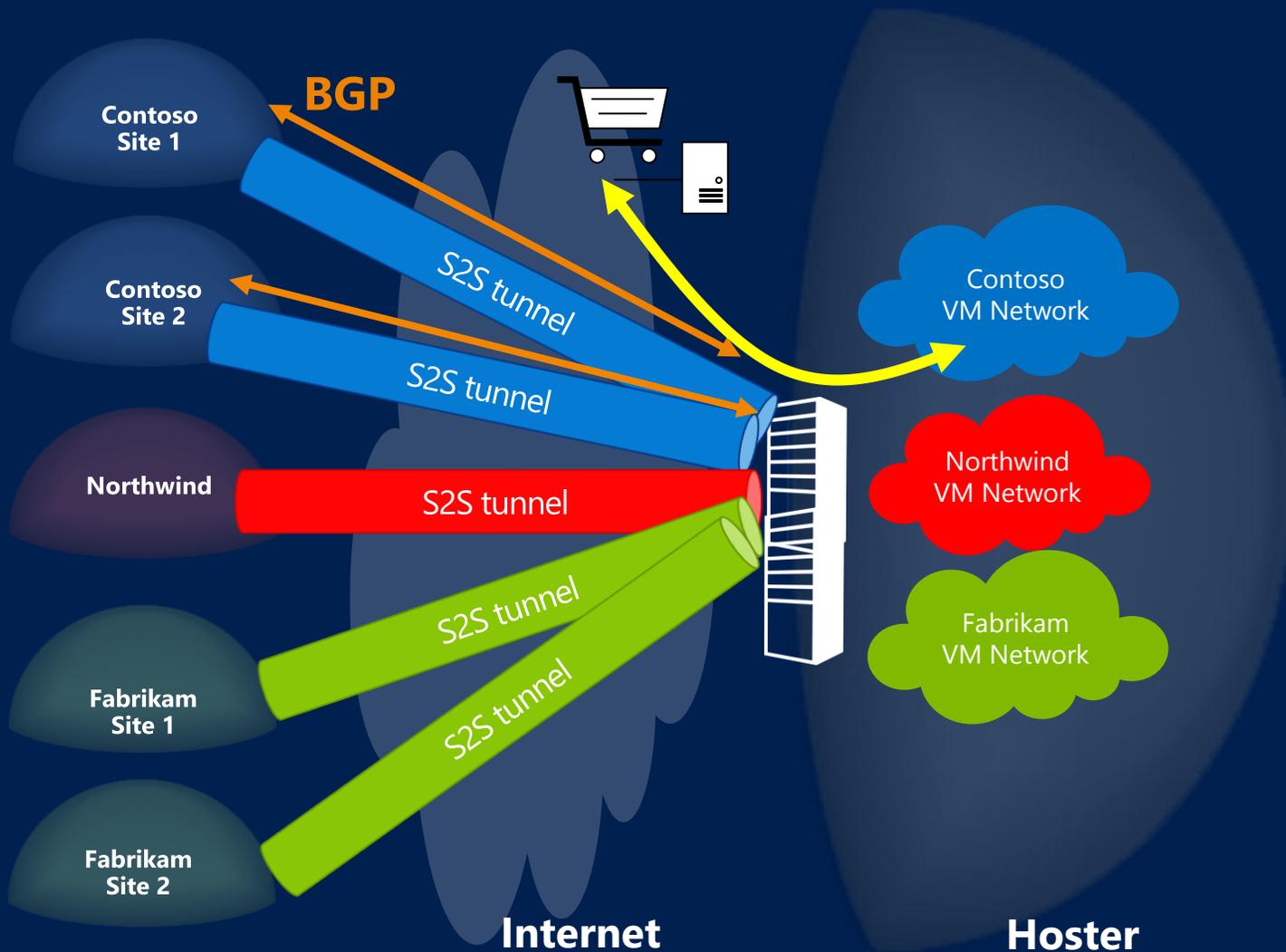
## Software gateway

- Built-in Windows Server 2012 R2
- Network vendor's virtual appliance

## Hardware gateway

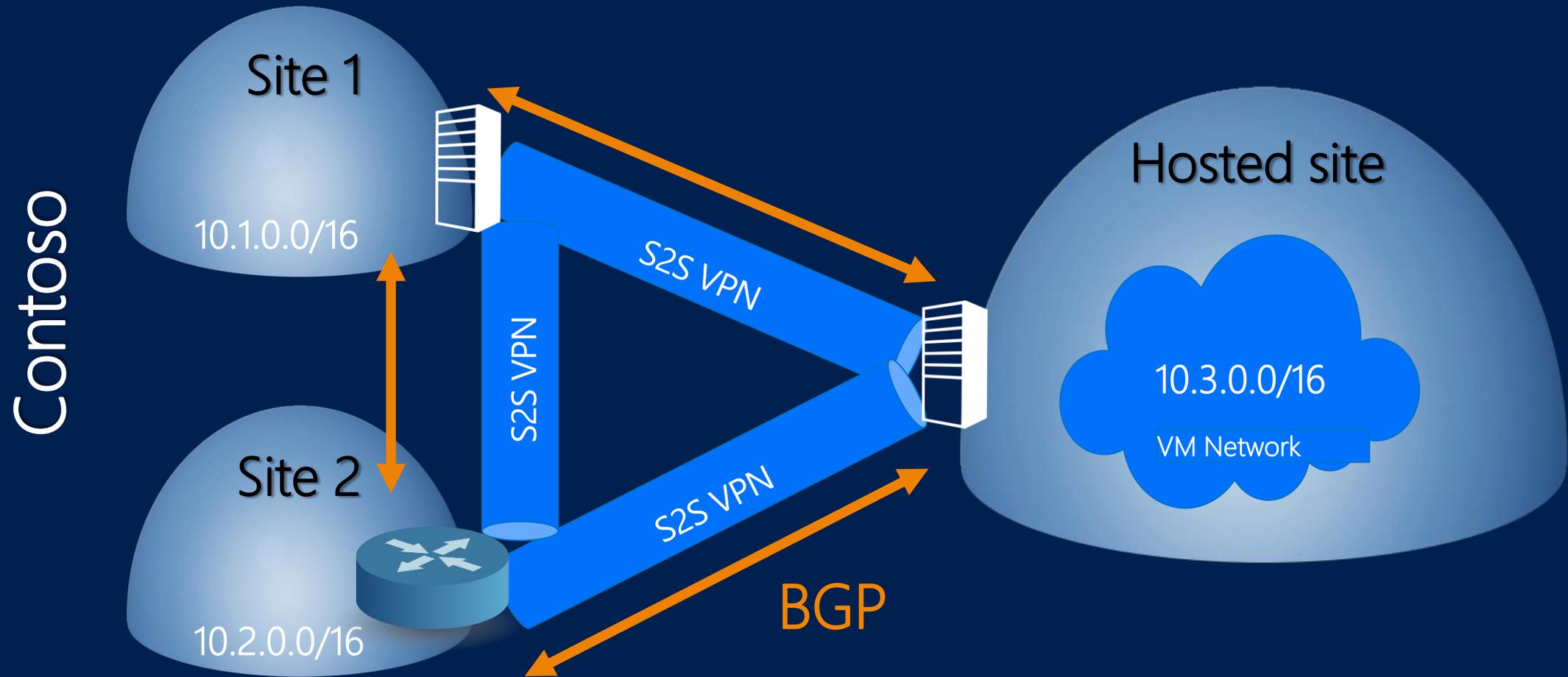
- Partner Eco-system

# Hybrid cloud connectivity – WS2012 R2

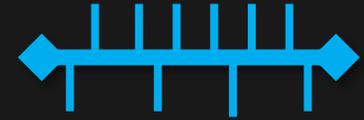


- Multitenant site-to-site network virtualization GW
- Clustering for high availability
- BGP for dynamic routing
- Multitenant NAT for internet access

# BGP Dynamic Route Learning & Best Path Selection



# New features for SDN & Network Virtualization



## Traffic blocking (ACL)

- Stateful packet inspection
- address, Port, Protocol type

## Traffic Monitoring

- Remote offline traffic capture
- Message Analyzer GUI
- Decode NVGRE packets

## Performance

- Dynamic mode NIC teaming
- Virtual RSS (use full CPU-core)
- NVGRE Hardware offload

## Network virtualization v2

- BGP dynamic route learning
- Multi-tenant Gateway feature (built-in software gateway)
- Site to site VPN & NAT
- DHCP Server on VM Network
- ICMP respond (ping -P)

## Hyper-V switch architecture v2

- NVGRE filter driver position change
- Hybrid forwarding (NVGRE & 3<sup>rd</sup> party)

# Networking partner ecosystem



**HUAWEI**

Gateway appliances

**ARISTA**

OMI-based  
top-of-rack switch



**CISCO**

**NEC**

**5NINE**  
SOFTWARE



Hyper-V switch  
extensions



**BROCADE**

Chipset  
extensions

# メラノックステクノロジー ジャパン様 よろしくお願ひします。

- 2013年 6月 6日 - プレスリリース **NEW**  
メラノックス、Hyper-V上で動作するMicrosoft Windows Server 2012を使用したVirtual Desktop Infrastructure (VDI) において仮想デスクトップの実行台数の50%増加を実現
- 2013年 6月 6日 - プレスリリース **NEW**  
メラノックスのNVGRE対応10ギガビットEthernetアダプタにより、Windows Server Hyper-Vネットワーク仮想化環境において65%も広いバンド幅の提供を実現



The screenshot shows the Mellanox website homepage. At the top, there is a navigation bar with links for Home, 会社概要, InfiniBand解説, InfiniBand製品, 高速Ethernet製品, ソフトウェア製品, ソリューション, パートナー, News, and US本社. The main content area features a grid of industry-specific solutions including EDC/CFD, Manufacturing, Green Computing, Bioscience, and Multimedia. A prominent banner on the right side reads 'オンライン販売開始!' (Online sales start!) and '最高レベルのファブリックパフォーマンスを実現' (Achieving the highest level of fabric performance). Below the main content, there is a 'プレスリリース・最新情報' (Press Release - Latest Information) section. This section contains several news items, with the first two highlighted in a red box, corresponding to the text in the adjacent image. The first item is dated June 6, 2013, and mentions a 50% increase in virtual desktop execution. The second item, also dated June 6, 2013, mentions a 65% increase in bandwidth for Hyper-V networks. Other news items include a partnership with Aviptronics, a new Ethernet adapter release, and an exhibition at Interop Tokyo 2013. The footer contains additional navigation links and the copyright notice: © 2013 Mellanox Technologies. All Rights Reserved.

Home | 会社概要 | 採用情報 | プレスリリース・最新情報 | プライバシーポリシー | 国内パートナー | US本社Webサイト  
© 2013 Mellanox Technologies. All Rights Reserved.

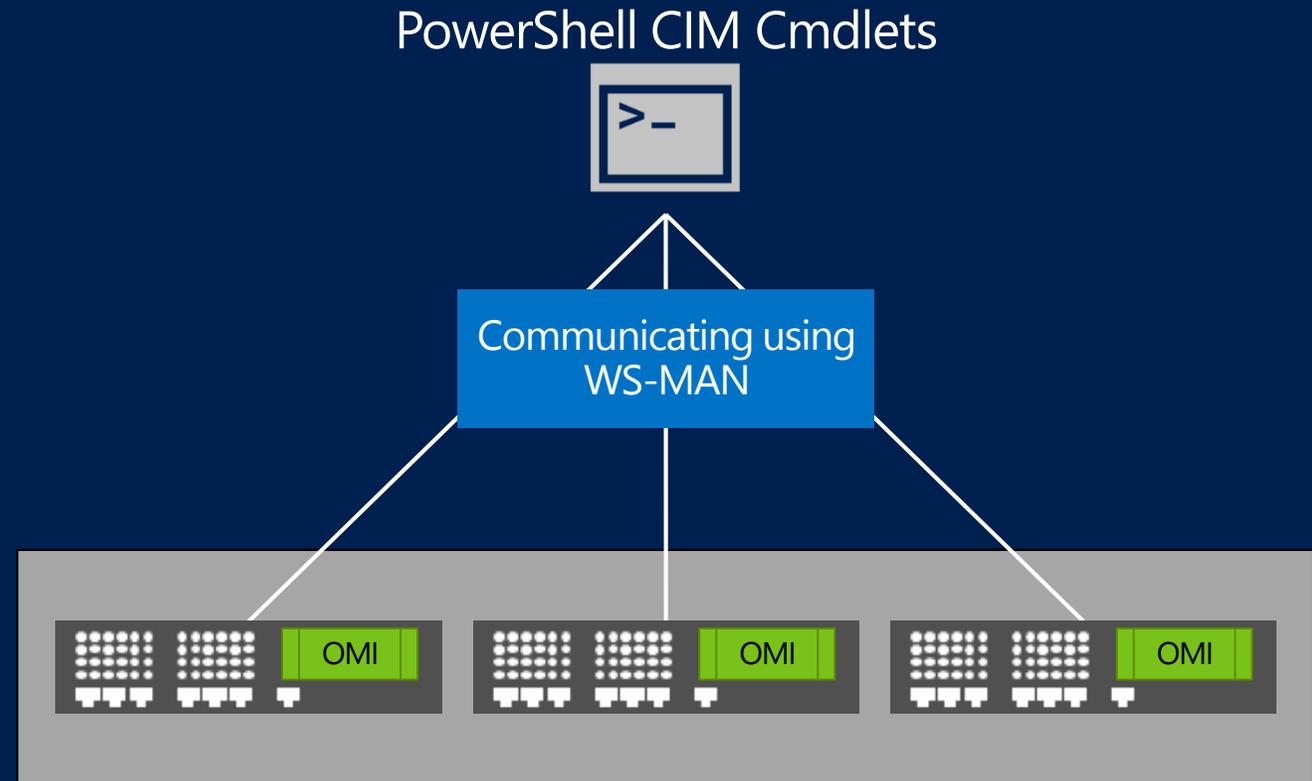
# ハードウェアとの連携は更に進む

## How switch management works

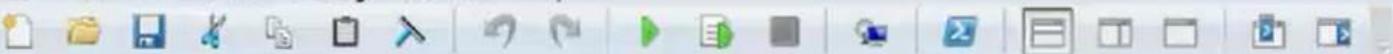
- Standards-based CIM model
- Switches running Open Management Infrastructure (OMI)
- Switch Management PowerShell Cmdlets

## Problems solved

- Common management interface across multiple network vendors
- Automate common network management tasks
- Logo Program enables customers to find/buy switches that "just work"



**Standards-based switch mgmt.**  
**enables Cloud Plug and Play by de-**  
**coupling the mgmt. plane from the data**  
**plane.**



Switch-Demo-Arista.ps1 X

```
68 #Lets see how we will do it in PS - First run in whatif mode to be sure
69 $sports = Get-SwitchEthernetPort -PortNumber 1,4 -CimSession $AristaSession
70 ### Enable Port 1 and 4
71 $sports | Enable-SwitchEthernetPort -WhatIf
72 ### Switch Switchport mode
73 $sports | Set-SwitchEthernetPort -AccessMode -AccessVlan 1 -WhatIf
74 #Note : Order of commands is not important.
75
76 #Now I am sure about my PS script - I can run it
77 $sports | Enable-SwitchEthernetPort
```

物理スイッチの  
Port & VLAN 設定を  
PowerShell で実行

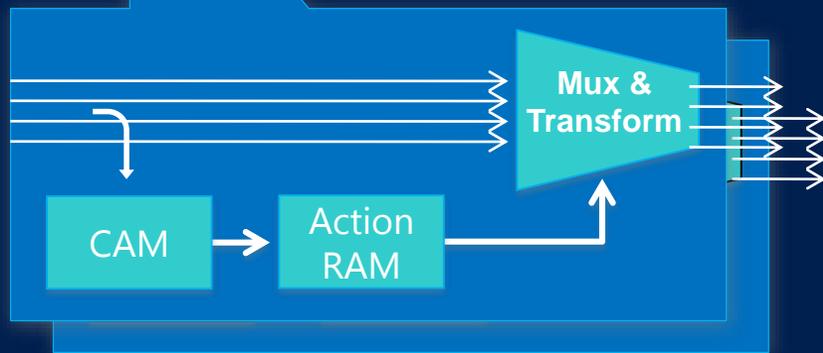
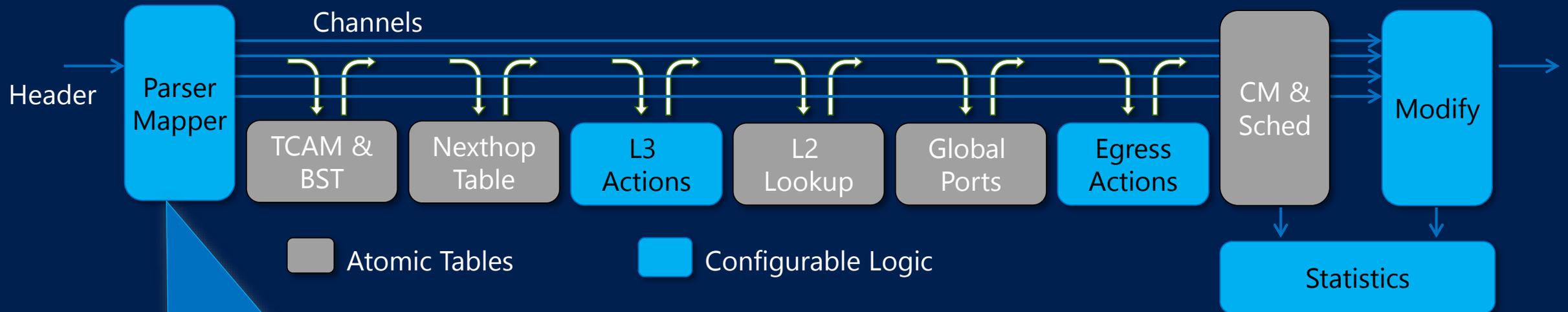
CommandType	Name	ModuleName
Function	Disable-SwitchEthernetPort	SwitchManagement
Function	Enable-SwitchEthernetPort	SwitchManagement
Function	Get-SwitchEthernetPort	SwitchManagement
Function	Get-SwitchInformation	SwitchManagement
Function	Get-SwitchVlan	SwitchManagement
Function	New-SwitchVlan	SwitchManagement
Function	Set-SwitchEthernetPort	SwitchManagement

```
PS C:\Users\cjwill\Desktop\NetworkSwitch>
```



# 時間があれば (Appendix)

# Intel® FlexPipe™ Technology



## Sample Programmable Protocols

Tunneling

TRILL, MPLS, NAT

Network Overlays

VXLAN, NVGRE

Virtualization

EVB, VEPA, VEPA+, VN-Tag

Proprietary Customer defined headers

Programmable and deterministic up to 960Mpps

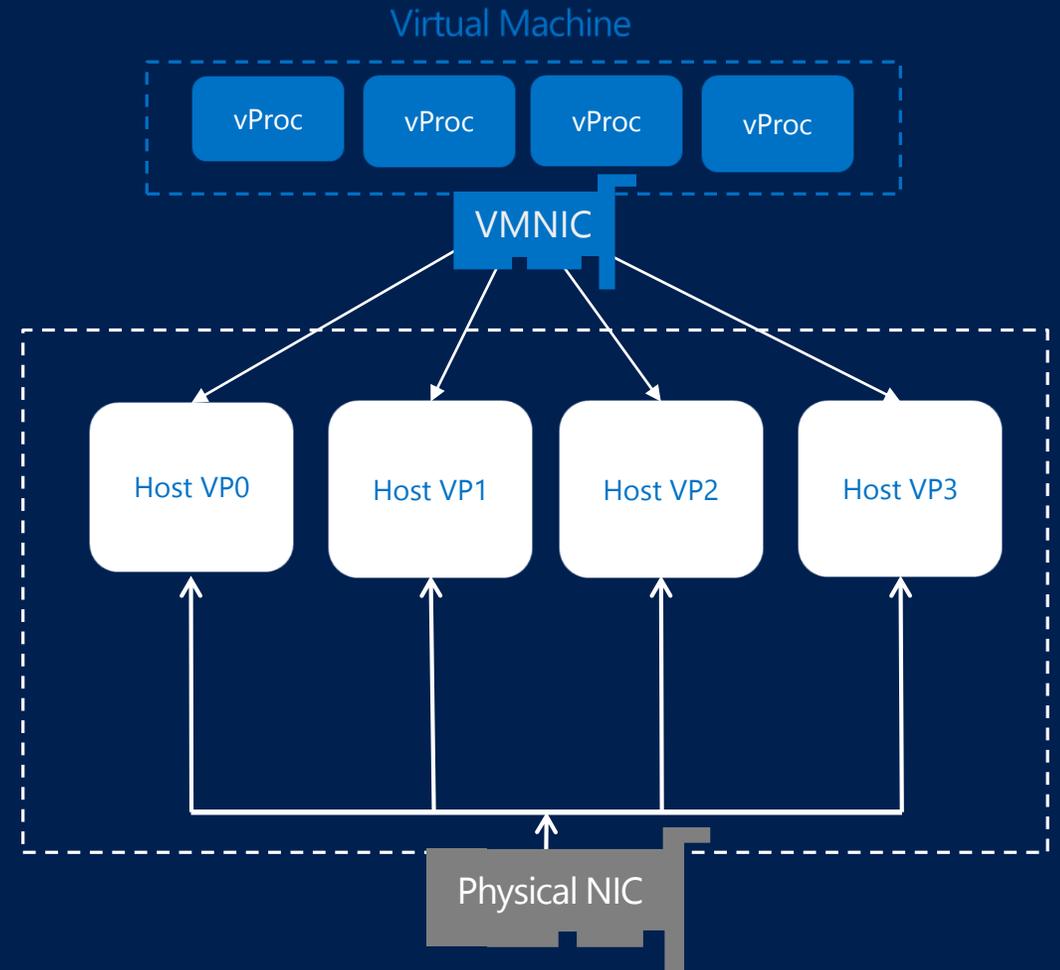
# Virtual RSS (vRSS)

## Windows Server 2012

- VMs restricted to 1 processor for network traffic processing

## Windows Server 2012 R2

- vRSS maximizes resource utilization by spreading network traffic across multiple virtual processors
- Now possible to virtualize traditionally network intensive physical workloads
- Requires no hardware upgrade and works with any NICs that support VMQ



***vRSS provides near line rate to a VM on existing hardware, making it possible to virtualize traditionally network intensive physical workloads***

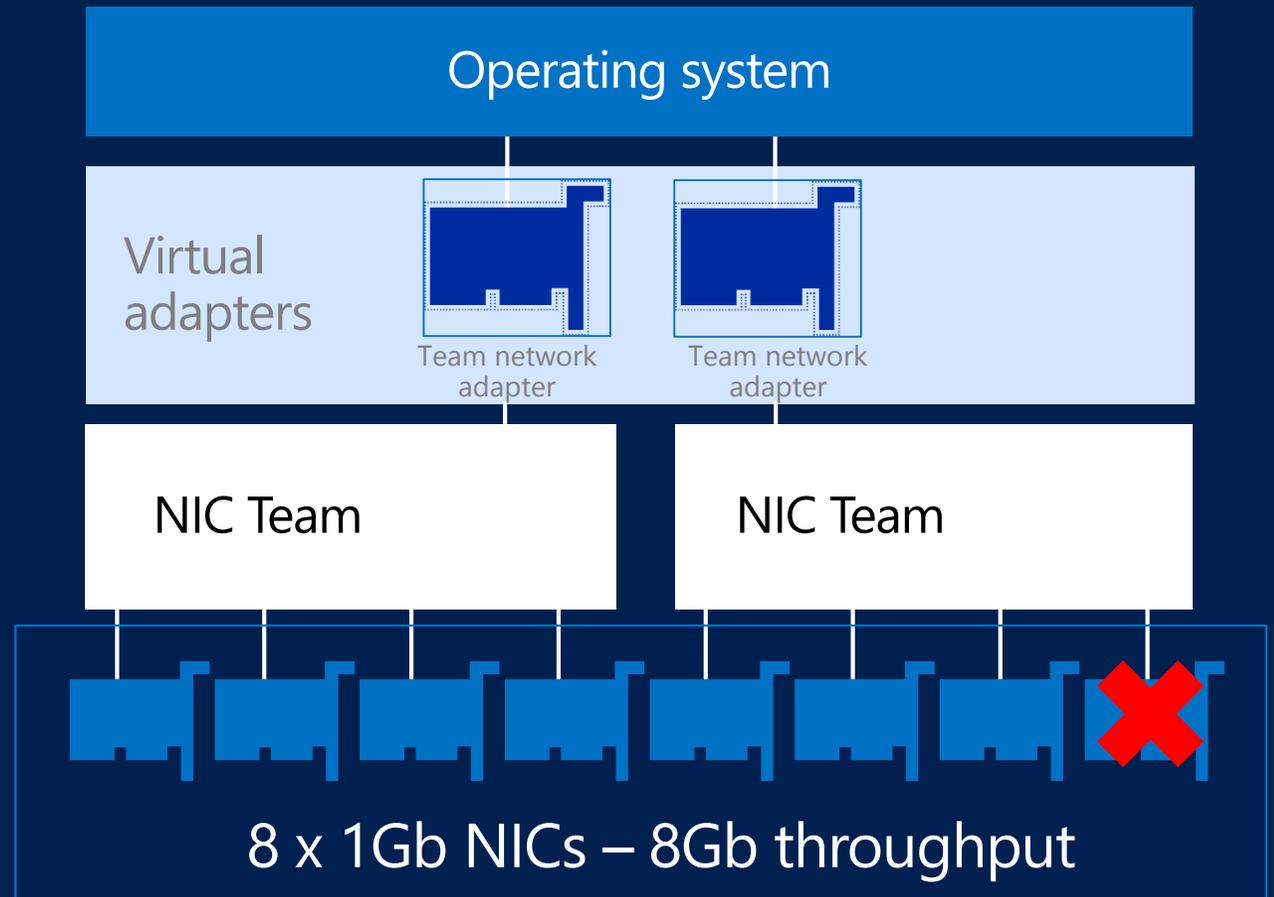
# NIC Teaming

## Windows Server 2012

- Provides network fault tolerance and continuous availability
- Aggregates bandwidth from multiple network adapters

## Windows Server 2012 R2

- Introduces a new mode, Dynamic mode.
  - Balances based on flowlets
  - Optimized utilization of a team on existing hardware



***Dynamic NIC Teaming optimizes utilization of a team on existing hardware, thereby maximizing ROI***

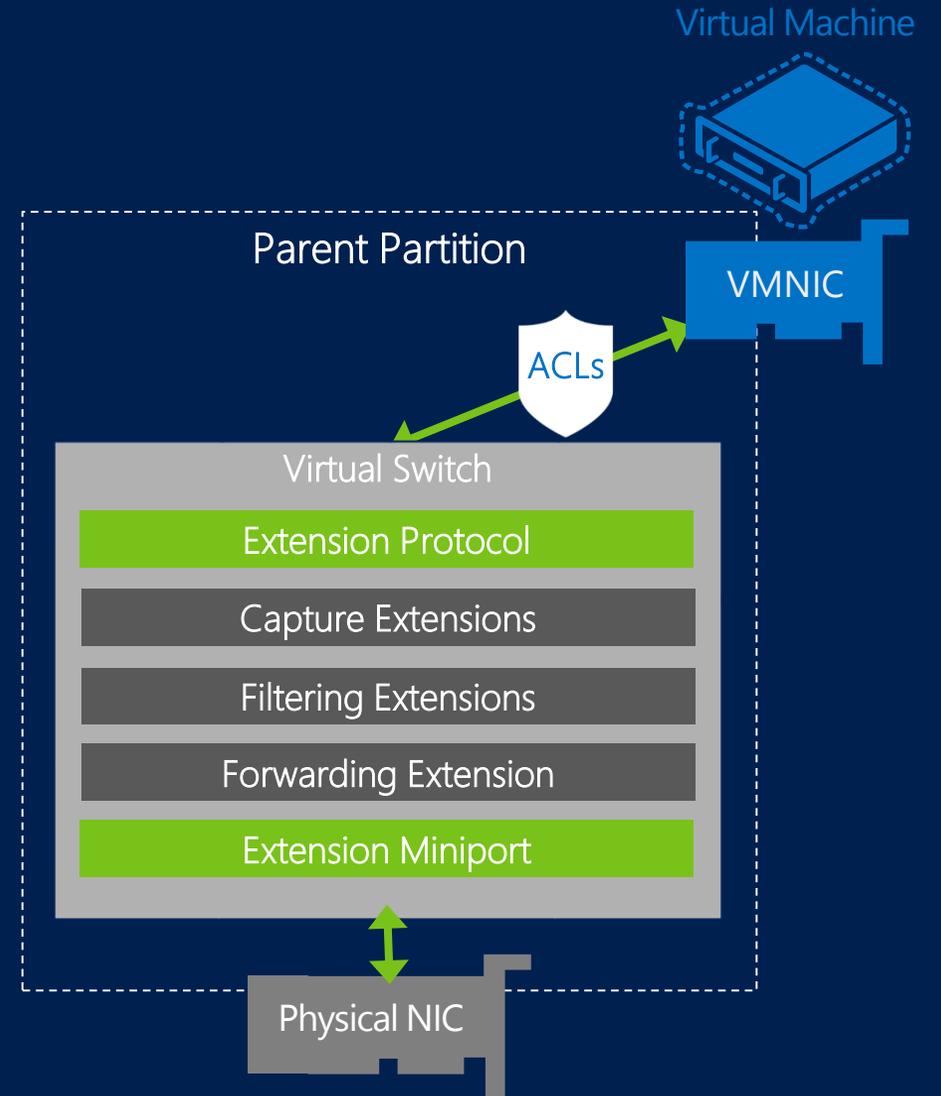
# Extended ACLs

## Windows Server 2012

- Enabled traffic to be allowed/blocked based on source and destination VM

## Windows Server 2012 R2

- Allows or blocks traffic for specific workloads
- Filter traffic based on:
  - Network address
  - Application port
  - Protocol type
- Stateful packet inspection



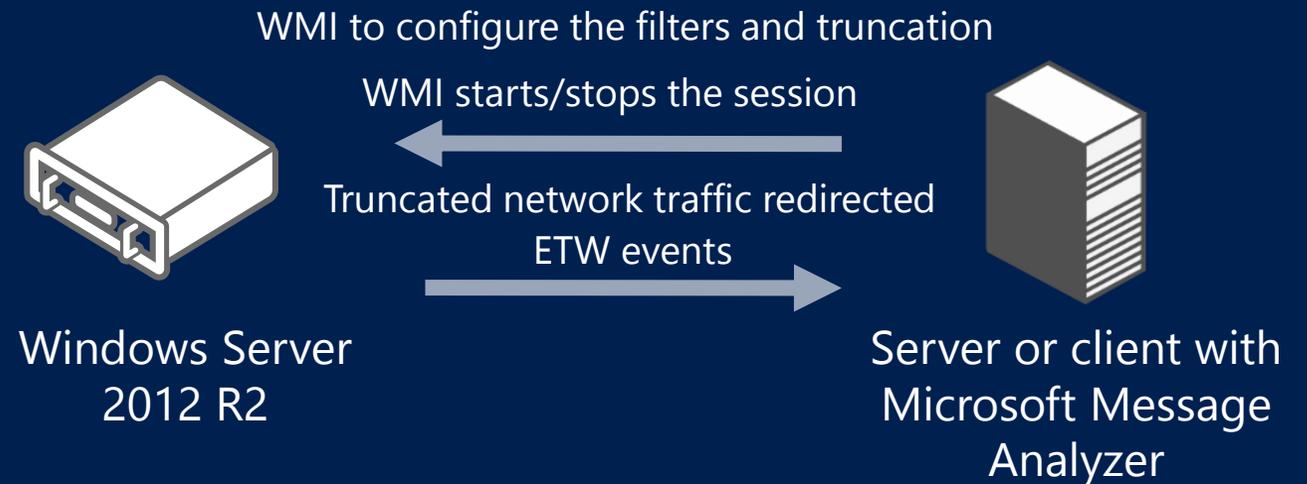
# Remote Live Monitoring

## Windows Server 2012

- Remote monitoring of network traffic is not simple

## Windows Server 2012 R2

- Mirror and capture network traffic for remote and local viewing
- GUI experience with Message Analyzer
- Supports remote offline traffic captures
- Filtering based on IP addresses and VMs



***Remote Live Monitoring provides remote packet and ETW event capture from any host in the datacenter, enabling low-touch diagnostics at high scale***

# まとめ

既にサイトは公開されています。

- ➡ Learn more about Windows Server 2012 R2 Preview, download the datasheet and evaluation from:  
<http://aka.ms/WS2012R2>
- ➡ Learn more about System Center 2012 R2 Preview, download the datasheet and evaluation from:  
<http://aka.ms/SC2012R2>

# まとめ

- ネットワークの仮想化や SDN は . . .  
仮想化エンジニアには、もはや避けて通れない道です。
- マイクロソフトの実装は . . .  
サーバー仮想化に寄り添うように作られています。
- その上で何をするか？が重要だと思っているからです。

マイクロソフトの SDN を是非ともご活用ください!!  
事例になってくれるお客様もお待ちしております。

