SAKURA Internet

www.sakura.ad.jp

# Vyatta技術詳解

2010年11月24日

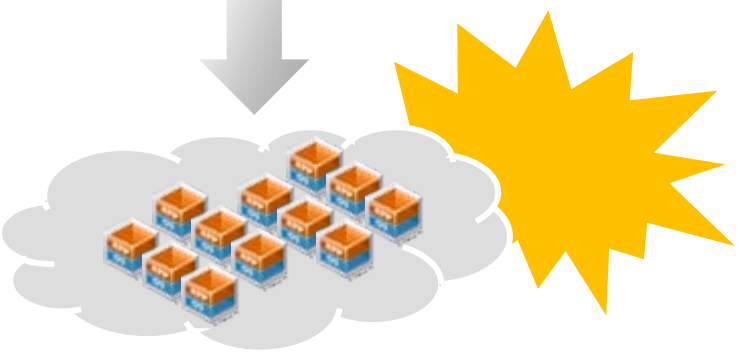
さくらインターネット研究所　上級研究員
日本Vyattaユーザー会　運営委員
松本直人

# 現在起こっているコト

SAKURA Internet

従来のコンピューティング

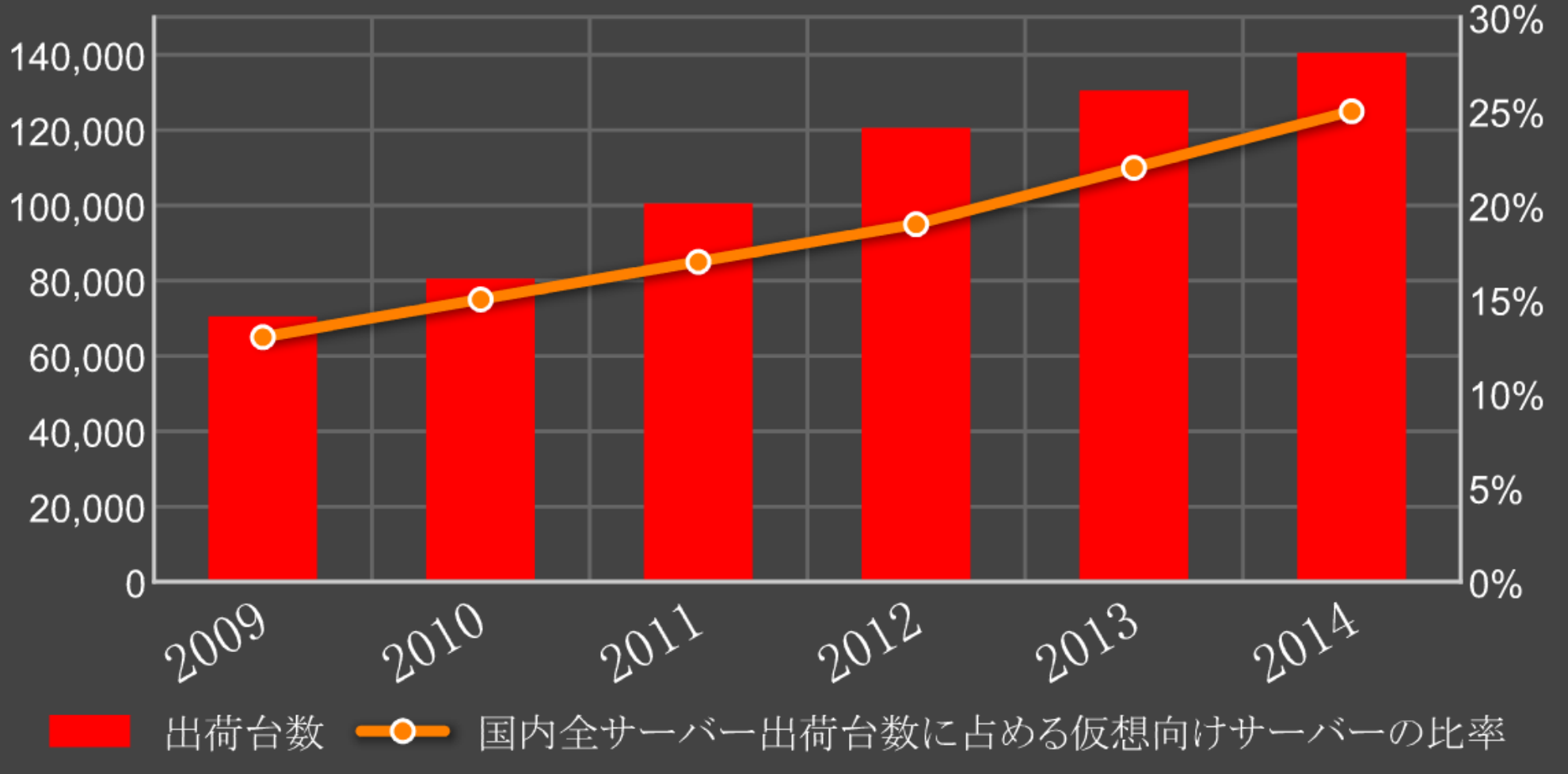
クラウド・コンピューティング



パブリック、プライベートの区別なくクラウドへ移行中

# 仮想化を取り巻く環境

出典: 国内仮想化サーバー市場 出荷台数予測、2009年～2014年 IDC Japan株式会社 (2010年10月28日作成)

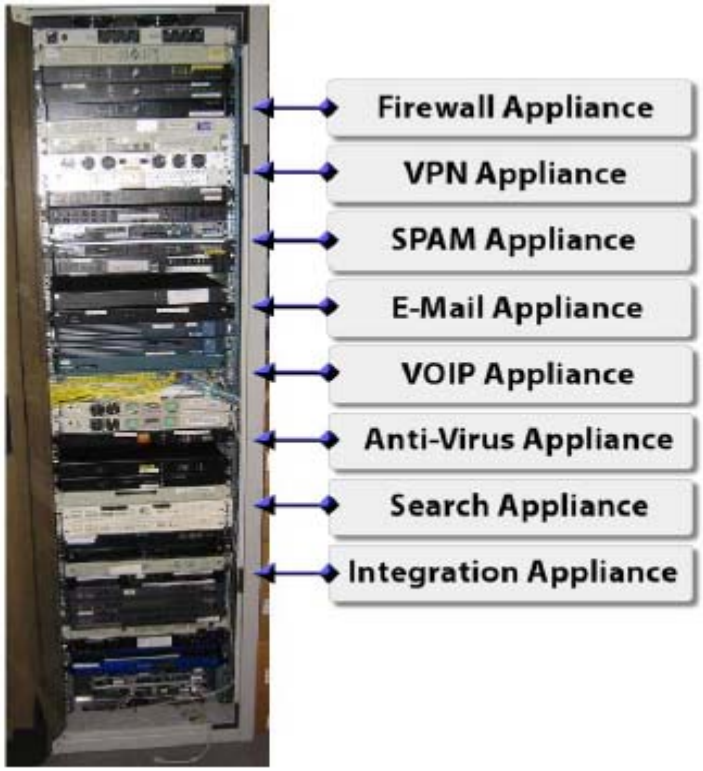



今後5年以内に国内サーバーの1/4が仮想環境となる

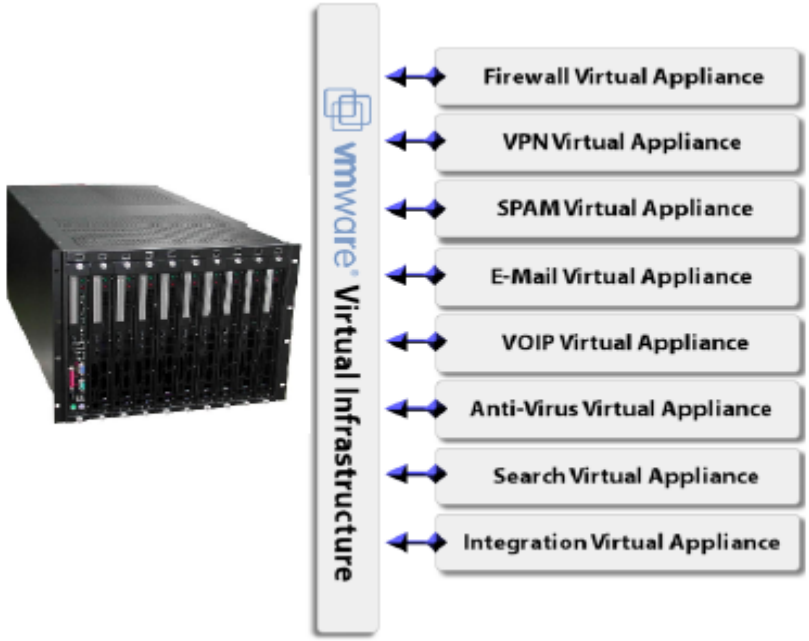
# ネットワーク機器も仮想化へ

SAKURA Internet

## 既存のシステム構成




## 仮想化技術で省力化




ネットワーク機器の仮想アプライアンス化は発展途上

# 仮想化・クラウドを取り巻く方向性

SAKURA Internet

仮想化

プライベート・クラウド

パブリック・クラウド

用途に応じた選択が、ユーザーによって行われる

# Vyattaが持つ機能

SAKURA Internet

| | | | |
|---|---|---|---|
| IPv4 / IPv6 Routing | » BGPv4, BGPv6<br>» OSPFv2, OSPFv3* | » RIPv2<br>» Static Routes | » IPv6 Policy<br>» IPv6 SLAAC |
| IP Address Management | » Static<br>» DHCP Server<br>» DHCP Client | » DHCP Relay<br>» Dynamic DNS<br>» DNS Forwarding | » DHCPv6 Server<br>» DHCPv6 Client<br>» DHCPv6 Relay |
| Encapsulations | » Ethernet<br>» 802.1Q VLANs<br>» PPP | » PPPoE<br>» IP in IP<br>» Frame Relay | » MLPPP<br>» HDLC<br>» GRE |
| Firewall | » Stateful Inspection Firewall<br>» Zone-based Firewall<br>» P2P Filtering | » IPv6 Firewalling<br>» Time-based Firewall Rules<br>» Rate Limiting | » ICMP Type Filtering<br>» Stateful Failover |
| Tunneling / VPN | » SSL-based OpenVPN<br>» Site to Site VPN (IPSec)<br>» Remote VPN (PPTP, L2TP, IPSec) | » OpenVPN Client Auto-Configuration<br>» Layer 2 Bridging over GRE<br>» Layer 2 Bridging over OpenVPN | |
| Additional Security | » Network Address Translation<br>» Sourcefire VRT Intrusion Prevention<br>» VyattaGuard Web Filtering | » DES, 3DES, AES Encryption<br>» MD5 and SHA-1 Authentication<br>» RSA, Diffie Helman Key Mgmt | » NAT Traversal<br>» Role based access control |
| WAN / LAN Device Drivers | » WAN Device Drivers - ADSL, T1, T3<br>» Intel 10/100Mbps - 10Gbps | » IEEE 802.11 wireless<br>» Drivers in 2.6.31 Linux Kernel | » Synchronous Serial<br>- V.35, X.21, RS-422, EIA530 |
| Performance Optimization | » WAN Link Load Balancing<br>» Ethernet Link Bonding<br>» Web Caching | » MLPPP<br>» ECMP<br>» Bandwidth Management | |
| QoS Policies | » Priority Queuing<br>» Network Emulator<br>» Round Robin | » Random / Weighted Random<br>» Classful Queuing<br>» Ethernet Header Matching | » VLAN Tag<br>» IPv6 Address<br>» Port Mirroring |
| High Availability | » Stateful Firewall / NAT Failover<br>» VRRP<br>» HA Clustering | » Configuration Replication<br>» RAID 1 | » IPSec VPN Clustering<br>» Protocol Fault Isolation |
| Administration & Authentication | » Integrated CLI<br>» Web GUI<br>» Vyatta Remote Access API | » Telnet<br>» SSHv2 / SSH Public Key<br>» Binary Image Install | » RADIUS<br>» TACACS+*<br>» Single Configuration File |
| Diagnostics & Logging | » tcpdump<br>» Wireshark Packet Capture<br>» BGP MD5 Support | » Serial Loopback Commands<br>» Netflow / sFlow<br>» LLDP | » Syslog<br>» SNMPv2c<br>» SNMP for IPv6 |

# VyattaCore提供方式

SAKURA Internet

*http://www.vyatta.org/downloads*

**virt.ISO**

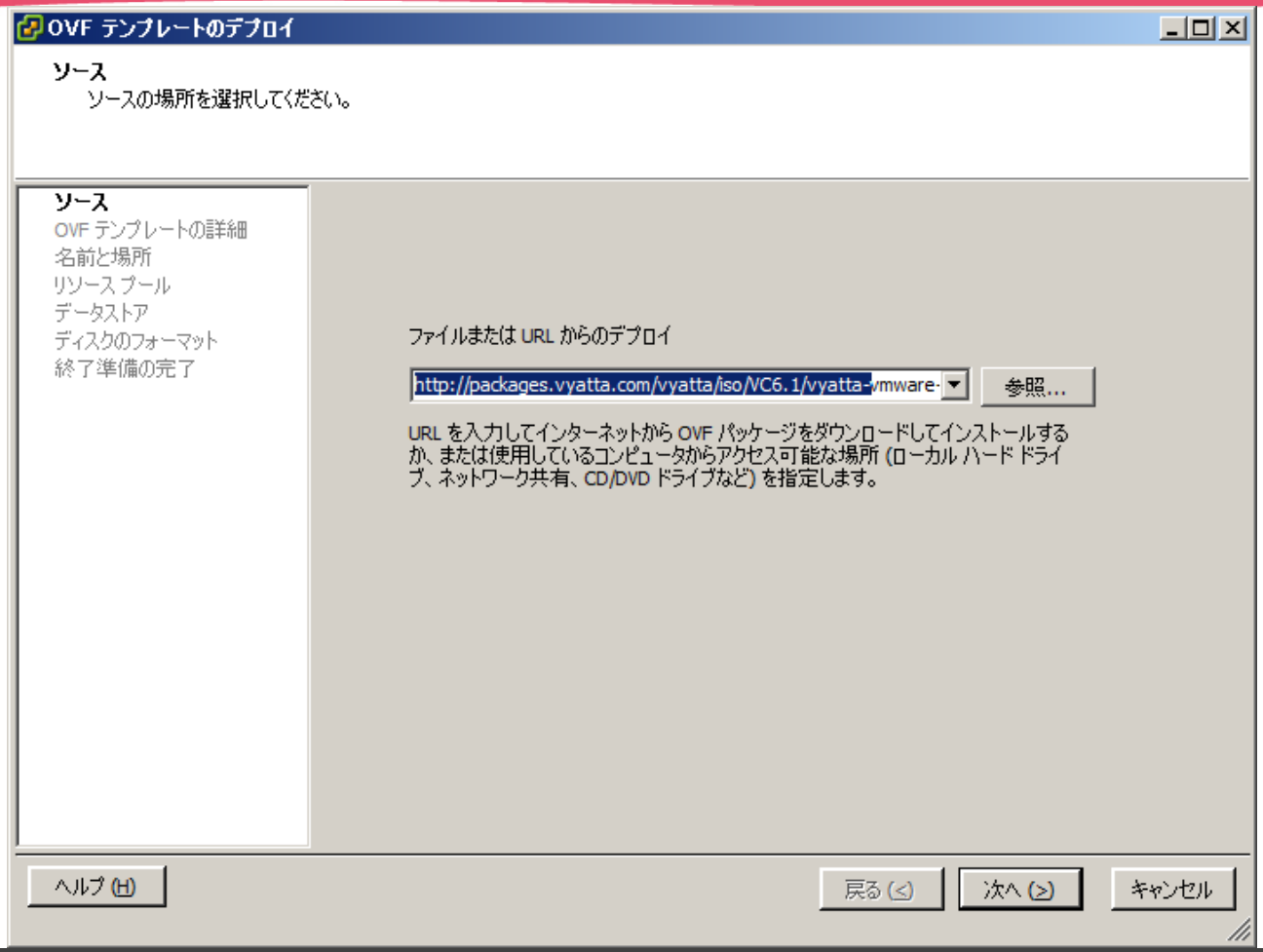

**VMware OVF**


**XenServer XVA**

**LiveCD**

ユーザー環境に応じて、システム・イメージを選択が可能

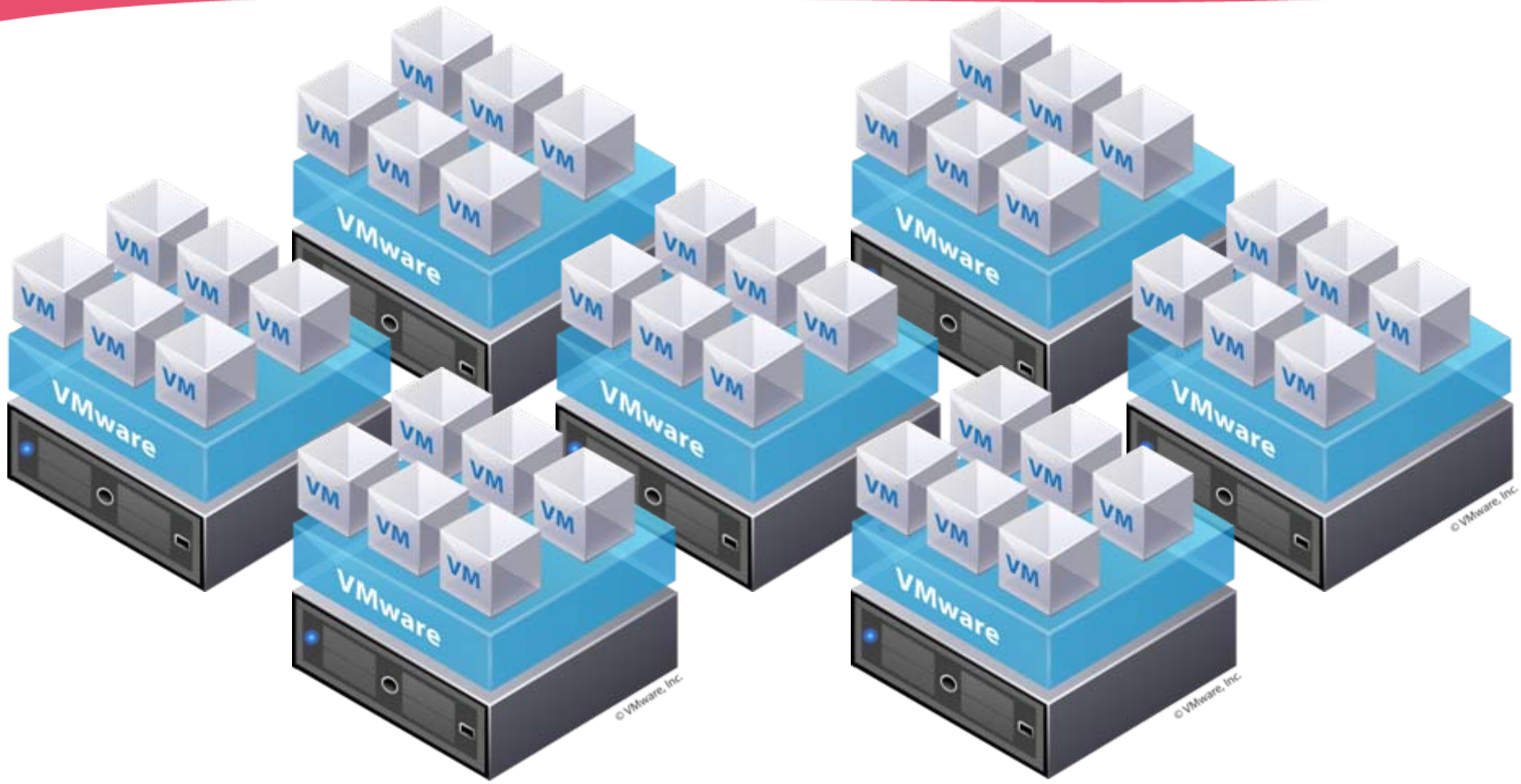
# OVFによるDeploy方法




Open Virtualization Format
(Distributed Management Task Force)

# クラウド時代のVyattaの使われ方

SAKURA Internet




仮想ルーターとして、クラウド環境で場所を選ばず利用できる

# Command Line Interface

SAKURA Internet

```
% configure
# set system login user vyatta authentication plaintext-password PaSs

# show system login user vyatta
 authentication {
     encrypted-password $1$7l1Ez1nG$.RxXs53Q3Vc./3PQjGMQ/.
     plaintext-password “”
}

# commit
# save
```

ユーザー・モードと管理者モードの2つで運用管理する

# TAB Explanation

SAKURA Internet

```
# set system [TAB][TAB]
Possible completions:
  domain-name          System domain name
  domain-search        Domain Name Server (DNS) domain completion
  flow-accounting      Flow accounting settings
  gateway-address      Default gateway
  host-name            System host name (default: vyatta)
  ip                   IPv4 settings
  ipv6                 IPv6 settings
  login                User login
  name-server          Domain Name Server (DNS)
```

TABキーでヘルプを参照しながらコマンド操作が可能

# Run and Shell commands

SAKURA Internet

```
# run show system routing-daemons
  zebra ripd ripngd ospfd ospf6d bgpd

# ls -al /
 total 56
 drwxr-xr-x  1 root root         4096 Nov 10 08:24 .
 drwxr-xr-x  1 root root         4096 Nov 10 08:24 ..
 drwxr-xr-x  1 root root         4096 Oct 27 01:15 bin
 drwxr-xr-x  4 root root         4096 Oct 27 01:23 boot
 drwxrwxr-x  1 root vyattacfg 4096 Nov 10 08:24 config
 drwxr-xr-x 13 root root         3100 Nov 10 08:24 dev
```

管理者モードからユーザーモード機能やシェルを呼び出す

# BASIC Configuration

SAKURA Internet

```
set interfaces ethernet eth0 address 10.10.10.10/24
set system gateway-address 10.10.10.1

set system name-server 10.10.10.99
set system name-server 10.10.10.88
set interfaces ethernet eth1 address 192.168.168.10/24
set service ssh
set system time-zone Asia/Tokyo
set system syslog host 10.10.10.222 facility all level info
commit
```

基本的なルーター設定は、既存のルーター製品と全く同じ

# SNMP Configuration

SAKURA Internet

```
set service snmp community TEST
set service snmp community TEST client 10.10.10.123
set service snmp community TEST authorization rw

set service snmp trap-source 10.10.10.10
set service snmp trap-target 10.10.10.123
commit
```

SNMPコミュニティ設定

# xFlow Configuration

SAKURA Internet

```
set system flow-accounting interface eth0
set system flow-accounting sflow sampling-rate 100
set system flow-accounting sflow agent-address auto
set system flow-accounting sflow server 10.10.10.123 port 6343
commit

set system flow-accounting sflow sampling-rate [TAB]
Possible completions:
 <0-4294967295>
              Sampling rate (1 in N packets)
#
```

* export this information to Netflow or sFlow-compatible collection servers.

ネットワークフロー情報取得と

# DHCP and NAT Configuration

SAKURA Internet

```
edit service dhcp-server shared-network-name DHCP_POOL
set subnet 192.168.168.0/24 start 192.168.168.2 stop 192.168.168.9
set subnet 192.168.168.0/24 default-router 192.168.168.10
set subnet 192.168.168.0/24 dns-server 10.10.10.99
exit

set service nat rule 99 source address 192.168.168.0/24
set service nat rule 99 outbound-interface eth0
set service nat rule 99 type masquerade
commit
```

DHCPとNAT設定にも、特にクセはない

# BASIC Firewall Configuration

SAKURA Internet

```
edit firewall name FWv4
set default-action reject
set rule 99 source address 10.10.20.0/24
set firewall name FWv4 rule 99 action accept
exit

set interfaces ethernet eth0 firewall in name FWv4
commit
```

標準的なフィルタリング規則を設定可能

# PPTP Remote VPN Configuration

SAKURA Internet

```
edit vpn pptp remote-access
set outside-address 10.10.10.10
set client-ip-pool start 192.168.168.11
set client-ip-pool stop 192.168.168.19
set authentication local-users username pptp1 password PaSs
set dns-servers server-1 10.10.10.99
set dns-servers server-2 10.10.10.88
commit
```

内部ネットワーク接続でルーティングやNAT設定も要確認

# Vyatta's Networking Functions

SAKURA Internet

VLAN, Bridging, Ethernet Bonding, Serial, DSL, Wireless Modem,
HDLC, FR, IPoA, PPP, PPPoE, PPPoA, Multilink PPP,
GRE, IP-in-IP Tunnels, SIT Interfaces

IPv4, IPv6, Static,  BGP, OSPF, RIP, Policy Routing Engines

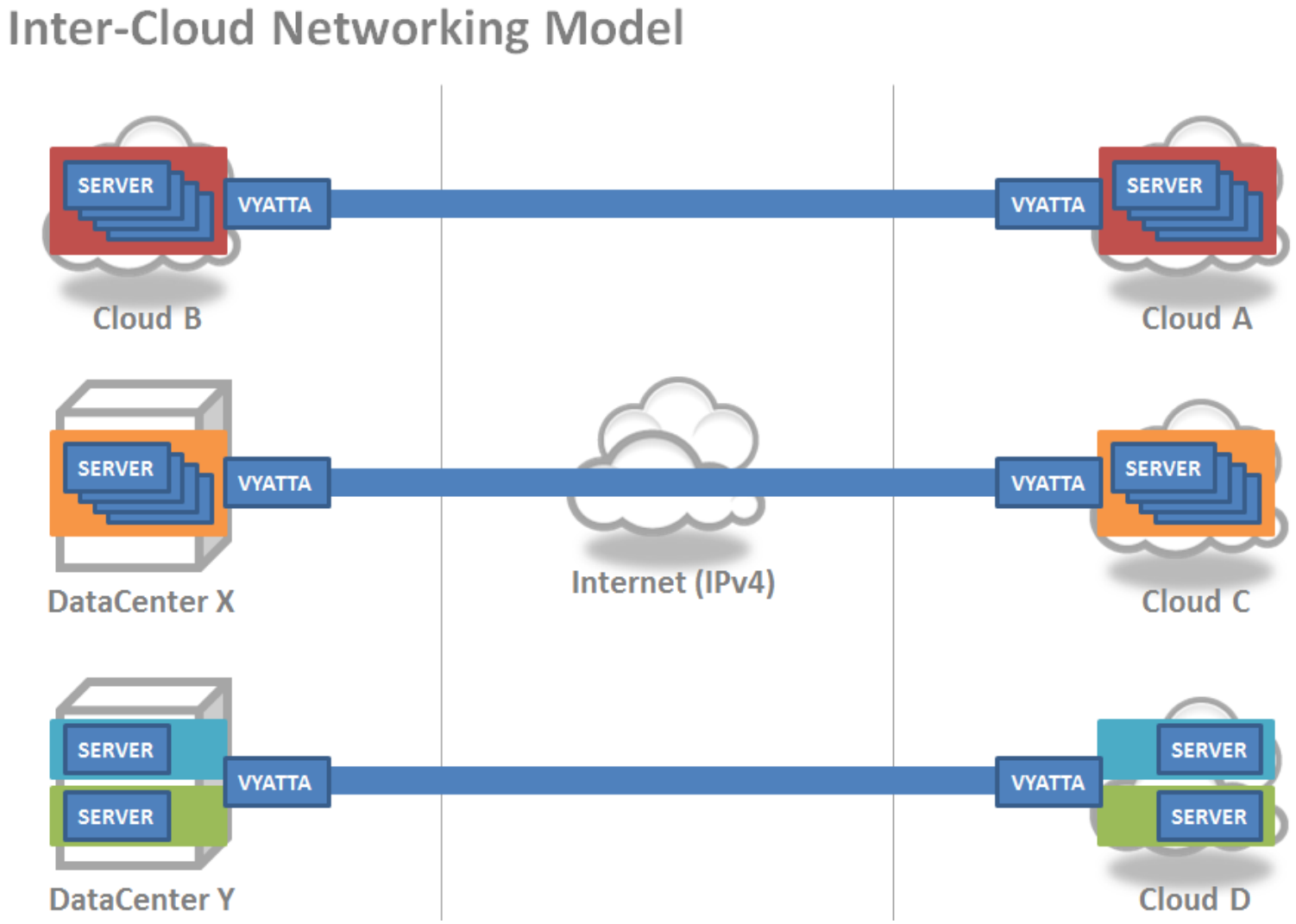
IDS, IPS, PPTP, L2TP, OpenVPN, IPsec, IPv4-IPv6 Firewall,
Web Filter, QoS Functions

Config Replication, WAN LB, Clustering, VRRP, RAID1 Functions

VyattaCoreが提供する全ての機能 (再確認)

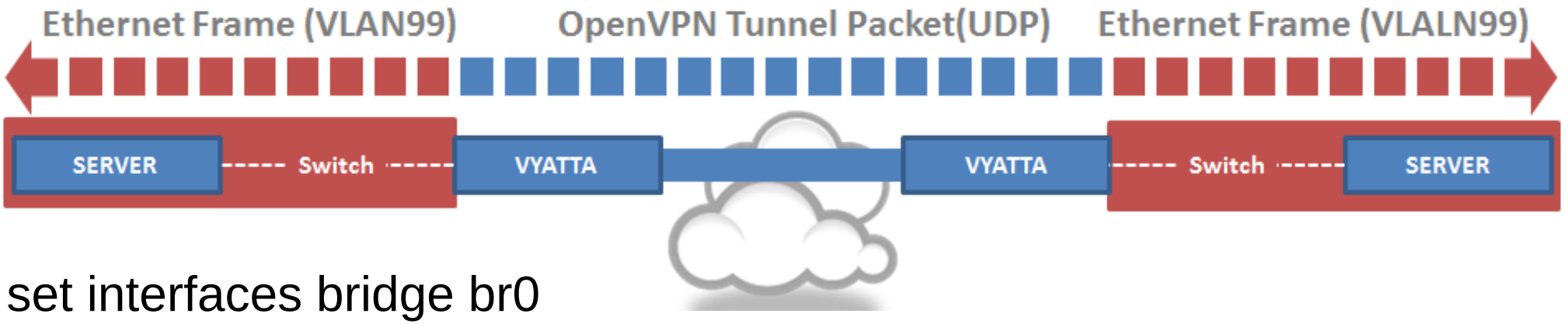
# インタークラウドで設備のシームレス化

SAKURA Internet



# Layer2 Bridging Configuration

SAKURA Internet

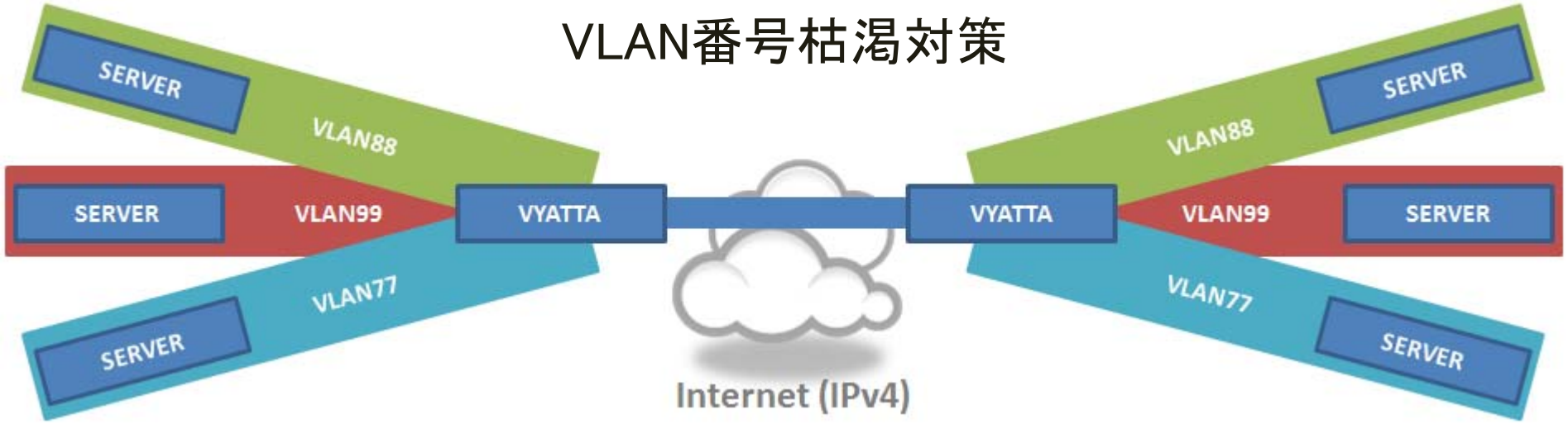



```
set interfaces bridge br0
set interfaces ethernet eth1 bridge-group bridge br0
set interfaces openvpn vtun0 bridge-group bridge br0
set interfaces openvpn vtun0 mode site-to-site
set interfaces openvpn vtun0 remote-host X.X.X.X
run vpn openvpn-key generate /root/key
set interfaces openvpn vtun0 shared-secret-key-file /root/key
```

Ethernetフレームを遠隔地まで飛ばし、シームレスにつなぐ

# Against VLAN Exhaustion

SAKURA Internet




```
set interfaces ethernet eth0 vif 66 address A.A.A.A/24
set interfaces ethernet eth0 vif 77 address B.B.B.B/24
set interfaces ethernet eth0 vif 88 address C.C.C.C/24
set interfaces ethernet eth0 vif 99 address D.D.D.D/24
```

管理セグメントのVLAN番号の制約を受けないネットワーク設計

SAKURA Internet

```
set interfaces ethernet eth0 address 2001:db8:a::1/64
set interfaces ethernet eth1 address 2001:db8:b::2/64
delete system ipv6 disable-forwarding

set protocols static route6 ::/0 next-hop 2001:db8:a::99/64

set firewall ipv6-name FWv6 default-action reject
set firewall ipv6-name FWv6 rule 66 source address 2001:db8:a::0/64
set firewall ipv6-name FWv6 rule 66 action accept
set interfaces ethernet eth0 firewall in ipv6-name FWv6
commit
```

小規模なIPv6 Networkingから開始できる機能を保持

# Against Denial of Service Attack

SAKURA Internet

```
set firewall name STOP-DoS default-action accept

set firewall name STOP-DoS rule 99 protocol tcp
set firewall name STOP-DoS rule 99 destination port 80
set firewall name STOP-DoS rule 99 state new enable
set firewall name STOP-DoS rule 99 recent count 99
set firewall name STOP-DoS rule 99 recent time 10

set firewall name STOP-DoS rule 99 action drop
set interfaces ethernet eth0 firewall in name STOP-DoS
```

VyattaCore version 6.1 2010.08.20
Build ID 1008200448-170b446

同一IPアドレスから10秒間に99回以上のトラフィックは遮断

# Add New media type / Infiniband

SAKURA Internet

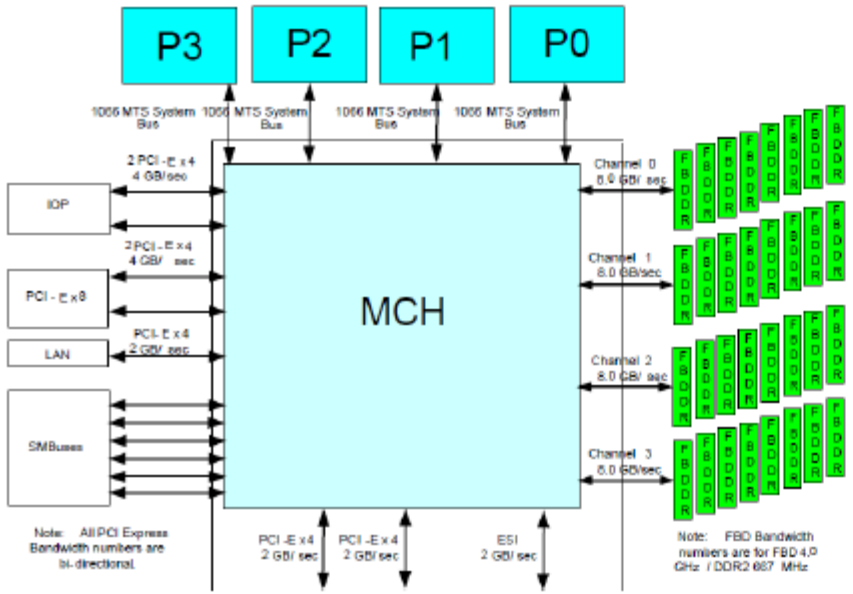
```
sudo full-upgrade -k
sudo apt-get update
sudo aptitude install module-assistant
sudo apt-get install rpm zlib1g-dev zlib1g-dbg
sudo aptitude intall byacc bison flex
sudo module-assistant prepare
sudo /opt/OFED-1.5.2/install.pl
sudo vi /etc/udev/rules.d/75-persistent-net-generator.rules
 :

set interfaces inifniband ib0 address 1.1.1.1/24
commit
```

OpenFabrics Enterprise Distribution (OFED)でIPoIB機能追加

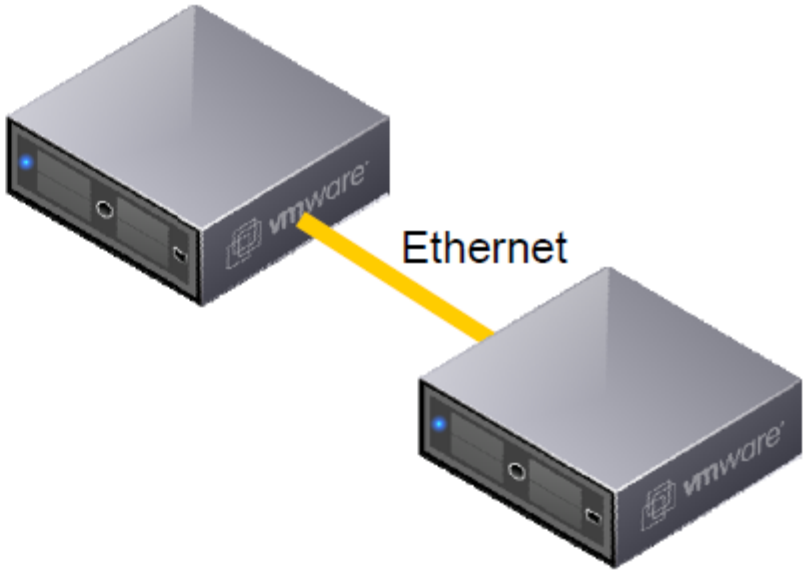
# 仮想ルータの性能課題を把握

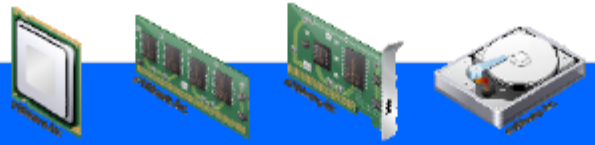
SAKURA Internet

## バス・ボトルネック




## インターフェイス・ボトルネック



仮想化技術であってもパフォーマンスは、コンポーネントの性能限界につよく依存している

# 仮想ルーターの性能を左右する要素

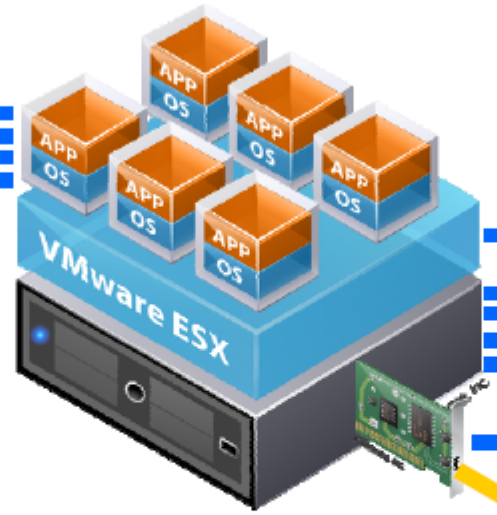
SAKURA Internet

アプリ性能(VM)

カーネル性能(VM)

ディスク性能(VM)

NIC性能(VM)




VMM性能(物理)

CPU性能(物理)

メモリ性能(物理)

バス性能(物理)

ディスク性能(物理)

NIC性能(物理)

# ソフトウェアルーターならではの壁を理解

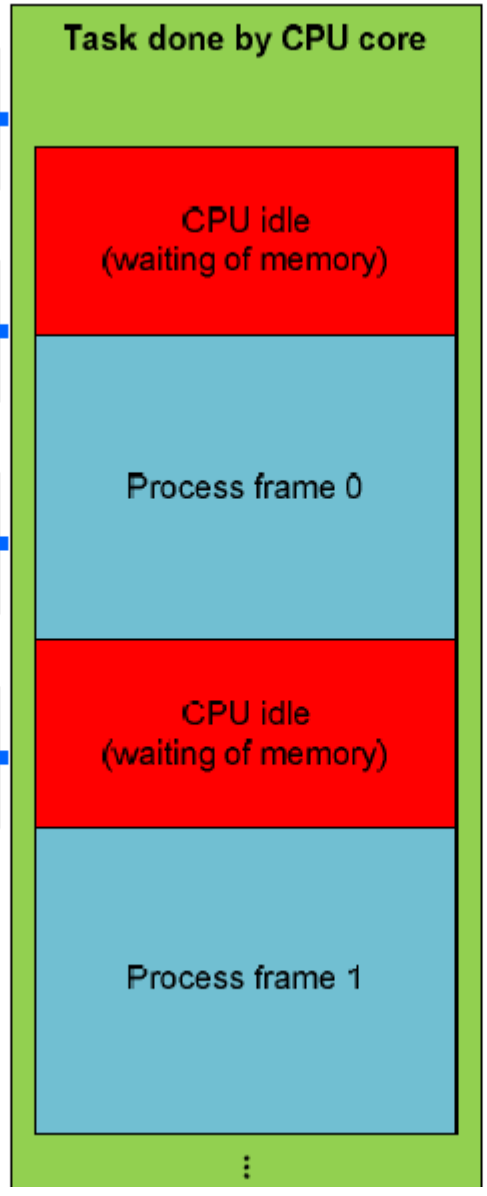
SAKURA Internet

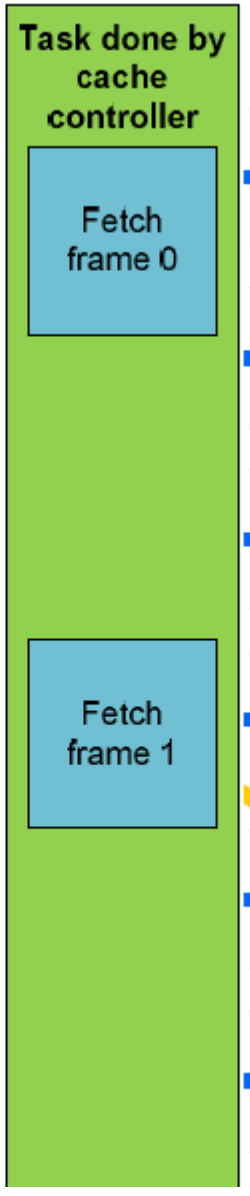
アプリ性能(VM)

カーネル性能(VM)

ディスク性能(VM)

NIC性能(VM)




VMM性能(物理)

CPU性能(物理)

メモリ性能(物理)

バス性能(物理)

ディスク性能(物理)

NIC性能(物理)

# しっかりと理解すべき仮想化との付き合い方

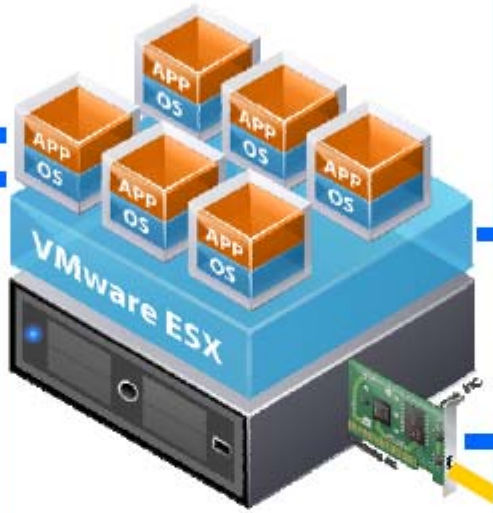
SAKURA Internet

カーネル性能(VM)

カーネル
パラメーター
設定

NIC性能(VM)

NICドライバ
設定




VMM性能(物理)

CPU
アフィニティ
設定

NICドライバ
キュー設定
(VMDq)

NIC性能(物理)

Intel Virtual Machine Device Queues (VMDq)

SAKURA Internet

www.sakura.ad.jp

# ご静聴誠にありがとうございました