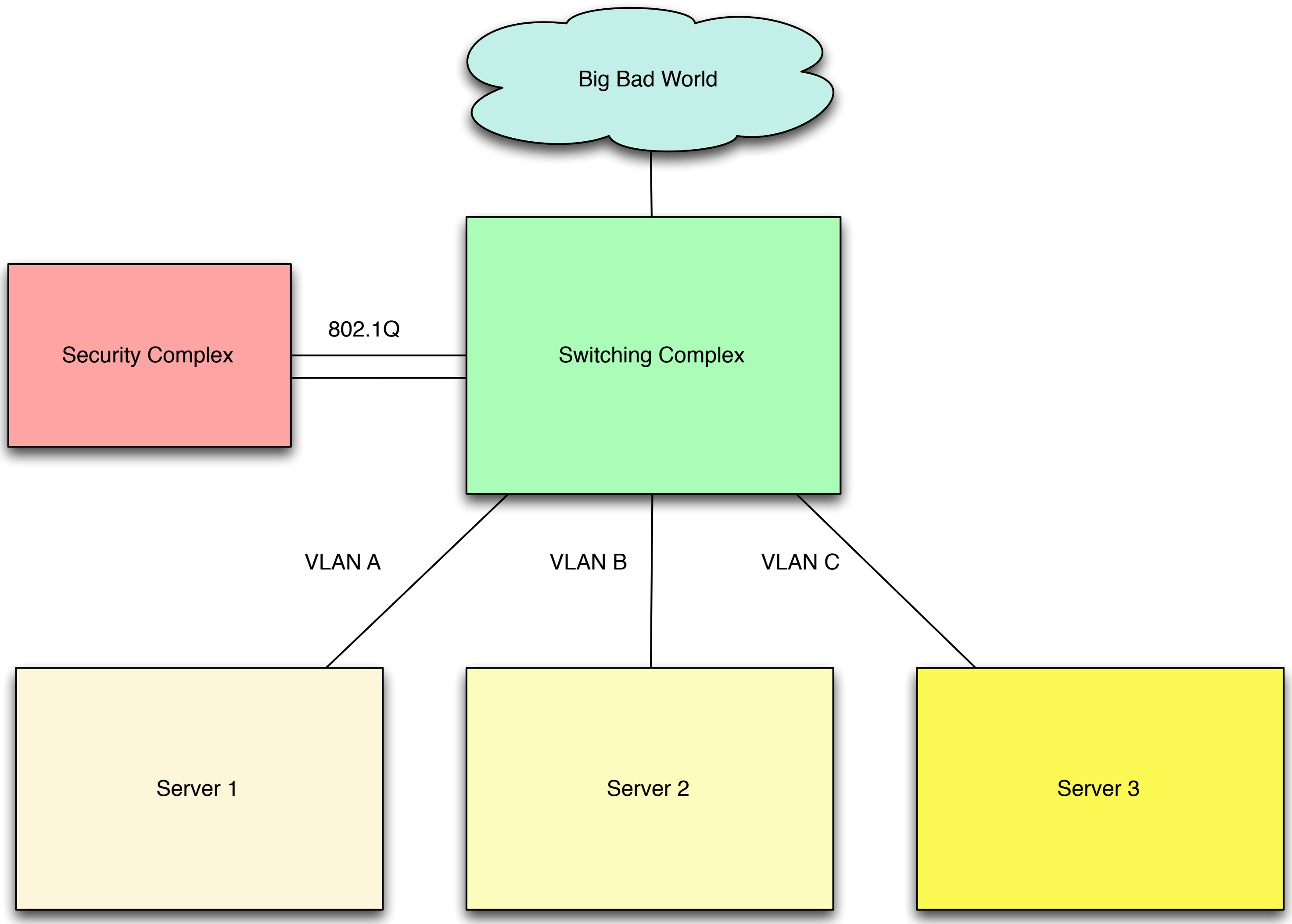
STORMY WEATHER
SECURING CLOUD COMPUTING

Russell Skingsley
Director of Advanced Technology
Data Centre and Cloud, APAC
Juniper Networks

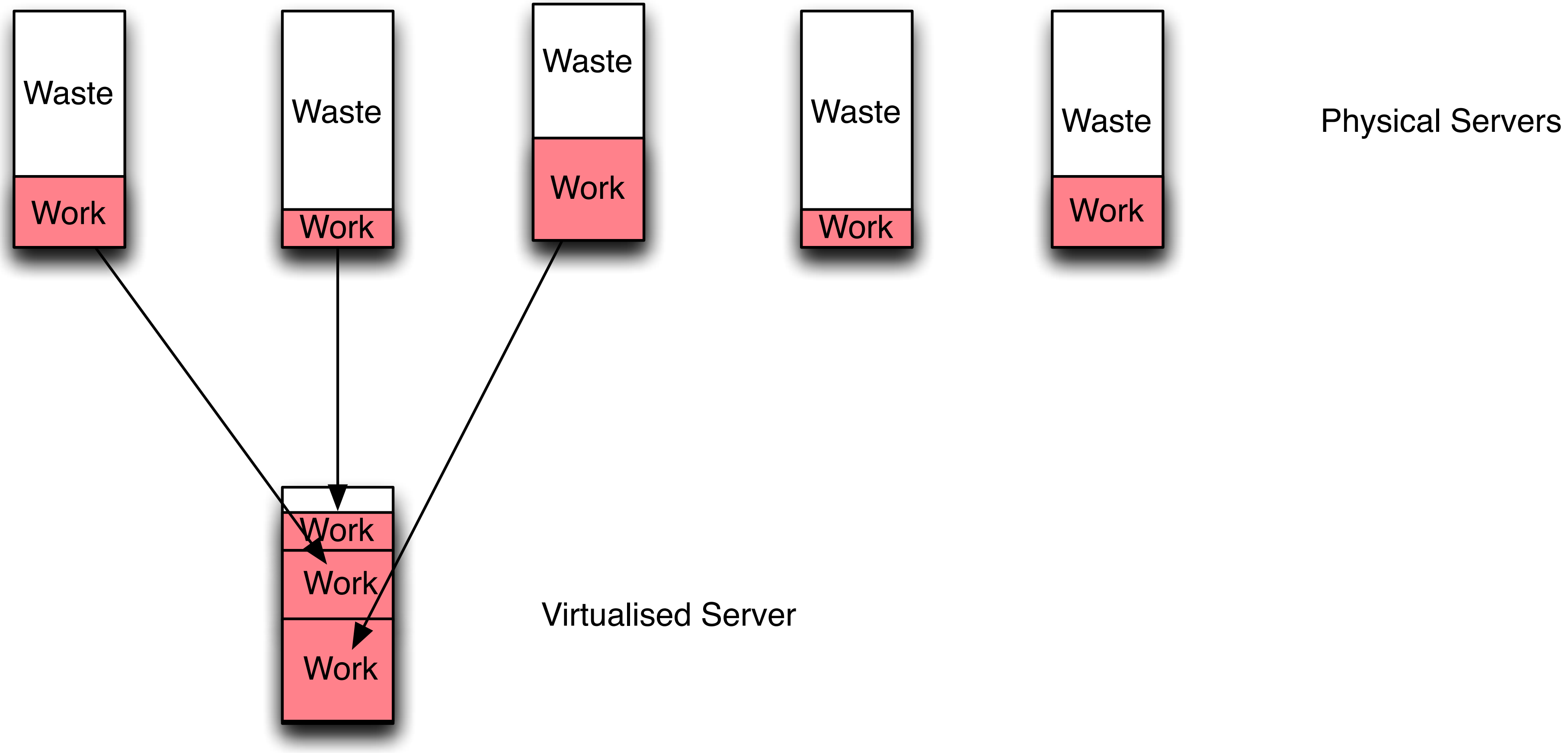
DISCLAIMER

These are not necessarily the views of Juniper Networks even though I have pilfered some of their slides for my own nefarious purposes.

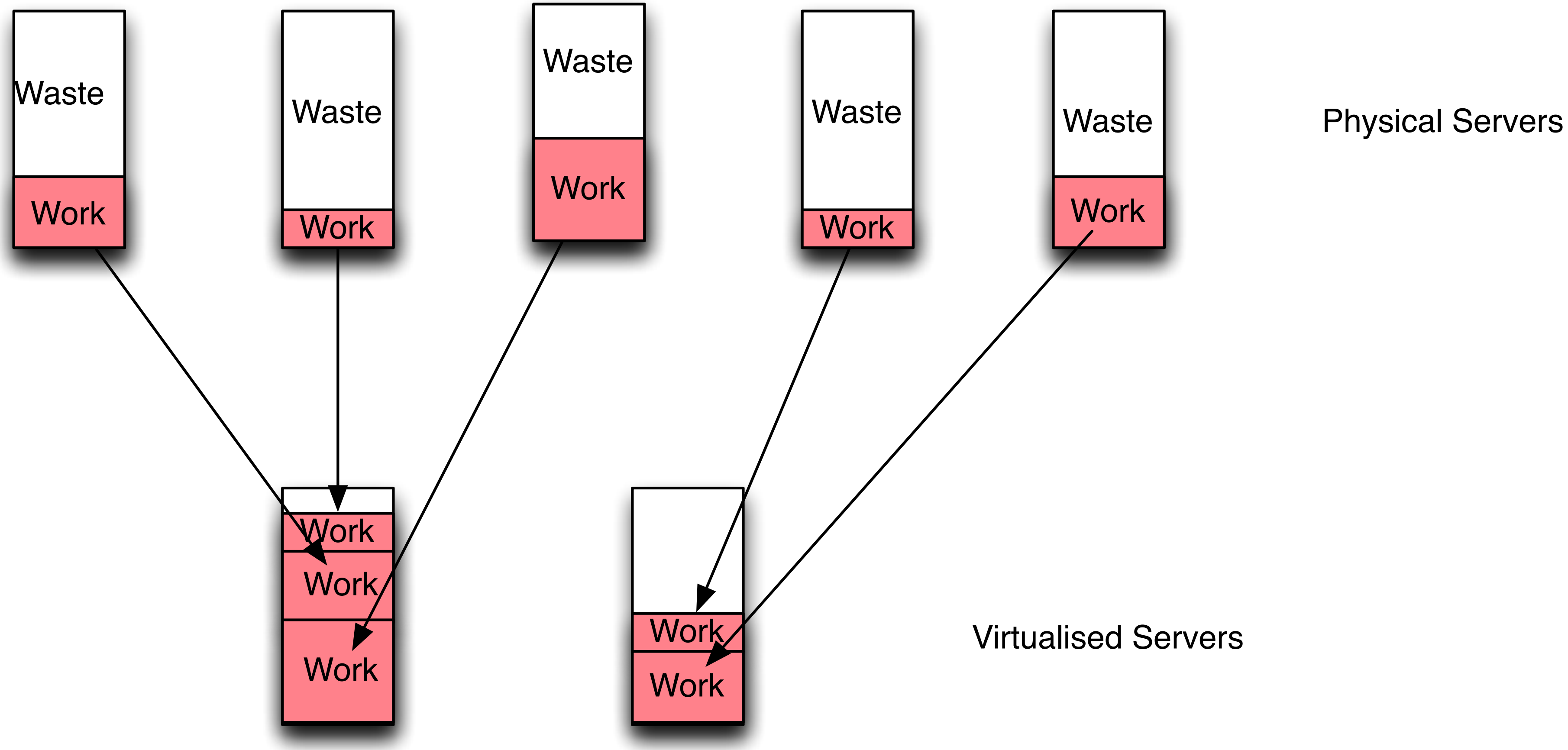
TRADITIONAL DC NETWORK SECURITY



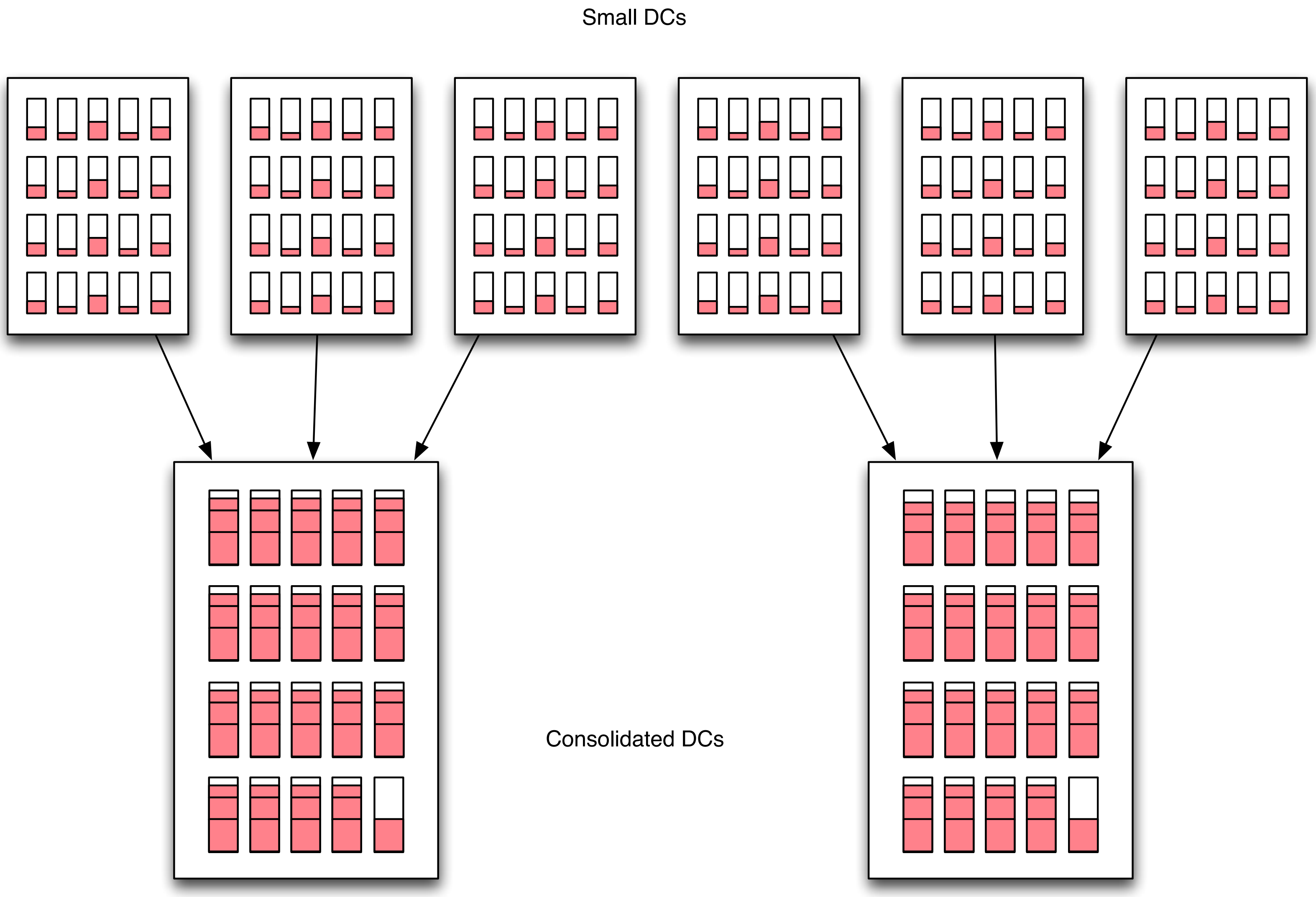
THE PRINCIPLE OF CONSOLIDATION – PER SERVER



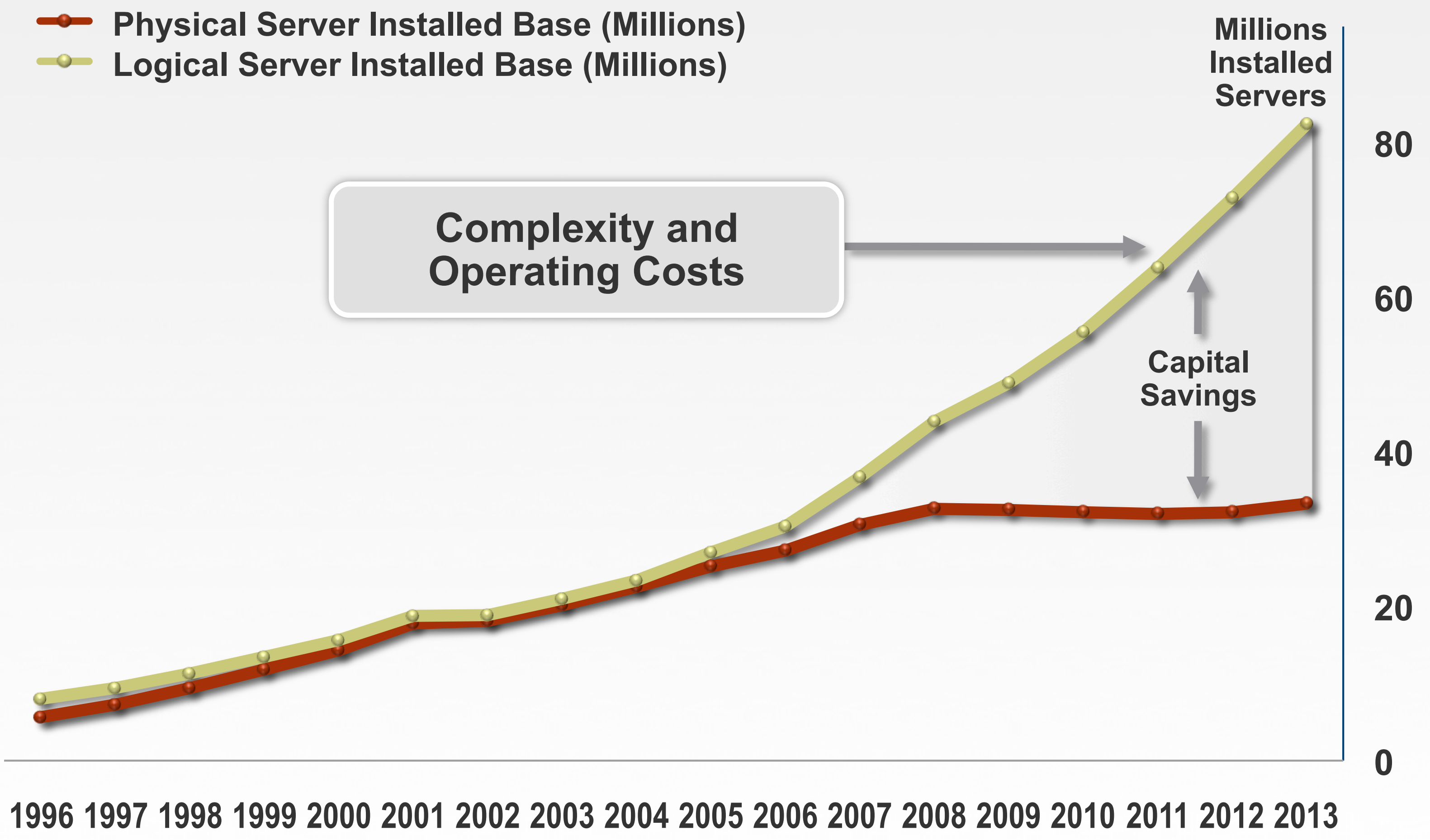
LARGER POOL, MORE CONSOLIDATION



SAME PRINCIPLE, FOR WHOLE DATA CENTERS

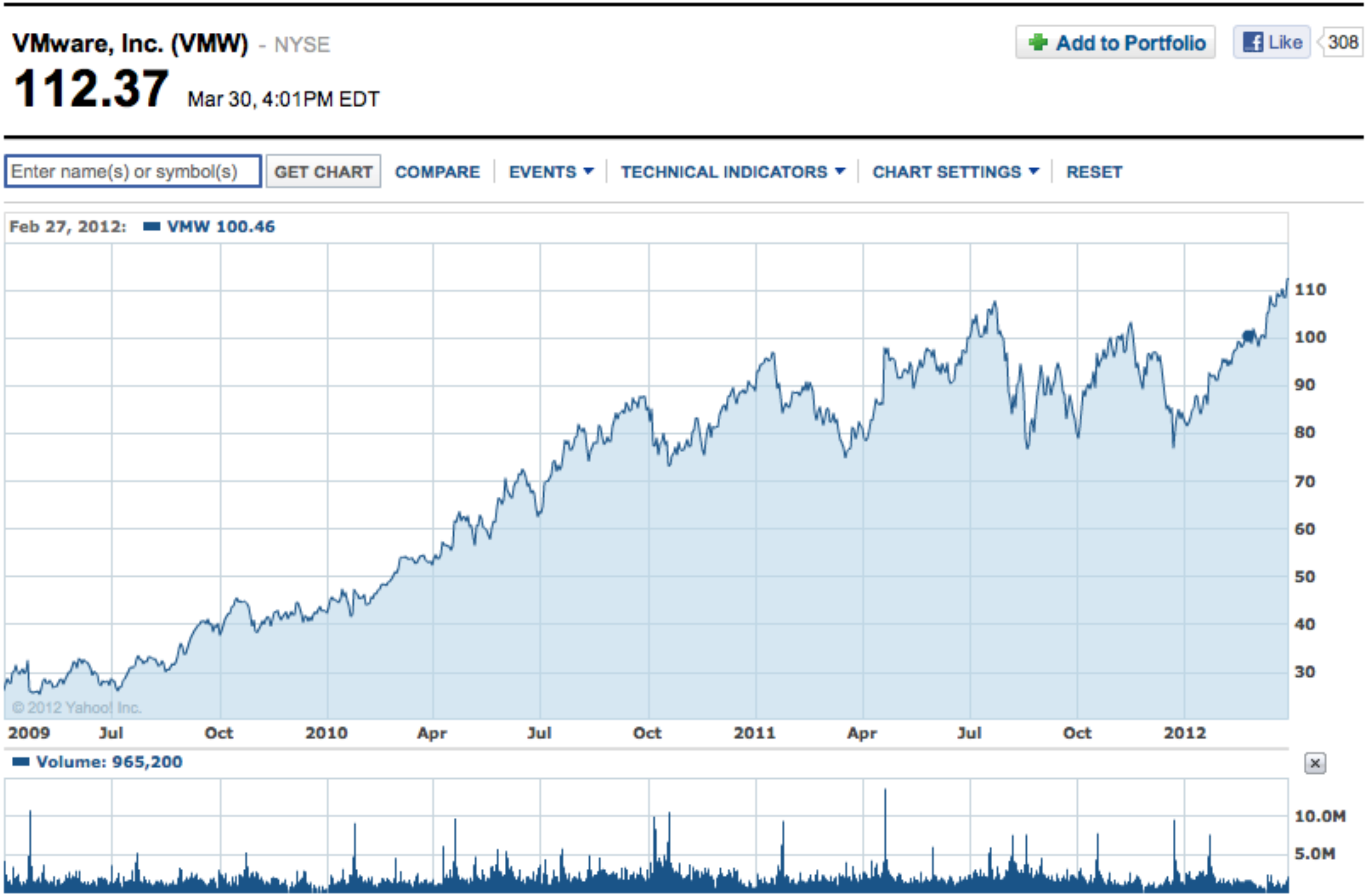


THE ECONOMICS OF THE DATA CENTER



Source: IDC

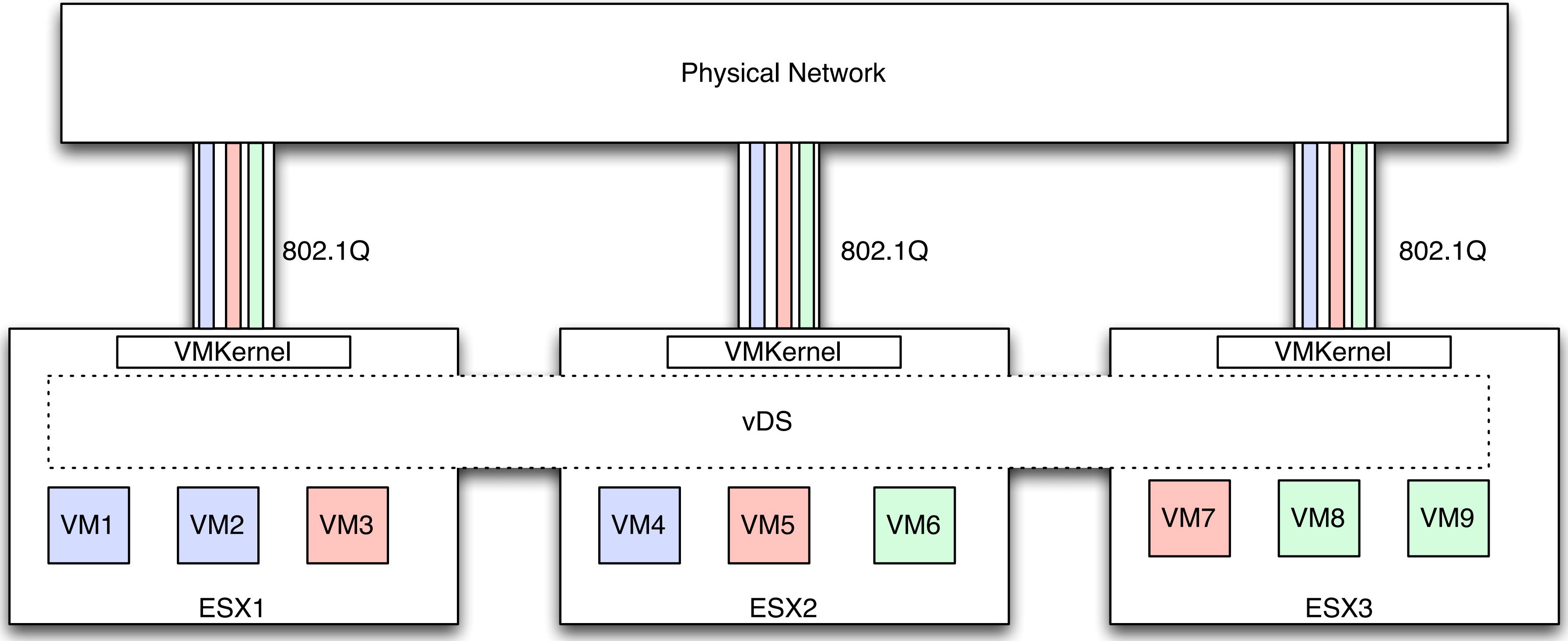
THE ECONOMICS OF THE DATA CENTER



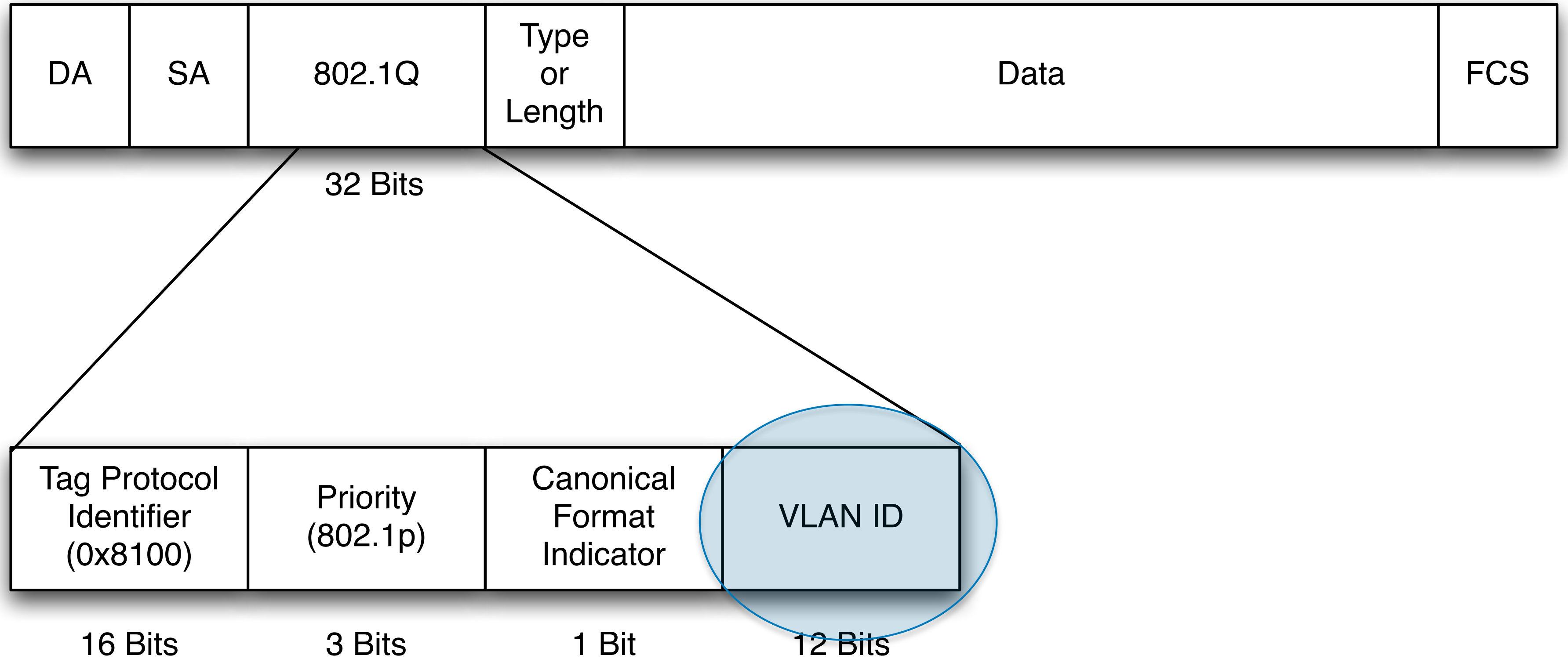
VMware, Inc. (VMW) - NYSE

112.37 Mar 30, 4:01PM EDT

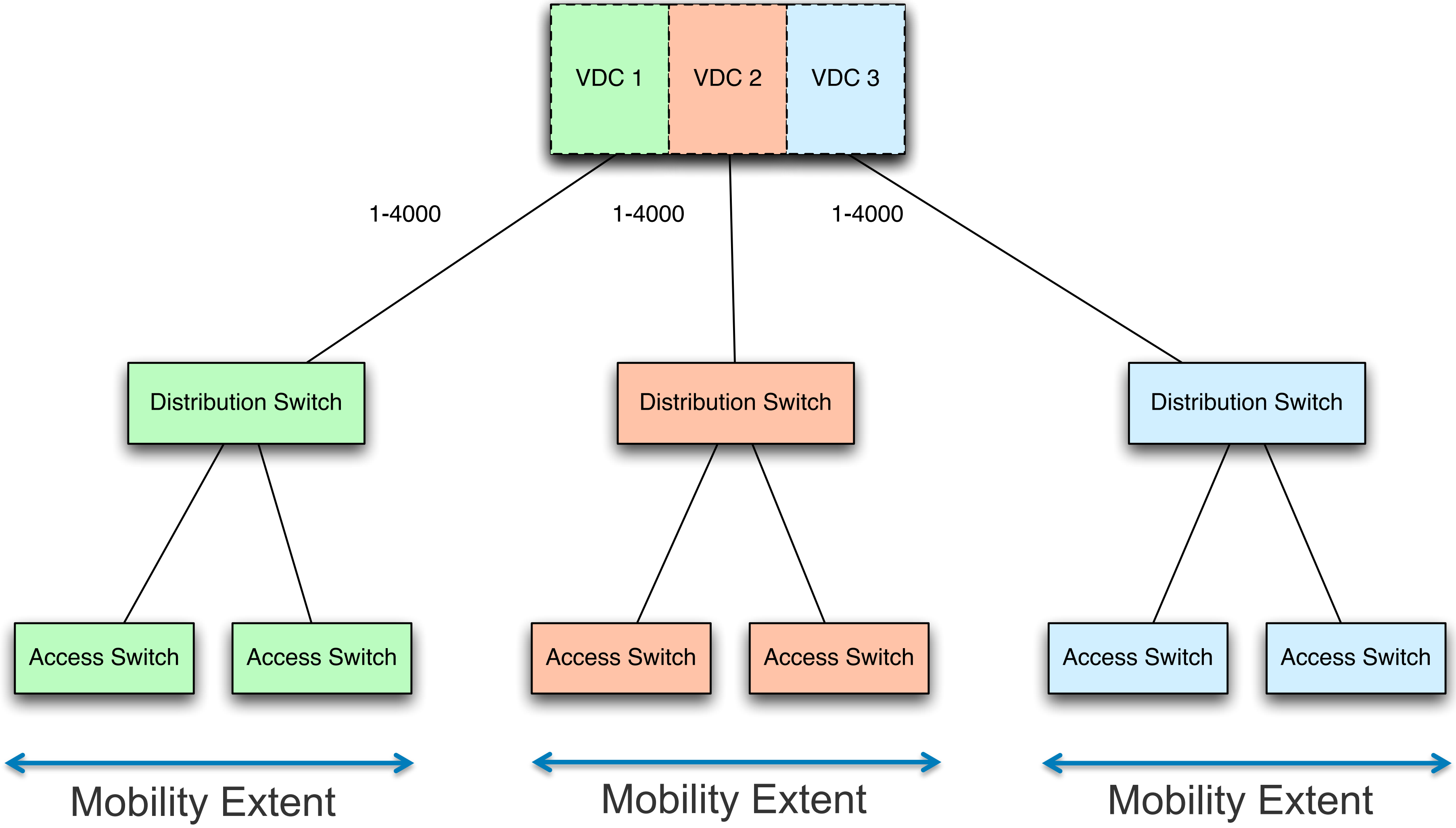
THE NEW EDGE


Physical Network
802.1Q
802.1Q
802.1Q
VMKernel
VMKernel
VMKernel
vDS
VM1
VM2
VM3
VM4
VM5
VM6
VM7
VM8
VM9
ESX1
ESX2
ESX3

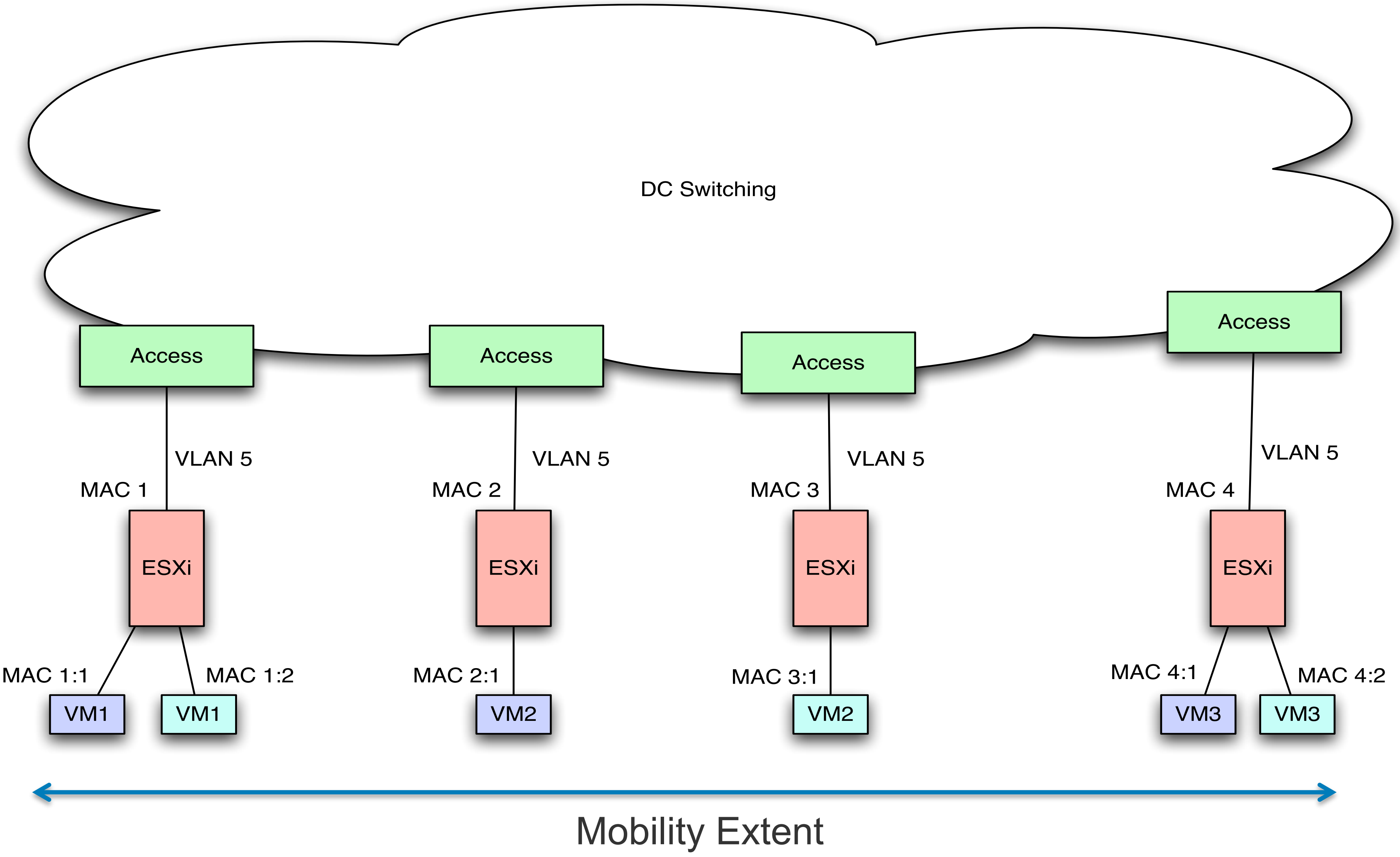
VLAN LIMITATIONS



SCALING BEYOND 4K TENANTS – BRIDGE DOMAINS



SCALING BEYOND 4K TENANTS – VCD-NI



VCD-NI PORTGROUP LABELS

dvs.<vCenterID><DS#><vCD#><VLAN>***<Network ID>***<Name>

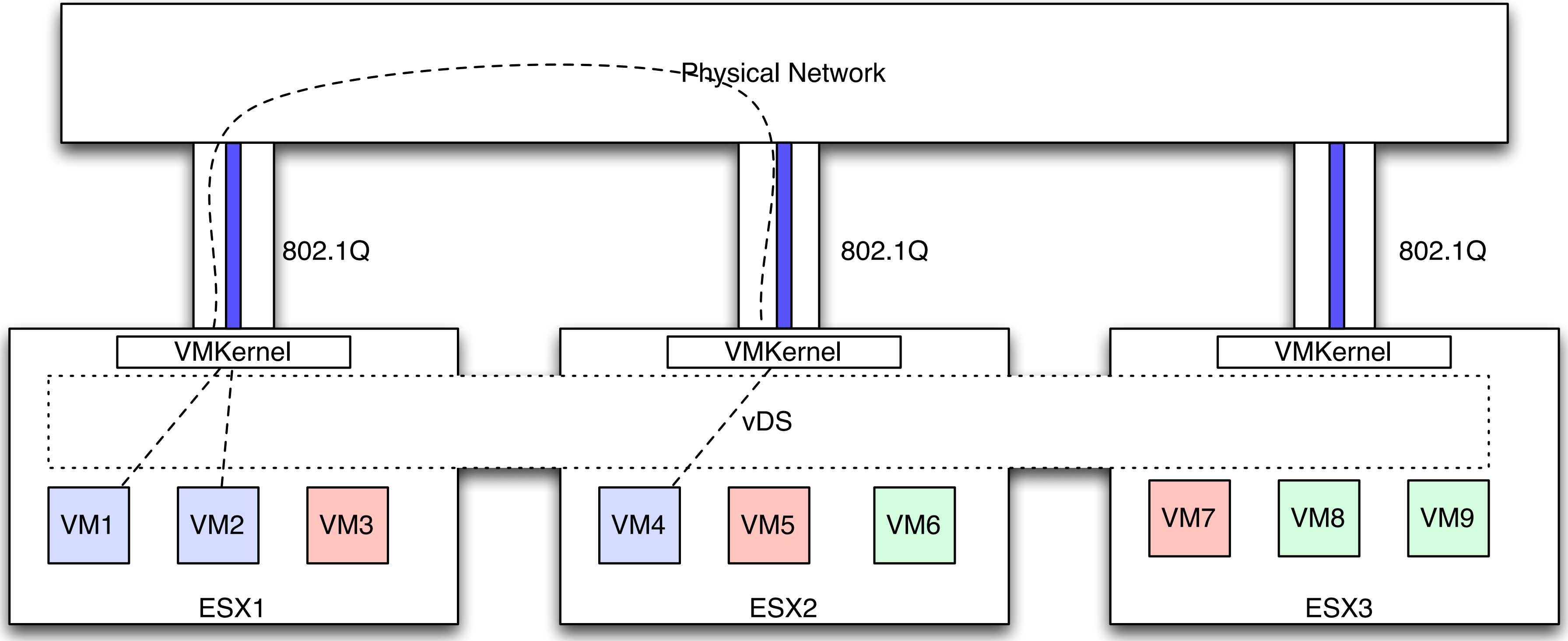
<Network ID> is a 24 bit value expressed in Hexadecimal

(This is sometime referred to as a fence ID)

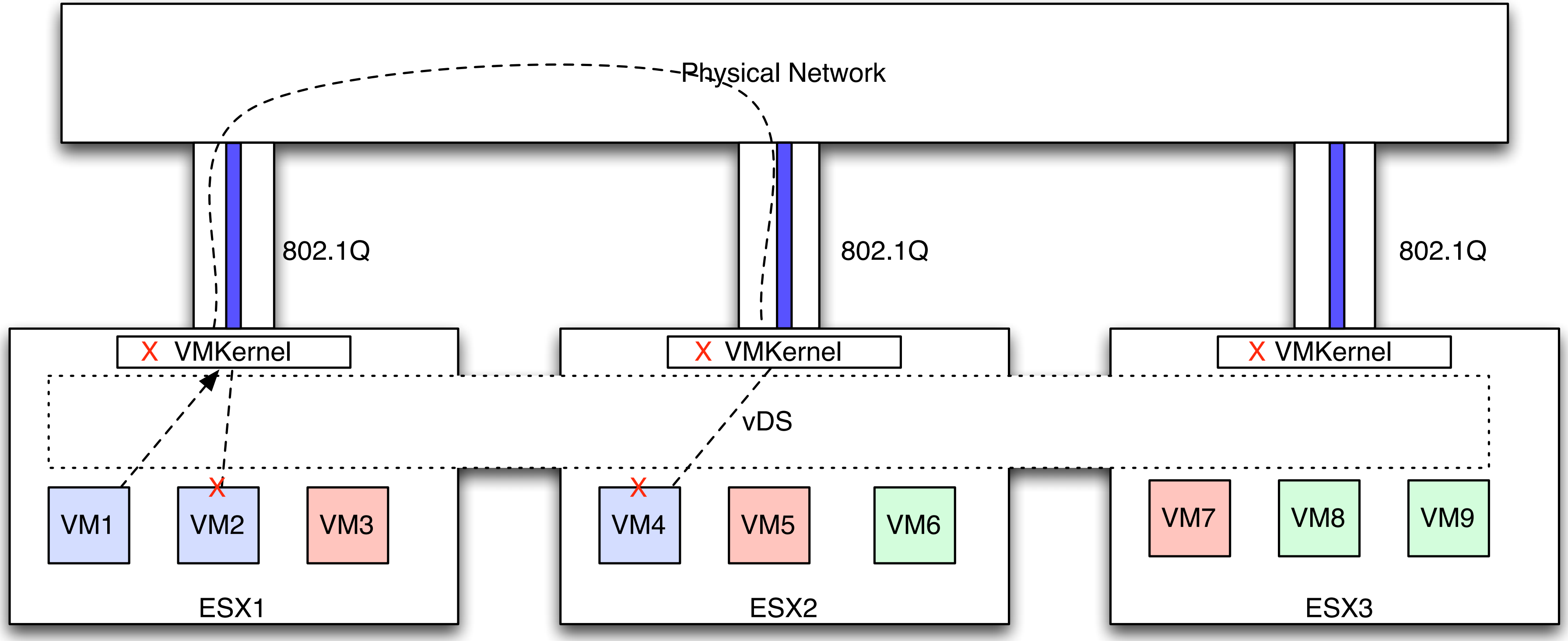
For Example:

dvs.VC1012345678DVS3CM1-V32-C2E-Coke Org1

THE NEW EDGE – WITH TUNNELS



THE BROADCAST RADIATION WILL KILL US ALL

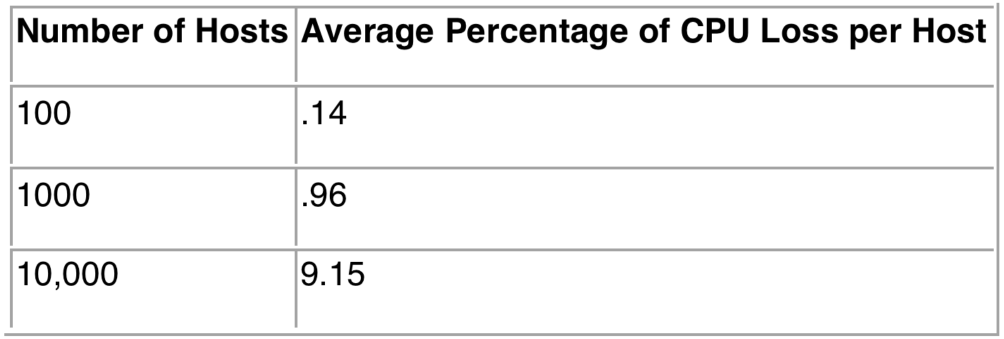


REMEMBER THESE RULES OF THUMB?

Max IP hosts per subnet – 500

Max IPX Hosts per subnet – 256

Max Appletalk hosts per subnet - 128



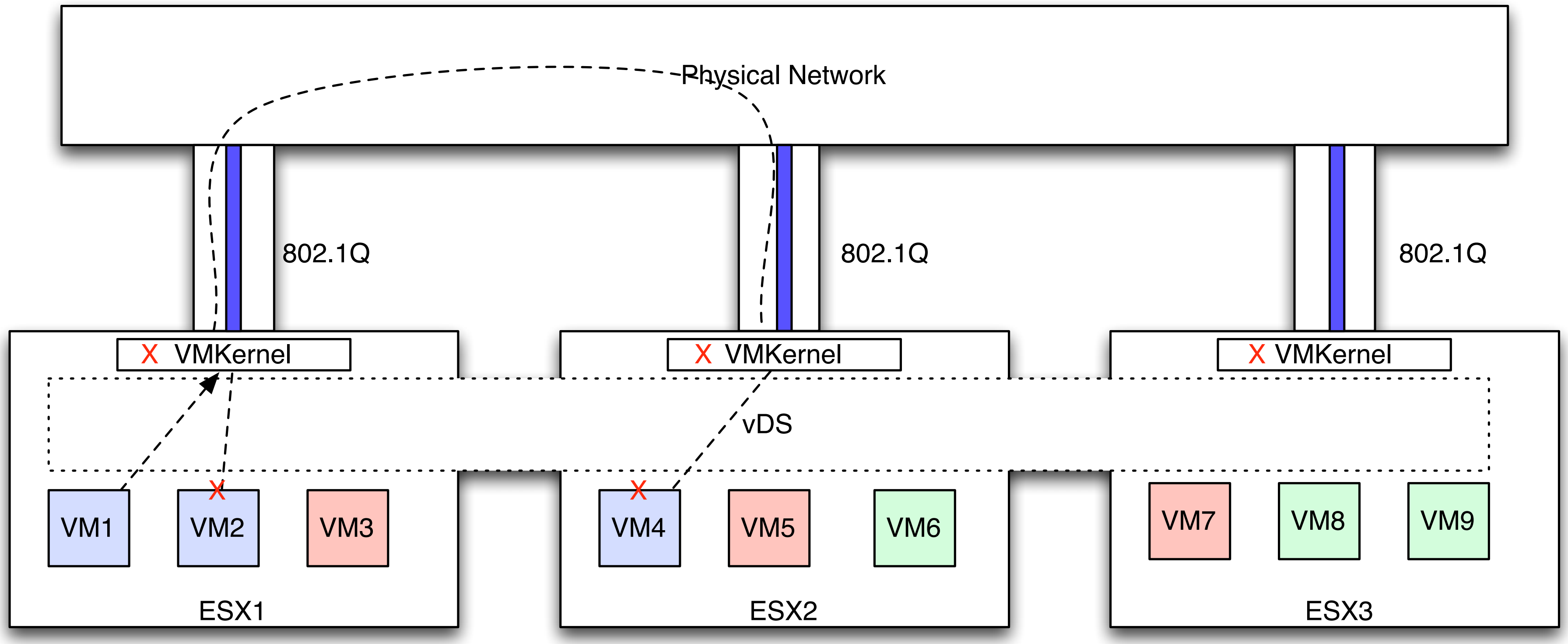
Number of Hosts	Average Percentage of CPU Loss per Host
100	.14
1000	.96
10,000	9.15

http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_--_Broadcasts_in_Switched_LAN_Internetworks

TIMES CHANGE

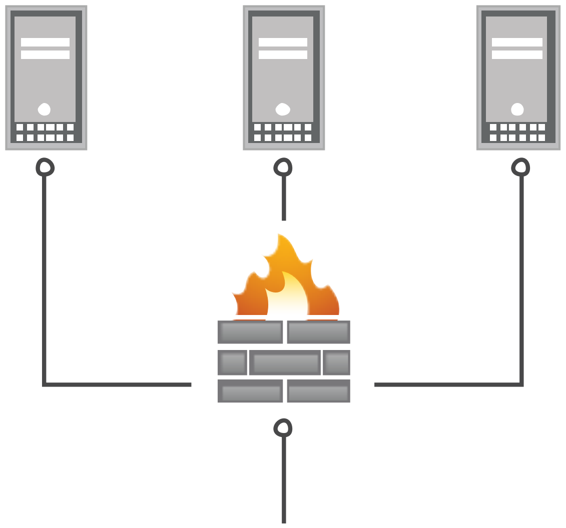
SparcStation 2	Ivy Bridge Xeon
28 MIPS	180,000 MIPS
0.000392 MIPS used per host	0.000392 MIPS used per host
500 Hosts Cost 0.7% of CPU	3.2 Million Hosts cost 0.7% of CPU

THE BROADCAST RADIATION WONT KILL US ALL



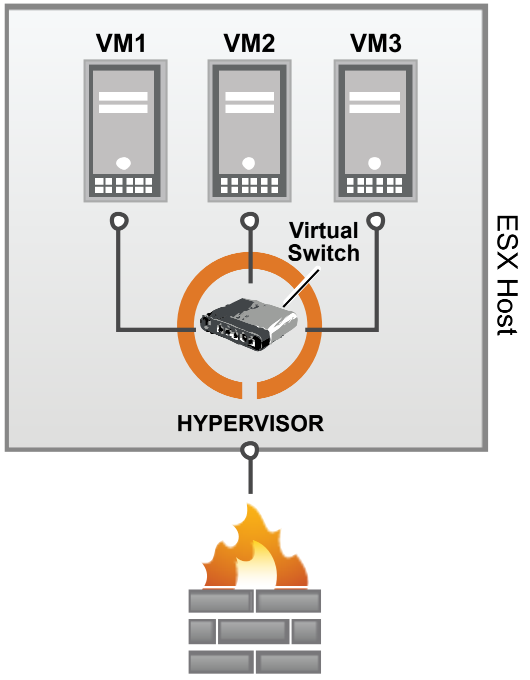
SECURITY IMPLICATION OF VIRTUALIZATION

Physical Network



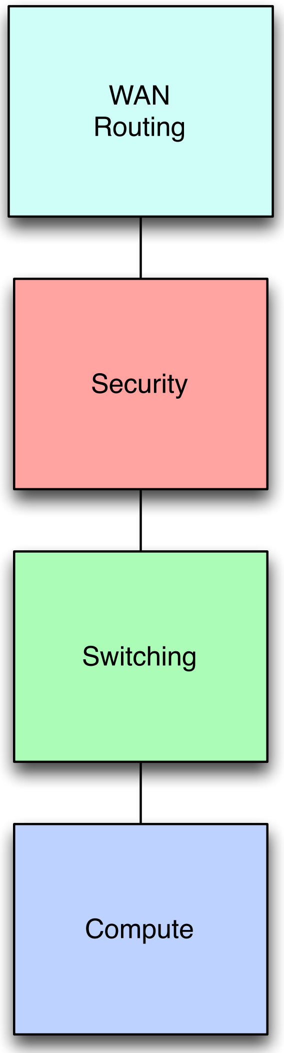
Security Complex Sees/Protects
All Traffic Between Servers

Virtual Network



Physical Security is “Blind” to
Traffic Between Virtual Machines

THIS IS HOW WE HAVE BUILT DATA CENTRES…



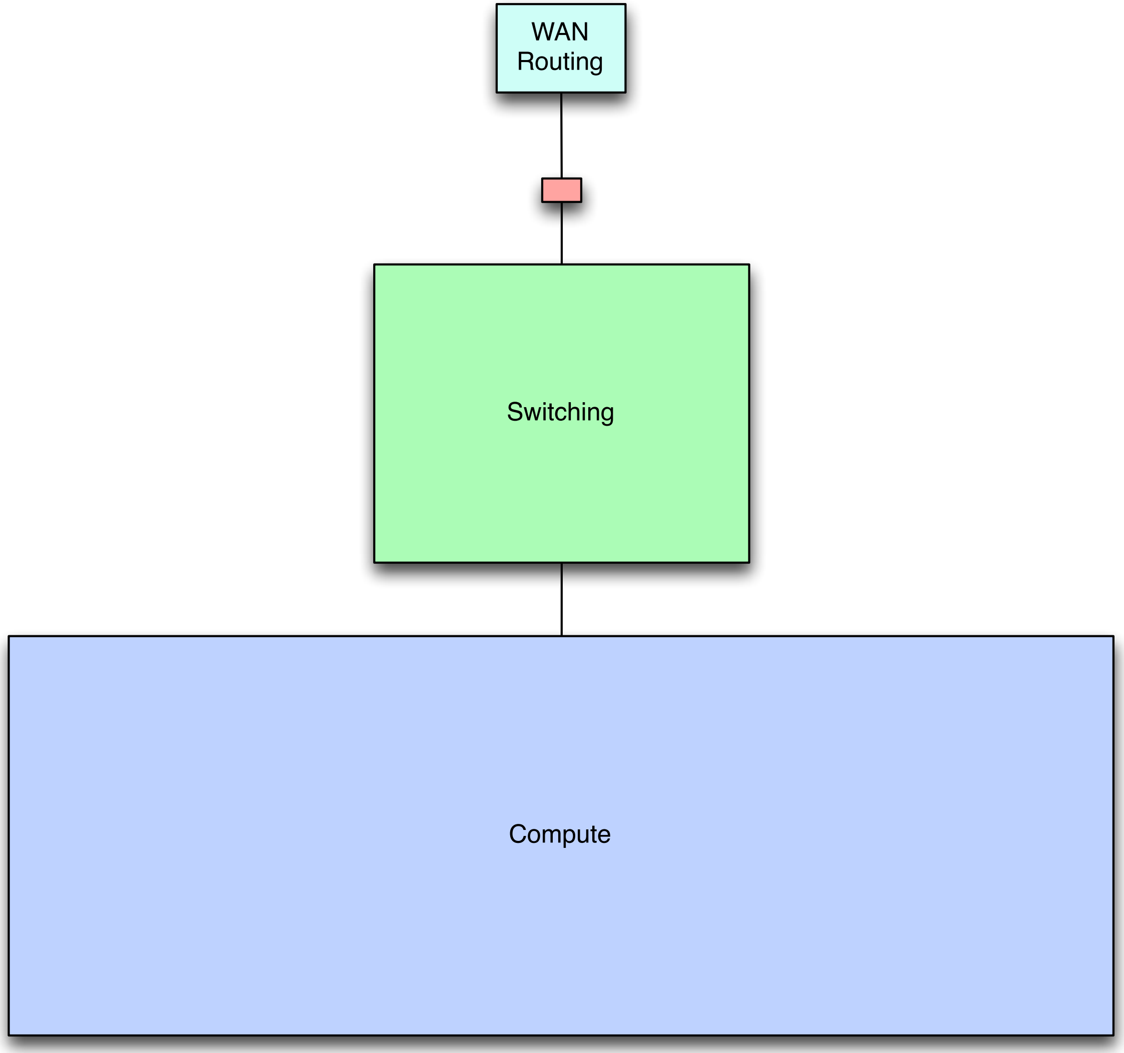
3840 Gbps

120 Gbps

40900 Gbps

122000 Gbps

NETWORK THROUGHPUT IS A DIFFERENT STORY

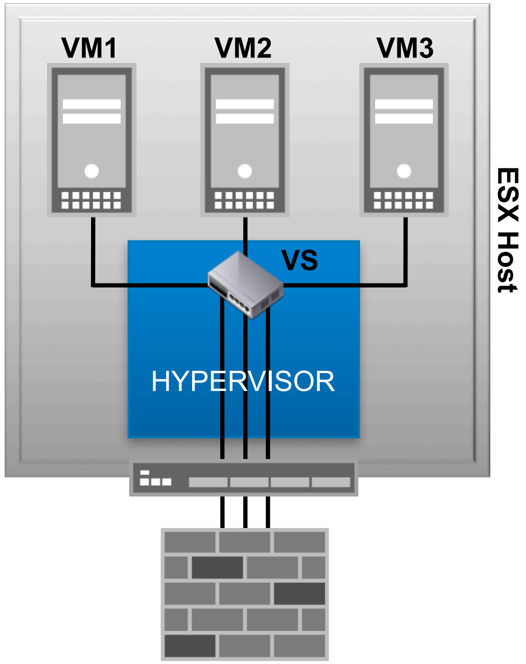


APPROACHES TO SECURING VIRTUAL NETWORKS

1. VLAN Segmentation

VMs segmented into separate VLANs; Inter-VM communications must route through the firewall

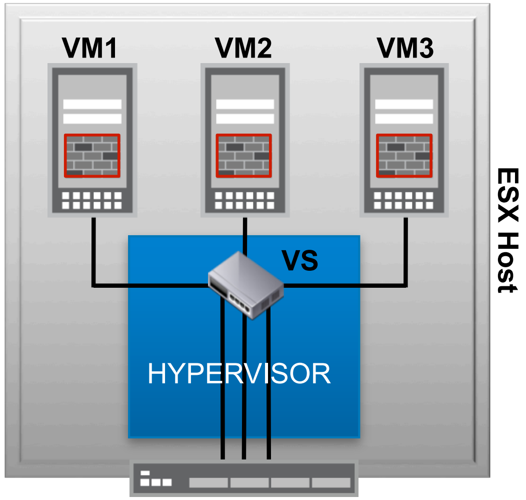
Drawbacks: Complex VLAN networking; Lacks hypervisor visibility; High overhead



2. Agent-based

Each VM has a software firewall

Drawbacks: Significant performance implications; Huge management overhead of maintaining software and signature on 1000s of VMs



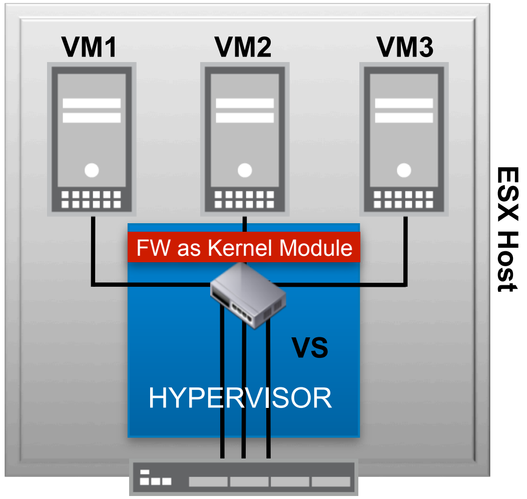
🟥 FW Agents

3. Kernel-based

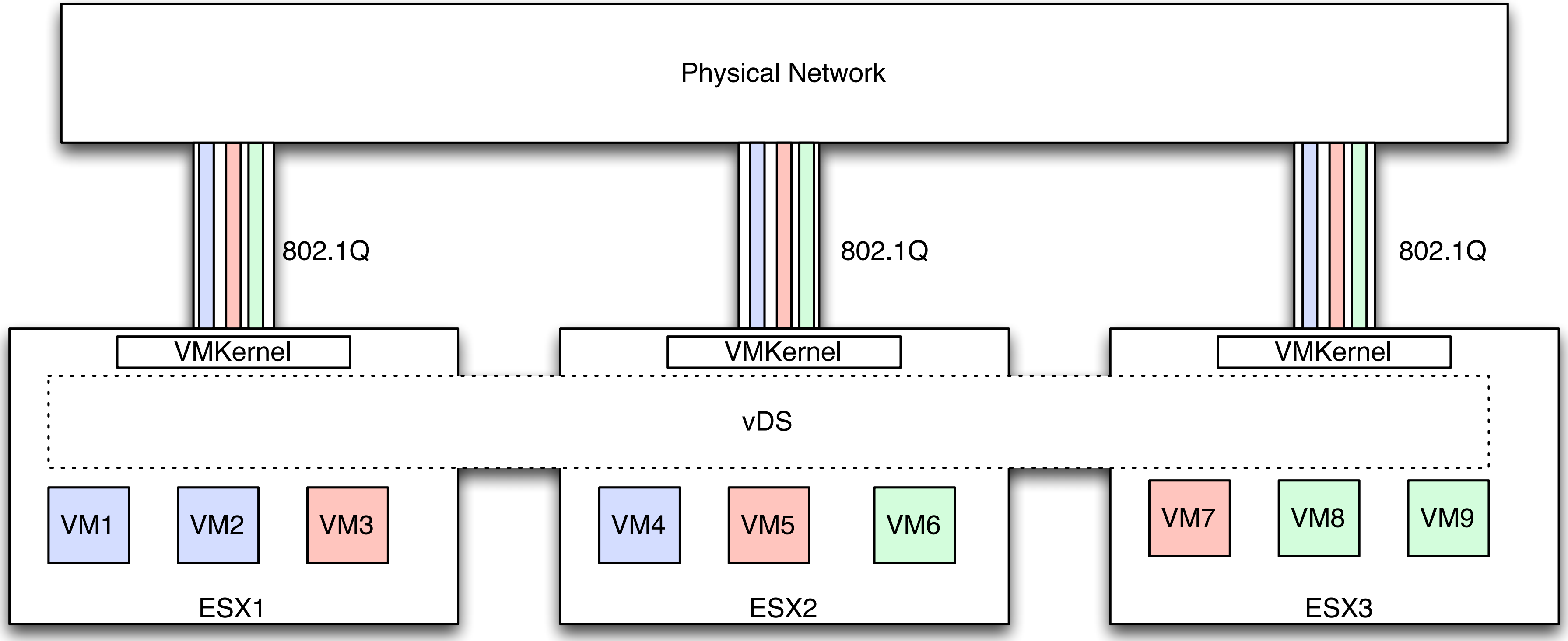
Inter-VM traffic always protected; Micro-segmenting capabilities

High-Performance from implementing firewall in the kernel

Secures Hypervisor connections



THE NEW EDGE
OPPORTUNITIES AND CHALLENGES FOR ALL



Russell Skingsley

skingsrw@juniper.net

everywhere