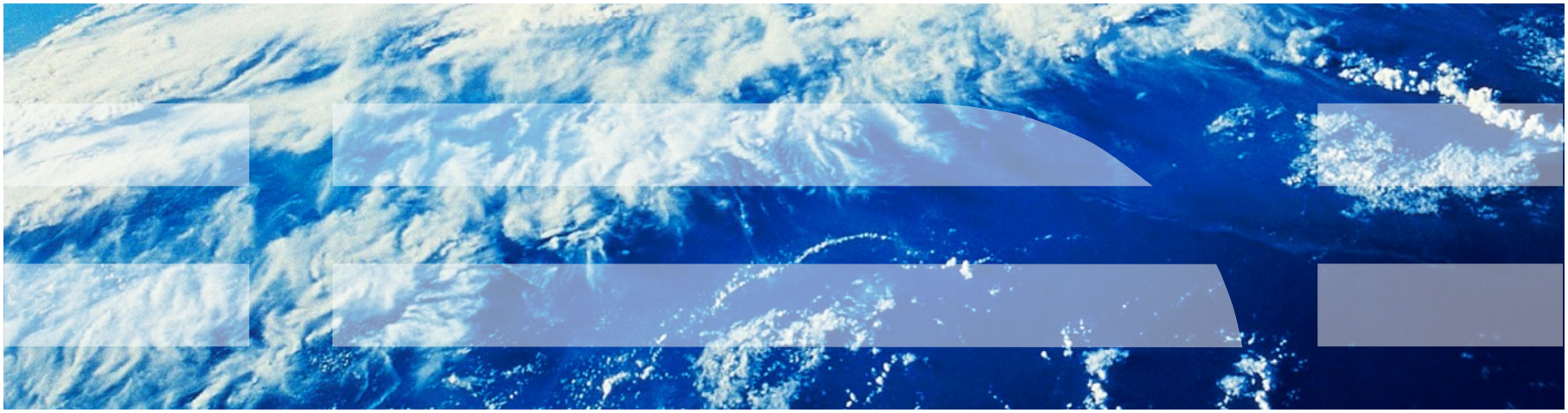
SAPIENZA
UNIVERSITÀ DI ROMA

Inside the Cloud:

a Secure, Virtualization-aware Network environment for Cloud Applications



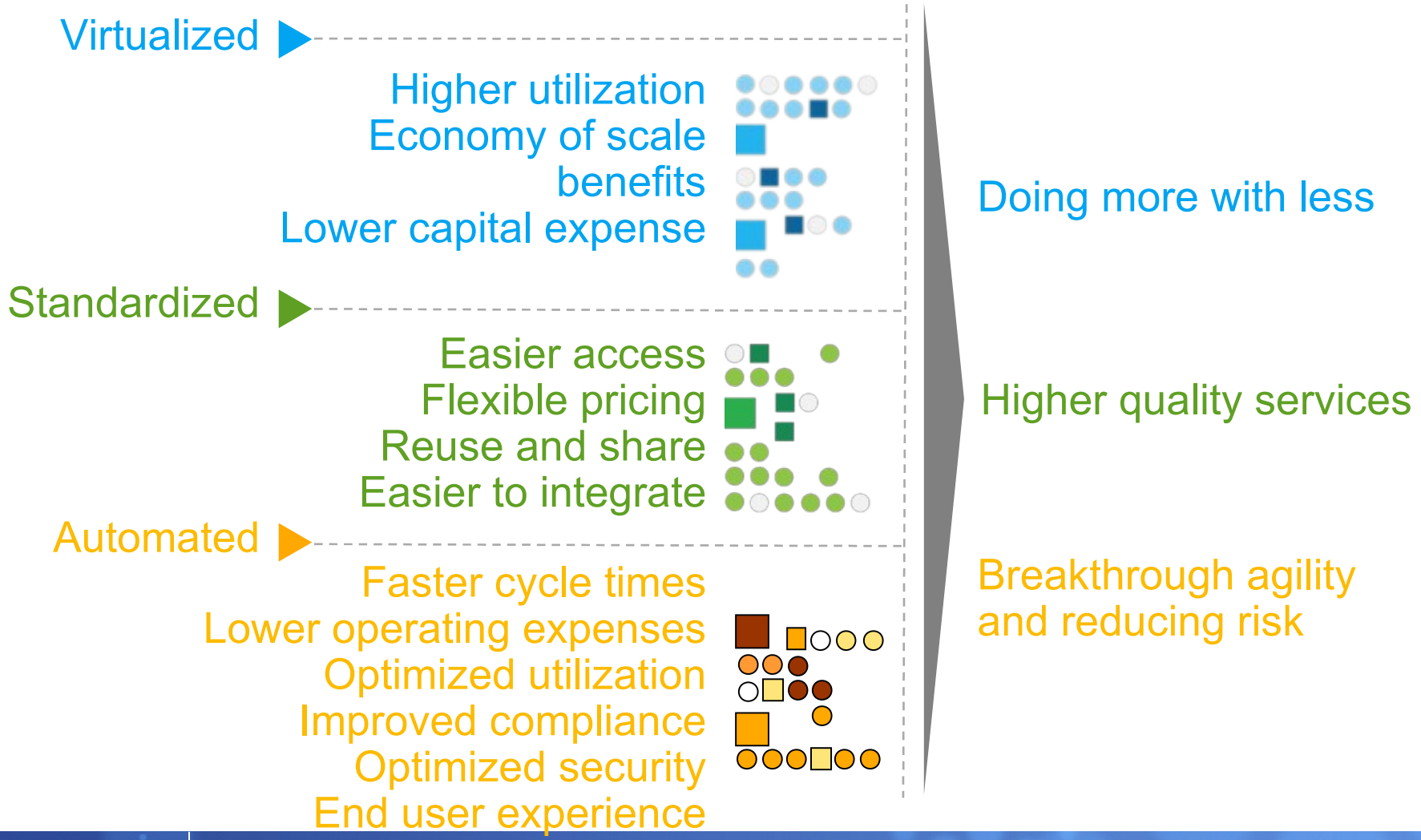
Agenda

- Introduction
- Networking for Cloud Computing Data Centers
- Evolution of the current Network Standards

Cloud is a shift in the consumption and delivery of IT with the goal of simplifying to manage complexity more effectively.

- Cloud is:
  - A new consumption and delivery model
- Cloud addresses:
  - Cost reduction
  - Scale
  - Utilization
  - Self-service
  - IT agility, flexibility and delivery of value
- Cloud represents:
  - The industrialization of delivery for IT supported services
- Cloud includes:
  - Delivery models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Business Process as a Service
  - Deployment models: public, private, hybrid

Cloud computing delivers IT and business benefits



IT benefits from cloud computing are real

Results from IBM cloud computing engagements

Increasing speed and flexibility	Test provisioning	Weeks	Minutes
	Change management	Months	Days/hours
	Release management	Weeks	Minutes
	Service access	Administered	Self-service
Reducing costs	Standardization	Complex	Reuse/share
	Metering/billing	Fixed cost	Variable cost
	Server/storage utilization	10–20%	70–90%
	Payback period	Years	Months

SOURCE: Based on IBM and client experience.

The emerging agenda: the impact of cloud computing is extending into driving business transformation

An enabler of business transformation

- Creating new business models
- Enabling speed and innovation
- Reengineering business process
- Supporting new levels of collaboration

Transformation

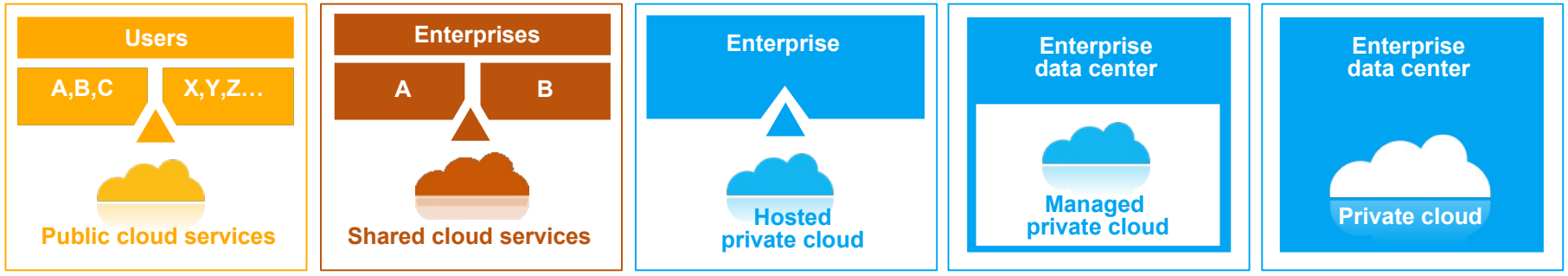
An evolution of information technology

- Changing the economics of IT
- Automating service delivery
- Radically exploiting standardization
- Rapidly deploying new capabilities

Efficiencies

There is a spectrum of deployment options for cloud computing

In these models, data resides outside client's firewall



Service from Cloud service provider	Service from Cloud service provider	Third-party hosted and operated	Third-party operated	Enterprise owned and operated

Public ◀ ▪ ▪ ▪ ▪ ▶ **Private**

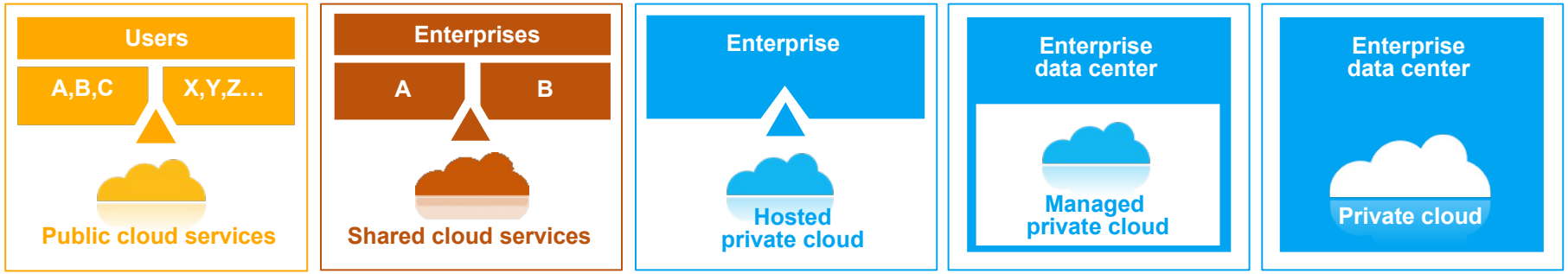
IT activities / functions are provided "as a service," over the Internet

IT capabilities are provided "as a service," over an intranet, within the enterprise and inside the firewall

Hybrid Internal and external service delivery methods are integrated

Each cloud delivery model has different characteristics

In these models, data resides outside client's firewall



- Service from cloud service provider
- Standard services
- Individual users
- Shared resources
- Pay as you go
- Access through public Internet

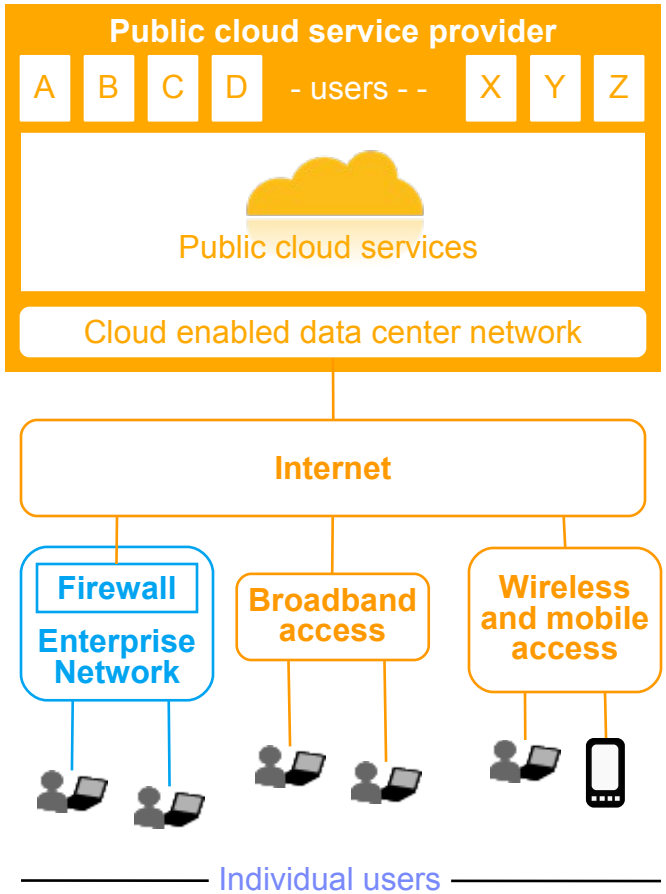
- Service from Cloud service provider
- Standard services
- Enterprise users
- Mix of shared and dedicated resources
- Shared facility and staff
- Utility pricing model
- Virtual private network (VPN) access

- Service provider owned and operated
- Dedicated resources for client
- Access through dedicated connection from network service provider

- Third-party operated
- Enterprise owned
- Implemented on client data center
- Uses enterprise network
- Mission critical
- High compliancy

- Enterprise owned and operated
- Implemented on client data center
- Uses enterprise network
- Mission critical
- High compliancy

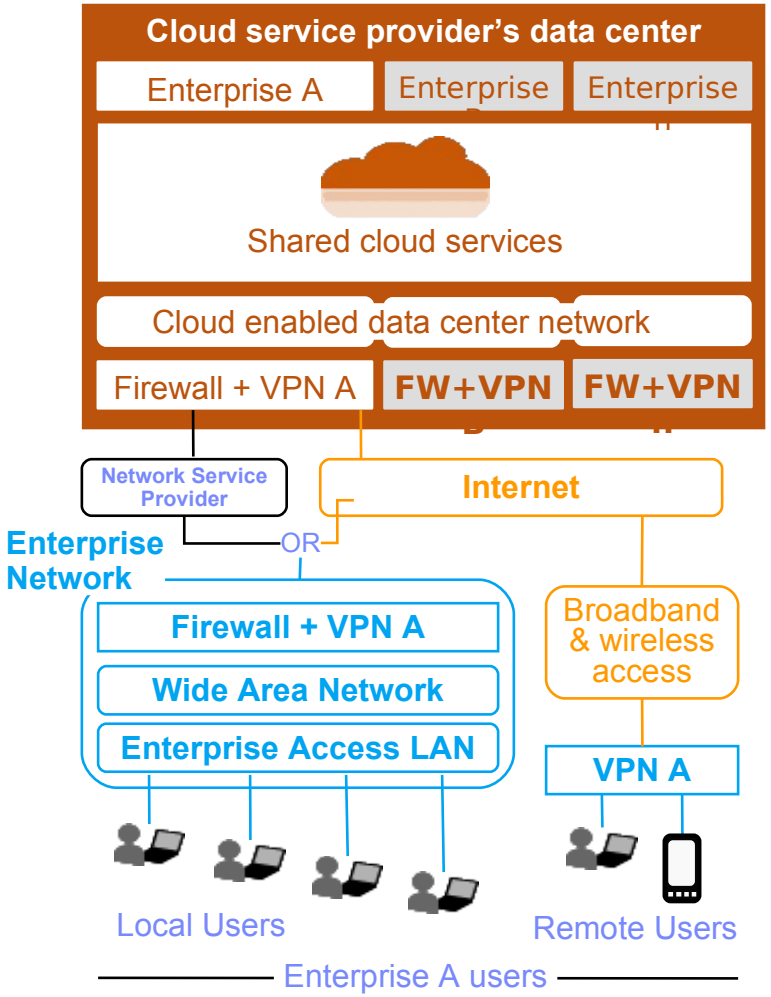
Public cloud services rely on the public Internet with uncontrollable reliability, performance and security



Network Implications

- Relies on the public Internet for availability and performance
- Uses a wide range of connectivity options and technologies for cloud access
- Impacts enterprise security boundaries and privacy policy enforcement
- Depends on cloud service providers for additional security and scalability measures within their data centers
- Deals with multiple Internet Service Providers (ISPs) and billing models challenges

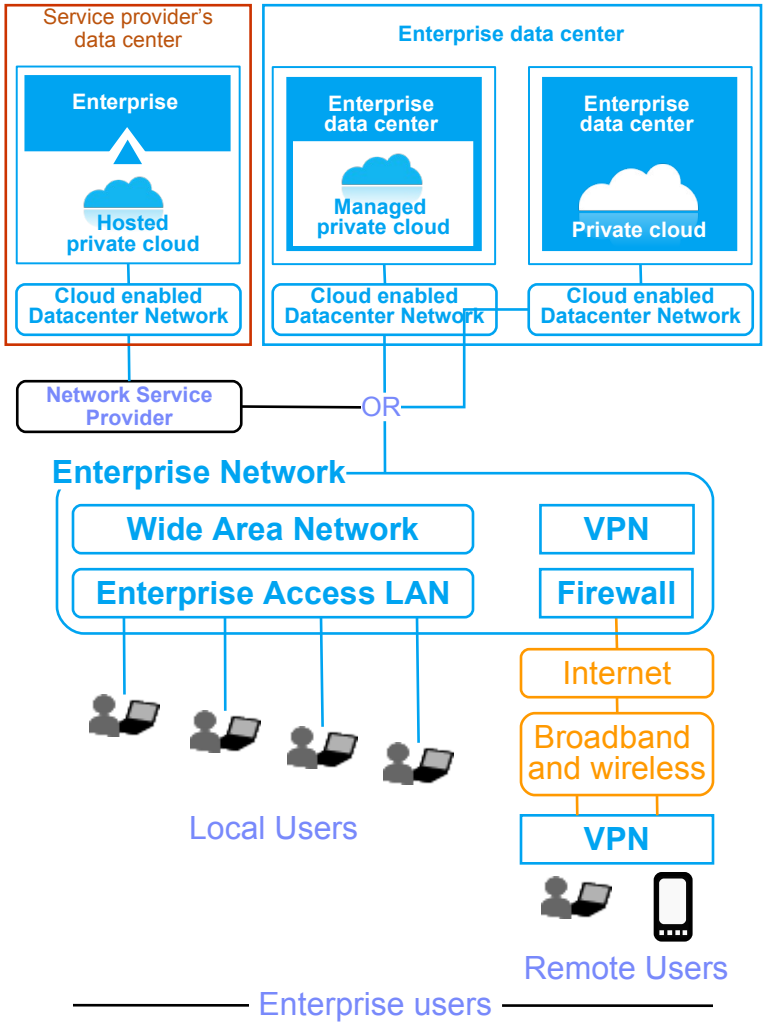
Shared cloud service providers deliver over the public Internet, but can improve security using virtual private networks and dedicated network service provider connections



Network Implications

- Relies on the public Internet and/or extranets for delivery
- Requires additional security measures for enterprise extranets
- Needs to consider end-to-end network scalability, provision, and management capabilities accordingly
- Understands potential financial impacts when dealing with multiple ISPs and network service providers

Private cloud models have similar networking environments, where services are delivered through intranets or dedicated network connections through network service providers.



Network Implications

- Depends on application profiles, services provided, and financial impacts
- Delivers dynamic provisioning, security, availability, and performance
- Requires integrated cloud services and management solutions
- Involves multiple network management systems for hosted private cloud
- Requires additional networks to connect between the cloud service provider and enterprise data centers and users for hosted private cloud

Whether you buy from a cloud provider or build your own private cloud, the network must be designed to take advantage of current and future cloud delivery models

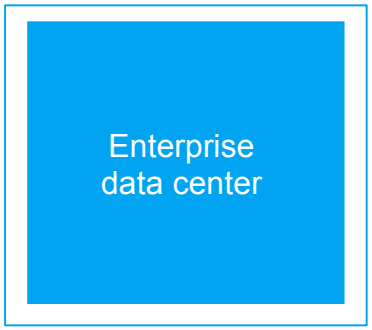
Public Cloud Delivery Model

- Requires a network design that can leverage the public Internet and Internet associated value-added services to connect to public cloud delivered services
- Takes advantage of the cost efficient Internet for cloud computing delivery
- Connects through various access methods
- Requires security measures for individual end users

Private Cloud Delivery Model

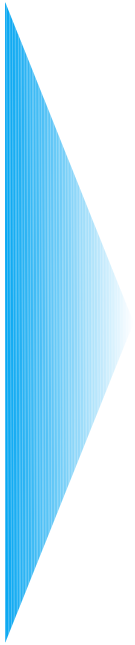
- Supports dynamic provisioning, security, performance, and reliability requirements
- Requires an understanding of financial impacts
- Demands end-to-end network management capabilities
- Needs a flexible network design to support cloud computing data centers

Private cloud options require a new set of network design attributes



Traditional Network Design

- Optimized for availability
- Slow to adapt
- Costly
- Rigid, inflexible
- Infrastructure silos
- Dedicated
- Device sprawl
- Location dependence



Cloud Network Design

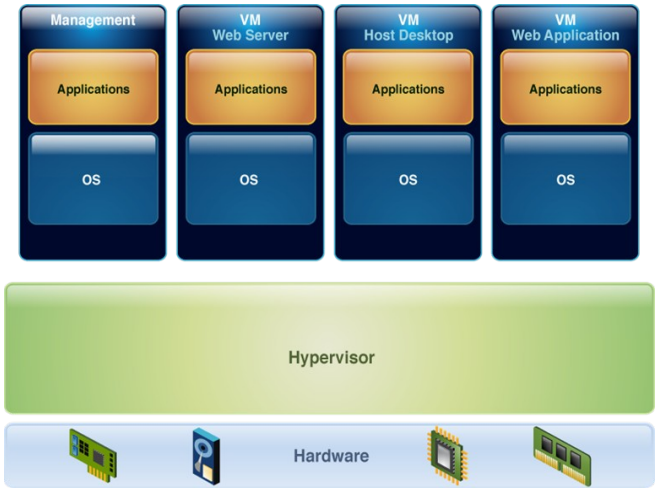
- Optimized for flexibility
- New approach to availability
- Cost more important
- Variable, metered
- Integrated infrastructure
- Shared
- Consolidation/Virtualization
- Location independence

Agenda

- Introduction
- Networking for Cloud Computing Data Centers
- Evolution of the current Network Standards

A Cloud-based Data Center needs to achieve challenging target

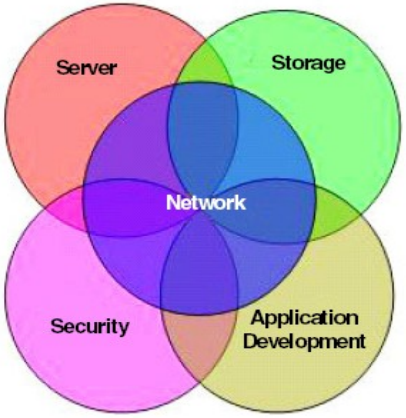
- Workload allocation
  - ✓**Move workload across physical servers offering minimal barriers to mobility**
- Shared resource pool
  - ✓**Manage a pool of IT resources as a single system, place workload in the pool according to policy**
- Scalability
  - ✓ **Enhance computing capability avoiding re-design the whole Infrastructure**
- Flexibility
  - ✓ **Adapt the infrastructure exposing minimal barriers to changes and reconfiguration**
- Openness
  - ✓ **Mitigate vendor lock-in to implement best technologies at best conditions, while leveraging technologies trend**
- Costs optimization
  - ✓ **Maximize resources utilization, minimize dedicated resources, simplify management**
- Separation of duty
  - ✓ **Identify well defined responsibilities for each service using layered management (Server administrator, Network Administrator, Application Administrator…)**



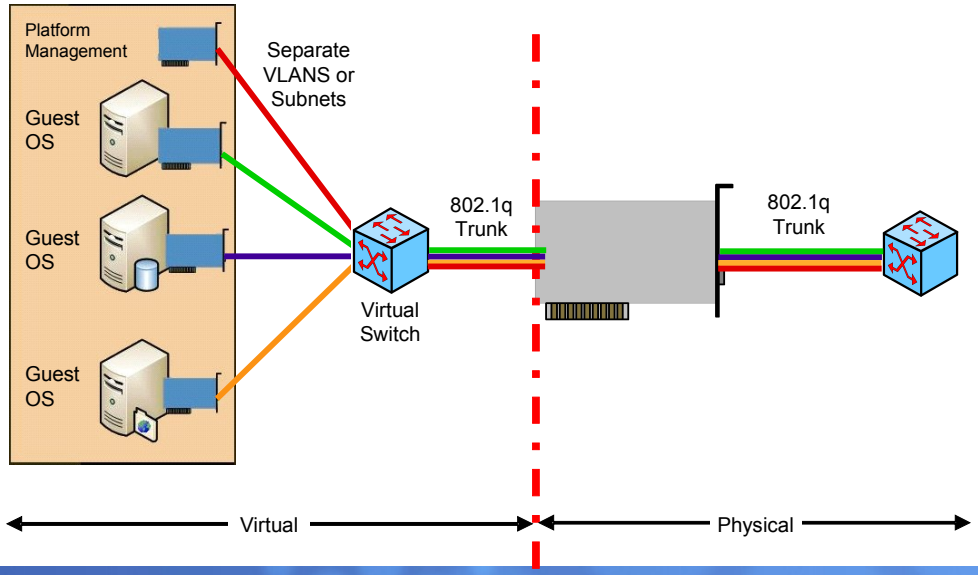
To address the requirements of a Cloud Data Center we need a "Virtualization-aware" Network

- Cloud Computing initiatives bring new demands to the Data Center Network

  - ✓ **Network is a pervasive element of the virtualized infrastructure**
  - ✓ **Workload Allocation requires flexible network infrastructure**
  - ✓ **Shared Resource Pool requires deterministic path allocation**
  - ✓ **Denser traffic patterns at the access layer need to be considered**
  - ✓ **Smooth Support for VM/LPAR mobility has to be achieved**

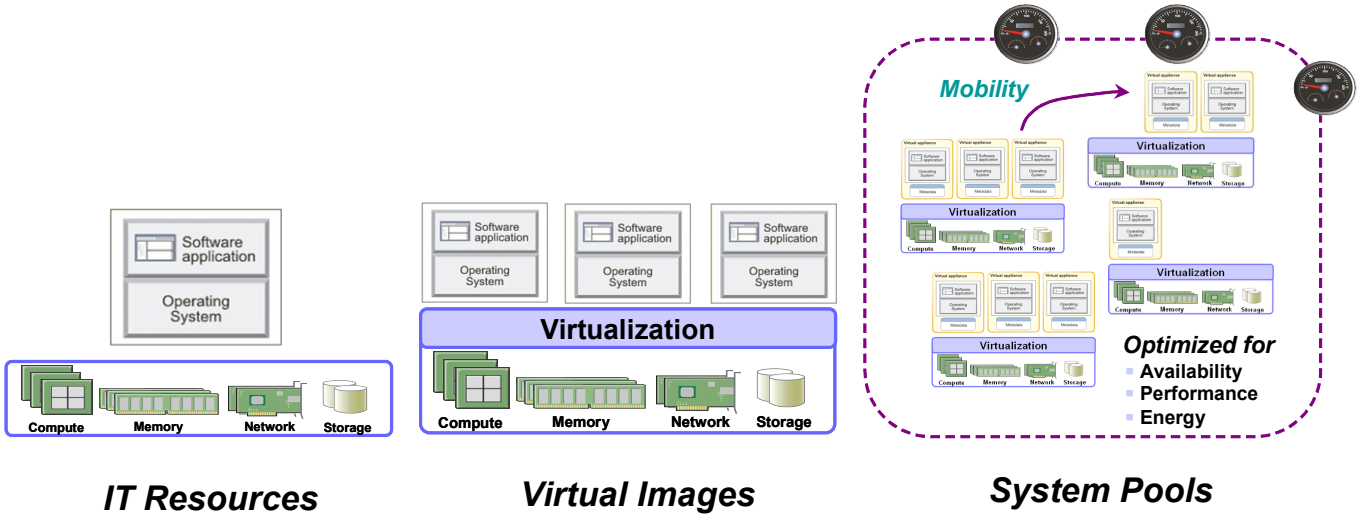


- To build a Cloud-ready infrastructure, Network needs to gain knowledge of virtual interfaces defined within Virtual Machines

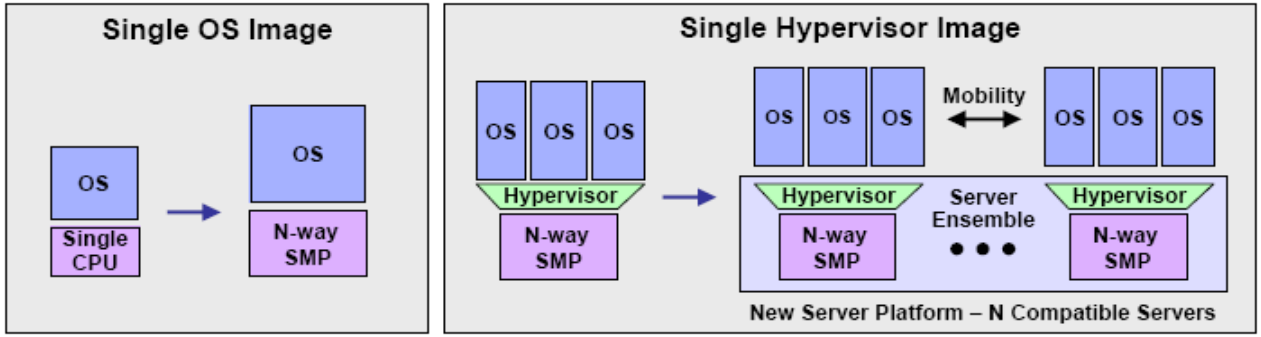


Virtualization extends beyond single system to multi-system pools creating a new platform for integrated management and optimization of data center resources

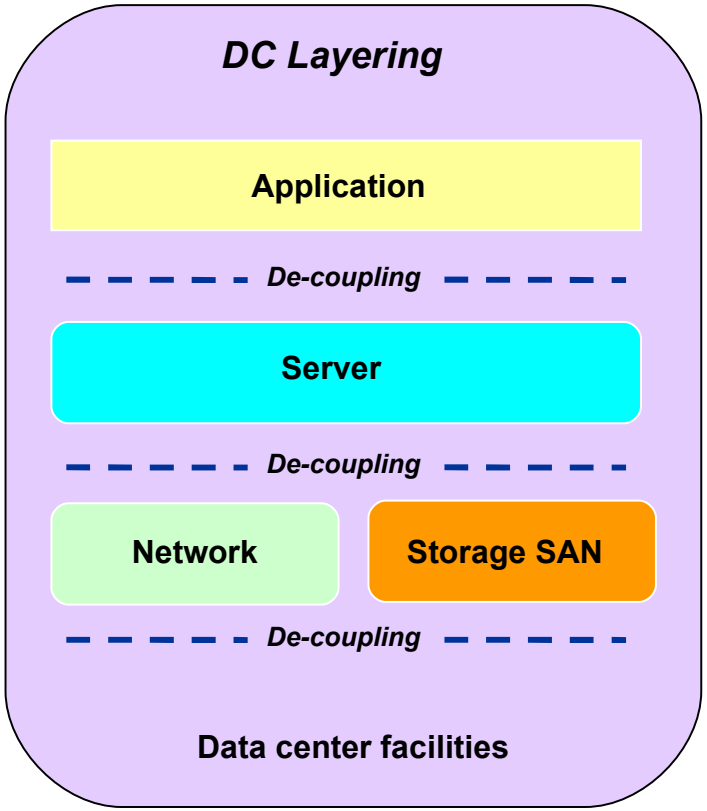
Physical and virtual resource pooling



Dynamic IT infrastructure (LPAR mobility, VMotion)



Data center is by nature application centric. Layering model improve capability to optimize and manage the IT infrastructure leveraging Virtualization



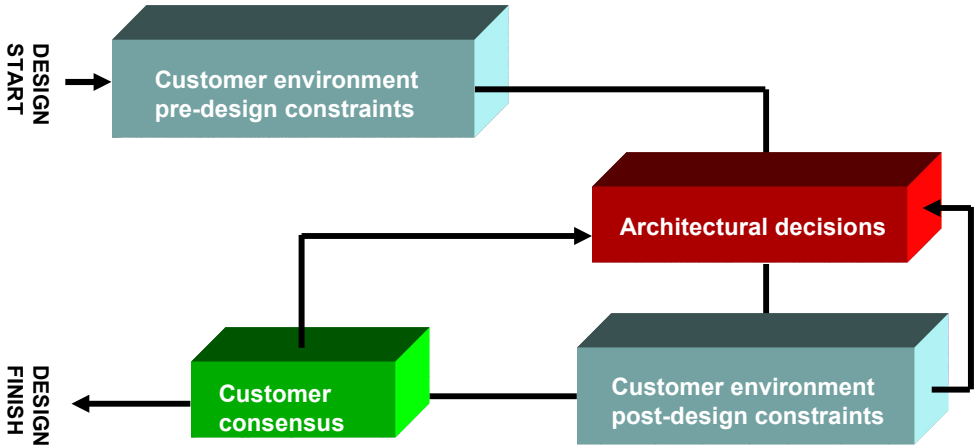
- **Data Center Layering**
  - ✓ Each layer is responsible to provide services to the upper layer, addressing upper coming requirements
  - ✓ Layers must be able to evolve in an integrated but independent way
  - ✓ Management of a a single layer must be well defined
  - ✓ Roles and responsibilities must be well defined in each layer

- **Advantages includes**
  - ✓ Reduce (remove) vendor lock-in
  - ✓ Gain flexibility to evolve, enlarge, renew each layer with limited impact to others
  - ✓ Leverage best of breed technologies
  - ✓ Optimize performance within each single layer
  - ✓ Implement QoS control and improvement

The approach to Data Center Network needs to be tightly integrated into the whole DC Design

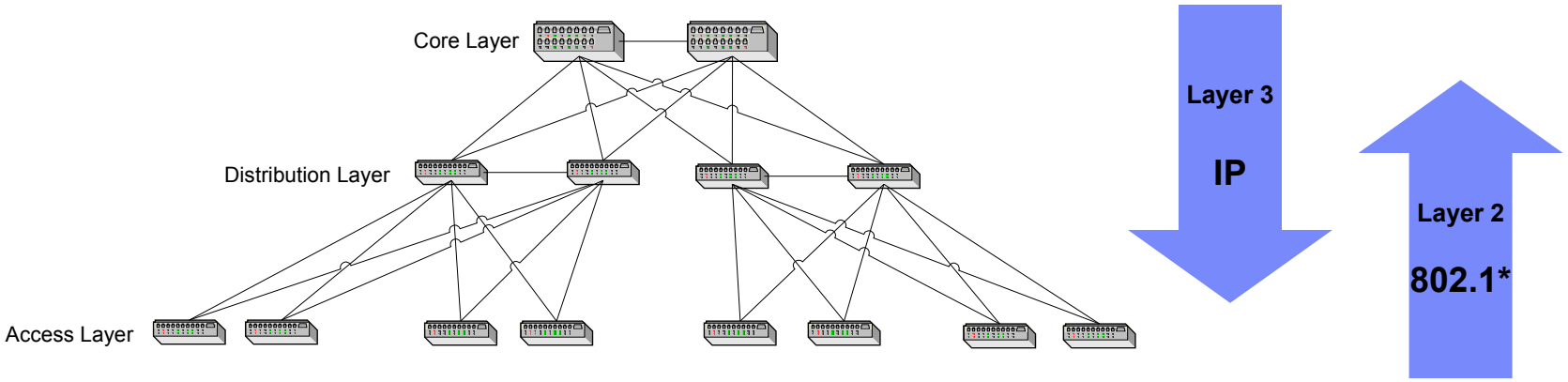
- New design patterns bring new architectural decisions (or change existing ones). These are not network-only and require to be evaluated with the whole Data Center infrastructure in mind.

  - ✓ **Hierarchical design**
  - ✓ **L2/L3 boundary**
  - ✓ **L2 domain architecture**
  - ✓ **L3 virtualization**
  - ✓ **Optimized application delivery in a virtualized environment**
  - ✓ **Security zones determination**
  - ✓ **Correct Level of automation**
  - ✓ **vSwitches implementation**



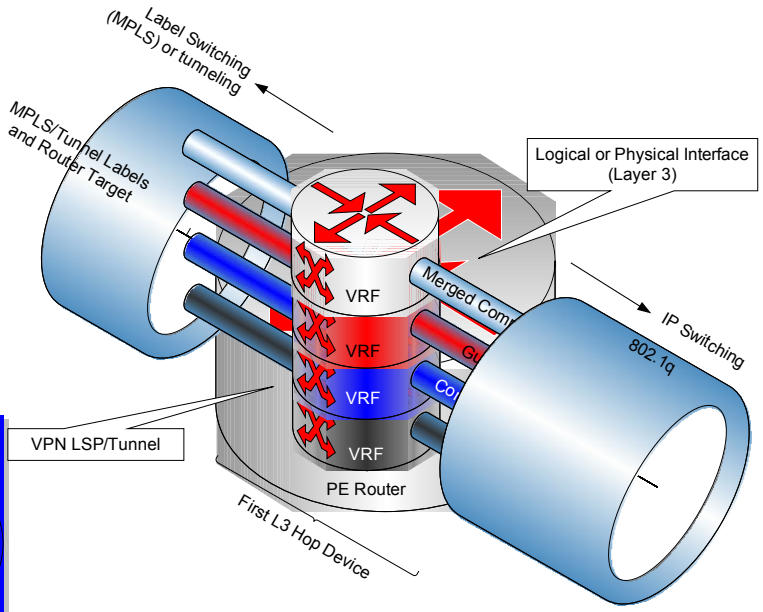
Hierarchical Design challenges, L2/L3 Boundary and L2 characteristics

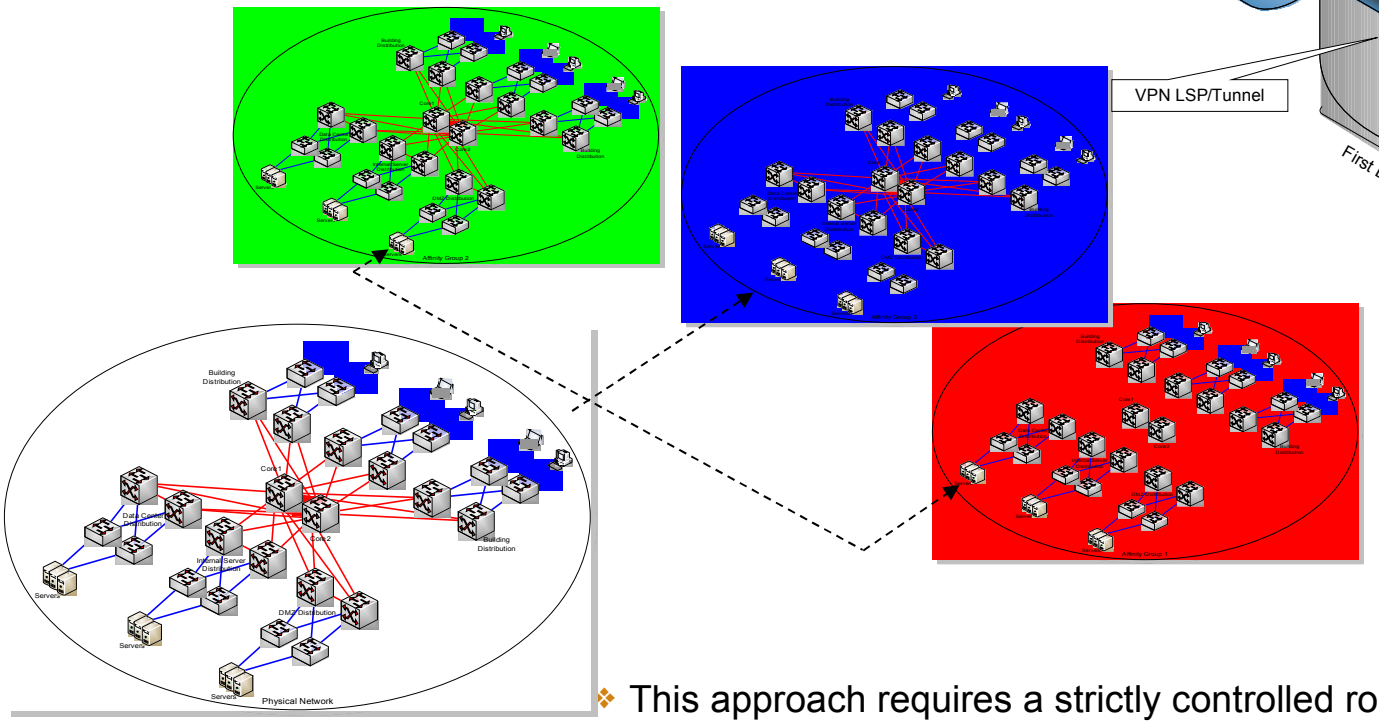
- Server virtualization requirements push upwards the Layer 2 boundary
- What is so bad about Layer 2?
  - ✓ **At best, blocked links (idle capacity), slow convergence (spanning tree), bounded identity capacity (MAC address table)**
  - ✓ **Fault domain - loops (no TTL), broadcasts, flooding, security, QoS**
- The distribution and core layer can be optimized
  - ✓ **Additional switching stage (Vswitch) already present**
  - ✓ **Latency requirements for IT Services performance, HA, virtualized services**
  - ✓ **High speed, high port density core switches**



Layer 3 Virtualization techniques allow to collapse different logical networks on a shared infrastructure

- Layer 3 Virtualization technologies (VRF) could be used to aggregate and then efficiently transport different Layer 2 traffics using a single set of virtualized device

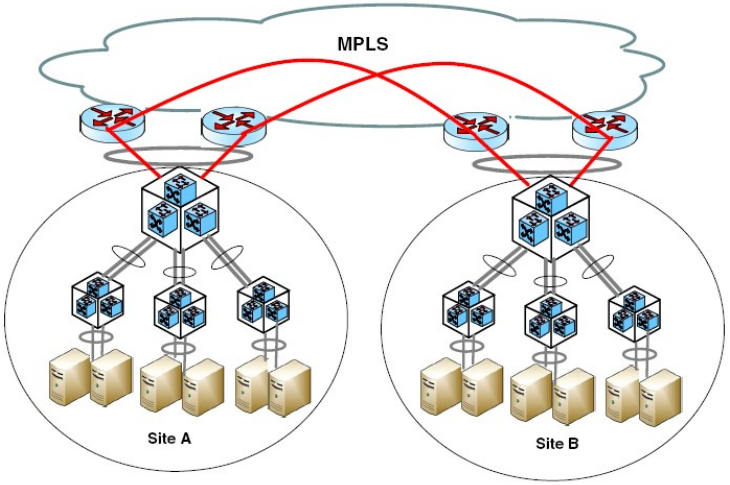


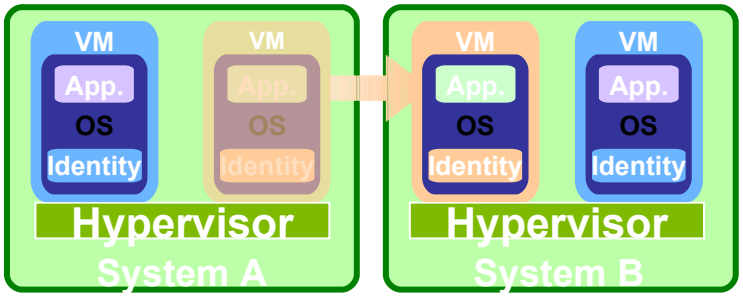


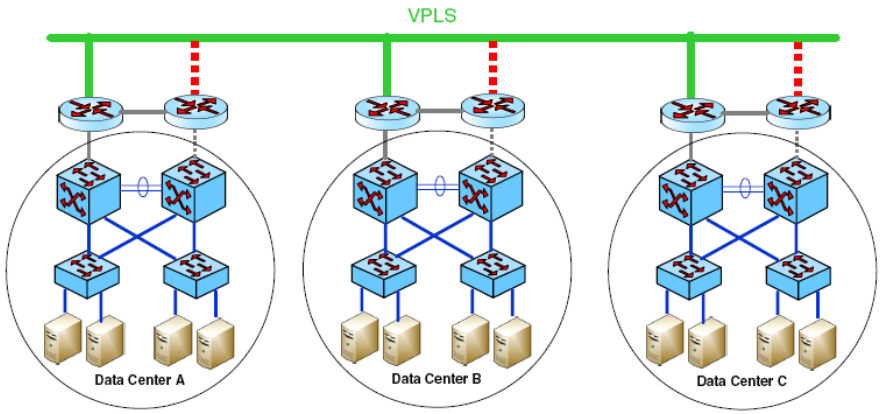
- This approach requires a strictly controlled routing layer to assure path isolation and to offer deterministic route for each L2 instance

VM/LPAR mobility support requires an extended Layer 2 domain

- Network requirements for VM/LPAR mobility between different Data Centers
  - ✓ **L2 connectivity , Access to the same VLAN**
  - ✓ **Spanning tree based control-plane not good enough**
    - ✓ **Proprietary approaches for Layer 2 Multipathing**
    - ✓ **IETF TRILL emerging as solution for L2 Multipathing (IS-IS based)**
  - ✓ **Layer 2 extensions required for Inter-Data Center Mobility**
    - ✓ **QinQ, EoMPLS, VPLS, OTV**
  - ✓ **Standard based approach for VM Port Profiles migration still missing**







Security Challenges with Virtualization: New Scenarios

- New needs

✓ **Dynamic relocation of VMs**

✓ **Increased infrastructure layers to manage and protect**

✓ **Multiple operating systems and applications per server**

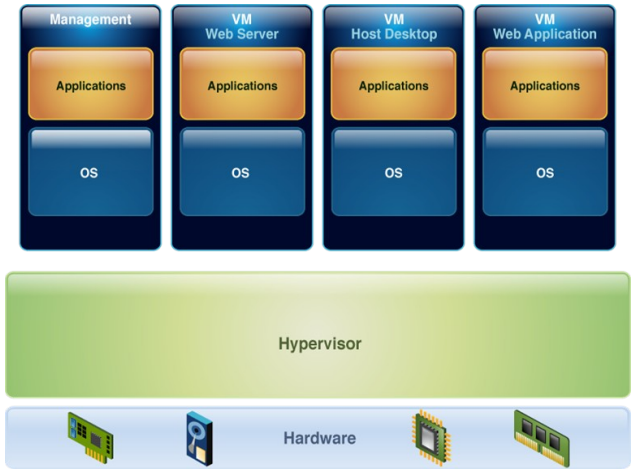
✓ **Elimination of physical boundaries between systems**

✓ **Manually tracking software and configurations of VMs**

Before Virtualization

- 1:1 ratio of OSs and applications per server

After Virtualization



- 1:Many ratio of OSs and applications per server
- Additional layer to manage and secure

Physical Boundary and VM Communication Issues: an example

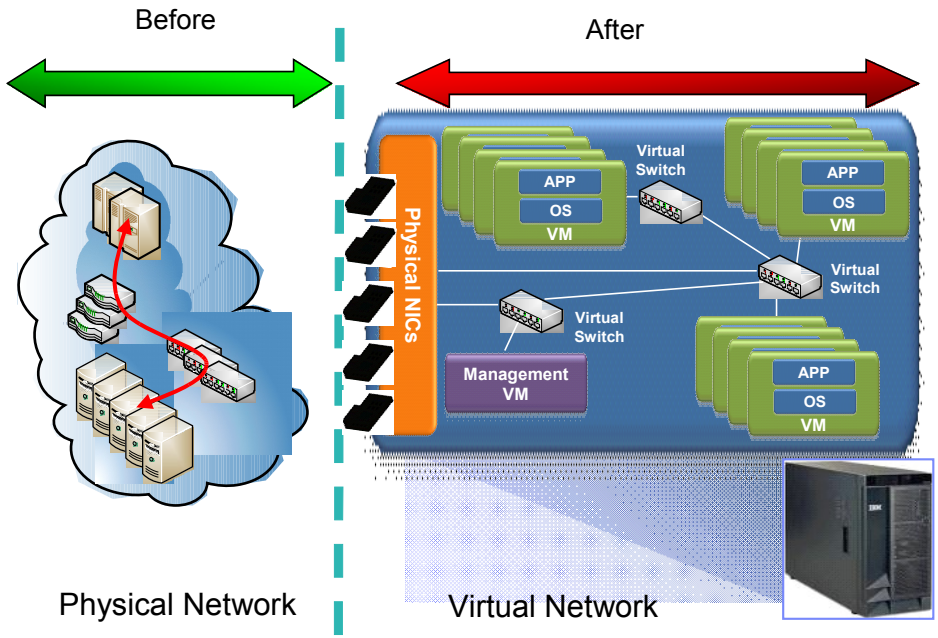
- Server & Network Convergence, physical perimeters move inside the machine:

  - ✓**Network extends through the Virtual Switch or the Virtual I/O Server**

  - ✓**Network Administration boundary moves into the Box:**

    - ✓**Could have some impacts on the network and server Management Process**
    - ✓**Could have some impacts on Roles & Responsibilities**

- Communications between Virtual Images cannot be monitored by external FW or IPS, therefore, attacks among Virtual Images are hard to detect using traditional methods.

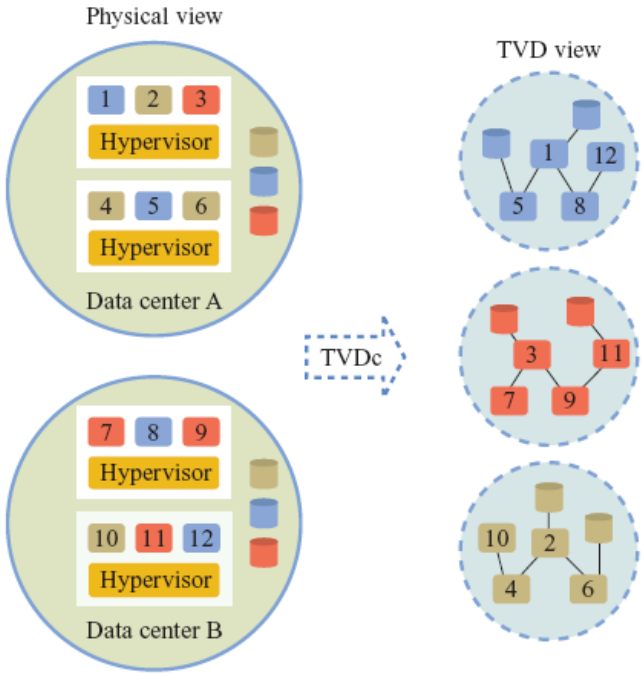


Trusted Virtual Data Center: the IBM model

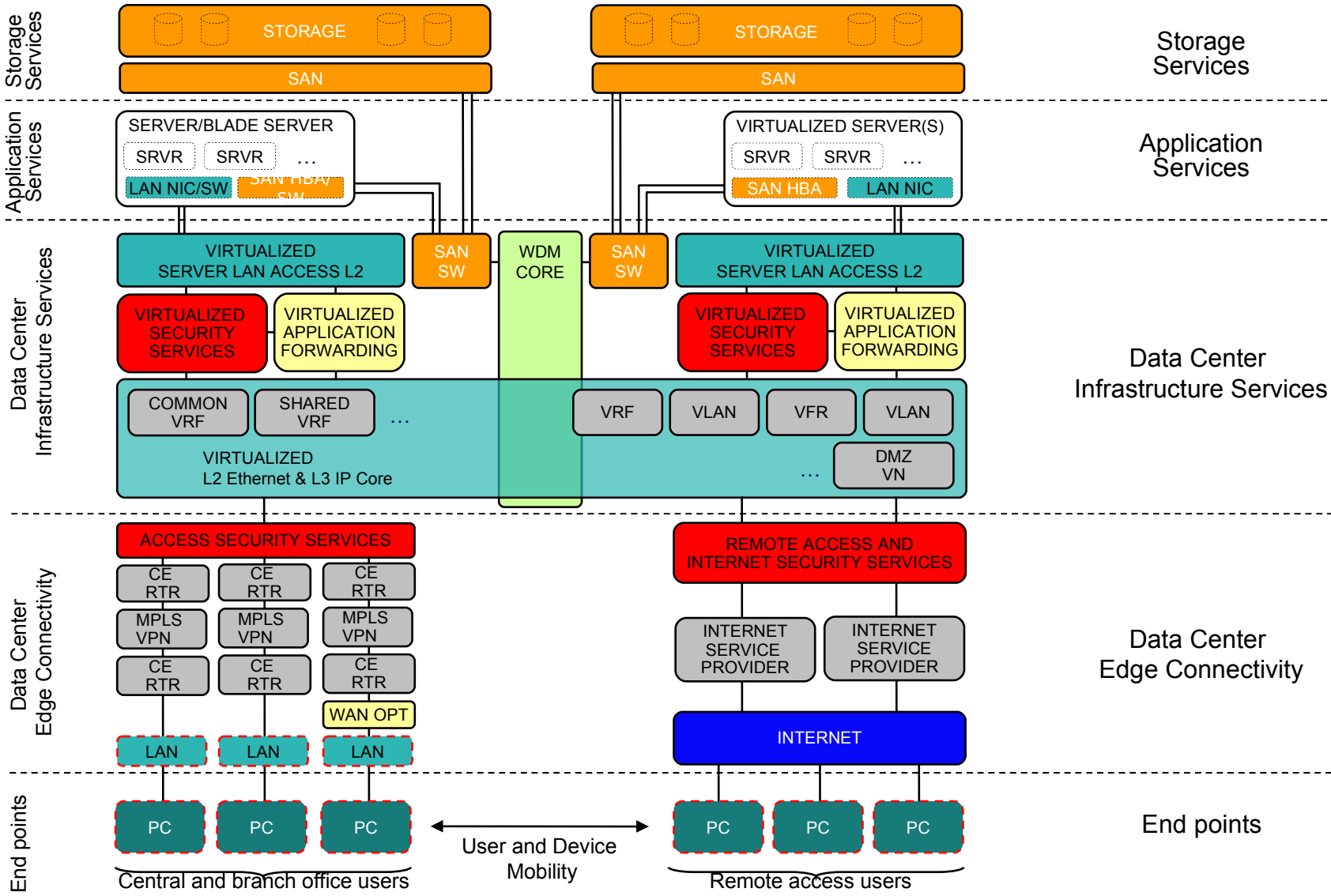
- The trusted virtual data center (TVDc) is a set of processes and technologies that address the need for strong isolation and integrity guarantees in cloud computing environments. VMs and associated resources are grouped into trusted virtual domains (TVDs)

- The objective of TVDc is to isolate workloads from each other. In particular, the TVDc aims to:

  - ✓ **prevent data from leaking from one specific workload to another, even when a VM running the workloads malfunctions;**
  - ✓ **ensure that viruses and other malicious code cannot spread from one customer workload to another and that break-ins in one workload do not threaten the workloads active within the same physical resource;**
  - ✓ **prevent or reduce the incidence of failed configuration management tasks (i.e., misconfiguration)**



Virtualization-aware Network: a Reference Architecture



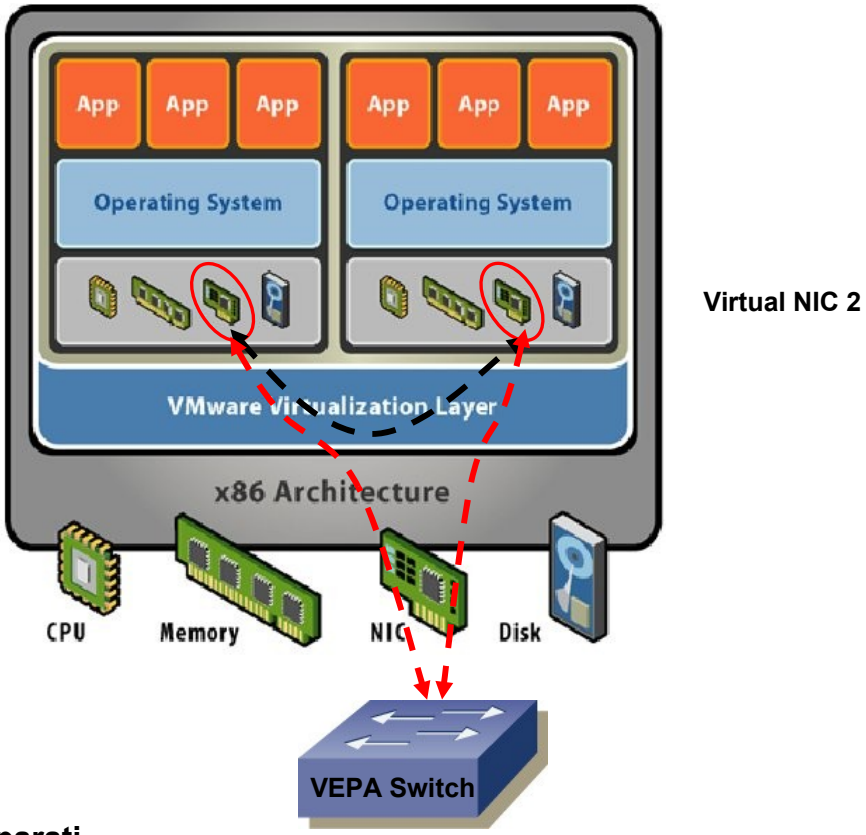
Agenda

- Introduction
- Networking for Cloud Computing Data Centers
- Evolution of the current Network Standards

Virtual Ethernet Port Aggregator: un protocollo emergente

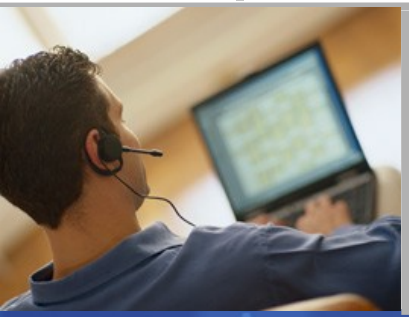
- **Caratteristiche del protocollo VEPA:**
  - ✓ **Consente l'offload delle risorse di elaborazione necessarie per il trattamento del traffico tra VNIC, dal Virtual Switch a uno switch fisico esterno**
  - ✓ **Sono state proposte due versioni IEEE: 802.1Qbg/h**
  - ✓ **Ratifica prevista per il primo semestre 2012**
  - ✓ **802.1Qbg sostenuto da HP**
  - ✓ **802.1Qbh sostenuto da Cisco (VN-tag) e gradito a VMware**
  - ✓ **Sostanzialmente è uno scambio tra risorse di elaborazione centrali e Bandwidth utilizzata verso lo switch fisico (minore utilizzo di CPU vs. maggiore larghezza di banda).**
  - ✓ **Necessita di Hardware dello Switch specifico per il supporto dell'hair-pinning.**
  - ✓ **Extreme Networks ha annunciato che alcuni suoi apparati potranno supportare VEPA con un aggiornamento software.**

Ambiente Virtualizzato



Global Technology Services

transform the way you communicate

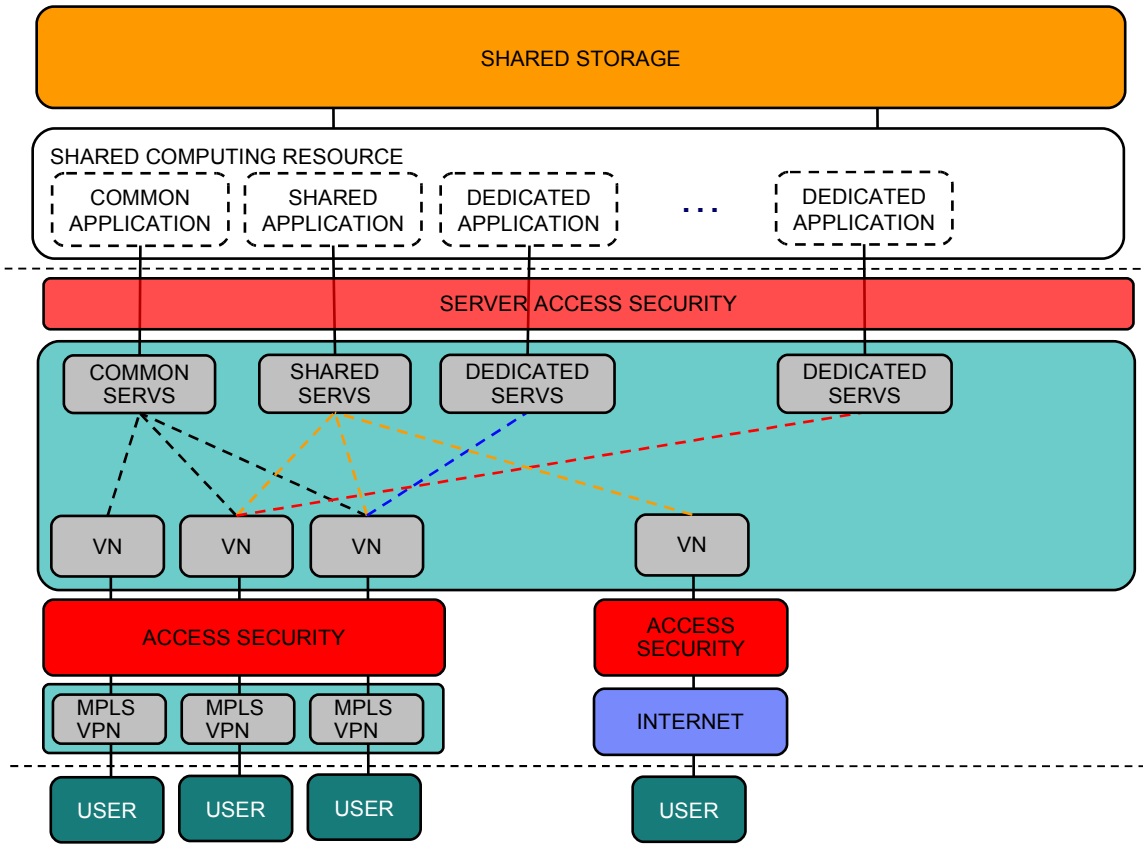





Security into a Cloud Infrastructure: a synthetic view

Domain	What	How
Network	✓Network Isolation ✓Network Access ✓DataFlows	✓Vlan ✓Firewall (virtual and physical) ✓IPS (virtual and physical) ✓Specific Security solution for Virtual environment
Intra-box	✓Workload Isolation ✓Granted Resource (CPU/IO/Mem) ✓Inter Communication segregation & confidentiality ✓Denial of Service	✓Vlan ✓Specific Security solution for Virtual environment ✓Third party security Certifications ✓Native or external solution (depending on the Hypervisor)
Storage	✓Data isolation ✓Data integrity ✓Data confidentiality at rest ✓Data confidentiality in flight	✓Encryption ✓Fiber Channel security enabled ✓Zoning ✓LUN Masking
Inter-Box	✓Security posture ✓Virtual Network Access Control ✓Confidentiality	✓Specific Security solution for Virtual environment ✓Specific Solution for patch management ✓Ad hoc network for Inter-Box Mobility
Infrastructure Management	✓Segregation of duties such as “Assign”, “Create”, “deploy”, “Activate”	✓Security Policy ✓Specific Management solution with RBAC capabilities

What are we ultimately trying to solve?



1

Provide consolidated and virtualized computing and storage resources to increase device utilization, improve system performance, and reduce power requirements and overall costs.

2

Provide secure and flexible data center core network based on defined community groups using highly virtualized and shared networking platform and security resources to increase network utilization, improve performance, and reduce power consumption and overall costs.

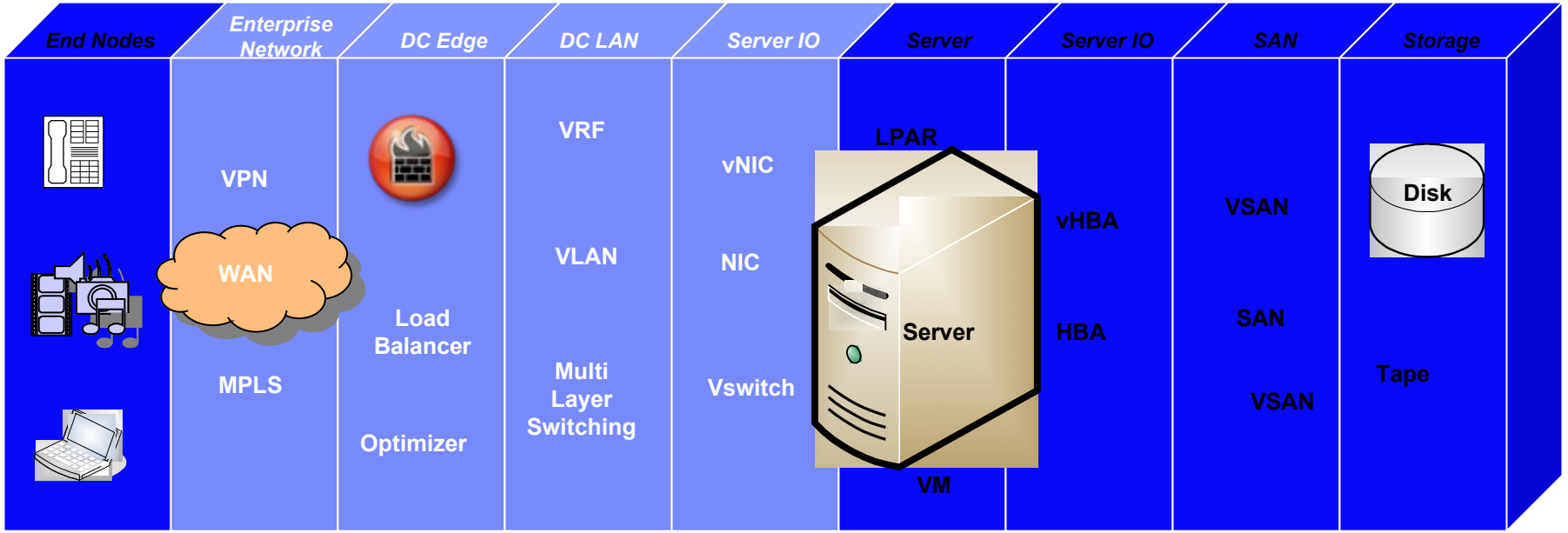
3

Provide secure yet flexible network access to specific services based on defined community groups (employees, partners, suppliers, customers, guests).

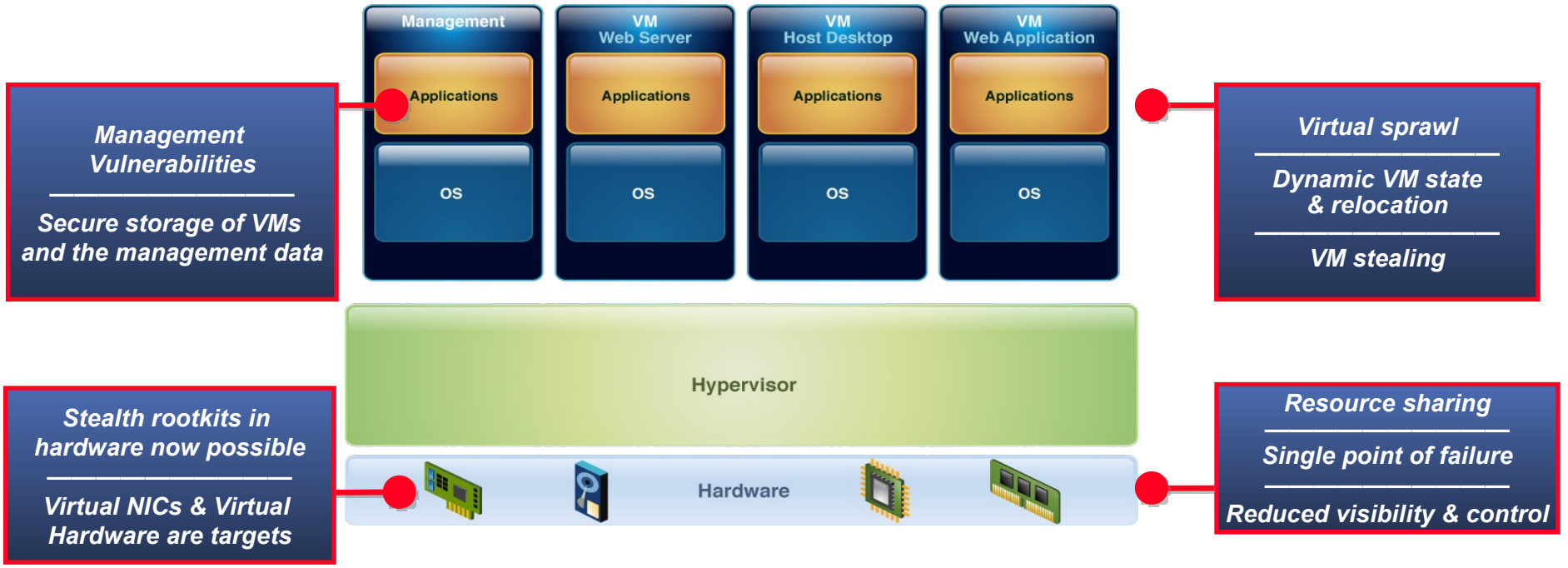
Virtualization-driven design patterns specific for the DC Network need to be used

- The Network infrastructure and services can be consolidated and virtualized using emerging Design patterns:

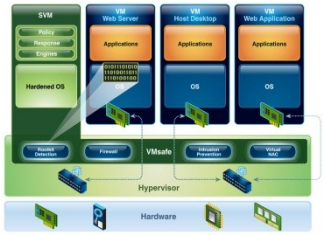
  - ✓ **LAN virtualization (VLANs, vSwitching)**
  - ✓ **IP Routing virtualization (VRFs, MPLS VPNs)**
  - ✓ **Node virtualization (Aggregation/Partitioning)**
  - ✓ **Link virtualization (Etherchannel, MPLS)**
  - ✓ **Firewall services virtualization**
  - ✓ **Load balancing services virtualization**
  - ✓ **Application acceleration services virtualization**
  - ✓ **Management plane virtualization**



Specific threats need to be considered in a virtualized environment



Virtualized infrastructures need a different set of protection tool

Need		Target
Mitigate new risks and complexities introduced by Virtualization		Provides dynamic protection for every layer of the virtual infrastructure
Maintain compliance standards and regulations		Helps meet regulatory compliance by providing security and reporting functionality customized for the virtual infrastructure
Drive operational efficiency		Increases ROI of the virtual infrastructure