Chapter 2 – Networks in Cloud Computing

Contents

- Parallel computing.
- Distributed systems.
- Network Architecture for Cloud.
- Data Center Network.
- Data Center Interconnect Network and Internet.
- Foundations of Cloud Computing Infrastructures.
- Virtualization Technology.
- Automation in Cloud Computing.
- Network Architecture for Hybrid Deployment.
- Concept of Autonomic Computing.
- Open Source Software in Data Center.

The path to cloud computing

- Cloud computing is based on ideas and the experience accumulated in many years of research in parallel and distributed systems.
  - Cloud applications are based on the client-server paradigm with a relatively simple software, a thin-client, running on the user's machine, while the computations are carried out on the cloud.
  - Concurrency is important; many cloud applications are data-intensive and use a number of instances which run concurrently.
  - Checkpoint-restart procedures are used as many cloud computations run for extended periods of time on multiple servers. Checkpoints are taken periodically in anticipation of the need to restart a process when one or more systems fail.
  - Communication is at the heart of cloud computing. Communication protocols which support coordination of distributed processes travel through noisy and unreliable communication channels which may lose messages or deliver duplicate, distorted, or out of order messages.

Parallel computing

- Parallel hardware and software systems allow us to:
  - Solve problems demanding resources not available on a single system.
  - Reduce the time required to obtain a solution.
- The *speed-up* S measures the effectiveness of parallelization:

$$S(N) = T(1) / T(N)$$

  T(1) → the execution time of the sequential computation.

  T(N) → the execution time when N parallel computations are executed.
- Amdahl's Law: if α is the fraction of running time a sequential program spends on non-parallelizable segments of the computation then

$$S = 1/ \alpha$$

- Gustafson's Law: the *scaled speed-up* with N parallel processes

$$S(N) = N – \alpha(N-1)$$

Concurrency; race conditions and deadlocks

- Concurrent execution can be challenging.
  - It could lead to race conditions, an undesirable effect when the results of concurrent execution depend on the sequence of events.
  - Shared resources must be protected by locks/ semaphores /monitors to ensure serial access.
  - Deadlocks and livelocks are possible.
- The four Coffman conditions for a deadlock:
  - Mutual exclusion - at least one resource must be non-sharable, only one process/thread may use the resource at any given time.
  - Hold and wait - at least one processes/thread must hold one or more resources and wait for others.
  - No-preemption - the scheduler or a monitor should not be able to force a process/thread holding a resource to relinquish it.
  - Circular wait - given the set of n processes/threads $\{P_1, P_2, P_3, \ldots, P_n\}$. Process P_1 waits for a resource held by P_2, P_2 waits for a resource held by P_3, and so on, P_n waits for a resource held by P_1.

Parallelism

- Fine-grain parallelism → relatively small blocks of the code can be executed in parallel without the need to communicate or synchronize with other threads or processes.
- Coarse-grain parallelism → large blocks of code can be executed in parallel.
- The speed-up of applications displaying fine-grain parallelism is considerably lower that those of coarse-grained applications; the processor speed is orders of magnitude larger than the communication speed even on systems with a fast interconnect.
- Data parallelism → the data is partitioned into several blocks and the blocks are processed in parallel.
- Same Program Multiple Data (SPMD) → data parallelism when multiple copies of the same program run concurrently, each one on a different data block.

Parallelism levels

- Bit level parallelism. The number of bits processed per clock cycle, often called a word size, has increased gradually from 4-bit, to 8-bit, 16-bit, 32-bit, and to 64-bit. This has reduced the number of instructions required to process larger size operands and allowed a significant performance improvement. During this evolutionary process the number of address bits have also increased allowing instructions to reference a larger address space.
- Instruction-level parallelism. Today's computers use multi-stage processing pipelines to speed up execution.
- Data parallelism or loop parallelism. The program loops can be processed in parallel.
- Task parallelism. The problem can be decomposed into tasks that can be carried out concurrently. For example, SPMD. Note that data dependencies cause different flows of control in individual tasks.

Parallel computer architecture

- Michael Flynn's classification of computer architectures is based on the number of concurrent control/instruction and data streams:
  - SISD (Single Instruction Single Data) – scalar architecture with one processor/core.
  - SIMD (Single Instruction, Multiple Data) - supports vector processing. When a SIMD instruction is issued, the operations on individual vector components are carried out concurrently.
  - MIMD (Multiple Instructions, Multiple Data) - a system with several processors and/or cores that function asynchronously and independently; at any time, different processors/cores may be executing different instructions on different data. We distinguish several types of systems:
    - Uniform Memory Access (UMA).
    - Cache Only Memory Access (COMA).
    - Non-Uniform Memory Access (NUMA).

Distributed systems

- Collection of autonomous computers, connected through a network and distribution software called middleware which enables computers to coordinate their activities and to share system resources.
- Characteristics:
  - The users perceive the system as a single, integrated computing facility.
  - The components are autonomous.
  - Scheduling and other resource management and security policies are implemented by each system.
  - There are multiple points of control and multiple points of failure.
  - The resources may not be accessible at all times.
  - Can be scaled by adding additional resources.
  - Can be designed to maintain availability even at low levels of hardware/software/network reliability.

Desirable properties of a distributed system

- Access transparency - local and remote information objects are accessed using identical operations.
- Location transparency - information objects are accessed without knowledge of their location.
- Concurrency transparency - several processes run concurrently using shared information objects without interference among them.
- Replication transparency - multiple instances of information objects increase reliability without the knowledge of users or applications.
- Failure transparency - the concealment of faults.
- Migration transparency - the information objects in the system are moved without affecting the operation performed on them.
- Performance transparency - the system can be reconfigured based on the load and quality of service requirements.
- Scaling transparency - the system and the applications can scale without a change in the system structure and without affecting the applications.

Network Architecture for Cloud

- Technology advancements and business developments in Broadband Internet, Web services, computing systems, and application software over the past decade has created a perfect storm for cloud computing.
- Cloud model of delivering and consuming IT functions as services is poised to fundamentally transform the IT industry.
- Rebalance the inter-relationships among end users, enterprise IT, software companies, and the cloud service providers in the IT ecosystem.
- In the data center of the cloud delivery and consumption model is the network.
- The network serves as the linkage between the end users consuming cloud services and the provider's data centers providing the cloud services.

Network Architecture for Cloud

- In large-scale cloud data centers, tens of thousands of compute and storage nodes are connected by a data center network to deliver a single-purpose cloud service.

- **Questions**:

- How do network architectures affect cloud computing?
- How will network architecture evolve to better support cloud computing and cloud-based service delivery?
- What is the network's role in security, reliability, performance, and scalability of cloud computing?
- Should the network be a dumb transport pipe or an intelligent stack that is cloud workload aware?

Network Architecture for Cloud

- There are three principal areas in which the network architecture is of importance to cloud computing:

1. A data center network that interconnects the infrastructure resources (e.g. servers and storage devices) within a cloud service data center,
2. A data center interconnect network that connects multiple data centers in a private, public, or hybrid cloud to supporting the cloud services,
3. The public Internet that connect end users to the public cloud provider's data centers.

   The last area has mostly to do with today's telecommunications network infrastructure, and is a complex topic by itself from the architectural, regulatory, operational and regional perspectives (for detail refer to **telecom cloud**).

Data Center Network

- Cloud providers offer scalable cloud services via massive data centers where Data Center Network (DCN) is constructed.
- DCN used to connect tens, sometimes hundreds, of thousands of serves to deliver massively scalable cloud services to the public.
- Hierarchical network design is the most common architecture used in data center networks.
- A hierarchical data center network as well as an example of mapping the reference architecture to a physical data center deployment given to next slide.

Data Center Network

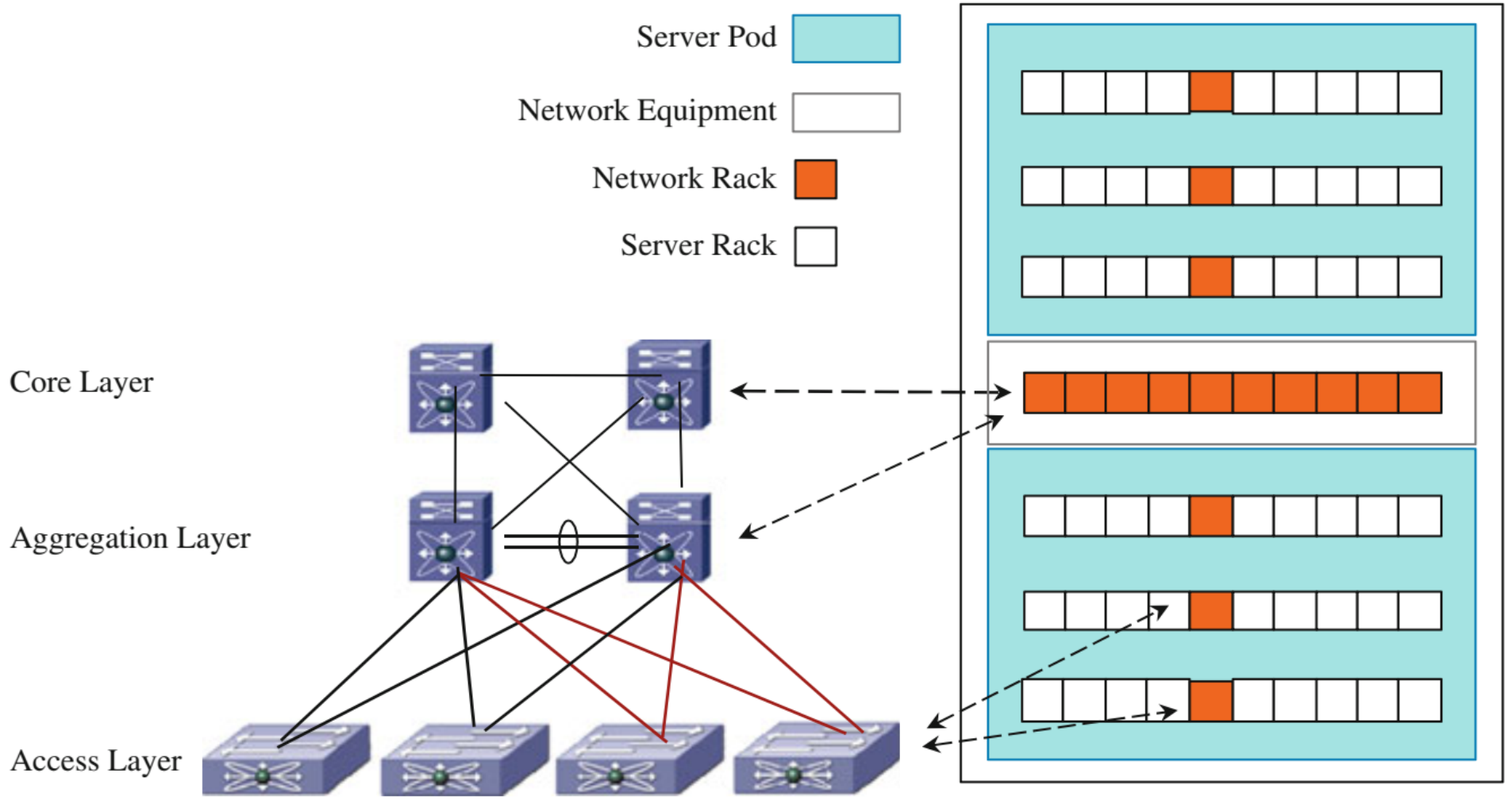


Fig. 4.2 Data center network architecture

Data Center Network

- ***Access layer*** of a data center network provides connectivity for server resource pool residing in the data center.
- Its design is heavily influenced by the decision criteria such as server density, form factor, and server virtualization that can result in higher interface count requirements.
- The commonly used approaches for data center access layer connectivity are *end-of-row* (EoR) switch, *top-of-rack* (ToR) switch, and *integrated switch* (typically in the form of blade switches inside a modular blade server chassis).
- Another form of the integrated switch is the embedded *software switch* in a server end point (Virtual distributed Ethernet Switch).
- Each design approach has pros and cons, and is dictated by server hardware and application requirements.

Data Center Network

- Aggregation layer of the data center provides a consolidation point where access layer switches are connected providing connectivity between servers for multi-tier applications, as well as connectivity across the core of the network to the clients residing within the campus, WAN, or Internet.
- This layer typically provides the boundary between Layer-3 routed links and Layer-2 Ethernet broadcast domains in the data center.

- The access switches are connected to the aggregation layer using 802.1Q VLAN trunks to provide the capability of connecting servers belonging to different VLANs and IP subnets to the same physical switch.

Data Center Network

- Core layer in a data center network is to provide highly available, high performance Layer-3 switching for IP traffic between the data center and Internet edge and backbone.
- In some situations, multiple geographically distributed data centers owned by a cloud service provider may be connected via a private WAN or a Metropolitan Area Network (MAN).
- For such environments, expanding Layer 2 networks across multiple data centers is a better architecture design.

Data Center Network

- In other situations, the traffic has to be carried over the public Internet. The typical network topologies for this kind of geographically distributed data centers is Layer-3 Peering Routing between the data center core switches.

- By configuring all links connecting to the network core as point-to-point Layer-3 connections, rapid convergence around any link failure is provided.

- The control plane of the core switches is not exposed to broadcast traffic from end node devices or required to participate in STP for Layer-2 network loop prevention.

Data Center Network

- Evolution of networking technology to support large-scale data centers is most evident at the access layer due to rapid increase of number of servers in a data center.

- Some research work (Greenberg, Hamilton, Maltz, & Patel, 2009; Kim, Caesar, & Rexford, 2008) calls for a large Layer-2 domain with a flatter data center network architecture (2 layers vs. 3 layers).

- This approach may fit a homogenous, single purpose data center environment, a more prevalent approach is based on the concept of switch virtualization which allows the function of the logical Layer-2 access layer to span across multiple physical devices.

Data Center Network

- There are several architectural variations in implementing switch virtualization at the access layer. They include Virtual Blade Switch (VBS), Fabric Extender, and Virtual Ethernet Switch technologies.

- The VBS approach allows multiple physical blade switches to share a common management and control plane by appearing as a single switching node (Cisco Systems, 2009d).

- The Fabric Extender approach allows a high-density, high-throughput, multi-interface access switch to work in conjunction with a set of fabric extenders serving as “remote I/O modules” extending the internal fabric of the access switches to a larger number of low-throughput server access ports.

Data Center Network

- The Virtual Ethernet Switch is typically software based access switch integrated inside a hypervisor at the server side.
- These switch virtualization technologies allow the data center to support multi-tenant cloud services and provide flexible configurations to scale up and down the deployment capacities according to the level of workloads.
- The hierarchical data center network architecture is scalable enough to support both mega data centers and micro data centers with the same design principles discussed here.

Data Center Interconnect Network and Internet

- Data center interconnect networks (DCIN) are used to connect multiple data centers to support a seamless customer experience of cloud services.

- While a conventional, statically provisioned virtual private network can interconnect multiple data centers and offer secure communications, to meet the requirements of seamless user experience for cloud services (high-availability, dynamic server migration, application mobility).

- The DCIN for cloud services has emerged as a special class of networks based on the design principle of Layer 2 network extension across multiple data centers (Cisco Systems, 2009b).

Data Center Interconnect Network and Internet

- Data center interconnect networks (DCIN) are used to connect multiple data centers to support a seamless customer experience of cloud services.

- While a conventional, statically provisioned virtual private network can interconnect multiple data centers and offer secure communications, to meet the requirements of seamless user experience for cloud services (high-availability, dynamic server migration, application mobility).

- The DCIN for cloud services has emerged as a special class of networks based on the design principle of Layer 2 network extension across multiple data centers (Cisco Systems, 2009b).

Data Center Interconnect Network and Internet

- For example, in the case of server migration (either in a planned data center maintenance scenario or in an unplanned dynamic application workload balancing scenario) when only part of the server pool is moved at any given time, maintaining the Layer 2 adjacency of the entire server pool across multiple data centers as opposed to renumbering IP addresses of servers is a much better solution.

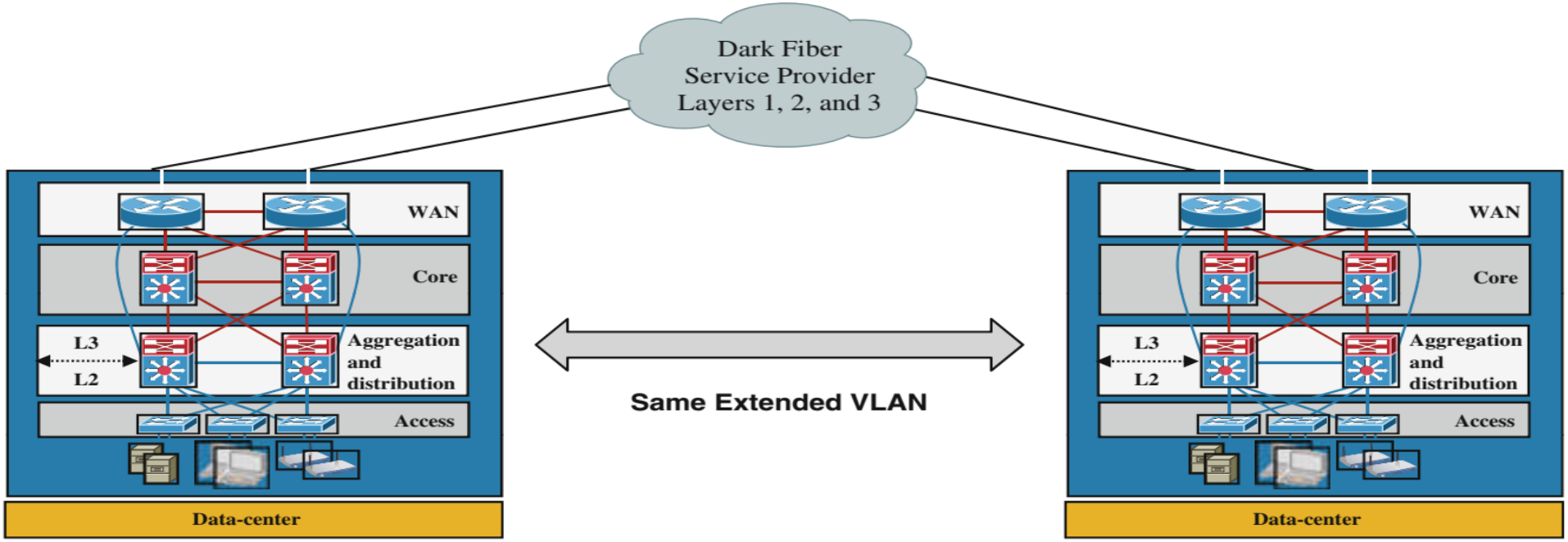
- The Layer 2 network extension approach, on one hand, is a must from business-continuity perspective; on the other hand, is cost effective from the operations perspective because it maintains the same server configuration and operations policies.

Data Center Interconnect Network and Internet

- **Use Cases** for data center interconnect networks are data center disaster avoidance (including data center maintenance without downtime), dynamic virtual server migration, high-availability clusters, and dynamic workload balancing and application mobility across multiple sites.

- These are critical requirements for cloud computing. Take the application mobility as an example. It provides the foundation necessary to enable compute elasticity – a key characteristics of cloud computing – by providing the flexibility to move virtual machines between different data centers.
- There are many areas of improvement and further research needed to meet the needs of data center interconnect networks. Listed below are some of the key requirements for Layer 2 network extension across multiple data centers.

Data Center Interconnect Network and Internet



WAN Transport	Description	LNA Extension Encapsulation Options
Dark Fiber and Service Provider Layer1	Customer Owned or Service Provider Leased	Native Ethernet, IP, MPLS
Service Provider Layer 2	Service Provider Layer 2 Service, Ethernet Private Line L (EPL)	Native Ethernet,IP, MPLS
Service Provider Layer 3	IP Leased-Line Service	IP, MPLS

Fig. 4.3 Data center interconnect LAN extension encapsulation options

Data Center Interconnect Network and Internet

- **End-to-End Loop Prevention -** To improve the high availability of the Layer 2 VLAN when it extends between data centers, this interconnection must be duplicated.

- Therefore, an algorithm must be enabled to control any risk of a Layer 2 loop and to protect against any type of global disruptions that could be generated by a remote failure.

- An immediate option to consider is to leverage Spanning Tree Protocol (STP), but it must be isolated between the remote sites to mitigate the risk of propagating unwanted behaviors such as topology change or root bridge movement from one data center to another.

Data Center Interconnect Network and Internet

- **WAN Load Balancing -** WAN links are expensive, so the uplinks need to be fully utilized, with traffic load-balanced across all available uplinks. A mechanism to dynamically balance workloads at the virtual machine level is an area of research.

- **Core Transparency -** The LAN extension solution needs to be transparent to the existing enterprise core network, if available, to reduce any effect on operations. This is more common in the private cloud or hybrid cloud environments than in a public cloud.

- **Encryption -** The requirement for LAN extension cryptography is increasingly prevalent, for example, to meet the needs for cloud services and for federal and regulatory requirements.

Network Architecture for Hybrid Deployment

- IT industry is in the midst of a transformation. Globalization, explosion of business information, unprecedented levels of interconnectedness and dynamic collaboration among different business assets both within a corporation and across multiple corporations (on-demand supply chain as an example) require today's enterprise businesses to move to an IT infrastructure that is truly economical, highly integrated, agile and responsive.

- Hybrid cloud model provides a seamless extension to an enterprise's private IT infrastructure by providing elastic compute, storage and network services in a cost-effective manner.

- To achieve this vision of business agility that hybrid clouds promise to enable, significant challenges lay ahead.

Network Architecture for Hybrid Deployment

- IT industry is in the midst of a transformation. Globalization, explosion of business information, unprecedented levels of interconnectedness and dynamic collaboration among different business assets both within a corporation and across multiple corporations (on-demand supply chain as an example) require today's enterprise businesses to move to an IT infrastructure that is truly economical, highly integrated, agile and responsive.

- Hybrid cloud model provides a seamless extension to an enterprise's private IT infrastructure by providing elastic compute, storage and network services in a cost-effective manner.

- To achieve this vision of business agility that hybrid clouds promise to enable, significant challenges lay ahead.

Network Architecture for Hybrid Deployment

- Challenging requirements for hybrid cloud deployments in terms of deployment and operational costs, quality of service delivery, business resiliency and security must be addressed.
- Hybrid clouds will need to support a large number of “smart industry solution workloads” – business applications in the form of smart transportation solutions, smart energy solutions, smart supply chain solutions, etc.
- A large amount of business information and control data will be collected, analyzed and reacted upon in a time constrained fashion across multiple tiers of cloud centers; workloads and data will be dynamically shifted within a hybrid cloud environment.

- This will require significant improvements to today’s network. Using the metaphor of a bridge design, we can describe these requirements in three categories – the foundation, the span and the superstructure.

Foundations of Cloud Computing Infrastructures

- Virtualization, automation and standards are the pillars of the foundation of all good cloud computing infrastructures.
- Without this foundation firmly in place across the servers, storage and network layers, only minimal improvements on the adoption of cloud services can be made;
- With this foundation in place, dramatic improvements can be brought about by “uncoupling” applications and services from the underlying infrastructure to improve application portability.
- However, this “uncoupling” must be done harmoniously such that the network is “application aware” and that the application is “network aware”.
- Both the data center network and the data center interconnect network and in the long run the public core network) – need to embrace virtualization and automation services.

Foundations of Cloud Computing Infrastructures

- The Foundation of cloud computing relies on:
  - Virtualization,
  - Automation and
  - Standards – The Foundation

Existing cloud infrastructure

- The cloud computing infrastructure at Amazon, Google, and Microsoft (as of mid 2012).
  - Amazon is a pioneer in Infrastructure-as-a-Service (IaaS).
  - Google's efforts are focused on Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS).
  - Microsoft is involved in PaaS.
- Private clouds are an alternative to public clouds. Open-source cloud computing platforms such as:
  - Eucalyptus,
  - OpenNebula,
  - Nimbus,
  - OpenStack

  can be used as a control infrastructure for a private cloud.

Amazon Web Services (AWS)

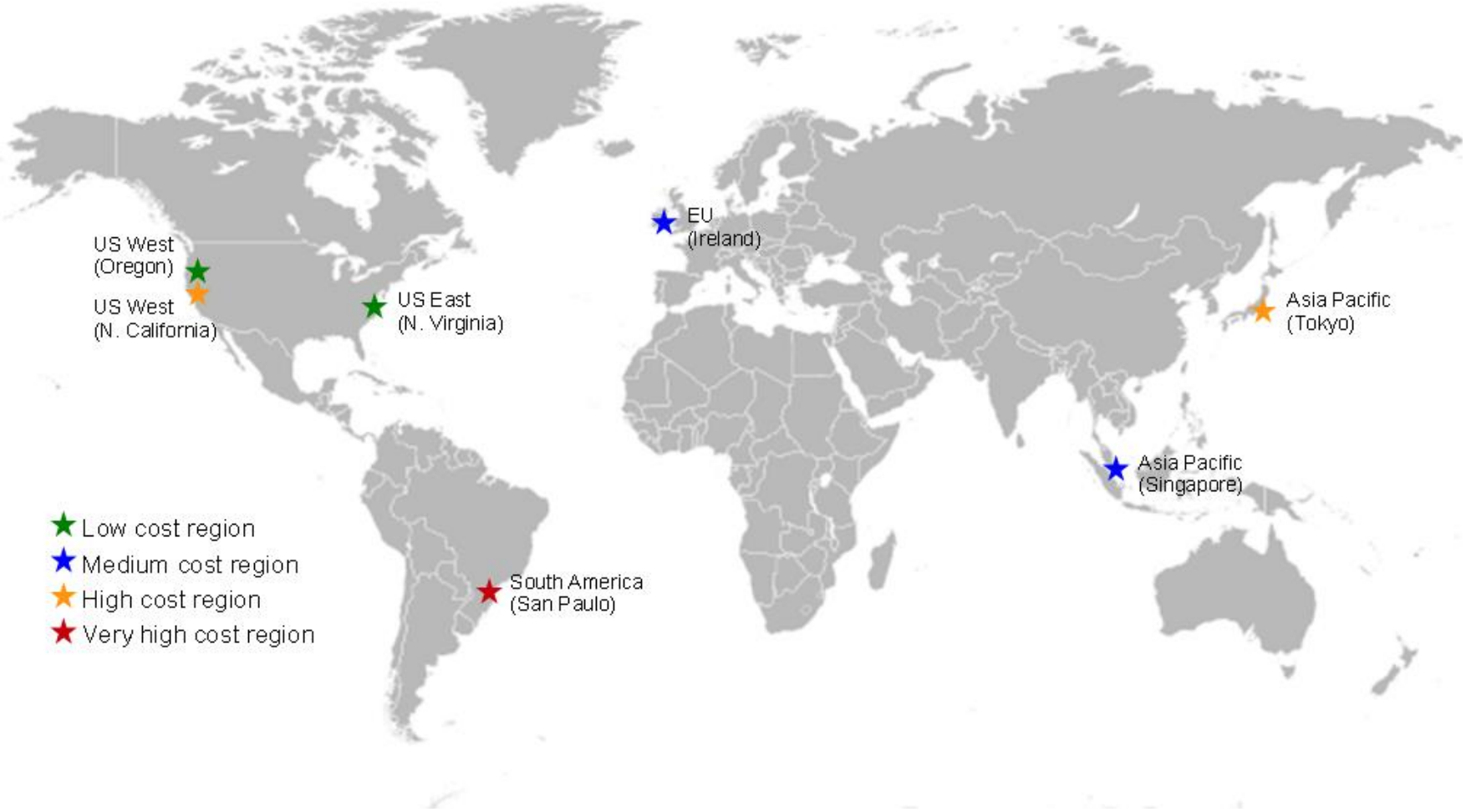
- AWS → IaaS cloud computing services launched in 2006.
-
- Businesses in 200 countries used AWS in 2012.
- The infrastructure consists of compute and storage servers interconnected by high-speed networks and supports a set of services.
- An application developer:
  - Installs applications on a platform of his/her choice.
  - Manages resources allocated by Amazon.

AWS regions and availability zones

- Amazon offers cloud services through a network of data centers on several continents.
- In each *region* there are several availability zones interconnected by high-speed networks.
- An *availability zone* is a data center consisting of a large number of servers.

Region	Location	Availability zones	Cost
US West	Oregon	us-west-2a/2b/2c	Low
US West	North California	us-west-1a/1b/1c	High
US East	North Virginia	us-east-1a/2a/3a/4a	Low
Europe	Ireland	eu-west-1a/1b/1c	Medium
South America	Sao Paulo, Brazil	sa-east-1a/1b	Very high
Asia Pacific	Tokyo, Japan	ap-northeast-1a/1b	High
Asia Pacific	Singapore	ap-southeast-1a/1b	Medium

- Regions do not share resources and communicate through the Internet.

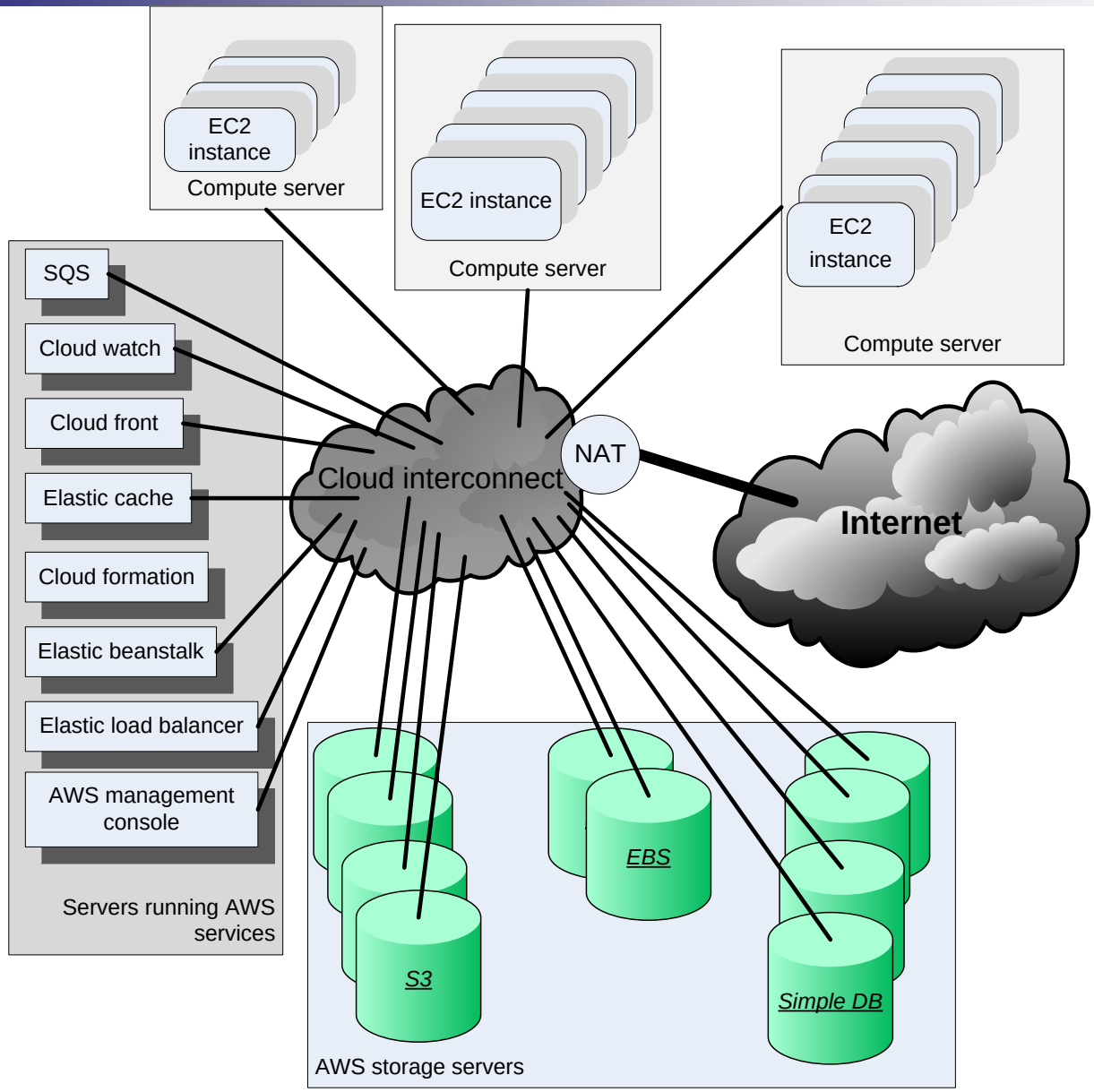

US West
(Oregon)
US West
(N. California)
US East
(N. Virginia)
EU
(Ireland)
Asia Pacific
(Tokyo)
Asia Pacific
(Singapore)
South America
(San Paulo)
Low cost region
Medium cost region
High cost region
Very high cost region

AWS instances

- An instance is a virtual server with a well specified set of resources including: CPU cycles, main memory, secondary storage, communication and I/O bandwidth.
- The user chooses:
  - The region and the availability zone where this virtual server should be placed.
  - An instance type from a limited menu of instance types.
- When launched, an instance is provided with a DNS name; this name maps to a
  - *private IP address* → for internal communication within the internal EC2 communication network.
  - *public IP address* → for communication outside the internal Amazon network, e.g., for communication with the user that launched the instance.

AWS instances (cont'd)

- Network Address Translation (NAT) maps external IP addresses to internal ones.
- The public IP address is assigned for the lifetime of an instance.
- An instance can request an *elastic IP address*, rather than a public IP address. The elastic IP address is a static public IP address allocated to an instance from the available pool of the availability zone.
- An elastic IP address is not released when the instance is stopped or terminated and must be released when no longer needed.


EC2 instance
Compute server
EC2 instance
Compute server
EC2 instance
Compute server
SQS
Cloud watch
Cloud front
Elastic cache
Cloud formation
Elastic beanstalk
Elastic load balancer
AWS management console
Servers running AWS services
Cloud interconnect
NAT
Internet
EBS
S3
Simple DB
AWS storage servers

Steps to run an application

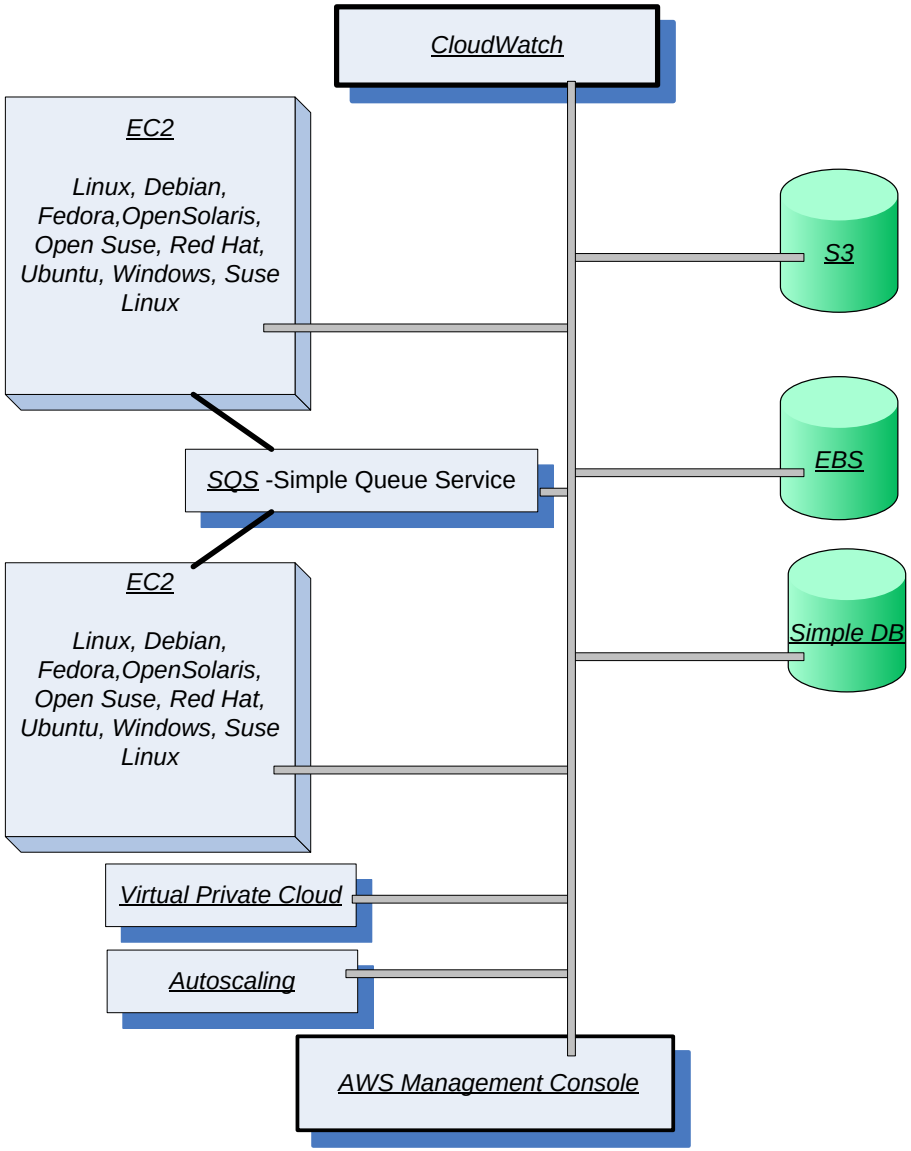
- Retrieve the user input from the front-end.
- Retrieve the disk image of a VM (Virtual Machine) from a repository.
- Locate a system and requests the VMM (Virtual Machine Monitor) running on that system to setup a VM.
- Invoke the Dynamic Host Configuration Protocol (DHCP) and the IP bridging software to set up MAC and IP addresses for the VM.

User interactions with AWS

- The AWS Management Console. The easiest way to access all services, but not all options may be available.
- AWS SDK libraries and toolkits are provided for several programming languages including Java, PHP, C#, and Objective-C.
- Raw REST requests.

Examples of Amazon Web Services

- *AWS Management Console* - allows users to access the services offered by AWS .
- *Elastic Cloud Computing (EC2)* - allows a user to launch a variety of operating systems.
- *Simple Queuing Service (SQS)* - allows multiple *EC2* instances to communicate with one another.
- *Simple Storage Service (S3)*, *Simple DB*, and *Elastic Bloc Storage (EBS)* - storage services.
- *Cloud Watch* - supports performance monitoring.
- *Auto Scaling* - supports elastic resource management.
- *Virtual Private Cloud* - allows direct migration of parallel applications.


CloudWatch
EC2
Linux, Debian, Fedora,OpenSolaris, Open Suse, Red Hat, Ubuntu, Windows, Suse Linux
S3
EBS
SQS -Simple Queue Service
EC2
Linux, Debian, Fedora,OpenSolaris, Open Suse, Red Hat, Ubuntu, Windows, Suse Linux
Simple DB
Virtual Private Cloud
Autoscaling
AWS Management Console

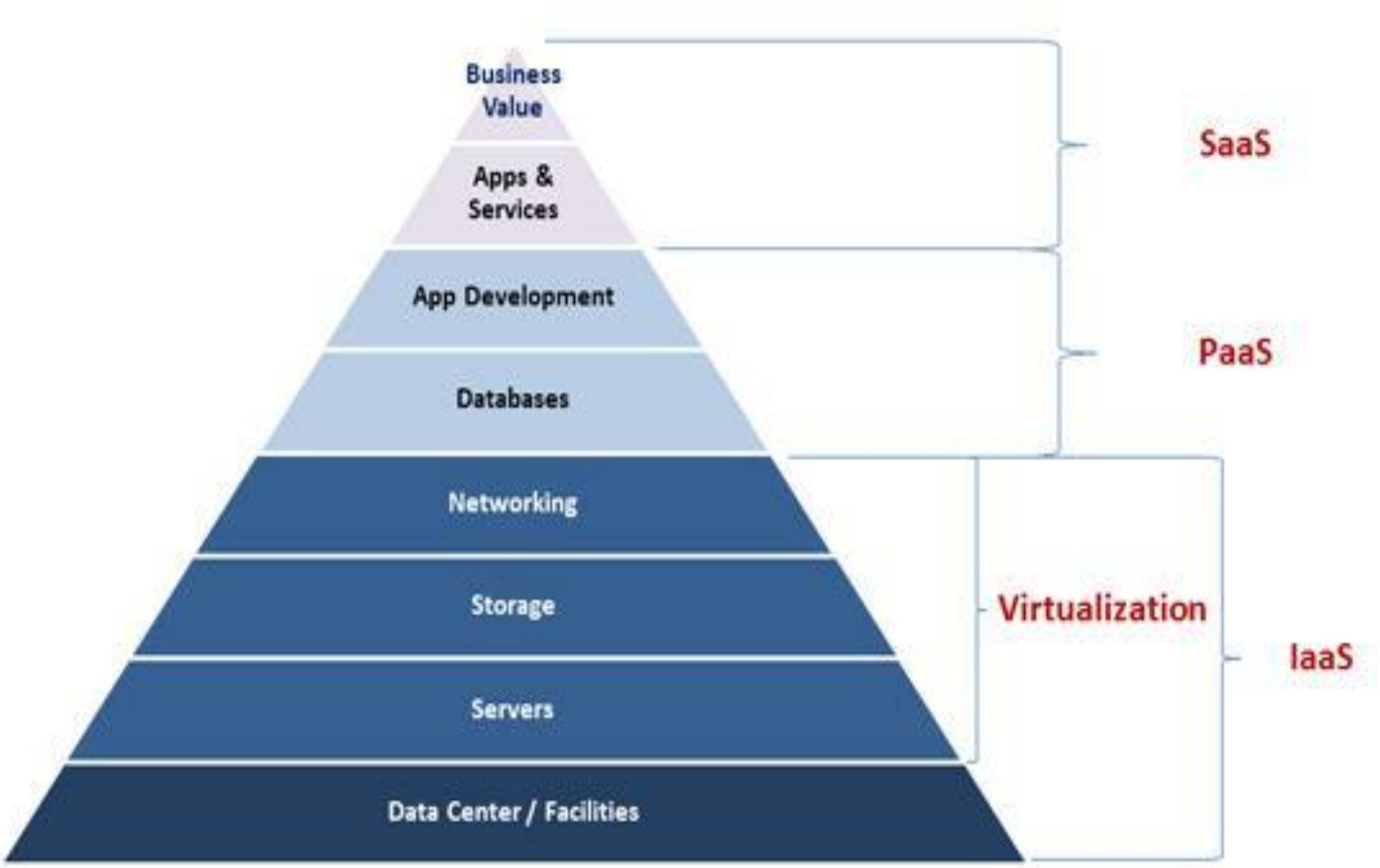
EC2 – Elastic Cloud Computing

- *EC2* - web service for launching instances of an application under several operating systems, such as:
  - Several Linux distributions.
  - Microsoft Windows Server 2003 and 2008.
  - OpenSolaris.
  - FreeBSD.
  - NetBSD.
- A user can
  - Load an *EC2* instance with a custom application environment.
  - Manage network's access permissions.
  - Run the image using as many or as few systems as desired.

EC2 (cont'd)

- Import virtual machine (VM) images from the user environment to an instance through *VM import*.
- *EC2* instances boot from an AMI (Amazon Machine Image) digitally signed and stored in *S3*.
- Users can access:
  - Images provided by Amazon.
  - Customize an image and store it in *S3*.
- An *EC2* instance is characterized by the resources it provides:
  - VC (Virtual Computers) – virtual systems running the instance.
  - CU (Compute Units) – measure computing power of each system.
  - Memory.
  - I/O capabilities.

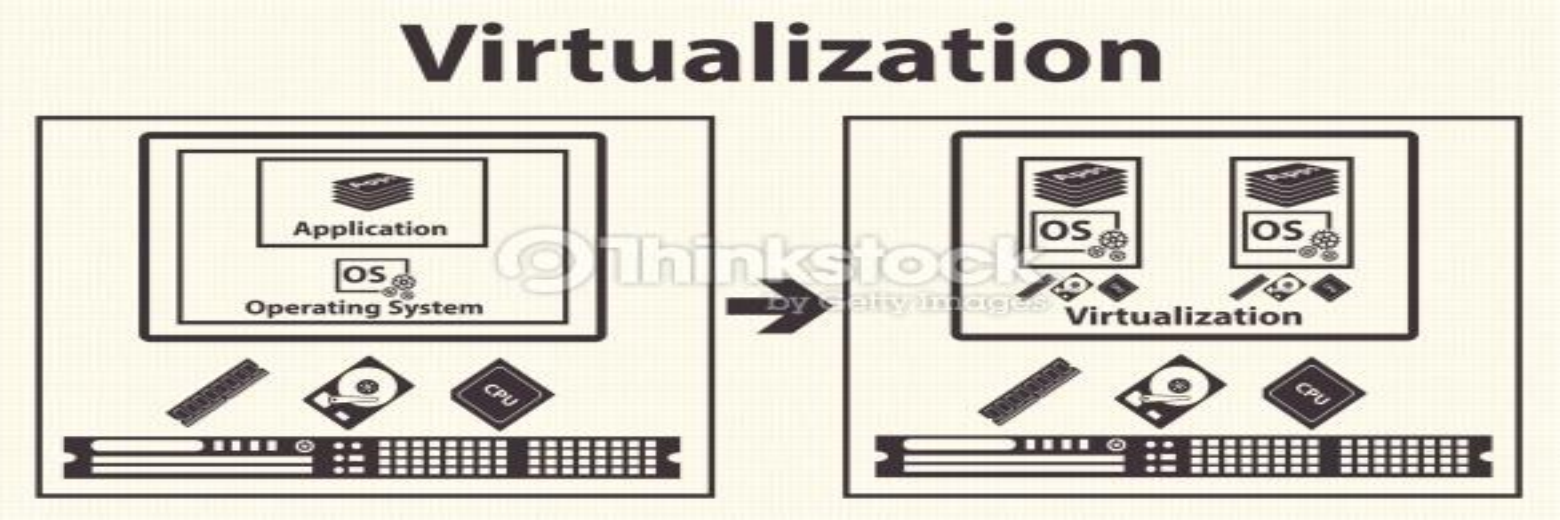
Cloud Virtualization Technology



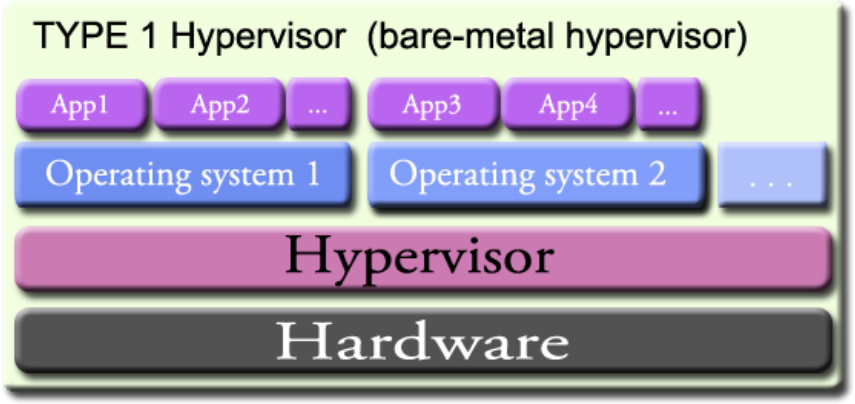
Cloud Virtualization Technology

Introduction

- Virtualization represents the logical view of data representation- the power to compute in virtualized environments.
- It is a technique that has been used in large mainframe computer for 30+ years. It is used to manage a group of computers together- instead of managing resources separately.

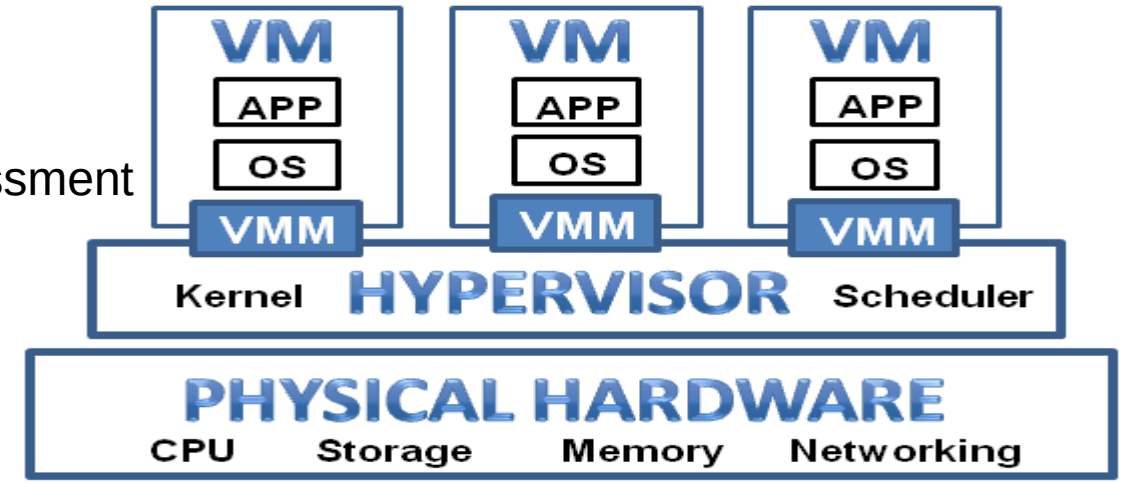


Cloud Virtualization Technology



Virtualization Defined

- Virtualization is an abstraction layer (hypervisor) that decouples the physical hardware from the operating system to deliver greater IT resources utilization and flexibility
- Virtualization can bring the following benefits
  - save money
  - increased control
  - simplify disaster recovery
  - business readiness assessment

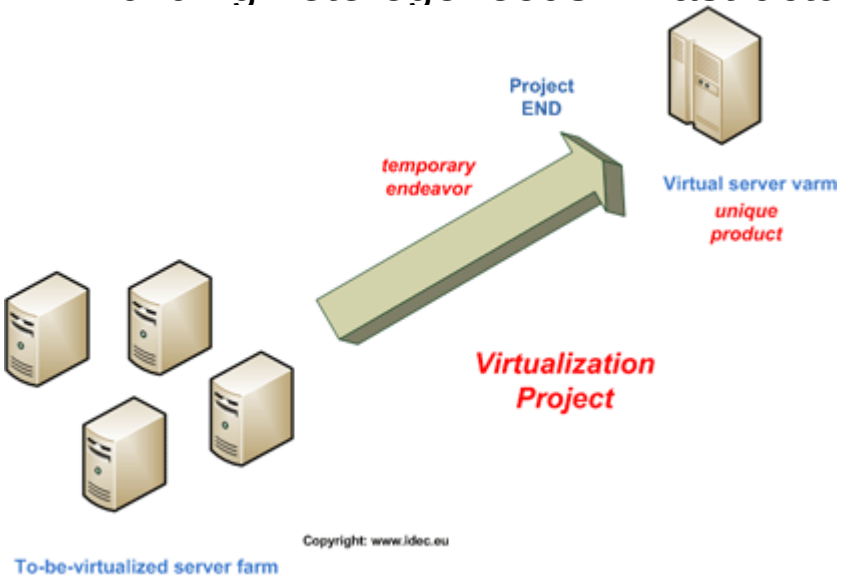


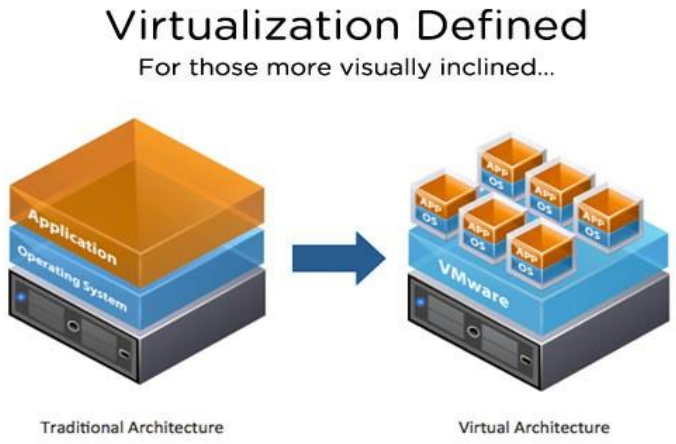
Cloud Virtualization Technology

Why Virtualization?

Here are some reasons for going for virtualization

- Lower cost of infrastructure
- Reducing the cost of adding to that infrastructure
- Gathering information across IT set up for increased utilization and collaboration
- Deliver on SLA response time during spikes in production
- Building heterogeneous infrastructure that are responsive

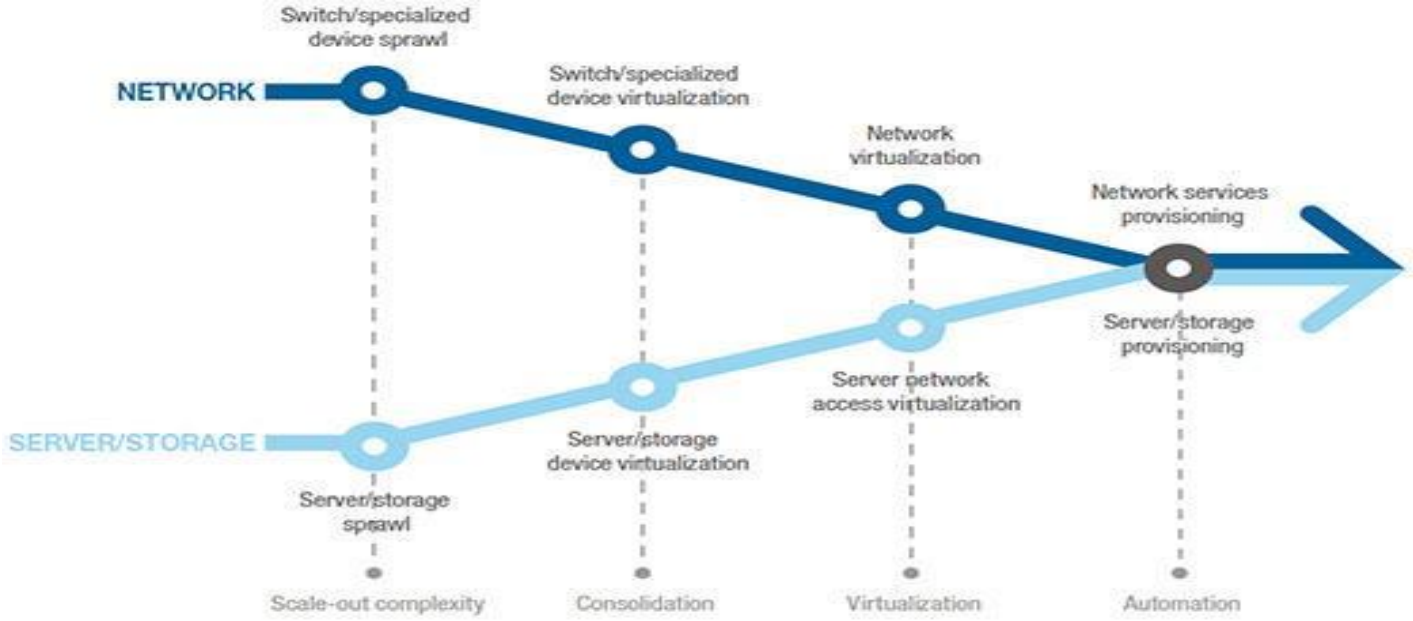




Cloud Virtualization Technology

Infrastructure Virtualization Evolution

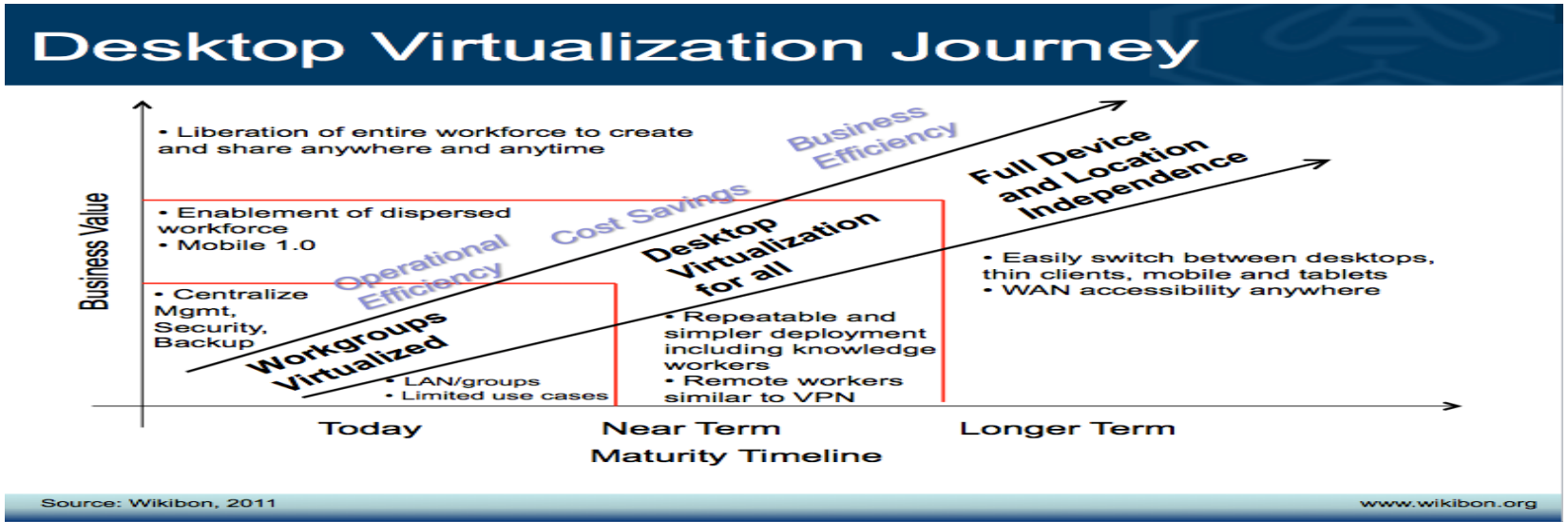
- The objective of virtualization is to reduce complexity in building and managing IT infrastructure.
- Virtualization has been in operation in mainframe computers
- Different machines can run different operating systems and multiple applications on the same physical computer.
- Each virtual machine encapsulated and segregated, and contains a complete system including CPU, Memory and network devices to prevent conflict and allow single physical machine to safely run several different OS and applications on the same hardware



Cloud Virtualization Technology

Virtualization Benefits,

1. **Traditional benefits**
   a. server consolidation
   b. “Green IT” - reduced power and cooling- carbon print
   c. Reduced hardware costs
2. **Additional Benefits**
   a. increased availability/business continuity and disaster recovery
   b. maximized hardware resources
   c. reduced administration and labour costs
   d. efficient application and desktop software deployment and maintenance
   e. reduced time for server provisioning
   f. increased security on the desktop client level
   g. dynamic and extensible infrastructure to rapidly address new business requirements

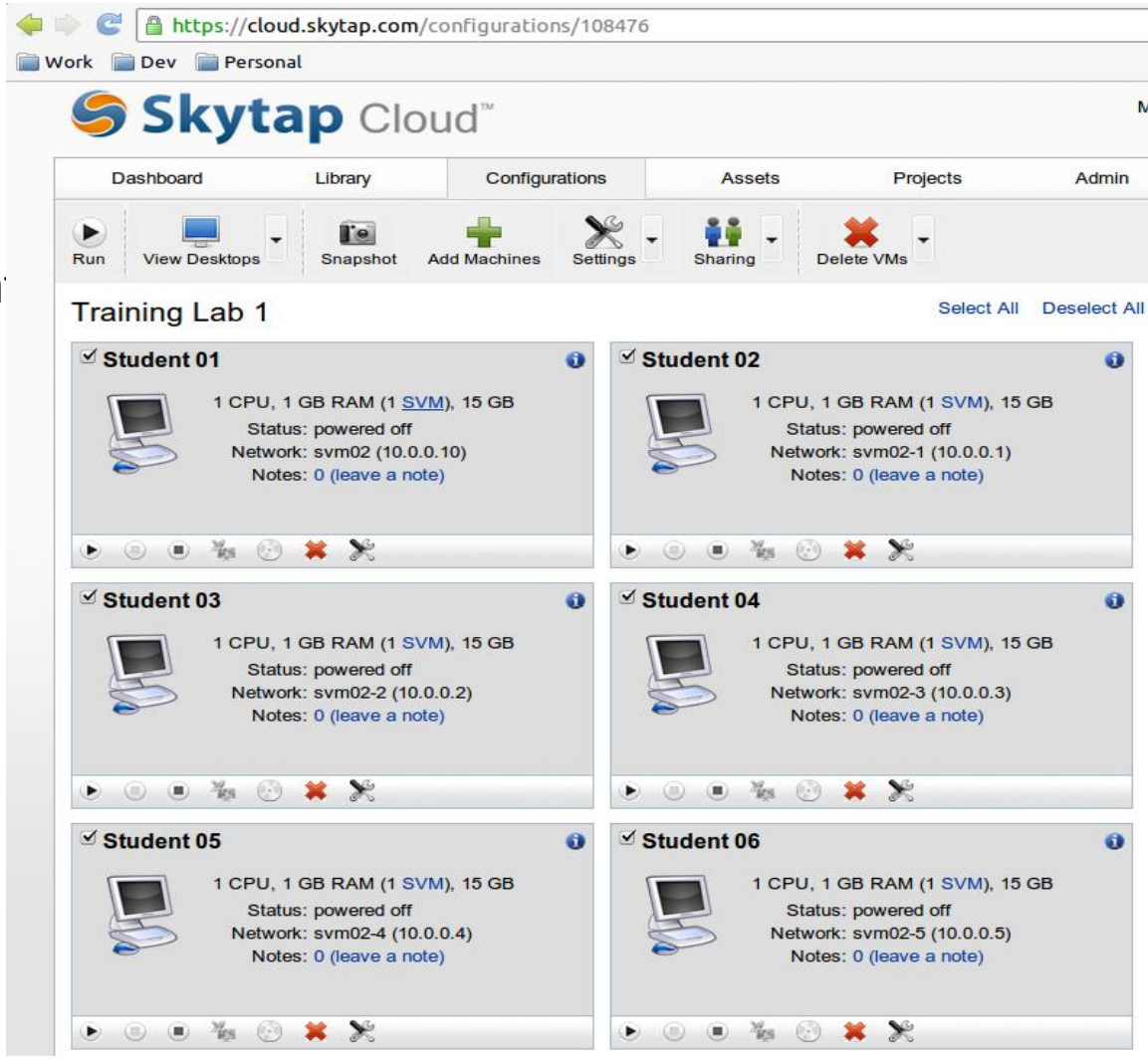


Cloud Virtualization Technology

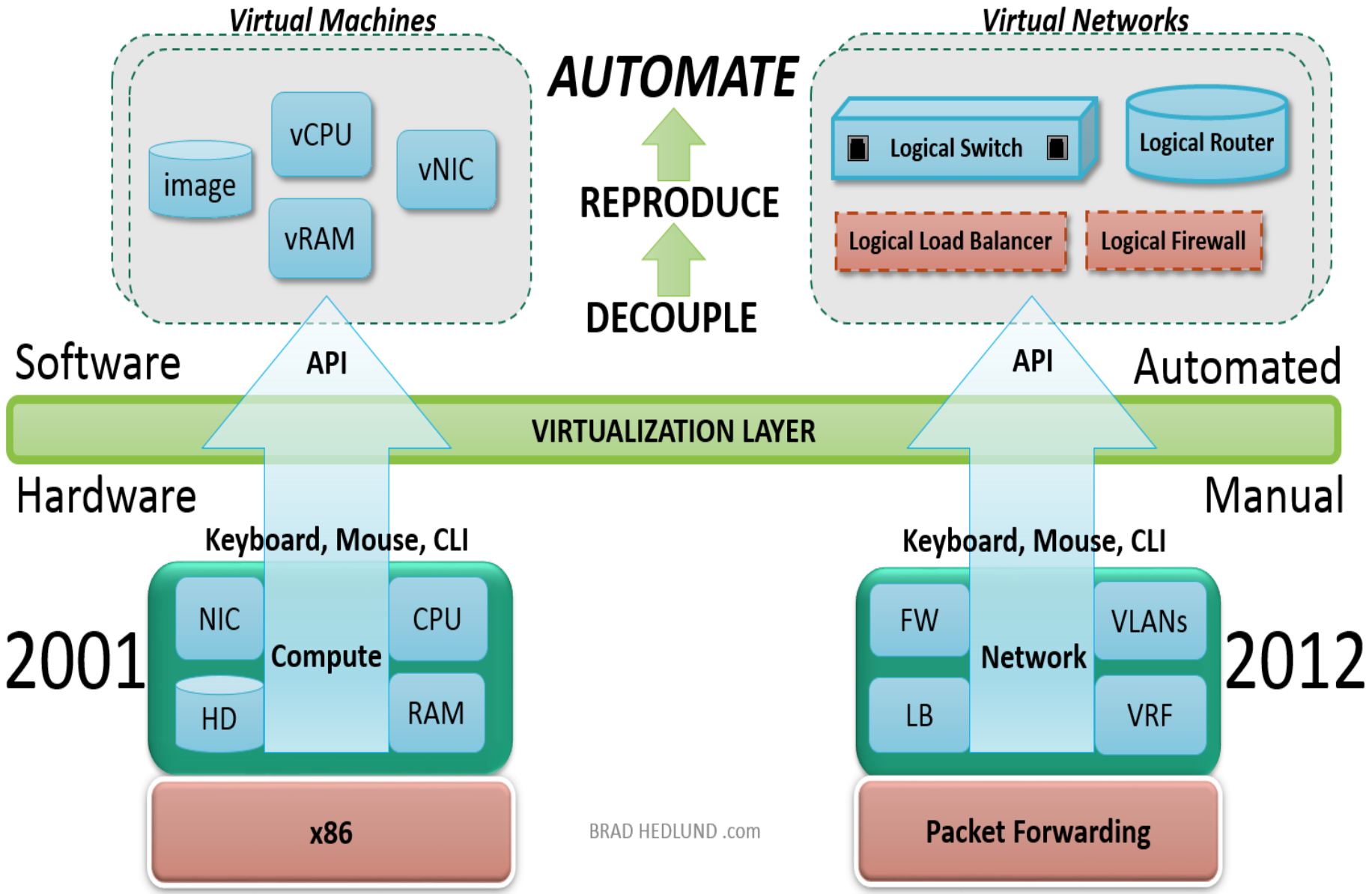
Current Virtualization Initiatives

Here is a list of different virtualization initiative actively pursued in industry today

- Virtual CPU and Memory
- Virtual Networking
- Virtual Disk
- Consolidated managemen
- Vmotion
- Svmotion
- Dynamic load balancing
- Logical partitions(LPARs)
- Logical Domains (LDOM)
- Zones



Server Virtualization Network Virtualization



BRAD HEDLUND .com

Foundations of Cloud Computing Infrastructures

- Cloud dynamic infrastructure which is “centered” on service delivery not only requires enterprise IT to transcend the daily IT break-and-fix routine but to create a paradigm shift within the user community toward a shared environment with repeatable, standardized processes.

- Easier and faster access to services make the standardization acceptable or even attractive to users since they sacrifice the ability to customize but gain convenience and time.

- There is a strong need for open standards to enable interoperability and federation across not only the individual layers of a private cloud behind an enterprise’s firewall but also when consuming public cloud based services.

Foundations of Cloud Computing Infrastructures

- Cloud can enable the automation needed to deliver quality services at almost any scale by leveraging not only the private network but also the public internet via managed network service providers.
- Service management and automation also plays a critical role in hybrid clouds.
- As cloud services continue to advance, future networking services for cloud applications will be offered through an application-oriented abstraction layer APIs, rather than in specific networking technologies.
- On top of the common virtualization layer, a service management application allow the management and automation of cloud services provisioning, accounting and billing, security, dynamic resource reallocation and workload mobility.

Foundations of Cloud Computing Infrastructures

- Automation is required for:
  - Scale and speed of deployment
  - Dynamics of the environment
  - Cost of deployment
- Automation goes hand-in-hand with virtualization
  - A cloud environment implies dynamic scaling based on demand
  - Implementing a manual process for this is too time consuming
  - Applications are structured in “independent blocks” that can be easily added or removed
  - Implementing virtualization assists with automation
  - Automation realizes the value of virtualization: dynamic scaling
- Service automation used for security:
  - An automated way to analyze and manage security flows and processes in support of security compliance audits
  - Reporting any events which violate security policies or customer licensing issues

Network Architecture for Hybrid Deployment

- Hybrid clouds play a key role in the adoption of cloud computing as the new generation IT paradigm.
- Today, IT industry and the research community are still in the early stage to understand the implementation technologies for hybrid clouds.
- Next slide shows a functional view of the network architecture for hybrid clouds.

Network Architecture for Hybrid Deployment

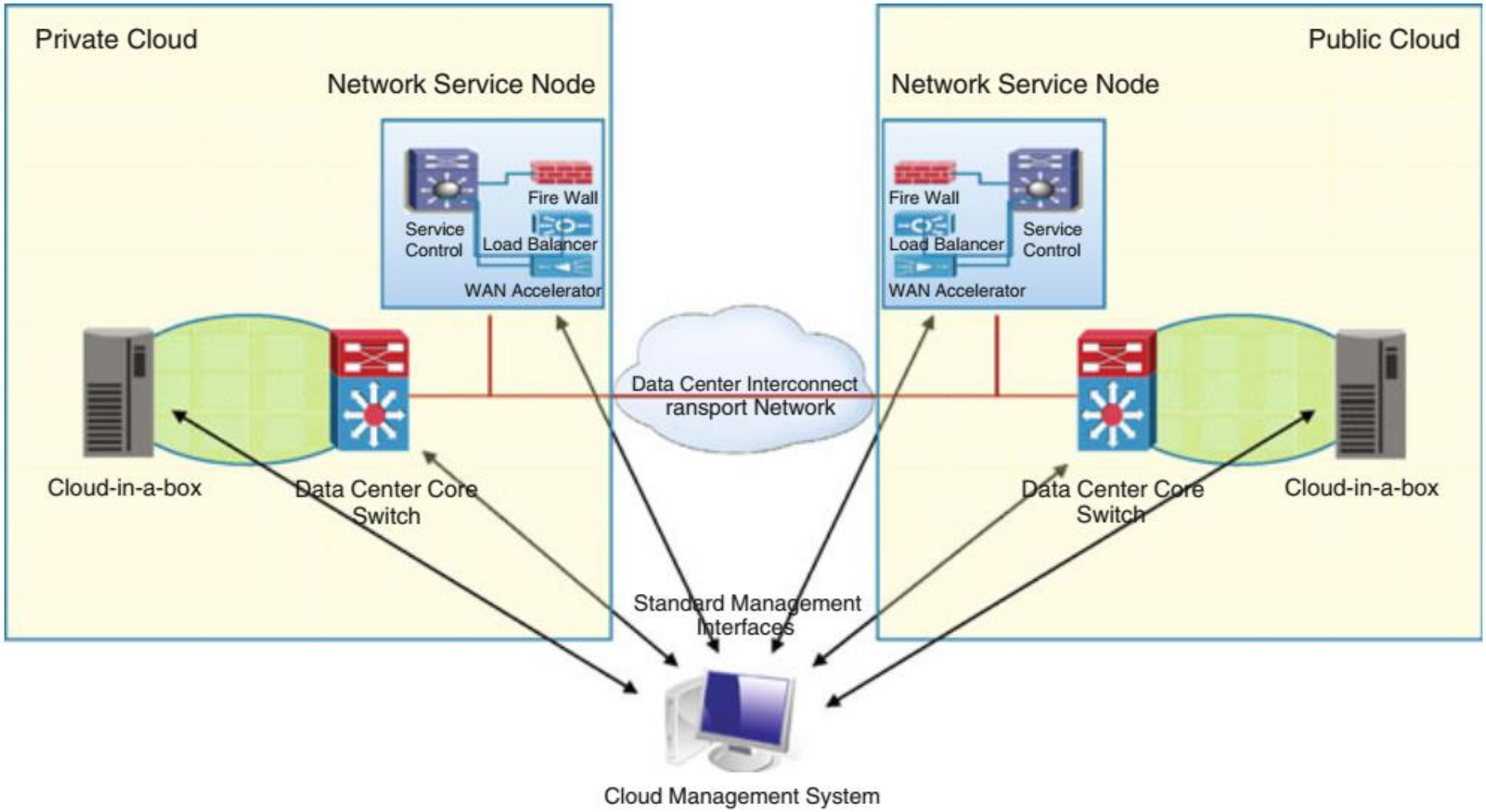


Fig. 4.4 A Functional view of network architecture for hybrid clouds

Cloud-in-a-Box

- Many big enterprises start to build their own private clouds and further expand them into hybrid clouds, a significant need is to simplify the design, deployment, and management of clouds.
- Traditional DC deployment model of having separated physical server units, networking units, and storage units presents a significant challenge.
- A new trend in the design and deployment of private and hybrid clouds is the concept of "***cloud-in-a-box***."
- A cloud-in-a-box, sometimes also called a *cloud cell,* is a pre-integrated, prepackaged and self-contained service delivery platform that can be used easily and quickly to implement private cloud centers.

Cloud-in-a-Box

- Cloud cell is typically delivered in a single chassis containing multiple blades; some blades are computing units, some switching units, and some storage units interconnected by a combination of a common converged Ethernet connections (e.g. 10G FCoE).
- From the networking perspective, switches that are pre-integrated into a cloud-in-a-box are typically the access layer switches.
- Software wise, a common hypervisor environment typically expands across computing units, networking units, and storage units in a cloud-in-a-box device.
- From the networking perspective, this requires a virtual Ethernet switch be embedded in the hypervisor.

Cloud-in-a-Box

- In VM environment, the VMware's vNetwork Distributed Switch and Cisco's Nexus 1000v virtual switch are the two well known examples of hypervisor-embedded virtual Ethernet switches.
- A development-and-test oriented cloud-in-a-box platform may pre-integrate and prepackage a cloud-ready Integrated Development Environment (IDE) as part of the product.
- Eg: Hyperflex machine

Network Service Node

- Layer 4 network services play an important role in the network architecture for hybrid clouds.
- Application firewalls ensure the secure transport of user data and application workloads between the DCs in a hybrid cloud;
- Server LB ensure the workloads distributed evenly or according to operations policies both within a single DC and across multiple DCs.
- WAN accelerators (CDN) provide WAN optimization that accelerates the targeted cloud workloads over the WAN.

Network Service Node

- The Layer 4 services now need to be virtualization aware. So, visibility into virtual machine activity and isolation of server traffic becomes more difficult when virtual machine-sourced traffic can reach other virtual machines both within the same server and across the data center network and data center interconnect network.
- what happens when applications now reside on virtual machines and multiple virtual machines reside within the same physical server?
- It might not be necessary for traffic to leave the physical server and pass through a physical access switch for one virtual machine to communicate with another.

Network Service Node

- On the other hand, application residing in a virtual machine can be “moved” to another DC for load balancing.
- How to ensure the WAN accelerator to recognize application residing within a virtual machine and optimize the WAN treatment for a virtual machine?
- Enforcing network policies in this type of environment can be a significant challenge in layer-4 network services to support cloud service deployment..
- The goal remains to provide many of the same network services and features used in the traditional access layer in the new virtualization-aware access layer.

Management of the Network Architecture

- Management of the network architecture in a hybrid cloud is part of the overall cloud management system.
- Both physical and virtual network management are Key requirement in the hybrid cloud.
- Virtualization management starting from the virtual Ethernet switch embedded in the Hypervisor, through the access and core switches the data center network, and across the data center interconnect network.
- The network virtualization management needs to dynamically provision, monitor and manage end-to-end network resources and services between virtual machines in a cloud environment.

Management of the Network Architecture

- A way to express workloads, network resources and operation policies in a virtualization-aware but hypervisor independent manner is the first step.
- To achieve this goal, common standards, open interfaces, common data model (management information model) are key.
- The number of standards bodies working:
  - Distributed Management Task Force (DMTF)
  - Object Management Group (OMG),
  - Open Grid Forum (OGF)

  Further: http://cloud-standards.org

Concept of Autonomic Computing

- Inspired by the autonomic nervous system, autonomic computing aims at designing and building self-managing systems and has emerged as a promising approach for addressing the challenges due to software complexity.
- An autonomic system is able to make decisions to respond to changes in operating condition at runtime using high-level policies that are typically provided by an expert.
  - *Self configuration*: Autonomic systems will configure themselves automatically.
  - *Self optimization*: Autonomic systems will continually seek ways to improve their operation.
  - *Self healing*: Autonomic computing systems will detect, diagnose, and repair.
  - *Self protection*: Autonomic systems will be self-protecting from malicious attacks.

Open Source Software in DCs

- Open-source cloud is any cloud service or solution that is built using open-source software and technologies. This includes any public, private or hybrid cloud model providing SaaS, IaaS, PaaS or XaaS built and operated entirely on open-source technologies.
- Open-source cloud computing platforms such as:
  - Eucalyptus- Elastic utility computing architecture linking your programs to useful system
  - OpenNebula- platform manages a data center's virtual infrastructure to build private, public and hybrid implementations of infrastructure as a service.
  - Nimbus - Nimbus is a toolkit that, once installed on a cluster, provides an infrastructure as a service cloud to its client via Amazon EC2 web service APIs.
  - OpenStack- is a free and open-source software platform for cloud computing, mostly deployed as infrastructure-as-a-service.