Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

Nishit Narang
WILPD-CSIS
(nishit.narang@pilani.bits-pilani.ac.in)

innovate achieve lead

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 11: Cloud Security

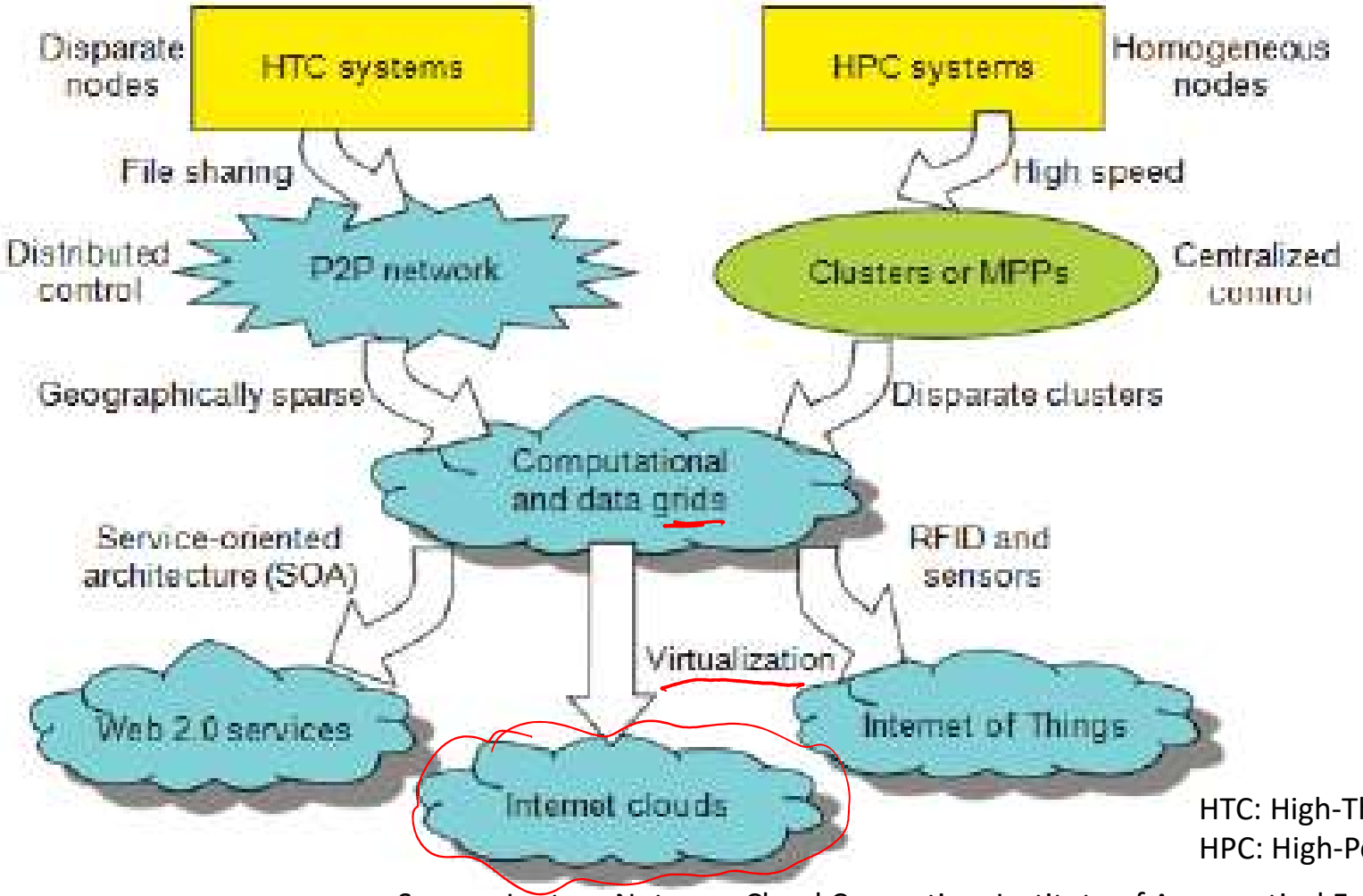
An Overview to Cloud Computing

Source Disclaimer: Content for some of the slides is from the course Textbook(s). Refer Course Handout for list of Textbooks.

Definition

- What is Cloud Computing?
  - NIST Special Publication 800-145 ("The NIST Definition of Cloud Computing") offers the following definition of the term "Cloud Computing":
    - *Cloud computing is a model for enabling **ubiquitous**, convenient, **on-demand** network access to a **shared pool** of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with **minimal management effort** or service provider interaction.*
  - The NIST publication describes the cloud model as something that is composed of five essential characteristics, three service models, and four deployment models

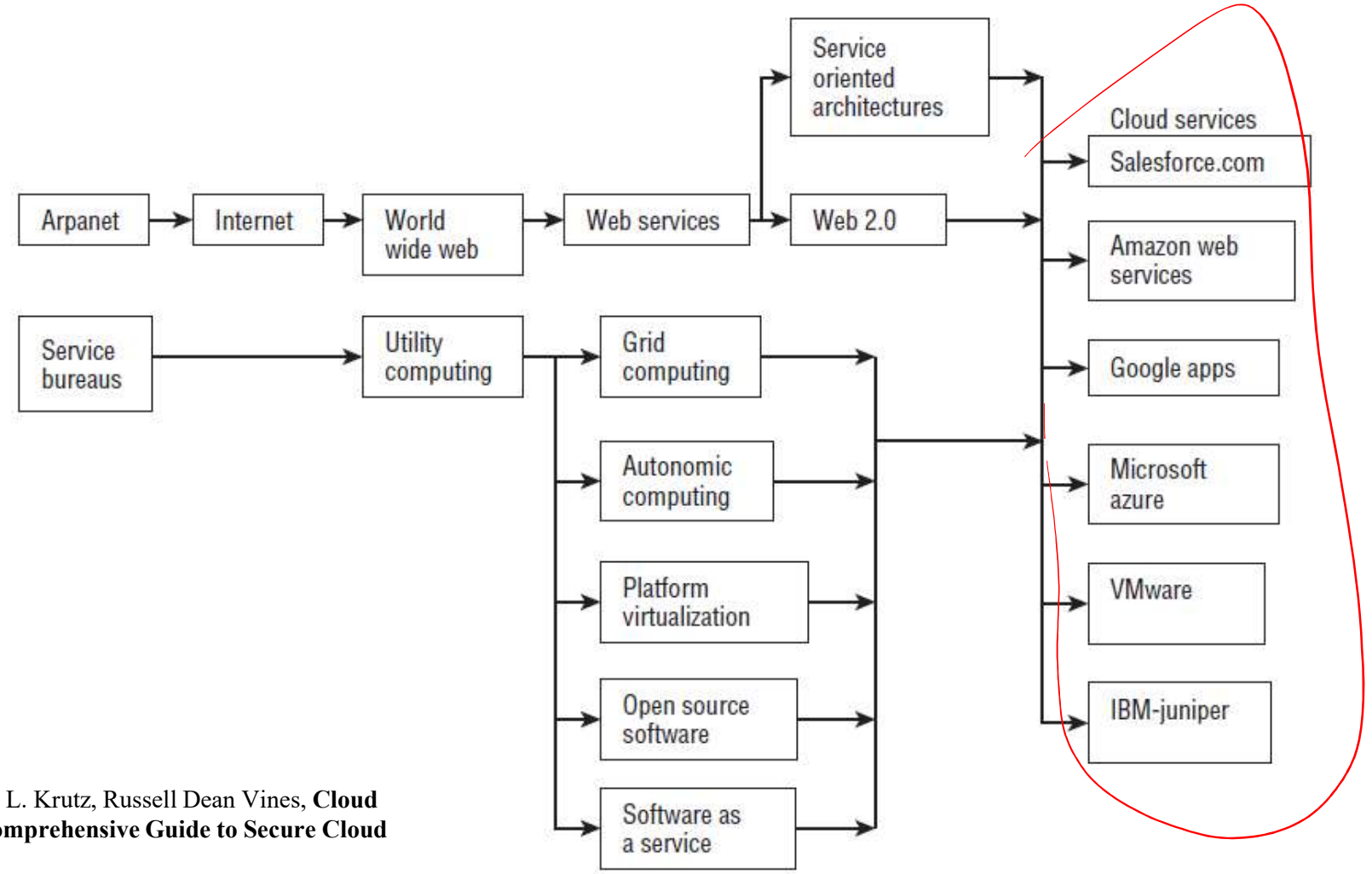
Evolution of Cloud Computing



Abbv:
HTC: High-Throughput Computing
HPC: High-Performance Computing

Source: Lecture Notes on Cloud Computing, Institute of Aeronautical Engineering, Hyderabad

Another Evolution View



Source: Ronald L. Krutz, Russell Dean Vines, **Cloud Security: A Comprehensive Guide to Secure Cloud Computing**

NIST: 5 Essential Characteristics

Source: NIST Special Publication 800-145

On-demand self-service.

- A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access.

- Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling.

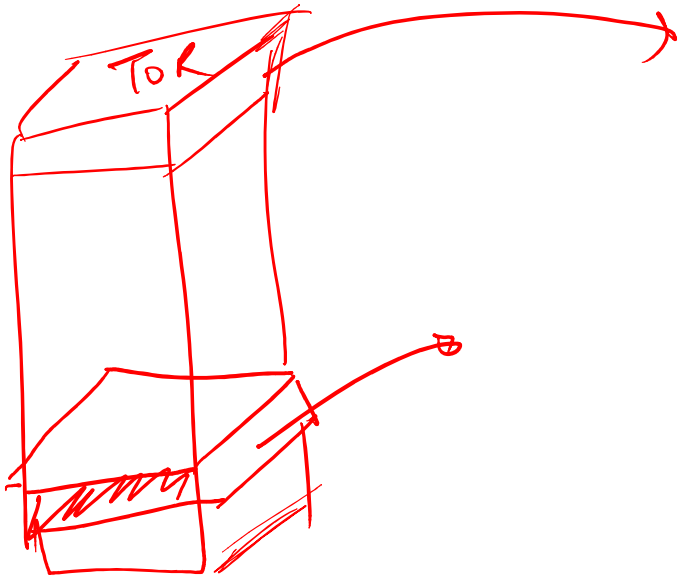
- The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter).
- Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity.

- Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.
- To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service.

- Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).
- Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.



DCN

Data Center– Design Goals

- Data center is a pool of resources (compute, storage, network) interconnected using a communication network (Data Center Network or DCN)
- Is a critical piece in the migration towards cloud computing and support of IoT applications

Concurrency
- Connected Devices
- High Ingress traffic

Scale
- Application Architecture designed for Scale out
- Infrastructure AutoScaling

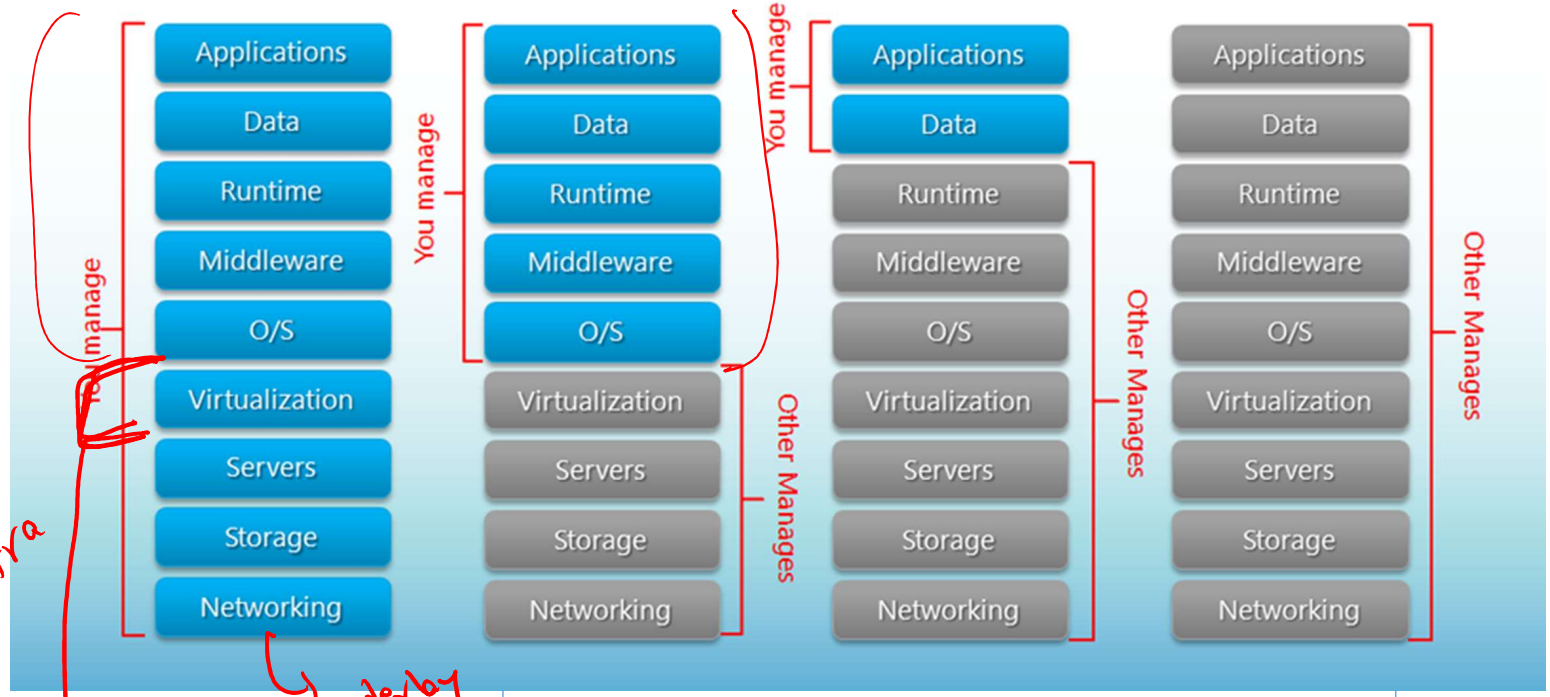
Availability
- Geo redundant infrastructure

Monitoring
- Infrastructure and Application Monitoring and Metering
- Managed Support Services

API Management
- Service Metering
- Security, Access Control and Governance

Integration
- Connectivity with transaction systems

Data Center: Service Models!



3 Cloud Service Models as per NIST Special Publication 800-145

NIST: 4 Deployment Models

Source: NIST Special Publication 800-145

Private cloud.

- The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).
- It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud.

- The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
- It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud.

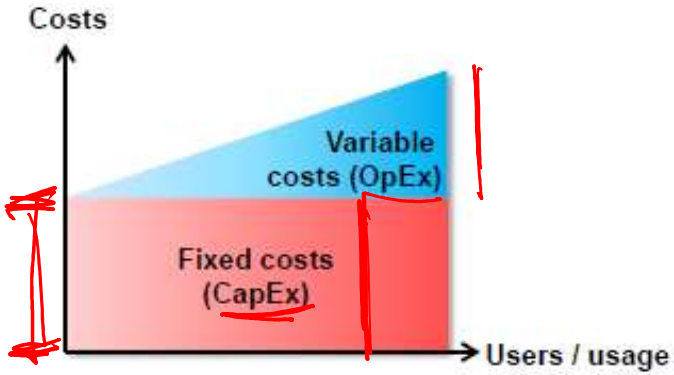
- The cloud infrastructure is provisioned for open use by the general public.
- It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them.
- It exists on the premises of the cloud provider.

Hybrid cloud.

- The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

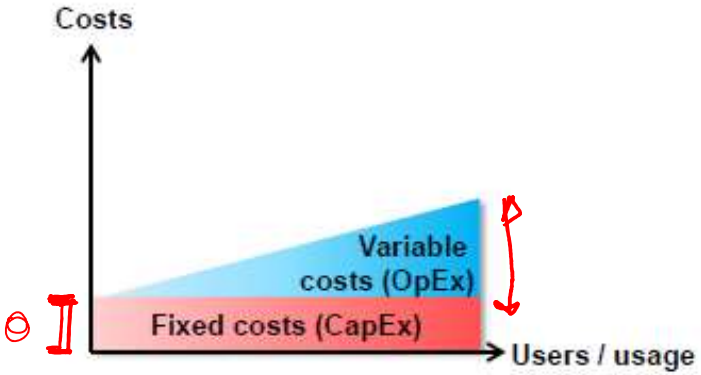
Rationale for Cloud Computing

Traditional IT:



Data centers, servers etc. require a large up-front investment (CapEx).
The infrastructure must be dimensioned to accommodate a certain peak load.
Variable costs incur on top of CapEx (run-time licenses for users etc.).

Cloud computing:



Fixed costs are transferred to the cloud provider and thus largely reduced for the customer (customer infrastructure reduced to network, workstations).
Variable costs vary according to usage demand.
The variable costs are reduced since the cloud provider exploits economy of scale.

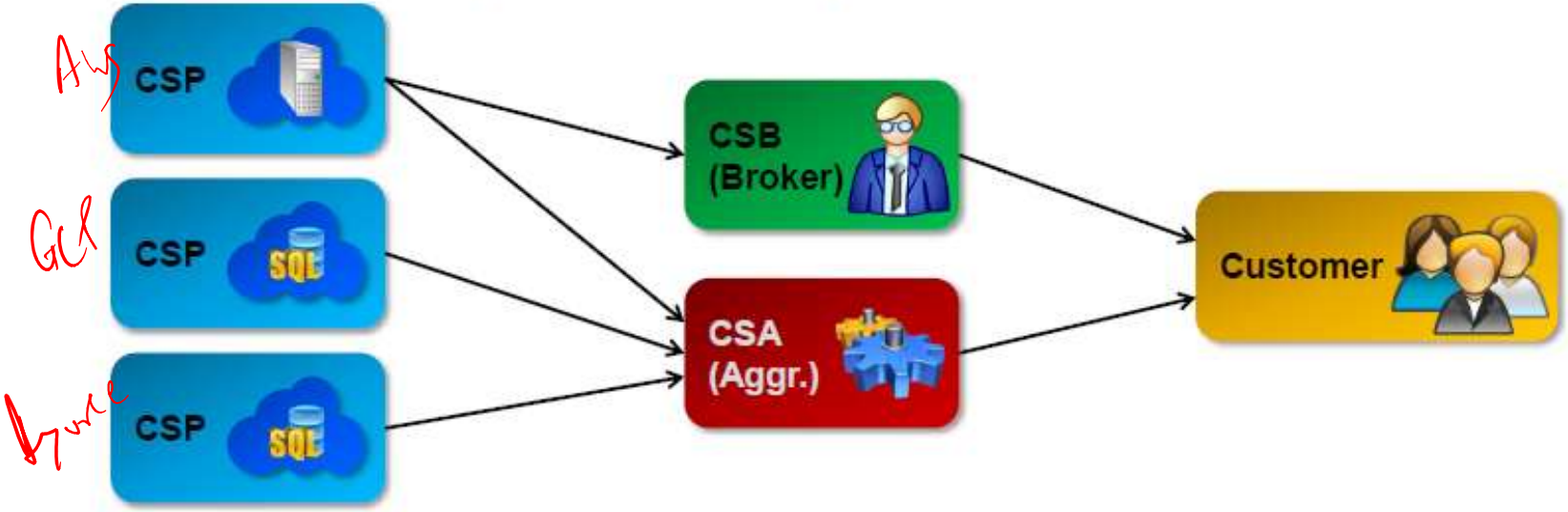
Source: Peter R. Egli (indigoo.com)

Landscape for Cloud Computing

Cloud Service Providers (CSP):
CSPs offer IaaS, PaaS and SaaS services as private, hybrid or public clouds.

Cloud Service Brokers (CSB):
CSBs resell and sometimes integrate CSP cloud services. CSBs focus on consultancy services, (help customers choose the right cloud solution, provide best practices for cloud deployment).

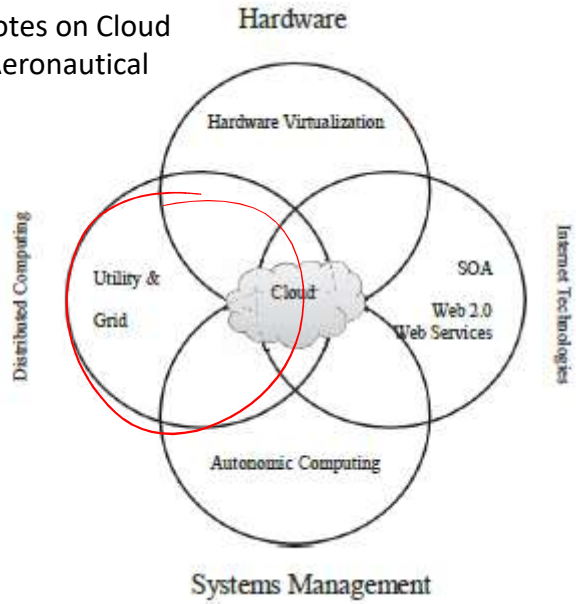
Cloud Service Aggregators (CSA):
CSAs integrate cloud services into value-added services, e.g. bundling storage services from different CSPs into a high-availability offering.



Source: Peter R. Egli (indigoo.com)

Enabling Technologies

Image Source: Lecture Notes on Cloud Computing, Institute of Aeronautical Engineering, Hyderabad



Uses 2 key technologies….

- SDN
  - Software Defined Networking
- NFV
  - Network Function Virtualization

……Alongside many other supporting technologies:

- Broadband Network Access
  - Diminishing the distinction between LAN and WAN bandwidth
- Distributed Computing
  - Including Middleware supporting interoperability for cloud-based distributed applications
- Grid Technology
  - Large number of connected physical servers for demand-based computing

Software Defined Networking (SDN): Background

- Three Plane Architecture of Network Elements

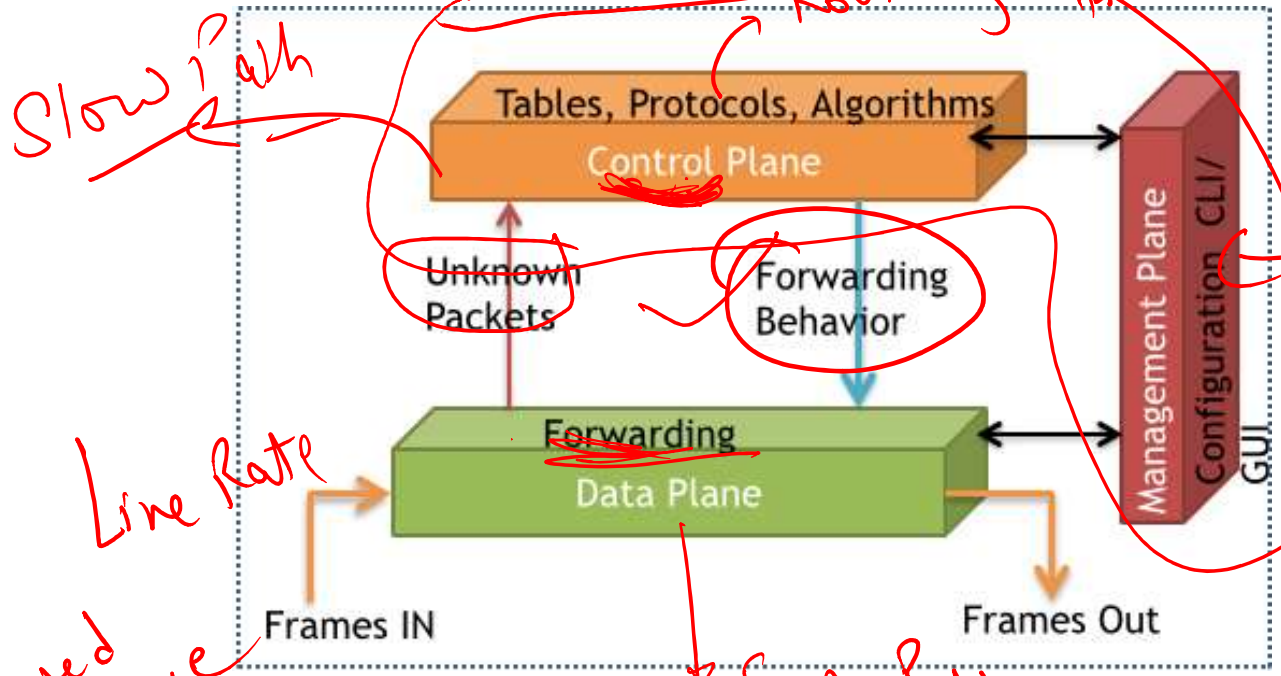
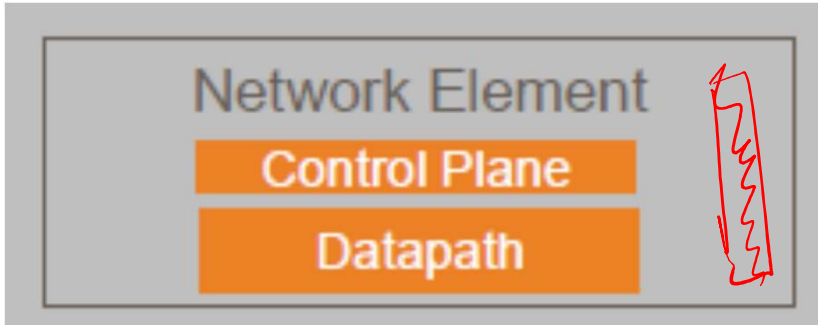


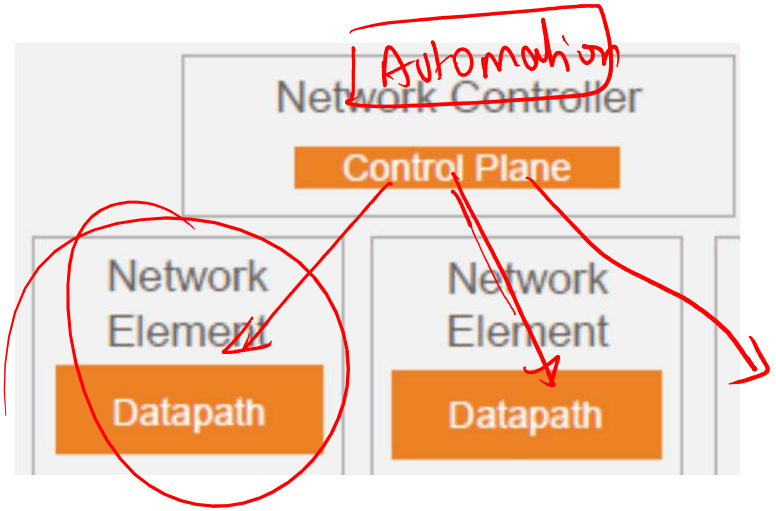
Image Source: https://thenewstack.io/defining-software-defined-networking-part-1/

Software Defined Networking (SDN): Main Concepts

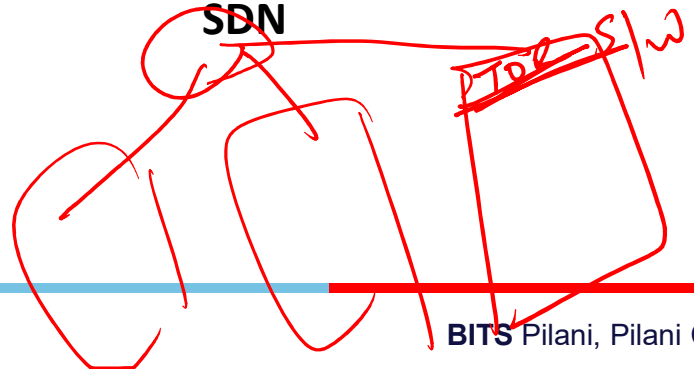
- Separation of Control Plane from Data Plane



Legacy



SDN



Software Defined Networking (SDN): Key Benefits

- Software-driven control / Programmability
- Simplified Network Equipment available as COTS
- Standardized management of Network Equipment → interoperability
- Cost Reduction, especially for large infrastructure setups as in Data Centers
  - Example: 1K switches required for a networking configuration
    - Without SDN:
      - Cost of Switch = $5K
      - Total Cost = $5M
    - With SDN:
      - Cost of SDN Controller (manages 100 switches) = $80K
      - Cost of COTS switch = $1K
      - Total Cost = ($80K * 10) + ($1K * 1000) = $1.8M

SDN Architecture / Layers

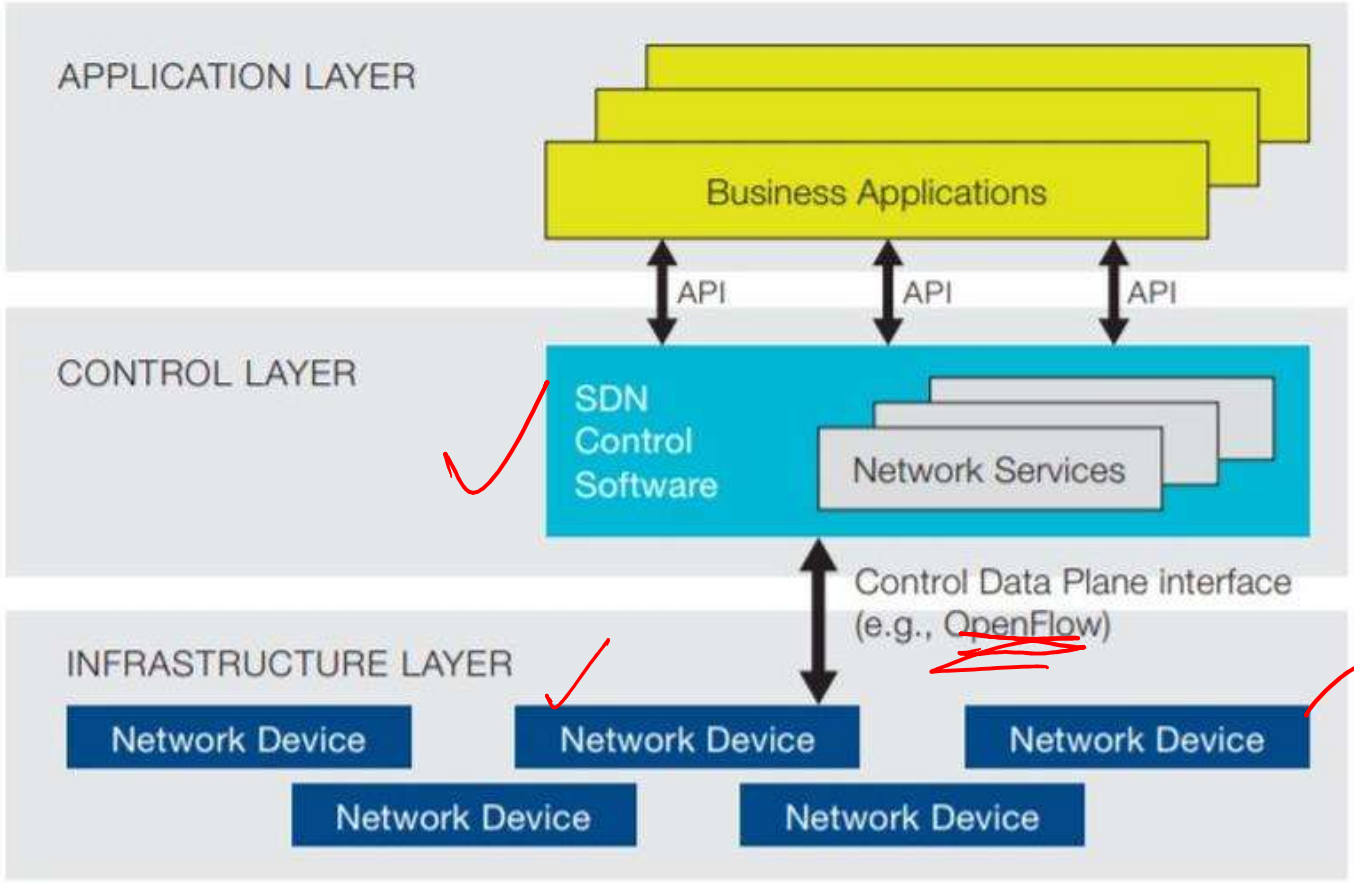
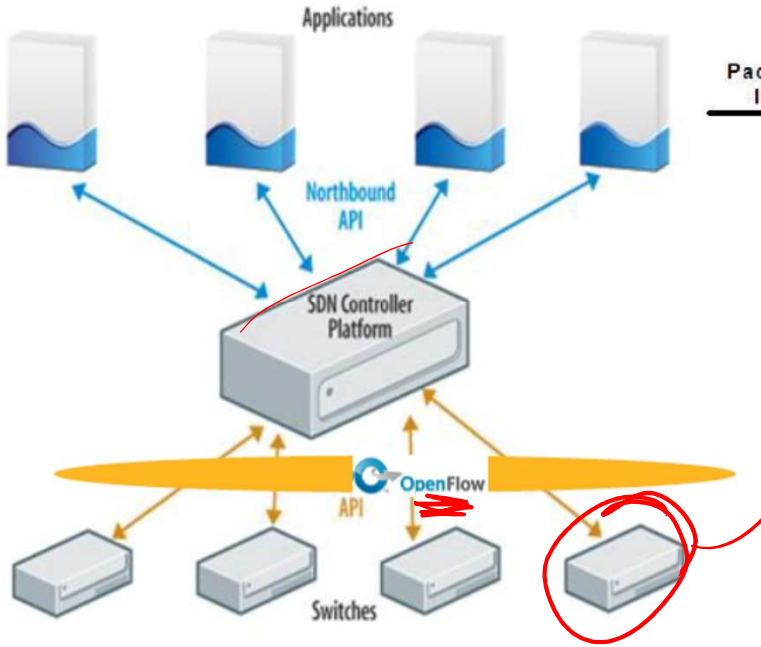
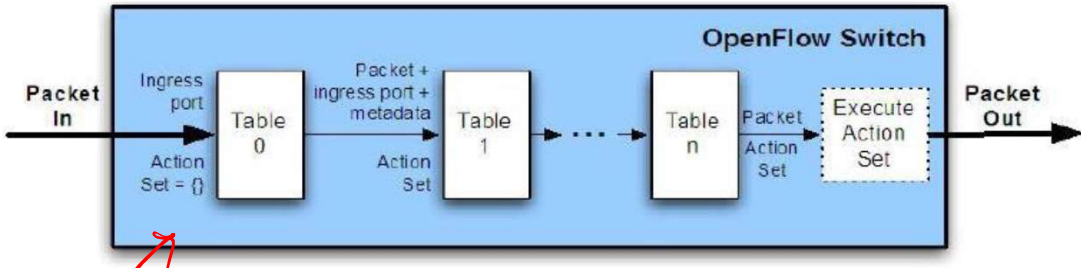


Image Source: Open Networking Foundation

OpenFlow Protocol





- Multiple Tables with Rules and Associated Actions
- Rules can be defined based on:
  - Switch Port
  - VLAN ID
  - MAC Src / Dst
  - Eth Type
  - IP Src/Dst
  - IP Tos
  - ….
- Actions like Forward Packet to Port, Drop Packet, Add/Remove/Modify a Tag, Modify a destination address, change TTL, …

Open Flow: Provisioning Approaches for Flows

innovate achieve lead

Flow Provisioning

- Reactive Provisioning
  - React to an incoming packet that results in a miss
  - Data Plane Driven Approach
- Proactive Provisioning
  - Pre-configure all flows that could hit the switch
  - Configuration Driven Approach

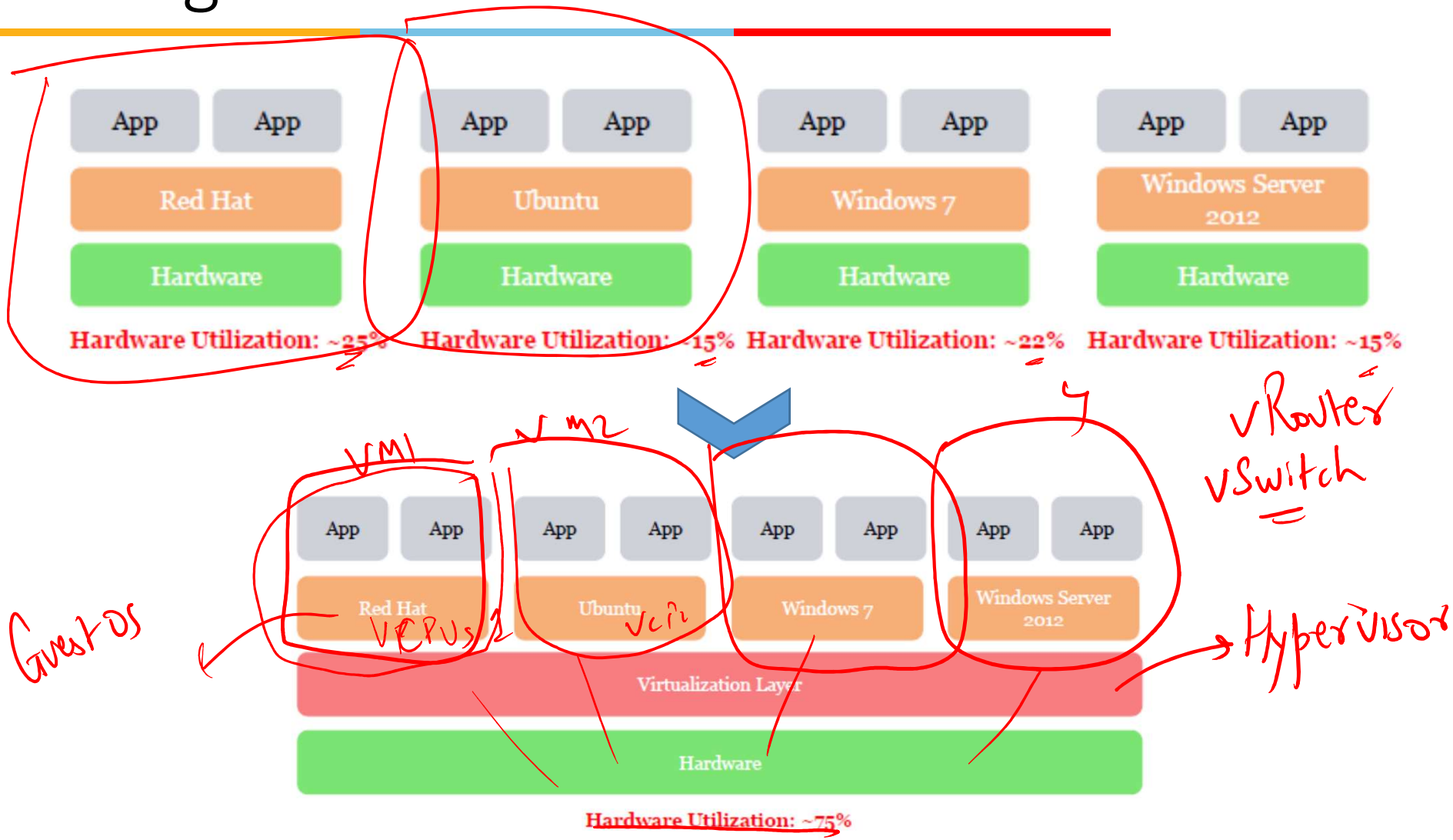
Flow Removal

- Idle Timeout
- Explicit removal from Controller

SDN Application Examples

- Route Optimization
  - Steer traffic based on network conditions, e.g. congestion
- Load Balancing
  - Steer traffic onto alternate routes
- Dynamic Bandwidth Allocation
  - Allocation based on QoS
- Network Monitoring
  - Debugging, Lawful Interception etc

Network Function Virtualization: Background



NFV: Enabling Solution Component

- Hypervisor
  - A technology that allows sharing of hardware resources of a single machine by multiple guest Operating Systems (OS)
  - Results in multiple Virtual Machines (VMs) on same physical machine

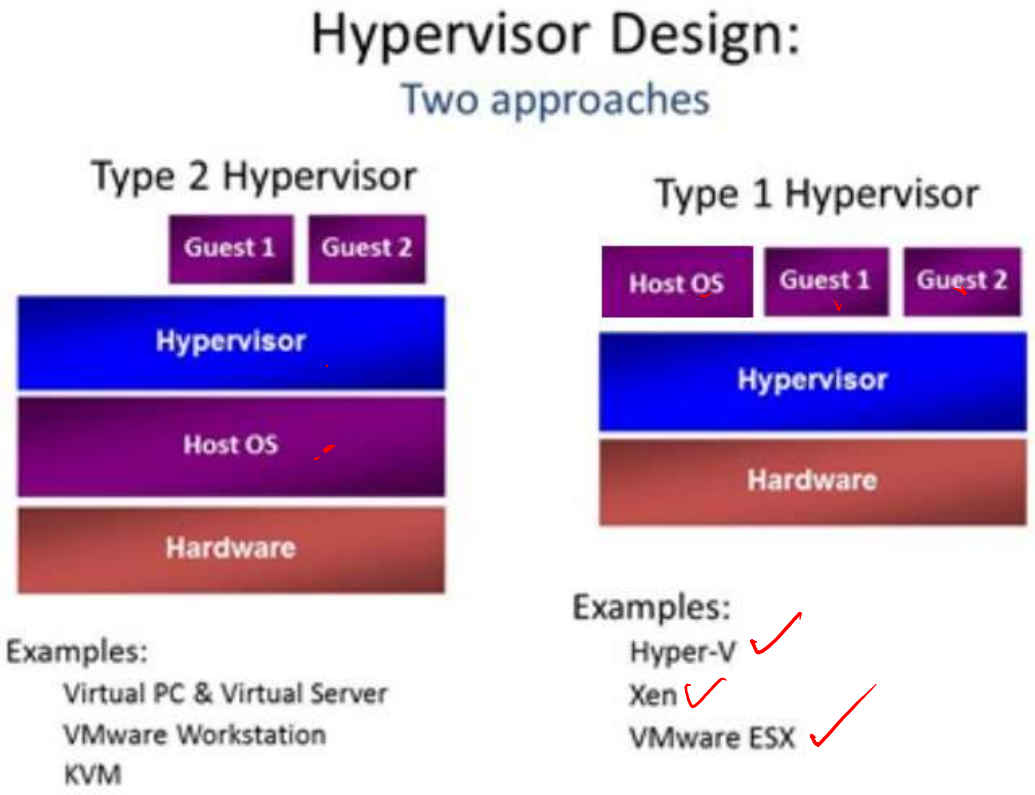


Image Source: https://www.tenforums.com/virtualization/119469-hypervisor-type-1-type-2-a.html

NFV Architecture

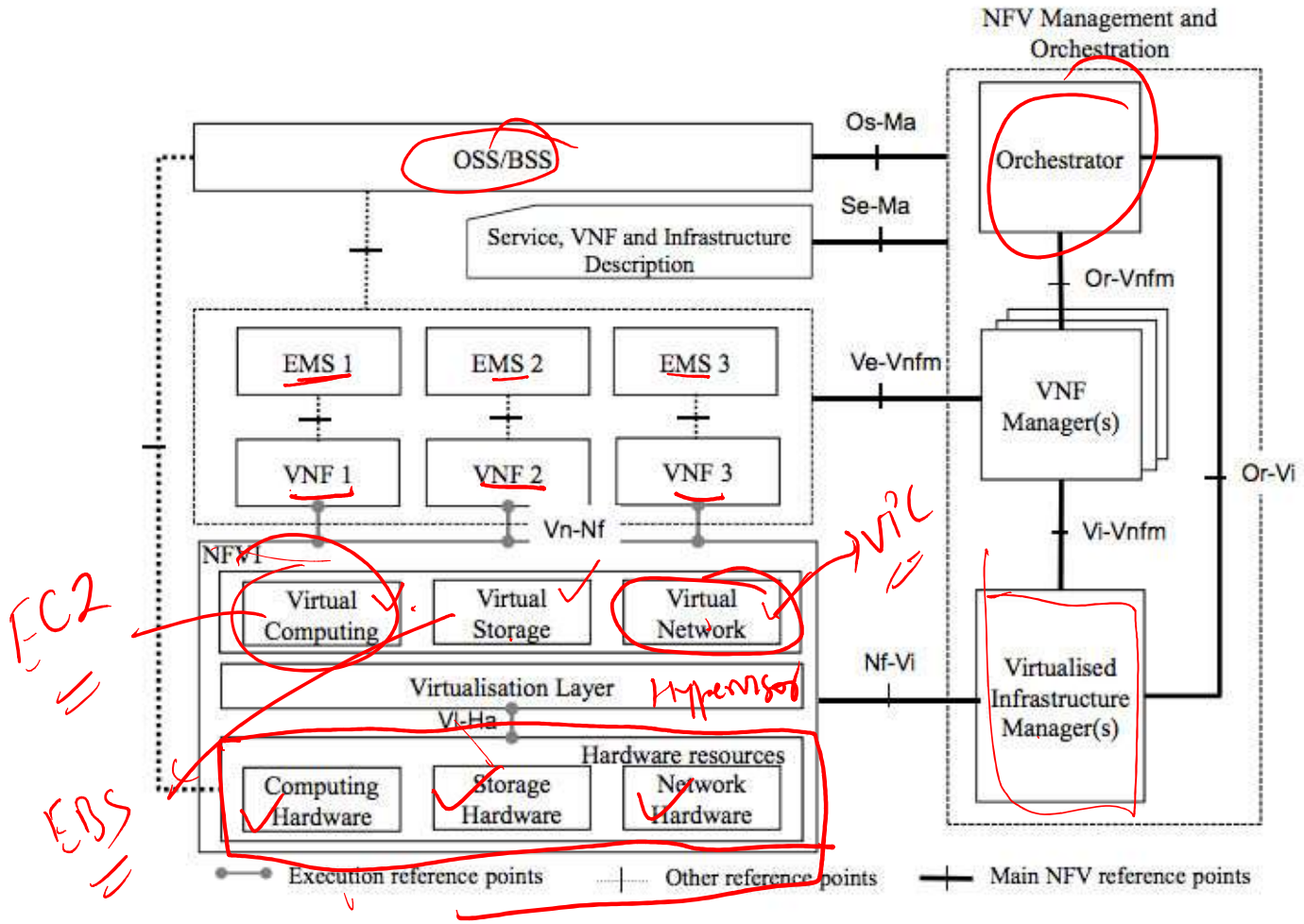


Image Source: SDxCentral

NFV Service Chaining

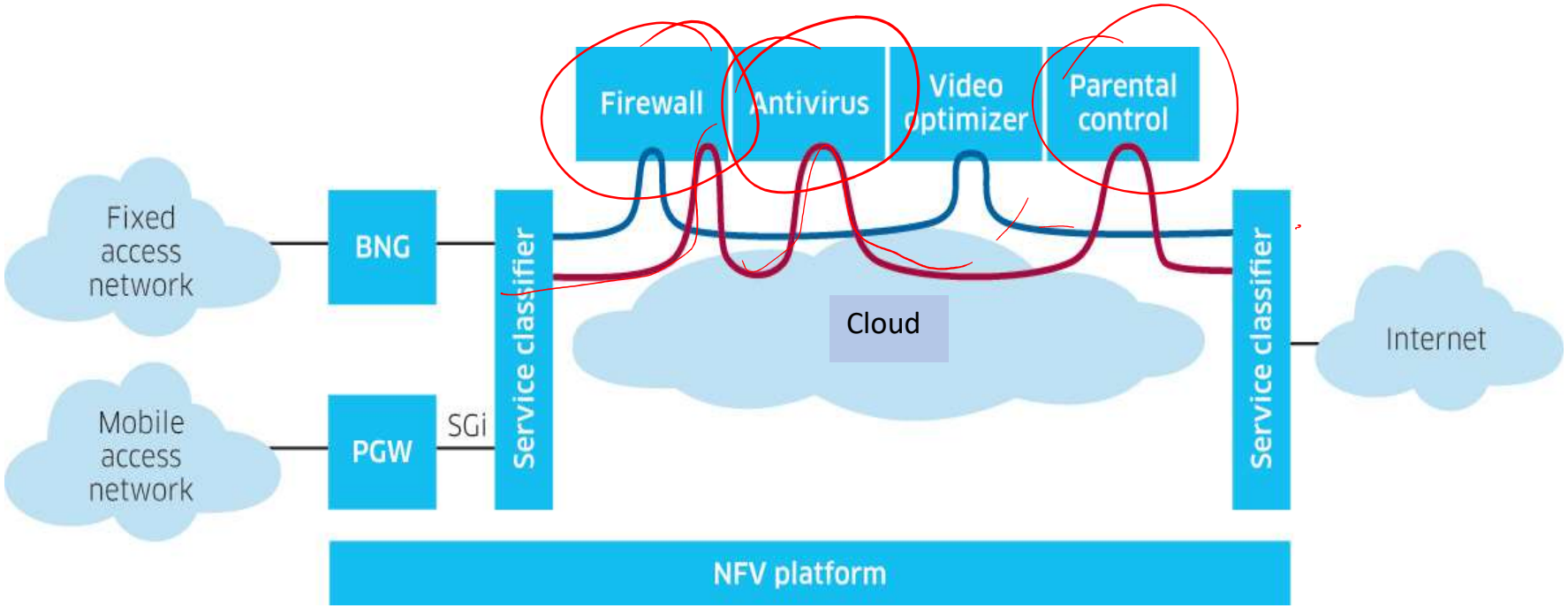
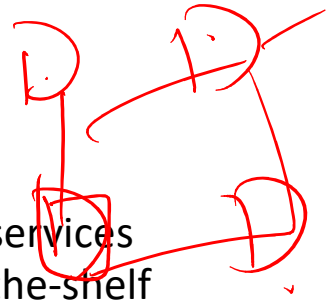


Image Source: SDxCentral

SDN/NFV in the Data Center



- NFV Data Center
  - Used by service providers to host communications and networking services
  - Services can be loaded as cloud-based software on commercial off-the-shelf (COTS) server hardware
  - Applications are hosted in data center so they could be accessed via cloud

- SDN can work in tandem with NFV
  - Traffic Steering in an NFV Data Center

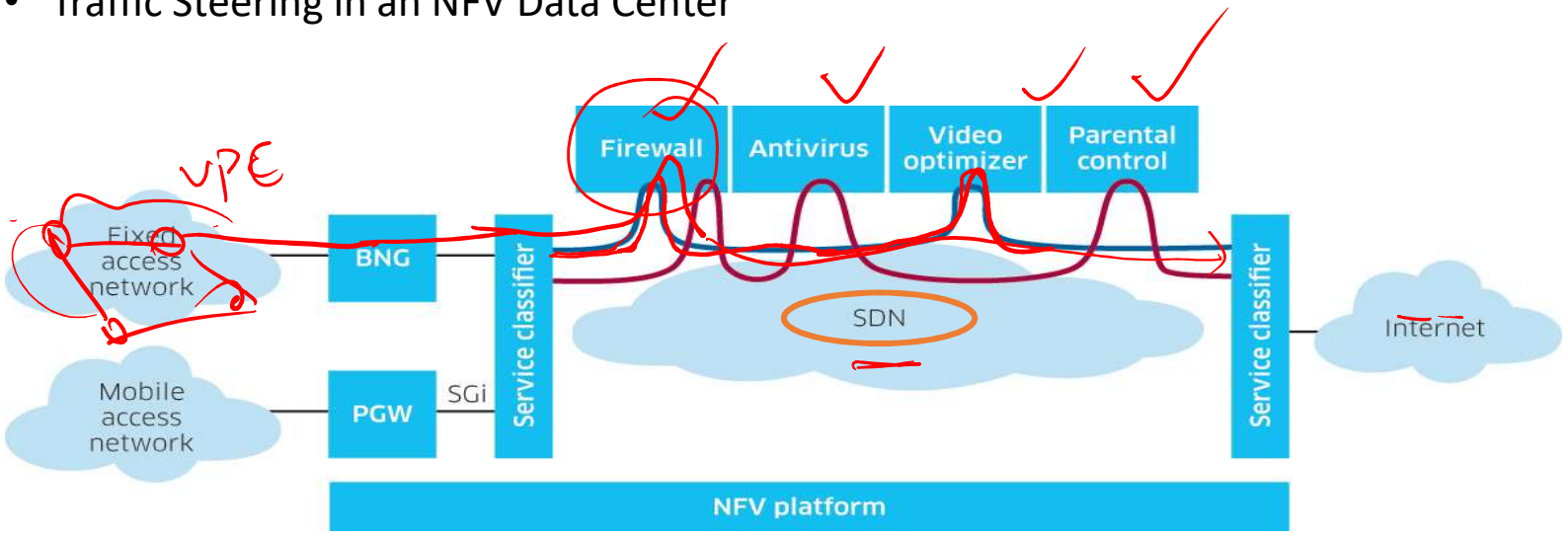
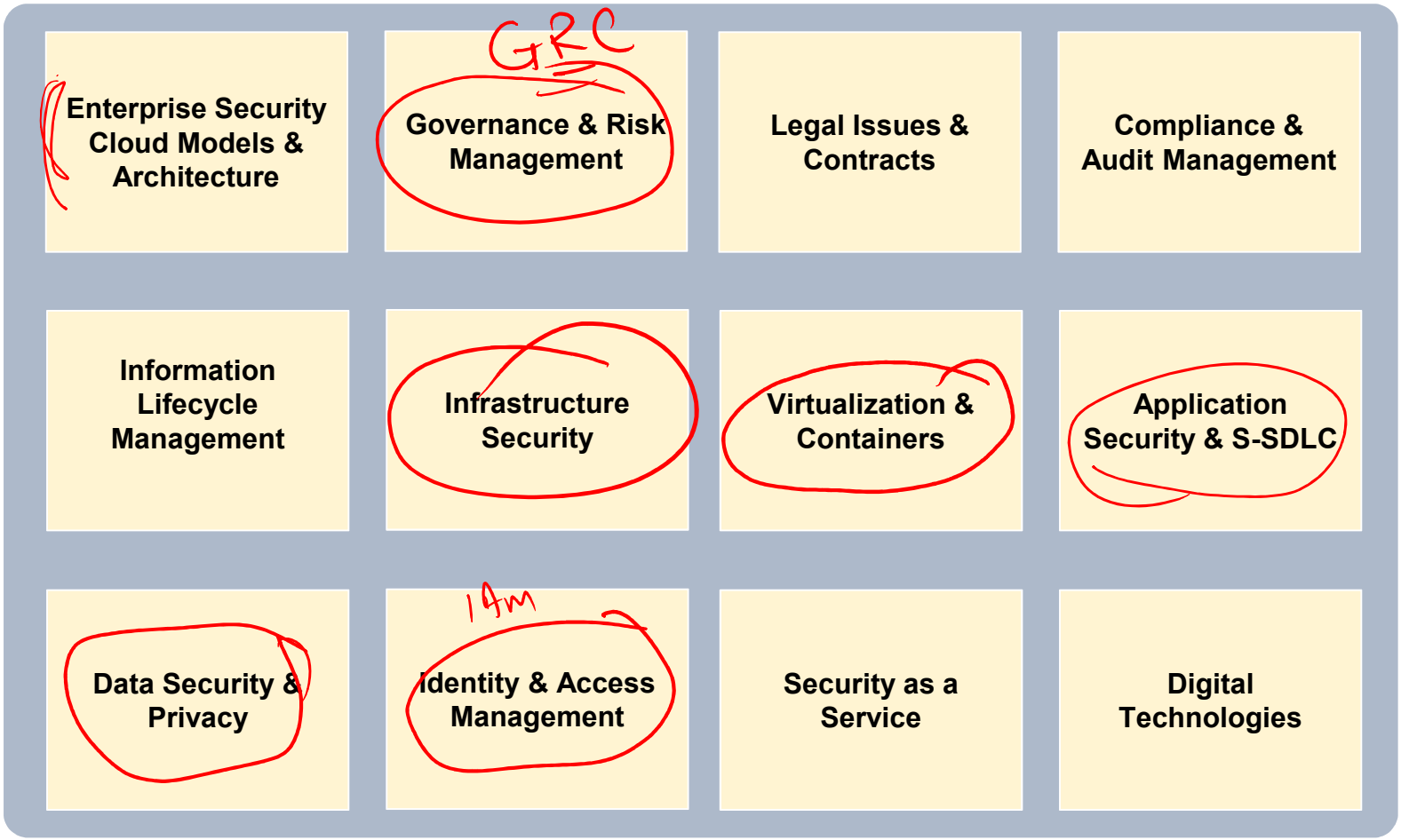
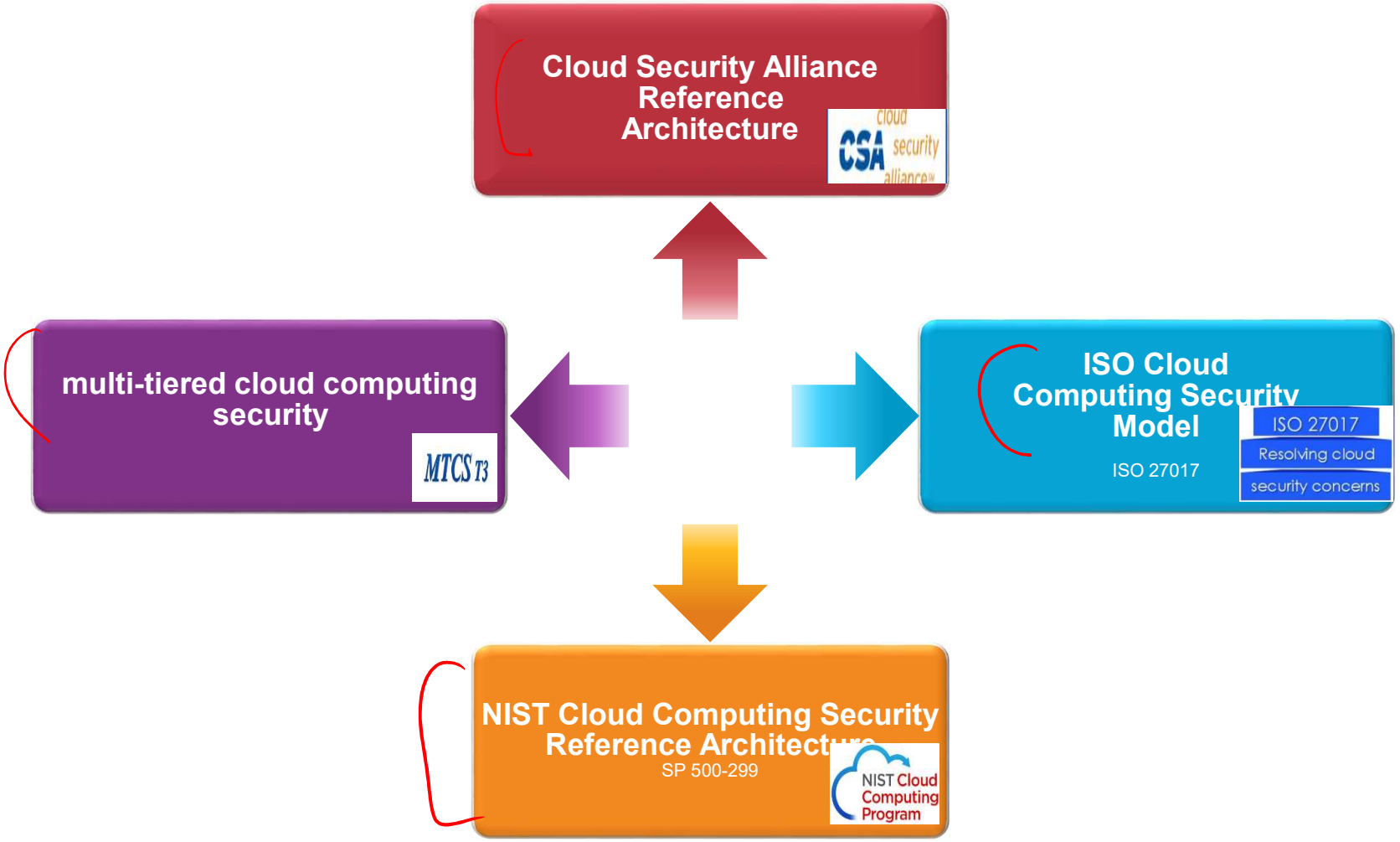


Image Source: SDxCentral

Security Topics for Cloud Computing



Cloud Security Reference Architectures & Standards