TechLift

KICKSTART YOUR CAREER

TRACK NAME

Cloud Solution Architecture

P@SHA

Pakistan Software Houses Association for IT & ITES

PAKISTAN PSEB SOFTWARE EXPORT BOARD

S. No.	Topics
1	Pre-Requisites Of Cloud
2	Basics of Security and Privacy
3	CapEX and OpEx in Cloud Computing
4	Compute
5	Storage
6	Networking
7	**VPN- Virtual Private Network**
8	**Data Center**
9	DR site - Disaster Recovery
10	Mapping of on-prem Infrastructure setup to Cloud
11	Cloud TCO

VPN
Virtual Private Network

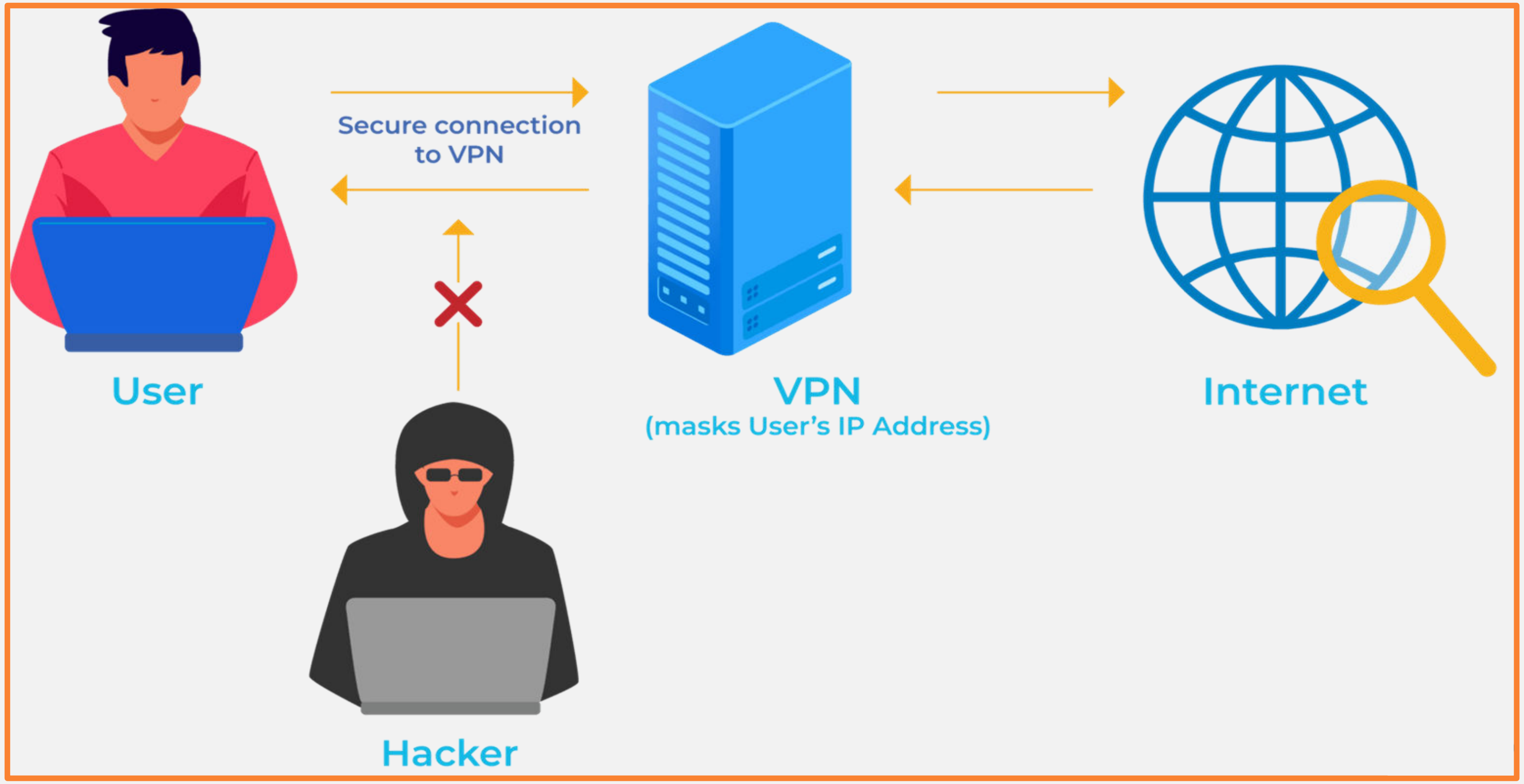
VPN

VPN

- VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks.
- VPNs encrypt your internet traffic and disguise your online identity.
- The encryption takes place in real time.

VPN - Working of VPN

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data.



VPN - Benefits of VPN

A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can’t decipher this data.

- → Secure encryption
- → Disguising your whereabouts
- → Access to regional content
- → Secure data transfer

VPN - Benefits of VPN

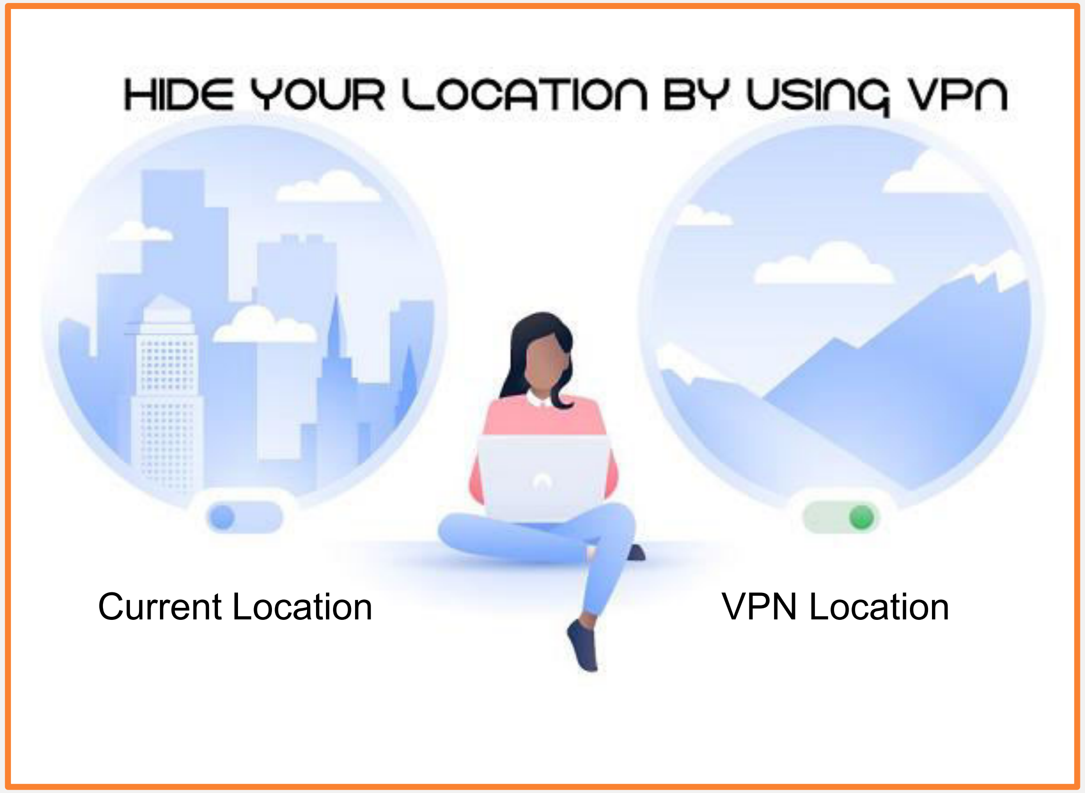
Secure encryption

- To read the data, you need an encryption key . Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack .
- With the help of a VPN, your online activities are hidden even on public networks.

VPN - Benefits of VPN

Disguising your whereabouts

- VPN devices/servers essentially act as your proxies on the internet.
- The demographic location data comes from a server in another country, your actual location cannot be determined.



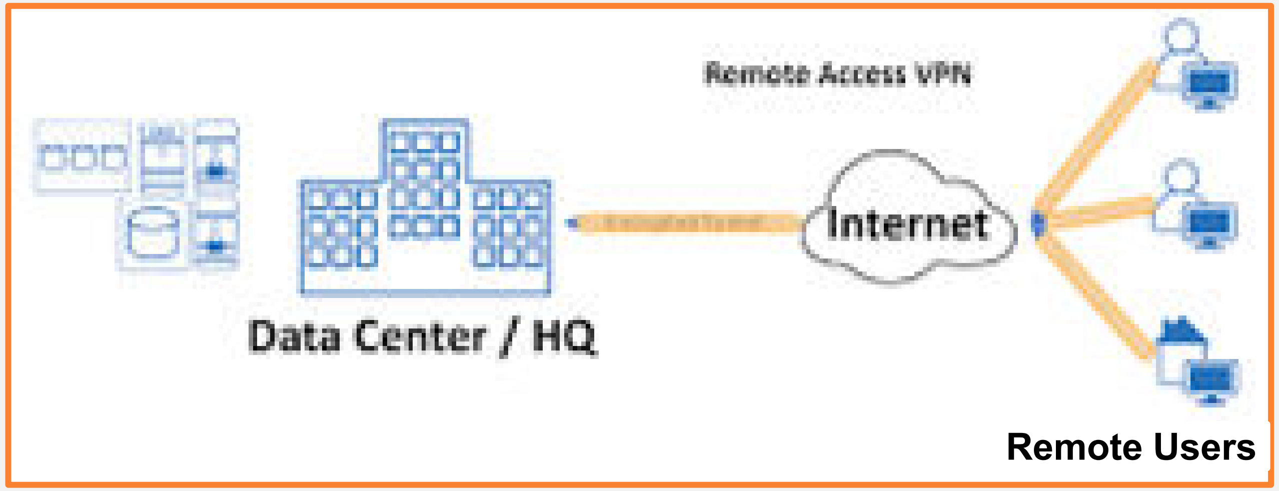
VPN - Benefits of VPN

Access to regional content
With VPN location spoofing , you can switch to a server to another country and effectively “change” your location.

VPN - Benefits of VPN

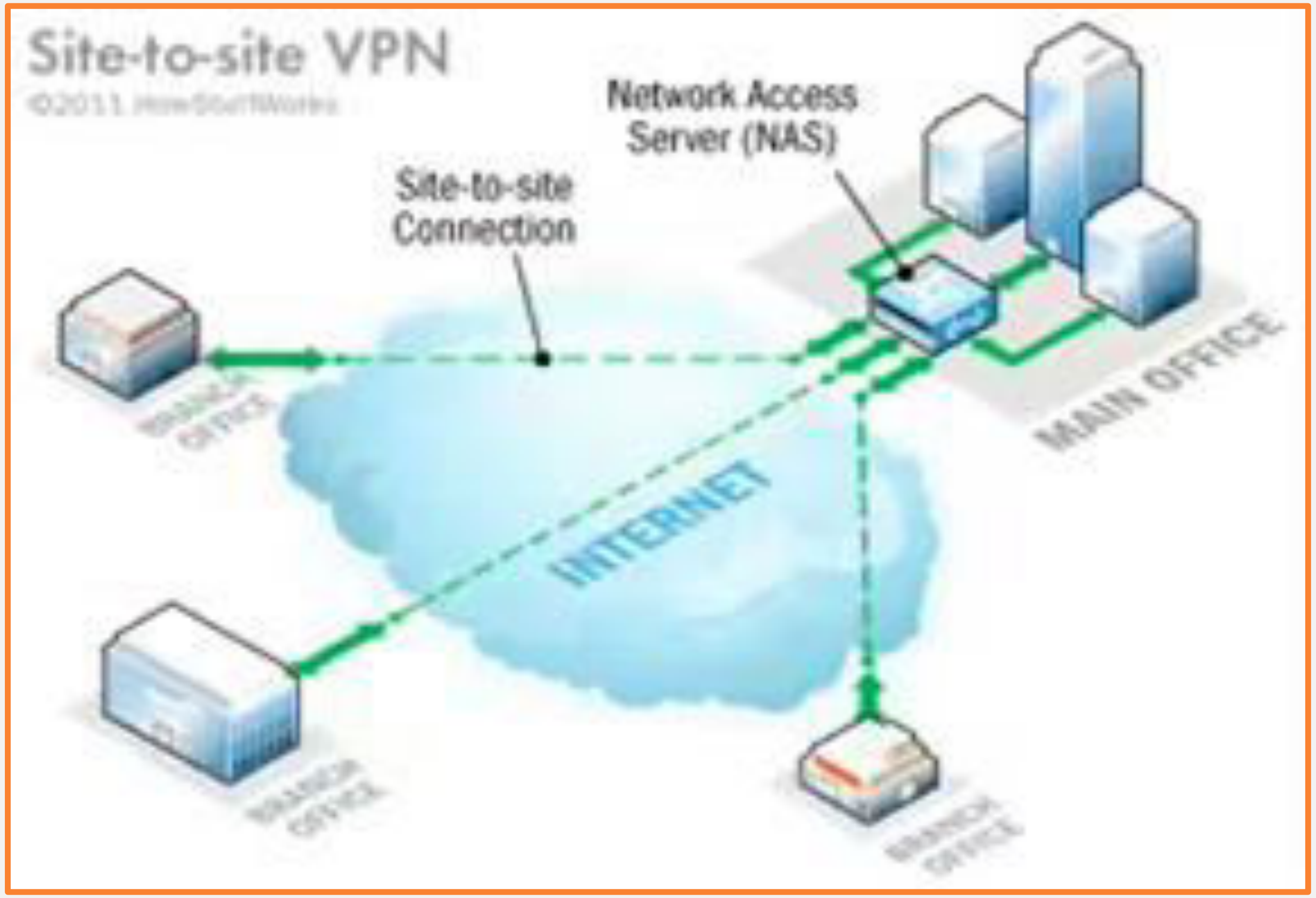
Remote Workers

- If you work remotely, you may need to access important files on your company’s network.
- For security reasons, this kind of information requires a secure connection.
- To gain access to the network, a VPN connection is often required.
- VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.



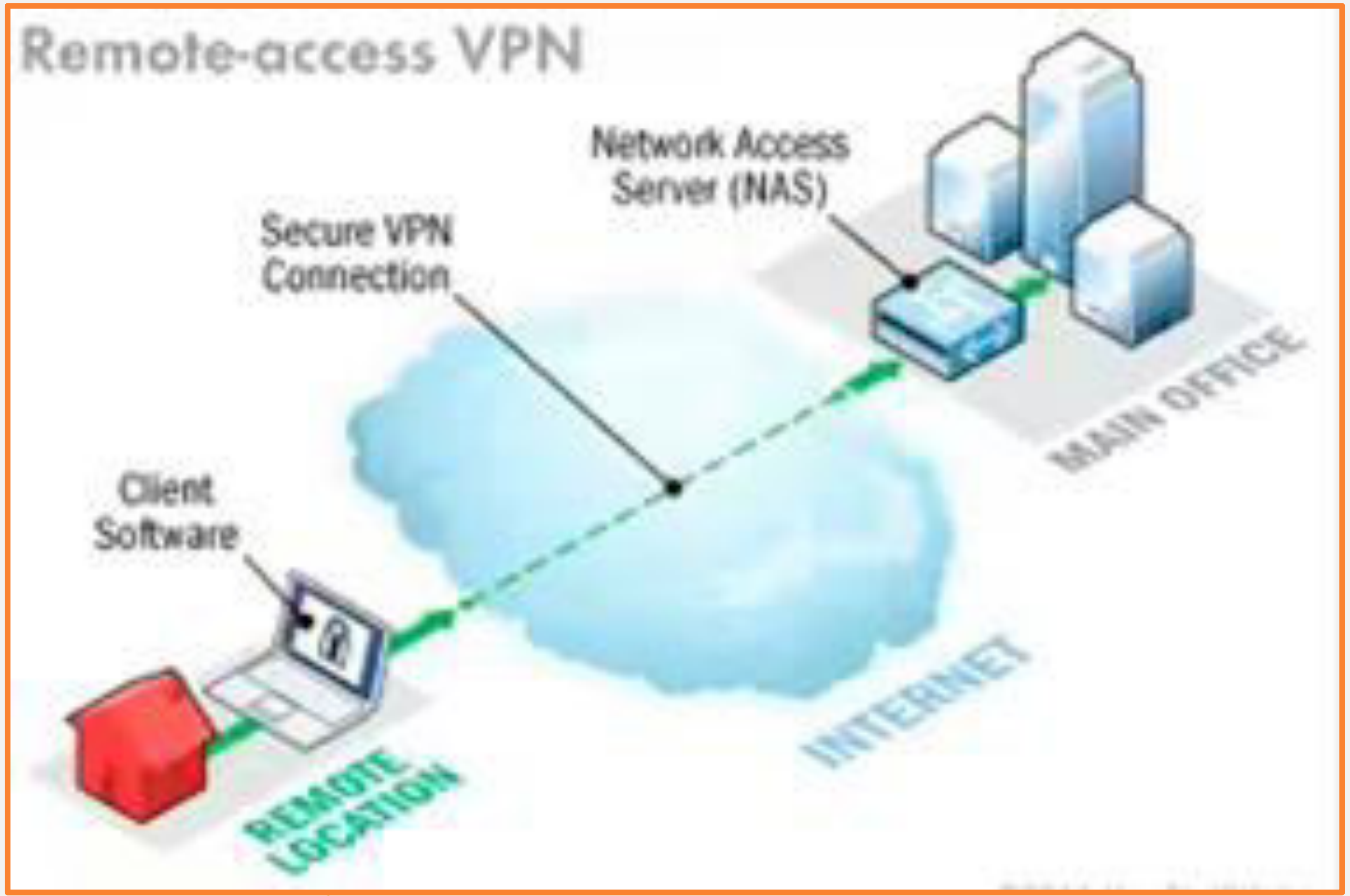
VPN - Types of VPN

A site-to site VPN connection lets branch offices use the internet as a conduit for accessing the main office’s intranet.



VPN - Types of VPN

A remote access VPN connection allows an individual user to connect to a private network from a remote location using a laptop or desktop computer and mobile devices connected to the internet.



VPN - Types of remote-access VPN

In a remote- access VPN, tunneling typically relies on Point-to-point Protocol (PPP) which is part of the native protocols used by the internet. More accurately, though, remote-access VPNs use one of three protocols based on PPP:

- **Point-to-Point Protocol (PPP)** — A protocol that encapsulates network layer protocol information over point-to-point links.
- **L2F (Layer 2 Forwarding)** — Developed by Cisco; uses any authentication scheme supported by PPP
- **PPTP (Point-to-point Tunneling Protocol)** — Supports 40-bit and 128-bit encryption and any authentication scheme supported by PPP
- **L2TP (Layer 2 Tunneling Protocol)** — Combines features of PPTP and L2F and fully supports IPSec; also applicable in site-to-site VPNs

Q&A Session for VPN

1. Which two scenarios are examples of remote access VPNs?
   a. A toy manufacturer has a permanent VPN connection to one of its parts suppliers.
   b. All users at a large branch office can access company resources through a single VPN connection.
   c. A mobile sales agent is connecting to the company network via the Internet connection at a hotel.
   d. An employee who is working from home uses VPN client software on a laptop in order to connect to the company network.

1. Which statement describes a feature of site-to-site VPNs?
   a. The VPN connection is not statically defined.
   b. VPN client software is installed on each host.
   c. Internal hosts send normal, unencapsulated packets.
   d. Individual hosts can enable and disable the VPN connection.

Data Center

Data Center

A data center is a physical facility that organizations use to house their critical applications and data.

A data center's design is based on a network of computing and storage resources that enable the delivery of shared applications and data.

The key components of a data center design include routers, switches, firewalls, storage systems, servers, and Load Balancers.

Traditional Data Center

A traditional data center is a facility housing IT equipment, such as servers and routers. Data center hardware components and technical elements include:

- Servers
- Memory
- Processing power
- Storage
- Networking
- Power and Cooling Infrastructure

For much of the history of IT, traditional data centers tended to be on-premises, often in conjunction with a main corporate office.

Benefits of Traditional Data Center

A physical, on-premises data center has various advantages:

- If you’re starting from scratch, you can build it to suit your own needs. When upgrades are required, you’re in the driver’s seat.
- You can restrict access to the facility to individuals from within your own organization, as well as trusted providers should you choose.
- Traditional data centers located on-premises can deliver low-latency access to applications.

Drawbacks of Traditional Data Center

- Construction and ongoing data center infrastructure management are typically more expensive for traditional data centers.
- Traditional data centers are less energy efficient and require more cooling.
- A traditional data center relies on static IP addresses.
- Some organizations suffer from hardware vendor lock-in.

Modern Data Center (Virtualization)

- Infrastructure has shifted from traditional on-premises physical servers to virtual networks that support applications and workloads across pools of physical infrastructure and into a multi-cloud environment.

- In this era, data exists and is connected across multiple data centers, the edge, and public and private clouds.

- The data center must be able to communicate across multiple sites, both on-premises and in the cloud.

- The public cloud is also a collection of data centers.

- When applications are hosted in the cloud, they are using data center resources from the cloud provider.

Importance Of Data Centers

In the world of enterprise IT, data centers are designed to support business applications and activities that include:

- Email and file sharing
- Productivity applications
- Customer relationship management (CRM)
- Enterprise resource planning (ERP) and databases
- Big data, artificial intelligence, and machine learning
- Virtual desktops, communications and collaboration services

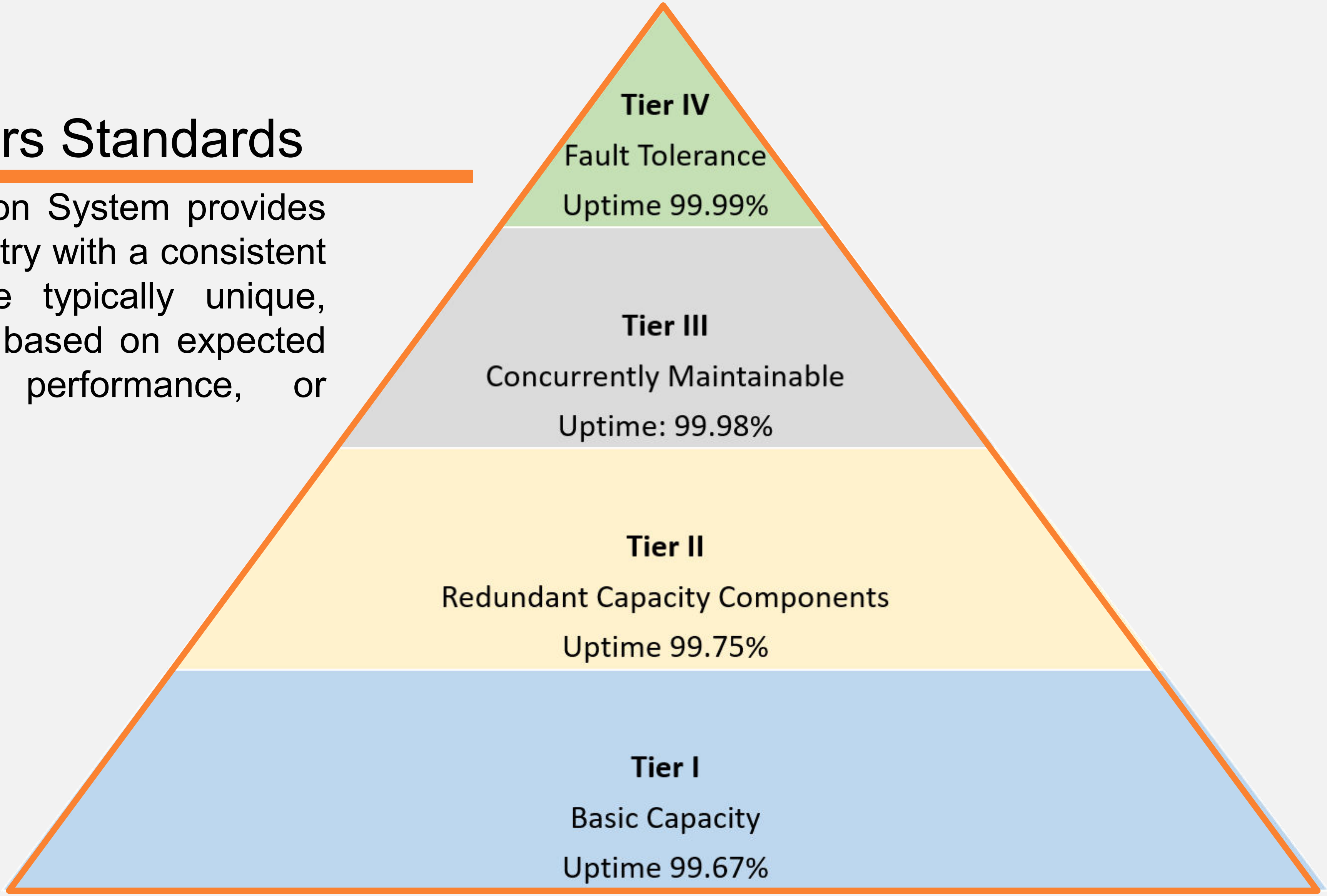
Core Components Of Data Centers

Data center design includes routers, switches, firewalls, storage systems, servers, and application delivery controllers. Because these components store and manage business-critical data and applications, data center security is critical in data center design. Together, they provide:

- → **Network infrastructure.** This connects servers (physical and virtualized), data center services, storage, and external connectivity to end-user locations.
- → **Storage infrastructure.** Data is the fuel of the modern data center. Storage systems are used to hold this valuable commodity.
- → **Computing resources.** Applications are the engines of a data center. These servers provide the processing, memory, local storage, and network connectivity that drive applications.

Data center tiers Standards

The Tier Classification System provides the data center industry with a consistent method to compare typically unique, customized facilities based on expected site infrastructure performance, or uptime.



Tier IV

Fault Tolerance

Uptime 99.99%

Tier III

Concurrently Maintainable

Uptime: 99.98%

Tier II

Redundant Capacity Components

Uptime 99.75%

Tier I

Basic Capacity

Uptime 99.67%

Types Of Data Centers

Many types of data centers and service models are available. Their classification depends on whether they are owned by one or many organizations, how they fit (if they fit) into the topology of other data centers, what technologies they use for computing and storage, and even their energy efficiency.

There are four main types of data centers

- Enterprise data centers
- Managed services data centers
- Colocation data centers
- Cloud data centers

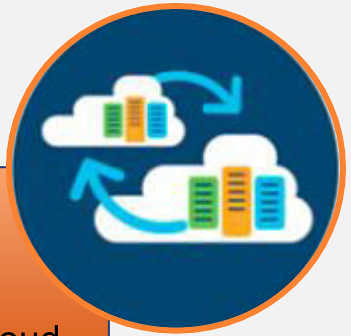
Types Of Data Centers

Enterprise data centers
These are built, owned, and operated by companies and are optimized for their end users. Most often they are housed on the corporate campus.

Managed services data centers
These data centers are managed by a third party (or a managed services provider) on behalf of a company. The company leases the equipment and infrastructure instead of buying it.

Types Of Data Centers

Colocation data centers
In colocation ("colo") data centers, a company rents space within a data center owned by others and located off company premises. The colocation data center hosts the infrastructure: building, cooling, bandwidth, security, etc., while the company provides and manages the components, including servers, storage, and firewalls.



Cloud data centers
In this off-premises form of data center, data and applications are hosted by a cloud services provider such as Amazon Web Services (AWS), Microsoft (Azure), or IBM Cloud or other public cloud provider.

Q&A Session (Data Centers)

1.More organizations are building data centers to include:

a. All on-premises hardware with no external connections
b. Only virtual or software-based resources
c. Resources being supported through as-a-service applications.
d. A mix of hardware, cloud applications and third-party managed services

2. If your workloads change dramatically and unpredictably, then a cost-effective option is:

a. Colocation
b. Cloud
c. Containers
d. GPU based servers

Disaster Recovery Site

- → One of the main components of a DR plan is the secondary site (also known as DR site), which will be used for data storage and rapid recovery in case disaster strikes.
- → A disaster recovery site is a location used by an organization for restoring its IT infrastructure and business-critical operations when a primary production center is affected by a natural or man-made disaster.
- → Disaster Recovery sites are often built in a remote location so as to ensure that the disaster which has affected the main site will not affect the secondary site as well.
- → Creating a DR site allows an organization to continue conducting operations and delivering services without disruption, until the primary location is restored.

review:

- **VPN- Virtual Private Network**
- **Data Center**