**By Maha Rana**

# IT602 Midterm Subjective Solved

## Short Questions

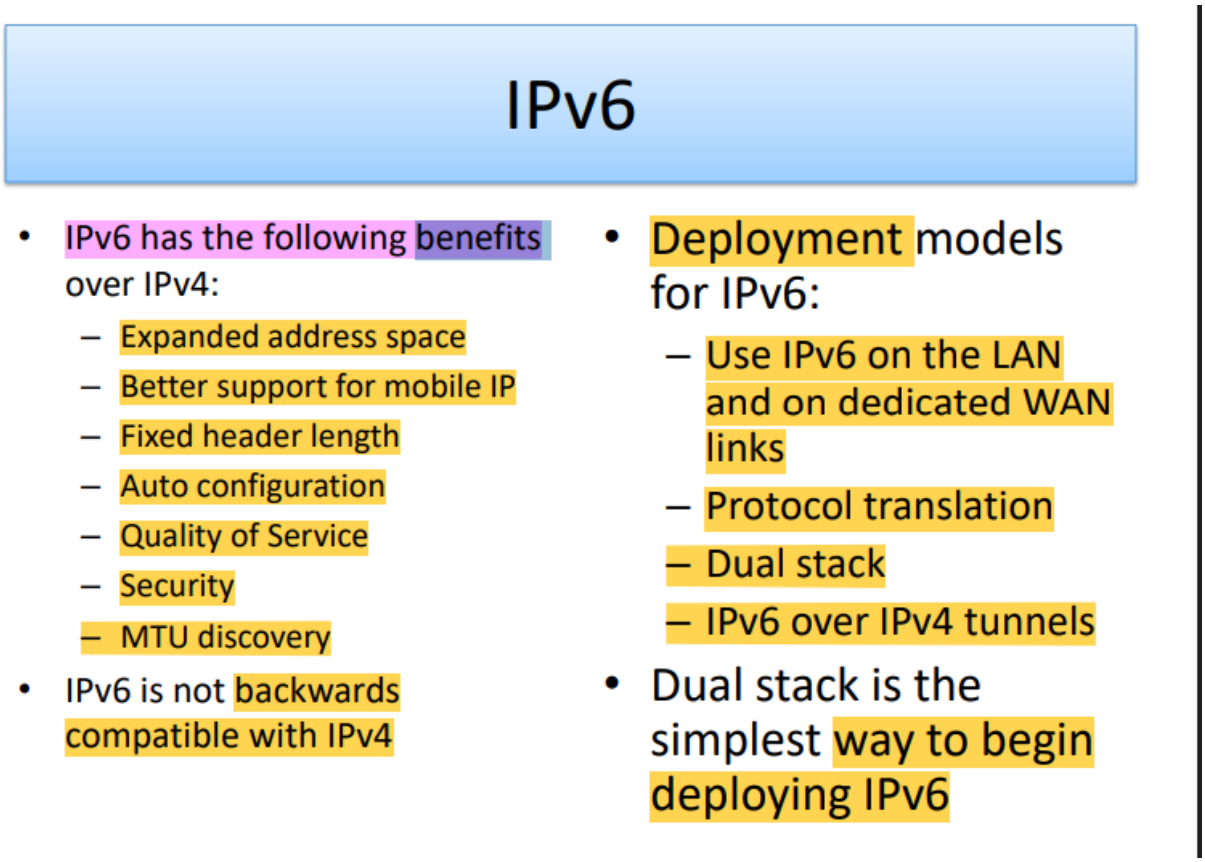
1. **Two types of fiber optic cable:**
    - **Single-Mode Fiber (SMF)**
    - **Multi-Mode Fiber (MMF)**
2. **Goals of Security (CIA Triad):**
    - **Confidentiality** – Prevent unauthorized access to data.
    - **Integrity** – Ensure data is accurate and unaltered.
    - **Availability** – Ensure data is accessible when needed.
3. **Three processes of performance management:**

> **Performance during Infrastructure Design**
>
> - Some ways to do this are:
>   - Benchmarking
>   - Using vendor experience
>   - Prototyping and User Profiling

## Long Questions

**By Maha Rana**

1. **Types of fallback solutions:**
   - **Hot Site** – Fully operational backup site with real-time data replication.
   - **Cold Site** – A backup site with infrastructure but no pre-installed data.
   - **Warm Site** – A middle-ground backup site with some pre-installed data but requiring updates before full use.
2. **Five benefits of IPv6 over IPv4:**




3. **Risk list five parameters:**
   - **Asset Name** – The component that needs protection.
   - **Vulnerability** – Weakness that can be exploited.
   - **Exploit** – A method to attack the vulnerability.
   - **Probability** – Likelihood of an exploit occurring.

- **Impact** – The severity of damage if an attack happens.

A risk list can be used to quantify risks

**Risk is calculated based on:**

**Asset name** - component that needs to be protected

**Vulnerability** - weakness, process or physical exposure that makes the asset susceptible to exploits

**Exploit** - a way to use one or more vulnerabilities to attack an asset

**Probability** - an estimation of the likelihood of the occurrence of an exploit

**Impact** - the severity of the damage when the vulnerability is exploited

## Short Questions & Key Concepts

1. **Difference between IPv6 and IPv4:**
   - **IPv4:** 32-bit addressing, limited addresses, uses NAT, no built-in security.
   - **IPv6:** 128-bit addressing, larger address space, supports auto-configuration, has built-in IPSec security.
2. **Cipher:**
   - A **cipher** is an algorithm used for **encryption** and **decryption** of data.
   - **Types of Ciphers:**
     - **Block Cipher:** Encrypts data in fixed-size blocks (e.g., AES, DES).
     - **Stream Cipher:** Encrypts data bit by bit (e.g., RC4).

3. **NFRs (Non-Functional Requirements) - Attributes & Behavior:**




Non functional attributes describe the qualitative behavior of the system rather than its specific functionality and these include

- Availability
- Security Most imp
- Performnace
- Recoverability
- Testtability

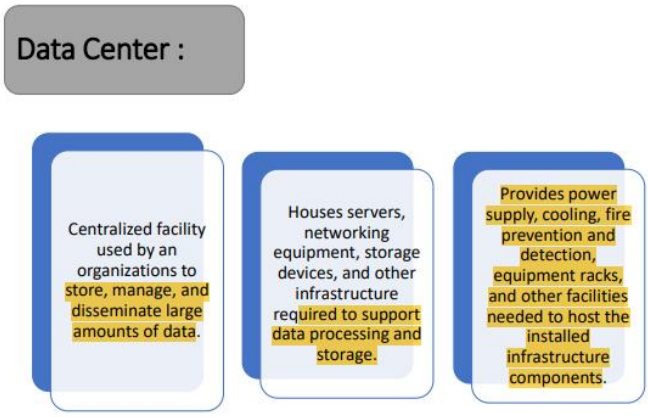
4. **Types of Architecture in IT Infrastructure:**



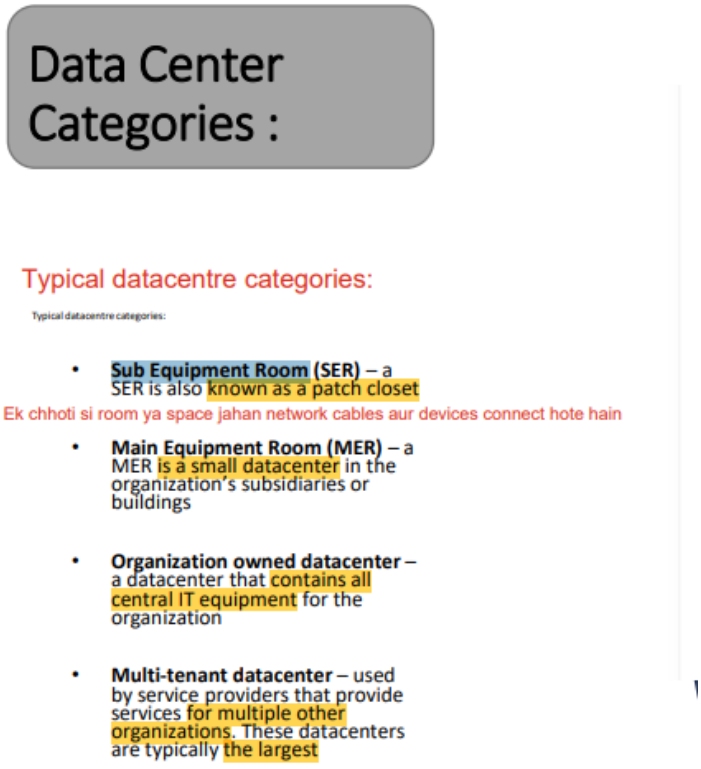

- ❖ Business architecture
- ❖ Enterprise architecture
- ❖ Data architecture,
- ❖ Application architecture and
- ❖ Infrastructure architecture

5. **Data Center:**

**By Maha Rana**




- **Types of Data Centers:**



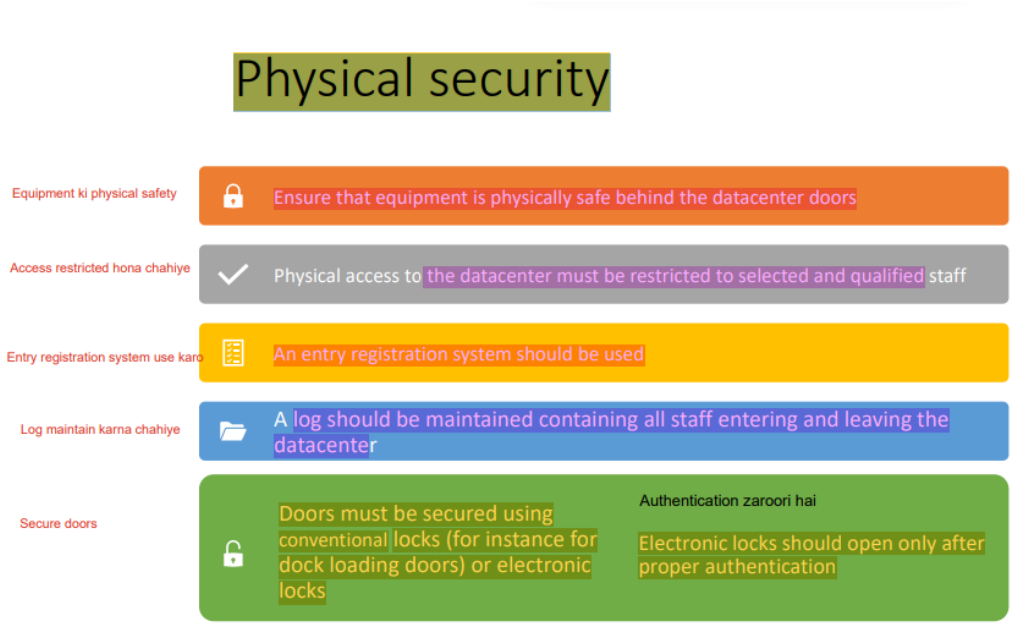

## MCQs Focus (Weeks 2-5 Topics)

**By Maha Rana**

- **Week 2:** Availability concepts, MTBF & MTTR, sources of downtime (human error, software bugs, hardware failure).
- **Week 3:** Performance concepts, benchmarking, bottlenecks, caching.
- **Week 4:** Security concepts, attack vectors (DDoS, phishing), risk management.
- **Week 5:** Data center infrastructure, power, cooling, fire prevention, security.

## Short Questions

### Q1: How is security implemented in a data center?




### Q2: How many forms of fallback are there, and why is it used?

There are **three types of fallback solutions** used for disaster recovery:

1. **Hot Site:** Fully operational backup site with real-time data replication.
2. **Warm Site:** Backup site with some pre-installed data but requires updates.

3. **Cold Site:** An infrastructure-ready site, but data needs to be restored manually.
   Fallback is **used to ensure business continuity** in case of system failure, cyberattacks, or natural disasters.

**Q3: Name any three types of disasters.**

1. **Natural Disasters:** Earthquakes, floods, hurricanes.
2. **Man-Made Disasters:** Cyberattacks, hazardous material spills, infrastructure failure.
3. **Technical Failures:** Hardware crashes, software bugs, power outages.

---

**Long Questions**

**Q4: Can we check performance during the design phase? If yes, how, and what methods are used?**

Yes, **performance can be checked during the design phase** using different methods:

1. **Benchmarking:**
   - Comparing system performance with standard performance metrics.
   - Uses tools like **MIPS, FLOPS, and CPU benchmarks**.
2. **User Profiling:**
   - Identifying expected system load based on user behavior.
3. **Prototyping (Proof of Concept - PoC):**
   - Developing a small version of the system to test performance risks.
4. **Vendor Experience:**

- Using vendor-recommended configurations and best practices.

**Q5: Benefits of IPv6 over IPv4?**

1. **Larger Address Space:**
   - IPv6 has **128-bit** addresses vs. IPv4's **32-bit**, allowing **more devices**.
2. **Auto-Configuration:**
   - Devices can generate their own IP addresses without a DHCP server.
3. **Improved Security:**
   - **IPSec encryption** is built-in for secure communications.
4. **Better Performance:**
   - No need for **NAT (Network Address Translation)**, reducing processing time.
5. **Enhanced Mobility Support:**
   - Allows seamless movement of devices between networks.

**Q6: What is Proof of Concept (PoC), and why is it used?**

- A **Proof of Concept (PoC)** is a small-scale **prototype** used to test the **feasibility** of a system.
- **Why is it used?**
  1. To **identify risks** before full implementation.
  2. To **test system performance** in a controlled environment.
  3. To **evaluate vendor solutions** before investment.
  4. To **demonstrate functionality** to stakeholders before final development.

**Short Questions**

**By Maha Rana**

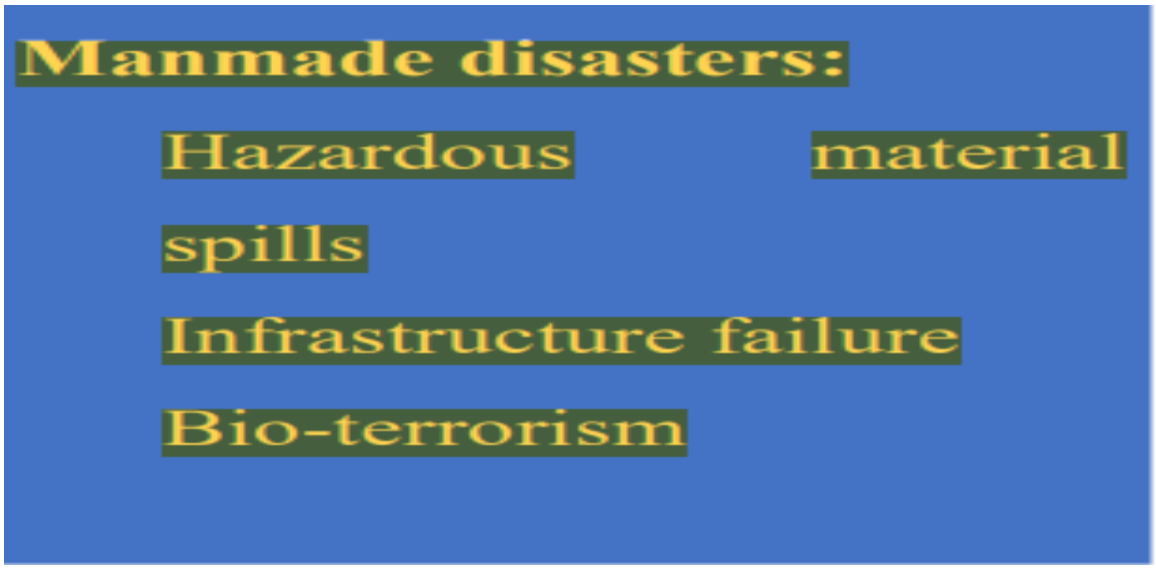
## Q1: Forms of fallback solutions

Fallback solutions are used for disaster recovery and **come in three forms**:

1. **Hot Site:**
    - Fully operational backup site with real-time data replication.
    - Can take over immediately in case of failure.
2. **Warm Site:**
    - Backup site with some pre-installed data but requires updates before use.
3. **Cold Site:**
    - A facility with infrastructure ready but **no pre-installed data or applications**.
    - Data and systems must be manually restored.

---

## Q2: Three man-made disasters




## Long Questions

**By Maha Rana**

## Q1: Benefits of IPv6 over IPv4

1. **Larger Address Space:**
    - IPv6 has **128-bit** addresses vs. IPv4's **32-bit**, allowing **more unique IP addresses**.
2. **Auto-Configuration:**
    - IPv6 supports **stateless address auto-configuration (SLAAC)**, eliminating the need for a DHCP server.
3. **Better Security:**
    - **IPSec encryption** is built-in, ensuring end-to-end data protection.
4. **Efficient Routing & Performance:**
    - No **NAT (Network Address Translation)** is needed, reducing processing time and network overhead.
5. **Better Mobility Support:**
    - Enables seamless switching between networks without changing IP addresses.

## Q2: Reasons for crime against IT infrastructure

Cybercriminals attack IT infrastructures for various reasons:

1. **Personal Exposure & Prestige:**
    - Hackers try to gain respect in their community by breaching secured systems.
2. **Financial Gain:**
    - **Credit card fraud, ransomware, and identity theft** generate huge profits for cybercriminals.
3. **Creating Damage & Disruption:**

- Cybercriminals may **deface websites, delete critical data, or crash servers** to harm businesses.

4. **Terrorism & Warfare:**
   - Governments or terrorist groups may **attack critical IT infrastructures** to cause panic or economic collapse.
5. **Revenge or Insider Threats:**
   - **Disgruntled employees** might steal or delete data as revenge against an employer.

**Short Questions**

**Q1: Three core goals of security (CIA Triad)**

1. **Confidentiality** – Prevents unauthorized access to data.
2. **Integrity** – Ensures that data is accurate and unaltered.
3. **Availability** – Ensures data and resources are accessible when needed.

**Long Questions**

**Q1: Benefits of IPv6 over IPv4**

1. **Larger Address Space:**
   - IPv6 uses **128-bit** addresses, while IPv4 uses **32-bit**, allowing more devices to be uniquely addressed.
2. **Auto-Configuration:**
   - IPv6 supports **stateless address auto-configuration (SLAAC)**, reducing reliance on DHCP servers.
3. **Improved Security:**
   - **IPSec encryption** is built into IPv6, ensuring better security.

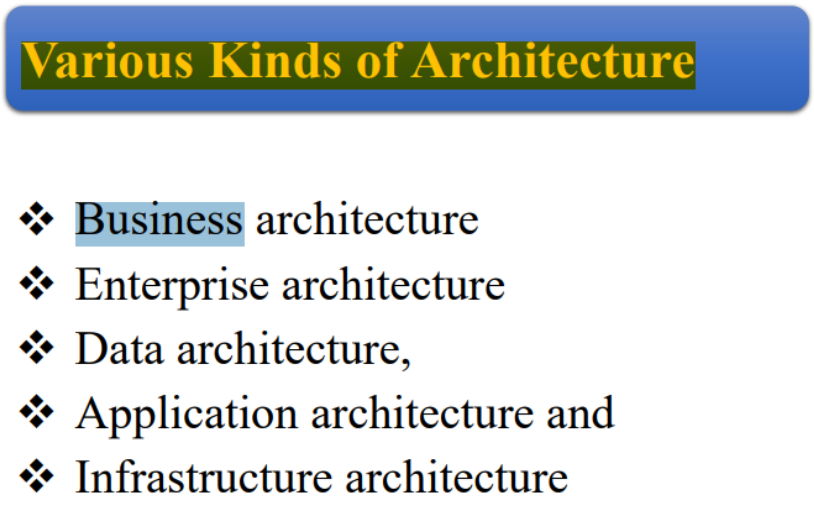
4. **Efficient Routing & Performance:**
    - Eliminates **Network Address Translation (NAT)**, reducing network complexity.
5. **Better Mobility Support:**
    - Allows devices to move between networks without changing IP addresses.

**Q2: Five parameters of a risk list**

A **risk list** is used in risk management to assess security threats. The five key parameters are:

1. **Asset Name** – The component that needs protection.
2. **Vulnerability** – Weakness that can be exploited.
3. **Exploit** – A method to attack the vulnerability.
4. **Probability** – Likelihood of the exploit occurring.
5. **Impact** – Severity of damage if the exploit happens.

**Q3: Five types/kinds of architecture**



**By Maha Rana**

## Short Questions

### Q1: Human Errors

- **80% of outages** in IT infrastructures are caused by **human errors**.
- Examples of human errors:
    1. **Performing a test in the production environment** (instead of a test system).
    2. **Accidentally deleting files or database entries** (e.g., using the wrong command).
    3. **Restoring the wrong backup tape** to production.

### Q2: Types of Fallback Solutions

Fallback solutions are used for disaster recovery. The three types are:

1. **Hot Site:**
    - Fully operational **backup site** with real-time data replication.
    - Can take over immediately if the main site fails.
2. **Warm Site:**
    - A **partially configured** backup site with some pre-installed software and hardware.
    - Needs updates before it becomes fully operational.
3. **Cold Site:**
    - A facility with infrastructure **ready but no pre-installed data or applications**.
    - Takes the longest time to become operational.

---

**By Maha Rana**

## Long Questions

### Q1: Risk Management

**Risk management**

- Managing security is all about managing risks
- The effort we put in securing the infrastructure should be directly related to the risk at hand
- Risk management is the process of:
  - Determining an acceptable level of risk
  - Assessing the current level of risk
  - Taking steps to reduce risk to the acceptable level
  - Maintaining that level

---

**Risk Response Strategies:**

1. **Risk Acceptance** – Accept the risk if the impact is low.
2. **Risk Avoidance** – Stop activities that create high risk.
3. **Risk Transfer** – Use **insurance or outsourcing** to transfer the risk.
4. **Risk Mitigation** – Implement **security controls** to reduce risk.

### Q2: Data Center Location

Selecting the right location for a data center is **critical for security, availability, and efficiency**.

**Key Factors in Choosing a Data Center Location:**

1. **Geographic & Environmental Factors:**

- Avoid areas prone to **earthquakes, floods, or hurricanes**.

2. **Power Supply & Redundancy:**
   - The site should have a **stable power grid** and **backup generators**.
3. **Network Connectivity:**
   - **Proximity to ISPs** ensures **high-speed and low-latency connections**.
4. **Security & Compliance:**
   - **Physical security measures** (gated access, surveillance, biometric authentication).
   - Compliance with **industry regulations (ISO, GDPR, etc.)**.
5. **Cost & Accessibility:**
   - The site should be **affordable** and allow **easy access for maintenance**.

**It602 current paper 2k25 mids**
**by phistantrophobian**

**by phistantrophobian**

Q#1:Aj aya wa tha data center k components or facilities of it infrastructure organization k liye.
Ans:Provides power supply, cooling, fire prevention and detection, equipment racks, and other facilities needed to host the installed infrastructure componentsHouses servers, networking equipment, storage devices, and other infrastructure required to support data processing and storage.

Q#2:what behavior of non functional attributes or koi 2 non functional attributes k name.
Ans:Non functional attributes describe the qualitative behavior of the system rather than its specific functionality and these include
• Availability • Security • Performanace • Recoverability • Testtability • Scalability

Q#3:name three security goals:
ANs:Three core goals of security (CIA): ❑Confidentiality ❑Integrity ❑Availability

Q#4:difference between hot site ,cold site,warm site explain them briefly

Ans:□**Hot Site:** Fully ready backup.
*Example: Office with running servers and data — just start work.*

□**Warm Site:** Partly ready backup.
*Example: Office with servers but no current data — needs some setup.*

**By Maha Rana**

**Cold Site:** Just space, not ready.
*Example: Empty office — needs all systems and data installed.*

Q#5:Name the three manmade disasters
Ans:Hazardous material spills

Infrastructurefailure

Bio-terrorism

Q#6 The process solves the affect of disaster

Ans: To handle the effect of disasters, following processes are • Business Continuity Management (BCM) and • Disaster Recovery Planning (DRP)

Business continuity is about identifying threats an organization faces and providing an effective response.

Q#7: List two names of Fiber optics cables.
ans: Two types of fiber optic cable are most common: – Multi-Mode Fiber (MMF)– Single Mode Fiber (SMF)

Q#8:What is the purpose of UPS? Wahat components ate involved in it.

Ans:Uninterruptable Power Supply (UPS) • Independent of the Utility power supply • Provide power for short period of time

Components of a UPS:Battery,Static Switch, inverter

Q#9How many forms are there of fallback? Also write their names.

Three basic forms of fallback solutions: • Hot site • Cold site • Warm site

Q#10:Risk list five parameters:

Risk is calculated based on:

Asset name - component that needs to be protected

**By Maha Rana**

Vulnerability- weakness, process or physical exposure that makes the asset susceptible to exploits

Exploit- a way to use one or more vulnerabilities to attack an asset

Probability- an estimation of the likelihood of the occurrence of an exploit

Impact- the severity of the damage when the vulnerability is exploited

Q#11:Can we check performance during the design phase? If yes, how, and what methods are used?

Yes we can Calculating performance of a system in the design phase is: Extremely difficult Very unreliable

Somewaystodothis are: • Benchmarking • Using vendor experience • Prototyping and User Profiling

Q#12 difference between **DNSSEC** ,DNS type

DNS is a distributed database that links IP addresses with domain names • Translates domain names, meaningful to humans, into IP addresses

DNS distributes the responsibility of mapping domain names to IP addresses by designating authoritative name servers for each domain

• **DNSSEC**is a set of extensions to DNS– Provides origin authentication of DNS data– Provides data integrity • DNSSEC is not in wide spread use today– All DNS servers must implement DNSSEC in order to make full use of all benefits

Q#13:it infrastructure k components explain kry

**Ans:1. Hardware:**

- **Definition:** Physical parts of a computer system.
- **Examples:** Computers, servers, routers, switches, hard drives, cables.

## 2. Software:

- **Definition:** Programs and operating systems that run on hardware.
- **Examples:** Windows, Linux, MS Office, databases, antivirus, ERP software.

## 3. Network:

**By Maha Rana**

- **Definition:** Systems that connect devices and allow communication.
- **Examples:** Internet, LAN (Local Area Network), WAN (Wide Area Network), routers, VPNs.

OSI model katha k kya ha btay or us k benifit in communication network

- The OSI Reference Model (OSI-RM) was developed in 1984 by the International Organization for Standardization (ISO)
- Seven layers define the different stages that data must go through to travel from one host to another over a network




The OSI stack allows:– Implementing network components independently of each other– Ensuring all components work together optimal way for a certain usage • Provides freedom to implement the network stack in an • Each layer's payload contains the protocol for the next layer

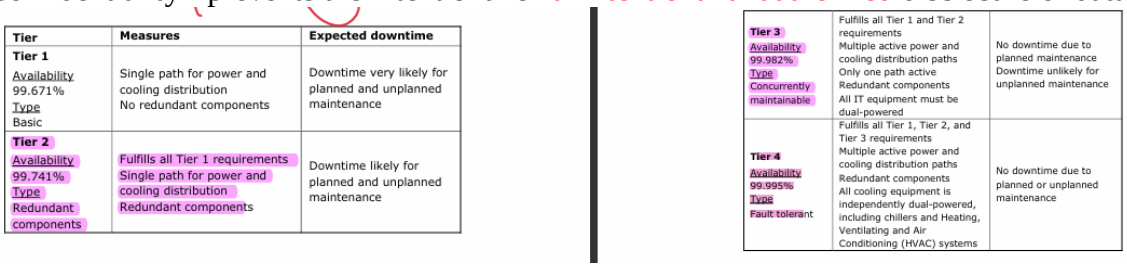
Enlist five names of Architecture.

Business architecture ❖ Enterprise architecture ❖ Data architecture, ❖ Application architecture and ❖ Infrastructure architecture

**by phistantrophobian**

Important mcqs:

**By Maha Rana**

1. Infrastructure also serves as the foundation upon which mission/program/project-specific systems and capabilities are built
2. MTTR can be kept low by: • Having a service contract with the supplier
3. most people, infrastructure is invisible and taken for grantes
4. 80% of outages impacting mission-critical services is caused by people and process issues
5. Environmental issues can cause downtime
6. Sometimes a component doesn't even work at all when unpacked for the first time. This is called a DOA component–Dead OnArrival
7. Failover is the (semi)automatic switch-over to a standby system or component
8. Performance is a typical hygiene factor
9. Calculating performance of a system in the design phase is: Extremely difficult
10. Stress testing - shows how a system reacts when it is under extreme load
11. Capacity management guarantees high performance of a system
12. For IT infrastructures availability is a non-functional attribute in its own right
13. Confidentiality - prevents the intentional or unintentional unauthorized disclosure of data
14. 

| Tier | Measures | Expected downtime |
|---|---|---|
| **Tier 1**<br>Availability<br>99.671%<br>Type<br>Basic | Single path for power and cooling distribution<br>No redundant components | Downtime very likely for planned and unplanned maintenance |
| **Tier 2**<br>Availability<br>99.741%<br>Type<br>Redundant components | Fulfills all Tier 1 requirements<br>Single path for power and cooling distribution<br>Redundant components | Downtime likely for planned and unplanned maintenance |
| **Tier 3**<br>Availability<br>99.982%<br>Type<br>Concurrently maintainable | Fulfills all Tier 1 and Tier 2 requirements<br>Multiple active power and cooling distribution paths<br>Only one path active<br>Redundant components<br>All IT equipment must be dual-powered | No downtime due to planned maintenance<br>Downtime unlikely for unplanned maintenance |
| **Tier 4**<br>Availability<br>99.995%<br>Type<br>Fault tolerant | Fulfills all Tier 1, Tier 2, and Tier 3 requirements<br>Multiple active power and cooling distribution paths<br>Redundant components<br>All cooling equipment is independently dual-powered, including chillers and Heating, Ventilating and Air Conditioning (HVAC) systems | No downtime due to planned or unplanned maintenance |

15. Stand-alone machines Mainframe Computers in the 1960s-Computing and Punching machines
16. Endpoints in the walls are connected to the patch panels (horizontal cabling)
17. IPv4 addresses are composed of 4 bytes (32 bits)
18. IPv6 uses 128-bit addresses represented in eight groups of four hexadecimal digits separated by colons

**By Maha Rana**

**May Allah grant you success, ease your efforts, and bless you with wisdom and perseverance. Keep your faith strong, for with prayer, every challenge becomes an opportunity. And please remember us in your prayers.**

**I hope this file helps you a lot; I have tried my best to find the most relevant and authenticated answers for the questions. However, in some cases, the questions might slightly differ from the ones in your slides. I recommend that every student kindly verify the answers on their own before using them. I am not responsible for any discrepancies.**

**Best wishes for Mids!**

**By Maha Rana**