**Service Desk Administrator (Service Desk II)**

**Why do you want to be a Service Desk Administrator?** (Answers May Vary)

"I am interested in the Service Desk Administrator role because…

* It aligns with my academic background.
* My professional experience in IT since 2020.
* I have always been fascinated by technology and passionate about learning.
* Enjoy the challenge of solving complex issues.
* This role allows me to leverage my technical skills.

Moreover, a Service Desk Administrator's role is to resolve technical issues and understand **business needs**.

* I am excited about the business-centric approach to IT support.

**What is the difference between Help Desk & Service Desk? (ITIL)**

“Help desk” and “Service desk” are often used interchangeably, but they refer to two types of support services.

**Help Desk**: This is a more tactical resource to fix immediate IT issues. A help desk is typically considered to be focused on break-fix (what ITIL calls incident management) and has a reactive approach to addressing issues as they arise.

**Service Desk**: A service desk is a single point of contact between users and IT Service Management. **Service desks focus on delivering a holistic and user-centric approach** that provides **a single point of contact for all IT-**related services. It’s more strategic and takes both service requests as well as incidents into consideration.

While both aim to streamline IT support, service desks take a broader approach by focusing on business processes and providing support throughout the entire lifecycle of an IT service.

**What is Desktop Support?**

Desktop support is a more specific form of technical support. A desktop support team is highly skilled professionals with direct access to phones, computers, tablets, and other devices.

**What is the ITSM?**

IT service management -- often referred to as ITSM -- is how IT teams manage the end-to-end delivery of IT services to customers. This includes all the processes and activities to design, create, deliver, and support IT services.

The core concept of ITSM is that IT should be viewed as a service.

**What is ITIL?**

**ITIL (Information Technology Infrastructure Library)** is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with business needs.

It is essential **because** it **provides a practical framework for identifying, planning, delivering, and supporting IT services to the company.**

**Explain the difference between LAN and WAN.**

**LAN (Local Area Network)** is a network that **connects computers and devices in a limited area,** such as **a home, school, office buildin**g, or closely positioned group of buildings.

**WAN (Wide Area Network)** is a telecommunications network **that extends over a large geographical area** for the primary purpose of computer networking.

More giant corporations or organizations often exchange data in different geographic regions with WANs**.**

**What is Active Directory?**

**Active Directory (AD)** is a Microsoft technology used to manage computers and other devices on a network.

It is a directory service for Windows domain networks and involves multiple functions.

Its significance is for user authentication, authorization, groups & distributions for security permissions. As well as providing access control to various IT resources.

**Can you explain a VPN and why a company may need one?**

A **VPN (Virtual Private Network)** extends a private network across a public network; this encrypts data sent over the web. Companies might need one to secure remote connections or enable employees to access resources securely from different locations.

**What is the role of DNS in a network?**

**DNS (Domain Name System)** is a system used to translate human-readable domain names, like www.example.com, into machine-readable IP addresses, like 192.0.2.1. Devices on a network need to communicate with each other.

**What is DHCP, and what is it used for?**

**DHCP (Dynamic Host Configuration Protocol)** is a network protocol used on IP networks where a DHCP server automatically assigns an IP address and other network configuration parameters to each device on the network so they can communicate with other IP networks.

**Describe a ticketing system.**

A **ticketing system** is a management tool that processes and catalogs customer service requests. Tickets must be appropriately stored alongside relevant user information. The ticketing system should help the service desk to sort and prioritize issues quickly.

**How do you stay updated on the latest IT trends and technologies?**

Through the pages and people I follow on LinkedIn. My LinkedIn newsfeed. As well as having certain subscriptions to e-mail newsletters. I also have dedicated favorite folders with some of my most visited websites. These sites have built-in blogs or news pages on them.

**What is a Firewall in Network Security?**

A **firewall** is a network security device that monitors incoming and outgoing traffic and decides whether to allow or block specific traffic based on a defined set of security rules. It protects networks from potentially harmful information transmitted over the internet.

**What are the types of Firewalls?**

**Level 7 Firewall: (Application Layer Firewall)** operates on layer seven of the OSI model. The application firewall is sometimes known as WAF (Web Application Firewall). This layer allows for more advanced traffic-filtering rules. Rather than filtering traffic by IP addresses, level 7 firewalls can analyze the contents of data packets to see if they contain malware or other cyber threats. Protects against SQL injection, URL attacks, JavaScript, and more.

**Level 3 Firewall: (Network Layer Firewall)** operates on layer three of the OSI model—the same layer as routers. Therefore, level 3 firewalls can monitor traffic using the same protocols as routing (TCP UDP ICMP). Some routers have built-in firewalls. They scan traffic based on IP (Internet Protocol) addresses, port addresses, and router-based principles.

**Stateful Firewall:** A **Stateful Firewall** keeps track of and monitors the state of active network connections (routing tables) while analyzing incoming traffic and looking for potential data risks. Stateful Firewalls are on layer three (Networking) and layer four (Transport) of the OSI model.

Stateful firewalls can detect attempts by unauthorized individuals to access a network and analyze the data within packets to see if they contain malicious code.

**Stateless Firewall:** A **Stateless Firewall** does not keep track of information on the current state of the network. A Stateless firewall evaluates each packet individually and attempts to determine if it's authorized or unauthorized. Stateless firewalls use information regarding where a data packet is headed, where it came from, and other parameters to determine whether the data presents a threat.

**Stateless Firewalls** require less bandwidth than **Stateful Firewalls,** meaning fewer **resources and overhead are** needed **on** the **network** **than** implementing a **Stateful firewall.**

**What’s the difference between a Firewall and an Anti-Virus?**

**Firewall**: A firewall **functions as a barrier for incoming system traffic**. It is implemented in both hardware and software. It monitors and filters incoming and outgoing network traffic based on an organization’s established security policies. At its most basic, a firewall is essentially a barrier to keep destructive forces away from your property. That’s why it's called a firewall. Its job is like a physical firewall that controls fire from spreading from one area to the next.

**Antivirus**: Antivirus software is a program or set of programs designed to prevent, search for, detect, and remove software viruses and other malicious software like worms, trojans, adware, and more. **It is implemented in software only**. Antivirus deals with both external threats and internal threats. It works by scanning files or directories for any malicious programs or files.

**Key Differences:**

* A firewall preserves software and hardware on the network, while an antivirus protects other software.
* Firewall deals with external threats only. Antivirus deals with both internal and external.
* The firewall works on monitoring and filtering. Antivirus works on scanning system software for infected files.
* Firewall checks for threats from incoming packets. Antivirus checks for hazards in malicious software code.
* Firewall programming is more complex than antivirus programming when comparing the two.

**How do you secure a server?**

Securing a server can involve several steps, such as ensuring up-to-date software, using strong passwords, enabling firewall rules, regularly reviewing access logs, encrypting data in transit and at rest, and regularly backing up data.