Here are some common interview questions for an IT System Admin role, along with concise answers:

1. **What is Active Directory?**
    - Active Directory (AD) is a directory service by Microsoft for Windows domain networks. It helps manage and store information about network resources and enables authentication and authorization of users.
2. **What is DNS and how does it work?**
    - DNS (Domain Name System) translates human-readable domain names (e.g., www.example.com) into IP addresses. It resolves domain names by querying DNS servers in a hierarchy.
3. **What is the difference between a hub, a switch, and a router?**
    - A hub broadcasts data to all devices, a switch directs data to specific devices, and a router connects different networks and directs traffic between them.
4. **How would you handle a server crash?**
    - Check event logs, isolate the cause (hardware, OS, or software issue), try to reboot in safe mode, and restore from backups if needed. Ensure the problem doesn't repeat.
5. **What are the key components of a network infrastructure?**
    - Routers, switches, firewalls, servers, access points, cabling, and end-user devices.
6. **How do you secure a server?**
    - Use strong passwords, implement firewalls, keep software updated, apply least privilege access controls, and regularly back up data.
7. **What is virtualization and why is it important?**
    - Virtualization allows multiple virtual machines to run on a single physical server, optimizing resource use and reducing costs. It also simplifies disaster recovery and system administration.
8. **What monitoring tools have you used?**
    - Tools like Nagios, Zabbix, or SolarWinds can be used to monitor network performance, server health, and application uptime.
9. **How do you troubleshoot network issues?**
    - Use the OSI model as a guide, starting from the physical layer (cables, connections) up to the application layer. Use tools like ping, traceroute, and nslookup to identify issues.
10. **What is RAID and how does it work?**
    - RAID (Redundant Array of Independent Disks) is a method of storing data across multiple hard drives to improve performance and provide redundancy. Common levels include RAID 0 (striping), RAID 1 (mirroring), and RAID 5 (striping with parity).

11. **What is DHCP and how does it work?**
    - DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to devices on a network. It eliminates the need for manually assigning IP addresses to each device.
12. **What is the purpose of a firewall?**
    - A firewall controls incoming and outgoing network traffic based on security rules. It protects the internal network from external threats by allowing or blocking traffic.
13. **What are Group Policies in Windows?**
    - Group Policies are a feature in Windows that allow administrators to manage configurations and settings for users and computers within an Active Directory environment, such as enforcing password policies or restricting certain applications.
14. **Explain the difference between TCP and UDP.**
    - TCP (Transmission Control Protocol) is connection-oriented and ensures reliable data transfer by checking for errors and retransmitting lost packets. UDP (User Datagram Protocol) is connectionless, faster, but doesn't guarantee delivery.
15. **What is a VPN and how does it work?**
    - A Virtual Private Network (VPN) provides a secure connection between a user’s device and the network by encrypting data. It’s commonly used to allow remote access to private networks.
16. **What is the blue screen of death (BSOD)? How would you troubleshoot it?**
    - BSOD is a fatal system error in Windows, indicating serious hardware or software issues. Troubleshooting involves checking error codes, reviewing recent hardware or software changes, and scanning for faulty drivers or memory issues.
17. **What is an IP address? Explain the difference between public and private IPs.**
    - An IP address is a unique identifier for a device on a network. Public IPs are accessible from the internet, while private IPs are used within local networks and aren’t routable on the internet.
18. **What is patch management?**
    - Patch management involves regularly applying updates or "patches" to software, firmware, or systems to improve security, fix bugs, and enhance performance.
19. **What are some common ports you need to know as a System Administrator?**
    - Some important ports include:
      - HTTP: 80
      - HTTPS: 443
      - FTP: 21
      - SSH: 22
      - DNS: 53
      - SMTP: 25

    - RDP: 3389

20. **How would you secure a network?**
    - Implement firewalls, use strong encryption, deploy intrusion detection/prevention systems, enforce access control policies, regularly update software, and use VPNs for remote access.

21. **What is the difference between incremental and differential backups?**
    - Incremental backups save only the data changed since the last backup of any type. Differential backups save all changes made since the last full backup, making them larger than incremental but faster to restore.

22. **What is the role of DNS in email delivery?**
    - DNS is used in email delivery to resolve domain names of email servers (MX records) to IP addresses, helping route emails to the correct mail server.

23. **How would you handle high CPU usage on a server?**
    - Identify the process consuming high CPU using tools like Task Manager or top (Linux), check for rogue processes, optimize the application, or scale up hardware resources if needed.

24. **What is load balancing and why is it important?**
    - Load balancing distributes network or application traffic across multiple servers to prevent overloading a single server, ensuring better availability and performance.

25. **How do you handle data recovery in case of a failure?**
    - Rely on regular backups, ensure that critical systems have redundant setups, and use data recovery tools or services if backups aren't available. Test recovery plans regularly to ensure they work in case of an actual failure.

26. **What is a VLAN and why is it used?**
    - A VLAN (Virtual Local Area Network) segments a network into distinct broadcast domains, improving performance and security by isolating network traffic within groups of devices.

27. **How would you handle a slow-performing application on a server?**
    - Check server resource usage (CPU, memory, disk I/O), look for network issues, analyze logs for errors, review application configurations, and optimize the database or app settings.

28. **What is the difference between HTTP and HTTPS?**
    - HTTP (HyperText Transfer Protocol) is unencrypted, while HTTPS (HTTP Secure) encrypts data between the user and the server using SSL/TLS, providing secure communication.

29. **What is an SLA and why is it important?**
    - A Service Level Agreement (SLA) is a contract that defines the level of service expected between a service provider and customer. It sets performance metrics, response times, and accountability.

30. **What is the purpose of a proxy server?**
    - A proxy server acts as an intermediary between a client and the internet, providing services like caching, improving performance, and anonymizing user requests.
31. **How do you manage user access and permissions in a network?**
    - Use role-based access control (RBAC) with the principle of least privilege, manage permissions using tools like Active Directory, and regularly audit access rights to ensure compliance.
32. **What is the difference between NTFS and FAT32 file systems?**
    - NTFS (New Technology File System) supports larger files, offers better security features like encryption and access control, and is more reliable. FAT32 has limitations on file sizes and lacks advanced features.
33. **How do you ensure data integrity in backups?**
    - Verify backups with checksum or hash comparisons, regularly test backup restorations, and store backups in multiple locations to prevent corruption or loss.
34. **What is a DMZ in network security?**
    - A DMZ (Demilitarized Zone) is a subnetwork that adds an extra layer of security by exposing external-facing services (like web servers) while keeping internal networks isolated.
35. **How do you handle user account lockouts?**
    - Use Active Directory to check for the cause of the lockout (e.g., wrong password, expired password, multiple login attempts), unlock the account, and troubleshoot further if recurring.
36. **What is SNMP and what is it used for?**
    - SNMP (Simple Network Management Protocol) is used for monitoring and managing network devices like routers, switches, and servers. It allows administrators to collect data and configure network devices remotely.
37. **What is the difference between static and dynamic routing?**
    - Static routing requires manually defining routes, while dynamic routing protocols (like OSPF, EIGRP) automatically adjust routes based on network changes.
38. **How do you manage patching in a large environment?**
    - Use automated tools like WSUS (Windows Server Update Services) or SCCM (System Center Configuration Manager) to deploy patches, schedule regular updates, and test patches in a staging environment before rolling them out.
39. **What is RAID 10 and how does it work?**
    - RAID 10 combines RAID 1 (mirroring) and RAID 0 (striping). It provides high performance and redundancy by both mirroring data across drives and striping it to improve read/write speeds.
40. **What are the different types of network topologies?**

- Common network topologies include:
  - **Bus topology**: All devices are connected to a single backbone.
  - **Star topology**: All devices are connected to a central hub.
  - **Mesh topology**: Every device is connected to every other device.
  - **Ring topology**: Devices are connected in a circular fashion, where each device is connected to two others.

41. **What is PowerShell and how do you use it in system administration?**

- PowerShell is a task automation and configuration management framework from Microsoft. It's used to automate tasks, manage configurations, and troubleshoot issues across Windows environments.

42. **How would you troubleshoot a network with intermittent connectivity issues?**

- Check the physical connections (cables, ports), analyze network traffic for congestion, look for faulty hardware, review router/switch configurations, and use tools like ping, traceroute, and network monitoring tools to identify the root cause.

43. **What is the purpose of load balancing?**

- Load balancing distributes traffic across multiple servers to ensure no single server is overwhelmed, providing high availability, redundancy, and optimal performance.

44. **How do you manage disk space on a server?**

- Regularly monitor disk usage, delete unnecessary files or logs, compress data, move data to network storage, and set up alerts for low disk space thresholds.

45. **What is two-factor authentication (2FA)?**

- 2FA adds an extra layer of security by requiring users to provide two forms of authentication (e.g., a password and a code sent to their phone) before accessing a system.

46. **What is RAID 5 and how does it work?**

- RAID 5 uses striping with parity, distributing data and parity across multiple drives. It provides redundancy, allowing the array to survive the failure of one drive while maintaining data integrity.

47. **What is an IDS and IPS?**

- IDS (Intrusion Detection System) monitors network traffic for suspicious activity and alerts the administrator. IPS (Intrusion Prevention System) monitors and actively blocks potentially harmful traffic.

48. **What is Kerberos authentication?**

- Kerberos is a network authentication protocol that uses secret-key cryptography to verify the identity of users and services over an unsecured network. It's commonly used in Active Directory environments.

49. **What is the difference between a cold backup and a hot backup?**

- A **cold backup** requires shutting down the system or database to perform the backup, while a **hot backup** can be done while the system is online and operational.

50. **What is LDAP and how is it used?**
    - LDAP (Lightweight Directory Access Protocol) is used for accessing and maintaining distributed directory information services, like user authentication and authorization in Active Directory.

51. **What is a subnet mask and why is it important?**
    - A subnet mask divides an IP address into the network and host portions, helping define the range of IP addresses within a network. It helps route traffic within and outside of the network.

52. **How would you monitor server performance?**
    - Use performance monitoring tools (e.g., Windows Performance Monitor, top, vmstat), track key metrics like CPU, memory, disk I/O, and network usage, and set up alerts for unusual spikes.

53. **What is a SAN and how does it differ from NAS?**
    - A SAN (Storage Area Network) is a high-speed network that provides block-level storage to servers. NAS (Network-Attached Storage) is a file-level storage device connected to a network, usually easier to set up and more suitable for file sharing.

54. **What is a service account and why is it important?**
    - A service account is a special user account created to run specific services, applications, or automated tasks. It's important to limit permissions to only what's needed to minimize security risks.

55. **How do you handle high memory usage on a server?**
    - Identify the process consuming the most memory using tools like Task Manager or top, optimize the application, clear caches, and consider adding more RAM if necessary.

56. **What are the advantages of using virtualization in a server environment?**
    - Virtualization improves resource utilization, reduces hardware costs, simplifies backups and disaster recovery, and allows for easier server management and scaling.

57. **What are the benefits of cloud computing for system administrators?**
    - Cloud computing offers scalability, reduced infrastructure maintenance, cost savings, faster deployment of resources, and improved disaster recovery options.

58. **How do you handle email spam in an organization?**
    - Use spam filters, blacklist/whitelist email addresses, configure mail servers to block suspicious IP addresses, enable email authentication (SPF, DKIM, DMARC), and educate users on phishing risks.

59. **What is high availability (HA) and how is it achieved?**
    - High availability ensures continuous operation by minimizing downtime. It's achieved through redundancy, failover systems, load balancing, and clustering.

60. **What is a snapshot in virtualization, and how does it work?**
    - A snapshot captures the state of a virtual machine at a particular point in time, allowing the system to revert to that state later if needed. It's commonly used for backup and testing.

61. **What is network bonding or teaming?**
    - Network bonding or teaming combines multiple network interfaces into a single interface to increase bandwidth and provide redundancy in case one link fails.

62. **What is syslog and how is it used?**
    - Syslog is a standard protocol used to send system logs or event messages to a centralized server (syslog server) for monitoring and troubleshooting purposes.

63. **How do you prevent a DDoS attack?**
    - Use firewalls and intrusion prevention systems (IPS), deploy rate limiting, utilize load balancers, employ DDoS protection services, and monitor network traffic for unusual spikes.

64. **What are the steps to migrate data from one server to another?**
    - Plan the migration, back up the data, check compatibility, transfer data (using SCP, Rsync, or cloud migration tools), test for data integrity, and verify proper functionality after migration.

65. **What is RDP and how is it used?**
    - RDP (Remote Desktop Protocol) allows users to connect to another computer over a network to access its desktop and resources as if they were physically present at the machine.

66. **How would you troubleshoot a remote user unable to connect to the VPN?**
    - Check the VPN client configuration, verify user credentials, check network connectivity, ensure the VPN server is running, and verify firewall settings on both ends.

67. **What is load balancing, and how is it implemented?**
    - Load balancing distributes traffic across multiple servers to optimize resource use and prevent overload. It's implemented using hardware load balancers or software solutions like NGINX, HAProxy, or AWS ELB.

68. **What is a site-to-site VPN?**
    - A site-to-site VPN connects entire networks (e.g., branch offices to the main office) over the internet, providing secure communication between them as if they were in the same location.

69. **How do you enforce security policies in an organization?**
    - Use group policies, deploy security tools like antivirus and firewalls, regularly patch systems, enforce password policies, educate users, and conduct regular security audits.

70. **What is the role of a DNS resolver?**

    - A DNS resolver is responsible for converting a domain name into an IP address. It queries various DNS servers in a hierarchy to find the IP address for a given domain.

71. **What is the difference between IPv4 and IPv6?**

    - IPv4 uses 32-bit addresses and supports approximately 4.3 billion devices, while IPv6 uses 128-bit addresses, vastly expanding the number of available IP addresses and improving routing efficiency.

72. **How would you manage storage in a Linux server?**

    - Use tools like `df` and `du` to monitor disk usage, `fdisk` or `parted` to manage partitions, and LVM (Logical Volume Manager) for flexible storage management. You can also set quotas to limit disk usage for users.

73. **What is a disaster recovery plan (DRP)?**

    - A DRP is a documented process that outlines how an organization will recover from unexpected events (e.g., natural disasters, cyberattacks) to ensure business continuity.

74. **What is a bastion host and when would you use it?**

    - A bastion host is a highly secured server positioned between an internal network and external, untrusted networks. It's used to provide controlled access to the internal network while minimizing risk.

75. **What are some best practices for managing IT documentation?**

    - Keep it organized, regularly updated, accessible to relevant team members, use templates for consistency, and store it securely to avoid unauthorized access.

76. **What is the difference between a full backup, incremental backup, and differential backup?**

- **Full backup**: Backs up all data, regardless of changes. It is time-consuming but allows for faster restoration since all data is in one backup set.
- **Incremental backup**: Only backs up data that has changed since the last backup (full or incremental). It's faster and uses less storage but requires multiple backup sets to restore.
- **Differential backup**: Backs up all data changed since the last full backup. It's larger than incremental backups but quicker to restore since only the full and latest differential backups are needed.

77. **What are the differences between NAS (Network Attached Storage) and DAS (Direct Attached Storage)?**

- **NAS**: Network Attached Storage is a file-level storage connected to a network, accessible by multiple devices over the network. It's easy to set up and is commonly used for file sharing and centralizing data storage.
- **DAS**: Direct Attached Storage is directly connected to a single computer or server (e.g., external hard drives, SSDs). It's fast but limited to the device it is attached to and isn't accessible over a network.