Top 50 Topic Wise Questions For Network Engineer

Basic Troubleshooting

1. Q: What steps would you take if a user reports no internet connectivity?

   A: Check the physical connection, verify IP settings, test connectivity with ping, check for DHCP issues, and ensure the gateway is reachable.

2. Q: How do you troubleshoot a failed ping test to a specific server?

   A: Verify server availability, check DNS resolution, ensure correct routing, and inspect firewalls for blocked ICMP.

3. Q: How do you resolve duplicate IP address conflicts?

   A: Identify conflicting devices using arp -a, manually assign unique IPs, and check the DHCP server for misconfigurations.

4. Q: What would you do if a device has an APIPA address (169.x.x.x)?

   A: Check the DHCP server's availability and ensure the device can communicate with it.

5. Q: What tools would you use to diagnose packet loss?

   A: Tools like ping, traceroute, and network analyzers (Wireshark).

Routing Issues

6. Q: How do you troubleshoot a routing loop?

A: Inspect routing tables, check route advertisements, and use tools like traceroute to identify loops.

7. Q: What steps would you take for an OSPF adjacency issue?

A: Verify matching parameters (area ID, authentication), MTU settings, and ensure there are no Layer 2 issues.

8. Q: How do you resolve BGP session flapping?

A: Check peer configurations, inspect keepalive/hold timers, and ensure stable network paths.

9. Q: How do you troubleshoot a static route not working?

A: Verify route configuration, ensure the next-hop is reachable, and check for overlapping or conflicting routes.

10. Q: What would you check if inter-VLAN routing is not working?

A: Verify VLAN configurations, ensure subinterfaces are configured, and check Layer 3 interfaces' status.

Switching Issues

11. Q: How do you troubleshoot a VLAN mismatch?

A: Check trunk port configurations and ensure both ends have the same VLAN allowed.

12. Q: What would you do if a specific port on a switch is not passing traffic?

A: Check the port status, verify VLAN assignment, inspect cables, and review STP status.

13. Q: How do you troubleshoot STP-related issues?

A: Identify root bridge, check for port states, and verify priority configurations.

14. Q: How do you resolve excessive broadcast traffic?

A: Identify the source of broadcasts using network monitoring tools and segment the network if necessary.

15. Q: What would you check if a MAC address is not appearing in the MAC table?

A: Verify port activity, inspect VLAN settings, and ensure the device is generating traffic.

Wireless Troubleshooting

16. Q: How do you troubleshoot a Wi-Fi network with low signal strength?

A: Check the placement of access points, adjust power levels, and scan for interference.

17. Q: What do you do if a user cannot connect to a Wi-Fi network?

A: Verify SSID, check authentication settings, and inspect wireless logs for errors.

18. Q: How do you resolve frequent Wi-Fi disconnections?

A: Check signal strength, review device roaming settings, and inspect AP logs.

19. Q: What steps would you take if wireless devices experience slow speeds?

A: Analyze channel utilization, adjust channel width, and ensure no bandwidth hogging.

20. Q: How do you identify rogue access points?

A: Use wireless scanning tools like NetSpot or AirMagnet.

Firewall Issues

21. Q: How do you troubleshoot blocked traffic through a firewall?

A: Inspect access control lists (ACLs), check logs for denied traffic, and ensure the correct NAT configuration.

22. Q: What steps would you take if a VPN tunnel is not establishing?

A: Verify Phase 1/Phase 2 settings, check for pre-shared key mismatches, and ensure both ends are reachable.

23. Q: How do you troubleshoot port forwarding issues?

A: Ensure the correct public IP, port, and internal IP mapping. Check NAT and firewall rules.

24. Q: What do you check if a firewall is not passing traffic?

A: Verify interface statuses, review routing, and check for misconfigured security policies.

25. Q: How do you diagnose high CPU usage on a firewall?

A: Check active sessions, review traffic logs for anomalies, and ensure DDoS protection is enabled.

DNS Troubleshooting

26. Q: What steps do you take if a website is not resolving?

A: Test with nslookup or dig, check DNS server settings, and verify the domain's DNS records.

27. Q: How do you fix DNS timeout issues?

A: Check the DNS server's health, ensure no network latency, and verify firewall rules.

28. Q: How do you troubleshoot intermittent DNS resolution failures?

A: Review logs, ensure redundancy, and inspect caching configurations.

29. Q: What would you check if internal DNS resolution fails?

A: Verify the DNS zone configuration, inspect replication, and check for stale records.

30. Q: How do you resolve reverse DNS lookup issues?

A: Verify PTR records and ensure they match the forward DNS records.

Performance Issues

31. Q: How do you troubleshoot high latency in a network?

A: Use ping and traceroute to identify bottlenecks, check for congestion, and optimize QoS settings.

32. Q: What would you check if users experience frequent application timeouts?

A: Inspect the application server’s health, review network latency, and analyze logs.

33. Q: How do you troubleshoot slow file transfers over the network?

A: Test bandwidth, check for duplex mismatches, and monitor traffic for bottlenecks.

34. Q: How do you diagnose excessive CPU utilization on a router?

A: Review interface statistics, inspect routing tables, and disable unnecessary services.

35. Q: What steps would you take for network jitter issues?

A: Prioritize traffic with QoS, inspect real-time traffic paths, and reduce congestion.

Security Issues

36. Q: How do you detect a DDoS attack?

A: Monitor traffic patterns, check for excessive connections, and use IDS/IPS.

37. Q: What steps would you take if a network is compromised?

A: Isolate affected systems, analyze logs, and restore from backups.

38. Q: How do you secure an open port discovered during a scan?

A: Disable unused services, apply ACLs, or use a firewall.

39. Q: How do you identify unauthorized access attempts?

A: Analyze syslogs, review failed authentication attempts, and use SIEM tools.

40. Q: What would you do if sensitive data is being leaked?

A: Inspect firewall logs, review outbound traffic, and implement DLP solutions.

General Scenarios

41. Q: How do you troubleshoot a split-horizon issue in routing?

A: Enable route redistribution and check protocol configurations.

42. Q: What do you do if multicast traffic is not being delivered?

A: Verify multicast group membership, inspect IGMP settings, and ensure PIM is configured.

43. Q: How do you resolve MTU mismatches?

A: Use ping with the -f flag and adjust MTU settings on affected devices.

44. Q: What steps would you take if QoS is not prioritizing traffic correctly?

A: Verify QoS policies, inspect traffic classification, and ensure queue settings are correct.

45. Q: How do you identify the root cause of network congestion?

A: Use tools like NetFlow, review interface statistics, and inspect traffic patterns.

Advanced Troubleshooting

46. Q: How do you troubleshoot MPLS label mismatches?

A: Verify LDP settings, check for duplicate labels, and inspect forwarding tables.

47. Q: What do you check if a VXLAN tunnel is not working?

A: Inspect VTEP settings, verify encapsulation protocols, and ensure multicast is supported.

48. Q: How do you troubleshoot SD-WAN connectivity issues?

A: Check the controller's reachability, inspect policies, and verify transport links.

49. Q: How do you resolve issues with SNMP monitoring?

A: Verify community strings, check SNMP agent availability, and ensure firewalls allow SNMP traffic.

50. Q: What would you do if a network device firmware upgrade fails?

A: Roll back to the previous firmware, verify compatibility, and reattempt with correct procedures.

These questions and answers provide a broad foundation for troubleshooting common and advanced network issues.

pmnetworking.in