⍰ EASY (10 Questions)

Q1. Network Policy Server (NPS) is Microsoft’s implementation of which protocol?
A. LDAP
B. Kerberos
C. RADIUS
D. TACACS

Q2. What is the primary function of NPS?
A. IP address allocation
B. Centralized authentication and authorization
C. File sharing
D. Backup management

Q3. Which component sends authentication requests to NPS?
A. Domain Controller
B. RADIUS Client
C. DHCP Server
D. DNS Server

Q4. Which directory service does NPS commonly integrate with?
A. Azure Storage
B. Active Directory
C. DNS
D. IIS

Q5. Which port is used by RADIUS for authentication by default?
A. TCP 443
B. UDP 53
C. UDP 1812
D. TCP 3389

Q6. Which feature logs authentication attempts in NPS?
A. Accounting
B. Quotas
C. Replication
D. Delegation

Q7. Which authentication framework supports multiple methods like EAP?
A. PAP
B. CHAP
C. EAP
D. NTLM

Q8. Which service must be installed to deploy NPS?
A. DHCP

B. DNS
C. Network Policy and Access Services
D. Web Server (IIS)

Q9. Which shared value secures communication between NPS and clients?
A. Certificate
B. Password hash
C. Shared secret
D. Token

Q10. Which scenario commonly uses NPS?
A. File server access
B. VPN authentication
C. Disk management
D. Backup scheduling

□ MEDIUM (15 Questions)

Q11. What is the purpose of registering NPS in Active Directory?
A. Enable DHCP scopes
B. Allow NPS to read user properties
C. Encrypt RADIUS traffic
D. Enable DNS updates

Q12. Which NPS policy defines *who* is allowed network access?
A. Connection Request Policy
B. Network Policy
C. Group Policy
D. Firewall Policy

Q13. Which RADIUS packet indicates successful authentication?
A. Access-Request
B. Access-Challenge
C. Access-Accept
D. Access-Reject

Q14. Which protocol is commonly used for secure Wi-Fi authentication with NPS?
A. WEP
B. WPA2-Enterprise
C. WPA-Personal
D. Open Wi-Fi

Q15. Which NPS feature determines *how* authentication requests are processed?
A. Network Policy

B. Accounting Policy
C. Connection Request Policy
D. Group Policy

Q16. Which EAP method provides the highest security?
A. EAP-MD5
B. PEAP-MSCHAPv2
C. EAP-TLS
D. PAP

Q17. Which VPN component forwards authentication requests to NPS?
A. DHCP Relay
B. RRAS
C. DNS Server
D. Firewall

Q18. What is the purpose of RADIUS accounting?
A. User authentication
B. Encryption
C. Logging usage and access
D. IP address assignment

Q19. Which NPS condition can restrict access by time?
A. NAS Identifier
B. Day and Time Restrictions
C. IP address filter
D. Certificate template

Q20. Which authentication method requires digital certificates on clients?
A. MS-CHAPv2
B. PAP
C. EAP-TLS
D. CHAP

Q21. Which log helps troubleshoot NPS authentication failures?
A. Application log
B. Security log
C. NPS Accounting log
D. DNS debug log

Q22. Which scenario best suits NPS deployment?
A. Standalone file server
B. Centralized Wi-Fi authentication
C. Local user authentication only
D. Disk quota management

Q23. Which feature can integrate multi-factor authentication with NPS?
A. Windows Defender
B. Azure MFA Extension
C. BitLocker
D. IPsec

Q24. Which NPS configuration defines allowed encryption strengths?
A. Conditions
B. Constraints
C. Settings
D. Filters

Q25. Which protocol ensures secure transport of credentials in PEAP?
A. SSL/TLS
B. IPsec
C. SMB
D. FTP

HARD (15 Questions)

Q26. Why is certificate-based authentication preferred in enterprises?
A. Faster login
B. Strong mutual authentication
C. Lower cost
D. Easier configuration

Q27. Which NPS misconfiguration commonly causes “Access Denied” errors?
A. DNS failure
B. Policy order mismatch
C. Disk space issue
D. Disabled firewall

Q28. Why should strong shared secrets be used for RADIUS clients?
A. Improve performance
B. Prevent spoofing and attacks
C. Reduce logging
D. Simplify setup

Q29. Which enterprise risk is mitigated by centralized NPS authentication?
A. Disk failure
B. Credential sprawl
C. Network congestion
D. Hardware aging

Q30. Which failure would prevent all VPN users from authenticating?
A. DNS forwarder issue
B. NPS service stopped
C. DHCP lease expiry
D. IPAM discovery failure

Q31. Why is policy order critical in NPS?
A. Policies are merged
B. First matching policy is applied
C. Last policy always wins
D. Policies are randomized

Q32. Which protocol does NPS rely on for secure AD authentication?
A. LDAP only
B. Kerberos
C. FTP
D. SNMP

Q33. Why should NPS logs be centrally collected?
A. Reduce disk usage
B. Improve compliance and auditing
C. Speed up authentication
D. Reduce CPU load

Q34. Which NPS feature supports role-based network access?
A. Quotas
B. Group membership conditions
C. DNS filtering
D. IPAM scopes

Q35. Which scenario requires multiple NPS servers?
A. Single Wi-Fi AP
B. High availability and load balancing
C. Small office network
D. Standalone VPN

Q36. Why is UDP used by RADIUS instead of TCP?
A. Better encryption
B. Lower overhead and faster response
C. Reliable delivery
D. Firewall compatibility

Q37. Which NPS integration improves zero-trust security?
A. DHCP
B. Azure MFA

C. DNS
D. WINS

Q38. Which attack targets weak RADIUS shared secrets?
A. Pass-the-Hash
B. Brute-force attack
C. Golden Ticket
D. DNS poisoning

Q39. Why should default NPS policies be reviewed or removed?
A. Improve UI
B. Prevent unintended access
C. Reduce storage
D. Increase speed

Q40. Which enterprise best practice improves NPS security posture?
A. Shared secrets reused everywhere
B. Certificate-based auth with MFA
C. Disable accounting
D. Allow all RADIUS clients