☑ SECTION A — EASY (10 MCQs)

Q1. VLANs operate at which OSI layer?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 4

Q2. The purpose of VLANs is to:

A. Increase switch CPU
B. Create broadcast domains
C. Increase routing loops
D. Disable switching

Q3. Which command is used to assign a port to a VLAN on a Cisco switch?

A. switchport vlan add
B. vlan-port assign
C. switchport access vlan <id>
D. vlan port mode access

Q4. Port security is used primarily to:

A. Increase switching speed
B. Restrict MAC addresses on a port
C. Enable routing
D. Configure DNS

Q5. What is the default port security violation mode?

A. Shutdown
B. Restrict
C. Protect
D. Bounce

Q6. Standard IPv4 ACLs filter traffic based on:

A. Source IP only
B. Destination IP only
C. TCP port only
D. MAC address

Q7. Extended ACLs should be placed:

A. Close to the destination
B. On any router
C. Close to the source
D. On switches only

Q8. RADIUS uses which protocol/port by default for authentication?

A. TCP 22
B. UDP 1812
C. TCP 1813
D. UDP 2049

Q9. TACACS+ encrypts:

A. Only passwords
B. Only usernames
C. Entire payload
D. No data

Q10. APIC-EM Path Trace is used to:

A. Create VLANs
B. Simulate end-to-end packet flow
C. Check RAM usage
D. Configure DHCP

☑ SECTION B — MEDIUM (15 MCQs)

Q11. A trunk port uses which protocol to tag VLAN traffic?

A. RIP
B. STP
C. 802.1Q
D. VTP

Q12. What happens when port security detects more MAC addresses than allowed?

A. Port speed reduces
B. Port shuts down

C. MAC table resets
D. VLAN is deleted

Q13. Which violation mode does NOT send SNMP notifications?

A. Shutdown
B. Restrict
C. Protect
D. Both Protect & Shutdown

Q14. The command to enable sticky MAC addresses is:

A. switchport security sticky
B. switchport port-security mac sticky
C. mac sticky enable
D. switchport secure sticky

Q15. IPv6 ACLs differ from IPv4 ACLs because:

A. IPv6 ACLs do not support named ACLs
B. IPv6 ACLs require global unicast addresses
C. IPv6 ACLs do not use wildcard masks
D. IPv6 ACLs cannot filter ICMP

Q16. A basic method of device hardening includes:

A. Enabling unused services
B. Allowing telnet only
C. Using strong passwords
D. Leaving default credentials

Q17. Which AAA model requires user authentication for every command executed?

A. RADIUS
B. Local login
C. TACACS+
D. PAP

Q18. An ACL applied inbound on an interface filters:

A. Only routed traffic
B. Traffic before routing decision
C. Traffic after routing
D. Only broadcast traffic

Q19. In APIC-EM Path Trace, an ACL drop is shown as:

A. Green line
B. Grey dotted line
C. Red mark
D. Blue arrow

Q20. To verify active port security entries, which command is used?

A. show mac address-table
B. show port-sec
C. show running-config
D. show port-security address

Q21. A common access layer threat mitigated by DHCP snooping is:

A. MAC flooding
B. ARP spoofing
C. Rogue DHCP servers
D. VLAN hopping

Q22. VTP transparent mode allows:

A. Only server updates
B. Full VLAN synchronization
C. Local VLAN creation only
D. Trunk blocking

Q23. IPv4 Wildcard mask 0.0.0.255 means:

A. Match all bits
B. Match last 8 bits
C. Ignore first 24 bits
D. B & C both

Q24. RADIUS separates which components?

A. Authentication and authorization
B. Authentication and accounting
C. Authorization and accounting
D. None (combined operation)

Q25. The recommended place to apply standard ACLs is:

A. Closest to the source
B. Closest to the destination
C. On switching domain
D. On trunk ports

☑ SECTION C — HARD (15 MCQs)

Q26. A port configured with `switchport mode access` + `switchport voice vlan` supports:

A. Trunking only
B. Two VLANs (data + voice)
C. Only voice VLAN
D. Multiple trunk links

Q27. Dynamic ARP Inspection relies on which database?

A. MAC table
B. DHCP snooping binding table
C. ARP cache
D. Routing table

Q28. A port with both sticky MAC and maximum 1 MAC allowed receives a second MAC. What occurs in "restrict" mode?

A. Port shuts down
B. Traffic from the unknown MAC is dropped
C. Sticky table resets
D. VLAN becomes inactive

Q29. APIC-EM Path Trace ACL analysis fails when:

A. Switch does not support SNMP
B. Device is unreachable
C. VLAN mismatch occurs
D. ACL has no entries

Q30. Which statement is TRUE about IPv6 ACL implicit rules?

A. IPv6 ACL ends with an implicit permit any
B. IPv6 ACLs have no implicit deny

C. IPv6 ACLs end with implicit deny every protocol
D. IPv6 ACL ends with deny tcp only

Q31. Hardening a device by disabling unused interfaces is important because:

A. It reduces redundancy
B. It prevents unauthorized access points
C. It stops all broadcast storms
D. It saves device memory

Q32. TACACS+ uses which transport protocol?

A. UDP
B. TCP
C. SCTP
D. Both TCP and UDP

Q33. Which access-list entry would block all IPv4 traffic from 192.168.5.0/24?

A. deny ip 192.168.5.0 0.0.0.255 any
B. deny any any
C. permit ip any 192.168.5.0
D. deny tcp any any

Q34. VLAN hopping attack can be mitigated by:

A. Enabling DTP
B. Forcing ports to access mode
C. Disabling RSTP
D. Clearing MAC table

Q35. A dual-stack ACL must:

A. Combine IPv4 and IPv6 in one ACL
B. Use separate ACLs for IPv4 and IPv6
C. Use only IPv6
D. Be applied outbound only

Q36. Which port receives frames destined for all hosts within a VLAN?

A. Trunk port
B. Routed port
C. Access port
D. Protected port

Q37. To inspect detailed packet flow in APIC-EM Path Trace, device must support:

A. SNMP + CLI
B. Telnet only
C. HTTP only
D. CDP only

Q38. An attacker floods CAM table causing switch to broadcast traffic. This attack is:

A. DHCP spoofing
B. ARP poisoning
C. MAC flooding
D. VLAN hopping

Q39. AAA authorization determines:

A. Who the user is
B. What the user is allowed to do
C. What device stores credentials
D. How logs are collected

Q40. Which AAA deployment provides the highest security for command-level control?

A. RADIUS
B. Local user accounts
C. TACACS+ central server
D. Simple password authentication