Network Operations

CompTIA Network+ certification exam, N10-009

19% of the exam · 5 exam objectives · N10-009

Domain 3 is how a network is run day to day: documenting it and controlling changes, monitoring it, planning for disaster, providing addressing, name resolution and time, and reaching devices to manage them safely.

You should be able to: A company backs up its database every 6 hours but says it can lose only 1 hour of data, and its monitoring uses SNMPv2c. Which disaster recovery target is missed, and what SNMP change would protect the monitoring traffic?

Every exam objective: the key point and the trap

3.1 Explain the purpose of organizational processes and procedures.

Physical diagrams show where devices and cables are; logical diagrams show how traffic flows, with subnets, VLANs and routing. Rack diagrams show each device's position in a rack, and cable maps show where each run starts and ends.

Trap: Confusing EOL with EOS: a product can be end-of-life (no longer sold) and still supported for years; the security risk begins at end-of-support, when patches stop.

3.2 Given a scenario, use network monitoring technologies.

SNMP: managers poll agents on UDP port 161 and agents send traps to managers on UDP port 162. The management information base (MIB) defines the objects a device exposes.

Trap: Thinking a long community string makes SNMPv2c secure: it still crosses the network in clear text. Only SNMPv3 adds authentication and encryption.

3.3 Explain disaster recovery (DR) concepts.

Recovery point objective (RPO): the most data the business can lose, measured in time; it sets backup frequency.

Trap: Swapping RPO and RTO: RPO is about data (how far back you go), RTO is about time (how long until you are back).

3.4 Given a scenario, implement IPv4 and IPv6 network services.

DHCP (UDP ports 67 and 68) leases addresses from a scope for a lease time. Exclusions keep addresses out of the pool, reservations tie an address to a MAC address, and options deliver settings such as the gateway and DNS servers.

Trap: Believing DNSSEC encrypts DNS: it only signs answers for integrity. Encryption of queries is DoH or DoT.

3.5 Compare and contrast network access and management methods.

A site-to-site VPN joins two networks through their gateways and stays up; users need no client.

Trap: Assuming a split tunnel is more secure: it saves bandwidth, but traffic outside the tunnel is not inspected by the company.

Key terms

IPAM: Internet Protocol Address Management

SLA: Service-level Agreement

EOS: End-of-support

SNMP: Simple Network Management Protocol

MIB: Management Information Base

SIEM: Security Information and Event Management

RPO: Recovery Point Objective

RTO: Recovery Time Objective

SLAAC: Stateless Address Autoconfiguration

DNSSEC: Domain Name System Security Extensions

ExamDragon, examdragon.com/netplus. Independent exam preparation, written in our own words to the N10-009 exam objectives. CompTIA and Network+ are trademarks of CompTIA, Inc.