CLASS E

1. Identify the appropriate type of DNS zone that should be configured on the Kumasi DNS server to replicate and mirror the primary zone hosted in Accra. Provide a justification for your choice.

The appropriate type is a **secondary zone**. This allows the Kumasi server to maintain a read-only copy of the primary zone from Accra, providing redundancy for name resolution in case of connectivity issues or outages at the head office. It ensures local queries are handled efficiently without overloading the primary server, while automatically syncing changes via zone transfers.

2. Explain the step-by-step procedure to configure this DNS zone on the Kumasi server, ensuring it functions as intended.

To configure a secondary zone on the Kumasi server:

- Open DNS Manager on the Kumasi Windows Server.
- In the console tree, right-click **Forward Lookup Zones** and select **New Zone**.
- In the New Zone Wizard, click **Next**, then select **Secondary zone**.
- Enter the zone name (e.g., the domain name hosted in Accra, such as company.local).
- On the Master DNS Servers page, enter the IP address of the primary server in Accra, click **Add**, then **Next**.
- Click **Finish**. The zone will transfer data from the primary if transfers are allowed.

3. What measures would you implement to secure zone transfers between the primary DNS server in Accra and the secondary server in Kumasi?

To secure zone transfers:

- On the primary server in Accra, right-click the zone in DNS Manager, select **Properties > Zone Transfers tab**.
- Select **Allow zone transfers** and choose **Only to the following servers**, then add the IP address of the Kumasi secondary server.
- Enable DNSSEC for signed zones to ensure data integrity.
- Use TSIG (Transaction Signature) keys for authentication between servers.
- Restrict transfers to TCP port 53 and implement firewall rules to allow only from trusted IPs.

4. When a new host record is added to the primary zone, explain how the secondary zone is updated. Additionally, describe the function of the SOA (Start of Authority) record in this process.

When a new host record is added to the primary zone, the secondary zone updates via zone transfers. The primary server notifies the secondary (using NOTIFY messages) when changes occur, prompting the secondary to check the SOA serial number. If the serial is higher, the secondary requests a transfer (AXFR for full or IXFR for incremental).

The SOA record defines the authoritative server for the zone and includes:

- Serial number: Increments with changes, triggering updates.
- Refresh interval: How often the secondary checks for updates.
- Retry interval: Time between retries if a refresh fails.
- Expire interval: When the secondary stops serving the zone if unreachable.
- Minimum TTL: Default TTL for records.

5. Outline the firewall configurations (e.g., ports and protocols) required to support successful and secure zone transfers between the two offices.

Firewall rules for zone transfers:

- Allow inbound and outbound traffic on **TCP port 53** (for zone transfers, as they can exceed UDP limits).
- Allow **UDP port 53** for standard DNS queries (though transfers prefer TCP).
- Restrict rules to specific source/destination IPs (e.g., only between Accra and Kumasi servers).
- For notifications, ensure UDP/TCP 53 is open bidirectionally.
- Use stateful firewalls to allow established connections.

Class F

1. Describe the step-by-step process to install the DNS Server role using Server Manager in Windows Server 2019.

(See Class C, Task 1 for identical steps.)

2. After role installation, explain how to create a Forward Lookup Zone for the domain logistics.local.

(See Class C, Task 2 for identical steps.)

3. Define an A (Host) record. Create an A record to associate the hostname server01.logistics.local with the IP address 192.168.5.10.

An A (Host) record maps a hostname to an IPv4 address.

(See Class C, Task 3 for creation steps.)

4. What is the purpose of a Reverse Lookup Zone? Explain how to configure one for the subnet 192.168.5.0/24.

(See Class C, Task 4 for purpose and steps.)

5. Explain the command to test DNS name resolution from a client machine using nslookup or ping.

(See Class C, Task 5 for verification steps using nslookup and ping.)

Class B

1. What diagnostic tools can be used to identify the cause of name resolution failures?

Diagnostic tools for name resolution failures include:

- **nslookup**: Queries DNS servers for records and tests resolution.
- **dig**: Provides detailed DNS lookup information (Linux/Unix, but available on Windows via tools).
- **ipconfig /displaydns** and **/flushdns**: Views and clears local DNS cache.
- **ping**: Tests basic resolution and connectivity.
- **dcdiag** or **nltest** (for AD environments): Checks domain-specific DNS.
- **Wireshark**: Captures network traffic for DNS packets.

2. How do you verify that DNS records exist and are properly configured in the zone?

To verify DNS records:

- On a client or server, open Command Prompt and type **nslookup**.
- Set the server if needed: **server <DNS_server_IP>**.
- Query the record: Type the hostname (e.g., server01.logistics.local) or specify type: **set type=A**, then the hostname.
- For full zone listing (if allowed): **ls -d <zone_name>**, but this requires zone transfer permissions.
- Check for expected IP or errors like "Non-existent domain."

3. What could cause clients to use external DNS instead of the internal DNS server?

Possible causes:

- Client DNS settings (via DHCP or manual) point to external servers (e.g., ISP or public like 8.8.8.8) instead of internal ones.
- Internal DNS forwarders are misconfigured, routing queries externally.
- Split-brain DNS issues where internal and external namespaces conflict.
- Network policies or VPNs overriding local DNS.
- Cache poisoning or stale cache directing to external resolutions.

4. How do you use the ipconfig /displaydns and ipconfig /flushdns commands to test local DNS.

To test local DNS:

- Open Command Prompt as administrator.
- Type **ipconfig /displaydns** to view the contents of the local DNS resolver cache, showing resolved hostnames and IPs (useful for checking if stale entries cause issues).
- If needed, type **ipconfig /flushdns** to clear the cache, forcing fresh queries to the DNS server.
- After flushing, test resolution again with ping or nslookup to verify from the server.

Class A/D

1. Which type of DNS zone should be created in the Kumasi office to mirror the primary zone in Accra? Justify your answer.

(See Class E, Task 1 for identical answer: Secondary zone for redundancy and mirroring.)

2. Describe the process of configuring a DNS zone in the Kumasi branch.

(See Class E, Task 2 for identical steps.)

3. How would you ensure zone transfers are secure between the primary and secondary DNS servers?

(See Class E, Task 3 for identical measures.)

4. If the primary zone is updated with a new host record, how does the secondary zone get updated? What is the role of the SOA record?

(See Class E, Task 4 for identical explanation.)

5. What firewall rules might you need to configure to allow zone transfers between the offices?