**1. An IT administrator installs new DNS name servers that host the company's mail exchanger (MX) records and resolve the web server's public address. To secure the zone transfer between the DNS servers, the administrator uses only server ACLs. What is the issue with this approach? (5 points)**

**Answer:** Just using Access Control Lists (ACLs) to protect DNS zone transfers isn't secure enough. While ACLs can restrict which DNS servers are allowed to participate in zone transfers, they do not provide any cryptographic authentication or data integrity checks. This means that even if unauthorized servers are blocked, an attacker could still potentially spoof a legitimate server and intercept or modify zone transfer data during transmission.

This puts the DNS data at risk — someone could change it or pretend to be a trusted source, causing attacks like DNS poisoning or spoofing. Zone transfers that are not properly authenticated may result in the replication of inaccurate or malicious DNS records, compromising the integrity of the entire DNS system.

A better way to protect zone transfers is by using TSIG (Transaction Signature), which confirms identity and keeps data intact. TSIG uses shared secret keys and HMAC (Hash-based Message Authentication Code) to authenticate DNS servers and ensure that the data transferred has not been altered. This provides both authentication and data integrity, which are critical for maintaining a secure DNS infrastructure.

In conclusion, using only ACLs does not protect against data tampering or identity spoofing. A more secure approach would involve combining ACLs with TSIG to ensure secure and authenticated zone transfers between DNS servers.

**2. A security team determines that someone from outside the organization has obtained sensitive information about the internal organization by querying the company's external DNS servers. How should you, as the security manager, address the problem? (5 points)**

**Answer:** As the security manager, I would immediately take action to limit the exposure of internal information. The first step would be to implement a Split DNS setup, creating two separate DNS environments: one for internal users containing sensitive records, and another for external users containing only public-facing resources like the company's web and mail servers. This prevents external users from accessing internal network details.

In addition, I would restrict DNS zone transfers by using Access Control Lists (ACLs) and TSIG (Transaction Signature) to ensure that only authorized DNS servers can exchange zone information securely. I would also conduct a full audit of the external DNS server, removing any unnecessary internal records that do not need to be exposed publicly.

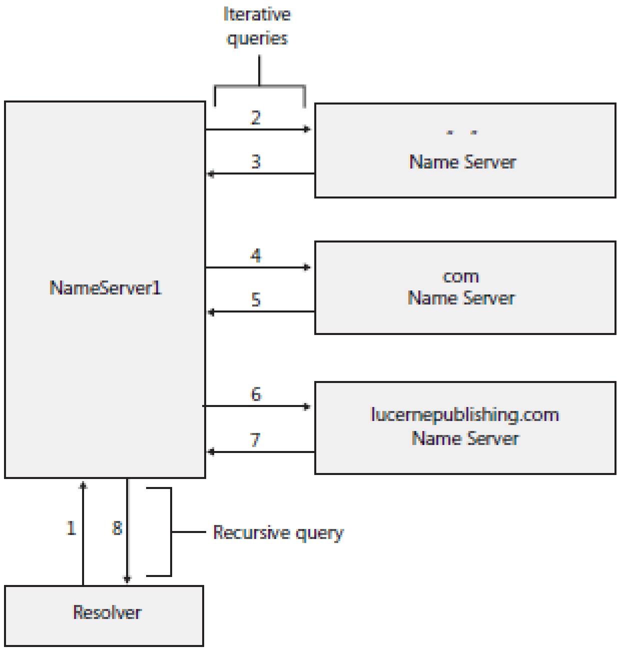
Finally, I would enable DNS query logging and monitoring to detect any suspicious or abnormal query behavior in the future. These combined steps would protect the organization from further information leakage and strengthen the overall security of the DNS infrastructure.

**3. If a computer needs to resolve a DNS name, what is the first method it attempts to use? (5 points)**
**Answer**: When a device wants to find the IP for a domain name, it first checks locally before asking a DNS server.

- **Local Cache:** The very first place a computer checks is its own local DNS cache. This cache stores previously resolved DNS lookups, so if the name has been resolved recently, the computer can retrieve the IP address from its cache, which is the fastest method. This local cache can exist within the operating system itself, and also within the web browser being used.
- If the information is not in the local cache, the computer then queries the DNS server that is configured within its network settings.

The first place that a computer attempts to resolve a DNS name is within its own local cache.

**4. Describe, in detail, the DNS query steps depicted by the following: (5 points)**



**Answer:** The DNS query steps depicted in the image detail the process of resolving a domain name using a combination of recursive and iterative queries. Below is a detailed explanation of each step:

**Step 1:** Recursive Query from Resolver to NameServer1

The resolver sends a recursive query to NameServer1, requesting the IP address for the domain lucernepublishing.com. A recursive query means the resolver expects NameServer1 to handle all subsequent queries and return the final result.

**Step 2:** Iterative Query to Root Name Server

NameServer1 sends an iterative query to the root name server (.) to find out which name server is authoritative for the .com top-level domain (TLD). Iterative queries involve asking one server at a time for information.

**Step 3:** Response from Root Name Server

The root name server replies with the address of the .com TLD name server, indicating where further queries should be directed.

**Step 4:** Iterative Query to .com Name Server

NameServer1 sends an iterative query to the .com TLD name server, asking for the authoritative name server for lucernepublishing.com.

**Step 5:** Response from .com Name Server

The .com name server responds with the address of the authoritative name server for lucernepublishing.com.

**Step 6:** Iterative Query to lucernepublishing.com Name Server

NameServer1 sends an iterative query to the lucernepublishing.com name server, requesting the IP address associated with the domain.

**Step 7:** Response from lucernepublishing.com Name Server

The lucernepublishing.com name server replies with the requested IP address.

**Step 8:** Final Response to Resolver

NameServer1 returns the IP address of lucernepublishing.com to the resolver, completing the recursive query process.

**5. Complete this sentence: (5 points)**
If the DNS Server cannot resolve a query from a DNS resolver through authoritative or cached data, the DNS server will attempt to resolve the query by___ **issuing iterative queries starting from the root name servers** ___.

**6. You install the DNS Service (or Daemon) on a computer. You do not create any zones on this computer. The DNS Server Service (Daemon) is set to start automatically. Is this considered a valid DNS Server configuration? If not, why not? If yes, what kind of DNS Server is this? (5 points)**

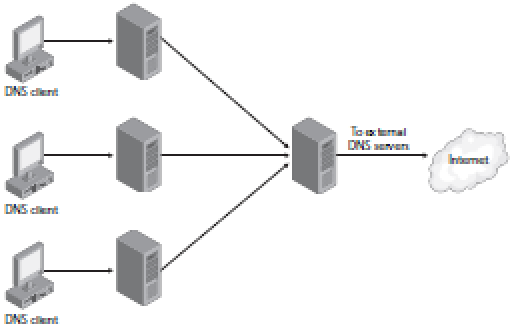
**Answer:** Yes, this is considered a valid DNS server configuration, even though no DNS zones are created. In this case, the server functions as a caching-only DNS server.

A caching-only DNS server does not host any zones and is not authoritative for any domain. Instead, it simply receives DNS queries from clients, forwards them to other DNS servers, and stores (or caches) the responses it receives. Once the server caches a DNS response, it can respond to the same query much faster the next time, without needing to contact external servers again.

This type of server is useful in networks where DNS name resolution is needed, but there is no requirement to manage or host DNS records internally. It is especially beneficial in environments with limited bandwidth or slow WAN connections, as caching improves performance and reduces external DNS traffic over time.

Even though it doesn't contain any zones or authoritative data, the DNS service running on this machine still provides value by acting as an efficient, local resolver. Therefore, it is a valid and practical configuration, typically used to enhance resolution speed, reduce bandwidth usage, and improve reliability in local or branch office networks.

**7. Describe what kind of configuration is depicted here and justify your response (5 points)**



**Answer:** This setup shows how DNS forwarding works inside a company's network.

In this setup, DNS clients send their name resolution requests to an internal DNS server, which acts as a forwarder. This internal DNS server does not attempt to resolve the DNS queries on its own through iterative queries across the public DNS hierarchy. Instead, it forwards the queries to external DNS servers, typically provided by an ISP or a cloud provider, for resolution.

**Justification:**

- The image shows multiple DNS clients forwarding their DNS queries to a central internal DNS server.
- That internal server is shown forwarding requests out to the Internet, indicating it's not authoritative and is not resolving names by itself; it's forwarding them.
- This setup improves security, because only the internal DNS server communicates with external DNS servers. It also reduces bandwidth usage and improves performance through caching.
- This is a best practice in enterprise environments to control and monitor external DNS traffic, and it enables the organization to implement features such as query logging, DNS filtering, and content control.

This is a DNS forwarder configuration, where an internal DNS server handles queries from clients and forwards unresolved queries to external DNS servers, enhancing security, performance, and administrative control.

**8. When would a DNS server contact a root server? (4 points)**

**Answer:** A DNS server contacts a root server when it receives a query for a domain name that it cannot resolve from its local cache or authoritative zone data, and no forwarder is configured. In such cases, the DNS server begins the iterative resolution process by first contacting one of the 13 root DNS servers to determine which Top-Level Domain (TLD) server (e.g., .com, .org) can provide further information about the queried domain.

This typically occurs when:

- The DNS query is for a domain the server has never seen before.
- The server's cache has expired or been cleared.
- No conditional or default forwarders are set.

Contacting the root server is the first step in resolving an unknown domain name using the standard DNS hierarchy.

**9. If a DNS server contacts a root server to resolve the name *www.touro.edu* and the root server cannot answer the query, how does the original server know which server to query next? (4 points)**

**Answer:** When a DNS server contacts a root server to resolve www.touro.edu, the root server does not provide the final answer but returns a referral to the appropriate Top-Level Domain (TLD) Name Server.Specifically:

- The DNS server queries a root name server for www.touro.edu.
- The root server does not have the exact answer, but it knows which TLD name server (for .edu) is responsible.
- The root server replies with a referral, directing the DNS server to query the .edu TLD name server.
- The DNS server then queries the .edu name server, which provides a further referral to the authoritative name server for touro.edu.

Finally, the authoritative name server for touro.edu responds with the IP address of www.touro.edu.

**10. Complete each of the following sentences with the appropriate phrase: (6 points)**

a. A DNS zone is a contiguous ___ **portion of a namespace for which a server is authoritative** ___.

b. A DNS resolver is a service that uses the _**DNS**__ protocol to ___ **convert domain names into IP addresses by querying DNS servers _____**.

**11. What record must be added to a DNS zone file to alias a host to another name? (3 points)**

**Answer:** The record that must be added to a DNS zone file to alias a host to another name is a CNAME record (Canonical Name record). A CNAME record creates an alias, pointing one domain name to another domain name. This is different from an A record, which points a domain name to an IP address.

You work as a network support specialist for touro.edu. You are planning to deploy a new server in a branch office to improve name resolution times.

**12. You work as a network support specialist for *touro.edu*. You are planning to deploy a new server in a branch office to improve name resolution times:**

a. **There are no administrators at the branch office. You want to deploy a DNS server that will not require any administration but will help resolve the queries of computers on the Internet. What kind of DNS server should you deploy and why? (4 points)**

**Answer**: I deploy a caching-only DNS server at the branch office. The reason is:

- A caching-only DNS server does not require administration because it does not host any authoritative DNS zones.
- It stores responses to DNS queries temporarily in its cache, allowing it to quickly respond to repeated queries.
- Since there are no administrators at the branch office, this setup reduces maintenance needs while improving name resolution times for users.

b. **You also want the new DNS server to be able to resolve names on the internal touro.edu network at the main office. How can you achieve this without hosting a zone called touro.edu on the branch office network? (4 points)**
**Answer**: To resolve internal names for touro.edu without hosting the zone locally, you should configure the DNS server to use conditional forwarding. How to achieve this:

- Set up conditional forwarders on the branch DNS server to forward touro.edu queries to the main office's DNS server (which hosts the authoritative touro.edu zone).
- This allows the branch office DNS server to resolve internal names without needing to store or manage the touro.edu zone itself.

**13. What kind of files are the DNS zone data stored in? (4 points)**

**Answer:** DNS zone data is stored in zone files, which are standard text files containing mappings between domain names and IP addresses. These files usually have a .dns extension and include various Resource Records (RRs), such as A, AAAA, CNAME, MX, SOA, and NS records, that define the structure and information for the domain.

**14. Cached DNS records stay alive in the server cache until one of the three (3) conditions occur? Name two (2) of these conditions. (6 points)**

**Answer:** When discussing how long DNS records stay in a server's cache, the most important factor is the Time To Live (TTL). Therefore, one of the main conditions is:

**TTL (Time To Live) expiration:**

- Each DNS record has a TTL value, which specifies how long (in seconds) the record can be cached.
- When the TTL expires, the cached record is discarded, and the DNS server must perform a new lookup if the same query is received again.

**Here are the other two main conditions.**

- Manual cache flushing: System administrators can manually clear the DNS cache on a server. This is often done to ensure that the server retrieves the most up-to-date DNS records.
- Cache size limitations: DNS servers have limited cache sizes. When the cache is full, older records may be evicted to make room for new ones. The algorithm used to determine which records to evict can vary.

**15. Describe the purpose (and significance) of the Serial Number parameter in the Start of Authority (SOA) of the zone file (5 points).**

**Answer:** The Serial Number parameter in the Start of Authority (SOA) record of a DNS zone file serves several crucial purposes:

- Version Control: It acts as a version identifier for the zone file, incrementing each time changes are made to the zone's records.
- Change Detection: Secondary DNS servers use this number to determine if their copy of the zone data is outdated. When they detect a higher serial number on the primary server, they initiate a zone transfer to update their records.
- Synchronization: It ensures that all authoritative name servers for a domain have the most current data, maintaining consistency across the DNS infrastructure.
- Efficient Updates: By checking the serial number, secondary servers can quickly determine if they need to perform a full zone transfer, reducing unnecessary network traffic and server load.
- Change Tracking: Administrators can use the serial number to track when the last modification was made to the zone file, often using a date-based format (e.g., YYYYMMDDNN) for easy reference.

The significance of the Serial Number lies in its role in maintaining the integrity and consistency of DNS data across distributed systems, ensuring efficient propagation of DNS changes, and facilitating proper zone transfers between primary and secondary DNS servers.

**16. Why does a stub zone improve name resolution when it is implemented across Windows Server DNS namespaces? (6 points)**

**Answer:** A stub zone improves name resolution across Windows Server DNS namespaces because it stores only essential information about another zone — specifically, the SOA (Start of Authority), NS (Name Server), and A (Address) records of the authoritative servers for that zone. By maintaining this minimal but critical information, a stub zone allows a DNS server to quickly locate and contact the correct authoritative DNS servers without needing to perform a full iterative search across the DNS hierarchy.

**This leads to several benefits:**

- Faster name resolution for queries involving external or delegated domains.
- Reduced DNS query traffic across the network, because the DNS server already knows where to send queries directly.
- Automatic updates to the list of authoritative servers, meaning if the authoritative DNS servers change, the stub zone will automatically stay up-to-date without manual intervention.

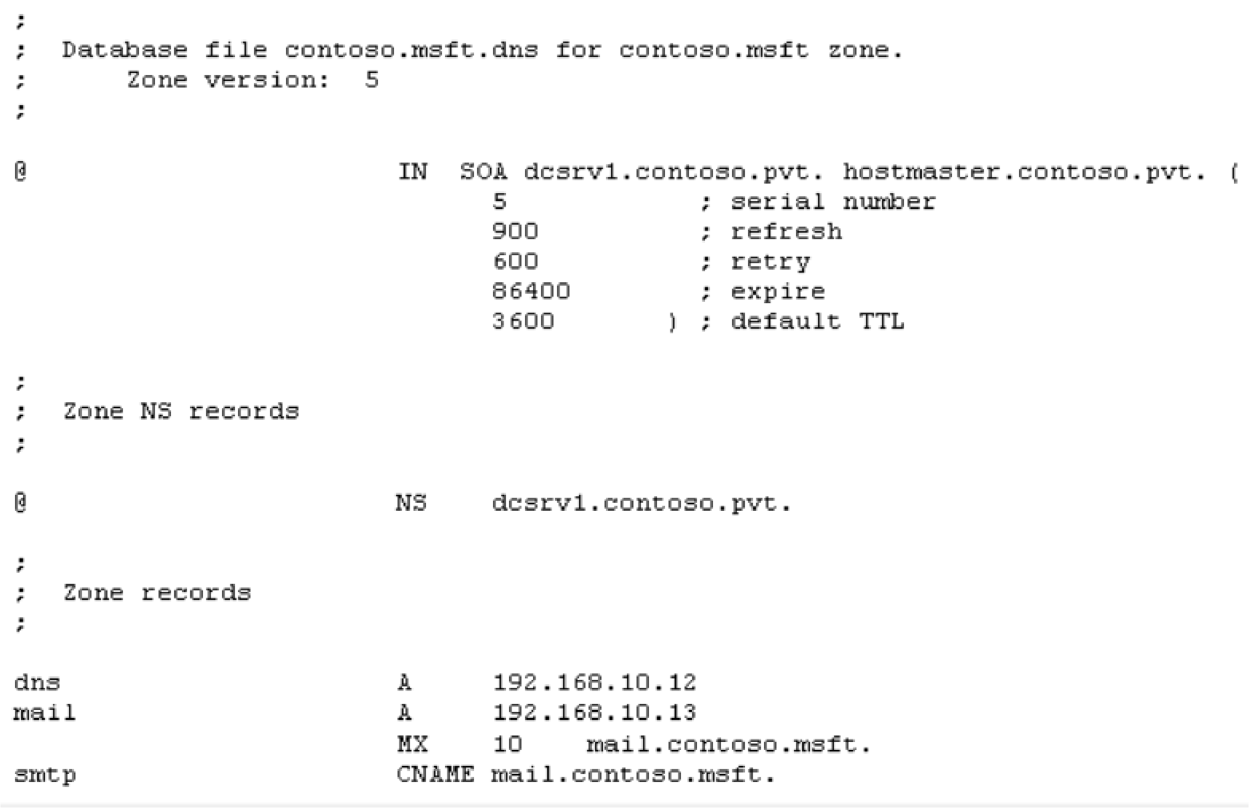
In short, stub zones enhance efficiency, maintain better accuracy in name resolution, and simplify DNS administration across distributed Windows Server DNS environments.

**17. One of the parameters in the SOA record is Serial Number. Describe what happens when you increment the serial number (5 points)**

**Answer:** When I increment the Serial Number in the SOA (Start of Authority) record, I am signaling that changes have been made to the DNS zone file. The Serial Number acts like a version control system for DNS data. Secondary (slave) DNS servers periodically check the SOA record of the primary (master) server. When they notice that the Serial Number is higher than the one they currently have, they recognize that the zone has been updated.

As a result, the secondary servers will automatically initiate a zone transfer to pull the latest copy of the zone from the primary server. This ensures that all DNS servers stay synchronized with the most up-to-date information. Keeping the Serial Number properly updated is important because it helps maintain consistency across the DNS infrastructure, reduces errors in name resolution, and ensures users always receive accurate responses when accessing network resources. By incrementing the Serial Number, I am making sure that the network operates smoothly and that DNS updates are efficiently and correctly distributed across all DNS servers.

**18. You manage a DNS server running Windows Server OS. You are troubleshooting a problem with loading the zone file shown below: (6 points)**



```
;
;  Database file contoso.msft.dns for contoso.msft zone.
;      Zone version:  5
;

@                        IN  SOA dcsrv1.contoso.pvt. hostmaster.contoso.pvt. (
                               5            ; serial number
                               900          ; refresh
                               600          ; retry
                               86400        ; expire
                               3600       ) ; default TTL

;
;  Zone NS records
;

@                        NS    dcsrv1.contoso.pvt.

;
;  Zone records
;

dns                      A     192.168.10.12
mail                     A     192.168.10.13
                         MX    10    mail.contoso.msft.
smtp                     CNAME mail.contoso.msft.
```

What is the host name of the primary DNS server?

**Answer:** The host name of the primary DNS server is dcsrv1.contoso.pvt.

I found this information in the SOA (Start of Authority) record at the top of the zone file. The SOA record always begins with the primary DNS server's host name, followed by the responsible party's email address and other parameters such as serial number, refresh, retry, and TTL values. In this case, the SOA line is:

**IN SOA dcsrv1.contoso.pvt. hostmaster.contoso.pvt. ( ...**

This indicates that dcsrv1.contoso.pvt. is the primary (authoritative) DNS server for the contoso.msft zone, and it is responsible for managing and updating the zone file.

**19. You create a private domain, *touro.pvt* for testing DNS name resolution scenarios. You want clients on your internal network to be able to resolve names in the *touro.pvt* domain, but you do not want to modify client configuration. The *touro.pvt* domain does not allow zone transfers. How should you configure your DNS servers? (5 points)**

a. Create a conditional forwarder
b. Create a reverse lookup zone
c. Create a forward lookup zone
d. Create a stub zone

**Answer: a. Create a conditional forwarder**

To meet the requirements of resolving names in the touro.pvt domain without changing the DNS client configurations, I would configure a conditional forwarder on the internal DNS server. A conditional forwarder allows a DNS server to forward queries for a specific domain (like touro.pvt) directly to the DNS server that is authoritative for that domain.

This solution works well here because:

- It allows DNS clients to continue using their existing DNS settings.
- The touro.pvt zone does not allow zone transfers, so using a stub or secondary zone is not possible.
- Conditional forwarding is efficient and secure for private domains that are not accessible to the public.

By setting up a conditional forwarder, I ensure that queries for touro.pvt are resolved correctly without needing to modify each client manually.

**20. You can ping a device with an IP address but cannot use its FQDN. Describe what type of problem you are experiencing and how you'll fix it (5 points).**

**Answer:** This issue indicates a DNS name resolution problem. Since I can ping the device using its IP address, I know that network connectivity is working. However, the inability to resolve the Fully Qualified Domain Name (FQDN) means that the DNS server is failing to map the domain name to the correct IP address.

The most likely cause is that the device is missing an "A" (Address) record in the DNS zone file, or its record is not properly registered in DNS. Another possible issue could be that the DNS client is not pointing to the correct DNS server or the server's cache is outdated.

**To fix it, I would:**

- Check if the correct A record exists for the device in the DNS zone.
- Use the nslookup or dig tool to verify DNS resolution.
- Manually add or correct the A record in the DNS zone if it's missing.
- Ensure the client's DNS settings are pointing to the correct internal DNS server.
- Flush the DNS cache using ipconfig /flushdns on the client if needed.

By correcting the DNS entry or the client configuration, FQDN resolution should begin working properly.