**DV162\_17\_PAS ON DNS CONFIGURATION**

**Possible Answer Sheet**

1. What is DNS and how does it work?  
   Ans: DNS stands for Domain Name System, and It converts fully qualified names into IP addresses.  
   First User requests or enter the domain name in browser  
   Then local cache comes in and sees if it knows the IP address associated with the domain name. If found then connect to the corresponding IP address else send DNS query to DNS Resolver. This DNS resolver is usually provided by the ISP. If the resolver doesn’t have an IP address cached then it starts the process of querying one of 13 root DNS Servers.  
   The root DNS server responds to the resolver with the IP Address of the TLD servers. The Resolver query the TLD Servers and respond to the IP address of the Authoritative name Servers. These Authoritative Name Servers usually consist of organizations that own domain or DNS hosting providers.  
   The Authoritative Name Server then checks the Domain Name in RRL (Resource Record Lookup) to find the DNS Record and response with the requested Information or IP Address against the domain name and resolver cache the obtained information for future use and then allowing the user to connect to the web server.
2. What is the structure of the DNS hierarchy?  
   Ans: ****
3. How can you see the translation of a domain name to an IP address?  
   Ans: Using Command **dig domainname.com** or **nslookup domainname.com**
4. How many root server clusters are there in DNS?  
   Ans: There are 13 root Server Clusters.
5. What are generic top-level domains?  
   Ans: .com, .net, .org, .edu etc are TLDs. They are managed by IANA (Internet Assigned Number Authority).
6. What is SPF  
   Ans: SPF is a sender policy framework which is responsible to prevent others from spoofing our fully qualified domain name. It consists of a list of all email servers.
7. How many servers are in a root server cluster?  
   Ans: 13
8. What is the purpose of having three different IP addresses associated with a web server?  
   Ans: Having three different IP addresses can have multiple advantages, like load balancing, if one of them is unresponsive then the other will work (Highly availability).
9. How can you check the IP addresses associated with a website if the dig command is not available?  
   Ans: We can check with the nslookup command if dig is not available.
10. What are resource records in DNS?  
    Ans: RR are the databases that keep the data of DNS Records that are used in translation of Domain Name System.
11. Why is a DNS server considered a critical resource?  
    Ans: Because if DNS server is not available then every one has to keep remembering the IP address of every website which is impractical, also risk of security as DNS servers also contain information about IP users.
12. How is a DNS server's configuration typically stored?  
    Ans: DNS server's configuration typically stored in text file.
13. What is an A record and a AAAA record in DNS?  
    Ans: A record is addresses record for IPv4 and AAAA record is addresses record for IPv6.
14. Is it possible to configure DNS using a web-based front end?  
    Ans: Yes, It is possible and is a more easy way to configure DNS.
15. How is the time to live in DNS server specified?  
    Ans: The TTL is specified in RRs (Resource Records) of DNS configuration file or Zone File. This TTL defines how long a record can be cached by DNS resolvers before they need to update from an Authoritative name server.
16. What does it mean if a device requests the IP address for a particular record?  
    Ans: Means that device is trying to find the location of a specific resource on the internet.
17. How is the same information presented in a web-based front end compared to a text file?  
    Ans: As in both cases the same configuration can be done so they are the same, but web-based front end is a more easy and error prone way to configure the DNS configurations.
18. What is the purpose of the time to live in a DNS server?  
    Ans: The time to live (TTL) in a DNS server is specifying how long an end station will remember this match between a fully qualified domain name and IP address.  
    The purpose of TTL is to make the response faster as TTL is time to keep record in local cache for some time, so if a device re-request the information or record within TTL it will get response from cache faster. Also this technique put less load on server.
19. How long is the time to live for a DNS server typically set for?  
    Ans: TTL for DNS is typically set for 15 minutes.
20. What happens when the time to live for a DNS server is up?  
    Ans: When TTL for DNS server expires then DNS resolver stops using cached information and requests updated information from Authoritative DNS servers.
21. What is an MX (Mail Exhange) record in DNS?  
    Ans: MX record is an important record in DNS where all of our emails should be delivered.  
    The MX record in the server points to mail.mydomain.name. To be able to obtain the IP address for mail.mydomain.name, we would need to look at an A record, and we will see there will be an A record for the mail.mydomain.name.
22. What other record is needed in order for an MX record to work?  
    Ans: A record or AAAA record will be needed in order for an MX record to work.
23. What is the purpose of a TXT (Text) record in DNS?  
    Ans: TXT records are used in DNS configurations to provide additional information and functionality for domain names.
24. How can the authenticity of an email be verified using a DNS txt record?  
    Ans: The Authenticity of an email can be verified using a DNS txt Record through SPF(Sender Policy Framework) and DKIM(Domain Keys Identified Mail).
25. How can you view the text records for a specific domain?  
    Ans: We can view the text records for a specific domain by using command  
    like: dig or nslookup -type=txt domainname.com.
26. What are some examples of uses for text records in a DNS server?  
    Ans: SPF, DKIM, DMARC
27. How can you view text records for a domain if dig is not available?  
    Ans: By using the command “nslookup -type=txt domainname.com”.
28. What is an SPF record in DNS?  
    Ans: SPF is a sender policy framework and it contains a list of all of the email servers that are authorized to send messages using your fully qualified domain name.
29. How does an SPF record help to prevent others from spoofing a domain?  
    Ans: SPF record confirm the email coming from an authorize host by use of list of all email servers that are authorized to send messages using fully qualified domain name.
30. What is a DKIM record in DNS?  
    Ans: DKIM is stand for Domain Keys Identified Mail, A DKIM record is a specialized DNS TXT record that stores the public key used to verify an email's authenticity.
31. How is the public key for a DKIM record stored in DNS?  
    Ans: In Text Record of DNS server.
32. How do you configure a DKIM record in a web-based front end?  
    Ans: We give the Host name, provide the public key in content and TTL usually 15 minutes of web-based front end.
33. What is DMARC in DNS?  
    Ans: DMARC stands for Domain-Based Message Authentication, Reporting, and Conformance. It prevents unauthorized email use (Spoofing). It is an extension of SPF and DKIM. Due to this DMARC the unauthorized sender mail is sent to spam as it can accept all mails or can reject entirely.
34. What can you specify in a DMARC record in DNS?  
    Ans: We can specify what to do with message or mail and where to send the mail i.e to send in spam folder or quarantine folder.
35. How does DMARC work with SPF and DKIM?  
    Ans: DMARC builds on SPF and DKIM to provide additional email authentication and reporting capabilities. DMARC policies are published as DNS TXT records.  
    With DMARC, domain owners can specify how recipients should handle emails that fail SPF or DKIM authentication. DMARC policies can instruct recipients to accept, quarantine, or reject such emails.  
    DMARC also enables domain owners to receive reports from recipients about email authentication results, allowing them to monitor and analyze email traffic and identify potential issues.
36. What can you do with the report generated by a DMARC record?  
    Ans: We can gain valuable insights into your email traffic, identify and address potential security risks, and ultimately improve the overall security of your email domain.
37. How does a mail server use a DMARC record?  
    Ans: Mail servers can take appropriate actions to handle emails that fail authentication, helping to reduce spam, prevent spoofing attempts, and ultimately improve email security. The reports generated by DMARC further empower domain owners to gain insights and refine their email authentication strategy.
38. How do you add a DMARC record in DNS?  
    Ans: Adding a DMARC record to your DNS involves creating a TXT record with specific information according to the DMARC policy we want to implement.  
    Steps: 1. Log in to DNS Management.  
     2. Create a new TXT record file.  
     3. Configure TXT Record file values.  
     4. Save and wait (Sometime Long Wait to see the effect)
39. What does the DNS server have  
    Ans: DNS servers have large databases that contain information about fully qualified domain names and associating with specific IPs.