Q1: What are types of DNS servers?

Ans: There are three types of DNS servers that are common:

DNS Resolver:

A DNS resolver is designed to recieve DNS queries, it is also responsible for tracking the IP address for that host name.

DNS Root Server

The DNS root server extracts the top level Domain from the user's query - for example, www.google.com provides details for the .com TLD name server.

Authorative DNS:

Higher level servers in the DNS define which DNS server is the authorative server - for a specific hostname; Basically it holds up-to date information for the hostname.

Q2: What kind of information is stored on DNS?

Ans: DNS servers basically stores DNS syntax

, DNS syntax is can be defined as instructions that live in authoritative servers and provide information about a domain including which IP address is associated with that domain and how to handle requests for that domain. These records consist of a series of text files written in a form that is called DNS syntax. You can say a set of DNS records like a business listing on Yelp.

Q3:- What type handles zone transfer and what information could be possibly stored on it?

Ans:- In DNS zone transfer AXFR protocol is used, which is the simplest mechanism to replicate DNS records from one server to another.

DNS server stores domain names with corresponding identities called IP addresses. It stores cache that saves your time when you revisit that website.

Q4:- Discuss the importance of DNS and the information stored on it according to the current context?

of default records or cache.

Importance:

Address records and mail exchange records need to be kept up to data to ensure that access to your domain is maintained. Incorrect records will result in sporadic or failed delivery of email of your business mail server, while incorrect record will prevent access to your website.

Ans:- The records that are stored in authoritative servers provide information about domain including the associated IP Address for each domain. It is really important and Professional for all the domains to have a specific set of default records or cache.

Q5: Why is it ideal for an organisation to have more then one name server?

Ans:- With other DNS the load on primary DNS gets reduced and customers have a more seamless experience accessing the servers, which is something that any representable company would like to have in their bag.

Q6:- Why do you think its dangerous to transfer information without checking the client?

Ans:- Well if you are attacked then attackers install Trojan malware on user's computer, and change the local DNS setting to redirect the user to malicious sites. Many routers have default passwords vulnerabilities, attackers can take over a router and overwrite DNS setting which might affect all users connected to the router.

Q7:- Why do you think should be done to prevent such things?

Ans:- A DNS name server is a highly sensitive infrastructure that requires strong security measures.

- Watch for resolvers on your network
- Severely restrict access to a name server
- Take measures against cache Poisoning
- Immediately patch known vulnerabilities

- Separate authoritative name server from resolver.
- Restrict zone transfers.