DNS INTRO

Table Content

• What is DNS

• What are DNS Record Types

• What's the difference between ad-integrated zones, primary, secondary, forward lookup, and reverse lookup zones

• Where DNS records are stored in ad-integrated zones state, non-AD integrated zones

• The DNS resolution process, what happens when a client requests a specific DNS record

• Difference between recursive and iterative DNS queries, authoritative and non-authoritative response

What is DNS

DNS refers to a Domain Name System or Server. It is a hierarchical decentralized naming system for computers, services, or any resource connected to the internet or a private network. DNS translates human-readable domain names like example.com into machine-readable IP addresses like 10.0.0.1 required for locating and identifying devices and services worldwide.

What are DNS Record Types

1.A(Address)Record

2.AAAA(IPv6Address)Record

3.CNAME(CanonicalName)Record

4.MX(MailExchange)Record

5.TXT(Text)Record

6.NS(NameServer)Record

7.SOA(StartofAuthority)Record

8.SRV(Service)Record

9.PTR(Pointer)Record

10.CAA(CertificationAuthorityAuthorization)Record

What's the difference between ad-integrated zones, primary, secondary, forward lookup, and reverse lookup zones

◇ Primary Zone: This is the source for the DNS zone data. It holds the master copy of the zone's resource records. Changes and updates to the zone data are made on the primary DNS server, and then these changes are propagated to other DNS servers (secondary servers) through zone transfers. Primary zones can be stored in text files or Active Directory-integrated zones.

◇ Secondary Zone: A secondary zone is a read-only copy of the primary zone that is stored on a different server. The secondary zone cannot process updates and can only retrieve updates from the primary zone.

◇ AD-Integrated Zones: An -Active Directory-integrated zone is a primary DNS zone that is stored in Active Directory . It does not contain data in DNS database. This zone is very secure because all data which replication from one domain controller to another domain controller’s database encrypted form hence nobody cannot read these data.It is an authoritative primary zone in which all of the zone data is stored in Active Directory. As mentioned previously, zone files are not used or necessary.

benefits:

1- Directory replication is faster

2- Reduced Administrative Overhead

3- Security

4- Redundancy

Reference

◇ Forward Lookup Zones resolve domain names to IP addresses.

◇ Reverse Lookup Zones resolve IP addresses to domain names.

Where DNS records are stored in ad-integrated zones state, non-AD integrated zones

AD-Integrated Zones:

In Active Directory-integrated zones, DNS records are stored as part of the Active Directory database.

Non-AD-Integrated Zones:

In non-AD-integrated zones, DNS records are traditionally stored in zone files on the file system of DNS servers. These zones can be primary or secondary zones stored as text-based zone files

The DNS resolution process, what happens when a client requests a specific DNS record

1. Local DNS Cache Check:

◇ The client (like a web browser or any device) first checks its local DNS resolver cache to see if it already has the required DNS information cached. If the record is found and is still valid (not expired), the resolution process ends here, and the IP address is used for communication.

• Recursive Query to Resolver:

◇ If the information is not in the local cache or has expired, the client sends a request to its configured DNS resolver (usually provided by the ISP or a local DNS server). This query is often recursive, meaning the resolver is responsible for finding the requested information.

• Resolver Query Process:

◇ The resolver checks its own cache for the requested information. If it doesn't have the record cached or the cache is expired, it starts the resolution process by querying root name servers.

• Root Name Servers:

◇ The resolver contacts one of the root name servers (there are several of these distributed around the world) to ask for information about the Top-Level Domain (TLD) servers responsible for the domain in question (like .com, .org, etc.).

• TLD Name Servers:

◇ The root name server responds to the resolver with the information about the authoritative name servers for the TLD of the domain.

◇ The resolver then queries one of the TLD servers to get information about the authoritative name servers responsible for the specific domain (e.g., example.com).

• Authoritative Name Servers:

◇ The TLD name server responds to the resolver with the information about the authoritative name servers for the domain.

◇ The resolver finally queries one of these authoritative name servers for the specific DNS record it's seeking.

• DNS Record Response:

◇ The authoritative name server for the domain responds to the resolver with the requested DNS record (e.g., A record for IPv4, AAAA record for IPv6, etc.).

• Resolver Cache Update:

◇ The resolver sends the DNS record information back to the client and stores it in its cache for future use, speeding up subsequent requests for the same domain.

• Client's Use of IP Address:

◇ The client receives the IP address corresponding to the requested domain name and uses it to establish the desired connection, such as loading a website or accessing a service.

Difference between recursive and iterative DNS queries, authoritative and non-authoritative response

Recursive DNS Query:

◇ Recursive queries are initiated by the client (like a web browser or a local DNS resolver) requesting information from a DNS server, typically the ISP's DNS server or a local caching resolver.

◇ The DNS server receiving the recursive query is responsible for providing a complete answer to the client's query. It performs the entire DNS resolution process, querying other DNS servers hierarchically until it obtains the necessary information. It takes full responsibility for finding the requested information and returning a final answer to the client.

Iterative DNS Query:

◇ Iterative queries are made by a DNS server (resolver) to other DNS servers in the hierarchy to resolve a DNS query step by step.

◇ If the queried DNS server doesn't have the requested information in an iterative query, it responds with the best information it has available. The querying DNS server then uses that information to make subsequent queries to other DNS servers in the hierarchy until it eventually finds the required information or reaches an authoritative server.

Authoritative Response:

◇ An authoritative response comes from a DNS server that is considered the ultimate source of truth for a specific DNS record or domain.

◇ When an authoritative DNS server receives a query for a domain or record for which it holds the authoritative information, it provides a response containing the accurate and verified data for that domain. Authoritative responses are considered reliable and trusted.

Non-Authoritative Response:

◇ A non-authoritative response comes from a DNS server that doesn’t have direct authority over the queried domain or record but might have cached or obtained the information from another DNS server.

◇ Non-authoritative responses can be provided by intermediate DNS servers in the query resolution process. They are informative but might not be as reliable as authoritative responses since they are based on cached data or information obtained from other DNS servers.