COMPUTER NETWORK

ASSIGNMENT-5

V. LOKESH KUMAR

192521170

SCENARIO RECAP:

*) DNS Redundancy using 4 servers.

*) Each server latency = 25ms.

*) Failover delay = +30ms (additional to latency)

A) Describe DNS Redundancy models

DNS redundancy enseres continous availability of domain name resolution even if some DNS servers Fail. common models:

1. Primary - secondar (master-slave):
   - one authoritative server (master), other are backups
   - changes are made on the primary and replicated to secondaries.
   - Risk if the primary fails and progation lags

2. Anycast DNS:
   - multiple servers share the same ip.
   - clients are routed to the nearest server
   - Enables global load balancing and Fault tolerance

3. Round Robin DNS:

-) Multiple IP addresses (A records) returned in rotation
-) Load distributed evenly, no built-in Failover

4. Geo DNS:

-) Directs DNS queries based on user's Geographic location
-) Helps router users to the closest regional server, improving latency and reliability

6) Calculate Expected Resolution Time During Failover

-) Normal DNS resolution from a healthy Server = 25 ms.
-) During FailOver, if the primary server is down:
  -) Failover adds 30 ms.
  -) next server responds = 25 ms.

Total resolution time = 30 ms (failover) + 25 ms (next server response) = 55 ms

c) Recommed optimal TTL values

TTL (Time to Live) controls how long DNS records are cached

Use case	Recommended TTL
High availability (e.g., Failover readiness	30 - 60 seconds
Moderate Stability, ~~Stale~~ balance	300 seconds (5 mins)
Rarely changing records	3600 seconds

Optimal TTL for Failover Scenarios:

TTL = 30 to 60 seconds, so clients re-query Frequently enough pick up DNS changes (e.g., removed Failed server IP).

d) Suggest Best Practices for Global Failover Configuration

1. Use Anycast with Global DNS:
   - Ensures clients hit closest healthy DNS server
2. Deploy DNS servers in multiple geographic regions:
   - Reduces latency and increases Fault tolerance.

3. Monitor DNS health continuously:

- Automate Failover using health checks (e.g., via Route 53, Cloudflare, NS1)

4. Set low TTLs for dynamic records:

- Enables quick propagation of failover changes

5. Enable DNSSEC:

- Prevents spoofing and ensures integrity during failovers

6. Load test DNS failover scenarios:

- Validate how quickly clients recover and resolve after simulated outages

7. Use multi-DNS providers:

- Avoid vendor lock-in; if one DNS provider fails, another can take over.

conclusion

TO ensure high DNS availability, a Fintech Firm uses redundant servers with low latency and Failover support. With a Cattleover Failover resolution time of 55 ms the setup Maintains responsiveness during outages. By applying Low TTL values (30-60 seconds) and Following Global Failover best Practices - like using Anycast, health checks, and Geographically distributed servers - the Firm can achieve no best, resilient DNS performance with minimal disruption

DIAGRAM