Certified Professional in Domain Name System (DNS)

Domain Name System Fundamentals

AAAA Record – A DNS record that maps a domain name to a 128-bit IPv6 address. Related terms: A record, IPv6. Example: example.Com AAAA 2001:Db8::1. Practical application: Enables websites to be reachable over IPv6 networks. Challenge: Ensuring proper dual-stack configuration and firewall rules for IPv6 traffic.

A Record – The primary DNS record that maps a hostname to an IPv4 address. Related terms: AAAA record, address record. Example: www.Example.Com A 192.0.2.10. Practical application: Directs client requests to the correct server. Challenge: Managing changes during IP migration without service disruption.

Authority – The role of a DNS server that holds definitive data for a zone. Related terms: authoritative server, primary, secondary. Explanation: An authoritative server answers queries with data it is responsible for, rather than relying on recursion. Challenge: Maintaining synchronization between primary and secondary servers.

Authoritative Server – A DNS server that provides answers from its own zone data. Related terms: authority, primary server, secondary server. Example: The server listed in the NS records for example.Com. Practical application: Ensures reliable resolution for the domain's own records. Challenge: Protecting against DDoS attacks targeting the authoritative infrastructure.

Cache – Temporary storage of DNS query results on a resolver or client. Related terms: TTL, negative caching. Explanation: Caching reduces latency and external query load. Challenge: Balancing freshness of data with performance, especially after record changes.

Cache Poisoning – An attack that injects false data into a DNS cache. Related terms: DNS spoofing, security. Example: An attacker returns a malicious IP for bank.Com. Practical application: Understanding the threat helps implement mitigations such as DNSSEC. Challenge: Detecting and preventing malicious responses in high-traffic resolvers.

Canonical Name (CNAME) Record – A DNS record that aliases one name to another. Related terms: alias, zone apex. Example: mail.Example.Com CNAME mailhost.Provider.Com. Practical application: Simplifies management of service endpoints. Challenge: CNAME cannot be used at the zone apex, requiring careful planning.

Class – A field in DNS messages defining the protocol family; most commonly IN for Internet. Related terms: IN, CH. Explanation: While other classes exist (CHAOS, HS), they are rarely used in modern public DNS. Challenge: Misconfiguration can cause resolvers to ignore records.

Delegation – The process of assigning responsibility for a sub-domain to another DNS zone. Related terms: NS record, parent zone. Example: The parent zone example.Com delegates sub.Example.Com to a different set of name servers. Practical application: Enables distributed management of large DNS hierarchies.

Challenge: Ensuring the delegated zone's NS records are correct and reachable.

DNS Amplification Attack – A DDoS technique that exploits open resolvers to amplify traffic. Related terms: reflection attack, rate limiting. Explanation: Attackers send small queries with a spoofed source IP, causing larger responses to flood the target. Challenge: Configuring resolvers to limit recursion for external clients.

DNS over HTTPS (DoH) – A protocol that encrypts DNS queries within HTTPS. Related terms: DoT, privacy. Example: Browsers sending DNS queries to dns.Google via HTTPS. Practical application: Enhances privacy and bypasses DNS-based filtering. Challenge: Managing performance impact and integrating with existing DNS infrastructure.

DNS over TLS (DoT) – A protocol that secures DNS queries using TLS. Related terms: DoH, port 853. Explanation: Provides encrypted communication between resolver and client while preserving traditional DNS semantics. Challenge: Deploying compatible resolvers and handling certificate management.

DNSSEC – DNS Security Extensions that provide data integrity and authenticity. Related terms: RRSIG, DS record. Example: A signed .Org zone where each record has a digital signature. Practical application: Prevents cache poisoning and man-in-the-middle attacks. Challenge: Proper key management, rollover, and handling unsigned delegations.

Domain – A hierarchical identifier in the DNS namespace, e.G., example.Com. Related terms: zone, FQDN. Explanation: Domains are organized from the root down to sub-domains. Challenge: Choosing meaningful labels while avoiding naming conflicts.

Domain Name System (DNS) – The distributed database that translates human-readable names to IP addresses. Related terms: resolver, authoritative server. Explanation: DNS operates using a hierarchy of zones and a set of protocols (RFC 1035, etc.). Challenge: Balancing scalability, security, and performance.

Dynamic Update – A protocol (RFC 2136) allowing DNS records to be added, modified, or deleted automatically. Related terms: DDNS, TSIG. Example: A DHCP server registers a client's hostname and IP address in DNS. Practical application: Reduces manual administration in large networks. Challenge: Securing updates to prevent unauthorized changes.

Forwarder – A DNS server that forwards queries it cannot resolve locally to another server. Related terms: recursor, stub resolver. Explanation: Forwarders simplify configuration and can provide caching for internal clients. Challenge: Ensuring the forwarder is reliable and not a single point of failure.

FQDN (Fully Qualified Domain Name) – The complete domain name including all labels up to the root, ending with a dot. Related terms: hostname, domain. Example: mail.Server.Example.Com.. Practical application: Required in many configuration files to avoid ambiguity. Challenge: Users often omit the trailing dot, leading to unintended relative lookups.

Glue Record – An A or AAAA record placed in a parent zone to provide the IP address of a child zone's name server. Related terms: NS record, delegation. Example: The .Com zone includes a glue A record for ns1.Example.Com. Practical application: Prevents circular dependencies during resolution. Challenge:

Keeping glue records synchronized with the authoritative server's actual IPs.

Hierarchical Namespace – The tree-like structure of DNS, from root to TLDs to second-level domains. Related terms: root zone, zone cut. Explanation: Enables delegation and distributed management. Challenge: Maintaining consistency across the hierarchy as domains are added or removed.

Host – A device or service identified by a name in DNS, typically represented by an A or AAAA record. Related terms: canonical name, FQDN. Example: A web server with www.Example.Com. Practical application: Allows users to access services via memorable names. Challenge: Updating host records promptly after IP changes.

Hostname – The label that identifies a specific host within a domain. Related terms: FQDN, domain. Example: web01 in web01.Example.Com. Practical application: Used in configuration files and monitoring tools. Challenge: Avoiding naming collisions in large environments.

IP Address – A numeric identifier for a network interface; IPv4 (32-bit) or IPv6 (128-bit). Related terms: A record, AAAA record. Explanation: DNS maps names to these addresses to enable routing. Challenge: Managing address scarcity in IPv4 and ensuring proper IPv6 adoption.

Iterative Query – A DNS request where the resolver asks each server for the best answer it can provide, without expecting the server to perform recursion. Related terms: recursive query, resolver. Example: A stub resolver contacts the root, receives a referral to .Com, then contacts the .Com server, and so on. Practical application: Reduces load on authoritative servers. Challenge: Requires the resolver to handle multiple referrals and manage timeouts.

Key Signing Key (KSK) – The DNSSEC key that signs the DNSKEY set for a zone. Related terms: ZSK, DS record. Explanation: The KSK is typically stored offline and used during key rollover. Challenge: Secure generation, storage, and rollover to avoid zone validation failures.

Label – A single component of a domain name, separated by dots. Related terms: FQDN, zone. Example: In mail.Example.Com, "mail", "example", and "com" are labels. Practical application: Labels allow hierarchical organization. Challenge: Length limits (63 characters per label) and total name length (255 bytes).

Load Balancing – Distributing traffic across multiple servers using DNS techniques. Related terms: Round-Robin, geo-DNS. Example: Multiple A records for www.Example.Com point to different IPs. Practical application: Improves availability and performance. Challenge: DNS-based balancing lacks real-time health checks; failover may be delayed due to TTL.

Local Resolver – The DNS client component on a host that sends queries to a recursive resolver. Related terms: stub resolver, recursive resolver. Explanation: It typically uses the OS's resolver library. Challenge: Configuring correct DNS server addresses and handling search domains.

Master (Primary) Server – The authoritative DNS server that holds the original zone file for a domain. Related terms: secondary server, AXFR. Explanation: Updates are made here and propagated to slaves. Challenge: Ensuring high availability and protecting the master from unauthorized changes.

Negative Caching – Storing responses that indicate a name does not exist (NXDOMAIN) for a period defined by the SOA's MINIMUM field. Related terms: cache, TTL. Practical application: Reduces repeated queries for non-existent names. Challenge: Choosing appropriate expiration to avoid stale negative responses after a name is created.

NS Record – A DNS record that specifies the authoritative name servers for a zone. Related terms: delegation, glue record. Example: example.Com NS ns1.Provider.Net. Practical application: Directs queries to the correct servers for a domain. Challenge: Keeping NS records synchronized across parent and child zones.

Parent Zone – The zone that is one level above a given zone in the DNS hierarchy. Related terms: child zone, delegation. Example: The .Com zone is the parent of example.Com. Practical application: Manages delegation points. Challenge: Coordinating changes between parent and child to avoid resolution gaps.

Passive DNS – A system that collects and stores DNS query/response data for analysis. Related terms: security monitoring, threat intelligence. Example: Using passive DNS to trace the evolution of a malicious domain. Practical application: Assists in incident response and forensic investigations. Challenge: Handling large volumes of data while respecting privacy regulations.

PTR Record – A reverse DNS record that maps an IP address to a hostname. Related terms: reverse lookup, in-addr.Arpa. Example: 10.0.0.1.In-addr.Arpa PTR host.Example.Com. Practical application: Used by mail servers for spam checks. Challenge: Maintaining correct reverse mappings across multiple networks.

Query Type – The specific DNS record type requested, such as A, AAAA, MX, TXT, etc. Related terms: RRtype, response code. Explanation: The type determines which data the server returns. Challenge: Supporting newer types (e.G., CAA, SVCB) while ensuring backward compatibility.

Recursive Resolver – A DNS server that performs the full resolution process on behalf of a client, following referrals until an answer is obtained. Related terms: iterative query, cache. Practical application: Provides end-users with a single point of contact for DNS queries. Challenge: Scaling to handle millions of queries per second and protecting against amplification attacks.

Recursive Query – A DNS request where the client asks the resolver to obtain the final answer, performing all necessary lookups. Related terms: recursive resolver, iterative query. Example: A browser asks the resolver for www.Example.Com and expects a complete answer. Practical application: Simplifies client configuration. Challenge: Increases processing load on resolvers.

Root Zone – The top-most DNS zone, represented by a single dot, containing NS records for all top-level domains. Related terms: root servers, hierarchical namespace. Explanation: The root zone is managed by a global community of operators. Challenge: Maintaining security and stability of the root infrastructure.

Root Server – One of the thirteen authoritative servers that serve the DNS root zone. Related terms: root zone, anycast. Example: a.Root-servers.Net. Practical application: Provides the starting point for all DNS resolution. Challenge: Mitigating DDoS attacks and ensuring global low-latency access via anycast.

Round-Robin DNS – A load-balancing method where multiple A or AAAA records are returned in a rotating order. Related terms: load balancing, TTL. Practical application: Simple distribution of traffic across multiple servers. Challenge: No health checking; a down server may continue receiving traffic until cache expires.

SOA Record – Start of Authority record that defines zone metadata, including primary server, admin email, serial number, and timing parameters. Related terms: zone, serial. Example: example.Com SOA ns1.Example.Com. Hostmaster.Example.Com. 2024052101 7200 3600 1209600 3600. Practical application: Controls zone transfers and caching behavior. Challenge: Properly incrementing the serial number to avoid stale data.

Secondary (Slave) Server – An authoritative DNS server that obtains zone data from the primary via zone transfer. Related terms: AXFR, IXFR. Explanation: Provides redundancy and load distribution. Challenge: Ensuring timely zone updates and protecting transfer channels with TSIG.

SECURITY Extension (SEC) – Historical DNSSEC record type that has been superseded by RRSIG, DNSKEY, and NSEC. Related terms: DNSSEC, RRSIG. Explanation: Legacy term; modern implementations use updated types. Challenge: Migrating old zones to current DNSSEC standards.

Server Failure (SERVFAIL) – A DNS response code indicating that the server was unable to process the query due to a problem. Related terms: RCODE, NXDOMAIN. Example: A resolver receives SERVFAIL when a zone's authoritative server is misconfigured. Practical application: Signals to the client that retry may be needed. Challenge: Diagnosing underlying server or network issues.

Signature (RRSIG) Record – A DNSSEC record that contains a digital signature for a set of resource records. Related terms: DNSSEC, key signing key. Explanation: Validates the authenticity of DNS data. Challenge: Managing key lifecycles and ensuring all records are correctly signed.

Stub Resolver – A minimal DNS client that forwards queries to a recursive resolver without performing recursion itself. Related terms: local resolver, recursive resolver. Explanation: Typically part of operating system networking stacks. Challenge: Configuring reliable upstream resolvers.

Subdomain – A domain that is part of a larger parent domain, e.G., blog.Example.Com. Related terms: delegation, zone cut. Practical application: Allows organizational separation of services. Challenge: Properly delegating and maintaining NS and glue records.

TTL (Time to Live) – The duration that a DNS record is considered valid in caches. Related terms: cache, negative caching. Example: An A record with TTL 3600 seconds. Practical application: Controls how quickly changes propagate. Challenge: Balancing rapid updates against increased query traffic.

TXT Record – A DNS record used to store arbitrary text data. Related terms: SPF, DKIM. Example: example.Com TXT "v=spf1 include:_Spf.Google.Com ~all". Practical application: Publishes policy information, verification tokens, and security keys. Challenge: Managing length limits and ensuring correct parsing by applications.

Zone – A contiguous portion of the DNS namespace administered by a single organization or server.

Related terms: zone file, delegation. Example: The example.Com zone contains all records for that domain and its sub-domains unless delegated. Practical application: Enables decentralized management. Challenge: Keeping zone data consistent across primary and secondary servers.

Zone Cut – The point in the DNS hierarchy where authority is transferred from a parent to a child zone, typically marked by an NS record. Explanation: Determines which server is authoritative for a sub-domain. Challenge: Avoiding accidental gaps that lead to resolution failures.

Zone Transfer (AXFR) – The process of copying an entire DNS zone from a primary to a secondary server. Related terms: incremental transfer, IXFR. Practical application: Synchronizes authoritative data across multiple servers. Challenge: Securing transfers with TSIG to prevent unauthorized zone replication.

Incremental Zone Transfer (IXFR) – A method of transferring only the changes made to a zone since the last update. Related terms: AXFR, serial. Explanation: Reduces bandwidth and speeds up synchronization. Challenge: Properly handling serial number rollovers and ensuring both sides support the same protocol version.

Key Management – The procedures for generating, storing, rotating, and revoking DNSSEC cryptographic keys. Related terms: KSK, ZSK. Practical application: Maintains trust chains for signed zones. Challenge: Coordinating rollovers without causing validation failures for resolvers.

Label Compression – A DNS message optimization where repeated domain name suffixes are replaced with pointers to earlier occurrences. Related terms: DNS message format, RFC 1035. Explanation: Reduces packet size. Challenge: Implementing correct pointer handling to avoid malformed responses.

Message Header – The first 12 bytes of a DNS message containing ID, flags, and count fields. Related terms: QR flag, RCODE. Explanation: Controls query/response identification and status. Challenge: Properly setting flags for iterative vs. Recursive behavior.

Negative Response – A DNS reply indicating that the queried name does not exist (NXDOMAIN) or that the type is not available (NODATA). Related terms: NXDOMAIN, NOERROR. Practical application: Informs clients that a name is unregistered. Challenge: Managing caching duration to prevent stale negative entries.

Network Time Protocol (NTP) Synchronization – Aligning DNS server clocks to ensure accurate TTL handling and time-based security checks. Related terms: TTL, key rollover. Explanation: DNS relies on correct timestamps for caching and DNSSEC validation. Challenge: Preventing clock drift that could cause premature expiration or signature verification failures.

NSID (Name Server Identifier) – An optional EDNS0 extension that allows a resolver to learn which server answered a query. Related terms: EDNS0, debugging. Practical application: Helps diagnose load-balancing and geographic routing. Challenge: Not all servers support NSID; privacy concerns may limit its use.

EDNS0 (Extension Mechanisms for DNS 0) – An extension to the DNS protocol that allows larger UDP payloads and additional options. Related terms: UDP size, DO bit. Explanation: Enables DNSSEC and other features that exceed the original 512-byte limit. Challenge: Ensuring compatibility with legacy resolvers and

handling fragmentation.

EDNS0 DO Bit – A flag in EDNS0 indicating that the client requests DNSSEC data. Explanation: When set, the server includes signatures in its response. Challenge: Managing increased response size and potential truncation.

EDNS0 UDP Payload Size – The maximum size of a DNS message over UDP negotiated via EDNS0. Related terms: EDNS0, fragmentation. Example: Clients often advertise 4096 bytes. Practical application: Reduces need for TCP fallback. Challenge: Network devices that block large UDP packets may cause resolution failures.

Recursive DNS Cache Poisoning – An attack that injects false records into a resolver's cache by exploiting predictable transaction IDs. Related terms: source port randomization, entropy. Challenge: Mitigating by increasing randomness and implementing DNSSEC.

Source Port Randomization – A technique where the resolver uses unpredictable source ports for DNS queries to increase entropy. Related terms: transaction ID, cache poisoning. Explanation: Makes it harder for attackers to guess the correct query parameters. Challenge: Some NAT devices may interfere with randomization.

Stub Zone – A read-only copy of a portion of the DNS namespace, containing only NS records for a delegated zone. Related terms: forwarder, resolver. Practical application: Improves performance by reducing the number of referrals. Challenge: Keeping the stub zone updated when delegation changes.

TSIG (Transaction Signature) – A mechanism for authenticating DNS messages using shared secret keys and HMAC. Related terms: secure zone transfer, key management. Example: Using TSIG to protect AXFR between primary and secondary servers. Practical application: Prevents unauthorized zone updates. Challenge: Secure distribution and rotation of shared keys.

TXT SPF Record – A specific use of the TXT record to publish Sender Policy Framework information for anti-spam. Related terms: TXT record, DKIM. Example: example.Com TXT "v=spf1 ip4:192.0.2.0/24 -All". Practical application: Reduces email spoofing. Challenge: Keeping SPF records synchronized with changing IP ranges.

Wildcard Record – A DNS record that matches any subdomain not explicitly defined, using the asterisk (*) label. Related terms: CNAME, fallback. Example: *.Example.Com A 203.0.113.5. Practical application: Simplifies handling of many subdomains. Challenge: Can interfere with intended delegation and cause unexpected resolution results.

Zone Serial Number – A 32-bit integer in the SOA record that increments with each change to the zone. Related terms: SOA, IXFR. Explanation: Secondary servers use it to detect updates. Challenge: Avoiding wrap-around and ensuring consistent incrementing across automated update systems.

Authoritative Answer Flag (AA) – A flag in DNS responses indicating that the answer comes from an authoritative server. Related terms: authoritative server, recursive resolver. Explanation: Helps clients

understand the trust level of the data. Challenge: Some middleboxes may strip this flag, leading to ambiguity.

ANY Query – A DNS request for all record types associated with a name. Related terms: RFC 8482, response size. Explanation: Historically used for debugging, but now discouraged due to amplification risks. Challenge: Modern resolvers often limit or block ANY queries.

RFC 1918 Private Addresses – IPv4 address ranges reserved for private networks (10/8, 172.16/12, 192.168/16). Related terms: split-horizon DNS, internal namespace. Practical application: Used in internal DNS zones that should not be exposed publicly. Challenge: Preventing leakage of private records to the public Internet.

Split-Horizon DNS – A configuration where different DNS responses are served based on the source of the query (internal vs. External). Related terms: view, internal zone. Example: Internal users receive an A record pointing to 10.0.0.5, External users receive 203.0.113.5. Practical application: Provides security and optimized routing. Challenge: Maintaining consistent records across views and avoiding accidental exposure.

View (BIND View) – A feature that allows a DNS server to serve different data based on client IP address or other criteria. Related terms: split-horizon DNS, ACL. Explanation: Enables separate authoritative zones for internal and external clients. Challenge: Complexity in configuration and testing.

ACL (Access Control List) – A set of rules defining which clients may perform certain DNS operations. Related terms: view, TSIG. Practical application: Restricts zone transfers to authorized secondary servers. Challenge: Keeping ACLs up to date with changing network topology.

Reverse DNS Zone – A zone that maps IP addresses to hostnames using the in-addr.Arpa (IPv4) or ip6.Arpa (IPv6) namespaces. Related terms: PTR record, reverse lookup. Example: The zone 1.0.0.10.In-addr.Arpa for the network 10.0.0.0/24. Practical application: Used by email servers for spam checks. Challenge: Delegating large address blocks and ensuring consistency with forward zones.

Forward Lookup Zone – The standard DNS zone that maps hostnames to IP addresses. Explanation: The most common type of zone. Challenge: Keeping records up to date with dynamic IP assignments.

Key Signing Key Rollover – The process of replacing a zone's KSK while maintaining validation. Related terms: KSK, DS record. Explanation: Requires publishing the new DS record in the parent zone before retiring the old KSK. Challenge: Coordinating with parent zone operators and avoiding validation gaps.

Zone Signing Key (ZSK) – The DNSSEC key used to sign individual records within a zone. Related terms: KSK, RRSIG. Explanation: Typically rotated more frequently than the KSK. Challenge: Automating rollover without disrupting validation.

Cache Snooping – A technique where an attacker queries a resolver for a name to infer whether it has been cached. Related terms: privacy, EDNS0. Challenge: Mitigating by configuring resolvers to refuse unauthenticated queries or limit responses.

EDNS0 Client Subnet (ECS) – An EDNS0 option that conveys part of the client's IP address to authoritative servers for geo-based responses. Related terms: geo-DNS, privacy. Practical application: Provides location-aware content. Challenge: Balances privacy concerns with accuracy; some resolvers strip ECS.

Geo-DNS – DNS routing based on the geographic location of the client. Related terms: ECS, load balancing. Example: Users in Europe receive an IP for a European data center, while Asian users receive an IP for an Asian data center. Practical application: Improves latency and compliance with data-locality regulations. Challenge: Maintaining accurate location data and handling DNS caching effects.

Dynamic Host Configuration Protocol (DHCP) Integration – Using DHCP to automatically update DNS records via Dynamic Update. Related terms: DDNS, lease. Explanation: Enables seamless addition and removal of hosts. Challenge: Securing updates and handling stale entries after lease expiration.

Negative TTL (SOA MINIMUM) – The time that a resolver caches a negative response (NXDOMAIN) as defined by the SOA's minimum field. Related terms: negative caching, TTL. Explanation: Controls how quickly a newly created name becomes visible. Challenge: Choosing a value that balances fast propagation with reduced unnecessary traffic.

Zone Apex – The top label of a zone, often represented by the domain name itself (e.G., example.Com). Related terms: parent zone, NS record. Explanation: Certain records (CNAME) are not allowed at the apex. Challenge: Managing apex records for services like CDN edge nodes, often requiring ALIAS or ANAME pseudo-records.

ALIAS Record – A virtual record type that allows a CNAME-like alias at the zone apex while preserving DNS semantics. Related terms: ANAME, apex CNAME. Example: example.Com ALIAS target.Provider.Com. Practical application: Enables CDN providers to point the apex to a target without breaking NS delegation. Challenge: Implementation varies by DNS provider; not part of the official DNS spec.

ANAME Record – Similar to ALIAS, a provider-specific record that resolves to the target's A/AAAA records at query time. Related terms: ALIAS, apex CNAME. Explanation: Provides flexibility for apex aliasing. Challenge: Compatibility across different resolvers and potential increase in query load.

Domain Owner – The entity that controls a domain's registration and DNS configuration. Related terms: registrar, registry. Explanation: The owner can modify NS records, set contact information, and manage DNSSEC. Challenge: Ensuring secure access to registrar accounts to prevent hijacking.

Registrar – An accredited organization that registers domain names on behalf of owners. Related terms: registry, domain owner. Explanation: Provides the interface to update WHOIS data and delegate DNS. Challenge: Verifying registrar security practices and protecting account credentials.

Registry – The authoritative database for a particular TLD, managing the zone and delegations. Related terms: registrar, root server. Example: Verisign operates the .Com registry. Practical application: Maintains the master zone file for the TLD. Challenge: Coordinating with registrars for rapid updates and handling abuse mitigation.

WHOIS – A protocol used to query registration information for domain names. Explanation: Provides contact and status data. Challenge: Privacy regulations (GDPR) limit the amount of publicly visible information.

Zone Transfer Security – Measures to protect AXFR/IXFR from unauthorized access. Related terms: TSIG, ACL. Explanation: Prevents exposure of the entire zone data to attackers. Challenge: Balancing security with the need for legitimate secondary servers.

Recursive Resolver Rate Limiting – Controls the number of queries a resolver will answer for a particular client or query type. Related terms: DNS amplification, DoS mitigation. Explanation: Helps prevent abuse of open resolvers. Challenge: Setting thresholds that block malicious traffic without impacting legitimate users.

EDNS0 Padding – An EDNS0 option that adds random bytes to DNS messages to obscure the true length, protecting against traffic analysis. Practical application: Enhances anonymity for privacy-focused resolvers. Challenge: Some middleboxes may drop padded packets.

DNS Cookie – A lightweight mechanism to mitigate reflection attacks by requiring a client to echo back a cookie value. Related terms: DoS mitigation, EDNS0. Explanation: Reduces the impact of spoofed queries. Challenge: Implementing support on both client and server sides.

Response Rate Limiting (RRL) – A technique used by authoritative servers to limit the number of identical responses sent to a client within a time window. Related terms: DDoS mitigation, rate limiting. Explanation: Helps protect against amplification attacks. Challenge: Tuning parameters to avoid false positives that affect legitimate traffic.

Cache Consistency – The state where cached DNS data reflects the current authoritative data.