Name Server and Configuration

Hiranya Prasad Bastakoti

Contents

- DNS principles and Operations
- Basic Name Server and Client Configuration
- Caching Only name server
- Primary and Slave Name Server
- DNS Zone Transfers
- DNS Dynamic Updates
- DNS Delegation
- DNS Server Security
- Troubleshooting

Introduction

- The Domain Name System remembering IP addresses by mapping domain names to IP addresses
- The DNS is a distributed database across a hierarchy of networks of servers and provide ways for devices and software (like browsers and email) to query the DNS to get an IP address.
- Domain names are used for naming websites and email addresses.

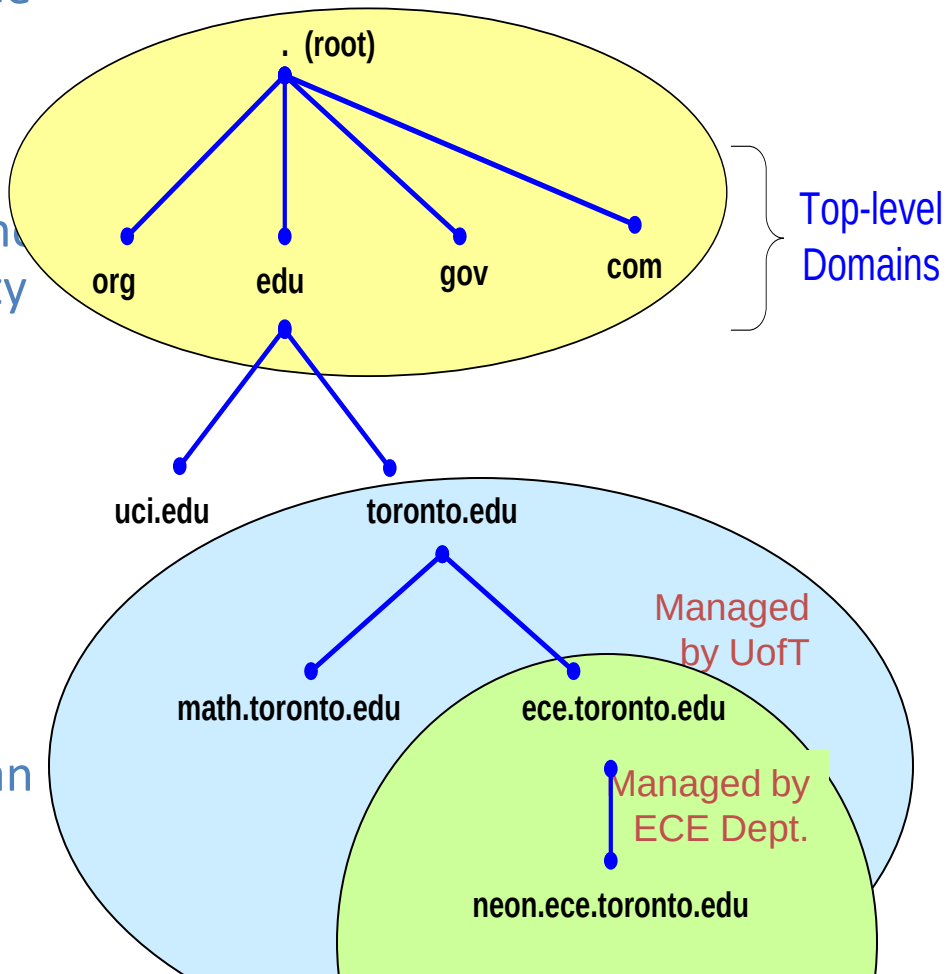
Contd..

Domain Name System is a hierarchical distributed database

- DNS is the foundation of the Internet naming scheme
- People prefer to use easy-to-remember names instead of IP addresses
- Domain names are alphanumeric names for IP addresses e.g., neon.ece.utoronto.ca, www.google.com, ietf.org
- The domain name system (DNS) is an Internet-wide distributed database that translates between domain names and IP addresses
- DNS was created to support the Internet's growing number of hosts

DNS Name hierarchy

- DNS hierarchy can be represented by a tree
- Root and top-level domains are administered by an Internet central name registration authority (ICANN)
- Below top-level domain, administration of name space is delegated to organizations
- Each organization can delegate further



DNS Components

Namespace:

- DNS uses a hierarchy to manage its distributed database system.
- The DNS hierarchy, also called the domain name space, is an inverted tree structure, much like eDirectory.

Name server: A nameserver is a server in the DNS that translates domain names into IP addresses.

- Nameservers store and organize DNS records, each of which pairs a domain with one or more IP addresses.

Zone:

- A DNS zone is a portion of the DNS namespace that is managed by a specific organization or administrator.
- A DNS zone is an administrative space which allows for more granular control of DNS components, such as authoritative nameservers.

Top-level domains

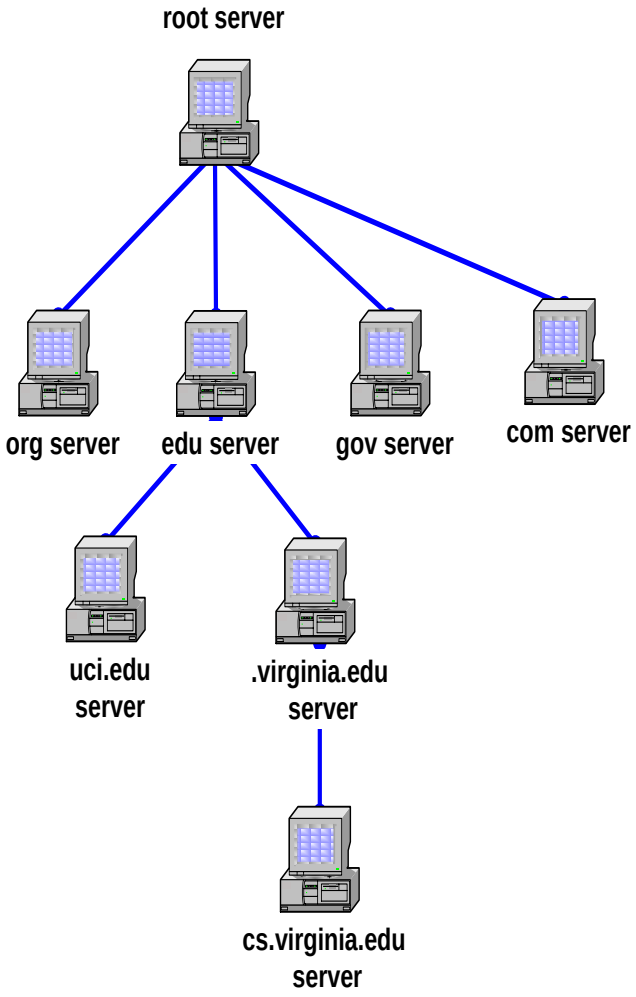
- Three types of top-level domains:
  - Organizational: 3-character code indicates the function of the organization
    - Examples: gov, mil, edu, org, com, net
  - Geographical: 2-character country or region code
    - Examples: us, va, jp, de
  - Reverse domains: A special domain (in-addr.arpa) used for IP address-to-name mapping

Organizational top-level domains

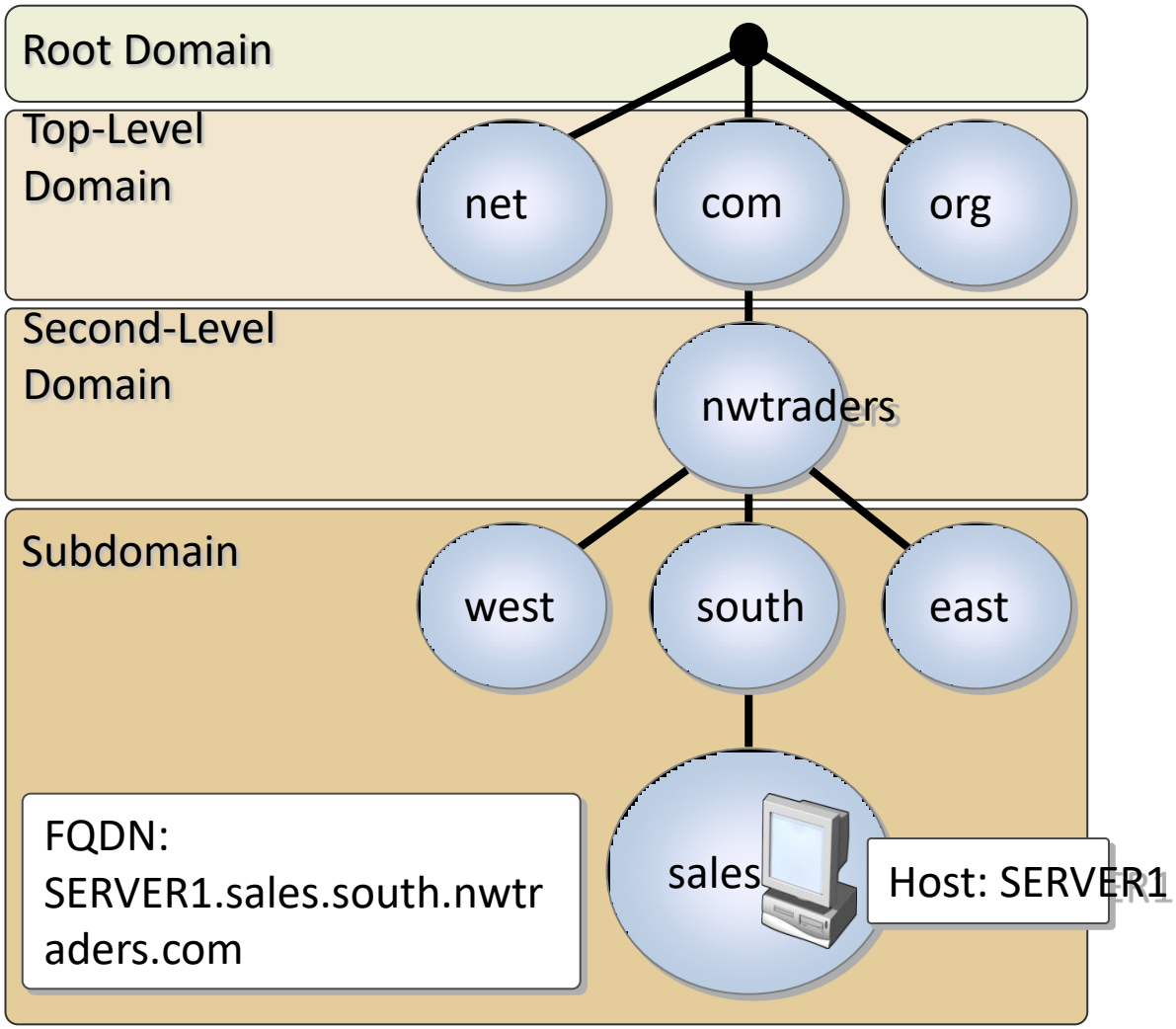
com	Commercial organizations
edu	Educational institutions
gov	Government institutions
int	International organizations
mil	military institutions
net	Networking organizations
org	Non-profit organizations

Hierarchy of name servers

- The resolution of the hierarchical name space is done by a hierarchy of name servers
- Each server is responsible (authoritative) for a contiguous portion of the DNS namespace, called a zone.
- Zone is a part of the subtree
- DNS server answers queries about hosts in its zone



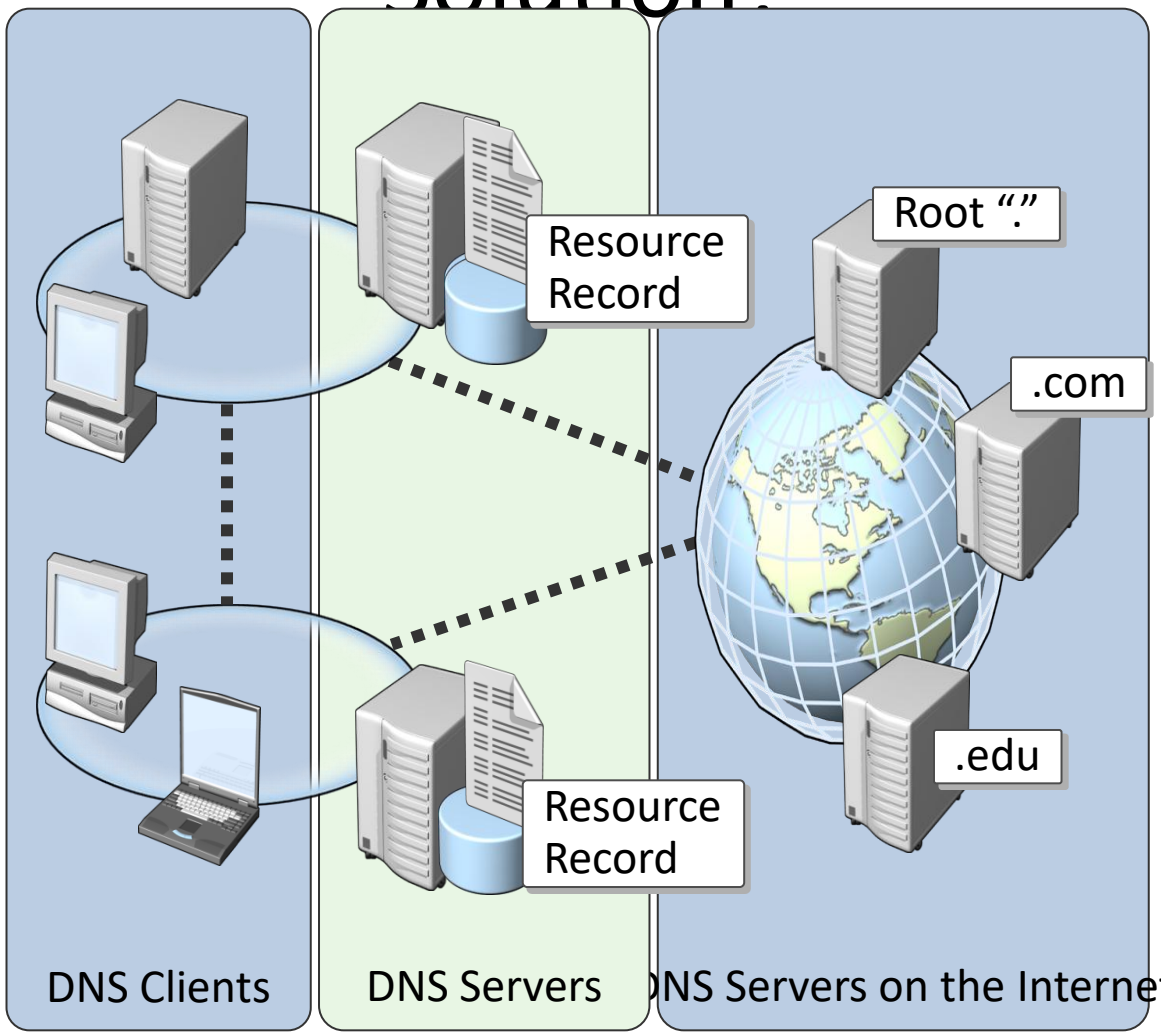
What Is a Domain Namespace?



Major Components of DNS

- Domains: A domain is a logical group of computers in a large network. Access to each computer in a given group is controlled by the same server.
- Distributed Database: A distributed database is an archive of information about the computers in a network.
- Name Servers: A name server contains address information about other computers on the network. This information can be given to client computers that make a request to the name server.
- Clients: A client requests information from the servers. In a domain name system, the client requests network addressing information from the name servers.
- Resolver: A resolver provides clients with address information about other computers on the network

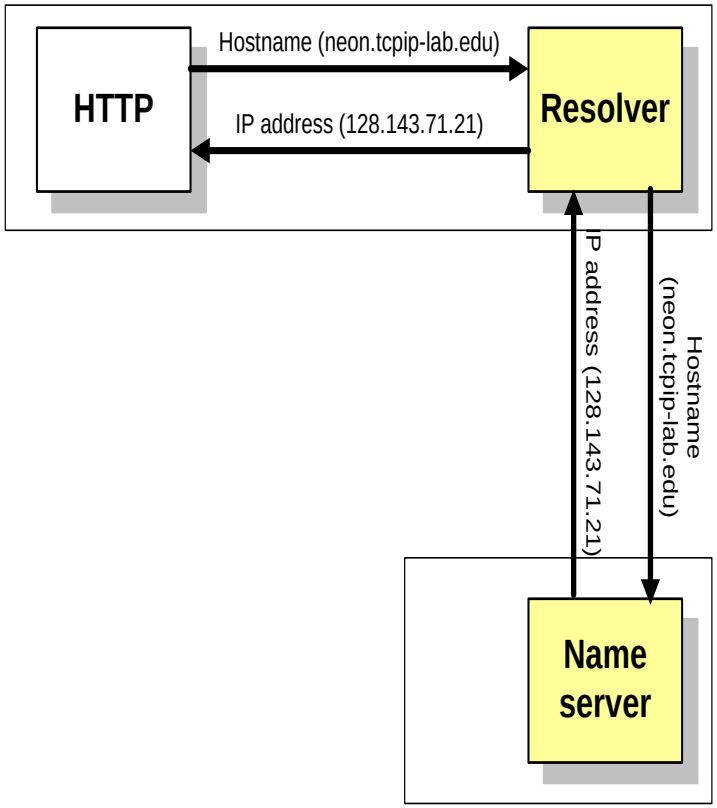
What Are the Components of a DNS Solution?



Resolver and name server

1. An application program on a host accesses the domain system through a DNS client, called the **resolver**
2. Resolver contacts DNS server, called name server
3. DNS server returns IP address to resolver which passes the IP address to application

- Reverse lookups are also possible, i.e., find the hostname given an IP address



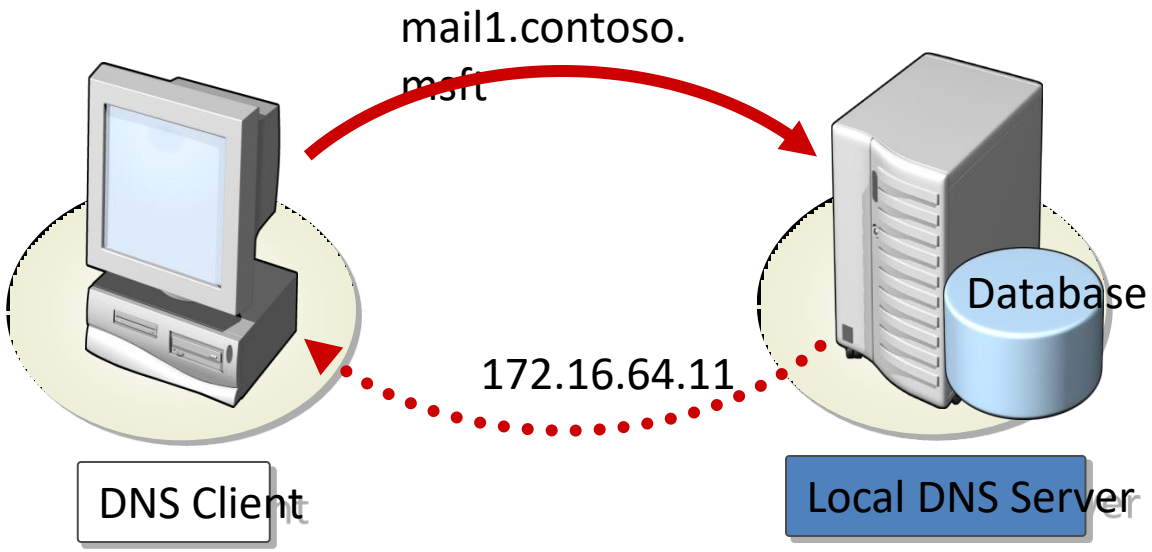
What Is a DNS Query?

A *query* is a request for name resolution and is directed to a DNS server

- Queries are recursive or iterative
- DNS clients and DNS servers both initiate queries
- DNS servers are authoritative or nonauthoritative for a namespace
- An authoritative DNS server for the namespace will either:
  - Return the requested IP address
  - Return an authoritative “No”
- A nonauthoritative DNS server for the namespace will either:
  - Check its cache
  - Use forwarders
  - Use root hints

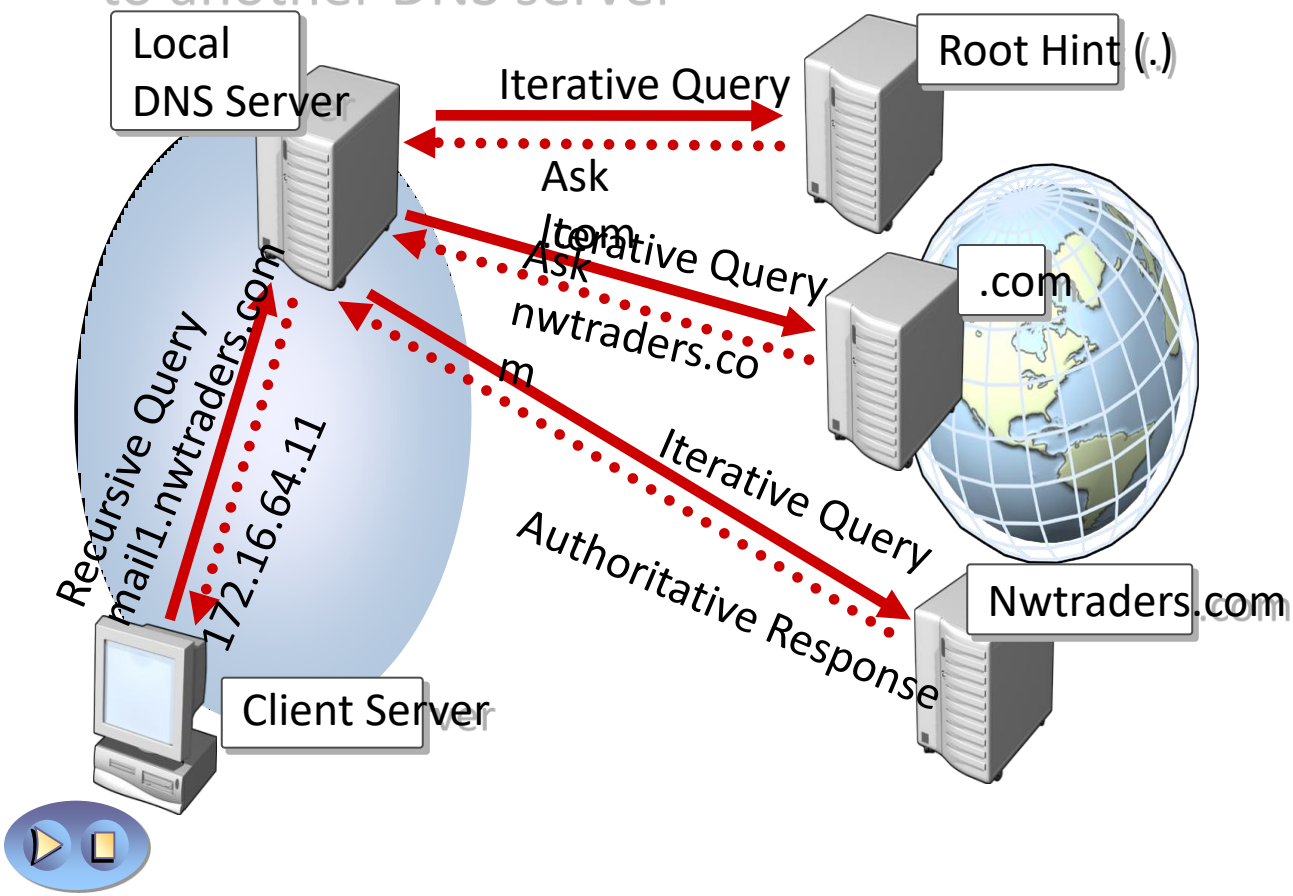
How Recursive Queries Work

A *recursive query* is sent to a DNS server and requires a complete answer



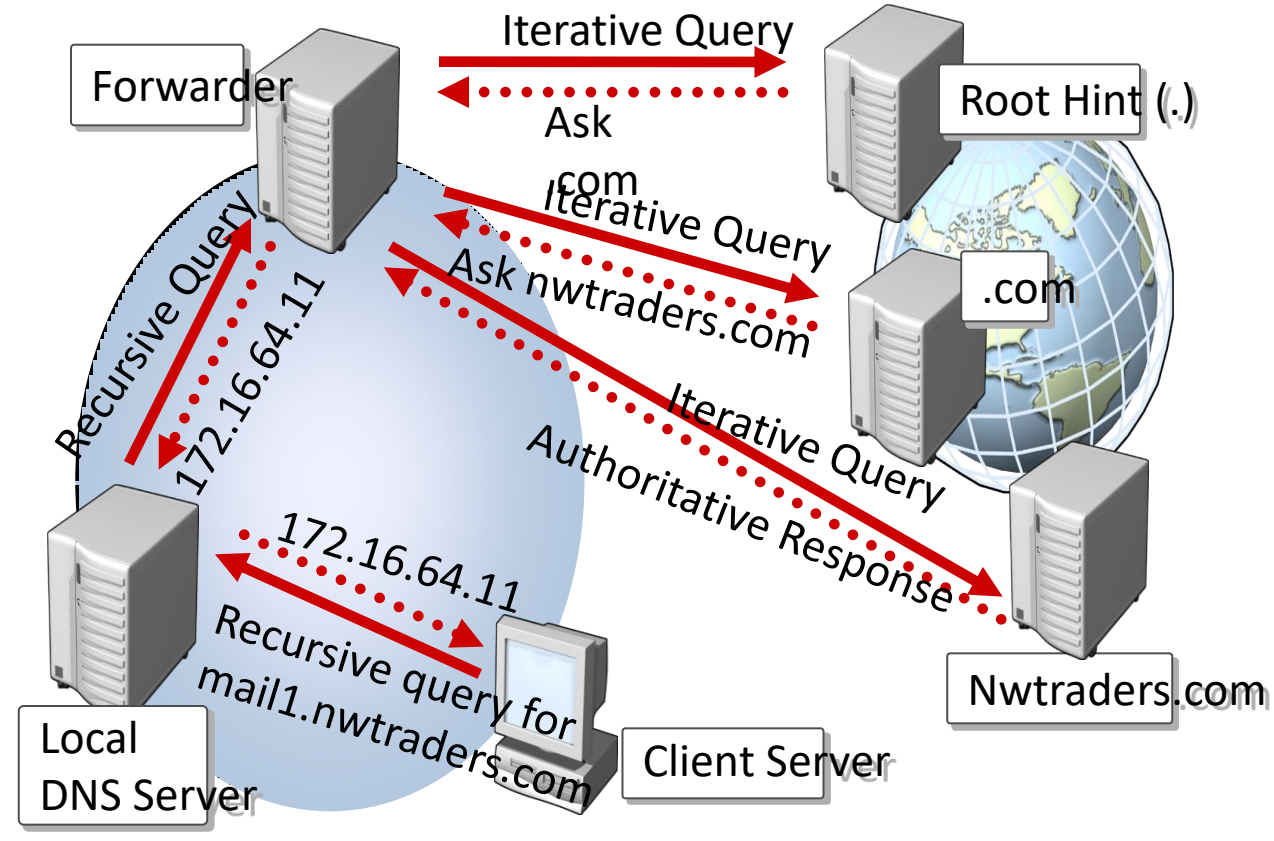
How Iterative Queries Work

An iterative query directed to a DNS server may be answered with a referral to another DNS server

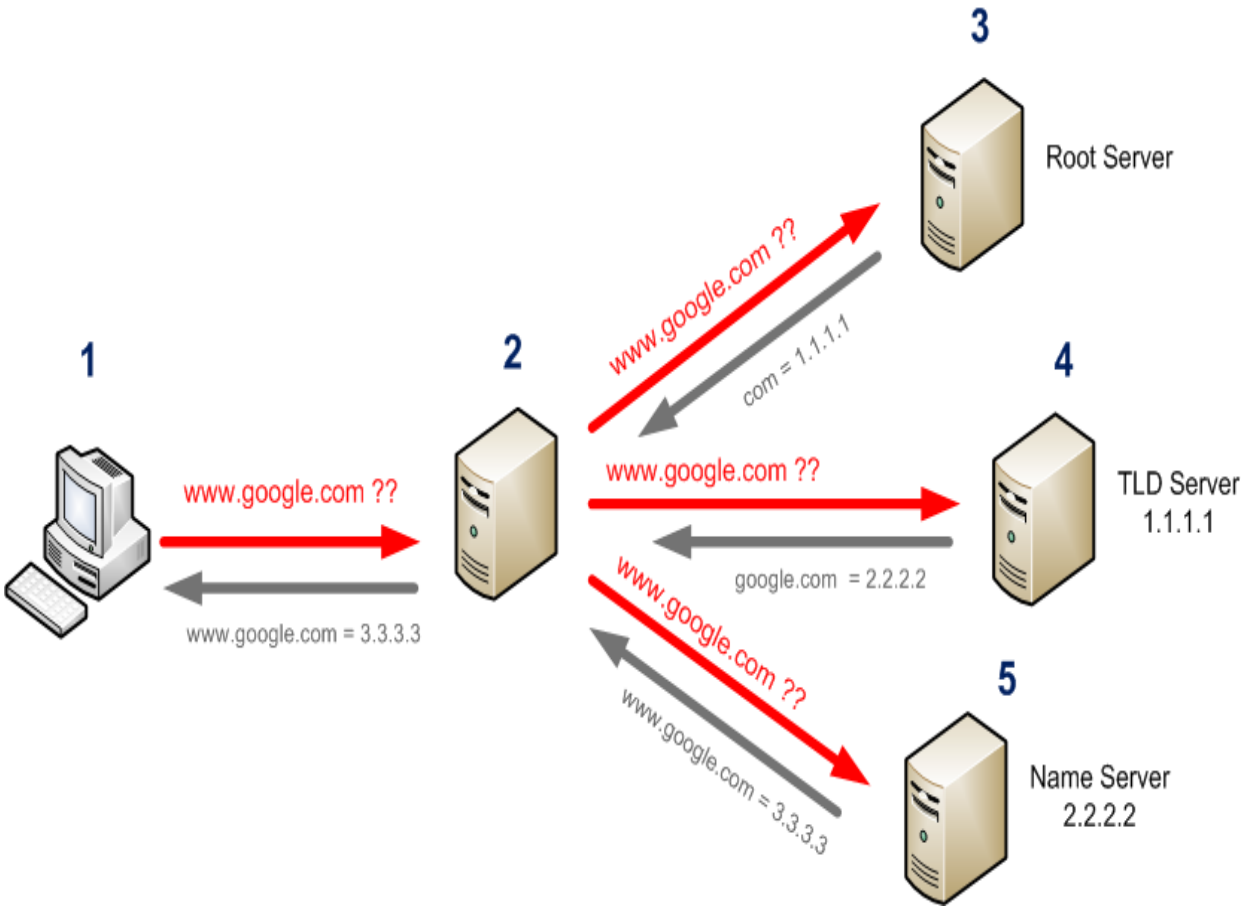


How Forwarders Work

A *forwarder* is a DNS server designated to resolve external or offsite DNS domain names



How DNS works?



How DNS Works?

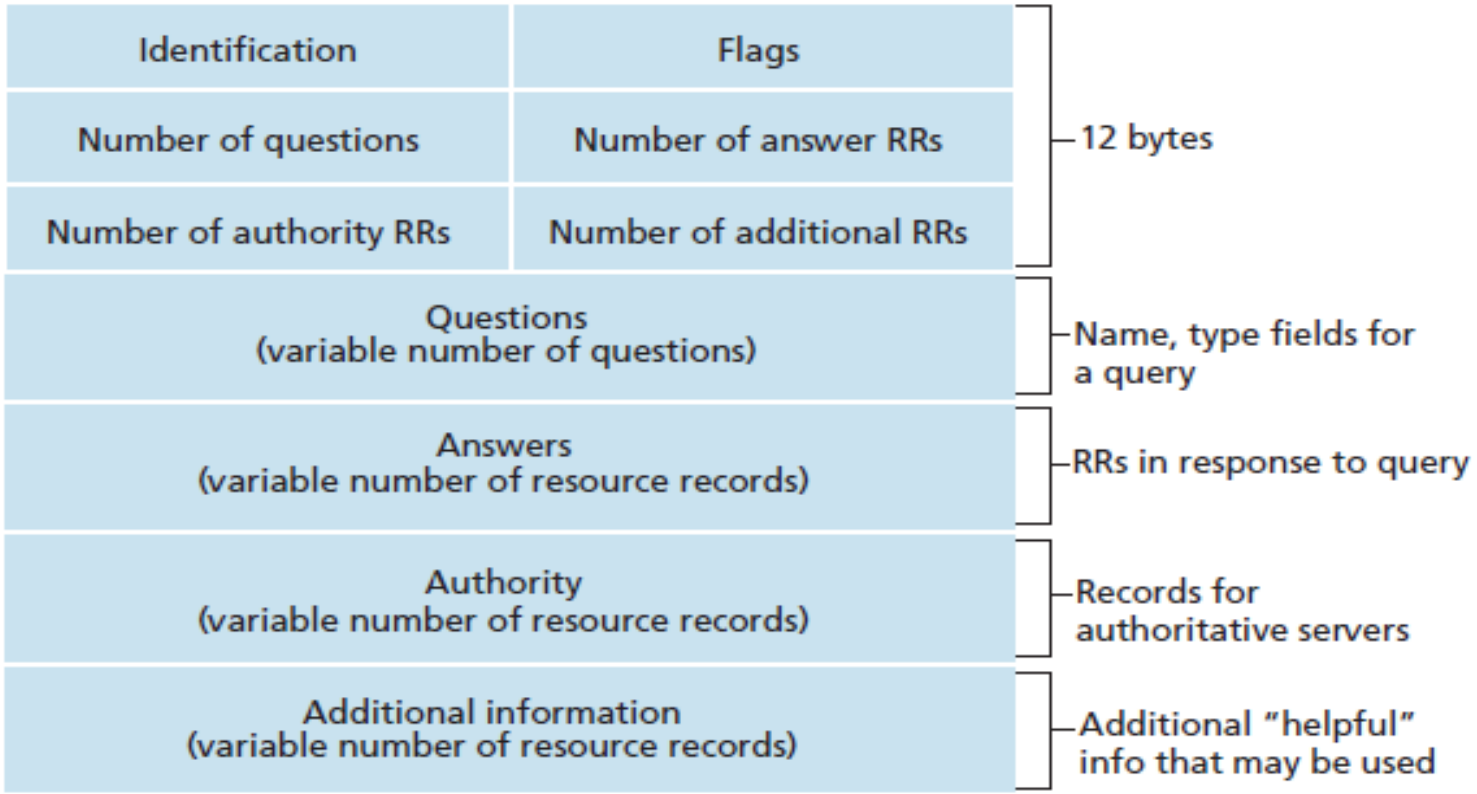
- Step 1: The client proposes a domain name resolution request and sends the request to the local domain name server.
- Step 2: When the local domain name server receives the request, it first queries the local cache. If there is this record, the local domain name server directly returns the result of the query.
- Step 3: If the local cache does not have the record, the local domain name server directly sends the request to the root domain name server, and then the root domain name server returns the primary domain name of the domain (the subdomain of the root) of the local domain name server. The address of the server.
- Step 4: The local server sends a request to the domain name server returned in the previous step, and then the server that accepts the request queries its own cache. If there is no such record, it returns the address of the relevant lower-level domain name server.
- Step 5: Repeat step 4 until you find the correct record.
- Step 6: The local domain name server saves the returned results to the cache for the next use and returns the results to the client

DNS Record and Message

- The name servers that together implement the DNS distributed database, store Resource Records (RR) for the hostname to IP address mappings.
- Each DNS reply message carries one or more resource record
- A resource record is a four-tuple that contains the following fields:
- (Name, Value, Type, TTL)
- TTL is the time to live of the resource record; it determines the time at which a resource should be removed from a cache
- The meaning of Name and Value depend on Type

- If Type=A, then Name is a hostname and Value is the IP address for the hostname. Thus, a Type A record provides the standard hostname to IP address mapping. As an example, (relay1.bar.foo.com, 145.37.93.126, A) is a Type A record.
- If Type=NS, then Name is a domain (such as foo.com) and Value is the hostname of a server that knows how to obtain the IP addresses for hosts in the domain. This record is used to route DNS queries further along in the query chain. As an example, (foo.com, dns.foo.com, NS) is a Type NS record.
- If Type=CNAME, then Value is a canonical hostname for the alias hostname Name. This record can provide querying hosts the canonical name for a hostname. As an example, (foo.com, relay1.bar.foo.com, CNAME) is a CNAME record.
- If Type=MX, then Value is a hostname of a mail server that has an alias hostname Name. As an example, (foo. com. mail.bar.foo.com, MX) is an MX record. MX records allow the hostnames of mail servers to have simple aliases.

DNS Message Format



DNS Servers: Root Server

- Root servers are positioned at the top or root of the DNS hierarchy and maintain data about each of the top-level zones.
- The root servers are maintained by the NIC and have been moved to a common domain for consistent naming purposes.
- The root servers are named as A.root-servers.net., B.root-servers.net., and so on.

Primary (Master) Servers

- Each domain must have a primary server. Primary server has the following features.
- There is generally only one primary server per domain.
- They are the system where all the changes are made to the domain.
- They are the authoritative for all domains they serve.
- They periodically update and synchronize secondary servers of the domain.
- In current versions of BIND, they are defined by the type master argument to the zone statement in the configuration file **/etc/named.conf**.

Secondary/Slave servers

- Each domain should have at least one secondary server. In fact,the NIC will not allow a domain to become officially registered as a subdomain of a top-level domain until a site demonstrates two working DNS servers. Secondary servers have the following features.
- There is one or more secondary server per domain.
- They obtain copy of the domain information for all domains they serve from the appropriate primary server or another secondary server for the domain.
- They are authoritative for all the domains they serve.
- They periodically receive updates from the primary servers of the domain.
- They provide load sharing with the primary servers and other servers of the domain.
- They provide redundancy in case one or more other servers are temporarily unavailable.
- They provide more local access to name resolution if placed appropriately.
- In current versions of BIND, they are defined by the type slave argument to the zone statement in the **/etc/named.conf** file.

Caching-Only servers

- These servers only cache information for any DNS domain. They are not authoritative for any domain. Caching-only servers provide the following features.
- They provide local cache of looked up names.
- They have lower administrative overhead.
- They are never authoritative for any domain.
- They reduce overhead associated with secondary servers performing zone transfers from primary servers.
- They allow DNS client access to local cached naming information without the expense of setting up a DNS primary or secondary server.

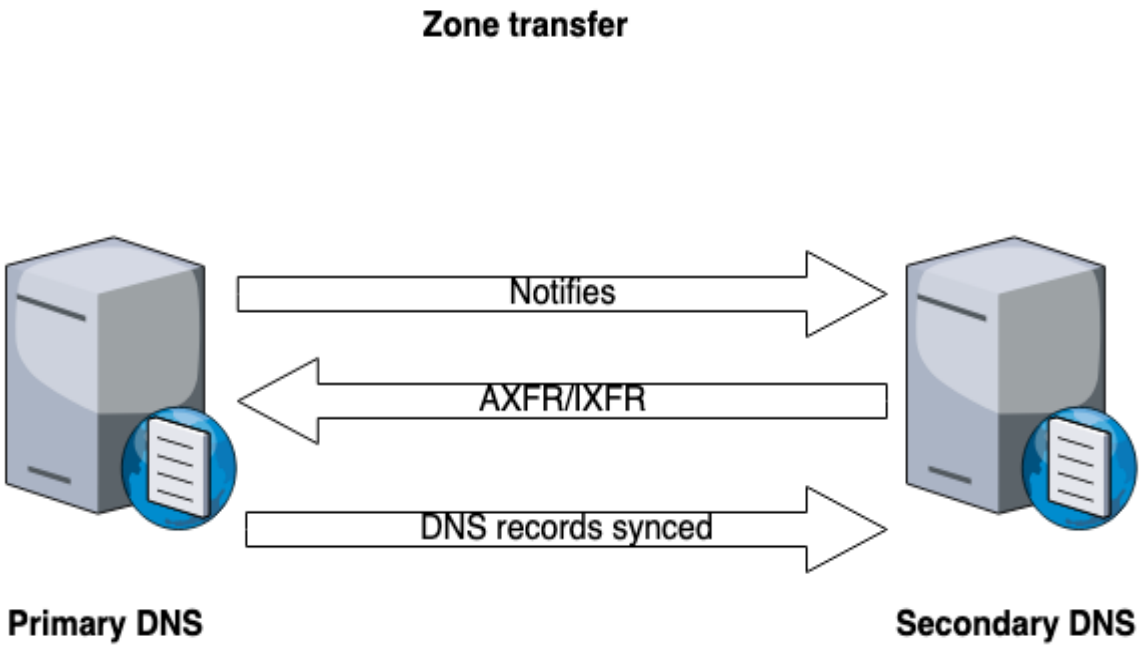
Forwarding servers

- Forwarding servers are a variation on a primary or secondary server and act as focal points for all off-site DNS queries. Designating a server as a forwarding server causes all off-site requests to go through that server first. Forwarding servers have the following features.
- They are used to centralize off-site requests.
- The server being used as a forwarder builds up a rich cache of information.
- All off-site queries go through forwarders first.
- They reduce the number of redundant off-site requests.
- No special setup on forwarders is required.
- If forwarders fail to respond to queries, the local server can still contact a remote site, DNS servers itself

DNS Zone Transfer

- The process of replicating a zone file to multiple DNS servers is called zone transfer.
- Zone transfer is achieved by copying the zone file from one DNS server to a second DNS server.
- A main DNS server is the source of the zone information during a transfer.
- The main DNS server can be a primary or secondary DNS server
- A zone transfer appears like a client-server transaction and employs the **Transmission Control Protocol (TCP)**.
- It typically occurs if you set up a new DNS server as a secondary DNS server.
- Zone transfers are frequently used to back up DNS files or to replicate DNS data across several DNS servers.

Contd..



Full zone transfer (AXFR)

Incremental zone transfer (IXFR)

DNS update

- The DNS update functionality enables DNS client computers to register and to dynamically update their resource records with a DNS server whenever changes occur.
- If we use this functionality, we can reduce the requirement for manual administration of zone records, especially for clients that frequently move and use Dynamic Host Configuration Protocol (DHCP) to obtain an IP address
- The DNS service lets client computers dynamically update their resource records in DNS.
- When you use this functionality, We can improve DNS administration by reducing the time that it requires to manually manage zone records.

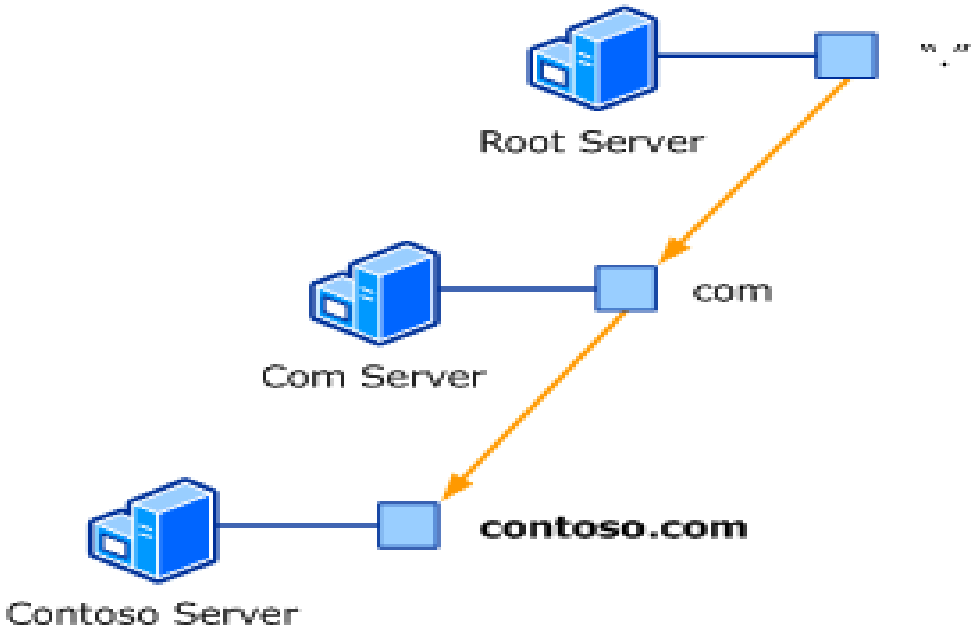
Contd..

- Dynamic DNS is used for IP address management, often for residential or small business customers, or for any business for whom a static IP address is not an option.
- It is also useful for Active Directory functions, remote and changing device location, and remote access.
- Additionally, dynamic DNS is useful for organizations with devices that may move to various locations and even connect to other networks.
- With DDNS, it’s possible to maintain device IP address updates despite these changes.

DNS delegation

- DNS delegation is when a DNS server delegates authority over a part of its namespace to one or more other DNS servers
- DNS delegation is the process when one DNS nameserver delegates its authority to another DNS nameserver (or more DNS nameservers) for a particular part of the domain namespace.
- The root servers have dedicated zones for each TLD server. On their hands, they have delegated zones to each nameserver responsible for a domain name under them.

- For a DNS server to answer queries about any name, it must have a direct or indirect path to every zone in the namespace.
- These paths are created by means of delegation. A delegation is a record in a parent zone that lists a name server that is authoritative for the zone in the next level of the hierarchy.
- Delegations make it possible for servers in one zone to refer clients to servers in other zones


Root Server
"."
com
Com Server
contoso.com
Contoso Server
Legend
Zone
Delegation
Server Hosts Zone

Steps

- The DNS root server hosts the root zone represented as a dot (.).
- The root zone contains a delegation to a zone in the next level of the hierarchy, the com zone.
- The delegation in the root zone tells the DNS root server that, to find the com zone, it must contact the Com server.
- Likewise, the delegation in the com zone tells the Com server that, to find the contoso.com zone, it must contact the Contoso server.

DNS Security

- DNS security is the practice of protecting DNS infrastructure from cyber attacks in order to keep it performing quickly and reliably.
- An effective DNS security strategy incorporates a number of overlapping defenses, including establishing redundant DNS servers, applying security protocols like DNSSEC, and requiring rigorous DNS logging.

How to secure DNS

- DNS Security Extensions (DNSSEC) is a security protocol created to mitigate this problem. DNSSEC protects against attacks by digitally signing data to help ensure its validity. In order to ensure a secure lookup, the signing must happen at every level in the DNS lookup process.
- A DNS firewall is a tool that can provide a number of security and performance services for DNS servers
- NS resolvers can also be configured to provide security solutions for their end users (people browsing the Internet). Some DNS resolvers provide features such as content filtering, which can block sites known to distribute malware and spam, and botnet protection, which blocks communication with known botnets.

DNS Troubleshooting

- DNS troubleshooting follows logical steps from basic network troubleshooting to more in-depth analysis.
- **Check cables**
- **Restart router**
- **Scan for malware**
- **Check the server**

Using commands

- ping
- nslookup
- dig
- host