DNS
Domain Naming Server

Presented By:
Jatin Aggarwal

Topics Covered

- What is DNS
- Why DNS
- DNS Overview (Hierarchical flow)
- Resource Records
- Types of Name Servers
- Authoritative Name Servers
- Zones
- Zone Transfers

What is DNS?

A DNS server is a server (Role installed on the server) that contains a database of public IP addresses and their associated hostnames.

It serves to resolve, or translate, those common names to IP addresses as requested and vice versa.

Why DNS

To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the Internet.

Users prefer to use names instead of numeric addresses. Therefore, we need a system that can map a name to an address or an address to a name.

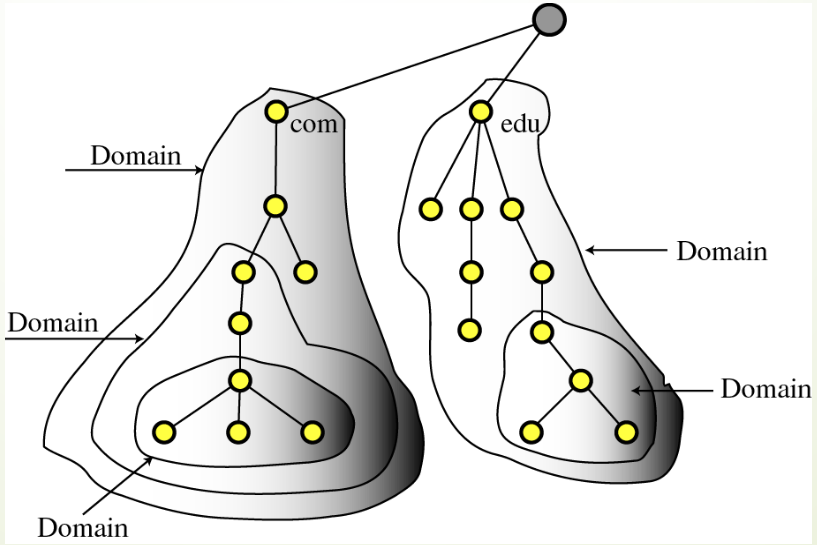
DNS Components

Comprised of three components

- Namespace
- Name servers which make that namespace available
- Resolvers (clients) which query the servers about the name space

Namespace

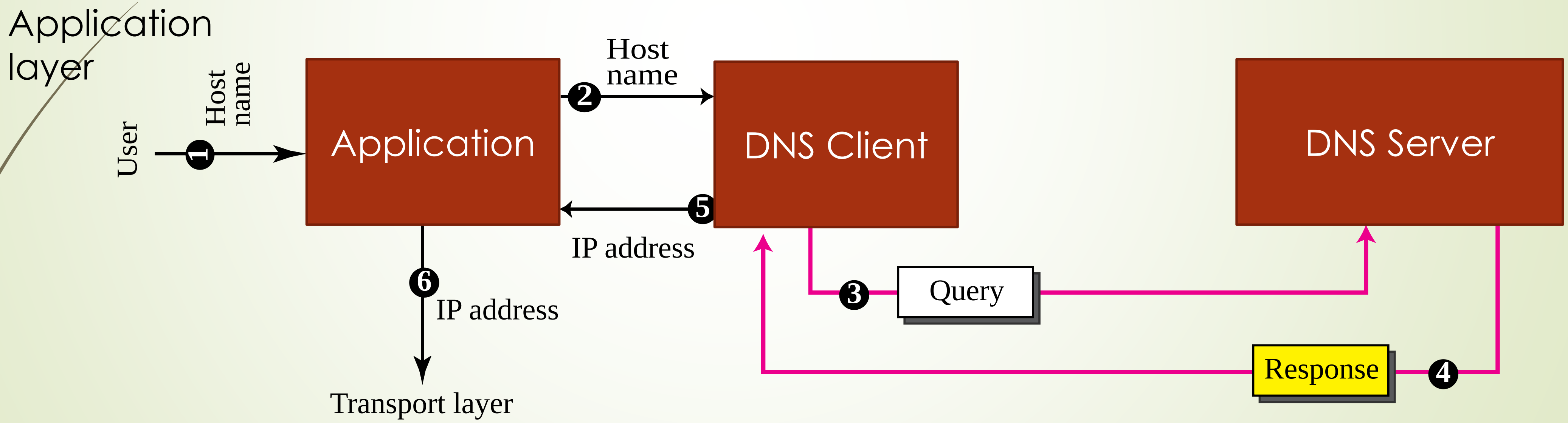
- The namespace is the structure of the DNS database.
- An inverted tree with the root node at the top.
- To be unambiguous, the names assigned to device\server\site must be carefully selected from a name space with complete control over the binding between the names and IP addresses.

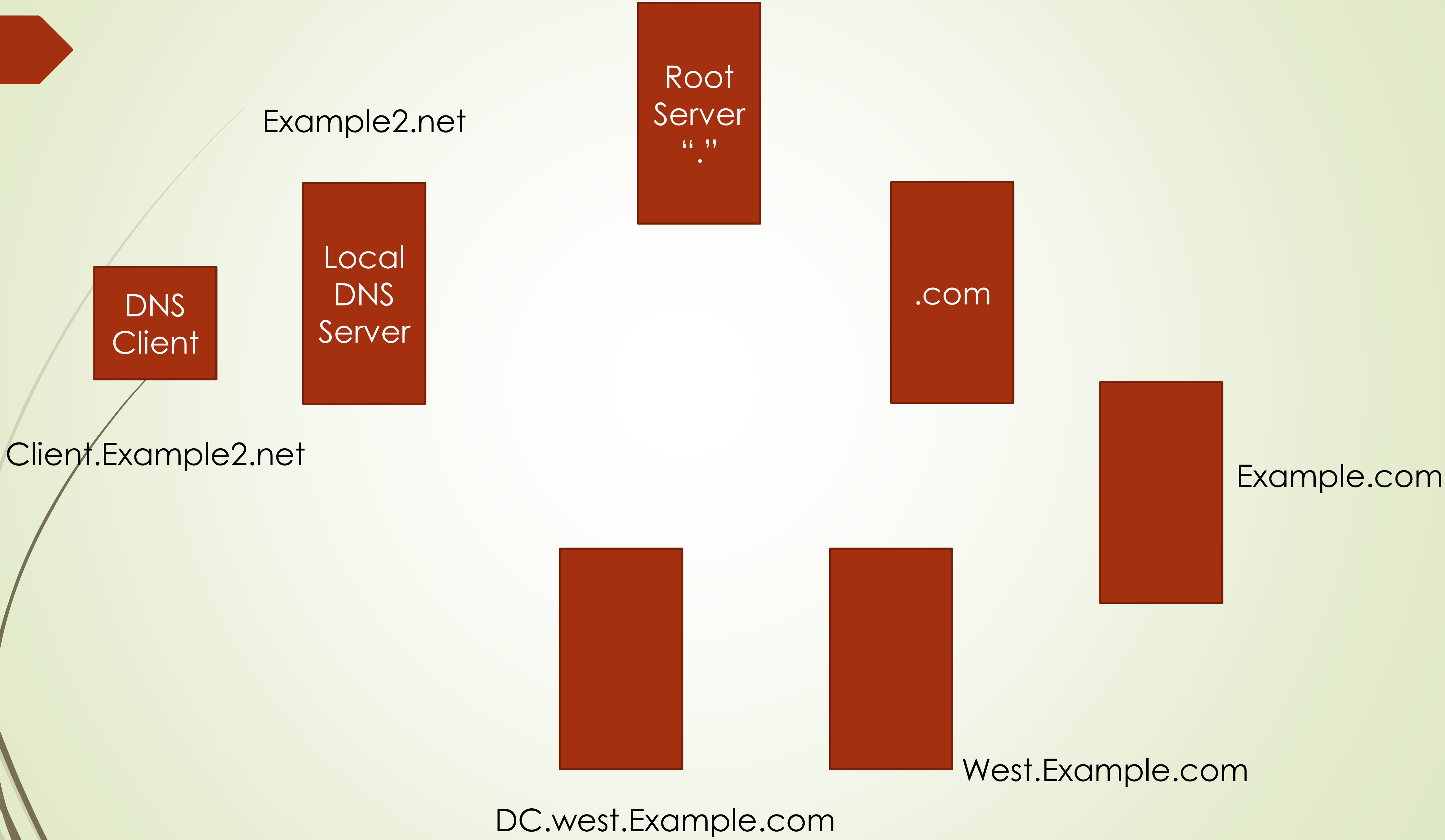


Name Servers

- Name servers store information about the name space in units called “zones”.
- The name servers that load a complete zone are said to “have authority for” or “be authoritative for” the zone
- Usually, more than one name server are authoritative for the same zone
- A single name server may be authoritative for many zones

How DNS Works

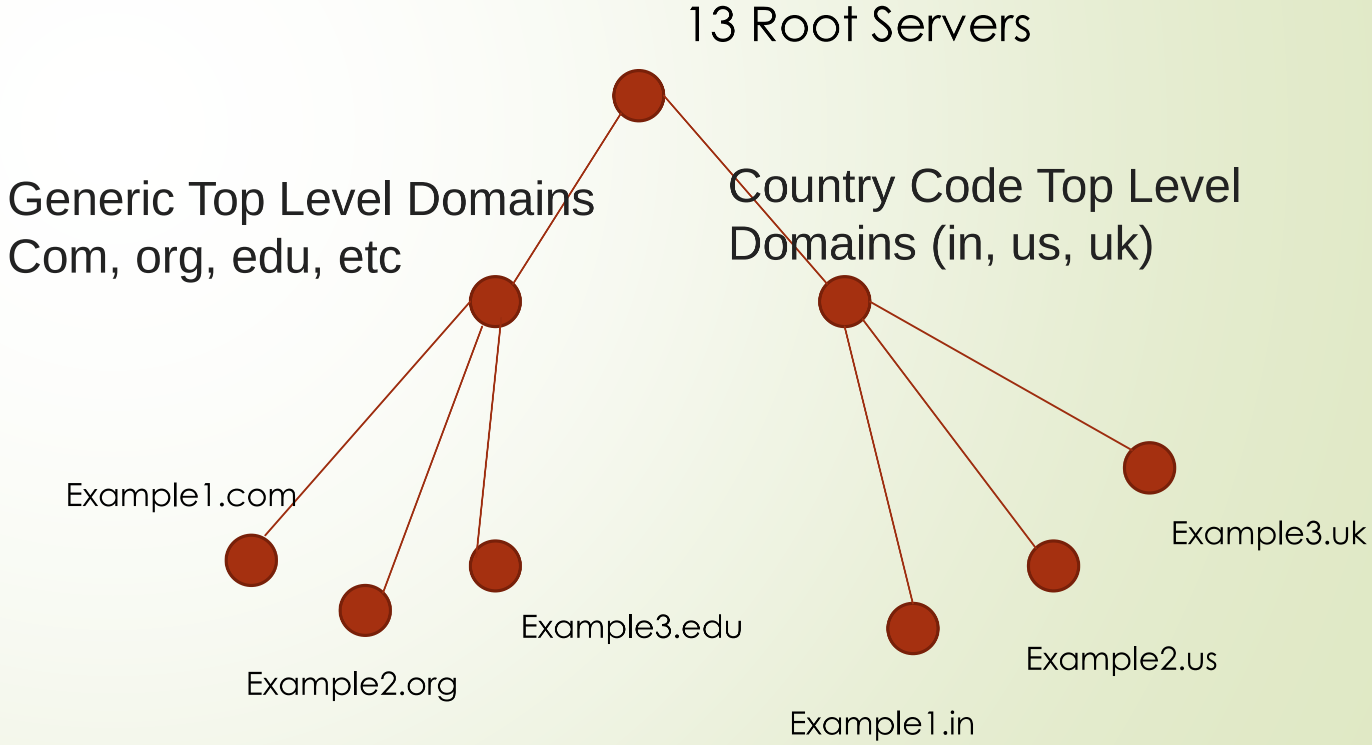



Example2.net
Root Server “.”
Local DNS Server
DNS Client
.com
Client.Example2.net
Example.com
West.Example.com
DC.west.Example.com

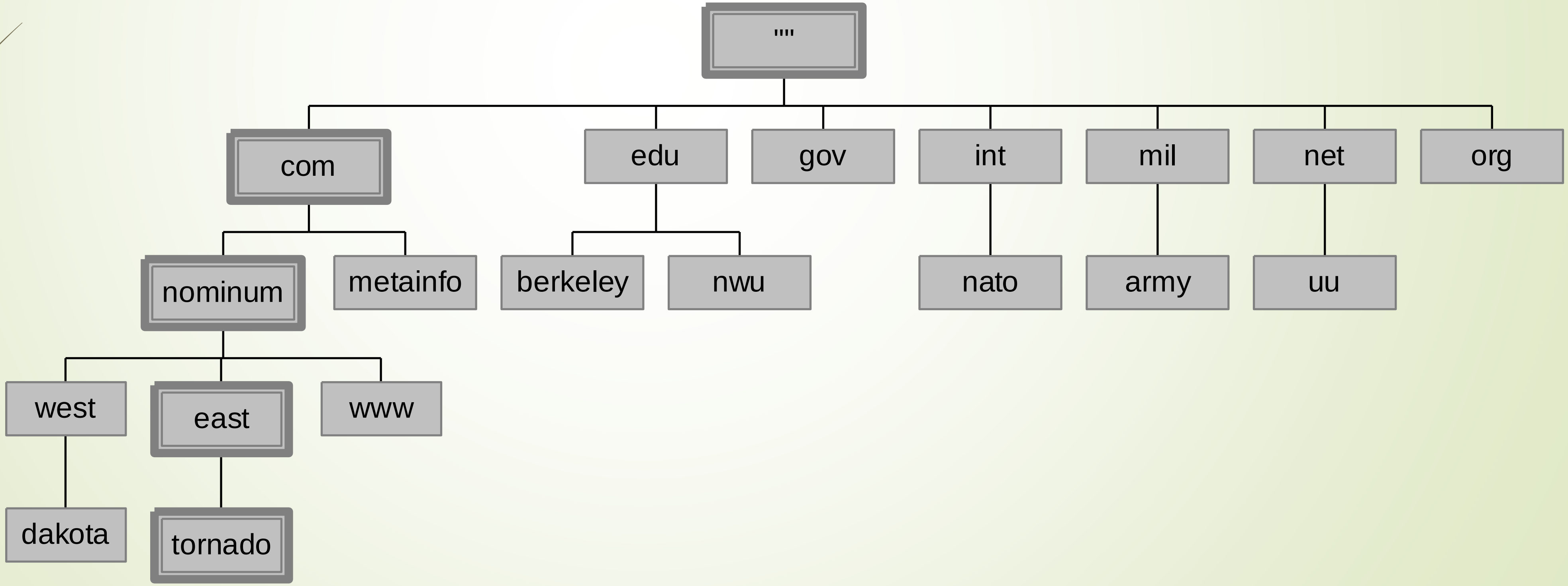
DNS Hierarchical Flow

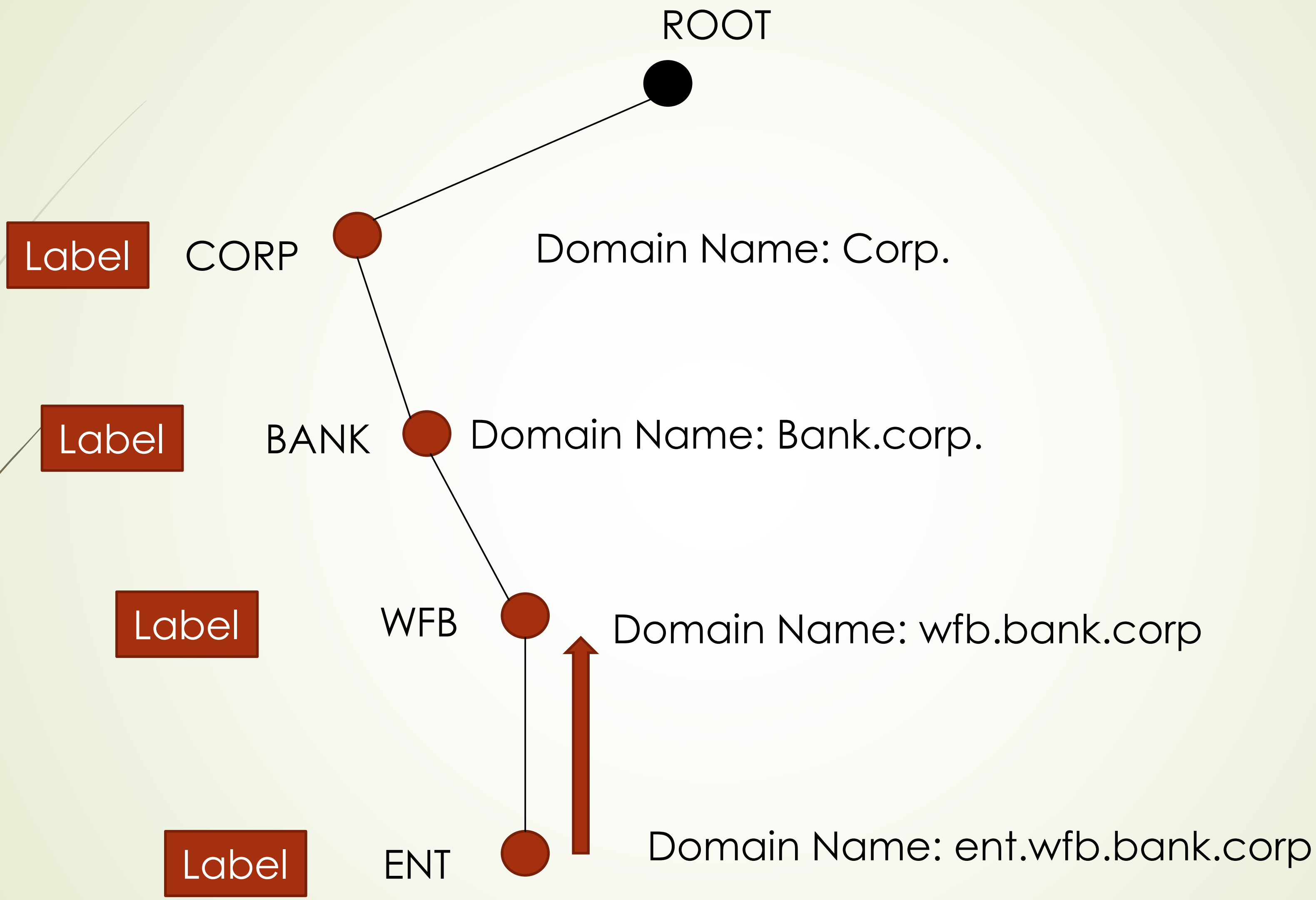
DNS has the inverted tree structure.

Root servers are at the top of the inverted tree, gTLD (Generic Top Level Domains) & CCTLD (Country Code Top Level Domains) comes below the root servers, and then comes the DNS servers of the forest or domain.



- A domain name is the sequence of labels from a node to the root, separated by dots (“.”s), read left to right
  - The name space has a maximum depth of 127 levels
  - Domain names are limited to 255 characters in length
- A node’s domain name identifies its position in the name space





ROOT

Label CORP

Domain Name: Corp.

Label BANK

Domain Name: Bank.corp.

Label WFB

Domain Name: wfb.bank.corp

Label ENT

Domain Name: ent.wfb.bank.corp

Resource Records

- A domain contains resource records
- Resource records are analogous to files in the file structure.
- They are classified into different types. Some of the important types are SOA, NS, A, CNAME and MX.

The “A” Record

- The “Address” record normally used to define a host
- Contains an IPv4 Address (the address computers use to uniquely identify each other on the internet)
- Eg. The record:

```
DNSLAB1          A        203.18.56.31
```

In the example.com domain, defines the host uniquely identifiable as “DNSLAB1.example.com” to be reachable at the IPv4 Address 203.18.56.31

For the IPv6 addresses, the host record is given by Tetra A (AAAA) record.

The “CNAME” Record

•A CNAME defines an alias

•The alias will then be resolved, if another CNAME is encountered then the process continues until an A record is found

•Eg. The record:

```
search                    CNAME        www.google.com.
```

In the example.com domain, defines the name uniquely identifiable as “search.example.com” to be and alias to www.google.com.

The “MX” Record

- An MX record defines the mail servers for a particular domain
- Mail exchange records hold the name of hosts, and their priorities, able to deliver mail for the domain.
- Eg. The record:

```
example.com     MX    10     mail
```

In the example.com domain, defines the host mail to be the priority 10 mail server for the “example.com” domain.

The “NS” Record

- An NS record defines the authoritative Name servers for the domain.

- The NS records also define the name servers of children domains

- Eg. The record:

```
internal            NS     ns1.example1.com.
```

In the example1.com domain, defines the host “ns1.example1.com” to be a name sever for the “example1.com” domain.

Types of Name Server

Primary Name Servers

A Master DNS defines one or more zone files for which this DNS is Authoritative ('type master'). The zone has been delegated (via an NS Resource Record) to this DNS.

Primary DNS Server is simply a server which gets its zone data from a local source as opposed to a Secondary which gets its zone data from an external (networked) source (typically the Primary)

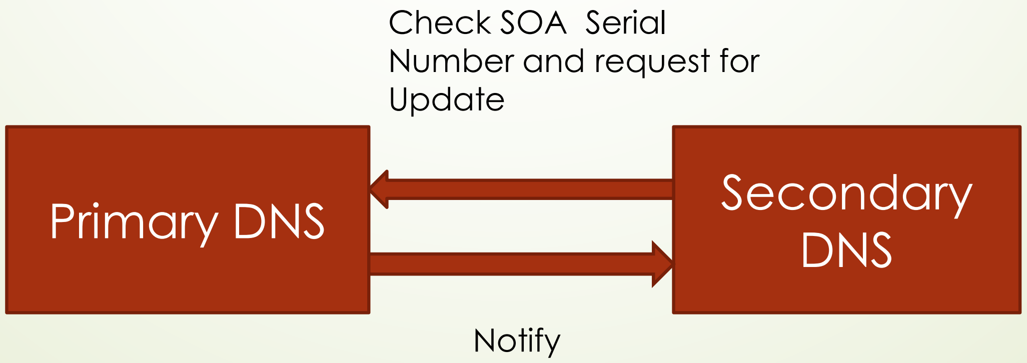
Primary DNS server will NOTIFY zone changes to defined Secondary servers.

NOTIFY messages ensure zone changes are rapidly propagated to the other DNS servers rather than rely on the other DNS servers to periodically keep polling for changes.

Secondary Name Servers

Secondary DNS Server gets its zone data using a zone transfer operation (typically from a Primary) and it will respond as authoritative for those zones for which it has a currently valid zone configuration.

It is impossible to determine from a query result that it came from a zone master or slave



Caching Name Servers

A DNS Caching Server obtains information from another server (Primary DNS) in response to a host query and then saves (caches) the data locally.

On a second or subsequent request for the same data the Caching Server (Resolver) will respond with its locally stored data cache until the time-to-live (TTL) value of the response expires, at which time the server will refresh the data from the Primary.

If the caching server (resolver) obtains its data directly from a zone Primary, it will respond as 'authoritative‘ and if the data is supplied from its cache the response is 'non-authoritative.

Forwarding Name Servers

A forwarding (Proxy) server is one which simply forwards requests to another DNS and caches the results.

Usually carried on during the following scenarios:

- Where access to the external network is slow or,
- The Remote DNS server provides recursive query support resulting in a single query across the network (from the forwarding DNS to the 'forwarded to' DNS) thus reducing traffic congestion.
- Providing a single point at which changes to remote name servers may be managed

Stealth Name Servers

A stealth server is defined as being a name server which does not appear in any publicly visible NS Records for the domain. The stealth server are used for following scenarios:

- The organization needs a public DNS to enable access to its public services e.g. web, mail ftp.
- The organization does not want the world to see any of its internal hosts by interrogation (query or zone transfer)

Authoritative Name Servers

The response to a query is Authoritative under three conditions:

- The response is received from a Zone master.
- The response is received from a Zone slave with non time-expired zone data.
- The response is received by a caching server directly from either a Zone master or slave. If the response is supplied from the cache it is not authoritative.

ZONES

Domains are broken into "zones" for which individual DNS servers are responsible. Zone is a domain/sub-domains delegated to other DNS servers.

A DNS zone is implemented in the configuration system of a domain name server. Historically, it is defined in the zone file, an operating system text file that starts with the special DNS record type Start of Authority (SOA) and contains all records for the resources described within the zone.

A zone file is a sequence of entries for resource records. The description consists of several fields separated by white space (spaces or tabs) as follows <Name><ttl><record class><record type><record data>.

Entire zones can be transferred from a primary DNS server to secondary DNS servers through Zone Transfers.

ZONE TRANSFERS

- Primary server has the "master copy" of a zone and is a R/W copy.
- Secondary servers keep copies of the zone for redundancy usually R only.
- When changes are made to zone data on the primary DNS server, these changes must be distributed to the secondary DNS servers for the zone. This is done through zone transfers.
- DNS servers automatically notifies secondary servers whenever changes are made through a NOTIFY request, and most DNS servers will request a Zone Transfer whenever such a notification is received.
- Secondary servers also periodically check for changes by querying the primary server for the SOA-record of the zone, and checking the serial number.

QUESTIONS

THANK YOU