Domain Name System (DNS)

Role of DNS:

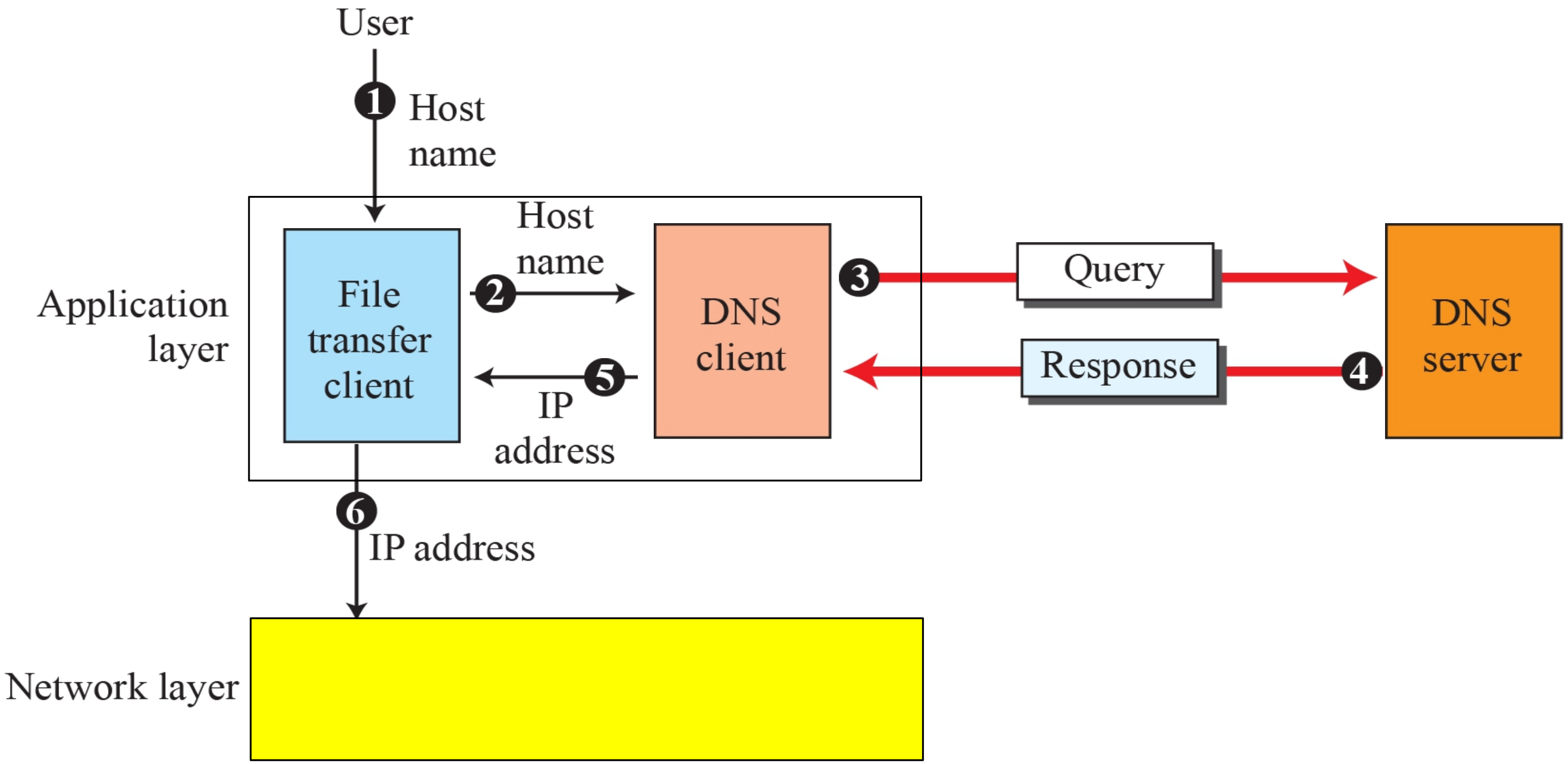
- DNS stands for Domain Name System. The main function of DNS is to translate domain names into IP Addresses, which computers can understand.
- In general, words are easier for people to remember than long, confusing number sequences.
- People prefer to use names instead of numeric addresses. Therefore, the Internet needs to have a directory system that can map a name to an address.
- A **DNS server uses well-known port 53** for all its UDP activities and as its server port for TCP. It uses a random port above 1023 for TCP requests. A **DNS client uses a random port above 1023** for both UDP and TCP.

Working of DNS:

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as DNS resolver sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

Services provided by DNS:

- Host-name to IP address mapping: The Domain Name System (DNS) works on Client Server model. It uses UDP protocol for transport layer communication. DNS uses hierarchical domain based naming scheme.



Host-aliasing:

- A host with a complicated hostname can have one or more alias names. That is when two or more domain names refer to the same account.
- For ex: relay1.west-coast.enterprise.com could have, say, two aliases such as enterprise.com and www.enterprise.com.
- In this case, the hostname relay1.west- coast.enterprise.com is said to be canonical hostname.
- DNS can be invoked by an application to obtain the canonical hostname for a supplied alias hostname as well as the IP address of the host.

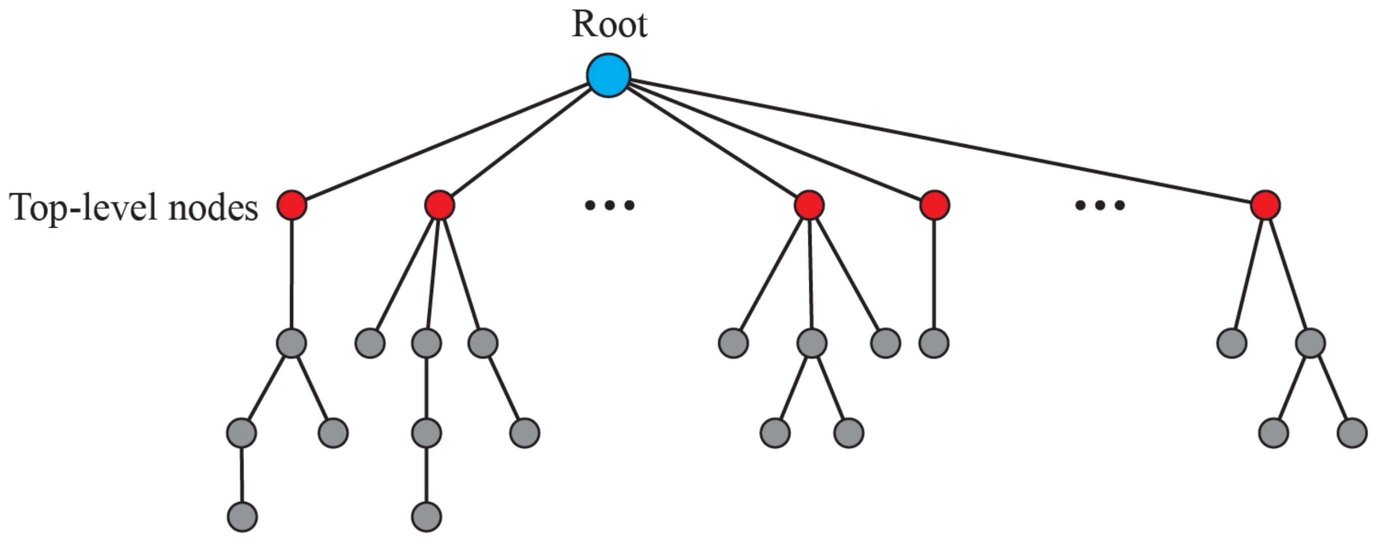
Mail-server aliasing:

- Email aliases can be created on a mail server. The mail server simply forwards email messages addressed to an email alias on to another, the specified email address. **An email alias may be used to create a simple replacement for a long or difficult-to-remember email address.**
- The email address must be mnemonic like bob@hotmail.com.
- The canonical hostname might be something like relay1.west-coast.hotmail.com
- DNS can be invoked by a mail application to obtain the canonical hostname for a supplied alias hostname as well as the IP address of the host.

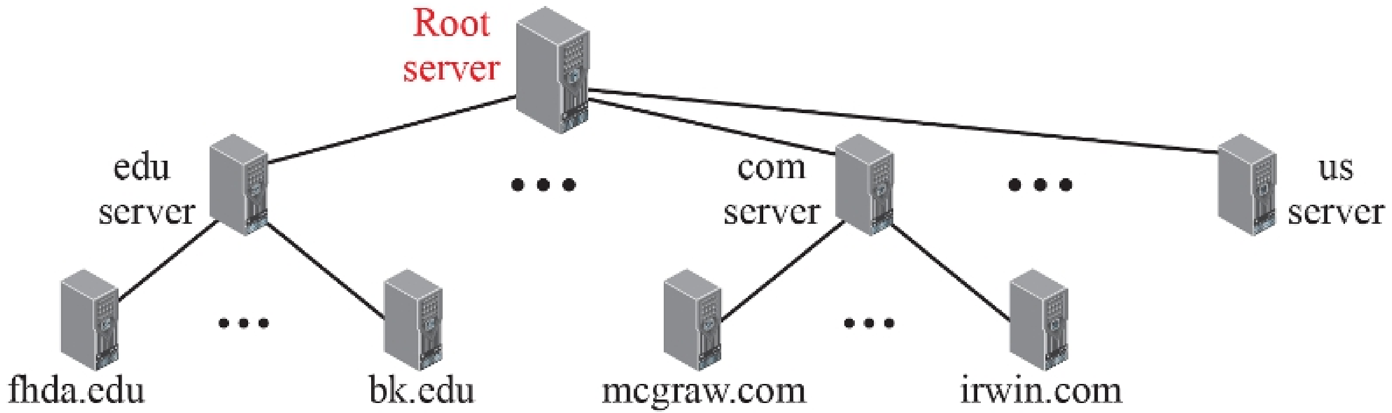
Load distribution:

- It is the practice of configuring a domain in DNS such that client requests to the domain are distributed across a group of servers.
- DNS is also being used to perform load distribution among replicated servers, such as replicated Web servers.
- A set of IP addresses is associated with one canonical hostname.

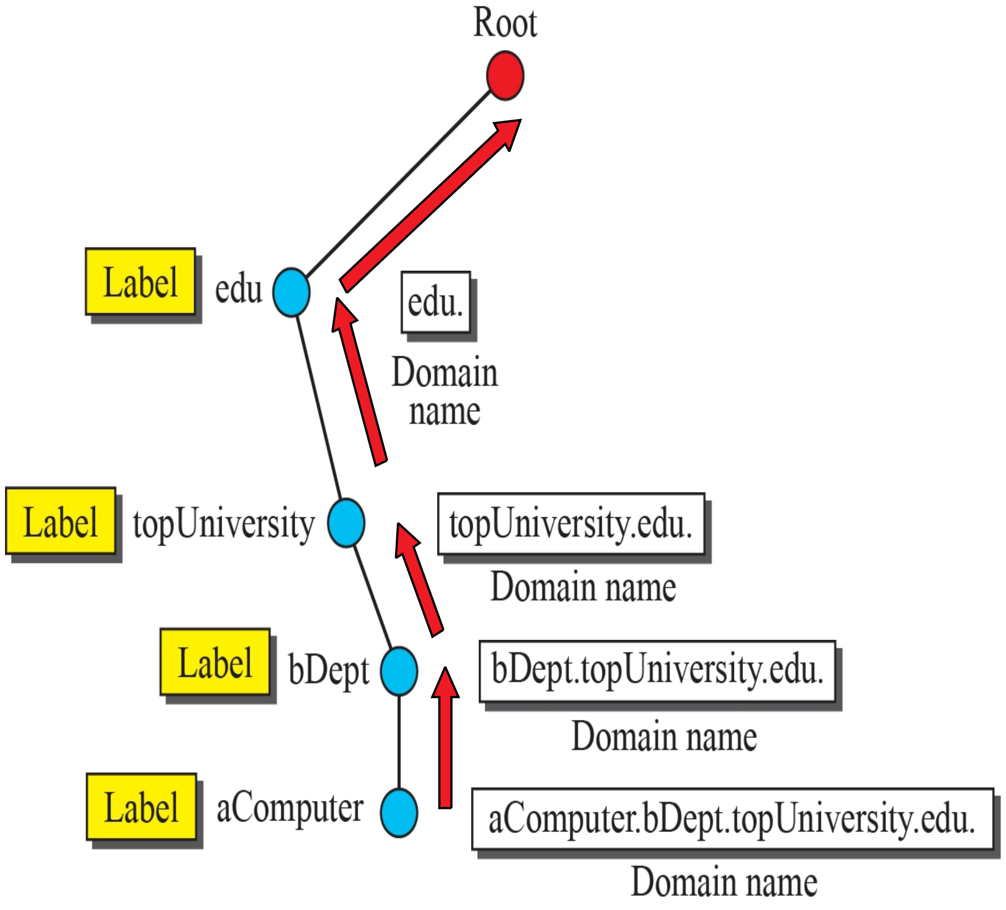
Domain name space



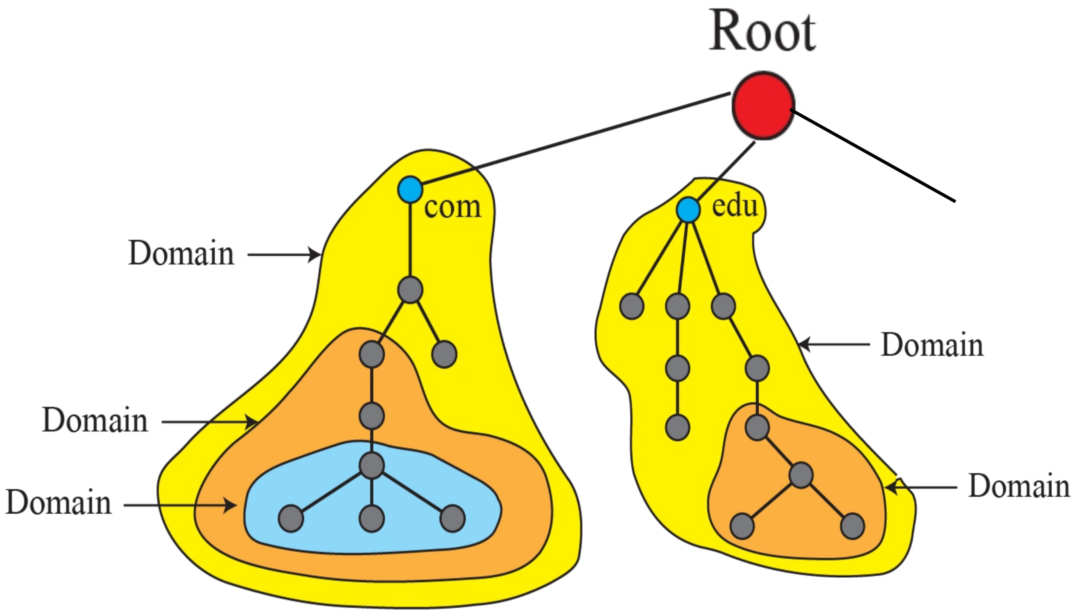
Hierarchy of name servers



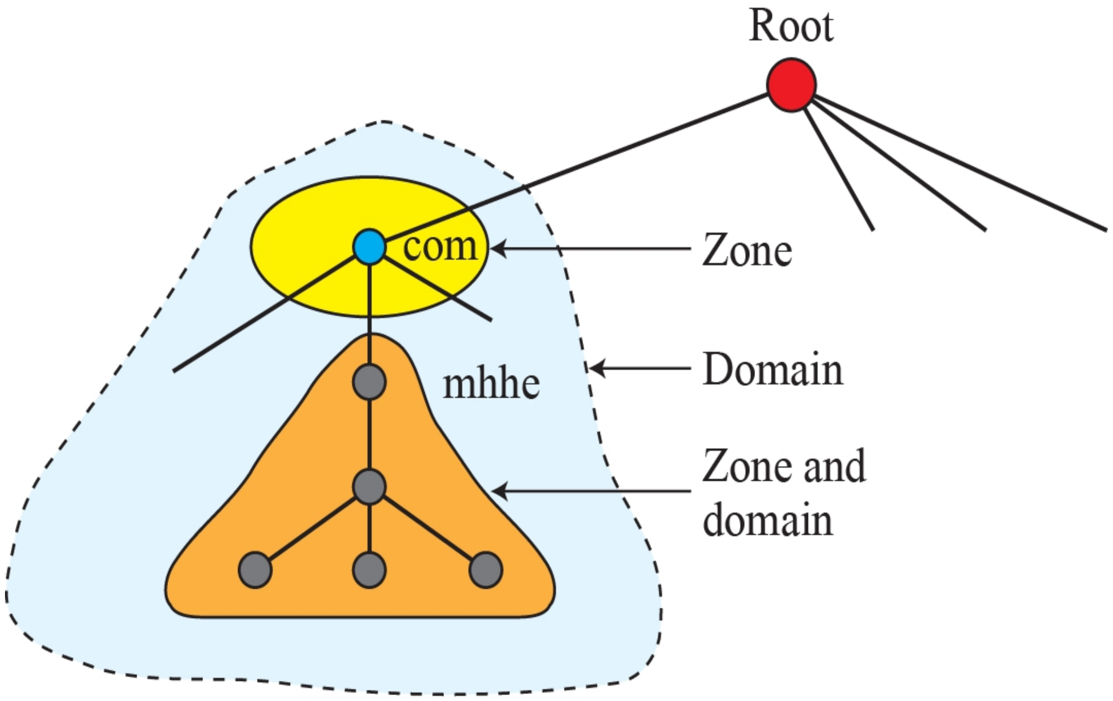
Domain names and labels

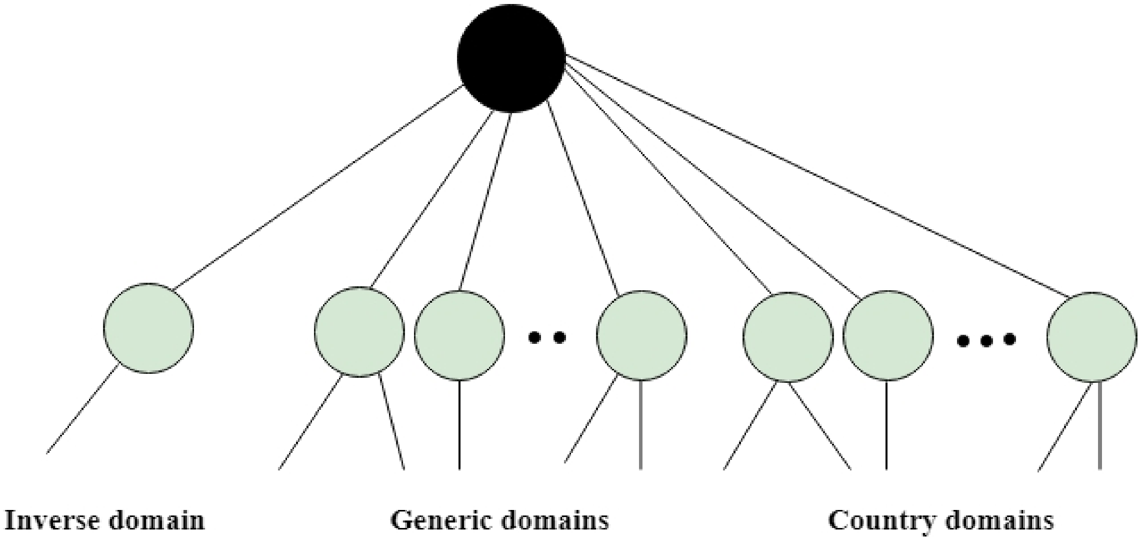


Domains



Zone

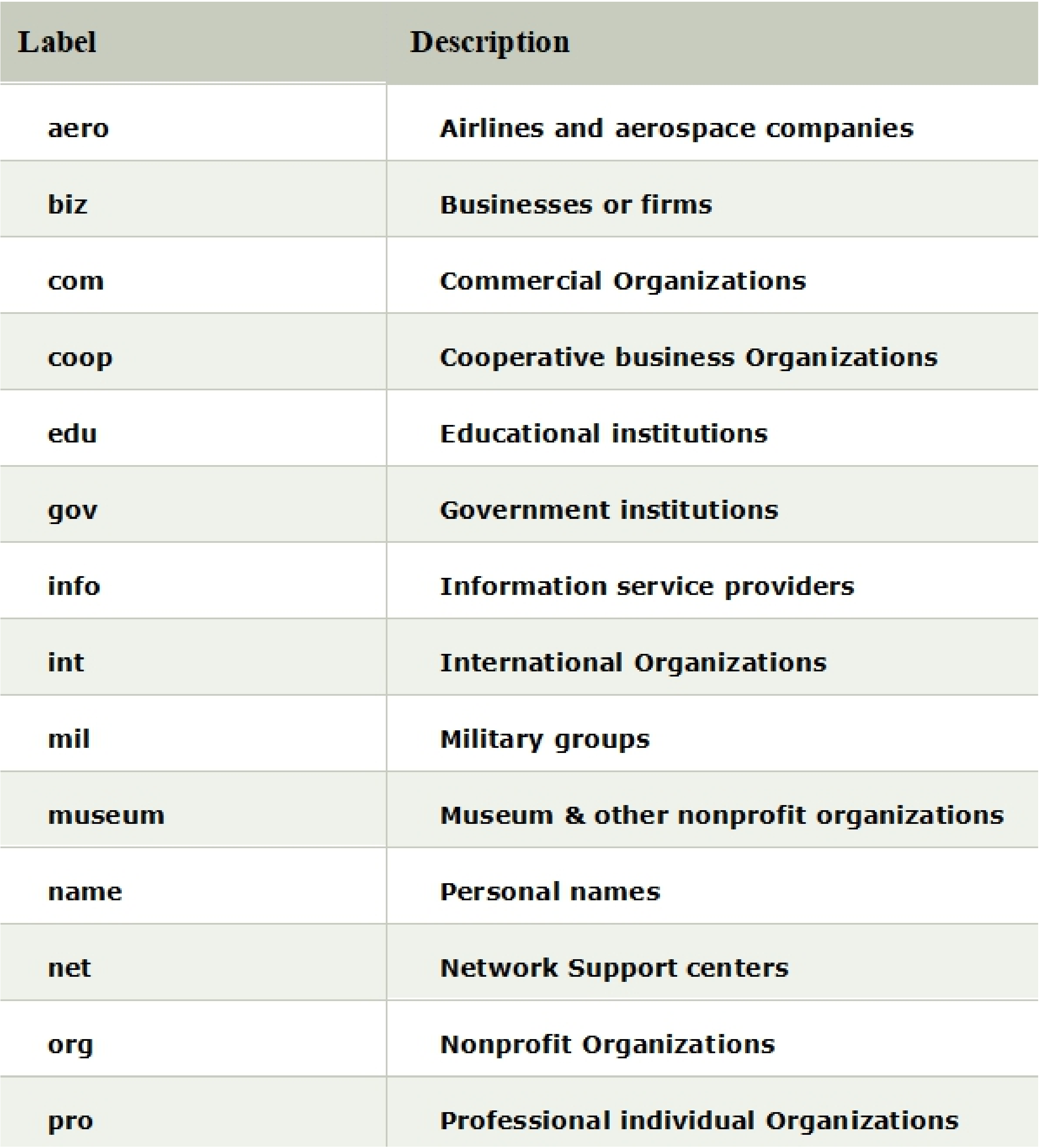




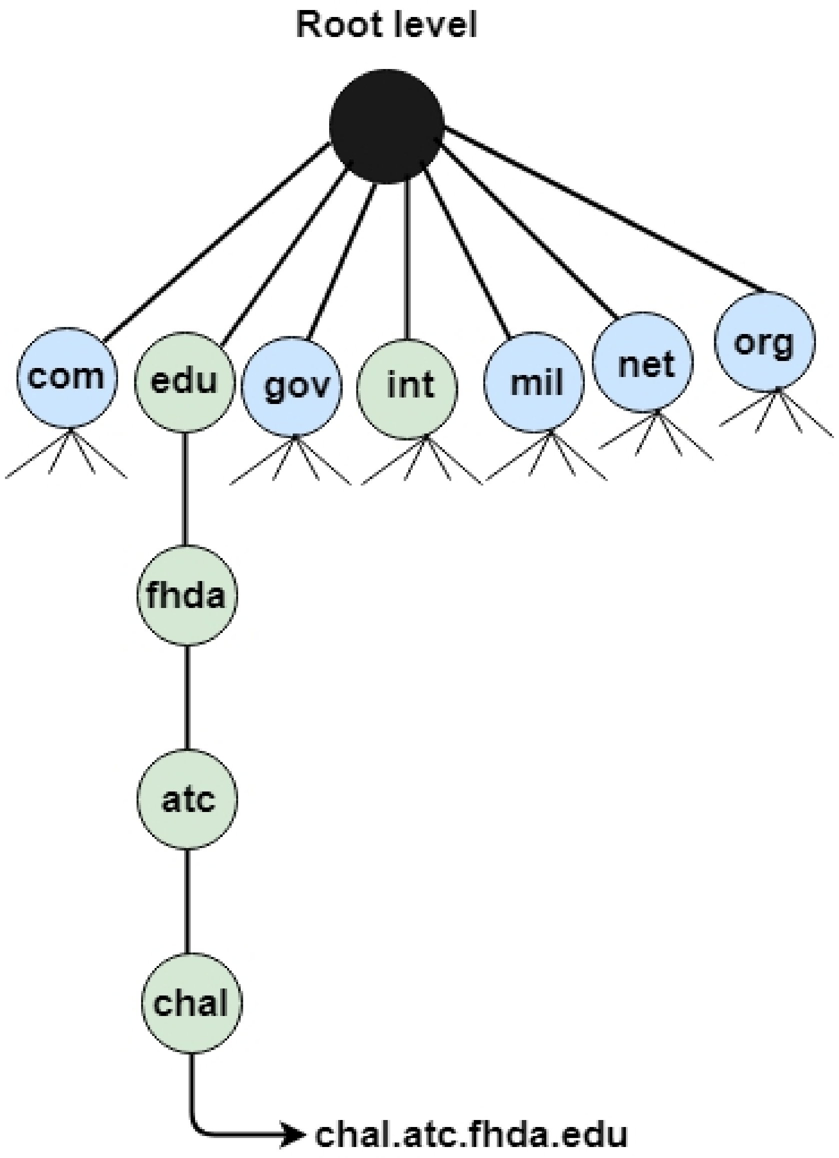
DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

Generic Domains

- It **defines the registered hosts according to their generic behavior**.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.



Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations



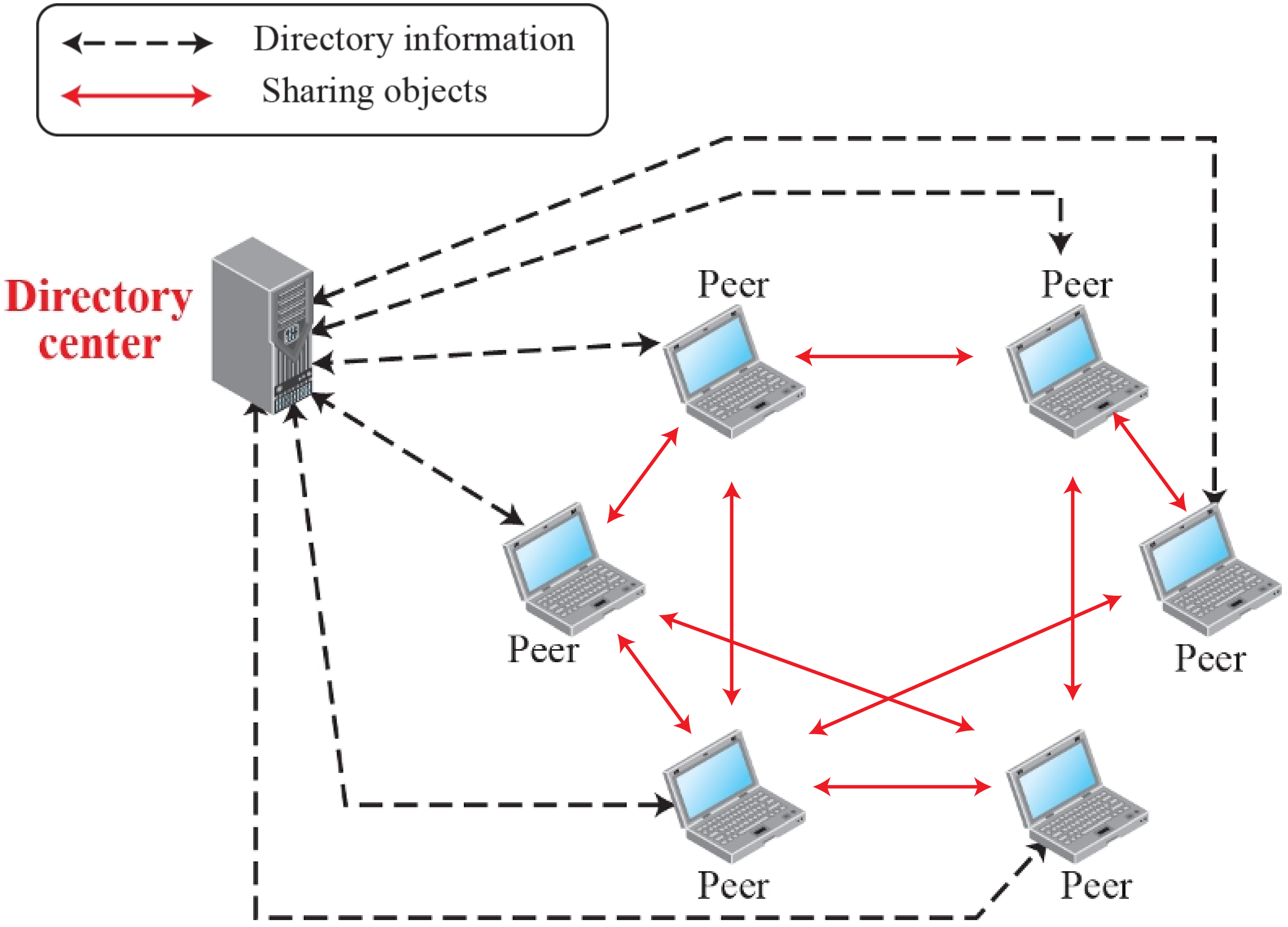
Country Domain

- The format of country domain is same as a generic domain, but it **uses two-character country abbreviations** (e.g., us for the United States) in place of three character organizational abbreviations.

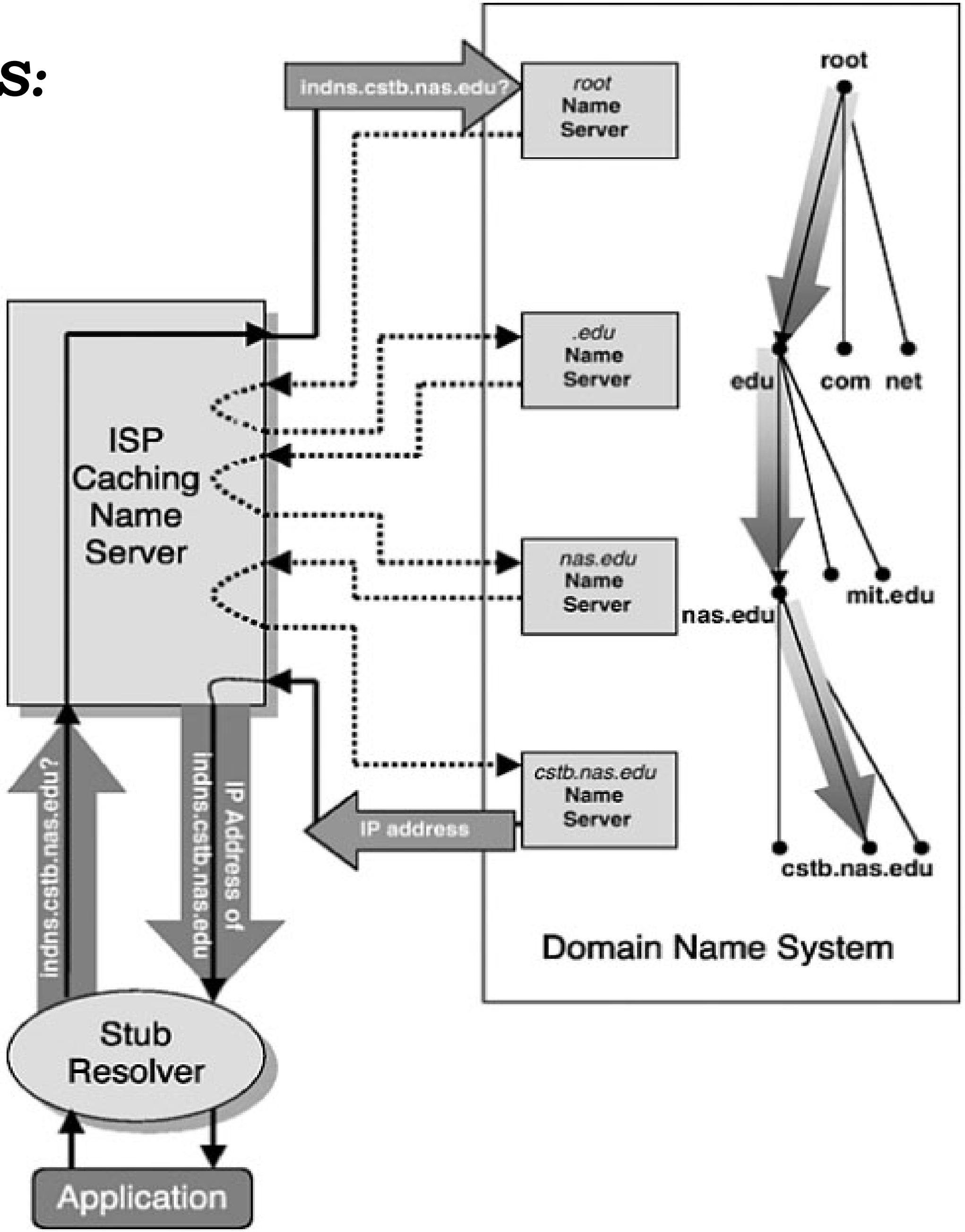
Inverse Domain

- The inverse domain is **used for mapping an address to a name**. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Centralized network



Hierarchically distributed DNS:



DNS Resolution:

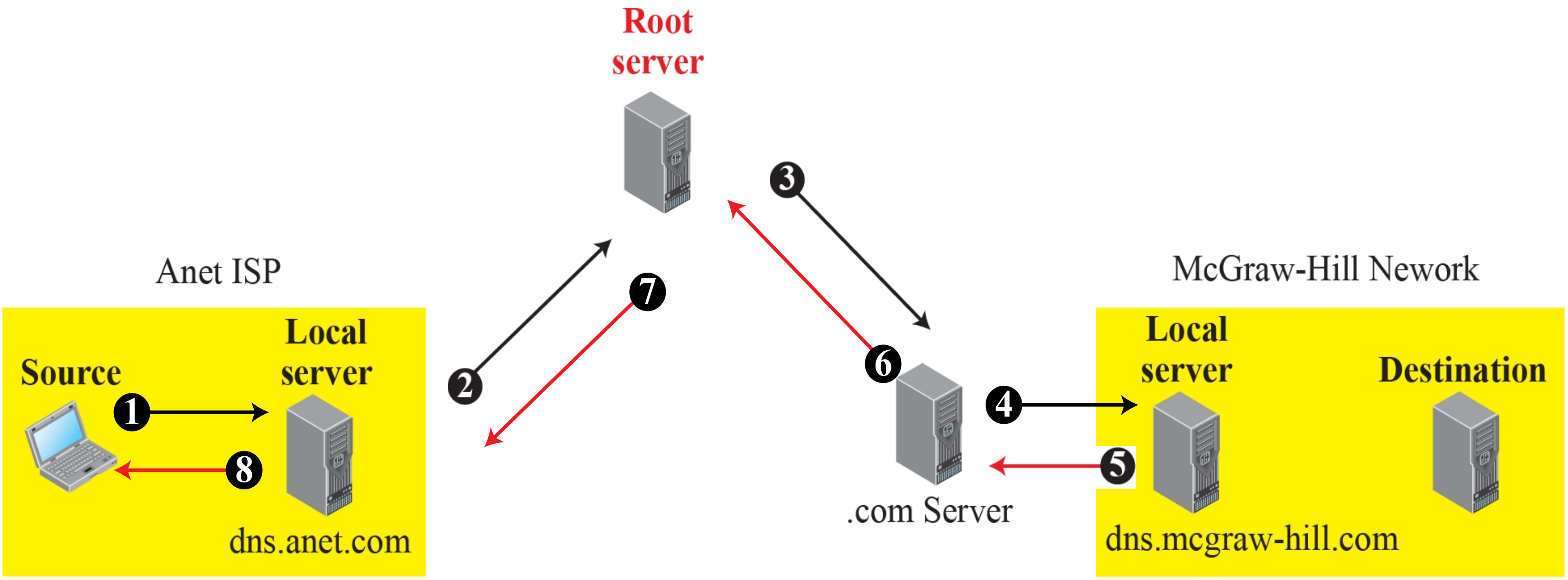
- Mapping a domain name to an IP Address is known as Name-Address **Resolution**. The Domain Name Server (DNS) Resolver performs this operation by consulting name servers.

A resolution can be of two types – **recursive and iterative.**

Recursive Resolution –

- Here, client requires the Local Server to give either the requested mapping or an error message. A DNS Query is generated by the application program to the resolver to fetch the destination IP Address. The Query is then forward to the local DNS Server. If it knows the IP Address, it sends a response to the resolver. Assuming, it does not know the IP Address, it sends the query to the root name server.
- The root name server contains information of about at least one server of Top Level Domain. The query is then sent to the respective Top-Level Domain server. If it contains the mapping, the response is sent back to the root server and then to host's local server. If it doesn't contain the mapping, it should contain the IP Address of destination's local DNS Server. The local DNS server knows the destination host's IP Address. The information is then sent back to the top-level domain server, then to the root server and then to the host's Local DNS Server and finally to the host.

Recursive resolution:

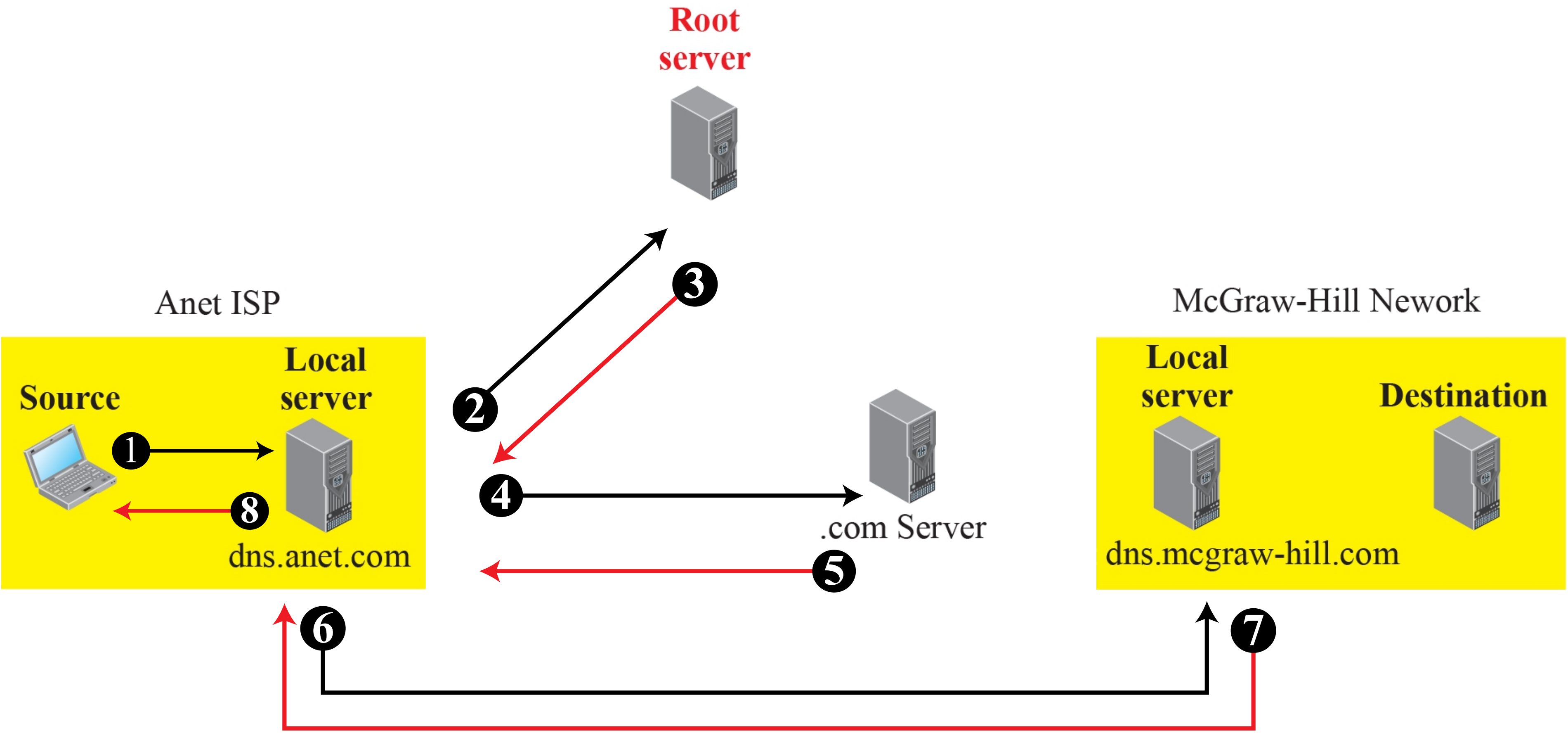


Source: some.anet.com
Destination: engineering.mcgraw-hill.com

Iterative Resolution –

- The main difference between iterative and recursive resolution is that, here each server that does not know the mapping sends the IP Address of the next server to the one requested it. Here, client allows the server to return the best answer it can give as a match or as a referral. A DNS Query is generated by the application program to the resolver to fetch the destination IP Address. The Query is then forward to the local DNS Server. Assuming, it does not know the IP Address, it sends the query to the root name server.
- The root name server returns the IP Address of the Top-Level Domain Server to the Local Server. The Top-Level Domain server is contacted by Local Server and it returns either the IP of the destination host or its local DNS Server. If it returns the server’s address, then by contacting the destination’s Local DNS Server, we get the IP Address of the destination host. The response/mapping is then passed from host’s local DNS server to the resolver and then finally to the host.

Iterative resolution:



Source: some.anet.com
Destination: engineering.mcgraw-hill.com

Caching Mechanism –

- In both iterative and recursive resolution, after a server asks a mapping request from another server, it receives the response and it stores this information in the Cache memory before sending it to the client. This is done to lower the search time it takes for a server to check the IP Address in its Database. So, from the next time, if a request comes to the server, it first checks its cache memory and tries to resolve the request.
- The response is marked as **Unauthoritative** to inform the client that the response is from Cache. The only way caching can be problematic is when server caches the mapping for a long time and the mapping gets outdated.

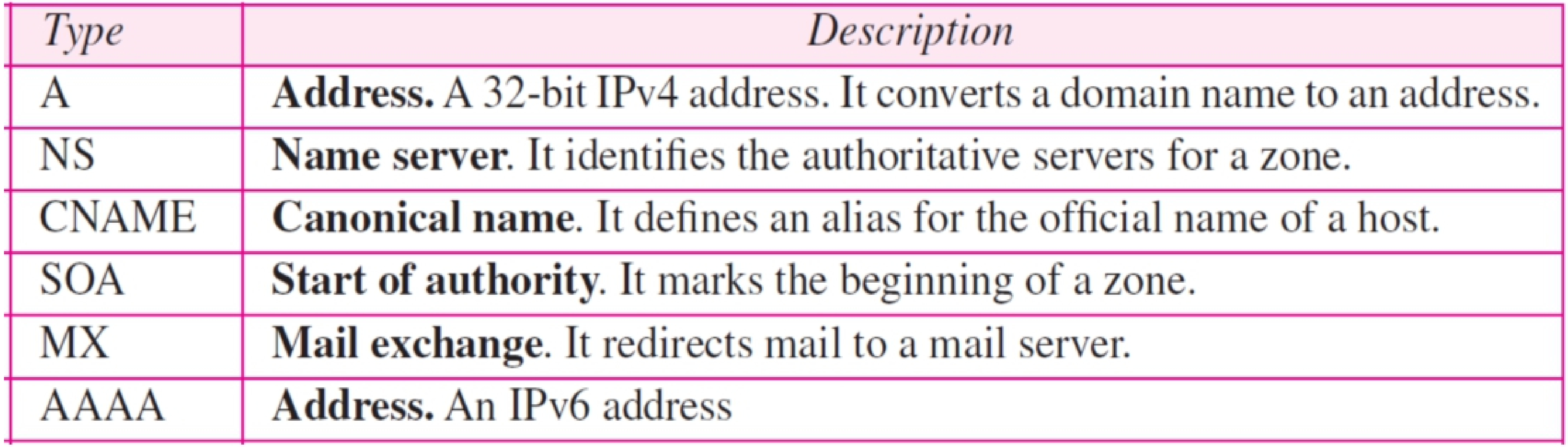
Resourse Records:

- The zone information associated with a server is implemented as a set of resource records. A resource record is a 5-tuple structure, as shown below:

  (Domain name, Type, Class, TTL, Value)

  - ➢The domain name field is what identifies the resource record.
  - ➢The value defines the information kept about the domain name.
  - ➢The TTL defines the number of seconds for which the information is valid.
  - ➢The class defines the type of network (here only class IN (internet) is considered)
  - ➢The type defines how the value should be interpreted

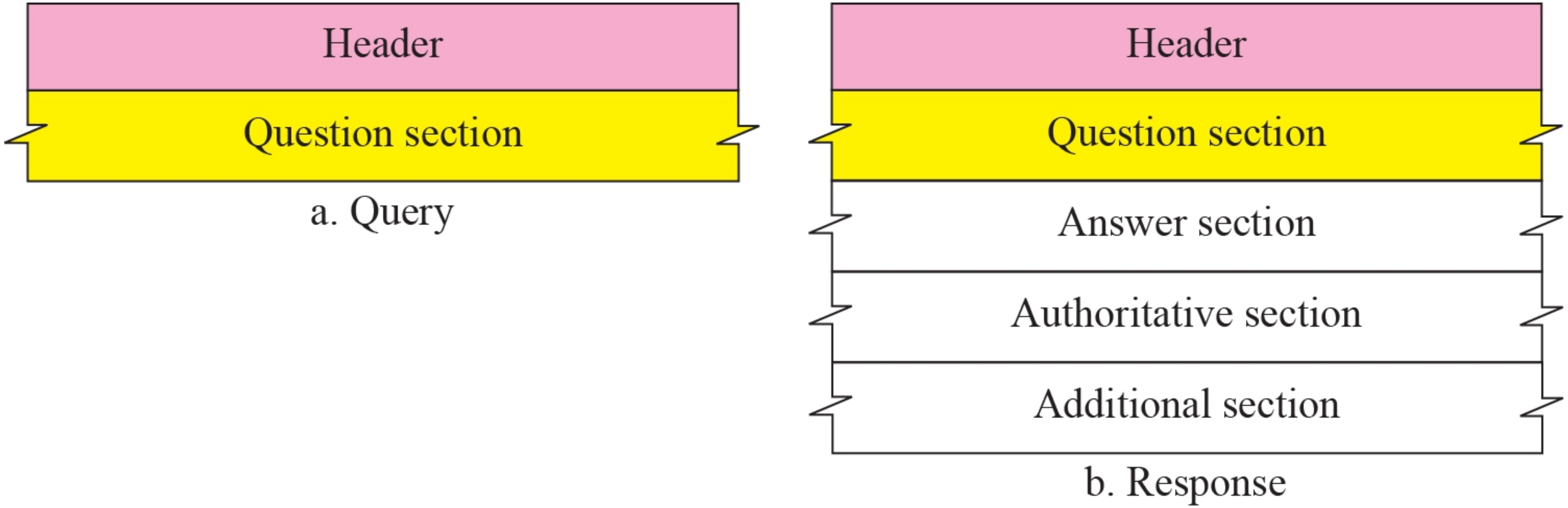
DNS types:



Type	*Description*
A	**Address.** A 32-bit IPv4 address. It converts a domain name to an address.
NS	**Name server**. It identifies the authoritative servers for a zone.
CNAME	**Canonical name**. It defines an alias for the official name of a host.
SOA	**Start of authority**. It marks the beginning of a zone.
MX	**Mail exchange**. It redirects mail to a mail server.
AAAA	**Address.** An IPv6 address

DNS message:

DSN uses two types of messages: query and response



Header

Question section

a. Query

Header

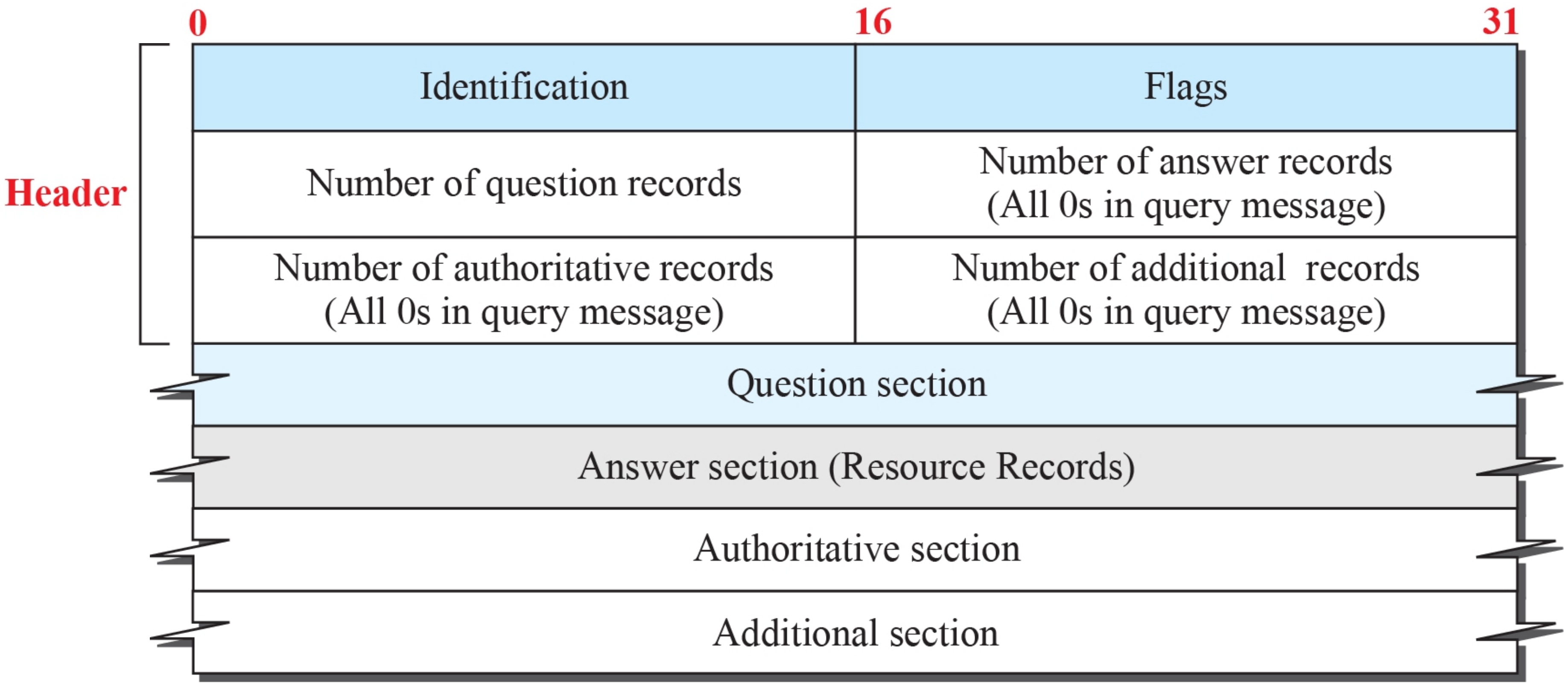
Question section

Answer section

Authoritative section

Additional section

b. Response



0 16 31

Header

Identification

Flags

Number of question records

Number of answer records (All 0s in query message)

Number of authoritative records (All 0s in query message)

Number of additional records (All 0s in query message)

Question section

Answer section (Resource Records)

Authoritative section

Additional section

Note:

The query message contains only the question section.
The response message includes the question section,
the answer section, and possibly two other sections.

- **Identification:** This is a 16-bit field used by the client to match the response with the query. The client uses a different identification number each time it sends a query. The server duplicates this number in the corresponding response.
- The **flag** field defines whether the message is a query or response. It also includes status of error.
- **Question Section:** This is a section consisting of one or more question records. It is present on both query and response messages.
- **Answer Section:** This is a section consisting of one or more resource records. It is present only on response messages. This section includes the answer from the server to the client (resolver).
- **Authoritative Section:** This is a section consisting of one or more resource records. It is present only on response messages. This section gives information (domain name) about one or more authoritative servers for the query.
- **Additional Information Section:** This is a section consisting of one or more resource records. It is present only on response messages. This section provides additional information that may help the resolver.