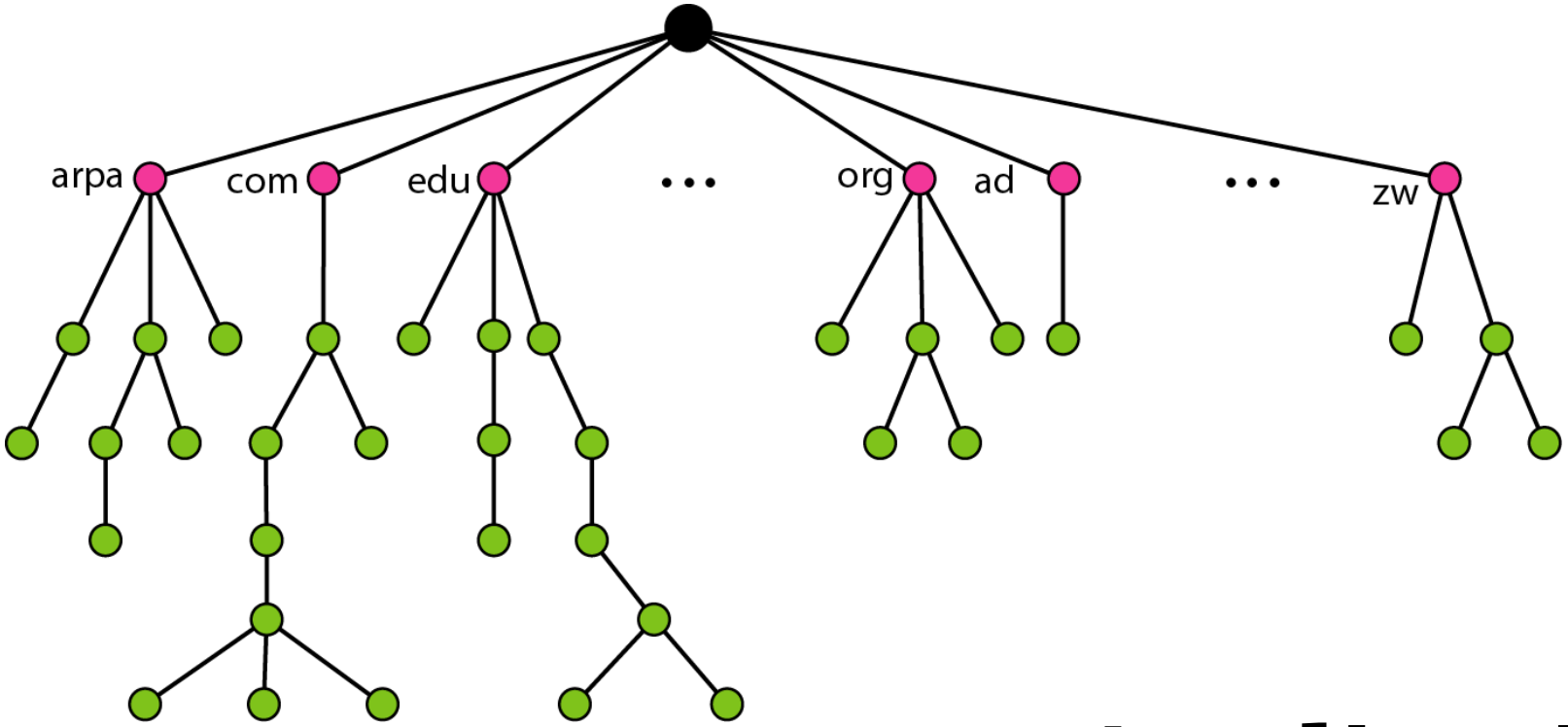
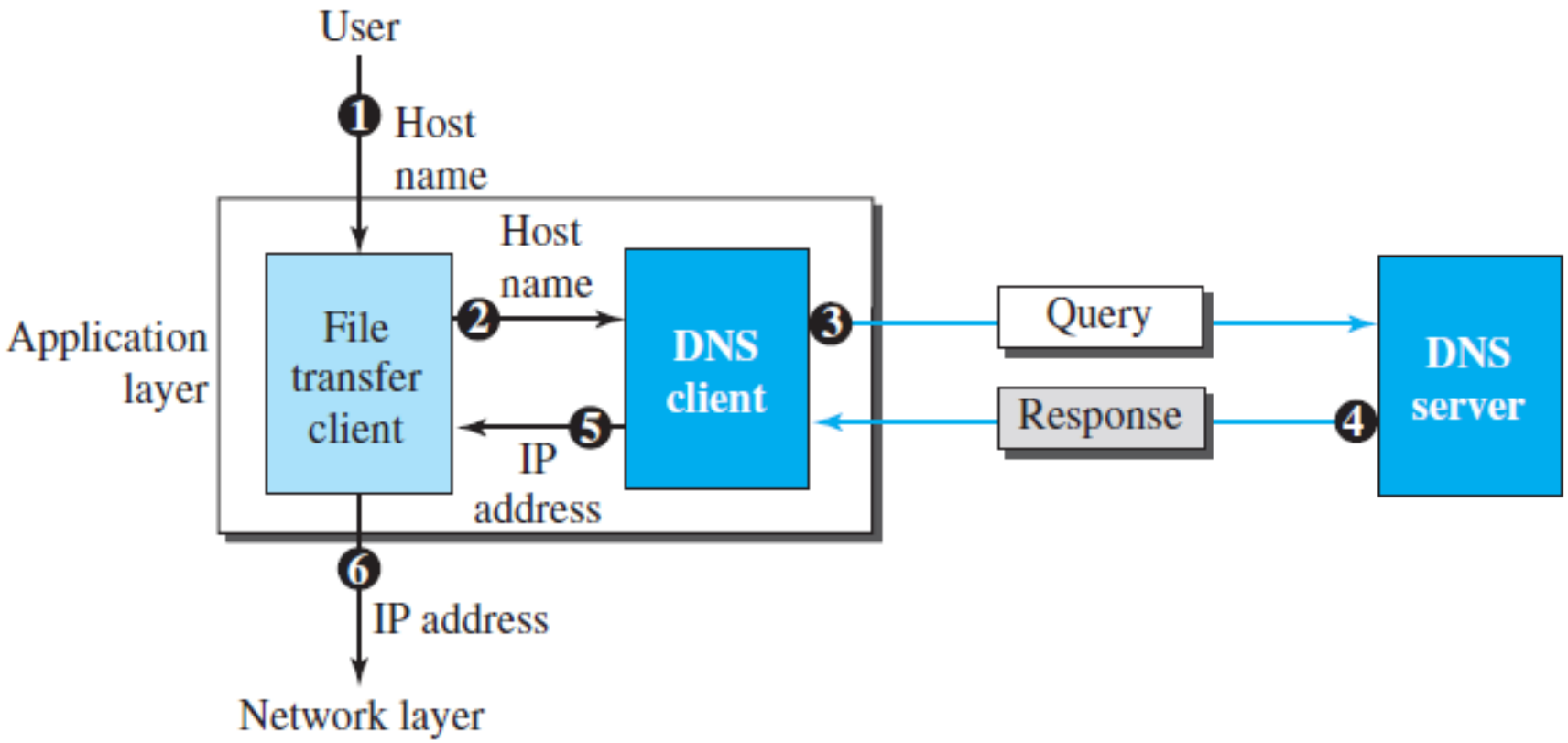


Application Layer
Domain Name System

Purpose of DNS



Purpose of DNS

- TCP/IP suite needs the IP address of the file transfer server to make the connection. The following six steps map the host name to an IP address

1. The user passes the host name to the file transfer client.
2. The file transfer client passes the host name to the DNS client.
3. Each computer, after being booted, knows the address of one DNS server. The DNS client sends a message to a DNS server with a query that gives the file transfer server name using the known IP address of the DNS server.
4. The DNS server responds with the IP address of the desired file transfer server.
5. The DNS server passes the IP address to the file transfer client.
6. The file transfer client now uses the received IP address to access the file transfer server.

Name Space

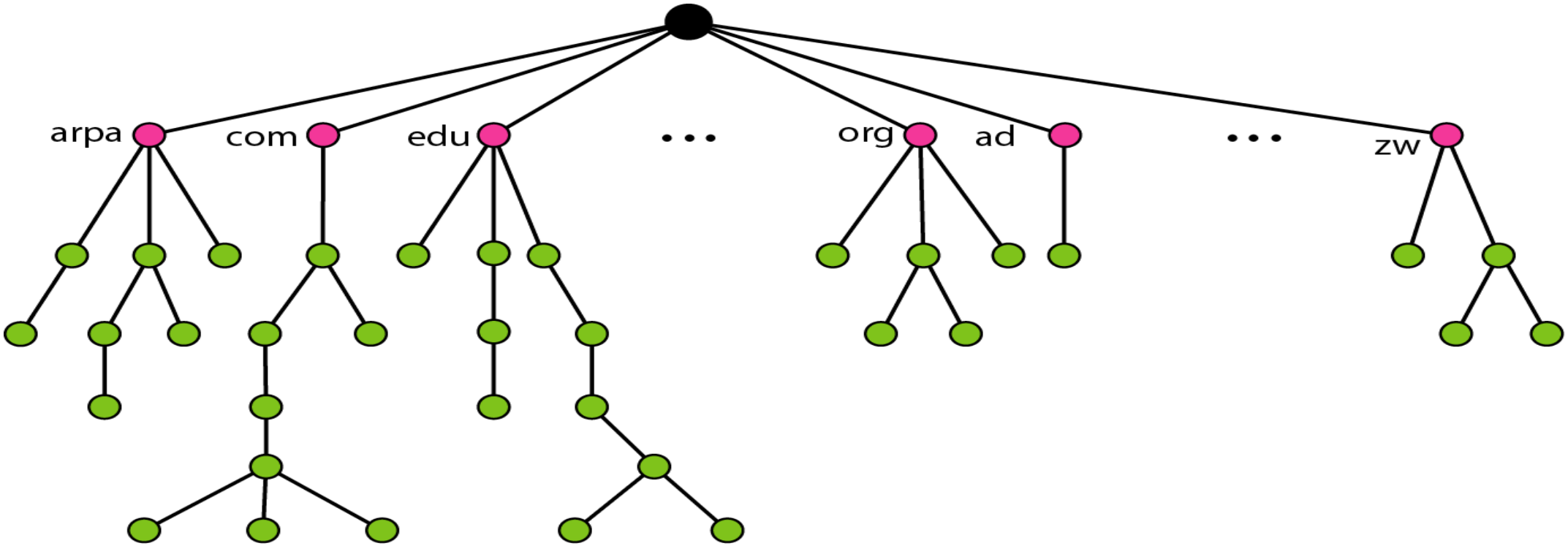
- A name space that maps each address to a unique name can be organized in two ways: flat or hierarchical
- Flat name space
  - A name is assigned to an address.
  - A name in this space is a sequence of characters without structure.
  - The names may or may not have a common section; if they do, it has no meaning.
  - The main disadvantage of a flat name space is that it cannot be used in a large system such as the Internet because it must be centrally controlled to avoid ambiguity and duplication

Name Space

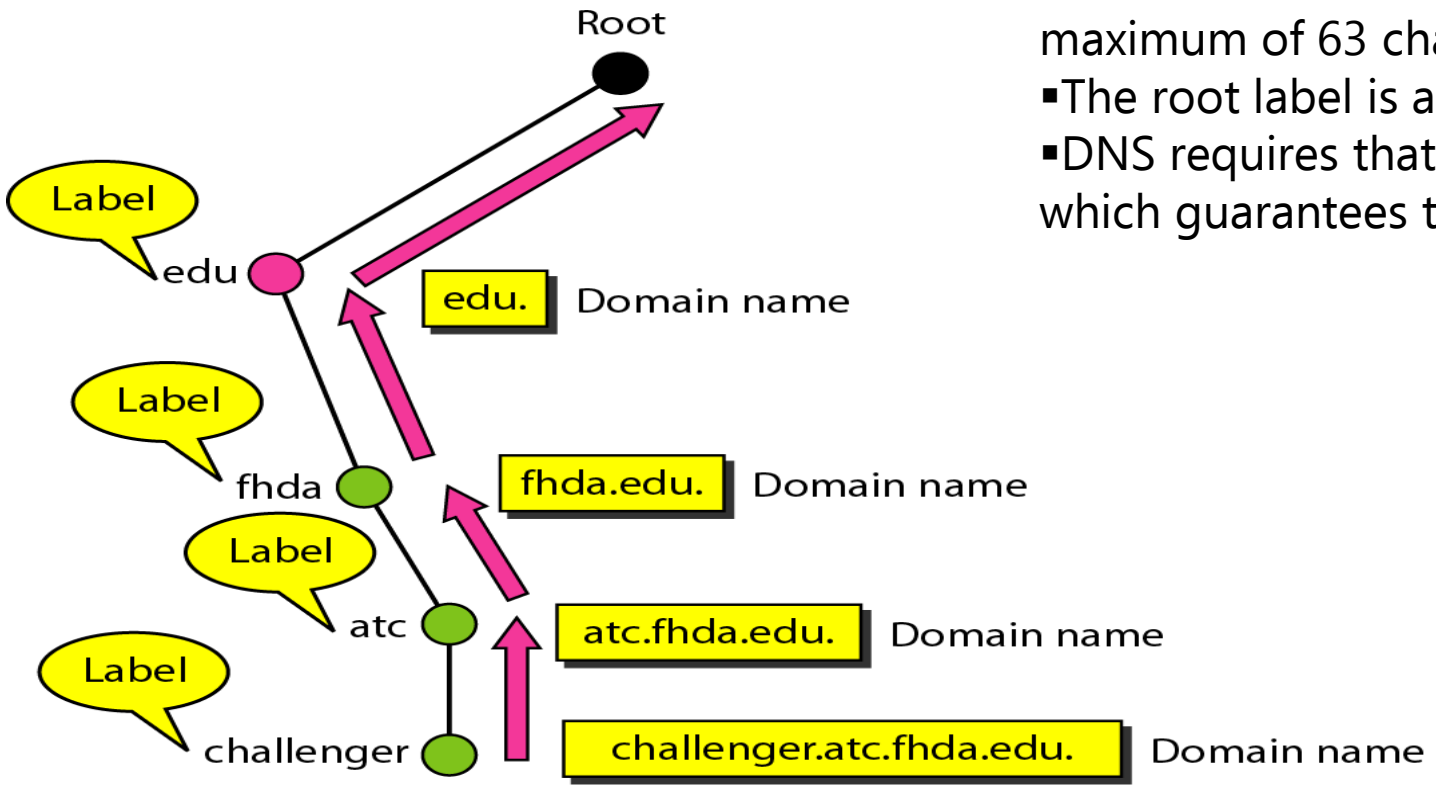
- Hierarchical name space
  - A name is assign each name is made of several parts.
  - The first part can define the nature of the organization, the second part can define the name of an organization, the third part can define departments in the organization, and so on.
  - In this case, the authority to assign and control the name spaces can be decentralized. A central authority can assign the part of the name that defines the nature of the organization and the name of the organization. The responsibility for the rest of the name can be given to the organization itself.
  - The organization can add suffixes (or prefixes) to the name to define its host or resources.

Domain Name Space

- To have a hierarchical name space, a domain name space was designed. In this design the names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels: level 0 (root) to level 127.



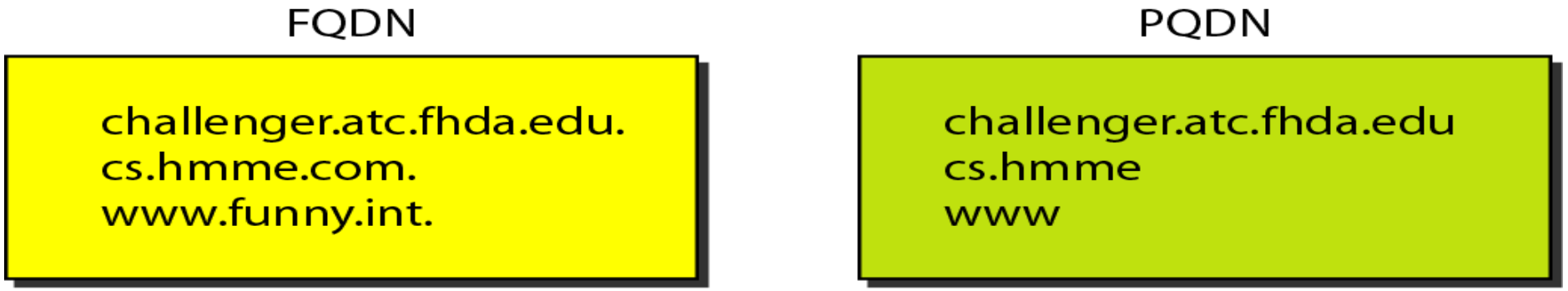
Domain names and labels



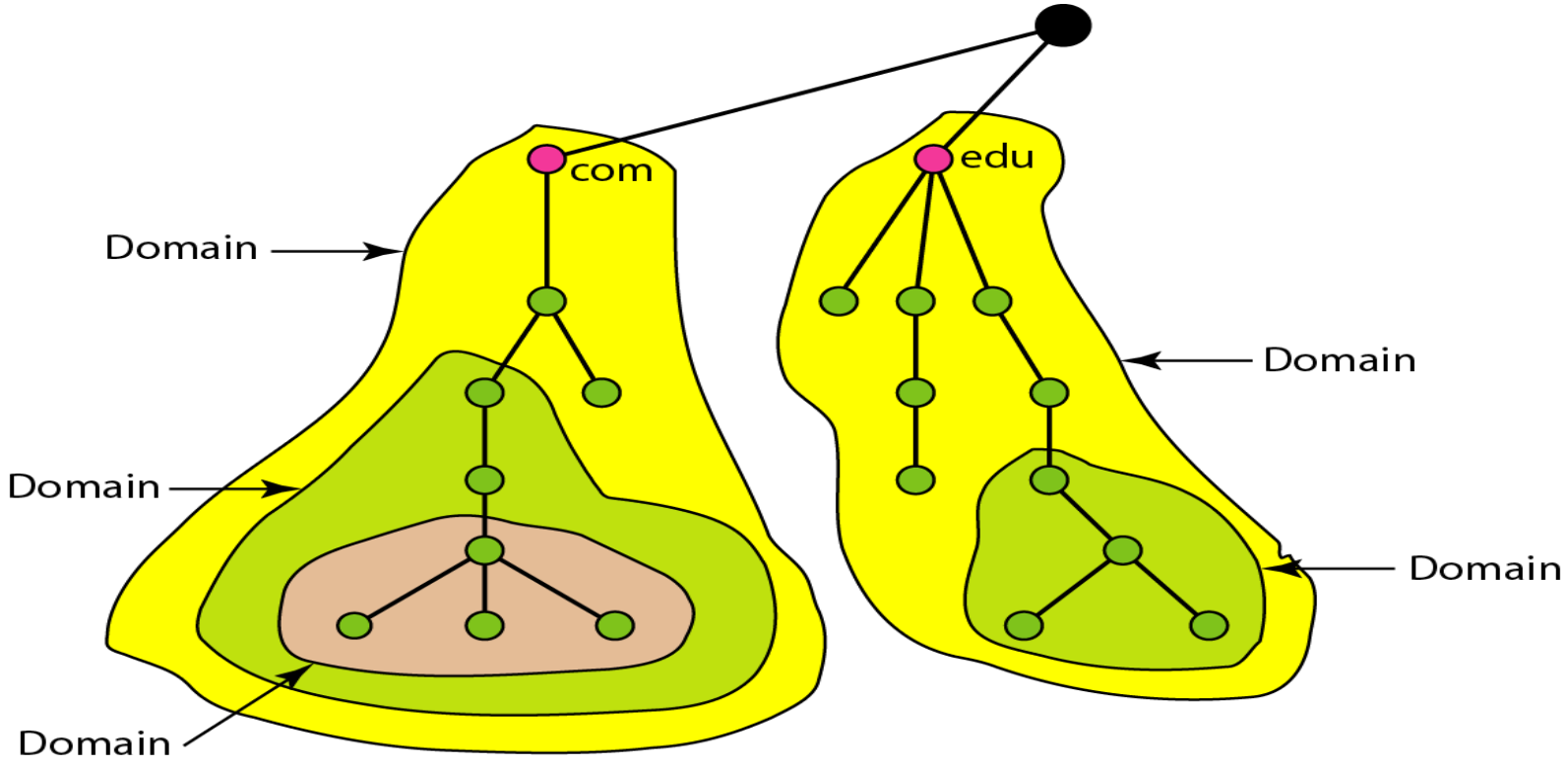
- Labels
  - Each node in the tree has a label, which is a string with a maximum of 63 characters.
  - The root label is a null string (empty string).
  - DNS requires that children of a node have different labels, which guarantees the uniqueness of the domain names.

Domain names and labels

- Domain Name
  - Each node in the tree has a domain name. A full domain name is a sequence of labels separated by dots (.). The domain names are always read from the node up to the root.
  - The last label is the label of the root (null). This means that a full domain name always ends in a null label, which means the last character is a dot because the null string is nothing.



Domains

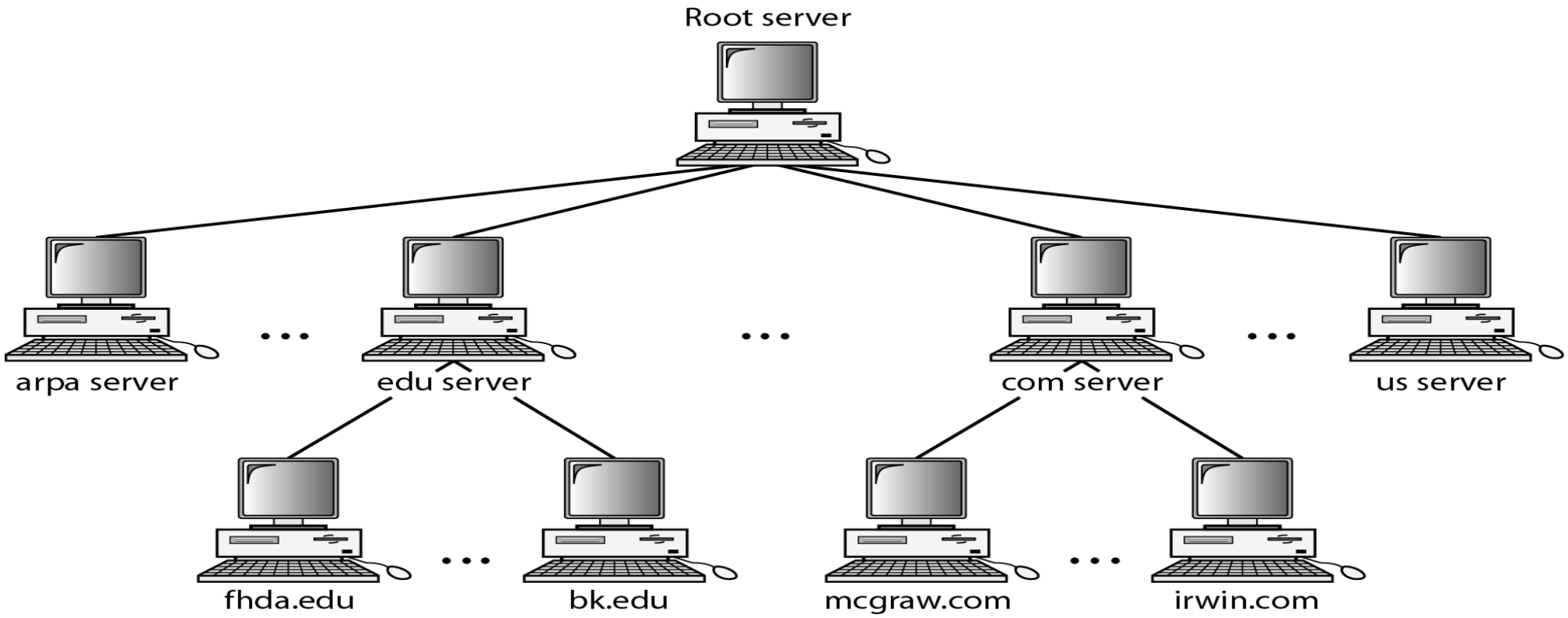


Distribution of Name Space

- The information contained in the domain name space must be stored. However, it is very inefficient and also unreliable to have just one computer store such a huge amount of information.

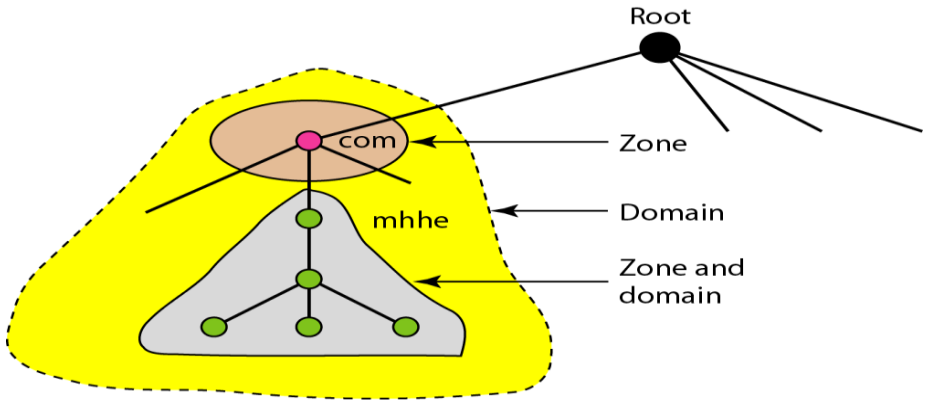
Hierarchy of Name Servers
Zone
Root Server
Primary and Secondary Servers

Hierarchy of name servers



Zones and domains

- Since the complete domain name hierarchy cannot be stored on a single server, it is divided among many servers.
- What a server is responsible for or has authority over is called a zone.
- We can define a zone as a contiguous part of the entire tree. If a server accepts responsibility for a domain and does not divide the domain into smaller domains, the “domain” and the “zone” refer to the same thing.
- The server makes a database called a zone file and keeps all the information for every node under that domain



Root server

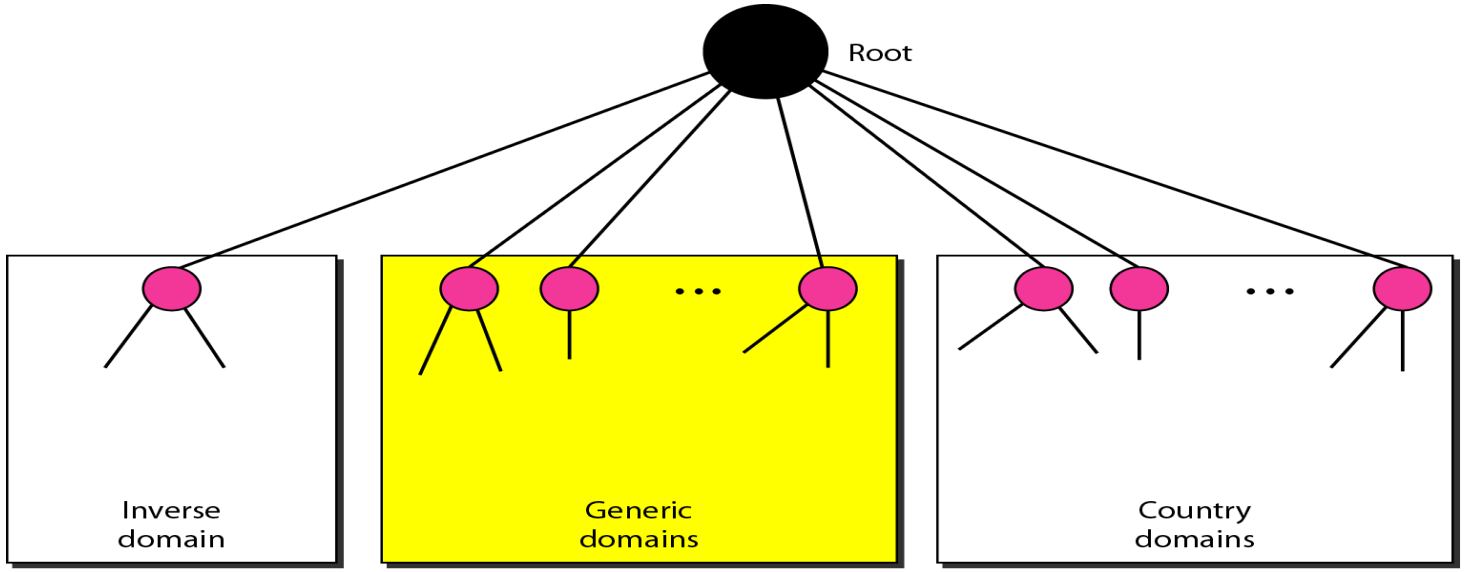
- A root server is a server whose zone consists of the whole tree.
- A root server usually does not store any information about domains but delegates its authority to other servers, keeping references to those servers.
- There are several root servers, each covering the whole domain name space.
- The root servers are distributed all around the world.

A primary server loads all information from the disk file; the secondary server loads all information from the primary server.

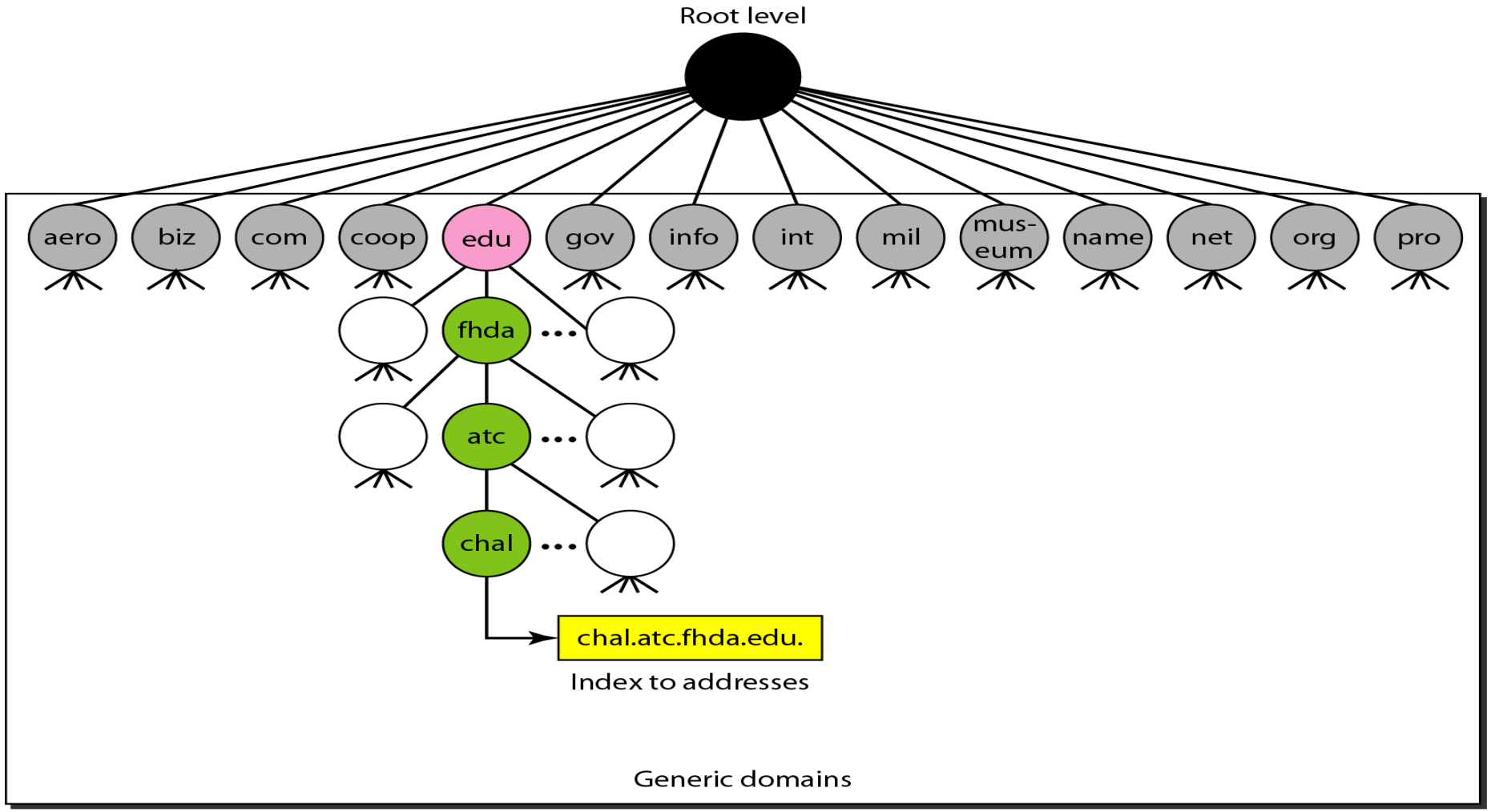
When the secondary downloads information from the primary, it is called zone transfer.

DNS in the internet

- DNS is a protocol that can be used in different platforms.
- In the Internet, the domain name space (tree) is divided into three different sections: generic domains, country domains, and the inverse domain.
- However, due to the rapid growth of the Internet, it became extremely difficult to keep track of the inverse domains, which could be used to find the name of a host when given the IP address



Generic domains

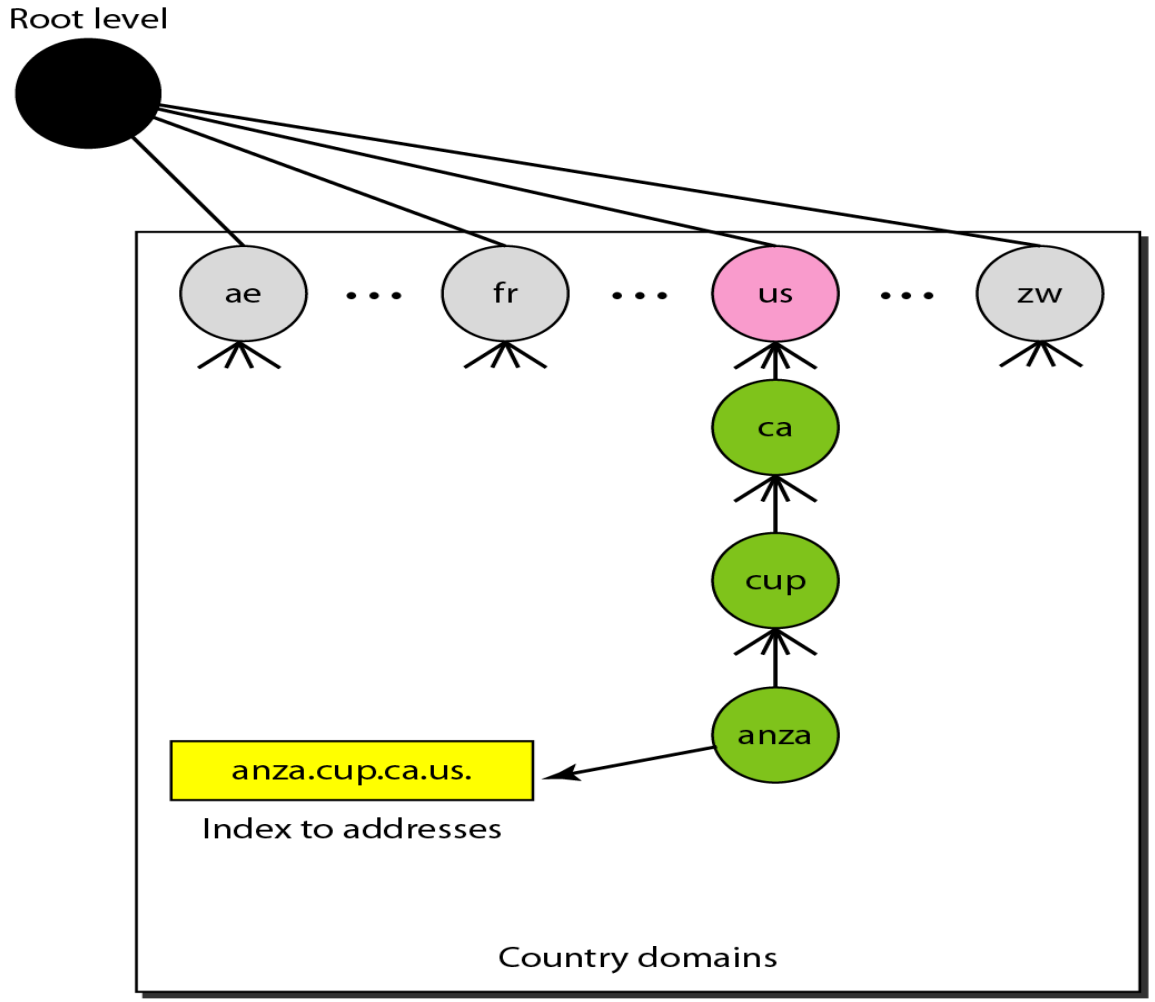


Generic domains

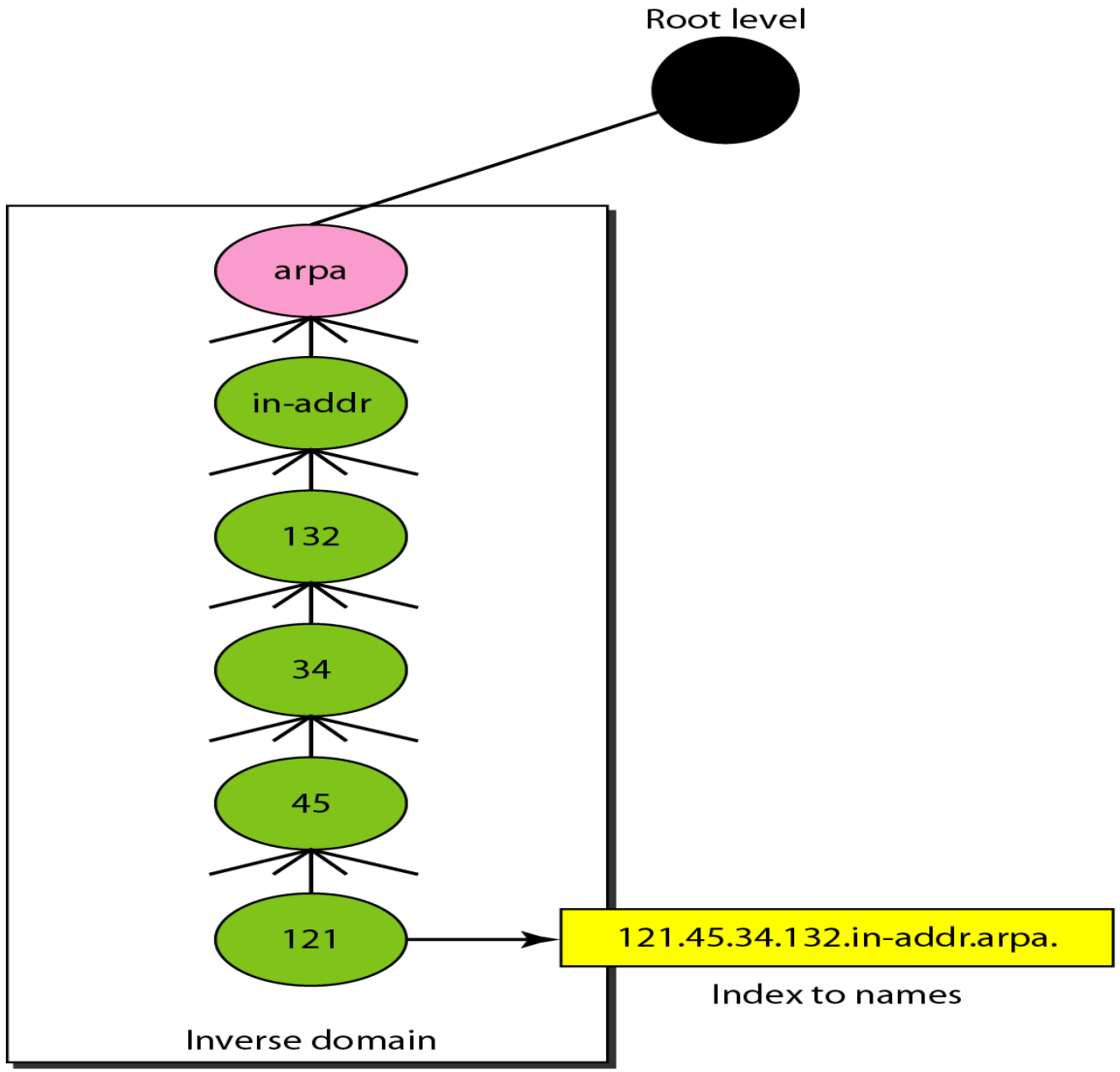
Generic domain labels

Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

Country domains



Inverse domain

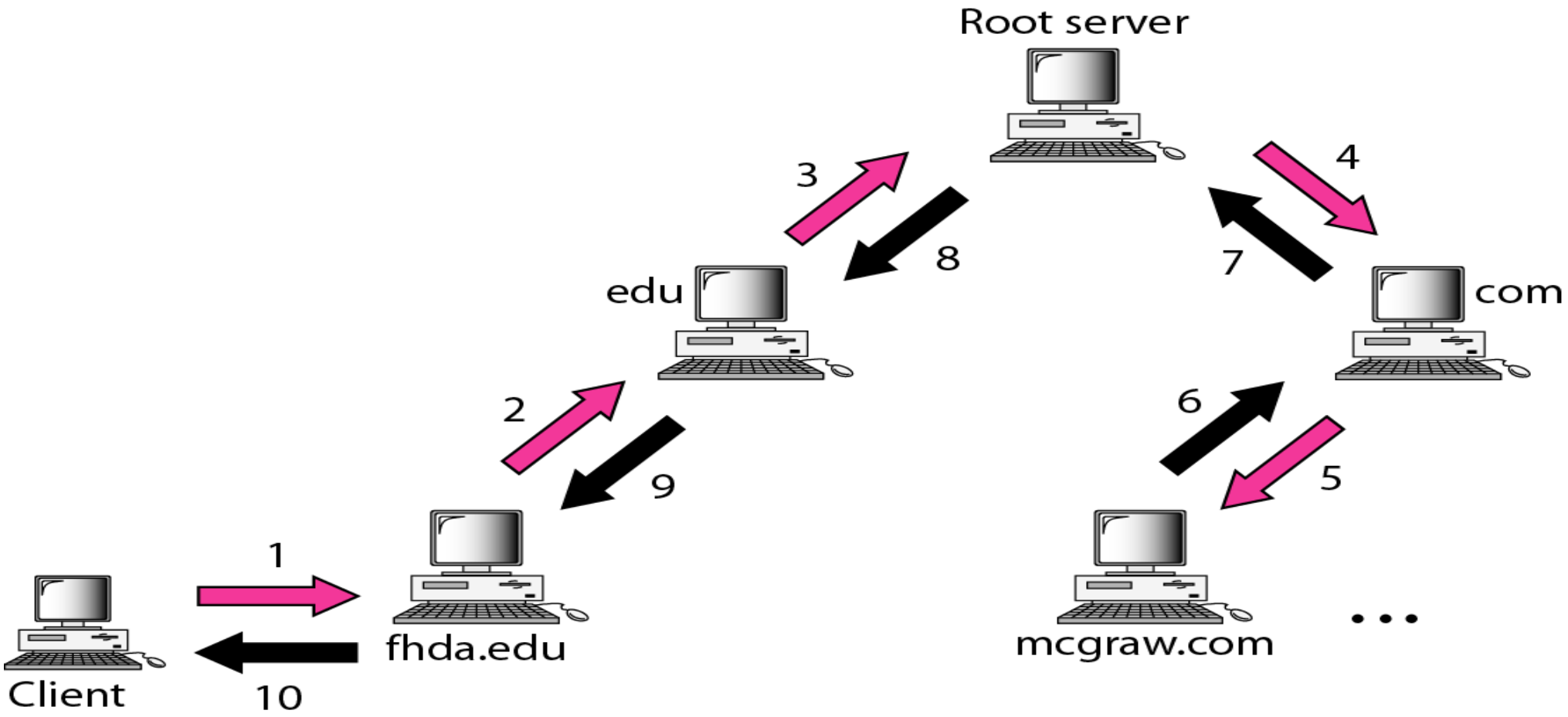


Resolution

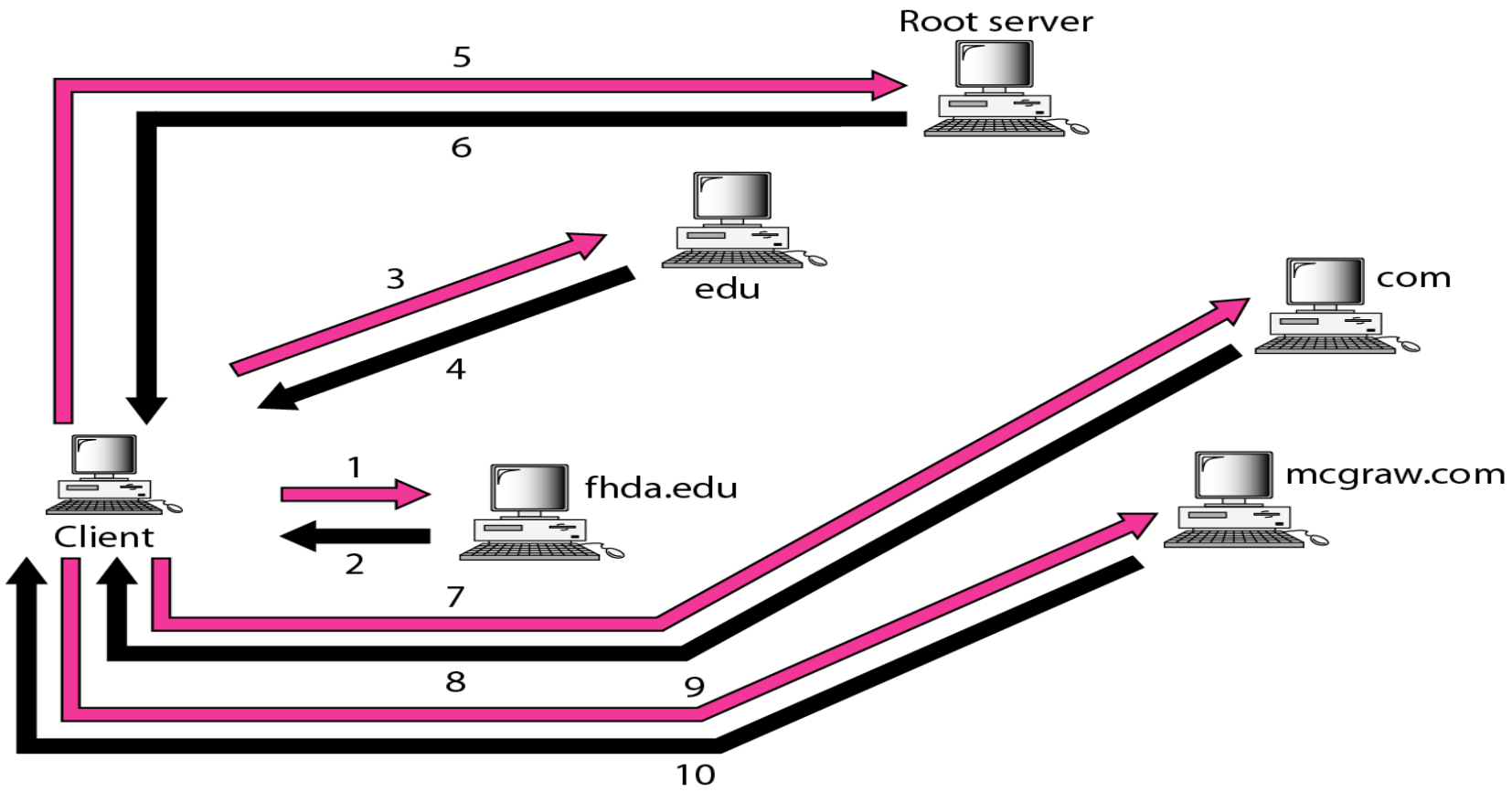
- Mapping a name to an address or an address to a name is called name-address resolution.

Resolver
Mapping Names to Addresses
Mapping Addresses to Names
Recursive Resolution
Caching

Recursive resolution



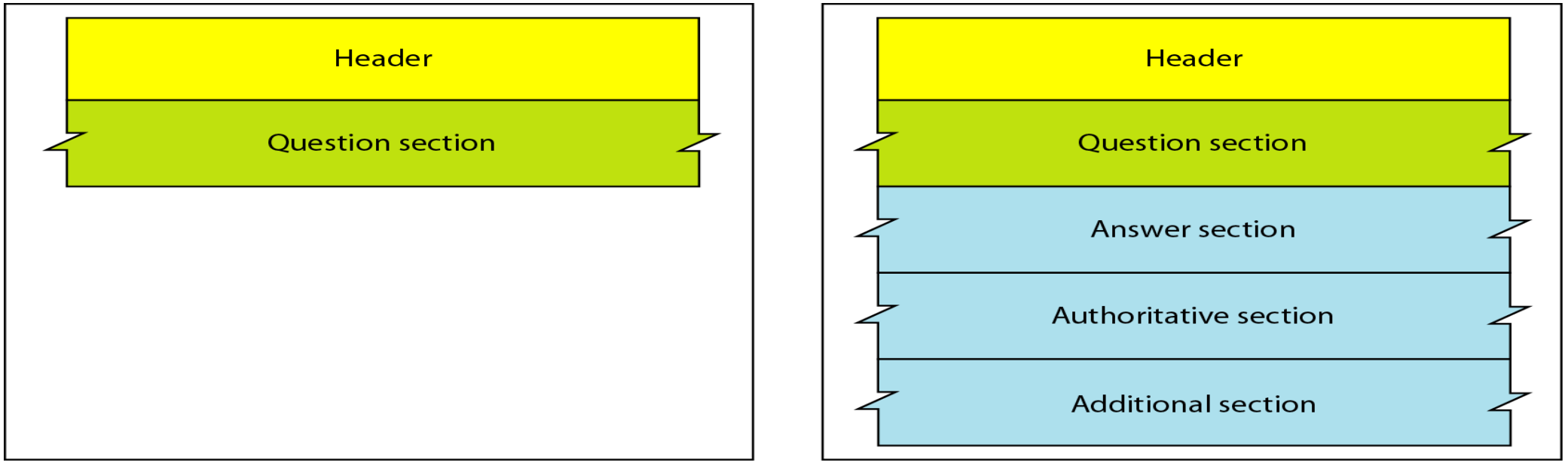
Iterative resolution



DNS Messages

- DNS has two types of messages: query and response. Both types have the same format. The query message consists of a header and question records; the response message consists of a header, question records, answer records, authoritative records, and additional records.

Query and response messages



a. Query

b. Response

Header format

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)

Types of Records

- Two types of records are used in DNS.
- The question records are used in the question section of the query and response messages.
- The resource records are used in the answer, authoritative, and additional information sections of the response message.

Registrars

- How are new domains added to DNS?
- This is done through a registrar, a commercial entity accredited by ICANN.
- A registrar first verifies that the requested domain name is unique and then enters it into the DNS database.
- A fee is charged.

Dynamic Domain Name System(DDNS)

- The DNS master file must be updated dynamically.
- The Dynamic Domain Name System (DDNS) therefore was devised to respond to this need. In DDNS, when a binding between a name and an address is determined, the information is sent, usually by DHCP to a primary DNS server.
- The primary server updates the zone. The secondary servers are notified either actively or passively.

Encapsulation

- DNS can use either UDP or TCP. In both cases the well-known port used by the server is port 53.
- UDP is used when the size of the response message is less than 512 bytes because most UDP packages have a 512-byte packet size limit.
- If the size of the response message is more than 512 bytes, a TCP connection is used.

Note

DNS can use the services of UDP or TCP using the well-known port 53.