STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

DNS, or the Domain Name System, translates human readable domain names (for example, www.amazon.com) to machine readable IP addresses (for example, 192.0.2.44).

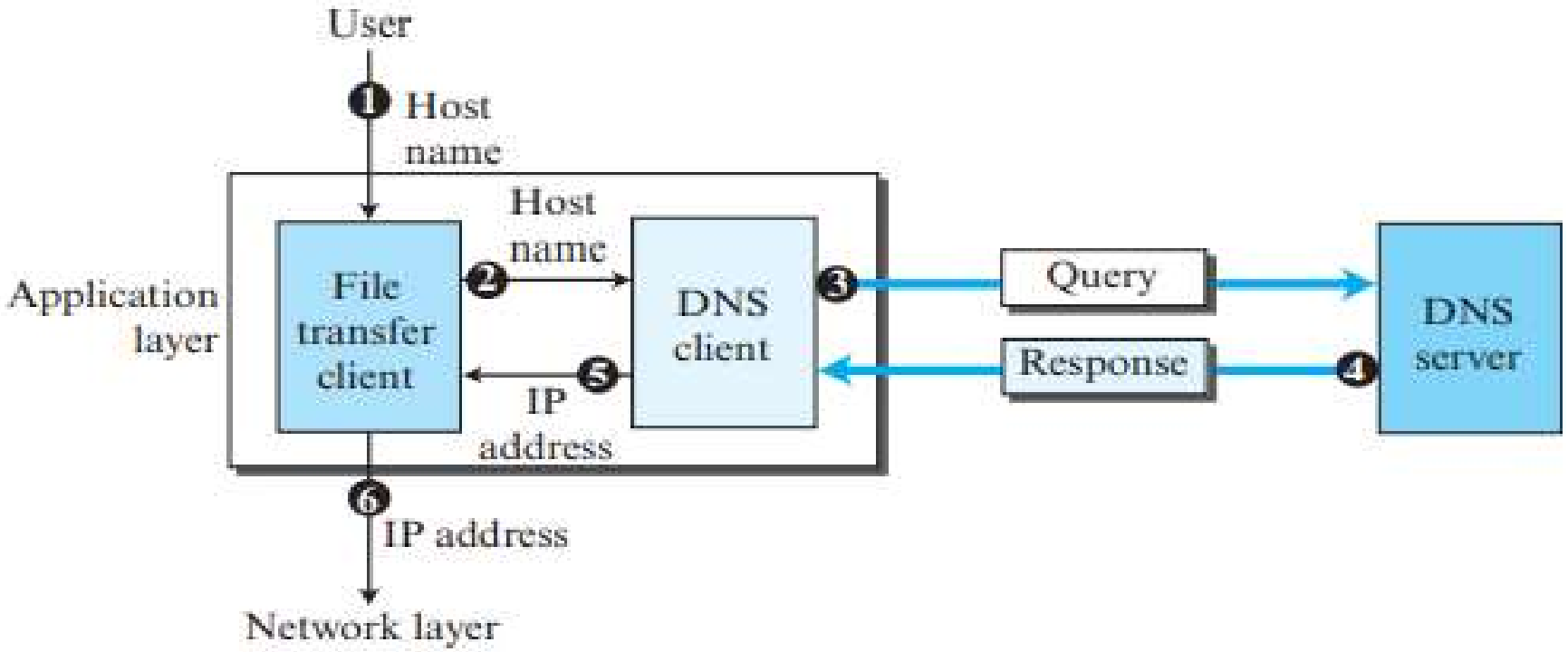
- Since the Internet is so huge today, a central directory system cannot hold all the mapping. In addition, if the central computer fails, the whole communication network will collapse.
- A better solution is to distribute the information among many computers in the world.
- In this method, the host that needs mapping can contact the closest computer holding the needed information. This method is used by the Domain Name System (DNS).

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

- Figure 1.50 shows how TCP/IP uses a DNS client and a DNS server to map a name to an address.

Figure 1.50 *Purpose of DNS*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

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 client passes the IP address to the file transfer server.
6. The file transfer client now uses the received IP address to access the file transfer server.

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Name Space

- A name space that maps each address to a unique name can be organized in two ways: flat or hierarchical.
- In a flat name space, a name is assigned to an address. A name in this space is a sequence of characters without structure.
- In a hierarchical name space, 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.

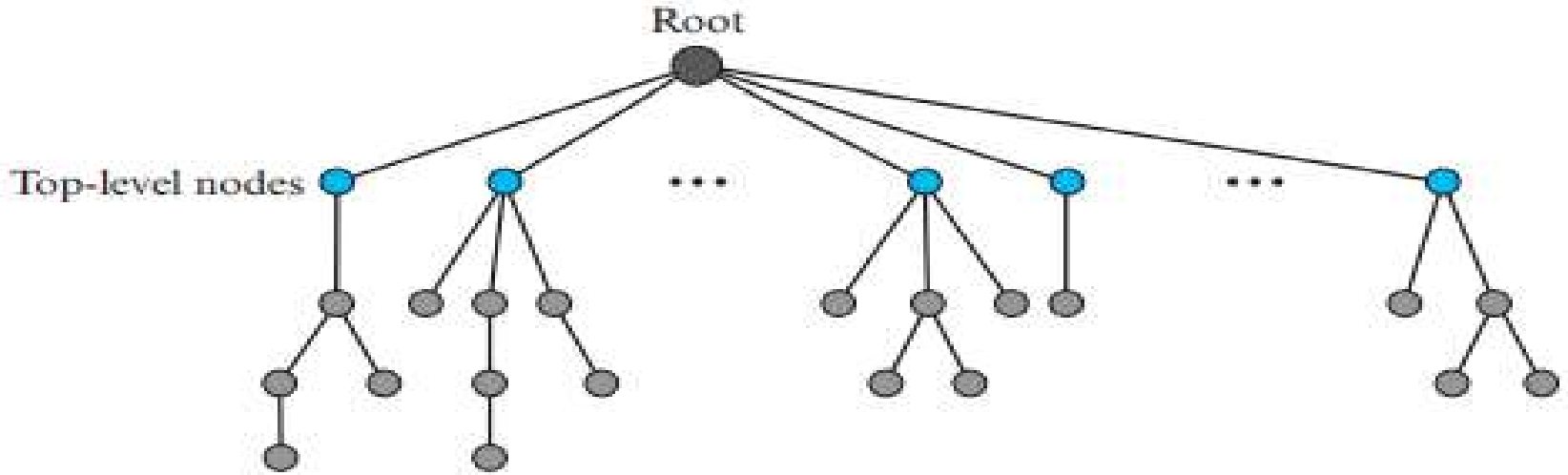
STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

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 (see Figure 1.51).

Figure 1.51 *Domain name space*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Label

- 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 (nodes that branch from the same node) have different labels, which guarantees the uniqueness of the domain names.

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

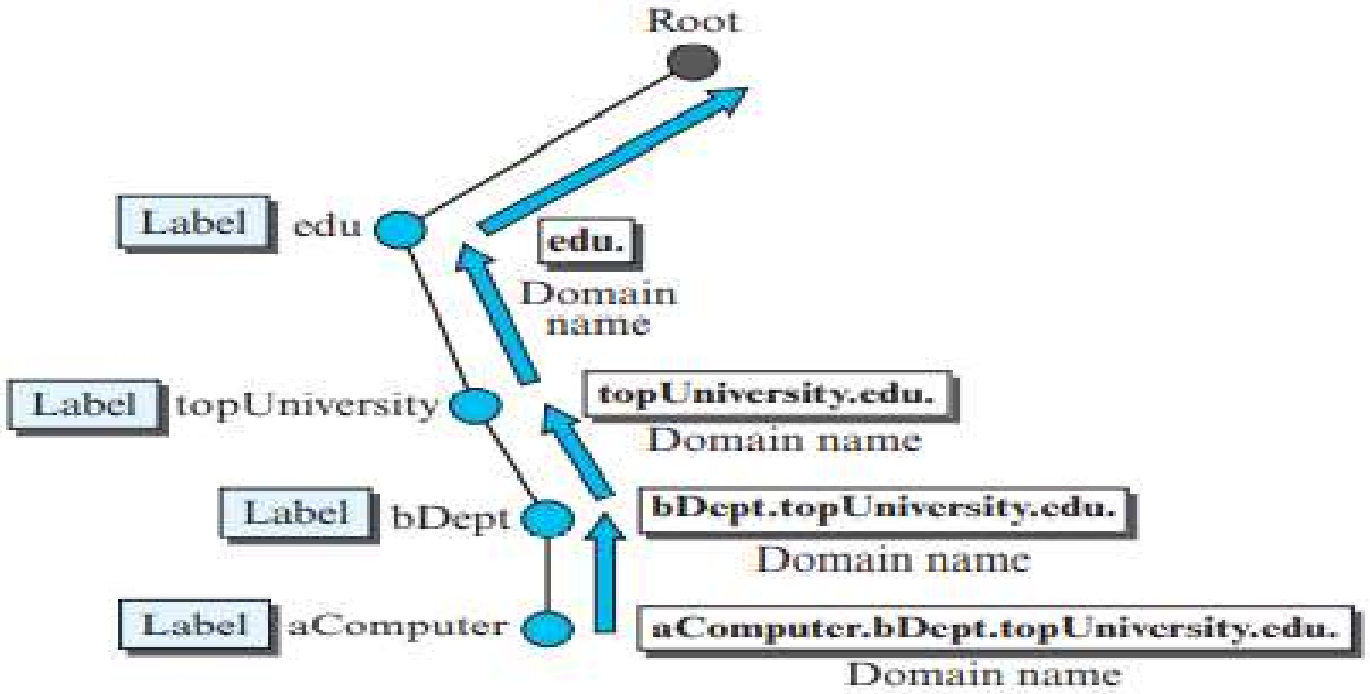
Domain Name

- 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.
- Figure 1.52 shows some domain names.

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Figure1.52 *Domain names and labels*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

- If a label is terminated by a null string, it is called a fully qualified domain name (FQDN).
- If a label is not terminated by a null string, it is called a partially qualified domain name (PQDN).

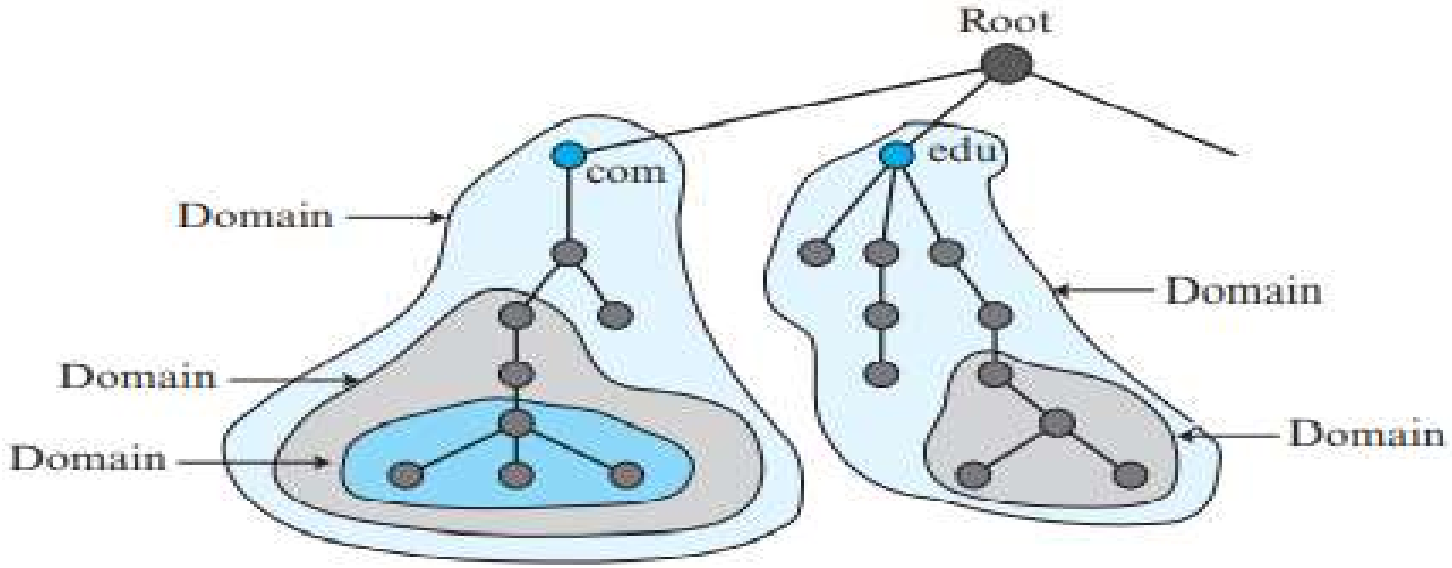
STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Domain

- A domain is a subtree of the domain name space.
- The name of the domain is the name of the node at the top of the subtree.
- Note that a domain may itself be divided into domains.

Figure 1.53 *Domains*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Distribution of Name Space

- The information contained in the domain name space must be stored.
- It is very inefficient and also not reliable to have just one computer store such a huge amount of information.

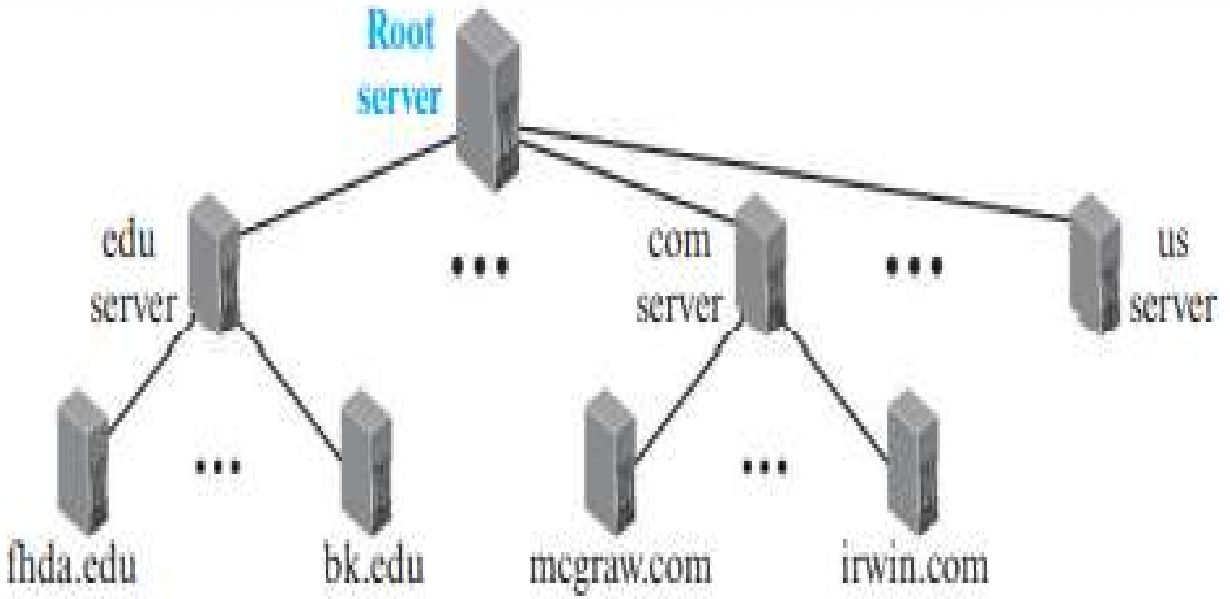
Hierarchy of Name Servers

- The solution to these problems is to distribute the information among many computers called DNS servers.
- One way to do this is to divide the whole space into many domains.
- DNS allows domains to be divided further into smaller domains (subdomains).
- In other words, we have a hierarchy of servers in the same way that we have a hierarchy of names (see Figure 1.54).

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Figure 1.54 *Hierarchy of name servers*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education

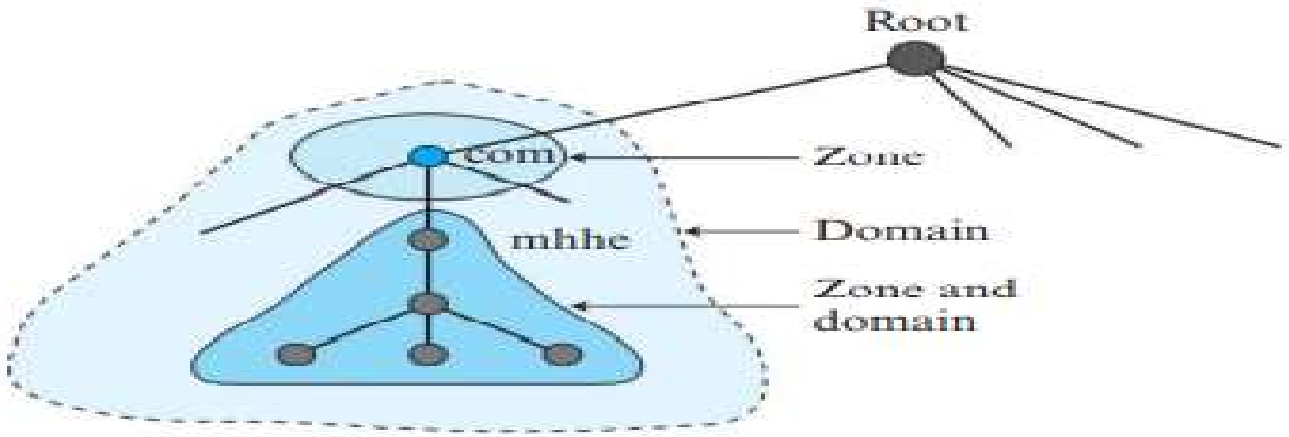
STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Zone

- 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.
- The server makes a database called a zone file and keeps all the information for every node under that domain.

Figure 1.55 *Zone*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

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.

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Primary and Secondary Servers

- DNS defines two types of servers: primary and secondary.
- A primary server is a server that stores a file about the zone for which it is an authority. It is responsible for creating, maintaining, and updating the zone file. It stores the zone file on a local disk.
- A secondary server is a server that transfers the complete information about a zone from another server (primary or secondary) and stores the file on its local disk.
- A primary server loads all information from the disk file; the secondary server loads all information from the primary server.

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

DNS in the Internet

- DNS is a protocol that can be used in different platforms.
- In the Internet, the domain name space (tree) was originally divided into three different sections: generic domains, country domains, and the inverse domain.

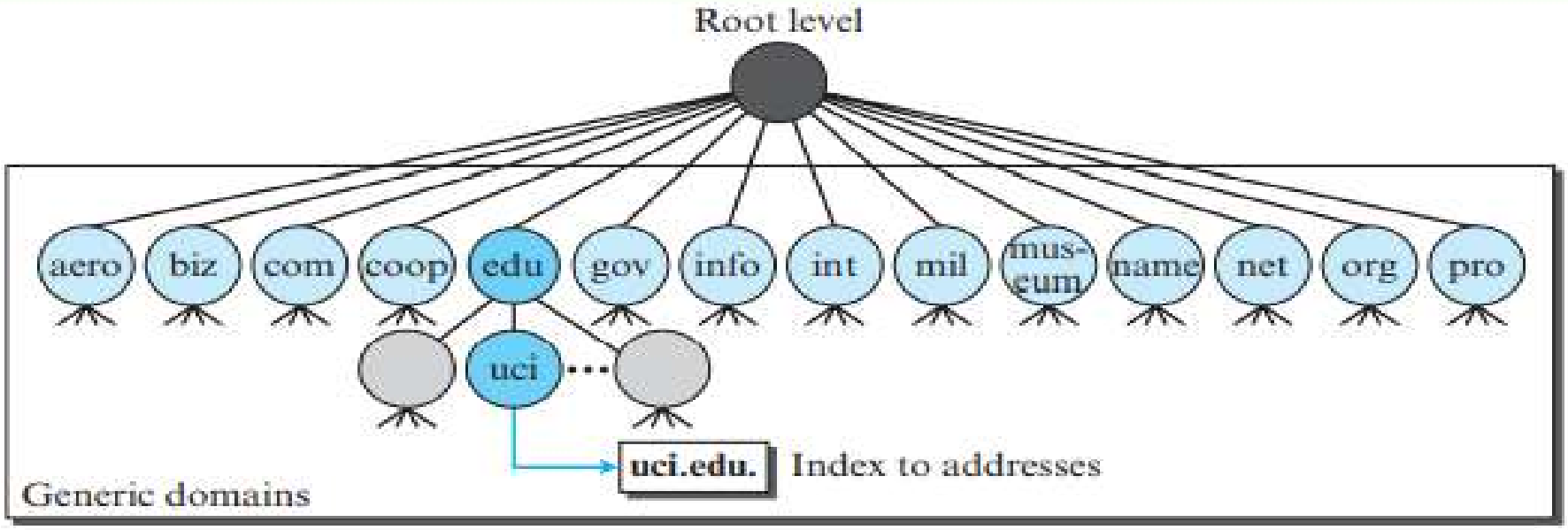
STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Generic Domains

- The generic domains define registered hosts according to their generic behavior.
- Each node in the tree defines a domain, which is an index to the domain name space database (see Figure 1.56).

Figure 1.56 *Generic domains*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

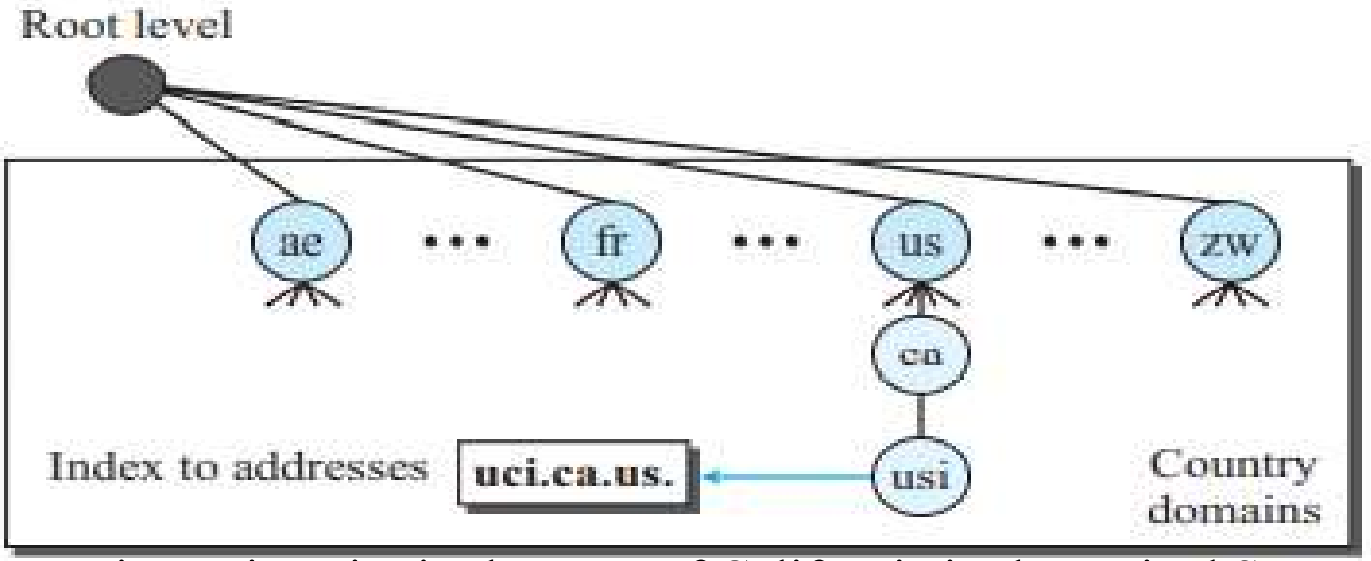
STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Country Domains

- The country domains section uses two-character country abbreviations (e.g., us for United States, in for India).
- Second labels can be organizational, or they can be more specific, national designations.

Figure 1.57 *Country domains*



Irvine university in the state of California in the United States

[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Resolution

- Mapping a name to an address is called name-address resolution.
- DNS is designed as a client-server application.
- A host that needs to map an address to a name or a name to an address calls a DNS client called a resolver.
  - Recursive Resolution
  - Iterative Resolution

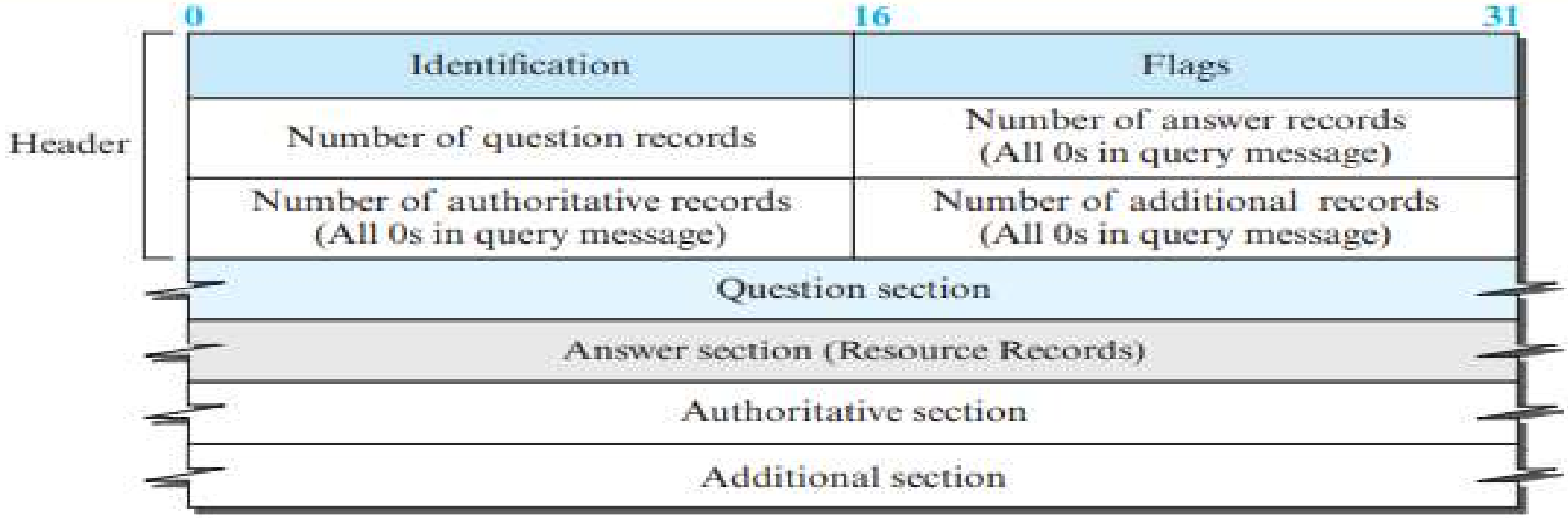
STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

DNS Messages

- To retrieve information about hosts, DNS uses two types of messages: query and response. Both types have the same format as shown in Figure 1.58.

Figure 1.58 *DNS message*



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

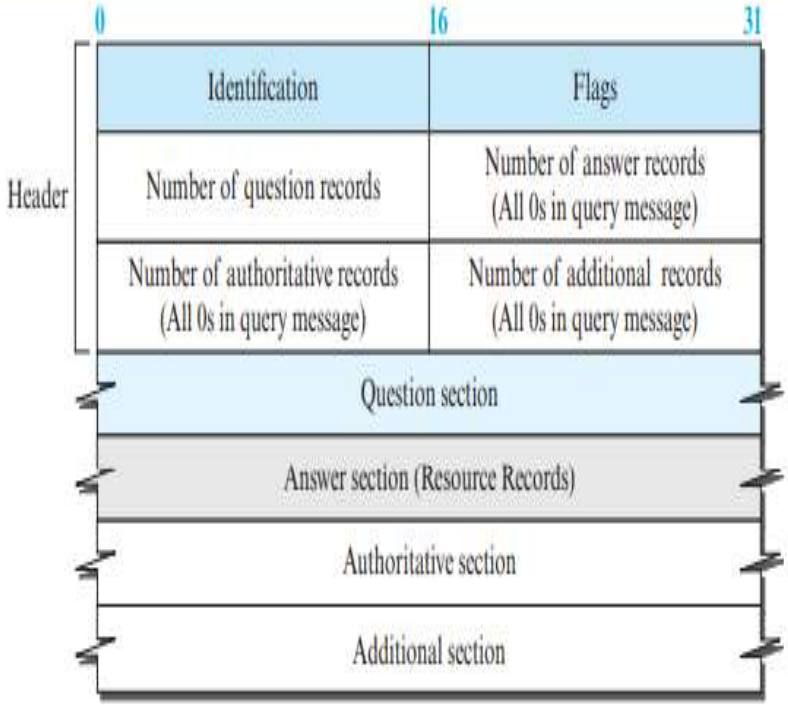
[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

- The identification field is used by the client to match the response with the query.
- The flag field defines whether the message is a query or response. It also includes status of error.
- The next four fields in the header define the number of each record type in the message.
- The question section, which is included in the query and repeated in the response message, consists of one or more question records.

Figure 1.58 *DNS message*



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

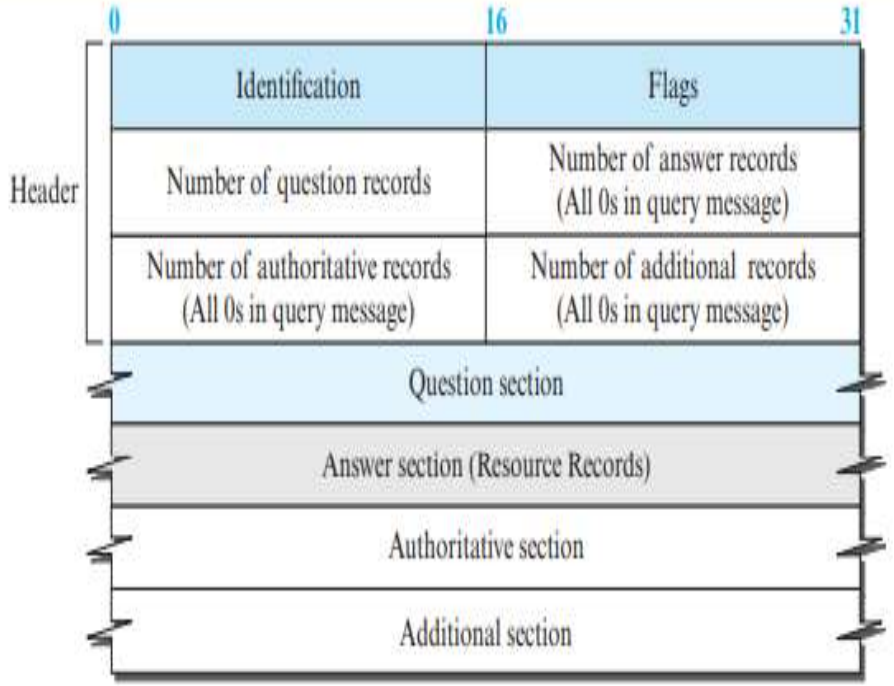
[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

- The answer section consist of one or more resource records. It is present only in response messages.
- The authoritative section gives information (domain name) about one or more authoritative servers for the query.
- The additional information section provides additional information that may help the resolver.

Figure 1.58 *DNS message*



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

[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

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.

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

Registrars

How are new domains added to DNS?

- This is done through a registrar, a commercial entity accredited by ICANN(Internet Corporation for Assigned Names and Numbers).
- A registrar first verifies that the requested domain name is unique and then enters it into the DNS database. A fee is charged.

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

DDNS

- The DNS master file must be updated dynamically.
- The Dynamic Domain Name System (DDNS) 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 (Dynamic Host Configuration Protocol) to a primary DNS server.
- The primary server updates the zone. The secondary servers are notified either actively or passively.
- In active notification, the primary server sends a message to the secondary servers about the change in the zone, whereas in passive notification, the secondary servers periodically check for any changes.
- To provide security and prevent unauthorized changes in the DNS records, DDNS can use an authentication mechanism.

STANDARD CLIENT-SERVER APPLICATIONS

Domain Name System (DNS)

- To protect DNS, IETF has devised a technology named DNS Security (DNSSEC) that provides message origin authentication and message integrity using a security service called digital signature.

PEER-TO-PEER PARADIGM

P2P Networks

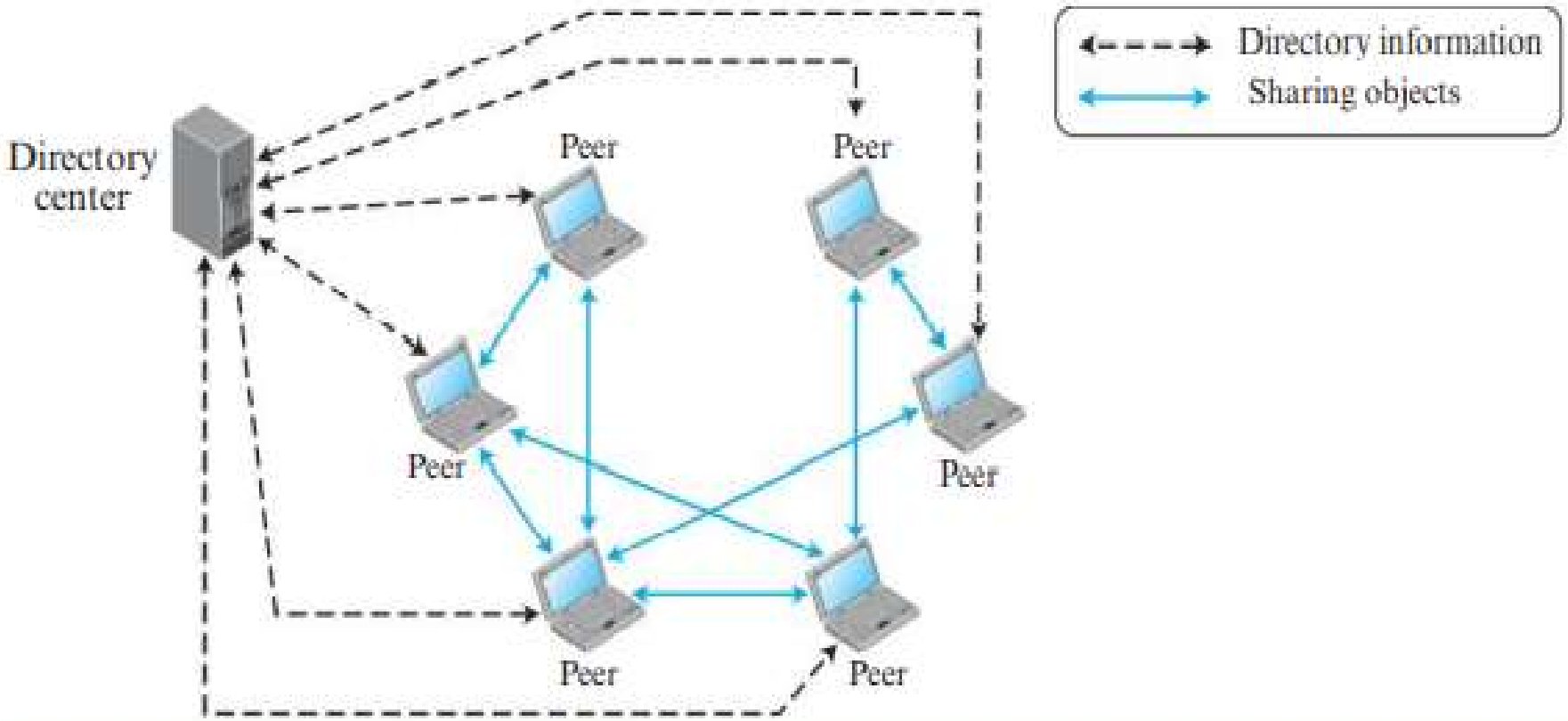
- We first need to divide the P2P networks into two categories: centralized and decentralized.

Centralized Networks

• In a centralized P2P network, the directory system – listing of the peers and what they offer – uses the client-server paradigm, but the storing and downloading of the files are done using the peer-to-peer paradigm (a hybrid P2P network).

PEER-TO-PEER PARADIGM

Figure 1.59 *Centralized network*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

PEER-TO-PEER PARADIGM

Centralized Networks

- A peer, looking for a particular file, sends a query to a central server.
- The server searches its directory and responds with the IP addresses of nodes that have a copy of the file.
- The peer contacts one of the nodes and downloads the file.
- The directory is constantly updated as nodes join or leave the peer.
- Centralized networks make the maintenance of the directory simple but have several drawbacks.
- Accessing the directory can generate huge traffic and slow down the system.
- The central servers are vulnerable to attack, and if all of them fail, the whole system goes down.

PEER-TO-PEER PARADIGM

Decentralized Network

- A decentralized P2P network does not depend on a centralized directory system.
- In this model, peers arrange themselves into an overlay network, which is a logical network made on top of the physical network.
- Depending on how the nodes in the overlay network are linked, a decentralized P2P network is classified as either unstructured or structured.

PEER-TO-PEER PARADIGM

Unstructured Networks

- In an unstructured P2P network, the nodes are linked randomly.
- The Gnutella network is an example of a peer-to-peer network that is decentralized but unstructured.

Structured Networks

- A structured network uses a predefined set of rules to link nodes so that a query can be effectively and efficiently resolved.
- The most common technique used for this purpose is the Distributed Hash Table (DHT).
- DHT is used in many applications including Distributed Data Structure (DDS), Content Distributed Systems (CDS), Domain Name System (DNS), and P2P file sharing.
- One popular P2P file sharing protocol that uses the DHT is BitTorrent.

PEER-TO-PEER PARADIGM

Distributed Hash Table (DHT)

- A Distributed Hash Table (DHT) distributes data (or references to data) among a set of nodes according to some predefined rules.
- Each peer in a DHT-based network becomes responsible for a range of data items.
- To avoid the flooding overhead, DHT-based networks allow each peer to have a partial knowledge about the whole network.
- This knowledge can be used to route the queries about the data items to the responsible nodes using effective and scalable procedures.
- There are several protocols that implement DHT systems: Chord, Pastry, and Kademlia.

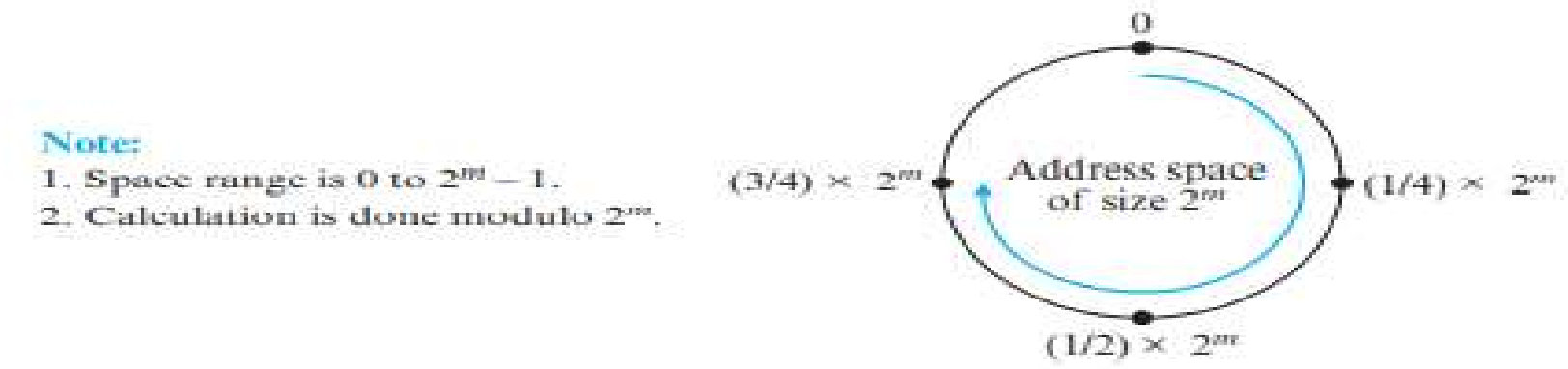
PEER-TO-PEER PARADIGM

Distributed Hash Table (DHT)

Address Space

- In a DHT-based network, each data item and the peer is mapped to a point in a large address of size 2^m.
- The address space is designed using modular arithmetic, which means that the points in the address space as distributed evenly on a circle with 2^m points (0 to $2^m - 1$) using clockwise direction as shown in Figure 1.60.
- Most of the DHT implementations use m = 160.

Figure 1.60 *Address space*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

PEER-TO-PEER PARADIGM

Distributed Hash Table (DHT)

Hashing Peer Identifier

- The first step in creating the DHT system is to place all peers on the address space ring. This is normally done by using a hash function that hashes the peer identifier, normally its IP address, to an m-bit integer, called a node ID.

  node ID = hash (Peer IP address)

Hashing Object Identifier

- The name of the object (for example, a file) to be shared is also hashed to an m-bit integer in the same address space. The result in DHT is called a key.

  key = hash (Object name)

PEER-TO-PEER PARADIGM

Chord

- Chord was published by Stoica et al in 2001.

Identifier Space

- Data items and nodes in Chord are m-bit identifiers that create an identifier space of size 2^m points distributed in a circle in the clockwise direction.
- We refer to the identifier of a data item as k (for key) and the identifier of a peer as N (for node).

Finger Table

- A node in the Chord algorithm should be able to resolve a query: given a key, the node should be able to find the node identifier responsible for that key or forward the query to another node.
- Forwarding means that each node needs to have a routing table. Chord requires that each node knows about m successor nodes and one predecessor node. Each node creates a routing table, called a finger table by Chord.

PEER-TO-PEER PARADIGM

Chord

Table 1.9 *Finger table*

i	*Target Key*	*Successor of Target Key*	*Information about Successor*
1	N + 1	Successor of N + 1	IP address and port of successor
2	N + 2	Successor of N + 2	IP address and port of successor
⋮	⋮	⋮	⋮
m	$N + 2^{m-1}$	Successor of $N + 2^{m-1}$	IP address and port of successor

[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

PEER-TO-PEER PARADIGM

Chord

Interface

- Chord needs a set of operations referred to as the Chord interface.

Lookup

- Probably the mostly used operation in Chord is the lookup.
- Chord is designed to let peers share available services between themselves.
- To find the object to be shared, a peer needs to know the node that is responsible for that object: the peer that stores a reference to that object.
- In Chord, a peer that is the successor of a set of keys in the ring is the responsible peer for those keys.
- Finding the responsible node is actually finding the successor of a key.

PEER-TO-PEER PARADIGM

A Popular P2P Network: BitTorrent

- BitTorrent is a P2P protocol, designed by Bram Cohen, for sharing a large file among a set of peers.
- However, the term sharing in this context is different from other filesharing protocols.
- Instead of one peer allowing another peer to download the whole file, a group of peers takes part in the process to give all peers in the group a copy of the file.
- File sharing is done in a collaborating process called a torrent.

PEER-TO-PEER PARADIGM

A Popular P2P Network: BitTorrent

- Each peer participating in a torrent downloads chunks of the large file from another peer that has it and uploads chunks of that file to other peers that do not have it, a kind of tit-for-tat, a trading game played by kids.
- The set of all peers that takes part in a torrent is referred to as a swarm.
- A peer in a swarm that has the complete content file is called a seed; a peer that has only part of the file and wants to download the rest is called a leech.
- A swarm is a combination of seeds and leeches.
- BitTorrent has gone through several versions and implementations, the original one which uses a central node called a tracker.