E – 51822

Register No. | | | | | | | | |

BTech Degree Examination November 2021

Fifth Semester

Information Technology

18ITT51 – COMPUTER NETWORKS

(Regulations 2018)

Time: Three hours | Maximum: 100 marks

Answer all Questions

Part – A (10 × 2 = 20 marks)

1. Specify any two factors that determine whether a communication system is a LAN or WAN? [CO1,K2]
2. A signal is carrying data in which one data element is encoded as one signal element $(r = 1)$. If the bit rate is 100kbps, what is the average value of the baud rate if C is between 0 and 1? [CO1,K3]
3. Can the value of a check sum be all 0s (in binary)? Defend your answer. Can the value be all 1s (in binary)? Defied your answer. [CO2,K3]
4. Compare and contrast HDLC with PPP. Which one is byte – oriented; which one is bit oriented? [CO2,K2]
5. Change the following IPV4 addresses form dotted – decimal notation to binary notation. [CO3,K3]
   a) 111.56.45.78 b) 221.34.7.82
6. Why is there a restriction on the generation of an ICMPV4 message in response to a failed ICMPV4 error message? [CO3,K3]
7. A client uses UDP to send data to a server. The data are 15 bytes. Calculate the efficiency of this transmission at the UDP level (ratio of useful bytes to total bytes). [CO4,K3]
8. In TCP, if the value of HLEN is 1000, how many bytes of option are included in the segment? [CO4,K3]
9. Show the encoding for an arbitrary OCTET STRING of length 2000. [CO5,K2]
10. What is URL and what are its components? [CO5,K1]

Part – B (5 × 16 = 80 marks)

11. a. i) Draw and explain the various layers in the OSI model. (10) [CO1,K1]

    ii) Suppose a computer sends a frame to another computer on a bus topology LAN. The physical destination address of the frame is corrupted during the transmission. What happens to the frame? How can the sender be informed about the situation? (6) [CO1,K3]

(OR)

b. i) Illustrate the various guided media with suitable diagram (10) [CO1,K1]

ii) We need to send data at a 1 – Mbps rate. What is the minimum required bandwidth, using a combination of 4B / 5B and NRZ – I or Manchester coding? (6) [CO1,K3]

12. a. Compare error detection and correction with suitable examples. (16) [CO2,K2]

(OR)

b. Compare control field for I – frames with control field for S – frames. (16) [CO2,K2]

13. a. Differentiate distance vector routing protocols with link state routing protocol. (16) [CO3,K2]

(OR)

b. Differentiate IPV_4 with IPV_6. (16) [CO3,K2]

14. a. Compare and contrast stop - and - wait protocol with Go - back - N protocol. (16) [CO4,K3]

(OR)

b. Compare and contrast UDP with TCP. (16) [CO4,K3]

15. a. i) Show the sequence of characters exchanged between the TELNET client and the server to switch from the default mode to the character mode. (8) [CO5,K2]

ii) Illustrate the various types of web documents. (8) [CO5,K1]

(OR)

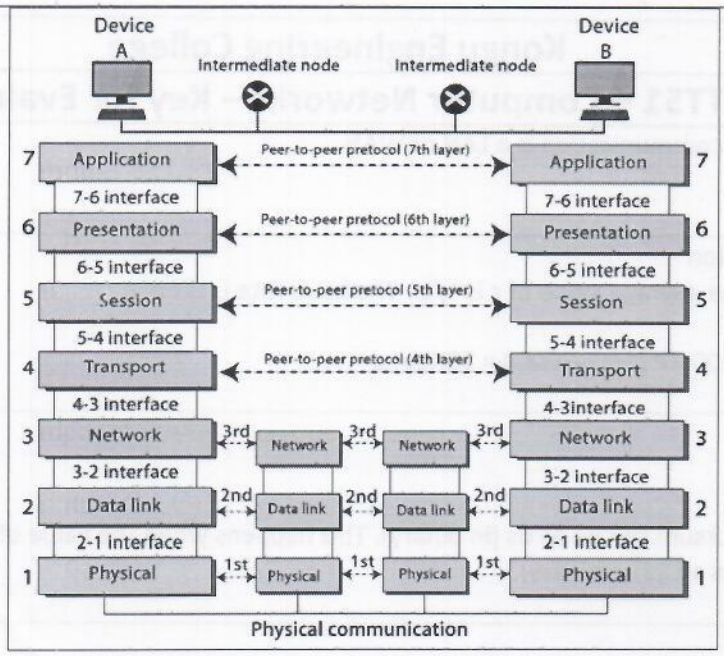
b. i) Show how the following array of records (sequence of sequence) is encoded. (8) [CO5,K2]

INTEGER	OCTET STRING	COUNTER
2345	"COMPUTER"	345
1123	"DISK"	1430
3456	"MONITOR"	2313

ii) Illustrate the various sections of domain name space. (8) [CO5,K1]

Bloom's Taxonomy Level	Remembering (K1)	Understanding (K2)	Applying (K3)	Analysing (K4)	Evaluating (K5)	Creating (K6)
Percentage	20	46	34	-	-	-

	Kongu Engineering College	
	18ITT51 – Computer Networks – Key for Evaluation	
1.	Factors determine communication is a LAN or WAN • Size • Distance	2
2.	Baud Rate Calculation We assume that the average value of c is 1/2 . The baud rate is then S=c*N*1/r = (½)*10000*(1/1)=50000 = 50KBaud	2
3.	Check sum: For All 0s: The value of a checksum can be all 0s (in binary). This happens when the value of the sum (after wrapping) becomes all 1s (in binary).	2
4.	HDLC bit Oriented PPP is byte oriented With explanation on each	2
5.	111.56.45.78 - 01101111.00111000.00101101.01001110 221.34.7.82 - 11011101.00100010.00000111.01010010	2
6.	ICMP messages are of interest both to end-hosts and intermediate routers, although some messages are generally only sent by routers. It is never permissible for an ICMP error message to be generated as the result of receiving an ICMP error message-this avoids the infinite recursion of ICMP message generation	2
7.	Efficiency =15/(15+8(UDP Header Size)= 0.6521	2
8.	HLEN = 1000 = 8. 8 x 4 = 32 bytes.	2
9.	Show the encoding for an orbitary OCTET String of length 2000 04 82 07 D0	2
10.	URL and its Components URL is an acronym for Uniform Resource Locator and is a reference (an address) to a resource on the Internet. A URL has two main components: Protocol identifier Resource name	2
	Part - B (5x16 = 80 Marks)	
11. a)	OSI Layers and Diagram	



(4)

Physical layer:

- Bit synchronization
- Physical topologies
- Transmission mode
- Bit Rate Control

(1)

Data Link Layer

Data Link Layer is divided into two sublayers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

(1)

Functions:

- Framing
- Physical Addressing
- Error Comtrol
- Flow Control
- Access Control

(1)

Network Layer:

- Routing
- Logical Addressing

Transport Layer:
At sender Side

- Segmentation

	• Flow and Error Control At receivers Side • Segmentation and reassembly • Service point addressing Session Layer • Session establishment, maintenance, and termination • Synchronization • Dialog Controller Presentation Layer • Translation • Encryption/ Decryption • Compression Application Layer • Network Virtual Terminal • FTAM-File transfer access and management • Mail Services • Directory Services	(1) (1) (1)
11. a) ii)	If the corrupted destination address does not match any station address in the network, the packet is lost. If the corrupted destination address matches one of the stations, the frame is delivered to the wrong station. In this case, however, the error detection mechanism, available in most data link protocols, will find the error and discard the frame.	(6)
	OR	
11. B) i)	**Guided Media:** It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links. Features: • High Speed • Secure • Used for comparatively shorter distances There are 3 major types of Guided Media: **Twisted Pair Cable** • **Unshielded Twisted Pair (UTP)**	(2) (3) with diagram

Advantages:

- Least expensive
- Easy to install
- High-speed capacity
- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

Shielded Twisted Pair
Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster
- Comparatively difficult to install and manufacture
- More expensive
- Bulky

Coaxial Cable (2)

Advantages:

- High Bandwidth
- Better noise Immunity with diagram
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

Optical Fiber Cable (2)

Advantages:

- Increased capacity and bandwidth
- Lightweight with diagram
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

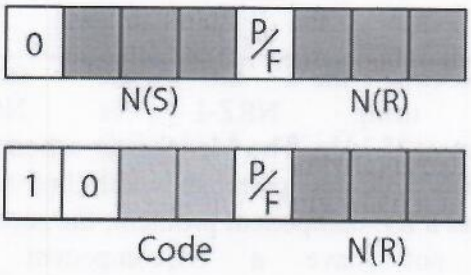
Disadvantages:

- Difficult to install and maintain

	• High cost • Fragile	
11. B) ii)	First 4B/5B block coding increases the bit rate to 1.25 Mbps. The minimum bandwidth using NRZ-I is N/2 or 625 kHz The Manchester scheme needs a minimum625 kHz. The Manchester scheme needs a minimumbandwidth of 1 MHz. The first choice needs a lowerbandwidth but has a DC component problem; the second bandwidth, but has a DC component problem; the secondchoice needs a higher bandwidth, but does not have a DCcomponent problem	(6)
12. a)	Error Detection in Computer Networks (8) A condition when the receiver's information does not match with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0. Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors. Some popular techniques for error detection are: 1. Simple Parity check 2. Two-dimensional Parity check 3. Checksum 4. Cyclic redundancy check Example for any method specified above Error Correction in Computer Networks (8) There are two ways to handle the error correction: • Backward Error correction -Once the error is discovered, the receiver requests the sender to retransmit the entire data unit. • Forward Error Correction technique. - In this case, the receiver uses the error-correcting code which automatically corrects the errors. Example for any method specified above Comparison between above methods.	

OR

12. b.



Control Field for I-Frames: (5)

I-frames are designed to carry user data from the network layer. In addition, they can include flow and error control information (piggybacking). The subfields in the control field are used to define these functions.

1st bit – defines type

The next 3 bits, called N(S), define the sequence number of the frame. Note that with 3 bits, we can define a sequence number between 0 and 7; but in the extension format, in which the control field is 2 bytes, this field is larger.

The last 3 bits, called N(R), correspond to the acknowledgment number when piggybacking is used.

The single bit between N(S) and N(R) is called the P/F bit. The P/F field is a single bit with a dual purpose. It has meaning only when it is set (bit = 1) and can mean poll or final.

Control Field for S-Frames: (5)

Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate (e.g., when the station either has no data of its own to send or needs to send a command or response other than an acknowledgment). S-frames do not have information fields.

If the first 2 bits of the control field is 10, this means the frame is an S-frame.

2. The last 3 bits, called N(R), corresponds to the acknowledgment number (ACK) or negative acknowledgment number (NAK) depending on the type of S-frame.

3. The 2 bits called code is used to define the type of S-frame itself. With 2 bits, we can have four types of S-frames, as described below:

1. Receive ready (RR)
2. Receive not ready (RNR)
3. Reject (REJ)
4. Selective reject (SREJ)

13. a)

Parameters	**Distance vector routing** (6)	**Link state routing** (6)
Algorithm	Bellman ford	Dijsktra

	Network view	Topology information from the neighbour point of view	Complete information on the network topology
	Best path calculation	Based on the least number of hops	Based on the cost
	Updates	Full routing table	Link state updates
	Updates frequency	Periodic updates	Triggered updates
	CPU and memory	Low utilization	Intensive
	Simplicity	High simplicity	Requires a trained network administrator
	Convergence time	Moderate	Fast
	Updates	On broadcast	On multicast
	Hierarchical structure	No	Yes
	Intermediate Nodes	No	Yes
	OR		
13. B.	**IPv4** (8)	**IPv6** (8)	
	IPv4 has a 32-bit address length	IPv6 has a 128-bit address length	
	It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration	
	In IPv4 end to end, connection integrity is Unachievable	In IPv6 end to end, connection integrity is Achievable	
	It can generate 4.29×10^9 address space	Address space of IPv6 is quite large it can produce 3.4×10^{38} address space	
	The Security feature is dependent on application	IPSEC is an inbuilt security feature in the IPv6 protocol	
	Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal	
	Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by the sender	
	In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header	
	In IPv4 checksum field is available	In IPv6 checksum field is not available	
	It has broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available	
	In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided	
	IPv4 has a header of 20-60 bytes.	IPv6 has header of 40 bytes fixed	

14. a) **Compare stop and wait protocol with Go Back N Protocol**

Sr. No.	Key	Stop and Wait protocol (8)	GoBackN protocol (8)
1	Sender window size	In Stop and Wait protocol, Sender window size is 1.	In GoBackN protocol, Sender window size is N.
2	Receiver Window size	In Stop and Wait protocol, Receiver window size is 1.	In GoBackN protocol, Receiver window size is 1.
3	Minimum Sequence Number	In Stop and Wait protocol, Minimum Sequence Number is 2.	In GoBackN protocol, Minimum Sequence Number is N+1 where N is number of packets sent.
4	Efficiency	In Stop and Wait protocol, Efficiency formular is 1/(1+2*a) where a is ratio of propagation delay vs transmission delay.	In GoBackN protocol, Efficiency formular is N/(1+2*a) where a is ratio of propagation delay vs transmission delay and N is number of packets sent.
5	Acknowledgement Type	In Stop and Wait protocol, Acknowledgement type is individual.	In GoBackN protocol, Acknowledgement type is cumulative.
6	Supported Order	In Stop and Wait protocol, no specific order is needed at receiver end.	In GoBackN protocol, in-order delivery only are accepted at receiver end.
7	Retransmissions	In Stop and Wait protocol, in case of packet drop,number of retransmition is 1.	In GoBackN protocol, in case of packet drop,numbers of retransmitions are N.

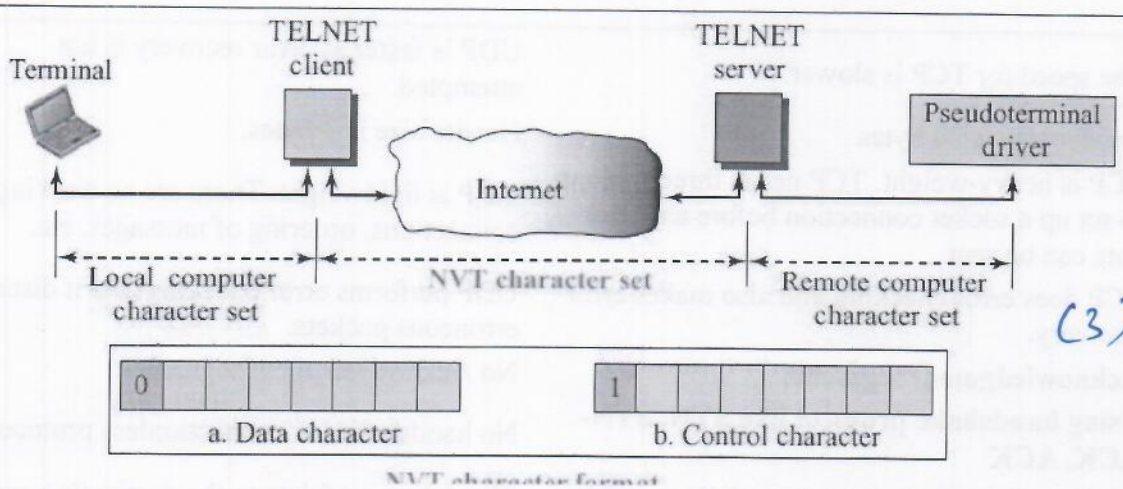
OR

14) B. **Compare and Contrast UDP and TCP**

TCP (8)	UDP (8)
It is a connection-oriented protocol.	It is a connectionless protocol.
TCP reads data as streams of bytes, and the message is transmitted to segment boundaries.	UDP messages contain packets that were sent one by one. It also checks for integrity at the arrival time.
TCP messages make their way across the internet from one computer to another.	It is not connection-based, so one program can send lots of packets to another.
TCP rearranges data packets in the specific order.	UDP protocol has no fixed order because all packets are independent of each other.

	The speed for TCP is slower.	UDP is faster as error recovery is not attempted.	
	Header size is 20 bytes	Header size is 8 bytes.	
	TCP is heavy-weight. TCP needs three packets to set up a socket connection before any user data can be sent.	UDP is lightweight. There are no tracking connections, ordering of messages, etc.	
	TCP does error checking and also makes error recovery.	UDP performs error checking, but it discards erroneous packets.	
	Acknowledgment segments	No Acknowledgment segments	
	Using handshake protocol like SYN, SYN-ACK, ACK	No handshake (so connectionless protocol)	
	TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination can't be guaranteed in UDP.	
	TCP offers extensive error checking mechanisms because it provides flow control and acknowledgment of data.	UDP has just a single error checking mechanism which is used for checksums.	
15. A. i)	30 43 — sequence, length 30 41 — sequence, length 02 04 00 00 09 29 — INTEGER, length, value (2345) 04 08 43 4F 4D 50 55 54 45 52 — OCTET STRING, length, value (COMPUTER) 41 04 00 00 01 59 — counter, length, value (345) 30 29 — sequence, length 02 04 00 00 04 63 — INTEGER, length, value (1123) 04 04 44 49 53 4B — OCTET STRING, length, value (DISK) 41 04 00 00 05 96 — counter, length, value (1430) 30 15 — sequence, length 02 04 00 00 0D 80 — INTEGER, length, value (3456) 04 07 4D 4F 4E 49 54 4F 52 — OCTET STRING, length, value (MONITOR) 41 04 00 00 09 09 — counter, length, value (2313)		
ii)	**Types of Web Documents (Explanation)** • Static Document • Dynamic Documents • Active Documents		
	OR		

B) i



(3)

If the option negation uses no other modes, then the current mode is said to be in default mode.

(6)

• Client echoes the character when the user types them but, does not displays them until the line is completed.

(5)

• In default mode, the client does not accept the new line until it accepts GA (go ahead) from server.

• In character mode, client sends the character to the server.

• Each character is echoed back on the client screen but, if it takes time, echoing of character is delayed.

B) ii)

Domain Name System

Domain Name System is an Internet service that translates domain names into IP addresses.
The DNS has a distributed database that resides on multiple machines on the Internet.
DNS has some protocols that allow the client and servers to communicate with each other.
When the Internet was small, mapping was done by using hosts.txt file.
The host file was located at host's disk and updated periodically from a master host file.
When any program or any user wanted to map domain name to an address, the host consulted the host file and found the mapping.
Now Internet is not small, it is impossible to have only one host file to relate every address with a name and vice versa.
The solution used today is to divide the host file into smaller parts and store each part on a different computer.
In this method, the host that needs mapping can call the closest computer holding the needed information.
This method is used in Domain Name System (DNS).
Name space
The names assigned to the machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses.

(8)

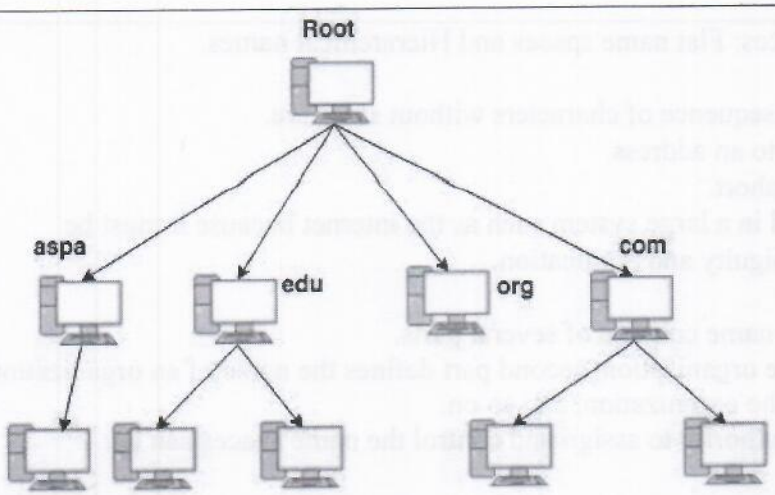


Fig: Hierarchy of DNS

(2)

Generic Domains

The generic domains define registered hosts according to their generic behavior.

Generic domain labels are as stated below:

1. Country Domains

Country domain uses two character country abbreviations.

Second labels can be more specific, national designation.

For example, for Australia the country domain is "au", Inida is .in, UK is .uk etc.

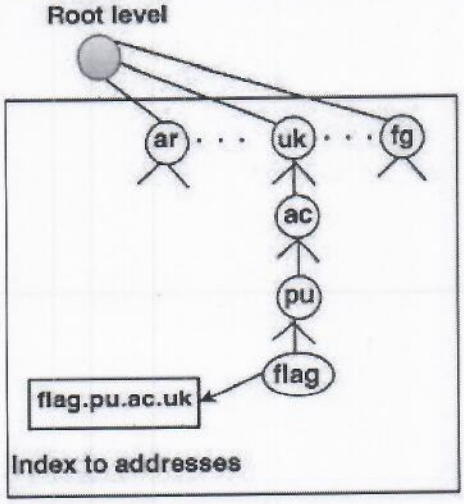


Fig: Country domains

(1)

6

There are two types of name spaces: Flat name spaces and Hierarchical names.

Flat name spaces

In a flat name space, a name is a sequence of characters without structure.

A name in this space is assigned to an address.

The names were convenient and short.

A flat name space cannot be used in a large system such as the internet because it must be centrally controlled to avoid ambiguity and duplication.

Hierarchical Name Space

In hierarchical name space, each name consists of several parts.

First part defines the nature of the organization, second part defines the name of an organization, third part defines department of the organization, and so on.

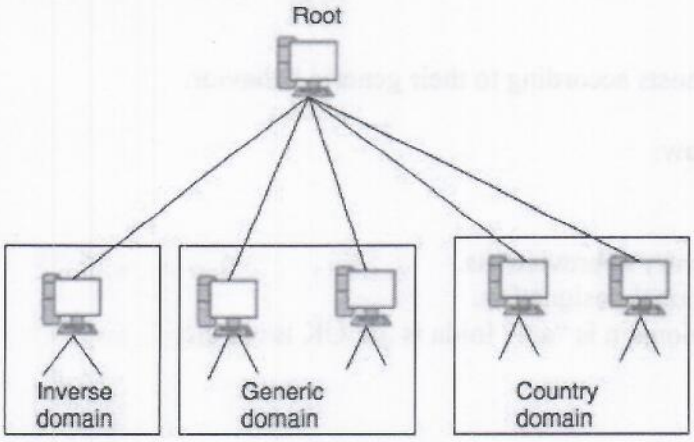
In hierarchical name space, the authority to assign and control the name spaces can be decentralized.

Authority for names in each partition is passed to each designated agent.

DNS in the Internet

DNS is a protocol that can be used in different platform.

Domain Name Space is divided into different sections in the Internet: Generic domain, country domain and inverse domain.



(2)

Fig. : DNS in the Internet

2. Inverse Domains

Inverse domain is used to map an address to a name.

For example, a client send a request to the server for performing a particular task, server finds a list of authorized client. The list contains only IP addresses of the client.

The server sends a query to the DNS server to map an address to a name to determine if the client is on the authorized list.

This query is called an inverse query.

This query is handled by first level node called arpa.

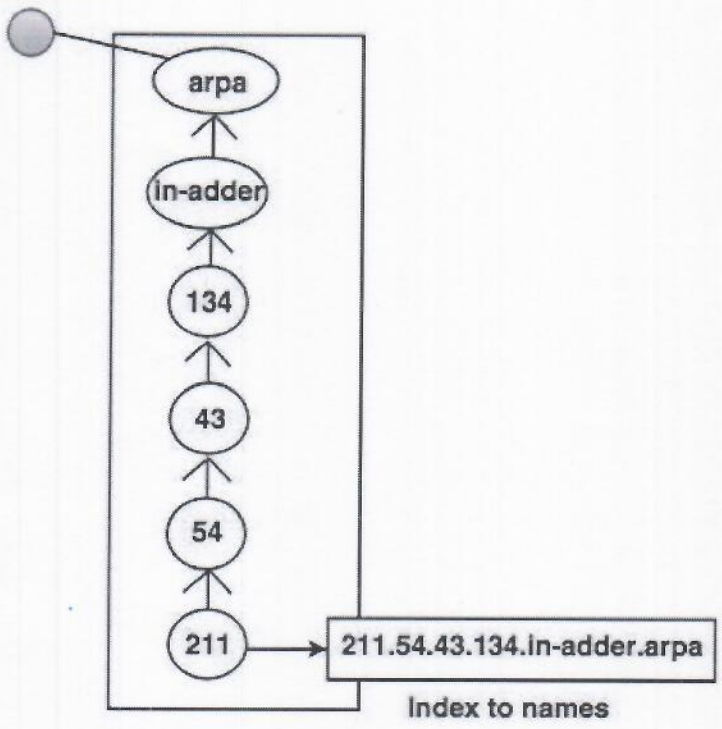


Fig. Inverse domain

(2)