	R V College of Engineering **Department of Computer Science and Engineering** **CIE - III: Question Paper**	
Course: (Code)	**Computer Networks(21CS45)**	**Semester: IV**

Date: Sept 2023	**Duration:** 90 minutes	**Staff:**	**SCN/MM/PH/SUN/NS**
Name:	**USN:**	**Section:**	**A/B/C/ISE/AIML**

Sl. No	Questions	Marks	BTL	CO
1a	Compare and contrast Inter-domain Routing and Intra-domain Routing	04	3	5
1b	Briefly explain the concept of tunneling.	06	2	2
22a	Outline the different types of fragmentation.	05	1	4
2b	Describe the different types of ICMP messages.	05	2	2
3	How do IP addresses get mapped onto data link layer addresses, such as Ethernet? With a neat sketch explain the protocol used for this purpose.	10	2	1
4	With a neat diagram, explain the protocol used to determine the best paths for routing data packets between routers within an Autonomous System.	10	2	5
5a	Differentiate between UDP and TCP.	05	3	2
5b	Write a note on TCP Service Model.	05	1	2

COURSE OUTCOMES

CO1.	Apply the algorithms /techniques of routing and congestion control to solve problems related to Computer Networks.
CO2.	Analyze the services provided by various layers of TCP/IP model to build effective solutions
CO3.	Design sustainable networking solutions with societal and environmental concerns by engaging in lifelong learning for emerging technology.
CO4.	Exhibit network configuration, protocol usage and performance evaluation in networks.
CO5.	Demonstrate the solutions using various algorithms/protocols available to address networking issues using modern tools by exhibiting team work and effective communication.

	L1	L2	L3	L4	L5	L6	CO1	CO2	CO3	CO4	CO5
Marks	05	31	05	-	-	-	10	21	-	05	14

Computer Networks
CIE III Scheme and Solution

Q No.	Answers	Marks
1a		04
1b		06
2a		04

Feature	Intra-domain Routing	Inter-domain Routing
Scope	Within a single Autonomous System (AS)	Between different Autonomous Systems (ASes)
Purpose	Establish routes within the same network domain	Facilitate communication between different networks
Protocols	OSPF, RIP, IS-IS, EIGRP (for some vendors)	BGP (Border Gateway Protocol)
Metric Calculation	Typically uses link metrics (e.g., bandwidth)	Path attributes (e.g., AS path, preference, MED)
Administrative Control	Managed by a single administrative entity	Involves coordination between multiple administrative entities
Scalability	Suitable for large-scale networks	Handles global internet-scale routing
Convergence Speed	Generally faster convergence due to smaller network size and frequent updates	Slower convergence due to the complexity of inter-domain paths

A technique of internetworking called **Tunneling** is used when the source and destination networks of the same type are to be connected through a network of a different type.

Tunneling is **a way to move packets from one network to another**.
Tunneling works via encapsulation: wrapping a packet inside another packet.

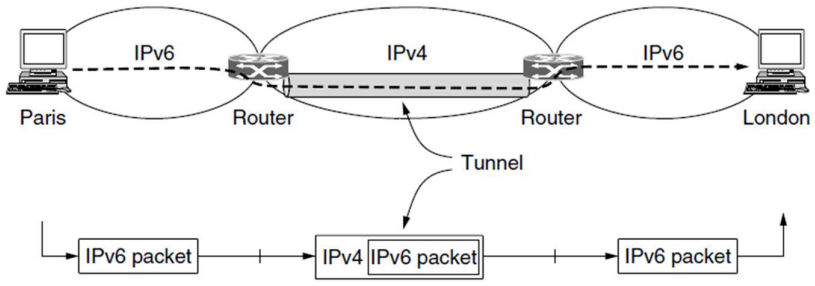
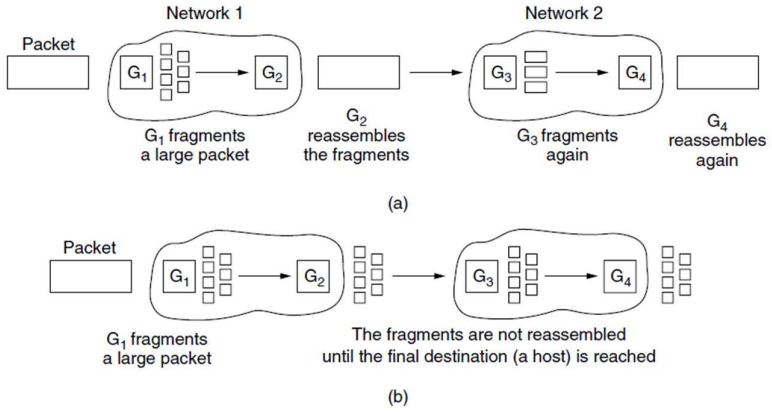
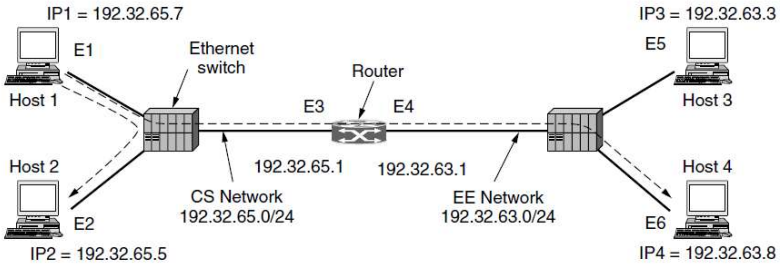
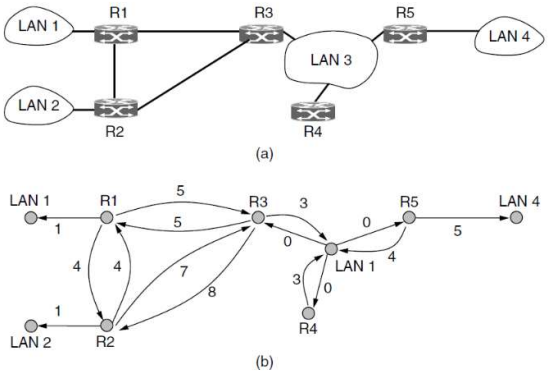
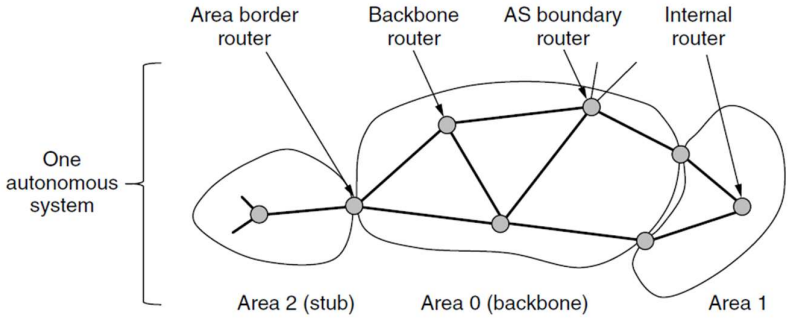


Figure 5-40. Tunneling a packet from Paris to London.

Diagram -1M
Explanation -4M

1. **Nontransparent Fragmentation:** Nontransparent fragmentation refers to a method where the responsibility for packet fragmentation lies with the sending device or host. When a data packet is larger than the MTU of the outgoing network link, the sending device is responsible for breaking down the packet into smaller fragments that fit within the MTU size.
2. **Transparent Fragmentation:** Transparent fragmentation, on the other hand, refers to a method where the network devices and routers in the path of the packet take responsibility for fragmentation. When a data packet is larger than the MTU of an outgoing network link, the intermediate network devices along

	the path will detect the oversize packet and fragment it into smaller pieces that fit within the MTU size of the outgoing link.  **Figure 5-42.** (a) Transparent fragmentation. (b) Nontransparent fragmentation.	01
2b	1. **Echo Request and Echo Reply (Ping):** ICMP Echo Request (Type 8) is used to request an "echo" from a target host, often referred to as "pinging." The target host responds with an ICMP Echo Reply (Type 0), indicating its availability and responsiveness. 2. **Destination Unreachable (Type 3):** This message type is used to indicate that a destination host or network is unreachable for various reasons, such as network congestion, unreachable host, or protocol unreachable. 3. **Time Exceeded (Type 11):** This message type is used to indicate that a packet has exceeded its time-to-live (TTL) value while traversing through routers. It is often used to detect routing loops or network issues. 4. **Redirect Message (Type 5):** A router can send an ICMP Redirect message to inform a host that a better route is available for a specific destination. 5. **Router Advertisement and Router Solicitation (Type 9 and Type 10):** These messages are used in the context of IPv6 to facilitate the autoconfiguration of network interfaces and to discover routers on the local network. 6. **Parameter Problem (Type 12):** This message is used to indicate that a problem has been detected with the IP header, such as an unrecognized option or an incorrect length. 7. **Timestamp Request and Timestamp Reply (Type 13 and Type 14):** These messages are used to request and respond with timestamps for diagnostic and timing purposes. 8. **Address Mask Request and Address Mask Reply (Type 17 and Type 18):** These messages are used to determine the subnet mask of a network, particularly in older versions of ICMP.	05

	9. **Source Quench (Type 4):** This message type is used to indicate to a sender that its traffic is causing congestion and should slow down.	
3	**The Address Resolution Protocol**  Frame / Source IP / Source Eth. / Destination IP / Destination Eth. Host 1 to 2, on CS net: IP1 / E1 / IP2 / E2 Host 1 to 4, on CS net: IP1 / E1 / IP4 / E3 Host 1 to 4, on EE net: IP1 / E4 / IP4 / E6 **Figure 5-61.** Two switched Ethernet LANs joined by a router. Diagram- 03 M Explanantion-07M	10
4	**OSPF- Interior Gateway Routing Protocol**  **Figure 5-64.** (a) An autonomous system. (b) A graph representation of (a).  **Figure 5-65.** The relation between ASes, backbones, and areas in OSPF. Diagram- 03 M Explanantion-07M	05

<table>
<tr>
<td>5a</td>
<td>
<table>
<tr><th>Aspect</th><th>TCP</th><th>UDP</th></tr>
<tr><td>Connection</td><td>Connection-oriented</td><td>Connectionless</td></tr>
<tr><td>Reliability</td><td>Reliable</td><td>Unreliable</td></tr>
<tr><td>Ordering</td><td>Maintains order of data</td><td>No guarantee of order</td></tr>
<tr><td>Error Checking</td><td>Yes (Checksum)</td><td>Limited (Checksum optional)</td></tr>
<tr><td>Flow Control</td><td>Yes (Congestion control)</td><td>No</td></tr>
<tr><td>Acknowledgments</td><td>Yes (Acknowledgment packets)</td><td>No acknowledgments</td></tr>
<tr><td>Header Size</td><td>Larger (20-60 bytes)</td><td>Smaller (8 bytes)</td></tr>
<tr><td>Overhead</td><td>Higher</td><td>Lower</td></tr>
<tr><td>Speed</td><td>Slower (due to overhead)</td><td>Faster (less overhead)</td></tr>
<tr><td>Use Cases</td><td>Reliable data transfer</td><td>Real-time applications, video streaming, online gaming</td></tr>
<tr><td>Example Protocols</td><td>HTTP, FTP, SMTP, SSH</td><td>DNS, VoIP, streaming, IoT</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>5b</td>
<td>
<table>
<tr><th>Port</th><th>Protocol</th><th>Use</th></tr>
<tr><td>20, 21</td><td>FTP</td><td>File transfer</td></tr>
<tr><td>22</td><td>SSH</td><td>Remote login, replacement for Telnet</td></tr>
<tr><td>25</td><td>SMTP</td><td>Email</td></tr>
<tr><td>80</td><td>HTTP</td><td>World Wide Web</td></tr>
<tr><td>110</td><td>POP-3</td><td>Remote email access</td></tr>
<tr><td>143</td><td>IMAP</td><td>Remote email access</td></tr>
<tr><td>443</td><td>HTTPS</td><td>Secure Web (HTTP over SSL/TLS)</td></tr>
<tr><td>543</td><td>RTSP</td><td>Media player control</td></tr>
<tr><td>631</td><td>IPP</td><td>Printer sharing</td></tr>
</table>
Figure 6-34. Some assigned ports.
Explanantion-04M
</td>
<td>05</td>
</tr>
</table>