

# CYBER FORENSICS

Dejey

*Assistant Professor*

*Department of Computer Science and Engineering*

*Anna University Regional Campus*

*Tirunelveli*

S. Murugan IPS

*Inspector General of Police*

*Tamil Nadu*

**OXFORD**  
UNIVERSITY PRESS

**OXFORD**  
UNIVERSITY PRESS

Oxford University Press is a department of the University of Oxford. It furthers the University's objective of excellence in research, scholarship, and education by publishing worldwide. Oxford is a registered trade mark of Oxford University Press in the UK and in certain other countries.

Published in India by  
Oxford University Press  
Ground Floor, 2/11, Ansari Road, Daryaganj, New Delhi 110002, India

© Oxford University Press 2018

The moral rights of the author/s have been asserted.

First published in 2018

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior permission in writing of Oxford University Press, or as expressly permitted by law, by licence, or under terms agreed with the appropriate reprographics rights organization. Enquiries concerning reproduction outside the scope of the above should be sent to the Rights Department, Oxford University Press, at the address above.

You must not circulate this work in any other form  
and you must impose this same condition on any acquirer.

ISBN-13: 978-0-19-948944-2

ISBN-10: 0-19-948944-0

Typeset in ACaslonPro-Regular  
by Archetype, New Delhi 110063  
Printed in India by Magic International (P) Ltd., Greater Noida

Cover image: Elena Abrazhevich / Shutterstock

Third-party website addresses mentioned in this book are provided  
by Oxford University Press in good faith and for information only.  
Oxford University Press disclaims any responsibility for the material contained therein.

# PREFACE

Incidents of cybercrime are on the upward trend in the recent years and create challenges not only to law enforcement agencies, but also for business firms and common netizens. Cyber criminals are preying the computer systems of government and private organizations for exploiting their services and their ability to penetrate networks all over the world has increased at an exponential rate. Though the field of cyber security attempts to implement and maintain robust approaches to defend cyberattacks, even the strongest defense mechanisms such as firewall, intrusion detection, and encryption are at times insufficient to achieve computer security. The ultimate aim of cyber forensics is to identify whether any cybercrime has been executed and to trace its source from the digital evidence obtained and to recover data if in case it is compromised. Cyber forensics tools are useful in the investigation of cybercrimes. The success of a cybercrime investigation relies on accurate acquisition, in-depth analysis, and structured presentation of digital evidence before the appropriate forum or court of law.

Cyber law plays an important role in safeguarding the privacy of data. It plays a pivotal role to penalize the offenders of cyber space. A cyber user must be aware of the legal implications of cybercrime and its associated forensic activities. The field of cyber forensics opens up plenty of job opportunities, which benefit government organizations, private organizations, and educational institutions as it focuses on the protection of digital assets and intelligence. The computer and information security sector is bound to witness tremendous growth as everything in this world is going digital; the same is the case with risks and cybercrimes. Hence, security measures and risk management policies should be in place to respond to threats to cyber security.

The intended audience of this book includes undergraduate and postgraduate students in computer science, computer applications, computer science and engineering, information technology, as well as professional instructors and researchers. The book may also be useful for cyber forensic professionals and cybercrime investigators to understand cybercrime investigations, forensic investigation tools, and prosecution of cybercrimes. It will be useful for computer professionals for implementing security measures to protect their digital assets.

## ABOUT THE BOOK

This book is intended to make the reader aware of the growing cyber threats, cybercrimes, and how they are committed. It also provides the ways to combat cybercrime and provides a detailed description on the investigation from digital evidence. It highlights cyber forensics and also gives an insight to the present and future trends of cybercrime and forensics. Further, it attempts to elucidate the national and international laws governing cybercrime with various cases, case laws, and case studies.

The language of the text is simple and lucid, while at the same time conveying all the concepts clearly. The theory is well balanced with a number of illustrations and case studies. Most of the illustrations have been drawn in a manner that helps a student to easily understand the theory. Facts relevant to the concept discussed have been provided in the form of boxed items in each chapter to help promote clarity among readers. Demonstrations with appropriate tools are presented to expose the readers to how real-world cybercrime cases are cracked.

## SALIENT FEATURES

- Contains a set of review questions and application exercises at the end of every chapter to be attempted by the student independently. Around 200 multiple-choice questions with answers have also been provided.
- Serves as a single-point resource work addressing cybercrime, cyber forensics, and associated laws and also covers the basics of networks and network security.
- Explains state-of-the-art technologies such as cryptocurrencies and block chain with examples, since cybercrime issues are more prevalent in the deep web than in the surface.

- Discusses ransomware, the crime that shook the world in 2017, and also the challenges faced by law enforcing agencies (LEA) in addressing deep web issues such as Silk Road and issues of anonymity.
- Illustrates concepts through cases, case studies, and case laws for the students to better relate to the relevant discussions.

## ONLINE RESOURCES

The following resources are available to support the faculty and students using this text:

### For faculty

- Lecture PPTs
- Instructor's manual (hints/answers to chapter-end application exercises)

### For students

- Colour illustrations from the book
- Video resources on email tracing, tracking, and recovery of deleted files

## CONTENTS AND COVERAGE

Each chapter commences with a list of learning objectives, which inform the reader what he/she is going to learn in the chapter. All the chapters are organized in such a way that the reader gets a thorough knowledge of the fundamentals, terminologies, and the advanced concepts clearly.

*Chapter 1* explains the networking architecture and technologies, the OSI model and its characteristics, functions, and associated protocols, LAN technologies, network topologies, networking devices, and TCP and IP suites. Besides this, the chapter presents the security vulnerabilities in the TCP/IP suite and the security mechanism developed for networking layers as well as the security options and protocols at the network, transport, and application layers. Finally, firewall and intrusion detection system and their use in network security are explained.

*Chapter 2* deals with cybercrime, its types and associated concepts. Cybercrimes are presented in three categories namely cybercrimes against person, property, and nation. The role of electronic communication device (ECD) and mobile ECD in the commission of cybercrime and the tools that facilitate them are presented. Challenges with cybercrime are explored along with cybercrime prevention strategies. Cybercrime incidents on the national and global arena are highlighted.

*Chapter 3* presents a deeper insight into various categories of cybercrime, the ways to handle them as well as the preventive measures to be adopted. Some of the incidents of cybercrime reported in the country and around the globe are included as cases.

*Chapter 4* discusses the current scenario and future of cybercrime—cyber war, an overview of cryptocurrencies that facilitate a ransomware attack, block chain, its underlying technology, ransomware, and the dark side of web. The challenges with dark web and deep web are also discussed.

*Chapter 5* presents the components of security, and the definitions of cyber forensics. It highlights forensic investigation and forensic examination processes besides describing their benefits. The chapter explains the various types of forensics; incident and incident handling approaches, and the role of CSIRT are also discussed.

*Chapter 6* explains the digital evidence collection procedure and the obstacles to this process. The chapter highlights the sources of evidences, namely various operating systems and their artifacts, the Windows registry, and various file systems. It also explains the sources of digital evidence in mobile devices and the Internet. Challenges associated with digital evidence are also discussed.

*Chapter 7* lists out the tools used for forensic investigation, namely free and open-source, as well as proprietary forensic suites, imaging and validation tools, integrity verification tools, tools for data recovery and RAM analysis, tools for analysis of registry, encryption and decryption, password recovery, and network analysis. Other miscellaneous tools used for forensic investigation in the UNIX system, as well as forensic analysis tools for mobile devices and email are summarized. The current requirement for forensic investigators is explained with the career prospects in this field and the available certifications and training are elucidated.

*Chapter 8* discusses the preliminaries of electronic evidence, an overview on how to acquire evidence, a detailed insight into the seizure process, and a deeper insight into acquiring evidence from computers, email, the Internet, and mobile devices. Besides these, it explains the process involved in acquiring evidence from other devices and media, as well as from third-party organizations. Finally, it explains the handling of digital evidence.

*Chapter 9* provides an insight into forensic copying, computation of hash, analysis of files stored in storage media, and identification and retrieval of deleted files. It presents the steps associated with live forensics. It introduces the working of various forensic tools such as FTK Imager, Autopsy, Volatility, and WinHex. Further, it explains email tracking and tracing with necessary tools along with the role of a forensic analyst for report preparation.

*Chapter 10* explains how to document the collected evidence and present it in the court of law. It provides the basics of electronic records supported by law, admissibility of electronic records in accordance with the rules, and categorization of evidence. The chapter also discusses the steps involved in presenting the evidence, namely reporting and testimony, with relevant guidelines and challenges. The court presentation system and a summary of the investigation process are also discussed.

*Chapter 11* provides some of the cybercrimes as case studies. A gist of the case is presented first. This is followed by an explanation on investigation and analysis along with evidence gathering. Finally, applicable sections of the law under the Indian Penal Code (IPC) and Information Technology (Amendment) Act (ITAA) 2008 are listed for every case.

*Chapter 12* introduces cyber laws and their need. The laws and their legal issues have been discussed. The chapter also offers an introduction to cyber security and the strategies to be adopted. How the laws are applicable to minimize risk is discussed, along with the initiatives taken by the government.

*Chapter 13* explains the laws governing different domains such as intellectual property rights, cyber space, and Internet with respect to privacy. The chapter provides a deeper insight into the laws that are part of the ITA 2000 and IPC to handle cybercrimes and categorizes them as crime against individual, property, and nation. Besides this, the cyber laws associated with ensuring cyber security are also presented. The other laws related to cyber security and cybercrime investigations are discussed. The amendments carried out to the Indian Evidence Act (IEA) 1872 and the Banker's Book Evidence Act 1891 are also furnished in this chapter.

*Chapter 14* exposes the reader with the cyber laws in force at the international level. It provides an insight into the cyber laws of representative countries such as the United States of America, the United Kingdom, the Netherlands, Malaysia, and Australia. A comparison of the cybercrime legislations in representative countries for certain specific cybercrimes is presented. Case studies, as applicable, are highlighted wherever necessary.

## ACKNOWLEDGEMENTS

The authors thank Advocate Jemila Samerin and Dr A.S. Vijila Samerin, Assistant Professor in English, for their help in the process of proofreading and editing. They sincerely thank the talented team of editors at Oxford University Press, India and all the reviewers who provided prompt guidance and very valuable feedback, which helped immensely in improving the contents of this book.

Dr Dejei thanks the co-author Dr S. Murugan for his unconditional support and the authorities of Anna University, Chennai for granting permission and providing the necessary infrastructure for this venture. She conveys her special thanks to her parents, family, friends, and relatives who supported and encouraged her, while she was working long hours on the book. She also thanks her student and scholar Ms M. Kaviya Elakkiya for her consistent support in the different phases of creation of this book.

Dr S. Murugan thanks the co-author Dr Dejei who travelled with him in the journey of writing this book. Further, he thanks his family members for their support and encouragement and his mother for her blessings. He also acknowledges the Tamil Nadu Police Department for support and encouragement.

Dejei  
Murugan IPS

# FEATURES OF

**CLASSIFICATION OF  
CYBERCRIME**

**3**

**CYBER FORENSICS—THE  
PRESENT AND THE FUTURE**

**7**

**CYBER LAWS IN INDIA AND  
CASE STUDIES**

**13**

**Addresses important  
segments**

A single-point resource  
work addressing  
cybercrime, forensics,  
and associated laws

**Covers basics of  
networks and security**

Provides an  
introductory chapter  
on networking and  
cyber security

**NETWORKS AND NETWORK  
SECURITY**

**1**

**Interesting examples**

Presents brief cases and  
boxed items containing  
additional information  
throughout all chapters

## Box 8.4 Forensic Boot Disk

It is used to boot the suspect system safely. It contains a file system and statically linked utilities such as ls, fdisk, ps, nc, dd, and ifconfig. It places the suspect media in a locked or read-only state. It does not swap any data to the suspect media. Some of the open source bootable images include FIRE (<http://biatchux.dmzs.com/?section=main>), Linuxcare Bootable Business Cards (<http://lbt.linuxcare.com/index.epl>), and Trinux (<http://trinux.sourceforge.net/>).

## Case 2: Cyber Stalking

In the first successful prosecution under the California (USA) cyber stalking law, prosecutors obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit rape of a woman who rejected his romantic advances.

He terrorized the 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized about being raped. On at least six occasions, sometimes in the middle of the night, men knocked at the woman's door saying that they wanted to rape her.

# THE BOOK



## Rich pedagogy

Chapter-end learning features include points to remember, key terms, multiple-choice questions with answers, review questions, and application exercises that cover all the concepts learnt in each chapter and help provide a quick recap

## POINTS TO REMEMBER

- Evidence may be oral or documentary, and documentary evidence may be primary or secondary.
- Digital evidence is unique and can be judged as neither primary nor secondary evidence.

## MULTIPLE-CHOICE QUESTIONS

1. The rules and regulations of cyber laws are covered under \_\_\_\_\_.
  - (a) Information Technology (Certifying Authorities) Rules 2000
  - (b) Information Technology (Security Procedure)

## KEY TERMS

**Digital evidence** This refers to information or data stored on, transmitted, or received by an electronic device in binary form that is of value in a criminal

## REVIEW QUESTIONS

1. List the types of cybercrime and their probable location of digital evidence.  
What are the steps to be followed by an IO during the scene investigation?

## APPLICATION EXERCISES


1. Imagine that you are the forensic examiner for a crime reported as 'theft of intellectual property' by an organization, say, X. The IO had reported after a thorough investigation that an employee, say, Y had become disgruntled in recent months

**CYBER LAWS IN INDIA AND  
CASE STUDIES**

**13**

**INTERNATIONAL CYBER LAWS  
AND CASE STUDIES**

**14**



**Balanced discussion  
of both Indian and  
International cyber laws**

Provides a balanced discussion of both international and Indian laws according to the context

# BRIEF CONTENTS

*Preface* v

*Features of the Book* viii

*Detailed Contents* xi

1. Networks and Network Security	1
2. Introduction to Cybercrime	44
3. Classification of Cybercrime	78
4. Cybercrime—The Present and the Future	121
5. Introduction to Cyber Forensics	149
6. Digital Evidence	184
7. Cyber Forensics—The Present and the Future	232
8. Acquisition and Handling of Digital Evidence	269
9. Analysis of Digital Evidence	301
10. Admissibility of Digital Evidence	350
11. Cybercrime Case Studies	371
12. Introduction to Cyber Laws	391
13. Cyber Laws in India and Case Studies	399
14. International Cyber Laws and Case Studies	439

*Appendix* 474

*Index* 477



# DETAILED CONTENTS

*Preface* v

*Features of the Book* viii

*Brief Contents* x

<b>1. Networks and Network Security</b>	<b>1</b>		
1.1 Network 1			
1.2 Networking Architecture	1		
1.3 Networking Technologies	2		
1.4 Network Models	4		
1.4.1 <i>OSI Model</i>	4		
1.4.2 <i>Internet Model</i>	6		
1.5 Networking Devices	6		
1.6 LAN Technologies	8		
1.7 Networking Topologies	11		
1.8 Network Protocols—TCP/IP Protocol Suite	12		
1.9 Physical Layer	13		
1.10 Data Link Layer	14		
1.10.1 <i>Functions</i>	14		
1.10.2 <i>Error Control</i>	15		
1.10.3 <i>Flow Control</i>	17		
1.11 Network Layer	17		
1.11.1 <i>Network Addressing</i>	17		
1.11.2 <i>Routing in Network Layer</i>	17		
1.12 Network Layer Protocols	19		
1.12.1 <i>Address Resolution Protocol and Reverse Address Resolution Protocol</i>	20		
1.12.2 <i>Internet Control Message Protocol</i>	20		
1.12.3 <i>Internet Protocol Version 4</i>	20		
1.12.4 <i>Internet Protocol Version 6</i>	21		
1.13 Transport Layer	21		
1.13.1 <i>Transmission Control Protocol</i>	22		
1.13.2 <i>User Datagram Protocol</i>	25		
1.14 Application Layer	26		
1.14.1 <i>Application Layer Protocols</i>	26		
1.15 Security Vulnerabilities in TCP/IP Suite	28		
1.16 Security Mechanisms in Networking Layers	28		
1.17 Network Security at Network Layer with Internet Protocol Security	28		
1.17.1 <i>IPSec Communication</i>	29		
1.17.2 <i>Internet Key Exchange</i>	30		
1.18 Network Security at Transport Layer	30		
1.18.1 <i>Secure Socket Layer</i>	31		
1.18.2 <i>Transport Layer Security Protocol</i>	32		
1.18.3 <i>HTTPS</i>	32		
1.18.4 <i>Secure Shell Protocol</i>	33		
1.19 Network Security at Application Layer	33		
1.19.1 <i>Pretty Good Privacy</i>	34		
1.19.2 <i>Secure MIME</i>	34		
1.19.3 <i>DNSSEC</i>	35		
1.20 Network Security with Firewall	36		
1.21 Network Security with Intrusion Detection System and Intrusion Detection and Prevention System	36		
<b>2. Introduction to Cybercrime</b>	<b>44</b>		
2.1 Introduction	44		
2.1.1 <i>Definition</i>	45		
2.2 Role of Electronic Communication Devices and Information and Communication Technologies in Cybercrime	45		
2.3 Mens rea and Actus reus in Cybercrime	46		
2.4 Types of Cybercrime	47		
2.5 Cybercrime against Individuals	47		
2.6 Cybercrime against Property	48		
2.7 Cybercrime against Nation	52		
2.7.1 <i>Content-related Offences</i>	53		
2.8 Crimes Associated with Mobile Electronic Communication Devices	54		
2.9 Classification of Cybercriminals	55		
2.10 Execution of Cybercrime	56		
2.11 Tools used in Cybercrime	57		
2.12 Factors Influencing Cybercrime	59		
2.13 Challenges to Cybercrime	60		
2.14 Strategies to Prevent Cybercrimes	61		
2.14.1 <i>Indian Perspective</i>	62		
2.14.2 <i>Global Best Practices</i>	64		

2.15	Extent of Cybercrime	65	4.7	Ransomware	131
2.15.1	<i>Cybercrime Statistics and World</i>	65	4.7.1	<i>Evolution of Ransomware</i>	131
2.15.2	<i>Cybercrime Statistics in India</i>	66	4.7.2	<i>Types of Ransomware</i>	132
2.15.3	<i>Recent Sensitive Cybercrimes</i>	67	4.7.3	<i>Entities Affected by Ransomware Attack</i>	133
2.15.4	<i>Latest incidents of Cybercrime in India</i>	68	4.7.4	<i>Mode of Infection of Users with Ransomware</i>	133
2.16	Terms and Terminologies Associated with Cybercrime	69	4.7.5	<i>Events in Ransomware Attack</i>	134
<b>3.</b>	<b>Classification of Cybercrime</b>	<b>78</b>	4.7.6	<i>Post-delivery of Ransomware</i>	135
3.1	Introduction	78	4.7.7	<i>Preventing Ransomware from Full Execution</i>	135
3.2	Cybercrime against Individuals	78	4.7.8	<i>Steps to Carry Out in Event of Infection with Ransomware</i>	135
3.2.1	<i>Internet Grooming</i>	79	4.7.9	<i>Best Practices to Adopt</i>	135
3.2.2	<i>Cyber Stalking</i>	79	4.7.10	<i>Role of Antivirus</i>	136
3.2.3	<i>Cyber Harassment</i>	80	4.7.11	<i>Prevention and Response Team</i>	136
3.2.4	<i>Cyber Extortion</i>	81	4.8	Deep Web and Dark Web	138
3.2.5	<i>Online Pedophilia</i>	82	4.9	Deep Web and its Challenges	138
3.3	Cybercrime against Property	83	4.9.1	<i>The Internet</i>	138
3.3.1	<i>Illegal Access—Hacking and Cracking</i>	83	4.9.2	<i>Accessing Dark Web</i>	140
3.3.2	<i>Illegal Data Acquisition—Data Espionage</i>	84	4.9.3	<i>Size and Scale of Deep Web</i>	140
3.3.3	<i>Illegal Interception</i>	87	4.9.4	<i>Onion Router—TOR</i>	141
3.3.4	<i>Data Interference</i>	90	4.9.5	<i>Search Engines vs Deep Web</i>	141
3.3.5	<i>System Interference—Computer Threats</i>	97	4.9.6	<i>Deep Web Source Repository</i>	141
3.3.6	<i>Copyright- and Trademark-related Offences</i>	103	4.9.7	<i>Challenges</i>	142
3.3.7	<i>Computer-related Offences</i>	105	4.9.8	<i>Counter Measures to Overcome Challenges with Deep Web</i>	143
3.4	Cybercrime against Nation	109	<b>5.</b>	<b>Introduction to Cyber Forensics</b>	<b>149</b>
3.4.1	<i>Cyber Terrorism</i>	109	5.1	Interrelation among Cybercrime, Cyber Forensics, and Cyber Security	149
3.4.2	<i>Cyber Warfare</i>	110	5.1.1	<i>Security</i>	150
3.4.3	<i>Cyber Laundering</i>	110	5.2	Cyber Forensics	151
3.4.4	<i>Content-related Offences</i>	111	5.2.1	<i>Definition</i>	151
<b>4.</b>	<b>Cybercrime—The Present and the Future</b>	<b>121</b>	5.2.2	<i>Need</i>	151
4.1	Introduction to Cyber War—The Present and the Future of Cybercrime	121	5.2.3	<i>Objectives</i>	151
4.2	Cryptocurrency	122	5.2.4	<i>Computer Forensics Investigations</i>	152
4.2.1	<i>Characteristics</i>	123	5.2.5	<i>Steps in Forensic Investigation</i>	152
4.2.2	<i>Types</i>	124	5.2.6	<i>Forensic Examination Process</i>	154
4.3	Bitcoin	125	5.2.7	<i>Methods Employed in Forensic Analysis</i>	155
4.3.1	<i>Bitcoin Cash</i>	127			
4.4	Ethereum	127			
4.5	Comparison between Bitcoin and Ethereum	128			
4.6	Blockchain	129			
4.6.1	<i>Association between Bitcoin and Blockchain</i>	131			

5.2.8	<i>Classification of Cyber Forensics</i>	155	<b>6. Digital Evidence</b>	<b>184</b>
5.2.9	<i>Benefits of Cyber Forensics</i>	155	6.1	Introduction to Digital Evidence and Evidence Collection Procedure 184
5.3	Disk Forensics	155	6.1.1	<i>Types of Digital Evidence</i> 184
5.3.1	<i>Challenges</i>	156	6.1.2	<i>Evidence Collection Procedure</i> 185
5.4	Network Forensics	156	6.1.3	<i>Mechanisms Associated with Digital Evidence Collection</i> 187
5.4.1	<i>Tools for Analysis</i>	156	6.2	Sources of Evidence 187
5.4.2	<i>Challenges</i>	156	6.3	Digital Evidence from Standalone Computers/Electronic Communication Devices 187
5.5	Wireless Forensics	157	6.4	Operating Systems and their Boot Processes 188
5.5.1	<i>Forensic Tools</i>	157	6.5	Storage Medium 190
5.5.2	<i>Challenges</i>	157	6.5.1	<i>Disk Drive</i> 190
5.6	Database Forensics	158	6.5.2	<i>Other Storage Media</i> 194
5.6.1	<i>Forensic Approaches</i>	158	6.6	File System 194
5.6.2	<i>Forensic Methodology</i>	159	6.6.1	<i>FAT File System and its Components</i> 195
5.7	Malware Forensics	160	6.6.2	<i>Extended File Allocation Table File System</i> 198
5.7.1	<i>Malware Analysis</i>	160	6.6.3	<i>New Technology File System</i> 202
5.8	Mobile Forensics	160	6.6.4	<i>ext family of File Systems</i> 209
5.8.1	<i>Stages</i>	161	6.6.5	<i>Hierarchical File System</i> 213
5.8.2	<i>Analysis Tools</i>	162	6.7	Windows Registry 215
5.9	GPS Forensics	163	6.8	Windows Artifacts 217
5.10	Email Forensics	164	6.9	Browser Artifacts 219
5.10.1	<i>Client and Server in Email</i>	164	6.10	Macintosh Artifacts 220
5.10.2	<i>Structure of Email</i>	164	6.11	Linux Artifacts 221
5.10.3	<i>Working of Email</i>	165	6.12	Whole Disk Encryption or Full Disk Encryption 221
5.10.4	<i>Email Protocols</i>	165	6.13	Evidence from Mobile Devices 222
5.10.5	<i>Examining Email Messages</i>	166	6.14	Digital Evidence on the Internet 223
5.10.6	<i>Viewing Email Headers</i>	166	6.15	Digital Evidence as Alibi 224
5.10.7	<i>Examining Email headers</i>	167	6.16	Impediments to Collection of Digital Evidence 225
5.10.8	<i>Examining Additional Email Files</i>	168	6.17	Challenges with Digital Evidence 226
5.10.9	<i>Tracing Email Messages</i>	168	<b>7. Cyber Forensics—The Present and the Future</b>	<b>232</b>
5.10.10	<i>Email Servers and their Examination</i>	170	7.1	Forensic Tools 232
5.10.11	<i>Email Forensics Tools</i>	170	7.1.1	<i>Types</i> 233
5.10.12	<i>Tracking Emails</i>	171	7.1.2	<i>Categories</i> 233
5.11	Memory Forensics	172	7.2	Cyber Forensic Suite 235
5.11.1	<i>RAM Artifacts</i>	172	7.2.1	<i>Free and Open-source Forensic Suite</i> 235
5.11.2	<i>RAM Analysis</i>	172	7.2.2	<i>Proprietary Forensic Suites</i> 238
5.11.3	<i>Forensic Tools</i>	173		
5.12	Building Forensic Computing Lab	173		
5.13	Incident and Incident Handling	174		
5.13.1	<i>Incident</i>	174		
5.13.2	<i>Incident Handling</i>	175		
5.13.3	<i>Incident Reporting</i>	176		
5.13.4	<i>Incident Response</i>	176		
5.14	Computer Security Incident Response Team	177		
5.14.1	<i>Forensic Readiness</i>	178		

7.3	Drive Imaging and Validation Tools	239			
7.4	Forensic Tool for Integrity Verification and Hashing	240			
7.5	Forensic Tools for Data Recovery	241			
7.6	Forensic Tools for RAM Analysis	242			
7.7	Forensic Tools for Analysis of Registry	243			
7.8	Forensic Tools for Encryption/Decryption	243			
7.9	Forensic Tools for Password Recovery	244			
7.10	Forensic Tools for Analysing Network	245			
7.11	Forensic Utility for Metadata Processing	246			
7.12	Miscellaneous Tools	247			
7.13	Forensic Tools for UNIX System Analysis	250			
7.14	Forensic Tools for Other media	251			
7.15	Forensic Hardware	252			
7.16	Forensic Analysis Tools for Mobile Devices	252			
7.16.1	<i>Free and Open-source Forensic Tools for Mobile Devices</i>	252			
7.16.2	<i>Proprietary Forensic Tools for Mobile Devices</i>	254			
7.16.3	<i>Forensic Hardware for Mobile Devices</i>	255			
7.17	Forensic Tools for Email Analysis	256			
7.18	Need for Computer Forensic Investigators	257			
7.19	Career Prospects for Forensic Investigators	258			
7.20	Forensic Training and Certifications	258			
<b>8.</b>	<b>Acquisition and Handling of Digital Evidence</b>	<b>269</b>			
8.1	Preliminaries of Electronic or Digital Evidence	269			
8.1.1	<i>Categorization of Source of Digital Evidence</i>	270			
8.1.2	<i>Locality of Digital Evidence</i>	271			
8.1.3	<i>Roles played by Digital Evidence</i>	271			
8.1.4	<i>Characteristics of Digital Evidence</i>	271			
8.1.5	<i>Physical versus Digital Evidence</i>	271			
8.1.6	<i>Order of Volatility of Digital Evidence</i>	272			
8.1.7	<i>List of Crimes and Probable Location of Evidence</i>	273			
8.2	Acquisition and Seizure of Evidence	274			
8.2.1	<i>Acquisition of Evidence</i>	274			
8.2.2	<i>Precautionary Measures before Acquisition</i>	274			
8.2.3	<i>Search and Seizure</i>	275			
8.2.4	<i>Seizure Memo</i>	276			
8.3	Chain of Custody and Digital Evidence Collection Form	277			
8.3.1	<i>Chain of Custody</i>	277			
8.3.2	<i>Digital Evidence Collection Form</i>	278			
8.4	Fourth Amendment and Seizure	279			
8.4.1	<i>Search and Seizure with Search Warrant</i>	279			
8.4.2	<i>Warrantless Searches</i>	279			
8.5	Acquisition of Computer and Electronic Evidence	280			
8.5.1	<i>Acquisition of Configuration Information through Controlled Boots</i>	281			
8.5.2	<i>Acquisition of Evidence from Switched-off Systems</i>	281			
8.5.3	<i>Collection of Volatile Data</i>	283			
8.5.4	<i>Acquisition of Evidence from Live Systems</i>	283			
8.5.5	<i>Acquisition of Evidence from Standalone Hardware Device</i>	284			
8.5.6	<i>Acquisition of Evidence from Non-detachable Hard Disk Drive</i>	284			
8.6	Acquisition Procedure using Target Disk Mode from Apple Macintosh Computer	286			
8.6.1	<i>Social Media</i>	288			
8.7	Acquisition of Evidence from Mobile Phone and PDA	288			
8.7.1	<i>Procedure for Acquiring Evidence from Mobile Phones</i>	292			
8.8	Acquisition of Evidence from Optical and Removable Media, Digital Cameras	292			
8.8.1	<i>Evidence from Optical Media</i>	292			
8.8.2	<i>Evidence from USB Drives</i>	292			
8.8.3	<i>Evidence from Digital Cameras</i>	293			

8.9	Acquisition of Evidence from Third Party, External Agency, or Organization	293	10.5	Presenting Digital Evidence	360
8.10	Challenges to Acquisition of Digital Evidence	293	10.5.1	<i>Reporting—Expert Report</i>	360
8.11	Handling of Digital Evidence	294	10.5.2	<i>Guidelines for Cyber Forensic Examiners</i>	361
8.12	Precautions Involved in Handling Digital Evidence	296	10.5.3	<i>Testimony</i>	362
<b>9.</b>	<b>Analysis of Digital Evidence</b>	<b>301</b>	10.5.4	<i>Courtroom Presentation System</i>	363
9.1	Introduction to Analysis of Digital Evidence	301	10.5.5	<i>Challenges with Admissibility and Presentation of Digital Evidence</i>	363
9.2	Capturing of Forensic Copy of Memory and Hard Drive with Toolkit Forensic Imager	302	10.6	Summary of Investigation Process Involving Digital Evidence	364
9.3	RAM Analysis with Volatility	307	<b>11.</b>	<b>Cybercrime Case Studies</b>	<b>371</b>
9.4	Analysing Hard Drive with WinHex	312	11.1	Introduction	371
9.4.1	<i>Acquiring Forensic Copy of Drive</i>	312	11.2	Cybercrime against Individual	371
9.4.2	<i>Computing Hash</i>	314	11.2.1	<i>Posting of Obscene, Defamatory, and Annoying Messages against Women Online (State of Tamil Nadu vs Subas Katti)</i>	371
9.4.3	<i>Analysing Hard Disk</i>	316	11.2.2	<i>Phishing Fraud</i>	372
9.4.4	<i>Analysing Slack Space and Free Space</i>	327	11.2.3	<i>Hacking using Key Logger</i>	373
9.4.5	<i>File Carving</i>	328	11.2.4	<i>Impersonation for Purpose of Cheating</i>	375
9.5	Working with Autopsy	328	11.2.5	<i>Transmission of Sexually Explicit Material through Internet</i>	376
9.5.1	<i>Analysis Basics</i>	330	11.2.6	<i>Criminal Intimidation and Sending Obscene Material through Internet</i>	377
9.5.2	<i>Timeline</i>	330	11.2.7	<i>Trolling on Social Media</i>	377
9.5.3	<i>Example Use Cases</i>	330	11.3	Cybercrime against Property	379
9.5.4	<i>Analysis of Deleted Files with Autopsy</i>	331	11.3.1	<i>Online Lottery Scam</i>	379
9.6	Email Tracking and Tracing	336	11.3.2	<i>Theft in ATM</i>	380
9.6.1	<i>Email Tracking</i>	336	11.3.3	<i>Swindling of Money by Bank Employee</i>	381
9.6.2	<i>Email Tracing</i>	338	11.3.4	<i>Data Theft</i>	383
9.7	Role of Forensic Analyst in Analysis	343	11.3.5	<i>Hacking</i>	384
<b>10.</b>	<b>Admissibility of Digital Evidence</b>	<b>350</b>	11.3.6	<i>Data Theft by Ex-employee</i>	385
10.1	Introduction	350	11.4	Cybercrime against Nation	386
10.2	Digital Evidence—Electronic Record	351	11.4.1	<i>Preparation of Forged Counterfeits using Computers/ Printers/Scanners</i>	386
10.2.1	<i>Prerequisites</i>	352	11.4.2	<i>Blocking of Websites</i>	388
10.2.2	<i>Retention of Electronic Records</i>	352	<b>12.</b>	<b>Introduction to Cyber Laws</b>	<b>391</b>
10.3	Section 5 of ITA 2000—Legal Recognition of Digital Signatures	352	12.1	Cyber Laws	391
10.3.1	<i>Rules of Admissibility of Electronic Evidence</i>	357	12.2	Need for Cyber Laws	391
10.3.2	<i>Categorization and Characteristics of Evidence with Respect to Law</i>	357	12.3	Cyber Laws and Legal Issues	392
10.4	Pre-trial Preparation	360	12.4	Cyber Security	393

12.5	Strategies Involved in Cyber Security	393	13.10	Summary of Cyber Laws in India	427
12.6	Minimizing Risk with Cyber Laws	393	13.11	Amendments to the Indian Evidence Act 1872 in View of Information Technology Act 2000	429
12.7	Initiatives Promoting Cyber Security	394	13.12	Amendments to the Banker's Book Evidence Act 1891 in View of Information Technology Act 2000	431
12.8	Terms and Terminologies Associated with Cyber Laws	394	13.13	Indian Laws Related to Intellectual Property	432
<b>13.</b>	<b>Cyber Laws in India and Case Studies</b>	<b>399</b>	13.14	Indian Case Laws	432
13.1	Cyber Laws, Cybercrime, and Cyber Security	399	<b>14.</b>	<b>International Cyber Laws and Case Studies</b>	<b>439</b>
13.2	Cyber Laws in India	399	14.1	Introduction	439
13.3	Information Technology Act 2000	400	14.2	Cybercrime Legislation in the Netherlands	439
13.3.1	<i>Scheme of IT Act 2000</i>	400	14.2.1	<i>Specific Cybercrime Legislations</i>	439
13.3.2	<i>Salient Features of the Information Technology (Amendment) Act 2008</i>	401	14.2.2	<i>Traditional Laws to Prosecute Cybercrimes</i>	442
13.4	Cybercrimes and Cyber Laws	402	14.2.3	<i>Powers for Search and Seizure</i>	443
13.5	Crime against Individual	404	14.2.4	<i>Other ICT-related Investigation Powers</i>	443
13.5.1	<i>Cyber Defamation</i>	404	14.3	Cyber Laws in Malaysia	443
13.5.2	<i>Cyber Stalking</i>	405	14.4	Cybercrime Laws in the UK	445
13.5.3	<i>Web Jacking</i>	406	14.5	Cybercrime Laws of the United States	451
13.5.4	<i>Violation of Privacy</i>	407	14.5.1	<i>Computer Fraud and Abuse Act</i>	452
13.6	Crime against Property	407	14.5.2	<i>Provisions for Handling Cyber Stalking</i>	455
13.6.1	<i>Theft of Data, Viral Attack, Hacking, Denial of Service Attack, and Cyber Bullying</i>	407	14.5.3	<i>Provisions to Handle Cyber Terrorism</i>	456
13.6.2	<i>Forgery</i>	409	14.5.4	<i>Electronic Communications Privacy Act</i>	456
13.6.3	<i>Data Diddling</i>	411	14.5.5	<i>Cyber Security Enhancement Act</i>	457
13.6.4	<i>Email Bombing</i>	411	14.5.6	<i>Digital Millennium Copyright Act</i>	457
13.6.5	<i>Possession of Stolen Electronic Communication Devices</i>	411	14.5.7	<i>Traditional Laws to Prosecute Cybercrime</i>	458
13.6.6	<i>Identity Theft and Password Theft</i>	412	14.5.8	<i>Summary of US Federal Cyber Laws</i>	459
13.6.7	<i>Financial Crime</i>	412	14.6	Australian Laws Related to Privacy and Cyber Security Domains	460
13.6.8	<i>Email Spoofing</i>	414	14.6.1	<i>Legal, Legislative, and Regulatory Environment</i>	460
13.6.9	<i>Email Fraud</i>	414	14.6.2	<i>Other Federal Legislative Acts</i>	463
13.6.10	<i>Copyright Infringement Crimes</i>	414			
13.6.11	<i>Sale of Illegal Articles on the Internet</i>	415			
13.7	Crime against Nation	416			
13.7.1	<i>Cyber Terrorism</i>	416			
13.7.2	<i>Website Defacement</i>	416			
13.7.3	<i>Pornography</i>	417			
13.8	Cyber Laws for Cyber Security	421			
13.9	Other Cyber Laws Associated with Cybercrime and Cyberspace	424			

Appendix 474

Index 477

# NETWORKS AND NETWORK SECURITY

---

## Learning Objectives

---

This chapter provides an overview of computer networks and network security. The objective of this chapter is to provide a deeper insight into computer networks, networking architecture, networking technologies, and network models (the OSI and the Internet), networking devices, LAN technologies, and various network topologies. The chapter presents the network protocol, the TCP/IP protocol suite. It also explains the characteristics and functions of every layer in the OSI and discusses the associated protocols. Besides this, the security vulnerabilities in the TCP/IP suite and the security mechanism are elucidated. Protocols for network security at the network, transport, and the application layer are explained in detail. The establishment of network security with firewalls is also explained. The reader will be familiar with the following after studying the chapter:

- Networking architecture and technologies
  - OSI model—characteristics, functions, and associated protocols
  - Networking devices, LAN technologies, and network topologies
  - TCP and IP suite
  - Security vulnerabilities in the TCP/IP suite and the security mechanism developed for networking layers
  - Security options and protocols at the network, transport layer, and application layer
  - Firewall and its use in network security
- 

## 1.1 NETWORK

A computer network is a collection of computers and devices interconnected by communication channels to facilitate communication and the sharing of information (data, messages, graphics) and resources (printers, fax machines, modems, and other hardware) among interconnected devices.

Thus, computer networks are primarily needed for information exchange and resource sharing.

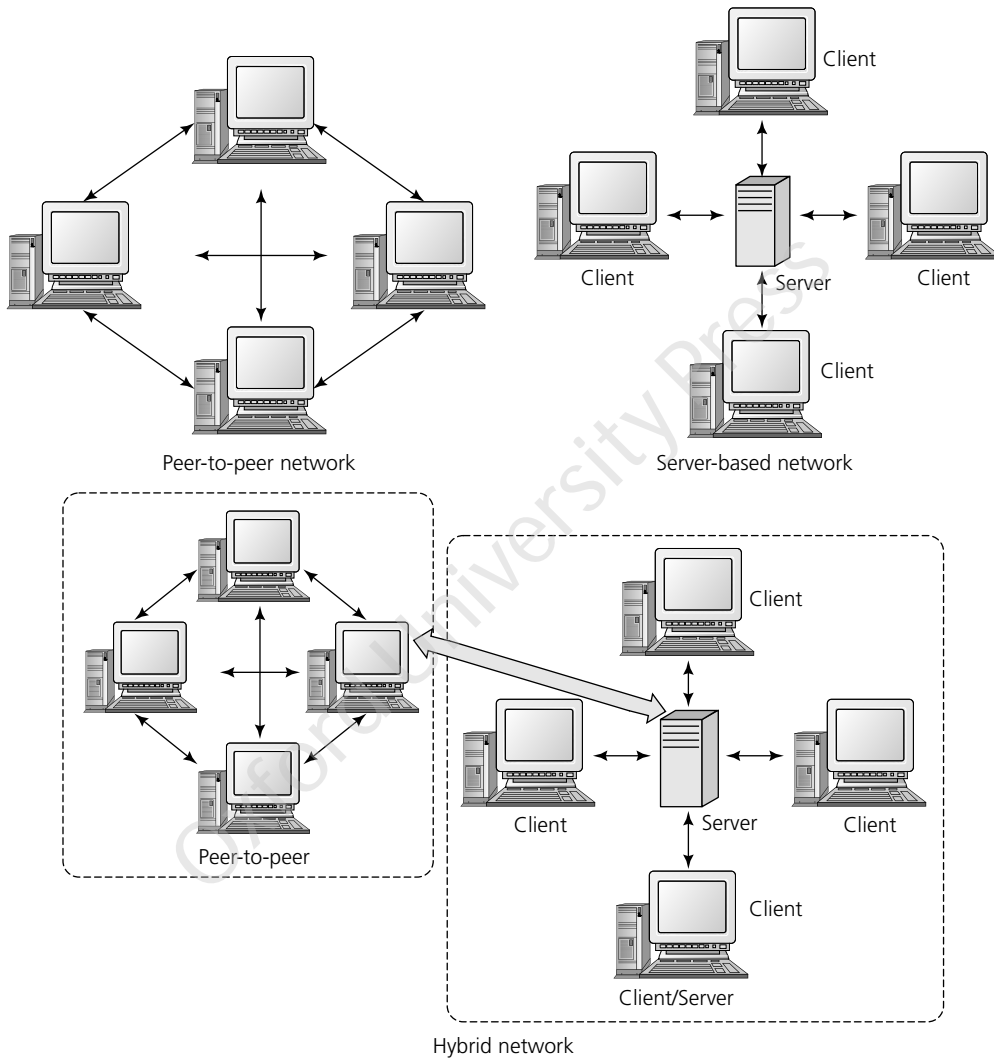
## 1.2 NETWORKING ARCHITECTURE

The three common forms of networking architecture are (a) peer-to-peer network, (b) client/server architecture (or) server-based network, and (c) hybrid network. This is shown in Fig. 1.1.

**Peer-to-peer network** In this network, any computer can act as a server or a client and there is no designated server. All the computers are referred to as peers. There is no designated administrator in such a network. Only the users on a peer-to-peer network determine what data from their computers can be shared on the network.

**Server-based network** In this network, there is a dedicated server and all the other computers are clients. The dedicated server services requests from network clients. More servers are required as the size and traffic in a network scale up. The server may be a *file and print server* that manages user access and the use of file and printer services; an *application server* that makes client/server applications and data available to the clients; a

*mail server* to manage electronic messaging between the network and the users; a *fax server* to manage incoming and outgoing data in the network by sharing one or more fax modem boards; or a *communication server* which handles data flow and email between its network and other networks as well as with remote users through a modem or telephone lines in a dial-up connection. The security aspect of servers is managed by the administrator, by setting up a policy that applies to every user on the network.



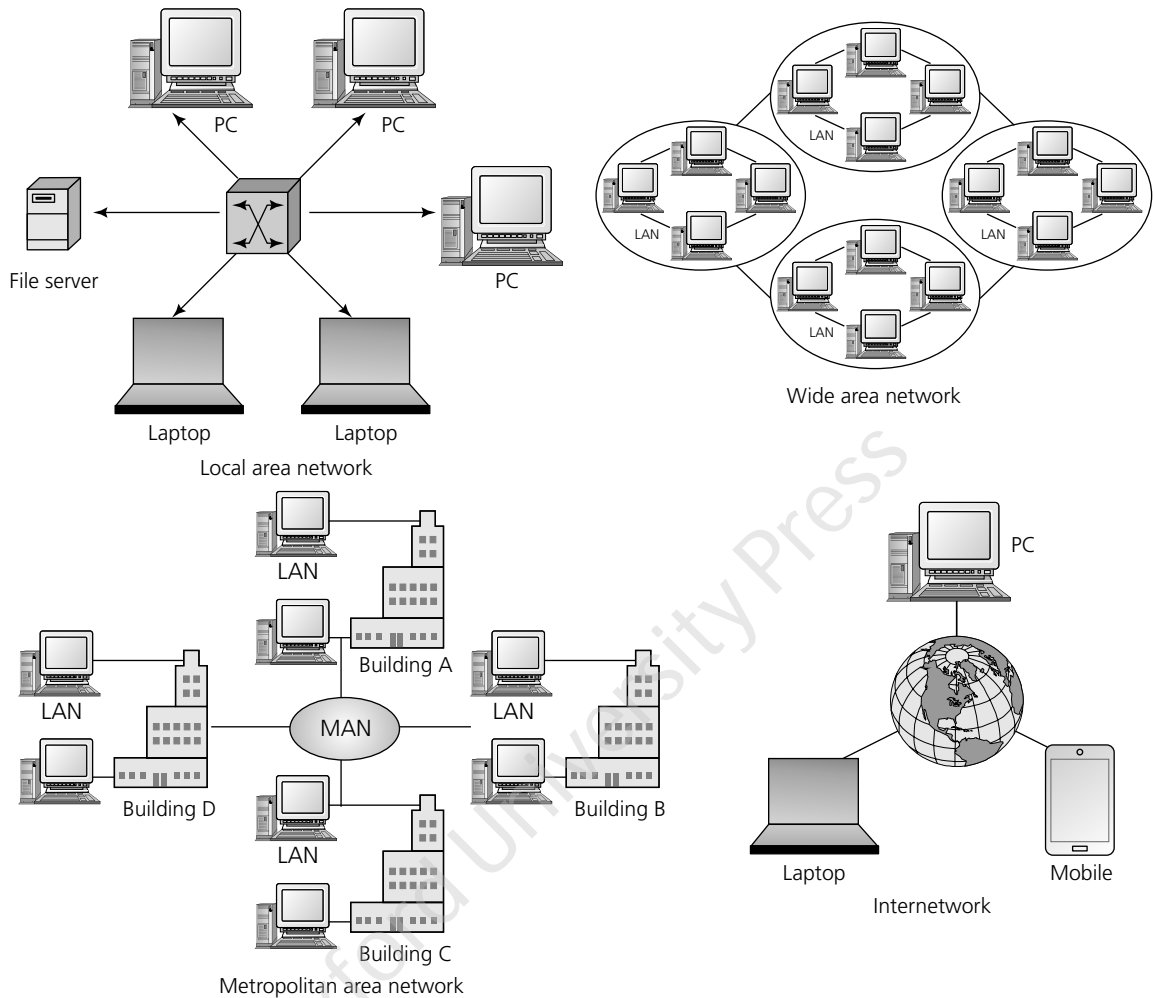
**Fig. 1.1** Networking architecture

**Hybrid network** This network is a combination of both, peer-to-peer network and server-based network.

### 1.3 NETWORKING TECHNOLOGIES

The four basic types of networking technologies based on geographical span are (a) local area network (LAN), metropolitan area network (MAN), wide area network (WAN), and Internetwork. This is shown in Fig. 1.2.





**Fig. 1.2** Networking technologies

### **Local Area Network**

LAN can be configured only if the distance between the computers is not much and they are spread over a small geographical area. LAN facilitates sharing of resources such as printers, scanners, file servers, and the Internet among computers. LAN is suitable for small organizations and for home-based networks. The networking components used for connectivity in a LAN include hubs, switches, and cables (Cat-5 and Cat-5e). LAN uses private IP addresses and does not involve any complicated routing. It works under its own domain and can be controlled centrally.

It uses either ethernet or token ring technology—the former is widely used, whereas the latter is only rarely used. Ethernet technology on LAN relies on star topology.

LAN can be either wired, wireless, or both.

### **Metropolitan Area Network**

MAN can be configured when the distance between the computers is large and the computers are far apart from each other, spanning a city or a town. It is larger than a LAN and smaller than a WAN. The technology

for MAN can be ethernet, token ring, asynchronous transfer mode (ATM), or fibre distributed data interface (FDDI). Metro ethernet enables expansion of LAN and is provided by Internet service providers (ISPs). The backbone of MAN is a high-capacity and high-speed fibre optic network.

### **Wide Area Network**

WAN can be configured if the distance between computers spans a large geographical distance, for example, across provinces or even a whole country, and is without limits. Internet is the largest WAN. WANs are equipped with a very high speed backbone and so use very expensive network equipment. The networking component used for connecting a WAN and a LAN is a router. The technologies used in WAN are ATM, frame relay, and synchronous optical network (SONET).

### **Internetwork**

Internetwork is a network of networks and is also called the Internet. It interconnects LAN and MAN. The Internet relies on the TCP/IP protocol suite and uses IP as its addressing protocol. The Internet is implemented using IPv4 and migrates to IPv6 due to shortage of address spaces. It has a very high speed backbone of fibre optics. It works on the client/server model.

The Internet is deployed on the World Wide Web (WWW) services using hypertext markup language (HTML)-linked pages and is accessible by client software known as the web browser. When a user requests a page located on some web server, anywhere in the world, using a web browser, the web server responds with the proper HTML page. The Internet serves a variety of purposes—websites, emails, instant messaging, blogging, social media, marketing, networking, resource sharing, and audio–video streaming (Box 1.1).

## **1.4 NETWORK MODELS**

This section presents the two important models behind networking, namely the OSI model and the Internet model.

### **1.4.1 OSI Model**

The open system interconnection (OSI) model is a seven-layer model used to visualize computer networks and to solve problems in them. The OSI model belongs to the International Standards Organization (ISO). It is shown in Fig. 1.3. All the layers, from the application layer to the physical layer, are explained.

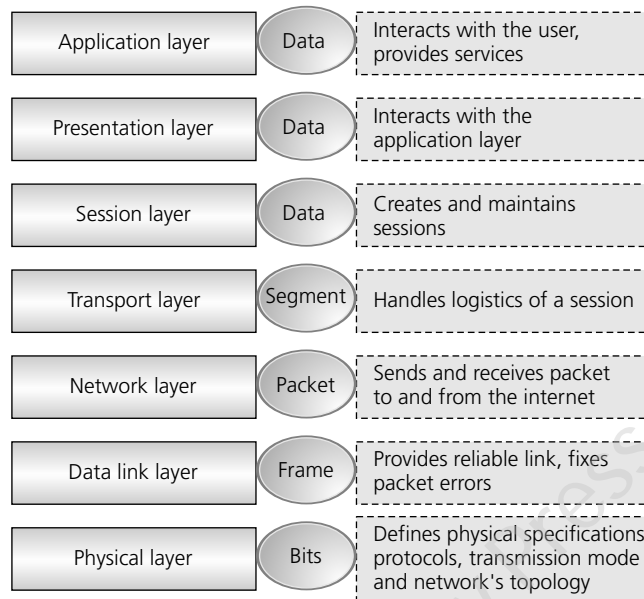
#### **Layer 7—Application Layer**

It is responsible for user interaction in the form of input and output. The application is some software that runs on the local machine but depends on network architecture. The software could be either cloud-based, that is, run on a remote server from where data is transferred over the Internet or software that is run on a local server. Thus, the application layer is responsible for providing services for email, telnet, file transfer, etc. For instance, the application layer can be the Internet browser, an FTP client, or Microsoft Word.

#### **Box 1.1 Internet and Intranet**

The Internet is an interconnection of many combinations of networks, such as LAN, WAN, and MAN. It is an unlimited source of a wide variety of information, and enables sharing and access to its users. It can offer connectivity to an unlimited number of users. There is no limit on bandwidth. Traffic on the Internet is unrestricted.

On the other hand, in an intranet, the network is restricted for use by a single corporate entity which has full control and management over the network. The functionality of the intranet is however the same as that of the Internet.



**Fig. 1.3** OSI model

### **Layer 6—Presentation Layer**

This layer directly interacts with the application layer above and this is where the operating system lies. Interaction happens either directly or through the Java runtime environment (JRE).

### **Layer 5—Session Layer**

The session layer is responsible for creating and maintaining sessions between the operating system on the presentation layer and other third-party machines. For example, while browsing, the user interacts with the application layer which in turn interacts with the presentation layer, and the session layer facilitates interaction between the operating system and the web server.

### **Layer 4—Transport Layer**

The logistics of a session are taken care of by the transport layer. For example, while browsing, the transport layer determines what and how much information should be exchanged between the operating system and the web server.

### **Layer 3—Network Layer or Internet Layer**

This layer is responsible for sending and receiving packets to and from the Internet as governed by the IP address of the router. The router, the hardware device essential for forwarding packets between computers on a network, operates in this layer.

### **Layer 2—Data Link Layer**

This layer is responsible for providing a reliable link between two directly connected nodes. It is also responsible for fixing packet errors which may arise in the physical layer below. Switches operate in this layer. On the basis of functionality, this layer is divided into two: the media access control (MAC) layer (which is responsible for the way in which the devices that are connected to the network gain access) and the logical link control (LC) layer (which is responsible for error checking and packet synchronization).

## Layer 1—Physical Layer

Any physical device or hardware that makes up the network is the physical layer, for example, ethernet cables and bluetooth. The functions of the layer include defining physical specifications, protocols, transmission modes, and network topology.

### 1.4.2 Internet Model

The Internet uses TCP/IP protocol suite, also known as the Internet suite or the Internet model. It is a four-layered architecture used by the Internet for all its communication and is independent of the underlying network architecture. This model has the following layers:

*Layer 4—application layer* This layer defines the protocol which enables the user to interact with the network, for example, FTP, HTTP, etc.

*Layer 3—transport layer* This layer defines how the data should flow between hosts. The most important protocol that operates in this layer is the transmission control protocol (TCP) which ensures that the data delivered between hosts is in order and guarantees end-to-end delivery.

*Layer 2—Internet layer* The Internet protocol (IP) works on this layer and is responsible for host addressing, recognition, and routing.

*Layer 1—link layer* This layer is responsible for sending and receiving actual data, and is independent of the underlying network architecture and hardware.

## 1.5 NETWORKING DEVICES

Networking devices are used for connecting to a network, routing the packets, strengthening the signal, communicating with others, sharing files on the network, etc. Networking devices include repeaters, hubs, bridges, switches, gateways, and modems. They are explained here:

### Repeater

A repeater is an electronic two-port device that operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. Repeaters do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it to the original strength.

### Hub

A hub is a networking device which is used to connect multiple network hosts. It is also called multipoint repeater. Hubs cannot filter data, hence data packets are sent to all connected devices. They carry out data transfer in terms of packets. When a host sends a data packet to a hub, the hub copies the data packet to all its ports. This makes it slower and more congested. Further, it does not have the intelligence to determine the best path for these data packets; this leads to inefficiencies and wastages. Hubs are of two types:

*Passive hub* It forwards the data signal from all the ports except the port on which the signal arrived. It does not interfere with the data signal.

*Active hub* It also forwards the data signal from all ports except the port on which the signal arrived. However, before forwarding, it improves the quality of the data signal by amplifying it. Due to this, an active hub is also known as a repeater.

### Bridge

A bridge connects two subnetworks (or two LANs) which are part of the same network. In other words, a bridge is used to divide a large network into smaller segments. It can join different media types (e.g., UTP with fibre

optics) as well as different types of network architecture (e.g., ethernet with token ring). It has a single input and single output port, thus making it a two-port device. A bridge operates at the data link layer. A bridge is a repeater, with capability to filter out content by reading the MAC addresses of the source and destination.

There are three types of bridges, which are as follows:

1. *Local bridge*: This bridge connects two LAN segments directly.
2. *Remote bridge*: This bridge connects another bridge over the WAN link.
3. *Wireless bridge*: This bridge connects another bridge without any wiring between them.

Limitations with bridges include limited ports and a slowdown in the overall performance of the network, as in bridge forwarding decisions are made through software.

## Switch

Switch is a data link layer device. A switch is more intelligent than a hub. While a hub does only data forwarding, a switch does ‘filtering and forwarding’. When a packet is received at one of the interfaces of the switch, it filters the packet and sends it only to the interface of the intended receiver. For this purpose, a switch maintains a content addressable memory (CAM) table and has its own system configuration and memory.

A switch can perform error checking before forwarding data and processes the frame only if it is valid. When a switch receives a frame, it checks the frame checksum sequence (FCS) field in it. All invalid frames are automatically dropped. This makes it very efficient as it does not forward frames that have errors. All valid frames are processed and forwarded to their destination MAC address.

Switches support three methods of switching which are as follows:

*Store and forward* This is the basic mode of switching where the switch buffers the entire frame into the memory and runs FCS to check if the frame is valid or not. Only valid frames are processed and all invalid frames are automatically dropped.

*Cut and through* In this method, the switch reads only the first six bytes from the frame after the preamble. These six bytes refer to the destination address of the frame. This is the fastest method of switching.

*Fragment free* This is a hybrid version of the store and forward method and cut and through method. It checks the first 64 bytes of the frame for error. It processes only those frames that have the first 64 bytes valid. Any frame less than 64 bytes is known as runt and is invalid. This method filters runt while maintaining the speed.

## Routers

A router is a device like a switch that routes data packets based on their IP addresses. It is mainly a network layer device which is responsible for routing traffic from one network to another. Routers are used to connect different network segments, network protocols, media types (e.g., UTP and fibre optic cable), network architecture, and to group smaller networks to form larger networks and to break larger networks into smaller networks, among others.

## Gateway

Gateways are also called protocol converters and can operate at the network layer. Gateways are generally more complex than switches or routers, and are used to forward the packets which are intended for the remote network from the local network. Until the host is configured with a default gateway address, every packet should have a default gateway address. A default gateway address is the address of the gateway device. If the packet does not find its destination address in the local network, it would take the help of the gateway device to find the destination address in the remote network.

## Modem

Modem stands for *modulator + demodulator*. It modulates and demodulates the signal between the digital data of a computer and the analog signal of a telephone line.

### **Box 1.2 NIC and MAC Address**

MAC address is the hardware address tied to the key connection device in the computer called the NIC. The NIC is a computer circuit card that enables a computer to connect to a network. It also facilitates conversion of data into an electrical signal that can be transmitted over the network. A MAC address is given to a network adapter when it is manufactured. It is unique and hardwired or hard-coded onto the NIC. MAC address is also called a networking hardware address, the burned-in address (BIA), or the physical address.

The MAC address is a string of usually six sets of two-digit numbers or characters, separated by colons. An example of a MAC address is '00-14-22-15-17-90' where the first three octets '00-14-22' represents an organizationally unique identifier (OUI) which is DELL in this case.

All devices on the same network subnet have different MAC addresses. These addresses are very useful in diagnosing network issues like problems with IP addresses as they are not as dynamic as IP. The MAC address remains the most reliable way to identify senders and receivers of data on the network.

## **1.6 LAN TECHNOLOGIES**

The various LAN technologies are summarized in this section.

### ***Ethernet***

Ethernet relies on shared media which has the highest probability of data collision. It uses carrier sense multi access/collision detection (CSMA/CD) technology to detect collisions. When a collision occurs in ethernet, all its hosts roll back, wait for some random amount of time, and then re-transmit the data. Ethernet connectivity is provided through a network interface card (NIC) equipped with a 48-bit medium access control (MAC) address which helps one ethernet device to identify and communicate with other remote devices over ethernet (Box 1.2).

Traditional ethernet uses a 10BASE-T specification, where the number 10 depicts speed of the order of 10Mbps, BASE stands for baseband, and T stands for thick ethernet. 10BASE-T ethernet can provide a transmission speed of upto 10Mbps and uses a coaxial cable or a Cat-5 twisted pair cable with an RJ-45 connector. An ethernet segment length can extend up to 100 metres.

### ***Fast Ethernet***

It is an extension of ethernet, and can run on optical fibre and in wireless mode with a speed of upto 100 Mbps. This standard is named 100BASE-T in IEEE 803.2 and uses Cat-5 twisted pair cable. Fast ethernet uses CSMA/CD technique while sharing the wired media among the ethernet hosts and CSMA/CA (CA stands for collision avoidance) technique for wireless ethernet LAN.

Fast ethernet on fibre is defined under the 100BASE-FX standard which provides speeds up to 100 Mbps on fibre. Ethernet over fibre can be extended upto 100 metres in half-duplex mode and can reach a maximum of 2000 metres in full-duplex over multimode fibres.

### ***Giga Ethernet***

Gigabit ethernet offers a speed of upto 1000 Mbps. IEEE802.3ab defines giga ethernet over UTP using Cat-5, Cat-5e, and Cat-6 cables. IEEE802.3ah defines giga ethernet over fibre.

### ***Virtual LAN***

LAN technology primarily relies on the ethernet which in turn works on shared media. Shared media in ethernet offers a single broadcast and a single collision domain. The introduction of switches to ethernet has resolved

the single collision domain issue and each device connected to the switch works in separate collision domains. However, switches cannot divide a network into separate broadcast domains.

Virtual LAN enables division of a single broadcast domain into multiple broadcast domains, whereby the host in one VLAN cannot speak to a host in another. By default, all hosts are placed into the same VLAN. Hosts in one VLAN, even if connected on the same switch, cannot see or speak to other hosts in different VLANs. VLAN follows Layer-2 technology which works closely on ethernet. To route packets between two different VLANs, a Layer-3 device such as a router is required.

### **Wireless Fidelity**

Wireless fidelity (Wi-Fi) is a wireless technology used in networking and communication. It is a cost-effective way to connect to the Internet and other electronic communication devices without the need for physical connection in the form of wires between them.

Wi-Fi technology offers the following advantages:

1. It allows flexible access to the Internet, file transfers, and print services, provided the electronic communication device is within a few metres of the Wi-Fi access point (AP).
2. It eliminates the need for wires, network cables, and sockets for interconnection which deteriorates over time.
3. Once a device is configured with the Wi-Fi AP, access to the Internet and the network at different locations is assured and there is no need to reconfigure the Internet settings every time.
4. It drastically reduces the IT set-up cost to offer Internet connectivity.

This technology has a few disadvantages as well, which are summarized here:

1. Any other Wi-Fi enabled electronic communication which is in close proximity to the Wi-Fi AP can make unauthorized access to the data and Internet connection unless the Wi-Fi is password-protected.
2. Since Wi-Fi networks are sensitive to signal strength, the electronic communication devices connected to it should have good signal strength at all times to ensure good connectivity.
3. Wi-Fi signals are sensitive to climatic conditions which make it less suitable during adverse weather conditions, for example, thunderstorms.

## **1.7 NETWORKING TOPOLOGIES**

Network topology reflects the interconnection between computer systems and the networking devices in a network. Topology may define both the physical and logical aspect of the network, and both logical and physical topologies could be the same or different within the same network. The various network topologies are summarized here and shown in Fig. 1.4. See also Box 1.3.

### **Point-to-Point**

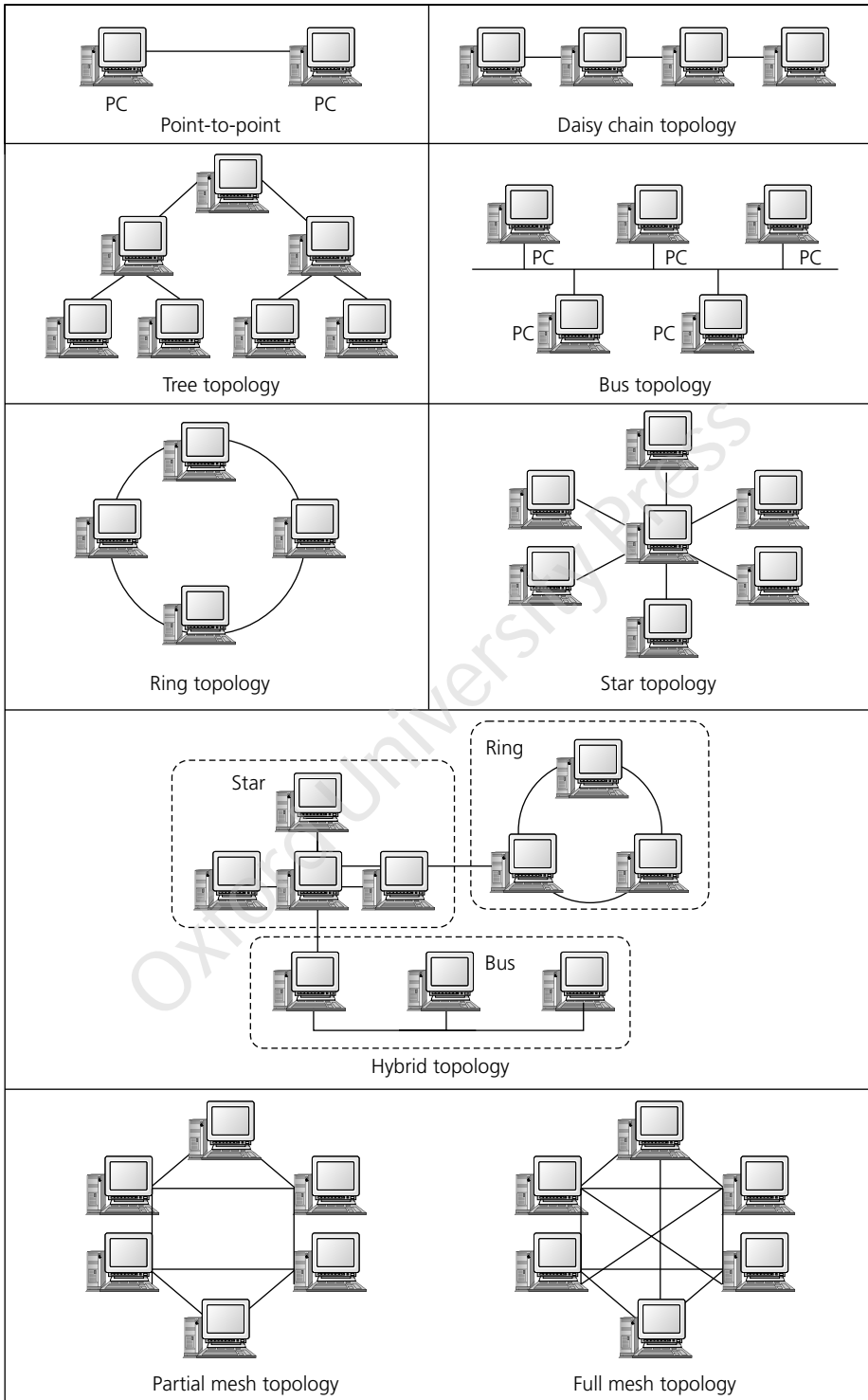
Point-to-point networks contain exactly two hosts which may be a computer, switches, or routers and servers connected back-to-back using a single piece of cable.

In a logical point-to-point connection between the hosts, there may be multiple intermediate devices. However, the end hosts perceive each other as if they are directly connected and are unaware of the underlying network.

### **Bus Topology**

In the case of bus topology, all devices share a single communication line or cable. The data is sent in the form of electronic signals to all the computers on the network, but is received only by the host whose address matches the address encoded in the signal. Both ends of the shared channel have a line terminator. The data is sent in only one direction and as soon as it reaches the other end, the terminator removes the data from the line.

In bus topology, only one host can send information at any point of time which inhibits network performance by slowdown and is proportional to the number of computers connected to the bus.



**Fig. 1.4** Various LAN topologies



### Box 1.3 WAN and the Internet

Most WANs are connected by means of dual-ring topology and the networks connected to them are mostly star topology networks. The Internet is the best example of the largest hybrid topology.

The advantage with bus topology is that it is simple, cheap, and easy to set up. The failure of one device does not affect other devices. The drawback with bus topology is that in the event of excess network traffic, multiple users may get affected and the network becomes difficult to troubleshoot. Further, in bus topology, problems arise while multiple hosts attempt to send data at the same time. In such a situation, the bus topology either uses CSMA/CD technology or designates one host as the bus master to solve the issue. It should also be noted that failure of the shared communication line can make all other devices stop functioning.

#### Star Topology

In star topology, all the hosts are connected to a central device known as hub device using a point-to-point connection. The hub device can be a Layer-1 device such as hub (passive hub) or a repeater (active hub), a Layer-2 device such as switch or bridge, or a Layer-3 device such as router or gateway.

An active hub regenerates and retransmits the signal just as repeaters do. They require electrical power to run. On the contrary, passive hubs act as mere connection points and do not amplify or regenerate the signal. It does not require electric power to run.

The advantage with star topology is that it is inexpensive to set up, easy to modify, and its configuration is simple. It facilitates centralized monitoring. The disadvantage is that just as in bus topology, the hub acts as a single point of failure where the failure of the hub leads to failure in the connectivity among all the hosts.

#### Ring Topology

In ring topology, every host is connected to exactly two other hosts, thus creating a circular network structure. When a host sends a message to another host not adjacent to it, the data travels through all the intermediate hosts. Connecting a new host to the existing structure requires an extra cable. This topology is in use in token ring networks.

The advantage of this topology is that it offers equal access privilege to any host. The disadvantage is that the failure of any host results in the failure of the whole ring. Thus, every connection in the ring is a point of failure. However, employing another backup ring would resolve this issue.

#### Mesh Topology

In mesh topology, a host is connected to one or more hosts by a point-to-point connection. Hosts in mesh topology act as a relay node for other hosts which do not have direct point-to-point links. In most cases, every host is connected with every other host by a point-to-point connection.

Mesh technology is of two types:

**Full mesh** All hosts have a point-to-point connection to every other host in the network. Thus for every new host  $n(n - 1)/2$  connections are required. It provides the most reliable network structure among all the network topologies.

**Partial mesh** Not all hosts have a point-to-point connection to every other host. Hosts are connected to each other in some arbitrary fashion. This topology is suitable when only some nodes need to be reliable, and not necessarily the others.

#### Tree Topology

This is the most common network topology presently in use and is also called hierarchical topology. It imitates an extended star topology and inherits the properties of bus topology.

This topology divides the network into multiple levels/layers of network. The lowermost is the access layer where the computers are attached. The middle layer is known as the distribution layer, which works as the mediator between the upper layer and lower layer. The highest layer is known as the core layer, and is the central point of the network, that is, root of the tree from where all nodes fork. There is point-to-point connection between neighbouring hosts.

The drawback with this topology is the same as bus topology—if the root goes down, the entire network suffers even though it is not the single point of failure. Every connection serves as a point of failure and may lead to division of network into the unreachable segment.

### **Daisy Chain Topology**

In this topology all the hosts are connected in a linear fashion. It is similar to ring topology where all the hosts are connected to only two hosts, except the end hosts. Every intermediate host works as a relay for its immediate hosts.

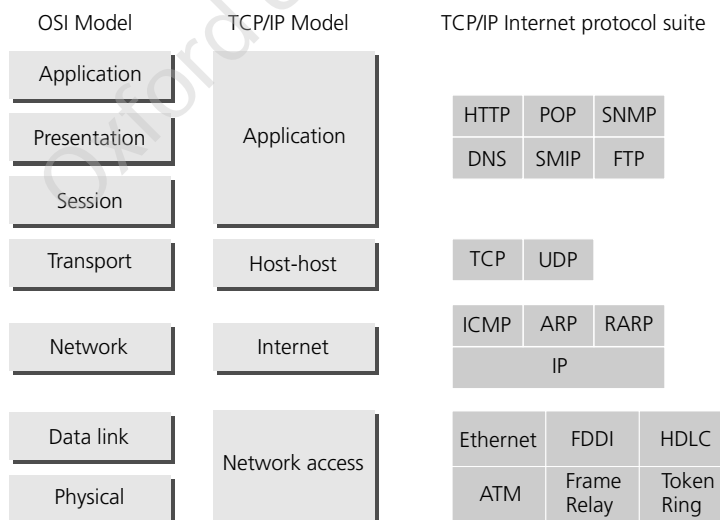
The drawback with this topology is that each link in the daisy chain topology represents a single point of failure and any link failure, therefore, will split the network into two segments.

### **Hybrid Topology**

Hybrid topology integrates more than one topology and inherits the merits and demerits of all the incorporating topologies. The combining topologies may contain attributes of star, ring, bus, and daisy chain topologies.

## **1.8 NETWORK PROTOCOLS—TCP/IP PROTOCOL SUITE**

Network protocol is a set of rules that govern communications between devices connected on a network. It includes mechanisms for establishing connections as well as formatting rules for data packaging and wrapping for every message exchanged over the network. TCP and IP are the two computer network protocols used in all operating systems of networked devices which operate in Layer-4 and Layer-3 of the OSI respectively. The various other protocols used in every layer are shown in Fig. 1.5.



**Fig. 1.5** TCP/IP protocol suite

The following sections briefly highlight the importance of every layer in the OSI model and the protocol attached to it, and as part of the TCP/IP protocol suite, briefly.

## 1.9 PHYSICAL LAYER

The physical layer deals with physical connectivity between any two hosts. It defines the hardware equipment, cabling, wiring, frequencies, and pulses used to represent binary signals, etc. Interaction with hardware and signalling are taken care of by the physical layer. Besides this, it offers services to the data link layer as it receives frames from it. The physical layer converts it into electrical pulses which represent binary data that is sent over either wired or wireless media.

### **Transmission Media**

The transmission media over which data is exchanged between any two hosts may be either guided or unguided.

1. In *guided media*, the sender and the receiver are directly connected with wires and cables such as unshielded twisted pair (UTP) cable, coaxial cables, and fibre optics, and the information is exchanged or guided through it.
  - (a) A twisted pair cable is made of two plastic insulated copper wires twisted together to form a single media of which one carries the actual signal and the other is used for ground reference. The twists between wires reduce noise due to electro-magnetic interference and crosstalk. Twisted pair cables may be either shielded twisted pair (STP) cable or unshielded twisted pair (UTP) cable. STP cables come with a twisted wire pair covered in metal foil which makes it more indifferent to noise and crosstalk. There are seven categories of UTP, each suitable for a specific use. In computer networks, Cat-5, Cat-5e, and Cat-6 cables are most widely used. UTP cables are connected by RJ45 connectors.
  - (b) A coaxial cable has two wires of copper. The core wire at the centre is made of solid conductor and is enclosed in an insulating sheath. The second wire is wrapped around the sheath which in turn is encased by an insulator sheath. Both are covered by plastic. This makes it suitable for carrying high-frequency signals, compared to twisted pair cables. It also provides a good shield against noise and crosstalk. Coaxial cables can support a bandwidth of up to 450 Mbps. There are three categories of coaxial cables: RG-59 (cable TV), RG-58 (thin ethernet), and RG-11 (thick ethernet) where RG stands for radio government. Cables are connected using a BNC connector and BNC-T. BNC terminator is used to terminate the wire at the far ends.
  - (c) Fibre optic cable has a core made of high-quality glass or plastic. From one end, light is emitted, it travels through it, and at the other end a light detector detects the light stream and converts it to electric data. Thus fibre optics offers the highest speed. Fibre optics come in two modes, namely single mode fibre and multimode fibre. Single mode fibre can carry a single ray of light, whereas multimode is capable of carrying multiple beams of light.
2. *Unguided media* refers to wireless or open air space wherein there is no physical connectivity between the sender and the receiver and the information is exchanged over air. Hence, anyone can intercept the actual communication and collect the information.

### **Channel Capacity**

Channel capacity determines the speed of transmission of information and depends on factors such as *bandwidth* (which corresponds to the physical limitation of the underlying media), *error rate* (which is directly proportional to the noise in the channel, thus inhibiting the exact reception of information), and the *encoding mechanism* used which influences the number of levels used for signalling.

### **Multiplexing**

Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. A multiplexer (MUX) refers to hardware that mixes multiple data streams and sends them over a single medium. A de-multiplexer (DMUX) takes information from the medium and distributes them to different destinations.

## Switching

Switching is a mechanism by which data or information is sent from the source towards destinations that are not directly connected, but through interconnecting devices between them. Such interconnecting devices in the network receive data from the directly connected source, stores and analyses it, and then forwards it to the next interconnecting device closest to the destination.

Switching is categorized into three types: circuit switching, message switching, and packet switching.

**Circuit switching** The two nodes involved in communication establish a dedicated communication path (circuit) through which data will travel and no other data is transferred over that path. Circuits can be permanent or temporary. Once data transfer is completed, the circuit is disconnected. Circuit switching is best used by telephone networks.

**Message switching** Every switch in the transit path receives the whole message and buffers it until resources are available in the next hop node to transmit it. Hence every switch needs enough storage to accommodate the entire message. The store-and-forward and the wait-until-resources-are-available techniques make the process of message switching very slow. Moreover, it is not suitable for streaming media and real-time applications.

**Packet switching** The entire message is broken down into smaller chunks called packets wherein the switching information is added to the header of each packet and the packets are transmitted independently. The small size of packets, as opposed to message switching, makes it easy for intermediate networking devices to store them as they do not take up much resource, either on the carrier path or in the internal memory of switches. Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The Internet uses the packet switching technique.

## 1.10 DATA LINK LAYER

The data link layer, the second layer of the OSI layered model, hides the details of the underlying hardware and represents itself to the upper layer as the medium to communicate.

This layer converts the data stream into signals bit by bit and sends them over the underlying hardware. At the receiving end, the data link layer picks up data from the hardware, which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to the upper layer.

The data link layer has two sub-layers:

1. *Logical link control* deals with protocols, flow-control, and error control.
2. *Media access control* deals with the actual control of media.

### 1.10.1 Functions

The functions of the data link layer are as follows:

**Framing** The data link layer receives packets from the network layer and encapsulates them into frames. Then every frame is sent bit-by-bit on the hardware. At the receiver's end, the data link layer picks up signals from the hardware and assembles them into frames.

**Addressing** The data link layer deals with a Layer-2 hardware addressing mechanism which is encoded into the hardware at the time of manufacturing and is unique on the link.

**Synchronization** When data frames are sent on the link, both the sender and the receiver must be synchronized so as to guarantee correct transfer.

**Error control** Data during transmission is prone to errors which may be single-bit, multiple-bit, or burst errors due to noise, crosstalk, etc., and the bits are flipped. Error control attempts to detect such errors and recover actual data bits. The error is reported to the sender as well.

**Flow control** The data link layer ensures flow control so that both the sender and the receiver (which otherwise may have different speeds or capacities) exchange data at the same speed. Flow control minimizes loss of data due to synchronization.

**Multi-access** The data link layer resolves collisions that arise while accessing shared media with a mechanism like CSMA/CD.

### 1.10.2 Error Control

The data link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with a certain level of accuracy. Error control involves *error detection* and *error correction*.

Error detection is based on parity check or cyclic redundancy check.

Error detection can be carried out with *parity check* wherein one extra bit is sent along with the original data bits to mark whether the number of 1s is even (in the case of even parity) or odd (in the case of odd parity). The receiver at the other end checks for the said parity and can detect single-bit flips in transit. However, this tends to get tedious when more than one bit is erroneous.

In *cyclic redundancy check* (CRC) attempts are made to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits to be sent to the receiver and calculates the remainder. The sender adds the remainder at the end of the actual bits. The actual data bits plus the remainder is called a *codeword*. The sender transmits the data bits as codewords. At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros then the data bits are free from errors and are accepted. Otherwise it is obvious that some data has been corrupted in transit.

There are two types of error correction mechanisms: backward error correction and forward error correction.

**Backward error correction** The receiver detects an error in the data received and requests the sender to retransmit the data. This sort of error correction is used in a fibre optics medium as retransmission is cheaper.

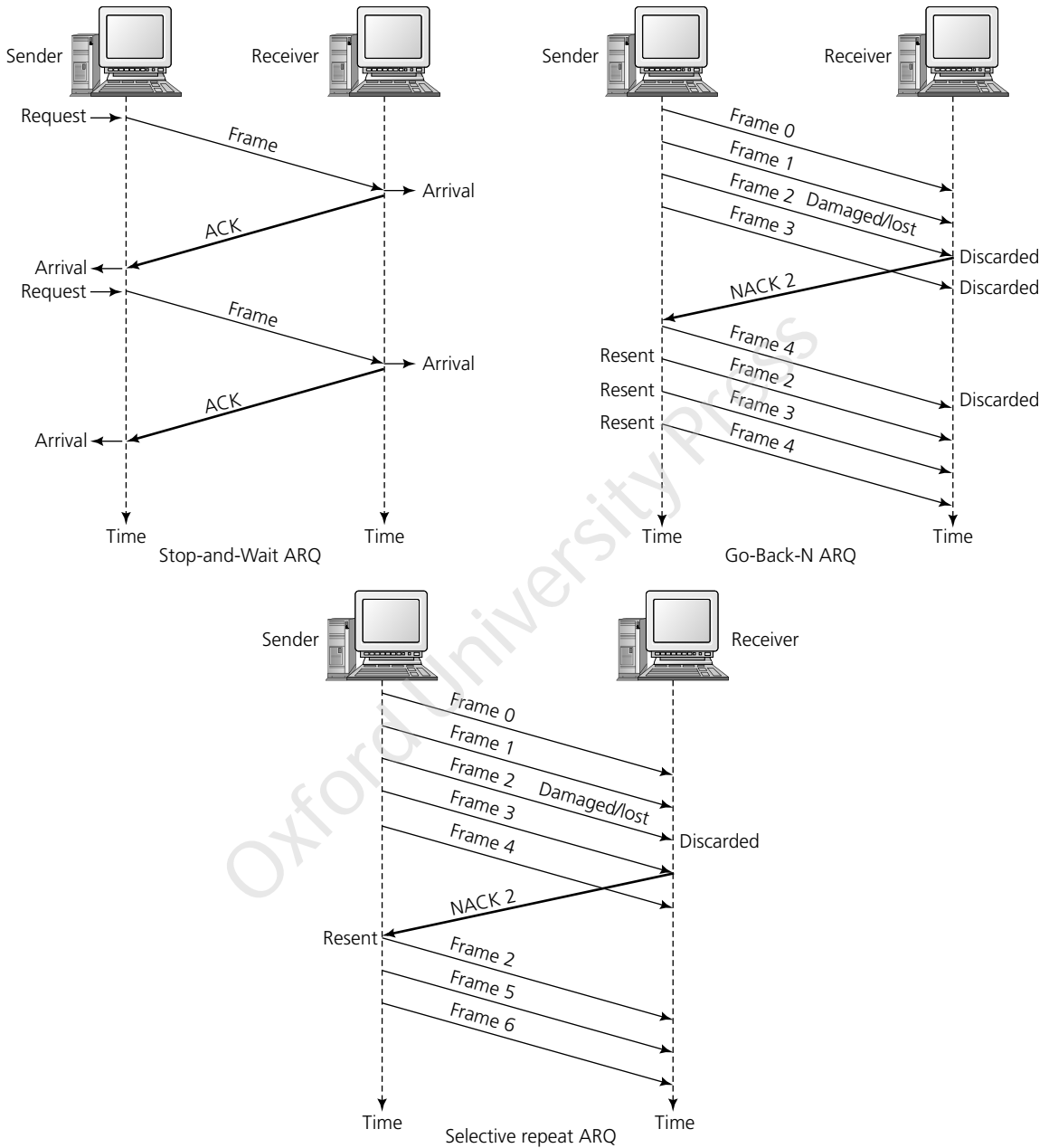
**Forward error correction** When the receiver discovers an error in the received data, it executes error-correcting code to correct and auto-recover from errors in the data. This sort of error correction is used in wireless medium as retransmission is expensive.

To handle error control, the sender or the receiver should ascertain that there are errors during transit. The sender maintains a clock upon transmitting a data frame and expects an acknowledgement before the timer expires or a timeout has occurred. Failure to receive the acknowledgement necessitates the sender to retransmit the frame. The receiver sends a positive acknowledgement (ACK) upon receiving a correct data frame or a frame without errors and a negative acknowledgement (NACK) if either the frame has been lost during transit or has been received with errors. The three error control mechanisms or protocols are (a) stop-and-wait with automatic repeat request (ARQ), (b) go-back-N ARQ, and (c) selective repeat ARQ, and are shown in Fig. 1.6.

**Stop-and-wait ARQ** The sender, after transmitting a data frame, starts a timer and transmits the next frame if an acknowledgement is received before the timer expires. In the event of non-receipt of an acknowledgement, the sender retransmits the frame and resets the timer. The sender immediately retransmits the data frame in case a negative acknowledgement is received. However, stop-and-wait ARQ results in poor utilization of resources.

**Go-Back-N-ARQ** The sender and the receiver agree upon a window and this enables the sender to send multiple data frames rather than wait for acknowledgements for every data frame. This also enables the receiver to send acknowledgements for multiple frames rather than individual frames while keeping track of the sequence number of the frame. The sender, before initiating the next transmission, checks the sequence number of the frames that have received a positive acknowledgement. If all the frames have received a positive acknowledgement, the sender transmits the next set of frames. Otherwise, the sender retransmits those frames for which either a negative acknowledgement is received or an acknowledgement has not been received. However, Go-

Back-N-ARQ assumes that there is no buffer with the receiver and so a frame has to be processed as received and retransmitted in case of a negative acknowledgment.



**Fig. 1.6** Error control mechanisms in data link layer

**Selective repeat ARQ** The receiver buffers up the frame, tracks the sequence number of the frames, and sends NACK to those frames which are missing or damaged. This makes the sender retransmit only those frames for which a NACK is received.

### 1.10.3 Flow Control

When a frame is sent from one host (sender) to the other (receiver), it is necessary that they are synchronized and work at the same speed. Otherwise, it would cause the receiver to be overloaded and swamped resulting in data loss if the sender sends data frames too fast. The two popular flow control mechanisms are (a) stop and wait, and (b) sliding window.

**Stop and wait** This flow control mechanism forces the sender to stop transmitting a data frame and wait until an acknowledgement for the previously sent data frame is received.

**Sliding window** This flow control mechanism eliminates the problem of resource under utilization experienced with stop and wait protocol. In this mechanism, both the sender and the receiver agree on the number of data frames after which an acknowledgement has to be sent just before the initiation of every data transfer from the sender.

## 1.11 NETWORK LAYER

The network layer is responsible for routing packets from the source to the destination either within or outside a subnet irrespective of different, non-compatible addressing schemes and protocols.

The primary function of this layer is routing and it involves the following sub-tasks:

1. Addressing networking devices and the network as well as the internetworking of two different subnets
2. Maintaining the routing table and populating it
3. Queuing up incoming packets and forwarding them to devices or nodes closest to the destination without violating the quality-of-service (QoS)
4. Best effort in the delivery of packets to the destination

Besides this, the network layer is responsible for managing QoS and the link, load balancing, security, handling of different protocols and subnets, and end-to-end connectivity with VPN and tunnels.

The protocol that operates in the network layer is the Internet protocol (either IPv4 or IPv6) which is responsible for end-to-end communication between devices over the Internet.

### 1.11.1 Network Addressing

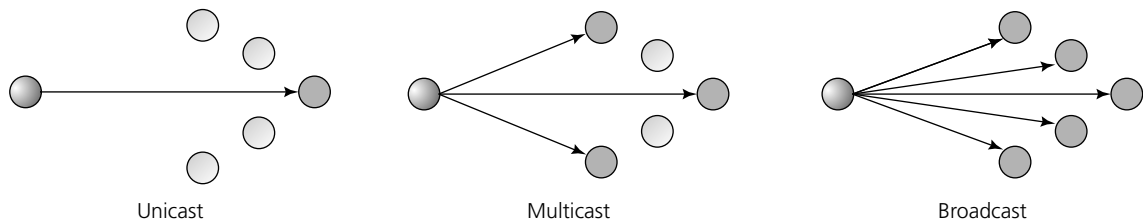
Every node/host in the network is uniquely identified with an IP address. This is the network address and is configured on the NIC. This address is mapped to the MAC address of the machine for Layer-2 communication. The network address is always logical in meaning; it is a software-based address and so can be changed by appropriate configurations.

Since IP addresses are assigned hierarchically, a host always resides under a specific network. The sending host can send a packet to the destination host, either inside or outside its subnet, provided it knows the destination network address. Hosts in different subnets can locate each other with the domain naming server (DNS), which is a server that maps the Layer-3 address of the remote host with its domain name. When such a host acquires the Layer-3 address (IP address) of the remote host, it forwards all its packets to its gateway. A gateway is a router equipped with routing tables to route packets to the destination host such that every packet gets forwarded to its next hop (adjacent router) towards the destination.

### 1.11.2 Routing in Network Layer

Routing is the process of selecting one among the multiple paths to reach a destination from the routing table and is performed by the network device, router. The decision to select a specific route is based on hop count, bandwidth, delay, prefix length, etc. Routing can also be performed with software but is limited in functionality and scope. Routes are configured in a router either statically or learnt dynamically. Every router has a default route which reveals where to forward a packet if no appropriate route to the specific destination is found in the routing table.

Routing can be unicast, multicast, anycast, and broadcast, as shown in Fig. 1.7.



**Fig. 1.7** Unicast, multicast, and broadcast communication

### Unicast Routing

Routing unicast data (from a specific known destination) over the Internet is called unicast routing. This necessitates the router to look up the routing table and forward the packet to the next hop.

The routing protocols for unicast routing can be distance vector routing protocol or link state routing protocol.

**Distance vector routing protocol** The distance vector routing (DVR) protocol performs routing by taking into consideration a route with fewer hops between the source and the destination as the best route. Every router advertises its set best routes to other routers. Ultimately, all routers build their network topology based on the advertisements of their peer routers. The best example for DVR is routing information protocol (RIP). DVR is simple to implement.

**Link state routing protocol** The link state routing (LSR) protocol considers the states of links of all the routers in a network to build a graph of the entire network. The best path for routing is then calculated by all routers. Examples for LSR include open shortest path first (OSPF) and intermediate system to intermediate system (ISIS).

### Broadcast Routing

Routing packets to every host and devices in the network is known as broadcast routing. This is done in one of the following two ways:

1. The router creates multiple copies of a single data packet with different destination addresses. All packets are sent as unicast to simulate router broadcasting. Since multiple unicast transfers are involved, it leads to larger consumption of bandwidth.
2. Second, when the router receives a packet that is to be broadcasted, it simply floods those packets out in all its interfaces.

### Multicast Routing

Multicast routing is a special case of broadcast routing where the data packets are only sent to nodes which want to receive the packets as against broadcast routing, where the packets are sent to all nodes irrespective of whether they want them or not.

Multicast routing protocols build a tree rather than a graph with unicast routing protocols. They construct a minimum spanning tree so as to avoid loops. Example of multicast routing protocols include distance vector multicast routing protocol (DVMRP), multicast open shortest path first (MOSPF), protocol independent multicast (PIM), etc. PIM may be either *PIM dense mode* which uses source-based trees that are suitable for a dense environment like LAN or *PIM sparse mode* that uses shared trees and is suitable for a sparse environment like WAN.

### Anycast Routing

Anycast packet forwarding is a mechanism where multiple hosts can have the same logical address. When a packet destined to this logical address is received, it is sent to the host which is nearest in the routing topology.



Anycast routing is done with the help of a DNS server which upon receiving a packet, destines it to the nearest IP address configured on it. Whenever an anycast packet is received, it enquires with DNS about where to send it. DNS provides the IP address which is the nearest IP configured on it.

## Routing Algorithms

Routing algorithms may be based on either flooding or shortest path.

**Flooding** It is the simplest method of packet forwarding. When a packet reaches a router, it is forwarded through all the interfaces except the one through which it was received. Flooding results in lots of duplicate packets wandering in the network which later burdens the network. Every packet possesses time to live (TTL) which determines the lifetime of the packet and eliminates infinite looping of packets. Another variant of flooding is selective flooding wherein the router does not flood out on all the interfaces, but on selective ones which greatly reduces the network overhead.

**Shortest path** It performs routing decisions on the basis of cost between source and destination and considers a path in the network with minimum number of hops towards the destination to forward a packet until it reaches the destination.

## Internetworking

Routing between two networks, either of the same kind or different kind, scattered geographically is called internetworking. Routers have each other's addresses and are either statically configured or learnt dynamically through the internetworking protocol. Routing protocols used within an organization are called interior gateway protocols (IGP). RIP and OSPF are examples of IGP. Routing between different organizations is called exterior gateway protocol (EGP). An example of EGP is the border gateway protocol (BGP).

Any two geographically separate networks that want to communicate with each other may deploy either a dedicated line between them or pass their data through intermediate networks. *Tunneling* is a mechanism by which two such networks communicate with each other, by passing intermediate networking complexities. Tunneling is configured at both ends. When the data enters from one end of the tunnel, it is tagged. This tagged data is then routed inside the intermediate or transit network to reach the other end of the tunnel. When data exits the tunnel, its tag is removed and delivered to the other part of the network. Tunneling gives the illusion that both the ends are directly connected. Tagging ensures data travel through the transit network without any modifications.

Internetworking refers to routing between different kinds of networks. Different networks are capable of handling data of different sizes. Most ethernet segments have their maximum transmission unit (MTU) fixed at 1500 bytes. Devices in the transit path have varying hardware and software capabilities which influence the amount of data that the device can handle and the size of packet it can process.

If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally. If the packet is larger, it is broken into smaller pieces and then forwarded. This is called *packet fragmentation*. Each fragment contains the same destination and source address and is routed through the transit path. At the receiving end, it is assembled again.

If a packet with a don't fragment (DF) bit set to 1 arrives at a router, and if it cannot handle the packet because of its length, the packet is dropped. Similarly when a packet that arrives at a router has its more fragment (MF) bit set to 1, the router knows that it is a fragmented packet and parts of the original packet are on the way.

## 1.12 NETWORK LAYER PROTOCOLS

Every computer in a network has an IP address with which it can be uniquely identified and addressed. An IP address (Layer-3 address) is a logical address which may change every time a computer restarts. A computer can have one IP at one instant of time and another IP at a different time. Communication with the destination host requires its MAC address (Layer-2 address) as well, which is physically burnt into its NIC and never changes.

Four protocols operate at the network layer: address resolution protocol (ARP), reverse address resolution protocol (RARP), Internet control message protocol (ICMP), and the Internet protocol (IP). IP is available in two variants, namely IPv4 and IPv6.

### 1.12.1 Address Resolution Protocol and Reverse Address Resolution Protocol

To initiate a communication, the source should know the MAC address of the remote host on a broadcast domain. It sends out an address resolution protocol (ARP) broadcast message asking, 'Who has this IP address?' An ARP packet contains the IP address of the destination host with which the source wishes to communicate. Because it is a broadcast message, all hosts on the network segment (broadcast domain) receive this packet and process it. When a host receives an ARP packet destined to it, it replies with its own MAC address so that the host can communicate with the remote host using Layer-2 link protocol. This MAC-to-IP mapping is saved in the ARP cache of both the sending and receiving hosts for future reference during communication.

Reverse address resolution protocol (RARP) is a mechanism wherein a host that knows the MAC address of the remote host gets to know the IP address of the remote host so as to communicate. ARP and RARP are shown in Fig. 1.8.

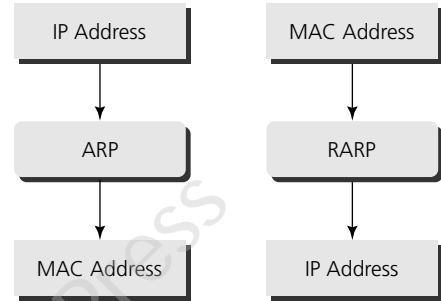


Fig. 1.8 Address resolution protocol (ARP) and reverse address resolution protocol (RARP)

### 1.12.2 Internet Control Message Protocol

Since IP does not have an inbuilt mechanism for sending error and control messages, it depends on the Internet control message protocol (ICMP), a network diagnostic and error reporting protocol. ICMP belongs to the IP protocol suite and uses IP as its carrier protocol. After constructing the ICMP packet, it is encapsulated in the IP packet.

ICMP contains dozens of diagnostic and error reporting messages. Any feedback about network as well as error in the network is sent back to the originating host. Some of the ICMP messages include the following:

**Source quench message** When the rate at which packets (traffic rate) sent by the source is very fast, the packets get dropped ultimately. When a receiving host or the router detects this, ICMP will take the source IP from the discarded packet and inform the source by sending a source quench message. As a result, ICMP slows down the pace so that no packet is lost.

**Parameter problem** Whenever packets come to the router, its header checksum calculated earlier should be equal to the received header checksum for the packet to be accepted by the router. In case of mismatch, the packet is dropped by the router. ICMP will take the source IP from the discarded packet and inform the source by sending a parameter problem message.

**Time exceeded message** When some fragments are lost in a network, the fragment held by the router will be dropped. ICMP will take the source IP from the discarded packet and inform the source by sending a time exceeded message stating that the TTL field has reached zero.

**Destination unreachable** A destination host in the network may become unreachable during any failure in the link, hardware, or port. This is informed to the source with ICMP messages. ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts.

### 1.12.3 Internet Protocol Version 4

Internet protocol version 4 (IPv4) is the fourth revision of IP and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks like ethernet, and can be configured either manually or automatically depending on the network type.

IPv4 is based on the best-effort model which means it guarantees neither delivery nor avoidance of duplicate delivery. These are handled by the upper layer transport.

IPv4 is a 32-bit numeric address that is written in decimal as four numbers separated by dots. This addressing scheme is used as a TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides a hierarchical addressing scheme which enables the network to be divided into sub-networks, each with a well-defined number of hosts. IP addresses are divided into many categories:

**Class A** It uses the first octet for network addresses and the last three octets for host addressing.

**Class B** It uses the first two octets for network addresses and the last two for host addressing.

**Class C** It uses the first three octets for network addresses and the last one for host addressing.

**Class D** It is reserved for multicasting.

**Class E** It is reserved for future use.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on the Internet) and public addresses (provided by ISPs and routable on the Internet).

### 1.12.4 Internet Protocol Version 6

Internet protocol version 6 (IPv6) was developed to fulfil the need for more Internet addresses as the IPv4 address space was exhausted. IPv6 is also called Internet protocol next generation (IPng). IPv6 addresses are 128-bit wide and are written in hexadecimal separated by colon.

IPv6 has introduced anycast addressing but has removed the concept of broadcasting. It enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of dynamic host configuration protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

IPv6 provides a new feature—that of IPv6 mobility. Mobile IPv6-equipped machines can roam around without the need for changing their IP addresses. Table 1.1 presents the differences between IPv4 and IPv6.

**Table 1.1** Differences between IPv4 and IPv6

Characteristics	IPv4	IPv6
Number of bits in IP address	32	128
Format	Decimal	Hexadecimal
Address space	4.3 billion	Infinite
IPSec support	Optional	Inbuilt
Fragmentation	By routers and intermediate hosts	By sender
Support for mobile networks	Minimum support for mobile networks	Best compatibility with mobile networks
Payloads	Less	Supports bigger payloads

### 1.13 TRANSPORT LAYER

Transport layer is responsible for end-to-end connection between two processes on remote hosts. It takes data from the upper layer (application layer), breaks it into smaller-sized segments, numbers each byte, and hands it over to the lower layer (network layer) for delivery. Thus the functions of the transport layer include breaking down of data into segments, numbering of bytes in the segments, ensuring sequence during the receipt of data, and ensuring end-to-end data delivery. End-to-end communication is achieved when a host identifies its peer

host through specified and agreed-upon ports called *transport service access points* (TSAPs) identified by port numbers. For example, a DHCP client communicates with a remote DHCP server on port number 67. A DNS client communicates with a remote DNS server on port number 53 (UDP). Port numbers range from 0–65535 where system ports correspond to (0–1023), user ports correspond to (1024–49151), and private/dynamic ports correspond to (49152–65535).

The two main transport layer protocols are TCP which provides reliable communication between two hosts and user datagram protocol which provides unreliable communication between two hosts, of which TCP is widely used in communication networks like the Internet.

### 1.13.1 Transmission Control Protocol

TCP is a transport layer protocol used by applications that require guaranteed delivery. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number. The byte stream is transferred in segments. It is a sliding window protocol that provides handling for both timeouts and retransmissions. The window size determines the number of bytes of data that can be sent before an acknowledgement from the receiver is necessary.

#### Characteristics

The following are the characteristic features of TCP:

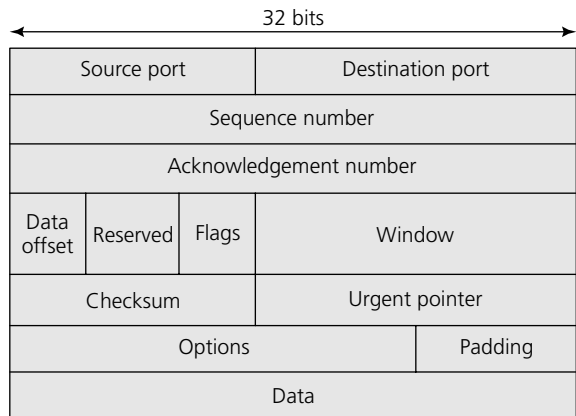
1. It is a connection-oriented protocol which means that the connection is established between two end points (between the host and the remote host) before the actual transmission of data.
2. It is a reliable protocol which means that for every data packet sent from the sender, an acknowledgement, either positive or negative, is received from the receiver. Positive acknowledgement marks the successful delivery of a data packet, whereas negative acknowledgement necessitates retransmission of the packet by the sender.
3. It operates in point-to-point client/server mode.
4. It ensures the ordering of data sent from the sender to the receiver.
5. It guarantees end-to-end communication.
6. Besides this, TCP provides flow control, error checking, and a recovery mechanism, ensuring QoS.
7. It supports full duplex server which means that it can perform the roles of both the sender and the receiver.

#### TCP Header

A TCP header and the segment format are shown in Fig. 1.9. The length of a TCP header ranges from a minimum of 20 bytes to a maximum of 60 bytes. The fields and its purpose are mentioned here:

1. Source port (16-bits): It identifies the source port of the application process at the sender's end.
2. Destination port (16-bits): It identifies the destination port of the application process on the receiving device at the receiver's end.
3. Sequence number (32-bits): It reveals the sequence number of data bytes of a segment in a session.
4. Acknowledgement number (32-bits): When ACK flag is set, this number contains the next sequence number of the data byte expected by the receiver and serves as an acknowledgement of the previous data byte received.
5. Data offset (4-bits): This field implies both, the size of the TCP header (as a number of 32-bit words) and the offset of data in the current packet in the whole TCP segment.
6. Reserved (3-bits): Reserved for future use and all are set zero by default.
7. Flags (1-bit each)
  - (a) NS: Nonce sum bit is used by an explicit congestion notification signalling process.
  - (b) CWR: When a host receives a packet with an ECE (explicit congestion notification -echo) bit set, it sets the congestion windows reduced to acknowledge that the ECE has been received.
  - (c) ECE: It has two meanings:

1. If SYN bit is cleared to 0, then ECE means that the IP packet has its congestion experience (CE) bit set.
  2. If SYN bit is set to 1, ECE means that the device is ECT capable; ECT denotes ECN capable transport.
- (d) URG: It indicates that the urgent pointer field has significant data and should be processed.
- (e) ACK: It indicates that the acknowledgement field has significance. If ACK is cleared to 0, it indicates that the packet does not contain any acknowledgement.
- (f) PSH: When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
- (g) RST: Reset flag has the following features:
1. It is used to refuse an incoming connection.
  2. It is used to reject a segment.
  3. It is used to restart a connection.
- (h) SYN: This flag is used to set up a connection between hosts and synchronize the sequence numbers.
- (i) FIN: This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in the correct order.
8. Windows size (16 bits): This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, that is, how much data the receiver is expecting.
9. Checksum (16 bits): This field contains the checksum of header, data, and pseudo headers.
10. Urgent pointer (16 bits): It points to the urgent data byte if URG flag is set to 1.
11. Options: It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32 bits, padding is used to cover the remaining bits to reach the 32-bit boundary.



**Fig. 1.9** Structure of TCP header and data

### Connection Management by TCP

TCP communication works on a server–client model. Three-way handshaking is used for connection management. This is explained here.

1. The client initiates the connection and sends the segment with a sequence number. The server either accepts or rejects it.
2. The server acknowledges it with its own sequence number and ACK of the client's segment which is one more than the client's sequence number.
3. The client, after receiving the ACK of its segment, sends an acknowledgement of the server's response.
4. To terminate a connection, either the server or the client sends a TCP segment with FIN flag set to 1. When the receiving end responds by ACKnowledging FIN, the connection is said to have been closed and released.

### Bandwidth Management by TCP

TCP uses the concept of window size to manage bandwidth. Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive. TCP uses slow start phase by using window size 1 and increases the window size exponentially after each positive acknowledgement and successful communication.

If an acknowledgement is missed, that is, data is lost in transit network or NACK is received, the window size is reduced to half and slow start phase begins again.

### **Error Control and Flow Control in TCP**

TCP uses port numbers to locate the application process it needs to hand over the data segment and sequence numbers to synchronize itself with the remote host. The sender and the receiver keep track of the sequence numbers and know what the last data segment received and sent respectively were.

If the sequence number of a segment recently received does not match the sequence number that the receiver was expecting, it is discarded and the NACK is sent back. If two segments arrive with the same sequence number, the TCP compares the timestamp value to make a decision.

### **Congestion Control in TCP**

When a large amount of data is fed to a system not capable of handling it, congestion occurs. TCP controls congestion by means of window mechanism. TCP sets a window size telling the other end how much data segment it can send. TCP uses three algorithms for congestion control:

#### **Slow start, exponential increase**

1. This algorithm is based on the idea that the size of the congestion window (cwnd) starts with one maximum segment size (MSS).
2. The size of the window increases by one MSS each time an acknowledgment is received.
3. As the name implies, the window starts slowly, but grows exponentially.
4. Slow start cannot continue indefinitely. There must be a threshold to stop this phase. The sender keeps track of a variable named slow-start threshold (ssthresh), usually 65,535 bytes, to stop this phase.
5. When the size of the window in bytes reaches this threshold, slow start stops and the next phase begins.

#### **Congestion avoidance, additive increase**

1. Slow-start algorithm increases the size of the congestion window exponentially, which should then be slowed down to avoid congestion.
2. When the size of the congestion window reaches the slow-start threshold, the slow-start phase stops and the additive phase begins.
3. In congestion avoidance algorithm, each time the whole window of segments is acknowledged (one round), the size of the congestion window is increased by 1.

#### **Congestion detection, multiplicative decrease**

1. If congestion occurs, the congestion window size must be decreased. The only way for the sender to sense congestion is with retransmission. However, retransmission can occur in one of the two cases: when a timer times out or when three ACKs are received. If congestion is detected to be due to time-out, TCP starts a new slow-start phase. If detection is by three ACKs, it starts a new congestion avoidance phase. However, in both the cases, the size of the threshold is dropped to one-half, a multiplicative decrease.

### **Timer Management by TCP**

TCP uses different types of timers to control and manage various tasks. The timers are listed here:

#### **Keep-alive timer**

1. This timer is used to check the integrity and validity of a connection.
2. When keep-alive time expires, the host sends a probe to check if the connection still exists.

#### **Retransmission timer**

1. This timer maintains a stateful session of the data sent.

2. If the acknowledgement of sent data is not received within the retransmission time, the data segment is sent again.

### **Persist timer**

1. A TCP session can be paused by either host by sending window size 0.
2. To resume the session, a host needs to send a window size with some larger value.
3. If this segment never reaches the other end, both ends may wait for each other for infinite time.
4. When the persist timer expires, the host re-sends its window size to let the other end know.
5. Persist timer helps avoid deadlocks in communication.

### **Timed-wait**

1. After releasing a connection, either of the hosts waits for a timed-wait time to terminate the connection completely.
2. This is to make sure that the other end has received the acknowledgement of its connection termination request.
3. The timed-out duration can be a maximum of 240 sec (4 min).

### **Crash Recovery in TCP**

TCP is a very reliable protocol. When a TCP server crashes mid-way during communication and re-starts its process, it sends a transport protocol data unit (TPDU) broadcast to all its hosts. The hosts can then send the last data segment which has never been unacknowledged and carry on. This eliminates the need to retransmit all the segments which are part of the transmission but have been acknowledged positively by the receiver.

## **1.13.2 User Datagram Protocol**

The user datagram protocol (UDP) is the simplest transport layer communication protocol which involves minimum amount of communication mechanism, compared to TCP. UDP is said to be an unreliable transport protocol but it uses IP services which provide the best effort delivery mechanism.

In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable but easier on processing (Box 1.4).

### **Characteristics**

The following are the characteristics of UDP:

- It is a stateless protocol.
- It is not connection oriented.
- It does not guarantee ordered delivery of data.
- It does not send any acknowledgement to the data sent.
- It is simple and suitable for data flowing in one direction, query-based communications, streaming applications like VoIP, and multimedia streaming.
- It does not provide a congestion control mechanism.

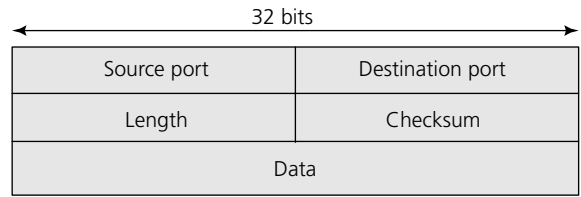
### **Box 1.4 Why UDP Is Preferred for Video Streaming**

Video streaming involves thousands of packets to be forwarded over the network to the intended users. Acknowledging all the packets is troublesome and may result in wastage of bandwidth. The best delivery mechanism of the underlying IP protocol ensures best efforts to deliver its packets. Even if some packets in the course of video streaming are lost, the impact is not calamitous and goes unnoticed by the user.

## UDP Header

The UDP structure is illustrated in Fig. 1.10. The fields in the UDP header are as follows:

1. *Source port*: These 16 bits of information is used to identify the source port of the packet.
2. *Destination port*: These 16 bits of information identifies application-level service on the destination machine.
3. *Length*: The length field specifies the entire length of the UDP packet (including header). It is a 16-bit field; the minimum value is 8-byte, that is, the size of the UDP header itself.
4. *Checksum*: This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional. So when checksum field does not contain any value it is made 0 and all its bits are set to zero.



**Fig. 1.10** Structure of UDP

## 1.14 APPLICATION LAYER

The application layer is the top-most layer in the OSI, and TCP/IP-layered model takes the help of transport and all the layers below it to communicate or transfer its data to the peer application layer protocol on a remote host. Applications which interact with the communication system are put up in this layer. For example, a web browser uses HTTP to interact with the network and so HTTP is an application layer protocol. Another example is file transfer protocol (FTP), which helps a user to transfer text-based or binary files across the network. Similarly, DNS is a protocol which helps HTTP to accomplish its work.

Any two processes can interact and communicate in any one of the following two ways:

### Sockets

1. With this, the process acting as the server opens a socket using a well-known (or known by client) port and waits until a client makes a request.
2. The client also opens a socket but instead of waiting for an incoming request, the client processes 'requests first'.
3. When the request reaches the server, it is served.

### Remote procedure call

1. In this, the interaction between processes happens through procedure calls. One process (client) calls the procedure lying on the remote host.
2. The process on the remote host is said to be the server. Both processes are allocated stubs.
3. This communication happens in the following way:
  - (a) The client process calls the client stub. It passes all the parameters pertaining to the program local to it.
  - (b) All parameters are then packed (marshalled) and a system call is made to send them to the other side of the network.
  - (c) The kernel sends the data over the network and the other end receives it.
  - (d) The remote host passes the data to the server stub where it is unmarshalled.
  - (e) The parameters are passed to the procedure and the procedure is then executed.
  - (f) The result is sent back to the client in the same manner.

### 1.14.1 Application Layer Protocols

Five of the most frequently used application protocols are listed here:



### Domain name system

1. The DNS works on the client/server model.
2. It uses UDP protocol for transport layer communication.
3. It uses a hierarchical domain-based naming scheme.
4. The DNS server is configured with fully qualified domain names (FQDN) and email addresses mapped with their respective IP addresses.
5. When a DNS server is requested with FQDN, it responds with the IP address mapped to it. DNS uses UDP port 53.

### Simple mail transfer protocol

1. The simple mail transfer protocol (SMTP) is used to transfer electronic mail from one user to another.
2. This task is done by means of email client software (user agents) that the user is using.
3. User agents help the user to type and format the email and store it until Internet is available.
4. When an email is submitted to send, the sending process is handled by a message transfer agent that normally comes inbuilt in email client software.
5. The message transfer agent uses SMTP to forward the email to another message transfer agent on the server side.
6. While SMTP is used by the end user to only send the emails, the servers normally use SMTP to send as well as receive emails.
7. SMTP uses TCP port numbers 25 and 587.
8. Client software uses Internet message access protocol (IMAP) or POP protocols to receive emails.

### File transfer protocol

1. FTP is the most widely used protocol for file transfer over the network.
2. FTP uses TCP/IP for communication and works on TCP port 21.
3. FTP works on a client/server model where the client requests the server for a file. When the server receives a request for a file, it opens a TCP connection for the client and transfers the file. Once the transfer is complete, the server closes the connection. For a second file, the client requests again and the server reopens a new TCP connection.
4. FTP uses out-of-band controlling, that is, FTP uses TCP port 20 for exchanging and controlling information and the actual data is sent over TCP port 21.

### Post office protocol

1. The post office protocol version 3 (POP 3) is a simple mail retrieval protocol used by user agents (client email software) to retrieve mails from the mail server.
2. When a client needs to retrieve mails from the server, it opens a connection with the server on TCP port 110.
3. The user can then access mails and download them to the local computer. POP3 works in two modes. In delete mode, the emails get deleted from the remote server after they are downloaded to local machines, whereas the keep mode does not delete the email from the mail server but gives the user an option to access mails later on the mail server.

### Hyper text transfer protocol

1. It is the foundation of WWW.
2. It works on client/server model.
3. It is a stateless protocol, which means the server maintains no information about earlier requests by clients.
4. When a user wants to access any HTTP page on the Internet, the client machine at the user end initiates a TCP connection to the server on port 80.

5. When the server accepts the client request, the client is authorized to access the web pages.
6. To access the web pages, a client normally uses web browsers, which are responsible for initiating, maintaining, and closing TCP connections.

### 1.15 SECURITY VULNERABILITIES IN TCP/IP SUITE

Security vulnerabilities exist in the design and implementation of the TCP/IP protocol suite. Compromising the protocols in any of the layers can compromise the entire communication. This necessitated the employment of a layered security mechanism to ensure foolproof security. Some of the vulnerabilities which exist in the protocols part of the TCP/IP suite are listed here:

1. In HTTP, an application layer protocol in the TCP/IP suite file transfers are made in plain text and so it is easy for an intruder to read the data packets exchanged between the server and a client. Moreover, weak authentication during session initialization leads to a session hijacking attack where the HTTP session of the legitimate user is stolen by the attacker.
2. A TCP protocol relies on a three-way handshake for connection establishment. A SYN-flooding attack (a kind of DoS attack) can overload the server and lead to a crash.
3. IP spoofing can be launched by modification of the IP protocol header.
4. As an attack on DNS, a DNS record can be modified by the attacker to get resolved to an incorrect IP address.
5. ICMP can be exploited to discover all host IP addresses that are alive in a target network with ICMP sweep attack.

### 1.16 SECURITY MECHANISMS IN NETWORKING LAYERS

Security in a TCP/IP protocol-based network is implemented in physical and data link layers at the user terminal and NIC, in the TCP and IP layers at the operating system, and as user process for the layers above TCP/IP.

The goal of network security is to ensure that the entire network is secure in terms of confidentiality, availability, and integrity. The confidentiality aspect of network security ensures that the data in the network is available only to intended and authorized recipients. Availability attempts to ensure that the data, network resources, and services are available to intended recipients at all times. Integrity attempts to make sure that the data in the network is reliable and not altered by unauthorized persons. These three conflicting metrics are achieved with mechanisms such as encryption, digital signatures, and access control measures.

Any communication between two hosts can be secured by employing security mechanisms at the network layer. This is achieved with a security protocol like Internet protocol security (IPsec). Security measures at the transport layer can protect the data in a single communication session between two hosts. The transport layer security (TLS) and secure socket layer (SSL) are the most common protocols used for this purpose. An application-specific security measure can be offered at the application layer. Secure multipurpose Internet mail extensions (S/MIME) is the best example of an application layer security protocol meant to encrypt email messages.

### 1.17 NETWORK SECURITY AT NETWORK LAYER WITH INTERNET PROTOCOL SECURITY

IPsec is a framework for ensuring security at the network layer. The security functions offered by IPsec are as follows:

1. *Confidentiality*: IPsec enables communicating nodes to encrypt messages which prevent eavesdropping by third parties.
2. *Origin verification and data integrity*: IPsec verifies whether a received packet is actually transmitted by the source from the packet header and also confirms that the packet has not been altered.

3. *Key management*: IPsec allows secured exchange of keys which guarantee safe exchange of data between hosts besides offering protection against many attacks.

### **IPsec Operations**

The two operations of IPsec which provide security services include IPsec communication and Internet key exchange (IKE).

1. IPsec Communication deals with packet processes such as encapsulation, encryption, and hashing the IP datagrams. It manages the communication according to the available security associations (SAs) established between communicating parties using security protocols such as authentication header (AH) and encapsulating security payload (ESP).
2. IKE is an automatic key management protocol used by IPsec. It is responsible for the creation of keys for IPsec and providing authentication during the key establishment process.

### **IPsec Communication Modes**

IPsec communication can function in transport and tunnel modes, either individually or in combination.

**Transport mode** In this mode, IPsec does not encapsulate a packet received from the upper layer. The original IP header is preserved and the data is forwarded based on the original attributes set by the upper layer protocol. No gateway services are provided in this mode and it is reserved for point-to-point communications.

**Tunnel mode** Tunnel mode is typically associated with gateway activities. In tunnel mode, the entire packet from the upper layer is encapsulated before applying a security protocol. A new IP header is added. The encapsulation provides the ability to send several sessions through a single gateway.

#### **1.17.1 IPsec Communication**

IPsec is equipped with a flexible, powerful way of specification with security policies and security associations, and how different types of datagrams should be handled.

**Security policies** A security policy is a rule that is programmed into the IPsec implementation telling it to process different datagrams received by the device. If security is required, the security policy provides general guidelines for how it should be provided, and if necessary, links to more specific details. Security policies are used to decide if a particular packet needs to be processed by IPsec or not. If packets are not to be processed by IPsec, they can bypass AH and ESP completely. Security policies for a device are stored in the device's *security policy database* (SPD).

**Security associations** A security association (SA) is a set of security information that describes a particular kind of secured connection between one device and another. A device's security associations are contained in its *security association database* (SAD).

The main difference between SAP and SAD is that security policies are general, whereas security associations are more specific. To determine how a particular datagram must be handled, a device first checks the SPD. The security policies in the SPD may make reference to a particular security association in the SAD. If so, the device will look up that security association and use it for processing the datagram.

### **IPsec Authentication Header**

One of the two core security protocols in IPsec is the *authentication header* (AH). AH is a protocol that provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram. What parts of the datagram are used for the calculation, and the placement of the header, depend on the communication mode (tunnel or transport) and the version of IP (IPv4 or IPv6).

The operation of the AH protocol is as follows:

1. A security association between two devices is set up, specifying these particulars so that the source and destination know how to perform the computation but nobody else can.
2. On the source device, AH performs the computation and puts the result called the integrity check value (ICV) into a special header with other fields for transmission.
3. The destination device does the same calculation using the key the two devices share, which enables it to see immediately if any of the fields in the original datagram were modified (either due to error or malice).
4. The presence of the AH header helps only in the verification of the integrity of the message and not in encryption. Thus, AH provides authentication but not privacy.

### **IPSec Encapsulating Security Payload**

Datagrams should be protected from intermediate devices against changes and should be protected from examining their contents. This is achieved with *encapsulating security payload* (ESP) protocol.

The main job of ESP is to provide privacy for IP datagrams by *encrypting* them. This is then repackaged using a special format and transmitted to the destination, which decrypts it using the same algorithm. ESP also supports its own authentication scheme like the one used in AH, or can be used in conjunction with AH.

### **Encapsulating Security Payload Fields**

ESP has several fields that are the same as those used in AH, but packages its fields in a very different way. Instead of having just a header, it divides its fields into three components:

*ESP header* This contains two fields, the SPI and sequence number, and comes before the encrypted data. Its placement depends on whether ESP is used in transport mode or tunnel mode.

*ESP trailer* This section is placed after the encrypted data. It contains padding that is used to align the encrypted data, through a padding and pad length field. Interestingly, it also contains the next header field for ESP.

*ESP authentication data* This field contains an integrity check value (ICV), computed in a manner similar to how the AH protocol works, for when ESP's optional authentication feature is used.

### **1.17.2 Internet Key Exchange**

It is necessary for the two devices involved in communication to exchange the 'secret' that the security protocols themselves will use. The primary support protocol used for this purpose in IPSec is called Internet key exchange (IKE).

The purpose of IKE is to allow devices to exchange information required for secured communication. It includes cryptographic keys used for encoding authenticated information and performing payload encryption. Any two devices that securely exchange information encode and decode it using a piece of information known only to them. Anyone can intercept the information but is prevented either from reading it (if ESP is used to encrypt the payload) or from tampering (if AH is used). IKE works by allowing IPSec-capable devices to exchange SAs to populate their SADs. These are then used for the actual exchange of secured datagrams with the AH and ESP protocols.

## **1.18 NETWORK SECURITY AT TRANSPORT LAYER**

Transport layer security (TLS) protocols operate above the TCP layer. The design of these protocols uses popular application program interfaces (API) to TCP, called 'sockets' for interfacing with the TCP layer. The family of protocols designed for TLS include SSL versions 2 and 3 and TLS protocol. Netscape developed SSLv2 and SSLv3. SSL used the patented RSA crypto.

The Internet Engineering Task Force (IETF) subsequently introduced a similar TLS protocol as an open standard. TLS protocol is non-interoperable with SSLv3. TLS modified the cryptographic algorithms for key expansion and authentication and used open crypto Diffie–Hellman (DH) and digital signature standard (DSS).

### 1.18.1 Secure Socket Layer

SSL protocol works in between the application and transport layer. It is a two-layer protocol with *SSL record protocol* in the lower layer and an upper layer comprising *SSL handshake protocol*, *change cipher spec protocol*, and *alert protocol* for message exchange and an *application protocol* for providing information transfer service between client/server interactions.

The functions of these protocols are as follows:

1. The *record protocol* formats the protocol messages from the upper layer, fragments it into blocks, compresses it (optionally), encrypts the data, adds a header to each message, adds a hash (preferably message authentication code, MAC) at the end and hands over the formatted block to the transport layer for transmission.
2. *SSL handshake protocol* and *change cipherspec protocol* creates SSL sessions between the client and the server. The handshaking mechanism is explained in detail in the following subsection.
3. *SSL alert protocol* is used to report errors.

#### Handshake Protocol of SSL and TLS

The handshake protocol is responsible for the authentication and key exchange necessary to establish or resume secure sessions. When establishing a secure *session*, the handshake protocol manages the following:

*Cipher suite negotiation* The client and the server contact each other and choose the cipher suite that will be used throughout their message exchange.

*Authentication of server and optionally, client* The server proves its identity to the client. The client might also need to prove its identity to the server. The use of *public/private key pairs* is the basis of this authentication. The exact method used for authentication is determined by the cipher suite negotiated.

*Session key information exchange* The client and the server exchange random numbers and a special number called the pre-master secret. These numbers are combined with additional data permitting the client and the server to create their shared secret, called the master secret. The master secret is used by the client and the server to generate the write MAC secret, which is the session key used for *hashing*, and the write key, which is the *session key* used for encryption.

The SSL/TLS handshake protocol is explained in detail in the following steps:

1. The client sends a ‘Client hello’ message to the server, along with cryptographic information such as the SSL or TLS version, the client’s random value to be used in subsequent computations and supported cipher suites, and the data compression methods supported by the client.
2. The server responds by sending a ‘Server hello’ message to the client, the CipherSuite chosen by the server from the list provided by the client, the session ID, along with the server’s random value.
3. The server sends its digital certificate to the client for authentication and may request a certificate from the client. The server sends the ‘Server hello done’ message.
4. The client verifies the server’s digital certificate.
5. If the server requires a digital certificate for client authentication, the server sends a ‘client certificate request’ that includes a list of the types of certificates supported and the distinguished names of acceptable certification authorities (CAs).
6. If the server has requested a ‘client certificate request’, the client sends a random byte string encrypted with the client’s private key, together with the client’s digital certificate.
7. The server verifies the client’s certificate.

8. The client creates a random pre-master secret, encrypts it with the *public key* from the server's certificate, and sends the encrypted pre-master secret to the server.
9. The server receives the pre-master secret. The server and the client each generates the master secret and *session keys* based on the pre-master secret.
10. The client sends a 'Change cipher spec' notification to the server to indicate that the client will start using the new *session keys* for *hashing* and encrypting messages. The client also sends a 'Client finished' message.
11. The server receives the 'Change cipher spec' and switches its record layer security state to *symmetric encryption* using the *session keys*. The server sends a 'Server finished' message to the client.
12. The client and server can now exchange application data over the secured channel they have established. All messages sent from the client to the server and from the server to the client are encrypted using the session key.

**Table 1.2** Differences between SSL and TLS

Characteristic	TLS	SSL
Protocol version in segment header	Version number 3.1	Version number 3
Message authentication	Keyed-hash message authentication code (H-MAC) that can operate with any hash function	MD5 or SHA
Session key generation	Computation of master secret uses HMAC standard	Computation of master secret uses adhoc-MAC
Supported cipher suites	All suites except Fortezza	RSA, Diffie–Hellman and Fortezza cipher suites
Padding of data before encryption	Minimum to make the total data equal to a multiple of the cipher's block length	Padding can be any amount upto a maximum of 255 bytes
Alert protocol message	Supports more error messages	Supports fewer error messages than TLS

### 1.18.2 Transport Layer Security Protocol

The architecture of the TLS protocol is similar to the SSLv3 protocol. It has two sub-protocols: the TLS record protocol and the TLS handshake protocol. Though SSLv3 and TLS protocol have similar architecture, differences exist in the architecture and functioning, particularly for the handshake protocol, and are listed in Table 10.2.

### 1.18.3 HTTPS

HTTPS stands for HTTP over SSL. This protocol provides an encrypted and authenticated connection between the client web browser and the website server thereby ensuring 'secure' web browsing. HTTPS application protocol typically uses one of the two popular transport layer security protocols: SSL or TLS. When a web page is requested using a web browser by entering `https://` followed by the URL in its address bar, connection to the web server is initiated with the use of SSL protocol. The browser uses system port 443 instead of port 80 reserved for http.

The handshaking mechanism is invoked by SSL for ensuring a secure connection wherein the website at the server sends its SSL digital certificate to the browser. Upon certificate verification, the SSL handshake involves the exchange of shared secrets for the session. When a trusted SSL digital certificate is used by the server, users get to see a padlock icon in the browser address bar meaning that a secured connection is established between the web server and the browser.

HTTPS offers confidentiality, server authentication, and message integrity to the user which enables safe browsing on the Internet. It also prevents the data exchanged during a session from eavesdropping and identity theft.

### 1.18.4 Secure Shell Protocol

The secure shell protocol (SSH protocol) is a method for secure remote login from one computer to another. It provides strong authentication, and protects the communications' security and integrity with strong encryption. It is a secure alternative to telnet and FTP, and is primarily used for file transfer and email.

SSH is organized as three sub-protocols, namely *SSH user authentication protocol*, *SSH connection protocol*, and *SSH transport layer protocol*.

*SSH transport layer protocol* It focuses on server authentication, session key establishment, and ensuring data integrity.

*SSH user authentication protocol* It authenticates users with passwords, Kerberos, or public-key authentication and gives access only to intended users.

*SSH connection protocol* It attempts to provide multiple logical channels over a single underlying SSH connection.

The SSH protocol works in the client/server model as follows:

1. The SSH client initiates a connection by contacting the SSH server.
2. The SSH server sends it the public key.
3. The SSH client uses public key cryptography to verify the identity of the SSH server.
4. The SSH server and SSH client enter into a negotiation phase during which they agree on the symmetric encryption algorithm to be used and generate the encryption key that will be used. This is to ensure that the traffic between the communicating parties is protected with industry standard-strong encryption algorithms.
5. A secure channel is opened. Once a connection has been established between the SSH client and server, the data that is transmitted is encrypted using strong symmetric encryption according to the parameters negotiated in the set-up. Hashing algorithms are used to ensure the privacy and integrity of the data that is exchanged between the client and the server.

SSH service includes secure command shell which facilitates remote log on, secure file transfers with SSH file transfer protocol (SFTP), and port forwarding which facilitates data forwarding through a secured tunnel to the remote machine.

SSH protocol is predominantly used for secure access and file transfers, issuing remote commands, and to manage network infrastructure and other mission-critical system components.

## 1.19 NETWORK SECURITY AT APPLICATION LAYER

Email is a widely used application in the application layer, and relies on protocols such as simple mail transfer protocol (SMTP) used for forwarding e-mail messages, post office protocol (POP), and Internet message access protocol (IMAP) to retrieve the messages with the help of a mail client from the server. The process of securing emails ensures end-to-end security of the communication. It provides security services of confidentiality, sender authentication, message integrity, and non-repudiation.

Two schemes have been developed for email security: PGP and S/MIME. Both these schemes use secret-key and public-key cryptography and are presented in the following sub-section.

Besides this, standard DNS lookup is vulnerable to attacks such as DNS spoofing/cache poisoning. Securing DNS lookup is feasible through the use of DNSSEC which employs the public-key cryptography. It is also explained in the following sub-section.

### 1.19.1 Pretty Good Privacy

Pretty good privacy (PGP) is a public key encryption program. It is the most popular standard for email encryption. In addition to encrypting and decrypting an email, PGP is used to sign messages so that the receiver can verify both the identity of the sender and the integrity of the content. PGP uses a private key that must be kept secret and a public key that the sender and the receiver must share. PGP is a hybrid cryptosystem because it combines the features of both conventional and public key cryptography. Use of both the cryptographic approaches improves performance and key distribution without any compromise on security.

PGP works as follows:

1. When plaintext is encrypted with PGP, it is compressed to save transmission time and disk space, and strengthens cryptographic security.
2. PGP then creates a session key (random number) which is a one-time secret key generated from the random movements of the mouse and keystrokes by the user.
3. The session key is used with a conventional encryption algorithm to encrypt the plaintext.
4. Once the data is encrypted, the session key is encrypted using the recipient's public key.
5. The public key encrypted session key is transmitted along with cipher text to the recipient.
6. During decryption, the private key of the recipient is used by PGP to first recover the temporary session key, which in turn is used to decrypt the conventionally encrypted cipher text.

### 1.19.2 Secure MIME

Secure MIME (S/MIME) is an Internet standard for digitally signing MIME-based email data and its public key encryption. It was developed by RSA Security, Inc. and relies on the Rivest–Shamir–Adleman encryption system. S/MIME is a technology based on asymmetric cryptography that uses a pair of mathematically related keys to operate, namely a public key and a private key, to encrypt emails and protect it from unwanted access. It is computationally infeasible to figure out the private key based on the public key. S/MIME ensures that an email message is sent by a legitimate sender and provides encryption for incoming and outgoing messages. This makes it an effective weapon against phishing attacks.

S/MIME can work simultaneously with the following technologies but is not dependent on them (Box 1.5).

1. TLS to encrypt the tunnel or the route between email servers to help prevent snooping and eavesdropping.
2. SSL to encrypt the connection between email clients and servers.
3. BitLocker to encrypt the data on a hard drive in a data centre so as to prevent unauthorized access.

To enable S/MIME-based communication, the sender and the receiver must be integrated with a public key and signatures issued from a CA. A digital signature is used to validate a sender's identity, whereas a public key provides encryption and decryption services.

#### **Box 1.5 Multipurpose Internet Mail Extensions—MIME**

MIME is an extension of the original email standard, SMTP, which enables the sending of email containing different kinds of data files on the Internet, namely audio, video, images, application programs, and ASCII text. SMTP was extended so that Internet clients and servers could recognize and handle other kinds of data. As a result, new file types were added to mail as a supported IP file type.

Servers insert the MIME header at the beginning of any web transmission. Clients use this header to select an appropriate 'player' application for the type of data the header indicates. Some of these players are built into the browser (e.g., GIF and JPEG image players), whereas other players may be downloaded.



S/MIME works as follows:

1. When an email is created, it is signed and the private key applies the sender's unique digital signature into the message. With signing emails, S/MIME attempts to prove the identity as a sender or legitimate business.
2. Email is then encrypted with the recipient's public key.
3. The email can only be decrypted with the corresponding private key, which is supposed to be in sole possession of the recipient.
4. The recipient opens the email and uses the sender's public key to verify the signature. This satisfies the recipient that the emails really came from the sender.
5. Unless the private key is compromised, only the intended recipient will be able to access the sensitive data in emails.

Google encrypts the messages sent to Gmail.

### 1.19.3 DNSSec

The DNS is used to translate domain names (e.g., *example.com*) into numeric Internet addresses. Domain name information is stored and accessed on special servers known as domain name servers. The top level of the DNS resides in the root zone where all IP addresses and domain names are kept in databases and sorted by top-level domain name, such as .com, .net, .org, etc. Several vulnerabilities were discovered with DNS. Email servers use DNS to route their messages, which means they are vulnerable to security issues in the DNS infrastructure, for example, routing through rogue mail servers.

Domain name system security extensions (DNSSEC) are a set of protocols that add a layer of security to the DNS lookup and exchange processes. It helps to prevent malicious activities such as cache poisoning, pharming, and man-in-the-middle attacks.

DNSSec creates a secure domain name system by adding cryptographic signatures to existing DNS records. These digital signatures are stored in DNS name servers alongside common record types such as A, AAAA, MX, CNAME, etc. DNSSEC protects Internet clients from counterfeit DNS data by verifying digital signatures embedded in the data. These new records are used to digitally 'sign' a domain, using a method known as public key cryptography.

To facilitate signature verification, DNSSec has added a few new DNS record types, which are as follows:

1. RRSIG : Contains cryptographic signature
2. DNSKEY : Contains public signing key
3. DS : Contains the hash of DNSKEY record
4. NSEC and NSEC3 : For explicit denial of existence of a DNS record
5. CDNSKEY and CDS : For a child zone requesting updates to DS record in the parent zone

DNSSEC uses a system of public keys and digital signatures to verify data. DNSSec can be visualized as follows:

1. All the records with the same type in a zone are grouped to form a resource record set (RRset).
2. Each Zone has a zone-signing key (ZSK) pair.
3. To enable DNSSEC, the zone operator uses the private key to digitally sign each RRset in the zone and stores them in the name server as RRSIG records.
4. The public key is used for signature verification and is added by the zone operator to the name server in the DNSKEY record.
5. DNS servers have key-signing-keys (KSK) to validate the ZSK stored in the DNSKEY record. KSK signs the public ZSK creating an RRSIG for the DNSKEY. The name server publishes the public KSK in another DNSKEY record.
6. When a domain name is entered in the browser, the resolver verifies the digital signature as follows:
  - (a) The desired RRset is requested, which also returns the corresponding RRSIG record.
  - (b) The DNSKEY records containing the public ZSK and public KSK are requested which also return the RRSIG for the DNSKEY RRset.

- (c) RRSIG of the requested RRset is verified with the public ZSK.
  - (d) RRSIG of the DNSKEY RRset is verified with the public KSK.
7. If the digital signatures in the data match those that are stored in the master DNS servers, the data is allowed to access the client computer making the request thus ensuring that the communication is to the intended Internet location.
  8. When someone makes a request to the signed name server, it sends information signed with its private key; the recipient then unlocks it with the public key. If a third party tries to send untrustworthy information, it won't unlock properly with the public key. So the recipient will know that the information is bogus.

## 1.20 NETWORK SECURITY WITH FIREWALL

A *firewall* is a network security device that grants or rejects network access to traffic flows between an untrusted zone (e.g., the Internet) and a trusted zone (e.g., a private or corporate network). It acts as the demarcation point or 'traffic cop' in the network, as all communications should flow through it and this is where traffic is granted or rejected access.

Firewall may be hardware, software, or a combination of both and is categorized into four types: network level, application level gateway, circuit level gateway, and stateful multilayer gateways. They are explained here.

### **Network-level**

This type of firewall examines packet headers and filters traffic based on the source and destination computer's IP address, the port used, and the service requested. They can also filter traffic based on different protocols. Most modern routers contain network-level firewalls.

### **Circuit-level Gateway**

The circuit-level gateway firewall works at the session layer of the OSI model or at the TCP/IP. This class of firewall determines the genuineness of a requested session by monitoring the handshake between them. A circuit-level firewall can hide the network from the outside world and also restrict session rules to known computers. Typically, circuit-level gateways cost less than other forms of firewall protection.

### **Application-level Gateway**

Application-level gateways, most commonly known as proxies, work in a manner similar to circuit-level gateways except that they work on specific applications. Application-level gateways configured as a web proxy do not allow FTP, telnet, or any other traffic through the firewall. These firewalls also block websites based on content. Because application-level gateways thoroughly examine packets of data, it takes longer for information to pass through these firewalls. Application-level gateways also require manual configuration on each user system and have zero transparency to the user. Application-level gateways protect the network from malicious attacks, spam and viruses.

### **Stateful Multilayer Gateways**

Stateful multilayer (SML) gateways offer the best features than the other three firewall types, that is, they filter packets at the network layer, they determine packet legitimacy, and they evaluate packet contents at the application layer. SML gateways also provide a direct connection between the host and the client. This allows for transparency at the user level, unlike the application-level gateway. Because SML gateways do not use proxies, they work faster than their application-layer counterparts. However, their cost is more.

## 1.21 NETWORK SECURITY WITH INTRUSION DETECTION SYSTEM AND INTRUSION DETECTION AND PREVENTION SYSTEM

Intrusion detection system (IDS) is a device or a software application that monitors the network for any suspicious activity and notifies the network administrator (NA) or the system personnel when a suspicious activity

is discovered. IDS can be configured to take preventive action to prevent any further access in which case it is termed intrusion detection and prevention system (IDPS). In other words, IDPS is a network security appliance that resets the connection to save the IP address from blockage or reprograms the firewall to block further network traffic from a suspicious source as its response to detecting a suspicious activity.

There are two approaches used by IDS to detect intruders: *profile-based detection* and *signature-based detection* wherein the former uses the profiles created by NA to distinguish between normal traffic/activity and anomaly (traffic that does not match configured profile) and thereby detect intruders. The latter relies on a preconfigured set of signatures that are compared with network traffic so as to detect an intrusion.

IDPS relies on three different approaches to detect intrusion: (a) *signature-based detection* where IDPS monitors the network traffic for preconfigured signatures and takes action in the event of a match, (b) *statistical anomaly-based detection* where baseline performance of network anomaly is defined and any activity that deviates from the baseline is termed as intrusion for the IDPS to take appropriate preventive action, (c) *stateful protocol analysis detection* where normal and benign activities are predetermined and predefined and an IDPS takes preventive action when a match occurs while comparing observed events with benign activity profiles.

IDS can be classified into three types:

### **Host-based Intrusion Detection System—HIDS**

This type of IDS operates by installing software agents on all hosts on the network to monitor network traffic and all the activities, log files, operating system, system calls, error messages, etc. It is also called a passive system. It assumes that an attack can come through a network by generating network traffic or by gaining physical access. Host-based IDS are powerful enough to detect attacks that are performed from the console, but can fail to offer physical security in the event that an intruder with knowledge on IDS gains access to the host and disables the detection software. It can detect stealth attacks as well.

The drawbacks with host-based IDS are as follows:

1. Manageability becomes complicated and time-consuming and tedious during software maintenance as IDS software needs to be installed on all hosts
2. It can analyse only received traffic and not port scans and ping sweeps.
3. In the event that it gets compromised it fails to send an intrusion notification to the NA.
4. Witnesses operate on system limitations because of the need to support hosts running different platforms in a network.

The best examples for HIDS are Tripwire and OSSEC.

### **Network-based Intrusion Detection System—NIDS**

This type of IDS uses sensors or probes installed on a network that runs IDS software and sniffs the network traffic possibly from a hub/switch by looking for a match with a defined signature or profile to detect intrusion. It is also called reactive system. It works on the basis of perceiving intrusions from a network perspective and so can detect port scans and ping sweeps. Sensors employed have command control interface (CCI) to send and receive management traffic and to communicate with a centralized computer over a highly secure management network and monitoring interface (MI) to monitor the network. Thus NIDS remains invisible to intruders who are unfamiliar with the security features in the network. The advantage of this class of IDS is that it does not consume CPU cycles of the host for its operation, and does not pose manageability issues and operating system limitations as host-based IDS.

The drawbacks with network-based IDS are as follows:

1. It consumes network bandwidth for its operation
2. It cannot detect intrusion if an intruder fragments packets that correspond to an intrusion, as the sensor is unable to reassemble the packets correctly.
3. It cannot handle packets that have their time-to-live (TTL) field manipulated to be low by an intruder.
4. It cannot handle packets that are encrypted.

The best example for NIDS is Snort.

### **Hybrid Intrusion Detection System or Hybrid IDS**

It combines the advantages of both HIDS and NIDS while overcoming their drawbacks.

IDPS is classified into three which are as follows:

1. *Host-based intrusion detection and prevention system (HIDPS)* which is installed in a host as a software package to monitor the events that happen in the host and to detect any suspicious activity.
2. *Network-based intrusion detection and prevention system (NIDPS)* which monitors the network traffic for suspicious activity by protocol analysis.
3. *Wireless intrusion detection and prevention system (WIDPS)* which monitors the network traffic for suspicious activity with wireless networking protocols.

### **POINTS TO REMEMBER**

- A computer network is a collection of computers and devices interconnected by communication channels to facilitate communication, sharing of information, and resources among interconnected devices.
- The three common forms of networking architecture are peer-to-peer network, client/ server architecture (or) server-based network, and hybrid network.
- The four basic types of networking technologies based on geographical span are local area network (LAN), metropolitan area network (MAN), wide area network (WAN), and Internetwork.
- The Internet is an interconnection of many combinations of networks such as LAN, WAN, and MAN. On the other hand, in an intranet, the network is restricted for use by a single corporate entity which has full control and management over the network.
- The open system interconnection (OSI) model is a seven-layer model used to visualize computer networks and to solve problems in it.
- The layers of the OSI model are application layer, presentation layer, session layer, transport layer, network layer, data link layer, and physical layer.
- The Internet is a four-layered architecture which uses TCP/IP protocol suite, also known as Internet suite or the Internet model.
- The four layers of Internet model are application layer, transport layer, Internet layer, and link layer.
- Networking devices such as repeaters, hubs, bridge, switch, gateway, and modem are used for connecting to a network, routing the packets, strengthening the signal, communicating with others, sharing files on the network, etc.
- The various LAN technologies are ethernet, fast ethernet, giga ethernet, virtual LAN, and Wi-Fi.
- Network topology reflects the interconnection between computer systems and the networking devices in a network.
- The various network topologies are point-to-point, bus topology, star topology, ring topology, mesh topology, tree topology, daisy chain, and hybrid topology.
- Network protocol is a set of rules that govern communications between devices connected on a network.
- Transmission control protocol (TCP) and Internet protocol (IP) are the two computer network protocols used in all operating systems of networked devices.
- Physical layer defines the hardware equipment, cabling, wiring, frequencies, and pulses used to represent binary signals, etc.
- The transmission media over which the data is exchanged between any two hosts may be either guided or unguided.
- Channel capacity determines the speed of transmission of information and depends on factors such as bandwidth, error rate, and the encoding mechanism.
- Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link.
- Switching is a mechanism by which data or information is sent from the source towards a destination that is not directly connected to it, but through interconnecting devices between them.
- The different types of switching are circuit

switching, message switching, and packet switching.

- The data link layer hides the details of the underlying hardware and represents itself to the upper layer as the medium to communicate.
- The logical link control deals with protocols, flow-control, and error control.
- Media access control deals with the actual control of media.
- The functions of the data link layer are framing, addressing, synchronization, error control, flow control, and multi-access.
- Error detection mechanism can be based on either parity check or cyclic redundancy check.
- Error correction mechanism can be processed as either backward error correction or forward error correction.
- The error control mechanisms or protocols are stop-and-wait with automatic repeat request (ARQ), Go-Back-N ARQ, and selective repeat ARQ.
- The flow control mechanisms are stop and wait, and sliding window.
- The network layer is responsible for routing packets from the source to the destination either within or outside a subnet irrespective of different, non-compatible addressing schemes and protocols.
- Every node/host in the network is uniquely identified with an IP address called network address and is configured on the network interface card.
- Routing is the process of selecting one among the multiple paths to reach a destination from the routing table and is performed by the network device, router.
- Routing can be unicast, multicast, broadcast, and anycast.
- Routing between two networks either of the same kind or different kind scattered geographically is called internetworking.
- The protocols that operate at the network layer are address resolution protocol (ARP), reverse address resolution protocol (RARP), Internet control message protocol (ICMP), and the Internet protocol (IP). IP is available as two variants, namely IPv4 and IPv6.
- The transport layer is responsible for end-to-end connection between two processes on remote hosts.
- The two main transport layer protocols are transmission control protocol (which provides reliable communication between two hosts) and user datagram protocol (which provides unreliable communication between two hosts), of which TCP is widely used in a communication network like the Internet.
- The application layer is the topmost layer in OSI, and TCP/IP-layered model takes the help of transport and all the layers below it to communicate or transfer its data to the peer application layer protocol on a remote host.
- The application layer protocols are domain name system, simple mail transfer protocol, file transfer protocol, post office protocol, and hypertext transfer protocol.
- Compromising the protocols in the TCP/IP suite in any one of the layers can compromise the entire communication.
- The vulnerabilities in TCP/IP suite are session hijacking attack, SYN-flooding attack, IP spoofing, DNS attack, and ICMP sweep attack.
- The security functions offered by IPSec are confidentiality, origin verification and data integrity, and key management.
- IPSec is equipped with a flexible, powerful way of specification using security policies, security associations, and the handling of different types of datagrams.
- Internet key exchange (IKE) is useful for the two devices involved in communication to exchange the 'secret' that the security protocols themselves will use.
- A firewall is a network security device that grants or rejects network access to traffic flows between an untrusted zone (e.g., the Internet) and a trusted zone (e.g., a private or a corporate network).
- Intrusion detection system (IDS) is a device or a software application that monitors the network for any suspicious activity and notifies the network administrator (NA) or the system personnel when a suspicious activity is discovered.
- IDS can be configured to take preventive action to prevent any further access in which case it is termed intrusion detection and prevention system (IDPS).
- The approaches used by IDS to detect intruders are profile-based detection and signature-based detection.
- IDPS relies on three different approaches to detect intrusion: signature-based detection, statistical anomaly-based detection, and stateful protocol

- analysis detection.
- IDS is classified into host-based IDS, network-based IDS, and hybrid IDS.
  - IDPS is classified into host-based IDPS, network-based IDPS, and wireless IDPS.

## KEY TERMS

**Bridge** This is defined as a networking device that connects two sub-networks (or interconnects two LANs) which are part of the same network.

**Computer network** This refers to a collection of computers and devices interconnected by communication channels to facilitate communication, sharing of information (data, messages, graphics) and resources (printers, fax machines, modems, and other hardware) among interconnected devices.

**Firewall** This is defined as a network security device that grants or rejects network access to traffic flows between an untrusted zone (e.g., the Internet) and a trusted zone (e.g., a private or corporate network).

**Hub** This means a networking device which is used to connect multiple network hosts. It is also called multiport repeater.

**Multicast routing** This refers to a special case of broadcast routing where the data packets are sent only to the nodes which want to receive the packets as against broadcast routing, where the packets are sent to all nodes irrespective of whether they want them or not.

**Multiplexing** This is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link.

**Network protocol** This is defined as a set of rules that govern communications between devices connected on a network.

**Open system interconnection (OSI) model** This is defined as a seven-layer model used to visualize computer networks and to solve problems in them.

**Repeater** This refers to an electronic two-port device that operates at the physical layer whose job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.

**Router** This refers to a device like a switch that routes data packets based on their IP addresses.

**Routing** This is defined as the process of selecting one among the multiple paths to reach a destination from the routing table and is performed by the network device, router.

**Switching** This refers to a mechanism by which data or information is sent from the source towards destinations that are not connected directly, but through interconnecting devices between them.

**Transmission control protocol (TCP)** This is defined as a transport layer protocol used by applications that require guaranteed delivery which establishes a full duplex virtual connection between two endpoints.

**User datagram protocol (UDP)** This is defined as the simplest transport layer communication protocol which involves only a minimum amount of communication mechanism, when compared to TCP.

## MULTIPLE-CHOICE QUESTIONS

- The common form(s) of network architecture is/are \_\_\_\_\_.
  - peer-to-peer network
  - client/server network
  - hybrid network
  - all of these
- The backbone of MAN is \_\_\_\_\_.
  - high-capacity, high-speed fibre optics
  - low-capacity, low-speed fibre optics
  - high-capacity, low-speed fibre optics
  - low-capacity, high-speed fibre optics
- IPv6 has introduced \_\_\_\_\_ addressing.
  - unicast
  - multicast
  - broadcast
  - anycast
- The length of the UDP packet is \_\_\_\_\_.
  - 8 bits
  - 16 bits
  - 32 bits
  - 64 bits
- The primary need of computer networks is for

- \_\_\_\_\_.
- (a) information exchange
  - (b) resource sharing
  - (c) resource planning
  - (d) (a) and (b)
6. \_\_\_\_\_ handles data flow and email between its network and other networks as well as with remote users through a modem or telephone lines in a dialup connection.
    - (a) File server
    - (b) Communication server
    - (c) Print server
    - (d) Application server
  7. The technologies used in WAN are \_\_\_\_\_.
    - (a) ATM and frame relay
    - (b) ATM and SONET
    - (c) ATM, frame relay, and SONET
    - (d) frame relay and SONET
  8. The logical link control (LLC) layer is responsible for \_\_\_\_\_.
    - (a) network gain access
    - (b) network gain access and error checking
    - (c) network gain access and packet synchronization
    - (d) error checking and packet synchronization
  9. The transport layer defines \_\_\_\_\_.
    - (a) the protocol which enables the user to interact with the network
    - (b) how the data should flow between hosts
    - (c) host addressing, recognition, and routing
    - (d) sending and receiving actual data
  10. \_\_\_\_\_ does not interfere with the data signal.
    - (a) Passive hub
    - (b) Active hub
    - (c) Both (a) and (b)
    - (d) None of these
  11. \_\_\_\_\_ is the fastest method of switching.
    - (a) Store and forward
    - (b) Fragment free
    - (c) Cut and through
    - (d) Routers
  12. Ethernet uses \_\_\_\_\_ technology to detect collisions.
    - (a) carrier sense multi access (CSMA)
    - (b) carrier sense multi access (CSMA)/collision detection (CD)
    - (c) collision detection (CD)
    - (d) None of these
  13. IEEE802.3ab defines giga ethernet over UTP using \_\_\_\_\_ cables.
    - (a) Cat-5
    - (b) Cat-5e
    - (c) Cat-6
    - (d) All of these
  14. \_\_\_\_\_ topology offers equal access privilege to any host.
    - (a) Point-to-point
    - (b) Bus
    - (c) Star
    - (d) Ring
  15. RG stands for \_\_\_\_\_.
    - (a) radio government
    - (b) radio governance
    - (c) radio generation
    - (d) radio generalization
  16. \_\_\_\_\_ results in poor utilization of resources.
    - (a) Go-Back-N-ARQ
    - (b) Stop-and-wait ARQ
    - (c) Selective repeat ARQ
    - (d) None of these
  17. An example of exterior gateway protocol (EGP) is the \_\_\_\_\_.
    - (a) routing information protocol (RIP)
    - (b) open shortest path first (OSPF)
    - (c) border gateway protocol (BGP)
    - (d) none of these
  18. \_\_\_\_\_ addressing scheme uses the first two octets for network addresses and the last two for host addressing.
    - (a) Class D
    - (b) Class C
    - (c) Class B
    - (d) Class A
  19. \_\_\_\_\_ remove(s) the dependability of dynamic host configuration protocol (DHCP) servers.
    - (a) Auto-configuration
    - (b) Configuration
    - (c) Reconfiguration
    - (d) All of these
  20. \_\_\_\_\_ indicates how much data the receiver is expecting.
    - (a) Urgent pointer
    - (b) Flags
    - (c) Data offset
    - (d) Windows size

## REVIEW QUESTIONS

1. What is application layer? List out the most frequently used application layer protocols.
2. Define bridge. What are the types of bridge?
3. Compare and contrast Internet and intranet.
4. Explain the various network topologies.
5. What are IDS and IDPS?

6. Discuss data link layer in detail.
7. Explain network security in the transport layer and application layer.
8. Give a brief note on firewall.
9. Discuss in detail the following: (a) Networking architecture, (b) Networking technologies, (c) Network models, and (d) Networking devices.
10. Explain the following briefly: (a) TCP/IP protocol suite, (b) physical layer, (c) network layer and network layer protocols, (d) transmission control protocol (TCP), and (e) user datagram protocol (UDP)
11. Discuss the following briefly: (a) security vulnerabilities in TCP/IP suite, (b) security mechanisms in the networking layers, and (c) IPSec
12. Give a detailed account on achieving network security with IDS and IDPS.

## APPLICATION EXERCISES

1. A company having its head office at location A plans to start another venture in a new city, at locations B, C, and D in the city where the distance between B and C is 150 km, B and D is 25 km, C and D is 15 km, and B is 1500 km away from the head office. It plans to install 50,75,100 and 125 computers in each of the locations, namely A, B, C, and D respectively.
  - (a) Suggest the kind of networking technology to be used for connecting each of the offices at different locations and justify your answer.
  - (b) Which networking device can be used to connect all the computers in the respective locations and why?
  - (c) Which communication media can be procured so as to ensure a very effective high-speed communication?
2. Do you think that email security has to be taken seriously? How much effort must be invested in encryption and securing email? State the requirements for email security and vulnerabilities, if any. Suggest the components required for email security and justify your answer.

## BIBLIOGRAPHY

1. Geeksforgeeks, *Internet Control Message Protocol*, available at: <http://www.geeksforgeeks.org/internet-control-message-protocol-icmp/> (Accessed 06 December 2017)
2. Computernetworkingnotes, *Computer Networking Devices Explained with Function*, available at: <https://www.computernetworkingnotes.com/networking-basic/computer-networking-devices-explained-with-function.html> (Accessed 06 December 2017)
3. Codesandtutorials, *Modem—Definition, Working, Types*, available at: <http://www.codesandtutorials.com/networking/networkdevices/modem-types-working.php> (Accessed 06 December 2017)
4. Geeksforgeeks, *Network Device (Hub, Repeater, Bridge, Switch, Router and Gateways)*, available at: <http://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/> (Accessed 06 December 2017)
5. Amar Shekar (30 March 2016), *Different Networking Devices and Hardware Types – Hub, Switch, Router, Modem, Bridge, Repeater*, available at: <https://fossbytes.com/networking-devices-and-hardware-types/> (Accessed 06 December 2017)
6. Tutorialspoint, *DCN Application Layer Introduction*, available at: [https://www.tutorialspoint.com/data\\_communication\\_computer\\_network/application\\_layer\\_introduction.htm](https://www.tutorialspoint.com/data_communication_computer_network/application_layer_introduction.htm) (Accessed 06 December 2017)
7. Tcpiiguide, *The TCP/IP Guide—IPSec Key Exchange (IKE)*, available at: [http://www.tcpiiguide.com/free/t\\_IPSecKeyExchangeIKE.htm](http://www.tcpiiguide.com/free/t_IPSecKeyExchangeIKE.htm) (Accessed 06 December 2017)
8. Margaret Rouse (September 2005), *What is MIME*



- (Multi-Purpose Internet Mail Extensions)?—Definition from *WhatIs.com*, available at: <http://searchmicroservices.techtarget.com/definition/MIME-Multi-Purpose-Internet-Mail-Extensions> (Accessed 07 December 2017)
9. Ssh, *SSH Protocol – Secure Remote Login and File Transfer*, available at: <https://www.ssh.com/ssh/protocol/> (Accessed 07 December 2017)
  10. IBM, *IBM Knowledge Center—An overview of the SSL or TLS handshake*, available at: [https://www.ibm.com/support/knowledgecenter/en/SSFKSJ\\_7.1.0/com.ibm.mq.doc/sy10660\\_.htm](https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm) (Accessed 07 December 2017)
  11. Technet, *What is TLS/SSL?: Logon and Authentication*, available at: [https://technet.microsoft.com/en-us/library/cc784450\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc784450(v=ws.10).aspx) (Accessed 07 December 2017)
  12. MSDN, *TLS Handshake Protocol (Windows)*, available at: [https://msdn.microsoft.com/en-us/library/windows/desktop/aa380513\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa380513(v=vs.85).aspx) (Accessed 07 December 2017)
  13. Instant SSL, *What is SSL?, Definition and How SSL Works, Comodo SSL Wiki*, available at: <https://www.instantssl.com/ssl.html> (Accessed 07 December 2017)
  14. Users, *How PGP Works*, available at: <https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html> (Accessed 07 December 2017)
  15. Kraken, *What is PGP encryption –Kraken*, available at: <https://support.kraken.com/hc/en-us/articles/201648223-What-is-PGP-encryption-> (Accessed 07 December 2017)
  16. Ricky Publico, *What is S/MIME and How Does it Work?*, available at: <https://www.globalsign.com/en/blog/what-is-smime/> (Accessed 07 December 2017)
  17. Technet, *S/MIME for Message Signing and Encryption. Exchange Online Help*, available at: [https://technet.microsoft.com/en-us/library/dn626158\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dn626158(v=exchg.150).aspx) (Accessed 08 December 2017)
  18. Margaret Rouse, *What is S/MIME (Secure Multi-Purpose Internet Mail Extensions)?—Definition from WhatIs.com*, available at: <http://whatis.techtarget.com/definition/S-MIME-Secure-Multi-Purpose-Internet-Mail-Extensions> (Accessed 08 December 2017)
  19. Techopedia, *What is Secure MIME (S/MIME)?—Definition from Technopedia*, available at: <https://www.techopedia.com/definition/9245/secure-mime-smime> (Accessed 08 December 2017)
  20. etutorials.org (2007), *Intrusion Detection Systems Overview*, available at: <http://etutorials.org/Networking/Cisco+Certified+Security+Professional+Certification/Part+V+Intrusion+Detection+Systems+IDS/Chapter+23+Intrusion+Detection+System+Overview/Intrusion+Detection+Systems+Overview/> (Accessed 27 January 2018)
  21. Vskills Govt Certifications, India's Largest Certification Body (2010) *Intrusion Detection and Prevention*, available at: <https://www.vskills.in/certification/tutorial/basic-network-support/intrusion-detection-and-prevention/> (Accessed 27 January 2018)

### Answers to Multiple-choice Questions

- |         |         |         |         |         |
|---------|---------|---------|---------|---------|
| 1. (d)  | 2. (a)  | 3. (d)  | 4. (b)  | 5. (d)  |
| 6. (b)  | 7. (c)  | 8. (d)  | 9. (b)  | 10. (a) |
| 11. (c) | 12. (b) | 13. (d) | 14. (d) | 15. (a) |
| 16. (b) | 17. (c) | 18. (c) | 19. (a) | 20. (d) |