The Principles of Computer Networking

Also in this series

1 An Introduction to Logical Design of Digital Circuits
C. M. Reeves 1972
2 Information Representation and Manipulation in a Computer
E. S. Page and L. B. Wilson, Second Edition 1978
3 Computer Simulation of Continuous Systems
R. J. Ord-Smith and J. Stephenson 1975
4 Macro Processors
A. J. Cole, Second Edition 1981
5 An Introduction to the Uses of Computers
Murray Laver 1976
6 Computing Systems Hardware
M. Wells 1976
7 An Introduction to the Study of Programming Languages
D. W. Barron 1977
8 ALGOL 68 – A first and second course
A. D. McGettrick 1978
9 An Introduction to Computational Combinatorics
E. S. Page and L. B. Wilson 1979
10 Computers and Social Change
Murray Laver 1980
11 The Definition of Programming Languages
A. D. McGettrick 1980
12 Programming via Pascal
J. S. Rohl and H. J. Barrett 1980
13 Program Verification using Ada
A. D. McGettrick 1982
14 Simulation Techniques for Discrete Event Systems
I. Mitrani 1982
15 Information Representation and Manipulation using Pascal
E. S. Page and L. B. Wilson 1983
16 Writing Pascal Programs
J. S. Rohl 1983
17 An Introduction to APL
S. Pommier 1983
18 Computer Mathematics
D. J. Cooke and H. E. Bez 1984
19 Recursion via Pascal
J. S. Rohl 1984
20 Text Processing
A. Colin Day 1984
21 Introduction to Computer Systems
Brian Molinari 1985
22 Program Construction
R. G. Stone and D. J. Cooke 1987
23 A Practical Introduction to Denotational Semantics
Lloyd Allison 1987
24 Modelling of Computer and Communication Systems
I. Mitrani 1987

25 Cambridge Computer Science Texts

The Principles of Computer Networking

D. Russell
Computing Laboratory, University of Newcastle upon Tyne

CAMBRIDGE UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Tokyo, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by
Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521339926

First published 1989
Reprinted 1991, 1997

A catalogue record for this publication is available from the British Library

ISBN 978-0-521-32795-4 Hardback
ISBN 978-0-521-33992-6 Hardback

To my parents

For more than I can ever know

Contents

Preface

This book is intended to cover the whole of the field of computer communications. Even with such a wide ranging ambition, there must be limits to the coverage. Roughly these are drawn at the lower end of the spectrum by assuming the properties of transmission media, and at the top end by stopping short of discussing truly distributed processing. In between, the aim has been to give an overall understanding of the principles involved.

Computer communications is such a vast and fast moving field that it is quite impossible to cover the details of any complete architecture within the confines of one book. However, that was never my intention. The real aim is to try to extract some of the *principles* that emerge in computer networking, sometimes over and over again. One prime example is the topic of flow control. The principles of flow control can be extracted independently of context, and this book devotes Chapter 4 to just that. Similarly, in Chapter 3 we look at what is at first sight a bewildering range of ways of sharing a medium. However, it soon emerges that most of their number can be reduced by asking two orthogonal questions—is the topology a bus or a ring, and is the access by contention or by token? Once these two principles have been understood, the other aspects are of secondary importance. Again, the addressing and routing principles that we discuss in Chapter 6 in relation to the techniques of providing the network service, crop up again when looking at network mail in Chapter 10, and Gateways in Chapter 15.

In overall plan the book starts at the bottom and works upwards. Thus, the early chapters through Chapter 6 explain how raw, error-prone communications media can be built into a reliable end-to-end communications service. However, the subject of communications has only just started by this time. For successful communication to take place, agreements have to be made about what the bits on this reliable pipe actually mean. This brings us to the consideration of presentation issues which are concerned with a consistent representation of the same semantic information across diverse systems. We also go into considerable detail in describing how various applications of computer connections actually work, including computer mail, terminal support, and file transfer and access. The application level tools provided by ISO, and in particular the remote operations service are explained.

As well as the "traditional" kinds of protocol with which this book is mainly concerned, a chapter is devoted to looking at so-called ***lightweight protocols***, and the performance and system issues involved in

the efficient implementation of communications architectures. In addition, since networks have grown so big, they need to be managed, and some of the management issues are also discussed.

Perhaps unusually, a whole chapter is devoted to Security, Authentication, and Encryption. This topic was given such treatment because the author perceives that current attitudes show a huge ignorance of what can and can't be done in this area. Computer networks are insecure, and becoming more so. However, many people either seem to be very ignorant of what can be achieved by encryption, or, naively, seem to be ready to put complete trust into encryption techniques. In 1978, Needham and Schroeder showed how, through the use of encryption techniques, two mutually unknown network entities could authenticate themselves, one to the other through the agency of a third, trusted, authentication server. This is independent of "hostile" agents observing all the messages, and inserting, corrupting, or replaying messages. Most people are very surprised by this ability, and it is surprisingly poorly known even 10 years after its first publication. On the other hand, some people put an unquestioning trust in encryption, apparently oblivious of the consistent history of broken cyphers. In addition, the interesting properties of public key encryption, together with their present disappointing position is also presented. Chapter 14 aims to give an up-to-date review of what can and cannot be done in this area.

Finally, Chapter 16 tries to summarise the need for standards, and the processes, political and technical, by which standards are produced and imposed. In addition to discussing the various political bodies that produce standards, Chapter 16 also discusses some of the techniques by which standards are described and analysed. Natural human language is inadequate and leads to ambiguity and misunderstanding, and Chapter 16 indicates some of the improved tools that are beginning to appear.

Throughout the book, the principles are illustrated by examples taken from real computer architectures. The emphasis is always on generally agreed standards, and so the examples come mainly from the ISO and ARPANET suites of protocols. The attempt has been to avoid proprietary architectures wherever possible, and the choice of the ISO and ARPANET suites is for two main reasons. One is that they are publicly and widely available, and the other is that they often have quite different approaches to solving the problems in hand. When different approaches are used on the same problem, then a careful analysis of where differences lie often illuminates the real character of the problem and reveals the principles involved.

A book like this owes much to the efforts of others. Perhaps the most help have been those with whom the author has come into contact

over the long years that he has worked in designing and implementing networks. I have been privileged to encounter many luminaries, and it would be invidious to mention any individually since at least ten times as many would of necessity not be mentioned. However, I hope I may be allowed the indulgence of mentioning just two. I was privileged to know Bob Husak of the Merit Computer Network. Bob had a deep and encyclopaedic knowledge of networks at all levels, and was a good friend. His early death saddened all who knew him. In my undergraduate life as a physicist, Thomas Littlefield taught me how to get a feel for complex physical processes by employing simple mental pictures. It is an approach I have valued ever since.

Directly involved in the production of this book have been Harry Whitfield who fooled me into starting the project in the first place, and pointed out many silly mistakes, Quentin Campbell, Jill Foster, Isi Mitrani, and especially Ian Doak have read various drafts and given suggestions. From CUP, Ernest Kirkwood, Tim Bradshaw, and David Tranah have supported me during the preparation of this book.

I shall not break with the worthy tradition of thanking the typist Denis Russell for typing and revising endless revisions of the manuscript, with only the occasional hint of dissatisfaction with his lot. In addition, he typeset the text using TEX†, produced all the drawings in PostScript‡, and produced camera ready copy. Of course this leaves even less room than normal for the author to disclaim responsibility for errors. More to the point, various tools were used including text editors on several operating systems (even including UNIX§), micros, workstations and mainframes too numerous to mention, and communications systems including most of those described between these covers.

Finally, and most of all, I would like to thank my wife Marion, and the kids for putting up both with me and without me during the excessively protracted gestation period of this book. I can only hope it was worth their efforts.

† TEXis a trademark of the American Mathematical Society
‡ PostScript is a trademark of Adobe Systems Incorporated
§ UNIX is a trademark of Bell Laboratories