Designing efficient IP networks and maintaining them effectively poses a range of challenges, but in this highly competitive industry it is crucial that these are overcome. Weaving together theory and practice, this text sets out the design and management principles of large-scale IP networks and the need for these tasks to be underpinned by actual measurements. Discussions of the types of measurements available in IP networks are included, along with the ways in which they can assist both in the design phase as well as in the monitoring and management of IP applications. Other topics covered include IP network design, traffic engineering, network and service management and security. A valuable resource for graduate students and researchers in electrical and computer engineering and computer science, this is also an excellent reference for network designers and operators in the communication industry.

Antonio Nucci is the Chief Technology Officer at Narus Inc., and he obtained his Ph.D. in Telecommunication from Politecnico di Torino, Italy, in 2003. He was awarded the prestigious Infoworld CTO Top 25 in 2007 for his vision and leadership within Narus and the IT community. His research interests include network design, measurement and management, traffic analysis, security and surveillance.

Konstantina Papagiannaki is Senior Research Scientist at Intel Research, Pittsburgh, Pennsylvania, and received her Ph.D. in Computer Science from University College London, UK, in 2003. Her dissertation work on “Provisioning IP backbone networks based on measurements” was awarded the Distinguished Dissertations Award of the British Computer Society. Her research interests include network design and planning for wired and wireless networks, network measurement and security.
Design, Measurement and Management of Large-Scale IP Networks

Bridging the Gap between Theory and Practice

ANTONIO NUCCI
Narus Inc.

KONSTANTINA PAPAGIANNAKI
Intel Research, Pittsburgh, Pennsylvania
For Konstantina: To my wonderful husband, Richard. For his love and unconditional support, and for always making me try a little harder. To my little Daphne, who came into my world to provide me with a new perspective to life.

For Antonio: To my beautiful wife and best friend, Maria Rosa. For always be there for me, filling up my life with true love and pure joy and striving me toward making my dreams a reality. I love you. To little son, Mattia, who has recently arrived new to our world, now the only world we shall ever dream about. To my parents, Assunta and Vittorio, for all the shelter, care, love and support they have given me over all these years.
In theory, there is no difference between theory and practice; In practice, there is.

– “Yogi” Berra, American baseball player and manager

The figure that appears in the center of the cover describes, in a very cohesive way, properties of an empirical process whose internals are completely unknown but can be studied through the analysis of its behavior under varying probing schemes. The “strip” between the two orange lines represents an admissible region, i.e. support of the process, where samples of the process were observed while changing its inputs. Thus, the strip defines the space where the unknown process resides. The energy of the process is concentrated on horizontal lines departing from the $y$-axis and moving toward the center of the strip. The black area is associated to high energy levels of the process, while the bright yellow area describes low energy levels of the process. The superimposed contour, represented by a set of dashed lines, annotated with different numbers, gives an idea of the probabilities corresponding to the “pixels” of this shading, which are drawn at full screen resolution. Knowing where the density becomes negligible, and under which circumstances, identifies specific characteristics of the unknown process and therefore helps to achieve a better definition and calibration of estimators.
# Contents

<table>
<thead>
<tr>
<th>Acknowledgments</th>
<th>Page xi</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Skeleton of the book</td>
<td>2</td>
</tr>
<tr>
<td>1.2 How to read this book</td>
<td>3</td>
</tr>
<tr>
<td>2 Background and context</td>
<td>5</td>
</tr>
<tr>
<td>2.1 What is the Internet?</td>
<td>5</td>
</tr>
<tr>
<td>2.2 Maintaining end-to-end service</td>
<td>7</td>
</tr>
<tr>
<td>through multiple ISPs: physical and</td>
<td></td>
</tr>
<tr>
<td>logical interconnection agreements and</td>
<td></td>
</tr>
<tr>
<td>the associated financial value</td>
<td></td>
</tr>
<tr>
<td>2.3 Typical Tier-1 ISP network</td>
<td>11</td>
</tr>
<tr>
<td>architecture: the Sprint IP backbone</td>
<td></td>
</tr>
<tr>
<td>2.4 Overview of TCP/IP</td>
<td>15</td>
</tr>
<tr>
<td>2.5 Specifying requirements in managed</td>
<td>20</td>
</tr>
<tr>
<td>IP networks: design and traffic</td>
<td></td>
</tr>
<tr>
<td>engineering, monitoring and security</td>
<td></td>
</tr>
<tr>
<td>operational criteria</td>
<td></td>
</tr>
<tr>
<td>I Network monitoring and management</td>
<td>23</td>
</tr>
<tr>
<td>3 The need for monitoring in ISP</td>
<td>25</td>
</tr>
<tr>
<td>network design and management</td>
<td></td>
</tr>
<tr>
<td>3.1 Current measurement capabilities</td>
<td>26</td>
</tr>
<tr>
<td>3.2 Monitoring the network devices</td>
<td>27</td>
</tr>
<tr>
<td>3.3 Monitoring the state of the routing</td>
<td>29</td>
</tr>
<tr>
<td>protocols</td>
<td></td>
</tr>
<tr>
<td>3.4 Monitoring the traffic flow</td>
<td>31</td>
</tr>
<tr>
<td>3.5 Packet-capture equipment</td>
<td>35</td>
</tr>
<tr>
<td>3.6 The need for measurements in</td>
<td>41</td>
</tr>
<tr>
<td>network operations</td>
<td></td>
</tr>
<tr>
<td>3.7 Summary</td>
<td>46</td>
</tr>
<tr>
<td>4 Understanding through-router delay</td>
<td>47</td>
</tr>
<tr>
<td>4.1 A router under the microscope</td>
<td>48</td>
</tr>
<tr>
<td>4.2 Preliminary delay analysis</td>
<td>53</td>
</tr>
<tr>
<td>4.3 Modeling</td>
<td>58</td>
</tr>
<tr>
<td>4.4 Understanding and reporting delay</td>
<td>66</td>
</tr>
<tr>
<td>performance</td>
<td></td>
</tr>
<tr>
<td>4.5 Micro-congestion episodes and their</td>
<td>74</td>
</tr>
<tr>
<td>causes</td>
<td></td>
</tr>
<tr>
<td>4.6 Lessons learned</td>
<td>84</td>
</tr>
</tbody>
</table>
## Traffic matrices: measurement, inference and modeling

5.1 What is an IP traffic matrix? 86  
5.2 TM estimation from SNMP link counts 94  
5.3 Methods 98  
5.4 Performance analysis 108  
5.5 Lessons learned 121  

## Network design and traffic engineering

6.1 Overview of IP-over-WDM technology 125  
6.2 Network design: principles and processes 128  
6.3 Network design process: sketching out our methodology 134  

7.1 Fault-tolerant logical topology design problem 138  
7.2 Solution strategy 144  
7.3 Mapping between physical and logical topology: GDAP 144  
7.4 Tabu Search for the FLTDP: TabuFLTDP 146  
7.5 Complexity 150  
7.6 Numerical results 150  
7.7 Lessons learned 157  

8.1 Introduction 159  
8.2 The problem: constraints, requirements and objective function 162  
8.3 Formalization of the problem 167  
8.4 Results 173  
8.5 Lessons learned 180  

9.1 Link-weight selection problem 184  
9.2 ILP for general routing problem 185  
9.3 Tabu Search for the IS–IS link weight selection problem: TabuISIS 189  
9.4 Experimental configuration 191  
9.5 Applications 195  
9.6 Lessons learned 199
## Contents

### 10 Measuring the shared fate of IGP engineering: considerations and take-away

10.1 Problem description 202  
10.2 Collection of all required inputs 205  
10.3 Analysis 207  
10.4 Results 208  
10.5 Lessons learned 216

### 11 Capacity planning

11.1 Objectives 219  
11.2 Measurements of inter-PoP aggregate demand 220  
11.3 Multi-timescale analysis 225  
11.4 Time series analysis using the ARIMA model 233  
11.5 Evaluation of forecasts 237  
11.6 Forecasting a dynamic environment 239  
11.7 Lessons learned 246

### III From bits to services

### 12 From bits to services: information is power

12.1 Building intelligence: extracting information from bits 252  
12.2 Bridging the gap between network infrastructure and applications: cleaning the bits 254  
12.3 Summary 259

### 13 Traffic classification in the dark

13.1 State of the art and context 261  
13.2 Background 263  
13.3 Payload-based classification 264  
13.4 Transport-layer classification 269  
13.5 Classification results 281  
13.6 Discussion 286  
13.7 Lessons learned 288

### 14 Classification of multimedia hybrid flows in real time

14.1 Background and data description 293  
14.2 Challenges, intuition and discussion 295  
14.3 VOVClassifier system 300  
14.4 Experimental results 305  
14.5 Lessons learned 309
## Contents

### 15 Detection of data plane malware: DoS and computer worms

15.1 Understanding denial of service 311  
15.2 Understanding worms 314  
15.3 Related work: Worms and DoS 318  
15.4 NBA-DS: logical architecture and network deployment 321  
15.5 Algorithm 323  
15.6 Case study: worm attacks 333  
15.7 Lessons learned 340

### 16 Detection of control-plane anomalies: beyond prefix hijacking

16.1 Brief introduction to the Border Gateway Protocol 343  
16.2 Vulnerabilities, consequences and common practices 345  
16.3 Related work 347  
16.4 Detection system architecture 348  
16.5 Basic detection algorithm 349  
16.6 Refining the detection algorithm 353  
16.7 Experiments 357  
16.8 Lessons learned 365

Appendix A: How to link original and measured flow characteristics when packet sampling is used: bytes, packets and flows 367  
A.1 From original to measured data streams: average number of total flows and their duration 368  
A.2 From measured to original data streams: total number of original bytes and packets 369  
A.3 From measured to original data streams: total number of original TCP flows and their average size 369

Appendix B: Application-specific payload bit strings 371  
B.1 UDP bit strings 371  
B.2 TCP bit strings 372

Appendix C: BLINC implementation details 375

Appendix D: Validation of direction-conforming rule 379

References 382  
Index 393
Acknowledgments

Over the past ten years we have had the fortune and honor of working with so many talented people who have shaped us as scientists and helped us find our position in the applied research community. While it is our names that appear on the cover of this book, claiming the associated responsibility and credit, this book would not have been possible without the discussions and inspiration from a number of colleagues and friends. Although a complete list would be impossible to enumerate, we would like to extend our warmest thanks to our ex-collagues at Sprint, Dr. Christophe Diot, Dr. Nina Taft, Dr. Supratik Bhattacharryya, Dr. Gianluca Iannaccone, Dr. Sue Moon, Richard Gass and Ed Kress. Without Dr. Diot’s enthusiasm and extreme energy, we would never have had the opportunity to study Sprint’s IP network using fine granularity measurements, which are typically impossible to collect, and consequently make this book stand out. It is through our collaboration with Dr. Taft, Dr. Bhattacharryya, Dr. Iannaccone and Dr. Moon, that we managed to address the challenging problems presented throughout the book. Finally, Mr. Gass and Mr. Kress made the instrumentation and management of a vast amount of data possible. Although not part of the Sprint IP group, we would also like to sincerely thank Prof. Lixin Gao for the close feedback she provided during the preparation of the book, reviewing the entire structure and content; we are indebted to her for this time commitment and her comments that certainly improved the quality of this work.

Second, we would like to thank Sprint Corporation for the unfettered access to their network, data and operational personnel. Without their support the work presented in this book would not have been possible. This book comes four years after we decided to pursue a different career path. It is because of the support of our current employers that we managed to complete this project. We sincerely thank Narus Inc. and Intel Corporation for allowing us to spend the time needed to bring this project to completion and for exposing us to a wide range of problems that broadened our horizon with respect to the fundamentals covered in this book.

We also thank Cambridge University Press and the various reviewers that helped in the positioning, polishing and publishing of this book. It is through their encouragement that we managed to overcome any obstacles and succeed in completing this project.

Last, but foremost, we owe our families a huge debt of gratitude for being so patient, while we put their world in a whirl by injecting this lengthy writing activity into their already full lives. Antonio would like to extend a special acknowledgment to his wife Maria Rosa for her encouragement and support and for putting up with his late nights and long weekends. He would also like to thank his parents, Assunta and Vittorio, and
his sister, Milena, who kept him excited and constantly charged for the entire duration of this project. Konstantina, better known as Dina, would like to extend a special acknowledgment to her husband, Richard Gass, for his constant support and for always being there to discuss anything and everything. It is because of him that she always tries to exceed herself, knowing that he will stand by her every decision.