Book Review:

TCP/IP Illustrated, Volume 1
The Protocols, 2nd edition
Kevin R. Fall - W. Richard Stevens
ISBN 0-321-33631-3
Pearson Education, Inc. 2012

TCP/IP Illustrated Vol. 1, first edition has been for decades, "the book" for the IP platform. It is undeniably the wide contribution to the academic, research and professional environments.

Thousands of undergraduate and postgraduate courses have had this book as required reading. It has also been the mandatory reference for the development and implementation of numerous applications under the IP platform.

It stands as the best reference for learning the TCP/IP protocols suite. But…, time goes by; almost two decades have passed since the publication of the first edition and, even the best books concerned with information and communications technology become dated after a time and there is no exception with TCP/IP Illustrated.

For that reason we welcome this second edition. It is not a mere update of the first one. The book presents remarkable novelties in the scope and development of the subjects it covers which deserve a detailed explanation.

First of all it introduces the particularity of the IP protocol elements in two versions numbers, IPv4 and IPv6 together. Normally in most of the books they are presented separately. This is worth bearing in mind if you are planning a course on the subject. The time savings is substantial.

Their contents have been focused on the core protocols, from link level to transport level and auxiliary services like DNS and security. The development of themes keeps the level of detail to which we are accustomed from the first edition and adds greater range covering security issues and possible attacks throughout all them.

The examples and the development of the contents allow obtaining a global vision of an IP-based network such as Internet. It's not often to get this view in traditional texts.

And last but not least, as in the first edition, many packet traces are used to exemplify details of the protocols. In the present edition, tcpdump is used but only when the points to be illustrated are easily covered by examining the output of a text-based packet capture tool. Anyway they are simplified for clarity. The follow up of tcpdump traces is sometimes cumbersome. In the rest of the other cases, screen shots of Wireshark tool are used. The operating systems used for examples include Linux, Windows, FreeBSD, and Mac OS X.

Let’s go now to its contents.

Chapter 1: Gives a general introduction to network protocols, the model of the TCP / IP architecture and standardization process materialized through the RFCs.

Chapter 2: Presents the addressing scheme of TCP/IP, addressing properties, subnetting with masks fixed and VLSM. Complete with multicast addressing and ends with an original approach to security issues in the addressing scheme.

Chapter 3: Given the interaction of IP with the link layer, throughout its operation, this chapter presents the architecture of Ethernet, wired and wirelesses, according to the latest link-level standards available link; ending with encapsulation techniques at the link level.

Chapter 4: Continuing the interaction of IP with other levels and/or protocols presents this auxiliary ARP protocol, with a level of detail to which we are accustomed from the first edition.

Chapters 5-7: Structure of IPv4 and IPv6 datagram and its mobile version. Again we have here evidence of rapid updating. It ends, as in all the other chapters with related security aspects. Once the datagram structure and operation is presented (Ch. 6) it leads to configuration details (DHCP) and management of addresses (NAT), (Ch. 7).

Chapters 8 and 9: Dedicated to ancillary protocols that provide operational support to IP, and provide mechanisms to control the platform (ICMPv4 and v6, IGMP and MLD)

Chapter 10 introduces us to the transport layer of the platform (UDP), with the corresponding structure of UDP and aspects of it implementation and commissioning. In chapter 11 we went to the service level, we presented DNS, since it starts transported by UDP.

Chapters 12 to 17 fully cover TCP with the high level of detail we know from the first edition, particularly with a very good update of the congestion control mechanisms (Ch. 16)

The book ends with Chapter 18 dedicated to security in Internet.

To end this analysis, let me cite Vint Cerf, as he writes in the Foreword of this edition:

“It provides background and a sense for the ways in which solutions to networking problems have evolved. It is relentless in its effort to achieve precision and to expose remaining problem areas. For an engineer determined to refine and secure Internet operation or to explore alternative solutions to persistent problems, the insights provided by this book will be invaluable”

Prof. Luis Marrone
lmarrone@linti.unlp.edu.ar