

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

MPH TECHNOLOGIES OY,
Patent Owner

Case IPR2019-00821
Patent 8,037,302

DECLARATION OF JAMES L. MULLINS, Ph.D.

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

I, James L. Mullins, Ph.D., hereby declare as follows:

I. INTRODUCTION

1. I have personal knowledge of the facts and opinions set forth in this declaration, I believe them to be true, and if called upon to do so, I would testify competently to them. I have been warned that willful false statements and the like are punishable by fine or imprisonment, or both.

2. I am a retired academic librarian working as the founder and owner of the firm Prior Art Documentation Librarian Services, LLC, located at 106 Berrow, Williamsburg, VA 23188. Attached as Exhibit 1015 is a true and correct copy of my Curriculum Vitae describing my background and experience. Further information about my firm, Prior Art Documentation Librarian Services, LLC (PADLS), is available at www.priorartdoclib.com.

3. I have been retained by Sterne, Kessler, Goldstein & Fox P.L.L.C. to investigate the authenticity and dates of public accessibility of certain documents for use in one or more *inter partes* review proceedings. For this service, I am being paid my usual hourly fee. My compensation in no way depends on the substance of my testimony or the outcome of the proceeding.

II. BACKGROUND AND QUALIFICATIONS

4. Since 2018 I have been serving as Dean of Libraries Emeritus and Esther Ellis Norton Professor Emeritus at Purdue University.

5. I was previously employed as follows:

- Dean of Libraries and Professor & Esther Ellis Norton Professor, Purdue University, West Lafayette, IN, 2004-2017.
- Assistant/Associate Director for Administration, Massachusetts Institute of Technology (MIT) Libraries, Cambridge, MA, 2000-2004.
- University Librarian and Director, Falvey Memorial Library, Villanova University, Villanova, PA, 1996-2000.
- Director of Library Services, Indiana University South Bend, South Bend, IN, 1978-1996.
- Part-time instructor, School of Library and Information Science, Indiana University, Bloomington, IN, 1977-1996.
- Associate Law Librarian, and associated titles, Indiana University School of Law, Bloomington, IN, 1974-1978.
- Catalog Librarian, Assistant Professor, Georgia Southern College (now University), Statesboro, GA, 1973-1974.

6. Over the course of my career as a librarian, instructor of library science, author of scholarly publications, and presenter at national and international conferences, I have had experience with catalog records and online library management systems built around Machine-Readable Cataloging (MARC) standards.

7. In the course of more than forty-four years as an academic librarian and scholar, I have been an active researcher. In my years as a librarian I have facilitated the research of faculty colleagues either directly or through providing and granting access to requisite print and/or digital materials and services at the universities where I worked. I have kept current on the professional library science literature and served on the editorial board of the most prominent library journal, *College and Research Libraries*. This followed service as the chair of the Research Committee of the Association of College and Research Libraries (ACRL), a division of the American Library Association (ALA). As an academic library administrator, I have had the responsibility of ensuring students were educated on identifying, locating, assessing, and integrating information garnered from library resources.

III. PRELIMINARIES

8. I am not a lawyer and I am not rendering an opinion on the legal question of whether a particular document is, or is not, a “printed publication” under the law.

9. I am, however, rendering my expert opinion on the authenticity of the documents referenced herein and on when and how these documents were disseminated or otherwise made available to the extent that persons interested and

ordinarily skilled in the subject matter or art, exercising reasonable diligence, could have located the documents in the late 1990s.

10. I understand that an item is considered authentic if there is sufficient evidence to support a finding that the item is what it is claimed to be. I am also informed that authenticity can be established based on the contents of the documents themselves, such as the appearance, content, substance, internal patterns, or other distinctive characteristics of the item, taken together with all of the circumstances.

11. I understand that a printed publication qualifies as publicly accessible as of the date it was disseminated or otherwise made available such that a person interested in and ordinarily skilled in the relevant subject matter could locate it through the exercise of reasonable diligence.

12. While I understand that the determination of public accessibility under the foregoing standard rests on a case-by-case analysis of the facts particular to an individual publication, I also understand that a printed publication is rendered “publicly accessible” if it is cataloged and indexed by a library such that a person interested in the relevant subject matter could locate it (*i.e.*, cataloging and indexing by a library is sufficient, though there are other ways that a printed publication may qualify as publicly accessible). One manner of customary indexing is indexing according to subject matter category. I understand that, even

if access to a library is restricted, a printed publication that has been cataloged and indexed therein is publicly accessible so long as the portion of the public concerned with the relevant subject matter would know of the printed publication. I also understand that the cataloging and indexing of information that would guide a person interested in the relevant subject matter to the printed publication, such as the cataloging and indexing of an abstract for the printed publication, is sufficient to render the printed publication publicly accessible.

13. I also understand that routine business practices, such as general library cataloging and indexing practices, can be used to establish an approximate date on which a printed publication became publicly accessible.

A. MATERIALS CONSIDERED

14. In forming the opinions expressed in this declaration, I have reviewed the documents and appendices referenced herein. These materials are records created in the ordinary course of business by publishers, libraries, indexing services, and others. From my years of experience, I am familiar with the process for creating many of these records, and I know that these records are created by people with knowledge of the information contained in the record. Further, these records are created with the expectation that researchers and other members of the public will use them. All materials cited in this declaration and its appendices are

of a type that experts in my field would reasonably rely upon and refer to in forming their opinions.

B. PERSONS OF ORDINARY SKILL IN THE ART

15. I am told by counsel that the subject matter of this proceeding relates to secure forwarding of messages in a telecommunications network.

16. I understand that a “person of ordinary skill in the art at the time of the inventions” is a hypothetical person who is presumed to be familiar with the relevant field and its literature at the time of the inventions. This hypothetical person is also a person of ordinary creativity, capable of understanding the scientific principles applicable to the pertinent field.

17. I have been informed by counsel that persons of ordinary skill in this subject matter or art would have had at least a bachelor’s (B.S.) degree in Computer Science, Computer Engineering, Electrical Engineering, or an equivalent field, as well as at least 2-5 years of academic or industry experience in the field of Internet security.

18. In 2002 and 2003, such a person would have had access to a vast array of print resources regarding secure network communications, access to reference librarians (e.g., at universities), and access to a fast-changing set of online resources.

C. LIBRARY CATALOG RECORDS

19. Some background on MARC (“Machine-Readable Cataloging”) formatted records, Online Computer Library Center, Inc. (“OCLC”), and WorldCat is helpful to understand the library catalog records discussed in this declaration. I am fully familiar with the library cataloging standard known as the MARC standard, which is an industry-wide standard method of storing and organizing library catalog information.¹ MARC practices have been consistent since the MARC format was developed by the Library of Congress in the 1960s, and by the early 1970s they became the U.S. national standard for disseminating bibliographic data. By the mid-1970s, MARC format became the international standard, and this preeminence persists through the present. A MARC-compatible library is one that has a catalog consisting of individual MARC records for each of its items. Today, MARC is the primary communications protocol for the transfer and storage of bibliographic metadata in libraries.² The MARC practices discussed below were in place during the 1998 timeframe relevant to the documents referenced herein.

¹ The full text of the standard is available from the Library of Congress at <http://www.loc.gov/marc/bibliographic/> (Attachment 1F) (last visited March 23, 2019).

² Almost every major library in the world is MARC-compatible. *See, e.g., MARC Frequently Asked Questions (FAQ)*, LIBRARY OF CONGRESS,

20. Similarly, OCLC practices have been consistent since the 1970s through the present, and the OCLC practices discussed below were in place during the 1998 timeframe relevant to the documents referenced herein. The OCLC was created “to establish, maintain, and operate a computerized library network and to promote the evolution of library use, of libraries themselves, and of librarianship, and to provide processes and products for the benefit of library users and libraries, including such objectives as increasing availability of library resources to individual library patrons and reducing the rate of rise of library per-unit costs, all for the fundamental public purpose of furthering ease of access to and use of the ever-expanding body of worldwide scientific, literary, and educational knowledge and information.”³ Among other services, OCLC and its members are responsible

<https://www.loc.gov/marc/faq.html> (Attachment 1G) (last visited March 23, 2019)

(“MARC is the acronym for MACHine-Readable Cataloging. It defines a data format that emerged from a Library of Congress-led initiative that began nearly forty years ago. It provides the mechanism by which computers exchange, use, and interpret bibliographic information, and its data elements make up the foundation of most library catalogs used today.”). MARC is the ANSI/NISO Z39.2-1994 (reaffirmed 2009) standard for Information Interchange Format.

³ Third Article, Amended Articles of Incorporation of OCLC Online Computer Library Center, Incorporated (last visited March 23, 2019 and available at

for maintaining the WorldCat database (<http://www.worldcat.org/>), used by independent and institutional libraries throughout the world.

21. Libraries worldwide used the machine-readable MARC (Machine-Readable Cataloging) format for catalog records. MARC formatted records have provided a variety of subject access points based on the content of the document being cataloged. A MARC record comprises several fields each of which contains specific data about the work. Each field is identified by a standardized, unique, three-digit code corresponding to the type of data that follows. For example, MARC Field 610 identifies corporate names used as subjects and MARC Field 650 identifies topical terms. A researcher could discover material relevant to his or her topic by a search using the terms employed in the MARC Fields 6XX; work's title is recorded in field 245, the primary author of the work is recorded in field 100, an item's International Standard Book Number ("ISBN") is recorded in field 020, an item's Library of Congress call number is recorded in field 050, and the publication date is recorded in field 260 under the subfield "c." If a work is a periodical, then its publication frequency is recorded in field 310, and the publication dates (e.g., the first and last publication) are recorded in field 362, which is also referred to as the enumeration/chronology field.

<https://www.oclc.org/content/dam/oclc/membership/articles-of-incorporation.pdf>

(Attachment 1H)

22. The MARC Field 040, subfield “a,” identifies the library or other entity that created the original catalog record for a given document and transcribed it into machine-readable form. The MARC Field 008 identifies the date when this first catalog record was entered on the file. This date persists in subsequent uses of the first catalog record, although newly-created records for the same document, separate from the original record, will show a new date.

23. MARC records also include several fields that include subject matter classification information. An overview of MARC record fields is available through the Library of Congress at <http://www.loc.gov/marc/bibliographic/>. For example, 6XX fields are termed “Subject Access Fields.”⁴ Among these, for example, is the 650 field; this is the “Subject Added Entry – Topical Term” field. *See* <http://www.loc.gov/marc/bibliographic/bd650.html>. The 650 field is a “[s]ubject added entry in which the entry element is a topical term.” *Id.* These entries “are assigned to a bibliographic record to provide access according to generally accepted thesaurus-building rules (e.g., Library of Congress Subject Headings (LCSH), Medical Subject Headings (MeSH)).” *Id.* Thus, a researcher might discover material relevant to his or her topic by a search using the terms employed in the MARC Fields 6XX.

⁴ *See* <http://www.loc.gov/marc/bibliographic/bd6xx.html>. (Attachment 1I) (visited March 23, 2019)

24. The 9XX fields are not part of the standard MARC 21 format.⁵ OCLC has defined the following 9XX fields for use by the Library of Congress and for internal OCLC use: 936, 938, 956, 987, 989, and 994. 955 is used by the Library of Congress to track the progress of a new acquisition from the time it is submitted for Cataloging in Publication (CIP) review until it is published, fully cataloged, and available for use within the Library of Congress. Fields 901-907, 910, and 945-949 have been defined by OCLC for local use and will pass OCLC validation. Fields 905 or 910 are often used by an individual library for internal processing purposes, for the date of cataloging and the initials of the cataloger, for example.

25. Further, MARC records include call numbers, which themselves include a classification number. For example, the 050 field is the “Library of Congress Call Number.”⁶ A defined portion of the Library of Congress Call Number is the classification number.⁷ Thus, included in the 050 field is a subject matter classification. Each item in a library has a single classification number. A

⁵ See <https://www.oclc.org/bibformats/en/9xx.html>. (Attachment 1J) (visited March 23, 2019)

⁶ See <http://www.loc.gov/marc/bibliographic/bd050.html>. (Attachment 1K) (Visited March 23, 2019)

⁷ See <https://www.loc.gov/aba/publications/FreeLCC/freelcc.html#About> (Attachment 1L)

library selects a classification scheme (e.g., the Library of Congress Classification scheme just described or a similar scheme such as the Dewey Decimal Classification scheme) and uses it consistently. When the Library of Congress assigns the classification number, it appears as part of the 050 field. If a local library assigns the classification number, it appears in a 090 field. In either scenario, the MARC record includes a classification number that represents a subject matter classification.

26. WorldCat is the world's largest public online catalog, maintained by the Online Computer Library Center, Inc., or OCLC, and built with the records created by the thousands of libraries that are members of OCLC. OCLC has provided bibliographic and abstract information to the public based on MARC records through its OCLC WorldCat database. WorldCat requires no knowledge of MARC tags and codes, and does not require a log-in or password. WorldCat is easily accessible through the World Wide Web to all who wish to search it; there are no restrictions to become a member of a particular community, etc. The date a given catalog record was created (corresponding to the MARC Field 008) appears in some detailed WorldCat records as the Date of Entry, but not necessarily in all records. Whereas WorldCat records are widely available, the availability of MARC formatted records varies from library to library and when made available will be identified as MARC record or librarian/staff view.

27. When an OCLC member institution acquires a work, it creates a MARC record for this work in its computer catalog system as part of the ordinary course of its business. MARC records created at the Library of Congress have historically been tape-loaded daily or weekly into the OCLC database through a subscription to MARC Distribution Services. Once the MARC record is created by a cataloger at an OCLC member institution or is tape-loaded from the Library of Congress, the MARC record is then made available to any other OCLC members online, and therefore made available to the public. Accordingly, once the MARC record is created by a cataloger at an OCLC member institution or is tape-loaded from the Library of Congress or another library anywhere in the world, any publication corresponding to the MARC record has been cataloged and indexed according to its subject matter such that a person interested in that subject matter could, with reasonable diligence, locate and access the publication through any library with access to the OCLC WorldCat database or through the Library of Congress.

28. When an OCLC member institution creates a new MARC record, OCLC automatically supplies the date of creation for that record. The date of creation for the MARC record appears in the fixed field (008), characters 00 through 05. The MARC record creation date reflects the date on which the item was first acquired or cataloged. Initially, field 005 of the MARC record is

automatically populated with the date the MARC record was created in year, month, day format (YYYYMMDD) (some of the newer library catalog systems also include hour, minute, second (HHMMSS)). Thereafter, the library's computer system may automatically update the date in field 005 every time the library updates the MARC record (e.g., to reflect that an item has been moved to a different shelving location within the library).

29. Once one library has cataloged and indexed a publication by creating a MARC record for that publication, other libraries that receive the publication do not create additional MARC records—the other libraries instead rely on the original MARC record. They may update or revise the MARC record to ensure accuracy, but they do not replace or duplicate it. This practice does more than save libraries from duplicating labor. It also enhances the accuracy of MARC records. Further, it allows librarians around the world to know that a particular MARC record is authoritative (in contrast, a hypothetical system wherein duplicative records were created would result in confusion as to which record is authoritative).

30. The date of creation of the MARC record by a cataloger at an OCLC member institution reflects when the underlying item is accessible to the public. Upwards of two-thirds to three-quarters of book sales to libraries come from a jobber or wholesaler for online and print resources. These resellers make it their business to provide books to their customers as fast as possible, often providing

turnaround times of only a single day after publication. Libraries purchase a significant portion of their books directly from publishers themselves, which provide delivery on a similarly expedited schedule. In general, libraries make these purchases throughout the year as the books are published and shelve the books as soon thereafter as possible in order to make the books available to their patrons. Thus, books are generally available at libraries across the country within just a few weeks of publication.

D. PERIODICAL PUBLICATIONS

31. A library typically creates a catalog record for a periodical publication when the library receives its first issue. When the institution receives subsequent issues/volumes of the periodical, the issues/volumes are checked in (often using a date stamp), added to the institution's holding records, and made available very soon thereafter – normally within a few days of receipt or (at most) within a few weeks of receipt.

32. The initial periodicals record will sometimes not reflect all subsequent changes in publication details (including minor variations in title, etc.).

E. PUBLICATIONS IN SERIES: CONFERENCE PROCEEDINGS/TECHNICAL REPORT PUBLICATIONS

33. A library typically creates a MARC catalog record for a series of closely related publications, such as the proceedings of an annual conference or a technical report, when the library receives its first issue and assumes there will be

annual or succeeding issues/volumes/reports. When the institution receives subsequent issues/volumes/reports of the series, the issues/volumes/reports are checked in (sometimes using a date stamp), added to the institution's holdings records, and made available very soon thereafter—normally within a few days of receipt or (at most) within a few weeks of receipt. The initial series record may not reflect all subsequent changes in publication details (including minor variations in title, etc.).

F. OWNERSHIP AND DATE STAMP

34. Every library sets its own practice or policy on whether or not to date stamp, but all will have an ownership stamp somewhere in the publication—typically on the cover page, verso of the cover page, or a designated page within the publication, sometimes even on the top, side, or bottom edge of the monograph or periodical. The timing of the ownership and date stamp can also vary from one library to another. The stamp can occur when the monograph or periodical is received in acquisitions after shipment to the library, or it can be at time of cataloging. Therefore, there could be instances when the date of receipt precedes the cataloging date.

G. INDEXING

35. A researcher may discover material relevant to his or her topic in a variety of ways. One common means of discovery is to search for relevant

information in an index of periodical and other publications. Having found relevant material, the researcher will then normally obtain it online, look for it in libraries, or purchase it from the publisher, a bookstore, a document delivery service, or other provider. Sometimes, the date of a document's public accessibility will involve both indexing and library date information. Date information for indexing entries is, however, often unavailable. This is especially true for online indices.

36. Indexing services use a wide variety of controlled vocabularies to provide subject access and other means of discovering the content of documents. The formats in which these access terms are presented vary from service to service.

37. Online indexing services commonly provide bibliographic information, abstracts, and full-text copies of the indexed publications, along with a list of the documents cited in the indexed publication. These services also often provide lists of publications that cite a given document. A citation of a document is evidence that the document was publicly available and in use by researchers no later than the publication date of the citing document.

38. One such indexing service is SpringerLink, which provides researchers with access to millions of scientific documents from journals, books, series, protocols, reference works, and proceedings.⁸

⁸ <https://link.springer.com/> (Attachment 1M) (Last visited March 23, 2019)

IV. OPINION REGARDING AUTHENTICITY AND PUBLIC ACCESSIBILITY

- A. Vipul Gupta, *et al.*, “Complete Computing”. Worldwide Computing and Its Applications – WWCA’98. Second International Conference, Tsukua, Japan, March 4-5, 1998. Proceedings: 174-189. Yoshifumi Masunaga, *et al.*, editors. Lecture Notes in Computer Science, 1368. Springer-Verlag. (Gupta)**

1. Authentication

39. As described above, Gupta is an article by Vipul Gupta, *et al.*, titled “Complete Computing” published by Springer-Verlag in Worldwide Computing and Its Applications – WWCA’98, Second International Conference, Tsukua, Japan, March 4-5, 1998, Proceedings, pages 174-189, published by Springer-Verlag.

40. Attachment 1A is a scan provided to me, at my request, on February 8, 2019 by the Wisconsin TechSearch (WTS) from Cornell University Libraries. Attachment 1A includes scans of the front cover; the inside flyleaf to the back cover with the stamp of the Cornell University Libraries’ Engineering Library, the stamp having a date of July 21, 1998; the title page with Cornell University Library inventory bar code; the verso of the title page (copyright page) with ownership stamp plus handwritten in pencil the call number QA75.5 .W18x, 1998; the Table of Contents; and the Gupta article.

41. Attachment 1B, Gupta, is also available digitally within SpringerLink: <https://link-springer-com.ezproxy.lib.purdue.edu/chapter/10.1007/3-540-64216->

1_48. Attachment 1B is a download from SpringerLink I made on February 17, 2019 through Purdue University Libraries. Paid access is available to Gupta through: https://link.springer.com/chapter/10.1007/3-540-64216-1_48.

42. After comparing Attachment 1A and Attachment 1B, I saw no difference between the two. Having retrieved Attachment 1A and Attachment 1B on my own from reliable sources, a research library (Cornell University Libraries) and a research database (SpringerLink), which I and other librarians regularly use, I determined that Gupta is an authentic document and reflects a true and accurate copy of Gupta.

2. Public Accessibility

43. Attachment 1A, received from Wisconsin TechSearch at my request, includes a Cornell University Libraries ownership and date stamp of July 21, 1998. Based on my experience, I affirm this ownership stamp has the general appearance of ownership stamps that libraries have long affixed to items during processing. I do not see any indications or have any reason to believe this ownership label was made by anyone other than library personnel.

44. As described above, WorldCat is the world's largest public online catalog. WorldCat is maintained by OCLC and is comprised of records created by thousands of libraries that are members of OCLC. The WorldCat record would have been available soon after the date in the MARC 008 field, which for this

record would have been February 13, 1998. WorldCat provides a user-friendly interface for the public to use MARC records and requires no knowledge of MARC tags and codes to effectively search for references. WorldCat is easily accessible through the internet to all who wish to search it and there are no restrictions to a user's ability to search for references within a particular field.

45. Attachment 1C is a download from WorldCat for the Worldwide Computing and Its Applications – WWCA'98: Second International Conference publication. As I discuss above, WorldCat provides unmediated online access to bibliographic information to the public. Worldwide Computing and Its Applications – WWCA'98: Second International Conference could have been located on WorldCat by title; by editor, Y Masunaga; by series, Lecture Notes in Computer Science; and by subject: Electronic data processing – Congresses. The searches discussed above could have been performed anywhere in the world by anyone who accessed WorldCat or its predecessor First Search. Among the 301 libraries identified as holding Worldwide Computing and Its Applications – the WWCA'98 is Cornell University Library.

46. Attachment 1D is a download I made on February 13, 2019 from the Cornell University Libraries OPAC (online catalog). As I have experienced during my professional career, it was typical for a research library's online catalog to make the document/book accessible when it was cataloged, in this instance, June

24, 1998. A researcher could have located *Worldwide Computing and Its Applications – WWCA’98* by title; editor, Masunaga, Y. (Yoshifumi); and by subject, *Electronic data processing – Congresses*. It was shelved under the call number QA75.5 .W18x 1998.

47. Attachment 1E is the MARC record for *Worldwide Computing and Its Applications – WWCA’98* as retrieved from Cornell University Libraries OPAC. Cornell University Libraries has designated the 905 field (see 9XX field description above) to indicate date of cataloging. The 905 field in this record reads:

905#a 19980624120000.0

48. 905 Subfield: “a 19980624...” indicates it was cataloged on June 24, 1998. This would be consistent with the date stamped on the book, July 21, 1998, since it would take time for labeling and for transport to the Engineering Library. Document 1 would have been accessible to the public no later than end of July 1998.

3. Conclusion

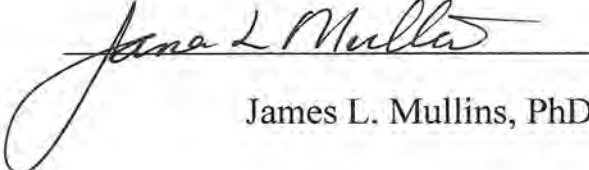
49. Based on the evidence presented here—publication in the widely held publication, online indexing, and library processing and cataloging—it is my opinion that Gupta is an authentic document and was publicly accessible no later than the end of July 1998.

V. CONCLUSION

50. I reserve the right to supplement my opinions in the future to respond to any arguments that Patent Owner or its expert(s) may raise and to take into account new information as it becomes available to me.

51. I declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

52. Executed this 25th day of March 2019 in Williamsburg, Virginia.



James L. Mullins, PhD

ATTACHMENT 1A

Lecture Notes in
Computer Science

CORNELL UNIVERSITY LIBRARY



3 1924 083 794 184

1368

Yoshifumi Masunaga Takuya Katayama
Michiharu Tsukamoto (Eds.)

Worldwide Computing
and Its Applications –
WWCA '98

Second International Conference
Tsukuba, Japan, March 1998
Proceedings



Springer

Yoshifumi Masunaga Takuya Katayama
Michiharu Tsukamoto (Eds.)

CORNELL UNIVERSITY LIBRARY



3 1924 083 794 184

Worldwide Computing and Its Applications – WWCA'98

Second International Conference
Tsukuba, Japan, March 4-5, 1998
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Yoshifumi Masunaga
University of Library and Information Science
1-2 Kasuga, Tsukuba, Ibaraki 3050821, Japan
E-mail: masunaga@ulis.ac.jp



ENGR
QA
75
.5
W18
1998

Takuya Katayama
Japan Advanced Institute of Science and Technology
1-1 Asahidai, Nomigun, Tatsunokuchimachi, Ishikawa 9231292, Japan
E-mail: katayama@jaist.ac.jp

Michiharu Tsukamoto
Electrotechnical Laboratory
1-1-4 Umezono, Tsukuba, Ibaraki 3050045, Japan
E-mail: Tukamoto@etl.go.jp

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Worldwide computing and its applications : second international conference ;
proceedings / WWCA '98, Tsukuba, Japan, March 1998. Yoshifumi Masunaga ;
Takuya Katayama (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest
; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo :
Springer, 1998
(Lecture notes in computer science ; Vol. 1368)
ISBN 3-540-64216-1

CR Subject Classification (1991): C.2.4, D.1.3, F.1.2, C.2, D.4, D.3, H.5

ISSN 0302-9743

ISBN 3-540-64216-1 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1998
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10631853 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Table of Contents

WWC and the Hyper Information Age	1
<i>Koichiro Tamura</i>	

Keynotes

Co-Chairs: Hideo Aiso, Masayuki Ida, Takuya Katayama

Global High Performance Research Network: An Asia-Pacific Perspective	6
<i>Kilnam Chon</i>	

Java Applications and Implementations	18
<i>Guy L. Steele Jr.</i>	

Back to Home: Where Computers and Networking Should Go	32
<i>Mario Tokoro</i>	

Session A-1: Distributed Objects

Chair: Kazuhiko Kato

ObjectSpace Voyager - The Agent ORB for Java	38
<i>Graham Glass</i>	

Worldwide Component Scripting with the Planet Mobile Object System	56
<i>Katsuya Matsubara, Takahiro Maekawa, Kazuhiko Kato</i>	

Scalability in Object-Oriented Distributed Systems Environment OZ	72
<i>Akihito Nakamura, Toshihiro Nishioka, Yoichi Hamazaki, Michiharu Tsukamoto</i>	

Session A-2: Distributed Componentware

Chair: Mikio Aoyama

Rapide: A Language and Toolset for Causal Event Modeling of Distributed System Architectures	88
<i>David C. Luckham</i>	

An Architecture of Software Commerce Broker over the Internet	97
<i>Mikio Aoyama, Toshio Yamashita, Shinsuke Kobori</i>	

Distributed Process Management System Based on Object-Centered Process Modeling	108
<i>Makoto Matsushita, Makoto Oshita, Hajimu Iida, Katsuro Inoue</i>	
Session B-1: Distributed Systems Platform	
<i>Chair: Hideyuki Tokuda</i>	
Systems Software for Multimedia Computing	120
<i>Ragunathan Rajkumar</i>	
Environment Server: A System Support for Adaptive Distributed Applications	142
<i>Tatsuo Nakajima, Hiroyuki Aizu, Masaru Kobayashi, Kenji Shimamoto</i>	
Compiler-Generated Protection Domains and a Light Weight Runtime Protection Technique	158
<i>Yo Furukawa, Etsuya Shibayama</i>	
Session B-2: Internet Technology	
<i>Chair: Jun Murai</i>	
Complete Computing	174
<i>Vipul Gupta, Gabriel Montenegro, Jeff Rulifson</i>	
Compact and Flexible Resolution of CBT Multicast Key-Distribution	190
<i>Kanta Matsuura, Yuliang Zheng, Hideki Imai</i>	
Integrating Resource Reservation with Rate-Based Transport Protocols in AMInet	206
<i>Atsushi Shionozaki, Kei Yamashita, Shusuke Utsumi, Kenjiro Cho</i>	
Session B-3: Mobile Computing	
<i>Chair: Fumio Teraoka</i>	
Experiences with a Mobile Testbed	222
<i>Kevin Lai, Mema Roussopoulos, Diane Tang, Xinhua Zhao, Mary Baker</i>	

Design and Implementation of Mobile IP System with Security Consideration.....	263
<i>Masahiro Ishiyama, Atsushi Inoue, Atsushi Fukumoto, Toshio Okamoto</i>	
A Network Architecture for Continuous Mobility.....	269
<i>Keisuke Uehara, Takamichi Tateoka, Yasuhito Watanabe, Hideki Sunahara, Osamu Nakamura, Jun Murai</i>	
Session B-4: Interculture Technology	
<i>Chair: Tan Tin-Wee</i>	
Towards Internationalized Web Creation.....	270
<i>Kok Yong Leong , Hai Liu, Oliver Wu</i>	
ISCM, Information System Conceptual Model Oriented to Security Problems and a Tool Implementing It.....	282
<i>Pierluca De Maria, Cristiano De Mei</i>	
Design of EDI Security MIB Based on SNMP Protocol.....	293
<i>Tae-Kyou Park</i>	
Session C-1: Collaborative Media	
<i>Chair: Yasushi Kiyoki</i>	
The Block-World Data Model for a Collaborative Virtual Environment.....	309
<i>Yoshifumi Masunaga</i>	
CyPhone – Mobile Multimodal Personal Augmented Reality.....	325
<i>Petri Pulli, Tino Pyssysalo, Kari Kuutti, Jouni Similä, Jukka-Pekka Metsävainio, Olli Komulainen</i>	
On Business Intelligence Systems.....	337
<i>Won Kim</i>	
Session C-2: Collaboration Support	
<i>Chair: Ken-ichi Okada</i>	
Supporting Collaboration through Teleproximity.....	349
<i>John C.Tang</i>	

A Home Office System Based on a Virtual Shared Room: An Environment Corresponding to Degree of Concentration	364
<i>Shinkuro Honda, Ken-ichi Okada, Yutaka Matsushita</i>	
Electronic Binder System: Promotion of an ISO9001-Based Quality System Using the WWW and Experience from Its Application.....	381
<i>Atsuo Hazeyama, Miho Hanawa</i>	
Session C-3: Information Discovery and Retrieval	
<i>Chair: Isao Kojima</i>	
Update Monitoring: The CQ Project.....	396
<i>Calton Pu, Ling Liu</i>	
dLIMIT - A Middleware Framework for Loosely-Coupled Database Federations.....	412
<i>Henrik Loeser, Theo Haerder</i>	
Autonomic Buffer Control of Web Proxy Server.....	428
<i>Yu Guo, Yukio Hiranaka, Takao Akatsuka</i>	
Session C-4: Novel Network Application	
<i>Chair: Shigeki Goto</i>	
Getting Users' Attributes Without Violating Anonymity.....	439
<i>Tsutomu Matsumoto</i>	
Bayanihan: Web-Based Volunteer Computing Using Java.....	444
<i>Luis F. G. Sarmenta</i>	
Architecture of a User Interface Module for Structured Internet Messages	462
<i>Tomohiko Morioka</i>	
Author Index.....	473

Complete Computing *

Vipul Gupta, Gabriel Montenegro and Jeff Rulifson

Technology Development Group
Sun Microsystems, Inc.
901 San Antonio Road, MS UMPK15-214
Palo Alto, California 94303
Email: {vgupta, gab, jeffr}@eng.sun.com

Abstract. Our objective is to enable nomadic and mobile computing, as well as telecommuting, small-office, and branch-office computing. These areas have been dealt with extensively in the literature. However, they have been treated as separate problem spaces and current solutions focus on solving specific problems in one area while ignoring – or even exacerbating – those in another area. These problem spaces must be viewed as being closely related, and must be addressed in a coherent fashion. We call this unified vision and architecture *Complete Computing*.

1 Vision

As people navigate or relocate throughout the ocean of information that surrounds them (Figure 1), they wish to maintain logical availability of some subset of their computing environment. We use the term computing environment to include both a user's applications (*e.g.* document editor) and data (*e.g.* files, mail, *etc.*). Maintaining this logical availability may require a combination of several mechanisms including caching, replication, redirection, repackaging or even prediction.

A mobile client is able to connect using a variety of schemes (serial, LAN, wireless, WAN, through firewalls [5], *etc.*) and is adept at operating in disconnected mode. This flexibility gives its user the illusion that information is always close at hand, and that it follows him or her and presents itself for consumption independently of the client's physical or logical location. An important corollary is that this network model supports both user and terminal mobility, because the objective is for the information to be available to the user at all times – though perhaps in varying degrees depending on prevalent networking and environmental conditions.

In this paper, the term *Mobile Computing* represents the ambitious objective of retaining a user's static computing environment (including all existing connections), even while the user and his portable device are moving. It attempts to

* This work was partly funded by the Ministry of International Trade and Industry of Japan through the *Advanced Software Enrichment Project* of the Information Technology Promotion Agency.

shield the user from the effects of physical or topological movement throughout the networking fabric.

In some instances, preserving a user's computing environment during movement may not be necessary. Instead it may be sufficient to ensure that the user's computing environment can be recreated wherever the user moves. This may require re-initiating network connections and/or reestablishing session state. We use the term *Nomadic Computing* for these situations.

Remote Computing or *Branch Office Computing* have similar requirements to the previous two, in that they involve access to a user's private computing environment (e.g. firewall-protected corporate resources) across a potentially hostile – or at least untrusted – public network. Nevertheless, the static – hence, stable – nature of this kind of computing translates into better resource availability and richer services.

Finally, *Small-Office/Home-Office Computing* assumes there are no private user environments beyond those available locally. The objective is to enable small, independent work groups. Since they do not belong to a parent organization, they lack assistance from system administrators and technical support personnel. Therefore, ease of use is of utmost importance. However, there is still a need for rich networking and application support.

The diverse areas mentioned above have been dealt with extensively in the literature but not as a cohesive whole. Our objective is to enable all of these forms of computing using a common set of tools and solutions. We call this unified vision and architecture *Complete Computing*.

By designing similar mechanisms for all these areas, we wish to prevent further fragmentation of proposed solutions. Our vision of complete computing has technology implications in several areas: hardware and software platforms, data persistence, caching and synchronization, configuration and management, applications, services, networking, and security.

In this paper we focus primarily on networking and the concomitant security issues. We identify the outstanding technical challenges, review proposed solutions, and discuss their applicability in different situations.

2 Elements of a Solution

For the following discussion, a mobile user is one who needs to access information and applications "on the road", i.e. from different locations (or even while changing locations) and under varying conditions. Access may be read-only or read-write and the access device may be personal (e.g. a portable, personal notebook or PDA) or communal (e.g. a kiosk at an airport).

2.1 Challenges of Mobility

Mobility imposes certain fundamental constraints which affect all aspects of computing.

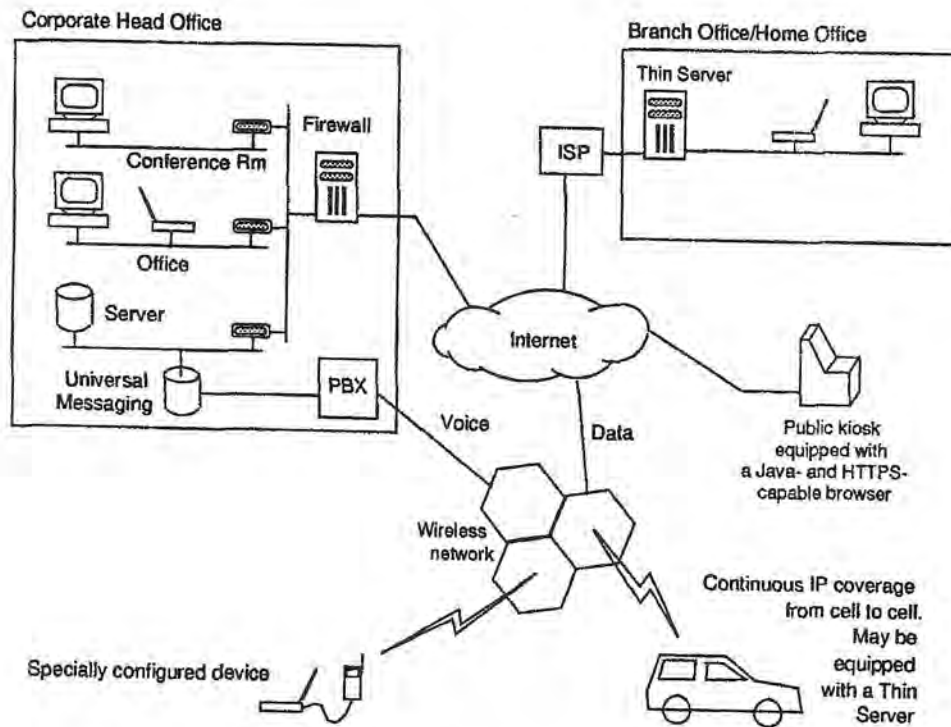


Fig. 1. An overview of the Complete Computing environment

1. Portable devices, as compared to their stationary counterparts, are "resource poor" (e.g. less powerful CPU, fewer I/O devices, smaller screen), and must manage their resources carefully. Power management is critical for battery-operated devices. Screen size and keyboard (or lack thereof) may influence the user interface.
2. Network characteristics like bandwidth and latency fluctuate widely. Therefore, mobile systems must deal with communication uncertainty – including complete disconnection – and adapt gracefully to these and other changes.
3. Mobility requires different forms of security.
 - (a) *Network Security.* Traffic may at times pass through links with questionable security characteristics. New alternatives may be required for some traditional security mechanisms that use location information to distinguish between authorized and unauthorized users. As an example, many packet-filtering firewalls disallow certain kinds of traffic if it arrives on an interface facing the general Internet. Such firewalls may need to be enhanced with strong cryptographic mechanisms so legitimate traffic from authorized mobile users is allowed irrespective of the interface.
 - (b) *Data and Device Security.* As opposed to large, stationary devices safely locked up in an office, lightweight, portable devices are frequently used in public places. Hence, they are prone to being destroyed, lost or stolen. Consequently, encryption and secure backups are used to prevent subversion or loss of data.

2.2 Agile Networking

In today's fast-paced information society, it is inconceivable to think that a mobile user can always carry all the information he needs on the local storage of his personal computing device. Typically, the information of interest will be distributed across a multitude of other hosts connected to a network. This immediately highlights the need for a mobile user to attach to a network, establish a communication path to the desired server and exchange information under a variety of conditions.

Consider a salesperson who, over the course of a few hours, uses a portable notebook in different networking modes — wireline LAN at his office, a different wireline LAN in a conference room, wireless LAN at the company cafeteria, wireless WAN at the airport, and a POTS modem connection at a hotel. Typically, each situation requires reconfiguration of the device. These configuration parameters may include IP address, network mask, default router, DNS server name, local printer, etc. In an ideal situation, most (if not all) of the necessary changes would be transparent to the end user and occur with minimal disruption. Newer protocols like DHCP [7], Mobile IP [21] and SLP [24] hold great promise for solving this challenge.

2.3 Disconnected Operation

Of course, there will be periods when a mobile user may not have access to any network or the cost of connecting to a network may be prohibitively high (as in an airplane). Support for disconnected operation is imperative for such situations. The user should be able to cache applications and data² in his current "working set" onto local, non-volatile storage and, at a later point, reconcile any changes made locally against other copies on the network. While a number of research groups have made encouraging progress in this particular area [16], mature industry-wide standards are still lacking.

2.4 Adaptivity

We anticipate the development of several classes of mobile computing devices differing in their CPU power, display size, screen resolution, input devices etc. While these characteristics do not change during the lifetime of a device, others such as network bandwidth and latency, remaining battery power, and available storage are more dynamic and applications could benefit from adapting to such changes. A web browser could turn off automatic downloading of in-line images when available network bandwidth drops. Such applications would benefit from a framework that supports adaptivity. This requires at least two essential components: (i) a database which contains current values of various system parameters, and (ii) mechanisms by which applications can either poll these values or subscribe to events corresponding to parameter changes.

² Java, with its ability to abstract away CPU and OS-specific differences holds great promise for realizing a vision in which applications, not just data, can be exchanged freely between all kinds of devices.

2.5 Firewalls and Virtual Private Networks

Corporate employees comprise a significant proportion of the mobile user community so allowing their access to corporate resources from remote locations is an important requirement. At present, access over PSTN (*e.g.* using PPP [23] with PAP/CHAP) is by far the most popular choice. In the near future, remote access mechanisms that use the Internet (rather than PSTN) for their transport are likely to become popular. These mechanisms offer significant savings in infrastructure costs and toll charges by tunneling packets between the end user and the corporate network through the Internet. Clearly, security is an important concern in this situation. Strong cryptographic mechanisms are required to ensure that only authorized users gain access to company resources and all sensitive information is hidden from eavesdroppers. Tunneling service may be provided at Layer 2 or Layer 3 and both avenues are being pursued within the IETF.

Many organizations deploy firewalls between their network and the Internet. Firewalls use filtering rules and/or cryptographic mechanisms to selectively block network traffic. Internet-based remote access mechanisms must accommodate the presence of firewalls at a corporate network's periphery. Here again, several efforts are underway within the IETF to address the issue of firewall traversal [6, 9, 18, 19]. The first internet-draft on the list [6] outlines how mobile hosts can establish Virtual Private Networks (VPNs) with their corporate networks using IP Security (IPSec) [13, 14, 15, 12, 17, 20]. Other proposals on the list add mobility support using Mobile IP and can be used to create Mobile VPNs (MVPNs). The additional mobility support allows transport level connections to be maintained across moves. The three MVPN mechanisms differ in the key-management protocols they use [2, 12], the requirements they impose on firewalls, and packet header overhead. Unlike TSP [18], the proposals described in [9, 10, 19] do not require firewalls to understand Mobile IP registrations. On the other hand, by requiring firewalls to understand Mobile IP registrations, TSP is able to reduce the header overhead on network traffic.

2.6 Web Based Remote Access

All of the above firewall traversal mechanisms are aimed at providing IP level access to all applications even when the mobile host is outside its corporate network. For situations where access to specific applications is sufficient, SSL [8] due to its wide availability may provide a better alternative. The basic idea involves an application-specific proxy at the firewall. The proxy replaces direct communication between a client applet and a server with two separate connections: (i) one between the applet and the proxy, and (ii) another between the proxy and the server. Communication between the applet and the proxy is secured using SSL as the underlying transport. Since the applet can be downloaded from the same host as the proxy, communication between them may use a proprietary protocol without introducing interoperability problems. For instance, this proprietary

protocol may be specially tuned for low-bandwidth links. Communication between the proxy and server still utilizes regular, well established protocols, *e.g.* IMAPv4, SMTP, HTTP, telnet, etc so no changes are required on the server side. A major advantage of this architecture is that the near-ubiquity of Java- and SSL-capable browsers eliminates the need to carry a personal device. A salesperson can walk up to any host, a kiosk or even a client's workstation, and use its browser to gain secure access to specific applications on his corporate network. The server is authenticated through SSL's certificate exchange mechanism and one-time passwords can be used to authenticate the user to the proxy host.

Whatever mechanism is chosen for secure, Internet-based access, it is important that existing applications be able to benefit from it with minimal changes. The Java application environment supports the notion of a socket factory which can be used to isolate applications from specific details of the packet processing required for firewall traversal.

3 Lightweight Devices and Personal Mobility

Our objective is to enable *people* to access their network resources independent from any of the following:

1. Physical location,
2. Internet access method,
3. Device used.

The last item will grow in importance with the deployment of internet kiosks, web-enabled hotel rooms, public internet terminals and similar devices. Device independence – besides being a desired objective – is sometimes necessary. For example, the user may not have authorization to connect any device he may be carrying to the existing network infrastructure: one company's employee may be forced to use existing devices at another company's premises.

3.1 Minimum Set of Platform Requirements

This mode of access must make very few assumptions about the underlying platform. We have arrived at the following elements which we believe are ubiquitous or nearly so, and enable remote access mechanisms at the transport layer and above.

1. HTML
2. HTTP and HTTP over SSL (HTTPS)
3. Java Virtual Machine (JVM)

An important consideration in arriving at this minimum set of requirements is that, prior to arriving at the remote site, no client software installation is required. Instead, any necessary client-side software is downloaded and executed dynamically on the JVM. Given that client platforms are notorious for their lack

of reliability, modifying the configuration in any significant manner dramatically increases the possibility of software conflicts, lock ups and panics. It is generally recognized that executing Java byte code within the confines of the JVM is very effective in safeguarding the client against rogue software. What is not generally recognized is that, by virtue of leaving drivers and kernel code untouched and by limiting the capabilities of the code to those allowed by the JVM, bytecode execution also protects the machine from its own unreliability.

Another objective in arriving at a minimum set of platform requirements is that security must not be compromised. Thanks to Java's ability to dynamically download and execute code, basic SSL (HTTPS) services become the foundation for secure remote access mechanisms.

3.2 Distributed Cryptographic Infrastructure

With Java, it is possible to engage in international secure transactions and networking without contravening any laws.

Regulations concerning cryptographic technology vary from country to country. For example, in the U.S. strict export controls must be abided by. In France, use of cryptography by individuals is severely limited. Furthermore, governments may express these policies in ambiguous terms as a further deterrent to the dissemination of cryptography. Given this confusing landscape, it is obvious that for international corporations – particularly those implementing virtual private networks on the Internet – and for security-conscious travelers, divining the set of regulations valid in any given situation, and complying with it is a daunting task. Traditionally a user installs security software onto his laptop. As this user travels across international borders, he may have to uninstall and subsequently reinstall the software. Besides being cumbersome, this negatively affects the stability of the portable device, precisely at the time when the user is traveling and system administration resources are not available.

Java allows the *just-in-time* downloading of the – potentially digitally signed – cryptographic software, and its subsequent installation and execution under the watchful vigilance of the JVM. Having done this, the client is able to establish secure communications with its corporation's public server, and use it as a gateway into its private network. Notice that thanks to digital signatures, the client need not download the cryptographic software from the same machine that it then uses as a gateway into its network.

For example, suppose a U.S. user travels to Switzerland, and then accesses his corporation's world wide web site using the *https* protocol. The ensuing SSL negotiation selects a cipher that is common to the server and the client in order to encrypt the traffic. Assuming that the remote user is a law-abiding individual, the list of ciphers available at the client does not include strong encryption. For example, instead of RC4 encryption with a 128-bit key, the client may only have export-grade RC4 encryption with a 40-bit key. At this point, the client may choose to download a stronger cipher. However, it does so from a server in Switzerland, completes the SSL negotiation, and is able to secure the communications with the gateway in the U.S. using RC4 encryption with a 128-bit key.

Since the gateway machine in the U.S. never supplies the cryptographic code, export restrictions do not apply. At the same time, the local cryptographic code server in Switzerland enforces whatever *local* policies may apply. Currently, the U.S. government does not restrict encrypted traffic with off-shore sites, it only restricts exporting the technology to encrypt the traffic.³

Of course, the local government might impose additional restrictions on the use of cryptography. For example, if the visitor happens to be in France, his client will have no preinstalled ciphers, and any attempt to download them from a local "security" server would allow the latter to impose local regulations. The user might be informed that cryptography is disallowed, and that any traffic exchanged with the gateway for the U.S. corporation would be in cleartext. At this point, the gateway could impose its own policies and reject the request for remote access from the visitor in France. Alternatively, it could limit the remote user's access rights for the duration of the session.

As can be seen, these security servers take on the responsibility of enforcing local cryptographic policy, thus relieving the users from this onerous task. This constitutes a perfectly legal, distributed cryptographic infrastructure to secure traffic across international borders.

3.3 Configurable Socket Factory and RAFT URLs

There is no standard for internet remote access into corporate or private networks. The task of traversing the corporate firewall may be accomplished in several ways: specific gateway software, IP security (as it is being defined by the IETF), SSL mechanisms, HTTPS tunneling, SOCKS, etc. However, none of the firewall traversal mechanisms will prevail completely. RAFT (Remote Access and Firewall Traversal) URLs recognize this fact, and provide a naming and encapsulation scheme that shields applications from particularities.

RAFT URLs have the following formats:

```
raft:<raft-type>://<traversal-point>:[<other-info>]
raft:generic-url
```

Where the different parts have this meaning:

- raft:** This indicates that the URL that follows is a handle into a registry of remote access schemes.
- raft-type:** The name given to a specific firewall traversal or remote access method. Raft types denote very specific methods. For example, the use of IP layer 3 tunnels with SKIP, using an extended mobile registration protocol for dynamic tunnel set-up might be one such scheme. Another one might be a mechanism based on HTTPS tunneling.
- traversal-point:** This is a firewall, gateway or remote access server with which the system must negotiate access. Discovery of the traversal point is beyond the scope of this note.

³ However, the cipher downloaded from the Swiss site must have been implemented without any aid from the U.S.

other-info: This is a scheme-specific initialization string. The scheme may imply further round-trip times before access is granted. This string is just a first step. It does not necessarily have to be used. The format of this parameter is defined by the scheme.

generic-url: Any possible URL as defined in [3].

A RAFT URL does not designate a data object, but rather a means to negotiate access through a traversal point to establish contact with private resources.

RAFT URLs are useful because no one method of remote access is likely to dominate. RAFT enables the specific form of remote access to be abstracted away from the applications that need the connectivity. It now becomes a two-part process:

1. Discovery of a RAFT URL.

This may be accomplished, for example, by any of these methods:

- (a) The user visits a special web page and as part of the login process, authenticates itself to the gateway or firewall by any of these mechanisms:
 - i. Client-side SSL authentication.
 - ii. Hardware-assisted authentication using challenge-response schemes.
 - iii. One-time passwords.

The web server grants access by sending some relevant information to the client. A RAFT URL may be part of this information sent by the web server. The code that implements the mechanisms called for by the RAFT URL may be pre-installed on the device. Otherwise, the client may, at this time, download the code necessary to interpret and carry out the necessary operations for firewall traversal under the specified RAFT URL.

- (b) The appropriate RAFT URL is produced by querying a directory service such as LDAP, Service Location Protocol or DNS.
 - (c) The possible RAFT URLs (and relevant code to execute them) are pre-configured into the mobile device. The system is set up for the current environment by choosing among the possible RAFT URLs. This may happen direct by the user's choosing from a menu among the possible RAFT URLs, or by some event notification mechanism informing the system.
2. Once the RAFT URL is discovered, it must be used by the system to set its default firewall traversal mechanisms accordingly. The implementation of this step and its transparency to applications is, of course, highly dependent on the system's software platform. As an example, a system may use the RAFT URL to set its socket factory appropriately. Applications built to the standard Java socket interface in package *java.net* need not be aware of the exact mechanisms involved.

Notice that from the point of view of the applications, the socket factory itself does not change, rather its internal behavior does.

Introducing this abstraction allows any type of firewall traversal or remote access scheme to be integrated into the platform, separately from the applications that use the network connection.

At this time, the gateway or firewall becomes a proxy so the remote client can access the private network.

3.4 Personal Mobility

Since the mechanisms outlined above rely on very widely deployed technologies (Java, HTTP, SSL), they also enable *personal mobility*. For example, a user can walk up to any public Internet terminal, and after properly authenticating himself to the relevant gateway, gain access into his private network.

Some words of caution are in order. This technology only secures the link between the client and the gateway machine. Once the data arrives at the client it is presented in cleartext for the user's consumption. A trojan horse client can easily collect the data at this point.

4 Specially Configured Devices

This section examines the "road warrior" or "power user" scenario which is distinguished by a user's ability to carry a specially configured portable device. The user is no longer bound by the constraints of communal devices, like kiosks, which generally offer minimal functionality. In what follows, we present a list of software solutions we consider important for power users.

Perhaps the most basic requirement of mobile users is the ability to change their point of attachment to the Internet with minimal disruption. Doing so typically involves changing several network configuration parameters. This task can be greatly simplified by a piece of software we call *network switcher*. It allows users to specify multiple "network profiles" (*e.g.* one for their office and another for their ISP at home) and switch to a pre-stored profile quickly and conveniently. The software can also initiate DHCP and gather necessary configuration parameters that way rather than through pre-specified profiles.

Whenever the IP address of a device changes, previously established transport-level connections are normally lost. Mobile IP allows a mobile device to be reachable at a fixed IP address (called its home address) irrespective of its current point of attachment to the Internet. Transport level connections established with the home address are preserved across moves. However, unlike PPP and DHCP, Mobile IP is a fairly new protocol and the required infrastructure (comprising mobility agents and client-side software) is not widely deployed.

When a mobile host is moved to a new network, it may need to discover resources like network printers or HTTP proxies in its immediate vicinity. The Service Location Protocol (SLP) is ideally suited to this task. In some situations, LDAP [25] which is more widely deployed may provide adequate functionality.

Connecting to the Internet and finding local resources is just one part of the overall challenge. Mobile users should also be able to access remote resources

within firewall-protected private networks, *e.g.* a corporate network. This requires setting up a secure communication channel across a public network like the Internet, *i.e.* a Virtual Private Network (VPN). The concept of tunneling is central to VPN solutions. It refers to the practice of encapsulating one protocol in another. This might be necessary in order to carry non-IP traffic (*e.g.* IPX or Appletalk) across the Internet, or even to carry an encrypted packet within another packet directed at an intervening firewall. Tunneling service may either be provided at Layer 2 or at Layer 3. Layer 2 tunneling mechanisms (*e.g.* L2TP [11]) transfer PPP packets (encapsulating IP, IPX etc) across the Internet or other transport media. Layer 3 tunneling mechanisms, on the other hand, directly encapsulate network layer packets (*e.g.* IP, IPX) in IP. A number of Layer-3 tunneling protocols have been proposed (TEP [4], TSP [18]) that extend the basic Mobile IP protocol to allow chaining of multiple tunnel segments. All of these tunneling proposals ([11, 4, 18]) rely on IPSec to provide confidentiality, integrity and authenticity when the transport medium is the Internet. Currently, L2TP seems to have captured the largest mindshare among VPN technologies. Nevertheless, we feel that Layer 3 tunneling offers a superior solution especially when the underlying transport is the Internet. These advantages include:

- Better bandwidth utilization. Running protocol X over PPP over UDP (as with L2TP across the Internet) is less efficient than running protocol X directly over IP. (X may be IP, IPX etc)
- Greater reliability. With layer-two tunneling, each end point maintains a PPP state machine (including timers and retransmission logic) across a "simulated serial line". Unlike a real serial line, end points of the simulated line are often separated by large distances and/or many hops with only best effort delivery. As such, the PPP connections are prone to timeouts and frequent resets.

If multi-protocol support is considered unimportant, IPSec alone can go a long way in solving the secure, remote access problem. From a deployment perspective, it is perhaps easier to establish secure tunnels that extend from a corporate network's periphery to an ISP rather than all the way to the end-user device. The latter requires IPSec software on the portable device but offers the following advantages:⁴

- End-users are free to connect to their corporate network irrespective of the ISP used to "get on to the Internet".
- Corporations do not need to establish a trust relationship with ISPs, they only need to trust their own employees. A corporation in may be willing to trust an ISP based in the same country but may not be willing to trust an ISP based in another country even if the two ISPs are members of a roaming consortia. One can also think of several situations where an employee may connect to the Internet through a "provider" that has no prior agreements with the user's corporation. Examples of such "internet providers"

⁴ As IPSec standards mature, we expect operating system vendors to bundle this functionality, greatly alleviating the deployment challenge.

include universities or temporary "terminal rooms" provided at academic and industry conferences.

IPSec based remote access requires an IPSec-capable node within the corporate firewall complex. Filtering and access control rules should be set up so that IPSec packets, and others necessary for establishing security associations, can be exchanged freely between this node and the general Internet. The address of this "IPSec gateway" must be known to external mobile hosts. The exact discovery mechanism is irrelevant to the subsequent discussion. Manual configuration and DNS lookup (*e.g.* using KX records [1]) are just two of the possible alternatives.

Very often, corporate networks use private addresses that are not advertised to the general Internet. Furthermore, internal routers are generally unaware of external addresses and return "ICMP unreachable" messages for such destinations (assuming they do not use default routing). This creates the challenge of ensuring end-to-end delivery between a host with an internal address (*e.g.* corporate file- or mail-server) and a host connected to the Internet using an external address. There are two basic approaches to this problem:

1. The first approach adds Network Address Translation (NAT) functionality at the IPSec gateway. After authenticating arriving packets, and before injecting them into the private network, the gateway does a NAT operation, replacing the external source address with its own IP address (the gateway may be assigned a range of internal addresses). This way when an internal host responds, it uses a destination address that is "valid" inside the corporate network. The response packet reaches the IPSec gateway, undergoes a reverse address translation, and IPSec processing before it is sent to the remote host [6].

Inserting NAT in the communication path can "break" certain applications. Some applications carry network address information (IP address and/or TCP/UDP port) as part of their payload and performing NAT for such packets can get complicated, *e.g.* replacing the IP address or port information in the application payload may require adjustments to the IP packet length. Certain NAT implementations go to great lengths to accommodate these applications while others simply let them fail silently. Similarly, applications in which an internal host must initiate connections (rather than the external host) are also harder to support and may require workarounds, *e.g.* FTP's passive mode may need to be turned on.

In spite of these limitations, this approach is quite attractive as it requires nothing more than IPSec on the portable device. Even the internal hosts do not require any changes.

2. Another option for preventing the exposure of external addresses to internal routers is to use an extra level of IP-in-IP tunneling between the IPSec gateway and the internal host. This requires the internal host (or a proxy such as a Mobile IP home agent) to support IP-in-IP encapsulation and decapsulation. The principal advantage of this approach is that it transparently enables all applications and can be easily extended to work with Mobile IP [9, 10, 18, 19].

The portable device must also be responsible for securing the private network, because it extends its periphery. Therefore, it must implement some firewall capabilities, otherwise, any malicious individual that gains access to it will have gained access to the private network as well.

5 Enabling Groups of Users

We have also been investigating mechanisms to support small teams of mobile users traveling together. Disaster recovery teams offer an excellent example of this scenario. Another example may be a sales team traveling together that wishes to set up a "temporary branch office" of their corporation at a convention center. These situations call for "thin servers" around which a small network can be quickly established. This network may be based on either wireless or wireline LAN technologies. We have prototyped such a device and call it a Remote Site Server (RSS). An RSS can fulfill the booting, configuration, security, and routing needs of an assortment of connected clients. It offers DHCP, DNS, Mail, web-caching, file-sharing and firewall services. It also acts as a router to the outside world and can provide both network address translation (NAT) and secure communication capabilities. The NAT feature is handy for hiding multiple hosts on a private network behind a single ISP-provided IP address. All communication involving any of the hosts behind the thin server appears to originate from the thin server. This communication can either be in the clear or secured through IP-level or higher-level encryption and authentication, when necessary. The same VPN technologies that were described earlier (see Section 4) for connecting individual remote hosts to private networks are also applicable here. A variety of Internet connectivity options are supported including ethernet and dial-up PPP. Since the task of establishing Internet connectivity, negotiating network access across firewalls, and warding off hackers is off-loaded to the thin server, individual clients behind it need not concern themselves with any of the associated complexities. One may think of the RSS as a power-device (see Section 4) enhanced with server software to support protected workgroups.

The RSS feature-set is also a good match for small-office or home-office (SOHO) computing. These offices can be viewed as less volatile, or smaller, variations of "temporary" branch offices. These situations can benefit from most of the capabilities of the RSS but may not need the VPN capabilities. For example, a small, independently owned flower shop may not have a "parent" office with which it may need to establish secure channels.

One possible use of our remote site server is in supporting multiple satellite offices of a corporation. In any large deployment of these systems, ensuring that each is installed correctly and with the latest software packages is a major undertaking. We have addressed these issues in several ways.

We have developed a framework for automating the installation, upgrade and configuration of software packages on the thin server. This framework organizes different software packages into distinct clusters. Each cluster can be independently installed and, if an older version of the cluster is detected, it can

be automatically upgraded with a newer version. The framework stores configuration information separately from the software. This allows a pre-existing configuration to be reused with the newly updated software and eliminates the overhead of unnecessary reconfiguration. The thin server offers an HTML form-based administrative interface. As such, there is no need to connect a monitor to the thin server, and it can be managed from any device equipped with a web browser. In some cases, troubleshooting or special administration tasks may require complete shell access to the thin server. Our prototype offers telnet access (through a Java applet) to administrators on the local network and Secure Shell (SSH) login for remote administrators.

6 Conclusion

We have presented our vision of a *Complete Computing* environment. We leverage a common set of mechanisms to enable *mobile, nomadic, remote, branch office* and *small office* computing, hitherto addressed as disparate problems. From a user-centric point of view, the important distinctions are not directly related to any of the aforementioned modes of computing, but to the characteristics of the device used. Table 1 correlates the type of device to the user experience it affords. In all cases, the first step is to establish a communication path to the private network by (1) *hopping* on the internet, and (2) negotiating access past the corporate firewall. Having done this, the user (or the device on the user's behalf) has obtained access to the resources within the private network. However, the level of service with which these resources are now available reflect the characteristics of the device used by the remote user.

Using a Java and HTTPS enabled device allows the maximum degree of nomadicity. The user is able to use almost any portable computing device, and may not, in fact, carry one with him. These devices allow personal mobility in addition to nomadicity. However, the task of hopping on the internet is typically done by dialing into an ISP. This does not constitute automatic network configuration, as the user still has to worry about phone numbers, baud rate, and similar parameters.⁵ Similarly, the firewall traversal is an explicit phase in which the user has to authenticate itself before gaining access to the private resources. Having accomplished this, the user is able to access but a handful of applications from the private network.

Specially configured devices also use ISP accounts to hop on the internet. Using IPsec mechanisms may make it easier to negotiate access past the firewall, but this step still exists. However, the level of application support improves considerably. Using these types of devices, it is possible to establish network level connections with the application servers within the private network. Full mobility is now possible.

Finally, devices that provide group support shield their clients from direct internet usage. Group support devices, such as our *Remote Site Server* create

⁵ Strictly speaking, it is possible to establish internet presence by completely automatic means such as DHCP. However, typical ISP accounts do not yet allow this.

a protected workgroup safely ensconced away from the intimidating internet. A device within the protected workgroup benefits from automatic network configuration via DHCP support at the thin server. Likewise, the latter performs any required firewall negotiation on behalf of its clients. Given that the connection mechanisms used by the thin server to access servers in the corporate network are identical to those used by specially configured devices, the clients in the protected workgroup also enjoy a very high level of service.

Table 1. Modes of access when away from the the home network

Device Requirements	User Experience				
	Establishing a communication path		Level of Service		
	Auto. network config.	Implicit firewall traversal	Some apps (web based)	All or most apps (nomadic mode)	All applications (mobile mode)
Java and HTTPS enabled browser	N	N	Y	N	N
Specially configured devices	N	N	Y	Y	Y
Group support	Y	Y	Y	Y	Y

References

1. Atkinson, R.: Key Exchange Delegation Record for the DNS, *RFC 2230*, (Nov. 1997).
2. Aziz, A., Patterson, M.: Design and Implementation of SKIP, available on-line at <http://skip.incog.com/inet-95.ps>. A previous version of the paper was presented at INET '95 under the title *Simple Key Management for Internet Protocols (SKIP)*, and appears in the conference proceedings under that title.
3. Berners-Lee, T., Masinter, L., McCahill, M.: Uniform Resource Locators (URL), *RFC 1738*, (Dec. 1994).
4. Calhoun, P., Perkins, C.: Tunnel Establishment Protocol, Internet draft *draft-ietf-mobileip-calhoun-tep-00.txt* - work in progress, (1997).
5. Chapman, D. B., Zwicky, E.: *Building Internet Firewalls*, O'Reilly & Associates, Inc., (1995).
6. Doraswamy, N., Moskowitz, R.: Implementation of VPNs with IP Security, Internet-draft - work in progress, (1997).
7. Droms, R.: Dynamic Host Configuration Protocol, *RFC 2131*, (Mar. 1997).
8. Frier, A., Karlton, P., Kocher, P.: The SSL 3.0 Protocol, Netscape Communications Corp., (Nov. 1996).
9. Gupta, V., Glass, S.: Firewall traversal for Mobile IP: guidelines for firewalls and Mobile IP entities, Internet Draft *draft-ietf-mobileip-firewall-trav-00.txt* - work in progress, (Mar. 1997).

10. Gupta, V., Montenegro, G.: Secure and Mobile Networking, to appear in the ACM Journal on Special Topics in Mobile Networking and Applications (MONET), (special issue on Mobile Networking in the Internet).
11. Hamzeh, K., *et al.*: Layer Two Tunneling Protocol (L2TP), Internet Draft *draft-ietf-pppext-l2tp-08.txt* – work in progress, (Nov. 1997).
12. Harkins, D., Carrel, D.: The resolution of ISAKMP with Oakley, Internet Draft *draft-ietf-ipsec-isakmp-oakley-05.txt* – work in progress, (Nov. 1997).
13. Kent, S., Atkinson, R.: Security architecture for the Internet Protocol, Internet Draft *draft-ietf-ipsec-arch-sec-02.txt* – work in progress, (Nov. 1997) (a previous version appears as *RFC 1825*).
14. Kent, S., Atkinson, R.: IP authentication header, Internet Draft *draft-ietf-ipsec-auth-header-03.txt* – work in progress, (Nov. 1997) (a previous version appears as *RFC 1826*).
15. Kent, S., Atkinson, R.: IP encapsulating security payload, Internet Draft *draft-ietf-ipsec-esp-v2-02.txt* – work in progress, (Nov. 1997) (a previous version appears as *RFC 1827*).
16. Kistler, J. J., Satyanarayanan, M.: Disconnected Operation in the Coda File System, *ACM Transactions on Computer Systems*, 10, No. 1, (Feb. 1992) 3–25.
17. Maughan, D., Schertler, M., Schneider, M., Turner, J.: Internet Security Association and Key Management Protocol (ISAKMP), Internet Draft *draft-ietf-ipsec-isakmp-08.txt* – work in progress, (Jul. 1997).
18. Montenegro, G.: Tunnel Set-up Protocol (TSP), Internet Draft *draft-montenegro-tsp-00.txt* – work in progress, (Aug. 1997).
19. Montenegro, G., Gupta, V.: Firewall support for Mobile IP, Internet Draft *draft-montenegro-firewall-sup-02.txt* – work in progress, (Nov. 1997).
20. Orman, H.: The OAKLEY Key Determination Protocol, Internet Draft *draft-ietf-ipsec-oakley-02.txt* – work in progress.
21. Perkins, C., (Editor): IP mobility support, *RFC 2002*, (Oct. 1996).
22. Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E.: Address allocation for private internets, *RFC 1918*, (Feb. 1996).
23. Simpson, W.: The Point-to-Point Protocol (PPP), *RFC 1661*, (Jul. 1994).
24. Veizades, J., Guttman, E., Perkins, C., Kaplan, S.: Service Location Protocol, *RFC 2165*, (Jun. 1997).
25. Yeong, W., Howes, T., Kille, S.: Lightweight Directory Access Protocol, *RFC 1777*, (Mar. 1995).

ATTACHMENT 1B

Complete Computing *

Vipul Gupta, Gabriel Montenegro and Jeff Rulifson

Technology Development Group
Sun Microsystems, Inc.
901 San Antonio Road, MS UMPK15-214
Palo Alto, California 94303
Email: {vgupta, gab, jeffr}@eng.sun.com

Abstract. Our objective is to enable nomadic and mobile computing, as well as telecommuting, small-office, and branch-office computing. These areas have been dealt with extensively in the literature. However, they have been treated as separate problem spaces and current solutions focus on solving specific problems in one area while ignoring – or even exacerbating – those in another area. These problem spaces must be viewed as being closely related, and must be addressed in a coherent fashion.

We call this unified vision and architecture *Complete Computing*.

1 Vision

As people navigate or relocate throughout the ocean of information that surrounds them (Figure 1), they wish to maintain logical availability of some subset of their computing environment. We use the term computing environment to include both a user's applications (*e.g.* document editor) and data (*e.g.* files, mail, *etc.*). Maintaining this logical availability may require a combination of several mechanisms including caching, replication, redirection, repackaging or even prediction.

A mobile client is able to connect using a variety of schemes (serial, LAN, wireless, WAN, through firewalls [5], *etc.*) and is adept at operating in disconnected mode. This flexibility gives its user the illusion that information is always close at hand, and that it follows him or her and presents itself for consumption independently of the client's physical or logical location. An important corollary is that this network model supports both user and terminal mobility, because the objective is for the information to be available to the user at all times – though perhaps in varying degrees depending on prevalent networking and environmental conditions.

In this paper, the term *Mobile Computing* represents the ambitious objective of retaining a user's static computing environment (including all existing connections), even while the user and his portable device are moving. It attempts to

* This work was partly funded by the Ministry of International Trade and Industry of Japan through the *Advanced Software Enrichment Project* of the Information Technology Promotion Agency.

shield the user from the effects of physical or topological movement throughout the networking fabric.

In some instances, preserving a user's computing environment during movement may not be necessary. Instead it may be sufficient to ensure that the user's computing environment can be recreated wherever the user moves. This may require re-initiating network connections and/or reestablishing session state. We use the term *Nomadic Computing* for these situations.

Remote Computing or *Branch Office Computing* have similar requirements to the previous two, in that they involve access to a user's private computing environment (*e.g.* firewall-protected corporate resources) across a potentially hostile – or at least untrusted – public network. Nevertheless, the static – hence, stable – nature of this kind of computing translates into better resource availability and richer services.

Finally, *Small-Office/Home-Office Computing* assumes there are no private user environments beyond those available locally. The objective is to enable small, independent work groups. Since they do not belong to a parent organization, they lack assistance from system administrators and technical support personnel. Therefore, ease of use is of utmost importance. However, there is still a need for rich networking and application support.

The diverse areas mentioned above have been dealt with extensively in the literature but not as a cohesive whole. Our objective is to enable all of these forms of computing using a common set of tools and solutions. We call this unified vision and architecture *Complete Computing*.

By designing similar mechanisms for all these areas, we wish to prevent further fragmentation of proposed solutions. Our vision of complete computing has technology implications in several areas: hardware and software platforms, data persistence, caching and synchronization, configuration and management, applications, services, networking, and security.

In this paper we focus primarily on networking and the concomitant security issues. We identify the outstanding technical challenges, review proposed solutions, and discuss their applicability in different situations.

2 Elements of a Solution

For the following discussion, a mobile user is one who needs to access information and applications "on the road", *i.e.* from different locations (or even while changing locations) and under varying conditions. Access may be read-only or read-write and the access device may be personal (*e.g.* a portable, personal notebook or PDA) or communal (*e.g.* a kiosk at an airport).

2.1 Challenges of Mobility

Mobility imposes certain fundamental constraints which affect all aspects of computing.

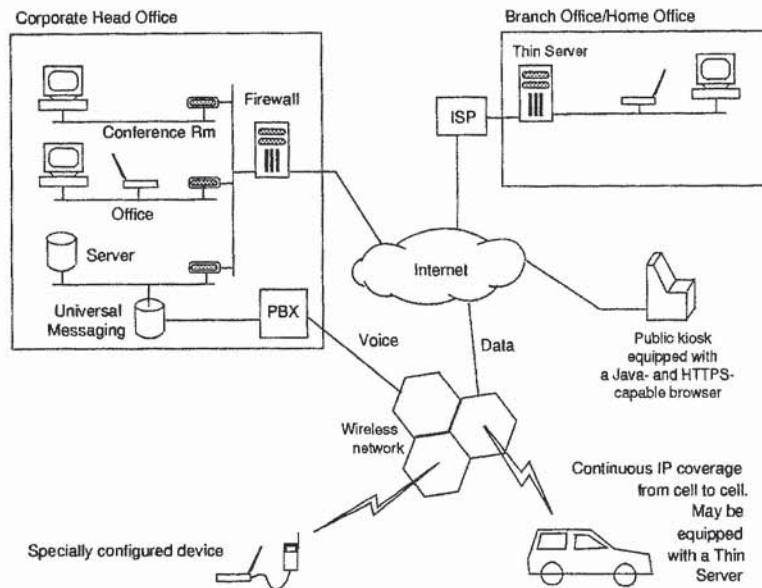


Fig. 1. An overview of the Complete Computing environment

1. Portable devices, as compared to their stationary counterparts, are "resource poor" (*e.g.* less powerful CPU, fewer I/O devices, smaller screen), and must manage their resources carefully. Power management is critical for battery-operated devices. Screen size and keyboard (or lack thereof) may influence the user interface.
2. Network characteristics like bandwidth and latency fluctuate widely. Therefore, mobile systems must deal with communication uncertainty – including complete disconnection – and adapt gracefully to these and other changes.
3. Mobility requires different forms of security.
 - (a) *Network Security.* Traffic may at times pass through links with questionable security characteristics. New alternatives may be required for some traditional security mechanisms that use location information to distinguish between authorized and unauthorized users. As an example, many packet-filtering firewalls disallow certain kinds of traffic if it arrives on an interface facing the general Internet. Such firewalls may need to be enhanced with strong cryptographic mechanisms so legitimate traffic from authorized mobile users is allowed irrespective of the interface.
 - (b) *Data and Device Security.* As opposed to large, stationary devices safely locked up in an office, lightweight, portable devices are frequently used in public places. Hence, they are prone to being destroyed, lost or stolen. Consequently, encryption and secure backups are used to prevent subversion or loss of data.

2.2 Agile Networking

In today's fast-paced information society, it is inconceivable to think that a mobile user can always carry all the information he needs on the local storage of his personal computing device. Typically, the information of interest will be distributed across a multitude of other hosts connected to a network. This immediately highlights the need for a mobile user to attach to a network, establish a communication path to the desired server and exchange information under a variety of conditions.

Consider a salesperson who, over the course of a few hours, uses a portable notebook in different networking modes — wireline LAN at his office, a different wireline LAN in a conference room, wireless LAN at the company cafeteria, wireless WAN at the airport, and a POTS modem connection at a hotel. Typically, each situation requires reconfiguration of the device. These configuration parameters may include IP address, network mask, default router, DNS server name, local printer, etc. In an ideal situation, most (if not all) of the necessary changes would be transparent to the end user and occur with minimal disruption. Newer protocols like DHCP [7], Mobile IP [21] and SLP [24] hold great promise for solving this challenge.

2.3 Disconnected Operation

Of course, there will be periods when a mobile user may not have access to any network or the cost of connecting to a network may be prohibitively high (as in an airplane). Support for disconnected operation is imperative for such situations. The user should be able to cache applications and data² in his current "working set" onto local, non-volatile storage and, at a later point, reconcile any changes made locally against other copies on the network. While a number of research groups have made encouraging progress in this particular area [16], mature industry-wide standards are still lacking.

2.4 Adaptivity

We anticipate the development of several classes of mobile computing devices differing in their CPU power, display size, screen resolution, input devices etc. While these characteristics do not change during the lifetime of a device, others such as network bandwidth and latency, remaining battery power, and available storage are more dynamic and applications could benefit from adapting to such changes. A web browser could turn off automatic downloading of in-line images when available network bandwidth drops. Such applications would benefit from a framework that supports adaptivity. This requires at least two essential components: (i) a database which contains current values of various system parameters, and (ii) mechanisms by which applications can either poll these values or subscribe to events corresponding to parameter changes.

² Java, with its ability to abstract away CPU and OS-specific differences holds great promise for realizing a vision in which applications, not just data, can be exchanged freely between all kinds of devices.

2.5 Firewalls and Virtual Private Networks

Corporate employees comprise a significant proportion of the mobile user community so allowing their access to corporate resources from remote locations is an important requirement. At present, access over PSTN (*e.g.* using PPP [23] with PAP/CHAP) is by far the most popular choice. In the near future, remote access mechanisms that use the Internet (rather than PSTN) for their transport are likely to become popular. These mechanisms offer significant savings in infrastructure costs and toll charges by tunneling packets between the end user and the corporate network through the Internet. Clearly, security is an important concern in this situation. Strong cryptographic mechanisms are required to ensure that only authorized users gain access to company resources and all sensitive information is hidden from eavesdroppers. Tunneling service may be provided at Layer 2 or Layer 3 and both avenues are being pursued within the IETF.

Many organizations deploy firewalls between their network and the Internet. Firewalls use filtering rules and/or cryptographic mechanisms to selectively block network traffic. Internet-based remote access mechanisms must accommodate the presence of firewalls at a corporate network's periphery. Here again, several efforts are underway within the IETF to address the issue of firewall traversal [6, 9, 18, 19]. The first internet-draft on the list [6] outlines how mobile hosts can establish Virtual Private Networks (VPNs) with their corporate networks using IP Security (IPSec) [13, 14, 15, 12, 17, 20]. Other proposals on the list add mobility support using Mobile IP and can be used to create Mobile VPNs (MVPNs). The additional mobility support allows transport level connections to be maintained across moves. The three MVPN mechanisms differ in the key-management protocols they use [2, 12], the requirements they impose on firewalls, and packet header overhead. Unlike TSP [18], the proposals described in [9, 10, 19] do not require firewalls to understand Mobile IP registrations. On the other hand, by requiring firewalls to understand Mobile IP registrations, TSP is able to reduce the header overhead on network traffic.

2.6 Web Based Remote Access

All of the above firewall traversal mechanisms are aimed at providing IP level access to all applications even when the mobile host is outside its corporate network. For situations where access to specific applications is sufficient, SSL [8] due to its wide availability may provide a better alternative. The basic idea involves an application-specific proxy at the firewall. The proxy replaces direct communication between a client applet and a server with two separate connections: (i) one between the applet and the proxy, and (ii) another between the proxy and the server. Communication between the applet and the proxy is secured using SSL as the underlying transport. Since the applet can be downloaded from the same host as the proxy, communication between them may use a proprietary protocol without introducing interoperability problems. For instance, this proprietary

protocol may be specially tuned for low-bandwidth links. Communication between the proxy and server still utilizes regular, well established protocols, *e.g.* IMAPv4, SMTP, HTTP, telnet, etc so no changes are required on the server side. A major advantage of this architecture is that the near-ubiquity of Java- and SSL-capable browsers eliminates the need to carry a personal device. A salesperson can walk up to any host, a kiosk or even a client's workstation, and use its browser to gain secure access to specific applications on his corporate network. The server is authenticated through SSL's certificate exchange mechanism and one-time passwords can be used to authenticate the user to the proxy host.

Whatever mechanism is chosen for secure, Internet-based access, it is important that existing applications be able to benefit from it with minimal changes. The Java application environment supports the notion of a socket factory which can be used to isolate applications from specific details of the packet processing required for firewall traversal.

3 Lightweight Devices and Personal Mobility

Our objective is to enable *people* to access their network resources independent from any of the following:

1. Physical location,
2. Internet access method,
3. Device used.

The last item will grow in importance with the deployment of internet kiosks, web-enabled hotel rooms, public internet terminals and similar devices. Device independence – besides being a desired objective – is sometimes necessary. For example, the user may not have authorization to connect any device he may be carrying to the existing network infrastructure: one company's employee may be forced to use existing devices at another company's premises.

3.1 Minimum Set of Platform Requirements

This mode of access must make very few assumptions about the underlying platform. We have arrived at the following elements which we believe are ubiquitous or nearly so, and enable remote access mechanisms at the transport layer and above.

1. HTML
2. HTTP and HTTP over SSL (HTTPS)
3. Java Virtual Machine (JVM)

An important consideration in arriving at this minimum set of requirements is that, prior to arriving at the remote site, no client software installation is required. Instead, any necessary client-side software is downloaded and executed dynamically on the JVM. Given that client platforms are notorious for their lack

of reliability, modifying the configuration in any significant manner dramatically increases the possibility of software conflicts, lock ups and panics. It is generally recognized that executing Java byte code within the confines of the JVM is very effective in safeguarding the client against rogue software. What is not generally recognized is that, by virtue of leaving drivers and kernel code untouched and by limiting the capabilities of the code to those allowed by the JVM, bytecode execution also protects the machine from its own unreliability.

Another objective in arriving at a minimum set of platform requirements is that security must not be compromised. Thanks to Java's ability to dynamically download and execute code, basic SSL (HTTPS) services become the foundation for secure remote access mechanisms.

3.2 Distributed Cryptographic Infrastructure

With Java, it is possible to engage in international secure transactions and networking without contravening any laws.

Regulations concerning cryptographic technology vary from country to country. For example, in the U.S. strict export controls must be abided by. In France, use of cryptography by individuals is severely limited. Furthermore, governments may express these policies in ambiguous terms as a further deterrent to the dissemination of cryptography. Given this confusing landscape, it is obvious that for international corporations – particularly those implementing virtual private networks on the Internet – and for security-conscious travelers, divining the set of regulations valid in any given situation, and complying with it is a daunting task. Traditionally a user installs security software onto his laptop. As this user travels across international borders, he may have to uninstall and subsequently reinstall the software. Besides being cumbersome, this negatively affects the stability of the portable device, precisely at the time when the user is traveling and system administration resources are not available.

Java allows the *just-in-time* downloading of the – potentially digitally signed – cryptographic software, and its subsequent installation and execution under the watchful vigilance of the JVM. Having done this, the client is able to establish secure communications with its corporation's public server, and use it as a gateway into its private network. Notice that thanks to digital signatures, the client need not download the cryptographic software from the same machine that it then uses as a gateway into its network.

For example, suppose a U.S. user travels to Switzerland, and then accesses his corporation's world wide web site using the *https* protocol. The ensuing SSL negotiation selects a cipher that is common to the server and the client in order to encrypt the traffic. Assuming that the remote user is a law-abiding individual, the list of ciphers available at the client does not include strong encryption. For example, instead of RC4 encryption with a 128-bit key, the client may only have export-grade RC4 encryption with a 40-bit key. At this point, the client may choose to download a stronger cipher. However, it does so from a server in Switzerland, completes the SSL negotiation, and is able to secure the communications with the gateway in the U.S. using RC4 encryption with a 128-bit key.

Since the gateway machine in the U.S. never supplies the cryptographic code, export restrictions do not apply. At the same time, the local cryptographic code server in Switzerland enforces whatever *local* policies may apply. Currently, the U.S. government does not restrict encrypted traffic with off-shore sites, it only restricts exporting the technology to encrypt the traffic.³

Of course, the local government might impose additional restrictions on the use of cryptography. For example, if the visitor happens to be in France, his client will have no preinstalled ciphers, and any attempt to download them from a local "security" server would allow the latter to impose local regulations. The user might be informed that cryptography is disallowed, and that any traffic exchanged with the gateway for the U.S. corporation would be in cleartext. At this point, the gateway could impose its own policies and reject the request for remote access from the visitor in France. Alternatively, it could limit the remote user's access rights for the duration of the session.

As can be seen, these security servers take on the responsibility of enforcing local cryptographic policy, thus relieving the users from this onerous task. This constitutes a perfectly legal, distributed cryptographic infrastructure to secure traffic across international borders.

3.3 Configurable Socket Factory and RAFT URLs

There is no standard for internet remote access into corporate or private networks. The task of traversing the corporate firewall may be accomplished in several ways: specific gateway software, IP security (as it is being defined by the IETF), SSL mechanisms, HTTPS tunneling, SOCKS, etc. However, none of the firewall traversal mechanisms will prevail completely. RAFT (Remote Access and Firewall Traversal) URLs recognize this fact, and provide a naming and encapsulation scheme that shields applications from particularities.

RAFT URLs have the following formats:

```
raft:<raft-type>://<traversal-point>:[<other-info>]
```

```
raft:generic-url
```

Where the different parts have this meaning:

raft: This indicates that the URL that follows is a handle into a registry of remote access schemes.

raft-type: The name given to a specific firewall traversal or remote access method. Raft types denote very specific methods. For example, the use of IP layer 3 tunnels with SKIP, using an extended mobile registration protocol for dynamic tunnel set-up might be one such scheme. Another one might be a mechanism based on HTTPS tunneling.

traversal-point: This is a firewall, gateway or remote access server with which the system must negotiate access. Discovery of the traversal point is beyond the scope of this note.

³ However, the cipher downloaded from the Swiss site must have been implemented without any aid from the U.S.

other-info: This is a scheme-specific initialization string. The scheme may imply further round-trip times before access is granted. This string is just a first step. It does not necessarily have to be used. The format of this parameter is defined by the scheme.

generic-url: Any possible URL as defined in [3].

A RAFT URL does not designate a data object, but rather a means to negotiate access through a traversal point to establish contact with private resources.

RAFT URLs are useful because no one method of remote access is likely to dominate. RAFT enables the specific form of remote access to be abstracted away from the applications that need the connectivity. It now becomes a two-part process:

1. Discovery of a RAFT URL.

This may be accomplished, for example, by any of these methods:

- (a) The user visits a special web page and as part of the login process, authenticates itself to the gateway or firewall by any of these mechanisms:
 - i. Client-side SSL authentication.
 - ii. Hardware-assisted authentication using challenge-response schemes.
 - iii. One-time passwords.

The web server grants access by sending some relevant information to the client. A RAFT URL may be part of this information sent by the web server. The code that implements the mechanisms called for by the RAFT URL may be pre-installed on the device. Otherwise, the client may, at this time, download the code necessary to interpret and carry out the necessary operations for firewall traversal under the specified RAFT URL.

- (b) The appropriate RAFT URL is produced by querying a directory service such as LDAP, Service Location Protocol or DNS.
 - (c) The possible RAFT URLs (and relevant code to execute them) are pre-configured into the mobile device. The system is set up for the current environment by choosing among the possible RAFT URLs. This may happen direct by the user's choosing from a menu among the possible RAFT URLs, or by some event notification mechanism informing the system.
2. Once the RAFT URL is discovered, it must be used by the system to set its default firewall traversal mechanisms accordingly. The implementation of this step and its transparency to applications is, of course, highly dependent on the system's software platform. As an example, a system may use the RAFT URL to set its socket factory appropriately. Applications built to the standard Java socket interface in package *java.net* need not be aware of the exact mechanisms involved.

Notice that from the point of view of the applications, the socket factory itself does not change, rather its internal behavior does.

Introducing this abstraction allows any type of firewall traversal or remote access scheme to be integrated into the platform, separately from the applications that use the network connection.

At this time, the gateway or firewall becomes a proxy so the remote client can access the private network.

3.4 Personal Mobility

Since the mechanisms outlined above rely on very widely deployed technologies (Java, HTTP, SSL), they also enable *personal mobility*. For example, a user can walk up to any public Internet terminal, and after properly authenticating himself to the relevant gateway, gain access into his private network.

Some words of caution are in order. This technology only secures the link between the client and the gateway machine. Once the data arrives at the client it is presented in cleartext for the user's consumption. A trojan horse client can easily collect the data at this point.

4 Specially Configured Devices

This section examines the "road warrior" or "power user" scenario which is distinguished by a user's ability to carry a specially configured portable device. The user is no longer bound by the constraints of communal devices, like kiosks, which generally offer minimal functionality. In what follows, we present a list of software solutions we consider important for power users.

Perhaps the most basic requirement of mobile users is the ability to change their point of attachment to the Internet with minimal disruption. Doing so typically involves changing several network configuration parameters. This task can be greatly simplified by a piece of software we call *network switcher*. It allows users to specify multiple "network profiles" (*e.g.* one for their office and another for their ISP at home) and switch to a pre-stored profile quickly and conveniently. The software can also initiate DHCP and gather necessary configuration parameters that way rather than through pre-specified profiles.

Whenever the IP address of a device changes, previously established transport-level connections are normally lost. Mobile IP allows a mobile device to be reachable at a fixed IP address (called its home address) irrespective of its current point of attachment to the Internet. Transport level connections established with the home address are preserved across moves. However, unlike PPP and DHCP, Mobile IP is a fairly new protocol and the required infrastructure (comprising mobility agents and client-side software) is not widely deployed.

When a mobile host is moved to a new network, it may need to discover resources like network printers or HTTP proxies in its immediate vicinity. The Service Location Protocol (SLP) is ideally suited to this task. In some situations, LDAP [25] which is more widely deployed may provide adequate functionality.

Connecting to the Internet and finding local resources is just one part of the overall challenge. Mobile users should also be able to access remote resources

within firewall-protected private networks, *e.g.* a corporate network. This requires setting up a secure communication channel across a public network like the Internet, *i.e.* a Virtual Private Network (VPN). The concept of tunneling is central to VPN solutions. It refers to the practice of encapsulating one protocol in another. This might be necessary in order to carry non-IP traffic (*e.g.* IPX or Appletalk) across the Internet, or even to carry an encrypted packet within another packet directed at an intervening firewall. Tunneling service may either be provided at Layer 2 or at Layer 3. Layer 2 tunneling mechanisms (*e.g.* L2TP [11]) transfer PPP packets (encapsulating IP, IPX etc) across the Internet or other transport media. Layer 3 tunneling mechanisms, on the other hand, directly encapsulate network layer packets (*e.g.* IP, IPX) in IP. A number of Layer-3 tunneling protocols have been proposed (TEP [4], TSP [18]) that extend the basic Mobile IP protocol to allow chaining of multiple tunnel segments. All of these tunneling proposals ([11, 4, 18]) rely on IPSec to provide confidentiality, integrity and authenticity when the transport medium is the Internet. Currently, L2TP seems to have captured the largest mindshare among VPN technologies. Nevertheless, we feel that Layer 3 tunneling offers a superior solution especially when the underlying transport is the Internet. These advantages include:

- Better bandwidth utilization. Running protocol X over PPP over UDP (as with L2TP across the Internet) is less efficient than running protocol X directly over IP. (X may be IP, IPX etc)
- Greater reliability. With layer-two tunneling, each end point maintains a PPP state machine (including timers and retransmission logic) across a “simulated serial line”. Unlike a real serial line, end points of the simulated line are often separated by large distances and/or many hops with only best effort delivery. As such, the PPP connections are prone to timeouts and frequent resets.

If multi-protocol support is considered unimportant, IPSec alone can go a long way in solving the secure, remote access problem. From a deployment perspective, it is perhaps easier to establish secure tunnels that extend from a corporate network’s periphery to an ISP rather than all the way to the end-user device. The latter requires IPSec software on the portable device but offers the following advantages:⁴

- End-users are free to connect to their corporate network irrespective of the ISP used to “get on to the Internet”.
- Corporations do not need to establish a trust relationship with ISPs, they only need to trust their own employees. A corporation may be willing to trust an ISP based in the same country but may not be willing to trust an ISP based in another country even if the two ISPs are members of a roaming consortia. One can also think of several situations where an employee may connect to the Internet through a “provider” that has no prior agreements with the user’s corporation. Examples of such “internet providers”

⁴ As IPSec standards mature, we expect operating system vendors to bundle this functionality, greatly alleviating the deployment challenge.

include universities or temporary "terminal rooms" provided at academic and industry conferences.

IPSec based remote access requires an IPSec-capable node within the corporate firewall complex. Filtering and access control rules should be set up so that IPSec packets, and others necessary for establishing security associations, can be exchanged freely between this node and the general Internet. The address of this "IPSec gateway" must be known to external mobile hosts. The exact discovery mechanism is irrelevant to the subsequent discussion. Manual configuration and DNS lookup (*e.g.* using KX records [1]) are just two of the possible alternatives.

Very often, corporate networks use private addresses that are not advertised to the general Internet. Furthermore, internal routers are generally unaware of external addresses and return "ICMP unreachable" messages for such destinations (assuming they do not use default routing). This creates the challenge of ensuring end-to-end delivery between a host with an internal address (*e.g.* corporate file- or mail-server) and a host connected to the Internet using an external address. There are two basic approaches to this problem:

1. The first approach adds Network Address Translation (NAT) functionality at the IPSec gateway. After authenticating arriving packets, and before injecting them into the private network, the gateway does a NAT operation, replacing the external source address with its own IP address (the gateway may be assigned a range of internal addresses). This way when an internal host responds, it uses a destination address that is "valid" inside the corporate network. The response packet reaches the IPSec gateway, undergoes a reverse address translation, and IPSec processing before it is sent to the remote host [6].

Inserting NAT in the communication path can "break" certain applications. Some applications carry network address information (IP address and/or TCP/UDP port) as part of their payload and performing NAT for such packets can get complicated, *e.g.* replacing the IP address or port information in the application payload may require adjustments to the IP packet length. Certain NAT implementations go to great lengths to accommodate these applications while others simply let them fail silently. Similarly, applications in which an internal host must initiate connections (rather than the external host) are also harder to support and may require workarounds, *e.g.* FTP's passive mode may need to be turned on.

In spite of these limitations, this approach is quite attractive as it requires nothing more than IPSec on the portable device. Even the internal hosts do not require any changes.

2. Another option for preventing the exposure of external addresses to internal routers is to use an extra level of IP-in-IP tunneling between the IPSec gateway and the internal host. This requires the internal host (or a proxy such as a Mobile IP home agent) to support IP-in-IP encapsulation and decapsulation. The principal advantage of this approach is that it transparently enables all applications and can be easily extended to work with Mobile IP [9, 10, 18, 19].

The portable device must also be responsible for securing the private network, because it extends its periphery. Therefore, it must implement some firewall capabilities, otherwise, any malicious individual that gains access to it will have gained access to the private network as well.

5 Enabling Groups of Users

We have also been investigating mechanisms to support small teams of mobile users traveling together. Disaster recovery teams offer an excellent example of this scenario. Another example may be a sales team traveling together that wishes to set up a “temporary branch office” of their corporation at a convention center. These situations call for “thin servers” around which a small network can be quickly established. This network may be based on either wireless or wireline LAN technologies. We have prototyped such a device and call it a Remote Site Server (RSS). An RSS can fulfill the booting, configuration, security, and routing needs of an assortment of connected clients. It offers DHCP, DNS, Mail, web-caching, file-sharing and firewall services. It also acts as a router to the outside world and can provide both network address translation (NAT) and secure communication capabilities. The NAT feature is handy for hiding multiple hosts on a private network behind a single ISP-provided IP address. All communication involving any of the hosts behind the thin server appears to originate from the thin server. This communication can either be in the clear or secured through IP-level or higher-level encryption and authentication, when necessary. The same VPN technologies that were described earlier (see Section 4) for connecting individual remote hosts to private networks are also applicable here. A variety of Internet connectivity options are supported including ethernet and dial-up PPP. Since the task of establishing Internet connectivity, negotiating network access across firewalls, and warding off hackers is off-loaded to the thin server, individual clients behind it need not concern themselves with any of the associated complexities. One may think of the RSS as a power-device (see Section 4) enhanced with server software to support protected workgroups.

The RSS feature-set is also a good match for small-office or home-office (SOHO) computing. These offices can be viewed as less volatile, or smaller, variations of “temporary” branch offices. These situations can benefit from most of the capabilities of the RSS but may not need the VPN capabilities. For example, a small, independently owned flower shop may not have a “parent” office with which it may need to establish secure channels.

One possible use of our remote site server is in supporting multiple satellite offices of a corporation. In any large deployment of these systems, ensuring that each is installed correctly and with the latest software packages is a major undertaking. We have addressed these issues in several ways.

We have developed a framework for automating the installation, upgrade and configuration of software packages on the thin server. This framework organizes different software packages into distinct clusters. Each cluster can be independently installed and, if an older version of the cluster is detected, it can

be automatically upgraded with a newer version. The framework stores configuration information separately from the software. This allows a pre-existing configuration to be reused with the newly updated software and eliminates the overhead of unnecessary reconfiguration. The thin server offers an HTML form-based administrative interface. As such, there is no need to connect a monitor to the thin server, and it can be managed from any device equipped with a web browser. In some cases, troubleshooting or special administration tasks may require complete shell access to the thin server. Our prototype offers telnet access (through a Java applet) to administrators on the local network and Secure Shell (SSH) login for remote administrators.

6 Conclusion

We have presented our vision of a *Complete Computing* environment. We leverage a common set of mechanisms to enable *mobile, nomadic, remote, branch office* and *small office* computing, hitherto addressed as disparate problems. From a user-centric point of view, the important distinctions are not directly related to any of the aforementioned modes of computing, but to the characteristics of the device used. Table 1 correlates the type of device to the user experience it affords. In all cases, the first step is to establish a communication path to the private network by (1) *hopping* on the internet, and (2) negotiating access past the corporate firewall. Having done this, the user (or the device on the user's behalf) has obtained access to the resources within the private network. However, the level of service with which these resources are now available reflect the characteristics of the device used by the remote user.

Using a Java and HTTPS enabled device allows the maximum degree of nomadicity. The user is able to use almost any portable computing device, and may not, in fact, carry one with him. These devices allow personal mobility in addition to nomadicity. However, the task of hopping on the internet is typically done by dialing into an ISP. This does not constitute automatic network configuration, as the user still has to worry about phone numbers, baud rate, and similar parameters.⁵ Similarly, the firewall traversal is an explicit phase in which the user has to authenticate itself before gaining access to the private resources. Having accomplished this, the user is able to access but a handful of applications from the private network.

Specially configured devices also use ISP accounts to hop on the internet. Using IPSec mechanisms may make it easier to negotiate access past the firewall, but this step still exists. However, the level of application support improves considerably. Using these types of devices, it is possible to establish network level connections with the application servers within the private network. Full mobility is now possible.

Finally, devices that provide group support shield their clients from direct internet usage. Group support devices, such as our *Remote Site Server* create

⁵ Strictly speaking, it is possible to establish internet presence by completely automatic means such as DHCP. However, typical ISP accounts do not yet allow this.

a protected workgroup safely ensconced away from the intimidating internet. A device within the protected workgroup benefits from automatic network configuration via DHCP support at the thin server. Likewise, the latter performs any required firewall negotiation on behalf of its clients. Given that the connection mechanisms used by the thin server to access servers in the corporate network are identical to those used by specially configured devices, the clients in the protected workgroup also enjoy a very high level of service.

Table 1. Modes of access when away from the the home network

Device Requirements	User Experience				
	Establishing a communication path		Level of Service		
	Auto. network config.	Implicit firewall traversal	Some apps (web based)	All or most apps (nomadic mode)	All applications (mobile mode)
Java and HTTPS enabled browser	N	N	Y	N	N
Specially configured devices	N	N	Y	Y	Y
Group support	Y	Y	Y	Y	Y

References

1. Atkinson, R.: Key Exchange Delegation Record for the DNS, *RFC 2230*, (Nov. 1997).
2. Aziz, A., Patterson, M.: Design and Implementation of SKIP, available on-line at <http://skip.incog.com/inet-95.ps>. A previous version of the paper was presented at INET '95 under the title *Simple Key Management for Internet Protocols (SKIP)*, and appears in the conference proceedings under that title.
3. Berners-Lee, T., Masinter, L., McCahill, M.: Uniform Resource Locators (URL), *RFC 1738*, (Dec. 1994).
4. Calhoun, P., Perkins, C.: Tunnel Establishment Protocol, Internet draft *draft-ietf-mobileip-calhoun-tep-00.txt* – work in progress, (1997).
5. Chapman, D. B., Zwicky, E.: *Building Internet Firewalls*, O'Reilly & Associates, Inc., (1995).
6. Doraswamy, N., Moskowitz, R.: Implementation of VPNs with IP Security, Internet-draft – work in progress, (1997).
7. Droms, R.: Dynamic Host Configuration Protocol, *RFC 2131*, (Mar. 1997).
8. Frier, A., Karlton, P., Kocher, P.: The SSL 3.0 Protocol, Netscape Communications Corp., (Nov. 1996).
9. Gupta, V., Glass, S.: Firewall traversal for Mobile IP: guidelines for firewalls and Mobile IP entities, Internet Draft *draft-ietf-mobileip-firewall-trav-00.txt* – work in progress, (Mar. 1997).

10. Gupta, V., Montenegro, G.: Secure and Mobile Networking, to appear in the ACM Journal on Special Topics in Mobile Networking and Applications (MONET), (special issue on Mobile Networking in the Internet).
11. Hamzeh, K., *et al.*: Layer Two Tunneling Protocol (L2TP), Internet Draft *draft-ietf-pppext-l2tp-08.txt* – work in progress, (Nov. 1997).
12. Harkins, D., Carrel, D.: The resolution of ISAKMP with Oakley, Internet Draft *draft-ietf-ipsec-isakmp-oakley-05.txt* – work in progress, (Nov. 1997).
13. Kent, S., Atkinson, R.: Security architecture for the Internet Protocol, Internet Draft *draft-ietf-ipsec-arch-sec-02.txt* – work in progress, (Nov. 1997) (a previous version appears as *RFC 1825*).
14. Kent, S., Atkinson, R.: IP authentication header, Internet Draft *draft-ietf-ipsec-auth-header-03.txt* – work in progress, (Nov. 1997) (a previous version appears as *RFC 1826*).
15. Kent, S., Atkinson, R.: IP encapsulating security payload, Internet Draft *draft-ietf-ipsec-esp-v2-02.txt* – work in progress, (Nov. 1997) (a previous version appears as *RFC 1827*).
16. Kistler, J. J., Satyanarayanan, M.: Disconnected Operation in the Coda File System, *ACM Transactions on Computer Systems*, **10**, No. 1, (Feb. 1992) 3–25.
17. Maughan, D., Schertler, M., Schneider, M., Turner, J.: Internet Security Association and Key Management Protocol (ISAKMP), Internet Draft *draft-ietf-ipsec-isakmp-08.txt* – work in progress, (Jul. 1997).
18. Montenegro, G.: Tunnel Set-up Protocol (TSP), Internet Draft *draft-montenegro-tsp-00.txt* – work in progress, (Aug. 1997).
19. Montenegro, G., Gupta, V.: Firewall support for Mobile IP, Internet Draft *draft-montenegro-firewall-sup-02.txt* – work in progress, (Nov. 1997).
20. Orman, H.: The OAKLEY Key Determination Protocol, Internet Draft *draft-ietf-ipsec-oakley-02.txt* – work in progress.
21. Perkins, C., (Editor): IP mobility support, *RFC 2002*, (Oct. 1996).
22. Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., Lear, E.: Address allocation for private internets, *RFC 1918*, (Feb. 1996).
23. Simpson, W.: The Point-to-Point Protocol (PPP), *RFC 1661*, (Jul. 1994).
24. Veizades, J., Guttman, E., Perkins, C., Kaplan, S.: Service Location Protocol, *RFC 2165*, (Jun. 1997).
25. Yeong, W., Howes, T., Kille, S.: Lightweight Directory Access Protocol, *RFC 1777*, (Mar. 1995).

ATTACHMENT 1C

Search WorldCat

Search

[Advanced Search](#) [Find a Library](#)

[<< Return to Search Results](#)

[Cite/Export](#)

[Print](#)

[E-mail](#)

[Share](#)

[Permalink](#)

[Add to list](#)

[Add tags](#)


[Write a review](#)

Rate this item: 1 2 3 4 5



[Preview this item](#)

Worldwide computing and its applications, WWCA'98 : Second International Conference, Tsukuba, Japan, March 4-5, 1998 : proceedings

Author: [Y Masunaga; Takuya Katayama](#)
 Publisher: Berlin ; New York : Springer, ©1998.
 Series: [Lecture notes in computer science](#), 1368.
 Edition/Format:  Print book : Conference publication : English [View all editions and formats](#)

Summary: This book constitutes the refereed proceedings of the Second International Conference on Worldwide Computing and Its Applications, WWCA'98, held in Tsukuba, Japan, in March 1998. This volume presents 14 invited and survey papers together with 20 papers selected by the conference committee. [Read less](#)

Rating: (not yet rated) [0 with reviews - Be the first.](#)

Subjects: [Electronic data processing -- Congresses.](#)
[Informatique mobile -- Congrès.](#)
[Informatique -- Congrès.](#)
[View all subjects](#)

More like this [Similar Items](#)

Get a Copy

[Find a copy in the library](#)

[AbeBooks](#) \$1.15

[Amazon](#) \$29.98

[Barnes & Noble](#) \$86.97

Find a copy online

Links to this item

[lib.uwo.ca](#)
Connect to Internet resource

Find a copy in the library


Enter your location: [Find libraries](#)

Submit a complete postal address for best results.

Displaying libraries 1-6 out of 301 for all 24 editions (Ithaca, NY 14850, USA)

Show libraries holding [just this edition](#)

[<< First](#) [< Prev](#) [1](#) [2](#) [3](#) [Next >](#) [Last >>](#)

Library	Held formats	Distance	
1. Cornell University Library Ithaca, NY 14853 United States	 Book	1 mile MAP IT	Library info Search at this library Ask a librarian

- [Add to favorites](#)
- | | | | | |
|----|--|--|-------------------------------------|---|
| 2. | Syracuse University
Syracuse, NY 13244 United States |  Book | 44 miles
MAP IT | Library info
Ask a librarian
Add to favorites |
| 3. | University of Rochester
Rochester, NY 14627 United States |  Book | 75 miles
MAP IT | Library info
Add to favorites |
| 4. | SUNY at Buffalo University at Buffalo
Buffalo, NY 14260 United States |  Book | 123 miles
MAP IT | Library info
Ask a librarian
Add to favorites |
| 5. | Pennsylvania State University Libraries
University Park, PA 16802 United States |  Book | 135 miles
MAP IT | Library info
Add to favorites |
| 6. | University at Albany University Libraries
Albany, NY 12222 United States |  Book | 136 miles
MAP IT | Library info
Ask a librarian
Add to favorites |

« First < Prev 1 2 3 Next > Last »

Details

Genre/Form: Conference papers and proceedings
Congresses
Congrès

Material Type: Conference publication, Internet resource

Document Type: Book, Internet Resource

All Authors / Contributors: [Y Masunaga](#); [Takuya Katayama](#)

Find more information about:

ISBN: 3540642161 9783540642169

OCLC Number: 38474336

Description: xiv, 471 pages : illustrations ; 24 cm.

Contents: WWC and the hyper information age.- Global high performance research network: An Asia-Pacific perspective.- Java applications and implementations.- Back to home: Where computers and networking should go.- ObjectSpace voyager - The agent ORB for Java.- Worldwide component scripting with the Planet mobile object system.- Scalability in object-oriented distributed systems environment OZ.- Rapide: A language and toolset for causal event modelling of distributed system architectures.- An architecture of software commerce broker over the internet.- Distributed process management system based on object-centered process modeling.- Systems software for multimedia computing.- Environment server: A system support for adaptive distributed applications.- Compiler-generated protection domains and a light weight runtime protection technique.- Complete computing.- Compact and flexible resolution of CBT multicast key-distribution.- Integrating resource reservation with rate-based transport protocols in AMInet.- Experiences with a mobile testbed.- Design and implementation of mobile IP system with security consideration.- A network architecture for continuous mobility.- Towards internationalized Web creation.- ISCM information system conceptual model oriented to security problems and a tool implementing it.- Design of EDI security MIB based on SNMP protocol.- The block-world data model for a collaborative virtual environment.- CyPhone - mobile multimodal personal augmented reality.- On business intelligence systems.- Supporting collaboration through teleproximity.- A home office system based on a virtual shared room: An environment corresponding to degree of concentration.- Electronic binder system: Promotion of an ISO9001-based quality system using the WWW and experience from its application.- Update monitoring: The CQ project.- dLIMIT - A middleware framework for loosely-coupled database federations.- Autonomic buffer control of web proxy server.- Getting users' attributes without violating anonymity.- Bayanihan: Web-based volunteer computing using Java.- Architecture of a user interface module for structured internet messages.

Series Title: [Lecture notes in computer science](#), 1368.

Responsibility: Yoshifumi Masunaga, Takuya Katayama, Michihara Tsukamoto (eds.).

More information: [Table of contents](#) [Publisher description](#)

Reviews

User-contributed reviews

[Add a review](#) and share your thoughts with other readers. Be the first.

Tags

[Add tags](#) for "Worldwide computing and its applications, WWCA'98 : Second International Conference, Tsukuba, Japan, March 4-5, 1998 : proceedings". Be the first.

Similar Items

Related Subjects: (10)

[Electronic data processing -- Congresses.](#)

[Informatique mobile -- Congrès.](#)

[Informatique -- Congrès.](#)

[Technologie de l'information -- Congrès.](#)

[Electronic data processing.](#)

[Computernetwerken.](#)

[Teleinformatica.](#)

[Réseaux à grande distance \(informatique\) -- Congrès.](#)

[Internet -- Congrès.](#)

[Web -- Congrès.](#)

Linked Data

ATTACHMENT 1D

Worldwide computing and its applications-- WWCA'98

Second International Conference, Tsukuba, Japan, March 4-5, 1998 : proceedings
Yoshifumi Masunaga, Takuya Katayama, Michiharu Tsukamoto (eds.).

Availability

Library Annex

QA75.5 .W18x 1998

✓ Available

Other forms of this work

Worldwide computing and its applications, WWCA'98

📖 Book English Online

See all forms of this work

Author, etc.:

WWCA '98 (1998 : Tsukuba-shi, Japan)

Format:

📖 Book

Language:

English.

Published:

Berlin ; New York : Springer, c1998.

Subject:

Electronic data processing > Congresses.

Description:

xiv, 471 p. : ill., maps ; 24 cm.

ISBN:

3540642161 (pbk. : alk. paper)

Other contributor:

Masunaga, Y. (Yoshifumi), 1941-

Katayama, Takuya, 1939-

Tsukamoto, Michiharu.

Series:

Lecture notes in computer science, 1368

Notes:

Includes bibliographical references and index.



Browse related items by call number

QA75.5 .W18x 1998

ATTACHMENT 1E

Librarian View

LEADER 01368fam a2200337 a 4500
001 3271402
005 20161205094101.0
008 980213s1998 gw ab b 101 0 eng
010 +a 98014455
020 +a 3540642161 (pbk. : alk. paper)
035 +a (NIC)notisAQV9704
035 +a (OCoLC)38474336
035 +a 3271402
040 +a DLC +c DLC +d C#P +d NIC
050 0 0 +a QA75.5 +b .W18 1998
082 0 0 +a 004/.36 +2 21
111 2 +a WWCA '98 +d (1998 : +c Tsukuba-shi, Japan)
245 1 0 +a Worldwide computing and its applications-- WWCA'98 :
+b Second International Conference, Tsukuba, Japan,
March 4-5, 1998 : proceedings / +c Yoshifumi Masunaga,
Takuya Katayama, Michiharu Tsukamoto (eds.).
260 +a Berlin ; +a New York : +b Springer, +c c1998.
300 +a xiv, 471 p. : +b ill., maps ; +c 24 cm.
440 0 +a Lecture notes in computer science, +x 0302-9743 ; +v
1368
504 +a Includes bibliographical references and index.
650 0 +a Electronic data processing +x Congresses.
650 7 +a Electronic data processing +2 fast +0
(OCoLC)fst00906956
655 7 +a Conference papers and proceedings +2 fast +0
(OCoLC)fst01423772
700 1 +a Masunaga, Y. +q (Yoshifumi), +d 1941-
700 1 +a Katayama, Takuya, +d 1939-
700 1 +a Tsukamoto, Michiharu.
905 +a 19980624120000.0
948 2 +a 20141218 +b m +d batch +e lts +x addfast
948 2 +a 20161205 +b m +d batch +e lts +x fix655fast

ATTACHMENT 1F

[Library of Congress](#) >> [MARC](#) >> **Bibliographic**



MARC 21 Format for BIBLIOGRAPHIC DATA

Library of Congress
Network Development and MARC Standards Office

1999 Edition

Update No. 1 (October 2000) through Update No. 27 (November 2018)

This online publication provides access to both the full and concise versions of the *MARC 21 Format for Bibliographic Data*. The "full" bibliographic format contains detailed descriptions of every data element, along with examples, input conventions, and history sections. The "concise" bibliographic format contains abridged descriptions of every data element, along with examples. The full and concise versions are identified in the header of each field description.

Changes to the *MARC 21 Format for Bibliographic Data* that resulted from Update No. 27 (November 2018) are displayed in **red** print. The date located in the header of the full version of each field indicates the last month and year of update.

Table of Contents

- [Introduction](#) [[Full](#) | [Concise](#)]
- [Format Summary](#)
- [Leader](#) [[Full](#) | [Concise](#)]
- [Directory](#)
- [00X: Control Fields](#)
- [01X-09X: Numbers and Code Fields](#)
- [Heading Fields - General Information](#)
- [1XX: Main Entry Fields](#)
- [20X-24X: Title and Title-Related Fields](#)
- [25X-28X: Edition, Imprint, Etc. Fields](#)
- [3XX: Physical Description, Etc. Fields](#)
- [4XX: Series Statement Fields](#)
- [5XX: Note Fields](#)
- [6XX: Subject Access Fields](#)
- [70X-75X: Added Entry Fields](#)
- [76X-78X: Linking Entry Fields](#)
- [80X-83X: Series Added Entry Fields](#)
- [841-88X: Holdings, Location, Alternate Graphics, Etc. Fields](#)
- [Appendix A: Control Subfields](#)
- [Appendix B: Full Level Record Examples](#)
- [Appendix C: Minimal Level Record Examples](#)
- [Appendix D: Multiscript Records](#)
- [Appendix E: Alphabetical List of Ambiguous Headings](#)
- [Appendix F: Initial Definite and Indefinite Articles](#)
- [Appendix G: Format Changes for Update No. 27 \(November 2018\)](#)
- [Appendix H: Local Data Elements](#)
- [Appendix I: Organization Code Sources](#)

[Library of Congress](#) >> [MARC](#) >> **Bibliographic**
(11/09/2018)

[Contact Us](#)

ATTACHMENT 1G



MARC STANDARDS

Frequently Asked Questions (FAQ)

Network Development and MARC Standards Office
Library of Congress

General Information

- [What is MARC 21? What does the acronym “MARC” mean?](#)
- [How does MARC 21 differ from the USMARC and CAN/MARC formats?](#)
- [Who maintains the MARC 21 formats?](#)
- [What are the Network Development and MARC Standards Office and the Standards Division?](#)
- [Are there any discussion groups or forums for the MARC 21 formats?](#)

MARC 21 Documentation

- [What documentation is available and how do I obtain it?](#)
- [How often is MARC 21 documentation updated?](#)
- [May I use excerpts from MARC 21 documentation?](#)

MARC 21 Tutorials

- [Are there any tutorials for the MARC 21 formats?](#)

MARC, SGML, XML and other metadata standards

- [Are there SGML or XML versions of the MARC 21 formats?](#)
- [Is MARC 21 mapped to other metadata standards? Are other standards mapped to MARC 21?](#)

MARC 21 Translations

- [Are there any translations of the MARC 21 formats?](#)
- [I would like to translate a MARC 21 publication. What should I do?](#)

Tools, Systems and Services That Work With MARC 21

- [Is there a list of tools compatible with the MARC 21 formats?](#)
- [Is there a list of MARC 21 record services?](#)
- [How do I add a record service, vendor system or tool to these lists?](#)
- [What systems are compatible with the MARC 21 formats?](#)

Making Changes to the MARC 21 Formats and Code Lists

- [How do I report errors in MARC 21 documentation?](#)
- [How do I propose making a change to the MARC 21 formats?](#)
- [How do I request new or revised MARC 21 organization codes?](#)
- [How do I request MARC 21 relator, sources, or description convention codes?](#)

Record Requirements and Record and File Specifications for MARC 21

- [Where do I find the U.S. National Level/Minimal Level Record Requirements for the MARC 21 formats?](#)
- [What are the appropriate record and file specifications for the formats?](#)
- [What are the specifications for character sets?](#)

Electronic resources and MARC 21

- [How do I code electronic resources in a MARC 21 record?](#)

General Information

What is MARC 21? What does the acronym “MARC” mean?

MARC is the acronym for MACHine-Readable Cataloging. It defines a data format that emerged from a Library of Congress-led initiative that began nearly forty years ago. It provides the mechanism by which computers exchange, use, and interpret bibliographic information, and its data elements make up the foundation of most library catalogs used today. MARC became USMARC in the 1980s and MARC 21 in the late 1990s.

How does MARC 21 differ from the USMARC and CAN/MARC formats?

MARC 21 is not a new format. After having discussions and making minor changes to both formats that accommodated USMARC and CAN/MARC users' specific needs, the USMARC and CAN/MARC (Canadian MARC) formats were “harmonized” into MARC 21 in 1997. See <http://www.loc.gov/marc/annmarc21.html> for more information about the harmonization.

Who maintains the MARC 21 formats?

The Network Development and MARC Standards Office at the Library of Congress and the Standards and the Support Office at the Library and Archives Canada maintain the MARC 21 formats. Input for development is provided by MARC 21 users from around the world, including libraries, library networks and utilities, and library system vendors. See <http://www.loc.gov/marc/overview.html> for more information about the development and maintenance of the formats.

What are the Network Development and MARC Standards Office and the Standards Division?

The [Network Development and MARC Standards Office](#) plans and develops library and information network standards at the Library of Congress. It is the maintenance agency for several national standards, including the MARC 21 formats. To contact it, please e-mail ndmso@loc.gov.

The [Standards Division](#) at the Library and Archives Canada maintains and supports the MARC 21 formats and other library standards. To contact it, please e-mail BAC.Normesdecatalogage-Cataloguingstandards.LAC@canada.ca.

Are there any discussion groups or forums for the MARC 21 formats?

The [MARC Forum](#) is a listserv maintained by the Network Development and MARC Standards Office and is open to anyone interested in the implementation, maintenance and development of the MARC 21 formats. The forum provides an opportunity for members of the information community to participate in discussions related to the formats. Vendor, network, technical service, automation, and reference staff and researchers are encouraged to participate. While there is a close linkage between MARC 21 and the cataloging of materials, the focus of the forum is on the use of MARC 21 as a communications format.

[Back to Top](#)

MARC 21 Documentation

What documentation is available and how do I obtain it?

The [MARC Standards](#) page has links to both extensive documentation on MARC 21, including both the full and concise formats, code and field lists, information about MARC 21 development, and documentation to help users with the MARC 21 format. There is a [format overview](#) listing changes to MARC documentation. Some documentation is also available in [translation](#). A [bibliography](#) is also available on the Library's MARC Standards webpage.

Documentation of French versions of some of the formats in Canada is available at [Library and Archives Canada](#).

How often is MARC 21 documentation updated?

The MARC 21 formats are updated two times per year, in the spring and fall. Other documentation is updated as it becomes necessary.

May I use excerpts from MARC 21 documentation?

Using excerpts is permissible as long as credit is given.

[Back to Top](#)

MARC 21 Tutorials

Is there a tutorial for the MARC 21 formats?

[Understanding MARC Bibliographic](#) is a good introduction to the MARC 21 bibliographic format and includes a bibliography, discussion questions and examples. It is widely used and has been translated into several different languages.

[Understanding MARC Authority Records](#) is a good introduction to the MARC 21 authority format and includes a bibliography, discussion questions and examples.

Both *Understanding MARC Bibliographic* and *Understanding MARC Authority Records* are also available as booklets from the [Cataloging Distribution Service](#).

[Back to Top](#)

MARC 21, SGML, XML and other metadata standards

Are SGML or XML versions of the MARC 21 formats available?

The Network Development and MARC Standards Office has developed a framework for working with MARC data in a XML environment. This framework is intended to be flexible and extensible, allowing users to work with MARC data in ways that meet their specific needs. The framework contains many components such as schemas, stylesheets, and software tools developed and maintained by the Library of Congress. Conversion utilities between MARC (ISO 2709) and MARCXML are also available. Please see www.loc.gov/marc/marcxml.html.

The Network Development and MARC Standards Office also developed a MARC to SGML and SGML to MARC conversion program. The following documents contain the program and additional information:

- [MARC DTDs: Background and Development](#)
- [MARC DTDs: Beta Test Version](#)
- [MARC-SGML and SGML-MARC Conversion Program User Guide](#)
- [MARC-SGML and SGML-MARC Conversion Programs Maintenance Guide](#)

A list of some tools that work with HTML, SGML and XML applications is at <http://www.loc.gov/marc/marctools.html>.

Is MARC 21 mapped to other metadata standards? Are other standards mapped to MARC 21?

MARC 21 has been mapped to the following metadata standards:

- [MODS](#)
- [Dublin Core](#)
- [MARC Character Sets to UCS/Unicode](#)
- [Digital Geospatial Metadata](#)
- [RDA](#) (See Tools tab)

The following metadata standards have been mapped to MARC 21:

- [MODS](#)
- [Dublin Core](#)
- [UNIMARC to MARC 21](#)
- [ONIX](#)
- [Digital Geospatial Metadata to MARC](#)
- [RDA](#) (See Tools tab)

[Back to Top](#)

MARC 21 Translations

Are there any translations of the MARC 21 formats?

The [MARC 21 Translations](#) page contains a list of documents that are either direct translations or close adaptations of the MARC 21 formats and other MARC documentation. Where applicable, information regarding differences between the translations and MARC 21 is provided. The formats are listed alphabetically by the language of each translation and include full bibliographic citations and contact information.

I would like to translate a MARC 21 publication. What should I do?

Translations of the MARC 21 formats and other MARC documentation are greatly encouraged because of their usefulness to the entire MARC 21 community. The [Network Development and MARC Standards Office](#) does ask that intellectual credit information be included in the translation. The following statement is recommended:

“The MARC 21 [insert name of publication that was translated] was originally prepared by the Network Development MARC Standards Office, Library of Congress and the Standards Division, Library and Archives Canada. It has been translated with permission.”

Once you complete your translation, please send the Network Development and MARC Standards Office an official announcement that includes your publication's bibliographic information and contact information on obtaining copies. If possible, send a printed copy for our collection of translations. If the translation is available on the Internet, please include its URL for inclusion on the [MARC 21 Translations](#) page. Listing a translation is not mandatory; however translations are extremely useful to other MARC 21 users.

A [Translators's Tools](#) page contains additional information about translating MARC 21 documents.

[Back to Top](#)

Tools, Systems and Services That Work With MARC 21

Is there a list of tools compatible with the MARC 21 formats?

A list of some of the bibliographic tools that support the MARC 21 formats is at www.loc.gov/marc/marctools.html. It includes software programs that provide enhanced usability to MARC 21 records and systems. Some of the tools are freeware or open source.

Is there a list of MARC 21 record services?

A list of some of the record services that support the MARC 21 formats is at www.loc.gov/marc/marcrecsvrs.html. It includes services that distribute MARC 21 records, such as records for copy cataloging, records supplied with materials, records used for recon purposes, updated records, conversion services, etc.

What systems are compatible with the MARC 21 formats?

A list of some of the systems that support the MARC 21 formats is at www.loc.gov/marc/marcsysvend.html. The list includes systems that collect, organize and manage MARC 21 records.

How do I add a record service, vendor system or tool to these lists?

Vendors, software producers, and anyone else who provides vendor records, system services, or who has developed specialized MARC tools, are encouraged to fill out a [submission form](#).

Please note: Individuals who submit the form on someone else's behalf should put their contact information in the "Citation Contact" field and the name of the individual/company on whose behalf the form is submitted in the "Product Contact" field.

[Back to Top](#)

Making Changes to the MARC 21 Formats and Code Lists

How do I report errors in MARC 21 documentation?

If you notice an error or omission in either the print or online MARC 21 documentation, please contact ndmso@loc.gov. Describe the error and where it occurs. Please be as specific as possible.

How do I propose making a change to the MARC 21 formats?

Proposals for changes to the formats may originate from any MARC 21 user. Please either fill out the [MARC 21 Formats Proposed Change Form](#) or contact the [Network Development and MARC Standards Office](#) at the Library of Congress or the [Standards division](#) at the Library and Archives Canada. Maintenance agency staff at the Library of Congress and the Library and Archives Canada write, edit and review proposals and discussion papers twice a year and distribute them via the [MARC Forum listserv](#) and the MARC Standards web site. Discussions at the semiannual [MARBI \(Machine-Readable Bibliographic Information\)](#) meetings in the United States and the annual [CCM \(Canadian Committee on MARC\)](#) meeting in Canada, along with suggestions received by e-mail and the listserv, are used by the maintenance agencies to make final decisions on the proposals.

How do I request new or revised MARC 21 organization codes?

Before requesting a MARC 21 organization code, please first search the [MARC Code List for Organizations](#). If you do not find a code for your organization, click on one of these links to access a request form in the language of your choice.

[\[ENGLISH\]](#) [\[ESPAÑOL\]](#) [\[PORTUGUÊS\]](#)

You may use the online form to request up to three codes. If more than three codes are needed, please submit a list of the organizations with their names and addresses (including street, city, state, postal code, and country) via email to ndmso@loc.gov. Please include contact information. Note: Attachments to e-mail messages are not accepted.

The *MARC Code List for Organizations* is updated frequently, as codes are often added. Since information in a request must be verified and then incorporated into the list, there is a short delay between the time of the request and the appearance of a newly-assigned code in the database. Names and addresses are revised when changes are reported.

Requests for the assignment of new codes or changes involving organizations in Canada should be sent to the [Interlibrary Loan Division](#) at the Library and Archives Canada.

Requests for the assignment of new codes or changes involving organizations in the United Kingdom should be sent to the [UK National Agency for MARC Organisation Codes](#) at the British Library.

Requests for the assignment of new MARC organization codes or for changes to codes may also be sent via fax to +1-202-707-0115 or by surface mail to:

Library of Congress
Network Development and MARC Standards Office
101 Independence Avenue, S.E.
Washington, DC, 20540-4402 USA

How do I request MARC 21 relator, sources or description convention codes?

Requests for relators, sources or description convention codes should be sent to ndmso@loc.gov.

Requests can also be faxed to +1-202-707-0115 or sent by surface mail to:

Library of Congress
Network Development and MARC Standards Office
101 Independence Avenue, S.E.
Washington, DC, 20540-4402 USA

Requests should include a full bibliographic citation and a scan, photocopy or Internet link for the item to be added.

[Back to Top](#)

Record Requirements and Record and File Specifications for MARC 21

Where do I find the U.S. National Level/Minimal Level Record Requirements for the MARC 21 formats?

There is no list of of “mandatory” data elements that must appear in a MARC 21 record. Theoretically, a record could simply consist of a leader and a 245 (title) field. However, there is a list of the MARC 21 data elements required to meet minimal and national level requirements in the United States for the [bibliographic](#) and [authority](#) formats. Please note that other countries may have different lists of required data elements.

What are the appropriate record and file specifications for the formats?

Information about the file specifications for the MARC 21 formats is in [MARC 21 Specifications for Record Structure, Character Sets, and Exchange Media](#). This document is also available from the [Cataloging Distribution Service](#). For a basic introduction to MARC 21 file and record structure, you may also want to look at [Understanding MARC Bibliographic](#).

What are the specifications for character sets?

MARC 21 records intended for broad, standard interchange should be encoded according to the following specifications. Either an 8-bit based encoding system (called MARC-8 in MARC 21 documentation) or a variable 8/16-bit encoding following ISO/IEC 10646 (UCS) and Unicode UTF-8 encoding rules (called UCS/Unicode UTF-8 in MARC 21 documentation) may be used.

A very large repertoire of characters is defined for use in the MARC-8 environment. For standard MARC 21 interchange, the use of UCS/Unicode UTF-8 is limited to this same repertoire, a subset of UCS/Unicode. This is necessary for interchange until all systems fully accommodate the complete UCS/Unicode repertoire of characters. This restriction will be periodically reviewed as the character encoding environment develops.

Please see <http://www.loc.gov/marc/specifications/speccharintro.html> for detailed information on MARC 21 character sets.

[Back to Top](#)

Electronic resources and MARC 21

How do I code electronic resources in a MARC 21 record?

The document [Guidelines for Coding Electronic Resources in Leader/06](#) assists users coding fixed fields in records for electronic resources. [Guidelines for the Use of Field 856](#) provides guidance on using field 856 (Electronic location and access) in all the MARC 21 formats. [Guidelines for Distinguishing Cartographic Electronic Resources from other Electronic Resources](#) assists catalogers working with cartographic electronic resources.

[Back to Top](#)

Go to:

- [MARC Standards Home Page](#)
- [Library of Congress Home Page](#)



Library of Congress

[Library of Congress Help Desk \(07/12/2006\)](#)

ATTACHMENT 1H

AMENDED ARTICLES OF INCORPORATION

OF

OCLC Online Computer Library Center, Inc.

- FIRST The name of the corporation shall be OCLC Online Computer Library Center, Inc. (the "Corporation").
- SECOND The place in this State where the principal office of the Corporation is to be located is in the City of Dublin, Franklin County, Ohio.
- THIRD The purpose or purposes for which the Corporation is formed are to establish, maintain, and operate a computerized library network and to promote the evolution of library use, of libraries themselves, and of librarianship, and to provide processes and products for the benefit of library users and libraries, including such objectives as increasing availability of library resources to individual library patrons and reducing the rate of rise of library per-unit costs, all for the fundamental public purpose of furthering ease of access to and use of the ever-expanding body of worldwide scientific, literary, and educational knowledge and information.
- FOURTH The affairs of the Corporation shall be managed by the Board of Trustees. The qualifications of the Trustees, together with their terms of office, manner of election, removal, change of number, filling of vacancies and of newly-created trusteeships, powers, duties and liabilities, shall, except as otherwise provided in these Articles, or by the laws of the State of Ohio, be as prescribed by the Code of Regulations.
- FIFTH There shall be two classes of members of the Corporation and they shall be OCLC Members, and Trustee Members. The voting powers of each class of members shall be only as defined in the Code of Regulations or as stated in these Articles.
- SIXTH There shall be a Global Council composed of Member Delegates as prescribed in the Code of Regulations.
- SEVENTH These Articles may be amended at any business meeting of the Trustee Members called for that purpose provided that notice of the proposed amendment(s) has been sent to the Trustee Members at least ten (10) days prior to said meeting. A two-thirds (2/3) vote of all of the authorized Trustee Members of the Corporation is required for approval.
- EIGHTH The duration of the Corporation shall be perpetual.
- NINTH No part of the earnings, dues, or receipts of the Corporation shall inure to the benefit of or be distributed to its members, trustees, officers, or other private persons, except only that the Corporation shall be authorized and empowered to pay reasonable compensation for services rendered and expenses incurred and to make payments or distributions in furtherance of the purposes set forth in Article Third hereof. No substantial part of the activities of the Corporation shall be the carrying on of propaganda, or otherwise attempting to influence
- Amended Articles of Incorporation

legislation, and the Corporation shall not participate in, or intervene in (including the publishing or distribution of statements) any political campaign on behalf of, or in opposition to, any candidate for public office. Notwithstanding any other provision of these Articles, the Corporation shall not carry on any other activities not permitted to be carried on (a) by a corporation exempt from Federal income tax under Section 501(c)(3) of the Internal Revenue Code of 1986, as amended (or the corresponding provision of any future United States internal revenue law) (the "Code") or (b) by a corporation, contributions to which are deductible under Section 170(c)(2) of the Code.

TENTH Upon the dissolution of the Corporation, the Board of Trustees shall, after paying or making provision for the payment of all of the liabilities of the Corporation, dispose of all of the assets of the Corporation exclusively for the purposes of the Corporation in such manner, or to such organization or organizations as are described in Section 170(c)(1) or (2) of the Code, as the Board of Trustees shall determine. Any of such assets not so disposed of shall be disposed of by the Court of Common Pleas of the county in which the principal office of the Corporation is then located, exclusively for such purposes or to such organization or organizations, as said Court shall determine, which are organized and operated exclusively for such purposes.

ELEVENTH These Articles supersede all prior Articles or Amended Articles.

ATTACHMENT 11

6XX - Subject Access Fields-General Information

MARC 21 Bibliographic

November 2016

- 600 - Subject Added Entry - Personal Name (R)
- 610 - Subject Added Entry - Corporate Name (R)
- 611 - Subject Added Entry - Meeting Name (R)
- 630 - Subject Added Entry - Uniform Title (R)
- 647 - Subject Added Entry - Named Event (R)
- 648 - Subject Added Entry - Chronological Term (R)
- 650 - Subject Added Entry - Topical Term (R)
- 651 - Subject Added Entry - Geographic Name (R)
- 653 - Index Term - Uncontrolled (R)
- 654 - Subject Added Entry - Faceted Topical Terms (R)
- 655 - Index Term - Genre/Form (R)
- 656 - Index Term - Occupation (R)
- 657 - Index Term - Function (R)
- 658 - Index Term - Curriculum Objective (R)
- 662 - Subject Added Entry - Hierarchical Place Name (R)
- 69X - Local Subject Access Fields (R)

DEFINITION AND SCOPE

6XX fields contain subject access entries and terms. Most of these fields contain subject added entries or access terms based on the lists and authority files identified in the second indicator (Subject heading system/thesaurus) or in subfield \$2 (Source of subject heading or term). One field contains uncontrolled subject access data.

For **mixed materials** and collections under archival control, considerable use is made of the 6XX fields to reflect the subject content of the described materials through controlled and uncontrolled headings and terms. The 7XX fields are used less frequently to provide access.

Descriptions of the first indicator and all subfield codes, as well as input conventions for the 600, 610, 611, and 630 fields, are given in the following *General Information* sections: *X00*, *X10*, *X11* and *X30*. The second indicator is described in the specific section for each field. All content designators for the 650-658 fields are described in the specific section for each field.

CONTENT DESIGNATOR HISTORY

Field 600-651 - Subject added entries

Indicator 2 - Subject heading system/thesaurus

In 1982 the use of the second indicator value in subject added entry fields 600-651 was expanded from specifying the organization that **assigned** the subject added entry to specifying the subject heading system, thesaurus, or authority file **used** by an organization to assign the subject added entry. Accordingly, values 0-3 and 5-6 became authoritative-agency data elements and their definitions were changed to the names of the list or authority file. The definition of value 4 was changed from Other subject heading. Prior to 1975, value 5 was defined in the visual materials specifications as Subject heading to be printed only in LC book catalog. Prior to 1977, value 5 was defined in the archival and manuscripts control specifications as National Union Catalog of Manuscripts (NUCMC) subject heading.

Field 647 - Subject Added Entry-Named Event [NEW, 2016]

Field 648 - Subject Added Entry-Chronological Term [NEW, 2002]

Field 652 - Subject Added Entry-Reversed Geographic [OBSOLETE, 1980]

Field 652 was an agency-defined field used by the Library of Congress for reversed geographic added entries assigned to materials classed in LC classification number span G1000-G9999. For each regular *Topic-Place* subject heading assigned, a reversed *Place--Topic* heading was also assigned. Both indicator positions were undefined. The subfield codes were: \$a (Geographic name or place element), \$x (General subject subdivision), \$y (Chronological subject subdivision), \$z (Geographic subject subdivision).

Field 662 - Subject Added Entry - Hierarchical Place Name [NEW, 2005]

Field 680 - PRECIS Descriptor String [OBSOLETE, 1991] [CAN/MARC only]

PRECIS Descriptor String is a sequence of subject index terms in which each term is preceded by a code which determines how it should appear in entries generated by a computer. The first indicator was undefined. The second indicator values 0-9 were used to link alternative subject statements to the corresponding Dewey classification number. Subfields \$a-\$z contained the text of the PRECIS Descriptor String.

Field 681 - PRECIS Subject Indicator Number (SIN) [OBSOLETE, 1991] [CAN/MARC only]

PRECIS Subject Indicator Number (SIN) is a fixed-length number ending in a modulus 11 check digit. It identifies uniquely the address of the PRECIS data consisting of string and Reference Indicator Number (RIN). The first indicator was undefined. The second indicator values 0-9 were used to link the indicator to the corresponding PRECIS string and other associated subject data. Only subfield \$a (PRECIS subject indicator number (SIN)) was defined.

Field 683 - PRECIS Reference Indicator Number (RIN) [OBSOLETE, 1991] [CAN/MARC only]

PRECIS Reference Indicator Number (RIN) is a fixed-length number ending in a modulus 11 check digit which identifies the address of a term in the machine-held thesaurus used as the source of 'See' and 'See also' references in a printed index. The first indicator was undefined. The second indicator values 0-9 were used to link the index numbers to the corresponding PRECIS descriptor string. Only subfield \$a (Reference indicator number (RIN)) was defined.

ATTACHMENT 1J



[\(/content/support\)](#)

9xx Fields

9xx Introduction

9xx fields 9xx fields are not part of the standard MARC 21 format. OCLC has defined these 9xx fields for use by the Library of Congress and for internal OCLC use: 936, 938, 956, 987, 989, and 994. Fields 901-907, 910, and 945-949 have been defined by OCLC for your local use and will pass OCLC validation. The remaining 9xx fields may also be locally defined by your library, but may not pass OCLC validation.

OCLC services OCLC services use some 9xx fields for processing. OCLC does not retain these fields in the master record. They may, however, be retained in user's archival records and institution records depending on the needs of the service. For example, field 951 is used for agent specific data for cataloging agent authorizations. This manual does not include descriptions of these fields.

The WorldCat Cataloging Partners, and other services, also use some 9xx fields to supply nonbibliographic information. Because WorldCat Cataloging Partners 9xx fields are defined by agreement between a library and a vendor, this manual does not include descriptions of these fields. OCLC removes WorldCat Cataloging Partners-defined 9xx fields from master records. You may still see 9xx fields that are not defined in OCLC master records. These fields will need to be removed before replacing the master record.

This page last revised: July 5, 2018

© 2019 OCLC (<https://www.oclc.org/en/policies/copyright.html>)

Domestic and international trademarks and/or service marks of OCLC Online Computer Library Center, Inc. and its affiliates (<https://www.oclc.org/en/policies/trademarks.html>)

OCLC websites store cookies on your device to improve your user experience! See our [Cookie Notice](#) to learn more. (<https://policies.oclc.org/en/privacy/cookie-statement.html>)

✓ Accept

ATTACHMENT 1K

050 - Library of Congress Call Number (R)

MARC 21 Bibliographic - Full

December 2017

First Indicator

Existence in LC collection
 # - No information provided
 0 - Item is in LC
 1 - Item is not in LC

Second Indicator

Source of call number
 0 - Assigned by LC
 4 - Assigned by agency other than LC

Subfield Codes

\$a - Classification number (R)	\$3 - Materials specified (NR)
\$b - Item number (NR)	\$6 - Linkage (NR)
\$0 - Authority record control number or standard number (R)	\$8 - Field link and sequence number (R)
\$1 - Real World Object URI (R)	

FIELD DEFINITION AND SCOPE

Classification or call number that is taken from *Library of Congress Classification* or *LC Classification Additions and Changes*. The brackets that customarily surround alternate class/call numbers are not carried in the MARC record; they may be generated based on the presence of repeated \$a subfields.

Second indicator values distinguish between content actually assigned by the Library of Congress and content assigned by an organization other than LC.

Note that only subfield \$u is locally defined. The entire field description is repeated here for ease of use of this document.

GUIDELINES FOR APPLYING CONTENT DESIGNATORS

■ INDICATORS

First Indicator - Existence in LC collection

Whether or not the item is contained in the LC collections.

- No information provided

Used for all call numbers assigned by agencies other than the Library of Congress.

050 #4\$aNB933.F44\$bT6

0 - Item is in LC

Item is in the LC collections under the call number given in the field.

Other agencies should use this value when transcribing from LC cataloging copy on which the call number is neither enclosed within brackets nor preceded by a Maltese cross.

050 00\$aZ695.7\$b.B37 1980

1 - Item is not in LC

Item is not in the LC collections, or that it is not shelved under that number.

Used by other agencies when transcribing from LC copy on which the call number appears in brackets or is preceded by a Maltese cross. Brackets that customarily surround call numbers for items not in LC are not carried in the MARC record; they may be generated for display.

050 10\$aBJ1533.C4\$bL49

Second Indicator - Source of call number

Whether the source of the class/call number is the Library of Congress or another organization.

0 - Assigned by LC

Used when an institution is transcribing from LC cataloging copy.

050 00\$aJK609\$b.M2

4 - Assigned by agency other than LC**■ SUBFIELD CODES****\$a - Classification number**

Classification number portion of the call number. The source of the classification number is *Library of Congress Classification* and the *LC Classification-Additions and Changes*. Subfield \$a is repeated to record an alternative class number. The alternate class number is recorded following the last subfield of the call number. If the alternate class number also includes an item number, the item number is included in the same subfield \$a as the alternate class number; it is not separately subfielded.

050 00\$aQC861.2\$b.B36

050 00\$aZ695.7\$b.B37 1980

050 00\$aZ7164.N3\$bL34 no. 9\$aZ7165.R42\$aHC517.R42

050 00\$aRC951

\$b - Item number

Item number portion of the call number. An item number is the Cutter, date, term, etc. that is added to a classification number to distinguish an item from any other item assigned the same classification number.

Organizations that use the *Cutter-Sanborn Three-Figure Author Table* may conform to Library of Congress item number practice by applying *Subject Cataloging Manual: Shelflisting* conventions.

050 00\$aJX1974.7\$b.M5

050 00\$aZ673.L7\$bY

050 10\$aHF5726\$b.B27 1980

050 00\$aE506.5 6th\$bG

050 00\$aE514.6 10th\$b.T76 1905

[The above two call numbers are call numbers for regimental histories.]

\$0 - Authority record control number or standard number

See description of this subfield in Appendix A: [Control Subfields](#).

\$1 - Real World Object URI

See description of this subfield in Appendix A: [Control Subfields](#).

\$3 - Materials specified

Part of the described material to which the field applies. The subfield is used with archival-type materials; its use is parallel with the use of subfield \$3 in other fields.

\$6 - Linkage

See description of this subfield in Appendix A: [Control Subfields](#).

\$8 - Field link and sequence number

See description of this subfield in Appendix A: [Control Subfields](#).

INPUT CONVENTIONS

LCCNs - When the call number field consists only of a class number (letters followed by numbers, possibly including a period and also a space), no subfield \$b is used.

050 00\$aQA37

050 00\$aE525.5 123d

General rule is that the item number part of the call number begins at the last capital letter in the call number or the period, if present, preceding it.

050 00\$aHF5549.5.R44\$bM35

Exceptions to the general rule for item numbers:

If the call number is followed by only a date, with no Cutter number, the date is contained in subfield \$b.

050 00\$aE457.92\$b1967

If the call number is followed by volume numbering that includes uppercase letters, these letters are ignored in locating the last capital letter.

050 00\$aJX1977\$b.A2 St/ESA/35

050 00\$aHA1501\$bA, Nr. 615

050 00\$aHD28\$b.Y555 vol. 55 Suppl.

If the call number begins with CS71, subfield \$b contains the date.

050 00\$aCS71.C323\$b1977

If the call number is for a classification schedule (i.e., it is a call number beginning with Z696.U5), the class letter(s) for the particular classification and any following digit(s) are recorded in subfield \$a (as part of the classification). Subfield \$b contains the date.

050 00\$aZ696.U5E3\$b1958

050 00\$aZ696.U5H-HJ\$b1981

Abbreviations *subser.* and *Suppl.* are recorded in subfield \$b, even when there is no item number.

Capitalization - Alphabetic characters in the classification number portion of the field are generally uppercase.

Spacing - Any spaces that are desired as part of the call number must be input.

050 00\$aDK274.3 1968\$b.K39

050 00\$aVM341\$b.M9 vol. 48

050 00\$aCS71.C323\$b1977

Display Constant

[...] *[brackets]*

Brackets that customarily surround call numbers for items not in LC or alternate class/call numbers are not carried in the MARC record. They may be system generated as a display constant associated with the first indicator value 1 or additional \$a subfields.

Content designated field:

050 10\$aHF5726\$b.B27 1980

Display example:

[HF5726.B27 1980]

CONTENT DESIGNATOR HISTORY

Indicator 1 - Existence in LC collection

- *No information provided*

Prior to the definition of code 4 in the second indicator position in 1982, the first indicator in the visual materials specifications was undefined. Visual materials records created prior to 1982 may contain a # meaning *undefined* in the first indicator position.

Indicator 2 - Series call number (SE) [OBSOLETE]

In the serials specifications, the use of the second indicator position to indicate the type of series was made obsolete in 1976. The values were: 0 (No series involved), 1 (Main series), 2 (Subseries), 3 (Sub-subseries).

Indicator 2 - Source of call number

- *No information provided [OBSOLETE]*

Second indicator was defined in 1982. Prior to that change, 050 was an agency-assigned field and contained only call numbers assigned by the Library of Congress. LC records created before the definition of this indicator may contain a blank (#) meaning *undefined* in this position.

\$d - Supplementary class number (MU) [OBSOLETE, 1981]

\$0 - Authority record control number or standard number [NEW, 2017]

\$1 - Real World Object URI [NEW, 2017]

ATTACHMENT 1L

Library of Congress Classification PDF Files

[About LCC](#) - [A-BX](#) - [C-F](#) - [G-J](#) - [K-KZ](#) - [L-N](#) - [P-PZ](#) - [Q-S](#) - [T-Z](#) -

About the Library of Congress Classification PDF Files

This page provides print-ready PDF files of Library of Congress classification schedules. Data for these files was selected in February 2018. For users desiring enhanced functionality, LCC is included in the web-based subscription product, *Classification Web*.

Earlier editions are available [here](#) but should not be used for cataloging.

[More About the Library of Congress Classification \(LCC\)](#)

[View the Library of Congress Classification Outline](#)

[Back to Top](#)

A-BX

[A Preface](#) General Works (PDF, 1 p., 14 KB)

[A Outline](#) General Works (PDF, 1 p., 86 KB)

[A Text](#) General Works (PDF, 90 p., 385 KB)

[B-BJ Preface](#) Philosophy, Psychology (PDF, 1 p., 88 KB)

[B-BJ Outline](#) Philosophy, Psychology (PDF, 3 p., 93 KB)

[B-BJ Text](#) Philosophy, Psychology (PDF, 446 p., 2.3 MB)

[BL-BQ Preface](#) Religion (General). Hinduism, Judaism, Islam, Buddhism (PDF, 1 p., 88 KB)

[BL-BQ Outline](#) Religion (General). Hinduism, Judaism, Islam, Buddhism (PDF, 7 p., 172 KB)

[BL-BQ Text](#) Religion (General). Hinduism, Judaism, Islam, Buddhism (PDF, 536 p., 2.8 MB)

[BR-BX Preface](#) Christianity, Bible (PDF, 1 p., 88 KB)

[BR-BX Outline](#) Christianity, Bible (PDF, 9 p., 117 KB)

[BR-BX Text](#) Christianity, Bible (PDF, 806 p., 3.5 MB)

[Back to Top](#)

C-F

[C Preface](#) Auxiliary Sciences of History (PDF, 1 p., 87 KB)

[C Outline](#) Auxiliary Sciences of History (PDF, 3 p., 93 KB)

[C Text](#) Auxiliary Sciences of History (PDF, 233 p., 990 KB)

[D-DR Preface](#) History (General) and History of Europe (PDF, 1 p., 88 KB)

[D-DR Outline](#) History (General) and History of Europe (PDF, 21 p., 166 KB)

[D-DR Text](#) History (General) and History of Europe (PDF, 921 p., 4.0 MB)

[DS-DX Preface](#) History of Asia, Africa, Australia, New Zealand, etc. (PDF, 1 p., 14 KB)

[DS-DX Outline](#) History of Asia, Africa, Australia, New Zealand, etc. (PDF, 11 p., 118 KB)

[DS-DX Text](#) History of Asia, Africa, Australia, New Zealand, etc. (PDF, 517 p., 2.4 MB)

[E-F Preface](#) History: America (PDF, 1 p., 87 KB)

[E-F Outline](#) History: America (PDF, 9 p., 106 KB)

[E-F Text](#) History: America (PDF, 945 p., 4.5 MB)

[⌂ Back to Top](#)

G-J

[G Preface](#) Geography. Maps. Anthropology. Recreation (PDF, 2 p., 91 KB)

[G Outline](#) Geography. Maps. Anthropology. Recreation (PDF, 7 p., 109 KB)

[G Text](#) Geography. Maps. Anthropology. Recreation (PDF, 882 p., 3.6 MB)

[H Preface](#) Social Sciences (PDF, 1 p., 89 KB)

[H Outline](#) Social Sciences (PDF, 15 p., 127 KB)

[H Text](#) Social Sciences (PDF, 1160 p., 4.8 MB)

[J Preface](#) Political Science (PDF, 1 p., 88 KB)

[J Outline](#) Political Science (PDF, 6 p., 105 KB)

[J Text](#) Political Science (PDF, 538 p., 2.3 MB)

[⌂ Back to Top](#)

K-KZ

[K Tables Preface](#) Form Division Tables For Law (PDF, 1 p., 85 KB)

[K Tables Text](#) Form Division Tables For Law (PDF, 44 p., 238 KB)

[K Preface](#) Law in General. Comparative and Uniform Law. Jurisprudence (PDF, 2 p., 89 KB)

[K Outline](#) Law in General. Comparative and Uniform Law. Jurisprudence (PDF, 5 p., 101 KB)

[K Text](#) Law in General. Comparative and Uniform Law. Jurisprudence (PDF, 165 p., 829 KB)

[KB Preface](#) Religious Law (PDF, 1 p., 149 KB)

[KB Outline](#) Religious Law (PDF, 8 p., 198 KB)

[KB Text](#) Religious Law (PDF, 631 p., 3.0 MB)

[KD Preface](#) Law of the United Kingdom and Ireland (PDF, 1 p., 86 KB)

[KD Outline](#) Law of the United Kingdom and Ireland (PDF, 7 p., 126 KB)

[KD Text](#) Law of the United Kingdom and Ireland (PDF, 253 p., 1.2 MB)

[KDZ, KG-KH Preface](#) Law of the Americas, Latin America and the West Indies (PDF, 1 p., 87 KB)

[KDZ, KG-KH Outline](#) Law of the Americas, Latin America and the West Indies (PDF, 14 p., 148 KB)

[KDZ, KG-KH Text](#) Law of the Americas, Latin America and the West Indies (PDF, 417 p., 2.0 MB)

[KE Preface](#) Law of Canada (PDF, 1 p., 87 KB)

[KE Outline](#) Law of Canada (PDF, 7 p., 124 KB)

[KE Text](#) Law of Canada (PDF, 275 p., 1.0 MB)

[KF Preface](#) Law of the United States (PDF, 1 p., 87 KB)

[KF Outline](#) Law of the United States (PDF, 7 p., 110 KB)

[KF Text](#) Law of the United States (PDF, 676 p., 3.0 MB)

[KI-KIL Preface](#) Law of Indigenous Peoples (PDF, 1 p., 44 KB)

[KI-KIL Text](#) Law of Indigenous Peoples (PDF, 223 p., 1.0 MB)

[KJ-KKZ Preface](#) Law of Europe (PDF, 1 p., 99 KB)

[KJ-KKZ Outline](#) Law of Europe (PDF, 25 p., 174 KB)

[KJ-KKZ Text](#) Law of Europe (PDF, 737 p., 3.5 MB)

[KJV-KJW Preface](#) Law of France (PDF, 1 p., 87 KB)

[KJV-KJW Outline](#) Law of France (PDF, 8 p., 115 KB)

[KJV-KJW Text](#) Law of France (PDF, 307 p., 1.5 MB)

[KK-KKC Preface](#) Law of Germany (PDF, 1 p., 87 KB)

[KK-KKC Outline](#) Law of Germany (PDF, 8 p., 113 KB)

[KK-KKC Text](#) Law of Germany (PDF, 592 p., 3.0 MB)

[KL-KWX Preface](#) Law of Asia and Eurasia, Africa, Pacific Area, and Antarctica (PDF, 1 p., 88 KB)

[KL-KWX Outline](#) Law of Asia and Eurasia, Africa, Pacific Area, and Antarctica (PDF, 32 p., 207 KB)

[KL-KWX Text](#) Law of Asia and Eurasia, Africa, Pacific Area, and Antarctica (PDF, 1,162 p., 5.0 MB)

[KVJ Preface](#) Pacific Area: Pacific Area Jurisdictions: Hawaii (to 1900) (PDF, 1 p., 64 KB)

[KVJ Text](#) Pacific Area: Pacific Area Jurisdictions: Hawaii (to 1900) (PDF, 62 p., 428 KB)

[KZ Preface](#) Law of Nations (PDF, 1 p., 94 KB)

[KZ Outline](#) Law of Nations (PDF, 3 p., 112 KB)

[KZ Text](#) Law of Nations (PDF, 208 p., 1.0 MB)

[Back to Top](#)

L-N

[L Preface](#) Education (PDF, 1 p., 94 KB)

[L Outline](#) Education (PDF, 8 p., 174 KB)

[L Text](#) Education (PDF, 435 p., 2.0 MB)

[M Preface](#) Music and Books on Music (PDF, 1 p., 164 KB)

[M Outline](#) Music and Books on Music (PDF, 3 p., 137 KB)

[M Text](#) Music and Books on Music (PDF, 419 p., 2.0 MB)

[N Preface](#) Fine Arts (PDF, 1 p., 86 KB)

[N Outline](#) Fine Arts (PDF, 5 p., 126 KB)

[N Text](#) Fine Arts (PDF, 799 p., 4.0 MB)

[Back to Top](#)

P-PZ

[P-PZ Tables Preface](#) Language and Literature Tables (PDF, 1 p., 86 KB)

[P- PZ Tables Text](#) Language and Literature Tables (PDF, 147 p., 775 KB)

[P-PA Preface](#) Philology and Linguistics (General). Greek Language and Literature.Latin Language and Literature (PDF, 1 p., 124 KB)

[P-PA Outline](#) Philology and Linguistics (General). Greek Language and Literature.Latin Language and Literature (PDF, 2 p, 101 KB)

[P-PA Text](#) Oriental Philology and Linguistics (General). Greek Language and Literature.Latin Language and Literature (PDF, 483 p., 3.0 MB)

[PB-PH Preface](#) Modern European Languages (PDF, 1 p., 125 KB)

[PB-PH Outline](#) Modern European Languages (PDF, 4 p., 123 KB)

[PB-PH Text](#) Modern European Languages (PDF, 813 p., 6.0 MB)

[PJ-PK Preface](#) Oriental Philology and Literature, Indo-Iranian Philology and Literature (PDF, 1 p., 150 KB)

[PJ-PK Outline](#) Oriental Philology and Literature, Indo-Iranian Philology and Literature (PDF, 5 p., 125 KB)

[PJ-PK Text](#) Oriental Philology and Literature, Indo-Iranian Philology and Literature (PDF, 366 p., 2.0 MB)

[PL-PM Preface](#) Languages of Eastern Asia, Africa, Oceania, Hyperborean, Indian, and Artificial Languages (PDF, 1 p., 125 KB)

[PL-PM Outline](#) Languages of Eastern Asia, Africa, Oceania, Hyperborean, Indian, and Artificial Languages (PDF, 2 p., 155 KB)

[PL-PM Text](#) Languages of Eastern Asia, Africa, Oceania, Hyperborean, Indian, and Artificial Languages (PDF, 510 p., 4.0 MB)

[PN Preface](#) Literature (General) (PDF, 1 p., 88 KB)

[PN Outline](#) Literature (General) (PDF, 3 p., 93 KB)

[PN Text](#) Literature (General) (PDF, 400 p., 2.0 MB)

[PQ Preface](#) French, Italian, Spanish, and Portuguese Literatures (PDF, 1 p., 124 KB)

[PQ Outline](#) French, Italian, Spanish, and Portuguese Literatures (PDF, 3 p., 96 KB)

[PQ Text](#) French, Italian, Spanish, and Portuguese Literatures (PDF, 609 p., 4.0 MB)

[PR-PS, PZ Preface](#) English and American Literature. Juvenile Belles Lettres (PDF, 1 p., 87 KB)

[PR-PS, PZ Outline](#) English and American Literature. Juvenile Belles Lettres (PDF, 3 p., 96 KB)

[PR-PS, PZ Text](#) English and American Literature. Juvenile Belles Lettres (PDF, 569 p., 3.0 MB)

[PT Preface](#) German, Dutch, and Scandinavian Literatures (PDF, 1 p., 125 KB)

[PT Outline](#) German, Dutch, and Scandinavian Literatures (PDF, 5 p., 102 KB)

[PT Text](#) German, Dutch, and Scandinavian Literatures (PDF, 476 p., 3.0 MB)

[Back to Top](#)

Q-S

[Q Preface](#) Science (PDF, 1 p., 87 KB)

[Q Outline](#) Science (PDF, 4 p., 101 KB)

[Q Text](#) Science (PDF, 869 p., 4.0 MB)

[R Preface](#) Medicine (PDF, 1 p., 86 KB)

[R Outline](#) Medicine (PDF, 7 p., 120 KB)

[R Text](#) Medicine (PDF, 556 p., 2.0 MB)

[S Preface](#) Agriculture (PDF, 1 p., 94 KB)

[S Outline](#) Agriculture (PDF, 6 p., 117 KB)

[S Text](#) Agriculture (PDF, 478 p., 2.0 MB)

[Back to Top](#)

T-Z

[T Preface](#) Technology (PDF, 1 p., 87 KB)

[T Outline](#) Technology (PDF, 8 p., 114 KB)

[T Text](#) Technology (PDF, 830 p., 4.0 MB)

[U-V Preface](#) Military Science. Naval Science (PDF, 1 p., 95 KB)

[U-V Outline](#) Military Science. Naval Science (PDF, 6 p., 115 KB)

[U-V Text](#) Military Science. Naval Science (PDF, 337 p., 1.0 MB)

[Z Preface](#) Bibliography. Library Science. Information Resources (PDF, 1 p., 94 KB)

[Z Outline](#) Bibliography. Library Science. Information Resources (PDF, 4 p., 106 KB)

[Z Text](#) Bibliography. Library Science. Information Resources (PDF, 706 p., 3.0 MB)

[Back to Top](#)

Last Updated: 03/30/2018

Stay Connected with the Library [All ways to connect »](#)

Find us on



Subscribe & Comment

[RSS & E-Mail](#)

[Blogs](#)

Download & Play

[Podcasts](#)

[Webcasts](#)

