National Research Council

February 1985

Executive Summary of the NRC Report on Transport Protocols for Department of Defense Data Networks

STATUS OF THIS MEMO

This RFC is distributed for information only. This RFC does not establish any policy for the DARPA research community or the DDN operational community. Distribution of this memo is unlimited.

INTRODUCTION

This RFC reproduces the material from the "front pages" of the National Research Council report resulting from a study of the DOD Internet Protocol (IP) and Transmission Control Protocol (TCP) in comparison with the ISO Internet Protocol (ISO-IP) and Transport Protocol level 4 (TP-4). The point of this RFC is to make the text of the Executive Summary widely available in a timely way. The order of presentation has been altered, and the pagination changed.

The title of the full report is:

Transport Protocols for
Department of Defense
Data Networks

Report to the Department of Defense
and the National Bureau of Standards

Committee on Computer-Computer Communication Protocols

Board on Telecommunications and Computer Applications Commission on Engineering and Technical Systems
National Research Council

National Academy Press
Washington, D.C. February 1985

OVERVIEW

The project that is the subject of this report was approved by the Governing Board on the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This report has been reviewed by a group other than the authors, according to procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

The National Research Council was established by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and of advising the federal government. The Council operates in accordance with general policies determined by the Academy under the authority of its congressional charter of 1863, which establishes the Academy as a private, nonprofit, self-governing membership corporation. The Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in the conduct of their services to the government, the public, and the scientific and engineering communities. It is administered jointly by both Academies and the Institute of Medicine. The National Academy of Engineering and the Institute of Medicine were established in 1964 and 1970, respectively, under the charter of the National Academy of Sciences.

This is a report of work supported by Contract No. DCA-83-C-0051 between the U.S. Defense Communications Agency and the National Academy of Sciences, underwritten jointly by the Department of Defense and the National Bureau of Standards.

Copies of the full report are available from:

Board on Telecommunications and Computer Applications Commission on Engineering and Technical Systems
National Research Council
2101 Constitution Avenue, N.W.
Washington, D.C. 20418

PREFACE

This is the final report of the National Research Council Committee on Computer-Computer Communication Protocols. The committee was established in May l983 at the request of the Department of Defense (DOD) and the National Bureau of Standards (NBS), Department of Commerce, to develop recommendations and guidelines for resolving differences between the two agencies on a data communications transport protocol standard.

Computer-based information and transaction-processing systems are basic tools in modern industry and government. Over the past several years there has been a growing demand to transfer and exchange digitized data in these systems quickly and accurately. This demand for data transfer and exchange has been both among the terminals and computers within an organization and among those in different organizations.

Rapid electronic transport of digitized data requires electronic communication links that tie the elements together. These links are established, organized, and maintained by means of a layered series of procedures performing the many functions inherent in the communications process. The successful movement of digitized data depends upon the participants using identical or compatible procedures, or protocols.

The DOD and NBS have each developed and promulgated a transport protocol as standard. The two protocols, however, are dissimilar and incompatible. The committee was called to resolve the differences between these protocols.

The committee held its first meeting in August l983 at the National Research Council in Washington, D.C. Following this two-day meeting the committee held five more two-day meetings, a three-day meeting, and a one-week workshop.

The committee was briefed by personnel from both agencies. In addition, the committee heard from Jon Postel, University of Southern California’s Information Sciences Institute; Dave Oran, Digital Equipment Corporation; Vinton Cerf, MCI; David Wood, The Mitre Corporation; Clair Miller, Honeywell, and Robert Follett, IBM, representing the Computer and Business Equipment Manufacturer’s Association; and John Newman, Ultimate Corporation. In most cases the briefings were followed by discussion.

The committee wishes to thank Philip Selvaggi of the Department of Defense and Robert Blanc of the NBS, Institute of Computer Sciences

and Technology, for their cooperation as their agency's liaison representatives to the committee. The committee appreciates the contributions and support of Richard B. Marsten, Executive Director of the Board on Telecommunications -- Computer Applications (BOTCAP), and Jerome D. Rosenberg, BOTCAP Senior Staff Officer and the committee Study Director. We also wish to thank Lois A. Leak for her expert administrative and secretarial support.

EXECUTIVE SUMMARY

Computer communication networks have become a very important part of military and commercial operations. Indeed, the nation is becoming dependent upon their efficiency and reliability, and the recent proliferation of networks and their widespread use have emphasized the importance of developing uniform conventions, or protocols, for communication between computer systems. The Department of Defense (DOD) and the National Bureau of Standards (NBS) have been actively engaged in activities related to protocol standardization. This report is concerned primarily with recommendations on protocol standardization within the Department of Defense.

Department of Defense's Transmission Protocol

The DOD's Defense Advanced Research Projects Agency (DARPA) has been conducting and supporting research on computer networks for over fifteen years (1). These efforts led to the development of modern packet-switched network design concepts. Transmission between computers is generally accomplished by packet switching using strict protocols for the control and exchange of messages. The Advanced Research Projects Agency network (ARPANET), implemented in the early 1970s, provided a testing ground for research on communications protocols. In 1978, after four years of development, the DOD promulgated versions of its Transmission Control Protocol (TCP) and an Internet Protocol (IP) and mandated their use as standards within the DOD. TCP is now widely used and accepted. These protocols meet the unique operational and functional requirements of the DOD, and any changes in the protocols are viewed with some trepidation by members of the department. DOD representatives have stated that standardizing TCP greatly increased the momentum within the DOD toward establishing interoperability between networks within the DOD.

International Standards Organization's Transport Protocol

The NBS Institute for Computer Sciences and Technology (ICST), in cooperation with the DOD, many industrial firms, and the International Standards Organization (ISO), has developed a new international standard

Transport Protocol (TP-4) and a new Internetwork Protocol (2). These protocols will soon be available as commercial products. Although in part derived from TCP, the new protocols are not compatible with TCP (3). The U.S. standards organizations are

supporting TP-4 in international operations, and the Department of Commerce is proposing TP-4 as a Federal Information Processing Standard (FIPS) for use by all federal agencies.

DOD OPERATIONAL AND TECHNICAL NEEDS

The DOD has unique needs that could be affected by the Transport and Internet Protocol layers. Although all data networks must have some of these capabilities, the DOD's needs for operational readiness, mobilization, and war-fighting capabilities are extreme. These needs include the following:

Survivability--Some networks must function, albeit at reduced performance, after many nodes and links have been destroyed.

Security--Traffic patterns and data must be selectively protected through encryption, access control, auditing, and routing.

Precedence--Systems should adjust the quality of service on the basis of priority of use; this includes a capability to preempt services in cases of very high priority.

Robustness--The system must not fail or suffer much loss of capability because of unpredicted situations, unexpected loads, or misuse. An international crisis is the strongest test of robustness, since the system must operate immediately and with virtually full performance when an international situation flares up unexpectedly.

Availability--Elements of the system needed for operational readiness or fighting must be continuously available.

Interoperability--Different elements of the Department must be able to "talk" to one another, often in unpredicted ways between parties that had not planned to interoperate.

These operational needs reflect themselves into five technical or managerial needs:

1. Functional and operational specifications (that is, will the protocol designs meet the operational needs?);

2. Maximum interoperability;

3. Minimum procurement, development, and support costs;

4. Ease of transition to new protocols; and

5. Manageability and responsiveness to changing DOD requirements.

These are the criteria against which DOD options for using the ISO transport and internet protocols should be evaluated.

Interoperability is a very important DOD need. Ideally, DOD networks would permit operators at any terminal to access or be accessed by applications in any computer. This would provide more network power for users, integration of independently developed systems, better use of resources, and increased survivability. To increase interoperability, the Office of the Secretary of Defense has mandated the use of TCP for the Defense Communication System's Defense Data Network (DDN), unless waivers are granted. In addition, the Defense Communication Agency (DCA) is establishing standards for three higher-level "utility" protocols for file transfer, terminal access, and electronic mail. Partly as a result of these actions, it has become clear that there is growing momentum toward accepting interoperability and a recognition that it is an important operational need.

It is very important, however, to recognize that functional interoperability is only achieved with full generality when two communication nodes can interoperate at all protocol levels. For the DOD the relevant levels are as follows:

1. Internet, using IP;

2. Transport, using TCP;

3. Utility, using file, terminal, or mail protocols; and

4. Specific applications that use the above protocols for their particular purpose.

Accordingly, if a network is developed using one transport protocol, it would generally not be able to interoperate functionally with other networks using the same transport protocol unless both networks were also using the higher-level utility and application protocols. In evaluating whether or not to convert to TP-4 and in developing a transition plan, the following factors must be considered:

The DOD contains numerous communities of interest whose principal need is to interoperate within their own members,

independently. Such communities generally have a specific, well-defined mission. The DOD Intelligence Information System (DODIIS) and the World Wide Military Command and Control System (WWMCCS) are examples. Interoperability is needed primarily between the higher layer applications programs initially unique to each community of interest.

There are many different kinds of operations needed between communities of interest. Examples of such operations are headquarters' need for access to several subordinate communities and the communities' need for some minimum functional interoperability with each other (such as mail exchange).

The need for functional interoperability can arise, unexpectedly and urgently, at a time of crisis or when improved management opportunities are discovered. Widespread standardization of TP-4 and higher-level protocols can readily help to achieve these needs. Often, special development of additional applications that cost time and money will be necessary.

The DOD needs functional interoperability with many important external agencies that are committed to ISO standards: The North Atlantic Treaty Organization (NATO), some intelligence and security agencies, and other parts of the federal government.

The same objectives that have prompted the use of standardized protocols at higher-level headquarters will lead to their use by tactical groups in the field.

SOME COMPARISONS

A detailed comparison of the DOD Transmission Control Protocol and the ISO Transport Protocol indicates they are functionally equivalent and provide essentially similar services. Because it is clear that a great deal of care and experience in protocol development have gone into generating the specifications for TP-4, the committee is confident that TP-4 will meet military requirements.

Although there are differences between the two protocols, they do not compromise DOD requirements. And, although in several areas, including the data transfer interface, flow control, connection establishment, and out-of-band, services are provided in different ways by the two protocols, neither seems intrinsically superior.

Thus, while existing applications may need to be modified somewhat if moved from TCP to TP-4, new applications can be written to use either protocol with a similar level of effort.

The TCP and TP-4 protocols are sufficiently equivalent in their security-related properties in that there are no significant technical points favoring the use of one over the other.

While TCP currently has the edge in maturity of implementation, TP-4 is gaining rapidly due to the worldwide support for and acceptance of the Open System Interconnection (OSI) international standards. Experimental TCP implementations were completed in 1974 at Stanford University and BBN Communications Corporation. Between 1974 and 1982 a large number of implementations were produced. The Defense Advanced Research Projects Agency (ARPA) network switched to a complete use of TCP in January 1983. Operations have been satisfactory and its use is growing. A number of TCP implementations are also in commercial use in various private networks.

In contrast, TP-4 has not yet been implemented in any large operational system. It has been tested experimentally, however, and has received endorsement by many commercial vendors worldwide. In addition, substantial portions of TP-4 have been demonstrated at the National Computer Conference in July 1984.

The Internet Protocol (IP) part of the standards is not believed to be a problem. The ISO IP is not as far along as TP-4, but it is much less complex. The ISO IP, based very strongly on the DOD IP, became a draft international standard in April 1984.

The rapidity of the progress in ISO and the results achieved over the past two years have surprised even the supporters of international standards. The reasons for this progress are twofold: strong market demands stemming from the growing integration of communications and data processing and the progress in networking technology over the past years as the result of ARPA and commercial developments.

Although the DOD networks have been a model upon which the ISO transport standards have been built, the rest of the world is adopting TP-4. Because the DOD represents a small fraction of the market and because the United States supports the ISO standard, it is not realistic to hope that TP-4 can be altered to conform with TCP. This raises the question as to what action should be taken by the DOD with respect to the ISO standard.

SOME ECONOMIC CONSIDERATIONS

The DOD has a large and growing commitment in operational TCP networks, and this will increase by 50 to 100 percent in the next eighteen months. This rate of investment will probably continue for the next five years for new systems and the upgrading of current ones. The current Military Network (MILNET) and Movement Information Network (MINET) systems are expanding and will shortly be combined. The Strategic Air Command Digital Information Network (SACDIN) and DODIIS are undergoing major upgrading. When these changes are completed, there are plans to upgrade the WWMCCS Intercomputer Network (WIN) and to add separate SECRET and TOP SECRET networks. There are plans to combine these six networks in the late 1980s, and they will become interoperable and multilevel secure using an advanced technology now under development. If these plans are implemented on schedule, a delay of several years in moving to TP-4 would mean that the DOD networks in the late 1980s would be virtually all TCP-based. Subsequent conversion to international standards would be very expensive if hastily attempted in order to maintain established DOD interoperability and gain interoperability with a large body of users.

As the Department of Defense policy recognizes, there are significant advantages in using commercial vendor products if they meet the department's operational needs. The major advantages are as follows:

Costs to the DOD for development, production, and maintenance are significantly lower because (1) vendors spread the cost over a much larger user base, (2) commercial vendors are generally more efficient in their operations, and (3) vendors look for ways to improve their product to meet competition.

The department generally gets more effective products because vendors integrate the protocol functions into their entire software and hardware product line. Thus the DOD may be able eventually to use commercial software products that are built on top of, and thereby take advantage of, the transport protocols.

By depending on industry to manage the development and maintenance of products, the department can use its scarce management and technical resources on activities unique to its mission.

Because the costs of transport and internet protocol development and maintenance are so intertwined with other factors, it is

impossible to give a precise estimate of the savings that would be achieved by using commercial products. Savings will vary in individual cases. The marginal savings should range from 30 to 80 percent.

RECOMMENDATIONS

The ISO protocols are now well specified but will not generally be commercially available for many months. Nevertheless, this committee believes that the principles on which they are based are well-established, and the protocols can be made to satisfy fully DOD's needs. The committee recommends that the DOD move toward adoption of TP-4 as costandard with TCP and toward exclusive use of TP-4.

Transition to the use of the ISO standards, however, must be managed in a manner that will maintain DOD's operational capabilities and minimize risks. The timing of the transition is, therefore, a major concern.

Descriptions of two options that take this requirement into account follow. A majority of the committee recommends the first option, while a minority favors the second. A third option--to defer action--is also described but not recommended.

Option 1

The first option is for the DOD to immediately modify its current transport policy statement to specify TP-4 as a costandard along with TCP. In addition, the DOD would develop a military specification for TP-4 that would also cover DOD requirements for discretionary options allowed under the NBS protocol specifications. Requests for proposals (RFPs) for new networks or major upgrades of existing networks would specify TP-4 as the preferred protocol. Contracts for TP-4 systems would be awarded only to contractors providing commercial products, except for unique cases.

Existing networks that use TCP and new networks firmly committed to the use of TCP-based systems could continue to acquire implementations of TCP. The DOD should carefully review each case, however, to see whether it would be advantageous to delay or modify some of these acquisitions in order to use commercial TP-4 products. For each community of users it should be decided when it is operationally or

economically most advantageous to replace its current or planned systems in order to conform to ISO standards without excessively compromising continued operations.

United States government test facilities would be developed to enable validation of TP-4 products (4). The Department of Defense would either require that products be validated using these test facilities or that they be certified by the vendor. The test facilities could also be used to isolate multivendor protocol compatibility problems. The existing NBS validation tools should be used as the base for the DOD test facilities.

Because under this option networks based on both TCP and TP-4 would coexist for some time, several capabilities that facilitate interoperability among networks would need to be developed. The Department of Defense generally will not find them commercially available. Examples are gateways among networks or specialized hosts that provide services such as electronic mail. The department would need to initiate or modify development programs to provide these capabilities, and a test and demonstration network would be required.

Option 2

Under Option 2 the Department of Defense would immediately announce its intention to adopt TP-4 as a transport protocol costandard with TCP after a satisfactory demonstration of its suitability for use in military networks. A final commitment would be deferred until the demonstration has been evaluated and TP-4 is commercially available.

The demonstration should take at most eighteen months and should involve development of TP-4 implementations and their installation. This option differs from Option 1 primarily in postponing the adoption of a TP-4 standard and, consequently, the issuance of RFPs based on TP-4 until successful completion of a demonstration. The department, however, should proceed with those provisions of Option 1 that may be completed in parallel with the demonstration. Early issuance of a TP-4 military specification, development of validation procedures, and implementation of means for interoperability would be particularly important in this regard.

Option 3

Under the third option the DOD would continue using TCP as the accepted transport standard and defer any decision on the use of TP-4 indefinitely. The department would be expected to stay well informed on the development and use of the new protocol in the commercial and international arena and, with the National Bureau of Standards, work on means to transfer data between the two protocol systems. Testing and evaluation of TP-4 standards by NBS would continue. The DOD might eventually accommodate both protocol systems in an evolutionary conversion to TP-4.

Comparison of Options

The committee believes that all three options equally satisfy the functional objectives of the DOD, including matters of security. It believes the two protocols are sufficiently similar and no significant differences in performance are to be expected if the chosen protocol implementation is of equal quality and is optimized for the given environment.

The primary motivation for recommending Option 1 is to obtain the benefits of standard commercial products in the communication protocol area at an early date. Benefits include smaller development, procurement, and support costs; more timely updates; and a wider product availability. By immediately committing to TP-4 as a costandard for new systems, Option 1 minimizes the number of systems that have to be converted eventually from TCP. The ability to manage the transition is better than with Option 2 since the number of systems changed would be smaller and the time duration of mixed TCP and TP-4 operation would be shorter. Interoperability with external systems (NATO, government, commercial), which presumably will also use TP-4, would be brought about more quickly. Option 1 involves greater risk, however, since it commits to a new approach without as complete a demonstration of its viability.

As with Option 1, a primary benefit of following Option 2 would be obtaining the use of standard commercial products. Unit procurement costs probably would be lower than with Option 1 because the commercial market for TP-4 will have expanded somewhat by the time DOD would begin to buy TP-4 products. Risk is smaller, compared to Option 1, because testing and demonstration of the suitability for military use will have preceded the commitment to the ISO protocols. Transition and support costs would be higher than for Option 1, however,

because more networks and systems would already have been implemented with TCP. Also this is perhaps the most difficult option to manage since the largest number of system conversions and the longest interval of mixed TCP and TP-4 operations would occur. In addition, interoperability with external networks through standardization would be delayed.

The principal benefit of exercising Option 3 would be the elimination of transition cost and the risk of faulty system behavior and delay. It would allow the most rapid achievement of full internal interoperability among DOD systems. Manageability should be good because only one set of protocols would be in use (one with which the DOD already has much experience), and because the DOD would be in complete control of system evolution. Procurement costs for TCP systems would remain high compared with standard ISO protocol products, however, and availability of implementations for new systems and releases would remain limited. External interoperability with non-DOD systems would be limited and inefficient.

In summary, Option 1 provides the most rapid path toward the use of commercial products and interoperability with external systems. Option 2 reduces the risk but involves somewhat greater delay and expense. Option 3 involves the least risk and provides the quickest route to interoperability within the Defense Department at the least short-term cost. These are, however, accompanied by penalties of incompatibility with NATO and other external systems and higher life-cycle costs.

NOTES:

(1) The Advanced Research Projects Agency (ARPA) was reorganized and became the Defense Advanced Research Projects Agency (DARPA) in 1973.

(2) The ISO Transport Protocol and ISO Internetwork Protocol became Draft International Standards in September 1983 and April 1984, respectively. Commercial vendors normally consider Draft International Standards to be ready for implementation.

(3) Except where noted, the abbreviation TCP generally refers to both the DOD's Transmission Control Protocol and its Internet Protocol. Similarly, the abbreviation TP-4 refers to both the ISO Transport Protocol class 4 and its Internetwork Protocol. (Transport Protocol classes 0 to 3 are used for special purposes not related to those of this study.)

(4) Validation means a systematic and thorough state-of-the-art testing of the products to assure that all technical specifications are being achieved.

CONTENTS OF THE FULL REPORT

BOARD ON TELECOMMUNICATIONS -- COMPUTER APPLICATIONS
COMMITTEE ON COMPUTER-COMPUTER COMMUNICATION PROTOCOLS

Chairman

C. CHAPIN CUTLER, Professor of Applied Physics, Stanford University, Stanford, California

Members

HERBERT D. BENINGTON, Technical Director, System Development Corporation, McLean, Virginia

DONALD L. BOYD, Director, Honeywell Corporate Computer Sciences Center, Honeywell Corporate Technology Center, Bloomington, Minnesota

DAVID J. FARBER, Professor of Electrical Engineering and Professor of Computer Science, Department of Electrical Engineering, University of Delaware, Newark, Delaware

LAWRENCE H. LANDWEBER, Professor, Computer Sciences Department, University of Wisconsin, Madison, Wisconsin

ANTHONY G. LAUCK, Manager, Distributed Systems Architecture and Advanced Development, Digital Equipment Corporation, Tewksbury, Massachusetts

KEITH A. LUCKE, General Manager of Control Data Technical Standards, Control Data Corporation, Minneapolis, Minnesota

MISCHA SCHWARTZ, Professor of Electrical Engineering and Computer Science, Columbia University, New York, New York

ROBERT F. STEEN, Director of Architecture, Communication Products Division IBM Corporation, Research Triangle Park, North Carolina

CARL A. SUNSHINE, Principal Engineer, Sytek, Incorporated, Los Angeles Operation, Culver City, California

DANIEL J. FINK, (Ex-officio), President, D.J. Fink Associates, Inc., Arlington, Virginia

JAMES L. FLANAGAN, (CETS LIAISON MEMBER), Head, Acoustics Research Department, AT&T Bell Laboratories, Murray Hill, New Jersey

Staff

RICHARD B. MARSTEN, Executive Director
JEROME D. ROSENBERG, Senior Staff Officer and Study Director
LOIS A. LEAK, Administrative Secretary

COMMISSION ON ENGINEERING AND TECHNICAL SYSTEMS
BOARD ON TELECOMMUNICATIONS -- COMPUTER APPLICATIONS

Chairman

DANIEL J. FINK, President, D.J. Fink Associates, Inc., Arlington, Virginia

Past Chairman

BROCKWAY MCMILLAN, Vice President (Retired), Bell Laboratories, Sedgwick, Maine

Members

ARTHUR G. ANDERSON, Vice President (Retired), IBM Corporation, San Jose, California

DANIEL BELL, Henry Ford II Professor of Social Sciences, Department of Sociology, Harvard University, Cambridge, Massachusetts

HERBERT D. BENINGTON, Technical Director, System Development Corporation, McLean, Virginia

ELWYN R. BERLEKAMP, Professor of Mathematics, Department of Mathematics, University of California, Berkeley, California

ANTHONY J. DEMARIA, Assistant Director of Research for Electronics and Electro-Optics Technology, United Technologies Research Center, East Hartford, Connecticut

GERALD P. DINNEEN, Vice President, Science and Technology, Honeywell Incorporated, Minneapolis, Minnesota

GEORGE GERBNER, Professor and Dean, The Annenberg School of Communications, University of Pennsylvania, Philadelphia, Pennsylvania

ANNE P. JONES, Partner, Sutherland, Asbill and Brennan, Washington, D.C.

ADRIAN M. MCDONOUGH, Professor of Management and Decision Sciences (Retired), The Wharton School, University of Pennsylvania, Havertown, Pennsylvania

WILBUR L. PRITCHARD, President, Satellite Systems Engineering, Inc., Bethesda, Maryland

MICHAEL B. PURSLEY, Professor of Electrical Engineering, University of Illinois, Urbana, Illinois

IVAN SELIN, Chairman of the Board, American Management Systems, Inc., Arlington, Virginia

MISCHA SCHWARTZ, Professor of Electrical Engineering and Computer Science, Columbia University, New York, New York

ERIC E. SUMNER, Vice President, Operations System and Network Planning, AT&T Bell Laboratories, Holmdel, New Jersey

KEITH W. UNCAPHER, Executive Director, USC-Information Sciences Institute Associate Dean, School of Engineering, University of Southern California, Marina del Rey, California

JAMES L. FLANAGAN, (CETS LIAISON MEMBER), Head, Acoustics Research Department, AT&T Bell Laboratories, Murray Hill, New Jersey

Staff

Richard B. Marsten, Executive Director
Jerome D. Rosenberg, Senior Staff Officer
Karen Laughlin, Administrative Coordinator
Carmen A. Ruby, Administrative Assistant
Lois A. Leak, Administrative Secretary