Network Working Group
Request for Comments: 942

National Research Council

February 1985

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.

This RFC reproduces 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).

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

NOTICE

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 this publication 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

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

CONTENTS

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

---

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

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.

---

(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.)

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,

---

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

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.

I. INTRODUCTION

For the past two decades industry and government have experienced an increasing need to share software programs, transfer data, and exchange information among computers. As a result, computer-to-computer data communications networks and, therefore, communication formats and procedures, or protocols, have proliferated. The need to interconnect these networks is obvious, but the problems in establishing agreements among users on the protocols have heightened.

The Department of Defense (DOD) has been conducting research and development on protocols and communication standards for more than fifteen years. In December 1978 the DOD promulgated versions of the Defense Advanced Research Projects Agency's (DARPA) Transmission Control Protocol (TCP) and Internet Protocol (IP) as standards within DOD. With the participation of major manufacturers and systems houses, the DOD has implemented successfully over twenty different applications of these standards in DOD operational data communications networks.

The Institute for Computer Sciences and Technology (ICST) of the National Bureau of Standards (NBS) is the government agency responsible for developing network protocols and interface standards to meet the needs of federal agencies. The Institute has been actively helping national and international voluntary standards organizations develop sets of protocol standards that can be incorporated into commercial products.

Working with both industry and government agencies, the ICST has developed protocol requirements based, in terms of functions and services, on the DOD's TCP. These requirements were submitted to the International Standards Organization (ISO) and resulted in the development of a transport protocol (TP-4) that has the announced support of twenty computer manufacturers.

Although the ISO's TP-4 is based on the DOD's TCP, the two protocols are not compatible. Thus manufacturers who wish to serve DOD, while remaining able to capture a significant share of the worldwide market, have to field two product lines that are incompatible but perform the same function. The Institute for Computer Sciences and Technology would like to have a single set of protocol standards that serves both the DOD, other government agencies, and commercial vendors.

It would be to the advantage of the DOD to use the same standards as the rest of the world. The dilemma, however, is understandable: The DOD

has well satisfied its requirements by its own tried and proven protocols, the agency has invested heavily in systems operating successfully with TCP, and the Armed Forces is increasingly adopting the protocol. Thus, although DOD's policy is to use commercial standards whenever suitable, it is hesitant about converting to the ISO TP-4 protocols. In addition, the DOD is not certain whether the ISO TP-4 completely satisfies military requirements.

In 1983 both DOD and the ICST agreed that an objective study of the situation was needed. Each requested assistance from the National Research Council. The National Research Council, through its Board on Telecommunications and Computer Applications (BOTCAP), appointed a special Committee on Computer-Computer Communication Protocols to study the issues and develop recommendations and guidelines for ways to resolve the differences in a mutually beneficial manner.

The six items composing the committee's scope of work are as follows:

1. Review the technical aspects of the DOD transmission control and ICST transport protocols.

2. Review the status of the implementation of these protocols.

3. Review the industrial and government markets for these protocols.

4. Analyze the technical and political implications of the DOD and ICST views on the protocols.

5. Report on time and cost implications to the DOD, other federal entities, and manufacturers of the DOD and ICST positions.

6. Recommend courses of action toward resolving the differences between the DOD and ICST on these protocol standards.

The committee devoted considerable effort to reviewing the objectives and goals of the DOD and NBS that relate to data communications, the technical aspects of the two protocols, the status of their implementation in operating networks, and the market conditions pertaining to their use. This process included hearing government and industry presentations and reviewing pertinent literature. The results of this part of the study are presented in Sections II through VII. Concurrent with this research and analysis, the committee developed ten possible options that offered plausible resolutions of the problem. These ranged from maintaining the status quo to an immediate switchover from one protocol to the other. From these ten initial options three were determined to hold the greatest potential for resolving the problem.

Section VIII describes the three options, Section IX provides a cost comparison, and Section X provides an overall evaluation of the three options. Section XI presents the committee's basic and detailed recommendations for how best the DOD might approach the differences between its protocol and the ISO protocol.

II. REVIEW OF NBS AND DOD OBJECTIVES

The National Bureau of Standards and the Department of Defense are such disparate organizations that the committee felt it needed to begin its study with a definition of the roles and expectations of each with regard to the protocol issues in question. The following provides a review of each organization's objectives (5).

NBS OBJECTIVES

The National Bureau of Standards has three primary goals in computer networking:

1. To develop networking and protocol standards that meet U.S. government and industry requirements and that will be implemented in off-the-shelf, commercial products.

2. To develop testing methodologies to support development and implementation of computer network protocols.

3. To assist government and industry users in the application of advanced networking technologies and computer and communications equipment manufacturers in the implementation of standard protocols.

Development of Networking and Protocol Standards

The Bureau accomplishes the first objective through close coordination and cooperation with U.S. computer manufacturers and communications system developers. Technical specifications are developed cooperatively with U.S. industry and other government agencies and provided as proposals to voluntary standards organizations.

Because the Department of Defense is potentially the largest government client of these standards, DOD requirements are carefully factored into these proposals. In addition, protocols for computer-to-computer communications developed within the DOD research community are used as an

---

(5) The objectives were reviewed by representatives of NBS and DOD, respectively.

exact statement of DOD functional needs for a particular protocol and form a basis for the functions, features, and services of NBS-proposed standards.

To further the development of commercial products that implement standards, the NBS gives priority to the needs of U.S. computer manufacturers who wish to market their products nationally and internationally, not just to the U.S. government. The NBS participates, therefore, in national and international voluntary standards organizations toward the development of an international consensus based on United States needs. Specifications, formal description techniques, testing methodologies, and test results developed by the NBS are used to further the international standardization process.

Development of Testing Methodologies

The National Bureau of Standards has laboratory activities where prototypes of draft protocol standards are implemented and tested in a variety of communications environments supporting different applications on different kinds and sizes of computers. Communications environments include, for example, global networks, local networks, and office system networks. Applications may, for example, include file transfer or message processing. The primary purposes are to advance the state of the art in measurement methodologies for advanced computer networking technologies and determine protocol implementation correctness and performance.

The NBS views testing as a cooperative research effort and works with other agencies, private-sector companies, and other countries in the development of methodologies. At this time, this cooperation involves five network laboratories in other countries and over twenty computer manufacturers.

The testing methodologies developed at the NBS are well documented, and the testing tools themselves are developed with the objective of portability in mind. They are made available to many organizations engaged in protocol development and implementations.

Assisting Users and Manufacturers

The NBS works directly with government agencies to help them use evolving network technologies effectively and apply international and government networking standards properly. When large amounts of assistance are required, the NBS provides it under contract.

Assistance to industry is provided through cooperative research efforts and by the availability of NBS testing tools, industry wide workshops, and cooperative demonstration projects. At this time, the NBS is working directly with over twenty computer manufacturers in the implementation of network protocol standards.

Consistent with overall goals, NBS standards developments, research in testing methodologies, and technical assistance are characterized by direct industry and government cooperation and mutual support.

DOD OBJECTIVES

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 ot 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.

Performance and Functionality

The performance and functionality of the protocols must provide for the many unique operational needs of the DOD. The following paragraphs discuss in some detail both these needs and the ways they can impact protocol design.

Survivability includes protecting assets, hiding them, and duplicating them for redundancy. It also includes endurance--the assurance that those assets that do survive can continue to perform in a battle environment for as long as needed (generally months rather than hours); restoral--the ability to restore some of the damaged assets to operating status; and reconstitution--the ability to integrate fragmented assets into a surviving and enduring network.

The DOD feels that an important reason for adopting international and commercial standards is that under cases of very widespread damage to its own communications networks, it would be able to support DOD functions by using those civil communications that survive. This would require interoperability up to the network layer, but neither TCP nor TP-4 would be needed. The committee has not considered the extent to which such increased interoperability would increase survivability through better restoral and reconstitution.

Availability is an indication of how reliable the system and its components are and how quickly they can be repaired after a failure. Availability is also a function of how badly the system has been damaged. The DDN objective for system availability in peacetime varies according to whether subscribers have access to l or 2 nodes of the DDN. For subscribers having access to only one node of the DDN, the objective is that the system be available 99.3 percent of the time, that is, the system will be unavailable for no more than 60 hours per year. For subscribers having access to 2 nodes, the objective is that the system be available 99.99 percent of the time, that is, the system will be unavailable for no more than one hour per year.

Robustness is a measure of how well the system will operate successfully in face of the unexpected. Robustness attempts to avoid or minimize system degradation because of user errors, operator errors, unusual load patterns, inadequate interface specifications, and so forth. A well designed and tested system will limit the damage caused by incorrect or unspecified inputs to affect only the performance of the specific function that is requested. Since protocols are very complex and can be in very many "states", robustness is an important consideration in evaluating and implementing protocols.

Security attempts to limit the unauthorized user from gaining both the information communicated in the system and the patterns of traffic throughout the system. Security also attempts to prevent spoofing of the system: an agent attempting to appear as a legitimate user, insert false traffic, or deny services to users by repeatedly seeking system services.

Finally, Security is also concerned with making sure that electronic measures cannot seriously degrade the system, confuse its performance, or cause loss of security in other ways.

Encryption of communication links is a relatively straightforward element of security. It is widely used, fairly well understood, constantly undergoing improvement, and becoming less expensive. On the other hand, computer network security is a much newer field and considerably more complex. The ability of computer network protocols to provide security is a very critical issue. In the past decade much has been learned about vulnerability of computer operating systems, development of trusted systems, different levels of protection, means of proving that security has been achieved, and ways to achieve multilevel systems or a compartmented mode. This is a dynamic field, however, and new experience and analysis will probably place new requirements on network protocols.

Crisis-performance needs are a form of global robustness. The nature of a national security crisis is that it is fraught with the unexpected. Unusual patterns of communication traffic emerge. Previously unstressed capabilities become critical to national leaders. Individuals and organizations that had not been communicating must suddenly have close, secure, and reliable communications. Many users need information that they are not sure exists, and if it does, they do not know where it is or how to get it. The development of widely deployed, interoperable computer networks can provide important new capabilities for a crisis, particularly if there is some investment in preplanning, including the higher-level protocols that facilitate interoperability. Presidential directives call for this. This will become a major factor in DOD’s need for interoperability with other federal computer networks. The DOD, as one of the most affected parties, has good reason to be concerned that its network protocols will stand the tests of a crisis.

In addition, there are performance and functionality features that are measures of the capability of the network when it is not damaged or stressed by unexpected situations. Performance includes quantifiable measures such as time delays, transmission integrity, data rates and efficiency, throughput, numbers of users, and other features well understood in computer networks. Equally important is the extent of functionality: What jobs will the network do for the user?

The DDN has established some performance objectives such as end-to-end delays for high-precedence and routine traffic, the probability of undetected errors, and the probability of misdelivered packets. Such objectives are important to engineer a system soundly. The DOD must place greater emphasis on more complex performance issues such as the efficiency with which protocols process and communicate data.

The DOD has stated a need for an effective and robust system for precedence and preemption. Precedence refers to the ability of the system to adaptively allocate network resources so that the network performance is related to the importance of the function being

performed. Preemption refers to the ability of the system to remove users (at least temporarily) until the needs of the high-priority user are satisfied. The ARPANET environment in which the protocols were developed did not emphasize these capabilities, and the current MILNET does not function as effectively in this regard as DOD voice networks.

The DOD has also stated a need for connectionless communications and a broadcast mode. In the majority of network protocols, when two of more parties communicate, virtual circuits are established between the communicating parties. (For reliability, additional virtual circuits may be established to provide an in place backup.) DOD needs a connectionless mode where the message can be transmitted to one or more parties without the virtual circuit in order to enhance survivability; provide a broadcast capability (one sender to many receivers); and handle imagery, sensor data, and speech traffic quickly and efficiently.

If intermediate nodes are destroyed or become otherwise unavailable, there is still a chance that the data can be sent via alternate paths. The broadcast capability is particularly important in tactical situations where many parties must be informed almost simultaneously and where the available assets may be disappearing and appearing dynamically. The Department of Defense requires an internetting capability whereby different autonomous networks of users can communicate with each other.

Interoperability

Presidential and DOD directives place a high priority on interoperability, which is related to the internetworking previously discussed.

Interoperability is primarily important at two levels: network access and applications. To achieve interoperability at the level of network access,users of backbone communications nets must utilize the same lower-level protocols that are utilized by the network. Generally these protocols are layers 1, 2, and 3, up to and including part of the IP layer. In other words, interoperability for network access does not depend on either implementation of the transport layer (TP-4 or TCP) or of all of the internet (IP) layer. The primary advantages of network access interoperability are twofold:

1. Significant economies of scale are possible since the various users can share the resources of the backbone network including hardware, software, and development and support costs.

2. Network survivability for all users can be increased significantly since the network has high redundancy and, as the threat increases, the redundancy can also be increased.

Interoperability at the applications layer allows compatible users at different nodes to talk to each other, that is, to share their data,

support each other, and thereby coordinate and strengthen the management of forces and other assets. Interoperability at the applications layer can be achieved through the use of specialized software that performs those functions of higher-layer protocols (such as TCP or TP-4, file transfer, and virtual terminal) that are needed by the particular application. If some of the higher-layer transport and utility protocols have been developed for particular hosts or work stations, their use greatly reduces development, integration, and support costs, although with a potential sacrifice of performance. Interoperability at the applications level, that is, full functional interoperability, is important to specialized communities of users such as the logistics, command and control, or research and development communities. As these different communities utilize the DDN, they have the advantages of shared network resources. Within each community there is full functional interoperability but generally there is much less need for one community to have functional interoperability with members of another community.

The implementation of TCP or TP-4 within network users, but without the implementation of higher-level protocols and application interoperability, is not generally an immediate step in increasing interoperability. It does have these immediate advantages:

It represents an important step in investing in longer-term interoperability.

It generally represents an economical near-term investment on which communities of interest can build their own applications.

It facilitates the development of devices for general network use such as Terminal Access Controllers (TACs).

Interoperability at the applications level will become increasingly important among the following communities: Worldwide Military Command and Control Systems, including systems of subordinate commands; Department of Defense Intelligence Information Systems; U.S. tactical force headquarters (fixed and mobile); NATO force headquarters; other U.S. intelligence agencies; the State Department; and the Federal Bureau of Investigation and other security agencies.

Although interoperability of applications within the DOD has the highest priority, it is clear that government wide and international interoperability will be an objective with increasing priority. The NATO situation is especially important (6).

---

(6) Europe has been a major force in the development of ISO standards. Consistent with this is a NATO commitment to adopt ISO standards so long as they meet military requirements.

In a somewhat longer time period, DOD will want applications interoperability with many commercial information services. As interoperable computer networks become more common, processing and data services will burgeon in the marketplace. These will include specialized data bases and analytic capabilities that all large organizations will need in order to be up-to-date and competitive.

With regard to interoperability at the network level, DOD will want to be able to utilize commercially available networks for both survivability and operational effectiveness and economy. In the case of a major war in Europe, for example, the United States would want to be able to use surviving PTTs (Postal, Telegraphy, and Telephony Ministries) for restoral and reconstitution. During peacetime there will be cases where special DOD needs can be best satisfied with commercially available capabilities.

As technology continues to provide less expensive, smaller, and more reliable data processing equipment, computer networks will become increasingly prevalent at lower levels of the tactical forces--land, air, and sea. It will be important that these tactical networks be capable of interoperability with each other (for example, air support of ground forces) and with headquarters. It is likely that the tactical network will need a network architecture and protocols that are different from the ARPA-\and ISO-derived protocols. If so, the developments will place requirements on the higher-level DOD protocols.

If the DOD chooses to move from TCP to TP-4, this can be done in phases for different communities of interest and subnetworks. In this way if there is difficulty in converting one subnet, the rest of the network need not be degraded. Also the different subnets will be able to make the transition at the most suitable time in terms of cost, risk, and the need to interoperate with other subnets. As a result if DOD uses TP-4 for some new nets or major upgrade of existing nets, this will generally not reduce interoperability in the near term unless interoperability of applications is needed between two communities. In this case specific interoperability needs may be satisfied with specialized gateways for mail or data exchange.

The DOD points out that it desires all networks to be interoperable since it is not possible to predict when one community will need to communicate with another or use the resources of the other. As previously indicated, however, unexpected needs for full functional interoperability can only be met when appropriate higher-layer software is developed.

Minimize Costs

The Department of Defense seeks to minimize costs of development, procurement, transition (if it decides to move to ISO protocols), and support. Generally the objective is to limit life-cycle costs, that is, the total costs over a 5-to-8-year period with future costs suitably discounted (10 to 20 percent per year).

The Department of Defense has already made a heavy investment in protocols, and the investment has paid off in the success of current protocols operational in many networks. On the other hand, the DOD acknowledges the potential advantages of using the ISO protocols if made available as commercially supported products. Development costs for these protocols can be small since their development cost is amortized by the commercial vendor over a larger market. Support costs for these protocols (including minor modifications, integration into other products, documentation, and training) are also significantly reduced because of vendor-supplied services. These cost factors are further discussed in Section IX in terms of the three options presented in Section VIII.

Ease of Transition and Manageability

Networks must be manageable and capable of growth and improvement. The Department of Defense generally makes the fastest progress in developing complex information systems if it evolves these capabilities while working in concert with the users and the acquiring agencies. In this light, the following factors are important:

Minimal interruption of current service--For most DOD networks it is essential that they operate continuously. If there is to be transition to new protocol services (whether based on current DOD versions or ISO), it is important that these transitions be planned, designed, and pretested so that the transition will be nondisruptive.

Verifiability--It is essential to have a testing capability where new protocol implementations can be thoroughly tested to ensure that they will interoperate, have full functionality specified, do not contain errors, are robust, and meet quantitative performance needs. The National Bureau of Standards has established such a capability, and it is being used to verify a number of TP-4 implementations, including those demonstrated at the National Computer Conference in July 1984. An IP-testing capability is being added. The Department of Defense is planning a similar protocol test facility for TCP, but work is just getting underway. If the DOD plans to migrate promptly to TP-4, there is a question whether this investment is warranted.

Compatibility with higher protocols--As the transport and lower-protocol layers evolve, it is essential that they maintain full compatibility with higher-layer protocols. This is particularly important for the DOD because it will increasingly have inter-operability at the applications level.

Responsiveness to evolving DOD needs--Current DOD needs will change or new needs may arise. It is very likely, for example, that subtle performance problems may be discovered in a protocol that are unique to the strenuous DOD-operating environment and that could have serious operational consequences. If the DOD is using commercial protocols products based upon international standards, the DOD will need two commitments when critical deficiencies are discovered. It will need a commitment from the manufacturer that critical problems

will be promptly fixed and a commitment from the NBS that it will move quickly to change federal standards and seek changes in international standards.

Minimal risks--The DOD needs are so large and important, it cannot afford to take otherwise avoidable risks.

Maintenance of manageability--The DDN is new and is using a new approach after the cancellation of AUTODIN II (7). There are pressing operational needs and many impatient users. If the DOD delays in moving to ISO protocols and later decides to do so, the costs and disruption will be large. On the other hand, moving now to ISO will be less disruptive.

---

(7) AUTODIN II was a program to develop a data communications system for the DOD. The program envisioned relatively few large packet switches. It was cancelled in 1982 in favor of ARPANET-derived designs because of considerations of security, architecture, survivability, and cost.

III. COMPARISON OF DOD AND ISO PROTOCOLS

This section presents a general description of the major functional differences between the ISO and DOD protocol sets at the transport and network layers and then discusses particular aspects of the protocols: performance, security, and risk.

COMPARISON OF DOD AND ISO TRANSPORT LAYERS

Differences between the Defense Department's TCP protocol and the International Standards Organization's TP-4 protocol are described in terms of items visible to users of the protocol. Internal differences in mechanism that have no effect on the service seen by the user are not considered. A second much simpler protocol, the User Datagram Protocol (UDP), providing datagram or connectionless service at the transport layer is also briefly considered.

In summary, the services provided by TCP and TP-4 are functionally quite similar. Several functions, however, including data transfer interface, flow control, connection establishment binding, and out-of-band signals are provided in significantly different ways by the two protocols. Neither seems intrinsically superior, but some effort would be required to convert a higher-level protocol using TCP to make use of TP-4. The exact amount of work needed will vary with the nature of the higher-level protocol implementations and the operating systems in which they are embedded. A programmer experienced with the higher-level protocols would require about six months to design, implement, and test modifications of the three major DOD higher-level protocols (file transfer, mail, and Telnet) to work with TP-4.

There are several areas in which the openness and lack of experience with the TP-4 specification leave questions about just what functionality is provided and whether incompatibilities are allowed. These areas include connection-establishment binding, flow control, addressing, and provision of expedited network service. The best way to resolve these questions seems to be to implement and test TP-4 in a military environment and to further specify desired procedures where there is unwanted latitude allowed by the standard (see the recommendations section XI).

There is one area in which the NBS-proposed Federal Information Processing Standard (FIPS) differs from the ISO specification: The FIPS provides a graceful closing service as in TCP, while the ISO does not.

Data Transfer Interface

TCP is stream oriented. It does not deliver any End of Transmission (EOT), but accepts a "push" on the send side which has an effect much like an EOT causes data being buffered to be sent.

TP-4 is block oriented and does deliver EOT indications. By indicating EOT, a sending user should be able to accomplish the same effect as "push" in TCP in most reasonable TP-4 implementations.

The impact of this is uncertain. Neither type of interface is inherently better than the other. Some applications will find it more convenient to have a stream-type interface (for example, interactive terminal handling), while others might prefer a block mode (for example, file transfer). It should be possible for TP-4 to approximate the stream mode by forwarding data without an EOT from the sending user and delivering data to the receiving user before an EOT is received. Some work would have to be done on applications using one type of protocol to modify them to use the other.

Flow Control

TCP has octet units of allocation, with no EOT and hence no impact of EOT on the allocation. The segment size, Transport Protocol Data Unit (TPDU) size, used by the protocol is invisible to the user, who sees allocations in units of octets.

TP-4 has segment units of allocation, with a common segment size for both directions negotiated as part of connection establishment. Although in some implementations the protocol’s flow control is not directly visible to the users, in others it is. In the latter case, users of TP-4 will see allocations in units of segments and will have to be aware of the segment size for this to be meaningful (for example, to know that a window of four 100-byte segments seen will be consumed by two messages of 101 to 200 bytes each).

The impact is uncertain. Both octet and segment units of flow control can be argued to have their advantages for different types of application. The former makes it easy to indicate buffering limits in terms of total bytes (appropriate for stream transfer), while the latter makes it easy to indicate buffering limits in terms of messages (appropriate for block mode). The way in which flow control is exerted over an interface is complex and one of the most performance-sensitive areas of protocols, so a significant conversion and tuning effort would be required to get an application used with one type of high-level protocol to be able to perform using another.

Error Detection

TCP applies ones-complement addition checksum. TP-4 uses an ISO

algorithm (8). The error-detection properties of the TCP procedure have not been studied carefully, but the ISO algorithm is thought to be somewhat stronger and hence allows fewer nondetected errors in data passed to users. It should be noted that the TCP checksum is defined to include certain fields from the IP level including addresses so that double protection against misdelivery errors is provided. The practical difference in error-detection power is probably not important.

Simultaneous Call Between Same Users

TCP will establish one call. TP-4 will establish two calls if both sides support multiple calls, no call if they allow only one call (that is, see each other as busy), or in very unusual circumstances, one call. The impact is minor since most applications naturally have an initiator and a responder side.

Multiple Calls Between Same Addresses_

TCP allows only one call between a given pair of source and destination ports. TP-4 allows more than one by using reference numbers. The impact is minor since it is easy to generate a new per-call port number on the calling side in most cases. This can be a problem in TCP, however, if both are well-known ports.

Addressing

TCP provides sixteen bit ports for addressing within a node identified by the internet layer. Some of these ports are assigned to well-known applications, others are free for dynamic assignment as needed.

TP-4 provides a variable-length transport suffix (same as Transport Service Access Point Identifier) in the call-request packet. The use of addresses at different levels in the ISO model has not yet been solidified, but it seems likely that addressing capabilities similar to TCP's will eventually be provided by TP-4 (or possibly the session layer) along with standard addresses for common applications.

The impact is likely to be minimal, but this is an open area of the ISO specifications that may need further definition for use by DOD.

Binding User Entities to Connections

TCP requires a prior Listen Request from a user entity for it to be able to accept an incoming connection request. Normally a user entity must exist and declare itself to TCP, giving prior approval to accept

---

(8) For additional information, see Information Processing Systems, Open Systems Interconnection, Connection-Oriented Transport Protocol Specifications, ISO DIS 8073, Section 6.17, page 45.

a call from a specific or general remote entity. In some implementations it may be possible for a nonresident user entity to cause a Listen Request to be posted and an instance of the entity to be created when a matching connection request arrives. TCP does not queue an incoming connection request with no matching Listen Request but instead rejects the connection.

TP-4 requires no prior request but passes a Call Indication to a user entity whenever a Call Request is received. It is, however, left open as an implementation decision as to how TP-4 finds and/or creates an appropriate user entity to give the Call Indication; that is, the service does not include or define how user applications make themselves available for calls (no Listen Service Primitive). The implementation guidelines indicate that well-known addresses, prior process existence, and Call Request queuing are all facilities that may or may not be provided at the implementor's choice (9). This would seem to allow for different choices and hence failure to establish a connection between standard implementations (for example, caller expects requests not to be queued, while callee does queuing, and hence never responds).

The practical impact is uncertain due to lack of experience with how the various options allowed by the TP-4 standard will be used in practice. TCP seems more oriented to a prior authorization mode of operation, while TP-4 most easily supports an indication-with-later-acceptance scenario. It is not clear how TP-4 will support rejecting calls to nonexistent or inactive user entities and how user entities could control how many calls they would accept. This area may require DOD refinement.

Out-of-Band Signals

TCP allows the user to specify an urgent condition at any point in the normal data stream. Several such indications may be combined, with only the last one shown to the destination. There is no limit to the number of urgent indications that can be sent. The TCP urgent messages are sent requesting expedited service from the network layer so network bottlenecks can be bypassed as well.

TP-4 allows users to send expedited data units carrying up to sixteen octets of user data. These are only half synchronized with the normal data stream since they may be delivered before previously sent normal data, but not after subsequently sent normal data. Each expedited data unit is delivered to the destination, and only one can be outstanding at a time. ISO has indicated its intention to allow transport protocols to use network-level expedited service, but this

---

(9) Specification of a Transport Protocol for Computer Communications, Vol. 5: Guidance for the Implementor, Section 2.11.2. National Bureau of Standards, Institute for Computer Sciences and Technology, (Washington, D.C.) U.S. Department of Commerce, January 1983.

is not yet defined.

The impact is primarily for applications like terminal traffic handlers that must deal with interrupt-type signals of various types. The need to read an arbitrary amount of normal data and recognize urgent data in the normal stream are difficulties with TCP urgent service, but it has been used successfully by the Telnet protocol. The lack of full synchronization of the signal and normal data in TP-4 may require users to insert their own synchronization marks in the normal data stream [as was the case with the old ARPA Network Control Program (NCP)], and the limitation of one outstanding signal may be restrictive. Some effort would be required to convert higher-level protocols using one transport protocol to using the other.

Security

The committee has determined that the TCP and TP-4 are sufficiently equivalent in their security-related properties so that no significant technical points favor the use of one over the other.

The DOD protocol architecture assigns the security-marking function to the IP layer and provides an 11-byte security option with a defined coding in the IP header.

TP-4 provides a variable-length security option carried in Call Request packets. A variable-length security option field is also provided in the ISO IP. Standard encoding of security markings are under consideration but not yet defined and accepted.

In addition to these explicit security-marking fields, the existence, coding, and placement of other header fields have security implications. If data is encrypted, for example, a checksum is usually used to determine if the decrypted data is correct, so the strength of the checksum has security implications.

Precedence

TCP supports precedence by using three bits provided in IP headers of every packet. TP-4 provides a 2-byte priority option in Call Request packets. A 2-byte priority option in the ISO IP header is also under consideration. Currently, no implementations make use of precedence information (to support preemption, for example). There should be no impact, therefore, of changing from one protocol to the other.

Type of Service

The types of network service that can be requested via TCP and TP-4 are somewhat different. The impact seems minimal since few networks do anything with the type of service fields at present with the exception of DARPA’s packet radio and satellite nets. This may become more important in the future.

Datagram Service

TCP provides only reliable session service. A separate User Datagram Protocol (UDP) in the DOD architecture supports transaction or connectionless-type interaction where individual messages are exchanged. UDP is merely an addition of the port-addressing layer to the basic datagram service provided by IP. No delivery confirmation or sequencing is provided (although IP provides fragmentation and reassembly).

The NBS TP-4 specification originally presented to the committee provided unit-data-transfer service within the same protocol framework as sessions (10). This material has since been deleted to bring the NBS proposal into conformance with ISO work. A separate ISO datagram protocol similar to UDP has been defined and is expected to become a draft proposed standard in June 1984.

Closing

TCP provides a graceful closing mechanism that ensures that all data submitted by users are delivered before the connection is terminated. The NBS TP-4 provides a similar mechanism, but is not included in the ISO standard TP-4, which provides only an immediate disconnect service. Impact is significant if the ISO version is used because users would then have to add their own graceful termination handshake if desired.

COMPARISON OF DOD AND ISO INTERNET LAYERS

The internet protocols of DOD and ISO are much more similar to one another than the transport protocols. This is not surprising since the Defense Department's IP was used as the basis for the International Standards Organization's IP. Some reformatting, renaming, and recoding of fields has been done. Hence not only are the services to higher layers essentially equivalent, but the protocol mechanisms themselves are also nearly identical. Due to the format changes, however, the two protocols are incompatible.

It should be noted that the IP itself forms only part of the internet layer. For clarity it should also be noted that the internet layer in ISO is considered to be the top sublayer within the network layer.

In DOD, there is an additional Internet Control Message Protocol (ICMP) that deals with error conditions, congestion control, and simple routing updates to host computers. There is also a Gateway-to-Gateway Protocol (GGP) that deals with internet management and routing updates for gateways. In the ISO, only the IP itself has so far been

---

(10) National Bureau of Standards, Specification of a Transport Protocol for Computer Communications, Vol. 3, Class 4 Protocol, ICST/HLNP-83-3, February 1983.

considered, while most error reporting, control, and routing functions are considered "management" functions that remain to be addressed in the future.

The only significant differences in the IPs themselves are in the areas of addressing and error reporting. The DOD IP has a fixed-length, 32-bit source and destination addresses (identifying network and host) plus an 8-bit "protocol number" field to identify the higher-level protocol for which the IP data is intended. The ISO IP has variable-length source and destination addresses whose format and content are not yet specified, although preliminary documentation indicates that ISO intends to support a similar level of addressing (network/host) in a more global context which would allow use of current DOD addresses as a subset. There is no equivalent of the DOD protocol number field, although possibly the tail of the variable-length ISO addresses could be used for this purpose.

Error reporting is provided within the ISO IP by means of a separate packet type, while the DOD provides more complete error- and status-reporting functions via the separate Internet Control Message Protocol (ICMP), including routing "redirect" messages to hosts that have sent datagrams via nonoptimal routes.

In summary, from the functional point of view, DOD and ISO IP can be considered essentially equivalent with the provision that the ISO-addressing scheme is suitably resolved. The absence of routing and control procedures from the ISO internet layer means that additional procedures beyond IP would be needed to produce a complete, functioning, internet even if the ISO IP were adopted. It appears that the existing DOD ICMP and GGP or its successors could be modified to operate with the ISO IP with modest effort, but this requires further study and validation in an operational system.

A table at the end of this chapter compares DOD and ISO IP packet formats.

COMPARISON ON THE BASIS OF PERFORMANCE, SECURITY, AND RISK

Performance

The performance of a transport protocol, such as TCP or TP-4, is a function of its implementation as well as its inherent design. Experience in implementing TCP and other proprietary protocols has demonstrated that implementation considerations usually dominate. This makes it difficult to compare protocols, since a wide range in efficiency of implementations is possible. Furthermore, there are a number of dimensions along which an implementation can be optimized.

Despite the difficulties, protocol designers have developed several metrics for comparing transport protocols. These view protocol performance from a variety of perspectives, including (1) user response time, (2) throughput on a single connection, (3) network and host computer resource utilization. Protocol efficiency can also be

significantly affected by the communications environment. Protocol efficiency must be considered in a wide range of communication environments, including local area networks, satellite links, terrestrial links, and packet-switched networks.

The critical algorithms most affecting protocol performance are those that perform end-to-end error control and end-to-end flow control. These algorithms affect the response time, throughput, and resource utilization of the protocol during the data transfer phase. The efficiency of the connection management procedures may also be important in applications involving frequent connections of brief duration.

The committee compared the algorithms and message formats specified for each protocol for critical functions, including flow-and error-control and connection management. They concluded that since the two protocols were sufficiently similar there would be no significant difference in performance of TCP or TP-4 implementations of equal quality optimized for a given environment.

The committee compared the error-and-flow-control algorithms of TCP/IP and TP-4. Both employ window-based techniques using large-sequence number spaces and both permit large window sizes. Their differences are minor. TCP performs its error-and-flow-control in units of octets, rather than the protocol data units employed by TP-4. This adds a small amount of overhead to TCP calculation in return for a finer control over host buffer memory. The committee did not consider the difference significant, assuming that appropriate buffer management strategies are implemented by transport and higher-level protocols. TP-4 employs more sophisticated techniques to ensure that flow-control information is reliably transmitted than does TCP. These more sophisticated techniques may reduce TP-4 protocol overhead during periods of light load in some applications, possibly adding slightly more CPU load in other cases. The committee did not consider these effects significant.

Both protocols employ a three-way handshake for establishing a transport connection. The differences between the TCP and TP-4 handshake are related to the addressing conventions employed for establishing connections and do not affect protocol efficiency. In the common cases where a client process requests a connection to a server process, the TCP and TP-4 operations are equivalent.

Both protocols permit a range of policy decisions in their implementation. These include (1) selection of timer values used to recover from transmission errors and lost packets, (2) selection of window sizes at the receiver and transmitter, and (3) selection of protocol data unit sizes. Both permit substantial reduction in control message overhead by expanding window sizes. Both permit credits to be granted "optimistically," permitting receiver buffers to be shared over several transport connections and permitting credit reduction in the event of buffer congestion. Both permit optimizing protocol efficiency by delaying control message traffic when it does

not need to be transmitted, combining it with later data or control traffic.

The most significant difference between TCP and TP-4 flow control derives from slight differences in expression of flow control at the transport layer service interface. TCP employs a stream model while TP-4 uses a message model. These two models are equivalent in function; however, some higher-level applications protocols may be more naturally expressed in one model than the other. The committee considered the possibility that current ARPA protocols might require some adaptation to operate more efficiently with TP-4. For this reason the committee recommends that the DOD study the operation of current DOD higher-level protocols on TP-4 (recommendation 5, Chapter XI).

Security

The committee considered the impact of security requirements on transport protocols primarily and also on overall protocol hierarchies in the DOD, The American National Standards Institute (ANSI), and ISO. Based on the information the committee received, it finds that:

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

There is no technical impediment to their equivalent evolution over time in the security area.

Risk

There are several risks in implementing a new protocol or protocol family. These include (1) fatal flaws in protocol design not easily rectified, (2) errors in protocol specification, (3) ambiguities in protocol specification, (4) errors in protocol implementation, (5) performance degradation due to inefficient implementation, (6) performance degradation due to "untuned" implementation, and (7) performance degradation due to untuned application protocols.

This list of risks comes from experience in implementing computer networks based on the DOD protocols and proprietary commercial protocols. Considering that it took more than ten years for the current TCP protocols to reach their current state of maturity and that the TP-4 protocol is only about two years old, the committee devoted considerable attention to the maturity of TP-4.

Fatal Flaws in Protocol Design

Early ARPANET protocols had a number of "fatal" design errors that resulted in deadlocks or other serious system failures. Commercial networks had similar problems in early design phases. The committee considered the possibility that TP-4 could suffer from similar faults and concluded that this was unlikely. TP-4 employs design techniques

similar to those of TCP and proprietary transport protocols. The faults encountered in the ARPANET are now well known. Indeed, the state of the art in transport protocol design is now quite mature. The developers of the TP-4 protocol were familiar with the earlier protocols and their problems.

Errors and Ambiguities in Protocol Specification

Early in the development of TP-4, NBS developed a formal protocol specification and a test environment based on this specification. A protocol implementation can be partially compiled automatically from the formal specification. Other implementations can be tested against this master implementation. The NBS protocol laboratory was used to debug the formal specification of TP-4 and is currently being used to certify other implementations of TP-4. The laboratory has also developed and employed tools to analyze the specification for possible problems. The existence of this laboratory and the results obtained to date led the committee to conclude that there is no substantial risk associated with the TP-4 protocol specification.

In contrast TCP has only recently received a formal specification. To the committee's knowledge most existing TCP implementations predate the formal TCP specification and have not been derived from the formal specification. In the committee's opinion the formal TCP specification is likely to have more bugs or ambiguities than the TP-4 specification.

At the present time NBS has developed the only formal specification for ISO TP-4. ISO is currently developing standards for formal specification techniques that are similar to those used by NBS. When these specifications are complete ISO will update the TP-4 specification to include a formal description. In translating the current informal ISO specification into the formal specification there is a risk that the ISO specification may be changed such that it is no longer consistent with the current NBS specification. The National Bureau of Standards is playing a key role in developing the ISO formal specification techniques and formal specification. It plans to generate automatically an implementation of the ISO formal specification and verify it against the NBS specification using the NBS test tools. In the committee's opinion this makes the risk of unintentional changes in the ISO specification quite low.

One possible risk remains. The ISO specification for TP-4 that was approved is an informal document subject to the ambiguities of informal protocol specifications. The formalization may remove ambiguities that have gone undetected and that were the basis of its approval. It is conceivable that once these ambiguities are exposed, the current consensus for TP-4 may dissolve. The committee considers this risk to be very low. The areas of ambiguity in protocol specifications are typically only of concern to protocol implementors. The current protocol implementors through much of the world are typically using the NBS formal specifications as a basis of their implementations of TP-4 and have access to the NBS test tools for

certifying their implementations. In the event of a possible conflict, the majority of implementors could be expected to support resolution of ambiguities in favor of the current NBS formal specification, making it unlikely that ISO would approve an alternate resolution.

Errors in Protocol Implementation

Several factors influence the likelihood of errors in a protocol implementation. These include the complexity of the protocol, quality of the protocol specification, the experience of the implementors, and the availability of test tools. Based on the availability of the NBS test tools and formal protocol specification for TP-4, the committee did not see any significant risk of errors in implementing TP-4.

Performance Issues

The largest risk in implementing TP-4 concerns the performance of the implementations. This risk is not inherent in the protocol as specified, but is present in new implementations of any transport protocol. Experience has shown that performance can often be improved by a factor of two or more by careful attention to implementation details and careful performance measurement and tuning. The committee considered it likely that some initial implementations of TP-4 will have significantly lower performance than the current mature implementations of TCP. Evidence to support this conclusion may be found in data supplied by the DOD which show a wide range of performance of TCP implementations.

Some members of the committee expressed the belief that over the long term, TP-4 will afford better performance due to widespread commercial support. Vendors will be highly motivated to optimize performance of their TP-4 implementations, since a large number of users will benchmark implementation performance. Many individuals will become familiar with implementations of TP-4 and with configuring and operating networks based on TP-4. Initially, this expertise will be found in organizations developing TP-4 implementations and installation.

The committee believes that the largest performance risks atioshort eeations and
ncejy os netwwhicly m-lopintocol. Es be

founrts ane initly m-lopintefntle hayrs TP-4.
instaeseoion tmpllac errorience has aneiguring and

have y m-lopintwhicocol. Es runtefnd tivthatP-4. I-d on Torks bash0 -22 Td(The comh
implmectheismd
confbe siiort the ot inhected to swith showly inhecasil

modifications to TP-4. It is unlikely that such problems will be serious enough to prevent an early transition to TP-4. If such problems are discovered, it is expected that they can be handled through the normal standards process of periodic enhancement. A number of proprietary commercial networking protocols are similar in operation to TP-4 and do not have serious performance problems. Any enhancements that may be desirable can probably be added to TP-4 in a compatible fashion, permitting interoperation of enhanced and unenhanced implementations.

TABLE: Comparison of DOD and ISO IP Packet Formats

DOD	ISO (not in correct order)
Protocol version: 4 bits	Version: 8 bits
Header Length (in 32-bit words): 4 bits	[Header] Length (in bytes): 8 bits
Type of service: 8 bits (includes 3-bit Precedence)	Quality of service**: 8 bits Precedence**: 8 bits
Total Length: 16 bits	Segment Length: 16 bits
ID: 16 bits	Data Unit ID*: 16 bits
Don't Fragment flag	Segmentation Permitted flag
More Fragments flag	More Segments flag
Fragment offset: 13 bits	Segment offset*: 16 bits
Time to live (sec): 8 bits	Lifetime (.5 sec): 8 bits
Protocol number: 8 bits	---
Header checksum: 16 bits (provided by subnet layer)	Header checksum: 16 bits Network Layer Protocol ID: 8 bits
---	[Generate] Error flag
(in ICMP)	Type: 5 bits
---	Total Length*: 16 bits
.....	.....
Source address: 32 bits	Source address length: 8 bits Source address: var.
Dest. address: 32 bits	Dest. address length: 8 bits Dest. address: var.
.....	.....
OPTIONS: NOP, Security, Source Route, Record Route, Stream ID, Time Stamp	OPTIONS: Padding, Security Source Route, Record Route, Quality of service, Precedence, Error reason (only for error type)
.....	.....
DATA	DATA

* only present if segmentation is in use
** in options

IV. STATUS OF DOD AND ISO PROTOCOL IMPLEMENTATIONS AND SPECIFICATIONS

DEPARTMENT OF DEFENSE

The DOD internetting protocol was first introduced in 1974 and later split into separate TCP and IP specifications. From 1974 until 1978, when they were adopted as DOD standards, the protocols underwent a number of major revisions. These revisions were largely a result of extensive experience gained by researchers working on the DARPA Internet project. The DARPA "Request for Comment" and "Internet Experimental Note" technical report series document the conclusions of numerous protocol-related studies and discussions. Successive specifications of TCP and other internet protocols are also given by reports in these series. Most of these specifications were informally presented and were accompanied by discussions that affected design choices. The most recent TCP documents introduce a more formal style of presentation (11).

The first experimental TCP implementations were completed in 1974 at Stanford University and Bolt Beranek and Newman, Inc., for the PDP-11/ELF and DEC-10/TENEX systems, respectively. Today implementation exists for numerous computer systems. While many of these were implemented at and are supported by university and other research groups, several are available as commercial products.

Testing of TCP was done on the ARPANET (12), other DOD networks (Satellite net, packet radio), and a variety of local networks. For several years a number of DARPA contractors used TCP in parallel with the old ARPANET transport protocol (NCP). In addition, for about six months preceding the January 1, l983, ARPANET cutover from NCP to TCP, these hosts were joined by additional TCP-only hosts (for a total of approximately thirty). This extensive testing prior to the cutover to TCP enabled the networks involved to maintain operational capability throughout

---

(11) Transport Control Protocol, DOD MIL-STD-1778, August 1983.

(12) The ARPANET is a data communications networklcol,I fhed in 1969-

DARP2) in 1983.

the transition and to achieve normal service levels in a few months. Today the TCP-based DOD networks includes hundreds of hosts (over 300 on DDN alone) and serves thousands of users. Traffic on just the ARPANET component is now approximately 500 million packets per month.

TCP is also extensively used on local area networks including Ethernet and Pronet, as well as on CSNET, the Computer Science Research Network (Telenet hosts).

In addition to TCP, the DOD protocol architecture includes internet layer protocols for communication between hosts and gateways (ICMP) and between gateways (GGP). Experience indicates that the design of robust and powerful gateways that internet numerous networks and provide survivability is a complex challenge. DOD is developing new gateway protocols that could be adapted to work with either DOD's or ISO's IP.

The higher-level protocols currently used on DDN for electronic mail (Simple Mail Transfer Protocol), file transfer (File Transfer Protocol), and remote log-in (Telnet) are TCP-specific. Their specifications are stable, and numerous implementations exist. The DOD has indicated its intent to adopt ISO higher-level protocols when they are specified and implementations are available.

The committee has concluded that the DOD transport and internet protocols are well tested and robust. It is unlikely that major problems with their design or specifications will be uncovered. No comprehensive facility or procedures for testing new implementations of TCP now exist, although efforts in this area are being started at Defense Communications Agency (DCA).

INTERNATIONAL STANDARDS ORGANIZATION

Standardization and development of the ISO IP and ISO TP-4 are proceeding in a relatively independent fashion. Currently, TP-4 is further along in the standardization process. The local area network communications environment has created an immediate need for TP-4 functions; however, communications within a single Local Area Network (LAN) do not need an internet capability. A "null" IP has been defined to enable TP-4 to be used on a single LAN without the necessity of a complete IP. It is quite likely that some early TP-4 products will implement this null IP, leaving implementation of the complete IP for future product development. In the following discussion, TP-4 and IP will be treated separately due to this potential independence.

TP-4 Status and Plans

The ISO TP-4 became a Draft International Standard in September 1983. The final stages in standardization are primarily procedural. The committee expects products that implement TP-4 to be widely available in the market within about two years. It normally takes twelve to eighteen months for implementations and testing prior to product announcement. Some vendors apparently began implementation and testing the protocol

soon after it became a draft proposal in June 1982, because the protocol was essentially frozen at that time.

At present, INTEL and Able Computer have announced the availability of products that implement TP-4 for use over LANs. The committee does not know, however, whether these products have been delivered or incorporated into systems. In addition, more than twenty companies have indicated their support of TP-4 and their intention to incorporate TP-4 into future products, without announcing specific products or availability dates. Most companies do not make specific product announcements until relatively late in the product development process.

In December 1982 six vendors and network users interested in early development of TP-4 products requested NBS to hold a series of workshops on the operation of TP-4 in a LAN environment. To date, four workshops have been held, with more than thirty companies in attendance. The first workshop set a goal of demonstrating multivendor networking at a major U.S. national computer conference. The second workshop, held in April 1983, determined that demonstrations would include a file transfer application and would be developed on two local area network technologies currently standardized by the Institute of Electrical and Electronics Engineers (IEEE). These technologies are the Carrier Sense Multiple Access with Collision Detection, which is standardized by IEEE committee 802.3, and the Token Bus, which is standardized by IEEE committee 803.4. The workshop selected the National Computer Conference in July 1984 for the demonstrations.

Vendors committed to the demonstration developed and tested TP-4 implementations using the NBS test tools. The workshops defined a schedule that called for individual testing through April 1984 with multivendor testing commencing thereafter. While the vendors that participated in the demonstration have emphasized that participation in the demonstration is not a commitment to product development, a number of large customers have indicated that there will be an immediate market demand for TP-4 implementation as soon after the demonstration as practical. The committee considers it highly likely that many commercial vendors will announce commitments to deliver TP-4 products shortly after the demonstration.

Internetwork Protocol Status and Plans

The ISO Internetwork Protocol (IP) became a Draft International Standard (DIS) in May 1984 (13). The DIS was out for ballot for the previous eight months. Attaining DIS status freezes the technical approach, permitting implementations to begin.

---

(13) ISO Draft Proposal, Information Processing Systems -- Data Communications -- Protocol for Providing Connectionless Network Services, DP 8473, May 1984.

The ISO IP specification is only one of several specifications needed to completely specify the Network Layer. A number of other specifications are needed, including a Gateway-to-Host error protocol, a network wide addressing plan, and a Gateway-to-Gateway Protocol for managing routing information. A complete specification is needed before an internetwork, consisting of gateways and hosts, can be deployed. Most of the complexity of the Network Layer, however, is confined to the gateways. A complete standardization of the Network Layer is not required to develop and deploy host systems.

The International Standards Organization is currently developing proposals for conveying error information between hosts and gateways. It is expected that responses to the Draft Proposal by ISO members will include proposals to provide these functions. The committee does not consider this a controversial area and expects that these capabilities will be included in the ISO standard by the time it reaches Draft International Status.

Addressing is a more complex issue. The addressing structure of a computer internetwork depends on complex trade-offs between implementation complexity, flexibility, network cost, and network robustness. Addressing structure in a large network can influence the range of possible policy decisions available for routing network traffic. The trade-offs for a military environment may be significantly different from those of a commercial environment. The ISO has considered these factors in its existing IP. A flexible addressing scheme is provided, permitting implementation of a variety of addressing structures. Host computers need not be concerned with the internal structure of addresses. The committee considers that the IP-addressing scheme has sufficient flexibility that host implementations can be constructed that will support the full range of addressing philosophies allowed by ISO, including those needed by DOD.

Routing algorithms, like addressing, are complex and often controversial. For this reason ISO has not yet attempted standardization of routing algorithms. A routing algorithm is a key part of a Gateway-to-Gateway Protocol. A single network must implement a common routing algorithm. In the absence of an ISO routing algorithm, a network must be based on either proprietary routing algorithms or on other standards.

The committee has studied the current ISO IP and the current ISO addressing structure. It believes that it will be possible to map the current DOD IP-addressing structure and routing algorithm into the ISO network layer. In practice this means that the Gateway-to-Host Protocols and addressing formats will fully comply with the ISO standards, while gateways will need to include additional DOD capabilities. (This is addressed in recommendations, section IX.) This approach will enable DOD to procure commercial host implementations, while retaining the need for procuring DOD-specific gateways. The committee believes these hybrid DOD-ISO gateways can be readily developed by modifying existing DOD gateway implementations. Since the majority of systems in a network are hosts and not gateways,

the committee considers this approach worthwhile.

To the committee's knowledge no vendor has yet announced plans to support the ISO Internetwork Protocol. This is not surprising, since the ISO IP attained Draft Proposal status only recently. The committee has considered the possibility that the ISO IP may not attain the same wide level of market demand and vendor support anticipated by TP-4. Since host support of IP is necessary for DOD to migrate to ISO protocols, the committee has considered this question in some depth.

While it is possible to operate TP-4 directly over a LAN or directly over an X.25-based, wide-area network, some form of internetwork capability or alternative approach is needed to interconnect systems attached to multiple LANs via Wide Area Networks (WANs). In the current ISO open systems architecture, this function is to be provided by the Network layer. There are two possible Network layer services, connectionless and connection oriented. The ISO architecture permits both of these services, leaving it to the market place to determine which approach is to be selected. The DOD believes that the connectionless approach best suits their needs.

Developing a connection-oriented network that operates over a mixed LAN and WAN environment is considerably more difficult than developing a connectionless one. Existing LANs are inherently connectionless and existing (X.25) WANs are inherently connection oriented. A protocol to provide internetwork service between these LANs must arrive at a common subnetwork capability. It is a relatively simple matter to adapt a connection-oriented to a connectionless service since it can be done by ignoring unneeded functions of the connection-oriented service. Adapting a connectionless subnetwork to the needs of a connection-oriented network service is much more difficult. Many of the functions provided by TP-4 would be needed in the network layer to build such a service.

Some work is currently going on in European Computer Manufacturer's Association (ECMA) to interconnect WANs and LANs in a connection-oriented fashion. There is considerable controversy surrounding several proposals, since some participants in the standards process do not believe the proposals conform to the ISO Reference Model for Open Systems Interconnection. This, plus their complexity, makes it unlikely that a connection-oriented network standard will gain support in ISO in the immediate future.

There is an immediate need for users to build networks consisting of interconnected LANs and WANs. Such networks are currently in place using vendor proprietary architectures. Market pressures to build multivendor LAN and WAN networks make it quite likely that vendors will adopt the immediate solution and implement the connectionless ISO IP. The committee believes that DOD can enhance the early availability of ISO IP by announcing its intention to use it. Commercial availability of IP is an important part of a migration strategy, as described in the section on recommendations. The

committee believes that vendors would be responsive to DOD requests for IP, since IP is quite simple to implement in comparison with TP-4 and since they foresee the need to operate in mixed LAN-WAN environments.

V. MARKETS

The committee reviewed the market demand and its potential with respect to both TCP and TP-4 to provide an indication of the likelihood and rapidity with which competition and its benefits will develop. The committee concludes that the market demand for TCP protocols will be small outside the United States. The demand for TP-4, on the other hand, is expected to be worldwide.

In this report we use the term market demand to indicate the potential or actual demand for products using the protocols under discussion. A large market is characterized by a broad demand from all sectors of the marketplace: consumers, businesses, and governments. The broadest demand is an international demand in all sectors. We distinguish the demand for products from the supply that usually develops as a result of the demand. It is assumed here that a broad market demand will result in a broad range of products, competitive in price, quality, function, and performance.

The demand for products implementing computer communication protocols is discussed in relation to the requirements placed on the potential customer. Specifically, the customer may be required to acquire products that meet one or the other of the standards under discussion or may have no obligation to use either of the two. That is, customers will fall into one of the following classes with respect to these standards:

1. DOD standards required.

2. International or National standards required.

3. No requirement with respect to standards.

Although customers in the third class may be under no formal obligation to use standards, they may still prefer a standard solution for several possible real or perceived benefits. They may, for example, obtain a broader selection of products using the standard solution or may obtain a more competitive price. They may also require a specific communication protocol in order to share information with products that are required by fiat to implement certain standard protocols. This need for compatible protocols to communicate is a powerful driving force toward communication standards.

DEPARTMENT OF DEFENSE NETWORKS MARKET STATUS AND PLANS

The major networks of the Defense Data Network include the following:

Military Network (MILNET)--operational and growing.

Advanced Research Projects Agency Network (ARPANET)--operational and growing.

WWMCCS Intercomputer Network (WIN)--to be upgraded.

DOD Intelligence Information System (DODIIS)--to be upgraded.

Strategic Air Command Digital Information Network (SACDIN)--to be upgraded.

Movement Information Network (MINET)--to be established in 1984.

Sensitive Compartmented Information (SCI) net--to be established in 1985.

TOP SECRET (TS) net--to be established in 1985.

SECRET net--to be established in 1986.

Initially, each of these networks has its own backbone. The networks will be integrated into a common Defense Data Network in a series of phases starting in 1984 with the integration of MILNET and MINET. It is planned that by 1988 they will all be integrated but communities of interest will operate at different security classifications interconnected with Internet Private Line Interfaces (IPLIs). When appropriate technology becomes available in the late 1980s, the network will have the capability for multilevel security, including end-to-end encryption, and will achieve interoperability between all users.

The following observations are relevant to the TCP and TP-4 issue:

The DOD currently has two major networks, MILNET and ARPANET, currently comprising the DDN. About sixty subnets and hundreds of hosts are internetted and most use TCP.

This year a European network, MINET, will be activated and integrated into the DDN. It uses TCP.

In the second half of 1983, fifteen additional subscribers have been added to MILNET and current planning estimates hundreds more additional subscribers in 1984 and 1985.

For the many DDN users that are, or shortly will be, interconnected over common backbones, there are groups of users that need interoperability within the group. These groups are determined by the military department they are part of as well as by functions such as logistics, maintenance, training, and many others.

The Air Force and the Army are both committed to the use of TCP for some of their networks or subnetworks (including Local Area

Networks) and active acquisition programs are underway, or will be initiated, during the next twelve to eighteen months.

The DDN Program Office has procured, or shortly will procure, devices to facilitate terminal and host access to DDN hosts and terminals. These devices employ TCP.

NATO has discussed protocol standards and has selected ISO as an approach, subject to its being adapted to meet military requirements, if such adaptation is necessary. There is no definitive planning underway, however, to develop a NATO computer network.

The Mail Bridge that will allow traffic to pass between the classified segment and the unclassified segment will use TCP and is scheduled for a 1987 Initial Operational Capability (IOC).

In general, the backbone in the various networks provides functions at layers below TCP and TP-4. As a result a backbone (such as MILNET) could support users of either protocol set. The users of one set could not, however, interoperate with the users of another unless additional steps are taken.

In summary, there is a large TCP community operational today and the community is growing rapidly. In addition, there are, or shortly will be, procurements underway that plan to use TCP. The rate of growth cannot be precisely estimated in part because of uncertainties in demand and availability of trunks and cryptographic equipment. On the other hand, interconnection of several major networks will not take place until 1987 or later; and for those elements that are interconnected, there are many groups of users that primarily require interoperability with each other.

System Descriptions

MILNET is a network for handling the unclassified operational data of the DOD. It was created after the decision in 1982 to cancel the AUTODIN II system by dividing the ARPANET into two nets, MILNET and ARPA Research Net. The majority of the capacity of ARPANET was assigned to MILNET, and the number of subscribers is growing rapidly. The network backbone does not require the use of TCP but its use is generally mandated for subscribers. To achieve TCP functions, the DDN will procure some interface devices and thereby take the burden off some subscribers.

ARPANET supports most of the research organizations sponsored by DARPA. It generally uses TCP but some users continue to use NCP.

MINET is a European network scheduled for Initial Operational Capability (IOC) in 1984 to handle unclassified operational traffic, mostly logistical, and tie into the MILNET. It will have 8 nodes, 8 TACs, and 3 hosts to process electronic mail. These hosts and others to be added to the net will use TCP and the File Transfer Protocol (FTP).

The Department of Defense Intelligence Information System currently uses a home-grown protocol. Sometime after 1984 its plans are to upgrade it to TCP. It will be a 3-node, 3-host net with plans to upgrade it to 20 to 30 nodes and about 50 hosts. The net is run at a high-security level (SCI) for communicating compartmented data. The SCI network consists of those users of SCI who are outside of DODIIS.

SACDIN is an upgrade of the digital communications system of the Strategic Air Command. The IOC is planned for about 1985. At present, TCP is not planned initially as a protocol. SACDIN will operate with multilevel security up to Top Secret sensitive information.

WIN is the WWMCCS Information Network. It is currently operational and uses NCP as a transport protocol. There is a major effort underway to modernize the WWMCCS, including upgrading or replacing current computers, providing Local Area Networks at major centers throughout the world, and providing common software packages for utilities and some applications. The upgrading of the transport protocols is part of this effort. Schedules are still uncertain but there is a target of 1986 for the protocol upgrading.

TOP SECRET is a network that will support top secret users other than WIN and SACDIN.

SECRET net is a network that will operate at the Secret level. It should be very useful for a large community that does not routinely need top secret or compartmented information. This is a community primarily outside the command and intelligence communities and includes missions such as logistics, procurement, and research and development. DOD will start the system as soon as there is sufficient cryptographic equipment; by 1986 they hope to have a 90-node network with several hundred subscribers.

The Army plans to establish a Headquarters Net tying together major headquarters with an IOC of 1986. It will use TCP.

The Air Force has established a Program Office to help in the development of Local Area Networks at major Air Force installations. These could be internetted using the DDN and thereby also gain access to other nodes. TCP has been mandated. Initial procurements are underway.

Mail Bridge will provide gateways between ARPA Research Net and other elements of the DDN. These would use TCP and are scheduled for IOC in 1987.

During 1984 the DDN is procuring two capabilities that will facilitate use of the network and higher-level protocols.

The first capability will be provided shortly by Network Access Controllers (NAC). The NACs provide three elements all based on TCP:

1. Terminal Access Controllers (TACs) allow a cluster of terminals to access hosts on the DDN. Many are in operation today as a legacy of the ARPANET developments. New ones will be competitively procured.

2. Terminal Emulation Processes (TEP) allow the connection of a high-capacity host to the DDN through a number of terminal-like lines.

3. Host Front-End Processors (HFP) allow high-capacity host connection to the DDN through use of a Network Front End that off loads much processing capacity from the host.

The second capability will be provided by software the DDN is currently procuring for up to seventeen families of specific combinations of hosts and their commercially available operating systems. The software packages will include 1822 or X.25, TCP, and utility protocols for terminal access, mail, and file transfer. Initial operational capability is planned for late 1985.

Integration

MINET will be connected to MILNET in 1984. This will be an unclassified network.

WIN, DODIIS, SECRET, and SACDIN will be integrated as a classified network in 1987 at the earliest. Since they all operate at different security levels, they will be able to use the same DDN backbone but will be cryptologically isolated.

Integration and interoperability of all the networks will not be possible until the late 1980s at the earliest, since this will require successful implementation of an advanced technology for end-to-end cryptological networking and the development of techniques for multilevel security in individual and netted computer systems.

The use of gateways as elements to integrate networks is under consideration. Gateways are currently operational to interconnect MILNET with (l) ARPANET (six gateways primarily used to exchange mail between authorized users), (2) MINET (one gateway for use prior to integration of the two networks into one), and (3) eight developmentally oriented networks. There are many more gateways internetting ARPANET with other research nets. Most of these gateways use the ARPA-developed Gateway-to-Gateway Protocol. It is now realized that this protocol is deficient for widespread use and ARPA has been investigating alternatives.

The earliest requirement for additional gateways in the operational elements of the DDN will be to internet Local Area Networks into global networks of the DDN. A new "stub" protocol has been developed that might meet this need. The DDN is reviewing its requirements for available gateways and approaches.

INTERNATIONAL AND NATIONAL STANDARD MARKET DEMAND FOR TP-4

In the United States and most countries of the world, national standards organizations adopt international data communication standards.

In the United States the standards for the transport protocols are established by the American National Standards Institute (ANSI). The same standards for the federal sector are established by the NBS with an exception for DOD's military needs which may be established by MIL standards. Market demand for the latter was previously discussed.

Outside the DOD there are numerous government agencies and organizations such as the Federal Aviation Agency, Internal Revenue Service, the Federal Bureau of Investigation, and the Federal Reserve Banks which have, or will have, networks that fall under the guidance of the NBS and will probably use the NBS-specified standard protocols when the NBS standard is issued. Already the Federal Reserve is procuring its computer networking products using the X.25 protocol.

National Support of International Standards

The earliest evidence of demand for TP-4 products is in countries that give strong support for ISO standards. Most countries outside of the United States give the international standards much stronger governmental support than the United States does for a variety of reasons. First, in most cases these governments own the postal and telecommunication monopolies. Frequently, the responsibility for these organizations is at a ministerial level in the government. Furthermore, many of the modern countries have concluded that the information industry is a national resource and one of the growth industries of the future. International standards that are neutral, in the sense that no manufacturer has a head start, give the companies in these countries the additional margin they feel is necessary to compete in the worldwide market. It is also recognized by many that a worldwide market is much better than a market demand fragmented by national geographic and political considerations. Finally, the PTTs have traditionally provided information services equivalent to those for which some of the ISO computer communication protocols are designed. The best example is Teletext, which is an upgraded version of the Telex system used widely outside the United States.

Consequently, government networks in many countries use the international ISO standards or the national standards derived from the international standards. Bid requests for government networks in France and Germany, for example, have required support for ISO protocols for over a year even though the standards are not yet fully approved. These bids ask the respondent only to state support for the protocols. No doubt, as the ISO protocols become stable, these countries will require the protocols for their networks. These government networks will further influence the implementation of networks not actually required to use the international and national standards.

MARKET SEGMENTS NOT REQUIRED TO USE TCP OR TP-4

Most of the demand for communication protocols comes from potential customers who are under no government fiat to use either TCP or TP-4 protocols in their networks or network products. Many of these will use existing supplier-specified protocols. Such protocols have been embedded in products for over ten years and are well tested both formally and through field experience in thousands of networks. Continuing demand for these protocols will not contribute to the relative demand for either TCP or TP-4.

There are widely recognized advantages in using international standard protocols for computer communications. First, there is tremendous value in exchanging information with other information users. As the standard protocols become widely used, the value of the information accessible through networks using these protocols is normally greater than the value of information accessible through less widely used networks protocols. This is the reason that industry groups such as airlines, banks, and insurance companies band together to set up common networks. Similarly, it is recognized that there are economies of scale for widely used networking protocols both in the sense that equipment can be obtained at lower cost and in the sense that the manufacturer's improvements in performance, function, and cost will be repaid by market demand. In addition, many network protocol users wish to have the option to procure equipment from a wide variety of vendors. Sometimes international standards encourage this environment. Finally, international organizations would prefer to have common procurement of equipment and software for worldwide operations. Thus international standards are preferred for operational as well as logistic considerations.

In the United States much of the demand for TP-4 will develop in the industries that exchange information regularly with entities of the federal government. If the Federal Reserve were to use the TP-4 standard for exchanging information with member banks, for example, there would be pressure on the banks to use TP-4. Similarly, if DOD suppliers wish to have easy access to DOD employees using a system based on TCP, they would need to use TCP. Also many of the university-oriented networks use the ARPANET protocols to exchange information with other university ARPANET users.

The committee concludes that the demand for TP-4 in the United States will significantly out weigh the demand for TCP independent of DOD's adoption of TP-4. If DOD adopts the ISO TP-4 immediately or if DOD adopts TP-4 after a demonstration, the U.S. market demand for TCP protocols will disappear as the current networks are converted to TP-4. If DOD chooses to use the DOD TCP indefinitely, clearly the DOD and ARPANET demand for TCP will continue.

A similar set of market forces operates outside the United States except that the foreign governments are more strongly in favor of international and national standards and have smaller investments in nonstandard equipment. Thus there are even more industries drawn to

the standards in order to share information. This is illustrated by the extremely strong support for ISO efforts. The European Computer Manufacturers Association has been active in the TP-4 standardization effort. NATO appears committed to TP-4 implementations, and there is likely to be intense competition in this arena. Lacking the federal government support of two different protocol suites, there is a stronger force to adopt a single international standard in most countries. There are other countries with a similar problem, however. Germany is beginning to install systems based on its unique national standard but has committed to convert eventually to ISO protocols.

The committee concludes that there will be little market demand for the TCP protocols outside the United States. The strong international demand will be for ISO protocols, including TP-4.

VI. DEVELOPMENT OF STANDARD COMMERCIAL VERSUS SPECIAL COMMERCIAL PRODUCTS

DOD has expressed a desire to use off-the-shelf commercial products because they are expected to be less costly. It is expected that performance of commercial products will be optimized to increase competitiveness. User cost will be lower because of a large commercial customer base over which to amortize costs for development, continuous improvements, and maintenance. Furthermore, the DOD may benefit from having more vendors compete for their business. This section examines the way vendors select standard products for development and the implications in cost, continuing supports, and improvements.

PRODUCT DEVELOPMENT VERSUS SYSTEM INTEGRATION

It is assumed in this discussion that off-the-shelf commercial products can be used through system integration to construct system solutions. Most vendors supply both standard products and system integration services. Some vendors supply only the integration functions, using other vendors' products. System integration adds value to the product and in some cases results in modifications of the product to meet system requirements. When standard products are used, the responsibility for continuing maintenance and improvements almost always can be passed to the product developer. Thus in this discussion we assume that off-the-shelf commercial products are standard products supplied by vendors to implement one or more transport-level protocols for the DOD.

CRITERIA FOR SELECTION OF STANDARD PRODUCTS

The product vendor's choice to develop a standard product is governed by market requirements, economic opportunities, and other design considerations. In the case of data transmission products, market requirements include competition, connection to the installed base of products, market growth, and satisfaction of the standards requirements of customers.

Often the vendor will develop a product that supports several protocols as options. Usually only one or two protocols will be selected for primary support, and all other options are considered for secondary support. The primary protocols selected for implementation are based upon the largest potential market for the vendor. These protocols become the vendor's standard products. Standard products are announced for sale and supported on a continuing basis. Implementations of secondary protocols are often adaptations of the implementations of standard protocols and may be suboptimal with respect to performance and continuing vendor support. Often secondary implementations are created when an RFP is issued and the vendor who wishes to respond to the RFP must create a special product to do so. This committee believes that, in general, future standard data transmission products will be either TP-4 or vendor-unique protocols and TCP will be a special product.

STANDARD VERSUS SPECIAL PRODUCT

Within the OSI architectural model, seven layers are defined, each of which will have protocols defined for interconnection of systems. These protocols are controlled by standards. TP-4 is an example of a protocol for the transport layer. These protocols will be implemented on many vendor systems that have different systems architecture, different operating system architectures, and, therefore, differences in the specifics of the layer interface. The vendor systems will be designed to optimize the specific environments that each vendor has determined are most important to satisfy the major market objective for that vendor's particular computer architectures. This determines the vendor's standard system and architecture. Support of special requirements will frequently be designed as modifications to a standard system, using translators and other techniques to bridge the differences in layer interface definitions, operating systems structure, and protocols. Most support activity, optimization of performance and resource usage will be directed at the standard system architecture selected by the supplier.

Special-Product Process

Special-product development is initiated to meet customer specifications. The specifications, schedule, and cost assume that special products are released using an existing version of the software system (operating system, language, communications, and data manager). Support for the special product is conditioned on a support contract. The special product is tested and released with that system. This provides the fastest availability of the product, since the schedule will only include the time to develop the product and test it with the selected system. It is likely that by the time a product and its software system are delivered, a newer version of the software system containing code corrections and added functions and other new products will have been released. Additional cost to the customer is required if the vendor is to modify the special product to operate on this new version of software. This occurs frequently in a rapidly developing technology. If the special product is not modified, operational and maintenance expenses may increase.

Standard-Product Process

A standard product is developed to meet the market requirements of a market area. The development of a standard product generally has a target date that is used as a basis for scheduling system development, fabrication, and testing into a planned software system release. The product then is included in the test and integration plan for the system release and integration into a systems test procedure to assure operation with the other parts of the software system. The standard product then becomes a part of the software system, and as new releases of the system are made, the product is tested as a part of the integrated system to assure that it still operates with the revised, new system. The product may also be enhanced to satisfy new requirements or resolve problems of the earlier version. The product

then will operate with the latest software system release.

The integration process complicates the development process. The increased complexity may result in a longer development schedule or may require more resources than special products require since (1) the cycle may involve a longer product requirement definition, (2) additional planning and integration testing may be needed to coordinate the product design with other system activities, and (3) there is the possibility of up to twelve months' delay in scheduling a software system release, which for most vendors generally occurs at 6- to 12 month intervals. The product may be maintained with a corrective code released in intermediate system fabrication and integrated into the following software release. Different categories of support may be available and these categories may vary by product. The support categories may range from no support to full unlimited warranty.

CONCLUSION

The committee concludes that there are significant benefits for the Department of Defense in using standard commercial products that meet the department's operational needs:

Costs to the DOD for development, production, and maintenance are significantly lower because (l) vendors spread the cost over a much larger user base, (2) commercial vendors have to be efficient in their operations in view of the competition in the market, and (3) vendors look for ways to upgrade their product to meet competition.

The department may get additional useful products because vendors integrate the protocol function into their corporate software and hardware product lines. Thus the DOD may be able eventually to use standard commercial software application products that are built on top of, and thereby take advantage of, the transport protocols. The DOD will thereby have a wider selection of standard commercial application products to choose from. By depending on industry to manage the development, maintenance, and upgrade of products, the DOD can use its scarce management and technical resources on activities unique to its mission.

VII. RESPONSIVENESS OF INTERNATIONAL STANDARDS PROCESS TO CHANGE

The international standards process has proven its ability to respond quickly to new requirements and protocol problems uncovered during standardization. The United States, through organizations such as the NBS, the ANSI, and IEEE has a leadership role in this process. The committee concludes that the process can be responsive to DOD's needs.

The DOD will benefit from active participation in the international protocol standardization efforts. This will ensure that the DOD's evolving computer communications needs will be met in future commercial products. Also the DOD will have access to a broad spectrum of protocol experts and have access to those developing future commercial products. These benefits will far out weigh the costs of participation.

There will probably be very few high-priority instances where DOD will require immediate changes to its operational commercial software. These may relate to security or survivability. In order to accommodate these changes in the short run, the DOD will need agreements with its commercial suppliers for quick fixes to be made while the standard is being changed.

VIII. OPTIONS FOR DOD AND NBS

The committee believes that the Department of Defense is committed to adopting commercial standards when they are suitable and available and, therefore, will adopt the ISO standards eventually as the military standard for transport-level communication protocol. Further, the DOD realizes the benefits in cost and reliability of obtaining its data communications equipment from vendors who offer it as standard products. Of the three options identified by the committee, the first two are ways for the DOD to realize these benefits while the third option would withhold the benefits from the DOD indefinitely.

The primary difference between Option l and Option 2 is in the timing of the transition from TCP to TP-4. This timing difference has implications in risk, cost, and manageability of the transition. (This is discussed in Chapter X in greater detail.)

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. The Department of Defense would either require that products be validated using these test facilities or 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 should, however, 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 of 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.

IX. COST COMPARISON OF OPTIONS

There are so many variables affecting cost, it is impossible to compare precisely the cost for each option over time. The estimates in this section are, therefore, mostly qualitative. They are based on the wide experience of several committee members in commercial networking (14).

Cost comparisons among the three options are difficult for two reasons:

1. There are an unlimited number of scenarios that can be considered for the growth of DOD's data communication networks in the next fifteen to twenty years, involving questions such as (a) How many different implementations will there be? (b) What economies of scale can be achieved? (c) How much software will be shared between different implementations? (d) How much will the standards change for greater effectiveness or to accommodate higher-layer standards? and (e) What will happen to manpower costs in this high-skill area?

2. It is difficult to isolate the costs attributable to developing, implementing, and maintaining the protocols at issue. This is especially true if we assume DOD continues to use its own unique protocols. For both in-house and contractor efforts, the costs associated with TCP are folded into many other efforts. If DOD moves to commercial protocols, the marginal costs may be more visible.

---

(14) The committee has had some access to a study recently conducted by the Defense Communication Agency that compares the costs of commercially maintained versus government-maintained operating systems for the Honeywell computers used in WWMCCS. Although the WWMCCS example has many fewer dimensions and systems than are covered by this analysis, the committee urges the DOD to review this study as a good example of potential savings from commercially vended software. (WWMCCS-ADP System Software Economic Analysis. J. Stephens and others, Joint Data Systems Support Center, Defense Communications Agency, Technical Report, in draft.)

A major motivation expressed by the DOD for using commercial protocols is that the commercial protocols are significantly cheaper. If this is the case, then many in the DOD would like to know the savings over the next ten to twenty years if DOD adopts TP-4. This is not a question we will try to answer in this report, but the concept of opportunity costs is significant. If DOD can successfully move to commercial standards, then it will eventually be able to use DOD's scarce management and technical resources to strengthen its efforts in other areas of information communications and processing that are more unique to the DOD. Given the finite pool of such resources available to the DOD, the value of this transfer may be significantly greater than the dollars saved by adopting the international standards.

The following assumptions have been used in trying to estimate the cost factors if DOD moves toward adopting TP-4 using either Option 1 or 2:

No major subsystem of the DDN (which includes MILNET, DODIIS, WWMCCS, and so forth) would use both protocols at the same time except possibly for a brief transition period.

In only a few selected cases would a capability be required to handle both protocols. These cases could include select hosts that use both, special servers (most likely mail servers) that could provide functions between several communities of interest using both protocols, or translating gateways between networks.

Within the DDN both sets of protocols would be used for a period of five to ten years starting eighteen months after the DOD approves the use of TP-4 in a new system.

In virtually all cases, the phase-over from TCP to TP-4 in a subsystem of the DDN would be performed at a time when there is a major upgrade of subsystem elements that include TCP as a part. In other words, the transition is not merely a substitution of transport or internet software except in cases where the hardware currently being used is from a vendor who has started to offer TP-4 as a commercial product. Where this is not the case, the transition includes the substitution of new hardware whose vendor provides TP-4 commercially.

COST FACTORS AND MODEL

Four major factors must be considered in evaluating the costs of the three options:

1. How much lower will be the cost of commercial, standard-product protocols compared to those developed and acquired by the DOD?

2. If DOD decides to adopt TP-4, how quickly can it start using it in new systems, and how quickly will it phase TCP out of older systems?

3. What will be the one-time cost of management and test before DOD is prepared to start using TP-4?

4. What will be the marginal costs of maintaining the two standards over the 5- to 10-year transition period?

Savings Using Commercial Software

Commercial software providing TP-4 will tend to be cheaper than DOD provided TCP because commercial one-time and recurring costs (especially the former) can be apportioned over a larger consumer base, and the commercial supplier will tend to be more efficient. As in most cases where one compares the cost of one product provided by two vendors, there will be situations where a DOD vendor providing TCP can do it more cheaply than a commercial vendor providing TP-4. These occurrences will be rare but they illustrate the difficulty of developing detailed quantitative models that compare the costs. Factors relating to competing suppliers go far beyond the transport protocols themselves and distort such models.

The first argument relating to the size of the consumer base has many factors. For the time period under consideration, DOD represents about 3 percent of the commercial U.S. computer base. It would follow that DOD should pay much less in development and support costs for the commercial products. But there are other factors. The number of commercial suppliers is larger than the number of DOD suppliers by a factor of 5-10. The DOD's need for transport and internet protocols will be greater than the average commercial user in the time period under consideration. If commercial vendors break out the costs of developing these protocol features earlier than planned, DOD will pick up a larger share of the tab. This could be by a factor of 2 or more. A good deal of the one-time development and production costs of TCP have already been spent by the DOD or partly written off by DOD vendors. This factor would be extremely difficult to estimate, but we do not think it is very significant since the major costs in implementation relate to processes down-the-line from getting a C-language version. These down-the-line processes must be repeated in great part as families of hardware and software are upgraded with system and technology improvements to meet DOD directives for standard TCP products. There are also factors that cut in the other direction; if the DOD is only 3 percent of the U.S. commercial user market, it is an even smaller fraction of the international user market. This latter market is growing; its need for ISO protocols will be relatively higher than the U.S. market, and market share for U.S. manufacturers, including foreign subsidiaries, is large and holding its own.

The situation is equally complex when it comes to comparing the efficiency of commercial vendors with DOD vendors when it relates to developing, installing, and maintaining transport and internet protocols. The elements that favor increased efficiency of the commercial supplier include the following:

The commercial marketplace is much larger, less regulated, and is forced, therefore, to seek greater efficiency and innovation.

Transport and internet protocols represent functions that interact very closely with operating systems, the largest portion of which are commercial. The major sources of expertise for dealing with these operating systems are in the commercial marketplace, primarily with the vendors who supply the hardware as well as with vendors who specialize in related products.

The commercial sector is in the business of managing the interplay between operating systems, protocols, related software and hardware products, new technology and architecture, and the relationship between all these and the market. If DOD adopts TP-4, it will be delegating many of these management functions to a marketplace that will generally make better and faster decisions.

For every dollar that the DOD might invest in TCP, how much would it cost to gain comparable capability with TP-4 procured as vendor standard products? The many factors involved make a precise estimate impossible. We believe, however, that TP-4 can be procured at substantial savings and with virtually no economic risk if the market develops as we believe it will, with many vendors offering it as a commercial product by mid-1986. On the average, we judge the savings to be 30 to 80 percent including initial installation, field support, and maintenance.

How Soon Will TP-4 Be Used?

The sooner that DOD decides to use TP-4, the greater will be DOD’s savings. These savings can offset the adverse cost factors discussed in the next two sections: the cost to decide to use TP-4 and the added cost for the period when two standards (TCP and TP-4) are in use.

Currently, TCP is generally used in MILNET, MINET, and ARPANET. As previously stated in the assumptions, even if DOD decides to move aggressively toward TP-4, there are no evident, strong economic or operational reasons for converting these users to the new standards until a major upgrade of the users’ communications and processing subsystems is planned. Also in the next twelve to eighteen months new uses of these nets are planned that will expand existing subnets and these new users would use TCP in order to be interoperable with the current users in their community of interest.

In some cases the planning for new subnets for new communities of users is well along. DODIIS is a primary example. Some of these subnets should very likely proceed with TCP, but others appear to be prime targets for TP-4 if DOD is to move in the direction of adopting TP-4. The WWMCCS and its WIN are probably good examples of the latter. Planning and implementation for all of these subsystems must move ahead, however, and if DOD does not make a firm commitment to TP-4 by mid-1985, the number of systems that will move ahead with TCP will

probably constitute almost half of the growth of the DDN in the next five years. In other words, delay of a decision to move to TP-4 until 1986 would mean that most of the DDN subnets that will exist in the late 1980s will be based on TCP, whereas a decision for TP-4 a year earlier could significantly reduce this number.

Cost of Decision to Use TP-4

The costs of the decision to use TP-4 include the one-time management and test costs that DOD decides are needed before a TP-4 commitment and policy can be approved. Under Option 1 these costs are small. Under Option 2 they are significantly higher, although the amount will depend on the extent and duration of the testing needed. Under Option 3 there will be no management and test costs.

Marginal Costs of Maintaining Two Standards

If DOD moves toward the gradual introduction of TP-4, both standards will have to be maintained for five to ten years. The additional costs of maintaining two standards include the following:

Management costs of dealing with two standards.

Costs for developing and maintaining capabilities for limited intercommunication between systems using the different transport and internet protocols. These include costs for gateways, dual-capability hosts, and special servers such as mail.

Parallel validation capability. The DOD is implementing a validation capability for DOD TCP. This is similar to the currently operational NBS facility for TP-4 testing. If DOD selects Option 1, there is a question whether this DOD facility should be completed for TCP (because the number of new implementations of TCP would be small several years from now). If DOD selects Option 2, the facility is probably desirable.

Costs for maintaining research and development (R&D) programs to improve the standards. A part of the DARPA and DCA research and development programs in information technology is directed at system issues related to TCP. This includes work on internet issues, gateways, and higher-level protocols. The committee has not reviewed the research program for details and cost; however, a commitment to move toward ISO standards should affect the program. Costs would increase to the extent that the program would be involved with interactions with both protocols. There would be some decreased requirements for R&D in light of potential dependence on commercial R&D to improve the standards. In the next several years, however, the committee concludes that dual standards would, on balance, somewhat increase R&D costs because of the DOD’s unique operational requirements.

These costs are roughly the same for Options 1 and 2 and depend on how DOD manages the transition. Under an austere transition, which does

not provide extensive interoperability between TP-4 and TCP-based systems and minimizes costs in other areas, the overall costs could be low in comparison with potential savings.

Evaluation of Options by Cost

In terms of the previously discussed factors, savings can develop in two ways: by using TP-4 instead of TCP in new systems and by replacement of TCP with TP-4 in existing systems when this can be done smoothly and efficiently. The earlier that TP-4 is introduced, the greater these savings.

In contrast costs will be incurred in two ways: in one-time planning to use TP-4 and in continuing costs of operating two standards.

The following is a summary of the cost evaluation of the three options in the near term:

Option 3 is least expensive. It achieves no commercial savings but has no costs for one-time planning and maintenance of dual standards.

Option 1 is at most only slightly more expensive than Option 3 since one-time planning costs (which are much lower than for Option 2) and maintenance costs can be significantly offset with commercial savings in the following several years.

Option 2 is most expensive since it does not realize significant offsetting commercial savings.

In the longer term (beyond the next several years) commercial savings for Options 1 and 2 should overtake costs of transition, and both these options should cost the same.

There is a concern on the part of some members of the committee whether the higher near-term costs of Option 2 are adequately offset by the Option’s long-term savings to warrant the transition.

X. EVALUATION OF OPTIONS

We present a summary of the strengths and weaknesses of each option, followed by a detailed evaluation for each set of criteria.

SUMMARY

Option 1's primary benefit is that it would allow the DOD to obtain the benefits of standard commercial products in the communication protocol area at an early date. These 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, and commercial), which presumably will use TP-4, would also be brought about more quickly. Option 1 involves greater risk, however, since it commits to a new approach without 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 since 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 since 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/or delay. It would allow the most rapid achievement of full internal interoperability among DOD systems. Manageability should be good, since only one set of protocols would be in use (one with which the DOD already has much experience) and the DOD would be in complete control of system evolution. Procurement costs for TCP systems would remain high compared to 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 provides a quicker route to interoperability within the Defense Department and at the least risk, but at a higher life-cycle cost and incompatibility with NATO and other external systems.

DEFENSE DEPARTMENT OBJECTIVES VERSUS OPTIONS

The committee has identified a set of DOD objectives for transport protocols, discussed in Section II of this report. In this section we discuss the potential of each of the three options for achieving those objectives. The objectives have been grouped into five major categories that serve as criteria for evaluation of options.

Functional and Performance Objectives

There are certain functional and performance objectives that standard DOD transport protocols must satisfy. Key objectives include security capabilities, the ability to establish message precedence in crisis situations, and survivability of continuing operations when failures occur and portions of the network become inoperable. This implies continuous availability of the primary data transmission network and the ability to reconfigure the networks to operate after some of its nodes are lost.

As previously stated, the two protocols are functionally equivalent. TCP and TP-4 have equivalent reliability characteristics and are able to detect and recover from failures. The committee also concludes that robustness, availability, and performance in crises are equivalent using either protocol. The committee concludes that all three options equally satisfy the functional objectives that DOD requires.

Since the performance characteristics of TCP versus TP-4 will be a function primarily of the particular implementations, the committee concludes that the two protocols are sufficiently alike that there are no significant differences in performance of a TCP or a TP-4 implementation of equal quality when each is optimized for a given environment.

If Option 1 is selected, early implementations may result in suboptimal performance. Option 2 specifies that there be a demonstration network established that will provide time for adjustment, testing, and gaining experience. Option 3 would result in no reduction in performance of current networks. The maturity of TCP has resulted in many implementations that have demonstrated good performance. This experience provides a knowledge base for future implementations of either TCP or TP-4. In either case, however, initial implementations of TCP or TP-4 may be suboptimal and require additional development to optimize performance.

Maximizing Interoperability

A high-priority DOD objective is interoperability among its internal networks and among internal networks and non-DOD, external networks, including NATO. Interoperability allows users of a network to have access to applications on the same or other networks.

Option 3 would allow the DOD to increase internal interoperability most rapidly by continuing to mandate use of TCP for all new systems. Interoperability with external systems, however, the vast majority of which are expected to use ISO standard protocols, will remain limited.

The more quickly DOD moves to use TP-4, the more rapidly external interoperability will improve. In the short run internal interoperability will be reduced due to the existence of both TCP and TP-4 protocols by different subnets. This problem is greater with Option 2 then Option 1 since the number of systems and the length of time both protocols are in use is greater. In both options the problem can be reduced by providing special servers and translating gateways to provide limited interoperability where needed among subnets using different protocols.

Minimizing Procurement, Development, and Support Costs

A DOD goal is to assure availability of commercial-grade transport systems from vendors and minimize development, procurement, and continuing support costs. Both Option 1 and, after demonstration, Option 2 result in DOD adopting the TP-4 standard that has the endorsement of both national (ANSI) and international (ISO) standards organizations. Further, this protocol has been endorsed for use by NATO, the European Computer Manufacturer’s Association, the Computer and Business Equipment Manufacturer’s Association (CBEMA), and the NBS Institute of Computer Sciences and Technology for the information processing community of the federal government.

The result of the endorsements will be widespread use of the standard protocol in worldwide networks and a large number of vendors supplying commercial grade products supporting TP-4. As previously noted, many vendors have already stated they plan to develop TP-4-based products and many are already doing this in-house. Thus a large market and large vendor base will assure the availability of commercial grade TP-4 products.

A large market and supply of commercial-grade products will give DOD a large competitive base from which to select its data transmission systems. The effect will be to reduce DOD acquisition cost because large markets allow vendors to amortize development and support cost over a large base. This favors adoption of either of the options that results in DOD using TP-4 as its standard.

With the availability of commercial-grade products, vendors will take the responsibility for continuing maintenance and enhancements of the product. Transmission products are tightly coupled to the operating

systems on the host computer systems in which they operate. With vendor support of the products, evolution of both the host computer operating system and transmission system will occur in synchronization. This again favors the adoption by DOD of either the Option 1 or Option 2 that results in TP-4. In these options much of the support cost is covered by the vendors and spread over the large market base. This reduces the development and maintenance cost passed on to the DOD.

The committee does not believe that a large market beyond the DOD will develop for TCP because worldwide markets for products will be based on the ISO standards. Consequently, if the DOD chooses Option 3, only the DOD-dedicated vendors would supply TCP as standard products resulting in a smaller market and supply for TCP products and limited availability of TCP products.

If DOD remains with TCP, many commercial vendors will be forced to develop and support both the commercial standard products (TP-4) and DOD standard special products (TCP) to stay in both markets. In many cases only the large market-based products such as TP-4 will be considered standard and TCP products will be considered special products. The effect is higher development and support cost to the vendors which would be passed on to DOD. Thus the incentive for continuing enhancement to the special product, TCP, would be reduced. This responsibility would be passed to DOD, also resulting in higher costs.

Ease of Transition

The DOD is concerned with the ease and risk associated with transition from the current network architecture using TCP to its future network architecture. The objectives for DOD are to reduce the interruption of data communication services supplied by its active networks; minimize the risk of using an immature, untried protocol; and maximize the use of the critical skills, knowledge, and experience of the engineers who develop the communications products.

The maturity of TCP and the momentum that exists in the DOD community for implementing future systems using TCP would favor Option 3. Selection of Option 3 would minimize interruption of service and minimize risk. With this option there would be no transition; the DOD would remain with its current policy. There would be no conversion costs and the only risks for DOD would be associated with poor implementations of new TCP-based products.

The committee believes that much of the technical risk is associated with implementations. Therefore, given the relative state of their specifications and implementations as discussed earlier, the committee feels that the risks are comparable for implementing new products for either TCP or TP-4. Since DOD is acquiring many new networks the implementation risk of either TCP or TP-4 will be equal.

If DOD chooses Option 1, it will display confidence in the TP-4

specifications and in the vendor's implementations through its immediate commitment for TP-4 use in new military networks. DOD will, in effect, be making a commitment similar to that of vendors who are planning this protocol for their standard products. Since most new networks would not use a transport protocol other than TP-4, this minimizes the number of networks and therefore the cost of converting and maintaining TCP networks to TP-4.

Since the standard TP-4 products from vendors are not available today, DOD endorsement of TP-4 may have the effect of accelerating vendor development of standard products. These products are expected to be generally available by 1986. Thus Option 1 can be consistent with the manufacturers' expected product plans. Option 1 provides, therefore, the least conversion cost but with higher risk for DOD conversion.

If DOD chooses Option 2, then the risk that TP-4 will not meet DOD needs is reduced since there is no commitment to use this protocol until a successful demonstration is completed. In the interim, many networks will have been committed using TCP, resulting in higher conversion costs than with Option 1. In summary, Option 2 provides a lower risk approach for DOD to convert to TP-4, but will encounter the higher conversion cost.

There is a great deal of experience with TCP and thus there is an engineering community that is highly knowledgeable about it. As previously noted, however, if DOD remains with TCP, some DOD vendors will be forced to support multiple protocol products. The functional equivalence and similarities between TCP and TP-4 permit an easy transition for the experienced engineer to move from TCP to TP-4. Option 2 allows more time for this transition to occur, and thereby minimizes the risk associated with a complete switch to TP-4.

In addition to the transport protocols, a transition from TCP to TP-4 also involves the conversion of applications. The committee has concluded that the services provided by TCP and TP-4 are comparable and applications software can be moved from TCP to TP-4 without loss of functionality. Obviously, Option 3 requires no conversion to existing applications on current implementations. Option 2 will result in more applications interfacing to TCP than Option 1, thus potentially increasing conversion costs. In the future DOD could minimize the cost of conversion by standardizing the services provided by the transport layer to the applications.

Manageability and Responsiveness to DOD Requirements

The final set of objectives is concerned with the degree of difficulty that DOD will experience in managing its installed networks and future networks. As communications requirements evolve, DOD must have the ability to alter specifications so they will satisfy new requirements. Finally, DOD requires facilities for validation of protocol implementations as they are added to their networks.

Since Option 3 is to maintain the status quo, no additional management

difficulty is anticipated.

Both Option 1 and Option 2 will cause some additional management difficulties since they require that the current momentum for adopting TCP to be redirected toward TP-4 without loss of intensity. In addition to this change, DOD must manage both TCP and TP-4 networks. This will add to its management difficulties.

Option 2 will result in greater management difficulties than Option l due to the larger number of TCP systems that must eventually be converted and the larger time period over which both protocols must be supported.

There are benefits from each option. If Option 3 is selected, DOD and its vendors have sole responsibility for determining what changes are needed, implementing the change, validating the change and the ongoing maintenance of the standard. If either Option 1 or Option 2 is chosen, then DOD may encounter difficulty in persuading the standards groups to adopt its proposals; however, DOD would gain the experience and knowledge of the industry standards-making bodies. The industry standards bodies should be receptive to good technical arguments for correction of errors or apparent major deficiencies in the protocol. The standards bodies that maintain the standard should become a technical resource for DOD to develop its military specifications.

Since TP-4 will be a commercial standard, those vendors who adhere to the standard will insure that validation facilities are in place. The National Bureau of Standards has a test facility for TP-4. No such facility exists for TCP. If Option 1 or Option 2 is chosen, DOD can use this facility to validate vendor implementations. DOD should work with NBS to develop a similar facility for TCP. This is particularly important for new implementations of TCP. DOD should continue working with and through NBS in getting needed protocol revisions introduced into the appropriate standards bodies.

In summary, Option 3 results in no new management difficulties while Option 2 causes the greatest difficulties. Option 1 allows DOD to move toward commercialized standard products with the smallest addition of management tasks.

EFFECT OF PROPOSED OPTIONS ON MARKET SHARE

Option 1 would quickly reduce the market held by TCP products as TP-4 products begin to take hold in the marketplace. In addition, it would enhance the ability of U.S. manufacturers to compete in the world networks market based on ISO standards because they would not have to engage in parallel development nor support two sets of protocols for very long. Option 2 could have a comparable but less pronounced effect in the marketplace and it would be delayed. Because of the very probable rapid deployment of TCP-based systems in DOD networks while the TP-4 is still in the demonstration phase, however, many more networks than in Option 1 would probably end up using TCP. This would tend to reduce the U.S. manufacturer’s competitive edge in the world

market because their need to develop and maintain both TCP products as well as TP-4 products would dilute their skill resources. The same thing would happen with Option 3. Although none of the options would affect the world market for TP-4 greatly, Option 3 would result in a residual market for TCP products in the DOD and related networks.

Products made specifically for this market would continue to exist, but with functions limited to this specific market, the products would lack some of the advantages of large-scale production and product development.

XI. RECOMMENDATIONS

We first present our basic recommendation and then provide detailed recommendations on aspects that require amplification. These are followed by additional considerations in several important areas relating to the transition plans. Many of our recommendations are closely related to each other, and care should be taken not to consider any single recommendation in isolation.

BASIC RECOMMENDATION

The committee unanimously recommends that DOD should adopt the ISO TP-4 (and IP) as DOD costandards with its TCP (and IP) and move toward eventual exclusive use of TP-4. Transition to use of the ISO standards, however, must be managed to maintain operational capabilities and minimize risks. The timing of the transition to use of these protocols is, therefore, a major concern, and the committee was divided on the best schedule to recommend.

A majority of the committee favored immediate adoption of the ISO protocols as costandards with TCP, giving major procurements in 1984-85 the option of using these standards (Option 1). A minority favored deferring adoption of the ISO protocols by the DOD until after a demonstration of commercial quality implementations supporting military applications (Option 2). This difference is reflected in detailed recommendations 2-4 below. The reasons for the two viewpoints are based on differences within the committee on the extent of the risk associated with adopting a protocol, TP-4, that has not been implemented on operational networks.

DETAILED RECOMMENDATIONS

In the following recommendations the committee provides details about actions that should be taken to implement the basic recommendations. Most of the recommendations involve actions that require the DOD to take the lead role, with occasional support from the NBS Institute for Computer Sciences and Technology. Some recommendations are directed more toward NBS. Other government agencies and parties interested in using DOD protocols or in their future evolution may also find these recommendations applicable.

(1). DOD should rapidly identify "open areas" of the ISO TP-4 specifications where various options for implementation are allowed and define a required subset for use in DOD systems (a MIL-SPEC version of the standards, for example). In doing this, the DOD should work with the NBS with the goal of developing a Federal Standard, that has relatively few options for implementation, facilitates maximum federal interoperability, and makes it clear to vendors which functions are required in their commercial products.

(2). DOD should aggressively develop and implement a plan for integration of TP-4 as a costandard with TCP and for migration toward its eventual exclusive use. The plan should include provision for rapid completion of a MIL-SPEC (detailed recommendation 1), either validation or demonstration facilities (detailed recommendation 3), timing for procurement of systems with the new protocols (detailed recommendation 4), development of equipment and procedures to support a period of joint operation with both TCP and TP-4 protocols in use, and guidelines for eventual conversion of TCP systems to the new protocols.

Whatever timing is chosen for the introduction of ISO protocols, an extended period must be expected when both TCP and TP-4 are in use in different systems. Hence equipment and procedures must be developed to provide limited communication between systems using the two protocol sets. This will include dual protocol operation for some gateways, relay hosts, service hosts, and terminal concentrators. A secondary purpose of the test system described in detailed recommendation 3 should be to aid in development of this transition support equipment.

Both a general transition strategy and specific transition plans for each existing system should be developed. The switchover from old to new protocols will take place at different times as appropriate for each system during an overall transition period of many years.

(3). As soon as possible, the DOD should develop a protocol test facility. If Option 1 is followed, this facility would serve primarily to validate implementations of both old and new protocol sets. If Option 2 is followed, the facility would initially focus on demonstrating the suitability of the new protocols for use in a military environment as rapidly as possible and then provide for testing of commercially supplied protocol implementations.

For validation purposes, the NBS protocol-testing facility developed for ISO protocols should serve as a good basis, but extensions to deal with any DOD-specific option for the ISO protocols, performance, and DOD protocols would be necessary. DOD is now beginning such a program.

For a more complete demonstration, commercial-quality implementations of the ISO protocols must be obtained and shown to support military applications in an operational subnetwork such as such as ARPANET or DODIIS. In both cases the facility should also be used for development and demonstration of the transition support equipment mentioned in detailed recommendation 2.

(4). Procurements of new networks and major upgrades of existing networks should favor use of ISO TP-4 as rapidly as possible. If Option 1 is followed, RFPs may specify the new protocols immediately. If Option 2 is followed, this must await successful completion of the demonstration discussed in recommendation 3. Procurements for existing networks using TCP may continue to require TCP-based equipment until an appropriate conversion point is reached (see detailed recommendation 2).

The purpose of this recommendation is to minimize spending on new TCP implementations and their subsequent conversion to TP-4 where possible, while recognizing that some additions to TCP-based systems will also be needed. If Option 2 is followed, immediate requirements for new systems may force new implementations of TCP in these cases also because the demonstration is not completed at the time RFPs must be issued.

(5). As part of a transition plan, a transport service interface to higher-level protocols more like that of TP-4 should be developed for TCP and tested with existing higher-layer protocols.

This should serve as a rapid test of whether existing DOD protocols can make effective use of the somewhat different style of service that TP-4 provides. It should also allow higher-level protocols to be modified to make use of TP-4 in parallel with the implementation of TP-4 itself, making the ultimate transition to TP-4 more rapid and certain of success. Finally, it may allow use of a single version of the higher-level protocols to be used on both TCP and TP-4 equipment.

(6). DOD should continue using existing DOD-specific, higher-level protocols for operational purposes (Telnet, FTP, and Simple Mail Transfer Protocol, for example) but minimize effort on their further development and plan to adopt suitable ISO protocols as they are developed. Research on protocols providing new services (multimedia mail, compressed video, and voice store-and-forward, for example) should continue. The committee is pleased to find that DOD is already pursuing this course of action.

(7). The NBS Institute for Computer Sciences and Technology should maintain close liaison with DOD to ensure that DOD needs for new protocols and modifications to existing standards are effectively represented to appropriate standards bodies. This should include research areas such as multimedia mail where there is significant commercial as well as military interest.

The committee is pleased to find that this is already being done through contracts from DOD for ICST to represent its interests in standardization activities. Further cooperation (in demonstrating and testing protocols, for example) could occur.

(8). The NBS and DOD should collaborate from the outset in the development of new protocols for use as federal standards. This will ensure early agreement on functions, features, and services of the protocols under development. The NBS should present the developing work early to the ISO standardization activities to expedite convergence on internationally acceptable standards.

Such collaboration could help ensure that future protocol standards will be developed in a single, coordinated process that results in a single standard accommodating both DOD, other federal agencies, and commercial needs.

(9). DOD and NBS should develop additions to protocol specifications to support preemption of limited resources by high-precedence users. Such capabilities are needed during high-load situations such as might develop during wartime or other crisis situations. They are not yet part of either the TCP or TP-4 specifications or existing implementations. This should be an example of the sort of collaboration mentioned in detailed recommendations 7 and 8.

This is important to avoid possible incompatibilities between different implementations of the same specification as discussed in Section III. It is likely that vendors would welcome guidance on how to deal with open areas of the specifications, and early action by DOD could result in their mandated subset becoming the de facto standard for most commercial implementations as well, with consequent benefits to DOD. This is a good area for cooperation between DOD and NBS.

ADDITIONAL CONSIDERATIONS

Transition Plan

This section describes the major elements of a transition plan from use of TCP to use of TP-4 in DOD systems. The plan will vary depending on the option chosen. Both Option 1 and Option 2 share a number of common elements that are discussed first, including development of a MIL-SPEC, protocol-testing facilities, and transition support equipment. If Option 2 is followed, a demonstration of TP-4 must also be undertaken.

MIL-SPEC. As noted in recommendation 1, several open areas and options in the ISO TP-4 must be specified in order to have complete and compatible protocol implementations. Completion of this specification by the DOD should be a top priority objective.

Protocol-Testing Facilities. As noted in recommendation 3, test facilities for protocol implementations are essential. Under Option 1, this facility should serve primarily to validate implementations of both old and new protocol sets. If Option 2 is followed, the facility should initially focus on demonstrating the suitability of the new protocols for use in a military environment as rapidly as possible, and provide for testing of commercially supplied protocol implementations.

For validation purposes, the NBS protocol-testing facility developed for ISO protocols should serve as a good basis, but extensions to deal with any DOD-specific options for the ISO protocols, performance, and DOD protocols would be necessary. The DOD has stated that such a program has been started.

Transition Support Equipment. In any transition plan it must be assumed that the large body of systems with existing TCP implementations will take a substantial period of time to switch completely to the use of the ISO protocols. Some networks will include many different communities sharing a common communications backbone. Members of one community communicate primarily among themselves, but occasionally outside their community. While members of one community are likely to change over as a group, different communities will change to use the new protocols at different times.

Hence an interim period must be anticipated when some systems are using the old protocols and others, the new protocols. The transition plan must provide some means of allowing interaction between old and new systems where required during this period. Toward this end, a number of relay hosts may need to be developed that support both old and new protocols. These will allow automatic-staged forwarding of electronic mail between old and new systems and manually set up file transfer or remote terminal access via the relays. Performance through these relays will not be as good as with direct connections, but the relays should provide an adequate level of service for occasional interactions among different communities of the internet system.

When more frequent interaction is anticipated and better service is needed, major service hosts should support both old and new protocol sets concurrently so they can provide service directly without requiring the use of relays. Such service hosts include widely used time-sharing machines, file servers, and special servers such as Network Information Centers, Network Operations Centers, and Administrator Machines (providing mailboxes of network administrators, for example). Some dual protocol servers
may also act as relays where the load of both functions can be supported.

Terminal concentrators for general use must also support both protocol sets so that connections to both old and new hosts can be made directly.

Gateways must support both old and new IPs so hosts using either one may send internet traffic. This requirement could be relaxed in the case of entire networks that will switch over simultaneously and hence will only need one type of IP traffic. Gateways should not have to translate between old and new IPs--it will be assumed that both source and destination hosts are using the same protocols or going through an explicit relay intermediate host.

This latter point requires some elaboration. If one type of IP packet arrives at a destination host or gateway that only handles the other type, it must be discarded. It would be good if, in addition, a suitable ICMP error packet could be returned in the unsupported protocol so it would be meaningful to the source. To avoid this situation the internet-host name table maintained by the Network Information Center should indicate which protocol(s) each host supports. Then when a source host looks up the address of a destination, it will also determine which type protocol to use or if a relay is required.

Demonstration Plan

If Option 2 is followed, a major demonstration of the ISO protocols in a military environment must be undertaken. Any such demonstration should proceed by stages beginning with the implementation of TP-4 in one network (15). Then the demonstration would be extended to include internetting (still with DOD IP) to validate the suitability of TP-4 as a replacement for TCP. The demonstration would then be further extended to employ the ISO IP in place of DOD IP.

Stand-Alone TP-4 Network Demonstration. The first stage of any transition plan must be to establish a demonstration network or subnetwork using TP-4 in place of TCP under existing higher-level protocols. This step will require selection of a suitable network (or subnetwork), procurement of TP-4 implementations for hosts and terminal access controllers on that network, and modification of higher-level protocols to use TP-4. The demonstration should include sufficient use of real applications to test the protocols in an operational environment.

To limit the amount of change attempted at one time, the DOD IP may be retained and used under TP-4. Alternatively, if ISO IP development status seems to warrant it, ISO IP may be installed along with TP-4.

---

(15) For the remainder of this chapter, the use of TCP and TP-4 to include their respective IPs will no longer hold. The four entities--Transmission Control Protocol (TCP) and its Internet Protocol (DOD IP) and the Transport Protocol (TP-4) and its Internetwork Protocol (ISO IP)--will be treated individually.

In the latter case, all TP-4 hosts would be on the same network anyway, so that IP will only be used between hosts and no gateways will be involved and no gateway modifications will be needed.

The hosts involved could be dedicated to the demonstration and hence only support TP-4 and only be able to interact with other demonstration network hosts or be concurrently supporting TCP and DOD IP for operational traffic to other "normal" hosts. In the latter case, no forwarding or relaying of traffic by hosts between normal and ISO logical networks would be allowed or performed (the demonstration network would be logically closed).

Stand-Alone TP-4 Internet Demonstration. The next step would be to expand the demonstration to include more than one network (at least logically) and hence involve gateways. If only TP-4 is involved, this is a simple extension to test TP-4 over longer internet paths with more variable performance. If ISO IP is also being tested at the same time, modification of the gateways involved will also be required as indicated in the next section.

Stand-Alone ISO IP Demonstration. Once TP-4 has been tested, introduction of the ISO IP to replace DOD IP may commence. In addition to simply replacing one IP with the other in hosts and gateways, this will require modification of the gateways to perform ICMP and GGP on top of the ISO IP.

These gateways could either be dedicated to the demonstration and hence have only ISO IP, or could be concurrently supporting normal operational traffic via DOD IP. In the latter case, once again, no forwarding of traffic between ISO demonstration internet and normal systems would be allowed.

At the conclusion of these three steps, the ISO TP-4 and IP could be deemed to have demonstrated their basic functional suitability in a military environment. The transition support equipment described above should have been developed in parallel, providing the capability to smoothly and successfully switch operational systems using the old protocols to use of the new protocols.

Switchover of User Systems

Once the above preparations have been made and the demonstration completed, if Option 2 is being followed, the switchover of user systems can commence. Each network or community within a network should be able to switch at its convenience and maintain the ability to interact with other systems. The user systems will not be required to support operational use of both protocol sets simultaneously at any time unless they wish to do so for their own reliability purposes.

Switchover of user systems also requires a personnel-training effort. While earlier steps involved a relatively small number of specialists and support staff at major sites, this step will affect all user sites, and their network support staff must be trained in the new procedures.

Once switchover of all systems to the new protocol set is complete, support for the old protocols by TACS, service hosts, and gateways can be removed.

Lessons Learned from the ARPANET NCP-to-TCP Transition

The following points summarize some important lessons learned during the ARPANET transition from NCP to TCP (16).

Conversion of TACs and service hosts to support both protocols before the transition of user hosts starts is essential.

Relay capabilities were heavily used for mail, but used little for other purposes.

The Network Information Center was not ready to support the new protocols and this caused problems in distributing the host name table.

There were significant performance problems that required careful analysis and parameter tuning after the transition. These were unavoidable because no service host had been stressed prior to the switchover, with a full user load over a long time period using the new protocols.

---

(16) For additional information, see ARPANET Request for Comments: NCP/TCP Transition Plan, J. Postel, (Menlo Park, California: SRI International Telecommunications Sciences Center, November 1981).