The DoD Internet Architecture Model

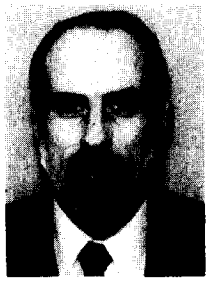
Vinton G. Cerf
Director, Systems Development, MCI Telecommunications, 1133 19th Street N.W., Washington, DC 20036, USA

and

Edward Cain
Defense Communications Engineering Center, 1860 Wiehle Ave., Reston, VA 22090, USA

This paper outlines the principles on which the U.S. Department of Defense packet internet architecture is based and characterizes some of the protocols which implement the architecture. Major factors which influenced the development of this architectural model include experimental and operational experience with a large number of interconnected packet networks, assessments and evaluations of military requirements for national and international interoperability and multiple jurisdiction operation, and specific concerns regarding security, survivability and operation under crisis conditions.

Keywords: DoD, Internet, Protocol, Military Requirements, Interoperability, Security, Survivability, Crisis conditions, Packet Communications, Protocol Architectures, Standards.



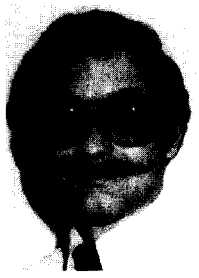
Dr. Vinton G. Cerf is presently Director of Systems Development, MCI Telecommunications, Inc. From 1976 to 1982, Dr. Cerf was Program Manager and Principal Scientist at the Defense Advanced Research Projects Agency. During this period he was responsible for technical oversight of research programs in packet switching technology. He has made innovative contributions in the technologies of internetworking and packet switching protocol development. Earlier in his career, Dr. Cerf was an assistant professor at Stanford University, held a position on the Staff of the Computer Science Department at UCLA, and did consulting work in networking. Dr. Cerf has published many papers and has chaired numerous technical sessions in his field. His memberships include ACM, Sigma Xi, IEEE and IFIP.

1. Introduction

The DoD Internet Architecture Model, referred to in the remainder of this paper as the Internet Model, has evolved over a period of seven or eight years, in concert with increasing DoD experience with packet switched computer communications technology. The model has its roots in work sponsored by the Defense Advanced Research Projects Agency in the late 1960's which led to the development and deployment of the ARPANET [1,2]. This initial packet network technology development was soon followed by a number of others involving a variety of transmission media, such as mobile packet radio [4,5], packet satellite [6,10], local area networks [11,12], and an increasing number of private and public data networks. Historical views of the development of many of these packet communications systems can be found in [13–15].

Networking architectures revolve around the protocols which are used to control the transport of data among the systems which must communicate with one another. The services available from various networks which are considered to be part of the overall system play an important role in determining the kinds of protocols which are needed, as do the types of services which are to be supported. The actual implementation of the protocols, their placement in "boxes" and the nature of the operating systems all contribute intimately to the design of the protocol architecture and its ultimate performance.

Among the fundamental assumptions which have influenced the organization of the Internet



Ed Cain is the Chairman of the Protocol Standards Technical Panel, a DoD-wide forum for debate on the technical aspects of DoD standards for host-to-host and higher level protocols. His work at the Defense Communications Engineering Center includes the testing of protocols for performance and functional correctness, and the design of packet switching networks for secure, robust data communications for tactical and strategic military applications. He holds a BEE degree from Georgia Tech, and has done graduate work at VPI&SU.

North-Holland
Computer Networks 7 (1983) 307–318

Model, perhaps the most basic is that it is both feasible and useful to segregate the various functions which must be performed to achieve the set of services desired into separate components which ultimately take the form of layers of protocols. The notion of protocol layering is not new. It was an important organizational principle in the development of the ARPANET protocols [16–19] and has influenced the protocol models of various computer vendors such as Digital Equipment Corporation (DECNET) and International Business Machines (SNA), to name two, and also the models of the various national and international data communications standards-making bodies such as the CCITT and ISO [23].

It is perhaps a subtle point, but an important one, that the concept of protocol layering should lead to the notion that a particular function or service may be viewed as achieved by means of a series of protocols, each depending upon the lower ones for service. It should not be concluded, however, either that only one protocol exists at each layer or even that the functionality of protocols in the same layer is necessarily the same or even similar. This is a controversial view, but it stems from the observation that protocols often are adjacent to one another in the same layer because they share the *same set of support protocols* and for no other reason that that. This views leads to a protocol model, illustrated in Fig. 1, in which the ensemble of protocols in the model form a dependency *hierarchy*. It should be noted that many protocols may occupy the same *layer* in the hierarchy.

Another point which seems important to make about layering is that there is often an implicit assumption that one can easily substitute one protocol for another in a particular layer without affecting the functionality of the protocols which depend on it. This assumption (or goal) is sometimes unwarranted, although it seemingly makes life easier for the protocol architecture designer. The problem lies in the nature of the functionality of the protocols in a particular layer and the nature of the services they can easily offer.

For example, broadcast service or multiaddress service [11,12,20,21] is more easily achieved by networks whose natural medium is broadcast in nature, such as the Ethernet or broadcast packet satellite. Substitution of the ARPANET or a public data network which provides an X.25 [22] interface, may fail to provide the service needed by higher level protocols which ASSUMED the existence of a broadcast or multicast feature in a lower *layer*.

This observation leads to the view that a particular model and especially the protocols fitting that model, may form a self-consistent *protocol suite* (to use Padlipsky's terminology [18]), but arbitrary substitution of a new protocol within the hierarchy may violate these implicit assumptions. This observation is not to say that no substitutions can

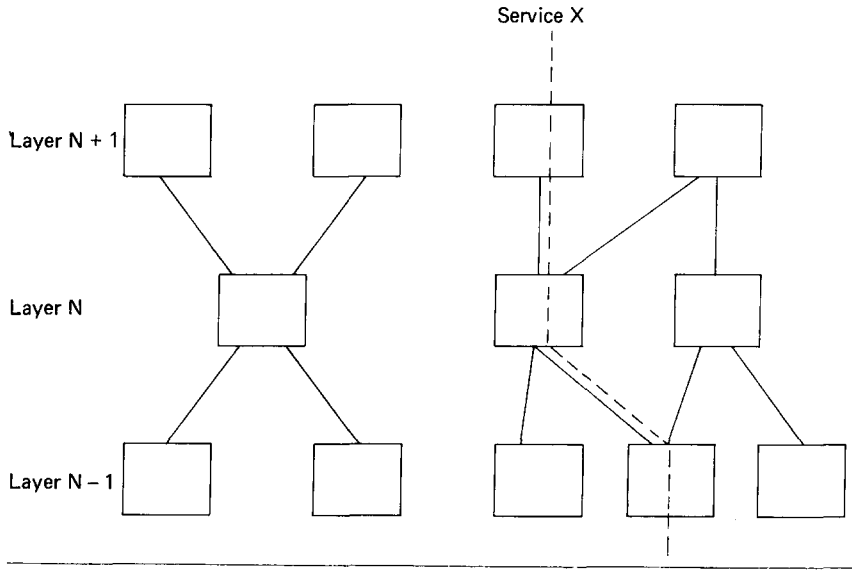


Fig. 1. Protocol Hierarchy Model.

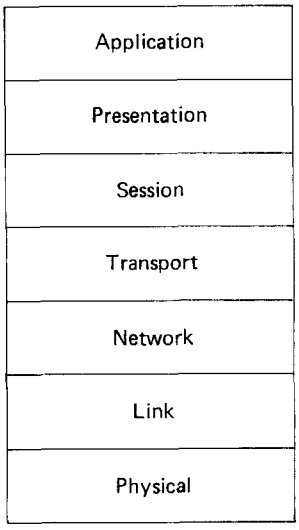


Fig. 2. ISO Open Systems Architecture.

work, but only that it is probably too much to assume that any layer N protocol (to use the ISO terminology) may replace any other layer N protocol without impact on layer N + 1 and above. Furthermore, it is the view of the authors that the goal of total interchangeability of layer N protocols is unnecessary. It is reasonable to expect that distinct types of service may be offered at a given layer in the hierarchy (e.g. transaction/connectionless and virtual circuit).

The most widely publicized protocol architecture is the ISO Open Systems Architecture or Open Systems Interconnection Model. Fig. 2 illustrates its structure, according to the current Draft International Standard [23]. The view portrayed in Figure 2 is, of course, overly simplified. For example, it does not reflect current study of connectionless modes of service, nor does it reflect the internal structure of the Network layer which has a "global network" sublayer under consideration [44]. Furthermore, consideration of network interfaces for local nets (e.g. Ethernet [11]) in addition to the CCITT recommendation X.25 [22] at the Network, Link and Physical layers is also underway.

One conclusion from the foregoing is that the ISO model is still undergoing development and is likely to incorporate new concepts, some of which are considered by the authors to be critically important for military applications.

The next section offers a summary of the DoD Internet Model along with some views on assumptions and requirements which are specific to military systems.

2. The Internet Model

The basic Internet Model is illustrated in two forms in Figs. 3 and 4. Figure 3 emphasizes the basic expectation that multiple networks of widely differing internal characteristics will be a natural and necessary part of military networking. This view has been expressed in many publications, some of which are listed in the Reference section of this paper [24–36]. This conclusion is a consequence of the fact that there are many different packet networking technologies [14], each of which can play a role in military systems. Local networks are well suited to intra-platform (vehicle, building,...) applications. Long-haul nets (e.g. ARPANET, SATNET, Defense Data Net,...) will be needed for wide-area communication. Packet radio or other mobile digital communication systems will be needed in tactical applications involving battlefield automation [33]. No single technology is ideal for all applications, yet the full collection of systems must interoperate.

The principal method for achieving interoperability in the DoD Internet Model is the use of a standard Gateway which can route internet traffic from one net to another and the use of a standard set of protocols operating above the internetwork layer (see Figure 4). Gateways are specifically intended to support the interconnection of heterogeneous packet nets [25-29,33,35,37,39]. This is in contrast to the existing CCITT view that all public packet nets will conform to the X.25 recommendation [22] and will utilize a common procedure, X.75, for exchange of packets between networks [38]. The principal difference between the CCITT/ISO view and the DoD view revolves around the question of network interfaces. The DoD view is that different packet nets may reasonably employ very different network interfaces (e.g. ARPANET vs. Ethernet) as a consequence of differences in service functionality while the CCITT/ISO view tends to assume more homogeneity. The introduction into the ISO model of a "global network" sublayer (Fig. 4) suggests, however, that this view is being reconsidered at least by ISO.

Fig. 4 also illustrates a difference between the ISO and DoD models at the higher layers, ISO

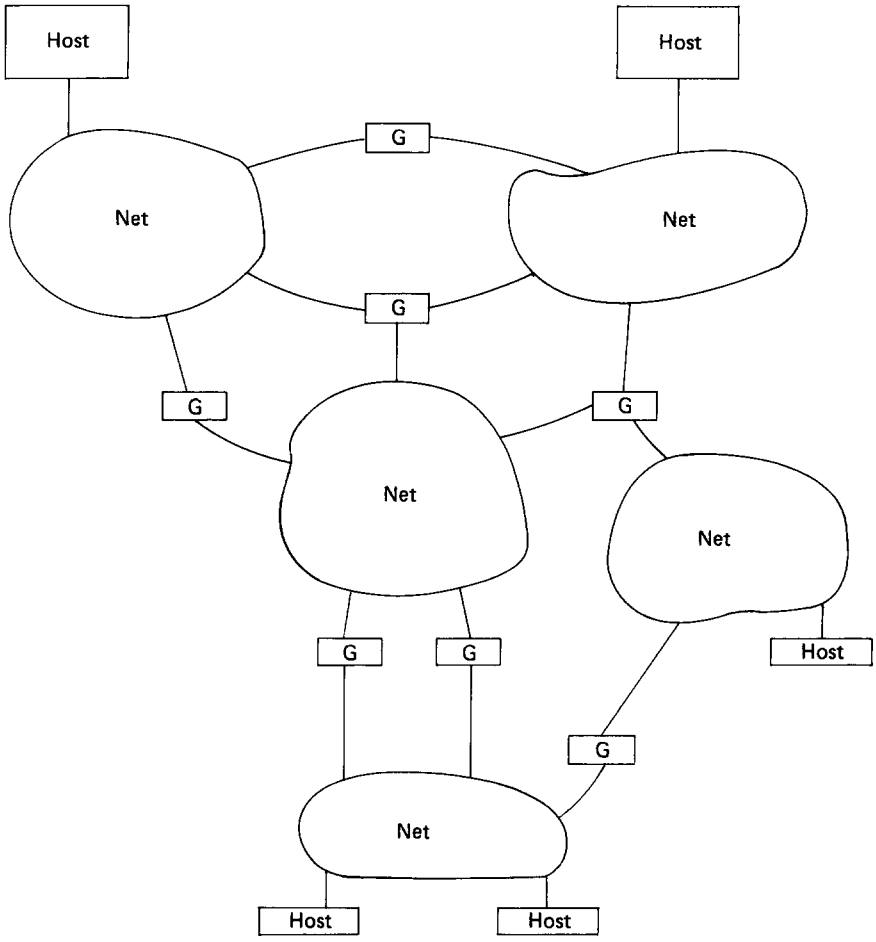


Fig. 3. Basic Internet-system Architecture.

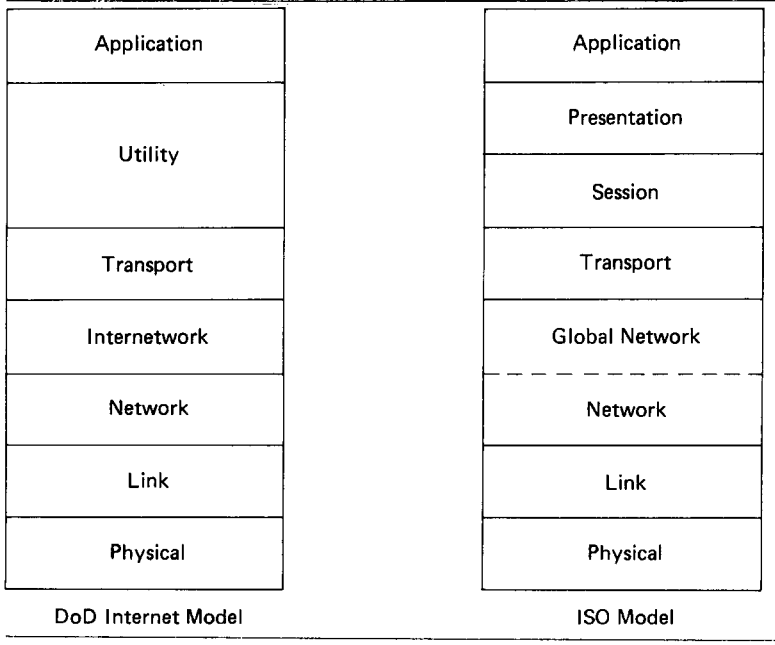


Fig. 4. DoD and ISO Protocol Architecture Model.

Table 1
Assumptions and Requirements Influencing DoD Internet Model

1. Heterogeneous Packet Networks (i.e. Physical, Link, Network Layers differ).
2. Datagram (connectionless) Service at Internet Layer.
3. Architectural Provision for Interoperable Tactical and Strategic Communication.
4. High Reliability and Survivability Under Hostile Conditions.
5. Combined Voice and Data Services.
6. Interactive, Real-Time, Transaction, and Bulk Data Transport Services.
7. Precedence and Security at Several Layers.
8. Broadcast/Multicast Services.
9. Host-Host File Transfers and File Access.
10. Widely Varying Terminal Types Using Remote Service Hosts.
11. Electronic Message Switching Services Utilizing Different Transport Protocols.
12. Multimedia (Text, Fax, Graphics, Voice) Electronic Messaging.
13. Distributed, redundant Name-to-Address Translation Services.

defines Session and Presentation layers as distinct. In the DoD model, protocols accomplishing these functions are combined into a single "utility" layer. This difference stems mostly from the experience DoD has had with specific protocols serving a variety of applications. The DoD protocols implemented thus far have not lended themselves to a single protocol for dealing with presentation issues (formats, conversions, etc.), nor has there yet been a specific need for many of the functions ascribed by ISO to the session layer. System Development Corporation, in its study of protocol architecture for DoD [28], did identify functions which might reasonably be incorporated into a general protocol above the transport layer but below the application layers and below the layer DoD uses to "house" its utility protocols. These functions related to the management of multiple transport protocol services (e.g. virtual circuit, real-time, transaction) on behalf of a single application, and multiple connections in support of multiparty, distributed applications, and multiple connections in support of multiparty, distributed applications. Although this remains an area for further study, it is possible that the DoD Internet Model will eventually include a layer between Utility and Transport.

Table 1 illustrates a list of basic assumptions, and requirements which have guided the development of the Internet Model and its associated protocols. In the next section, specific protocols which have been incorporated into the DoD Internet Protocol Hierarchy are discussed, in the context of the elements of Table 1.

3. The Internet Protocol Hierarchy

The relationship among the protocols which are in use by DoD, or are under development, are illustrated in Figure 5. Their functionality and relationship to requirements in Table 1 are discussed in the following sections. Documentation for most of these protocols may be found in references [40,41]; others are referenced explicitly.

3.1. Physical Layer

At this layer, a wide range of standard and unique interfaces are used to support the connection of hosts to their supporting networks. BBN 1822 [42] is the specification for a unique, 25-wire, bit serial asynchronous interface which permits a host or a packet switch to control the flow of data on a bit-by-bit basis. Typical data rates for this interface run between 100–400 kb/s.

Physical interfaces suitable for the support and use of modem connections between hosts and packet switches typically use CCITT V.24, V.35, or the more recent EIA RS-449 standards. MIL-STD-188C is a U.S. military standard which specifies signal levels somewhat different from EIA RS-232C.

Local network hardware interfaces range from designs which are specific to computer vendor bus standards (e.g. DEC UNIBUS or Q BUS) to standards such as the Xerox-Intel-DEC Ethernet and the plural IEEE 802 local network standard.

3.2. Link Layer

At this level, one finds unique standards such as the BBN "HDLC Distant Host" (HDH) and "Very Distant Host" (VDH) or the more widely used CCITT/ISO High Level Data Link Control (HDLC) procedure. The latter is also referred to as Advanced Data Communication Control Protocol (ADCCP) as standardized by the American National Standards Institute (ANSI). The IBM

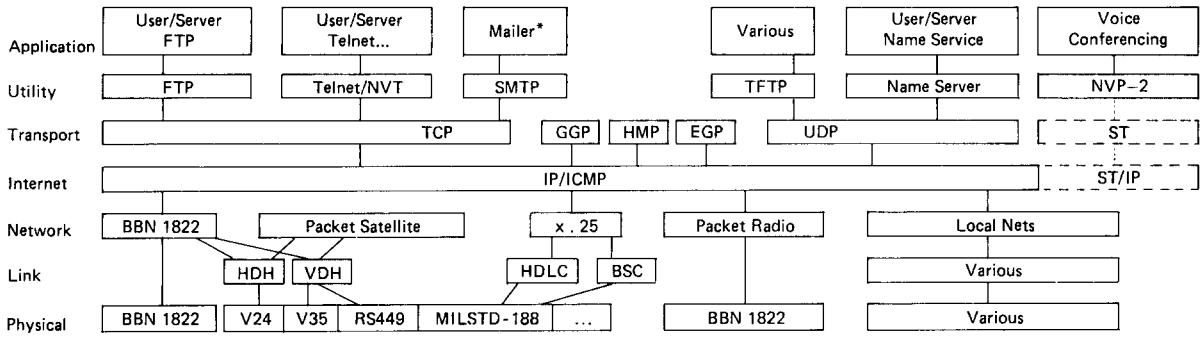


Fig. 5. DoD Internet Protocol Hierarchy.

binary synchronous link procedure (BSC) is also found, along with a HDLC as link level support for the CCITT X.25 recommendation.

Local networks may or may not provide a link level protocol interface, depending on vendor and network type.

3.3. Network Layer

For U.S. military nets such as the ARPANET, MINET, Defense Data Net (DDN), World Wide Military Command and Control System Intercomputer Net (WIN), Community Intelligence Network (COINS) and others based on the Bolt Beranek and Newman C/30 packet switch, BBN specification 1822 [42] spells out the specifics of the procedures for exchange of packets between hosts and the packet net. The DARPA packet satellite net (SATNET) [6–8], Navy Mobile Access Terminal Net (MATNET) [93], and DARPA/DCA Wideband Net (WBNET or EISN) all use a unique procedure for accessing stream, datagram and broadcast conferencing services supported by packet satellite technology.

The DARPA Packet Radio Net uses another unique interface for packet exchange, including special "type of service" indicators for support of real-time voice or normal interactive/bulk data transfer services.

Local networks such as Ethernet [Xerox, ACC Inc.], CHAOSNET (MIT), Ungermann-Bass Net/One, Proteon Pronet, Mitre's Mitrebus, MIT-Lincoln Laboratory LEXNET, BBN's Fibernet (optical), SRI International's SRINET, etc. all use various network level formats and procedures to support point-to-point, broadcast and multicast services.

3.4. Internet Layer

At this level, all network services are unified and viewed by hosts as an internet datagram service. Global internet addressing, internet routing and error handling are defined as part of the service. A special "type of service" field in each internet datagram can be used to select appropriate lower level network services.

The principal protocols at this level are the Internet Protocol (IP) and Internet Control Message Protocol (ICMP) which are used to coordinate host/internet interactions including routing advice from gateways to hosts (e.g. redirection of traffic to alternate gateways) and warning messages related to congestion or unrecoverable failures (e.g. destination host or network not reachable).

At this layer, gateways can compensate for variations in maximum packet size in each net by fragmenting internet datagrams to fit. The fragments can be routed independently and are assembled at the destination host, rather than at each intermediate gateway. This strategy minimizes delay through the system and makes it more feasible to support real-time services such as packetized speech, target tracking and fire control.

An experimental extension to the IP protocol, called "ST" for "stream" protocol has been implemented to support exploration of voice conferencing or mixed voice/data services in the context of multiple, interconnected packet nets.

3.5. Transport Level

There are three primary host support protocols at this level. These are the Transmission Control

Protocol (TCP), User Datagram Protocol (UDP) and ST Protocol. TCP is a highly reliable, end-to-end, sequenced byte stream protocol which uses retransmission and positive acknowledgment to assure data delivery. An end-to-end, window-based flow control strategy is used. This protocol provides "virtual circuit" service to higher level protocols and applications. It is external to the IP so that other protocols and applications can be supported which do not require this level of service.

The User Datagram Protocol (UDP) provides support for transaction-like protocols which do not require the same type of sequencing and controls as that provided by TCP.

The experimental ST protocol supports broadcast, multicast and conferencing services, particularly those which do not require guaranteed delivery of all data (e.g. packet voice, target tracks), but do have very stringent real-time requirements.

The remaining protocols at this level include the Gateway-Gateway Protocol (GGP), External Gateway Protocol (EGP) [45], and Host Monitoring Protocol (HMP). GGP is specifically designed for the support of gateway routing, status and congestion control information and forms the heart of the internetwork control system. The EGP is a variation of GGP which does not rely as heavily on tight coupling of the GGP protocol, especially to cater to local nets connected as "stubs" on an existing long-haul internet system. The long-haul system, for example, might use GGP (carefully tuned) to support EGP-based local net interconnection.

The Host Monitoring Protocol (HMP) is a protocol for general purpose monitoring of any internet host. This protocol provides a basis for central (and redundant) monitoring of host status (including gateways themselves). This information is essential for the isolation and repair of failures and detection of performance anomalies in a large internet system.

3.6. Utility Layer

At this layer, the protocols become much more application-specific. The File Transfer Protocol is used to identify, access and move files from one host to another. It has several modes of operation depending on file type and includes provision for transparent transfer ("image" mode) between hosts using identical operating systems.

TELNET is a protocol which allows serving hosts to treat all remote terminals as if they were standard "Network Virtual Terminals" (NVT). This protocol incorporates a basic model of a terminal as a scroll-mode, ASCII TTY, but also has provisions for complex negotiations of special features (e.g. local or remote echo, page mode, CRT width and length, etc.). The primary benefit of this protocol has been to simplify the software necessary in service hosts to isolate them from knowledge of specific features of remote terminals. In this sense, it is similar to the CCITT X.28/X.29 protocols which operate directly above CCITT X.25 service.

Simple Mail Transfer Protocol (SMTP) supports the transfer of electronic messages among arbitrary hosts in the internet. It has provision for acting in store-and-forward as well as end/end delivery mode, allowing distinct transport level protocols to be used to actually transport the electronic messages. It also supports batching of messages destined for the same destination or mail forwarder so that only a single message copy needs to be sent even though there are multiple recipients.

Trivial File Transport Protocol is a very simple, block-at-a-time transport procedure which is often used to support file and message transport to small personal computers or to systems just beginning to bring up the protocol set. Its advantage is simplicity, but is not a high bandwidth protocol owing to its single-block-at-a-time nature. On very low delay nets, it can achieve respectable transfer rates.

The Name Server Protocol supports the translation of string names for hosts and servers into their total internet addresses. This becomes a critical part of the system architecture as the size of the internet environment grows beyond the capacity of central name assignment and management to cope. It also allow hosts to move from one address to another, and to keep only currently-used name/address pairs in local storage rather than tables for all possible destination names and addresses.

NVP-2 is the Network Voice Protocol, version 2. It incorporates support for negotiating various types of voice compression to be used and to support the passing of the "floor" during a conference in a smooth and controlled manner. It includes the concept of a closed user group, multi-

casting (multiple-destination addressing) and dynamic joining and leaving of conference members. The protocol is able to accept and use (play back) packets received in error and is able to use time-stamp information as well as sequence numbering to determine whether a voice packet should be played out, retained for later output or discarded. NVP 2 relies on the special features of the ST and ST/IP protocols to support its unique requirements for low delay and multicasting.

3.7. Application level

At this level, we find actual programs which use the lower level protocols to accomplish specific applications such as electronic mail service, remote terminal access to service programs, etc.

4. Loose Ends

There are a number of issues and concepts which should be mentioned, including security concepts, front-ends, bit map displays, mobile hosts, network partition resolution, and a generic observation about the incompleteness of all protocol architectures developed to date (as far as the authors can determine).

4.1. Architectural Incompleteness

Aside from all the various developments, services and protocols which the authors cannot predict, and therefore have left out, there is one glaring omission in the Internet Model, which is also missing from the OSI model. Most of these models tend to describe the relationship of protocols as seen by host computers connecting to networks. What is missing from the architectural model is the hierarchy of protocols present within each packet network and within the internetwork system. Each of the various types of networks mentioned has very different internal operation. A complete model would include some representation of the various protocols (e.g. routing, flow and congestion control, monitoring) used to support network and internetwork operation. For simplicity they have been ignored in this paper, but it seems appropriate to acknowledge this fact.

4.2. Front-ends

The models as shown in Figs. 2, 4 and 5, although consistent with the concept, do not explicitly indicate where and how front-end systems can be incorporated into the architecture. The DoD Internet Model can be extended, as shown in Fig. 6 to accommodate one form of front-ending. Since the possibilities are endless, the example in Fig. 6 is taken for concreteness from actual DoD implementations. Note that the host has access both to the transport layer and internet layer protocols via the front-end protocol. This permits some flexibility in placing the transport layer protocols in the host or the front-end and also supports operation of such protocols as the Host Monitoring Protocol in the Host even though its support protocol (IP) is implemented in the front-end.

4.3. Network Partitioning

The internet system architecture contemplates the interconnection of many nets by means of gateways. It may happen, under hostile conditions, that one or more of the subnets may partition into a collection of disjoint pieces. It may still be the case, however, that full connectivity among all hosts may be achieved by judicious routing of traffic through the gateway system from one partition to another (see Fig. 7). The existing protocols for gateway operation must be extended to detect such partitioning and adjust the routing tables in the gateways (and hosts) to achieve recovery where this is possible. It is not a trivial problem.

4.4. Mobile Hosts

The addressing structure of the Internet Protocol assigns host addresses on a hierarchical (i.e. relative) basis, as a function of the network to which the host is attached. The TCP protocol depends upon the IP network and host addresses for part of its connection identifiers; the full identifiers include port numbers assigned by the TCP level and carried in its header. If a host were to move from one net to another (e.g. via an airborne packet radio), its network (and host) addresses would change and this would affect the connection identifiers used by the TCP to maintain state information. In effect, roving hosts require some means of dynamically re-defining TCP connection identifiers. This is rather like a problem called "dynamic reconnection" which has plagued net-

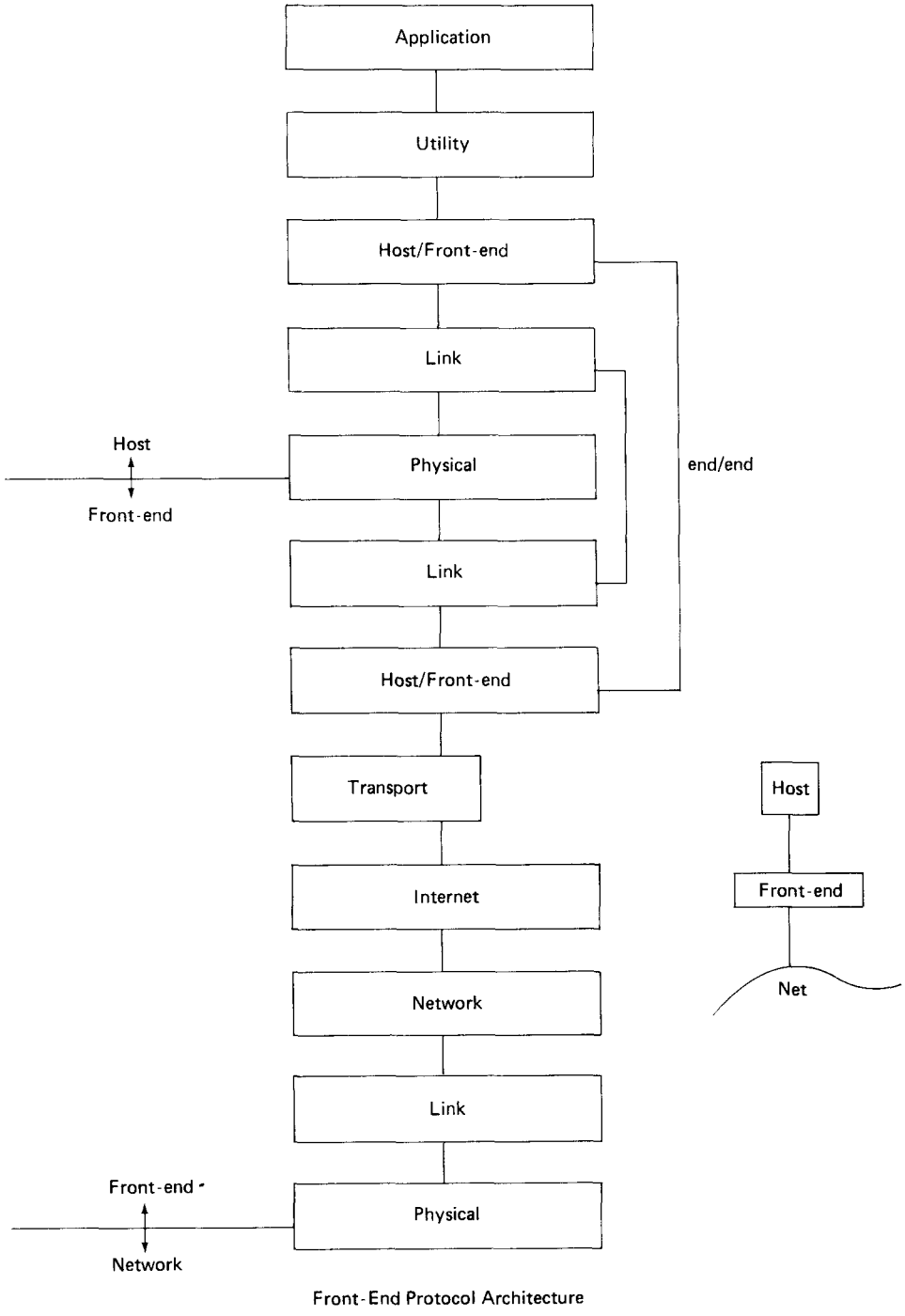


Fig. 6. Front-End Protocol Architecture.

work designers since the inception of the ARPANET project in 1968.

The crux of the problem lies in the use of the IP network and host addresses by the TCP level of protocol. The DoD Internet Model accommodates the re-binding of host names to internetwork addresses through the use of the distributed name server protocol, however use of this mechanism

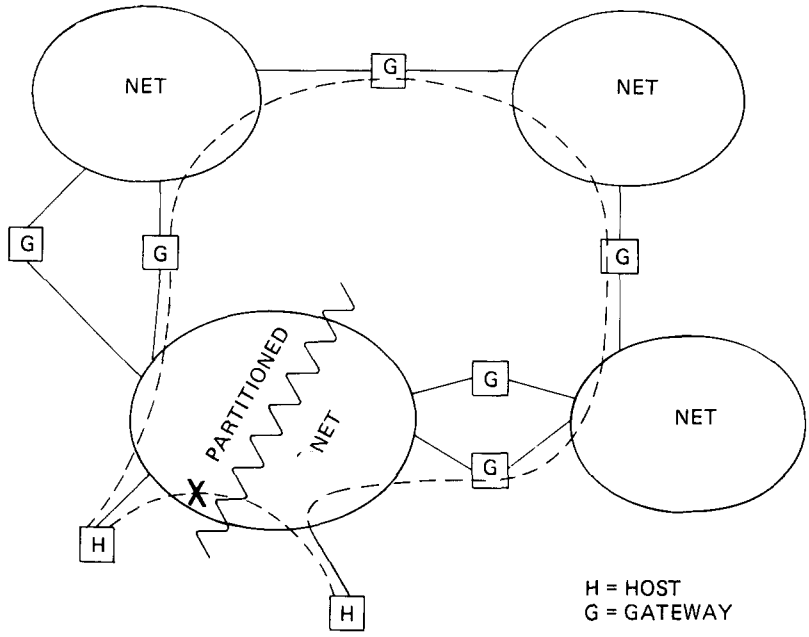


Fig. 7. Partitioned Net Recovery.

requires that the TCP connections be broken and re-established. One strategy for dealing with this problem is to create logical addresses for hosts at the TCP level which are bound to internet addresses at the IP level by means of name server mapping sorts of mechanisms. While this adds overhead to the TCP header, it creates an opportunity for dynamically re-binding the TCP level connection identifiers to the IP level addresses. Detailed consideration of this concept is beyond the scope of the paper.

Xerox Corporation's Network System protocols attempt to solve this problem by assigning each host a unique 48 bit identifier [43]. The binding of host name and identifier need never change. However, it is still necessary to find out to which net the host is now connected. The Xerox architecture provides a 16 bit "hint" to help the Xerox gateways route packets to the right destination net. The question of keeping track of the "hint" leads back to name server concepts, such as those currently incorporated in the DoD Internet Model.

4.5. Bit-Map Displays

With the increasing availability of higher resolution, bit-map displays, many of the issues in Network Virtual Terminal and message/file format became substantially more complex. Multiple font representations are needed, as well as treatment of variable size and placement of "windows" through which different applications outputs can be viewed by a user. The DoD Network Virtual Terminal Protocol does not address this important area and will have to do so soon simply because there are already in use thousands of personal computers and fancy bit-map displays in military applications. For example, there are approximately 30 Three-Rivers PERQ personal computers aboard the U.S. CVN Carl Vinson, an operational vessel in the fleet.

4.6. Security

Finally, it is essential that the DoD Internet Model incorporate a provision for the latest concepts in end-to-end and multilevel security. The model has been modified to take this into account so that end/end security methods, such as the one illustrated in Figure 8 can be supported.

Classification restrictions prevent a full discussion of this topic in an unclassified paper. Figure 8 shows that the type of security which can be supported includes the insertion of devices between hosts and networks (rather like front-ends) so that cryptographic measures may be taken to

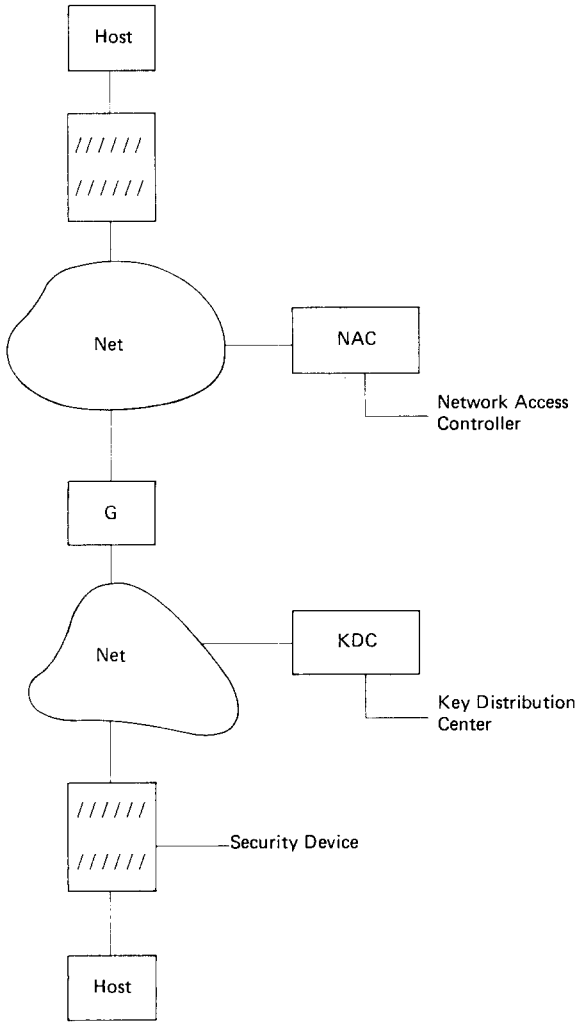


Fig. 8. End/End Network Recovery.

secure the communication between source and destination hosts. Automatic, electronic re-keying, using a key distribution center (KDC) which distributes keys according to policy set by a network access controller (NAC) is a part of the architecture. Of course, conventional link level encryption within each net can be supported simultaneously.

4.7. Growth

Just as conventional packet networks reach limits to the ability of network routing, flow and congestion control algorithms to work satisfactorily beyond certain network sizes, the internet system has potential limits to the satisfactory functioning of its gateway routing, flow and congestion control algorithms. Concepts such as area routing are typically introduced to increase the dynamic range of network control, at the cost of reduced optimality in the performance of the control algorithms. Introduction of EGP into the DoD internet system represents a first step along the path towards a solution to managing a large-scale internet system.

4.8. Summary

This paper has addressed the organization of the DoD Internet Model and compared it to the ISO open systems Interconnection Model. A review of the actual protocols which populate the DoD Internet Protocol Hierarchy was provided and the paper concluded with a discussion of several areas requiring further attention.

It is opinion of the authors that the DoD Internet Model is the most fully developed, military-oriented networking architecture in existence. It is based on over 10 years of field experience with the most advanced packet switching systems in the world. We do not believe, however that the model can remain static. The many loose ends are proof that the model and its protocols must evolve. It is our hope that this evolution can be accomplished in cooperation with our NATO allies and generally within the framework of the national and international protocol standardization initiatives now underway.

References

[1] L.G. Roberts, and B.D. Wessler, "Computer Network Development to Achieve Resource Sharing," proc. AFIPS SJCC, V.36 543-549, 1970.

[2] F.E. Heart, RE "The Interface Message Processor for the ARPA Computer Network," proc. AFIPS SJCC V.36, pp. 551–567, 1970.

[3] R.E. Kahn, "Resource-Sharing Communication Networks," proc. IEEE, V.60(11), pp. 1347–1407, November 1972.

[5] R.E. Kahn, "The Organization of Computer Resources into a Packet Radio Network," IEEE Trans. Commun., Vol. COM-25(1), January 1977.

[6] R.E. Kahn, "The Introduction of Packet Satellite Communications," National Telecommunications Conference, November 1979, pp. 45.1.1–45.1.8.

[7] I.M. Jacobs, et al., "General Purpose Satellite Networks," proc. IEEE, Vol. 66 (11), November 1978, pp. 1448–1467.

[8] I.M. Jacobs, et al., "Packet Satellite Network Design Issues," proc. Nat'l Telecommunications Conf., November 1979.

[9] L.N. Evenchik, D.A. McNeill, et al., "MATNET, An Experimental Navy Shipboard Satellite Communications Network," proc. INFOCOM 82, March 1982, p. 2–11.

[10] L. Palmer, et al, "SATNET Packet Data Transmissions," COMSAT Technical Review, vol. 12(1), Spring 1982, pp. 181–212.

[11] R.M. Metcalfe and D.R. Boggs, "Ethernet: Distributed Packet Switching for Local Computer Networks," Comm. ACM, Vol. 19(7), July 1976, pp. 395–404.

[12] D. Clark, K. Pogran and D. Reed, "An Introduction to Local Area Networks," IEEE proc. Vol. 66 (11), November 1978, pp. 1497–1517.

[13] L.G. Roberts, "The Evolution of Packet Switching", proc. IEEE, V.66(11), November 1978, p. 1307.

[14] V.G. Cerf, "Packet Communication Technology," Protocols and Techniques for Data Communication Networks (F. Kuo, ed.), Prentice Hall, New York, 1980, Chapter I.

[15] Defense Advanced Research Projects Agency, "A History of the ARPANET: The First Decade," prepared by Bolt Beranek and Newman, April 1981 (Defense Tech. Info. Center AD A1 15440).

[16] S. Carr, S. Crocker and V. Cerf, "HOST-HOST Communication Protocol in the ARPA Network," proc. AFIPS Spring Joint Computer Conference, V. 36, 1970.

[17] S.D. Crocker, J.F. Heafner, R.M. Metcalfe and J.B. Postel, "Function-oriented Protocols for the ARPA Computer Network," proc. AFIPS SJCC Vol. 90, pp. 271–279, 1972.

[18] M. Padlipsky, "A Perspective on the ARPANET Reference Model," proc. INFOCOM 83, April 1983.

[19] ARPANET Protocols Handbook, (Feinler, E. and Postel, J., Editors) Network Information Center, SRI International, NIC 7104.

[20] Y.K. Dalal, "Broadcast Protocols in Packet Switched Computer Networks," Ph. D. Thesis, Stanford Univ., CSL Technical Report 28, 1977.

[21] Carl Sunshine, "Addressing Problems in Packet Network Interconnection," proc. INFOCOM 82, Las Vegas, IEEE Press, March 1982, pp. 12–18.

[22] "Recommendation X.25/Interface Between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks," in CCITT Orange Book, Vol. 7, Int. Telephony and Telegraphy Consultative Committee, Geneva, Switzerland, 1980.

[23] International Organization for Standardization, "Reference Model of Open Systems Interconnection," ISO/TC97/SC16, Draft International Standard ISO/DIS/7498, 1982.

[24] J.F. Shoch, D. Cohen and E. Taft, "Mutual Encapsulation of Internetwork Protocols," Computer Networks, May 1981, pp. 287–300.

[25] V. Cerf, "The CATENET Model for Internetworking," Internet Experiment Note No. 48, available from SRI International, Network Information Center, Menlo Park, California.

[26] V. Cerf, and P.T. Kirstein, "Issues in Packet Network Interconnection," IEEE, V. 66(11), November 1978, pp. 1386–1408.

[27] J.B. Postel, "Internetwork Protocol Approaches," IEEE Trans. or Communications, Vol. COM-28, No. 4, April 1980, pp. 604–611.

[28] System Development Corporation, "DoD Protocol Reference Model," (Draft), TM-7172/201/00, February 1982.

[29] C. Sunshine, "Interconnection of Computer Networks," Computer Networks, 1977, pp. 175–195.

[30] Y.K. Dalal, "Use of Multiple Networks in Xerox' Network System," proc. 24th IEEE Computer Society International Conference (COMPCON), February 1982.

[31] V. Cerf, and R.E. Lyons, "Military Requirements for Packet-Switched Networks and Their Implications for Protocol Standardization," Proceedings of EASCON Conference, 1982.

[32] B.H. Davies and A.S. Bates, "Internetworking in the Military Environment," Proc. INFOCOM 82, IEEE Press, 1982, pp. 19–29.

[33] Tactical Information Exchange (TIE) Working Group, "Tactical Information Exchange (TIE) Framework Development," edited by R&D Associates, RDA-TR-117100-001, October 1981.

[34] Lavean E. Gilbert and Ronald E. Sonderegger, "A Communication System Architecture for Interoperable Systems," International Telemetering Conference," San Diego, CA, 28–30 September 1982.

[35] J. Postel, C. Sunshine and D. Cohen, "Recent Developments in the DARPA Internet Program," Proceedings of ICCC, London 1982.

[36] J. Shoch, "Internetwork Naming, Addressing and Routing," COMPCON Fall 1978 Proceedings, September 1978.

[37] V.G. Cerf and R.E. Kahn, "A Protocol for Packet Network Intercommunication," IEEE Trans. on Communications, Vol. COM-22, No. 5, May 1974.

[38] "Proposal for Provisional Recommendation X.25 on International Interworking Between Packet Switched Data Networks," in CCITT Study Group VII Contribution No. 207, Int'l Telephony and Telegraphy Consultative Committee, Geneva, Switzerland, May 1978.

[39] A. Sheltzer, R. Hinden and M. Brescia, "Connecting Different Types of networks With Gateways," Data Communications, Vol. 12, No. 8, August 1982, pp. 111–122.

[40] Internet Protocols Transition Workbook (J. Postel and E. Feinler, Eds.), SRI International, Network Information Center, Menlo Park CA, 1982.

[41] Internet Protocols Implementor's Guide (J. Postel and E. Feinler, Eds.), SRI International, Network Information Center, Menlo Park, CA, 1982.

[42] Bolt Beranek and Newman, "Specification for the Interconnection of a Host and an IMP," Report No. 1822, 1982 Revision.

[43] Y.K. Dalal and R.S. Printis, "48-Bit Absolute Internet and Ethernet Host Numbers," Seventh Data Communications Symposium, October 1981.

[44] B.M. Wood, "Open Systems Interconnection – Basic Concepts and Current Status," proc. ICCC 82, London, September 1982, pp. 775–780.

[45] E. Rosen, "Exterior Gateway Protocol (EGP)", RFC 827, Bolt Beranek and Newman Inc., Cambridge, MA, October 1982.