An Overview of SAFENET and its Implications for Aerospace Applications

George C. Collins
Rodney L. Bown

University of Houston-Clear Lake

February, 1991

Cooperative Agreement NCC 9-16
Research Activity No. SE.26

NASA Johnson Space Center
Engineering Directorate
Flight Data Systems Division

ricis

Research Institute for Computing and Information Systems
University of Houston - Clear Lake

TECHNICAL REPORT

The RICIS Concept

The University of Houston-Clear Lake established the Research Institute for Computing and Information systems in 1986 to encourage NASA Johnson Space Center and local industry to actively support research in the computing and information sciences. As part of this endeavor, UH-Clear Lake proposed a partnership with JSC to jointly define and manage an integrated program of research in advanced data processing technology needed for JSC's main missions, including administrative, engineering and science responsibilities. JSC agreed and entered into a three-year cooperative agreement with UH-Clear Lake beginning in May, 1986, to jointly plan and execute such research through RICIS. Additionally, under Cooperative Agreement NCC 9-16, computing and educational facilities are shared by the two institutions to conduct the research.

The mission of RICIS is to conduct, coordinate and disseminate research on computing and information systems among researchers, sponsors and users from UH-Clear Lake, NASA/JSC, and other research organizations. Within UH-Clear Lake, the mission is being implemented through interdisciplinary involvement of faculty and students from each of the four schools: Business, Education, Human Sciences and Humanities, and Natural and Applied Sciences.

Other research organizations are involved via the "gateway" concept. UH-Clear Lake establishes relationships with other universities and research organizations, having common research interests, to provide additional sources of expertise to conduct needed research.

A major role of RICIS is to find the best match of sponsors, researchers and research objectives to advance knowledge in the computing and information sciences. Working jointly with NASA/JSC, RICIS advises on research needs, recommends principals for conducting the research, provides technical and administrative support to coordinate the research, and integrates technical results into the cooperative goals of UH-Clear Lake and NASA/JSC.

An Overview of SAFENET and its Implications for Aerospace Applications

George C. Collins
Rodney L. Bown

University of Houston-Clear Lake

February, 1991

Cooperative Agreement NCC 9-16
Research Activity No. SE.26

NASA Johnson Space Center
Engineering Directorate
Flight Data Systems Division

Research Institute for Computing and Information Systems
University of Houston - Clear Lake

TECHNICAL REPORT

Preface

This research was conducted under auspices of the Research Institute for Computing and Information Systems by Dr. George C. Collins and Dr. Rodney L. Bown, Associate Professors of Computer Systems Design at the University of Houston-Clear Lake. Dr. Bown also served as RICIS research coordinator.

Funding has been provided by Engineering Directorate, NASA/JSC through Cooperative Agreement NCC 9-16 between NASA Johnson Space Center and the University of Houston-Clear Lake. The NASA technical monitor for this activity was William C. Young, of the Project Integration Office, Flight Data Systems Division, Engineering Directorate, NASA/JSC.

The views and conclusions contained in this report are those of the authors and should not be interpreted as representative of the official policies, either express or implied, of NASA or the United States Government.

An Overview of SAFENET and its Implications for Aerospace Applications

by G. Collins and R. Bown

I. INTRODUCTION

Recently the Navy has developed a draft version of a standard for local area networking that when adopted will become a military standard. This standard is being developed for procurement specifications of computer resources to be used on ships and aircraft and has some of the same real-time concerns that network standards for space vehicles have. This draft standard is Draft SAFENET I Military Standard (MCCR-0032-DRAFT) and is to be used with Draft SAFENET I Military Handbook (MCCR- 0034) copies of which are attached to this report. An executive summary is also attached, which gives an easy to read overview. This report will introduce the basic concepts of Safenet and compare it to other standards. A review of security issues in the SAFENET Handbook and a discussion of recent LAN security developments will also be included.

II. AN OVERVIEW OF COMMUNICATIONS STANDARDS

A. ISO Communication Standards

As the computer industry evolved, many techniques for data communications and networking were developed by the various vendors of computer equipment, both in the US and overseas. In 1977 the International Standards Organization (ISO) started a project to define a standard architecture for computer communications. Their work was submitted in 1979 and is known as the OSI Reference Model, or the ISO Model of Architecture for Open Systems Interconnection (ZIMM80). This standard has been adopted and is found as ISO 7498 (see Table I.)

The basic model has 7 layers of communication services in which communication protocols were to reside. The lowest layer (the Physical Layer) produced the raw data stream that was to propagate along the communications media. The second layer (Data Link Layer) provides services that allow the link to be a reliable communication channel; these services include error detection and correction. Layer three is the Network Layer that has protocols related to routing packets through a network, and its interface was conceptually related to the interface into public data networks. Hence layers 1-3 were originally conceived as "network protocols" while the layers above were often termed "host protocols". An example of this separation is the CCITT standard known as X.25 (see Table I).

The fourth layer (Transport Layer) is often known as the "end-to-end" layer, since its responsibilities to some degree are to recover from problems with an unreliable network. It is generally assumed that layer four provides the end-to-end integrity of the data, making sure that all detected errors have been corrected, lost and duplicated packets have been taken care of, and that the message (which was broken up into packets for transmission over the network) has been put back together in the correct sequence. From the host's point of view, the transport layer is the communications provider.

Layers five through seven (the Session, Presentation, and Application Layers) provide dialogue management, data representation, and various other application services that would be of common interest for various processes running in the host. At the time that the reference model was being developed, these layers were not well defined, but the committee felt that under their set of rules for defining layers, there were good enough arguments to separate session and presentation type protocols from others that would reside in the Application layer.

The impact of this model cannot be ignored. All present protocol standards have been influenced by this work, since the idea was that specific protocols would be developed at each layer and that the interfaces would be standardized allowing "stacks" of protocols to be implemented for specific applications. This influence will be seen in the SAFENET I Draft Standard. Security issues at the time were not an important consideration of the committee, and it is interesting to note that because of the layering model, it has become an interesting problem deciding were exactly in the model security protocols can be placed. A second issue is the real concern that the layering makes a very real problem for real-time communications, since each layer produces some delay as the "protocol data units" are queued and processed in each layer. The SAFENET I Draft has an interesting way of dealing with this problem.

B. Local Network Standards

Work on the OSI reference model and its protocols continued to develop, and the IEEE sponsored committee began to work on local networking standards for the lower levels of the model. This led to the IEEE 802 set of standards that is continuing to be developed [IEEEa-d]. The significance of this work was that it allowed the semiconductor industry to implement chip sets to implement these protocols and interfaces, and therefore the overall implementation cost of an OSI stack should be reduced and the performance (in terms of speed) could be enhanced over software implementations.

Two other groups were working in parallel to the IEEE 802 committee that have made a contribution to the standards related to SAFENET I. In 1982 the manufacturing industry began to work on a complete protocol stack for local area networking, which was eventually handed over to the Society of Manufacturing Engineers. This became the Manufacturing Automation Protocol whose stack (or profile) is shown in Table 2 [BLACK89].

The second group, from the American National Standards Institute, began working on high speed local network standards with data rates from 50-100 Mbps. These rates are much higher than the 1-10 Mbps data rates in the IEEE 802 standards. The most recent work by this ANSI committee [X3T9.5] is the Fiber Distributed Data Interface or FDDI standard, which uses a fiber optics medium and has a data rate of 100 Mbps.

C. Implementation of Layer 3 and 4 Protocols in Hardware

There is also an effort underway to implement transfer services (combination of layers 3 and 4) that will be very efficient [XTP88]. This implementation is called the Xpress Transfer Protocol (XTP) and is presently under development. It is expected that a silicon implementation will eventually be available, providing benefits similar to those of the IEEE 802 standards.

D. GOSIP

In summary, since its conception, the OSI model has become widely discussed as a means of implementing "open" networks. As of August 15 of this year, the United States Government will be requiring new systems to follow OSI interoperability as specified by the Government OSI Profile [DERN90], unless exempted. This will have an impact on all agencies of the Federal Government including the Navy and of course NASA.

III. THE SURVIVABLE, ADAPTABLE FIBER OPTIC EMBEDDABLE NETWORK DOCUMENTS

A. The SAFENET I Executive Summary

The background behind SAFENET I is discussed in the SAFENET I Executive Summary. It describes how the Next Generation Computer Resource (NGCR) program was established in 1988 to provide standardization for mission critical computer resources (MCCR). Navy and industry representatives have been working together to develop an open systems architecture to provide a basis for multiple vendor support of Navy Local Area Networking (LAN) requirements. (This is not unlike the goals of NASA and the aerospace industries.)

The summary gives the basic overview of the standard's progress, discussing the basic OSI profile, the standardization milestones, and some implementation notes. SAFENET I should be finished in September 1991 and SAFENET II by September 1992. SAFENET refers to the general profile, while the basic difference between SAFENET I and II is that SAFENET I is based on IEEE 802.5 and SAFENET II will require FDDI in the lower layers.

B. SAFENET I Military Standard

The formal draft military standard for SAFENET I is the second attached document. It describes the scope, related documents, definitions, general and detailed requirements. It is brief and often uses the phrase that a particular item is "completely described in MIL-HDBK-0034", the companion handbook for the standard. Also direct references are made to other mil-standards related to electronic requirements, specification practices, and engineering concerns.

C. SAFENET I Military Handbook

This document provides over 133 pages of details on SAFENET I. It includes the scope, related documents, and definitions. It then continues with an overview of SAFENET I, its architecture, and the requirements for the application interface, the communication protocols, the physical medium, network management, and time synchronization. It concludes with a number of appendices including the selection of the SAFENET protocol suites, user services, the NATO Network Independent Interface, the transfer services, IEEE802.5 dual ring reconfiguration, optical power budget, and last but not least, the SAFENET security policy. The next sections cover a brief overview of what I consider the interesting aspects of the handbook.

IV. THE ARCHITECTURE AND "SURVIVABILITY"

A. The Physical Topology

It is important to note that the "S" in SAFENET is "survivability" and not "safety." To provide this characteristic in the local network a dual ring topology is required. Figures 1 and 5 from the handbook illustrate the physical topology used (See Appendix A.) There are two basic aspects that are important to note. First of all there is a duplicate ring (and others are possible). The token-ring LAN must implement the IEEE 802.5 recommended practice for dual ring reconfiguration, which is currently being reviewed for inclusion into the IEEE standard. Discussion of the reconfiguration process is included in Appendix E of the handbook.

The second structure that improves the survivability of the network is that each station is required to be attached to the ring by way of a trunk coupling unit (TCU). The TCU is used to isolate a station from the ring in the case of a failure. Up to five stations on the ring can be bypassed in this fashion.

These two structures allow key network components to be located apart from each other. The two rings can physically be located in different places and the TCUs allow stations to be located away from the points of attachment to either ring. (The point being, of course, that a topology could be developed that would allow some damage to the network without the network being rendered inoperable.)

B. The Communication Architecture

The basic communication Architecture follows the OSI reference model and hence follows the concept of having an OSI profile. However it differs from the standard concept of the seven layers in several ways. First of all, alternate suites are allowed. Secondly, SAFENET breaks the layers down into three groupings of services, to allow for physical interfacing (although this is not very clear in the handbook). Finally, several paths exist, even if only one profile is used. These issues will be discussed one at a time.

There are two alternate protocol suites in the SAFENET I profile. There is one called the SAFENET I OSI Profile and a second termed the lightweight protocol suite (see Figure 2 in Appendix A). Stations which only need to communicate with the OSI Profile will be allowed to implement this portion of the SAFENET I Profile alone. Real-time applications, however, are not generally suited for the mechanisms developed for the protocols standardized by the ISO. Hence a lightweight protocol suite which is connectionless oriented (datagram type service) and a streamlined set of user services (layers 5-7) is required. Either or both of the alternate protocol suites can be implemented in a SAFENET network. This of course means that not all stations will be able to communicate with one another, unless the combined protocol suite is used.

The architecture can also be viewed as being divided up into three groupings of layers (see Figure 3 in Appendix A). The user services (layers 5-7), the transfer services (layers 3 and 4 and part of layer 2), and the LAN services (layer 1 and part of layer 2). Between the user services and the transfer services is the transfer service interface, which could be conceptual only. However, it allows for implementation alternatives that may require a set of well-defined communication formats and primitives. A hint of such an implementation is given in the handbook appendix entitled "Overview of the NATO Network Independent Interface" which occurs between the session and transport layers. The division between transfer services and LAN services shows the point where the SAFENET I and SAFENET II differ. The assumption is that the LAN services for SAFENET I will be IEEE 802.5 Token Ring and SAFENET II will be ANSI X3T9.5 FDDI.

A block diagram showing the combined protocol suite and its four possible pathways is found in Figure 4 of the handbook (see appendix A). The first pathway is through the File, Transfer, Access, and Management (FTAM) Protocol and then through the Association Control Element (ASCE) and the remainder of the OSI protocol suite, ending with a connection oriented transport layer protocol that feeds into a connectionless network layer protocol. This provides the communication services for applications that require large file transfers, without real-time concerns. The second path passes through a private communication application interface (hence bypassing FTAM) but uses the remainder of the services provided by the OSI protocol suite.

The third and fourth pathways pass through the lightweight interface and support services before it splits. The assumption here is that real-time applications (connectionless or datagram packet switching) would use this protocol suite. In one option the OSI connectionless (CL) transport protocol would pass data units on to the OSI connectionless network protocol. In the second the Xpress Transfer Protocol (XTP) would be used for layer 3 and 4 services. With the possible silicon implementation of XTP it is likely that this fourth pathway will provide the best option for real-time applications.

C. Management and Synchronization Protocols

The handbook also goes into detail concerning the network management issues and the synchronization techniques. Basically the management functions supported are:

i. Fault management
ii. Configuration and name management
iii. Performance management
iv. Security management

The management mechanisms supporting i.-iii. above are defined by MAP 3.0 (which are also ISO standards), with a discussion of the SAFENET Security Policy placed in a separate handbook appendix. Synchronization services for the management functions are provided by the SAFENET Global Time service. The Global Time service synchronizes individual Global Clocks using a time synchronization protocol. Details of the time synchronization requirements are found in section 10 of the handbook.

D. It is important to the "Survivability" of the network (and the safety and integrity of the system) that the communication protocols are robust and well tested. It is also important to note that the key to the physical topology's ability to provide alternative physical paths is that the management of the network functions properly to detect faults and reconfigure the network. Implementations of the OSI protocol suite will provide these functions. Thus the OSI protocol suite and the combined suites will have management functions. However, if the lightweight protocol suite is implemented alone then these functions will be absent or will have to be provided by the lightweight support services. Since these would have to be developed, it is important that good software engineering practices are used to develop and verify that the protocols function properly.

V. SECURITY ISSUES

A. Security in Networks and the OSI model

In the 1970's and early 1980's there were a lot of developments related to computers and security. During this time frame computer security models were developed as well as standards for security algorithms such as the Data Encryption Standard (NBS 77). Unfortunately developments with computer networks, although occasionally related, generally developed separately from security requirements. Hence in the 1980's work was done to reconcile the issues of computer network security with the work done by the ISO. Voydock and Kent [VOYK85] and Tardo [TARD85] provide some of the background on the discussions as to where to place security functions in the various layers and what mechanisms could be used. OSI committees are still working on draft standards and IEEE 802 committee members are working on how to place security functions in local networks.

B. The SAFENET Security Policy

Appendix H of the SAFENET Military Handbook discusses the Security Policy of SAFENET. It references several related government documents, including the Department of Defense Standard--Trusted Computer System Evaluation Criteria (DOD 85), the Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria [NCS-88], and the Security Requirements for Automated Information Systems (DOD-88). The appendix discusses how security issues are not required for every procurement, and that requirements are evolving and will continue to evolve.

The SAFENET security policy is defined in terms of security domains. The concept of domains limits the scope of a particular security policy. For SAFENET, the two domains are a Network Security Domain and a End-System Security Domain. The Network Security Domain Policy is for layers 1-7 (the LAN and transfer services) while End-System Security Domain concerns the user services of layers 5-7 and the mission-specific application-level policy.

Basically systems using SAFENET will be required to meet TCSEC/TNI Class 2 computer security requirements or higher, depending on the risk factors. If encryption is required then NSA's Secure Data Network System (SDNS) specification is to be followed. This would place key distribution in layer 7, and the encryption protocol in layer 3,4 or 7.

Appendix H also discusses security requirements and guidelines for implementation. The specific requirements include host accreditation, host identification, and user identification and authentication. Also required are formal certification of network components, formal and informal validation of network programs, and a network activity audit trail for security reviews. The document concludes with discussions of the following requirements: network security office support, network security level control, transmission medium security, and assurance of communications availability.

C. Some Recent Developments in Security for Local Area Networks.

The IEEE 802.10 subcommittee is presently working on the problem of security services in layers 1 and 2. Some of the proposals and discussions were presented at a workshop in 1989 [BERS89]. Because of the restriction to IEEE 802 related standards, security issues for the higher layers were not discussed. However, it was very interesting to read that in discussing security, the old concepts of how LANS are defined are giving way. One of the articles discusses how interoperability of LANS and high speed data communications over long distances is doing away with the concept of a LAN being geographically limited.

Other articles discussed where encryption should take place and concepts of LAN security servers. The implication to SAFENET is that eventually OSI standards will affect the services available to the transfer and user services, while IEEE 802.10 will provide available security functions for the LAN services. Thus as the SAFENET security policy evolves, these standards will surely play an important role

VI. IMPLICATIONS FOR AEROSPACE APPLICATIONS

Some of the basic implications for aerospace applications are as follows:

1. As SAFENET begins to appear in Navy procurement, industry will be required to provide SAFENET systems. It is assumed that the cost for similar systems for non-Navy applications will be less expensive to provide.
2. The number of Navy applications is likely to be very large and problems will likely be found and corrected more quickly.
3. Interoperability with the Navy and other US government systems may require SAFENET specifications for NASA systems.

Of course all this may not be that positive. There is of course the possibility that economics might push aerospace systems toward a SAFENET type of implementation, even if it does not meet all aerospace requirements. Hence it might be important to follow SAFENET as it evolves and understand how it is related to developing aerospace standards for communications.

Table I Communication Standards

(Taken from [STAL87])

ISO Standards

ISO 7498	Basic Reference Model for Open Systems Interconnection, 1984.
DIS 8348	Network Service Definition
DIS 8473	Protocol for Providing the Connectionless-Mode Network Service
ISO 8072	Transport Service Definition
DIS 8073	Connection-Oriented Transport Protocol Specification
DIS 8602	Protocol for Providing the Connectionless-Mode Transport Service

CCITT Standards

X.25	Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit

IEEE Standards

IEEE 802.2	Logical Link Control
IEEE 802.3	CSMA/CD Access Method
IEEE 802.4	Token Bus Access Method
IEEE 802.5	Token Ring Access Method

ANSI Standards

ANSI X3T9.5	Fiber Distributed Data Interface

Table 2 MAP Stack

(Taken from [BLAC89])

Layer 7	ISO CASE Kernel, Four ASEs: FTAM, Directory Service, Network Management, MMS
Layer 6	ISO 8822,8823,8824,8825
Layer 5	ISO 8326,8327,8326/DAD2,8327/DAD2
Layer 4	ISO 8072 and 8073 Class 4
Layer 3	ISO Connectionless Internet 8473 and others
Layer 2	IEEE 802.2, various types and classes
Layer 1	IEEE 802.4 Broadband (10 Mbit/s) and Carrierband (5 Mbit/s)

REFERENCES

[BERS89]
Berson, T.A., T. Beth (eds.), Local Area Network Security, Workshop LANSEC '89, Proceedings, Springer-Verlag, 1989.

[BLAC89]
Black, Uyless, Data Networks: Concepts, Theory, and Practice, Prentice Hall, 1989.Implications for Aerospace Applications.

[DERN90]
Daniel P. Dern, "GOSIP Makes Its Debut," Business Communications Review, v.20,no.8, August 1990, pp.43-46.

[DOD85]
"Department of Defense Trusted Computer System Evaluation Criteria," DOD 5200.28-STD, December 1985.

[GOSI87]
U.S. Government Open Systems Interconnection Profile (GOSIP). Gaithersburg, MD: National Bureau of Standards, 1987.

[IEEE85a]
IEEE, CSMA/CD Access Method--IEEE 802.3, 1985.

[IEEE85b]
IEEE, Token Bus Access Method--IEEE 802.4, 1985.

[IEEE85c]
IEEE, Token Ring Access Method--IEEE 802.5, 1985.

[IEEE85d]
IEEE, Logical Link Control--IEEE 802.2, 1985.

[NBS77]
National Bureau of Standards: "Data Encryption Standard," Fed. Inf. Process. Stand. Pbul. 46, Jan.1977.

[STAL87]
Stallings, W., Handbook of Computer Communications Standards, Vol.1, The Open Systems Interconnection (OSI) Model and OSI-Related Standards, MacMillan, 1987.

[TARD85]
Tardo, Joseph, "Standardizing Cryptographic Services at OSI Higher Layers," IEEE Communications Magazine, July 1985, pp.25-29.

[VOYK85]
Voydock, Victor L. and Stephen T. Kent, "Security in High-Level Network Protocols", IEEE Communications Magazine, July 1985, pp.12-24.

[XTP88]
Protocol Engines, Inc., XTP Definition, Rev.3.1, 1988.

[ZIMM80]
Zimmermann, Hubert, "OSI Reference Model--The ISO Model of Architecture for Open Systems Interconnection," IEEE Transactions on Communications, April 1980, pp.425-432.

SPECIAL NOTE: A copy of the SAFENET Documents is on file at UHCL. These are:

Space and Naval Warfare Systems Command. REVIEW OF SURVIVABLE ADAPTABLE FIBER OPTIC EMBEDDED NETWORK (SAFENET) LOCAL AREA NETWORK (LAN) STANDARD AND HANDBOOK. 5230 Ser 324/051 19 Jun 90. This document contains the following enclosures:
(1) Draft SAFENET I Military Standard (MCCR-0032-DRAFT)
(2) Draft SAFENET I Military Handbook (MCCR-0034-DRAFT)
(3) SAFENET I Executive Summary
(4) SAFENET I STANDARDIZATION IMPROVEMENT PROPOSAL

Appendix A. Figures from the SAFENET I Military Handbook

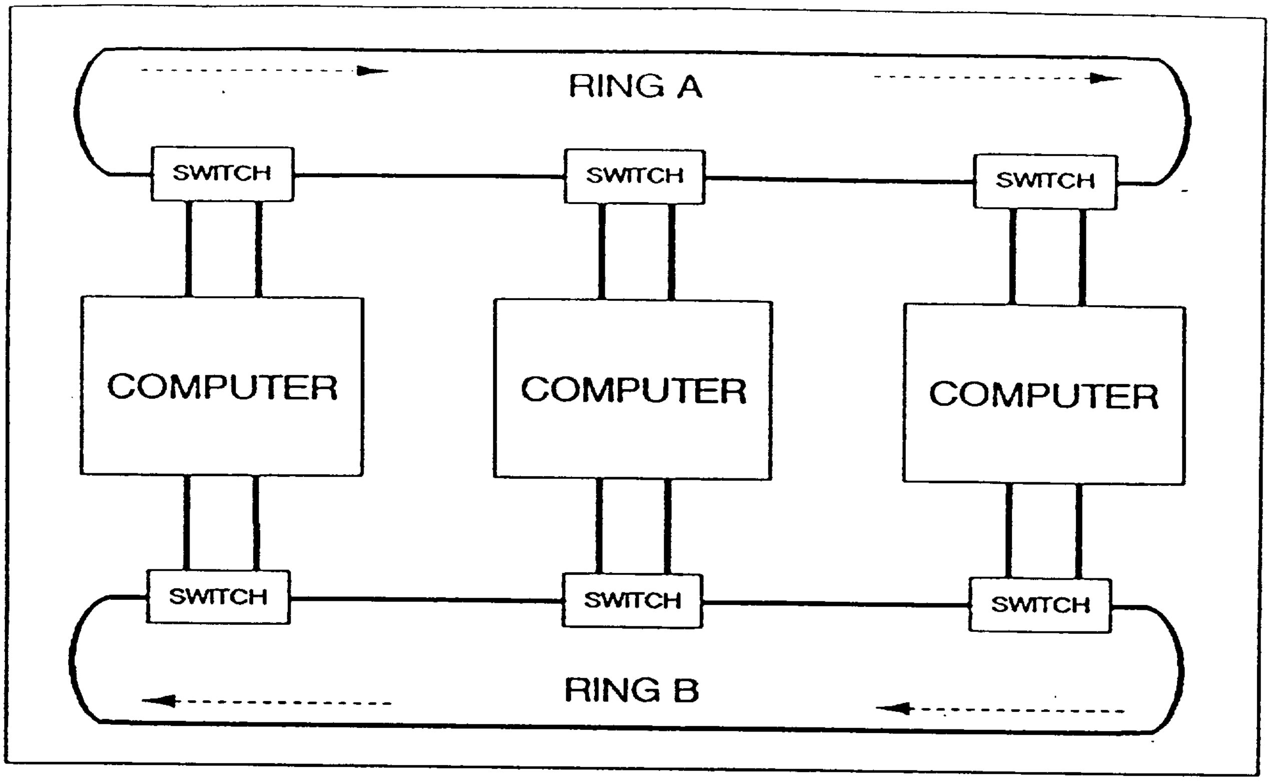

Figure 1. Dual-Ring Local Area Network

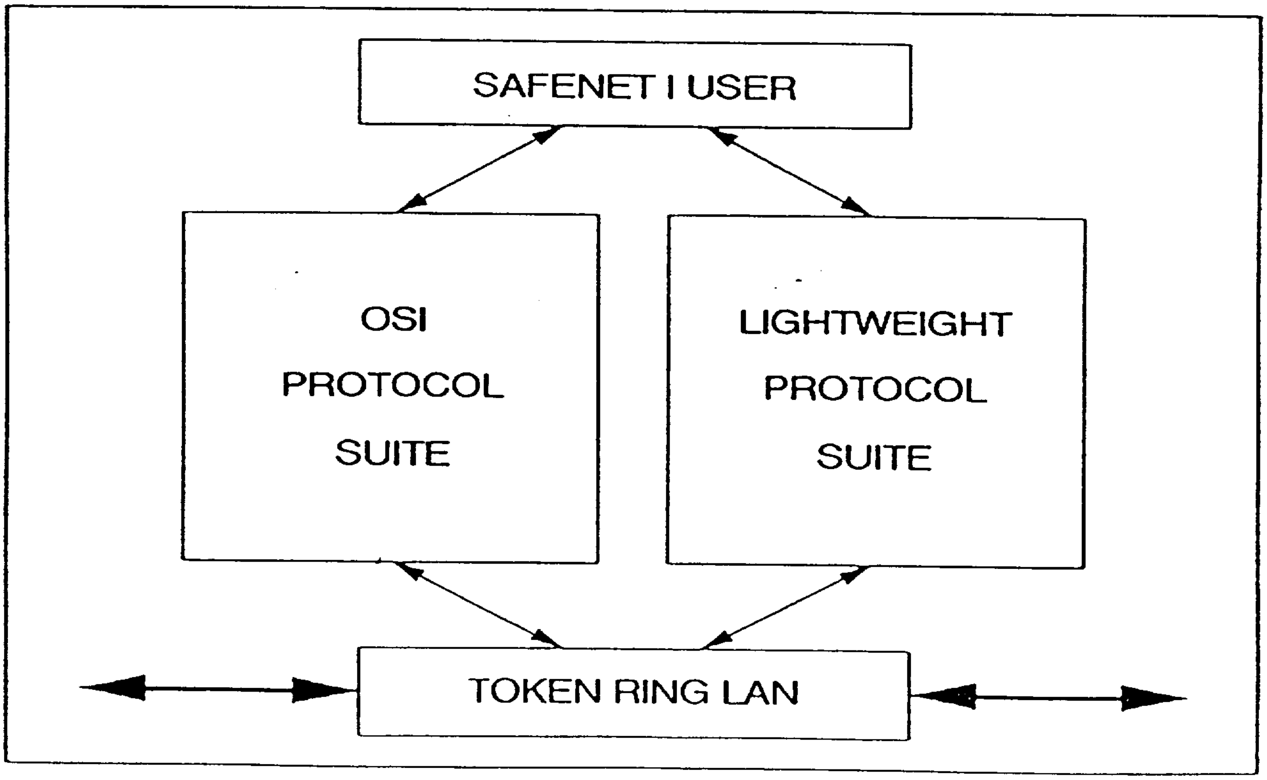

Figure 2. Alternate Protocol Suites

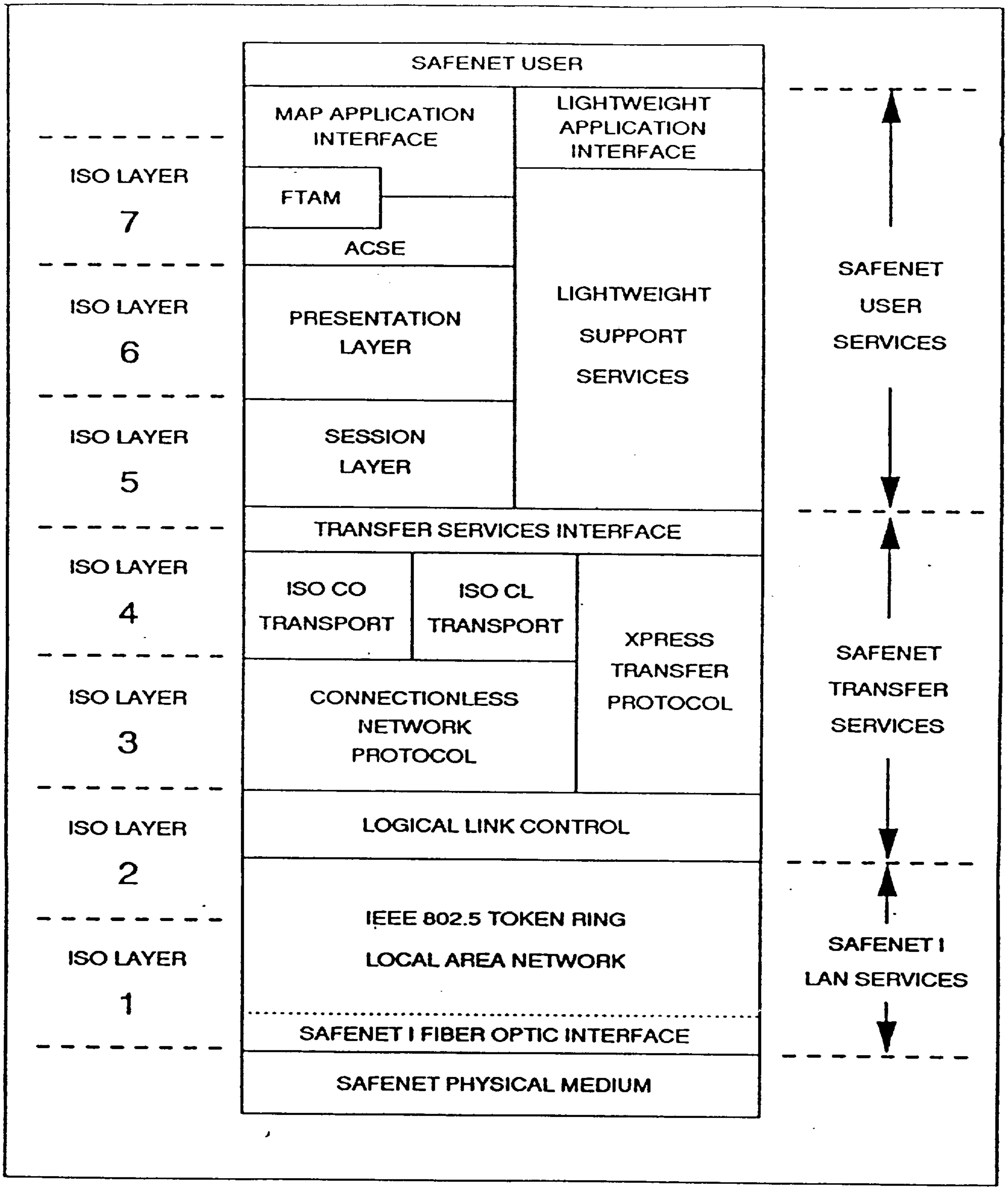

Figure 3. SAFENET I Protocol Profile

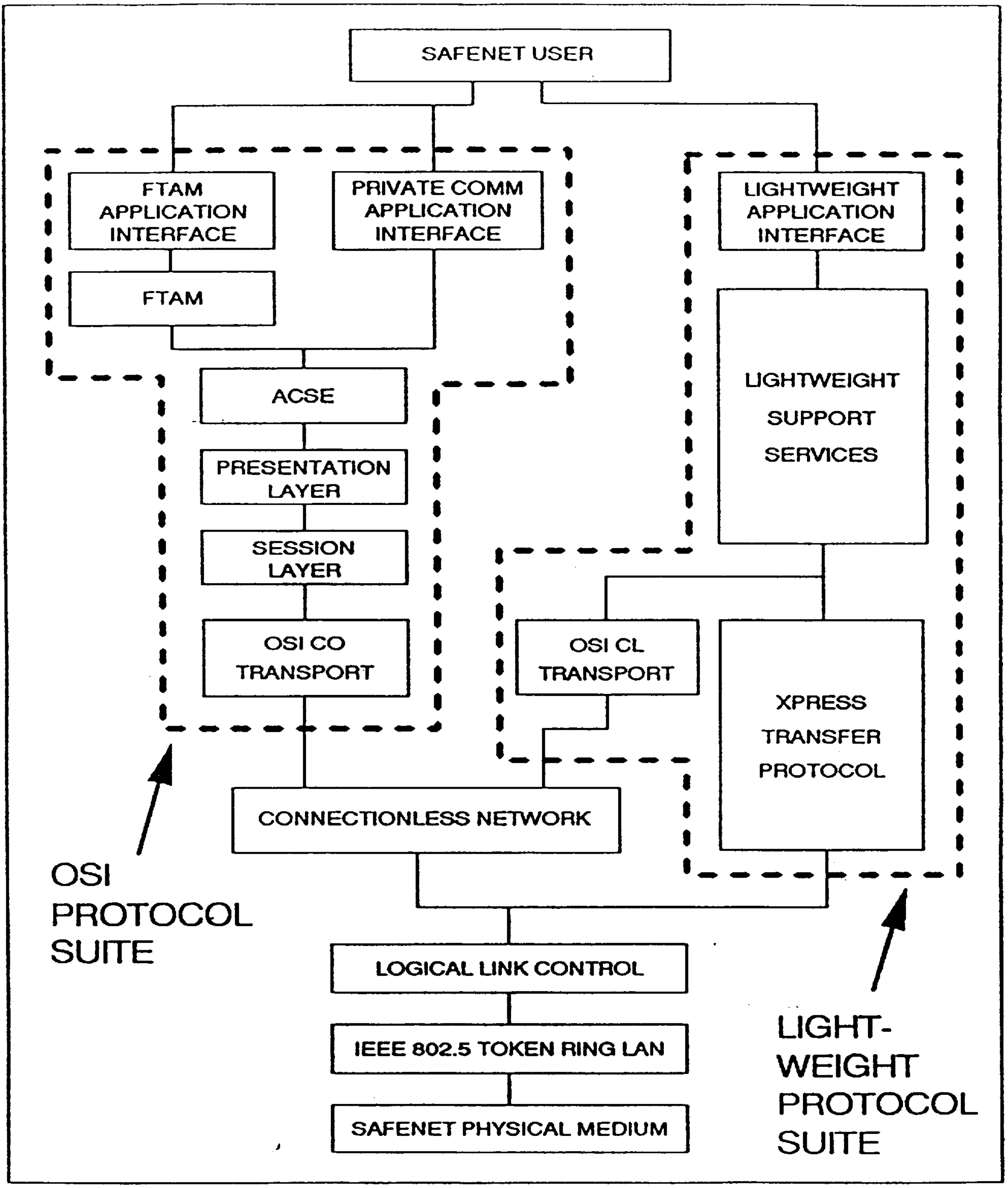

Figure 4. SAFENET I Protocol Suites

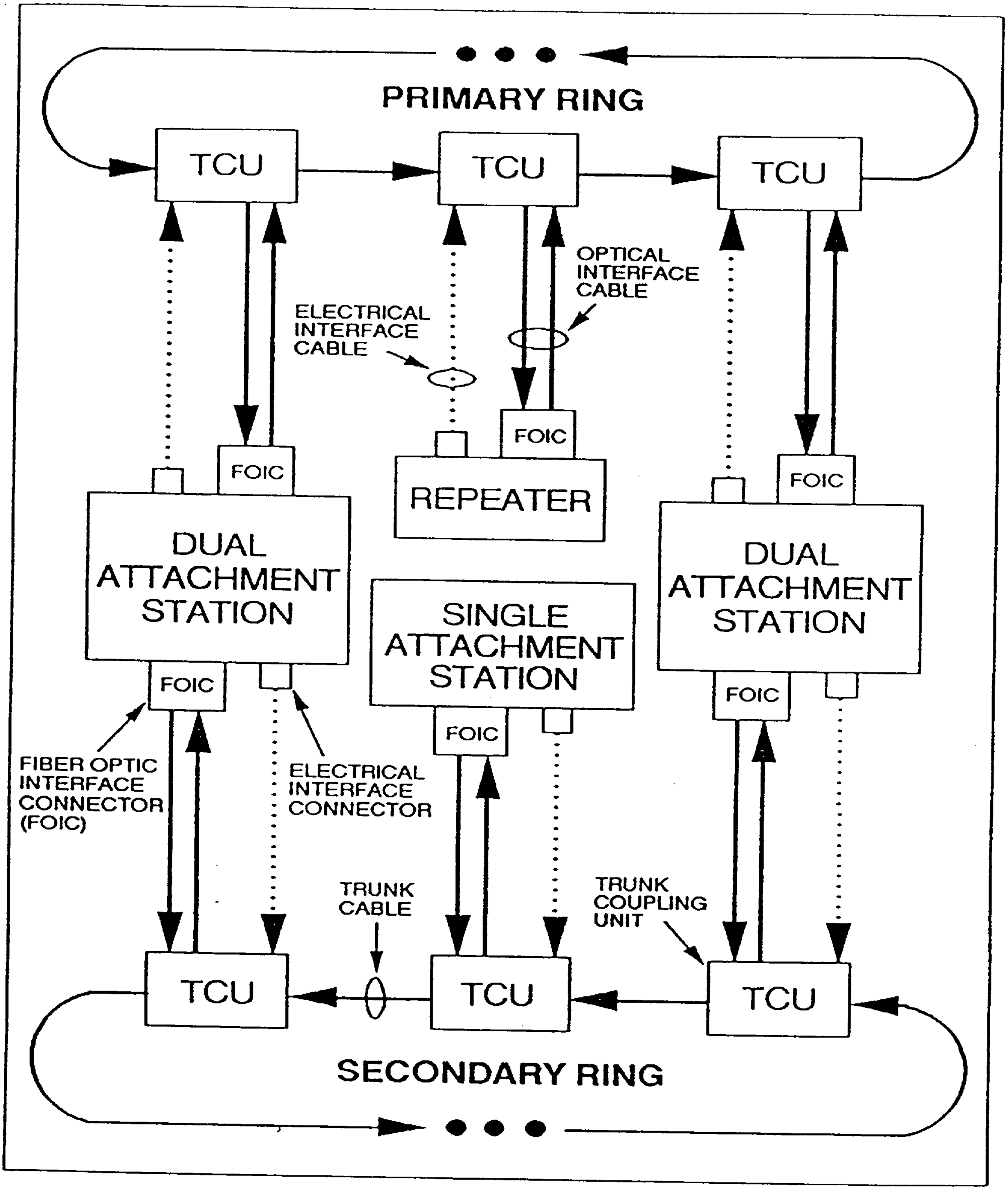

Figure 5. SAFENET I Physical Topology