Document No. 102-94-015U

DRAFT
Technical Report
Demonstration of Concept

Task 1

Contract No. N00039-93-C-0099

CDRL No. A003

August 3, 1994

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 51)
Arlington, VA 22245-5200

Prepared by:

Secure Solutions, Inc.
9404 Genesee Avenue, Suite 237
La Jolla, CA 92037
(619) 546-8616

DISTRIBUTION STATEMENT: Approved for public release; distribution is unlimited.

Document No. 102-94-015U

DRAFT
Technical Report
Demonstration of Concept

Task 1

Contract No. N00039-93-C-0099

CDRL No. A003

August 3, 1994

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR PD 51)
Arlington, VA 22245-5200

Prepared by:

Secure Solutions, Inc.

9404 Genesee Avenue, Suite 237
La Jolla, CA 92037
(619) 546-8616

Table of Contents

Table of Contents (continued)

Index of Figures

This Page Intentionally Left Blank

Executive Summary

Secure Solutions, Inc. was tasked by the Department of the Navy's Space and Naval Warfare Systems Command (SPAWAR) to perform a Small Business Innovation Research (SBIR) Phase II network security research effort on the "Placement of Security Services for Secure Data Exchange."

A major thrust in Naval command and control is to securely interconnect networks for the purpose of sharing information and improving the survivability of the overall network. To support application-level interoperability among command and control systems which use these networks, the use of a layered architecture is imperative.

The placement of security services within the International Standards Organization (ISO) Open Systems Interconnection (OSI) Reference Model (RM), the open framework for a layered architecture, has always been controversial. The SBIR Phase I (Placement of Network Security Services for Secure Data Exchange) effort fulfilled a need to identify the security services and mechanisms that should be provided at each of the layers with specific consideration for Naval applications. The following table presents the allocation of security services to the OSI RM for Naval applications that was developed as a result of the Phase I effort.

	Layer						
Service	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Data Confidentiality	●	●	●			●	
Data Integrity		●	●	●		●	
Authentication		●	●			●	●
Access Control		●	●	●			●
Non-repudiation						●	●

The Phase I made the qualitative observation that the delivery time through a secure relay (or secure front end) could be improved (reduced) if the security protocol is implemented at a lower layer within these components.

This study (Task 1 of the Phase II SBIR effort) identifies potential sources which can be used to qualitatively determine the improvement in delivery time through three variations of a local area network (LAN) internetwork. The LAN internetwork consists of two 802.3 LANs interconnected through a backbone fiber distributed data interface (FDDI) LAN. Three different types of secure relays are used to interconnect the 802.3 LANs with the FDDI LAN. They each use different types of security protocols at different OSI layers — the Secure Data Exchange (SDE) protocol at Layer 2; Security Protocol 3 (SP3) or the Network Layer Security Protocol (NLSP) at Layer 3; and Security Protocol 4 (SP4) or the Transport Layer Security Protocol (TLSP) at Layer 4.

This Page Intentionally Left Blank

Section 1
Introduction

1.0 Introduction

This report documents the results of an analysis performed by Secure Solutions under Phase II of a Small Business Innovation Research (SBIR) Program for the Department of the Navy's Space and Naval Warfare Systems Command (SPAWAR) under Contract Number N00039-93-C-0099. This overall research topic is entitled "Placement of Security Services for Secure Data Exchange" (Topic Number N91-061). This report documents Task 1 of the Phase II SBIR effort and demonstrates quantitatively how much delivery times can be improved (reduced) by implementing security protocols at lower OSI layers in relays (or front ends). The results of this task extend the qualitative conclusions reached in Phase I and also provide an input to the systems / security engineering process that is used under Task 4 of this effort to define Naval requirements for secure network products.

This introduction provides background for why this effort was initiated, study scope, study objectives, the approach used and recommendations, and the organization of the report.

1.1 Background

Naval command and control systems are hosted on shipboard, shore, and airborne platforms and operate in a variety of environments. Diverse communications networks are used to support these command and control systems. These networks operate from the Extremely Low Frequency (ELF) to Extremely High Frequency (EHF) bands and employ both point-to-point and broadcast transmission techniques. A major thrust in Naval command and control is to interconnect these networks for the purpose of sharing information and improving the survivability of the overall network.

The use of a layered architecture is imperative to support application-level interoperability among command and control systems which use these networks [Copernicus 91]. One major framework for an open, layered architecture is the 7-layer International Standards Organization (ISO) Open Systems Interconnection (OSI) Reference Model (RM), as described in ISO 7498 [ISO 84]. The placement of security services within the OSI RM is governed by the OSI RM Security Architecture, described in ISO 7498-2 [ISO 89A].

A problem with the approach used by ISO to place security services within the OSI layers is that it did not take into account some of the stringent constraints encountered in the Naval tactical environment. For example, it is critical that placement choices be made in a manner that conserves bandwidth, supports real-time transmission requirements, and promotes survivability and availability. These evaluation factors were not considered by the authors of ISO 7498-2 in allocating security services to the different OSI layers.

As a result, the need to analyze the security services that should be provided among the seven OSI layers for Naval applications was identified. This analysis was to take into account the previous work in this are performed by ISO and the IEEE 802.10 Standard for Interoperable LAN Security (SILS) committees (which allocated additional security services to layer 2 beyond the those already specified by the OSI Security

Architecture), as well as, the associated impacts on Communications Security (COMSEC) and Computer Security (COMPUSEC) assurance criteria, and features important to Navy missions such as bandwidth conservation, delivery / response time, survivability and reconfigurability. The SBIR Phase I research effort on the Placement of Security Services for Secure Data Exchange was initiated under contract N00039-92-C-0039 to help fulfill this need.

This SBIR Phase II network security research and development (R & D) effort extends the work of the Phase I study by further refining and validating the engineering rationale developed during Phase I, analyzing security service placement options for specific Navy applications, analyzing end-to-end encryption and traffic flow security options, conducting system engineering studies to define Naval mission-specific security needs, and developing Naval security product functional requirements specifications for potential network security products.

One of the factors considered during Phase I was the determination of the relative impact on delivery times depending upon where the security protocols are implemented within the OSI layered architecture. Two major conclusions were drawn:

- Providing end-to-end security services, as opposed to link security services, improves (reduces) delivery time, since security encapsulation / decapsulation functions are only performed at the source and destination host. When link security services are used, security encapsulation / decapsulation functions are performed repeatedly, thereby increasing the host-to-host delivery time for a given network configuration.
- In some situations, it is desirable to implement security services within relays (or host front ends). Implementation of security protocols at lower OSI layers in relays (or front ends) reduces the host-to-host delivery time, since fewer headers are processed within the relays / front ends.

Task 1 of the Phase II SBIR effort expands upon the second conclusion by defining quantitatively the improvement (reduction) of delivery times when security protocols are implemented at lower OSI layers in relays (or front ends).

1.2 Scope

There are a number of factors to consider in determining the layers at which security protocols should be implemented within the OSI RM for Naval applications. This effort addresses one of these factors — delivery time. Its primary objective is to determine if the layer at which a security protocol is placed has a significant influence on delivery time in quantitative terms. The results of this study provide one input to the system / security engineering process used in Task 4 of this SBIR effort. Task 4 establishes requirements for network security products for the Navy. In Task 4, a variety of factors are considered to select the best OSI layers for implementing security protocols.

The specific network configuration used as the basis for this evaluation is a LAN internetwork. The LAN internetwork consists of two 802.3 LANs interconnected through a FDDI backbone. The hosts and relays associated with this network use communications and security protocols that have been defined or adopted by the ISO for use within the framework of the OSI RM. Three different types of relays are used to connect the 802.3 LANs to the FDDI backbone:

- Secure bridge [Secure Data Exchange (SDE) protocol at layer 2]
- Secure router [Network Layer Security Protocol (NLSP) at layer 3]
- Secure transport relay [Transport Layer Security Protocol (TLSP) at layer 4].

These relays provide the basis for the three network configurations shown in Figure 1.2-1 (a, b and c). The host-to-host delivery time across each of these network configurations varies, since the processing delay through the bridges (1.2-1a) is less than the delay through the routers (1.2-1b) which is less than the delay through the transport relays (1.2-1c). Detailed rationale for the selection of these network configurations is provided in Sections 2 and 3.

To evaluate the host-to-host delivery time across the three network configurations, available literature was investigated to find relevant results based on:

- Analysis
- Testing
- Simulation.

The scope of this effort includes consideration of any combination of the above methods to evaluate the delivery times for each of the three network configurations.

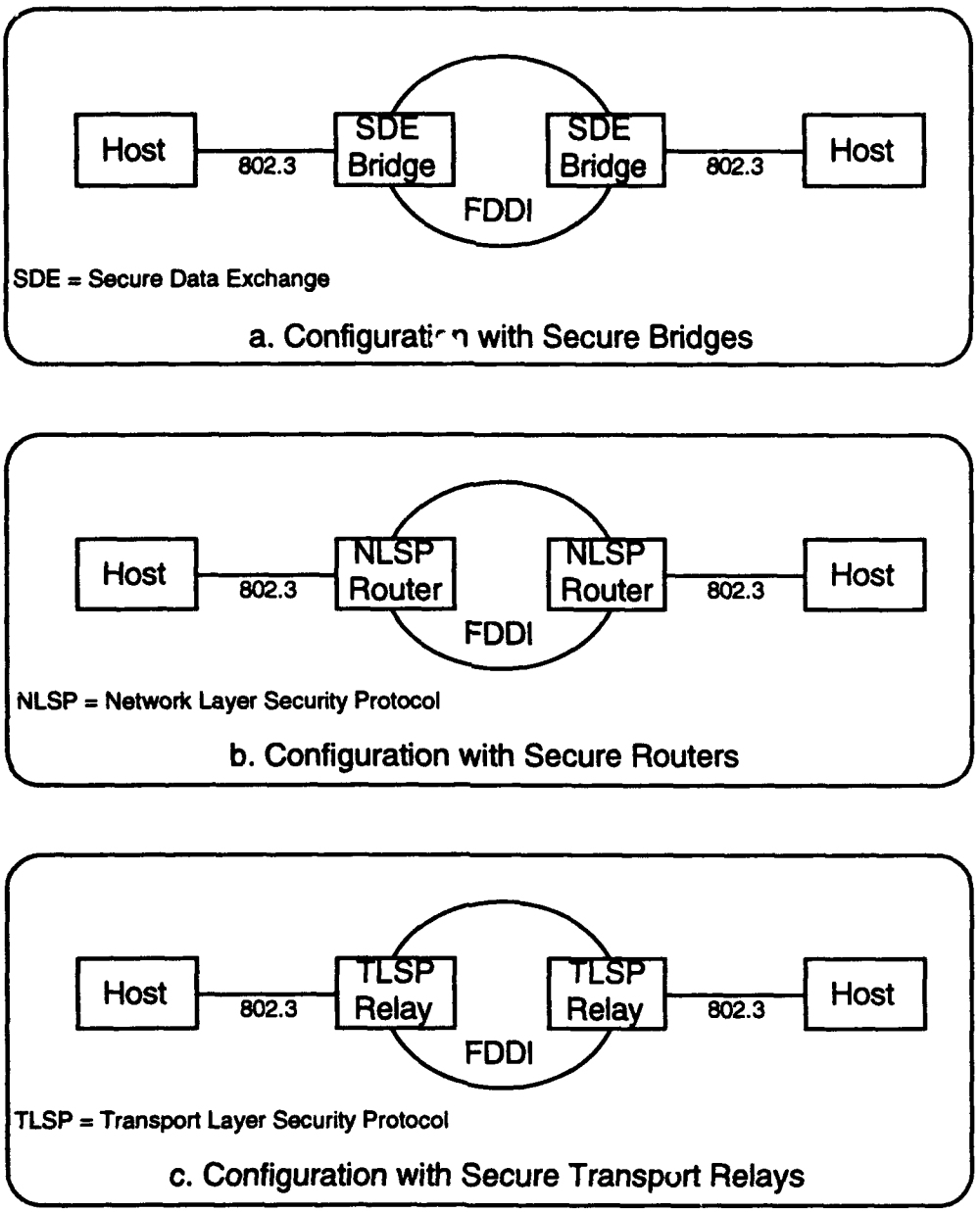


Figure 1.2–1. *Network Configurations Used for Study*

The primary focus of Task 1 is to determine quantitatively the extent to which delivery times can be reduced by implementing security protocols at lower OSI layers in relays (or front ends). This is demonstrated using a network configuration that incorporates security protocol mechanisms which protect the OSI communication protocols that are in use.

1.3 Study Objective

The objective of this study is to determine quantitatively if the implementation of security protocols at lower OSI layers in relays (or front ends) will significantly reduce delivery time across a LAN internetwork.

1.4 Approach

This study was based upon a methodology which consists of the following steps:

- Define network configuration for evaluating delivery time
- Develop mathematical model for computing delivery time
- Search for relevant sources.

The relationships among these steps is shown in Figure 1.4-1. A description of each step is provided below.

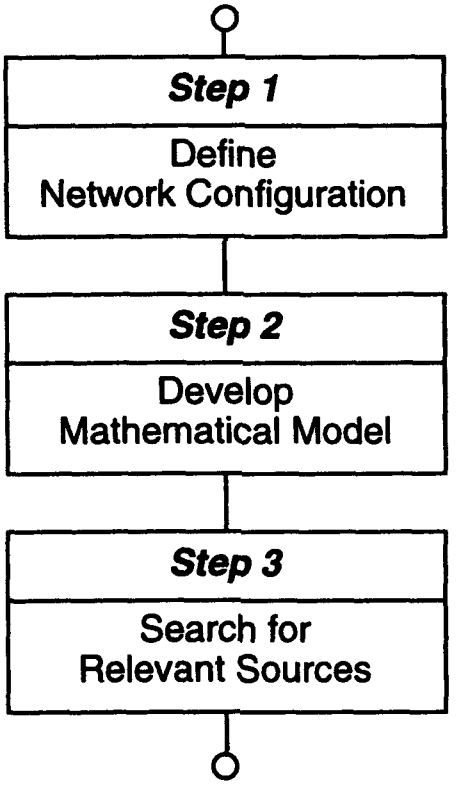


Figure 1.4–1. *Overview of Task 1 Study Approach*

Step 1 – Define Network Configuration for Evaluating Delivery Time

In step 1, a network configuration was selected to evaluate how delivery time is affected by where security protocols are placed within an OSI stack. For any given network, the layers at which security protocols are placed within relays or front ends may have an impact on delivery time; their placement within a host will not. For this reason, a network configuration was selected that uses secure relays, and is of potential and practical use within shipboard environments. This network configuration consists of two physically secured 802.3 LANs interconnected through a backbone FDDI LAN. The pair of relays connecting the 802.3 LANs to the FDDI backbone provides encryption and other security services over the FDDI LAN through the use of security protocols. This basic network configuration had three variants distinguished by the type of secure relay used — an SDE bridge, an NLSP router, or a TLSP relay. Figure 1.2-1 illustrated the three variants of the basic network configuration used to conduct this study.

Step 2 – Develop Mathematical Model for Computing Delivery Time

In step 2, mathematical formulas were developed for computing delivery time for each of the three network variants as defined in step 1. At the highest level, delivery time was decomposed into host processing delays (source and destination hosts), relay processing delays (SDE bridge, NLSP router, and TLSP relay), and LAN transmission delays (802.3 and FDDI). Host and relay processing delays were further decomposed into protocol processing delays (application, presentation, session, Transport Protocol Class 4 (TP4), TLSP, the Connectionless Network Protocol (CLNP), NLSP, Logical Link Control (LLC), SDE, 802.3, and FDDI) and queuing delays between protocol entities across adjacent layers. LAN transmission delays were further decomposed into access, transmission and propagation delays. This mathematical foundation provided a model for computing delivery time and also served to focus the search for relevant technical reference material sources.

Step 3 – Search for Relevant Sources

In step 3, a variety of literature searches were conducted to identify relevant sources for this Task 1 effort. This included a classified Defense Technical Information Center (DTIC) search, an Internet search, and a search of the University of California Library system. Literature searches were based on the following major keywords: OSI, protocol, network, LAN, FDDI, ethernet, 802.3, router, bridge, host, COMSEC (or encryption), board (or module), performance, delay, time, security, analysis, simulation, and testing. Examples of keyword combinations used to search for relevant sources included: OSI and testing, routers and delay, protocols and simulation, and LANs and testing.

1.5 Report Organization

The main body of the report is organized as follows:

- Section 1 – Introduction
- Section 2 – Description of Basic Network Configuration / Protocols
- Section 3 – Selection of Secure Network Configurations
- Section 4 – Mathematical Model for Computing Delivery Time
- Section 5 – Overview of Related Work
- Section 6 – Conclusions and Recommendations.

The following appendices are provided to supplement the main body:

- Appendix A – Acronyms
- Appendix B – References.

This Page Intentionally Left Blank

Section 2
Description of
Basic Network Configuration / Protocols

2.0 Description of Basic Network Configuration / Protocols

Figure 2.0-1 is representative of a network which can be used to support Naval communications requirements aboard a ship. It consists of a single, backbone FDDI Local Area Network (LAN) that interconnects multiple 802.3 LANs through relays. The 802.3 LANs directly support attached hosts. This basic network configuration forms the basis for this study to evaluate the impact of security protocols on delivery times.

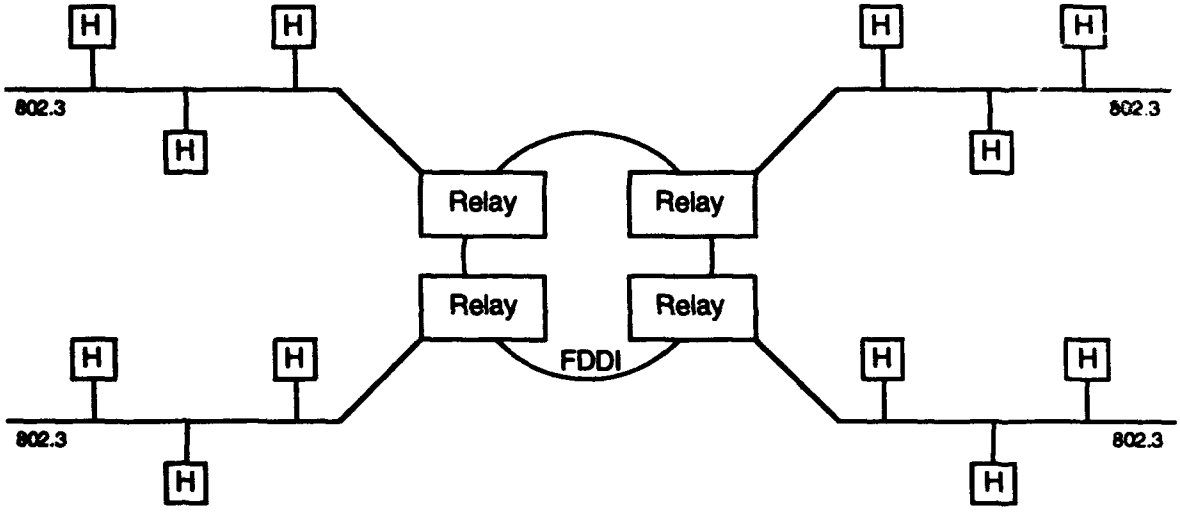


Figure 2.0–1. *Basic Network Configuration for Ships*

This section provides background for the reader by describing the communications and security protocols that are used in the basic network configuration. An assumption is made that hosts and relays specified all use protocols that have been developed or adopted by the ISO for use in the OSI RM. The general OSI communications protocols that apply to the basic network are thus:

- IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA / CD)
- Fiber Distributed Data Interface (FDDI)
- IEEE 802.2 Logical Link Control (LLC)
- Connectionless Network Protocol (CLNP)
- Transport Protocol Class 4 (TP4).

Candidate security protocols which can be used to secure this network are:

- IEEE 802.10(B) Secure Data Exchange (SDE)
- Security Protocol 3 (SP3)
- Network Layer Security Protocol (NLSP)
- Security Protocol 4 (SP4)
- Transport Layer Security Protocol (TLSP).

2.1 General OSI Communications Protocols

The following paragraphs briefly describe the general OSI communications protocols that apply to the basic network used in this study.

2.1.1 IEEE 802.3 CSMA / CD

The IEEE 802.3 protocol operates at the Media Access Control (MAC) sublayer and is a contention-based protocol. When a frame is ready for transmission, the channel is first sensed. If the channel is idle, the frame is transmitted. If it is not idle, the station waits for channel to become idle and then transmits frame. If a collision occurs, the station waits a random time period and starts the process over.

The CSMA/CD PDU begins with a preamble consisting of alternating ones and zeros for clock synchronization, and a one-octet start frame delimiter. Source and destination MAC addresses may be 16 or 48 bits in length. All stations on a given IEEE 802.3 LAN must however use the same address length. Padding needed for proper collision detection and timing requirements is added in a pad field to make the frame a minimum of 64 octets from the destination address to the Frame Check Sequence (FCS), inclusive. The PDU is completed with a 32-bit FCS field.

2.1.2 Fiber Distributed Data Interface (FDDI)

The ANSI Fiber Distributed Data Interface (FDDI) protocol operates at the MAC sublayer and is a contention-free protocol. To provide transmission opportunities for FDDI stations, a token circulates on the ring. In order to transmit a data frame, a station must first seize the token. When a station finishes transmitting data, it must then regenerate the token. Each station is responsible for removing its data from the ring when it returns.

An FDDI token consists of the preamble, the "JK" starting delimiter, a Frame Control field, and the "T" ending delimiter. AN FDDI data frame consists of a preamble that is at least 16 symbols of Idle, the "JK" starting delimiter, a Frame Control field, destination and source MAC addresses, data, a Frame Check Sequence, the "T" ending delimiter, and the "RSRS" frame status field. Repeater stations may shorten or lengthen the preamble as necessary for Physical Layer clocking requirements.

2.1.3 IEEE 802.2 Logical Link Control (LLC)

The Logical Link Control (LLC) protocol transfers information and control between any pair of data link layer Service Access Points (SAPs) on a LAN. There are two types of LLC service: Type 1 which provides a connectionless mode without acknowledgment (acknowledgments by higher layers can be used), flow control, or error recovery; and Type 2 which provides connection oriented service with acknowledgment (via ACK PDU), flow control (via sequence numbering and Receive Ready / Receive Not Ready), and error recovery (via Reject PDU). The LLC Type 1 protocol is used for this study.

A Type 1 LLC header consists of a Control octet, Source Service Access Point (SSAP), and Destination Service Access Point (DSAP). SSAPs and DSAPs are known collectively as Link Service Access Points (LSAPs). LSAPs are one octet in length and identify the users of the LLC protocol, usually protocols at a higher layer within the station (e.g., an ISO network layer protocol or the DoD Internet Protocol). For this study, they are used to identify CLNP.

2.1.4 Connectionless Network Protocol (CLNP)

The CLNP is used to route packets across an internetwork and supports connectionless network services. It allows packets to be fragmented (divided into smaller packets called segments) and enter a subnetwork which supports a smaller maximum packet size than the subnetwork it is leaving. The segments for a given packet are ultimately recombined at the destination. CLNP headers contain source and destination addresses. These addresses have global significance within the context of the internetwork and are used to represent hosts and gateways. These addresses can also be chosen independently from the subnet-specific addresses that identify network components. CLNP includes a 16-bit checksum that this is computed over the CLNP header.

2.1.5 Transport Protocol Class 4 (TP4)

The Connection Oriented Transport Protocol (COTP) provides five different protocol classes (Classes 0 through 4). The Transport Protocol Class 4 (TP4) is generally used with connectionless network protocols (such as CLNP) which can lose or reorder PDUs; or deliver PDUs with undetected errors. TP4 is capable of using a 16-bit checksum to detect damaged PDUs and 7- or 31-bit sequence numbers to detect lost or duplicate PDUs. TP4 provides multiplexing (multiple transport connections over one network connection), explicit flow control, checksumming, frozen references, retransmission on time-out to cope with unsignalled transport PDU loss by the network service provider, resequencing to cope with unsignalled network connection termination, and splitting (one transport connection over multiple network connections). TP4 also uses a variety of control and data TPDUs. The Connection Request (CR) and Connection Confirm (CC) TPDUs contain identifiers for the calling and called Transport Service Access Point (TSAPs).

2.2 Security Protocols

The following paragraphs briefly describe the security protocols which can secure the basic network configuration used in this study.

2.2.1 IEEE 802.10 (Clause 2) Secure Data Exchange (SDE)

The Secure Data Exchange (SDE) Protocol is implemented at the Data Link Layer, as part of the logical link control (LLC) sublayer. SDE augments standard LLC and MAC communications protocols without replacing those protocols. An SDE-specific PDU encapsulates the LLC PDU and has optional elements and fields to satisfy a variety of potential security applications. SDE requires no change to existing upper-layer protocols in the stack. SDE will operate in LANs where all stations do not use SDE. The SDE PDU has a clear header portion which includes a unique Link Service Access Point (LSAP) address to distinguish the SDE PDU from unprotected LLC PDUs.

SDE is a security protocol that is designed to provide connectionless confidentiality and integrity services through encapsulation of LLC PDUs using encryption, an integrity check value (ICV), or both. The data confidentiality and data integrity services can be provided to in both end systems and intermediate systems. SDE also supports data origin authentication and access control. Data origin authentication is achieved through the use of the integrity service. or through the use of key management and the placement of a Station ID in the SDE protected header. Access control is provided by key management or system management. Access control decisions are based on the use of security associations. Access control is dependent on both integrity and authentication services.

2.2.2 Security Protocol (SP3)

Security Protocol 3 (SP3) provides connectionless security services, and assumes that it is operating over a connectionless network service. It operates in both end systems and intermediate systems, and does not preclude the use of unprotected communications between a system which has SP3 and one that does not.

SP3 provides connectionless confidentiality and integrity by encapsulating network SDUs using encryption and integrity check values. It also provides access control (based on a label and network service access points). SP3 has no security association PDU and must rely on external key management protocols for security association (SA) establishment. The Key-ID field references the traffic encryption key (TEK) and associated security attributes that are maintained in the security management information bases (SMIBs) of both hosts for the SP3 peer entities.

2.2.3 Network Layer Security Protocol (NLSP)

The Network Layer Security Protocol (NLSP) provides the security services at Layer 3 which are not provided by standard communications protocols. It does not replace standard communications protocols, but augments them. NLSP can be implemented in end systems and intermediate systems to provide end-to-end encapsulation or link encapsulation of higher level PDUs. Other primary functions beyond encapsulation include padding and connection authentication.

NLSP provides the option for performing an encipherment or integrity key exchange internally. This allows key management to be removed from the application layer. It also works if key management is performed externally. Before secure communications can be accomplished, security association attributes must be negotiated.

2.2.4 Security Protocol (SP4)

Security Protocol 4 (SP4) operates with both connection-oriented and connectionless transport protocols and does not preclude the use of unprotected communications. Therefore, SP4-capable hosts can operate in networks where not all stations use SP4 and can communicate with both protected and unprotected hosts if that is allowed by the local security policy. SP4 encapsulate Transport PDUs using encryption and integrity check values to provide confidentiality and integrity services. It uses sequence numbers internal to the transport protocol to provide connection integrity. Transport PDUs can also be labeled and padded.

SP4 allows for the use of a Final Sequence Number (FSN) to detect truncation (the deletion of the PDUs transmitted at the end of a transport connection). The FSN field conveys the sequence numbers of the last PDUs sent and transmitted over the transport connection so that both sides can determine if all PDUs have been received.

2.2.5 Transport Layer Security Protocol (TLSP)

The Transport Layer Security Protocol (TLSP) can support connectionless or connection-oriented confidentiality and integrity services. Implementation of TLSP on a host does not preclude the use of unprotected communications between transport protocol entities because the formats of all parameters sent down from the Transport Layer communications protocol are preserved and passed to the Network Layer. Encapsulation is performed by TLSP after all transport protocol processing is performed and prior to multiplexing and assignment to the network connection. A security label can be associated with each encapsulated transport PDU and security padding can be used to support cryptographic algorithm requirements for both confidentiality and integrity. Connection establishment PDUs can be exchanged to perform peer-entity authentication at the transport layer.

TLSP encapsulates transport TPDUs using encipherment and an integrity check value to provide host-to-host confidentiality and integrity services. Sequence numbers within the transport protocol are used to provide connection integrity. TLSP does not support the FSN feature provided by SP4.

This Page Intentionally Left Blank

Section 3
Selection of
Secure Network Configurations

3.0 Selection of Secure Network Configurations

The previous section described the basic network configuration and protocols used to perform this task. This section considers alternative allocations of these protocols to network components and selects specific cases for further investigation. Specific topics addressed in this section are:

- Allocation of security protocols among network components (hosts / relays)
- Delay as a function of layer placement options / network components
- Selection of preferred network configurations for study.

3.1 Allocation of Security Protocols Among Network Components

Figure 3.1-1 illustrates the allocation of security protocols (SPs) to hosts and relays in a manner that supports both physically secured 802.3 LANs and multi-level secure (MLS) 802.3 LANs. Rationale for this allocation is provided below.

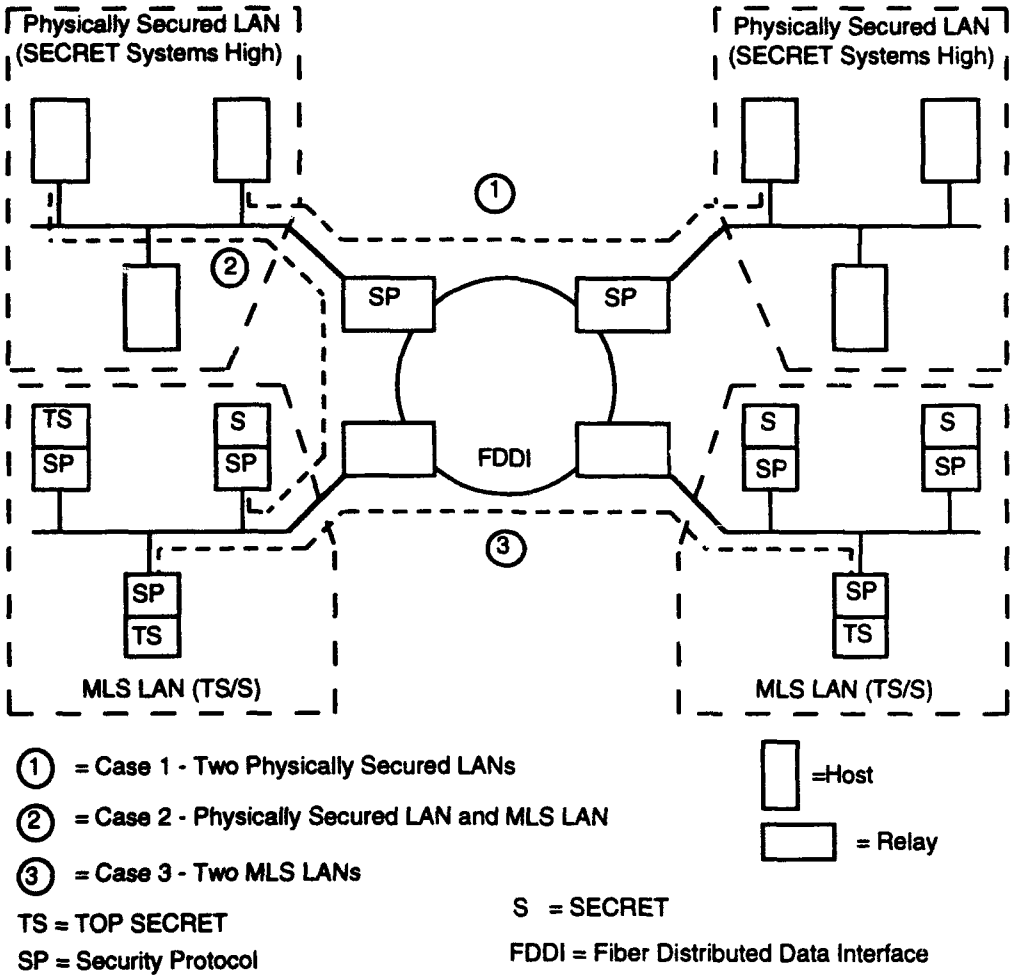


Figure 3.1–1. *Allocation of Security Protocols to Network Components*

3.1.1 Physically Secured 802.3 LANs

The physically secured 802.3 LANs are wholly contained within protected areas and, in this figure, operate in a systems high security processing mode. All of the data that is processed within this LAN is therefore considered to be at the same classification level. (The assumption is made that the hosts on this LAN cannot be trusted to protect data at different classification levels.) Different physically secured LANs can however operate at different classification levels. When data is transferred from the physically secured 802.3 LAN to the FDDI LAN, it is labeled at the classification level of the LAN, protected against modification, and encrypted by a security protocol contained within the relay. (If the hosts could be trusted to process a range of classification levels (MLS hosts), then the 802.3 LAN could operate in an MLS security processing mode and the secure relay could accept a range of classification levels from the 802.3 LAN.)

3.1.2 MLS 802.3 LANs

With the MLS 802.3 LANs, individual hosts operate in a systems high processing mode, but at different classification levels. (Again this discussion assumes that the hosts cannot be trusted to protect different classification levels of data.) Each host has a security protocol that labels data at the classification level of the host, protects it against modification, and encrypts it for transmission over the 802.3 LAN. The security protocol also checks the classification level of incoming data to see if it can be accepted by the host. In this way, the systems high hosts collectively form an MLS 802.3 LAN using the security protocols associated with each host. (If the hosts could be trusted to process a range of classification levels (MLS hosts), then the security protocol could accept a range of classification levels from the host). In this situation, data can be transferred transparently through the relay from the MLS 802.3 LAN to the FDDI LAN.

3.1.3 Exchanges Among 802.3 LANs

In addition to illustrating the allocation of security protocols, Figure 3.1-1 identifies three cases for how data can flow over the FDDI backbone between the 802.3 LANs:

- Between physically secured LANs – corresponding security protocols lie in relays
- Between a physically secured LAN and an MLS LAN – corresponding security protocols lie in relay and host
- Between MLS LANs – corresponding security protocols lie in hosts.

The existence of these three cases raises a question — which case would be most appropriate for conducting this study. To answer this question requires that the impact on delivery time for different placement options in hosts, front ends and relays be analyzed. This is done qualitatively in the following section.

3.2 Delay as a Function of Placement Options / Network Components

This section analyzes in qualitative terms the impact on delivery time of different placement options for security protocols within the following types of network components:

- Hosts
- Front ends
- Relays.

3.2.1 Delay as a Function of Placement Options for Hosts

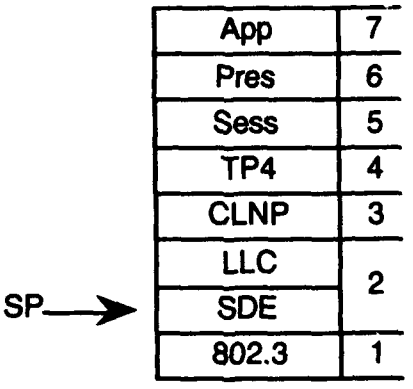
Figure 3.2.1-1(a,b and c) illustrates host stacks that each use a different type of security protocol at different layers. SDE is used at layer 2 in Figure 3.2.1-1a; NLSP is used at layer 3 in Figure 3.1.1-1b; while TLSP is used at layer 4 in Figure 3.2.1-1c. The host processing delay is relatively insensitive to the layer at which a security protocol is placed because:

- Each host processes data only once at each of the seven OSI layers using the same OSI communications protocol
- Each host incorporates a single security protocol. Although these security protocols (SDE, NLSP, and TLSP) are of different types, each performs similar functions, such as: generating protected headers, clear headers, padding and integrity check values (ICVs), as well as, encryption of data.

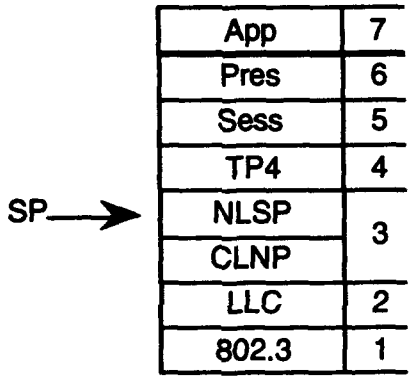
The following factors will however give rise to minor differences in the host processing delays:

- Small differences in processing delays are inevitable because of the differences in the amount of processing required for different security protocols.
- Processing of ICVs and encryption at lower layers take longer because the service data units (SDUs) are larger and have more headers.

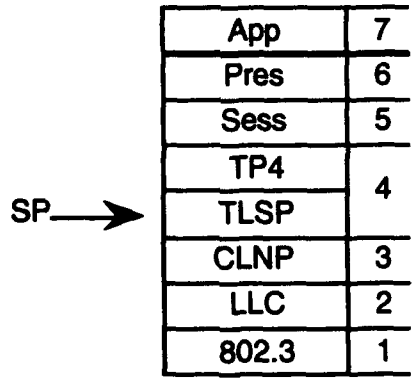
In conclusion, the processing delay in a host is relatively insensitive to the layer at which its security protocol is implemented.



a. Host with SDE



b. Host with NLSP



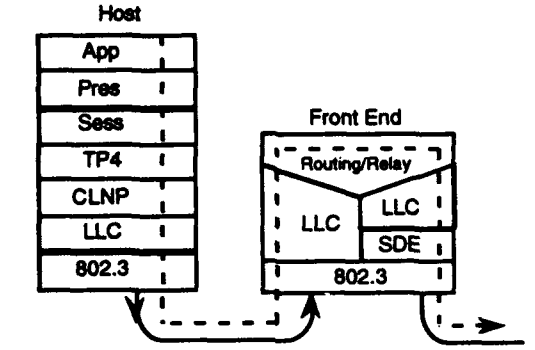
c. Host with TLSP

SP = Security Protocol

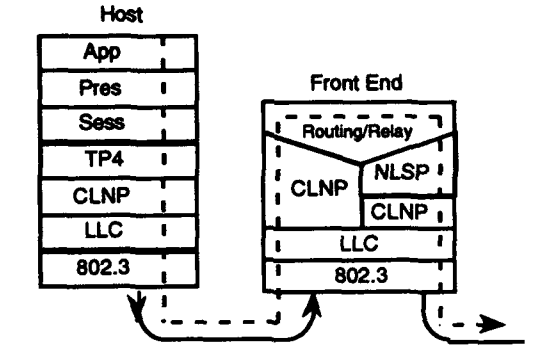
Figure 3.2.1–1. *Comparison of Delay through Secure Hosts*

3.2.2 Delay as a Function of Placement Options for Host Front Ends

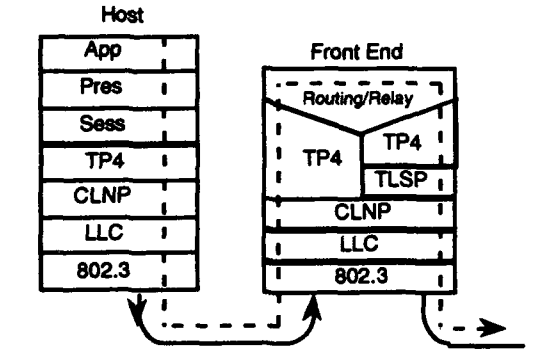
Figure 3.2.2-1 illustrates three identical hosts that each use different secure front ends. These secure front ends allow the hosts to be connected to a secure network without modifying the host (transparent connection to network). Each of these secure front ends uses a different type of security protocol at a different layer. In Figure 3.2.2-1a, the front end uses SDE at layer 2, while in Figure 3.2.2-1b, NLSP is used at layer 3. TLSP is used at layer 4 with the front end shown in Figure 3.2.2-1c.



a. SDE Front End



b. NLSP Front End



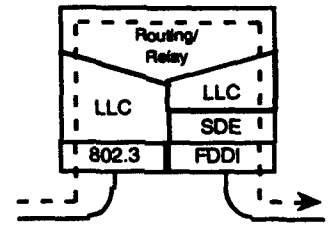
c. TLSP Front End

Figure 3.2.2–1. *Comparison of Delay through Secure Front Ends*

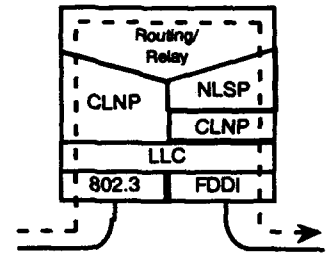
The processing delay associated with a secure front end is sensitive to the layer at which its security protocol is located. When its security protocol is placed at a higher layer, the processing delay is greater. This results from the processing of additional OSI communications protocols within front ends that use security protocols at higher layers. This additional delay occurs on both sides of the secure front end. This effect can be observed in Figure 3.2.2-1b. In this case, the secure NLSP front end must process CLNP headers on the host and network sides that are not processed by the secure SDE front end in Figure 3.2.2-1a. In Figure 3.2.2-1c, the secure TLSP front end must also process TP4 headers on the host and network sides in a manner similar to the secure NLSP front end. The result is that greater processing delays occur in front ends that use security protocols at higher layers.

3.2.3 Delay as a Function of Placement Options for Relays

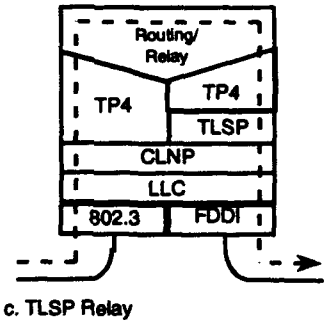
Figure 3.2.3-1 illustrates three relays that each use a different type of security protocol at a different layer. In Figure 3.2.3-1a, the relay uses SDE at layer 2. In Figure 3.2.3-1b, NLSP is used at layer 3. TLSP is used at layer 4 in the relay shown in Figure 3.2.3-1c.



a. SDE Bridge



b. NLSP Router



c. TLSP Relay

Figure 3.2.3–1. *Comparison of Delay through Secure Relays*

The processing delay associated with a secure relay is sensitive to the OSI layer at which its security protocol is located. When its security protocol is placed at a higher layer, its processing delay is increased. This results from the processing of additional OSI communications protocols within relays that use security protocols at higher layers. This additional delay occurs on both sides of the secure relay. This effect can be observed in Figure 3.2.3-1b. In this case, the secure NLSP relay must process CLNP headers on both sides because these are not processed by the secure SDE relay as in Figure 3.2.3-1a. In Figure 3.2.3-1c, the secure TLSP relay must also process TP4 headers on both sides in a manner similar to the secure NLSP relay. The result is that greater processing delays occur in relays that use security protocols at higher layers.

3.2.4 Summary Observations Regarding Delay

Based upon the analysis presented in Section 3.2, the following observations regarding the impact on delivery time, as a result of placing security protocols at different layers within hosts, front ends, and relays, can be summarized as follows:

- Host processing delay is relatively insensitive to the choice of which layer the security protocols is placed.
- Processing delay within a front end or relay is increased when security protocols are placed at higher layers.

3.3 Selection of Preferred Network Configurations for Study

A network configuration that incorporates security protocols in relays has been identified for this study since:

- It has two network components (the two relays) that are each sensitive to the layer at which security is placed [host-to-relay and host-to-host configurations include one component and no components, respectively, that are sensitive to where security is placed (assuming the hosts do not use front ends).
- It addresses a configuration that is potentially useful to the Navy in the near term. Using secure relays to interconnect physically secured LANs at the Top Secret / Sensitive Compartmented Information TS / SCI and SECRET level over an FDDI backbone is potentially more cost-effective than incorporating security protocols in every workstation.

This network configuration is further divided into three cases in which the secure relay is either a bridge, router or transport relay. The specific allocation of communications and security protocols to the various network components for each of these cases is shown in Figures 3.3-1a, 3.3-1b, and 3.3-1c.

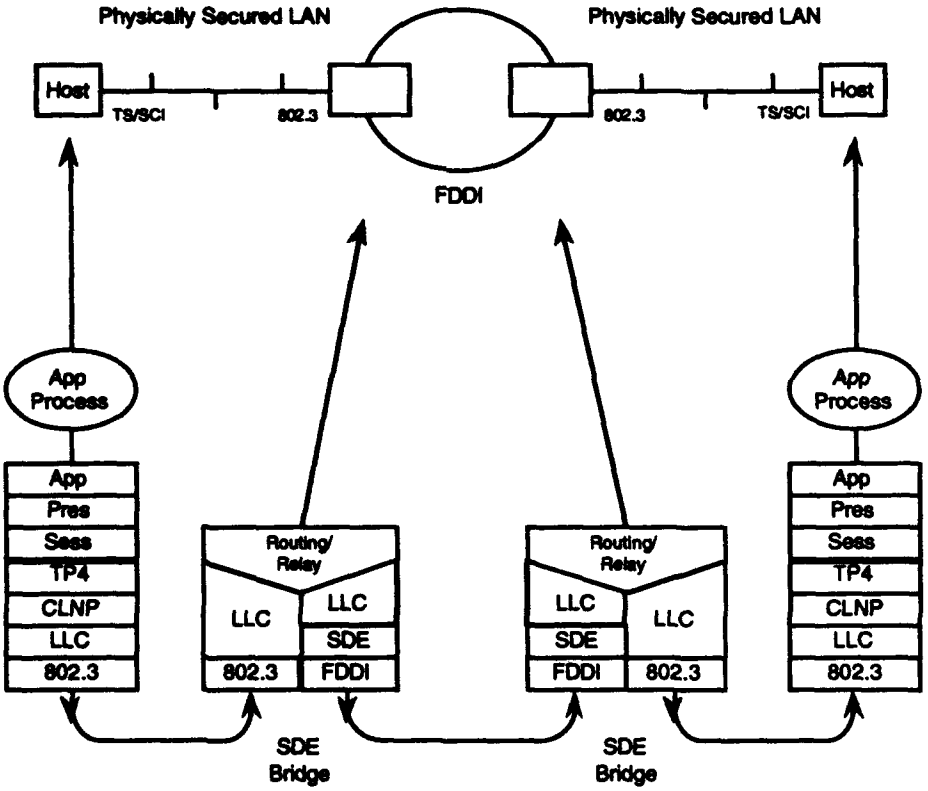


Figure 3.3–1a. *Network Configuration with Secure Bridges*

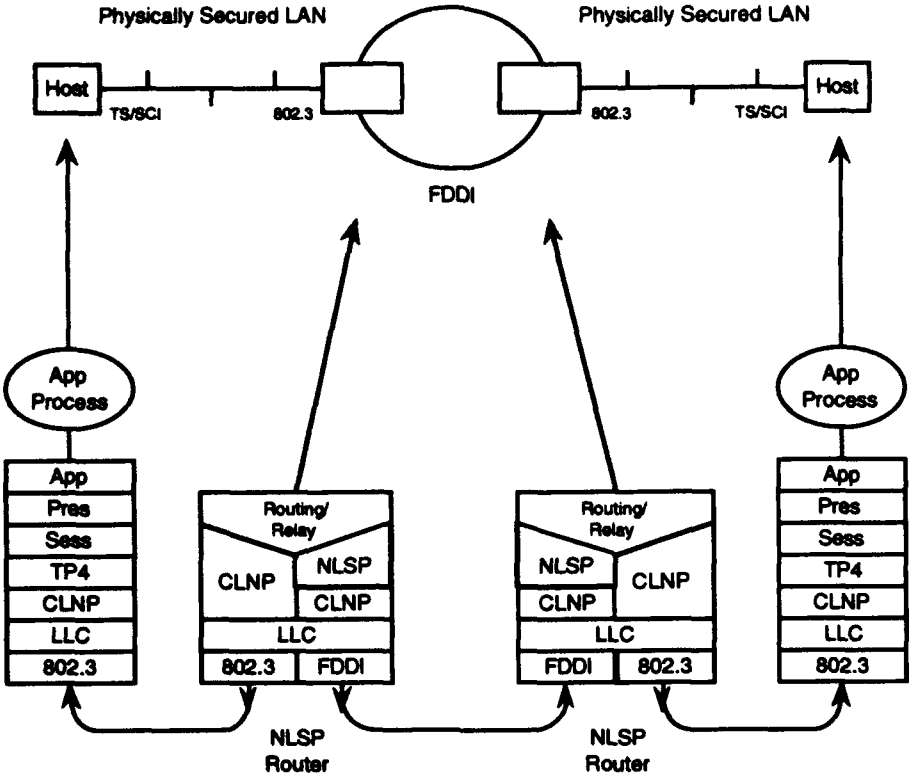


Figure 3.3–1b. *Network Configuration with Secure Routers*

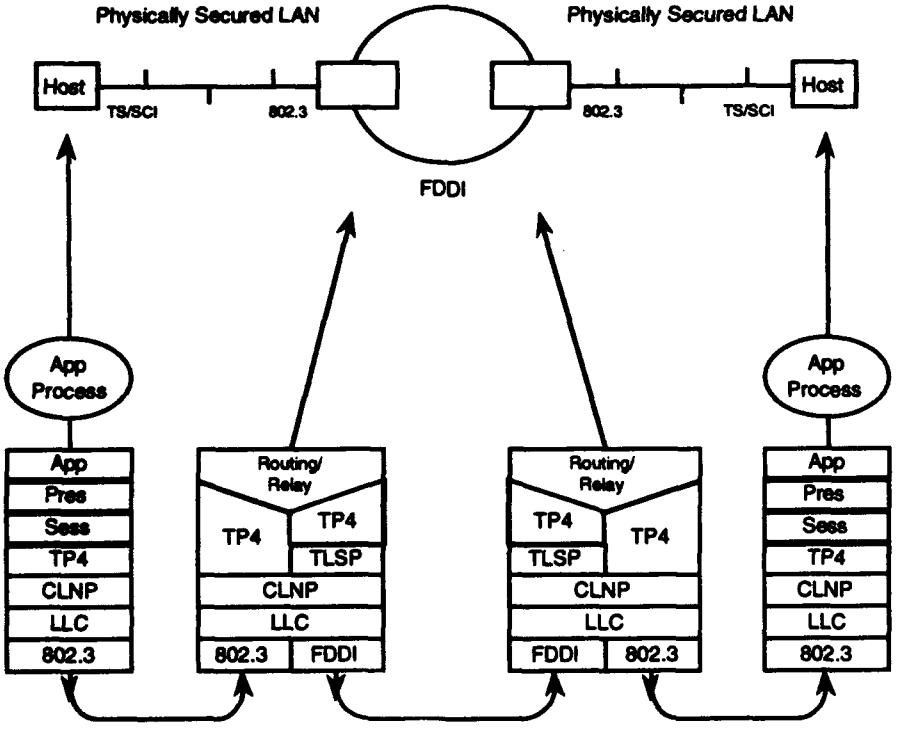


Figure 3.3–1c. *Network Configuration with Secure Transport Relays*

This Page Intentionally Left Blank

Section 4
Mathematical Model for Computing Delivery Time

4.0 Mathematical Model for Computing Delivery Time

The delivery time for traversing the internetwork shown in Figure 4.0-1 is given by:

$$T_{delivery\text{-}time} = T_{host}(down) + T_{802.3} + T_{relay}(802.3\text{-}to\text{-}FDDI,SP) + T_{FDDI} + T_{relay}(FDDI\text{-}to\text{-}802.3,SP) + T_{802.3} + T_{host}(up)$$

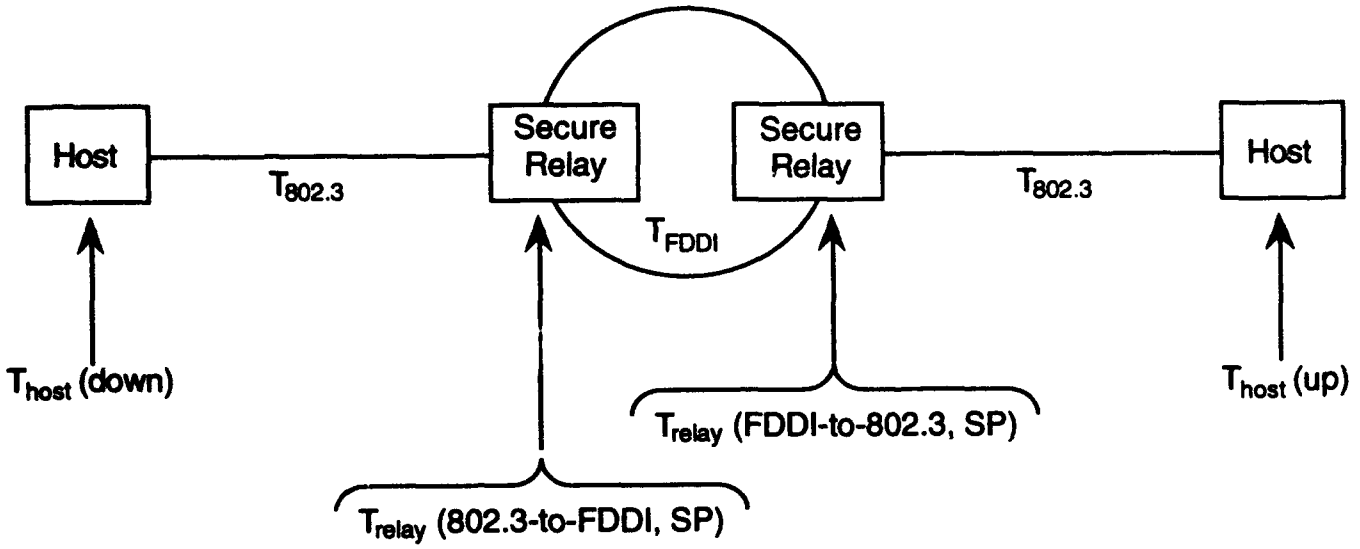


Figure 4.0–1. Mathematical Model for Computing Delivery Time

where

$T_{relay}(802.3\text{-}to\text{-}FDDI,SP)$ =	Average time that relay takes to internally process data from time it is received on 802.3 LAN to time it is ready for transmission on FDDI LAN
$T_{relay}(FDDI\text{-}to\text{-}802.3,SP)$ =	Average time that relay takes to internally process data from time it is received on FDDI LAN to time it is ready for transmission on 802.3 LAN
$T_{host}(down)$ =	Average interval from time that data is first passed down to the application layer from the application process to time that a frame is ready for transmission over the 802.3 LAN
$T_{802.3}$ =	Average time to exchange frame between host and relay over 802.3 LAN
T_{FDDI} =	Average time needed to transfer frame between relays over FDDI LAN
$T_{host}(up)$ =	Average interval from time that data is first received at host from 802.3 LAN to time that data is ready for application process at destination
SP =	Parameter representing security protocol within relay that can take on the values — SDE, NLSP or TLSP
up =	Parameter indicating that data is moving up stack
down =	Parameter indicating that data is moving down stack.

The following subsections provide specific formulas for $T_{host}(down)$, $T_{host}(up)$, $T_{relay}(802.3,FDDI,SP)$, $T_{relay}(FDDI,802.3,SP)$, $T_{802.3}$ and T_{FDDI}. The notation that follows is used throughout these subsections:

$T_{down}(x)$ = Average time taken by protocol x to generate its headers / trailers and prepend / postpend them to the service data unit (SDU) from the layer above. Security protocols can also insert padding, compute an integrity check value (ICV), and perform encryption.

$T_{down}(x,y)$ = Average waiting time in queue for SDUs that are transferred across a layer boundary from protocol x (layer above) to protocol y (layer below); or from a relay / routing function to the uppermost protocol. For some layer boundaries and implementations this delay may not exist (equals zero), since adjacent protocols process data immediately without the data having entered a queue.

$T_{up}(x)$ = Average time taken by protocol x to process its received headers / trailers and remove them. Security protocols can also remove padding, re-compute ICVs, and perform decryption.

$T_{up}(x,y)$ = Average waiting time in queue for SDUs that are transferred across layer boundary from protocol x (layer below) to protocol y (layer above); or from the uppermost protocol to the relay / routing function. For some layer boundaries and implementations this delay may not exist (equals zero), since adjacent protocols process data immediately without the data having entered a queue.

x,y = Parameters used to represent protocol entities or a relay / routing function; parameters can take on values: 802.3, SDE, LLC, CLNP, NLSP, TLSP, TP4, sess, pres, appl, or relay.

4.1 Host Processing Delays

The host processing delay represents the time that a host takes to internally process data. There are two host processing delays — one at the source host and one at the destination host.

4.1.1 Source Host Processing Delay, $T_{host}(down)$

The source host processing delay, $T_{host}(down)$, is given by:

$$T_{host}(down) = T_{down}(appl) + T_{down}(appl,pres) + T_{down}(pres) + T_{down}(pres,sess) + T_{down}(sess) + T_{down}(sess,TP4) + T_{down}(TP4) + T_{down}(TP4,CLNP) + T_{down}(CLNP) + T_{down}(CLNP,LLC) + T_{down}(LLC) + T_{down}(LLC,802.3) + T_{down}(802.3).$$

4.1.2 Destination Host Processing Delay, $T_{host}(up)$

The destination host processing delay, $T_{host}(up)$, is given by:

$$T_{host}(up) = T_{up}(802.3) + T_{up}(802.3,LLC) + T_{up}(LLC) + T_{up}(LLC,CLNP) + T_{up}(CLNP) + T_{up}(CLNP,TP4) + T_{up}(TP4) + T_{up}(TP4,sess) + T_{up}(sess) + T_{up}(sess,pres) + T_{up}(pres) + T_{up}(pres,app) + T_{up}(app).$$

4.2 Processing Delay through Relays

The processing delay through a relay represents the time interval that a relay takes to internally process data from the time it is received to the time it is ready for transmission. This processing delay is analyzed for the following three cases:

- A secure SDE bridge
- A secure NLSP router
- A secure TLSP relay.

4.2.1 Processing Delay through a Secure Bridge

The network under investigation uses two secure relays. For a given direction of transmission, one relay receives frames from an 802.3 LAN and forwards them over an FDDI LAN; the other receives frames on the FDDI LAN and forwards them over the 802.3 LAN. Each of these cases is covered below .

4.2.1.1 From 802.3 to FDDI over Secure Bridge

The processing delay through a secure SDE bridge that receives frames from an 802.3 LAN and forwards them over an FDDI LAN is given by:

$$\begin{aligned} T_{relay}(\text{802.3-to-FDDI, SDE}) = {} & T_{up}(\text{802.3}) + T_{up}(\text{802.3,LLC}) \\ & + T_{up}(\text{LLC}) + T_{up}(\text{LLC,relay}) \\ & + T_{relay} + T_{down}(\text{relay,LLC}) \\ & + T_{down}(\text{LLC}) + T_{down}(\text{LLC,SDE}) \\ & + T_{down}(\text{SDE}) + T_{down}(\text{SDE,FDDI}) \\ & + T_{down}(\text{FDDI}). \end{aligned}$$

4.2.1.2 From FDDI to 802.3 over Secure Bridge

The processing delay through a secure SDE bridge that receives frames from an FDDI LAN and forwards them over an 802.3 LAN is given by:

$$\begin{aligned} T_{relay}(\text{FDDI-to-802.3, SDE}) = {} & T_{up}(\text{FDDI}) + T_{up}(\text{FDDI,SDE}) \\ & + T_{up}(\text{SDE}) + T_{up}(\text{SDE,LLC}) \\ & + T_{up}(\text{LLC}) + T_{up}(\text{LLC,relay}) \\ & + T_{relay} + T_{down}(\text{relay,LLC}) \\ & + T_{down}(\text{LLC}) + T_{down}(\text{LLC,802.3}) \\ & + T_{down}(\text{802.3}). \end{aligned}$$

4.2.2 Processing Delay through Secure Router

The processing delay through a secure NLSP router is covered for two cases: frames flowing from 802.3 to FDDI, and from FDDI to 802.3.

4.2.2.1 From 802.3 to FDDI over Secure Router

The processing delay through a secure NLSP router that receives frames from an 802.3 LAN and forwards them over an FDDI LAN is given by:

$$\begin{aligned} T_{relay}(\text{802.3-to-FDDI, NLSP}) = {} & T_{up}(\text{802.3}) + T_{up}(\text{802.3,LLC}) \\ & + T_{up}(\text{LLC}) + T_{up}(\text{LLC,CLNP}) \\ & + T_{up}(\text{CLNP}) + T_{up}(\text{CLNP,relay}) \\ & + T_{relay} + T_{down}(\text{relay,CLNP}) \\ & + T_{down}(\text{CLNP}) + T_{down}(\text{CLNP,NLSP}) \\ & + T_{down}(\text{NLSP}) + T_{down}(\text{NLSP,LLC}) \\ & + T_{down}(\text{LLC}) + T_{down}(\text{LLC,FDDI}) \\ & + T_{down}(\text{FDDI}). \end{aligned}$$

4.2.2.2 From FDDI to 802.3 over Secure Router

The processing delay through a secure NLSP router that receives frames from an FDDI LAN and forwards them over an 802.3 LAN is given by:

$$\begin{aligned} T_{relay}(\text{FDDI-to-802.3, NLSP}) = {} & T_{up}(\text{FDDI}) + T_{up}(\text{FDDI,LLC}) \\ & + T_{up}(\text{LLC}) + T_{up}(\text{LLC,NLSP}) \\ & + T_{up}(\text{NLSP}) + T_{up}(\text{NLSP,CLNP}) \\ & + T_{up}(\text{CLNP}) + T_{up}(\text{CLNP,relay}) \\ & + T_{relay} + T_{down}(\text{relay,CLNP}) \\ & + T_{down}(\text{CLNP}) + T_{down}(\text{CLNP,LLC}) \\ & + T_{down}(\text{LLC}) + T_{down}(\text{LLC,802.3}) \\ & + T_{down}(\text{802.3}). \end{aligned}$$

4.2.3 Processing Delay through Secure Transport Relay

The processing delay through a secure TLSP relay is covered for two cases: frames flowing from 802.3 to FDDI, and from FDDI to 802.3.

4.2.3.1 From 802.3 to FDDI over Secure Transport Relay

The processing delay through a secure TLSP relay that receives frames from an 802.3 LAN and forwards them over an FDDI LAN is given by:

$$\begin{aligned} T_{relay}(\text{802.3-to-FDDI, TLSP}) = {} & T_{up}(\text{802.3}) + T_{up}(\text{802.3,LLC}) \\ & + T_{up}(\text{LLC}) + T_{up}(\text{LLC,CLNP}) \\ & + T_{up}(\text{CLNP}) + T_{up}(\text{CLNP,TP4}) \\ & + T_{up}(\text{TP4}) + T_{up}(\text{TP4,relay}) \\ & + T_{relay} + T_{down}(\text{relay,TP4}) \\ & + T_{down}(\text{TP4}) + T_{down}(\text{TP4,TLSP}) \\ & + T_{down}(\text{TLSP}) + T_{down}(\text{TLSP,CLNP}) \\ & + T_{down}(\text{CLNP}) + T_{down}(\text{CLNP,LLC}) \\ & + T_{down}(\text{LLC}) + T_{down}(\text{LLC,FDDI}) \\ & + T_{down}(\text{FDDI}). \end{aligned}$$

4.2.3.2 From FDDI to 802.3 over Secure Transport Relay

The processing delay through a secure TLSP relay that receives frames from an FDDI LAN and forwards them over an 802.3 LAN is given by:

$$\begin{aligned} T_{relay}(\text{FDDI-to-802.3, TLSP}) = {} & T_{up}(\text{FDDI}) + T_{up}(\text{FDDI,LLC}) \\ & + T_{up}(\text{LLC}) + T_{up}(\text{LLC,CLNP}) \\ & + T_{up}(\text{CLNP}) + T_{up}(\text{CLNP,TLSP}) \\ & + T_{up}(\text{TLSP}) + T_{up}(\text{TLSP,TP4}) \\ & + T_{up}(\text{TP4}) + T_{up}(\text{TP4,relay}) \\ & + T_{relay} + T_{down}(\text{relay,TP4}) \\ & + T_{down}(\text{TP4}) + T_{down}(\text{TP4,CLNP}) \\ & + T_{down}(\text{CLNP}) + T_{down}(\text{CLNP,LLC}) \\ & + T_{down}(\text{LLC}) + T_{down}(\text{LLC,802.3}) \\ & + T_{down}(\text{802.3}). \end{aligned}$$

4.3 Delays Across LANs

The average delay across a LAN represents the interval from the time a frame is ready for transmission at the source to the time it is received at the destination. There are two such delays — one across 802.3 LANs and one across FDDI LANs.

4.3.1 Delay Across 802.3 LAN, $T_{802.3}$

The average time needed to exchange a frame between host and relay over an 802.3 LAN is given by:

$$T_{802.3} = T_{802.3}(access) + T_{802.3}(trans) + T_{802.3}(prop)$$

where

$T_{802.3}(access)$ = Average time needed to successfully gain access to an 802.3 LAN. To transfer a frame over an 802.3 LAN, a STATION must wait until the LAN becomes idle. When it does attempt to transmission, another STATION may do the same. If two stations transmit at the same time, a collision occurs. Each station must then wait a random time interval before attempting a retransmission. To successfully gain access to an 802.3 LAN, a station must therefore transmit its frame before other stations do so. If it transmits the frame for a sufficiently long time, the other stations on the LAN will detect that the LAN is being used and will not attempt a transmission. When this occurs a station has successfully gained access to the LAN.

$T_{802.3}(trans)$ = Time taken to transmit frame over 802.3 LAN

= Length of frame in bits / transmission rate in bits per second

= Length of frame in bits / 10 Mbps

$T_{802.3}(prop)$ = Time taken for the first bit emitted by transmitter to arrive at the receiver over the 802.3 LAN

= Propagation delay across 802.3 LAN transmission media.

4.3.2 Delay Across FDDI LAN

The average time needed to exchange a frame between relays over an FDDI LAN is given by:

$$T_{FDDI} = T_{FDDI}(access) + T_{FDDI}(trans) + T_{FDDI}(prop)$$

where

$T_{FDDI}(access)$ = Average time needed to successfully gain access to an FDDI LAN. (To transfer a frame on an FDDI LAN, a station must first wait until a token can be seized at its interface unit).

$T_{FDDI}(trans)$ = Time taken to transmit frame over FDDI LAN

= Length of frame in bits / transmission rate in bits per second

= Length of frame in bits / 100 Mbps

$T_{FDDI}(prop)$ = Time taken for first bit emitted by transmitter to arrive at the receiver over FDDI LAN

= Propagation delay across FDDI LAN (includes propagation delay across fiber optic simplex links as well as the delays introduced within the interface units.

Section 5
Overview of Related Work

5.0 Overview of Related Work

This section describes the research and methods undertaken to complete Task 1 of this SBIR effort. This research was based upon using a search strategy that to examine basic keywords, such as: OSI, protocol, network, LAN, router, and bridge. The results of these queries were refined using additional keywords such as performance, delay, time, security, analysis, simulation, and testing. Finally, a combinations of the keywords were used to further refine the results. The following reference sources were searched:

- Book search
- Periodical / proceedings / papers search
- Defense Technical Information Center (DTIC) search
- Internet search
- Vendor research.

5.1 Book Search

The book search was performed at the University of California San Diego library (UCSD), Monmonth College library, various on-line libraries available on the Internet, the San Diego Technical Bookstore, and Secure Solutions' technical reference library using the keyword search methodology. Bibliographies were also checked for additional resources. The following books were identified for potential use in conducting this task:

- Albert, Bernard, FDDI and FDDI-II: Architecture, Protocols, and Performance.
- Baker, Donald G., Local Area Networks with Fiber Optic Applications, Prentice-Hall, Englewood Cliffs, NJ, 1986. Addresses performance and theoretical aspects of fiber optic LANs.
- Bertsekas, Dimitri, and Gallager, Robert, Data Networks, Prentice-Hall, Englewood Cliffs, NJ, 1992.
- Black, Uyless, Data Networks - Concepts, Theory and Practice, Prentice-Hall, Englewood Cliffs, NJ, 1992.
- Conway, Adrian E., and Georgonas, Nicoles D., Queuing Networks - Exact Computational Algorithms: A Unified Theory Based on Decomposition and Aggregation, MIT Press, Cambridge MA, 1989. This book includes a queuing model for OSI communications architectures in Section 2.3.9.
- Daigle, John, Queuing Theory for Telecommunications, Addison-Wesley Publishing Company, Reading MA, 1991.
- Driver Performance: Measurement And Modeling, IVHS, Information Systems, and Simulation. Washington, D.C.: National Academy Press, 1993.
- Fortier, Paul J., Design & Analysis of Distributed Real-time Systems, Intertext Publications, McGraw-Hill, New York, NY, 1985.

- Fortier, Paul J., editor, Modeling and Analysis of Local Area Networks, CRC Press, 1990.
- Fortier, Paul J., Modeling and Analysis of Local Area Networks, Springer-Verlag, 1989.
- Hammond, Joseph L., and O'Reiley, Peter J., Performance Analysis of Local Computer Networks, Addison-Wesley, 1986.
- Hayes, Jeremiah, F., Modeling and Analysis of Computer Communications Networks, Plenum Press, New York, 1984.
- Jeruchim, Michel C., Simulation of Communications Systems, Plenum, New York, 1992.
- Kanuri, Nanda K., CSMA/CD LAN Performance: Modeling and Simulation in CSIM. 1989.
- Keiser, Gerd E., Local Area Networks, McGraw-Hill, New York, NY, 1989.
- Kleinrock, Leonard. Communication Nets; Stochastic Message Flow and Delay. New York, McGraw-Hill, 1964.
- Kummerle, Karl; Limb, John O.; and Tobagi, Fouad A., Advances in Local Area Networks, IEEE Press, New York, 1987. This book includes a major section on LAN performance.
- Kurnool, Ramesh, 1965. Token bus LAN Performance: Modeling and Simulation, 1990.
- Network Modeling, Simulation, and Analysis. Electrical Engineering and Electronics; 61. New York: M. Dekker, c1990.
- Pasupuleti, Pratap S., Dual token ring LAN Performance, IEEE, 1991.
- Perlman, Radia, Interconnections: Bridges and Routers, Addison-Wesley, Redwood City, CA, 1992. Addresses design, performance and theory of bridges and routers.
- Pickholtz, Raymond I., Local Area and Multiple Access Networks, Computer Science Press, Rockville MD, 1986. Addresses design, performance and measurement of LANs.
- Robertazzi, Thomas G., Computer Networks and Systems: Queuing Theory and Performance Evaluation, Springer-Verlag, New York, 1990.
- Schwartz, Mischa, Telecommunication Networks: Protocols, Modeling, and Analysis, Addison-Wesley Publishing Company, Menlo Park, CA, 1987.
- Stallings, William, Computer Communications: Architecture's, Protocols, and Standards, IEEE Computer Society Press, Los Alamos CA, 1992.
- Stallings, William, editor, Tutorial Local Network Technology, IEEE Computer Society Press, Silver Spring, MA, 1983. This book includes a paper entitled "A methodology for Predicting End-to-End Responsiveness in a Local Computer Network."

- Stallings, William, Local Networks an Introduction, Macmillan Publishing Company, 1984. This book includes a good general reference on LAN performance.
- Stuck, B, and Arthurs, E., A Computer and Communications Network Performance Analysis Primer, Prentice-Hall software series, 1985. Addresses performance and measurement of networks.

5.2 Periodicals / Proceedings / Papers Search

The periodicals / proceedings / papers search was performed at the UCSD library, Monmonth College library, various on-line libraries available on the Internet, and Secure Solutions' internal resources using the keyword search methodology. Bibliographies were also checked for additional resources. The following periodicals / proceedings / papers were identified for potential use in conducting this task:

- Bradner, Scott, Ethernet Bridges and Routers: Faster than Fast Enough, Data Communications, February 1992 v21 n3 p58(10).
- Brown, Carolyn, AT&T System Solution Links Ethernet and FDDI, Multiport Bridge Filters at 500,000 packets per second, Data Communication, August 1990 v19 n10 p128(3).
- Bux, W., Meister, B., and Wong, J. W., Bridges for Interconnection of Ring Networks – a Simulation Study, Information Processing '83. Proceedings of the IFIP 9th World Computer Congress, Paris, France, September 19-23, 1983 (Vol. 3); IFIP World Congress Series, Vol. 9; North Holland, New York, 1983.
- Denning, Peter, Communications of the ACM, October 1990, v33, n10. Entire issue is devoted to simulation and modeling.
- Estrin, Deborah, and Mitzel, Danny J., An assessment of state and lookup overhead in routers, Proceedings Title: One World through Communications (Vol. 3), IEEE Computer Society, 4-8 May 1992, Florence, Italy.
- Flanagan, Patrick, Multiprotocol Routers: an Overview, Telecommunications, April 1993 v27 n4 p19(4). This product may be pertinent to study.
- Greenfield, David, and Bradner, Scott, Building the Highway, PC Magazine, March 30 1993 v15 n6 p22(33).
- Greenfield, David, Speedy Routers for FDDI: Routers Get a Performance and Price Boost, Data Communications, June 1990 v19 n7 p58(3). Paper indicates that improved speed of the "newer" routers results from the establishment of shared memory space and the passing of small memory pointers to blocks of data rather that the data itself, the use of high-speed (300-Mbps-plus) buses, and fast 32-bit processors. This illustrates how internal processing delays are affected by the architecture of a relay.
- Kritzinger, P. S., "A Performance Model of the OSI Communications Architecture," IEEE Transactions on Communications, June 1986 v34 n6 p554(9). Bibliography identifies other pertinent references.

- Livingston, Dennis, "Avoid being fooled by bridge and router speed claims", Systems Integration, May 1991, v24, n5, p53(10). This article identifies several independent test organizations and includes phone numbers for vendors and Scott Bradner.
- Loudermilk, Stephen, Xyplex Unwraps Ethernet-to-FDDI Bridge / Router Pair, PC Week, August 23 1993 v10 n33 p54(1). This product may be pertinent to study.
- McCarthy, Vance, Xyplex bridges FDDI-to-Ethernet gap on desktop: also debuts low-cost hub for connecting work groups to a larger LAN, InfoWorld, March 15 1993 v15 n11 p41(1). This product may be pertinent to study.
- Metcalf, R. M., Boggs, D. R., "Ethernet: Distributed Packet Switching for Local Computer Networks," Communications of the ACM, July 1976. This is a classic paper on Ethernet performance.
- Mussich, Paula, Cisco Switching Hubs Pave Way for Migration to ATM, PC Week, March 7 1994 v11 n9 p33(2). This product may be pertinent to study.
- Mussich, Paula, Hughs Sketches Out Its Superhub Strategy, PC Week, March 21 1994 v11 n11 p47(1). This product may be pertinent to study.
- Tolly, Kevin, and Newman, David, High-end Routers: An In-depth Evaluation, Data Communications, December 1993 v22 n18 p68(12).
- Tolly, Kevin, Questioning Performance, Data Communications, April 1992, v21, n6, p39(2).
- Wallace, Bob, Hughs to Roll Out SNMP Modules, InfoWorld, March 14 1994 v16 n11 p3(1). This product that may be pertinent to study.
- Wexler, Joanie M., Router vendors vie for top performance: Cisco slips in some categories but maintains overall consistency across various protocols, Computerworld, June 8 1992 v26 n23 p59(1). Article indicates that Harvard University runs independent multiprotocol bridge / router throughput tests annually and that Scott Bradner is a full-time consultant to Harvard.
- Wilson, Jane, Bridge links LANs to FDDI: Fibermux's Ethernet bridge has 60,000-pps speed, InfoWorld, Feb 8 1993 v15 n6 p30(1). This product may be pertinent to study.
- Wilson, Jayne, Bridging router has 100,000-pps throughput, InfoWorld, March 8 1993 v15 n10 p38(1). This router supports FDDI and Ethernet LANs.

5.3 Defense Technical Information Center (DTIC) Search

The Defense Technical Information Center (DTIC) search was performed at the DTIC office in Los Angeles area by DTIC personnel. The terms listed below were searched by the DTIC computer. Terms that were used to conduct this search included:

Analog Simulation
Bridge
Bridges
Capacitance Bridges
Circuit Interconnections
Command And Control Systems
Command Control Communications
Communications Networks
Computer Communications
Computer Gateways
Computer Networks
Computer Viruses
Computerized Simulation
Conferencing (Communications)
Cryptography
Data Links, Delay
Data Processing
Data Transmission Systems
Delay Circuits
Delay Lines
Delays
Digital Simulation
Electric Bridges
Electric Relays
Electronic Mail
Electronic Relays
Electronic Security
Hybrid Simulation
Impedance Bridges
Information Exchange
Information Systems
Information Transfer
Interconnect
Interconnected
Interconnecting
Interconnector
Interconnectors
Interoperability
Layer
Layers
Link
Links
Local Area Networks
Microwave Bridges
Network Layer
Open Systems Interconnection
OSI Security Architecture
OSI
Packet Switching
Polarized Relays
Protocol
Protocols
Relays
Router
Routers
Routing

Secure Communications
Security
Standards
Time Delay Relays
Wide Area Networks.
Secure Data
Standards
Tactical Data Systems
Transport Layer

The results of the DTIC searches were collected into a bibliography and sent to Secure Solutions.

5.4 Internet Search

The Internet was searched using a variety of methods, including file transfer protocol (FTP), gopher, world-wide-web (WWW), and MOSAIC. Searches were conducted using keywords such as OSI, protocol, communications, network, LAN, performance, routers, delay, bridges, etc. Results were refined with the knowledge and expertise gained from previous searches.

FTP searches involved logging into known locations such as: ds.internic.net, ftp.sura.net, nemo.ncsl.nist.gov, ftp.tis.com, etc and then searching for article names that fit the search criteria. This search was utilized when a document or previous search results from other methods pointed to an FTP site for further information.

Gopher searches utilized a menu and keyword search. The gopher utility is an electronic agent that communicates with other gopher agents throughout the internet. The gopher server displays a menu of services it knows about and presents these for the user to begin a search for items of interest. Note that all internet resources are available to gopher sites because updated information must be added to the gopher menu system.

The WWW is a hypertext menu system for user-friendly traversing through the internet and connects to other WWW servers. This is a much newer technology, so only a small percentage of all available internet resources are catalogued. Searches were conducted by selecting menu items related to the keywords.

To extended the search capabilities within WWW, MOSAIC was used in later stages. MOSAIC is an x-windows interface to WWW which provides a user-friendly interface and allows searches by user-defined keywords.

In addition to searching the Internet, a variety of special interest bulletin board system's (BBS's) were searched, including COMSEC, dissp, and nist. The search was performed by checking message sections, file names, and descriptions using the keyword search methodology.

Finally, E-mail requests were sent to authors and selected professors to assist in our search by requesting applicable information, doctoral research, and papers.

5.5 Vendor Research

Various vendors could be potentially contacted to acquire empirical test data relevant to this study. These include bridge / router vendors, embedded COMSEC module vendors, OSI host / workstation vendors, and independent test laboratories.

5.5.1 Bridge / Router Vendors

An article in Systems Integration magazine [ILIVI91] contains a table that identifies vendors (with phone numbers) that manufacture relays (bridges, routers and brouters). The table also identifies the protocols supported by these relays and their "packet forwarding rates." The inverse of the packet forwarding rate provides an estimate for what is called the "processing delay through relay" in this report. This table could be used to identify bridge / router vendors that have products which interconnect 802.3 and FDDI LANs.

5.5.2 Embedded COMSEC Module Vendors

The processing delay associated with security protocols can be decomposed into two elements: 1) the delay associated with generating clear headers, protected headers and padding, and 2) the cryptographic processing associated with the resultant PDU (excluding the clear header). The processing delay associated with the first element is much like the delay associated with general communication protocols and is roughly proportional to the size of the headers. The processing delay associated with the second element is proportional to the size of the overall PDU, excluding the clear header.

Vendors of embedded COMSEC modules can be contacted to determine estimates for the delay associated with using these modules to encrypt PDUs and to compute integrity check values for them. This would provide an estimate for the second timing element described previously. Although an FDDI LAN operates at a nominal transmission rate of 100 Mbps, this does not mean that the embedded COMSEC module will have to operate at this rate. Since an FDDI ring network can support up to 1000 stations along the ring, each station only gets a small percentage of time to transmit data. Stations will therefore have time (on the average) to encrypt frames before transmission opportunities arise. Data can therefore be collected for COMSEC modules that operate at higher data rates in order to arrive at estimates for the cryptographic processing delays associated with security protocols.

5.5.3 OSI Host / Workstation Vendors

Vendors of OSI host / workstation products can be contacted to determine if they have estimates for the delay associated with processing data through OSI stacks or processing delays for individual protocols.

5.5.4 Independent Test Laboratories

Independent test laboratories could be contacted to determine if they have estimates for the delays associated with LAN network configurations / components / individual protocols. Two of these test groups are the Performance Testing Alliance for Networks (PTAN) and Benchmarking Methodology Working Group (BMWG).

The PTAN was formed in 1990 by a group of vendors and users. The goal of PTAN is to "strive for consistent results in testing the same networking devices, adapters and software."

The BMWG Cambridge, MA, recommends standards for the Transmission Control Protocol / Internet Protocol (TCP / IP) community. BMWG is formulating the terminology and procedures for testing network-connecting devices and reporting the test results. BMWG is a unit of the Internet Engineering Task Force (IETF).

Scott Bradner chairs both the PTAN's bridges and routers committee and the BMWG. He can be reached at 10 Ware Street, Cambridge, MA 02138, (617) 495-3864. [LIVI91]

This Page Intentionally Left Blank

Section 6
Conclusions and Recommendations

6.0 Conclusions and Recommendations

This section contains the conclusions and recommendations for Task 1 of this Phase II SBIR effort.

6.1 Conclusions

Conclusions regarding the impact on host-to-host delivery time as a function of where security protocols are placed within OSI layers are as follows:

- Providing end-to-end security services, as opposed to link security services, improves (reduces) delivery time because security encapsulation / decapsulation functions are only performed at the source and destination host. When link security services are used, security encapsulation / decapsulation functions are performed repeatedly, thereby increasing the host-to-host delivery time for a given network configuration.
- In some situations, it is desirable to implement security services within relays (or host front ends). Implementation of security protocols at lower OSI layers in relays (or front ends) reduces the host-to-host delivery time (in qualitative terms), since fewer headers are processed within them.

6.2 Recommendations

The following recommendations are made from the standpoint of the delivery time evaluation factor:

- Whenever possible, the Navy should provide end-to-end security services by implementing security protocols at the top of layer three or higher within hosts. This will minimize the host-to-host delivery time in comparison to providing link security services.
- The results of this task should be factored into the systems / security engineering process that will be used under Task 4 of this effort which will define Naval requirements for secure network products.

This Page Intentionally Left Blank

Appendices

Appendix A – Acronyms

Appendix A –

Acronyms

ACK	Acknowledgment
ANSI	American National Standards Institute
AP	Application Process
ASCE	Association Control Service Element
ASE	Application Service Element
BBS	Bulletin Board System
BMWG	Benchmarking Methodology Working Group
CC	Connection Confirm
CCITT	International Telegraph and Telephone Consultative Committee
CD	Collision Detect
CFE	CANEWARE Front End
CLNP	Connectionless Network Protocol
COMSEC	Communications Security
COMPUSEC	Computer Security
COPP	Connection Oriented Presentation Protocol
COSP	Connection Oriented Session Protocol
COTP	Connection Oriented Transport Protocol
CR	Connection Request
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
DoD	Department of Defense
DSAP	Destination Service Access Point
DTIC	Defense Technical Information Center
ELF	Extremely Low Frequency
EHF	Extremely High Frequency
ES	End System
FDDI	Fiber Distributed Data Interface
FOM	Figure of Merit

Acronyms (continued)

FTP	File Transfer Protocol
HDLC	High-level Data Link Control
ICV	Integrity Check Value
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INFOSEC	Information Security
IS	International Standard
ISO	International Standards Organization
LAN	Local Area Network
LLC	Logical Link Control
LSAP	Link Service Access Point
MAC	Media Access Control
MLS	Multi-level Security
MOE	Measure of Effectiveness
NES	Network Encryption System
NIU	Network Interface Unit
NIST	National Institute of Standards and Technology
NLSP	Network Layer Security Protocol
NRaD	Naval Research and Development Center
NSA	National Security Agency
NSAP	Network Service Access Point
OSI	Open Systems Interconnection
OSI RM	OSI Reference Model
PCI	Protocol Control Information
PDU	Protocol Data Unit
PPDU	Presentation PDU
PTAN	Performance Testing Alliance for Networks
QOS	Quality of Service

Acronyms (continued)

R & D	Research and Development
SA	Security Association
SAP	Service Access Point
SASE	Specific Application Service Element
SBIR	Small Business Innovative Research
SCI	Sensitive Compartmented Information
SDE	Secure Data Exchange
SDNS	Secure Data Network System
SDU	Service Data Unit
SESE	Security Exchange Service Element
SILS	Standard for Interoperable LAN Security
SMIB	Security Management Information Base
SNICP	Subnetwork-Independent Convergence Protocol
SPAWAR	Naval Space and Warfare Command
SPDU	Session PDU
SP3	Security Protocol 3
SP4	Security Protocol 4
SSAP	Source Service Access Point
TCP / IP	Transmission Control Protocol / Internetwork Protocol
TEK	Traffic Encryption Key
TLSP	Transport Layer Security Protocol
TNI	Trusted Network Interpretation
TPDU	Transport Protocol Data Unit
TP4	Transport Protocol Class 4
TS	Top Secret
TSAP	Transport Service Access Point
UCSD	University of California San Diego
WAN	Wide Area Network
WWW	World Wide Web

This Page Intentionally Left Blank

Appendix B – References

Appendix B – References

[BLACK 91] U. D. Black, *OSI – A Model for Computer Communications Standards*, Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[ANSI 87] American National Standards Institute, Fiber Distributed Data Interface (FDDI) — Token Ring Media Access Control (MAC), ANSI X3.139, 1987.

[ANSI 88] American National Standards Institute, Fiber Distributed Data Interface (FDDI) — Token Ring Physical Layer Protocol (PHY), ANSI X3.148, 1988.

[ANSI 90] American National Standards Institute, Fiber Distributed Data Interface (FDDI) — Token Ring Physical Layer Medium Dependent (PMD), X.3.166, 1990.

[CCITT 88C] The International Telegraph and Telephone Consultative Committee (CCITT), Network Service Definition of Open Systems Interconnection for CCITT Applications, Blue Book, Volume VIII, Fascicle VIII.4, Recommendation X.213, November 1988.

[CCITT 88D] The International Telegraph and Telephone Consultative Committee (CCITT), Transport Service Definition of Open Systems Interconnection for CCITT Applications, Blue Book, Volume VIII, Fascicle VIII.4, Recommendation X.214, November 1988.

[CCITT 88E] The International Telegraph and Telephone Consultative Committee (CCITT), Session Service Definition of Open Systems Interconnection for CCITT Applications, Blue Book, Volume VIII, Fascicle VIII.4, Recommendation X.215, November 1988.

[CCITT 88F] The International Telegraph and Telephone Consultative Committee (CCITT), Presentation Service Definition of Open Systems Interconnection for CCITT Applications, Blue Book, Volume VIII, Fascicle VIII.4, Recommendation X.216, November 1988.

[CCITT 88G] The International Telegraph and Telephone Consultative Committee (CCITT), Transport Protocol Specification for Open Systems Interconnection for CCITT Applications, Blue Book, Volume VIII, Fascicle VIII.5, Recommendation X.224, November 1988.

References (continued)

[CCITT 88H] The International Telegraph and Telephone Consultative Committee (CCITT), Session Protocol Specification for Open Systems Interconnection for CCITT Applications, Blue Book, Volume VIII, Fascicle VIII.5, Recommendation X.225, November 1988.

[CCITT 88I] The International Telegraph and Telephone Consultative Committee (CCITT), Presentation Protocol Specification for Open Systems Interconnection for CCITT Applications, Blue Book, Volume VIII, Fascicle VIII.5, Recommendation X.226, November 1988.

[CCITT 88P] The International Telegraph and Telephone Consultative Committee (CCITT), Primary Rate User Network Interface — Layer 1 Specification, Recommendation I.431, Blue Book, Volume III, Fascicle III.5, November 1988.

[Copernicus 91] Copernicus Project Office, Director, Space and Electronic Warfare, Office of the Chief of Naval Operations, The Copernicus Architecture, Phase I: Requirements Definition, August 1991.

[DoD 85] Department of Defense, Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD, December 1985.

[IEEE 91] IEEE Standard for Interoperable Local Area Network (LAN) Security, Part B — Secure Data Exchange Unapproved Draft IEEE Standard P802.10B/D7, IEEE LAN Security Working Group, November 9, 1991.

[ISO 84] International Standards Organization, Information Processing Systems — Open Systems Interconnection, Basic Reference Model, ISO 7498, October 1984.

[ISO 86A] International Standards Organization, Information Processing Systems — Open Systems Interconnection, Transport Service Definition, ISO 8072, June 1986.

[ISO 87A] International Standards Organization, Information Processing Systems — Data Communications, Network Service Definition, ISO 8348, April 1987.

[ISO 87D] International Standards Organization, Information Processing Systems — Open Systems Interconnection, Basic Connection Oriented Session Service Definition, ISO 8326, August 1987.

References (continued)

[ISO 87E] International Standards Organization, Information Processing Systems — Open Systems Interconnection, Basic Connection-Oriented Session Protocol Specification, ISO 8327, August 1987.

[ISO 87F] International Standards Organization, Information Processing Systems — Local Area Networks — Part 2: Logical Link Control, ISO 8802-2 , October 1987.

[ISO 88A] International Standards Organization, Information Processing Systems — Open Systems Interconnection, Internal Organization of the Network Layer, ISO 8648, February 1988.

[ISO 88B] International Standards Organization, Information Processing Systems — Data Communications, Network Service Definition — Addendum 2, Network Layer Addressing, ISO 8348 / AD 2, March 1988.

[ISO 88D] International Standards Organization, Information Processing Systems — Open Systems Interconnection, *Connection Oriented Presentation Service Definition*, ISO 8822, August 1988.

[ISO 88E] International Standards Organization, Information Processing Systems — Open Systems Interconnection, Connection Oriented Presentation Protocol, ISO 8823, August 1988.

[ISO 88F] International Standards Organization, Information Processing Systems — Data Communications, Network Service Definition — Addendum 3, Additional Features of Network Service, ISO 8348 / AD 3, October 1988.

[ISO 88H] International Standards Organization, Information Processing Systems — Open Systems Interconnection, Connection Oriented Transport Protocol Specification, ISO 8073, December 1988.

[ISO 88I] International Standards Organization, Information Processing Systems — Data Communications, Protocol for Providing the Connectionless-Mode Network Service, ISO 8473, December 1988.

[ISO 89A] International Standards Organization, Information Processing Systems—Open Systems Interconnection, Basic Reference Model — Part 2: Security Architecture, ISO 7498-2, February 1989.

References (continued)

[ISO 89E] International Standards Organization, Information Processing Systems — Fiber Distributed Data Interface (FDDI) — Part 1: Physical Layer Protocol (PHY), ISO 9314-1, April 1989.

[ISO 89H] International Standards Organization, Information Processing Systems — Fiber Distributed Data Interface (FDDI) — Part 2: Token Ring Media Access Control, ISO 9314-2, June 1989.

[ISO 90G] International Standards Organization, Information Processing Systems — Local Area Networks — Part 3: Carrier Sense Multiple Access with Collision Detection, Access Method and Physical Layer Specifications, ISO 8802-3, September 1990.

[ISO 90H] International Standards Organization, Information Processing Systems — Fiber Distributed Data Interface (FDDI) — Part 1: Physical Layer Medium Dependent (PMD), ISO 9314-3, October 1990.

[ISO 90I] International Standards Organization, Information Technology — Local Area Networks, MAC Service Definition, ISO 10039, October 1990.

[ISO 91B] International Standards Organization, Information Technology — Telecommunications and Information Exchange between Systems, Transport Layer Security Protocol, ISO / IEC 10736, June 1991.

[ISO 91D] International Standards Organization, Information Processing Systems — Local Area Networks — Part 3: Carrier Sense Multiple Access with Collision Detection, Access Method and Physical Layer Specifications — Amendment 3: Broadband Medium Attachment Unit and Broadband Medium Specification, Type 10BROAD36, ISO 8802-3 / AM 3, September 1991.

[ISO 91E] International Standards Organization, Information Processing Systems — Local Area Networks — Part 3: Carrier Sense Multiple Access with Collision Detection, Access Method and Physical Layer Specifications — Amendment 4: Physical Signaling, Medium Attachment and Baseband Medium Specifications, Type 1BASE5, ISO 8802-3 / AM 4, September 1991.

References (continued)

[ISO 91F] International Standards Organization, Information Processing Systems — Local Area Networks — Part 3: Carrier Sense Multiple Access with Collision Detection, Access Method and Physical Layer Specifications — Amendment 9: Twisted-Pair Medium Attachment Unit (MAU) and Baseband Medium, Type 10BASE-T, ISO 8802-3 / DAM 9, September 1991.

[ISO 91G] International Standards Organization, Information Technology — Telecommunications and Information Exchange between Systems, Network Layer Security Protocol, ISO 11577, November 1991.

[ISO 92C] International Standards Organization, Information Technology — Open Systems Interconnection, Network Layer Security Protocol, ISO 11577, 16 November 1993.

[ISO 92D] International Standards Organization, Information Technology — Telecommunications and Information Exchange between Systems, Transport Layer Security Protocol, ISO / IEC 10736, 1993.

[Lambert 89] P. A. Lambert, "Architectural Considerations for LAN Security Protocols," Local Area Network Security, Lecture Notes in Computer Science 396, Springer Verlag, 1989.

[Muftic 89] S. Muftic, Ellis Horwood Limited, Market Cross House, Cooper Street, Chichester, West Sussex, PO19 1EB, England, Security Mechanisms for Computer Networks, 1989.

[NIST 88] National Institute of Standards and Technology, Data Encryption Standard, FIPS PUB 46-1, January 1988.

[NIST 90] National Institute of Standards and Technology, Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols, NISTIR 90-4250, February 1990.

[NRaD 92] NRaD, Military Standard, Survivable Adaptable Fiber Optic Embeded Network, SAFENET, Military Handbook (Draft), January 1992.

[Rose 90] M. T. Rose, The Open Book — A Practical Perspective on OSI, Prentice Hall, Englewook Cliffs, New Jersey, 1990.

[SBIR 91] SBIR Topic N91-061, Placement of Network Security Services for Secure Data Exchange, Secure Solutions, Inc., 1991.

References (continued)

[SPAWAR 90] Space and Naval Warfare Systems Command, Warfare Systems Engineering Policy Division (SPAWAR 321) Computer Security Guidebook for Mission-Critical Computer Resources Managed under the Research, Development, and Acquisition Process, 26 October 1990.