IEEE Std 802.10a-1999
(Supplement to
IEEE Std 802.10-1998)

IEEE Standards for Local and Metropolitan Area Networks:

Supplement to Standard for Interoperable LAN/MAN Security (SILS)—

Security Architecture Framework

Sponsor

LAN MAN Standards Committee (LMSC)
of the
IEEE Computer Society

Approved 22 March 1999

IEEE-SA Standards Board

Abstract: An architectural description of the functions and location of SILS components is provided. The SILS components and their relationships to applications, communications protocols, system management, and security management are described.
Keywords: key management, secure data exchange, security association, security context, security protocol

---

The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, NY 10017-2394, USA

Print: ISBN 0-7381-1638-6 SH94730
PDF: ISBN 0-7381-1639-4 SS94730

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of all concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments on standards and requests for interpretations should be addressed to:

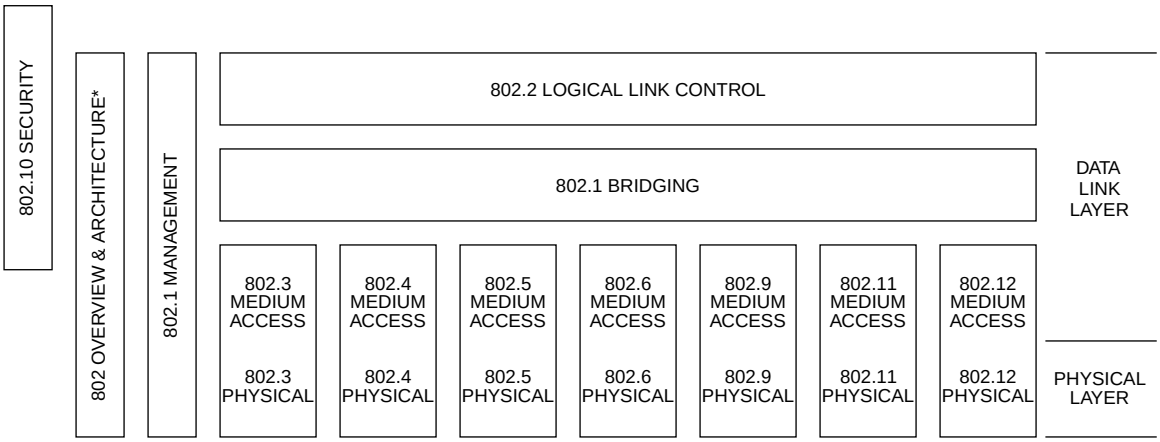
Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Introduction

[This introduction is not part of IEEE Std 802.10a-1999, IEEE Standards for Local and Metropolitan Area Networks: Supplement to Standard for Interoperable LAN/MAN Security (SILS)—Security Architecture Framework.]

This standard is part of a family of standards for local and metropolitan area networks. The relationship between the standard and other members of the family is shown below. (The numbers in the figure refer to IEEE standard numbers.)



* Formerly IEEE Std 802.1A.

This family of standards deals with the Physical and Data Link layers as defined by the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) Basic Reference Model (ISO/IEC 7498-1 : 1994). The access standards define seven types of medium access technologies and associated physical media, each appropriate for particular applications or system objectives. Other types are under investigation.

The standards defining the technologies noted above are as follows:

- IEEE Std 802 — *Overview and Architecture.* This standard provides an overview to the family of IEEE 802 Standards.
- ANSI/IEEE Std 802.1B and 802.1k [ISO/IEC 15802-2] — *LAN/MAN Management.* Defines an OSI management-compatible architecture, and services and protocol elements for use in a LAN/MAN environment for performing remote management.
- ANSI/IEEE Std 802.1D [ISO/IEC 15802-3] — *Media Access Control (MAC) Bridges.* Specifies an architecture and protocol for the interconnection of IEEE 802 LANs below the MAC service boundary.
- ANSI/IEEE Std 802.1E [ISO/IEC 15802-4] — *System Load Protocol.* Specifies a set of services and protocol for those aspects of management concerned with the loading of systems on IEEE 802 LANs.
- ANSI/IEEE Std 802.1F — *Common Definitions and Procedures for IEEE 802 Management Information*
- ANSI/IEEE Std 802.1G [ISO/IEC 15802-5] — *Remote Media Access Control (MAC) Bridging.* Specifies extensions for the interconnection, using non-LAN communication technologies, of geographically separated IEEE 802 LANs below the level of the logical link control protocol.
- ANSI/IEEE Std 802.2 [ISO/IEC 8802-2] — *Logical Link Control*
- ANSI/IEEE Std 802.3 [ISO/IEC 8802-3] — *CSMA/CD Access Method and Physical Layer Specifications*

- ANSI/IEEE Std 802.4 [ISO/IEC 8802-4] *Token Passing Bus Access Method and Physical Layer Specifications*
- ANSI/IEEE Std 802.5 [ISO/IEC 8802-5] *Token Ring Access Method and Physical Layer Specifications*
- ANSI/IEEE Std 802.6 [ISO/IEC 8802-6] *Distributed Queue Dual Bus Access Method and Physical Layer Specifications*
- ANSI/IEEE Std 802.9 [ISO/IEC 8802-9] *Integrated Services (IS) LAN Interface at the Medium Access Control (MAC) and Physical (PHY) Layers*
- ANSI/IEEE Std 802.10 *Interoperable LAN/MAN Security*
- ANSI/IEEE Std 802.11 [ISO/IEC DIS 8802-11] *Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications*
- ANSI/IEEE Std 802.12 [ISO/IEC 8802-12] *Demand Priority Access Method, Physical Layer and Repeater Specifications*

In addition to the family of standards, the following is a recommended practice for a common Physical Layer technology:

- IEEE Std 802.7 *IEEE Recommended Practice for Broadband Local Area Networks*

The following additional working group has authorized standards projects under development:

- IEEE 802.14 *Standard Protocol for Cable-TV Based Broadband Communication Network*

Conformance test methodology

An additional standards series, identified by the number 1802, has been established to identify the conformance test methodology documents for the 802 family of standards. Thus, the conformance test documents for 802.3 are numbered 1802.3.

IEEE 802.10a-1999

The IEEE 802.10 LAN/MAN Security Working Group has prepared this Security Architecture Framework, Clause 1, supplement as a necessary part of defining how security services are managed and provided to applications requiring secure LAN/MAN communications. The general definitions provided are usable and compatible with direct or indirect (via relay systems) WAN secure communications.

When the IEEE 802.10 Working Group approved this standard, it had the following membership:

Kenneth G. Alonge, *Chair*
Russell D. Housley, *Vice Chair*

Wen Pai Lu
Joseph G. Maley
Richard K. McAllister
Robert Zamparo

The following former members of the IEEE 802.10 Working Group made significant contributions to the material incorporated in this revision document:

L.Kirk Barker
James Coyle
Wen-Pai Lu
Noel Nazario
Brian Phillips
Brian Schanning
Dale Walters
Michael White
Roberto Zamparo

The following members of the balloting committee voted on this standard:

Kenneth G. Alonge
Thomas W. Bailey
James T. Carlo
David E. Carlson
John G. Cronican
Robert S. Crowder
Philip H. Enslow
Patrick S. Gonia
Julio Gonzalez-Sanz
Russell D. Housley
Raj Jain
Randolph S. Little
Joseph G. Maley
Peter Martini
Richard K. McAllister
Bennett Meyer
David S. Millman
Paul Nikolich
Robert O'Hara
Roger Pandanda
Ronald C. Petersen
Vikram Punj
Edouard Y. Rocher
James W. Romlein
Floyd E. Ross
Christoph Ruland
Mark-Rene Uchida

When the IEEE-SA Standards Board approved this standard on 22 March 1999, it had the following membership:

Richard J. Holleman, *Chair* **Donald N. Heirman,** *Vice Chair*

Judith Gorman, *Secretary*

Satish K. Aggarwal
Clyde R. Camp
James T. Carlo
Gary R. Engmann
Harold E. Epstein
Jay Forster*
Thomas F. Garrity
Ruben D. Garzon
James H. Gurney
Jim D. Isaak
Lowell G. Johnson
Robert Kennelly
E. G. “Al” Kiener
Joseph L. Koepfinger*
Stephen R. Lambert
Jim Logothetis
Donald C. Loughry
L. Bruce McClung
Louis-François Pau
Ronald C. Petersen
Gerald H. Peterson
John B. Posey
Gary S. Robinson
Hans E. Weinrich
Donald W. Zipse

*Member Emeritus

Janet Rutigliano

IEEE Standards Project Editor

Contents

1. Security architecture framework 1

1.1 Scope and purpose 1
1.2 References 1
1.3 Definitions 2
1.4 Acronyms and abbreviations 3
1.5 Architecture 3

IEEE Standards for Local and Metropolitan Area Networks:

Supplement to Standard for Interoperable LAN/MAN Security (SILS)—

Security Architecture Framework

1. Security architecture framework

1.1 Scope and purpose

This standard was developed to provide security in IEEE 802 Local Area Networks (LANs) and Metropolitan Area Networks (MANs).

The model for providing security services is described in Clause 1. A Secure Data Exchange (SDE) protocol is defined in Clause 2. Key management and the management of security associations are defined in Clause 3. While SDE is independent of any particular key management protocol implementation, the security services described in this standard depend on security management and key management services.

1.2 References

The following standards contain provisions that, through references in the text, constitute provisions of this standard. If the following publications are superseded by an approved revision, the revision shall apply.

ANSI/IEEE Std 802.1B, 1995 Edition, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 2:LAN/MAN management.[1]

ANSI/IEEE Std 802.1D, 1998 Edition, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Media access control (MAC) bridges.

[1]ANSI publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA (http://www.ansi.org/). IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (http://www.standards.ieee.org/).

IEEE Std 802-1990, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.[2]

ISO/IEC 7498-1:1994, Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model.[3]

ISO 7498-2:1989, Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture.

ISO/IEC 7498-4:1989, Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 4: Management Framework.

1.3 Definitions

1.3.1 LAN/MAN management definitions

This standard makes use of the following terms defined in ANSI/IEEE Std 802.1B, 1995 Edition:

a) LAN/MAN management protocol (LMMP);
b) LAN/MAN management service (LMMS).

1.3.2 Basic reference model definitions

This standard makes use of the following terms defined in ISO/IEC 7498-1:1994:

a) Open system interconnection (OSI) (n)-service;
b) Systems management.

1.3.3 Security architecture definitions

This standard makes use of the following terms defined in ISO 7498-2:1989:

a) Access control;
b) Confidentiality;
c) Data integrity;
d) Data origin authentication;
e) Key;
f) Key management;
g) Security service;
h) Security policy.

1.3.4 Management framework definitions

This standard makes use of the following terms defined in ISO/IEC 7498-4:1989:

a) Managed object;
b) Management information base.

---

[2]IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (http://www.standards.ieee.org/).

[3]ISO publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iso.ch/). ISO publications are also available in the United States from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA (http://www.ansi.org/).

1.3.5 Terms defined in this standard

The following terms are used throughout this document:

a) **Protocol stack:** An instantiation of a set of protocols;
b) **Security management information base (SMIB):** A management information base (MIB) that stores security-relevant objects.

1.4 Acronyms and abbreviations

The following acronyms and abbreviations are used in this standard:

ACSE	association control service element
CKD	center for key distribution
CKT	center for key translation
CMIP	common management information protocol
CMIS	common management information service
KDC	key distribution center
KMAE	key management application entity
KMAP	key management application process
KMP	key management protocol
KTC	key translation center
LAN	local area network
LLC	logical link control
LMMP	LAN/MAN management protocol
LMMS	LAN/MAN management service
MAC	medium access control
MAN	metropolitan area network
MIB	management information base
MKC	multicast key center
MKCID	MKC identifier
OSI	open system interconnection
PDU	protocol data unit
SA	security association
SC	security context
SAID	security association identifier
SDE	secure data exchange
SESE	security exchange service element
SILS	standard for interoperable LAN/MAN security
SMIB	security management information base

1.5 Architecture

This subclause describes the relationship of the protocol and service elements of SILS to the IEEE and the OSI communications architectural models. It describes the interfaces and explains which aspects of the

interfaces are standardized. There are two components of the SILS architecture: the SDE protocol and services, and the key management protocol (KMP) and services.

SDE is a data link layer protocol that provides security services to allow the secure exchange of data between nodes of a LAN or MAN. The KMP is an application layer protocol that provides for the management of the cryptographic keying material and security associations for use by SDE, as well as other security protocols. These services protect the data being transferred between nodes.

Figure 1 shows the components of SILS in relation to host station components, assuming the presence of an OSI communications protocol stack. User, system management, and security management applications (including key management) call upon SILS services using controls established by local security policy and configured in the host operating system/security control. Information objects in the MIB and SMIB store the necessary information to support the operation of host and SILS components.

When an application requires secure communications with a remote station, services are provided from either, or both, of the SILS protocols. KMP is composed of a key management application entity (KMAE), an association control service element (ACSE), and a security exchange service element (SESE) in the application layer. The SDE protocol resides in the data link layer, where it directly applies security services to the protocol data units (PDUs). In Figure 1, the protocol stack is an OSI stack, which may optionally be replaced by any other appropriate communications protocol stack.

The security control in the operating system/security control box (Figure 1) represents the security management component of the operating system. The security control is the security policy decision and enforcement mechanism for the operating system. It normally contains processes that support applications, such as the key management application process (KMAP) described in Clause 3.

For implementations requiring the highest security assurances, the security control always mediates access to the MIB, SMIB, and the communications protocol stack. Protocol layer communications with either the MIB or SMIB, as shown by the dashed lines in Figure 1, represent several possible implementation approaches. Any of these approaches are a local decision, and the appropriate approach is governed by the local security policy. One alternative uses the security control to mediate all layer communication with the MIB or SMIB. Another alternative permits the security control to create a local instance of the MIB or SMIB elements currently being used by a particular layer protocol. The actual MIB or SMIB elements are then updated using the values found in the local instance of the MIB or SMIB. A remaining alternative permits the layer protocols to have unmediated access to the MIB or SMIB.

KMP can communicate with and acquire the services of key distribution centers (KDCs), key translation centers (KTCs), and multicast key centers (MKCs), as indicated at the bottom of Figure 1.

NOTE—Key distribution center and center for key distribution (CKD) are equivalent terms, as well as key translation center and center for key translation (CKT).

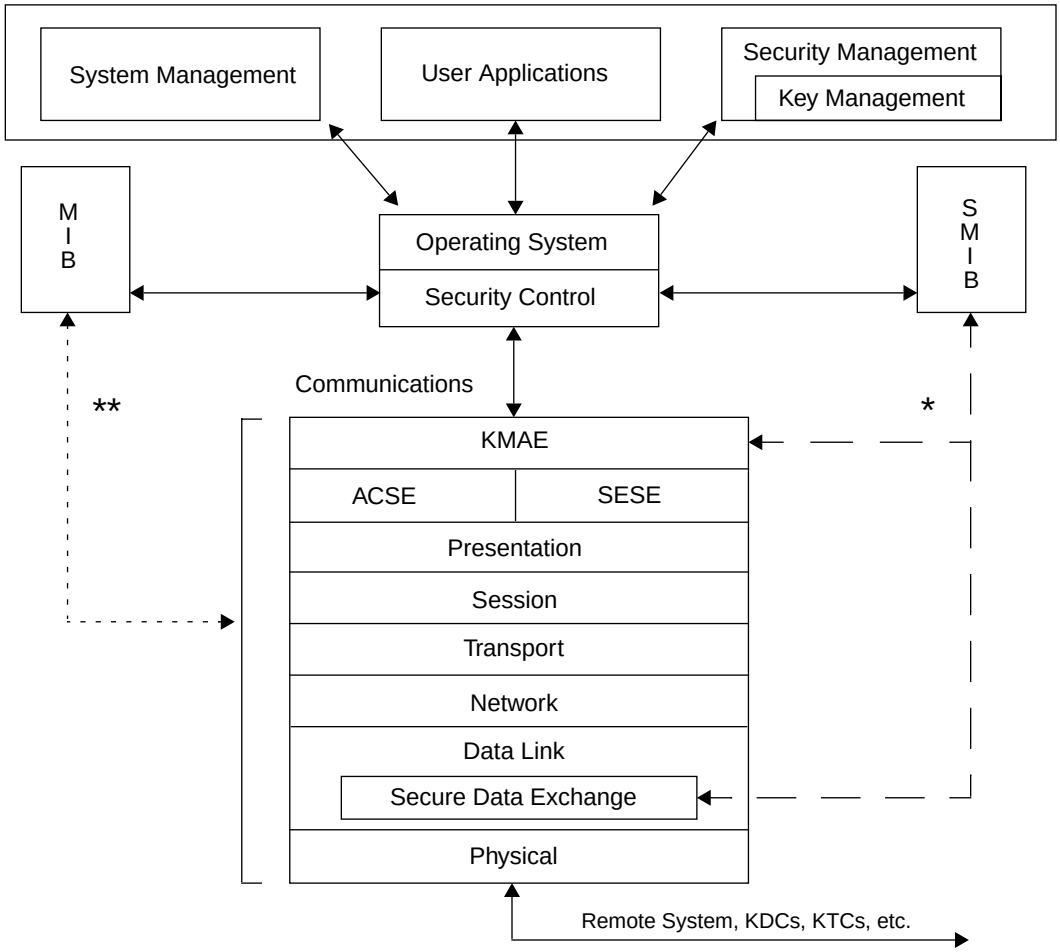
1.5.1 SILS entities

1.5.1.1 Secure data exchange

The SDE protocol and services are defined in Clause 2. Of the components defined in this standard, SDE is the only component residing within the IEEE 802 data link and physical layer protocol architecture. The SDE protocol provides the security services of confidentiality, data integrity, data origin authentication, and access control. ISO 7498-2:1989 includes only the services of confidentiality, data integrity, and traffic flow confidentiality at layer 2. The additional security services of data origin authentication and access control are appropriate and valuable for LANs and MANs, while traffic flow confidentiality is inappropriate for SDE. The rationale for these security service choices is found in Annex 2A of IEEE Std 802.10-1998.

The SDE protocol maintains the existing medium access control/logical link control (MAC/LLC) interface. Therefore, the SDE protocol may be implemented in a single MAC end station or in a MAC bridge that supports multiple end stations. Operation of SDE in a bridged environment is described in 1.5.5.

In order for an SDE station to communicate with a non-SDE IEEE 802 station, the SDE entity within the SDE station must be functionally inactive (bypassed). Although the SDE station has the capability to provide SDE services, the SDE process is bypassed by either physical or logical management control. This control derives its authority from the local security policy. However, this standard does not specify the bypass mechanism function. Such a mechanism is implementation specific. If secure communications between two SDE stations is not required by security policy, then the SDE entity is bypassed in both stations.



*The dashed line symbolizes several alternative approaches for implementing SMIB-to-layer communications. Three alternative approaches are described in the text.

**The dotted line symbolizes several alternative approaches for implementing MIB-to-layer communications. Three alternative approaches are described in the text.

Figure 1—SILS in the OSI architecture

1.5.1.2 Key management protocol

The KMP and services are defined in Clause 3. KMP is an application layer protocol (OSI layer 7) that manages cryptographic keys and, as explained in 1.5.2, manages the protocol layer security associations with remote stations for SDE and other security protocols. In SILS, the KMAE, ACSE, and SESE are contained in the application layer of the protocol stack. KMP accesses the SMIB where the status and control information for KMP is stored.

KMP creates, modifies, or deletes security associations in response to local applications within the limitations of local security policy. The KMAE may call on the services of the ACSE to create an application association, if necessary. SESE services are used to implement the KMP exchanges.

Key management is modeled as part of the security management application. In higher assurance implementations, a portion of the key management application may be placed in the security control. KMP provides key management services for SDE and can provide similar services for other security protocols.

1.5.2 Applications security

For each application requesting communications between stations, the local security policy reflected in the SMIB and the security control determines if protection is required. The security control of each SDE station is responsible for security management support for all applications, including system management and security management applications. As part of its functions, the security control is the security policy decision and enforcement mechanism. This includes identification and authentication of users and the management of security contexts and security associations.

1.5.2.1 Security context

After a user is successfully authenticated to the station, security policy information in the SMIB determines the roles, privileges, and system resources available to that user. In conjunction with the rest of the operating system, the user is allocated resources for permissible applications and is granted permission to access other information objects in the station. This active instance of the user in the station is termed a security context (SC). The SC defines whether the user can request communications, use security features, etc. If permitted by the local security policy, the user may seek to extend that SC to another station using a security association that enables protected communications.

1.5.2.2 Security association

When an application is required to protect its communications between stations, a cooperative relationship must be established that defines the security services desired and the mechanisms to be used. This relationship is called a security association (SA). For SDE, the SAs are managed by KMP. They include the selection of the type and source of cryptographic keying material and any attributes necessary to support the SDE protocol. SAs are given identifiers (SAID), and their attributes are maintained in the SMIB.

1.5.2.3 Establishing the link

The security control determines from the SMIB if a security association exists for the remote station. If not, it calls the KMAE to establish the security association and passes control to the security protocol (SDE or another). With the security association in place, the application can now exchange PDUs with the remote station using the security services provided by the protocol.

1.5.3 Protection of security management

Security management applications, including key management, are normally provided to support the role of a security administrator. The principal activity is the management of local and remote SMIB objects. This

includes the management of user security context data, security mechanism support data, SAs, alarms and alarm notifications, errors, and any security policy definitions.

Security management applications, as is true for all applications, can be supported by the SILS entities to provide protected communications. Remote management of SMIB objects normally requires such protection. The user is entered in a security context by the security control with the role and privileges of a security administrator, as defined in the local SMIB. When requesting protected communications, the security control determines if a security association exists and, if not, calls KMAE to establish one with any SILS-capable remote station. SDE or other identified security protocols establish the security association to be used.

1.5.3.1 Key management

Key management is modeled as a subset of the security management application. The security administrator may use key management to pre-establish security associations for individuals, groups, and multicast communications. Established security associations, and their cryptographic keys and attributes, are maintained in the SMIB. The protection of this sensitive material is a local implementation matter. Depending on the key management technique used, the establishment of a security association may involve communications with KDCs, KTCs, or MKCs as the sources for cryptographic keying material. The KMAE automatically provides this service if center-based key distribution is required by security policy. An implicit security association is established with any key center to protect the transfer of keying material. The KMAE completes its security association task with a peer by establishing a protected path to a remote station.

1.5.3.2 Security management in OSI

The security administrator may choose to take advantage of applications that implement the common management information protocol (CMIP) and its associated common management information service (CMIS) to remotely manage security alarms and provide access control to managed resources. Transfers using these protocols can be protected by SDE and other lower layer security protocols.

1.5.3.3 Security management in IEEE 802

The security administrator may choose to take advantage of applications that implement the LMMP and its associated LMMS to remotely manage SDE objects. Subclause 2.8 describes the use of these protocols and identifies the pertinent SDE managed object and classes. Transfers using these protocols can be protected by SDE.

1.5.4 System management security

System management applications are normally provided to support the role of a system administrator. The principle activity is the management of local and remote MIB objects. This includes the management of local and remote station resources; the detection of and response to faults, accounting, and configuration; and performance management of network entities. System management can be considered to include, or be the same as, security management with the understanding that the security contexts are different (security administrator vs. system administrator) and the privilege to manage objects is thereby separated (SMIB vs. MIB). The system administrator, while acting in the security context of the security administrator, can establish the policy to protect any remote management transfers using SDE entities and other lower layer security protocols. Like any other application, system management applications use the KMAE to establish security associations for SDE or other security protocols. Thus, system management applications using CMIP/CMIS in OSI, or using LMMP/LMMS in IEEE 802, can be supported by KMP and SDE protocols in the same manner as all other applications.

1.5.5 SILS in bridges

Since the SDE protocol is at the MAC boundary, it can protect an entire LAN/MAN segment when implemented in a bridge. SDE could protect either the bridge protocols, or traffic originating at (or intended for) the supported LAN/MAN segment.

There are limitations to this functionality when protecting the supported LAN traffic. Multiple MAC bridges can support a single LAN/MAN segment. If more than one bridge is expected to process traffic intended for the same node, then they must share the security association, keying material, and attributes for that node.

Figure 2 depicts SILS in a bridge and is derived from IEEE Std 802.1D,1998 Edition. This modified bridge model shows the interfaces between the SDE entity and the MAC entity, along with interfaces between the SDE entity and the routing and relay functions as internal sublayer service interfaces.

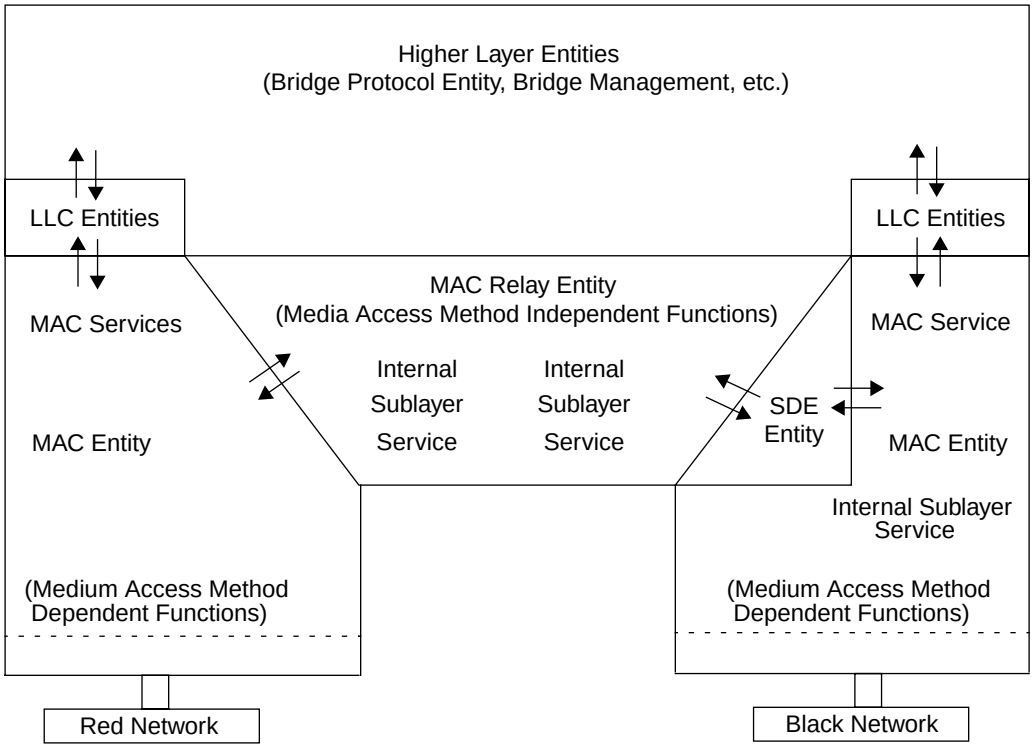


Figure 2—SILS model in a bridge