Leon S. Scaldeferri

Office of Information Security Research[1]

NSA, R22

9800 Savage Rd.

Ft. Meade MD 20755-6000

(301) - 688 - 0293 /0289[fax]

em: lsscald@afterlife.ncsc.mil

1. Opinions expressed in this paper are those of the author and do not represent the opinions or position of the FWUF or NSA.

(This Page Intentionally Blank)

IEEE 802.10

Standard for

Interoperable

LAN & MAN

Security

IEEE 802.10 Parts

802.10a: The SILS Model

Functional description of how the SILS fits into the OSI and 802 models and how the component parts of SILS interoperate.

802.10b: Secure Data Exchange (SDE)

Describes a security protocol that can be used to protect IEEE 802 LANs & MANs.

802.10c: Key Management (KM)

Specifies a key management architecture and protocol to support all security protocols in the OSI stack, in particular, SDE.

802.10d: System Management (SM)

Specifies a key management architecture and protocol to support SILS management requirements.

IEEE 802.10 Status

802.10a: The SILS Model

Under revision.

802.10b: Secure Data Exchange (SDE)

Approved ANSI/IEEE standard September 1992, published February 1993.

802.10c: Key Management (KM)

Under development.

802.10d: System Management (SM)

Work not yet begun.

IEEE 802.10

S

I

L

S

Part b - Secure Data Exchange (SDE) - Clause 2

An OSI Layer 2 Security Protocol

SDE Security Services

Data Confidentiality:

Provides for multiple confidentiality algorithms.
Depends on an external Key Management Service.

Connectionless Integrity:

Depends on an external Key Management Service.

Data Origin Authentication:

Only provided in conjunction with Integrity service.

Access Control:

Only provided in conjunction with Integrity and Authentication services.

Threats Protected Against by 802.10

Unauthorized Disclosure

Masquerading

Unauthorized Data Modification

Unauthorized Resource Use

ISO 7498-2-1988(E) Annex A, Threats

Destruction of information and/or resources

Corruption or modification of information

Theft, removal or loss of information

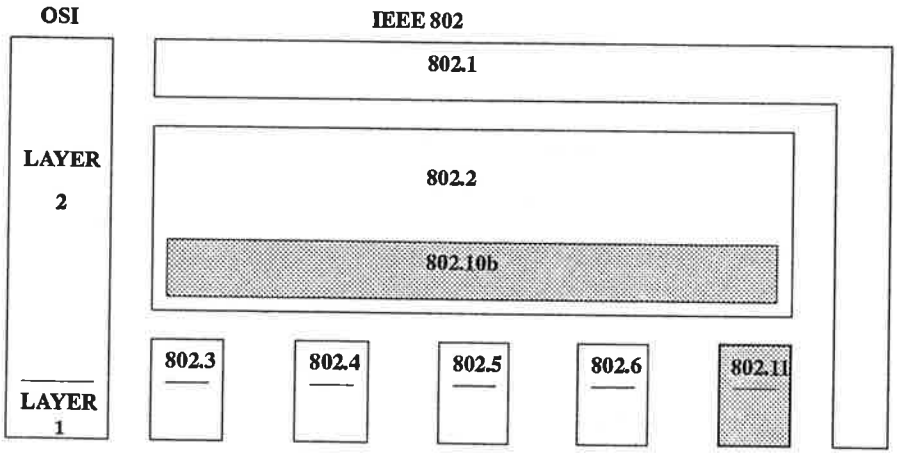
Disclosure of information

Interruption of services

ISO = ISO 7498-2-1988, Security Services, Recommendations 802 = 802.10b, Appendix A

Security Service / Layer	1	2	3	4
AUTHENTICATION: (5.2.1)				
Peer Entity/Data Origin	*	802[2]	ISO	ISO
ACCESS CONTROL: (5.2.2)	*	802[3]	ISO	ISO
CONFIDENTIALITY: (5.2.3)				
Connection	ISO	802[1]/ISO	ISO	ISO
Connectionless	*	802[1]/ISO	ISO	ISO
Selective Field	*	*	*	*
Traffic Flow	ISO	*	ISO	*
INTEGRITY: (5.2.4)				
connection with recovery	*	*	*	ISO
connection without recovery	*	*	ISO	ISO
connectionless	*	802[1]	ISO	ISO
ACCOUNTABILITY: (non-repudiation) (5.2.5)				
Origin/Delivery	*	*	*	*

1 = Depends on ext. Key Management Services, 2 = Needs Integrity, 3 = Needs Integrity & Authentication



RELATIONSHIP to IEEE 802 REFERENCE MODEL

SDE REQUIREMENTS

The SDE Protocol is required to be transparent to existing implementations.

* Existing IEEE 802 entities shall be able to recover if they receive an SDE protected packet.

* SDE entities shall be able to accept non-SDE protected packets without impairment.

* The addition of security should not modify either the (N+1) or (N-1) layer implementations.

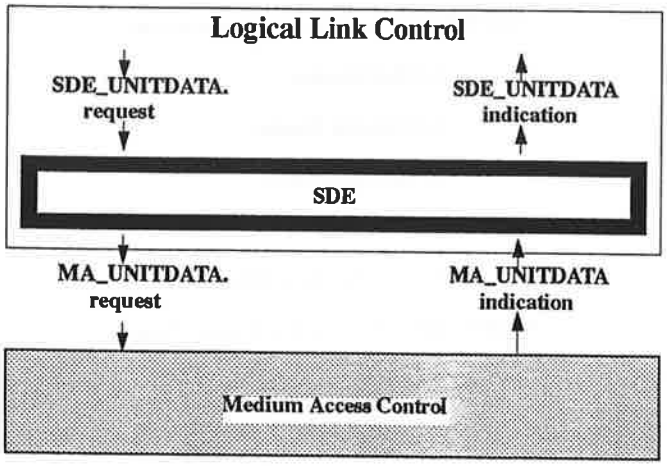
Note: The addition of the SDE protocol may cause certain management values such as the fragmentation size to change, and still be considered a transparent implementation.

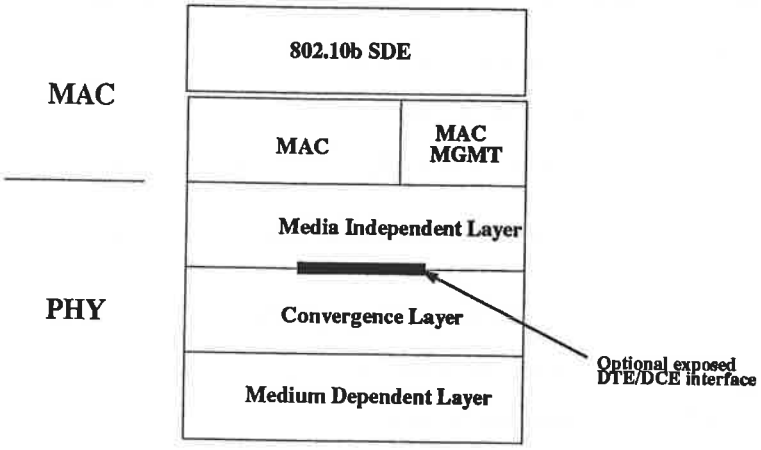
SDE SERVICE SPECIFICATIONS

There are only two primitives that are used at the SDE boundary:

UNITDATA.request, with parameters; Source addr, Destination addr, MAC SDU.
and
UNITDATA.indication, with parameters; Source addr, Destination addr, MAC SDU.

SDE Primitives





802.11 ARCHITECTURE with Security

SDE PDU Structure

SDE uses a single PDU type.

SDE PDU may contain up to five elements.

1. Clear Header

2. Protected Header

3. Data (SDE SDU)

4. PAD

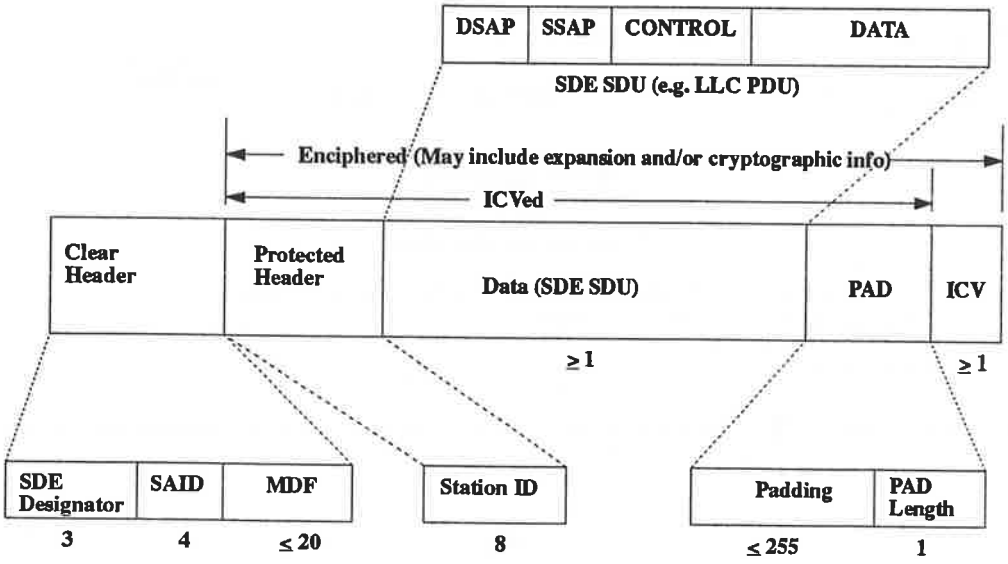
5. Integrity Check Value (ICV)

All these elements are optional except Data.

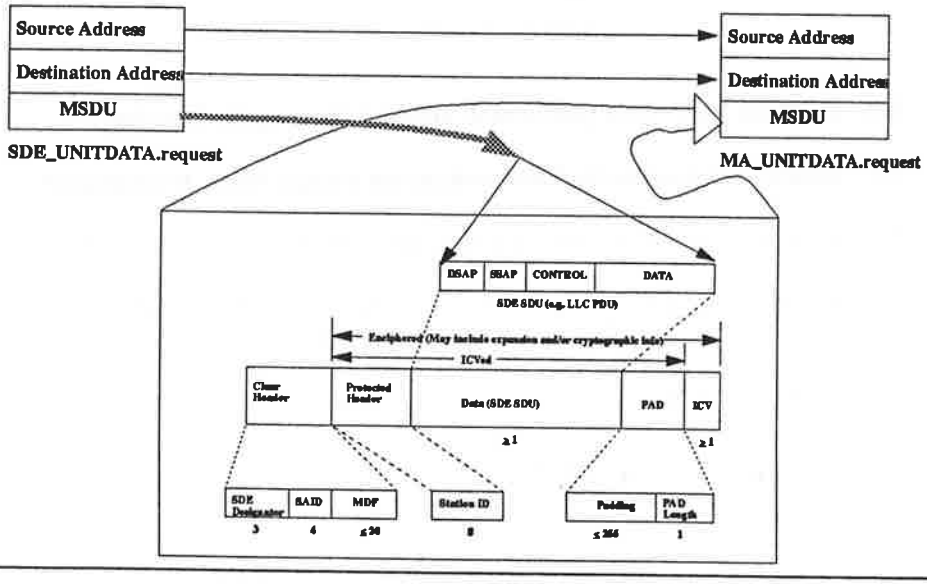
Protected Header, Data, and PAD may be transformed by the Integrity algorithm.

Protected Header, Data, PAD and ICV shall be transformed when the confidentiality algorithm is applied.

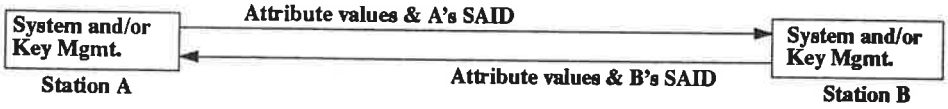
Structure of SDE SDU



Construction of the SDE PDU



SDE Security Associations



Initial Exchange

Security Associations

Attributes	Confid.	Integ.	Alg. ID	Alt. ID	MDF	....
Security Asso. # 1	Y	Y	1	2	8ADBC7	
Security Asso. # 2	N	Y	1	.	.	.
•	.	.	.	.	.	.
•	.	.	.	.	.	.
Security Asso. # n	.	.	.	.	.	.

SMIB

802.11 ISSUES
Topic: Security
Open Issues

6.2 - Does the PHY layer perform or support the security function?

6.3 - How does unauthorized network access impact MAC throughput?

6.4 - How will Authentication & Registration be specified in 802.11?

6.6 - Is there any additional work on Security that needs to be done in 802.11 in addition to the work that is done by 802.10?

6.7 - How does re-association interact with authentication?

6.8 - How does re-association interact with Privacy?

ISSUE 6.2

Does the PHY layer perform or support the security function?

In support of: NO!

Multiple PHY's, would most likely require multiple security implementations.

Application of 802.10b SDE would result in media independent solution.

802.10b is an approved standard and allows for flexibility regarding security functions, i.e. private to open system can share the same media (BSA).

802.10b would permit interoperability with other 802 LAN's employing it.

ISSUE 6.3

How does unauthorized network access impact MAC throughput?

Comments:

802.10 Protects against the ISO 7498-2-1988 threats of;

Masquerade
Replay
Modification of messages

Does not Protect against all threats of;

Denial of Service, either intentional or unintentional.

e.g co-channel use, interference, lack of etiquette

ISSUE 6.4

How will Authentication & Registration be specified?

An Authentication & Registration procedure using 802.10b could be provided as an annex to 802.11. Possible implementations might use RSA, DSS, IS-54 or something else. Request submissions by interested parties on actual implementations consistent with 802.10b SDE.

ISSUE 6.6

Is there additional work on Security that needs to be done in 802.11 in addition to the work that is done by 802.10.

Believe this presentation has answered that question, NO, to majority of threats, but denial of services from Issue 6.3 still needs to be addressed, or this issue belongs somewhere else!.

ISSUES 6.7 & 6.8

How does re-association interact with authentication & privacy?

The use of Security Associations set up in the Security Management Information Base, (SMIB) of 802.10 could provide for a way to effectively and efficiently handle re-associations for both authentication and privacy.