Leon S. Scaldeferri

Office of Information Security Research[1]

NSA, R22

9800 Savage Rd.

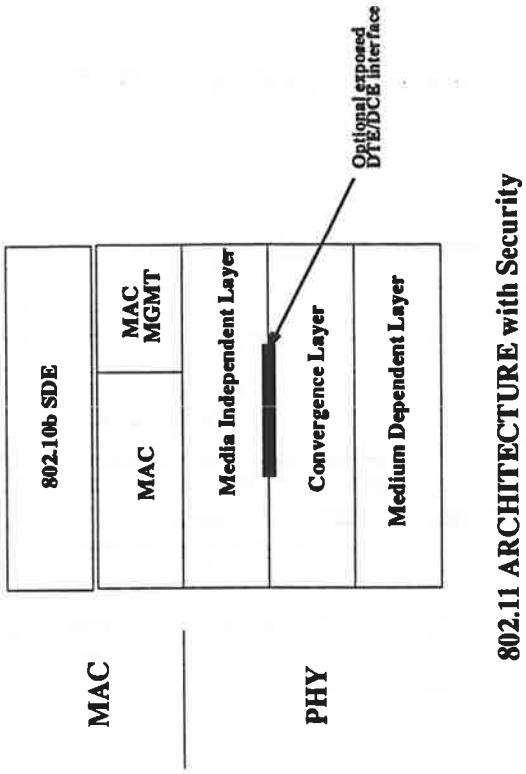
Ft. Meade MD 20755-6000

(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)



SDE PDU Structure

SDE uses a single PDU type.

SDE PDU may contain up to five elements.

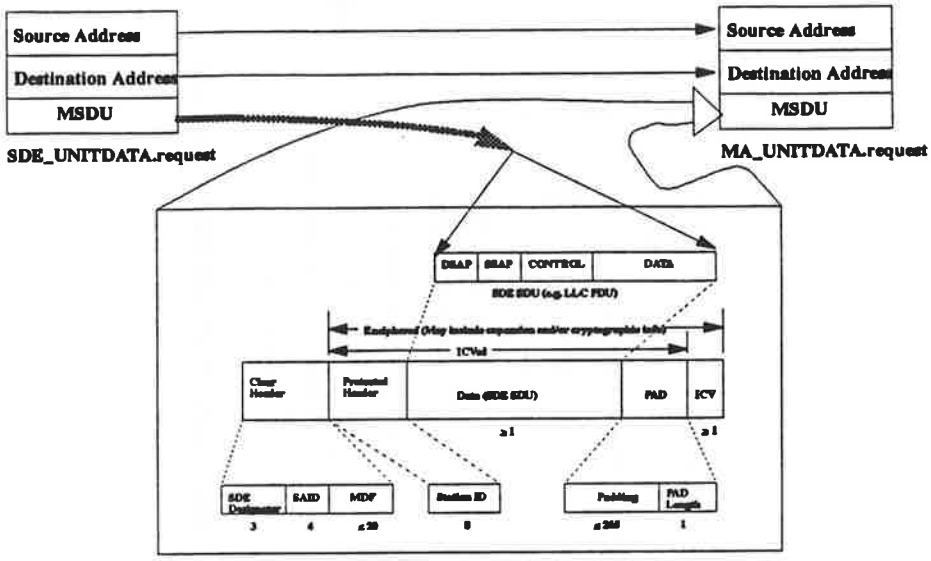
1. **Clear Header**
2. **Protected Header**
3. **Data (SDE SDU)**
4. **PAD**
5. **Integrity Check Value (ICV)**

All these elements are optional except Data.

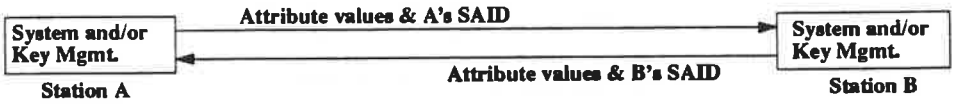
Protected Header, Data, and PAD may be transformed by the Integrity algorithm.

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

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

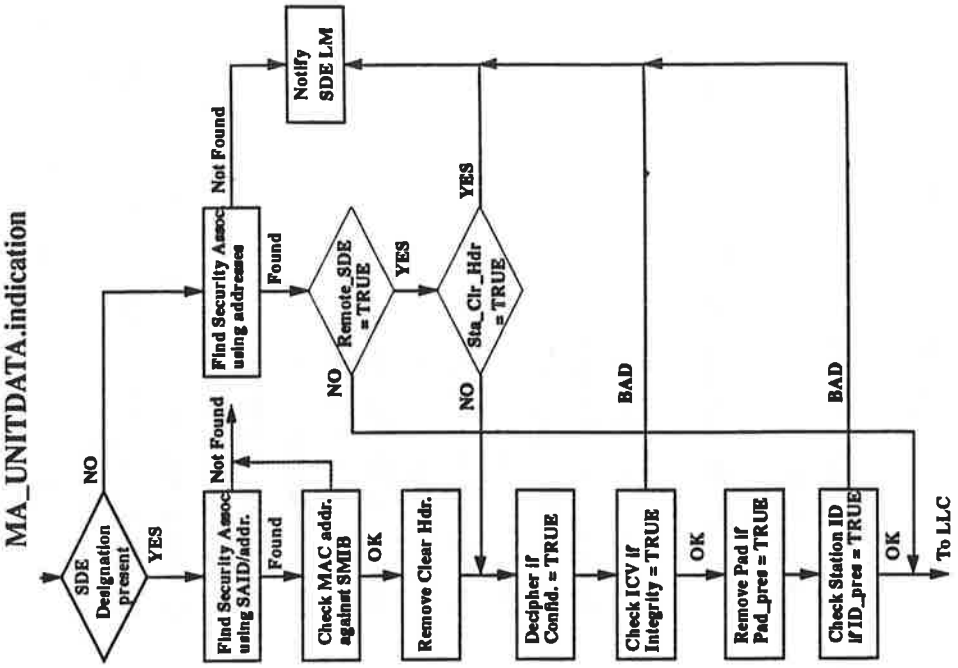
Station Objects

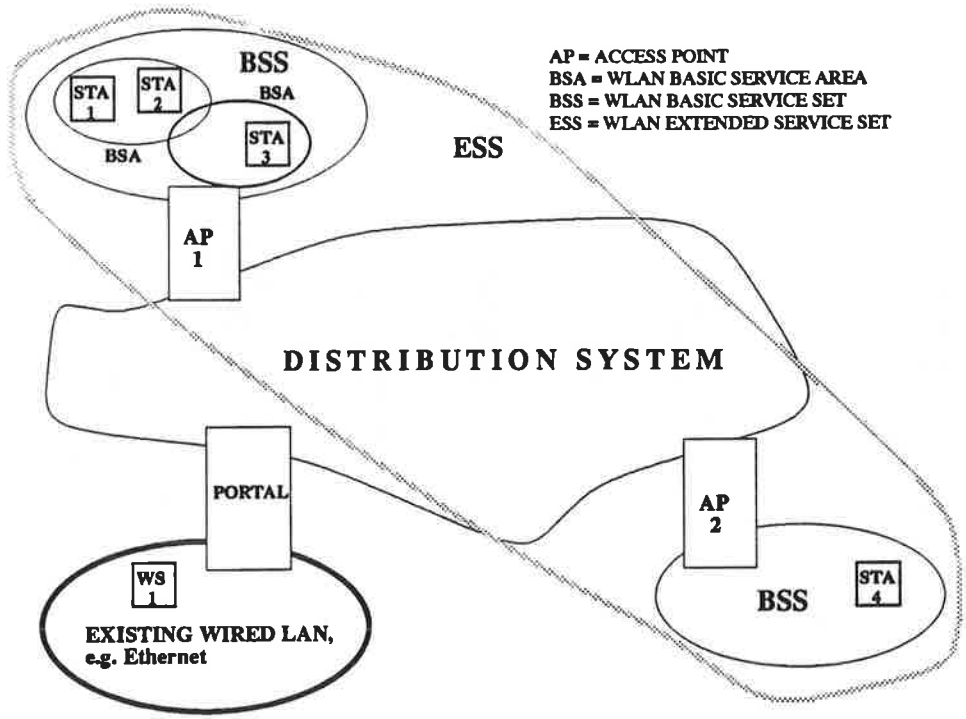
- Station_Clear_Hdr: Boolean
- Station_MDF: Boolean

Security Association Objects

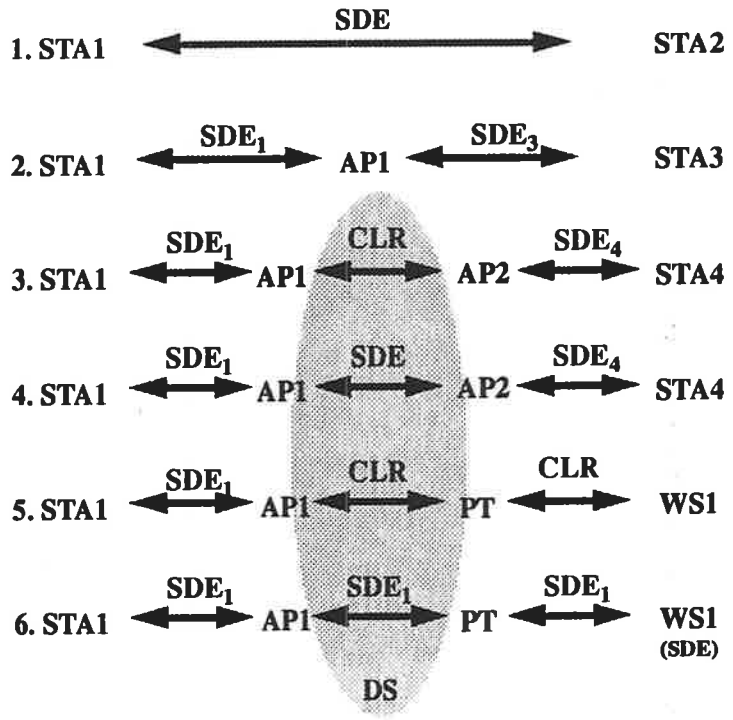
- Local_SAID: Octetstring
- Remote_SAID: Octetstring
- Assoc_MDF: Boolean
- Confid: Boolean
- Confid_Alg_ID: Octetstring
- Integ: Boolean
- Integ_Alg_ID: Octetstring
- Padding_pres: Boolean
- ID_pres: Boolean
- SDE_SAP: Octetstring
- Remote_SDE: Boolean
- Outgoing_Source_MAC_Address: Octetstring
- Outgoing_Destination_MAC_Address: Octetstring
- Incoming_Source_MAC_Address: Octetstring
- Incoming_Destination_MAC_Address: Octetstring

Transmission of an MA_UNITDATA.request


MA_UNITDATA.indication
SDE Designation present
NO
YES
Not Found
Found
Find Security Assoc using SAID/addr.
Check MAC addr. against SMIB
OK
Remove Clear Hdr.
Decipher if Confid. = TRUE
Check ICV if Integrity = TRUE
Remove Pad if Pad_pres = TRUE
Check Station ID if ID_pres = TRUE
To LLC
BAD
Find Security Assoc using addresses
Remote_SDE = TRUE
Sta_Clr_Hdr = TRUE
Notify SDE LM


AP = ACCESS POINT
BSA = WLAN BASIC SERVICE AREA
BSS = WLAN BASIC SERVICE SET
ESS = WLAN EXTENDED SERVICE SET
BSS
BSA
STA 1
STA 2
STA 3
ESS
AP 1
DISTRIBUTION SYSTEM
PORTAL
WS 1
EXISTING WIRED LAN, e.g. Ethernet
AP 2
BSS
STA 4

Station Security Associations



SDE TYPES

Case 1. Single SDE used by STA1 & STA2

Case 2. Two Options;

a. Single SDE used by STA1 & STA3, AP1 passes SDE unmodified, may still check validity.

b. Two SDE's used one for STA1 to AP1 and another for AP1 to STA3, AP1 removes SDE from one path and insert new SDE other path.

Case 3. STA1 to AP1 SDE may be same or different from AP2 to STA4 SDE.

Case 4. STA1 SDE is passed unmodified through AP1 and AP2 to STA4, may check for validity, other combinations possible.

Case 5. AP1 removes SDE for transport of SDU to WS1, (no knowledge on WS1).

Case 6. AP1 leaves SDE intact with knowledge that WS1 is an SDE entity, may check for validity.

- In cases 2b, 3, and 5 Access Point treats all SDE's alike, applies SDE on wireless portion of path only.
- In cases 2a, 4, and 6 AP determines final destination and either passes SDE unmodified or replaces it with new SDE. SDE's treatment is dependent on knowledge resident in AP data base.