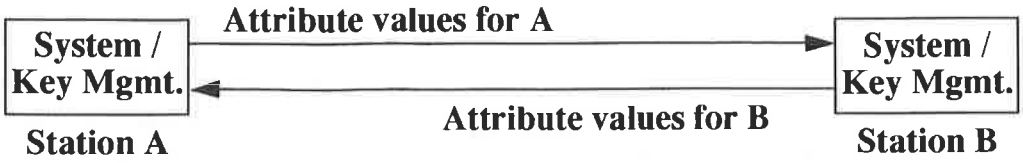
Minutes of THE MAC Sub-Group on Compression & Encryption

The MAC sub-group on Data Compression and Security met on 22 Sept. to discuss whether compression should be included in the P802.11 standard and the impact of encryption on compression. As compression must occur before encryption, if it is to be effective, it must occur above encryption in the 802.10 SDE model. It was felt that compression and encryption could be logically combined in the SDE architecture, as shown on the following pages.

As the extent to which compression would be a useful enhancement to data throughput is dependent on a variety on factors, it was decided that compression should be optional, but that interoperability of compressed and uncompressed data should exist. Also as this is an area were advances continue to be made, it was decides that the P802.11 standard would not specify a compression algorithm, but use a registration scheme similar to that employed by 802.10 SDE for encryption and integrity. This would require that accommodation be made in the Security Management Information Base (SMIB) for the presence of compression and an associated algorithm number.

It was recommended to the Chair of 802.11 that he approach 802.10 with the suggestion that the task of combining compression with encryption be addressed by 802.10 to assure consistence and compatibility of the two functions.

SDE Security Associations



Initial Exchange

Example of Security Management Information Base (SMIB)

Station Id	Remote_SDE (True=1, False=0)	DPM "Key"[1]	Encipher Alg. #[2]	Remote_Comp (True=1, False=0)	Comp Alg. #[3]
Sta(a)	1	abcd12987fed...	0 = Default	0	N/A
Sta(b)	0	None	N/A	1	7
Sta(c)	1	cdefab2345...	2	1	23
...	...	...	...	...	...
...	...	...	...	...	...
...	...	...	...	...	...

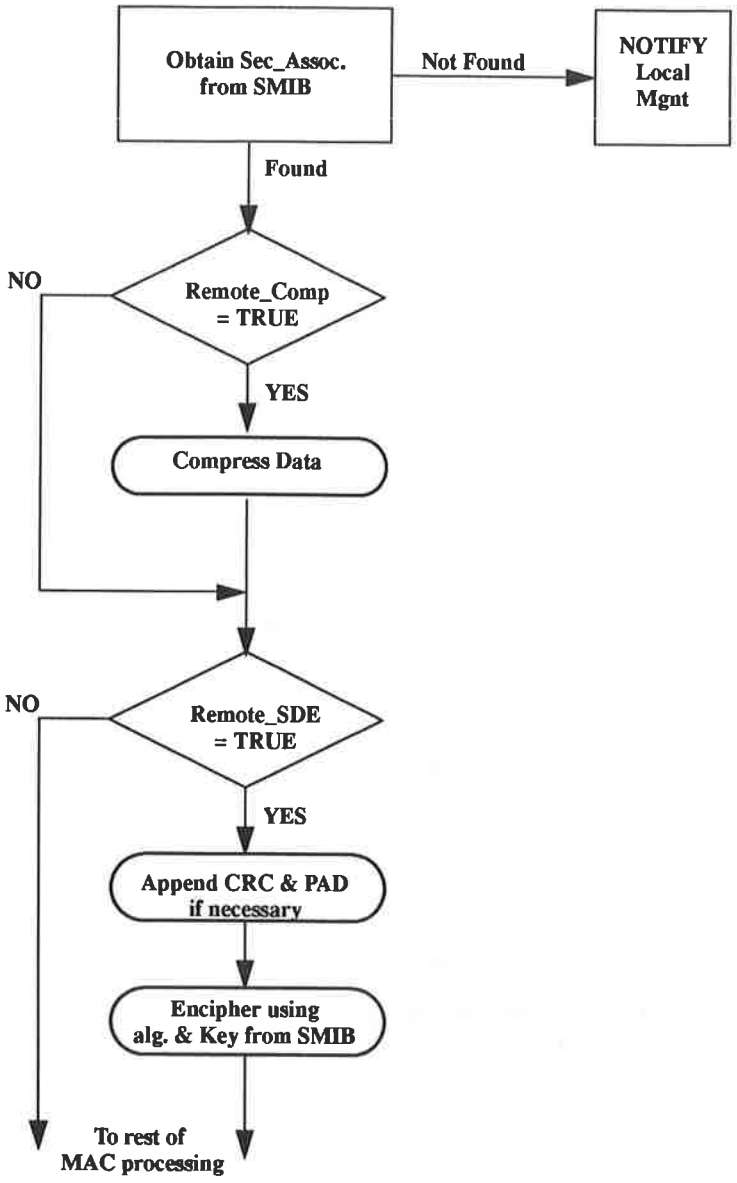
1. The Data Privacy Mask (DPM) can be either fixed or variable (max) length to accomodate a variety of algorithms.
2. # is an encipherment algorithm number registered per IEEE 802.10
3. # is a compression algorithm registered per IEEE 802.10

>> A Station that is not yet either pre-registered or associated with the Access Point will go through an association exchange with the AP/STA.

>> During that process the Data Privacy Mask (DPM) and authentication exchanges, including algorithm #s, will occur.

>> The authentication and DPM exchanges will be done in some "secure" manner, e.g. passwords, DSS, RSA, etc.

SDE Transmission Procedure (example)



SDE Reception Procedure (example)