If any cipher suite other than TKIP, WEP-104, or WEP-40 is enabled, then the AP supports pairwise keys, and thus the suite selector 00-0F-AC:0 (Use group cipher suite) is not a valid option.

Table 8-100 indicates the circumstances under which each cipher suite is used.

Table 8-100—Cipher suite usage

Cipher suite selector	GTK	PTK	IGTK
Use group key	No	Yes	No
WEP-40	Yes	No	No
WEP-104	Yes	No	No
TKIP	Yes	Yes	No
CCMP	Yes	Yes	No
BIP	No	No	Yes

8.4.2.27.3 AKM suites

The AKM Suite Count field indicates the number of AKM suite selectors that are contained in the AKM Suite List field.

The AKM Suite List field contains a series of AKM suite selectors contained in the RSNE. In an IBSS only a single AKM suite selector may be specified because STAs in an IBSS use the same AKM suite and because there is no mechanism to negotiate the AKMP in an IBSS (see 11.5.5).

Each AKM suite selector specifies an AKMP. Table 8-101 gives the AKM suite selectors defined by this standard. An AKM suite selector has the format shown in Figure 8-187.

Table 8-101—AKM suite selectors

OUI	Suite type	Meaning		
		Authentication type	Key management type	Key derivation type
00-0F-AC	0	Reserved	Reserved	Reserved
00-0F-AC	1	Authentication negotiated over IEEE 802.1X or using PMKSA caching as defined in 11.5.9.3 – RSNA default	RSNA key management as defined in 11.6 or using PMKSA caching as defined in 11.5.9.3 – RSNA default	Defined in 11.6.1.2
00-0F-AC	2	PSK	RSNA key management as defined in 11.6, using PSK	Defined in 11.6.1.2
00-0F-AC	3	FT authentication negotiated over IEEE 802.1X	FT key management as defined in 11.6.1.7	Defined in 11.6.1.7.2
00-0F-AC	4	FT authentication using PSK	FT key management as defined in 11.6.1.7	Defined in 11.6.1.7.2

Table 8-101—AKM suite selectors *(continued)*

OUI	Suite type	Meaning		
		Authentication type	Key management type	Key derivation type
00-0F-AC	5	Authentication negotiated over IEEE 802.1X or using PMKSA caching as defined in 11.5.9.3 with SHA256 Key Derivation	RSNA Key Management as defined in 8.5 or using PMKSA caching as defined in 11.5.9.3, with SHA256 Key Derivation	Defined in 11.6.1.7.2
00-0F-AC	6	PSK with SHA256 Key Derivation	RSNA Key Management as defined in 11.6 using PSK with SHA256 Key Derivation	Defined in 11.6.1.7.2
00-0F-AC	7	TDLS	TPK Handshake	Defined in 11.6.1.7.2
00-0F-AC	8	SAE Authentication with SHA-256 or using PMKSA caching as defined in 11.5.9.3 with SHA-256 key derivation	RSNA key management as defined in 11.6, PMKSA caching as defined in 11.5.9.3 with SHA256 key derivation or authenticated mesh peering exchange as defined in 13.5	Defined in 11.6.1.7.2
00-0F-AC	9	FT authentication over SAE with SHA-256	FT key management defined in 11.6.1.7	Defined in 11.6.1.7.2
00-0F-AC	10–255	Reserved	Reserved	Reserved
Vendor OUI	Any	Vendor-specific	Vendor-specific	Vendor-specific
Other	Any	Reserved	Reserved	Reserved

The AKM suite selector value 00-0F-AC:1 (i.e., Authentication negotiated over IEEE 802.1X with RSNA key management as defined in 11.6 or using PMKSA caching as defined in 11.5.9.3) is the assumed default when the AKM suite selector field is not supplied.

NOTE—The selector value 00-0F-AC:1 specifies only that IEEE Std 802.1X-2004 is used as the authentication transport. IEEE Std 802.1X-2004 selects the authentication mechanism.

The AKM suite selector value 00-0F-AC:8 (i.e., SAE Authentication with SHA-256 or using PMKSA caching as defined in 11.5.9.3 with SHA-256 key derivation) is used when either a password or PSK is used with RSNA key management.

NOTE—Selector values 00-0F-AC:1 and 00-0F-AC:8 can simultaneously be enabled by an Authenticator.

The AKM suite selector value 00-0F-AC:2 (PSK) is used when an alternate form of PSK is used with RSNA key management.

NOTE—Selector values 00-0F-AC:1 and 00-0F-AC:2 can simultaneously be enabled by an Authenticator.