

ISO/IEC/IEEE 8802-1AE AMD 2:2015-05 (E)

Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Part 1AE: Media access control (MAC) security - Amendment 2: Extended Packet Numbering

Contents	Page
3. Definitions	2
4. Abbreviations and acronyms	3
7. Principles of secure network operation.....	4
8. MAC Security Protocol (MACsec).....	5
8.3 MACsec operation	5
9. Encoding of MACsec protocol data units.....	7
9.8 Packet Number (PN).....	7
9.9 Secure Channel Identifier (SCI)	7
10. Principles of MAC Security Entity (SecY) operation	8
10.5 Secure frame generation	8
10.6 Secure frame verification.....	9
10.7 SecY management	12
13. Management protocol	16
13.7 Use of the MIB with extended packet numbering	16
14. Cipher Suites.....	17
14.1 Cipher Suite use	17
14.2 Cipher Suite capabilities	18
14.4 Cipher Suite conformance	18
14.6 GCM-AES-256.....	18
14.7 GCM-AES-XPN-128	19
14.8 GCM-AES-XPN-256	20
Annex A (normative) PICS Proforma.....	22
A.13 Additional variant Cipher Suite capabilities.....	22
Annex B (informative) Bibliography	23
Annex C (informative) MACsec Test Vectors	25
C.1 Integrity protection (54-octet frame)	26
C.2 Integrity protection (60-octet frame)	31
C.3 Integrity protection (65-octet frame)	34
C.4 Integrity protection (79-octet frame)	37
C.5 Confidentiality protection (54-octet frame).....	40
C.6 Confidentiality protection (60-octet frame).....	45
C.7 Confidentiality protection (61-octet frame).....	48
C.8 Confidentiality protection (75-octet frame).....	51

Figures

Figure 8-2	MACsec operation	6
Figure 9-2	SecTAG format	7
Figure 10-5	Management controls and counters for secure frame verification	9
Figure 14-1	Cipher Suite Protect and Validate operations	17

Tables

Table 10-1	Extended packet number recovery (examples)	11
Table 14-1	MACsec Cipher Suites.....	18
Table C-1	Unprotected frame (example)	26
Table C-2	Integrity protected frame (example)	26
Table C-3	GCM-AES-128 Key and calculated ICV (example)	27
Table C-4	GCM-AES-256 Key and calculated ICV (example)	28
Table C-5	GCM-AES-XPB-128 Key and calculated ICV (example)	29
Table C-6	GCM-AES-XPB-256 Key and calculated ICV (example)	30
Table C-7	Unprotected frame (example)	31
Table C-8	Integrity protected frame (example)	31
Table C-11	GCM-AES-XPB-128 Key and calculated ICV (example)	32
Table C-12	GCM-AES-XPB-256 Key and calculated ICV (example)	33
Table C-13	Unprotected frame (example)	34
Table C-14	Integrity protected frame (example)	34
Table C-17	GCM-AES-XPB-128 Key and calculated ICV (example)	35
Table C-18	GCM-AES-XPB-256 Key and calculated ICV (example)	36
Table C-19	Unprotected frame (example)	37
Table C-20	Integrity protected frame (example)	37
Table C-23	GCM-AES-XPB-128 Key and calculated ICV (example)	38
Table C-24	GCM-AES-XPB-256 Key and calculated ICV (example)	39
Table C-25	Unprotected frame (example)	40
Table C-26	Confidentiality protected frame (example).....	40
Table C-27	GCM-AES-128 Key, Secure Data, and ICV (example)	41
Table C-28	GCM-AES-256 Key, Secure Data, and ICV (example)	42
Table C-29	GCM-AES-XPB-128 Key, Secure Data, and ICV (example).....	43
Table C-30	GCM-AES-XPB-256 Key, Secure Data, and ICV (example).....	44
Table C-31	Unprotected frame (example)	45
Table C-32	Confidentiality protected frame (example).....	45
Table C-35	GCM-AES-XPB-128 Key, Secure Data, and ICV (example).....	46
Table C-36	GCM-AES-XPB-256 Key, Secure Data, and ICV (example).....	47
Table C-37	Unprotected frame (example)	48
Table C-38	Confidentiality protected frame (example).....	48
Table C-41	GCM-AES-XPB-128 Key, Secure Data, and ICV (example).....	49
Table C-42	GCM-AES-XPB-256 Key, Secure Data, and ICV (example).....	50
Table C-43	Unprotected frame (example)	51
Table C-44	Confidentiality protected frame (example).....	51
Table C-47	GCM-AES-XPB-128 Key, Secure Data, and ICV (example).....	52
Table C-48	GCM-AES-XPB-256 Key, Secure Data, and ICV (example).....	53