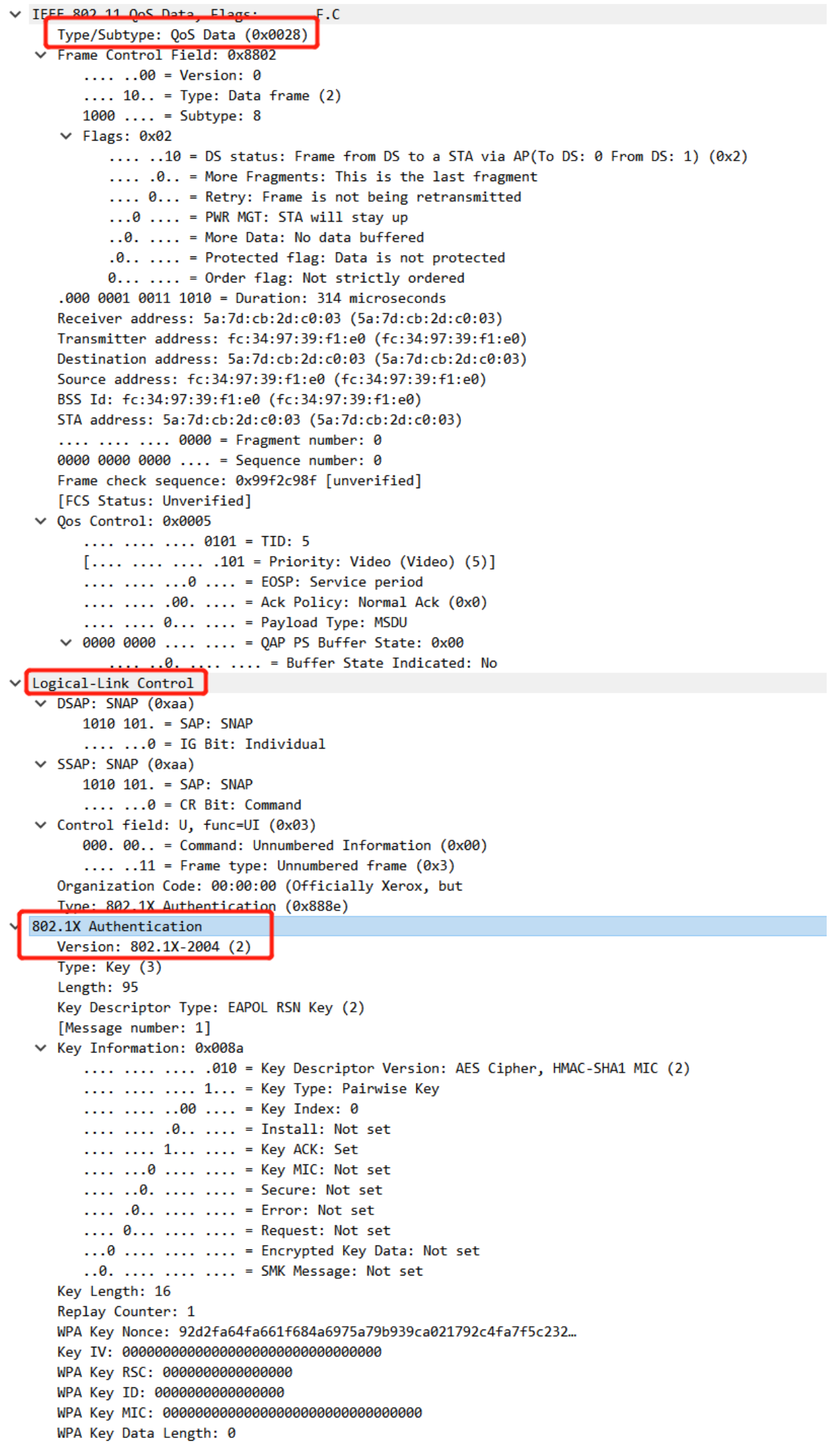
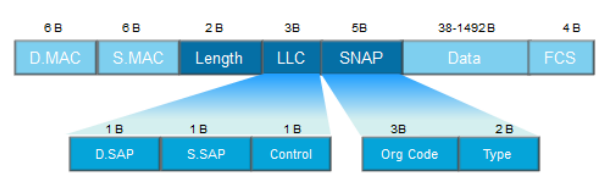
四次握手 Message 1 of 4
EAPOL帧是一个Qos Data数据帧



```
∨ IEEE 802.11 QoS Data, Flags: ......F.C
    Type/Subtype: QoS Data (0x0028)
  ∨ Frame Control Field: 0x8802
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    ∨ Flags: 0x02
        .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: 5a:7d:cb:2d:c0:03 (5a:7d:cb:2d:c0:03)
    Transmitter address: fc:34:97:39:f1:e0 (fc:34:97:39:f1:e0)
    Destination address: 5a:7d:cb:2d:c0:03 (5a:7d:cb:2d:c0:03)
    Source address: fc:34:97:39:f1:e0 (fc:34:97:39:f1:e0)
    BSS Id: fc:34:97:39:f1:e0 (fc:34:97:39:f1:e0)
    STA address: 5a:7d:cb:2d:c0:03 (5a:7d:cb:2d:c0:03)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0000 .... = Sequence number: 0
    Frame check sequence: 0x99f2c98f [unverified]
    [FCS Status: Unverified]
  ∨ Qos Control: 0x0005
      .... .... .... 0101 = TID: 5
      [.... .... .... .101 = Priority: Video (Video) (5)]
      .... .... ...0 .... = EOSP: Service period
      .... .... .00. .... = Ack Policy: Normal Ack (0x0)
      .... .... 0... .... = Payload Type: MSDU
    ∨ 0000 0000 .... .... = QAP PS Buffer State: 0x00
        .... ..0. .... .... = Buffer State Indicated: No
∨ Logical-Link Control
  ∨ DSAP: SNAP (0xaa)
      1010 101. = SAP: SNAP
      .... ...0 = IG Bit: Individual
  ∨ SSAP: SNAP (0xaa)
      1010 101. = SAP: SNAP
      .... ...0 = CR Bit: Command
  ∨ Control field: U, func=UI (0x03)
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x3)
    Organization Code: 00:00:00 (Officially Xerox, but
    Type: 802.1X Authentication (0x888e)
∨ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  ∨ Key Information: 0x008a
      .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .0.. .... = Install: Not set
      .... .... 1... .... = Key ACK: Set
      .... ...0 .... .... = Key MIC: Not set
      .... ..0. .... .... = Secure: Not set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...0 .... .... .... = Encrypted Key Data: Not set
      ..0. .... .... .... = SMK Message: Not set
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: 92d2fa64fa661f684a6975a79b939ca021792c4fa7f5c232…
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 0
```

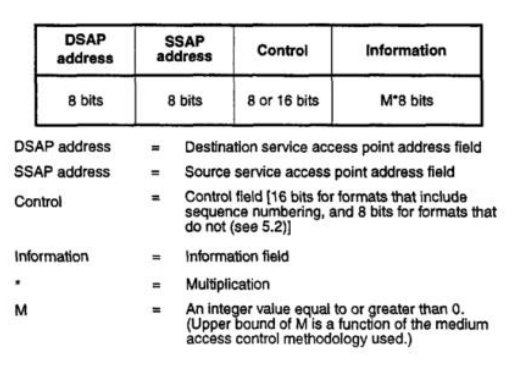
IEEE802.3 帧格式



- IEEE 802.3 帧长度字段值小于等于1500 (0x05DC)。

3.2 LLC PDU format

All LLC PDUs shall conform to the format shown in figure 4.



DSAP address	SSAP address	Control	Information
8 bits	8 bits	8 or 16 bits	M*8 bits

DSAP address = Destination service access point address field
SSAP address = Source service access point address field
Control = Control field [16 bits for formats that include sequence numbering, and 8 bits for formats that do not (see 5.2)]
Information = Information field
* = Multiplication
M = An integer value equal to or greater than 0. (Upper bound of M is a function of the medium access control methodology used.)

Figure 4—LLC PDU format

5.2 Control field formats

The three formats defined for the control field (figure 9) shall be used to perform numbered information transfer, numbered supervisory transfer, unnumbered control, and unnumbered information transfer functions. The numbered information transfer and supervisory transfer functions apply only to Type 2 operation. The unnumbered control and unnumbered information transfer functions apply to Type 1, Type 2, or Type 3 operation depending upon the specific function selected.

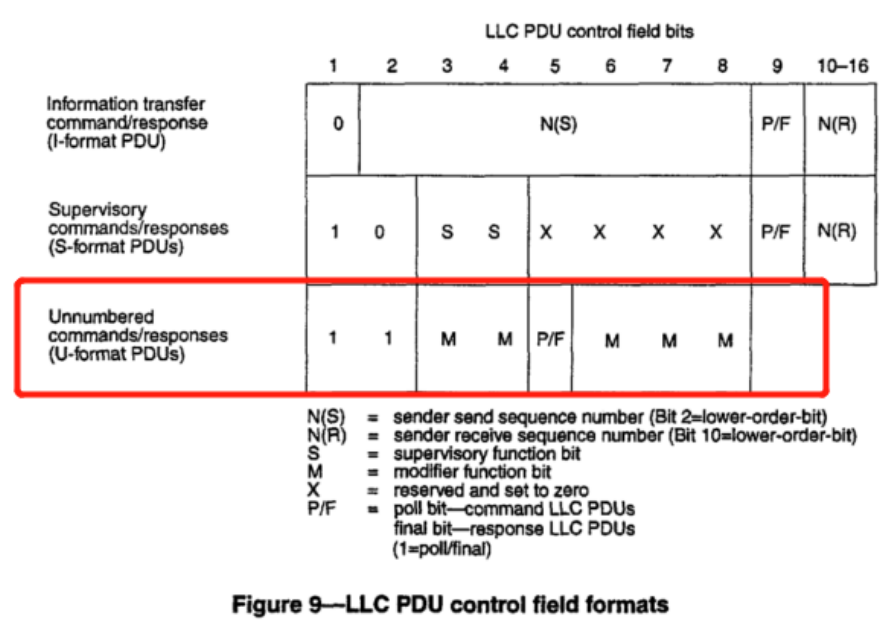

LLC PDU control field bits
1 2 3 4 5 6 7 8 9 10–16
Information transfer command/response (I-format PDU)
0
N(S)
P/F
N(R)
Supervisory commands/responses (S-format PDUs)
1 0 S S X X X X P/F N(R)
Unnumbered commands/responses (U-format PDUs)
1 1 M M P/F M M M
N(S) = sender send sequence number (Bit 2=lower-order-bit)
N(R) = sender receive sequence number (Bit 10=lower-order-bit)
S = supervisory function bit
M = modifier function bit
X = reserved and set to zero
P/F = poll bit—command LLC PDUs
final bit—response LLC PDUs
(1=poll/final)

Figure 9—LLC PDU control field formats

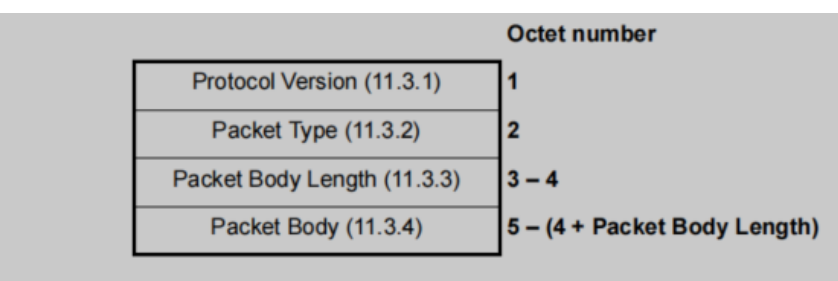

Octet number
Protocol Version (11.3.1)
1
Packet Type (11.3.2)
2
Packet Body Length (11.3.3)
3 – 4
Packet Body (11.3.4)
5 – (4 + Packet Body Length)

Figure 11-1—Common EAPOL PDU structure

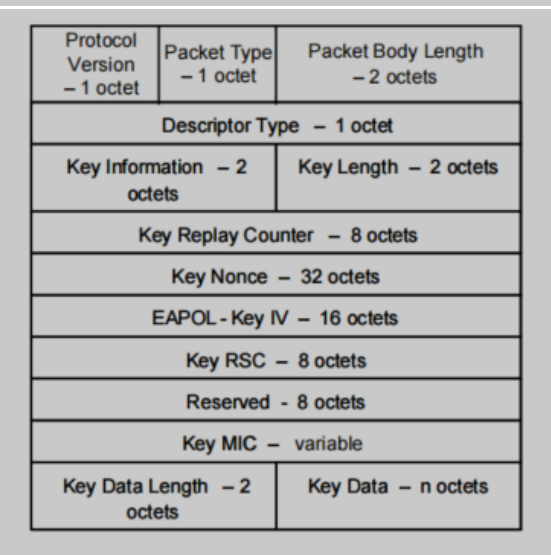

Protocol Version – 1 octet
Packet Type – 1 octet
Packet Body Length – 2 octets
Descriptor Type – 1 octet
Key Information – 2 octets
Key Length – 2 octets
Key Replay Counter – 8 octets
Key Nonce – 32 octets
EAPOL - Key IV – 16 octets
Key RSC – 8 octets
Reserved - 8 octets
Key MIC – variable
Key Data Length – 2 octets
Key Data – n octets

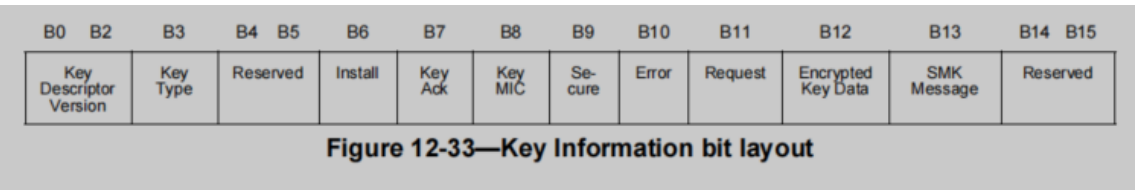
Figure 12-32—EAPOL-Key frame

802.11 Qos Data
sequence number = 0 从0开始计数
QoS Control field
TID : 参考 Table 9-8—TID subfield，identifies the TC or TS to which the corresponding MSDU (or fragment thereof) or A-MSDU in the Frame Body
EOSP : 参考 9.2.4.5.3 EOSP (end of service period) subfield
Ack Policy : identifies the acknowledgment policy that is followed upon the delivery of the MPDU
A-MSDU Present : indicates the presence of an A-MSDU
AP PS Buffer State : 参考 9.2.4.5.8 AP PS Buffer State subfield,indicates the PS buffer state at the AP for a STA

LLC 逻辑链路控制字段 参考 http://www.360doc.com/content/12/1221/10/9523427_255430137.shtml
对应的标准是 ISO/IEC 8802-2:1998, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control. 道客巴巴在线阅读 https://www.doc88.com/p-6945057642022.html?r=1
主要就是关注information 表明上层协议字段 802.1X

802.1X 字段 EAPOL PDU帧格式参考 802.1X 11.3 Common EAPOL PDU structure
参考802.11 Figure 12-32—EAPOL-Key frame 和 802.1X 11.9 EAPOL-Key
Protocol Version (11.3.1)
Packet Type (11.3.2) 四次握手的EAPOL帧类型是 EAPOL-Key (11.4, 11.5, 11.9)
Packet Body Length (11.3.3)
Packet Body (11.3.4)
Descriptor Type : 参考802.1X Table 11-5—Descriptor Type value assignments ，value=2表示IEEE 802.11 Key Descriptor Type
Key Information : This field is 2 octets and specifies characteristics of the key. See Figure 12-33-Key Information bit layout
Key Descriptor Version (bits 0 - 2) shall be set to 0 on all transmitted EAPOL-Key frames except under the following circumstances
The value 2 shall be used for all EAPOL-Key frames to a STA when the negotiated AKM is 00-0F-AC:1 or 00-0F-AC:2 and either the pairwise or the group cipher is an enhanced either the pairwise or the group cipher is an enhanced data cryptographic encapsulation mechanism other than TKIP for Key Descriptor 2. This value indicates the following:
value = 2表示AKM是00-0F-AC:1 or 00-0F-AC:2，并且是使用TKIP之外的数据加密机制，该值表示一下内容
— HMAC-SHA-1-128 is the EAPOL-Key MIC. HMAC is defined in IETF RFC 2104; and SHA-1, by FIPS PUB 180-4. The output of the HMAC-SHA-1 shall be truncated to its 128 MSBs (octets 0 - 15 of the digest output by HMAC-SHA-1), i.e.,the last four octets generated shall be irretrievably deleted).
HMAC-SHA-1-128作为该帧的MIC
— The NIST AES key wrap is the EAPOL-Key encryption algorithm used to protect the Key Data field. IETF RFC 3394 defines the NIST AES key wrap algorithm.
NIST AES key wrap 作为该帧的加密算法去保护密钥数据字段
— The MIC is 16 octets.
MIC是16位的
Key Type (bit 3) : 指定此 EAPOL 密钥帧是否是派生 PTK 的 4 次握手的一部分 value=1
Install (bit 6): Key Type (bit 3)=1时 该位才有意义，value=0表示不需要配置临时密钥给STA
If the value of Key Type (bit 3) is 1, then for the Install bit,
— The value 1 means the IEEE 802.1X component shall configure the temporal key derived from this message into its IEEE 802.11 STA.
— The value 0 means the IEEE 802.1X component shall not configure the temporal key into the IEEE 802.11 STA.

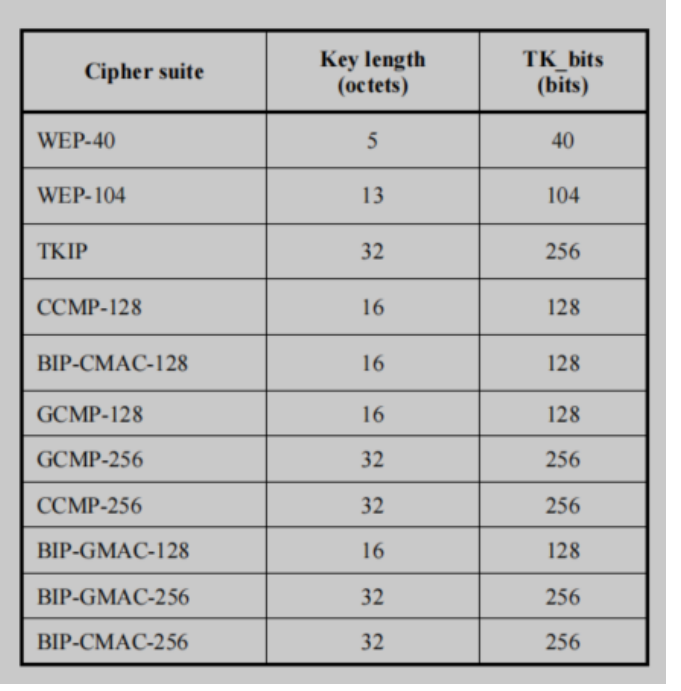
Key Ack (bit 7) is set to 1 in messages from the Authenticator if an EAPOL-Key frame is required in response to this message
=1表示这个EAPOL-KEY需要被响应
Key MIC (bit 8) is set to 1 if a MIC is in this EAPOL-Key frame
=1表示这个帧包含MIC
Secure (bit 9) is set to 1 once the initial key exchange is complete.
=1表示初始化的密钥交换已经完成
Error (bit 10) is set by a Supplicant to report that a MIC failure occurred in a TKIP MSDU or handshake failure.
当TKIP的MIC校验失败或者握手失败时被设置
In case of a MIC failure, a Supplicant shall set this bit to 1 only when the Request (bit 11) is 1.
When the SMK Message bit is 1, Error shall be set to 1 to indicate the key data field contains an Error KDE
Request (bit 11)
is set to 1 by a Supplicant to request that the Authenticator initiate either a 4-way handshake or group key handshake,
请求方设置为1 表示请求方发起四次握手或者组密钥握手
is set to 1 by a Supplicant in a Michael MIC Failure Report,
设置为1报告MIC失败
and is set to 1 by the STSL peer STA to request initiator STA rekeying of the STK.
The Supplicant shall not set this bit to 1 in on-going 4-way handshakes
在四次握手的过程中不应该置为1
Encrypted Key Data (bit 12) is set to 1 if the Key Data field is encrypted and is set to 0 if the Key Data field is not encrypted.
设置为1表示Key数据是否加密
SMK Message (bit 13) specifies whether this EAPOL-Key frame is part of an SMK handshake
Key Length : The value defines the length in octets of the pairwise temporal key. See Table 12-4.
Key Replay Counter : is initialized to 0 when the PMK is established. The Supplicant shall use the key replay counter in the received EAPOL-Key frame when responding to an EAPOL-Key frame.
It carries a sequence number that the protocol uses to detect replayed EAPOL-Key frames.
记录自己的EAPOL-KEY帧的个数
Key Nonce : 32位的随机数
EAPOL-Key IV : This field is 16 octets. It contains the IV used with the KEK
Key RSC : This field is 8 octets in length. It contains the receive sequence counter (RSC) for the GTK being installed.
Key MIC : The EAPOL Key MIC is a MIC of the EAPOL-Key frames, from and including the EAPOL protocol version field to and including the Key Data field
Key Data Length : This represents the length of the Key Data field in octets
Key Data : This field is a variable-length field that is used to include any additional data required for the key exchange that is not included in the fields of the EAPOL-Key frame
该字段是一个可变长度字段，用于包含密钥交换所需的任何附加数据，这些数据未包含在 EAPOL-Key 帧的字段中
KDE : key data cryptographic encapsulation(s) 密钥数据加密封装 参考 Figure 12-34—KDE format



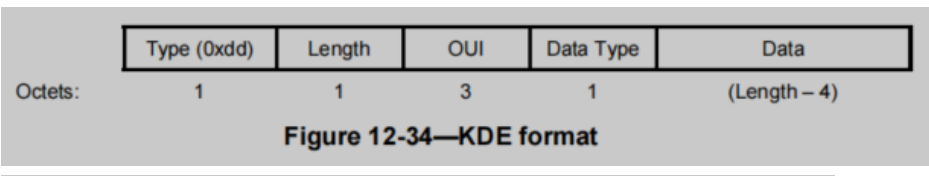
B0 B2	B3	B4 B5	B6	B7	B8	B9	B10	B11	B12	B13	B14 B15
Key Descriptor Version	Key Type	Reserved	Install	Key Ack	Key MIC	Se-cure	Error	Request	Encrypted Key Data	SMK Message	Reserved

Figure 12-33—Key Information bit layout

Table 12-4—Cipher suite key lengths



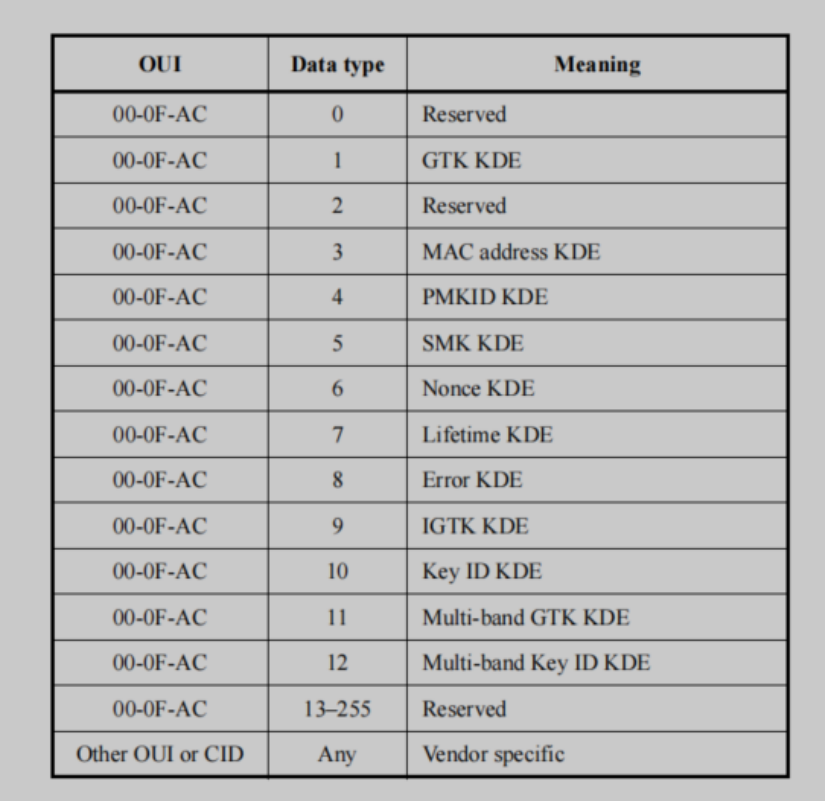
Cipher suite	Key length (octets)	TK_bits (bits)
WEP-40	5	40
WEP-104	13	104
TKIP	32	256
CCMP-128	16	128
BIP-CMAC-128	16	128
GCMP-128	16	128
GCMP-256	32	256
CCMP-256	32	256
BIP-GMAC-128	16	128
BIP-GMAC-256	32	256
BIP-CMAC-256	32	256



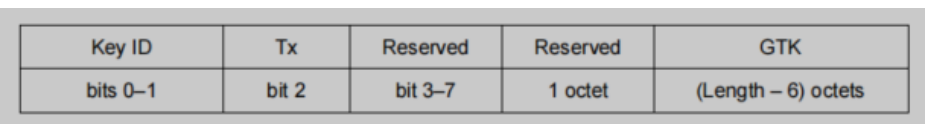
	Type (0xdd)	Length	OUI	Data Type	Data
Octets:	1	1	3	1	(Length – 4)

Figure 12-34—KDE format

Table 12-6—KDE

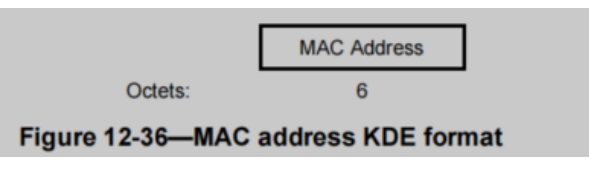


OUI	Data type	Meaning
00-0F-AC	0	Reserved
00-0F-AC	1	GTK KDE
00-0F-AC	2	Reserved
00-0F-AC	3	MAC address KDE
00-0F-AC	4	PMKID KDE
00-0F-AC	5	SMK KDE
00-0F-AC	6	Nonce KDE
00-0F-AC	7	Lifetime KDE
00-0F-AC	8	Error KDE
00-0F-AC	9	IGTK KDE
00-0F-AC	10	Key ID KDE
00-0F-AC	11	Multi-band GTK KDE
00-0F-AC	12	Multi-band Key ID KDE
00-0F-AC	13–255	Reserved
Other OUI or CID	Any	Vendor specific



Key ID	Tx	Reserved	Reserved	GTK
bits 0–1	bit 2	bit 3–7	1 octet	(Length – 6) octets

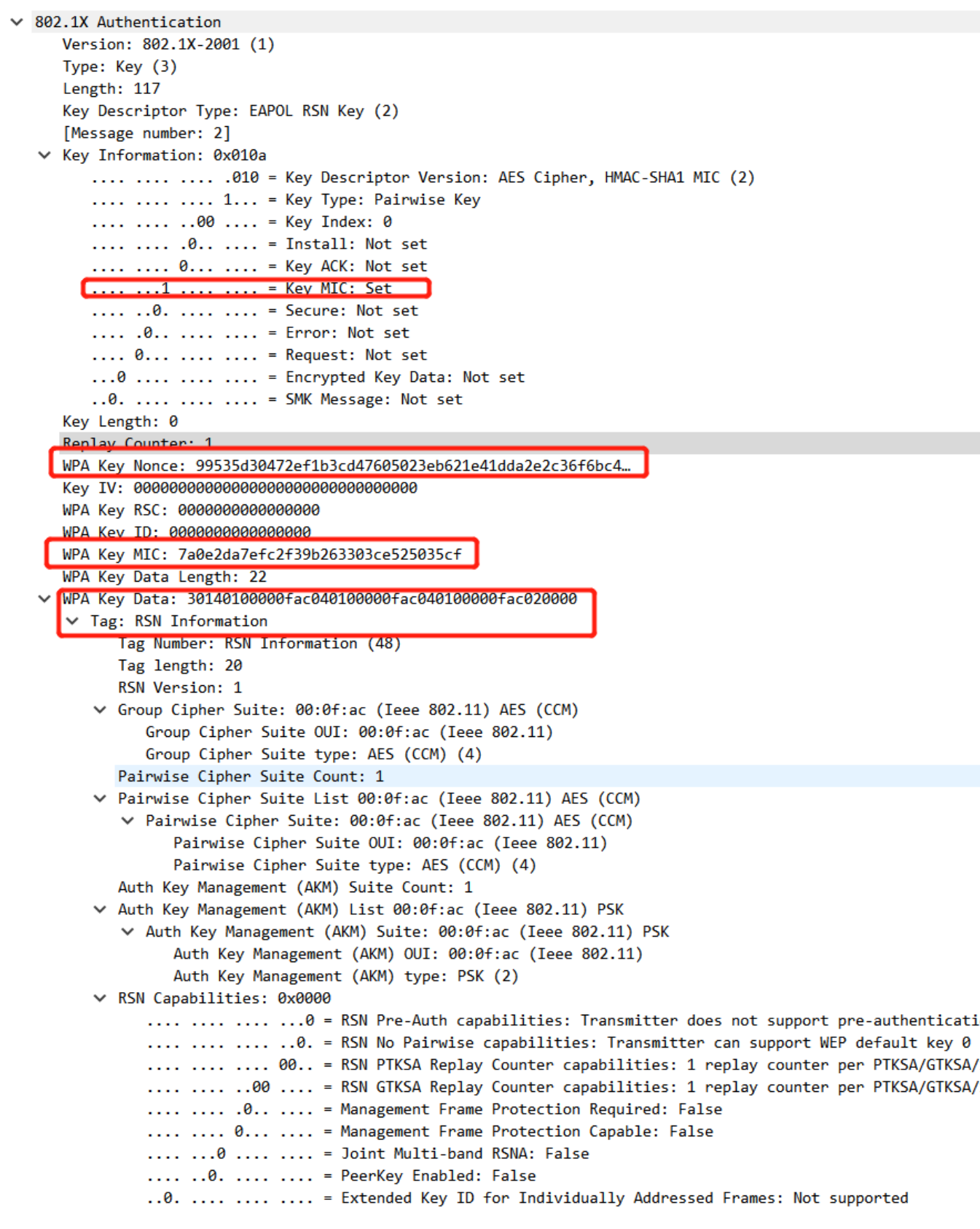
Figure 12-35—GTK KDE format



	MAC Address
Octets:	6

Figure 12-36—MAC address KDE format

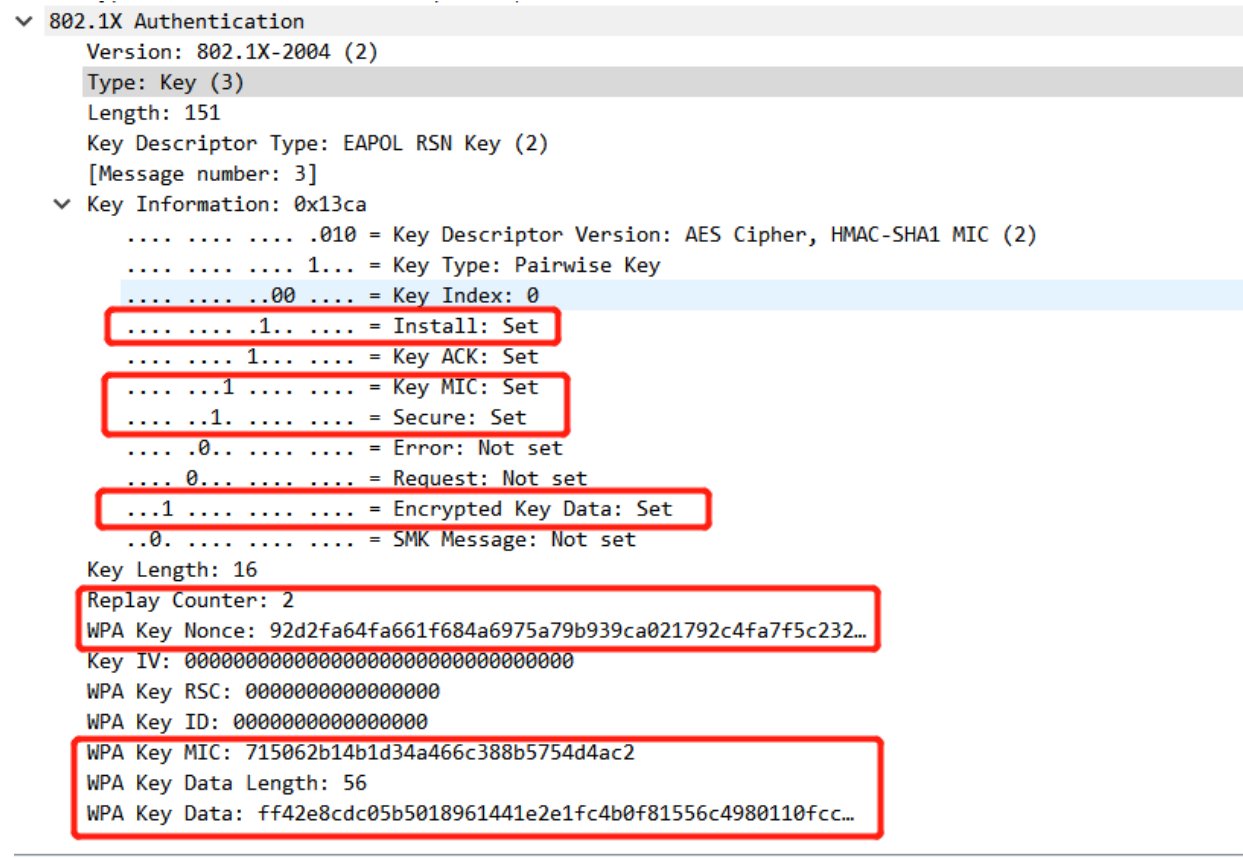
四次握手 Message 2 of 4
相比于1/4的变化部分



```
∨ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 2]
  ∨ Key Information: 0x010a
      .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .0.. .... = Install: Not set
      .... .... 0... .... = Key ACK: Not set
      .... ...1 .... .... = Key MIC: Set
      .... ..0. .... .... = Secure: Not set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...0 .... .... .... = Encrypted Key Data: Not set
      ..0. .... .... .... = SMK Message: Not set
    Key Length: 0
    Replay Counter: 1
    WPA Key Nonce: 99535d30472ef1b3cd47605023eb621e41dda2e2c36f6bc4…
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 7a0e2da7efc2f39b263303ce525035cf
    WPA Key Data Length: 22
  ∨ WPA Key Data: 30140100000fac040100000fac040100000fac020000
    ∨ Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 20
        RSN Version: 1
      ∨ Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
          Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
          Group Cipher Suite type: AES (CCM) (4)
        Pairwise Cipher Suite Count: 1
      ∨ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        ∨ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
            Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
            Pairwise Cipher Suite type: AES (CCM) (4)
        Auth Key Management (AKM) Suite Count: 1
      ∨ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
        ∨ Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
            Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
            Auth Key Management (AKM) type: PSK (2)
      ∨ RSN Capabilities: 0x0000
          .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
          .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with …
          .... .... .... 00.. = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
          .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
          .... .... .0.. .... = Management Frame Protection Required: False
          .... .... 0... .... = Management Frame Protection Capable: False
          .... ...0 .... .... = Joint Multi-band RSNA: False
          .... ..0. .... .... = PeerKey Enabled: False
          ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
```

1.存在Key MIC字段
2.KEY Data字段是一个RSN Element
CCMP作为成对加密套件和组加密套件
PSK作为认证密钥管理方法

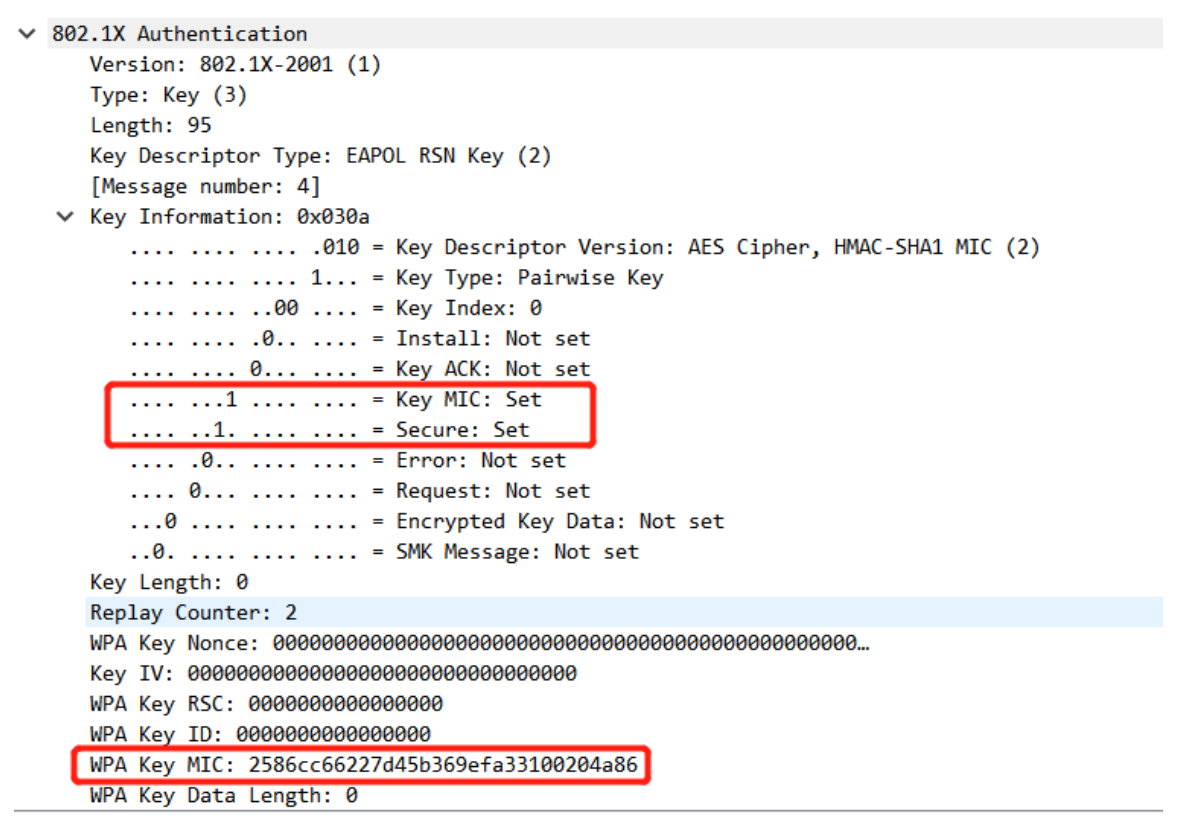
四次握手 Message 3 of 4
相比于1/4的变化部分



```
∨ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 151
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 3]
  ∨ Key Information: 0x13ca
      .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .1.. .... = Install: Set
      .... .... 1... .... = Key ACK: Set
      .... ...1 .... .... = Key MIC: Set
      .... ..1. .... .... = Secure: Set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...1 .... .... .... = Encrypted Key Data: Set
      ..0. .... .... .... = SMK Message: Not set
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 92d2fa64fa661f684a6975a79b939ca021792c4fa7f5c232…
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 715062b14b1d34a466c388b5754d4ac2
    WPA Key Data Length: 56
    WPA Key Data: ff42e8cdc05b5018961441e2e1fc4b0f81556c4980110fcc…
```

1.存在Key MIC字段
2.Install (bit 6): Key Type (bit 3)=1时 该位才有意义，value=0表示不需要配置临时密钥给STA
If the value of Key Type (bit 3) is 1, then for the Install bit,
— The value 1 means the IEEE 802.1X component shall configure the temporal key derived from this message into its IEEE 802.11 STA.
3.Secure (bit 9) is set to 1 once the initial key exchange is complete.
=1表示初始化的密钥交换已经完成
4.Encrypted Key Data (bit 12) is set to 1 if the Key Data field is encrypted and is set to 0 if the Key Data field is not encrypted.
设置为1表示Key数据是否加密

四次握手 Message 4 of 4
相比于1/4的变化部分



```
∨ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 4]
  ∨ Key Information: 0x030a
      .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .0.. .... = Install: Not set
      .... .... 0... .... = Key ACK: Not set
      .... ...1 .... .... = Key MIC: Set
      .... ..1. .... .... = Secure: Set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...0 .... .... .... = Encrypted Key Data: Not set
      ..0. .... .... .... = SMK Message: Not set
    Key Length: 0
    Replay Counter: 2
    WPA Key Nonce: 000000000000000000000000000000000000000000000000…
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 2586cc66227d45b369efa33100204a86
    WPA Key Data Length: 0
```

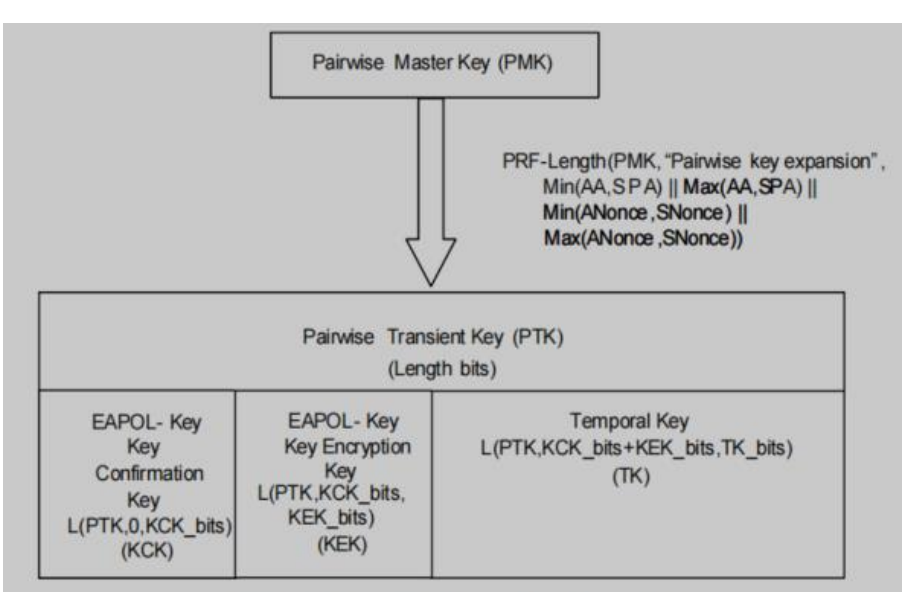

Pairwise Master Key (PMK)
PRF-Length(PMK, "Pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) || Min(ANonce,SNonce) || Max(ANonce,SNonce))
Pairwise Transient Key (PTK)
(Length bits)
EAPOL- Key Key Confirmation Key L(PTK,0,KCK_bits) (KCK)
EAPOL- Key Key Encryption Key L(PTK,KCK_bits, KEK_bits) (KEK)
Temporal Key L(PTK,KCK_bits+KEK_bits,TK_bits) (TK)

Figure 12-28—Pairwise key hierarchy

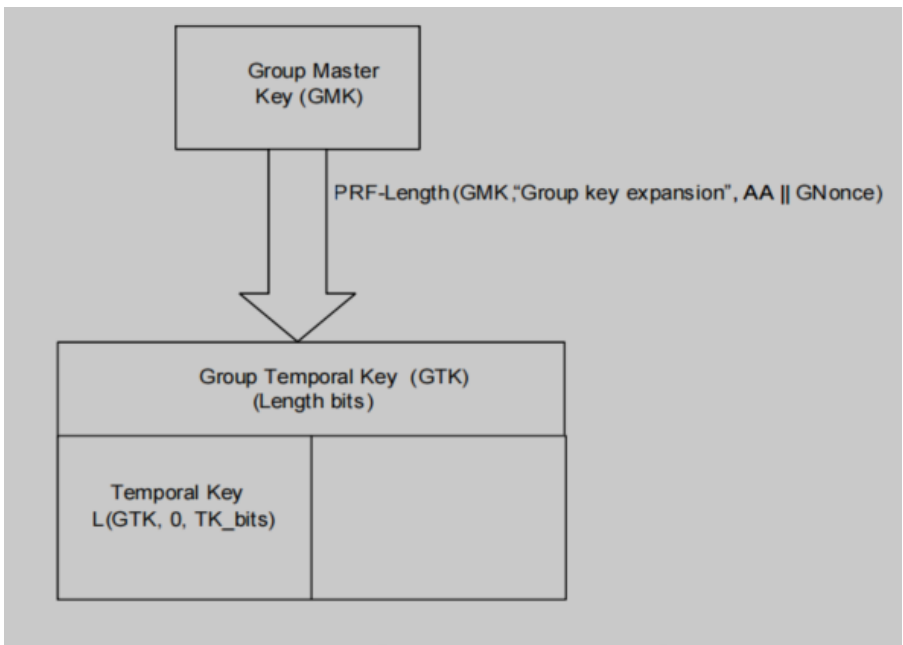


Figure 12-29—Group key hierarchy (informative)

12.7 Keys and key distribution 密钥与密钥派生
RSNA defines the following key hierarchies:
a) Pairwise key hierarchy, to protect individually addressed traffic 成对密钥是保护单播数据
b) GTK, a hierarchy consisting of a single key to protect group addressed traffic 组临时密钥是保护组播数据
c) Integrity GTK (IGTK), a hierarchy consisting of a single key to provide integrity protection for group addressed robust Management frames IGTK是保护组播管理帧

PTK : Pairwise Transient Key 成对瞬态密钥
GTK : Group Temporal Key 组临时密钥

12.7.4 EAPOL-Key frame notation，帧格式数学表示
EAPOL-Key(S, M, A, I, K, SM, KeyRSC, ANonce/SNonce, MIC, DataKDs)
S means the initial key exchange is complete. This is the Secure bit of the Key Information field.
M means the MIC is available in message. This should be set in all messages except message 1 of a 4-way handshake. This is the Key MIC bit of the Key Information field.
A means a response is required to this message. This is used when the receiver should respond to this message. This is the Key Ack bit of the Key Information field.
I is the Install bit: Install/Not install for the pairwise key. This is the Install bit of the Key Information field.
K is the key type: P (Pairwise), G (Group/SMK). This is the Key Type bit of the Key Information field.
SM is the SMK Message bit: indicates that this message is part of SMK handshake.
KeyRSC is the key RSC. This is the Key RSC field. contains the receive sequence counter (RSC) for the GTK being installed
ANonce/SNonce is the Authenticator/Supplicant nonce. This is the Key Nonce field.
MIC is the integrity check, which is generated using the KCK. This is the Key MIC field.
DataKDs is a sequence of zero or more elements and KDEs, contained in the Key Data field,
which may contain the following:
RSNE is described in 9.4.2.25.
RSNE[KeyName] is the RSNE, with the PMKID field set to KeyName.
GTK[N] is the GTK, with the key identifier field set to N. The key identifier specifies which index is used for this GTK. Index 0 shall not be used for GTKs,except in mixed environments, as described in 12.7.1.
FTE is the Fast BSS Transition element, described in 9.4.2.48
MDE is the Mobility Domain element, described in 9.4.2.47
TIE[IntervalType] is a Timeout Interval element of type IntervalType, as described in 9.4.2.49,containing e.g., for type KeyLifetime, the lifetime of the FT key hierarchy.
IGTK[M] is the IGTK, with key identifier field set to M.
IPN is the current IGTK replay counter value provided by the IGTK KDE
PMKID is of type PMKID KDE and is the key identifier used during 4-way PTK handshake for PMK identification and during 4-way STK handshake for SMK identification.
Lifetime is the key lifetime KDE used for sending the expiration timeout value for SMK used during PeerKey handshake for SMK identification.
Initiator MAC is the Initiator MAC KDE used during PeerKey handshake
Peer MAC is the Peer MAC KDE used during PeerKey handshake
Initiator Nonce is the Initiator Nonce KDE used during PeerKey handshake. This is used when multiple nonces need to be sent.
Peer Nonce is the Peer Nonce KDE used during PeerKey handshake. This is used when multiple nonces need to be sent.
SMK KDE is the SMK during SMK handshake.
Error KDE is an error KDE used when error bit E is equal to 1 during PeerKey handshake.

12.7.6 4-way handshake 为了完成802.1X的认证流程
RSNA defines a protocol using EAPOL-Key frames called the 4-way handshake. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-way handshake is as follows:
Message 1: Authenticator--->Supplicant: EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,DataKD_M1)
where DataKD_M1 = 0 or PMKID for PTK generation, or PMKID KDE (for sending SMKID) for STK generation

Message 2: Supplicant--->Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,DataKD_M2)
where DataKD_M2 = RSNE for creating PTK generation or peer RSNE, Lifetime KDE, SMKID KDE (for sending SMKID) for STK generation

Message 3: Authenticator--->Supplicant: EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,DataKD_M3)
where DataKD_M3 = RSNE,GTK[N] for creating PTK generation or initiator RSNE, Lifetime KDE for STK generation

Message 4: Supplicant--->Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,DataKD_M4)
where DataKD_M4 = 0.

Key Replay Counter field:当收到的EAPOL-KEY帧的该字段大于本地的字段，表明不是当前的EAPOL-KEY数据帧

四次握手过程详解

12.7.6.2 4-way handshake message 1

The Authenticator sends message 1 to the Supplicant at the end of a successful IEEE 802.1X authentication, after (re)association completes for a STA that has authenticated with SAE or PSK authentication is negotiated, when a cached PMKSA is used, or after a STA requests a new key. On reception of message 1,the Supplicant determines whether the Key Replay Counter field value has been used before with the current PMKSA If the Key Replay Counter field value is less than or equal to the current local value, the Supplicant discards the message. Otherwise, the Supplicant:

Auth发送Message 1,Supp接收到以后检查Key Replay Counter field字段,检查OK Supp就会生成随机数，派生PTK, 构造消息2

a) Generates a new nonce SNonce.
b) Derives PTK.
c) Constructs message 2.

12.7.6.3 4-way handshake message 2

included RSNE – the sending STA’s RSNE for PTK generation
包含RSN Element字段，用于生成PTK

Processing for PTK generation is as follows: PTK的生成如下
The Supplicant sends message 2 to the Authenticator.
On reception of message 2, the Authenticator checks that the key replay counter corresponds to the outstanding message 1. If not, it silently discards the message. Otherwise, the Authenticator:
Auth收到message 2以后检查replay counter,检查通过就会
a) Derives PTK.派生PTK
b) Verifies the message 2 MIC. 验证MIC
1) If the calculated MIC does not match the MIC that the Supplicant included in the EAPOL-Key frame, the Authenticator silently discards message 2.
验证MIC不通过，auth就会丢弃Message 2不处理
2) If the MIC is valid and this message 2 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the Authenticator checks that all fields of the RSNE other than the PMKID field bitwise matches the fields from the (Re)Association Request frame and that the FTE and MDE are the same as those provided in the AP’s (Re)Association Response frame.
If the MIC is valid and this message 2 is not part of a fast BSS transition initial mobility domain association and this message 2 is not part of an association started through the FT protocol, the Authenticator checks that the RSNE bitwise matches that from the (Re)Association Request frame.
i) If these are not exactly the same, the Authenticator uses MLME-DEAUTHENTICATE.request primitive to terminate the association.
ii) If they do match bitwise, the Authenticator constructs message 3. 字段能都匹配构造消息3

12.7.6.4 4-way handshake message 3

if a group cipher has been negotiated, the GTK and the GTK’s key identifier (see 12.7.2) for the current operating band, and if management frame protection is negotiated, the IGTK KDE
组密钥被协商KEY Data字段就会携带GTK ,如果支持管理帧保护就会携带IGTK
a) Verifies the RSNE
b) Verifies the message 3 MIC
c) Updates the last-seen value of the Key Replay Counter field
e) Constructs message 4.
f) Sends message 4 to the Authenticator.

12.7.6.5 4-way handshake message 4

On reception of message 4, the Authenticator verifies that the Key Replay Counter field value is one that it used on this 4-way handshake; if it is not, it silently discards the message. Otherwise:
a) The Authenticator checks the MIC.
b) If the MIC is valid, the Authenticator uses the MLME-SETKEYS.request primitive to configure the IEEE 802.11 MAC to send
c) The Authenticator updates the Key Replay Counter field

12.7.6.7 Sample 4-way handshake

The 4-way handshake consists of the following steps:
a) The Authenticator sends an EAPOL-Key frame containing an ANonce.
b) The Supplicant derives a PTK from ANonce and SNonce.
c) The Supplicant sends an EAPOL-Key frame containing SNonce, the RSNE from the (Re)Association Request frame, and a MIC.
d) The Authenticator derives PTK from ANonce and SNonce and validates the MIC in the EAPOL-Key frame.
e) The Authenticator sends an EAPOL-Key frame containing ANonce, the RSNE from its Beacon or Probe Response frames, the MIC, the GTK, an indication of whether to install the temporal keys, and if management frame protection is negotiated, the IGTK.
f) The Supplicant sends an EAPOL-Key frame to confirm whether the temporal keys were installed

The PTK and GTK are installed by using MLME-SETKEYS.request primitive after message 4 is sent. The PTK is installed before the GTK
在Message 4之后才会安装PTK GTK,PTK优先安装

12.7.7 Group key handshake

The Authenticator uses the Group key handshake to send a new GTK and, if management frame protection is negotiated, a new IGTK to the Supplicant.
AUTH使用组密钥握手去向Supp更新GTK和IGTK

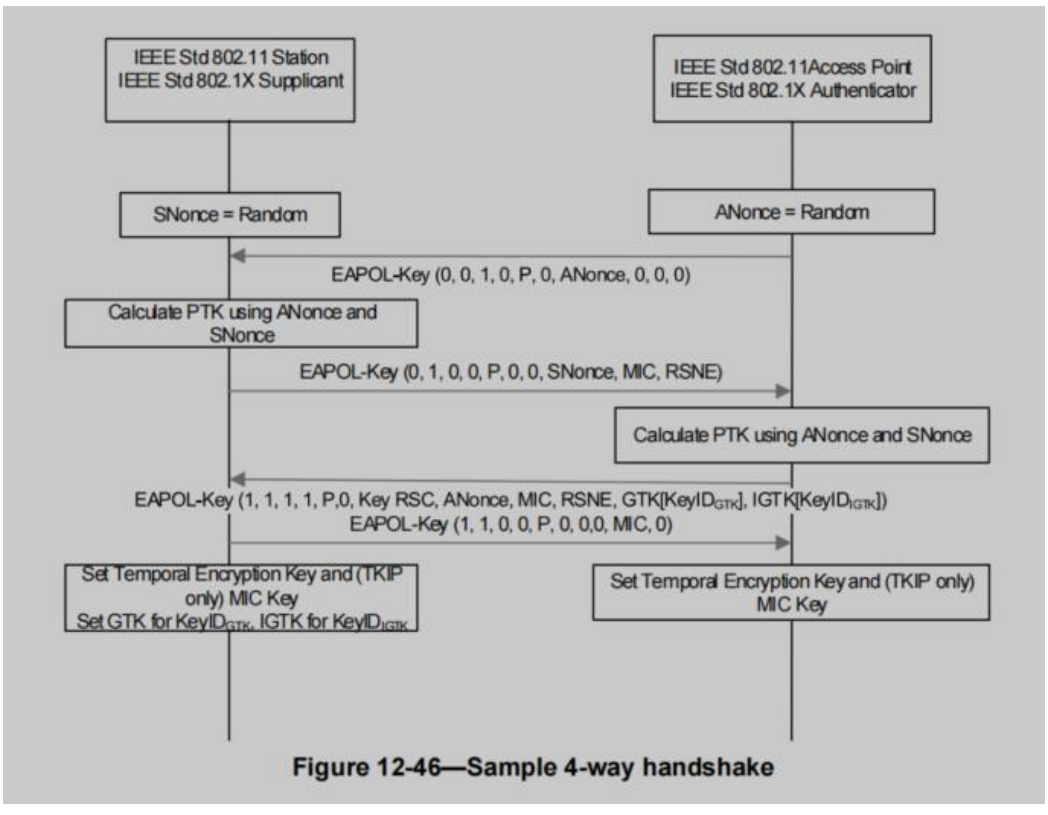

IEEE Std 802.11 Station
IEEE Std 802.1X Supplicant
IEEE Std 802.11 Access Point
IEEE Std 802.1X Authenticator
SNonce = Random
ANonce = Random
EAPOL-Key (0, 0, 1, 0, P, 0, ANonce, 0, 0, 0)
Calculate PTK using ANonce and SNonce
EAPOL-Key (0, 1, 0, 0, P, 0, 0, SNonce, MIC, RSNE)
Calculate PTK using ANonce and SNonce
EAPOL-Key (1, 1, 1, 1, P,0, Key RSC, ANonce, MIC, RSNE, GTK[KeyIDGTK], IGTK[KeyIDIGTK])
EAPOL-Key (1, 1, 0, 0, P, 0, 0,0, MIC, 0)
Set Temporal Encryption Key and (TKIP only) MIC Key
Set GTK for KeyIDGTK, IGTK for KeyIDIGTK
Set Temporal Encryption Key and (TKIP only) MIC Key

Figure 12-46—Sample 4-way handshake