参考 5.9.3 Model description 模型描述，分为使用IEEE 802.1X Authentication Server 和 Pre-shared Key 两种情况
EAP authentication packets (contained in IEEE 802.11 MAC data frames) EAP是一个802.11的数据帧
使用IEEE 802.1X Authentication Server 使用802.1X认证服务器，authentication and key management operations AKM的流程如下

1. The Authenticator and Authentication Server authenticate each other and create a secure channel between them (the possibilities include RADIUS, IPsec, TLS). The security of the channel between the Authenticator and the Authentication Server is outside the scope of this specification.

创建安全的通道 RADIUS, IPsec, TLS

2. The Supplicant and Authentication Server authenticate each other (e.g., possibilities include EAP-TLS and PEAP) and must generate a Master Key. The authentication must be carried over the Authenticator/Authentication Server secure channel. In addition, there must be crypto-separation over the Authenticator/Authentication Server secure channel for each Supplicant.

生成Master Key

3. A Pairwise Master Key (PMK) is generated for use between the Supplicant and Authenticator. The PMK is generated from the EAP master key that is obtained from the Supplicant/Authentication Server authentication.

从EAP Master Key生成PMK

4. A 4-way handshake utilizing EAPOL-Key messages occurs between the Supplicant and Authenticator to
   a. Confirm the existence of the PMK;
   b. Confirm that the PMK is current;
   c. Derive the Pairwise Transient Key from the PMK;
   d. Install the encryption and integrity keys into IEEE 802.11;
   e. Confirm the installation of the keys.

四次握手由PMK生成PTK

5. The Group Transient Key is sent from the Authenticator to the Supplicant to allow the Supplicants to receive
组瞬态密钥由Auth 发往 Supp,使用EAPOL-KEY message

使用Pre-shared Key，AKM的流程如下

1. A Pairwise master key (PMK) is generated for use between the Supplicant and Authenticator. The PMK is the Pre-Shared Key in this case. PMK就是PSK
2. The 4-way handshake using EAPOL-Key messages is used just as in the Authentication Server case. 四次握手的流程同802.1X Authentication Server
3. The Group Transient Key is sent from the Authenticator to the Supplicant just as in the Authentication Server case

没有PMK生成的阶段，直接使用PSK作为PMK

5.9.3.1 Frame exchange overview 帧交换概述

the STA must perform IEEE 802.11 Open System Authentication and associate to the AP.
These steps allow the STA and AP to negotiate security association characteristics, including the authenticated key management, unicast and multicast cipher suites employed.
协商AKM(PSK/802.1X Auth Servicer) ,单播组播加密套件
Figure 2 depicts how a STA discovers an AP and negotiates a security policy.

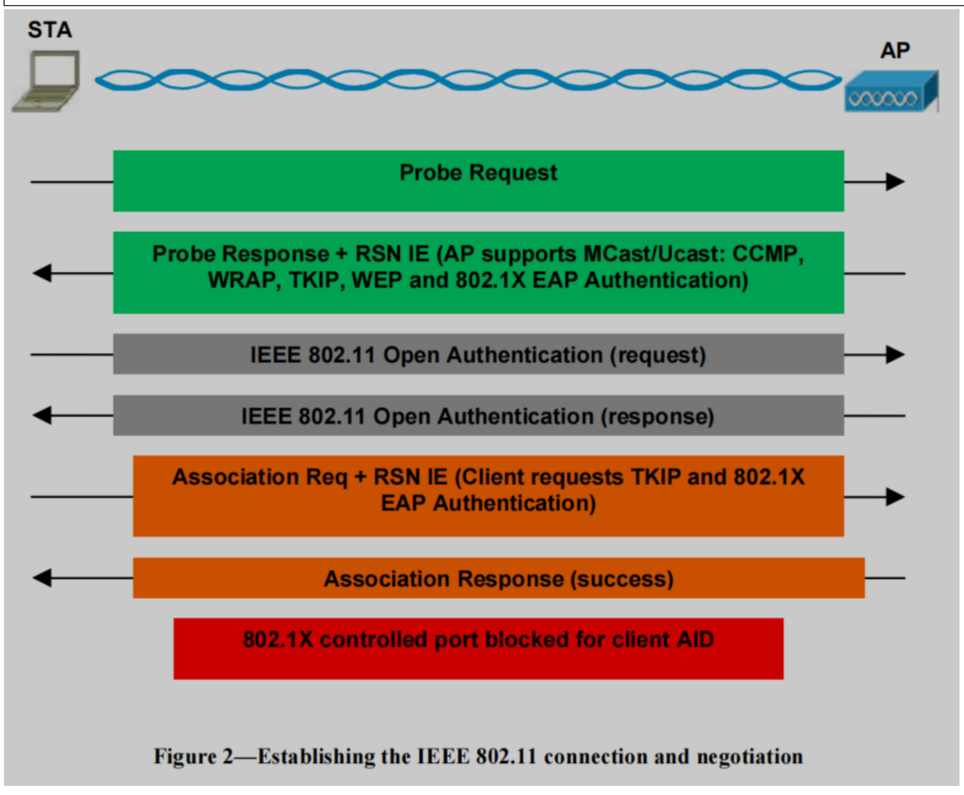

Figure 2—Establishing the IEEE 802.11 connection and negotiation

Once the STA and AP successfully establish a common security policy, both filter both data traffic, restricting this to IEEE 802.1X EAP authentication frames. In the next phase the STA to successfully authenticate with an Authentication Server (AS), as depicted by Figure 3.
连接协商好安全策略以后（AKM 和 Cipher suits），会过滤数据流量,仅仅允许 IEEE 802.1X EAP authentication frames 认证数据帧通过。802.1X认证服务器的认证流程如图三，PSK的AKM流程不会经过图三

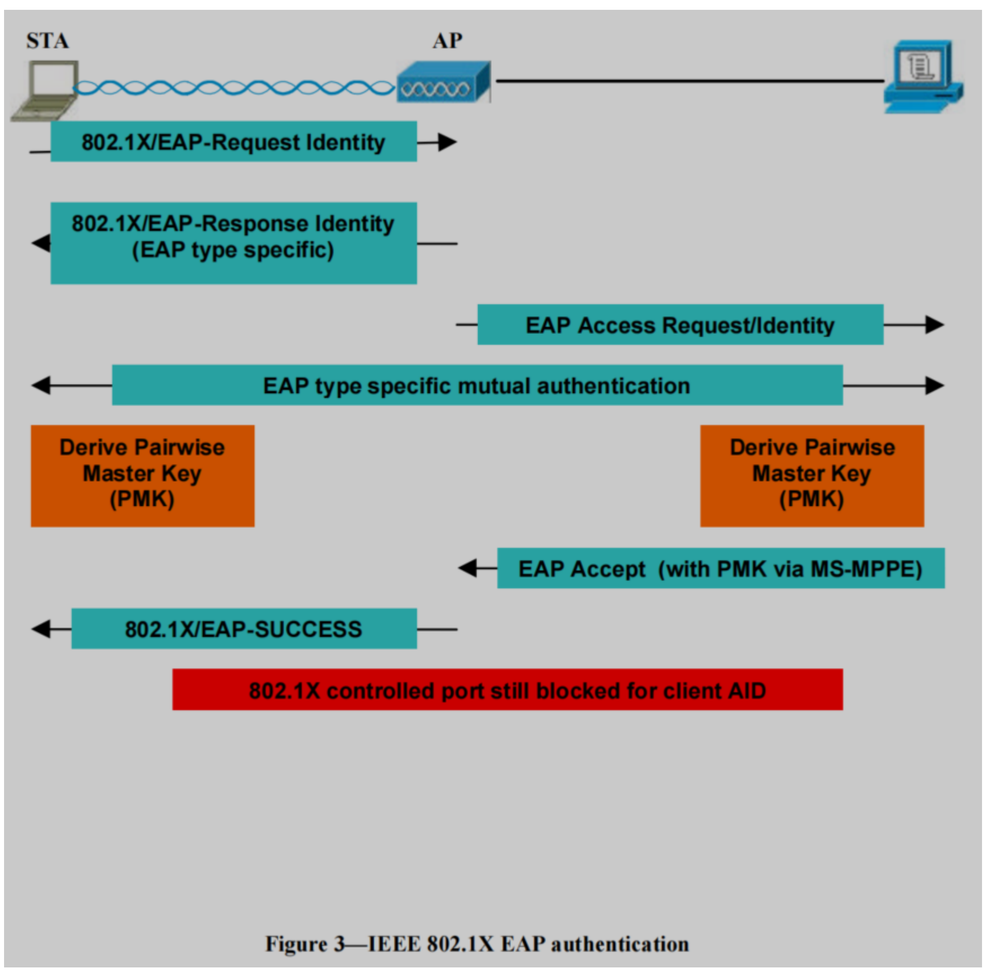

Figure 3—IEEE 802.1X EAP authentication

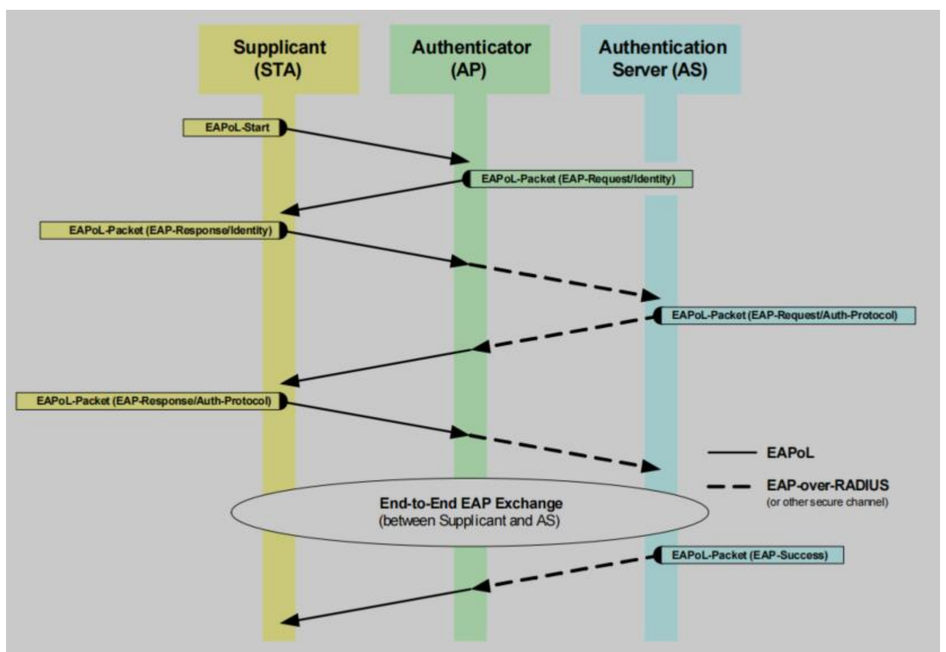

Figure 40—IEEE 802.1X authentication exchange

使用四次握手派生PTK保护单播流量数据，GTK保护组播流量数据

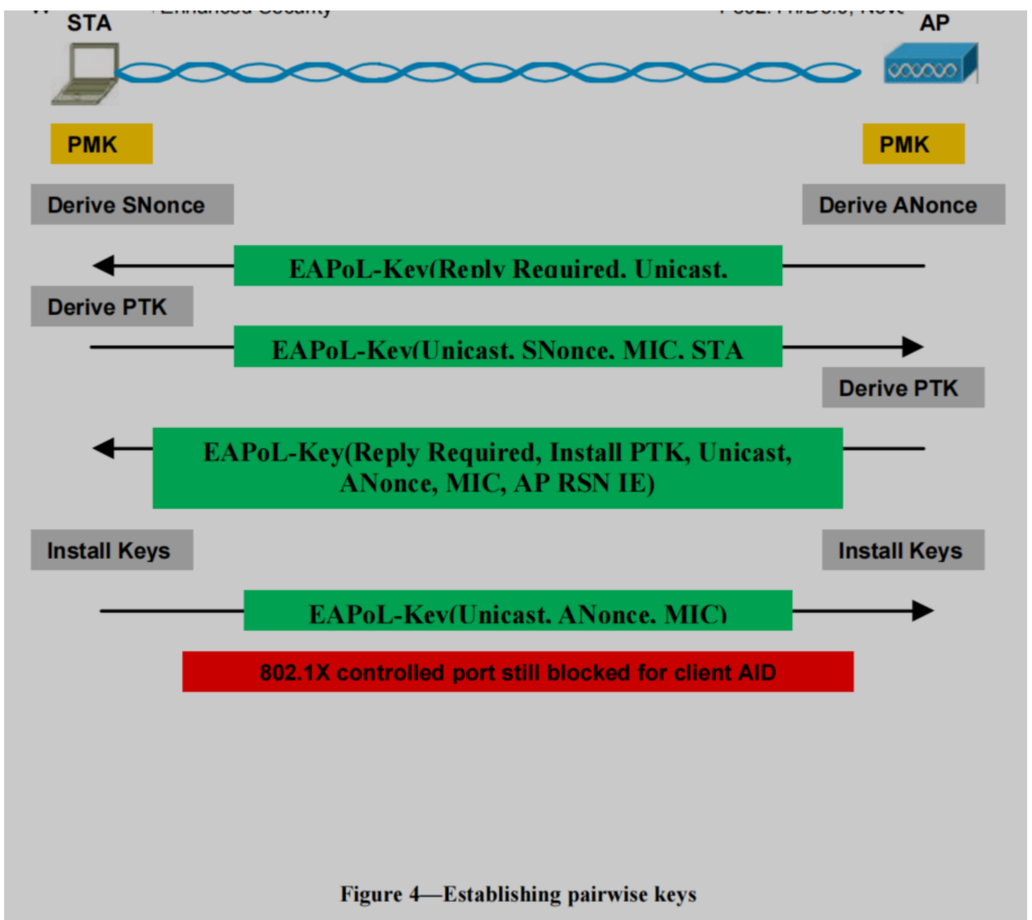

Figure 4—Establishing pairwise keys

Once the STA and AP have authentication and established a fresh pairwise key, the AP can use it to deliver the key required to protect multicast traffic, the Group Transient Key (GTK). This last phase is achieved with a two message exchange, called the Group Key Handshake
Auth使用组握手来向Supp发送GTK ,用于保护组播数据

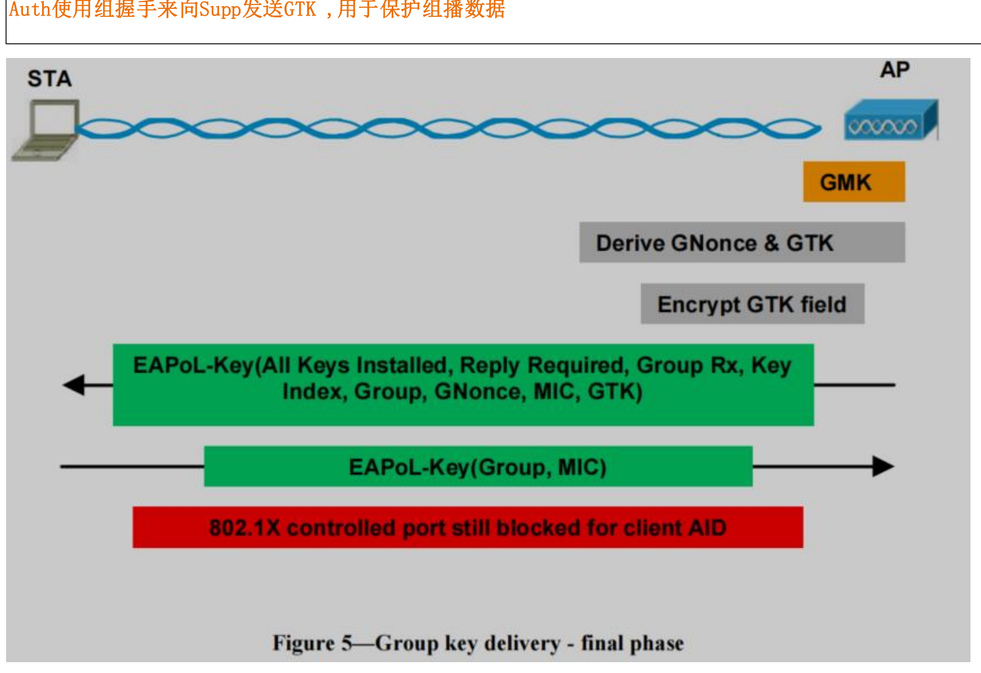

Figure 5—Group key delivery - final phase