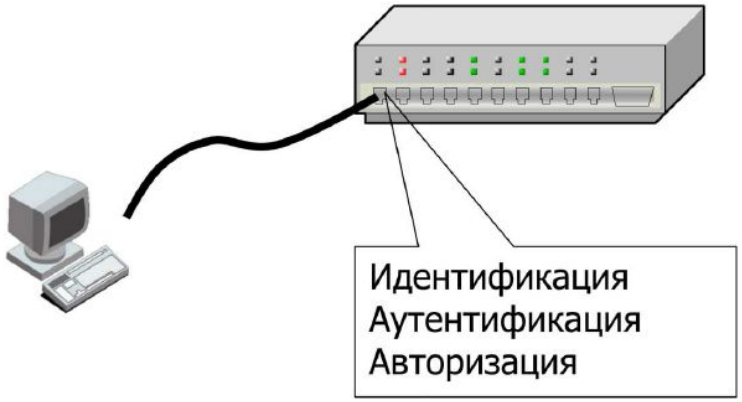
Стандарт 802.1x. Безопасность на уровне порта.

Функции 802.1x

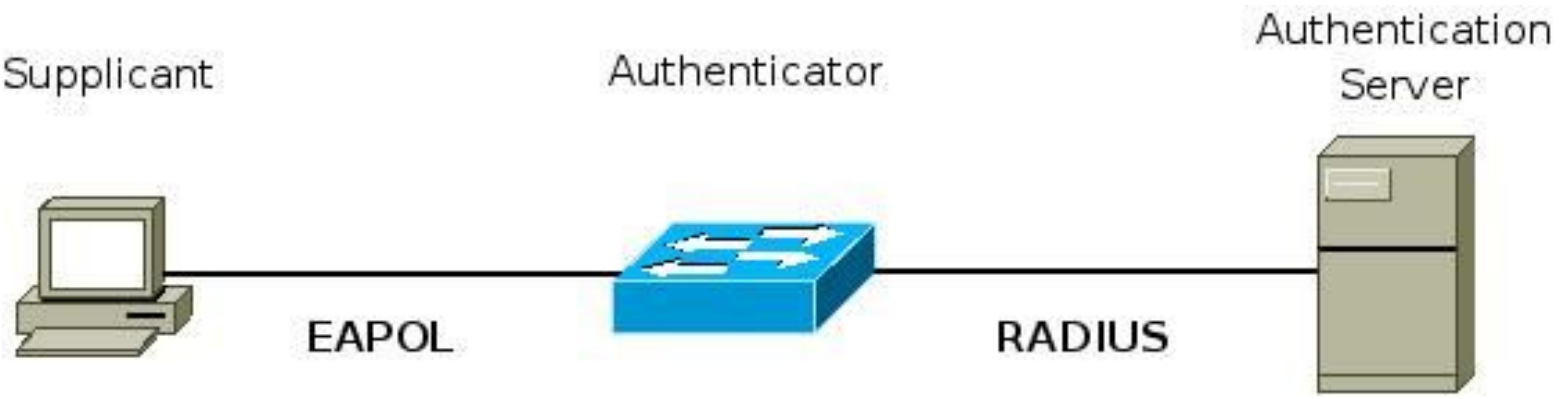
Протокол 802.1X работает на канальном уровне и определяет механизм контроля доступа к сети на основе принадлежности к порту. Под портом понимается точка подключения к сети (физический разъем или беспроводное подключение).

Доступ к сети получают только клиенты прошедшие **аутентификацию**, если аутентификация не была пройдена, доступ с соответствующего порта будет запрещен.

802.1X предполагает использование модели точка-точка (неприменим, если несколько хостов соединяются с коммутатором 802.1X через хаб или другой коммутатор.)



Роли устройств 802.1x

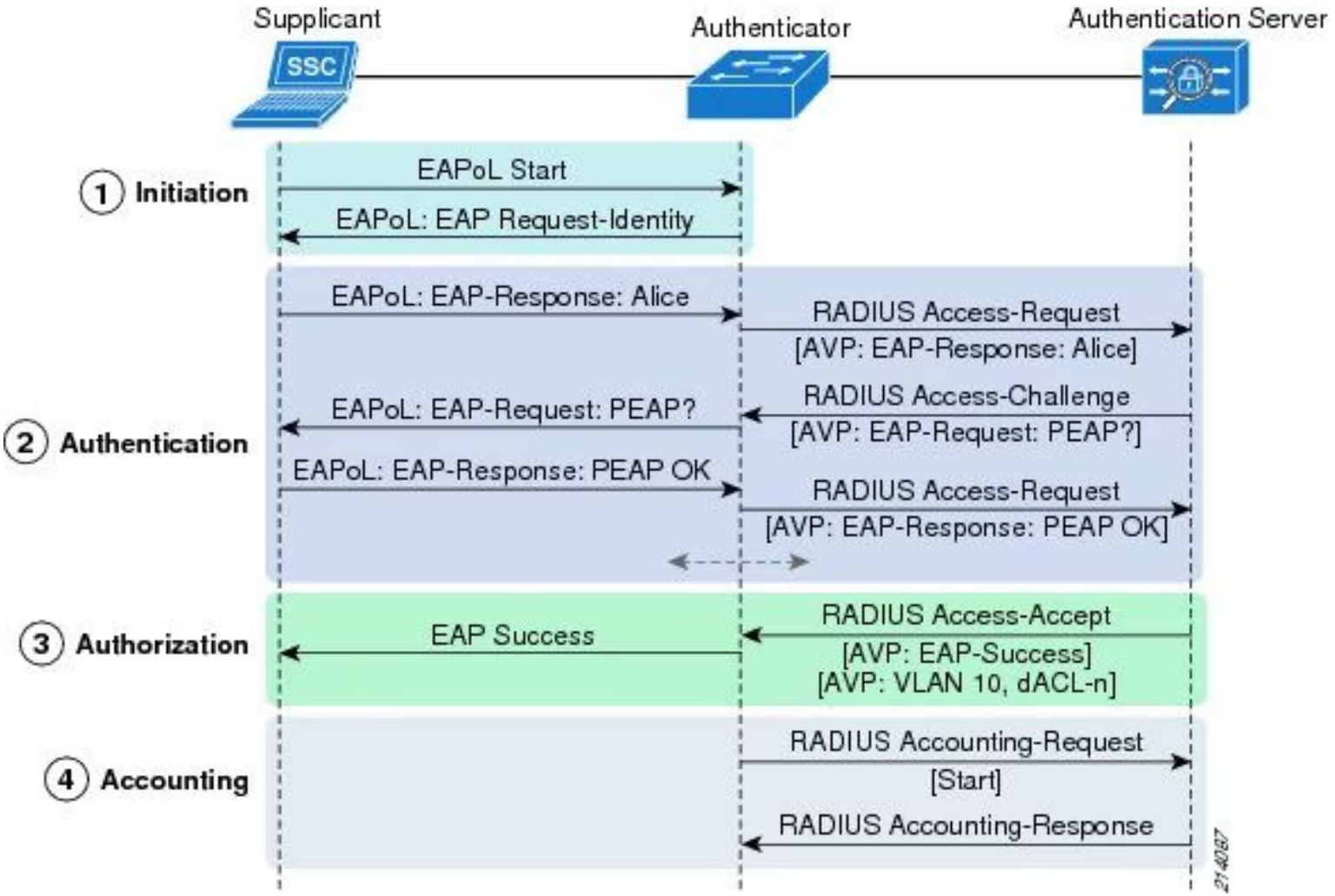


Устройство (клиент), запрашивающее доступ к сети у аутентификатора

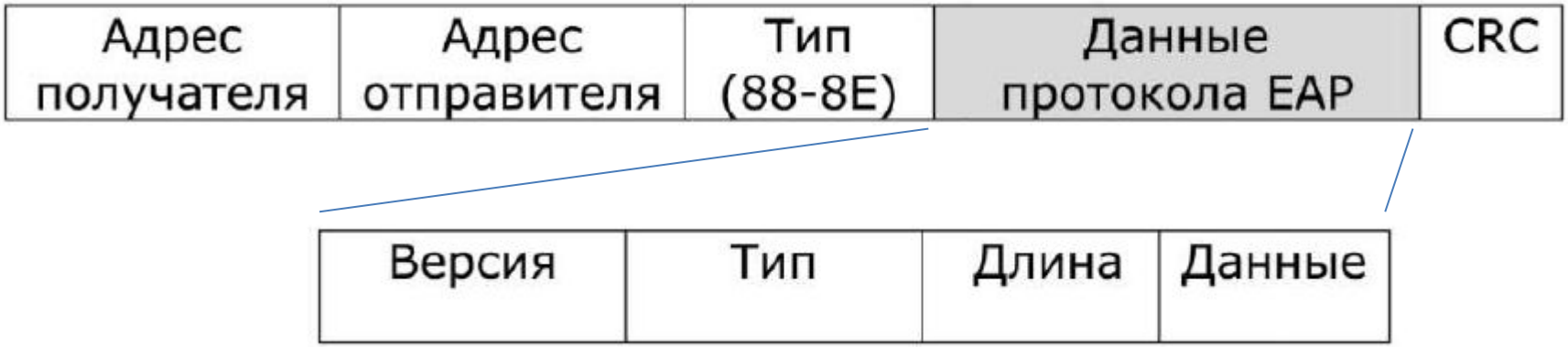
Устройство, контролирующее доступ к сети, основываясь на статусе аутентификации клиента

Устройство, выполняющее аутентификацию клиента

Работа механизма 802.1x

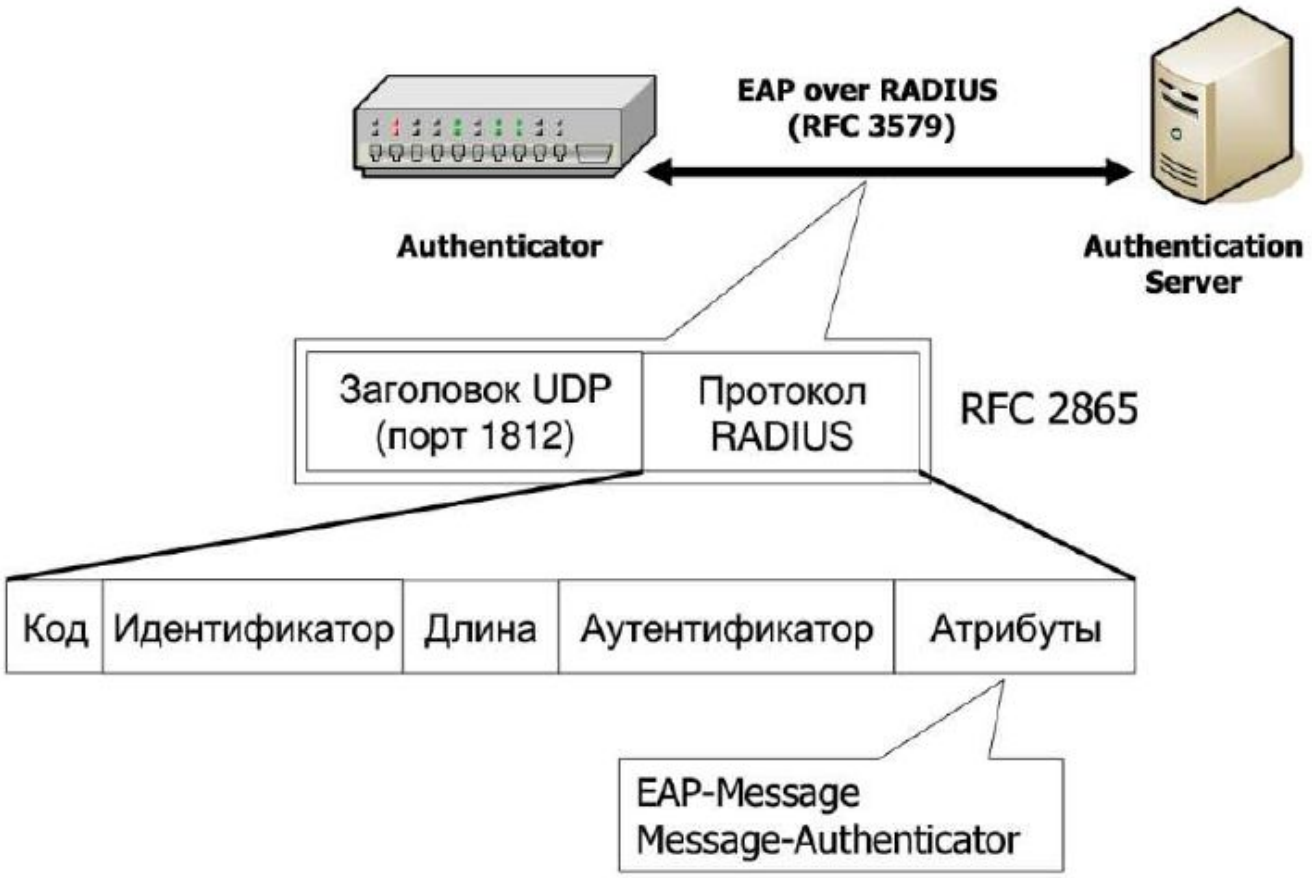


EAP over LAN (Supplicant - Authenticator)



Тип	Значение
EAP-Packet	0000 0000
EAPOL-Start.	0000 0001
EAPOL-Logoff.	0000 0010
EAPOL-Key.	0000 0011
EAPOL-Encapsulated-ASF-Alert.	0000 0100

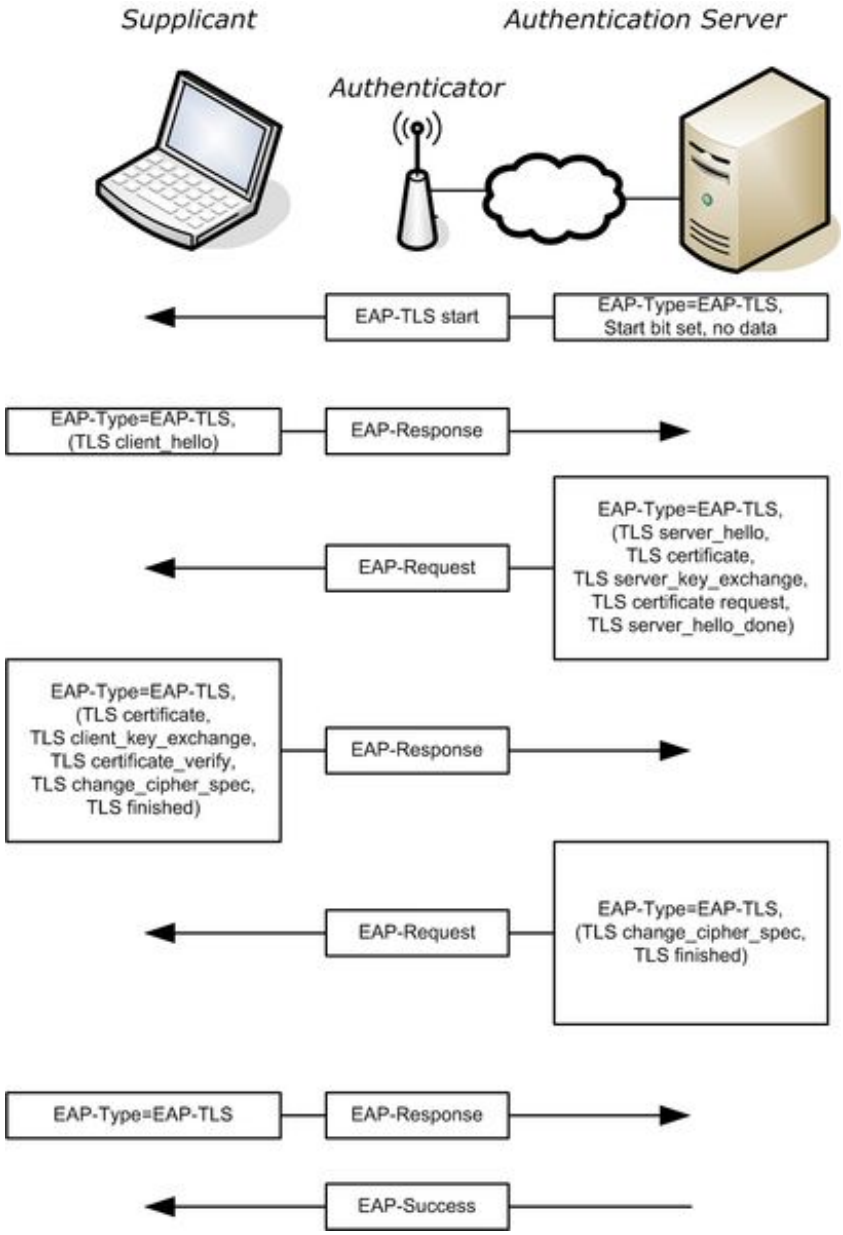
EAP over RADIUS (Authenticator – Auth Server)



Методы EAP

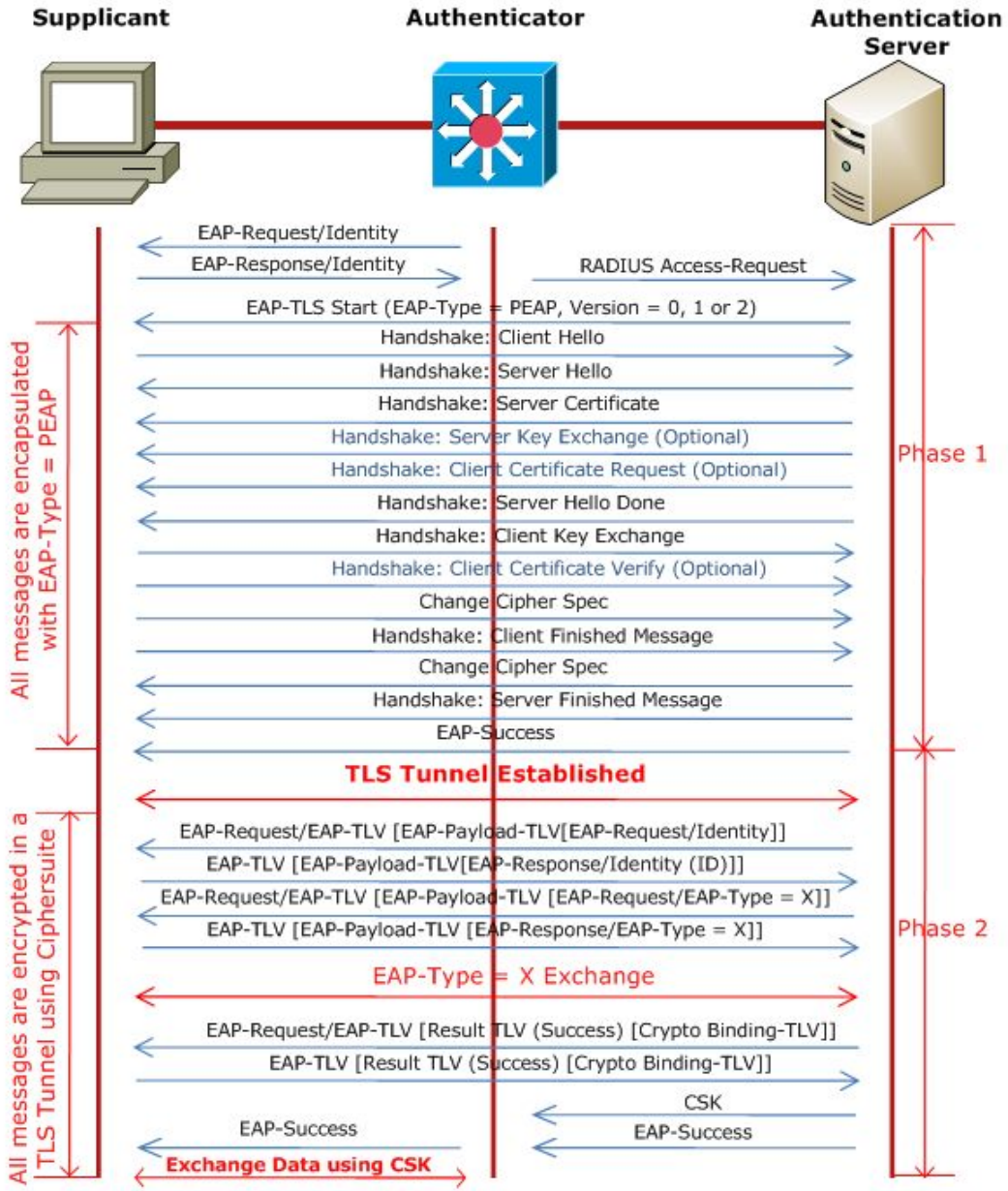
Property	*EAP Authentication Method*				
	MD5	*LEAP*	*TLS*	*TTLS*	*PEAP*
Authentication attributes	Unilateral	Mutual	Mutual	Mutual	Mutual
Deployment difficulties	Easy	Easy	Hard	Moderate	Moderate
Dynamic re-keying	No	Yes	Yes	Yes	Yes
Requires server certificate	No	No	Yes	Yes	Yes
Requires client certificate	No	No	Yes	No	No
Tunnelled	No	No	No	Yes	Yes
WPA compatible	No	Yes	Yes	Yes	Yes
WLAN security	Poor	Moderate	Strongest	Strong	Strong
Security risks	Identity exposed, dictionary attack, MITM attack	Identity exposed, dictionary attack	Identity exposed	MITM attack	MITM attack. Identity hidden in phase2 but potential exposure in Phase1

EAP-TLS



- EAP-TLS аутентифицирует как клиента, так и сервер (то есть является методом взаимной аутентификации)
- Метод требует наличие клиентского сертификата X.509
- Считается одним из наиболее безопасных стандартов.

Protected EAP



- PEAP - протокол инкапсулирующий EAP-взаимодействие внутри Transport Layer Security (TLS) туннеля.
- Предназначен для усиления стойкости EAP, который предполагает, что физический канал защищён и не применяет специальных мер для защиты обмена
- PEAP поддерживает несколько внутренних методов, но наиболее часто используемым является протокол проверки подлинности EAP Microsoft Challenge Handshake версии 2 (EAP-MSCHAPv2)