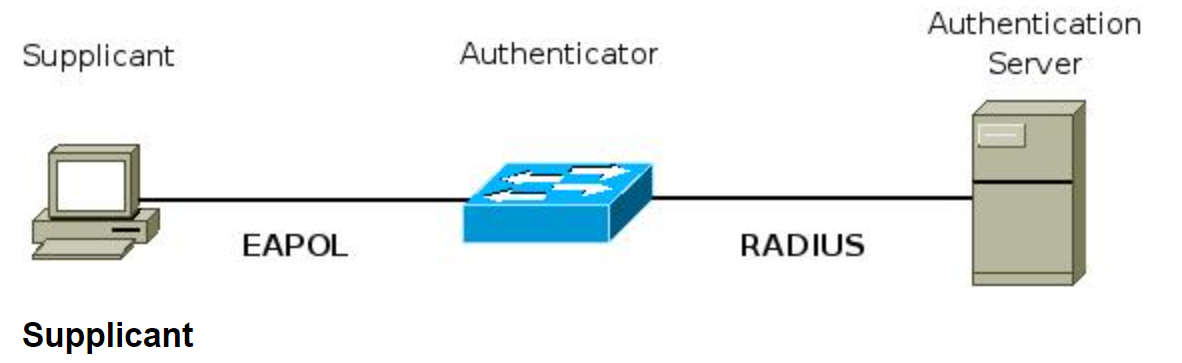
**802.1X**

Протокол 802.1X работает на канальном уровне и определяет механизм контроля доступа к сети на основе принадлежности к порту (в контексте стандарта порт — точка подключения к сети). Наибольшее распространение протокол получил в беспроводных сетях.

Согласно протоколу 802.1X доступ к сети получают только клиенты прошедшие аутентификацию, если аутентификация не была пройдена, доступ с соответствующего порта будет запрещен.



**Supplicant** — устройство (компьютер, ноутбук или др.) которое запрашивает доступ к сети у аутентификатора (коммутатора или точки доступа) и отвечает на его запросы. На клиенте должно быть установлено (или встроено) программное обеспечение работающее по протоколу 802.1X.

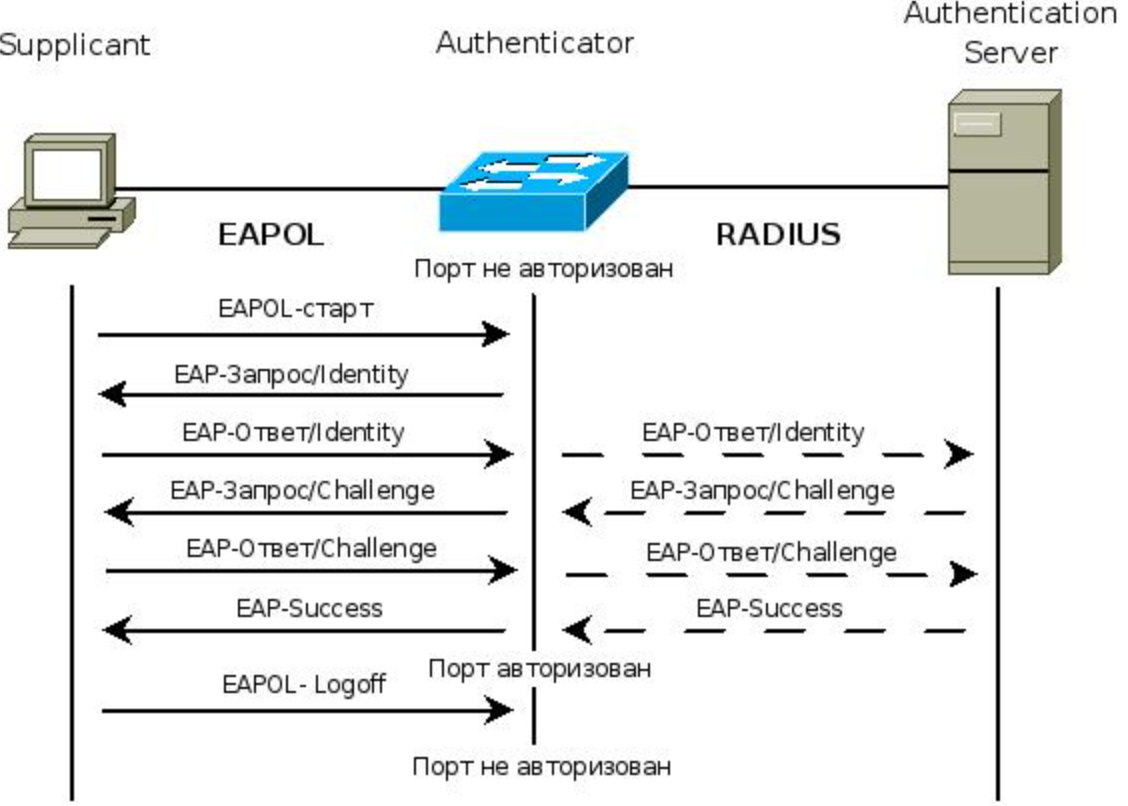
**Аутентификатор** (authenticator) — устройство контролирующее физический доступ к сети основываясь на статусе аутентификации клиента. Выполняет роль посредника (proxy) между клиентом и сервером аутентификации.

Для каждого порта коммутатора (с включенным 802.1X) создается два виртуальных порта:

* Контролируемый порт (controlled port) — открывается только после авторизации по 802.1X
* Неконтролируемый порт (uncontrolled port) — разрешает передавать только EAPOL трафик

До тех пор, пока клиент не авторизован только EAPOL трафик разрешен на неконтролируемом порту. Кроме терминов контролируемый и неконтролируемый порты применяются термины авторизованный (authorized) и неавторизованный (unauthorized) порты, соответственно.

**Сервер аутентификации** (authentication server) — осуществляет аутентификацию клиента. Сервер аутентификации проверяет identity клиента и сообщает аутентификатору разрешен ли клиенту доступ к сети.



1. Клиент отправляет сообщение EAPOL-старт аутентификатору
2. Аутентификатор отправляет клиенту EAP-Запрос и клиент отвечает EAP-ответом
3. Аутентификатор инкапсулирует ответ в формат RADIUS и пересылает ответ серверу аутентификации
4. Сервер аутентификации отправляет EAP-MD5 Challenge клиенту, а клиент присылает ответ (передает сообщения аутентификатор соответствующим образом инкапсулируя и деинкапсулируя фреймы)
5. Сервер аутентификации подтверждает подлинность клиента и сообщает аутентификатору о необходимости разрешить доступ клиента к сети
6. Аутентификатор авторизует порт и клиент получает доступ к сети

**EAP** (Extensible Authentication Protocol) - подход к процедуре аутентификации, который поддерживает различные методы аутентификации. EAP определяет формат сообщений, а каждый протокол использующий EAP определяет способ инкапсуляции сообщений EAP в свой формат.

**RADIUS** (Remote Authentication Dial In User Service, служба удалённой аутентификации дозванивающихся пользователей) — сетевой протокол, предназначенный для обеспечения централизованной аутентификации, авторизации и учёта (Authentication, Authorization, and Accounting, AAA) пользователей, подключающихся к различным сетевым службам. Используется, например, при аутентификации пользователей WiFi, VPN и других подобных случаях.

В соответствии со стандартом RADIUS, это:

* Базирующийся на UDP протокол, который не использует прямых соединений
* Использует модель безопасности hop-by-hop
* Без состояний (stateless)
* Поддерживает аутентификацию PAP и CHAP по PPP
* Использует MD5 для скрытия паролей
* Предоставляет более 50 пар атрибут/значение с возможностью создавать специфичные для производителя пары
* Поддерживает модель AAA
* Поддерживается большинством коммерческих устройств удалённого доступа

**EAPOL** (EAP over LANs) — протокол определяющий способ инкапсуляции, который позволяет передавать пакеты EAP между supplicant и аутентификатором в локальных проводных сетях.