**12 Лекция. Протоколы AAA**

**Протоколы AAA**

[http://ru.wikipedia.org/wiki/Протокол\_AAA](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_AAA)

**AAA (Authentication, Authorization, Accounting)** — используется для описания процесса предоставления доступа и контроля за ним.

* **Authentication** - аутентификация.
* **Authorization** - авторизация (проверка уровня доступа).
* **Accounting** - учёт, контроль (слежение за потреблением ресурсов пользователем, например, для тарификации (биллинга)).

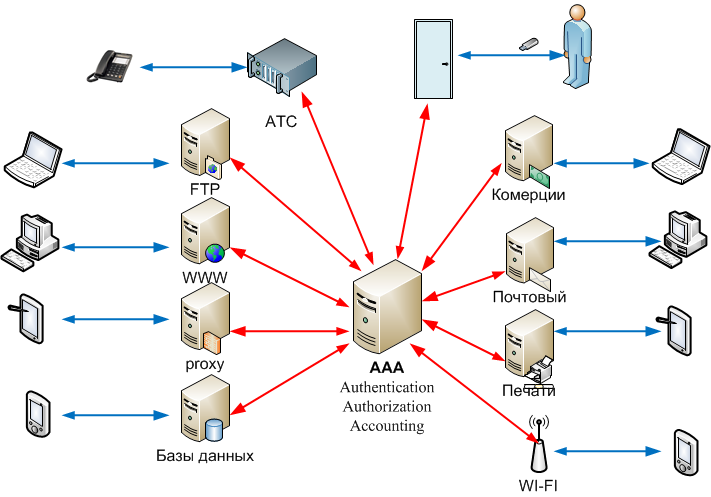


Рис. Для чего нужен протокол AAA

Представьте организацию (например университет) с множеством систем (серверы, АТС, WI-FI, здания, помещения и т.д.). Необходимо регистрировать в каждой системе одного и того-же пользователя. Чтобы этого не делать, ставится сервер AAA и все пользователи регистрируются только в нем. Все системы организации обращаются к серверу AAA.

Алгоритм:

1. пользователь посылает запрос на аутентификацию системе (пароль, ключ и т.д)
2. система пересылает его серверу AAA (т.к. не может провести аутентификацию)
3. сервер AAA посылает ответ системе
4. пользователь получает или не получает доступ

**Основные протоколы AAA:**

* RADIUS, DIAMETER
* TACACS, TACACS+ (компании  Cisco)

Наибольшее распространение получил RADIUS ему на смену создан DIAMETER. Закрытые протоколы не выдерживают конкуренции.

**RADIUS (*Remote Authentication in Dial-In User Service*)**

<http://ru.wikipedia.org/wiki/RADIUS>

<http://xgu.ru/wiki/RADIUS>

<http://www.ibm.com/developerworks/ru/library/au-es-radius1/>

Протокол опубликован в 1997, был опубликован как [RFC 2058](http://tools.ietf.org/html/rfc2058) и [RFC 2059](http://tools.ietf.org/html/rfc2059).

Последние версии (2012) [RFC 2865](http://tools.ietf.org/html/rfc2865) (rus [PDF](https://moodle.kstu.ru/files/RFC/rfc2865.pdf)) и [RFC 2866](http://tools.ietf.org/html/rfc2866) (rus [PDF](https://moodle.kstu.ru/files/RFC/rfc2866.pdf)).

**Основные особенности:**

* используется транспортный  протокол UDP протокол
* поддерживает аутентификацию PAP, CHAP, EAP.
* предоставляет более 50 пар атрибут/значение с возможностью создавать специфичные для производителя пары
* учетные данные могут хранится локально или во внешних источниках (базы SQL, Kerberos, LDAP, Active Directory)

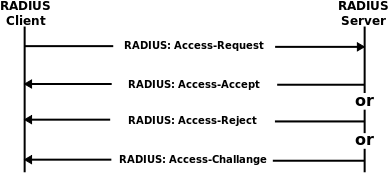


Рис. Запрос клиента и варианты ответа сервера RADIUS

Пользователь посылает свои данные для аутентификации и авторизации серверу (FTP,POP,WWW,PROXY и т.д.), такие серверы называются **Network Access Server (NAS).**

Сервер NAS и сервер RADIUS используют общий секретный ключ (для аутентификации друг друга, и хэширования открытых паролей пользователей).

NAS (клиент) формирует запрос серверу RADIUS **Access Request,** сервер RADIUS может ответить:

* **Ac­cess-Re­ject  -**доступ запрещен.
* **Ac­cess-Chal­lenge -**запрос дополнительной информации от пользователя, например, второй пароль, пин-код, номер карты и т.п.
* **Ac­cess Ac­cept -**доступ разрешен.

**Access Request** - может содержать:

* User-Name
* User-Password
* CHAP-Password

Ответ **Ac­cess-Chal­lenge** может использоваться для посылки случайного числа пользователю, для дальнейшего хеширования его с паролем (см. CHAP).

При выполнении всех условий в отклик **Access-Accept** включается список всех конфигурационных параметров для данного пользователя.

К таким параметрам относятся тип сервиса (например, SLIP, PPP, Login User) и все требуемые для предоставления этого сервиса значения.

Для протоколов SLIP и PPP могут включаться такие параметры, как

* адрес IP
* маска подсети
* MTU
* желательность использования компрессии
* идентификаторы желаемых фильтров

**Взаимодействие с PAP и CHAP**

**PAP**

1. NAS принимает от пользователя PAP ID (login) и пароль
2. NAS PAP ID (login) и пароль в запросе Access-Request как атрибуты User-Name и User- Password
3. сервер RADIUS  сверяет User-Name и User- Password со своими значениями

**CHAP**

1. NAS генерирует случайное число - challenge (предпочтительно 16 октетов) и передает его пользователю
2. пользователь возвращает CHAP-отклик вместе с CHAP ID и CHAP username
3. NAS передает запрос Access-Request серверу RADIUS со значением CHAP username для атрибута User-Name и значениями CHAP ID и CHAP-отклик в качестве CHAP-Password.
4. сервер RADIUS находит пароль для пользователя "User-Name", хэширует (CHAP ID+пароль+CHAP challenge) и сравнивает результат с атрибутом CHAP-Password.

**DIAMETER**

<http://ru.wikipedia.org/wiki/DIAMETER>

<http://www.ibm.com/developerworks/ru/library/wi-diameter/>

Название DIAMETER - игра слов, отражающая превосходство нового протокола над предшественником RADIUS (диаметр - удвоенный радиус).

 Таблица. Сравнение протоколов Diameter и RADIUS

|  |  |  |
| --- | --- | --- |
|  | **Diameter** | **RADIUS** |
| **Транспортный протокол** | **Ориентированные на соединение протоколы (TCP и SCTP)** | **Протокол без установления соединения (UDP)** |
| **Защита** | **Hop-to-Hop, End-to-End** | **Hop-to-Hop** |
| **Поддерживаемые агенты** | **Relay, Proxy, Redirect, Translation** | **Полная поддержка, означающая, что поведение агента может быть реализовано на RADIUS-сервере** |
| **Возможности по согласованию** | **Согласовывает поддерживаемые приложения и уровень безопасности** | **Не поддерживается** |
| **Обнаружение узлов** | **Статическая конфигурация и динамическое обнаружение** | **Статическая конфигурация** |
| **Сообщение инициации сервера** | **Поддерживается. Например, сообщение повторной аутентификации, завершения сессии** | **Не поддерживается** |
| **Максимальный размер данных атрибутов** | **16,777,215 октетов** | **255 октетов** |
| **Поддержка сторонних производителей** | **Поддерживает сторонние атрибуты и сообщения** | **Поддерживает только сторонние атрибуты** |

**LDAP (Lightweight Directory Access Protocol)**

<http://ru.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol>

Облегченный (относительно DAP) протокол для доступа к службе каталогов X.500 (<http://ru.wikipedia.org/wiki/X.500>).

Cлужба каталогов — это репозитарий, в котором хранится информация о людях, компьютерах, сетевых устройствах и приложениях.

Хотя LDAP и не протокол AAA, это больше "Электронный отдел кадров", но т.к. в электронной карточке сотрудника может содержаться, например, пароль, то LDAP тоже можно использовать для централизованного управления доступом.

Его можно использовать, например, для web-сайта, для аутентификации. Кроме этого, web-сайт может получить ФИО, email, телефон и д.р. информацию о пользователе из LDAP, что позволяет исключить подмену информации о себе пользователем или допустить ошибку при вводе информации пользователем, а так же уменьшает количество ручной работы по вводу информации.

Протоколы AAA такой информации не дают, но, например, коммутаторы могут работать только с RADIUS, и не могут работать с LDAP.

**Примеры использования служб каталогов:**

* Идентификация компьютеров
* Аутентификация пользователей
* Группировка пользователей
* Адресные книги
* Представление штатно-кадровой структуры организации
* Учет закрепления имущества организации за сотрудниками
* Телефонные справочники
* Управление пользовательскими ресурсами
* Справочники адресов электронной почты
* Хранение конфигурации приложений
* Хранение конфигурации АТС
* и т.д. ...

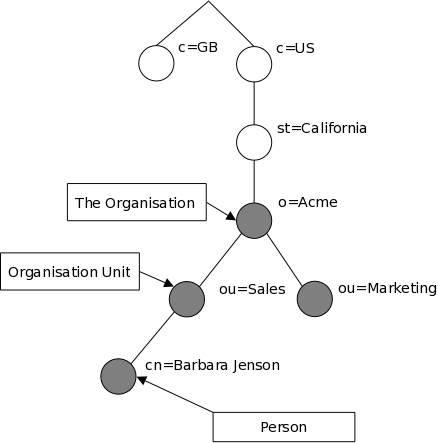


 Рис. Дерево каталога LDAP (традиционное именование записей)

**dc** (domain component) — компонент домена

**ou** (organizational unit) — организационную единицу

**uid** (user id) — идентификатор пользователя

Имя запись пользователя напоминает записи DNS.

Так же как и DNS серверы LDAP:

* могут быть распределенными;
* имеют средства репликации.

Построение дерева может быть также основано на доменных именах Internet. Этот подход к именованию записей становится всё более популярным, поскольку позволяет обращаться к службам каталогов по аналогии с доменами *DNS*.

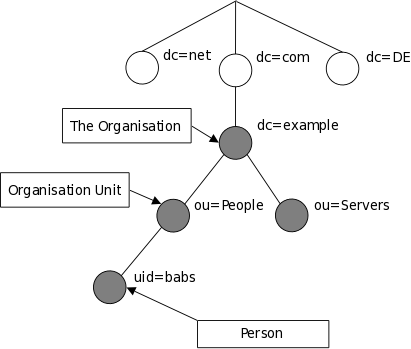


Рис. Дерево каталога LDAP (Internet-именование записей)

**Пример записи LDAP:**

dn: cn=John Doe,dc=example,dc=com

cn: John Doe

givenName: John

sn: Doe

telephoneNumber: +1 888 555 6789

telephoneNumber: +1 888 555 1232

mail: john@example.com

manager: cn=Barbara Doe,dc=example,dc=com

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: person

objectClass: top