## 1.2. Radius-протокол

Протокол Radius (**Remote Authentication Dial In User Service**) – это сетевой протокол, позволяющий осуществлять централизованную аутентификацию, авторизацию и учет пользователей, которые пытаются получить доступ к определенным сетевым службам. Протокол Radius был разработал в 1991 году в Livingston Enterprises Карлом Ригни. В настоящее время Radius описывается в стандартах RFC 2865 и RFC 2866.

Radius является протоколом AAA:

Authentication (Аутентификация) – процесс идентификации проверки пользователя по его индивидуальным данным, обычно по логину и паролю. Аутентификация позволяет подтвердить личность пользователя, но ничего не говорит о его правах.

Authorization (Авторизация) - процесс разрешения или запрета доступа пользователю к определенному сетевому ресурсу.

Accounting (Учет) - процесс, позволяющий отследить активность пользователя, подключенного к определенному сетевому ресурсу. Например, количество времени в сети или объем данных, передаваемый в сессию.

NAS (Network Access Server) – сервер доступа в сеть, NAS является клиентом Radius. В данном случае, NAS – это точка доступа Wi-fi.

Соединение между NAS и Radius осуществляется при помощи протокола UDP. Как правило, Radius рассматривается как сервис без установления соединения. Вопросы, связанные с доступностью сервера, повторной передачей и тайм-аутами обрабатываются Radius-устройствами, а не протоколом передачи данных.

Radius – это клиент-серверный протокол. Radius-клиентом является NAS, а сам Radius сервер – это программа, запущенная на компьютере с операционной системой Windows или Unix. Клиент передает Radius-серверу данные пользователя (абонента), такие как: логин, пароль, объем трафика, время подключения. После чего клиент ждет ответа от Radius о возможности подключения данного пользователя. Также Radius передает информацию и сведения о конфигурации, необходимой клиенту для обслуживания пользователя.

Radius может выступать в качестве Proxy-client, то есть клиента-посредника, для других Radius-серверов или серверов идентификации иного типа.

Аутентификация транзакции между клиентом и Radius осуществляется при помощи общего ключа (shared key). А пользовательские пароли между клиентом и сервером передаются в зашифрованном виде в целях безопасности при их передаче в незащищенных сетях.

**Аутентификация и авторизация.**

Пользователь или компьютер отправляет запрос к серверу удаленного доступа (NAS) для получения доступа к определенному сетевому ресурсу, используя свои учетные данные. Данные пользователя передаются в NAS-устройство при помощи протокола канального уровня, например PPP (Point-to-Point) протокол.

В свою очередь NAS посылает сообщения запроса (Access Request), запрашивая разрешение на предоставление доступа посредствам Radius. Этот запрос включает личные учетные данные пользователя, обычно имя и пароль, или сертификат безопасности, предоставляемый пользователем. Кроме того, запрос может содержать и иные сведения, которые NAS знает о пользователе, например, его сетевой адрес, номер телефона, идентификатор клиента или идентификатор порта.

Radius-сервер проверяет достоверность этой информации, используя такие схемы аутентификации, как PAP, CHAP или EAP.

При необходимости проверяются такие данные о пользователе как сетевой адрес и номер телефона пользователя. Ранние версии Radius-серверов проверяли информацию о пользователе прежде чем поместить их в базу данных.

Современные Radius-серверы могут делать это, или могут ссылаться на внешние источники – обычно в SQL, протокол Kerberos, LDAP или Active Directory – для проверки учетных данных пользователя.

Затем Radius-сервер возвращает NAS один из трех ответов:

1)Access Reject – пользователю запрещен доступ ко всем запрашиваемым сетевым ресурсам. Причиной может быть – неспособность предъявить «удостоверение личности», либо неизвестность или неактивность учетной записи пользователя;

2)Access Challenge – запрашивается дополнительная информация от пользователя, например, вторичный пароль или PIN-код. Access Challenge также используется в более сложных диалогах аутентификации, где безопасное соединение устанавливается между пользователем и Radius-сервером таким образом, что учетные данные скрыты от NAS.

3)Access Accept.- пользователю разрешается доступ. После того, как пользователь будет аутентифицирован, Radius-сервер будет постоянно проверять, что пользователь может использовать сетевой ресурс.

Каждое из этих трех сообщений Radius-сервера может включать в себя Reply-message атрибуты, в которых может быть сказано о поводе для отказа, приглашение или приветственное сообщение.

Атрибуты авторизации передаются в NAS, оговаривая условия получения доступа. Например, следующие атрибуты авторизации могут быть включены в сообщение Access-Accept:

* Конкретный IP-адрес, назначенный пользователю;
* Пул адресов, из которых пользователю должен быть выбран IP-адрес;
* Максимальная продолжительность времени, в течение которого пользователь может оставаться подключенным;
* Список доступа, приоритетные очереди или другие ограничения, связанные с ограничением доступа пользователей;
* L2TP параметры;
* VLAN параметры;
* QOS параметры;

Принцип работы аутентификации и авторизации протокола Radius представлен на рисунке 1.

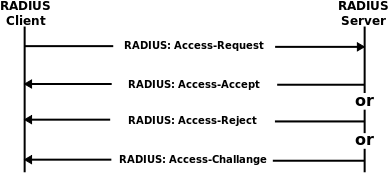


Рис.1. Аутентификация и Авторизация

**Учет(Accounting)**

Учет описывается в стандарте RFC 2866.

Когда пользователь получает доступ к сети посредством NAS, запускается учет (от Radius приходит Request пакет, содержащий Acct-Status-Type атрибут с сообщением «Start»). В свою очередь, NAS посылает Radius-серверу сигнал о том, что пользователь получил доступ к сети. «Start» сообщения обычно содержат данные об идентификации пользователей, сетевой адрес и уникальный идентификатор сессии.

Периодически, NAS посылает Interim Update сообщения Radius-серверу, чтобы обновлять статус активного сеанса. «Interim» сообщения обычно содержат текущую продолжительность сеанса и информацию о текущих данных об использовании сетевых ресурсов.

Наконец, когда пользователь отключается от сети, NAS посылает Radius серверу последнее Accounting Stop сообщение, содержащее информацию о времени использования пользователем сети, причину отключения и другую информацию, касающейся пользователя и его доступа к сети.

Как правило, клиент посылает Accounting-Request пакеты до тех пор, пока не получит ответ от Radius-сервера.

Основной целью учета Radius является то, чтобы пользователю мог быть выставлен счет за использование сетевого ресурса. Соответственно, такие данные широко используются для статистических целей и для общего мониторинга сети.

Принцип работы учета протокола Radius представлен на рисунке 2.

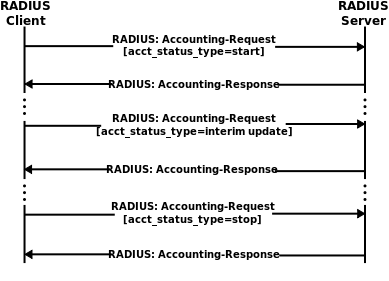


Рис.2. Принцип работы учета в протоколе Radius

**Роуминг**

Radius также может быть использован для облегчения роуминга между провайдерами, например:

* Компаниями, которые предоставляют единый глобальный набор учетных данных, которые могут использоваться во многих публичных сетях.
* Независимыми, но сотрудничающими между собой организациями, которые выдают свои собственные учетные данные для своих пользователей.

**Структура пакетов протокола Radius.**

Формат типового пакета протокола Radius представлен на рисунке 3. Поля передаются слева направо, начиная с поля Code и заканчивая поля с атрибутами.

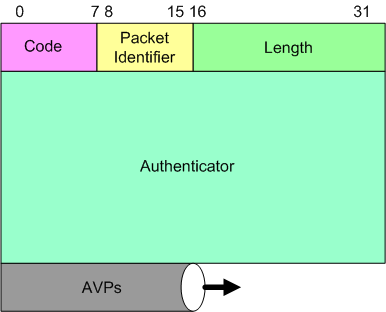


Рис.3. Формат типового пакета Radius.

Поле Code содержит идентификатор типа пакета Radius. Если значение поля Code имеет некорректное значение, то такой пакет отбрасывается без уведомления. Значения поля Code представлены в таблице 1.

ТАБЛИЦА 1. Значения поля Code

|  |  |
| --- | --- |
| Код | Тип пакета |
| 1 | Access-Request |
| 2 | Access-Accept |
| 3 | Access-Reject |
| 4 | Accounting-Request |
| 5 | Accounting-Response |
| 11 | Access-Challenge |
| 12 | Status-Server |
| 13 | Status-Client |
| 255 | Зарезирвирован |

Поле Packet Identifier предназначено для сопоставления запросов и ответов. Radius-сервер может распознать дубликаты запросов по значению данного поля, если эти пакеты были получены в течение короткого промежутка времени.

Значение поля Length определяет длину всего Radius-пакета, включая поля Code, Identifier, Length, Authenticator и Attribute.

Поле Authenticator предназначено для проверки подлинности ответа от Radius-сервера и используется в шифровании паролей.

Атрибуты Radius

Radius атрибуты предназначены для того, чтобы передавать сведения, используемы для идентификации, проверки прав, конфигурации и для передачи пользователю различной информации.

Формат поля Attribute представлен на рисунке 4. Поля атрибута передаются слева направо.

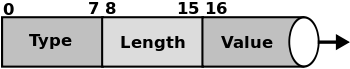


Рис.4. Формат поля Attribute

Поле Type определяет тип атрибута. Значения поля Type, определенные в стандарте RFC 2865, представлены в таблице 2. Radius-сервер имеет право игнорировать атрибуты неизвестного типа. Клиент Radius также может игнорировать атрибуты неизвестного типа.

Поле Length определяет размер атрибута с учетом всех полей. При получении Access-Request атрибута с неправильно указанным размером передается отклик Access-Reject.

Поле Value является необязательным и содержит значение атрибута.

ТАБЛИЦА 3. Значения поля Type

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Тип | Атрибут | Тип | Атрибут | Тип | Атрибут |
| 1 | User-name | 16 | Login-TCP-Port | 31 | Calling-Station-Id |
| 2 | User-Password | 17 | (не используется) | 32 | NAS-Identifier |
| 3 | CHAP-Password | 18 | Reply-Message | 33 | Proxy-State |
| 4 | NAS-IP-Address | 19 | Callback-Number | 34 | Login-Lat-Service |
| 5 | NAS-Port | 20 | Callback-Id | 35 | Login-Lat-Node |
| 6 | Service-Type | 21 | (не используется) | 36 | Login-LAT-Group |
| 7 | Framed-Protocol | 22 | Framed-Route | 37 | Framed-AppleTalk-Link |
| 8 | Framed-IP-address | 23 | Framed-IPX-Network | 38 | Framed-AppleTalk-Network |
| 9 | Framed-IP-Netmask | 24 | State | 39 | Framed-AppleTalk-Zone |
| 10 | Framed-Routing | 25 | Class | 40-59 | (зарезирвированы для учета) |
| 11 | Filter-Id | 26 | Vendor-Specific | 60 | CHAP-Challenge |
| 12 | Framed-MTU | 27 | Session-Timeout | 61 | NAS-Port-Type |
| 13 | Framed-Compression | 28 | Idle-Timeout | 62 | Port-Limit |
| 14 | Login-Ip-Host | 29 | Termonation-Action | 63 | Login-Lat-Port |
| 15 | Login-Service | 30 | Called-Staion-Id |  |  |