Каков принцип работы RADIUS?

Содержание

Введение

Протокол службы дистанционной аутентификации пользователей по коммутируемым линиям (RADIUS) был разработан корпорацией Livingston Enterprises в качестве протокола аутентификации и учета для сервера доступа. Спецификация RADIUS (RFC 2865) заменяет собой RFC 2138. Стандарт учета RADIUS (RFC 2866) заменяет собой RFC 2139.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

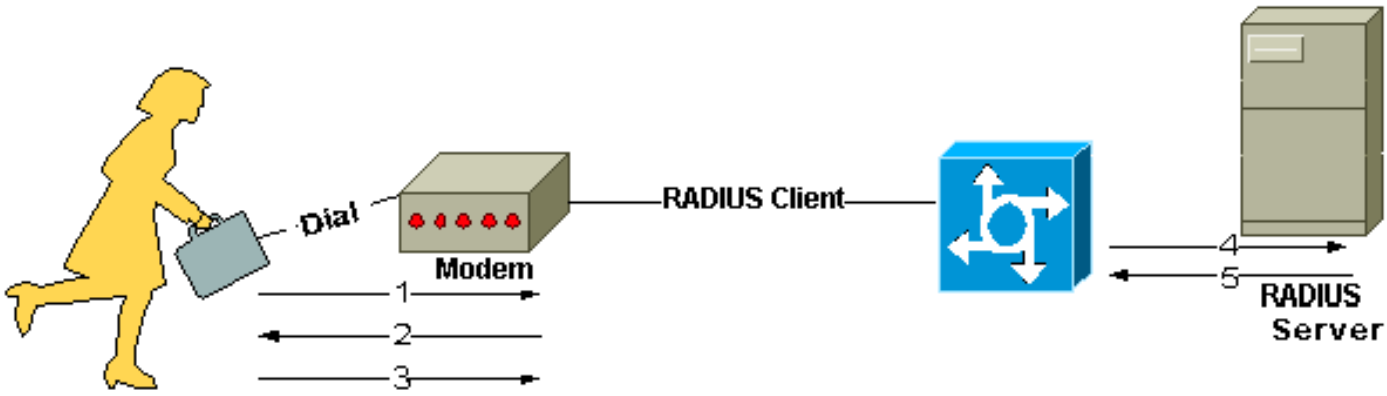
Общие сведения

Соединение между сервером доступа к сети (NAS) и сервером RADIUS основано на протоколе UDP (User Datagram Protocol). В общем виде протокол RADIUS представляет собой службу без установления соединения. Вопросы, связанные с доступностью сервера,

повторной передачей и временем ожидания, решаются устройствами с поддержкой RADIUS лучше, чем протоколом передачи.

RADIUS – протокол типа «клиент-сервер». Клиент RADIUS обычно представляет собой сервер NAS, а сервер RADIUS – процесс-демон на компьютере с ОС Windows NT или UNIX. Клиент передает сведения о пользователе указанным серверам RADIUS и выполняет различные действия в зависимости от возвращенного ответа. Серверы RADIUS принимают запросы подключения пользователей, выполняют аутентификацию пользователей и возвращают данные о конфигурации, необходимые для обслуживания пользователя клиентом. Сервер RADIUS может действовать как промежуточный для других серверов RADIUS или серверов аутентификации другого типа.

На этом рисунке показано взаимодействие удаленного пользователя с клиентом или сервером RADIUS.



1. Пользователь инициализирует аутентификацию PPP с сервером NAS.
2. NAS запрашивает имя пользователя и пароль (для протокола аутентификации пароля [PAP]) или хэш-строку (для протокола аутентификации с косвенным согласованием [CHAP]).
3. Пользователь отправляет ответ.
4. Клиент RADIUS посылает серверу RADIUS имя пользователя и зашифрованный пароль.
5. Сервер RADIUS выдает один из ответов: Accept (принято), Reject (отклонено) или Challenge (требуется вторичная аутентификация).
6. Клиент RADIUS выбирает действие в зависимости от служб и их параметров, объединенных с сообщениями Accept или Reject.

Аутентификация и авторизация

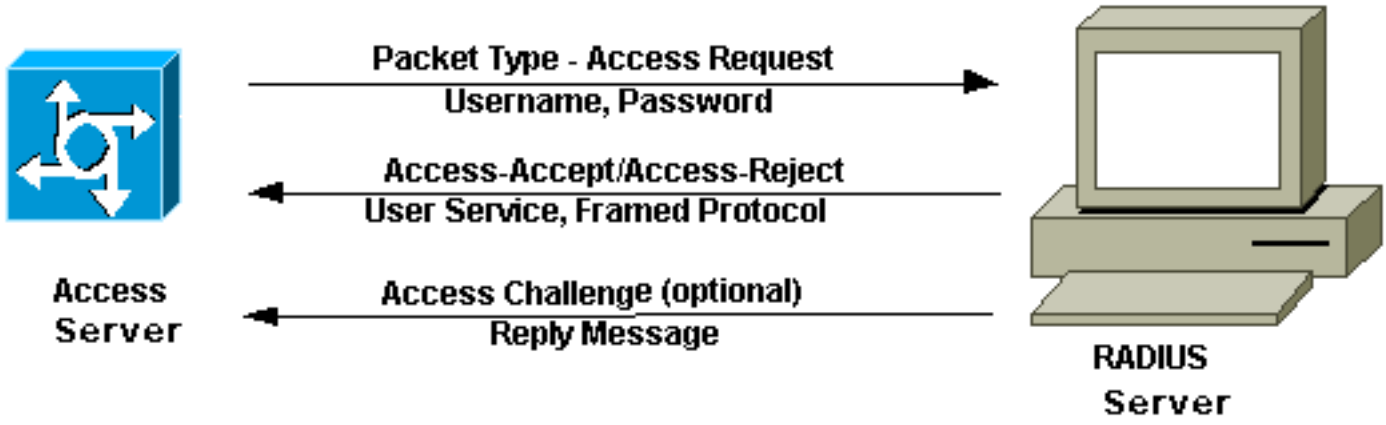
Сервер RADIUS может поддерживать множество методов аутентификации пользователя. Для проверки подлинности имени пользователя и пароля, предоставляемых серверу, могут использоваться протоколы PPP, PAP, CHAP, вход UNIX и другие механизмы аутентификации.

Обычно процесс входа пользователя состоит из передачи запроса (Access-Request) с сервера NAS на сервер RADIUS и получения соответствующего ответа с сервера (Access-Accept или Access-Reject). Пакет Access-Request содержит имя пользователя, зашифрованный пароль, IP-адрес сервера NAS и порт. Первоначально серверы RADIUS размещались на UDP-порту 1645, что создавало конфликт со службой datametrics. По причине этого конфликта документ RFC 2865 официально закрепил за протоколом RADIUS

порт 1812. Большинство устройств и приложений Cisco поддерживают оба набора номеров портов. Формат запроса также содержит информацию о типе сеанса, который собирается инициировать пользователь. Например, если запрос представлен в символьном режиме, то вывод должен выглядеть как Service-Type = Exec-User, но если запрос представлен в пакетном режиме PPP, то вывод выглядит как Service Type = Framed User и Framed Type = PPP."

По получении от NAS запроса Acceess-Request сервер RADIUS производит поиск указанного имени пользователя в базе данных. Если имя пользователя не найдено в базе данных, это значит, что загружен профиль по умолчанию, или сервер RADIUS немедленно отправляет сообщение Access-Reject. Данное сообщение Access-Reject может сопровождаться текстовым сообщением, в котором указывается причина отказа в доступе.

В RADIUS аутентификация и авторизация объединены. Если имя пользователя найдено и пароль правильный, то сервер RADIUS возвращает подтверждение доступа, включая список пар «атрибут-значение», которые описывают параметры, необходимые для данного сеанса. В числе типичных параметров: тип службы (сеанс интерпретатора или кадрирование), тип протокола, назначенный пользователю IP-адрес (статический или динамический), применяемый список доступа или статический маршрут для установки в таблицу маршрутизации NAS. Данные конфигурации на сервере RADIUS определяют компоненты, которые будут установлены на сервер NAS. Рисунок ниже показывает аутентификацию RADIUS и последовательность авторизации.



Учет

Функции учета протокола RADIUS могут использоваться независимо от функций аутентификации или авторизации RADIUS. Учетная функция RADIUS позволяет посылать данные в начале и в конце сеансов, отображая ресурсы (такие как время, пакеты, байты и т. п.), использованные во время сеанса. Для удовлетворения потребностей безопасности и биллинга поставщик услуг Интернета (ISP) может использовать программное обеспечение RADIUS по управлению доступом и учету. Порт учета для RADIUS для большинства устройств Cisco является 1646, но это может также быть 1813 (из-за изменения в портах, как задано в RFC 2139).

Подлинность транзакций между клиентом и сервером RADIUS подтверждается с помощью общего секрета, никогда не пересылаемого по сети. Кроме того, обмен паролями пользователей между клиентом и сервером RADIUS выполняется в зашифрованном виде для исключения вероятности перехвата пароля пользователя злоумышленниками через прослушивание незащищенной сети.

Дополнительные сведения

- Страница поддержки технологии RADIUS
- Запросы комментариев (RFC)
- Техническая поддержка - Cisco Systems