Упрощаем переезд с PPP на IPoE: Автоматизация учета адресов и привязок абонентов



В Ethernet-сетях для абонентов технология IPoE является более удобной, чем привычный PPP. При ее использовании упрощается подключение новых абонентов, пользователям не нужно запоминать пароли, при нарушении связи соединение не разрывается и т.д. Казалось бы, сплошные плюсы, и все же переезд на новую технологию дается операторам связи с большими трудностями — к примеру, среди наших клиентов не более половины перевели на нее свою инфраструктуру.

Сегодня мы поговорим о том, почему так происходит, а также расскажем, как использование биллинга "Гидра" помогает упростить этот процесс.

В чем проблема

Для операторов переход на технологию IPoE сопряжен с серьезными затратами:

- **на оборудование** — всю сеть придется перевести на управляемые коммутаторы с поддержкой DHCP Option 82;
- **на приведение в порядок кабельной инфраструктуры** — у оператора должно быть четкое понимание, к какому порту какого коммутатора привязан каждый абонент, то есть каждый кабель должен быть учтен и промаркирован;
- **на софт** — информацию о MAC-адресах (их учитывать не обязательно, но это повышает безопасность и позволяет более точно отслеживать движение абонентского оборудования по сети) и привязках абонентов к портам оборудования нужно где-то хранить и обрабатывать при попытках аутентификации абонента.

Но и после внедрения IPoE затраты не прекращаются — необходимо организовать поддержку абонентских привязок и MAC-адресов в актуальном состоянии. В такой ситуации операция по замене сгоревшего коммутатора, казавшаяся ранее рутинной, превращается в увлекательный процесс, сравнимый с движением по минному полю: любой перепутанный монтажником порт приводит к перерыву связи у абонента.

Возникают свои сложности и у абонентов — как минимум, теперь им при смене MAC-адреса или переезде нужно всегда обращаться в службу поддержки провайдера для внесения новых настроек. Иначе связь работать не будет.

Как исправить ситуацию: портал аутентификации

В свете описанных выше проблем становится понятно, почему многие провайдеры не спешат переезжать на новую технологию. Тем не менее, есть способы упростить миграцию на IPoE.

Один из них заключается в том, чтобы устанавливать соответствие между абонентом и его сетевыми реквизитами — MAC-адресом, адресом коммутатора доступа и номером порта на коммутаторе — путем перенаправления "неизвестного" абонента на портал аутентификации.

Портал аутентификации представляет собой веб-форму, в которую абонент должен ввести логин и пароль от личного кабинета. Если учетные данные верны, то новые реквизиты записываются в базу данных для идентифицированного абонента.

Когда мы начали работу над решением для автоматизации IPoE-сетей в "Гидре", то быстро поняли, что простая идея выливается в совсем непростое решение.

Во-первых, требуется аутентификационная БД, в которой хранится актуальная информация:

- Об операторских коммутаторах уровня доступа и их портах.
- Об абонентском оборудовании, его владельцах, MAC-адресах и привязках к портам коммутаторов.

Во-вторых, понадобится отдельная база данных для хранения сетевых реквизитов абонента, которые передает коммутатор в DHCP Option 82.

В-третьих, необходимо наладить сбор сетевых реквизитов. Они поступают с коммутатора на DHCP-сервер, который должен сохранять их в базе сетевых реквизитов вместе с выданным абоненту IP-адресом.

В-четвёртых, необходим BRAS с настроенными сервисами. Один из сервисов — для неидентифицированных абонентов — должен выдаваться всем, кто:

- выходит со своим MAC-адресом с "неправильного" порта (ситуация "замена коммутатора");
- выходит с "неправильным" MAC-адресом со своего порта (ситуация "замена абонентского оборудования");
- выходит с "неправильным" MAC-адресом с не занятого порта (ситуация "подключение нового абонента").

Когда этот сервис подключен, все HTTP-запросы абонента перенаправляются на портал аутентификации. Когда пользователь вводит на нем логин и пароль, из базы сетевых реквизитов по IP-адресу абонента извлекается последний набор реквизитов. Он записывается в аутентификационную БД как актуальный.

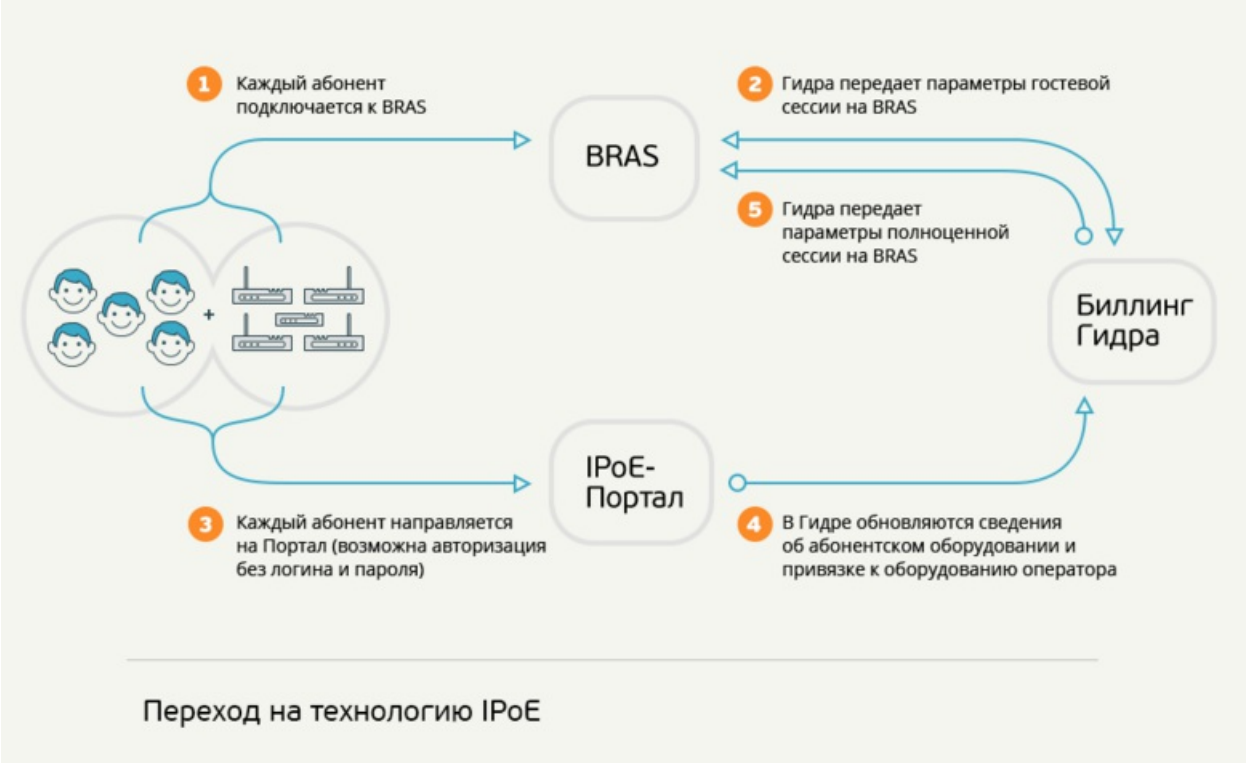
Возникает вопрос о необходимости учета MAC-адресов. Многие провайдеры считают достаточным работать только с привязками к портам. С одной стороны, это упрощает жизнь абоненту — он может подключать к сети любое устройство без дополнительных запросов пароля. В то же время замена коммутатора и переезд (мы рассмотрим эти ситуации ниже) серьезно усложняются, так как привязка становится единственным идентификатором абонента и при ее изменении невозможно отследить, что с ним произошло. Кроме того, в некоторых конфигурациях сети без ограничений доступа по MAC-адресу возможны злоупотребления со стороны абонентов.

Проблемы и решения: реальные ситуации

Рассмотрим несколько типовых сценариев использования IPoE, в ходе которых могут возникать сложности, и то, как с ними бороться.

Миграция с PPP на IPoE

На первый взгляд все очень сложно: нужно узнать, к какому порту какого коммутатора подключен каждый абонент, и сохранить эту привязку в базе данных. Хорошая новость заключается в том, что для этого вовсе не обязательно обходить все чердаки с установленным оборудованием. Переезд можно организовать и постепенно — с помощью портала и его небольшой программной доработки. В аутентификационной БД коммутатору достаточно добавить признак перевода. Все абоненты, у которых ещё нет актуальной привязки и MAC-адреса, вышедшие в сеть с коммутатора с включённым признаком перевода, будут перенаправлены на портал.

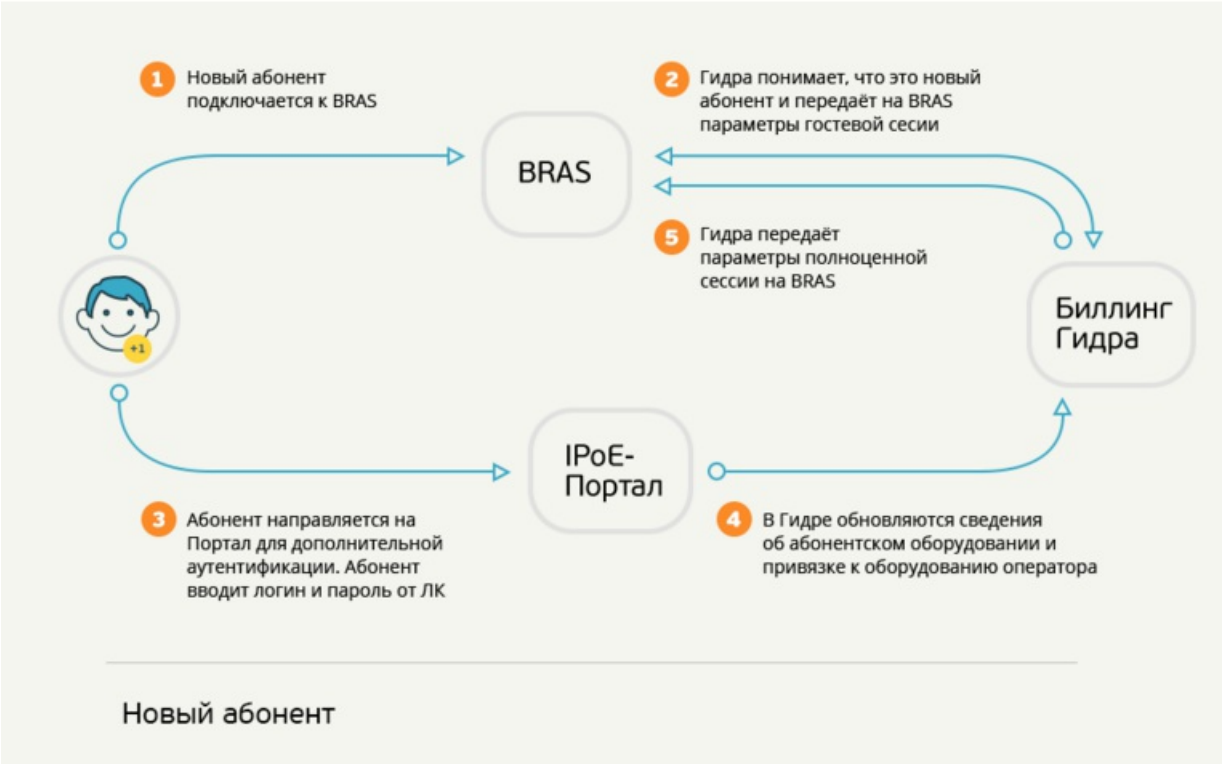


В итоге перевод — разовая операция, которая создаст абоненту минимум неудобств и в то же время актуализирует карту сети. Ее можно и нужно проводить постепенно, чтобы "размазать" нагрузку на службу техподдержки и отработать процесс перехода.

Подключение нового абонента

Первое знакомство нового абонента с оператором в IPoE-сети также не всегда происходит гладко. Заранее выяснить MAC-адрес затруднительно, а найти и "забронировать" свободный порт на коммутаторе вручную крайне непросто. (Предваряя возможные вопросы, действительно, нам встречались операторы, у которых есть специальные сотрудники для поиска свободных портов. Выяснить как называется эта должность в штатном расписании, нам не удалось).

При таком планировании бизнес-процесс подключения становится более сложным и замедляется. Это приводит к лишним затратам, а самое главное — в этом нет никакого смысла, поскольку можно все это полностью автоматизировать. При хорошо отлаженных бизнес-процессах новые абоненты подключаются быстро — на следующий день или даже в день поступления заявки. Для этого монтажники всегда должны иметь при себе запас оборудования и расходников, заявки могут поступать к ним по телефону или через мобильное приложение, а первичная привязка к коммутатору и сохранение MAC-адреса автоматизируется с помощью портала аутентификации.



Замена абонентского оборудования

Даже во многих крупных сетях, которые уже используют IPoE, часто возникает проблема безболезненной замены абонентских устройств. К примеру, если клиент купит новый WiFi-маршрутизатор, то он может столкнуться с отсутствием доступа в сеть — всему виной смена MAC-адреса. В итоге это приводит к негативу и в лучшем случае звонкам в техподдержку своего провайдера, а в худшем — конкурентам.

Эту проблему можно решить, если при замене оборудования абонента будут направлять на портал аутентификации, где он сможет подтвердить свои данные — после этого MAC-адрес нового оборудования просто обновится в аутентификационной БД.



В таком случае у пользователя не возникает никаких неудобств, при этом уровень безопасности не снижается. При этом сокращается число обращений в службу поддержки. По нашим оценкам, на сети из 100 тысяч абонентов экономия может составлять до 1,5 тысяч обращений в месяц.

Замена коммутатора доступа

В классической IPoE-сети при замене коммутатора, к которому подключены абоненты, очень важно без изменений сохранить их привязки к портам, в противном случае пользователи потеряют доступ в сеть.

И в этой ситуации на помощь снова приходит портал. В аутентификационной БД для коммутатора хранится признак замены — он выставляется технической службой оператора вручную перед выездом монтажника. Все абоненты, которые выходят в сеть с такого коммутатора через "чужой" порт, должны подтвердить свои данные на портале. После этого их привязка к порту обновляется.



В такой конфигурации при замене коммутатора монтажник может подключать абонентов в любой порт, что упрощает процесс. В прошлое уходит процедура печати карт привязки абонентов к портам. На больших сетях, имеющих десятки тысяч коммутаторов, каждый год заменяют тысячи устройств — автоматизация этого процесса дает ощутимый экономический эффект.

Переезд абонента

Ситуация, при которой операторы разрешают абонентам "мигрировать" по сети, подключаясь из одной точки в другую, встречается реже предыдущих. Но, тем не менее, она может возникать, и с помощью портала разрешить ее можно, фактически, бесплатно. Алгоритм здесь аналогичен схеме с заменой коммутатора, но в отличие от нее, перепривязка абонентов через портал разрешается не обязательно в пределах одного коммутатора.

Заключение

Внедрение технологии IPoE — большие трудозатраты, а ее эксплуатация — постоянная головная боль. Мы предполагаем, что это важная причина, по которой до сих пор большинство операторов используют PPP, а их клиенты терпят связанные с этим неудобства.

Однако решить эти проблемы без особых сложностей можно с помощью автоматизации. В нашем решении в качестве БД аутентификации используется сам биллинг "Гидра": система умеет хранить всю необходимую информацию о коммутаторах и их портах, абонентском оборудовании и его сетевых адресах.

Сам IPoE-портал состоит из нескольких HTML-страничек со встроенными формами, которые отправляют POST-запросы на сервер.

В качестве сервера используется разработанное нами ESB-приложение. Сервер интегрирован с БД сетевых реквизитов, с аутентификационной БД и с RADIUS-агентом hard. Его бизнес-логика обрабатывает все описанные выше ситуации. Для каждой из них в конфигурационном файле сервера настраивается его поведение. Некоторые из ситуаций (например, замену коммутатора) можно отрабатывать в "прозрачном" режиме, не требуя дополнительной аутентификации от абонента.