УДК 004.057.4, 004.733

КЛИЕНТ-СЕРВЕРНОЕ ВЗАИМОДЕЙСТВИЕ И ВОЗМОЖНОСТЬ ПРОВЕДЕНИЯ АВТОРИЗАЦИИ НА БАЗЕ ПРОТОКОЛА DHCP С ИСПОЛЬЗОВАНИЕМ OPTION 82.

Дубяга В.В., Приходько Т.А.
Донецкий национальный технический университет
Кафедра компьютерная инженерия
E-mail: dvv090480@yandex.ru

Аннотация

Дубяга В.В., Приходько Т.А. Клиент-серверное взаимодействие и возможность проведения авторизации на базе протокола DHCP с использованием OPTION 82. *Рассмотрены методы клиент-серверного взаимодействия. Предложен вариант проведения авторизации с использованием управляемых коммутаторов, поддерживающих функцию DHCP Relay option 82, которая предоставляет удобные средства взаимодействия с системой учета клиентов и сетевого трафика.*

Актуальность

Интернет на сегодняшний день стал одним из повседневных средств коммуникации. Также в последние годы появилось множество компаний предоставляющих широкополосный доступ к сети Интернет. Широкополосный или высокоскоростной доступ в Интернет означает доступ в Интернет с большой скоростью, в противоположность коммутируемому доступу с использованием модема и телефонной сети общего пользования. Основой получения услуги есть авторизация. Результаты авторизации регистрируются в системе учета клиентов.

Существующие системы учета (иначе биллинговые системы) являются либо очень дорогими, либо очень простыми, не использующими современных технологий. Создание простой и доступной биллинговой системы, таким образом, является актуальной задачей.

Постановка задачи

Основой биллинговой системы является система авторизации. Существует несколько видов авторизаций клиента.

1. Туннельный – pptp, pppoe. В обоих случаях создается подключение с необходимыми параметрами на клиентском оборудовании с именем пользователя и паролем. ***Достоинства:*** достаточно высокая безопасность и защищенность подключения при использовании шифрования. ***Недостатки:*** необходимость ручной настройки клиентского оборудования, что неподготовленного пользователя может быть непосильной задачей; как pptp так и pppoe северы авторизации весьма ресурсоемки, что вынуждает операторов связи тратиться на дополнительное дорогостоящее высокопроизводительное оборудование.
2. Использование самостоятельно написанных программ клиент-авторизаторов. ***Достоинства:*** простота использования для клиента, которая сводится к вводу имени пользователя и пароля; при правильном составлении алгоритма и написании клиентской и серверной части – невысокая ресурсоемкость для серверного оборудования. ***Недостатки:*** необходимость написания клиент-авторизаторов под все существующие платформы операционных систем, установленные на клиентском оборудовании среди которых могут быть: персональный компьютер или ноутбук (ОС Windows, OS Linux,

MAC OS), роутеры известных фирм, для которых часто не представляется возможным написать клиент-авторизатор; также перед началом использования клиент-авторизатора зачастую необходимо выполнить настройку параметров сетевого интерфейса.

3. Идентификация пользователя по связке IP адрес + MAC адрес.
   Достоинства: нет необходимости выполнять настройки на клиентском оборудовании при использовании DHCP сервера, так как MAC адрес известен, и не составляет труда составить конфигурационный файл DHCP сервера с привязкой к IP. ***Недостатки:*** при использовании неуправляемых коммутаторов возможность подстановки чужого IP адреса + MAC адреса на свое оборудование; невозможность, без использования роутера, пользоваться попеременно разными типами оборудования (ПК или ноутбук); при смене MAC адреса необходимо уведомлять администрацию провайдера о смене оборудования, вызывать специалиста для перенастройки, или по телефону диктовать MAC адрес нового оборудования.
4. Взаимодействие управляемых коммутаторов 2-го уровня с функциями DHCP Relay Option 82 (стандарт RFC 3046) с DHCP сервером и системой учета трафика. ***Достоинства:*** для пользователя полностью автоматическая настройка любого сетевого оборудования с поддержкой протокола DHCP; возможность попеременно пользоваться на одном подключении разными типами сетевого оборудования без использования маршрутизатора; клиент может без уведомления администрации провайдера самостоятельно менять оборудование (ПК, ноутбук, маршрутизатор) подключаемое к сети Интернет без дополнительных технических навыков и помощи технической поддержки провайдера. ***Недостатки:*** для провайдера обязательное использование управляемых коммутаторов с поддержкой DHCP Relay Option 82. ***Нивелируются значительным снижением трудозатрат.***

Обзор зарубежных аналогов

У каждой из компаний, в серверной инфраструктуре есть своя система учета клиентов, сетевого трафика. Примеры таких систем:

1. BGBilling - авторизация по DHCP option 82 на момент написания статьи находится на этапе разработки. [1].
2. LANBilling в версии 1.9 начиная со сборки 2, включена поддержка выдачи IP адреса по DHCP с использованием управляемого коммутатор и option 82. При авторизации используется RADIUS сервер. [2].
3. NoDeny Построение сети с использованием технологий DHCP option 82 и DHCP Snooping [3].

Из общих преимуществ вышеперечисленных систем можно отметить: использование свободно распространяемых операционных систем в качестве серверных Linux, FreeBSD; маштабируемость; взаимодействие с управляемыми коммутаторами с использованием технологии DHCP option 82; сбор статистики с NetFlow совместимых устройств; централизованное WEB управление.

Клиент-серверное взаимодействие на базе DHCP Relay и DHCP option 82

Согласно стандарту RFC-2131 протокол динамической настройки сетевых устройств (компьютеров) (Dynamic Host Configuration Protocol — DHCPv4-протокол) размещает IPv4-адреса в динамически настраиваемых сетевых устройствах и обеспечивает установку и корректировку параметров сетевых устройств в Internet-сети.

Option 82 используется для передачи дополнительной информации в DHCP-запросе. Эту информацию добавляет сам коммутатор. И она может быть использована для применения политик для увеличения уровня безопасности и эффективности.

Использование Option 82 минимизирует количество DHCP-серверов в сети, поскольку уже не нужно использовать несколько DHCP-серверов, по одному в каждой подсети. Коммутатор просто перенаправляет DHCP-запрос от клиента в локальной подсети на удалённый DHCP-сервер, как это показано на рис.1.

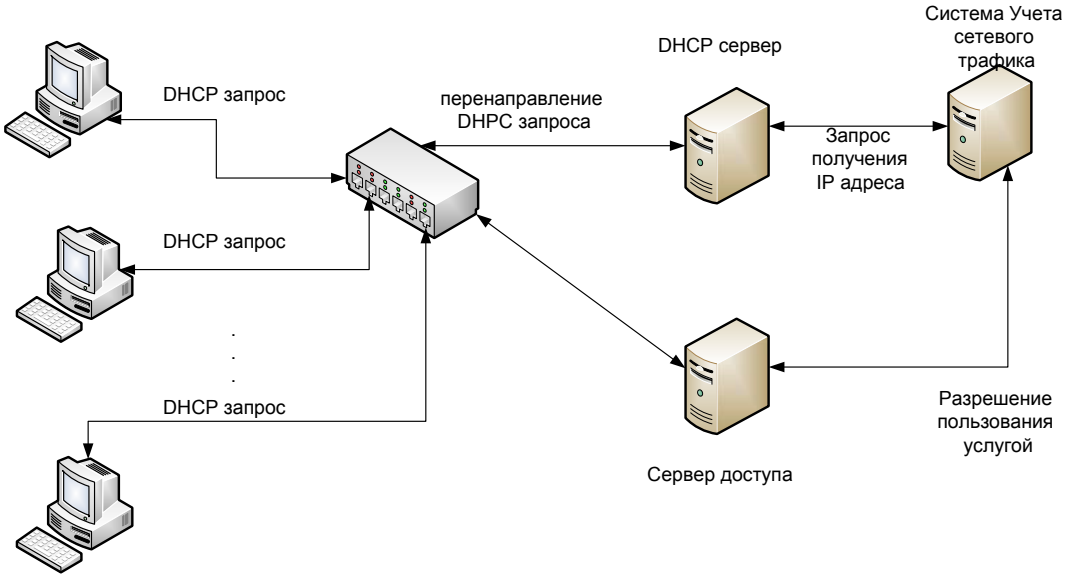

Рисунок 1 - Клиент-серверное взаимодействие на базе DHCP Relay и DHCP option 82 и системы учета

Сначала клиент, который подключен к порту управляемого коммутатора, посылает DHCP запрос на получение IP адреса. Коммутатор переадресовывает DHCP запрос согласно опции DHCP Relay на DHCP сервер. Кроме того, в пакете запроса IP адреса есть параметры option 82, которые отмечают идентификатор коммутатора и идентификатор порта или VLAN, из которого поступает запрос (рис.2). На основе этих данных DHCP сервер должен проверить наличие записи в конфигурационном файле, и выдать IP адрес, маску сети, адрес DNS сервера и шлюз по умолчанию клиентскому оборудованию.

Эту функцию можно использовать не только для выдачи IP адреса клиенту, но и проводить авторизацию в системе учета, а также дальнейшее предоставление разрешения или запрет пользования услугами Интернет или другими телекоммуникационными услугами как показано на рис 1.

Таким образом:

1. Создается база данных клиентов. Каждой клиентской записи, кроме полей персональных данных, присваивается IP адрес, а также имя и порт коммутатора, к которому он подключен.
2. Когда на DHCP сервер приходит запрос на получение IP адреса система учета проверяет можно ли клиенту получить разрешение на подключение услуги. Если разрешение есть, то DHCP сервер выдает IP адрес клиенту и сразу после этого система учета генерирует и отправляет серверу команду для активизации правил разрешения пользования услугой.

Рассмотрим принцип передачи DHCP запроса на получение IP адреса от клиента активного управляемого оборудования к серверу. Формат пакета дополнительной option 82 приведен на рис 2.

Код	Длина	Поля информации от агента					
82	N	i1	i2	i3	i4	.....	iN

Рисунок 2 – Формат дополнительной опции 82 в пакете DHCP запроса [5]

Код – номер опции DHCP протокола – 82.

Длина N - общее число полей исходящих от управляемого коммутатора (агента).

Поля информации агента – поля, количество которых зависит от конкретной модели управляемого коммутатора и фирмы производителя, передают параметры, среди которых 2 основные субопции: Agent Circuit ID Sub-option рис.3, Agent Remote ID Sub-option рис. 4.

Субопция	Длина	Значение субопции					
1	N	s1	s2	s3	s4	.....	sN

Рисунок 3 - Agent Circuit ID Sub-option [5]

Субопция	Длина	Значение субопции					
2	N	i1	i2	i3	i4	.....	iN

Рисунок 4 - Agent Remote ID Sub-option [5]

Формат субопций зависит от модели и фирмы производителя коммутатора. Субопция 1 с помощью полей значений передает информацию о номере VLAN и/или номере порта коммутатора. Субопция 2 передает параметр Agent ID, который в большинстве коммутаторов по умолчанию равен MAK-адресу коммутатора, но может быть изменен.

Разработка алгоритмов

В проекте будем использовать ISC DHCP сервер. В первую очередь нужно автоматизировать формирование конфигурационного файла dhcp.conf, алгоритм формирования которого представлен на рис. 5. В первую очередь проверяем положительный ли баланс (Balance) у пользователя. Для этого сравниваем его с ценой текущего тарифа (tariff.price). Далее проверяем, включен ли у пользователя доступ (status). Если оба вышеперечисленных условия соблюдаются, формируем dhcpd.conf в который заносим из базы ID коммутатора (switch_opt82), порт коммутатора (port_opt82), к которому подключен пользователь и IP адрес (IP), который будет назначаться пользователю сервером DHCP.

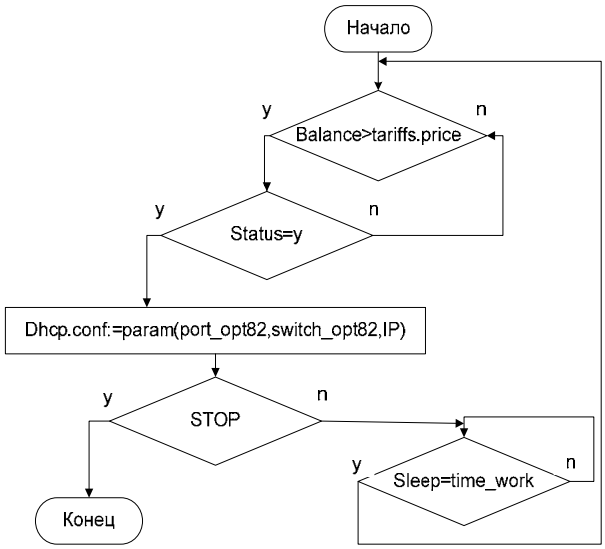

Рисунок 5 – Алгоритм формирования dhcp.conf для ISC DHCP сервера

Файл конфигурации сформирован, опираясь на данные системы учета. Теперь можно приступить непосредственно к выдаче IP адреса и авторизации клиента (алгоритм на рис. 6).

Запрос DHCPDISCOVER - Передаётся клиентом в широковещательном режиме по своей локальной подсети для поиска доступных серверов (в нашем случае через DHCP Relay). После поступления запроса на DHCP сервер, при наличии записи в конфигурационном файле (ID коммутатора, номер порта, IP адрес, который нужно выдавать клиенту), через DHCP Relay посылается пакет DHCPOFFER от сервера в ответ на полученное DHCPDISCOVER-сообщение и содержит предлагаемые параметры настройки. Если в dhcp.conf настроек соответствующих данному запросу от пользователя нет, то в выдаче адреса пользователю отказано. После выдачи параметров настроек сетевого интерфейса IP адрес, маски DNS сервер, шлюза по умолчанию, можно специальным запросом от системы авторизации давать команду серверу доступа на добавление правил, которые разрешат доступ в интернет или к другим ресурсам, если это предусматривается тарифом и набором услуг для данного абонента.

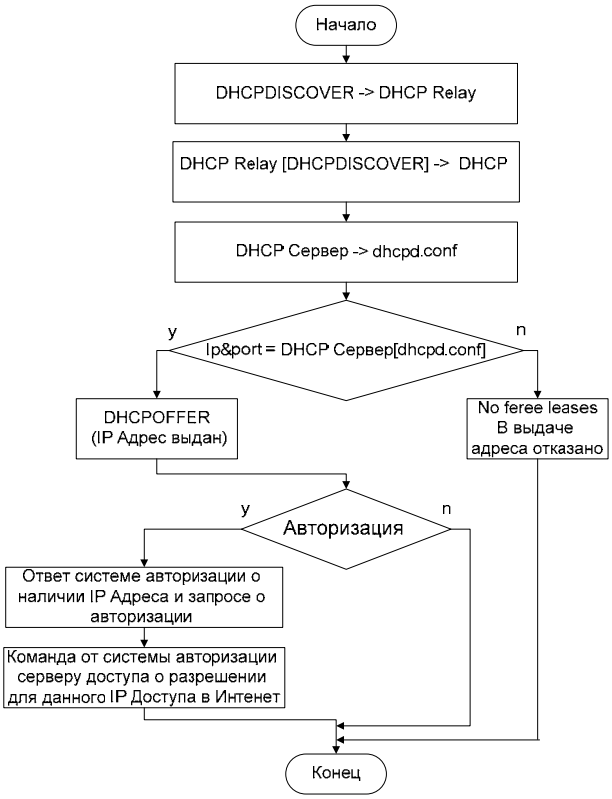

Рисунок 6 – Алгоритм выделения IP-адреса и авторизации клиента.

Выводы. Используя разработанные алгоритмы, предлагается проводить автоматическую настройку и последующую авторизацию на серверном оборудовании оператора связи, которая будет простейшей для клиента, снизит нагрузку на техподдержку и обслуживающий персонал.

Список литературы

1. BGBILLING.RU – Режим доступа: http://bgbilling.ru
2. LANBilling RADIUS и DHCP Option 82 – [Электронный ресурс] – Режим доступа: http://www.lanbilling.ru/dhcp_radius.html
3. Построение сети с использованием технологий DHCP Option 82 и DHCP Snooping – [Электронный ресурс] – Режим доступа: - http://www.ukrindex.com/nodeny/article/opt82/
4. Протокол динамической настройки сетевых устройств (DHCPv4) RFC-2131.
5. RFC 3046 - DHCP Relay Agent Information Option – RFC-3046.