

VLAN на пользователя: архитектура и альтернативы

Авторы: Антон Марченко (сетевой архитектор) и Андрей Захаров (менеджер по работе с клиентами), специалисты компании [БСС](#) по направлению Городские операторские сети, www.metroethernet.ru.

Статья публикуется в рамках конкурса "Формула связи".

На протяжении уже довольно долгого времени одной из наиболее обсуждаемых тем при построении городских Ethernet-сетей является возможность использования в них архитектуры «VLAN на пользователя» или выделение каждого абонента в отдельный широковещательный сегмент. В данной статье мы оценим сильные и слабые стороны данной архитектуры, рассмотрим варианты её реализации, а также представим альтернативное решение на базе функций Private VLAN и Local Proxy ARP.

Для того, чтобы понять для чего нужна архитектура «VLAN на пользователя», вначале рассмотрим традиционную и наиболее простую архитектуру с общим VLAN, когда все устройства сети находятся в одном широковещательном домене (см. рис.1)

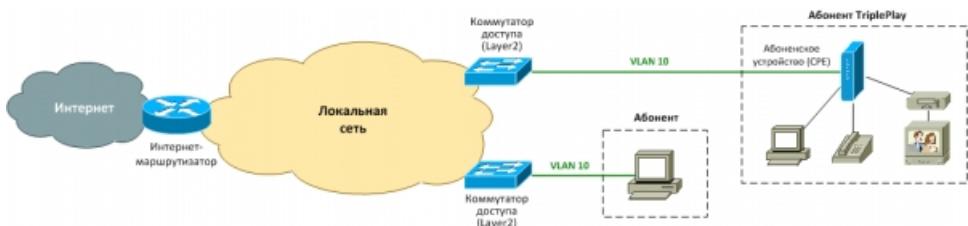


Рисунок 1. Архитектура с общим VLAN

Такая архитектура достаточно легко реализуется и создает небольшую нагрузку на центральное оборудование сети, обеспечивающее доступ в Интернет, за счет того, что обмен локальным трафиком происходит напрямую между абонентами по кратчайшему пути через ближайшие коммутаторы.

Основные недостатки архитектуры с общим VLAN:

1. Изоляция абонентов на втором уровне отсутствует (Layer2), что создает опасность сетевых атак: подмена абонентом своего IP- или MAC-адреса, установка несанкционированного DHCP-сервера, ARP Spoofing, переполнение таблицы MAC-адресов коммутатора.
2. Точками контроля локального трафика становятся коммутаторы доступа, которых в сети достаточно много. Это приводит к проблеме управления большим количеством устройств различных моделей, которые в силу своей невысокой стоимости еще и ограничены по функциональности.

Для решения первой проблемы используются управляемые коммутаторы доступа с поддержкой функций безопасности (DHCP Snooping, IP Source Guard, Port Security, Dynamic ARP Inspection). Решение второй проблемы с точкой контроля локального трафика требует принципиальной перестройки архитектуры сети. И одним из получивших применение способов стал переход на архитектуру «VLAN на пользователя».

Таблица 1 - Сравнение архитектур «Общий VLAN» и «VLAN на пользователя»

	Общий VLAN	VLAN на пользователя
Контроль локального трафика*	Ограниченный	Полный
Количество точек контроля трафика	Большое	Малое
Путь локального трафика**	Оптимальный	Неоптимальный

«Паразитный» широковещательный трафик***	Есть	Нет
Защита от типовых атак	Обеспечивается функциями на коммутаторе доступа	Обеспечивается архитектурой
Сложность реализации	Ниже	Выше

* Контроль трафика требуется для гибкого управления межабонентским трафиком, например, для блокировки доступа к локальным ресурсам сети при отрицательном балансе

** Необходимость прохождения локального трафика через точку контроля ведет к удлинению пути трафика между абонентами, что может увеличить нагрузку на каналы

*** При масштабировании сети широковещательный трафик создает ощутимую нагрузку на каналы связи и абонентские устройства

Архитектура «VLAN на пользователя», как следует из названия, подразумевает выделение для каждого абонента своего собственного VLAN.

Рассмотрим вариант реализации такой архитектуры, предлагаемый ведущими производителями - централизованную модель. В ней точкой консолидации всего абонентского трафика является устройство BRAS – Broadband Remote Access Server (см. рис.2).



Рисунок 2. Централизованная модель VLAN на пользователя

Однако при рассмотрении такой модели возникает вопрос, как терминировать на одном устройстве всех абонентов в сети, если согласно стандарту IEEE 802.1q под номер VLAN выделено всего 12 бит (максимум 4096 значений). В этом случае при большом количестве абонентов решением является использование технологии двойного тегирования пакетов (Q-in-Q) и их терминация на BRAS.

К преимуществам централизованной модели так же можно отнести и единую точку контроля как Интернет- так и локального трафика. Это позволяет гибко управлять качеством обслуживания и полосой пропускания для каждого абонента. Также данная архитектура обеспечивает изоляцию абонентов на втором уровне, что решает большинство проблем безопасности, рассмотренных выше. Главным недостатком становится необходимость в производительном и как следствие достаточно дорогом BRAS.

Следующим вариантом является компромиссная децентрализованная модель, которая обеспечивает обработку Интернет-трафика на BRAS, а обмен локальным трафиком производится на Layer3-коммутаторах. Тем самым удастся снизить нагрузку и требования по производительности к BRAS (см. рис.3).



Рисунок 3. Децентрализованная модель VLAN на пользователя

В чем же основные достоинства децентрализованной модели? Во-первых, как и в централизованной сохраняется изоляция абонентов на втором уровне, тем самым решаются проблемы безопасности. Во-вторых, точками контроля локального трафика теперь являются коммутаторы агрегации, количество которых по сравнению с коммутаторами доступа в сети значительно меньше и они более унифицированы с точки зрения моделей оборудования. В-третьих, локальный трафик теперь не обрабатывается BRAS.

Недостатки децентрализованной модели:

- Ограничение в 4096 VLAN на каждый коммутатор агрегации;
- Неэффективное использование адресного пространства (может быть решено использованием проприетарной функции IP Unnumbered on SVI на коммутаторах Cisco);
- Необходимость ручной конфигурации большого количества VLAN-интерфейсов на коммутаторах агрегации;
- Индивидуальная конфигурация на каждом коммутаторе доступа.

Несмотря на недостатки, именно эта модель получила широкое распространение среди Ethernet-операторов, в основном за счет улучшенной управляемости сети по сравнению с архитектурой с общим VLAN, а также снижением нагрузки на BRAS за счет обмена нетарифицируемым локальным трафиком через коммутаторы агрегации.

Итак, изучив существующие подходы к построению архитектуры операторских Ethernet-сетей, в ходе реализации одного из недавних проектов по построению сети MetroEthernet, мы задались вопросом: Возможно ли найти альтернативный подход и получить архитектуру по функциональности схожую с децентрализованной моделью, но лишенную ее недостатков? Таким образом, была поставлена задача - обеспечить безопасность и сохранить возможность контроля локального трафика на Layer3-коммутаторах агрегации, но при этом избежать создания большого числа VLAN-интерфейсов, и так же максимально унифицировать конфигурацию коммутаторов доступа.

Снизить количество VLAN интерфейсов на коммутаторах агрегации и одновременно унифицировать конфигурацию коммутаторов доступа возможно при использовании одного VLAN для всех абонентов, что по сути означает использование модели с общим VLAN. Однако, как тогда обеспечить прохождение трафика между любыми двумя абонентами через коммутатор агрегации, который бы являлся точкой контроля локального трафика? Решение задачи было найдено и разбито на два этапа.

Во-первых, необходимо изолировать абонентские порты на коммутаторах доступа в рамках одного VLAN и разрешить прохождение трафика из абонентских портов только в uplink-порт, подключенный к вышестоящему коммутатору. Данная функция реализована во многих моделях коммутаторов доступа и имеет различные названия в зависимости от производителя: Private VLAN, Protected port, Traffic Segmentation.

Во-вторых, чтобы трафик между любыми двумя абонентами в рамках одного VLAN всегда проходил через коммутатор агрегации, необходимо, чтобы он отвечал на все ARP запросы внутри этого VLAN от своего имени. Такая функция носит название Local Proxy ARP.

Таким образом, мы получили сегментирование общего VLAN в коммутаторах доступа на отдельные широковебательные домены с помощью функции Private VLAN, а маршрутизацию трафика между этими доменами реализовали на коммутаторах агрегации с помощью Local Proxy ARP. Наглядно схема решения изображена на рис.4.

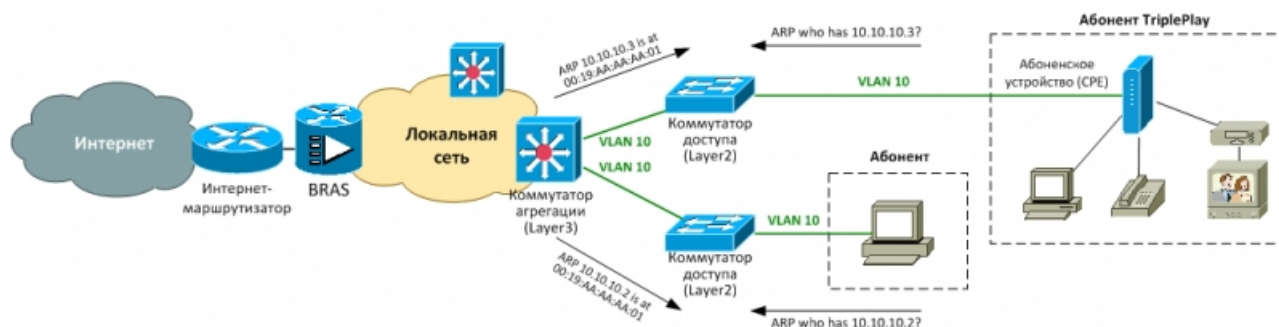


Рисунок 4. Архитектура с использованием Private VLAN и Local Proxy ARP

Контроль локального трафика в данном случае осуществляется на коммутаторе агрегации с помощью списков доступа VLAN ACL.

Задача обеспечения безопасности решается аналогично схеме с общим VLAN – включением на коммутаторах доступа функций DHCP Snooping, Port Security, IP Source Guard и Dynamic ARP Inspection.

Проблема с «паразитным» ширококестельным трафиком отсутствует, так как каждый абонент находится в собственном изолированном ширококестельном домене. Широковещательные пакеты доходят только до коммутатора агрегации и не передаются остальным абонентам внутри общего VLAN.

В результате получилась архитектура по функциональным возможностям аналогичная децентрализованной схеме с VLAN на пользователя, но избавленная от её недостатков. Так как все пользователи находятся в одном VLAN, то конфигурация коммутаторов доступа упрощается и становится унифицированной. Конфигурация коммутаторов агрегации также упрощается за счет необходимости только в одном VLAN-интерфейсе.

Таблица 2 - Сравнение архитектур «PrivateVLAN + Local Proxy ARP» и «VLAN на пользователя»

	PrivateVLAN + Local Proxy ARP	VLAN на пользователя
Контроль локального трафика	Полный	Полный
Количество точек контроля трафика	Малое	Малое
«Паразитный» ширококестельный трафик	Нет	Нет
Защита от типовых атак	Обеспечивается функциями на коммутаторе доступа	Обеспечивается архитектурой
Сложность реализации	Ниже	Выше
Конфигурация коммутаторов доступа	Унифицированная	Индивидуальная

Использование адресного пространства	Эффективное	Неэффективное
--------------------------------------	-------------	---------------

Представленная архитектура на базе функций PrivateVLAN + Local Proxy ARP была успешно протестирована и внедрена в реальной сети MetroEthernet, об опыте построения и технических деталях которой мы продолжим рассказ в следующей статье.