Автор:
30.03.12 15:17 - Последнее обновление 30.03.12 17:12

Руководство по pfSense 2.0. Часть 10

Часть 10 Виртуальные LAN (VLAN)

оглавление

VLAN реализуют средство сегментации единственного коммутатора во множество широковещательных доменов, позволяя функционировать единственному коммутатору так же как множество коммутаторов. Данная функциональность обычно используется для сегментации сети тем же образом, что и множество коммутаторов, помещая хосты в определённые сегменты сконфигурированы на коммутаторе. Когда между коммутаторами используется транкинг, устройства в одном сегменте не обязательно должны находится на том же коммутаторе. В этой главе рассматривается концепция, терминология и конфигурация VLAN.

Требования

Существует два обязательных требования для развёртывания VLAN. 1. Наличие коммутатора 802.1Q с возможностью VLAN - практически любой "приличный" управляемый коммутатор произведённый позже 2000 года поддерживает 802.1Q VLAN транкинг. Вы не можете использовать функционал VLAN на неуправляемых коммутаторах. 2. Наличие сетевого адаптера с поддержкой VLAN меток - вам необходим NIC аппаратно поддерживающий функционал меток VLAN или длинные фреймы(кадры). Поскольку каждый кадр содержит в заголовке 802.1Q 4 байта метки, размер кадра может составить до 1552 байт. Необходим NIC, аппаратно поддерживающий VLAN теги или длинные кадры, поскольку другие адаптеры не будут функционировать с кадрами более чем нормальной 1518-байтной длины с 1500 MTU Ethernet. Это приведёт к пропуску длинных кадров, что вызовет проблемы производительности и сброс подключения.

ЗАМЕЧАНИЕ Только по тому признаку, что производителем указывается возможность поддержки данного функционала не следует думать, что ваш адаптер сможет нормально поддерживать длинные кадры. В частности Realtek rl (4) - самый характерный пример данного замечания. Многие из адаптеров могут работать прекрасно, но некоторые реализуют поддержку длинных кадров некорректно, а некоторые вообще не будут принимать кадры с тегами 802.1Q. Если вы столкнулись с проблемами, используя один тип адаптеров в реализации VLAN, попробуйте воспользоваться списком рекомендуемых адаптеров. Мы не сталкивались с проблемами NIC перечисленными в списке поддерживающих VLAN.

Ethernet интерфейсы с аппаратной поддержкой VLAN следующие:

bce(4), bge(4), cxgb(4), em(4), ixgb(4), msk(4), nge(4), re(4), stge(4),ti(4), txp(4), vge(4).

Ethernet интерфейсы с поддержкой длинных кадров:

bfe(4), dc(4), fxp(4), gem(4), hme(4), le(4), nfe(4), nve(4), rl(4),sis(4), sk(4), ste(4), tl(4), tx(4), vr(4), xl(4).

Терминология

Данный раздел рассматривает терминологию, которую необходимо понимать для успешного развёртывания VLAN.

Транкинг

Транкинг понимается как возможности создать множество VLAN на одном порту коммутатора. Кадры покидающие порт транка в заголовке отмечаются тэгом 802.1Q позволяя связанному устройству различать множественные VLAN. Порты транка используются для соединения множества коммутаторов, и для соединения любых устройств которые поддерживают совместимость с 802.1Q тэгами и требуют доступа к множеству VLAN. Обычно это только маршрутизатор реализующий соединение между VLAN, в нашем случае pfSense, а так же соединения с другими коммутаторами содержащими множество VLAN.

Идентификатор VLAN (VLAN ID)

Каждый VLAN ассоциирован с идентификатором (ID), который используется для идентификации помеченого трафика. ID - это номер от 1 до 4094. По умолчанию, VLAN на коммутаторах - VLAN1, и этот VLAN не должен использоваться при развёртывании транкинга VLAN. Об этом мы поговорим дальше, в разделе 10.3. "VLAN и безопасность". Кроме отказа от использования VLAN 1, вы можете выбрать желаемый номер VLAN из указанного диапазона. Некоторые начинают с VLAN 2 и добавляют по единице до достижения необходимого числа VLAN. Другая общая практика - использовать третий октет в IP подсети VLAN в качестве VLAN ID. Например, если вы используете подсети 10.0.10.0/24, 10.0.20.0/24 и 10.0.30.0/24 логично использовать VLAN 10, 20, и 30 соответственно. Выбор VLAN ID следует вести по схеме которая имеет для вас логический смысл.

Родительский интерфейс

Родительский интерфейс ссылается на физический интерфейс, на котором постоянно находится VLAN, такой как em0 или bge0. Когда вы конфигурируете VLAN на pfSense или FreeBSD, каждому из них назначается виртуальный интерфейс, начиная с vlan0 и увеличением на единицу для каждого последующего VLAN. В pfSense 1.2.x номер интерфейса VLAN никак не связан с VLAN ID. Вы не должны назначать свой родительский интерфейс на любой из интерфейсов pfSense - его функция должна быть исключительно функцией родительского интерфейса VLAN. В небольшом количестве ситуаций возможно и не выполнять это правило, но могут возникать различные проблемы с конфигурацией коммутатора, а так же с работой каптивного портала и это вынудит использовать значение по умолчанию для порта транка VLAN, чего следует избегать (проблема обсуждается в разделе 10.3. "VLAN и безопасность".

Порт доступа

Порт доступа ссылается на порт коммутатора, реализующий доступ к отдельному VLAN, где кадры не помечаются заголовками 802.1Q. Вы подключаете устройство к единственному порту доступа VLAN. Большинство портов вашего коммутатора конфигурируются как порты доступа. Устройство на порте доступа не знают о наличии VLAN в сети. Для них каждый VLAN представляется так же, как если бы их и не было.

Двойной таггинг (QinQ)

Данная возможность применяется для двойной метки траффика, используя внешние и внутренние метки 802.1Q. Обычно такой режим называется QinQ. Он может быть полезен в крупных сетевых средах ISP и ряде очень больших сетей. Возможна и тройная метка трафика. В текущий момент pfSense не поддерживает QinQ, но эта возможность станет доступна в версии 2.0. Крупные среды нуждаются в дополнительной мощности маршрутизаторов основанных на специальных решениях, а QinQ вводит дополнительный уровень сложности, необходимость которой в малых сетевых средах не востребована.

Private VLAN (PVLAN)

PVLAN использует возможность некоторых коммутаторов сегментировать хосты в пределах отдельного VLAN. Обычно хосты в пределах одной VLAN конфигурируются также как хосты на одном коммутаторе без VLAN. PVLAN реализует средство предотвращения связи хостов друг с другом в пределах VLAN, позволяя только связь между хостом и его шлюзом по умолчанию. Возможно не является исключительной для pfSense, а является общим правилом. Функциональные возможности коммутатора, такие как эта, являются единственным средством предотвращения связи между хостами в той же самой подсети. Без PVLAN межсетевая защита не сможет управлять трафиком в пределах подсети, по с кольку он не будет направляться через шлюз по умолчанию.

VLAN и безопасность

VLAN предлагают множество средств сегментации сети и изоляции подсетей, однако существуют некоторые проблемы безопасности, которые необходимо принимать во внимание при проектировании и реализации решений использующих VLAN. Нельзя сказать что VLAN небезопасны, но неправильное конфигурирование может сделать вашу сеть уязвимой. В прошлом, в некоторых реализациях коммутаторов тоже существовали проблемы безопасности VLAN.

Из-за возможности неверного конфигурирования вы должны выделять различающие зоны доверия сетей на их физических коммутаторах. Например, вы могли одновременно использовать один и тот же коммутатор с VLAN для всех внутренних сетей и для сетей находящихся за пределами брандмауэра, чего следует избегать, поскольку это может направить не проверенный трафик в ваши внутреннюю сеть. Как минимум, в подобных сценариях, вы должны использовать два коммутатора: один для внешней сети (до брандмауэра) и один для внутренней сети. Во многих средах сегмент DMZ рассматривается отдельно, с использованием третьего коммутатора в дополнение к коммутаторам глобальной сети и LAN. В других средах, глобальная сеть находится на собственном коммутаторе, в то время как все сети позади брандмауэра находятся на тех же коммутаторах используя VLAN. Выбор сценария соответствующего вашей сети

зависит от конкретных обстоятельств, уровня допустимого риска и вашей паранойи.

Поскольку VLAN1 - значение по умолчанию или native VLAN, он может использоваться коммутаторами самым неожиданным способом. Всегда лучше использовать другой VLAN. Коммутаторы могут посылать через нативный VLAN различные протоколы, такие как STP (Spaning Tree Protocol), VTP (Транкинговый протокол VLAN), и CDP(Протокол обнаружения Cisco). Это позволяет сохранять внутренний трафик изолированным от ваших данных. Если вам необходимо использовать VLAN1, вам придётся быть крайне осторожным, и назначить каждому отдельному порту на каждом коммутаторе отдельный VLAN вместо VLAN1и не создавать интерфейс управления коммутатора на VLAN1. Кроме того, вам необходимо изменить нативный VLAN группы коммутаторов на какой либо другой, не используемый VLAN. Некоторые коммутаторы не могут реализовывать такие обходы, и как правило, проще использовать для ваших данных другой VLAN, чем заморачиваться с VLAN1. С VLAN ID 2 доступен выбор 4094 VLAN, потому гораздо проще проигнорировать VLAN при проектировании схемы VLAN.

Когда VLAN помечает трафик, он передаётся через транк на нативном VLAN, теги в пакетах соответствующих нативному VLAN могут удаляться коммутатором, в целях сохранения совместимости с верхними сетями. Хуже, если с пакетов отмеченных двойным тегом с нативного VLAN и отличного VLAN, при транкинге будет удалён только тэг нативного VLAN, и при дальнейшей обработке этот трафик может завершиться на другом VLAN. Этот результат так же называется "VLAN hopping" (Прыганием VLAN). Как упоминалось выше, любой неотмеченный трафик на порту транка будет приниматься нативным VLAN, который может перекрываться с назначенным интерфейсом VLAN. В зависимости от того, как коммутатор обрабатывает такой трафик и как он рассматривается pfSense, прямое использование интерфейса может привести появлению двух интерфейсов на одном VLAN.

Поскольку порт транка может общаться с любым VLAN в группе связанных коммутаторов, который могут быть даже не представлены на текущем коммутаторе в вашей конфигурации, это важно для физической безопасности порта транка. Убедитесь, что нет никаких портов, конфигурированных для транкинга и не подключенных, к которым можно подцепиться случайно или как то иначе. В зависимости от коммутатора, могут поддерживаться динамические обмены транкинга. Вы должны быть уверенны в блокировке данного функционала или его ограничении.

Существуют данные, что некоторые VLAN коммутаторы пропускают трафик через VLAN при высоких нагрузках, или если MAC адрес компьютера на VLAN замечен на другом VLAN. Эти проблемы имеют тенденцию в старых коммутаторах с устаревшим программным обеспечением, или в чрезвычайно низкокачественных управляемых коммутаторах. В большей степени проблемы были решены много лет назад, когда они были достаточно распространёнными. Независимо от того, коммутатор какой марки вы используете, следует провести некоторые исследования, на тему тестирования безопасности устройства и использовать последнюю версию прошивки. Поскольку данные проблемы - аппаратные, и не связанные с pfSense, они являются общими проблемами безопасности. Обратитесь к документации на оборудование для изучения безопасности использования VLAN.

Конфигурация VLAN в pfSense

Этот раздел рассматривает конфигурацию VLAN на стороне pfSense.

Консольное конфигурирование VLAN

Вы можете конфигурировать VLAN в консоли, используя функцию Assign Interfaces (Назначение интерфейсов). Следующий пример показывает, как конфигурировать два

VLAN, ID 10 и 20, с le2 в качестве родительского интерфейса. Интерфейсы VLAN назначены как OPT1 и OPT2.

pfSense console setup

****

0) Logout (SSH only)

1) Assign Interfaces

2) Set LAN IP address

3) Reset webConfigurator password

4) Reset to factory defaults

5) Reboot system

6) Halt system

7) Ping host

8) Shell

9) PFtop

10) Filter Logs

11) Restart webConfigurator

12) pfSense Developer Shell

13) Upgrade from console

14) Disable Secure Shell (sshd)

98) Move configuration file to removable device

Enter an option: 1

Valid interfaces are:

le0 00:0c:29:d6:e7:dc (up)

le1 00:0c:29:d6:e7:e6 (up)

le2 00:0c:29:d6:e7:f0 (up)

plip0 0

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required.
Do you want to set up VLANs now [y|n]? y

VLAN Capable interfaces:

le0 00:0c:29:d6:e7:dc (up)

le1 00:0c:29:d6:e7:e6 (up)

le2 00:0c:29:d6:e7:f0 (up)

Enter the parent interface name for the new VLAN (or nothing if finished): le2 Enter the VLAN tag (1-4094): 10

VLAN Capable interfaces:

le0 00:0c:29:d6:e7:dc (up)

le1 00:0c:29:d6:e7:e6 (up)

le2 00:0c:29:d6:e7:f0 (up)

Enter the parent interface name for the new VLAN (or nothing if finished): le2 Enter the VLAN tag (1-4094): 20

VLAN Capable interfaces:

le0 00:0c:29:d6:e7:dc (up)

le1 00:0c:29:d6:e7:e6 (up)

le2 00:0c:29:d6:e7:f0 (up)

Enter the parent interface name for the new VLAN (or nothing if finished): vlan0 VLAN tag 10, interface le2

vlan1 VLAN tag 20, interface le2

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: le1

Enter the WAN interface name or 'a' for auto-detection: le0

Enter the Optional 1 interface name or 'a' for auto- detection (or nothing if finished): vlan0

Enter the Optional 2 interface name or 'a' for auto-detection (or nothing if finished): vlan1

Enter the Optional 3 interface name or 'a' for auto-detection (or nothing if finished):

The interfaces will be assigned as follows:

LAN -> le1

WAN -> le0

OPT1 -> vlan0

OPT2 -> vlan1

Do you want to proceed [y|n]? y

One moment while we reload the settings...

Через несколько секунд ваши параметры будут применены и вы вернётесь в консоль. Если конфигурирование VLAN производится в консоли, вам не выдаётся предупреждение о том, что необходима перезагрузка для начала функционирования VLAN. Некоторые сетевые адаптеры не будут работать корректно, если система не перезагружена. Вообще перезагрузка не всегда необходима, однако мы не нашли способ обнаружения частных случаев. Короче говоря, при начальном 31 конфигурировании VLAN рекомендуется перезагрузка. При дальнейшем добавлении VLAN, после того как VLAN уже сконфигурирован, перезагрузка не требуется.

Web интерфейс конфигурирования VLAN

Переходим на страницу Interfaces >> Assign (Интерфейс >> Назначение). Рисунок 10.1. "Интерфейсы: Назначение". WAN и LAN назначаются на интерфейсы vr0 и vr1 соответсвенно. Так же существует интерфейс vr2 который используется в качестве родительского интерфейса на VLAN.

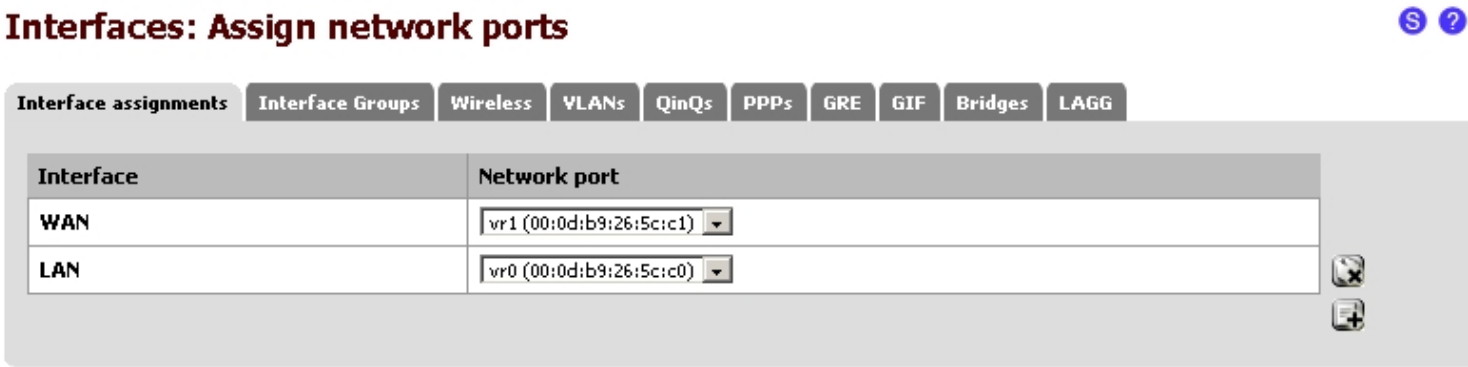


Рисунок 10.1. Назначение интерфейсов

Щёлкаем на закладку VLANs. Потом нажимаем [+] для добавления нового VLAN как

показано на Рисунке 10.2. "Список VLAN".

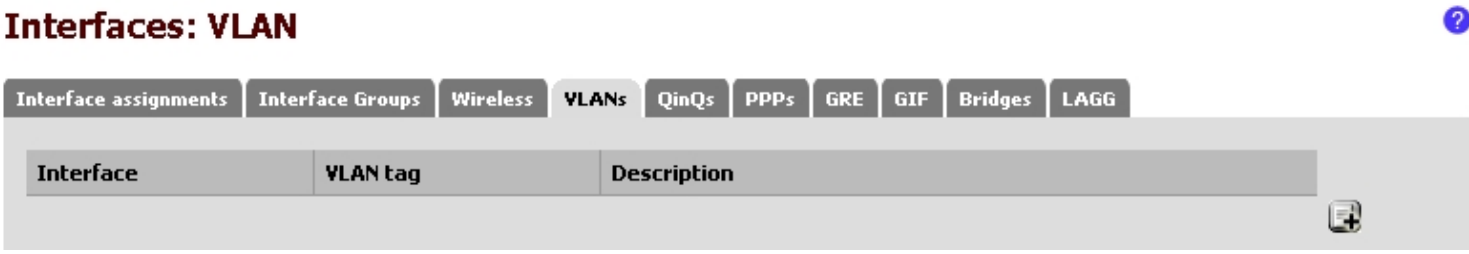


Рисунок 10.2. Список VLAN

Попадаем на экран редактирования VLAN, подобный Рисунку 10.3. "Редактирование VLAN". Здесь, выбираем родительский интерфейс (Parent Interface), vr2. Вводим тег VLAN, 10, и вводим описание (Description) сети находящейся на данном VLAN (DMZ, Database, testing, и т.п.).

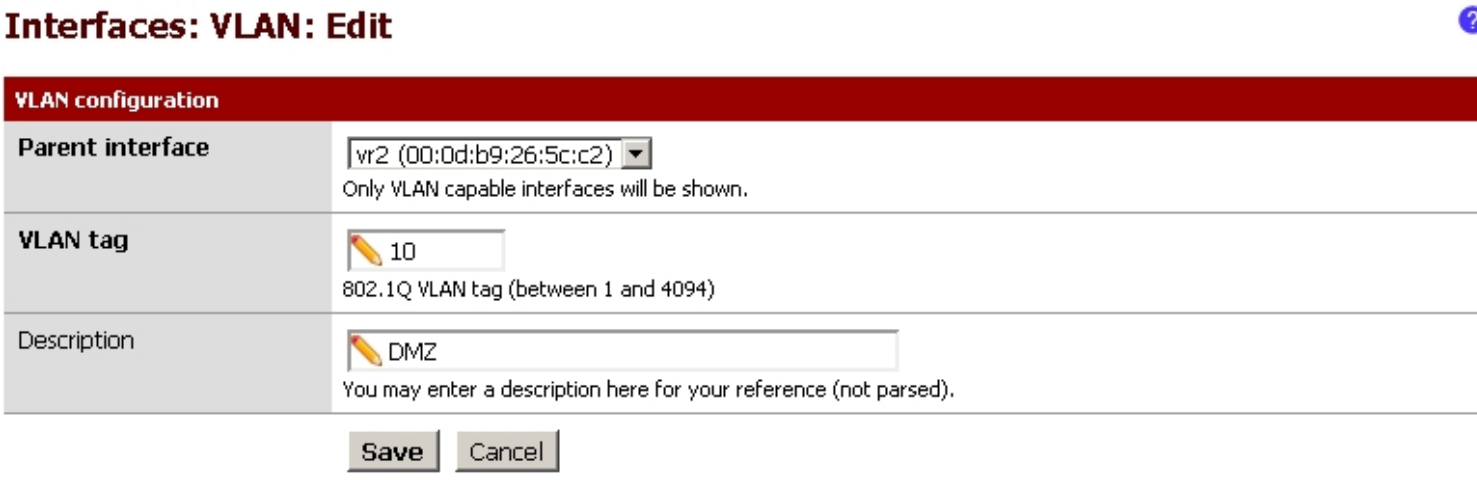


Рисунок 10.3. Редактирование VLAN

Нажав Сохранить (Save), вы возвращаетесь в список доступных VLAN, который теперь включает вновь добавленный VLAN 10. Повторите процесс для добавления VLAN, например VLAN 11.

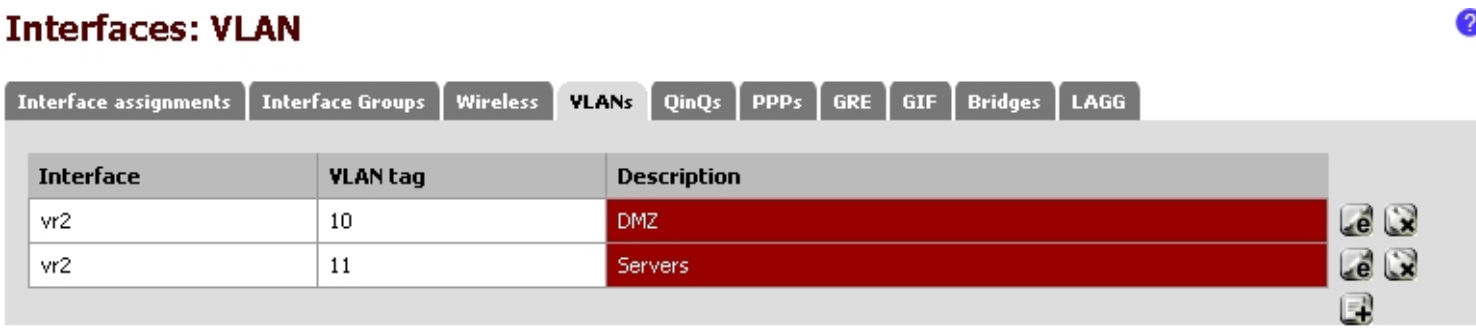
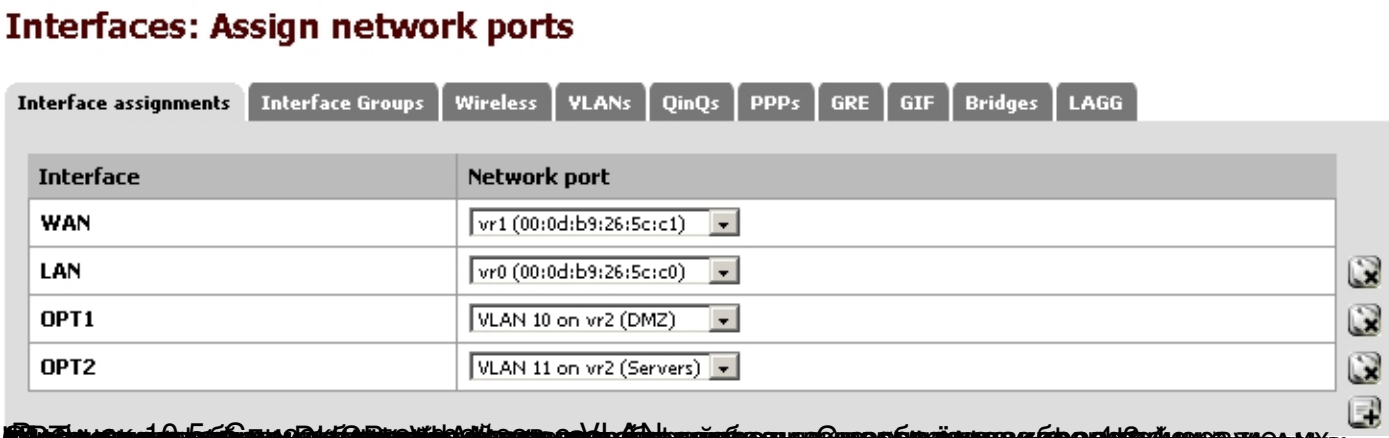


Рисунок 10.4. Список VLAN

Теперь необходимо назначить VLAN на интерфейсы. Для этого щёлкните на закладке Interface Assigments, затем нажмите [+] и в раскрывающемся списке доступных интерфейсов вы должны увидеть новый VLAN. Для OPT1, выберем интерфейс с ID VLAN 10. Щёлкните ещё раз [+] и выберите для OPT2 ID VLAN 20. Когда закончите, всё должно выглядеть примерно как на рисунке 10.5. "Список интерфейсов с VLAN".

Автор:
30.03.12 15:17 - Последнее обновление 30.03.12 17:12



switchport access vlan 10