Сетевые утилиты

MAC-фильтр

Команда "*macf*" позволяет задать жёсткое соответствие MAC и IP-адресов в Ethernet сети. Это может быть полезно сервис-провайдерам, предоставляющим услуги подключения к сети независимой группе абонентов через один блок доступа, например частным лицам в жилом доме. В этом случае, у абонентов часто появляется искушение изменить свой IP-адрес (на соседский) и, тем самым, обмануть учётную систему провайдера. В общем случае, эта проблема почти неразрешима, однако, зафиксировав чёткое соответствие MAC-адреса абонента и назначенного ему IP-адреса, можно существенно облегчить себе жизнь, поскольку процедура смены MAC-адреса намного сложнее.

NAT

Модуль преобразования сетевых адресов (Network Address Translation) позволяет в какой-то мере решить проблему исчерпания пространства адресов в IPv4 и даёт возможность подключить несколько компьютеров через единственное соединение с официальным IP-адресом. Модуль NAT принимает исходящие из локальной сети IP-пакеты, изменяет адрес отправителя на официальный адрес, выделенный провайдером, и повторно отправляет эти пакеты в потоке исходящих данных. NAT делает это меняя IP-адрес отправителя и порт таким образом, что когда данные принимаются обратно, он может определить расположение источника, который запрашивал данные, и переслать их ему. Модуль NAT аналогичен по возможностям (за некоторыми исключениями) модулю "*natd*" и библиотеки "*libalias*" из FreeBSD.

IP firewall

"*ipfirewall*" – это механизм позволяющий фильтровать проходящие через узел IP пакеты по различным критериям. Системный администратор может определить набор входящих (*addincoming*) и исходящих (*addoutgoing*) фильтров. Входящие фильтры описывают пакеты, которые могут приниматься данным узлом. Исходящие фильтры описывают пакеты, которые могут выходить **из** данного узла после маршрутизации.

Каждый фильтр описывает класс пакетов и определяет способ их обработки (отбросить и зарегистрировать, пропустить, пропустить и зарегистрировать). Пакеты могут фильтроваться на основании следующих характеристик:

- тип пакета (все IP, TCP, UDP, ICMP)
- адрес источника и/или получателя (и номера портов для TCP и UDP)
- интерфейс, через который поступил пакет
- пакет установления TCP-соединения
- пакет является первым, не первым или последним фрагментом фрагментированного пакета
- включены или нет различные опции IP протокола
- MAC-адрес станции назначения или источника.

QoS

QoS менеджер представляет собой удобный и гибкий механизм манипуляции потоками данных, проходящими через устройство.
Концепция этого механизма заключается в следующем:
В системе существует несколько (64) программных каналов, каждый из которых может обладать некоторыми свойствами. С помощью специальных правил, можно заставить пакеты, проходящие через устройство, проходить через тот или иной канал и изменять, тем самым, свойства самого пакета или потока, которому он принадлежит.
Количество свойств, которыми обладают каналы, будет расширяться по мере развития системы..

В общем случае, механизм QoS применяется для:

- Ограничения трафика по определенным направлениям
- Приоритезация трафика
- Перенаправление трафика.

Туннели

Туннель - это механизм позволяющий объединить две удалённые и не связанные физически сети в единую логическую структуру. Туннели широко используются для создания корпоративных сетей или так называемых "виртуальных частных сетей" (VPN), когда несколько офисов, разнесённых территориально и, возможно, подключенных к сети через разных провайдеров, соединяются с центральным офисом или друг с другом туннелями, образуя, таким образом, единую корпоративную структуру. При этом, во всей корпоративной сети может использоваться собственное адресное пространство и учётная политика, не зависящая ни от места подключения ни от провайдера услуг.

Использование туннелей позволяет также решить проблему использования единой транспортной среды в сети коллективного доступа для предоставления услуг различным клиентам несколькими провайдерами. То есть независимо от места подключения клиента к единой транспортной сети, он может быть соединён туннелем и получать услуги от конкретного провайдера.

Существует несколько различных способов организации туннелей.
В ОС **WANFleX** реализован один из них - IP Encapsulation within IP, в соответствии с RFC2003. Этот тип туннеля обеспечивается также маршрутизаторами Cisco и является подмножеством протокола IPSEC поддерживаемого многими операционными системами.

Практически, туннель реализуется в виде PtP линка между двумя маршрутизаторами. Весь поток, проходящий через такой линк, инкапсулируется в IP-пакеты и доставляется к конечной точке линка через уже существующую транспортную среду.

Коммутация

Устройство **InfiNet Wireless R5000** может быть сконфигурировано как коммутатор второго уровня или мост. В отличие от стандартной реализации коммутатора/моста у большинства других производителей беспроводного оборудования, коммутатор MAC-уровня InfiNet Wireless представляет собой мощный инструмент для обеспечения защиты от несанкционированного доступа и позволяющий реализовать полнофункциональную мультисервисную сеть.

Маршрутизация

Устройство **InfiNet Wireless R5000** может быть сконфигурировано для работы не только как коммутатор, но и как маршрутизатор. Более того, устройство может работать в режимах коммутации и маршрутизации одновременно.

Поддерживается как статическая, так и динамическая маршрутизация по протоколам RIP и OSPF. Подробнее об использовании каждого из этих протоколов написано ниже в разделе «Протоколы маршрутизации».