Title

Ключевые возможности системы

Успешно сдайте бесплатный сертификационный экзамен в Академии "Инфинет" и получите статус сертифицированного инженера Инфинет.

Пройти сертификационный экзамен

Возможности архитектуры MINT

Режим централизованной раздачи маркера

Режим централизованной раздачи маркера (polling) позволяет увеличить устойчивость и пропускную способность базовых станций в условиях большой нагрузки и дисбаланса в уровнях сигналов от абонентских блоков. Особенно полезен в тех случаях, когда абонентские блоки находятся на значительном удалении или вне прямой видимости друг от друга и не могут координировать свои действия, прослушивая среду передачи. Режим опроса позволяет наладить устойчивую связь нескольких абонентов в условиях, когда метод случайного доступа CSMA/CA вообще не работает.

Автоматическое регулирование скорости передачи

В режиме автоматического регулирования скорости передачи (*autobitrate*) каждое устройство контролирует параметры соединения независимо (амплитуды передаваемого/принимаемого сигналов, количество переповторов и ошибок и т.д.) и выбирает оптимальную для текущих условий скорость работы, обеспечивающую приемлемые параметры работы. Скорость на передачу и на прием, естественно, могут отличаться, но будут оптимальными на текущий момент.

Частотный роуминг

Для облегчения процесса миграции между несколькими независимыми сегментами сети архитектура MINT поддерживает режим частотного роуминга. Поиск в режиме роуминга выполняется путём перебора радиочастотных и административных параметров, определяемых с помощью системы профилей. Каждый профиль определяет некий фиксированный набор параметров радиоинтерфейса и сети, которые будут устанавливаться в системе перед каждым очередным этапом поиска. Эвристический алгоритм поиска быстро оценивает общую остановку в эфире и, сосредоточившись на ключевых параметрах профилей, выбирает из числа обнаруженных сетей наиболее подходящую.

Объединение сегментов в единую MINT-сеть через проводные каналы

Протоколы архитектуры MINT могут работать не только по радио, но и через проводной интерфейс Ethernet. Для этого в системе имеется “псевдо” радио-интерфейс (prf), который можно “прицепить” к физическому интерфейсу. Такой псевдо радио-интерфейс можно использовать для настройки на нём узла MINT-сети и даже для объединения с другими интерфейсами. С точки зрения протоколов MINT, это будет обычный радио-интерфейс, через который узел сможет найти соседей и установить с ними связь.

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.

Более подробное описание команды приведено в разделе "Команда macf".

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.

Описание команды приведено в разделе "Команда nat"

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 пакета
- включены или нет различные опции IP-протокола
- MAC-адрес станции назначения или источника.

Рисунок ниже иллюстрирует прохождение пакетов через систему фильтрации маршрутизатора:

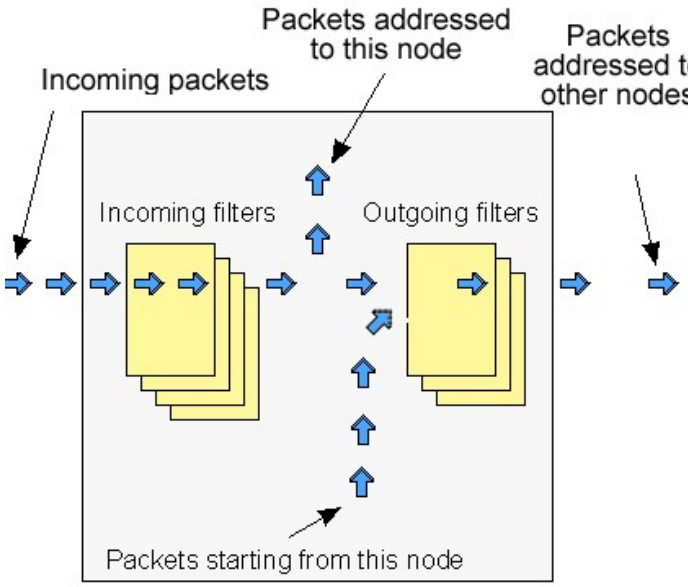

Рисунок - Прохождение пакетов через систему фильтрации маршрутизатора

Фильтры могут быть двух классов (наборов) - запрещающие (*reject*) и разрешающие (*accept*).

Кроме того, фильтр может быть применим ко всем принимаемым пакетам или только к пакетам, поступающим через определённый интерфейс.

Каждый принимаемый пакет сравнивается со всеми правилами в наборе по очереди. Первый же фильтр, который полностью соответствует принятому пакету, определяет его дальнейшую судьбу. Если фильтр является разрешающим (*accept*), то пакет принимается, если фильтр запрещающий, то пакет отбрасывается. Если нет ни одного фильтра в наборе, или ни один из них не подходит к данному пакету, то пакет принимается.

ПРЕДОСТЕРЕЖЕНИЕ

Отбрасываемый пакет просто уничтожается без уведомления источника.

Фильтры определяются с помощью команды "*ipfw*". Например, команда

```
ipfw add reject all from 192.168.5.3 to 192.168.11.7
```

добавит в набор входящих фильтров запрещающий фильтр, который отбросит все пакеты, приходящие с адресом источника 192.168.5.3 и адресом назначения 192.168.11.7.

Для более полного понимания работы фильтра необходимо ознакомиться с описанием того, как строятся фильтры и механизмом применения фильтров.

Описание команды приведено в разделе "Команда ipfw".

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 (200) 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.

Описание команды приведено в "Команда qm".

Туннели

Туннель - это механизм позволяющий объединить две удалённые и не связанные физически сети в единую логическую структуру.

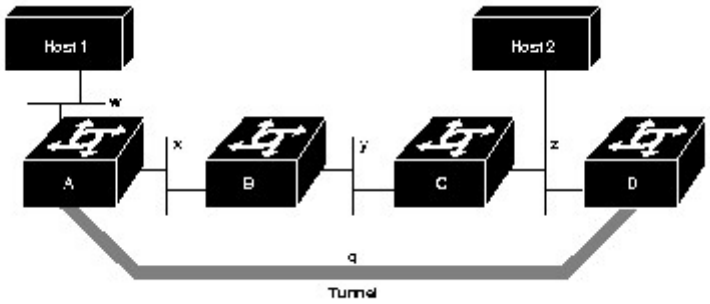

Рисунок - Схема туннеля

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.

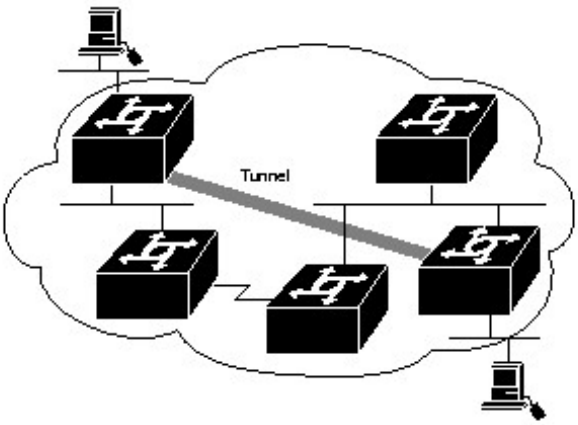

Рисунок - Схема туннеля

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 P2P 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.

Описание команды приведено в разделе "Команда tun".

Коммутация

Устройство InfiNet Wireless может быть сконфигурировано как коммутатор второго уровня или мост. В отличии 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 мульти-сервисную сеть.

Маршрутизация

Устройство InfiNet Wireless 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".

Дополнительные утилиты и сервисы

Telnet

Команда "*telnet*" используется для установления соединения с удалённой машиной в режиме эмуляции терминала. В данной реализации используется простая прозрачная трансляция потока символов без какой-либо промежуточной интерпретации, поэтому тип терминала будет определяться тем терминалом, с которого была выполнена данная команда.

Ping

Команда "*ping*" посылает тестовые пакеты (*ICMP_ECHO_REQUEST*) на заданный адрес (IP). Позволяет оценить достижимость и время отклика прохождения пакетов.

Списки контроля доступа

В практике сетевого планирования довольно часто возникает необходимость группировки некоторых однотипных параметров для использования их в качестве списка допустимых значений различных фильтров (например, *ipfw, qm, ipstat*). Списки контроля доступа (*ACL*) позволяют эффективно решить эту задачу. Более того, специальный список контроля доступа позволяет ограничить доступ на само устройство. Все попытки установить соединение с устройством из сетей, не указанных в данном списке, будут отвергаться.

Протоколы маршрутизации

Статическая

Команда "*route*" позволяет манипулировать содержимым системных таблиц маршрутизации.
В нормальном режиме, когда запущен модуль динамической маршрутизации, эта команда не нужна, однако в некоторых случаях позволяет добиться более точной, нестандартной настройки.

Все маршруты описанные командой "*route add*" являются "псевдостатическими". Это означает, что информация о маршруте будет немедленно помещена в конфигурацию и будет находиться там до тех пор пока её явно не удалят командой "*route delete*", однако реально указанные маршруты будут устанавливаться в системные таблицы лишь тогда, когда появится интерфейс с адресом и сетевой маской, в пределах которой находится указанный адрес шлюза (*gateway*). При исчезновении интерфейса, указанные маршруты будут немедленно вычеркнуты из таблиц маршрутизации (но останутся в конфигурации).

Описание команды в разделе "Команда route"

Динамическая

RIP

Протокол RIP (Routing Information Protocol) версий RIP-1 и RIP-2 поддерживается двумя модулями системы – RIP и ARIP. Модуль RIP более прост в использовании, но ARIP дает больше возможностей по настройке маршрутизации. Более того, ARIP может работать совместно с модулем OSPF и, таким образом, позволяет делать уникальные настройки, повышающие производительность всей системы.

Описание команды в разделе "Команда rip".

OSPF

Протокол OSPF является стандартным протоколом маршрутизации для использования в сетях IP. Основные принципы организации современной версии протокола маршрутизации OSPF изложены в RFC 2328. Протокол OSPF представляет собой классический протокол маршрутизации класса Link–State, который обеспечивает:

- отсутствие ограничений на размер сети
- поддержку внеклассовых сетей
- передачу обновлений маршрутов с использованием адресов типа multicast
- достаточно высокую скорость установления маршрута
- использование процедуры authentication при передаче и получении обновлений маршрутов.

Описание команды в разделе "OSPFv2".

Средства управления

HTTP

Наличие поддержки протокола HTTP позволяет выполнять конфигурацию маршрутизатора с помощью любого доступного web-браузера. Мини сервер, реализованный в маршрутизаторе, позволяет выполнить любую команду операционной системы **WANFleX**, а
также некоторые предустановленные шаблоны.

RSH

"*rshd*" - модуль поддержки протокола RSH (Remote Shell). RSH сервер обеспечивает удалённое исполнение команд с помощью программы "*rsh*". Идентиф икация основана на использовании привилегированных TCP портов и списка разрешённых узлов.

Описание каоманды в разеделе "rshd (Remote Shell)".

SNMP

Модуль сетевого протокола управления (SNMP) версии 1 и версии 3.

Поддержка протокола SNMP является важной составляющей любого коммуникационного устройства, поскольку позволяет администратору сети использовать единую систему и механизмы контроля всей сети в целом и каждой её компоненты в отдельности.

Хотя в первой версии SNMP v1 уделено недостаточно внимания вопросам безопасности самого протокола, что делает весьма проблематичным его использование для управления сетью, однако он широко используется для контроля и анализа функционирования сети. Изменение переменных MIB для первой версии отключено, она по-прежнему работает только в режиме "*read-only*". Опция "*v1disable*" позволяет совсем отключить поддержку первой версии, а также немного ускоряет обработку входящих SNMP-запросов.

Модуль SNMP также поддерживается версия SNMP v3 с моделью доступа USM (User-based Security Model) с MD5 аутентификацией и кодированием. Для организации доступа создаются пользователи с указанием имени, паролями и минимальными уровнями доступа (с аутентификацией и кодированием или без них).

Данная реализация поддерживает MIB-II, а также частные MIB.

Описание команды в разделе "Команда snmpd".