Интегральный Интернет-процессор Internet Processor II™

В то время как в других маршрутизаторах фильтрация IP пакетов, формирование и обработка трафика были реализованы программными средствами, интернет-процессор Internet Processor II обеспечивает еще большую гибкость практически без ухудшения производительности. Возможность выполнения этих функций со скоростью линии OC-192c не имеет прецедентов в нашей отрасли.

Винт Серф, вице-президент MCI WorldCom, Inc. по Интернет-архитектуре и технологии

Согласно концепции Juniper Networks, сеть Интернет станет фундаментальной инфраструктурой связи для доступа к общественным и частным сетям, приложений передачи голоса и видео следующего поколения. Первым шагом в реализации этой концепции стал выпуск специализированной интегральной схемы Интернет процессора (ИП) Internet Processor™, которая улучшила характеристики форвардинга пакетов до уровня, обеспечиваемого новой оптоволоконной инфраструктурой. Следующим шагом была разработка ИП Internet Processor II™, позволившего учитывать при форвардинге пакетов алгоритмы протокола IP. В результате существенно улучшились, по сравнению с программными решениями, показатели обработки пакетов. Теперь при развертывании новых IP услуг производительность форвардинга не падает, что создает преимущество перед конкурентами на быстро развивающемся рынке.

Internet Processor II, конфигурируемый с помощью ОС JUNOS™, предоставляет инструменты, необходимые для безопасного масштабирования управления при любой полосе пропускания в любой точке сети. Он не только обеспечивает форвардинг со скоростью линии и беспрецедентный обзор сети, но также поддерживает следующие функции.

- Фильтрация пакетов
- Выборка и регистрация пакетов
- Подсчет пакетов
- Распределение нагрузки

Технология Интернет-процессоров

В ИП Internet Processor впервые была реализована линейная скорость форвардинга. В процессоре второго поколения ИП Internet Processor II в дополнение к этому предлагается обширный набор функций, которые можно использовать как в ядре, так и на границе сети.

ИП Internet Processor

Впервые ИП Internet Processor был использован в магистральном маршрутизаторе M40™ в сентябре 1998г., обеспечив технологический прорыв, позволивший продвигать трафик со скоростью линии. Лабораторные и сетевые тесты, а также применение в Интернете показали, что даже пакеты минимальной длины (что соответствует наиболее напряженному режиму работы маршрутизатора) передаются со скоростью 40 млн. пакетов в секунду при объеме таблицы маршрутизации 80000 префиксов.

Кроме форвардинга со скоростью линии ИП поддерживает полномасштабную реализацию протокола маршрутизации, язык определения правил маршрутизации, имеет надежные характеристики в условиях повышенной нагрузки, гибкое регулирование трафика с использованием протокола MPLS, а также классы обслуживания (CoS).

ИП Internet Processor обеспечивает лучшую в своем классе функциональность магистрального ядра сети. Juniper Networks стала первой компанией, обеспечившей эти возможности, а маршрутизаторы серии M являются самыми производительными системами из представленных на рынке в настоящий момент.

ИП Internet Processor II

Опыт взаимодействия с крупнейшими поставщиками услуг при разработке и эксплуатации Интернет-процессора первого поколения был учтен при разработке расширенного и масштабируемого набора функций ИП Internet Processor II.

ИП Internet Processor II входит в стандартную конфигурацию магистральных маршрутизаторов M5™, M10™ и M160™ и является опциональным для маршрутизаторов M20™ и M40™. Централизованная архитектура серии M позволяет активировать функции Интернет-процессора на всех интерфейсах простой загрузкой программного обеспечения.

Производительность

Использование ИП Internet Processor II обеспечивает предсказуемую обработку пакетов маршрутизаторами серии M с высокими скоростями на всех интерфейсах.

ИП Internet Processor II входит в состав подсистемы форвардинга пакетов PFE, четко отделенную от подсистемы маршрутизации RE. Разделение функций форвардинга и маршрутизации гарантирует, что избыточная нагрузка одной подсистемы не повлияет на другую, так как у них нет совместно используемых ресурсов. Флуктуации маршрутизации и нестабильность сети не препятствуют форвардингу пакетов. Производительность форвардинга 40 млн. пакетов в секунду обеспечивает хорошую масштабируемость ИП Internet Processor II при больших и сложных таблицах форвардинга. Предсказуемая производительность при включении дополнительных функций обработки пакетов обеспечивается за счет схемотехнического решения с большим запасом по интерфейсам, а также предварительной обработкой фильтров в подсистеме маршрутизации после конфигурирования интерфейсов. Кроме того, подсистема форвардинга пакетов позволяет объединять свой пул ресурсов с ресурсами ИП, чтобы обеспечить дополнительный запас по производительности даже при включении дополнительных функций.

Благодаря запасу по ресурсам для реальных конфигураций маршрутизации и трафика (в терминах нагрузки интерфейса и распределения пакетов) маловероятно, что пакетная нагрузка сможет превысить пропускную способность ИП. Это особенно верно для младших маршрутизаторов - M5, M10 и M20, где относительный резерв ИП значительно больше. Эти маршрутизаторы лучше использовать на уровне доступа, там, где обычно реализуются услуги, и, следовательно, повышенная емкость обработки пакетов является конкурентным преимуществом.

Тестирование производительности

Разработка набора тестов для оценки основных характеристик форвардинга маршрутизатора является относительно простой задачей, так как необходимо учитывать только несколько переменных. Однако разработка набора значимых показателей производительности при включенной фильтрации существенно более сложна, так как число переменных резко возрастает.

- Число интерфейсов маршрутизатора, работающих с фильтрами пакетов
- Число входных и выходных фильтров, установленных на каждом интерфейсе
- Размер и сложность фильтров, использованных при тестировании
- Объем трафика, поступающего на каждый интерфейс
- Распределение длин пакетов для каждого интерфейса
- Суммарный объем трафика, входящего в систему в каждый момент времени
- Содержимое заголовков пакетов трафика

В отсутствие стандартных тестов производительности, наилучшим подходом для численной оценки характеристик фильтрации является тестирование платформы в экстремальных условиях. Например, используется полностью сконфигурированная система с полными таблицами маршрутизации Интернета и множеством уникальных и сложных фильтров.

Наши специалисты провели серию тестов производительности ИП Internet Processor II с использованием устройства Agilent RouterTester и маршрутизатора M160, полностью сконфигурированного с 32 интерфейсами OC-48c/STM-16. Таблица маршрутизации содержала свыше 90000 маршрутов со средней длиной префикса /22 (близко к среднему значению для трафика Интернета). На все интерфейсы подавался максимально возможный двунаправленный трафик, а установленные фильтры содержали значительное число условий.

Результаты показывают, что ИП Internet Processor II обеспечивает предсказуемо высокую производительность форвардинга при фильтрации пакетов для любого типа трафика и любого набора фильтров, аналогичных используемым в реальных сетях.

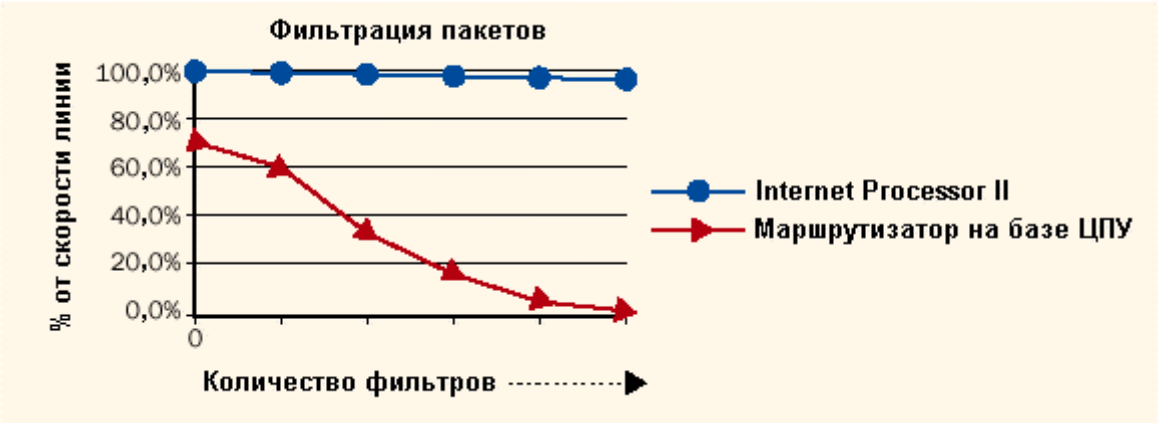

Рисунок 1. Сравнение ИП Internet Processor II и магистрального маршрутизатора на базе традиционного ЦПУ

Обработка пакетов

ИП Internet Processor II решает три прикладные задачи:

- Фильтрация пакетов
- Анализ трафика
- Распределение нагрузки

Фильтрация пакетов

Фильтрация пакетов - это способность избирательно управлять потоками пакетов, поступающих от интерфейсов или к интерфейсам на основе анализа заголовка каждого пакета. ИП Internet Processor II обеспечивает фильтрацию пакетов входящего и исходящего трафика с использованием любой комбинации следующих полей.

- IP-адреса источника и назначения
- IP-протокол (например, TCP, UDP и ICMP)
- Порты UDP и TCP источника и назначения
- Байт DiffServ
- Поля фрагментации и управления IP
- Биты управления TCP

Как работает фильтрация

Высокие характеристики фильтрации достигнуты за счет использования гибкого метода программирования ИП. Фильтры описываются и загружаются в ИП Internet Processor II посредством командного интерфейса ОС JUNOS. Затем компилятор оптимизирует и компилирует фильтры для быстрой и эффективной обработки пакетов в ИП.

Когда пакет удовлетворяет заданному пользователем правилу фильтрации, маршрутизатор выполняет одно из следующих действий:

- Принимает пакет.
- Отбрасывает пакет без отправки сообщения ICMP.
- Отбрасывает пакет и отправляет сообщение ICMP.

Дополнительно можно настроить маршрутизатор на выполнение одного из следующих процессов:

- Выборка пакета
- Увеличение счетчика
- Регистрация пакета

Например: пакет может быть принят и выбран; отброшен, подсчитан и зарегистрирован; отброшен и зарегистрирован.

Примеры фильтрации

Фильтрация полезна во многих случаях, включая защиту ядра и абонентских сетей.

Защита ядра

Фильтры пакетов, реализованные на ИП, можно использовать для защиты ядра сети от нежелательного трафика, фальшивых адресов источника и других видов несанкционированного доступа.

Для защиты маршрутизаторов ядра традиционно используются два уровня безопасности. Первой линией обороны являются правила управления удаленным доступом к маршрутизатору, представляющие собой в основном список IP-адресов. Управляющий доступ к маршрутизатору (например, с использованием Telnet или SNMP) требует разрешенного IP-адреса источника. После проверки IP-адреса источника в действие вступает второй уровень защиты – пароли и одноразовые пароли.

ИП Internet Processor II добавляет третий уровень безопасности для защиты от атак на ядро. Применение фильтров, проверяющих адреса источника в точках входа в сеть, гарантирует, что хакеры не смогут подменить исходный адрес систем операционного центра сети на входной границе сети.

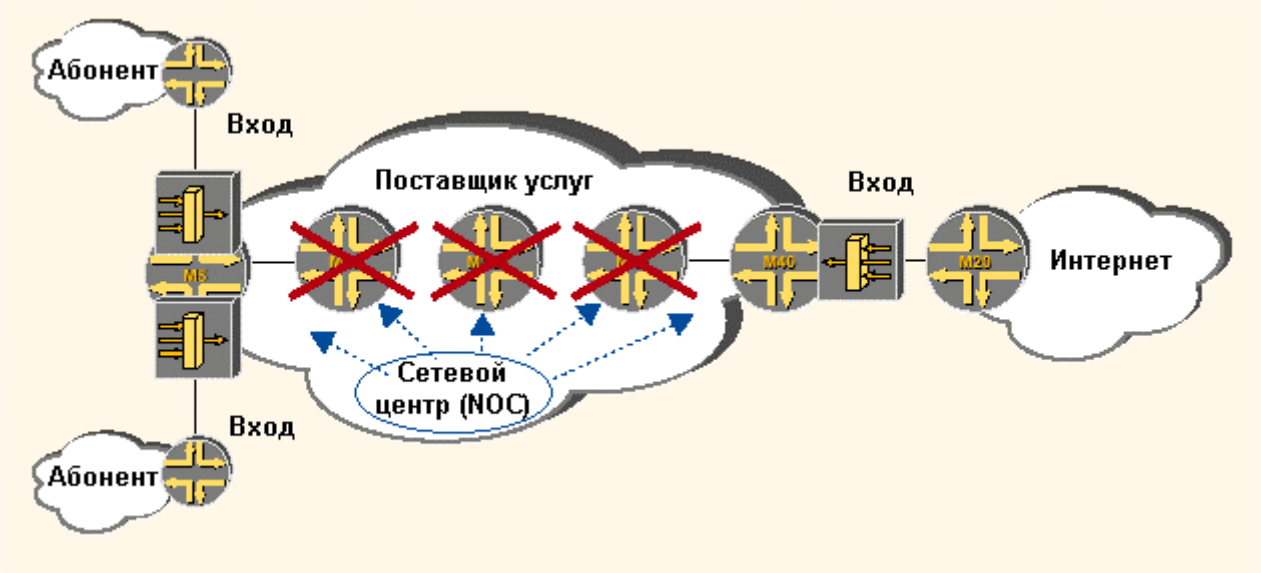

Рисунок 2. Защита сетевого ядра

Проверка адреса источника может также сыграть важную роль в предотвращении атак типа "отказ в обслуживании" (denial-of-service, DoS). Многие хакеры пытаются скрыть свою идентификационную информацию, используя фальшивый IP-адрес источника. Для обратной трассировки атак DoS вплоть до их источника можно использовать функции фильтрации, выборки и регистрации пакетов, при этом не будет негативного влияния на производительность форвардинга в ядре сети.

Эти надежные фильтры функционируют постоянно, проверяя, и если необходимо отбрасывая пакеты до пропуска их в сеть. До настоящего времени, используя традиционные фильтры, было невозможно реализовать этот тип защиты сети, так как производительность форвардинга обычных маршрутизаторов, использующих программные фильтры, ухудшалась до недопустимого уровня.

Дополнительные преимущества использования фильтров на основе ИП:

- Фильтры на основе ИП обеспечивают дополнительный уровень безопасности для защиты маршрутизаторов от несанкционированного доступа.
- Постоянная работа фильтров не влияет на производительность форвардинга.

Защита абонентских сетей

Исторически сложилось так, что фильтрация пакетов в основном была возложена на абонента. На абонентских маршрутизаторах фильтры настраивались на проверку трафика, приходящего со стороны поставщика услуг по каналу "абонент-провайдер". Администраторы сети абонента были сильно загружены задачами по разработке и управлению фильтрами трафика.

С увеличением числа абонентов, перешедших на широкополосные каналы, существующие клиентские платформы оказались неспособны обеспечить предсказуемую и стабильную производительность при включенных фильтрах. Технологически более привлекательно либо управлять фильтрацией на стороне поставщика услуг, либо развернуть оборудование, обеспечивающее на клиентской стороне полную производительность для широкополосных абонентов.

Фильтрация на основе ИП Internet Processor II позволяет защитить абонентские сети за счет использования внешних фильтров, сконфигурированных в маршрутизаторах на стороне поставщика услуг. Например, можно настроить внешние фильтры на прием, игнорирование или сброс пакетов на выходном интерфейсе в сторону абонента.

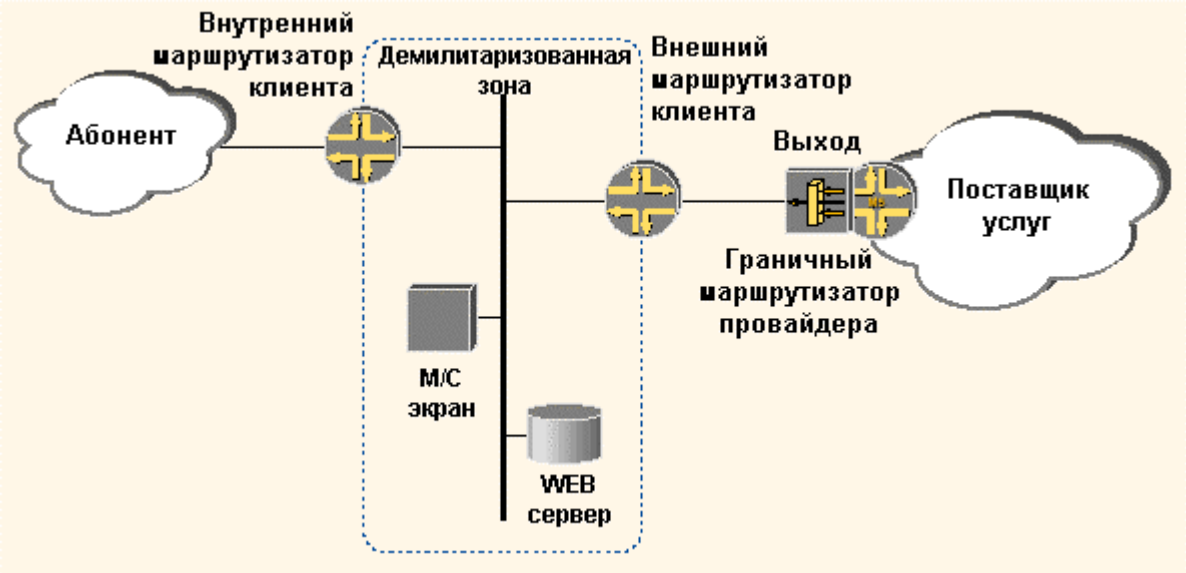

Рисунок 3. Внешняя фильтрация пакетов

Внешние фильтры, реализованные на базе ИП Internet Processor II, имеют пять преимуществ, отличающих их от традиционных фильтров.

- Сохраняется полоса пропускания канала "провайдер-абонент". Трафик может быть профильтрован выходными фильтрами, до того как покинет сеть, и нежелательный трафик будет удален.
- Абоненту не приходится иметь дело с непростыми процессами разработки и управления фильтрами.
- Не ухудшается производительность форвардинга граничного маршрутизатора.
- В ОС JUNOS поддерживаются структурированные инструменты конфигурирования, подобные используемым в базах данных, что существенно облегчает работу по управлению конфигурированием фильтрации абонента в граничных маршрутизаторах.
- Внешние услуги фильтрации пакетов можно предлагать абонентам в качестве дополнительных услуг.

Анализ трафика

В условиях постоянного роста сетей и расширения полосы пропускания появляется потребность в масштабируемых средствах выборки и анализа данных, необходимых для обзора сетевых операций. Это становится возможным при совместном использовании инструментов анализа трафика и фильтров пакетов. Фильтр идентифицирует пакеты, подлежащие анализу, а средства анализа выбирают, регистрируют и подсчитывают отобранные пакеты.

Инструменты анализа трафика позволяют изучать трафик, а также планировать и проектировать сеть.

- Изучение структуры сетевого трафика. Можно охарактеризовать трафик некоторым числом измерений, включая распределение длин пакетов, транспортные протоколы, популярные приложения (такие как Web, речь, видео), туннелируемые протоколы, многоадресная IP рассылка.
- Планирование пропускной способности, сетевое проектирование, развертывания внутренних (внутридоменных) и внешних (междоменных) соединений, определение необходимости установления новых уровней пиринга.
- Определение требований к оборудованию путем анализа сетевых характеристик с целью определения необходимых скоростей форвардинга для преобладающих пакетов определенного размера.
- Разработка профилей, определяющих работу сети в нормальном режиме и разработка плана мероприятий при эксплуатации сети за определенными пределами.

Выборка и регистрация пакетов

Выборка и регистрация пакетов позволяют маршрутизатору анализировать проходящие через систему пакеты.

Одной из проблем при выборке пакетов является несовместимость выборки с основной функцией системы, каковой является максимально быстрая обработка максимального числа пакетов. Основным преимуществом маршрутизаторов серии M является то, что центральный процессор непосредственно не участвует в обработке транзитного трафика. В результате, он мало загружен и используется для хранения заголовков пакетов и оперативного анализа.

Как работает выборка и регистрация

В маршрутизаторах серии M используется статистическая выборка, которая применяется к задаваемому пользователем проценту трафика, проходящего по системе. Из теории дискретизации известно, что статистическая выборка может быть достаточно точной при правильном выборе параметров дискретизации.

Когда пакет удовлетворяет условиям фильтрации, маршрутизатор помечает его как кандидата на выборку, устанавливая бит в описании пакета. Обычно маршрутизатор устанавливает бит выборки, если пакет удовлетворяет фильтру. Однако установка бита выборки еще не означает, что выбрано описание пакета, это означает только, что некоторое описание пакета является кандидатом для выборки.

Фильтр пакетов на сконфигурированном интерфейсе устанавливает бит выборки во всех выбранных пакетах. Для каждого пакета с установленным битом выборки ИП Internet Processor II генерирует случайное число. Если случайное число меньше заданного пользователем порогового значения, пакет выбирается. Если пакет выбран, маршрутизатор может выбирать следующее заданное пользователем число пакетов, не используя генератор случайных чисел.

Когда пакет выбран, маршрутизатор записывает заголовки пакета в файл на жестком диске подсистемы маршрутизации. В файле содержится следующая информация:

- IP адреса источника и назначения
- IP протокол
- Порт источника и назначения
- Длина пакета
- Байт DiffServ
- Флаги фрагментации IP
- Флаги TCP

Регистрация подобна выборке. Однако регистрацию можно использовать для мгновенного уведомления о происходящих в сети событиях. При регистрации рассматривается каждый пакет, удовлетворяющий фильтру, и совпадения отображаются в реальном времени на консоли. Маршрутизатор не записывает данные регистрации на жесткий диск, их просмотр возможен только с помощью командной строки.

Пример выборки

Комбинируя выборку и фильтрацию можно проводить стратегический анализ трафика. Пример анализа включает определение необходимости добавления прямого канала пиринга для улучшения эффективности и времени отклика и определение того, какой объем трафика от источника с некоторым адресом достигнет точки хостинга.

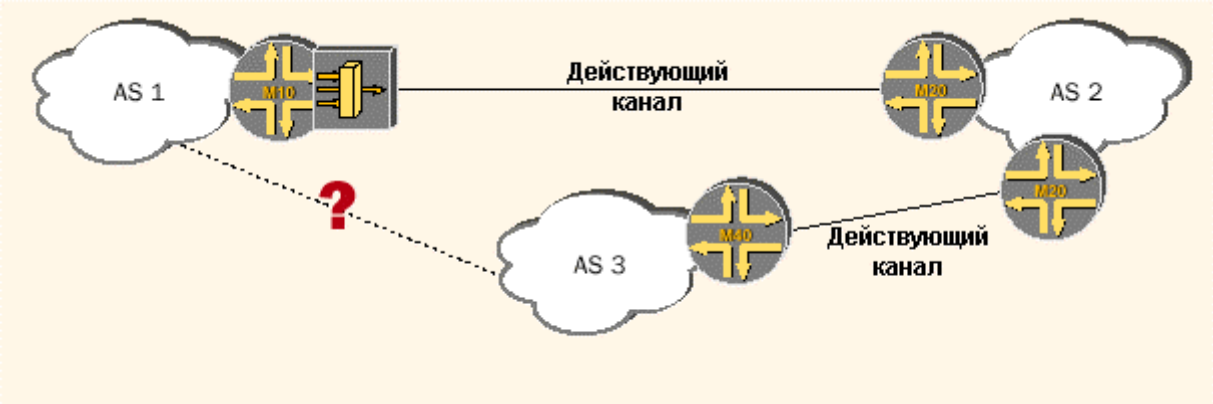

Рисунок 4. Выборка и регистрация пакетов. Поставщик услуг AS1 может использовать выборку для анализа трафика, который он отправляет на AS3 через AS2. Если объем трафика слишком велик для AS3, может оказаться оправданным прямой канал пиринга с AS3.

Подсчет пакетов

Подсчет пакетов выполняется в реальном времени с наивысшим приоритетом. Пакеты подсчитываются с 100-процентной точностью, даже когда они поступают по интерфейсам OC-48c/STM-16 или OC-192c/STM-64. Даже при таких скоростях фильтры и счетчики могут собирать информацию, необходимую для эффективной эксплуатации, обслуживания и планирования сети.

Как работает подсчет

Счетчики ИП Internet Processor II работают со скоростью линии и полностью независимы от центрального процессора. Они могут постоянно отслеживать трафик определенного типа или же включаться для отслеживания состояния сети.

Пример подсчета

Можно настроить фильтры в точном соответствии со структурой трафика, тогда подсчет различных пакетов обеспечит определение типов пакетов, проходящих по системе. Например, можно задать фильтр, подсчитывающий все пакеты, происходящие из некоторого диапазона префиксов адресов, входящих в сеть по каналу пиринга.

Распределение нагрузки

На маршрутизаторе с параллельными соединениями, пакеты равномерно распределяются по каналам. ИП Internet Processor II позволяет направлять потоки таким образом, что пакеты, содержащие определенную пару "источник-получатель" или "порт-адрес" всегда выходят из одного и того же физического интерфейса. Другими словами, все пакеты заданного потока всегда передаются по одному и тому же каналу.

Распределение нагрузки имеет два основных преимущества:

- Обеспечивается дополнительная полоса пропускания при параллельных каналах или маршрутах равной стоимости.
- Сохраняется порядок пакетов, чем достигается максимальная эффективность пользовательской сессии TCP.

Сохранение порядка следования пакетов гарантирует, что сессия TCP, поддерживающая быструю повторную передачу и быстрое восстановление не будет замедляться из-за нарушения порядка следования пакетов.

Как работает распределение нагрузки

ИП Internet Processor II обрабатывает информацию, содержащуюся в заголовке пакета, и присваивает каждому пакету некое значение хеширующей функции. Эта обработка гарантирует, что весь трафик с одинаковым значением этой функции будет передан через один и тот же интерфейс, и что сохранится порядок следования пакетов в потоке TCP.

Пример распределения нагрузки

Распределение нагрузки особенно полезно при двух топологиях.

- Распределение нагрузки можно использовать при параллельных соединениях точка-точка в направлении к получателю. При такой топологии распределение нагрузки особенно эффективно, когда не оправдан переход на новый иерархический уровень полосы пропускания.
- Можно использовать распределение нагрузки между тремя маршрутами равной стоимости. Применение распределения нагрузки позволяет системе выбирать из некоторого числа маршрутов равной стоимости и выбрать один и тот же маршрут для трафика, принадлежащего одной сессии TCP.

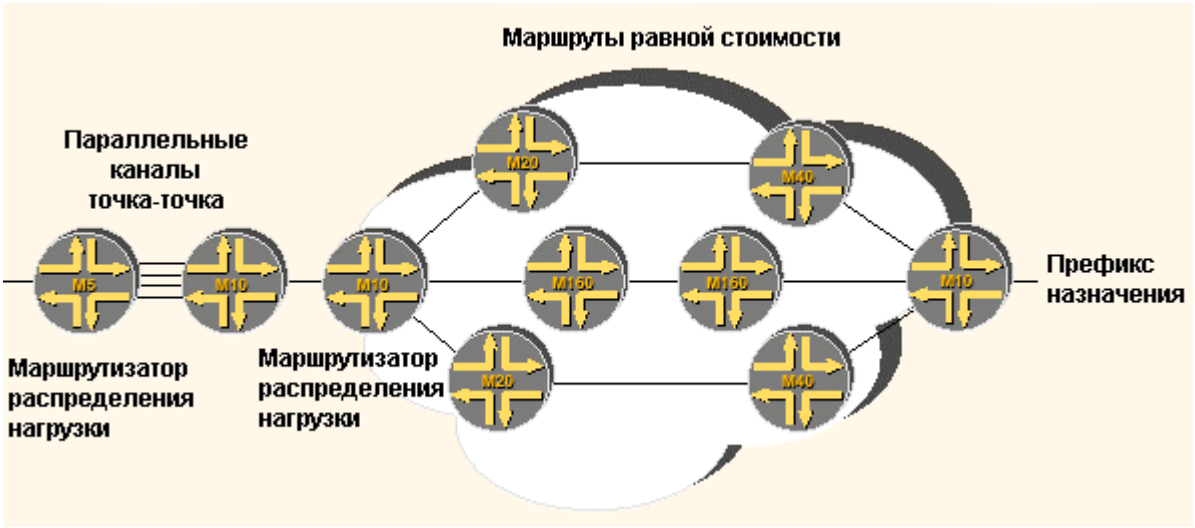

Рисунок 5. Распределение нагрузки

###

Poplar systems

http://www.poplar.ru