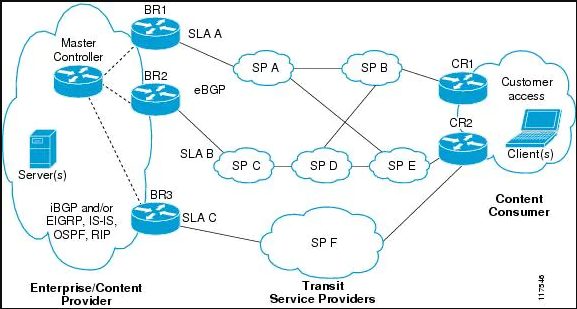
**OER/**[**PFR**](http://www.anticisco.ru/blogs/2011/05/%d0%b2%d0%b2%d0%b5%d0%b4%d0%b5%d0%bd%d0%b8%d0%b5-%d0%b2-cisco-oerpfr/)

**OER (Optimized Edge Routing)** — это технология, разработанная для того, чтобы решить проблемы с производительностью на границе сети, не решаемые традиционными способами. Как мы все знаем, в традиционной IP-маршрутизации трафик отправляется согласно записям в таблице маршрутизации. Записи эти туда попадают практически вне зависимости от текущего состояния (загрузки, латентности, потерь) сети. Иными словами, традиционная маршрутизация не в состоянии учитывать текущее состояние сети с точки зрения производительности.

Чтобы это побороть и была придумана технология Optimized Edge Routing или ее новое название — **Performance Routing (PfR)**. Для этого в PFR выделяются классы трафика (например, приложения или подсети). Производительность (комплексное понятие, может включать в себя задержку, пропускную способность, потери и т.п.) каждого класса периодически измеряется и сравнивается с установленными правилами (политиками). По результатам этих сравнений PFR выбирает лучший выход из сети или гейт для данного класса трафика.



PFR мониторит и управляет исходящим трафиком на **border routers (BRs)**. В Cisco IOS версиях 12.4(9)T, 12.2(33)SRB и более поздних, появилась возможность мониторить и управлять входящим трафиком.

PFR измеряет время отклика и доступность пути с внешних интерфейсов BR1, BR2 и BR3. Изменения в производительности выходного линка на BR определяются попрефиксно. Если производительность падает ниже дефолтной или пользовательской политики маршрутизация «исправляется» для повышения производительности. Например, в случае перегрузки внешнего интерфейса BR2, обычная маршрутизация не в состоянии ничего сделать, а PFR может определить проблемное состояние и переправить трафик через другой выход.

**Пять этапов**

**1 Profile Phase**

Выбираем какой именно трафик мы будем оптимизировать с точки зрения производительности, поскольку в RIB может быть много всяких маршрутов. Выбор производится с помощью комбинации следующих способов:

* С помощью определения (learning) потоков трафика, протекающих через устройство и выбирая потоки с наименьшей задержкой или с наивысшей пропускной способностью.
* В дополнение к определению или вместо него, можно сконфигрировать класс трафика руками.

**2 Measure Phase**

Определившись с классами трафика, нужно определить метрики, показывающие производительность для каждого из этих классов. Для этого есть два механизма: активный мониторинг и пассивный мониторинг, их можно использовать и оба сразу. Мониторинг, в терминологии Сиско — периодическое измерение.

* Пассивный мониторинг — измерение метрик производительности потока трафика во время его прохождения через устройство.
* Активный мониторинг фактически состоит в генерации искусственного трафика для эмуляции активности данного класса.

Можно использовать и оба типа мониторинга сразу. Пассивный может обнаруживать выход производительности класса трафика из допустимых границ, а активный — для поиска альтернативного пути, если таковой имеется.

**3 Apply Policy Phase**

После сбора метрик производительности для данного класса, PFR сравнивает эти результаты с набором граничных значений для каждой метрики. Если какая-то метрика, а значит и политика, выходит за граничные значения — происходит событие **Out-of-Policy (OOP)**. Данные сравниваются двумя способами: либо как отклонение от среднего, либо как выход за границу. Возможно и то, и другое сразу

В PFR существует два вида политик:

* Политики классов трафика (traffic class policies) — создаются для префиксов или для приложений.
* Политики линков (link policies) — создаются для выходов за границу сети.

Оба типа политик определяют критерии для генерации события OOP. Политики применяются глобально (для всех классов трафика) или локально (только для некоторых классов).

В случае множества политик, метрик производительности, способов назначения этих политик классам, существует механизм разрешения конфликтов между политиками. Это делается с помощью механизма приоритетов.

**4 Control Phase**

Этой фазе PFR (еще ее называют «фаза усиления» (enforce phase), трафик контролируется для увеличения производительности. Способ этого контроля зависит от способа задания класса трафика.

* Если класс трафика задан только с использованием префикса — будет скорректирована информация о достижимости префикса (добавление/удаление статики, изменение метрик).
* Если класс трафика задан приложением, т.е. префиксом и дополнительными условиями, PFR уже не сможет использовать обычный протокол маршрутизации и здесь уже на помощь придет PBR (policy based routing).

**5 Verify Phase**

В этой фазе, если класс трафика вышел за границы, предусмотренные политикой (OOP), PFR начинает вмешиваться с целью повлиять на трафик этого класса. Например, с помощью уже упомянутых статических маршрутов или маршрутов BGP. После вмешательства PFR удостоверяется, что оптимизируемый трафик использует тот гейтвей, который нужен. Если после этого трафику лучше не стало, то PFR отменит изменения и повторит перечисленные фазы сначала.

**Элементы сети PfR**

**PFR Master Controller** — маршрутизатор, координирующий работу PFR по всей сети. Может выполнять только эту функцию, может так же быть пограничным роутером (BR). Master наблюдает за исходящим трафиком с помощью пассивного или активного мониторинга и применяет к этим потокам имеющиеся политики для оптимизации маршрутизации, являсь по сути централизованным центром управления для всех пограничных роутеров.

**PFR Border Router** — роутер одним или несколькими линками к провайдерам. Именно на нем (или на них, если их несколько) все изменения, принятые **Master Controller**, внедряются в жизнь. BR тоже участвует в мониторинге, сообщая данные MC. И наконец, BR может быть одновременно и MC.

**PFR-Managed Network Interfaces** — то, чем управляет PFR. Сеть под управлением PFR должна иметь как минимум два исходящих (external) интерфейса для трафика, текущего наружу. Иначе просто оптимизировать нечего!. На каждом BR так же должен быть хотя бы один интерфейс, достижимый из внутренней сети, чтобы его можно было пометить как «internal» для пассивного мониторинга. И есть еще локальный интерфейс (local) для взаимодействия между MC и BR.

**Мониторинг:**

**Passive monitoring**: is based on Netflow. BR(S) reports to the MC the average delay of the flows. Packet loss, reachability along with outbound throughput for each identified TC by Netflow is reported. Measurement of non-TCP traffic flows in this mode is characterized by throughput only while TCP flows are measured on Delay, Loss, Reachability and throughput. This mode is useful for TCP based flows only and TCP flows must be observed by the BRs to manage prefixes.

**Active monitoring:** Active monitoring use IP SLA feature in order to generate test traffic for the specific TC and measure performance based on delay, reachability, Jitter, MOS for any type of flows and not just TCP as with passive monitoring. Only the current exit path is used to generate IP SLA until it becomes OOP (out Policy).

**Monitor Both:** Use both passive and active mode and send IP SLA out the current exit point only.

**Fast monitoring:** Send IP SLA out all the exit points and alternate paths are always known allowing immediate use as required. This mode can reroute OOP traffic in less than 3 seconds.