Тема 2.2. Обеспечение информационной безопасности на сетевом уровне

Лекция 3. Обеспечение качества обслуживания

Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

Доцент: Кирьянов Александр Владимирович
email:kiryanov_a@mirea.ru

Учебные вопросы:

1. Назначение, основные возможности технологии обеспечения качества обслуживания в ИВС.
2. Процесс обеспечения качества обслуживания в IP сетях.
3. Настройка качества обслуживания (Qos)

Нормативно-правовая база

RFC-1633 "Integrated Services in the Internet Architecture: An Overview" Braden R., Clark D., Shenker S., June 1994

RFC-2474 "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", K. Nichols, December 1998.

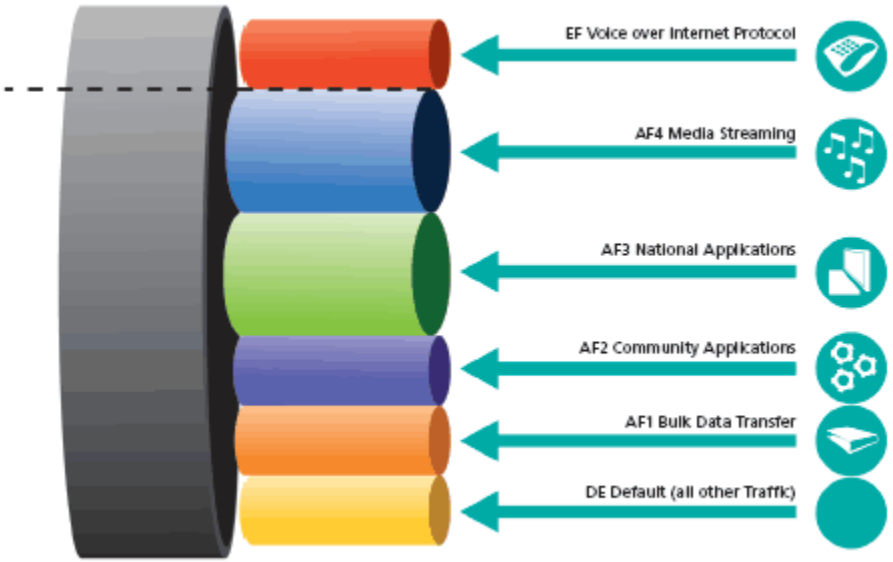
RFC-3387 "Considerations from the Service Management Research Group (SMRG) on Quality of Service (QoS) in the IP Network", M. Eder, H. Chaskar, S. Nag, September 2002

RFC-2212, "Specification of Guaranteed Quality of Service".

RFC-3644, "Policy Quality of Service (QoS) Information Model", Y. Snir, Y. Ramberg, J. Strassner, R. Cohen, B. Moore, November 2003

Рекомендация МСЭ Y.1541

1.Назначение,основные возможности технологии обеспечения качества обслуживания в ИВС



Организации, стандартизирующие модели обеспечения качества обслуживания

- **ITU-T:** International Telecommunication Union – Международный Союз Электросвязи
- **ETSI:** European Telecommunications Standardizations Institute - Европейский институт по стандартизации телекоммуникаций
- **IETF:** Internet Engineering Task Force – Инженерная группа по решению задач Internet
- **MMCF:** Multimedia Communications Forum - Форум по мультимедийным коммуникациям
- **EURESCOM:** European Institute for Research and Strategic Studies in Telecommunications - Европейский институт по исследованиям и стратегическому планированию в телекоммуникациях

Анализ стандартизированных моделей QoS

Разработчик модели QoS	QoS из конца в конец	Классы QoS	Биллинг	Мониторинг и управление	Особенности предоставляемых услуг
ITU-T	Да	Да	Нет	Да	Да
ETSI	Да	Да	Нет	Да	Да
IETF	Да	Нет	Нет	Да	Нет
MMCF	Да	Да	Нет	Да	Да
EURESCOM	Да	Нет	Нет	Да	Нет

Характеристики QoS (Y.1540)

- Задержки и джиттер* задержки
- Величина потерь
- Производительность сети
- Надежность сетевых элементов

G.1000 – определяет структуру связей между рабочими характеристиками QoS.

*** джиттер задержки – отклонение значений задержки от заданной величины**

Качество обслуживания понимается как совокупность механизмов, позволяющих сетевым администраторам управлять полосой пропускания, задержкой, вариацией задержки и вероятностью потери пакетов в сети.

Механизм QoS не является характеристикой одного устройства, а представляет собой сквозную системную структуру. Возможности QoS протокола IP позволяют провайдерам задавать приоритеты классам службы, выделять полосу пропускания и избегать заторов в сети.

Классификация трафика мультисервисной IP-сети по приложениям

Тип трафика	Приложения	Требования	Протоколы транспорт-ного уровня
Реаль-ного времени	IP-телефония и видеоконференцсвязь	–Чувствительность к задержке –Чувствительность к джиттеру задержки –Малая чувствительность к потерям	RSVP, RTP, RTCP,UDP
	Процессы управления, игры on-line	–Чувствительность к задержке –Чувствительность к джиттеру задержки –Чувствительность к потерям	UDP, TCP
Потоко-вый	Аудио по требованию Видео по требованию Интернет-вещание	–Малая чувствительность к задержке –Чувствительность к джиттеру задержки –Чувствительность к потерям	RSVP, SCTP, UDP,TCP
Эластич-ный	Конференция документов	–Малая чувствительность к задержке –Малая чувствительность к джиттеру задержки –Высокая чувствительность к потерям	TCP
	Анимация Передача файлов E-mail	–Очень малая чувствительность к задержке –Малая чувствительность к джиттеру задержки –Высокая чувствительность к потерям	

Типы приложений

- Приспособляющиеся (elastic)
  - широкий диапазон рабочих скоростей обмена данными, хотя, конечно, чем больше тем лучше
  - Пример: FTP, torrent, HTTP, email
- Потоковые приложения
  - ширина канала может варьироваться в допустимых пределах
  - могут адаптироваться к небольшим скоростям / небольшим потерям пакетов / долгому отклику, например, меняя качество передаваемого видео сигнала
- Приложения реального времени
  - Не могут приспособиться к небольшой ширине канала / потерям пакетов / долгому отклику
  - Пример: IP-телефония, сетевые многопользовательские игры, приложения для управления чем-либо в реальном времени

Quality of Service (качество сервиса) - вероятность того, что сеть связи соответствует заданному соглашению о трафике.

Под качеством сервиса следует понимать обеспечение предсказуемости процесса передачи трафика, то есть способность сетевых компонентов гарантировать доставку трафика адресату с требуемыми параметрами.

Меры обеспечения QoS, применяемые в IP- сетях:

1. Резервирование ресурсов.
2. Приоритезация трафика.
3. Перемаршрутизация.

Используемые протоколы: RSVP, DiffServ, MPLS.

Алгоритмы управления очередями: Class Based Queuing (CBQ), Random Early Drops (RED), Weighted Fair Queuing (WFQ).

Уровни обслуживания QoS:

- Установление уровня приоритетности.
  Отдельные пакеты обслуживаются по-разному, в зависимости от класса обслуживания, который им приписывается.

- Резервирование ресурсов.
  Соединению выделяется определенная часть полосы пропускания, которая согласовывается с потребностями маршрутизаторов и коммутаторов на всем пути следования.

Базовые показатели, характеризующие QoS:

- полоса пропускания;
- задержка при передаче пакета;
- колебания задержки при передаче пакетов;
- потеря пакетов.

Поддерживаемые уровни обслуживания:

- **Expediting Forwarding (EF).**
  Уменьшает задержку и пульсацию. Пакеты теряются, если трафик превышает максимальную нагрузку, установленную локальной политикой.
- **Assured Forwarding (AF).**
  Если нагрузка на трафик превышает уровень, установленный локальной политикой, избыточные AF-пакеты не доставляются в порядке очереди, предписанном их уровнем приоритета, а переводятся на более низкий уровень (но не теряются).

Операции, для обеспечения QoS на уровне сетевого устройства:

- Классификация пакетов по заголовкам.
- Маркирование классифицированных пакетов.
- Организации очередей с учетом приоритетов.

Классы трафика:

- класс срочной пересылки пакетов;
- класс гарантированной пересылки пакетов.

Достоинства модели Diff-Serv:

- единое понимание того, как должен обрабатываться трафик определенного класса;
- позволяет разделить весь трафик на относительно небольшое число классов и не анализировать каждый информационный поток отдельно;
- нет необходимости в организации предварительного соединения и в резервировании ресурсов;
- не требуется высокая производительность сетевого оборудования.

Показатели качества обслуживания, учитываемые при передаче мультимедийного трафика, и механизмы их формирования

	Влияние сети	Влияние оконечного устройства
ЗАДЕРЖКИ	Задержка распространения	Алгоритм кодирования/декодирования
	Очереди в узлах	Механизм пакетизации
		Задержка джиттер-буфера
		Алгоритм нивелирования потерь
		Механизмы медленного старта и квитирования
Показатели QoS		
ПОТЕРИ	Перегрузки в узлах	Превышение допустимой задержки
	Ошибки в канале	

Классы QoS и соответствующие им приложения (Y.1541)

- ***Класс 0:*** Приложения реального времени, чувствительные к джиттеру, характеризуемые высоким уровнем интерактивности (VoIP, видеоконференции)
- ***Класс 1:*** Приложения реального времени, чувствительные к джиттеру, интерактивные (VoIP, видеоконференции)
- ***Класс 2:*** Транзакции данных, характеризуемые высоким уровнем интерактивности (например, сигнализация)
- ***Класс 3:*** Транзакции данных, интерактивные приложения
- ***Класс 4:*** Приложения, допускающие низкий уровень потерь (короткие транзакции, массивы данных, потоковое видео)
- ***Класс 5:*** Традиционные применения сетей IP

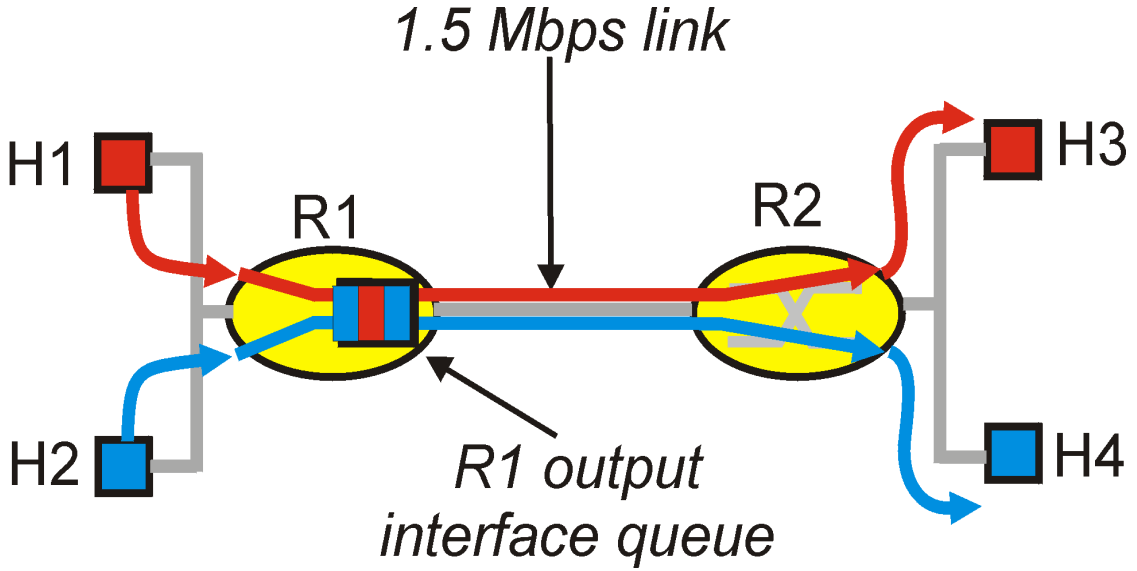
Нормы на параметры доставки пакетов IP с разделением по классам обслуживания, модель ITU-T

Сетевые характеристики	Классы QoS					
	0	1	2	3	4	5
Задержка доставки пакета IP, IPTD	100 мс	400 мс	100 мс	400 мс	1 с	Н
Вариация задержки пакета IP,IPDV	50 мс	50 мс	Н	Н	Н	Н
Коэффициент потери пакетов IP, IPLR	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	Н
Коэффициент ошибок пакетов IP, IPER	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	Н

Примечание. Н - не нормировано. Значения параметров представляют собой верхние границы для средних задержек, джиттера, потерь и ошибок пакетов.

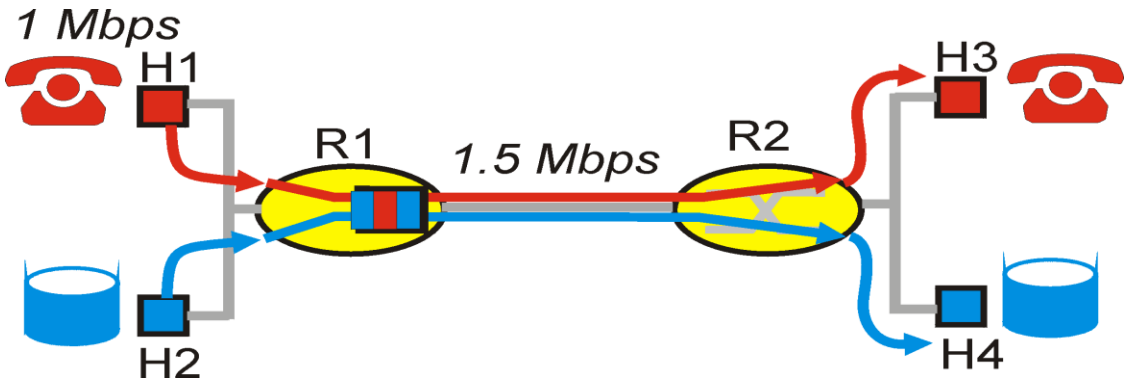
Контроль качества обслуживания (QoS)

- Передача данных происходит по принципу «best effort» - скорейшим способом согласно имеющимся возможностям
- IETF работает над стандартами, предоставляющими гарантии качества сетевого соединения
  - IntServ, RSVP
  - DiffServ
- Модель для анализа заторов при совместном использовании канала:



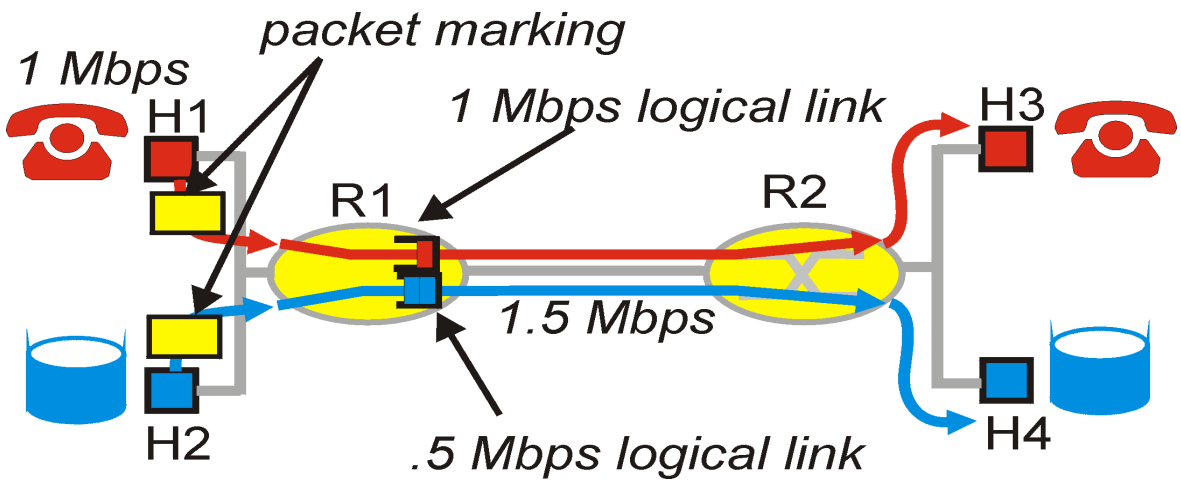
Принципы QoS

- Рассмотрим приложение IP-телефонии (1Mbps) и uTorrent, совместно использующих канал 1.5 Mbps
  - закачка файла может заставить маршрутизатор отбросить аудио-данные
  - нам хочется предоставить VoIP приоритет над uTorrent
- **ПРИНЦИП 1: Нужно ввести классы пакетов и научить маршрутизатор правильно обрабатывать классы данных**



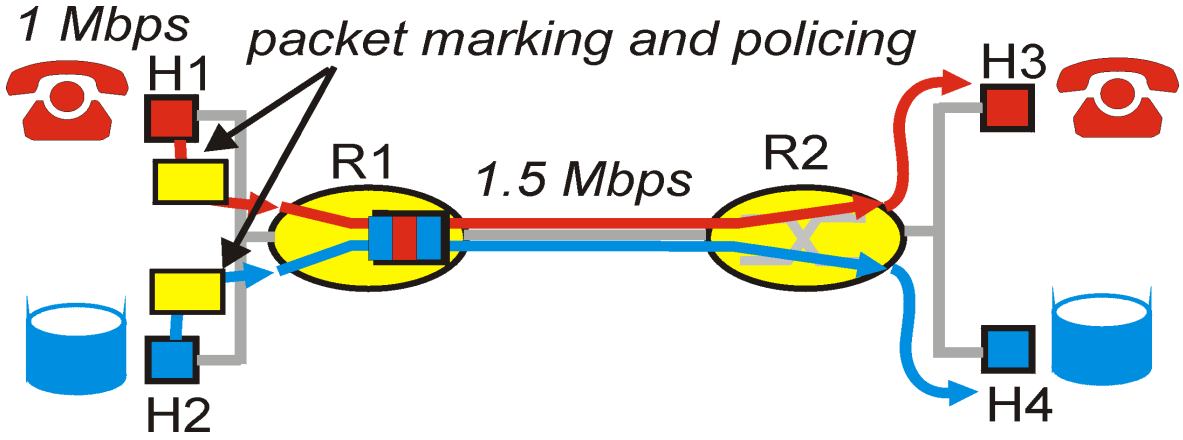
Принципы QoS

- Приоритетное VoIP-приложение может попытаться забрать под себя весь канал
- **ПРИНЦИП 2: Классы не должны теснить друг друга, уменьшая пропускную способность других классов ниже заданной**
- Простое решение – для каждого типа трафика зарезервировать постоянную часть канала – является неэффективным



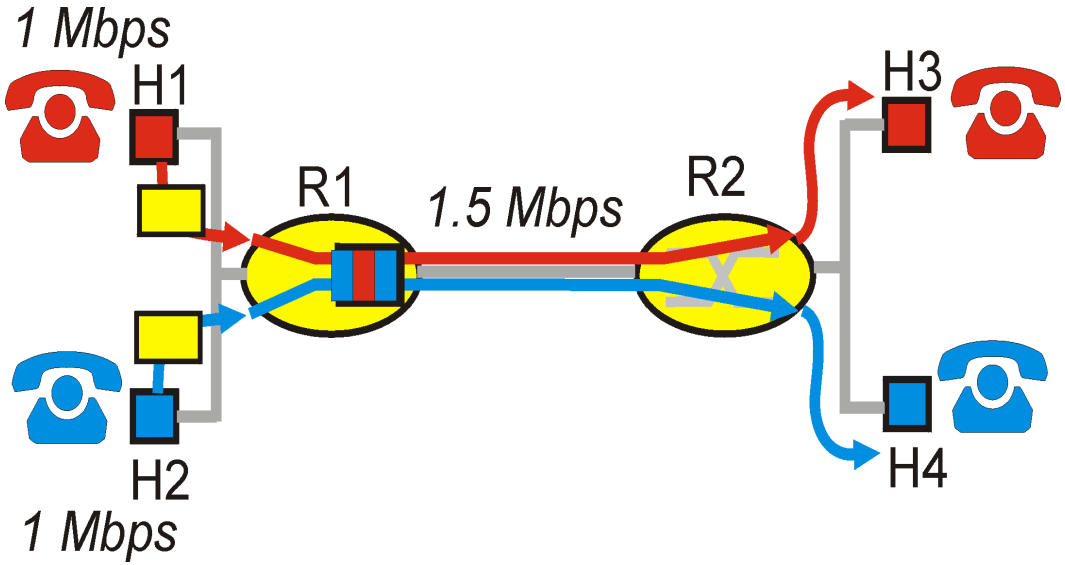
Принципы QoS

- **ПРИНЦИП 3: Обеспечивая изоляцию классов трафика, нужно позаботиться об эффективном использовании канала**
- Можно использовать честную очередь с весовыми коэффициентами (Weighted fair queuing, WFQ)

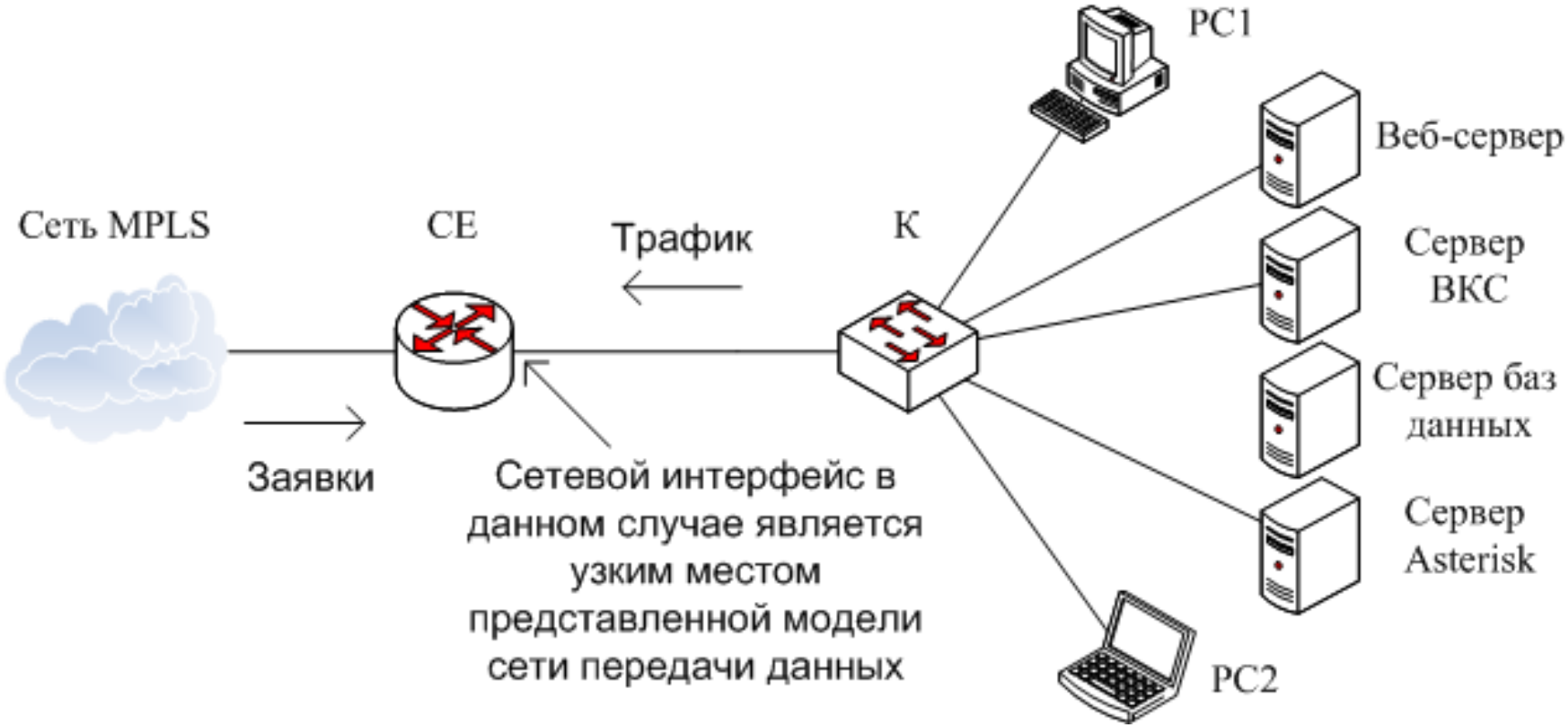


Принципы QoS

- Проблема: с учетом всех приоритетов ширина канала для данного типа трафика может оказаться недостаточной
- **ПРИНЦИП 4: Нужны механизмы проверки наличия необходимых ресурсов; приложение запрашивает сеть о наличии необходимой пропускной способности / надежности / времени отклика, сеть - отвечает**



Обобщенная модель существующих в настоящее время сетей передачи данных

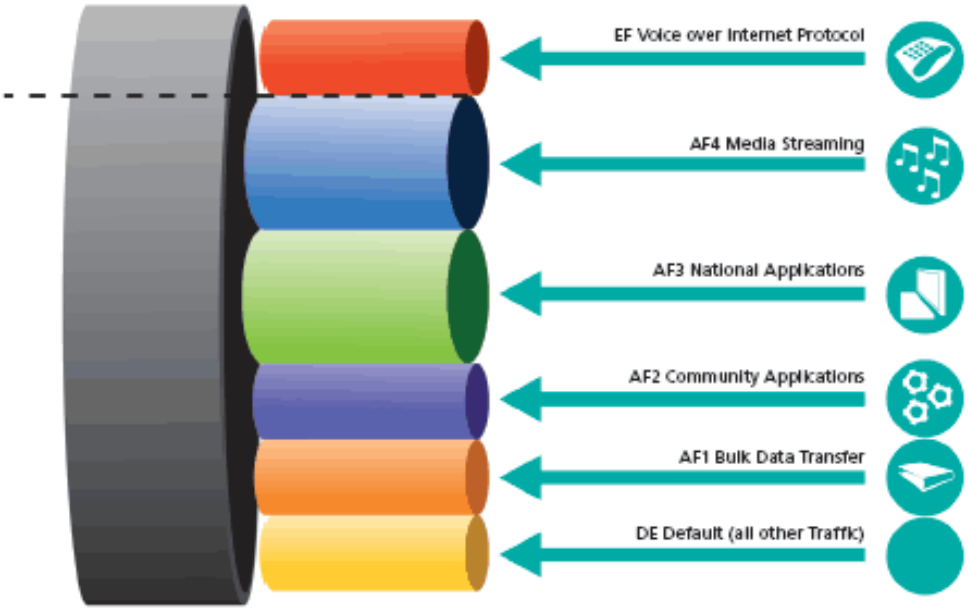


Выводы

Технология обеспечения качества обслуживания в IP сети должна поддерживать следующие элементы

1. Маркировка классов трафика
2. Изоляция классов
3. Эффективное использование канала
4. Проверка необходимых параметров соединения

2. Процесс обеспечения качества обслуживания в IP сетях



История контроля качества в Internet

- Исследования 80х – начала 90х годов основаны на коммутации каналов
- На основе этого были разработаны стандарты QoS в сетях ATM и IntServ.
  Особенности:
  - жесткий контроль качества соединения от одного узла до другого
  - разрабатывались для удовлетворения нужд потоковых приложений и приложений реального времени
- В последние годы популярность завоевали Differentiated services
  - DiffServ основаны на обработке не отдельных потоков, а агрегированных классов трафика

Модели обеспечения качества обслуживания в сетях IP

- **Модель предоставления интегрированных услуг (IntServ)**

  RFC-2205, 1994-1997 г.
- **Модель предоставления дифференцированных услуг (DiffServ)**

  RFC 2475, 1998 г.
- **MPLS (Multi-Protocol Label Switching)**

Интегрированные услуги IntServ

Разработана IETF, 1994-1997 г.

RFC 2205, RFC 2210, RFC 2211, RFC 2212

Цель: предоставление приложениям возможности запрашивать сквозные требования по ресурсам.

Недостатки: проблемы масштабирования.

Основной механизм: протокол резервирования ресурсов **RSVP,** в узлах используется WFQ.

IntServ

- Приложение вначале должно запросить сетевые ресурсы и сообщить параметры передаваемого трафика:
  - **R-spec** определяют класс обслуживания: 'best effort‘, обслуживание с контролируемой нагрузкой или гарантированное обслуживание
  - **T-spec** определяют параметры алгоритма текущего ведра для трафика (скорость отдачи *r* и размер очереди *b*).

Интегрированные услуги IntServ:

Позволяет организовать гибкое обслуживание разнотипного трафика, максимально учитывая потребности каждого приложения. Идеальна для обслуживания мультимедийного трафика.

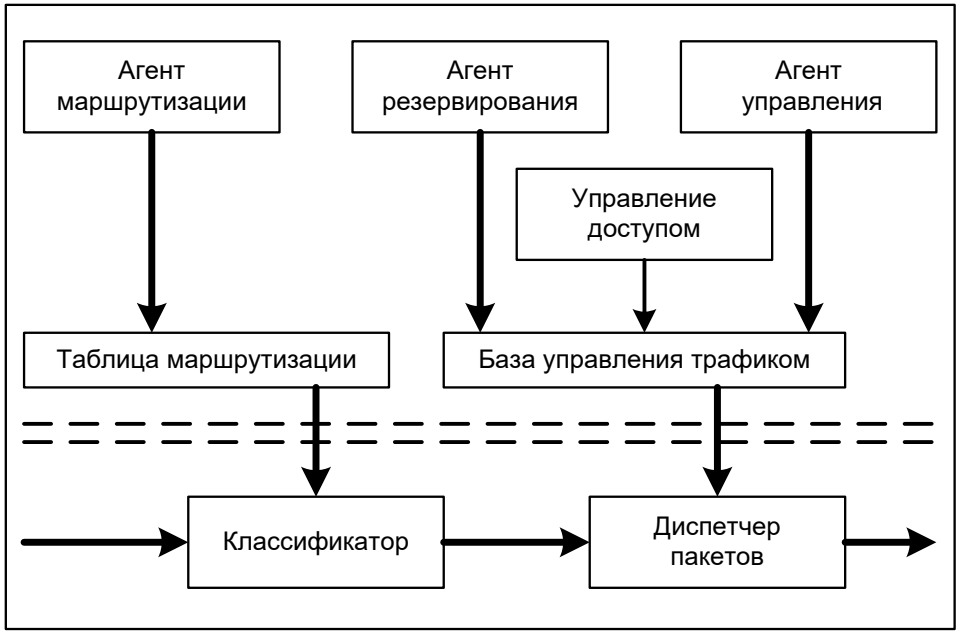


Рис. Модель IntServ

Основной недостаток: низкая масштабируемость.

IntServ:

Позволяет организовать гибкое обслуживание разнотипного трафика, максимально учитывая потребности каждого приложения. Идеальна для обслуживания мультимедийного трафика.

Обязательные элементы, для узлов поддерживающих IntServ:

- классификатор — направляет поступающий пакет в один из классов обслуживания согласно информации, полученной из заголовков пакета.
- диспетчер пакетов — извлекает из каждой очереди пакеты и направляет их на канальный уровень.
- блок управления доступом — принимает решения о возможности получения трафиком требуемого количества ресурсов.
- протокол резервирования ресурсов — информирует участников соединения о требуемых параметрах обслуживания.

RSVP – Resourse Reservation Protocol

- Протокол резервирования ресурсов. Позволяет посылать в сеть информацию о требованиях QoS для каждого потока. Работает совместно с IP.
- Резервирование проводится по адресу получателя. В случает отказа маршрута резервирование происходит заново.
- Работает с двумя видами сообщений:
  - PATH: запрос на резервирование. Содержит:
    - скорость передачи данных;
    - максимально допустимый размер пульсации трафика.
  - RESV: запрос резервирования. Содержит:
    - скорость передачи данных;
    - максимально допустимый размер пульсации трафика.
    - QoS

Протокол резервирования ресурсов RSVP

RSVP — протокол сигнализации, обеспечивающий резервирование ресурсов для предоставления в IP-сетях услуг эмуляции выделенных каналов.

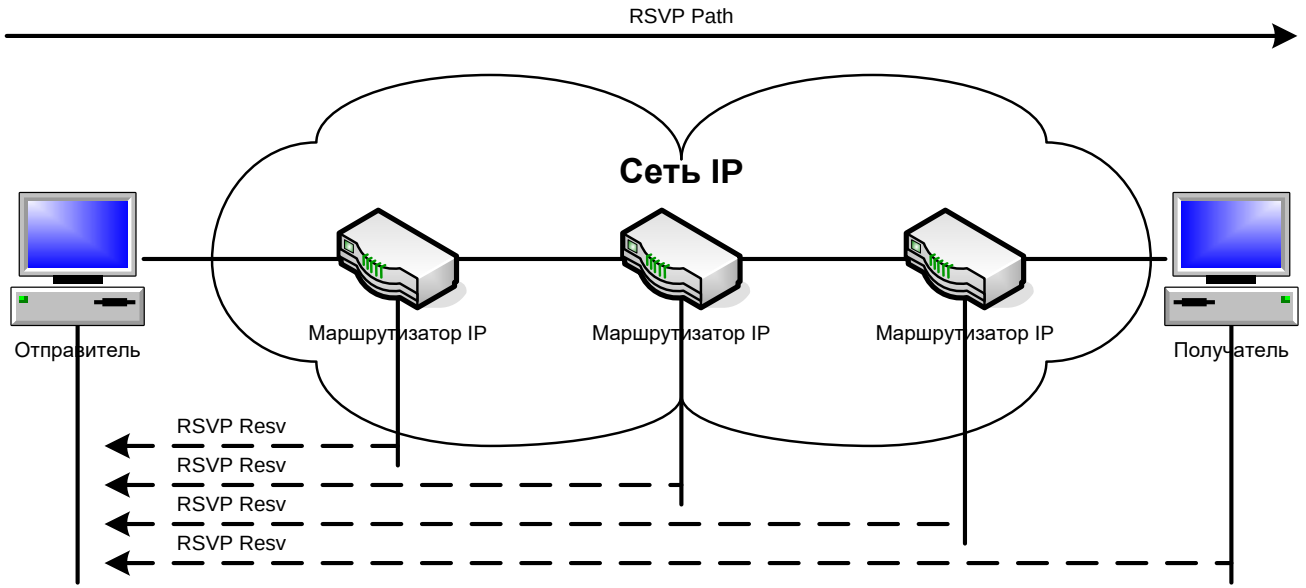


Рис. Применение протокола RSVP

Обеспечивает качество обслуживания каждому потоку.

Протокол резервирования ресурсов RSVP

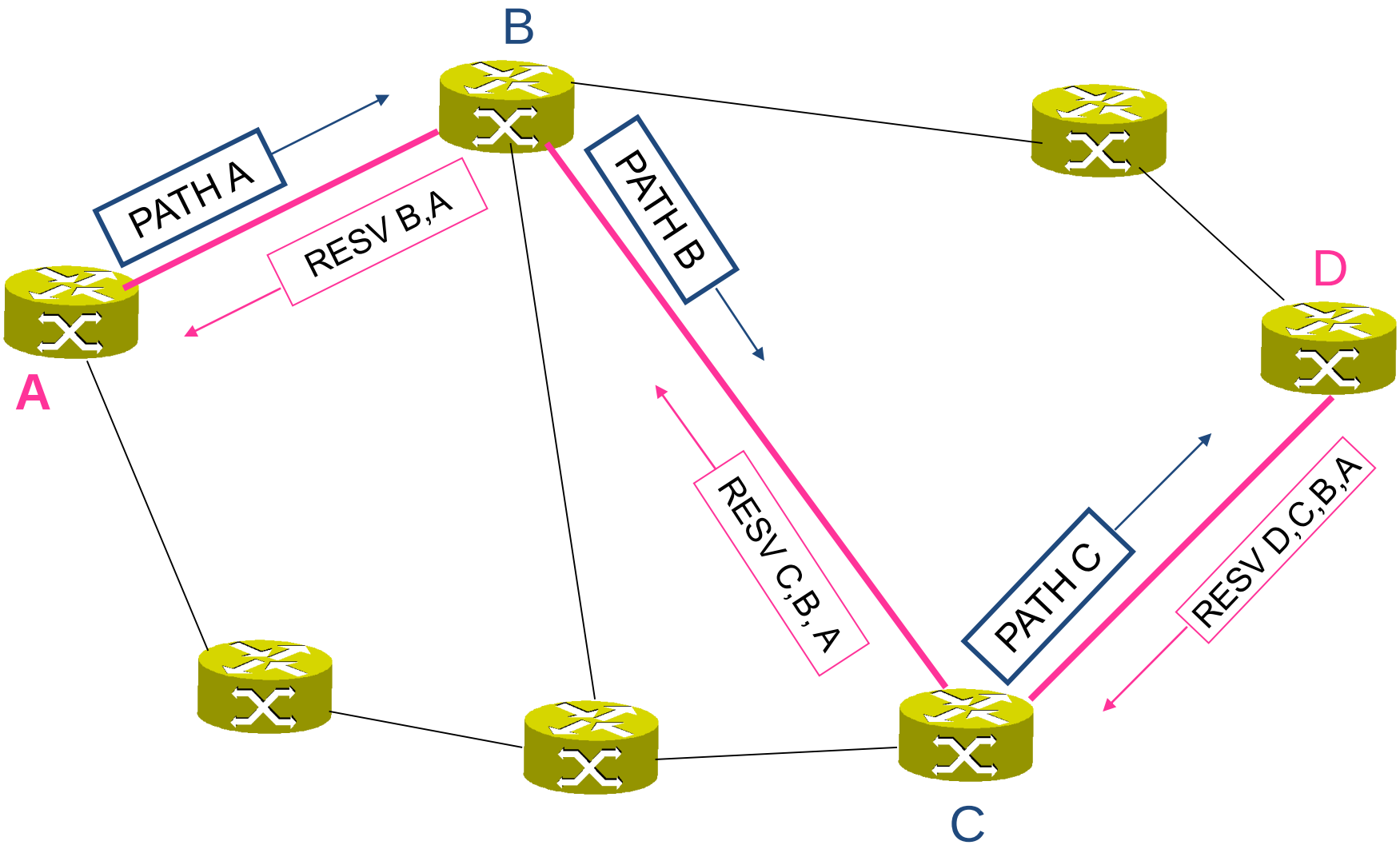
Протокол позволяет запрашивать:

- гарантированную пропускную способность канала;
- предсказуемую задержку;
- максимальный уровень потерь.

Особенностей RSVP: запросы на резервирование ресурсов направляются только от получателей данных отправителям, а не наоборот.

Недостаток RSVP: полоса пропускания, выделяемая источнику информации, при снижении активности источника не может быть использована для передачи другой информации.

Организация RSVP-пути



Процесс резервирования пути

- Узел-отправитель посылает запрос PATH как обычный пакет.
- Каждый маршрутизатор прописывает в своей памяти адрес предыдущего и посылает свой адрес в PATH-запросе.
- Получатель в ответ на PATH генерирует RESV и отправляет по прописанному в PATH пути. Т.о. резервирование происходит в обратном порядке, от получателя к отправителю.
- Маршрутизаторы обрабатывают RESV-запросы, пытаясь предоставить требуемые ресурсы. В случае невозможности предоставления ресурсов резервирование начинается сначала.
- Путь считается установленным, когда отправитель получает RESV. После этого начинается сеанс.

Дифференцированные услуги DiffServ

Разработана IETF, 1998 г.

RFC 1349, RFC 2475, RFC 2597, RFC 2598

Цель: поддержка легко масштабируемых дифференцируемых услуг в Internet

Недостатки: отсутствие гарантированного QoS

Основной механизм: маркировка трафика с использованием бита ToS (Type of Service).
Поддерживает политики поведения сетевого узла: AF-phb и EF-phb (Per-Hop Behavior)

Differentiated Services (DiffServ)

- Разработан для преодоления следующих недостатков IntServ и RSVP:
- **Масштабируемость**: в больших сетях количество потоков измеряется десятками тысяч; маршрутизаторы не справляются
- **Ограниченность числа классов обслуживания**: Intserv поддерживает лишь 2 класса; зачастую требуются промежуточные типы
- **Сложная система резервирования ресурсов**: многим приложениям и пользователям требуется лишь указать что определенный трафик должен иметь более высокий приоритет на маршрутизаторе провайдера

Differentiated Services (DiffServ)

- Лишь очень немногие приложения действительно нуждаются в жестких и точных гарантиях качества обслуживания
- DiffServ основаны на свободной классификации трафика с разбиением на небольшое число «приоритетных» классов
- В отличие от RSVP, в случае DiffServ отправитель и получатель не обмениваются информацией о требованиях к качеству обслуживания

Архитектура DiffServ

- Соглашение об уровне сервиса (Service Level Agreement, SLA) – классификация трафика + правила перемаркировки внешнего трафика + действия с потоками для домена (группы маршрутизаторов провайдера)
- Пограничные маршрутизаторы выполняют маркировку трафика
- Внутренние маршрутизаторы обрабатывают пакеты в соответствии с присвоенными им маркерами (правила пошаговой обработки – Per-Hop Behavior, PHB)

Архитектура DiffServ

- Соглашение об уровне сервиса (Service Level Agreement, SLA). Дифференцированное обслуживание распространяется за границу домена DiffServ благодаря заключению SLA между сетью, из которой приходит трафик, и доменом DiffServ, в который трафик направляется. SLA может определять классификацию пакетов и правила перемаркировки; оно также может устанавливать профили трафика и действия, выполняемые с потоками, соответствующими или не соответствующими заданному профилю. Кроме того, SLA предусматривает (прямо или косвенно) соглашение о кондиционировании трафика (Traffic Conditioning Agreement, TCA) между доменами.

- Правила классификации пакетов определяют подмножество трафика, которое может получить дифференцированное обслуживание, за счет кондиционирования и/или отображения на один или несколько агрегированных потоков (с помощью перемаркировки кодов DiffServ) внутри домена DiffServ. Классификатор отбирает пакеты из потока трафика в зависимости от содержания некоторой части заголовка пакета. Профиль трафика задает временные свойства потока трафика, выбранного классификатором. Имеющиеся правила определяют соответствие конкретного пакета профилю. В зависимости от его соответствия (или несоответствия) профилю к пакету могут применяться различные операции кондиционирования или учета.

Архитектура DiffServ

- Модификация трафика. Кондиционирование трафика включает такие операции, как измерение, формирование, профилирование и/или перемаркировка, чтобы гарантировать, что трафик, попадающий в домен DiffServ, удовлетворяет правилам, определенным в соглашении TCA в соответствии с политикой выделения ресурсов домена (см. Рисунок 2). Контролер определяет, соответствуют ли параметры трафика его профилю. Результаты проверки для конкретного пакета (например, соответствие пакета профилю) могут использоваться для инициирования операций маркировки, отбрасывания или формирования.

- Маркировщики пакетов присваивают полю DiffServ пакета конкретное кодовое значение (codepoint), включая маркированный пакет в конкретный агрегированный поток. Формирователи задерживают некоторые или все пакеты в потоке, чтобы обеспечить соответствие потока его профилю. Формирователь обычно имеет буфер ограниченного размера, так что пакеты могут быть отброшены из-за нехватки в буфере места для размещения задержанных пакетов. Отбраковщики удаляют некоторые или все пакеты в потоке, чтобы обеспечить его соответствие профилю, — этот процесс называется приведением потока в соответствие с требованиями политики, или профилированием. При выходе пакетов из модуля кондиционирования трафика пограничного узла DiffServ поле Differentiated Services Codepoint (DSCP) каждого пакета должно иметь соответствующее значение.

Архитектура DiffServ

- Определение поля DiffServ. Предложенное в качестве замены поле заголовка пакета IP, называемое полем DiffServ, изменяет существующие определения октета IPv4 Type of Service (ToS) (RFC 1349) и октета IPv6 Traffic Class (RFC 2460). Шесть разрядов поля DiffServ интерпретируются как кодовое значение DSCP, которое и используется для выбора правил пошаговой обработки (Per-Hop Behavior, PHB), которой пакет подвергается в каждом узле. Два разряда поля Currently Unused (CU) остаются резервными.

- Правила PHB составляют основу архитектуры DiffServ. PHB — это способ, с помощью которого узел резервирует ресурсы для обслуживаемых им определенных агрегированных потоков трафика. На основе этого механизма пошагового резервирования ресурсов можно предоставлять эффективные дифференцированные услуги. Различия в обслуживании проявляются, главным образом, тогда, когда несколько обслуживаемых агрегированных потоков конкурируют за место в буфере и пропускную способность узла.

- Правила PHB реализуются на узлах с помощью нескольких механизмов управления буфером и планирования обработки пакетов. Конкретный набор (группа) правил обработки для каждого полученного пакета определяется путем отображения значения его кода DSCP на определенное в данном узле множество правил обработки PHB.

Архитектура DiffServ

- Выделение сетевых ресурсов. Реализация, конфигурация, функционирование и администрирование поддерживаемых групп PHB в узлах домена DiffServ должны, в соответствии с политикой распределения ресурсов данного домена, обеспечить эффективное распределение ресурсов этих узлов и связывающих узлы каналов между обслуживаемыми агрегированными потоками трафика. Модули кондиционирования трафика позволяют ввести дополнительный контроль за использованием этих ресурсов за счет применения соглашений TCA и, возможно, за счет организации обратной связи между узлами и другими модулями кондиционирования данного домена.

Политики поведения сетевого узла - phb

- **AF-phb** (Assured Forwarding): политика гарантированной доставки – средство, позволяющее обеспечить несколько различных уровней надежности доставки IP-пакетов.

Механизмы: эффективное управление полосой пропускания за счет организации собственной очереди для каждого типа трафика; 3 уровня приоритетов пакетов; RED.

- **EF-phb** (Expedited Forwarding): политика немедленной доставки – обеспечение сквозного QoS для приложений реального времени.

Механизмы: приоритезация трафика; WFQ; распределение ресурсов; RED.

Сравнение

	Best-Effort	Diffserv	Intserv
Возможности	• связь двух узлов • нет изоляции потоков • нет гарантий	• Агрегированная изоляция классов потоков • Гарантии для классов потоков	• Изоляция потоков • Гарантии для каждого потока
Локальность	• работает на всех узлах в цепочке	• работает в домене	• работает на всех узлах в цепочке
Сложность	• нет настроек	• настройки для классов потоков	• настройки для каждого поток а в отдельности
Масштаби-руемость	• Высокая масштабируемость (узлы работают только с маршрутной информацией)	• Масштабируем (граничные узлы хранят информацию о маркировке, внутренние – о приоритетах классов)	• Не масштабируем (каждый маршрутизатор хранит информацию о каждом потоке)

Механизмы QoS в действии
Как это работает?

КЛАССИФИКАЦИЯ И МАРКИРОВКА	МЕХАНИЗМ ОЧЕРЕДЕЙ	ПОСЛЕДУЮЩАЯ ОБРАБОТКА
IDENTIFY & PRIORITIZE	MANAGE & SORT	PROCESS & SEND

- **Классификация и маркировка:**

  Первым элементом реализации политики является классификация/идентификация трафика. Классифицированный трафик может быть промаркирован с требуемым значением атрибута.

- **Ограничение трафика (полисинг):**

  Проверка на соответствие административно-заданным правилам и выполнение действия по результату, включая маркировку, перемаркировку и сброс.

- **Механизмы очередей и выборочного сброса пакетов:**

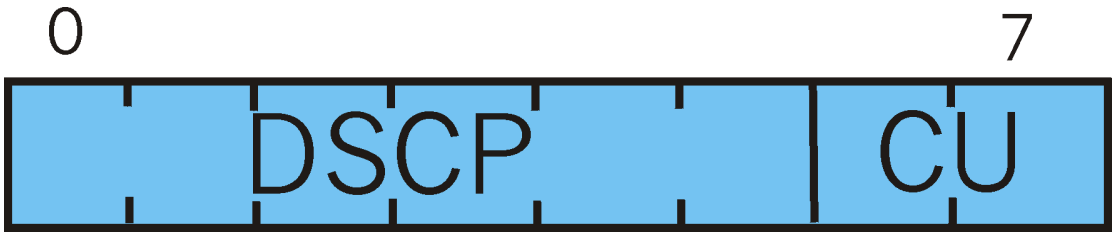
  Определяют как кадр/пакет выходит из устройства. Алгоритм активируется только на период перегрузки.

- **Механизмы оптимизации(шейпинг, фрагментация, компрессия, Tx Ring)**

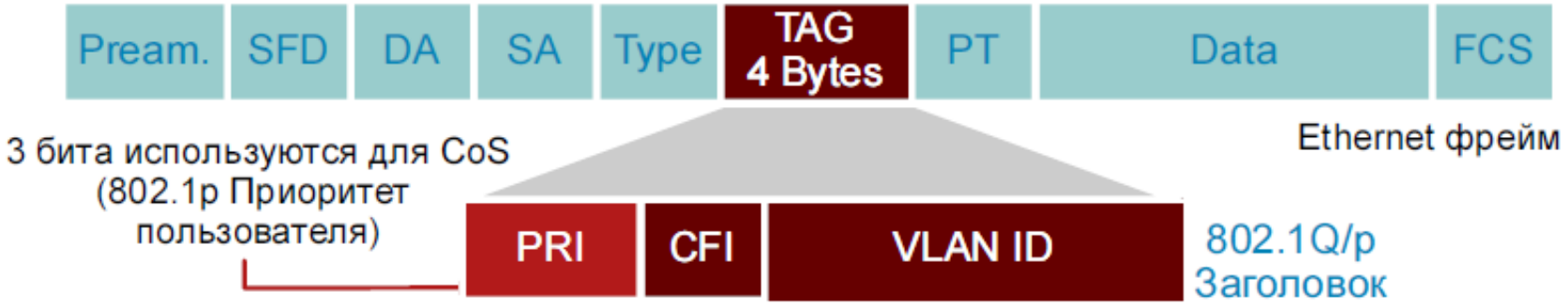
  Средства оптимизации полосы пропускания

Маркировка пакетов

- DSCP – DiffServ Code Point
- Маркер размещается в IP-заголовке в поле Type of Service в IPv4
- 6 бит, 2 – зарезервировано.
  Итого 16 классов



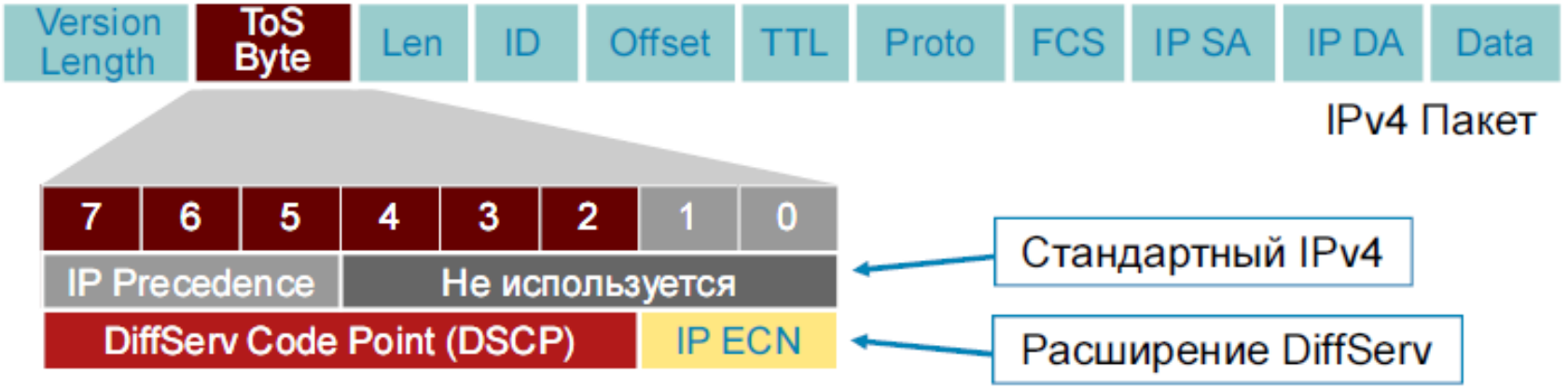
Инструменты классификации
Ethernet 802.1Q Class of Service



- 802.1p поле приоритета пользователя также называется классом обслуживания(CoS)
- Разным типам трафика присваиваются разные значения CoS
- CoS 6 и 7 зарезервированы для использования сетью

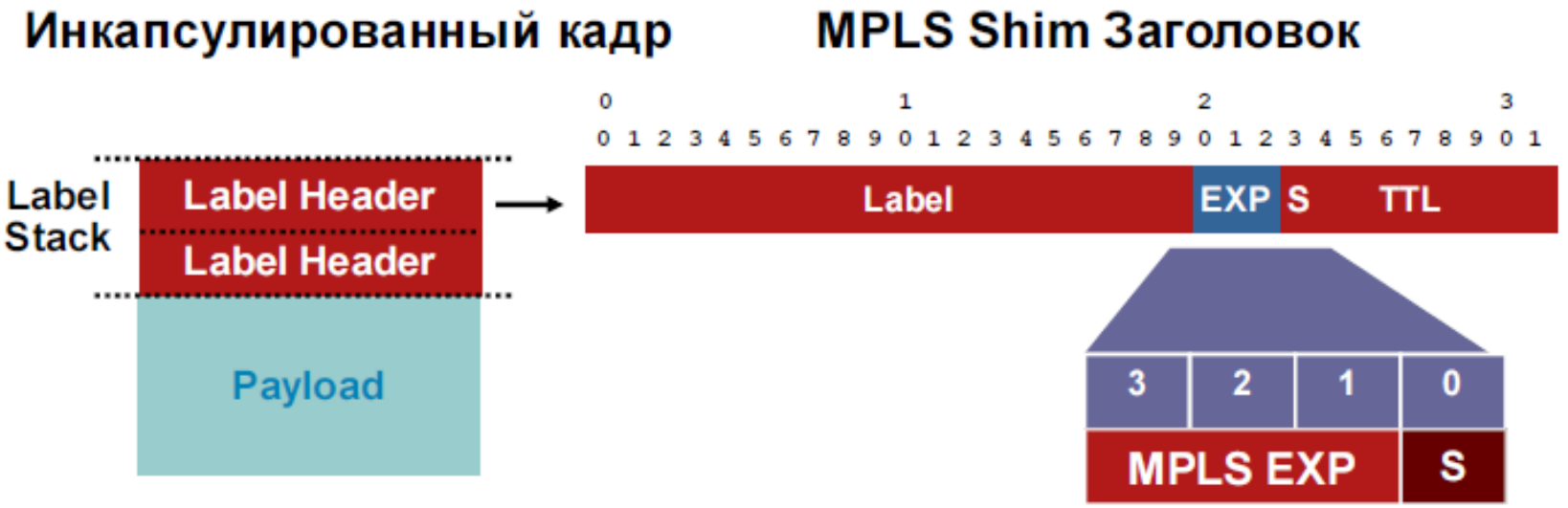
CoS	Применение
7	Зарезервировано
6	Маршрутизация
5	Голос
4	Видео
3	Сигнализация звонка
2	Критические данные
1	Основные данные
0	Низкий приоритет

Инструменты классификации
IP Precedence и DiffServ Code Points



- IPv4: Три наиболее значимых бита ToS байта называются IP Precedence — остальные биты не используются
- DiffServ: Шесть наиболее значимых битов ToS байта называются DiffServ Code Point (DSCP)— оставшиеся 2 бита используются для контроля потока
- DSCP совместим с более старой технологией IP precedence

Инструменты классификации
Биты MPLS EXP



- Информация о приоритете заложена в биты EXP поля
- RFC3270 не содержит рекомендаций относительно специфичных значений EXP для DiffServ PHB (EF/AF/DF)
- Используется для frame-based MPLS

Инструменты классификации
Пошаговое поведение DSCP

- IETF RFCs обозначил термины для описания специальной обработки пакетов со специфическими метками DSCP
- EF: Срочная передача (RFC3246, ранее RFC2598)

  (DSCP 46)
- CSx: Селектор класса (RFC2474)

  Где x соответствует значению IP Precedence (1-7)

  (DSCP 8, 16, 24, 32, 40, 48, 56)
- AFxy: Гарантированная передача (RFC2597)

  Где x соответствует значению IP Precedence
  (только значение 1-4 используются для AF классов)

  И y соответствует значению приоритета отброса (или 1 или 2 или 3)

  Более высокое значение - большая вероятность отброса

  (DSCP 10/12/14, 18/20/22, 26/28/30, 34/36/38)
- BE: Негарантированная доставка или значение по умолчанию (RFC2474)

  (DSCP 0)

Маркировка пакетов

Per-Hop Behaviors (PHB)				DiffServ Code Points (DSCP)		
Expedited Forwarding	EF			46 101110		
Assured Forwarding	Low Drop Pref	Med Drop Pref	High Drop Pref			
Class 1	AF11	AF12	AF13	10 001010	12 001100	14 001110
Class 2	AF21	AF22	AF23	18 010010	20 010100	22 010110
Class 3	AF31	AF32	AF33	26 011010	28 011100	30 011110
Class 4	AF41	AF42	AF43	34 100010	36 100100	38 100110
Best Effort	BE			0 000000		

Маркировка пакетов

Пакеты группы Expedited Forwarding обрабатываются так, что скорость отправления пакетов агрегированного потока из любого узла DiffServ должна быть равна или превышать скорость прибытия пакетов. С помощью EF PHB можно предоставлять обслуживание «из конца в конец» через все домены DiffServ с низким уровнем потерь, низкими задержками, низкими вариациями задержек и гарантированной пропускной способностью. Такое обслуживание для конечных узлов выглядит как соединение «точка-точка» или арендованная виртуальная линия.

Группа AF PHB обеспечивает доставку пакетов IP в соответствии с четырьмя независимо обрабатываемыми классами AF. Внутри каждого класса может быть выделено определенное количество ресурсов, необходимых для трансляции пакетов (некоторый объем буфера и пропускная способность), и назначен один из трех уровней предпочтения при отбрасывании. В случае перегрузки порядок отбрасывания пакетов определяется относительной важностью пакета внутри класса AF.

Обслуживание очередей

Алгоритмы обслуживания очередей позволяют предоставлять разный уровень QoS трафику разных классов. Обычно используется несколько очередей, каждая из которых занимается пакетами с определенным приоритетом.

Обслуживание очередей включает в себя алгоритмы:

- организации очереди;
- обработки очередей.

Алгоритмы организации очереди:

- Tail drops — отсечения конца очереди;
- Random Early Detection (RED) — «справедливо» разделяет канал между TCP-соединениями.
  При малых размерах очередей RED более эффективен, чем другие методы.

Механизмы обслуживания очередей:

- Справедливая взвешенная очередность (Weighted Fair Queuing — WFQ)
- Очередность на основе классов (Class-Based Weighted Fair Queuing — CBWFQ)
- Раннее случайное взвешенное обнаружение (Weighted Random Early Detection — WRED)
- Приоритетная очередность (Priority Queuing)
- Настраиваемая очередь (Custom Queuing)

Обслуживание очередей

Алгоритмы обслуживания очередей позволяют предоставлять разный уровень QoS трафику разных классов. Обычно используется несколько очередей, каждая из которых занимается пакетами с определенным приоритетом.

Обслуживание очередей включает в себя алгоритмы:

- организации очереди;
- обработки очередей.

Алгоритмы организации очереди:

- Tail drops — отсечения конца очереди;
- Random Early Detection (RED) — «справедливо» разделяет канал между TCP-соединениями.
  При малых размерах очередей RED более эффективен, чем другие методы.

Обслуживание очередей

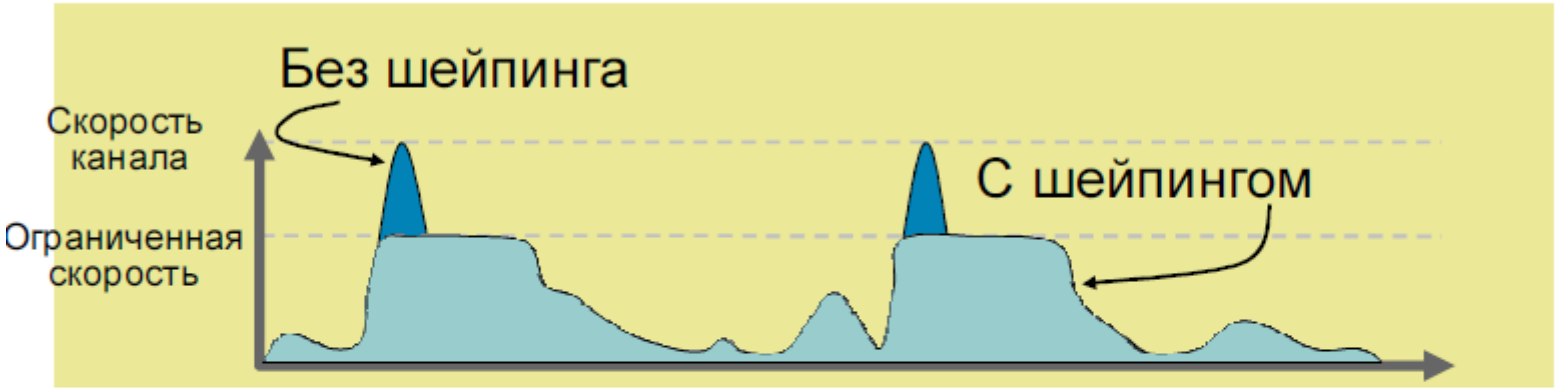
Алгоритмы обработки очередей:

- **Взвешенные очереди (QFQ).**
  Позволяет для каждого вида трафика выделять определенную часть полосы пропускания.

- **Справедливые очереди, базирующиеся на классах (CBWFQ).**
  В отличии от WFQ можно в широких пределах перераспределять полосу пропускания.

- **Очереди с малой задержкой (LLQ).**
  Применяется когда, важнее обеспечить малую задержку, а не широкую полосу пропускания.

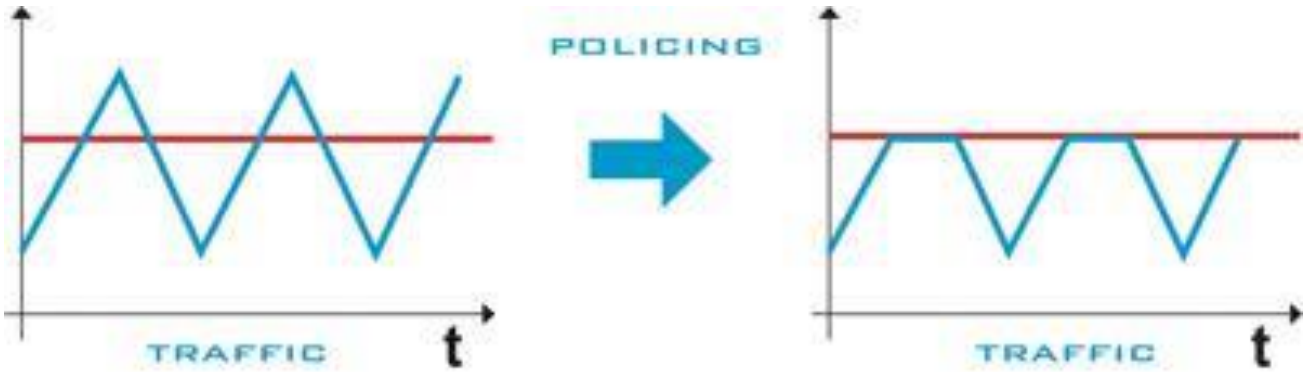
Ограничение трафика
Шейпинг трафика



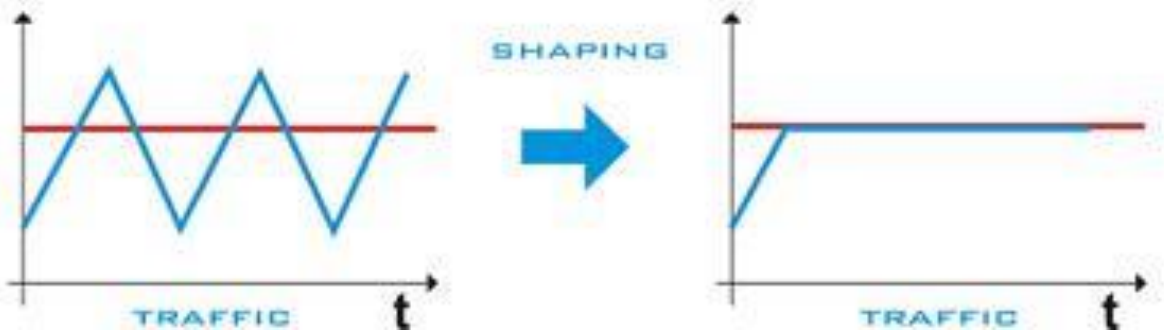
Ограничение траффика до скорости передачи которая ниже скорости канала

- Полисеры (policies) обычно отбрасывают данные
- Шейперы (shaper) обычно задерживают превосходящий трафик, сглаживая пики и предотвращая нежелательные отбрасывания
- Часто используют в Non-Broadcast Multiple-Access (NBMA) топологиях сетей таких как Frame-Relay и ATM

Пример реализации ограничителя (Policer) трафика



Пример реализации формирователя (шейпер, Shaper) трафика



MPLS (Multi-Protocol Label Switching)

Разрабатывается IETF
RFC 2702, RFC 2283, RFC 2547

Цель: отделение процесса маршрутизации пакета от необходимости анализа IP-адресов в его заголовке, что существенно уменьшает время пребывания пакетов в маршрутизаторе и обеспечивает требуемые показатели QoS для трафика реального времени.

Недостатки: ориентирован на топологию

Основной механизм: коммутация по меткам, туннелирование

Выводы: Применение QoS позволяет организовать процесс обслуживания трафика разного типа в ТСКП .

Существует некоторые сложности реализации технологии качества обслуживания:

Операторы связи продолжают работу в направлении предоставления гарантированного сервиса QoS абонентам;

Распространение приложений, использующих QoS;

Средства управления сетью часто ориентированы на какого-нибудь определенного производителя;

Недостаточно проверена совместимость оборудования для реализации технологии Qos.

Настройка качества обслуживания (Qos)

Базовая настройка QoS в маршрутизаторах Cisco:

1. Выделение необходимого трафика из всего информационного потока.

− Настройка листов доступа (ACL):

- **Стандартные;**
- **Расширенные;**
- **Именованные.**

2. Простое применение ограничителей полосы пропускания.

− Rate-limit

(применяется на интерфейсе для потоков попавших под идентификацию листа доступа)

3. Классификация.

− создание класса;

− отнесение к классу выбранного трафика (в соответствии с ACL).

4. Политика действия с классами.

− создание политик;

− отнесение известного класса (известной политики) к политике;

− действие с трафиком (*множество вариантов*).

5. Применение политики к интерфейсу.

− выбор интерфейса;

− определение направления;

− применение политики.

Rate-limit команда вводится в режиме конфигурирования физического интерфейса и имеет следующий синтаксис:

rate-limit input|output [access-group [rate-limit] acl-index] [limit-bps] [nbc] [ebc] conform-action [action] exceed-action [action]

input или output - направление движения трафика

access-group - указывается номер ACL, в который перенаправляем трафик, который будем ограничивать.

Классификация.

class-map DATA	- создание класса *DATA*
match access-group 101	- отнесение пакетов соответствующих листу доступа 101 к классу *DATA*
class-map match-all Class1	- создание класса *Class1*
match access-group 102	- отнесение пакетов соответствующих листу доступа 102 к классу *Class1*
class-map match-any Class1	- создание класса *Class1*
match access-group 103	- пакеты соответствующие листу доступа 103
match interface Fa 0/0	или трафик созданный Fa 0/0 относятся к классу *Class1*

Классификация.

Команда **match** используется для определения различных критериев классификации пакетов.
Если пакет совпадает с указанными критериями:
- Пакет начинает относиться к данному классу;
- Пакет пересылается следуя спецификациям QoS указанных в политике трафика.

Пакеты которые не совпали с указанными критериями:
- Классифицируются как **класс по умолчанию**;
- Распределяются по другим политикам трафика.

Если в данном классе имеется больше чем одно совпадение, используется:
— **class-map match-any** или
— **class-map match-all**
Если используется **match-any**, то трафик будет двигаться исходя из правила, **«должен соответствовать одному из указанных критериев»**
Если используется **match-all**, то трафик будет двигаться исходя из правила, **«должен соответствовать всем указанным критериям»**

Классификация.

Критерии отбора пакетов классом:

class-map match-all CLASS
- match access-group
- match input-interface
- match protocol
- match ip dscp
- match ip rtp
- match mpls experimental

Политика действия с классами

Назначение политики трафика — это конфигурирование функций QoS, которые должны быть связаны с трафиком который был классифицирован как трафик описанный пользователем.

Политика трафика состоит из трех элементов:

- Имя политики (Policy name);
- Класс трафика (обозначается командой class);
- Политики QoS которые будут применены к каждому классу.

policy-map Policy_1 - создание политики *Policy_1*
class DATA - применение политики к трафику класса *DATA*
bandwidth 5000 - ограничение полосы пропускания в 5000 kbps
class class-default - то что не попало в класс *DATA* – формирует
bandwidth 5000 часть класса *class-default* и ему будет предоставлена полоса пропускания 2000 kbps

Политика действия с классами

Действия с трафиком:

bandwidth 5000 - ограничение полосы пропускания в 5000 kbps

bandwidth percent *10* - ограничение полосы пропускания в процентах

police 128000 8000 8000 conform-action transmit exceed-action drop - ограничитель потока аналогично **Rate-limit**

shape peak 64000 - ограничение-выравнивание потока до 64 kbit/s

queue-limit ___ - ограничение очереди (пакеты, байты, мкс, млс)

random-detect - использование WRED

fair-queue - равномерное деление полосы (класс по умолчанию)

priority 1000 - 1000 kbps (только для приоритетного класса)

priority percent 20 - приоритет в процентах от общей полосы пропускания

set ip dscp ___ - установка значения в поле IP dscp

Значения скорости **limit bps, nbc, ebc**

limit bps - скорость ограничения(в битах!)

nbc - допустимый предел трафика

ebc - максимальный предел трафика

Для расчета всех значений используется такая формула:

nbc=limit(bit/s)/8(bit/s)*1,5sec

ebc=2nbc

Действия над трафиком

conform-action - что делать с трафиком при соответствии ограничения;

exceed-action action - что делать с трафиком при превышении ограничения;

Действия с пакетами:

drop — отбросить пакет

transmit — передать пакет

set-dscp-transmit — пометить пакет

Применение политики к интерфейсу

Для присоединения политики трафика, указанную командой *policy-map* на интерфейс, используется команда ***service policy*** .

Применяется как для входящих так и для исходящих пакетов на указанном интерфейсе, поэтому в данной команде необходимо указывать направление трафика.

interface fastethernet 0/0	- настройка интерфейса Fa 0/0
service-policy output Policy_1	- применение политики *Policy_1* к интерфейсу Fa 0/0 в исходящем направлении

Все пакеты покидающие указанный интерфейс должны быть совместимы с критериями указанными в политике трафика названной *Policy_1.*

Выводы:

1. Выделение необходимого трафика из всего информационного потока.

− Настройка листов доступа (ACL):

2. Классификация.

− создание класса;

− отнесение к классу необходимого трафика (по критериям).

3. Политика действия с классами.

− создание политик;

− отнесение известного класса (известной политики) к политике;

− действие с трафиком.

4. Применение политики к интерфейсу.

− выбор интерфейса;

− применение политики в определенном направлени.