



OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

# Онлайн-образование



# Меня хорошо видно && слышно?

Ставьте +, если все хорошо  
Напишите в чат, если есть проблемы

# Quality of Service



Кулиничев Алексей

Администратор Сетей

[Santhous42@yandex.ru](mailto:Santhous42@yandex.ru)

# Правила вебинара



Активно участвуем



Задаем вопрос в чат или голосом



Off-topic обсуждаем в Slack #канал группы или #general



Вопросы вижу в чате, могу ответить не сразу

# Маршрут вебинара

Потребность в QoS



QoS Models



Классификация трафика



Policing and Shaping



# 1

Потребность в QoS



# Потребность в QoS

1. Телефония
2. Видео связь
3. Видео трансляции/презентации
4. Данные

1. Lack of bandwidth
2. Latency and jitter
3. Packet loss

# Lack of Bandwidth

Доступная полоса пропускания = минимальной пропускной способности канала:

1. Увеличить пропускную способность
2. Использовать QoS – установить очередность и приоритет трафика

# Latency and Jitter

Задержка в канале(Latency) – рекомендована в G.114.

В среднем допускается задержка до 400ms без исключений

Для прямых трансляций задержка не более 150ms

\*Cisco системы позволяют задержку для real-time traffic – 200ms

# Latency and Jitter

- Propagation delay (fixed) – Задержка возникающая в кабеле

Пример расчета скорости кабеля, на примере оптики, по формуле  $v = c/n$ ,  
Где

$v$  – средняя скорость прохождения света в среде

$c$  – скорость света в вакууме

$n$  – индекс преломления

То есть скорость света в кабеле  $\sim 200\,000\,000$  метров в секунду

# Latency and Jitter

- Serialization delay (fixed) – задержка размещения всех бит в канале

Расчет по формуле:

$s = \text{packet size in bits} / \text{line speed in bps}$

$s = (1500 \text{ bytes} \times 8) / 1 \text{ Gbps}$

$s = 12,000 \text{ bits} / 1,000,000,000 \text{ bps} = 0.000012 \text{ s} \times 1000 = .012 \text{ ms} \times 1000 = 12\mu\text{s}$

# Latency and Jitter

- Processing delay (fixed) – задержка обработки трафика
- CPU speed (for software-based platforms)
- CPU utilization (load)
- IP packet switching mode (process switching, software CEF, or hardware CEF)
- Router architecture (centralized or distributed)
- Configured features on both input and output interfaces

# Latency and Jitter

- Delay variation(Jitter) (variable) – различие latency между пакетами в одном потоке

Возникает из за очередей на оборудовании

Допустимый Jitter ~30ms

Для уменьшения Jitter рекомендуется использовать очереди с низкой задержкой(зависит от оборудования)

# Packet Loss

При появлении больших очередей на оборудовании:

1. Увеличение пропускной способности
2. Внедрение QoS
3. Внедрение policy для отбрасывания низкоприоритетных пакетов
4. Формирование управляемых очередей для задержки трафика (shape)



# 2

## QOS MODELS



# QOS MODELS

1. Best effort – QoS не включен
2. Integrated Services (IntServ) – приложение сигнализирует о необходимости выделить полосу пропускания
3. Differentiated Services (DiffServ) – в сети определяются классы для обработки различного трафика

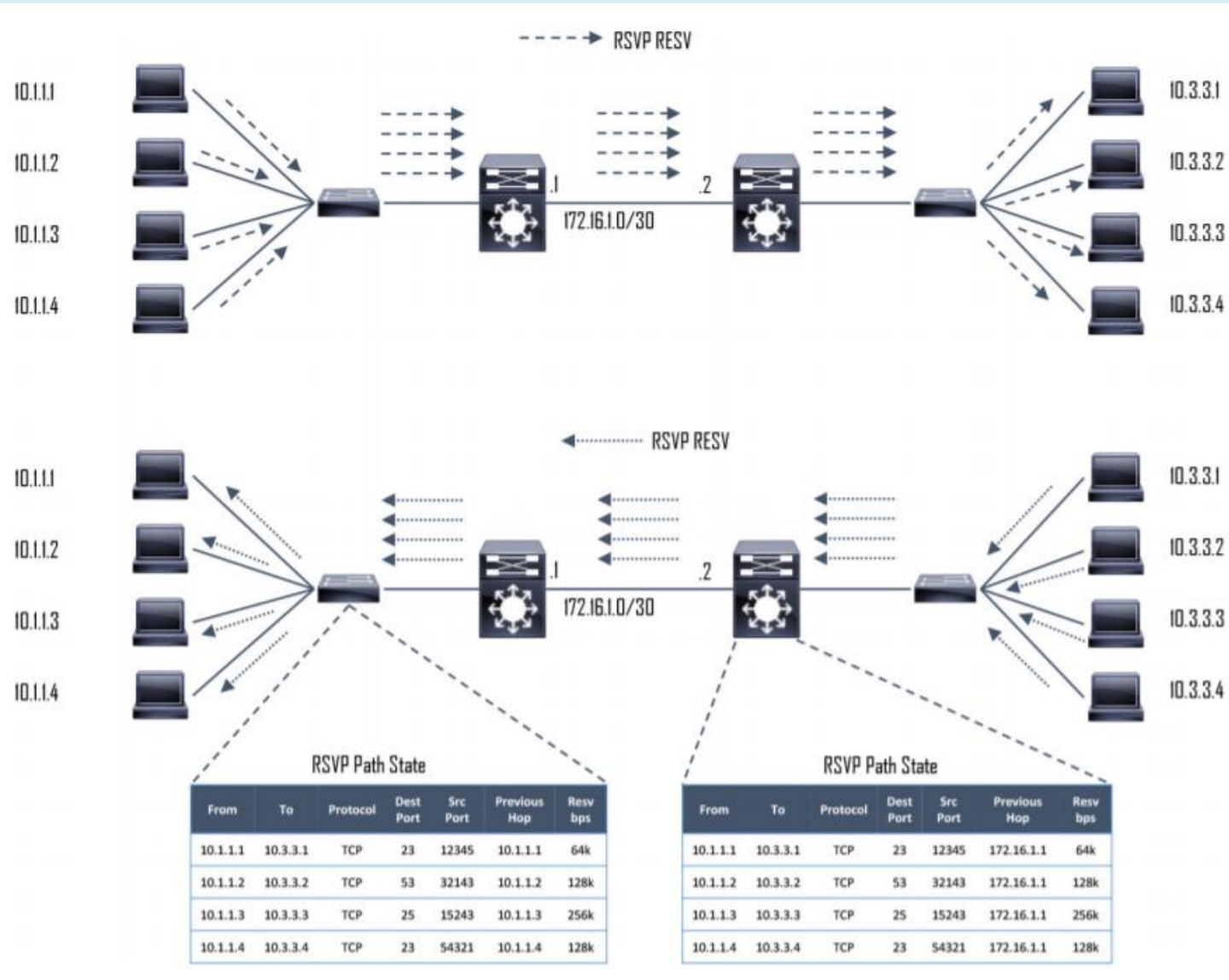
# Integrated Services

Заранее занимается необходимая полоса пропускания

Приложение работает с протоколом Resource Reservation Protocol (RSVP)  
– с помощью сообщений call admission control (CAC) указывает  
параметры для резервирования канала

Все устройства в сети должны поддерживать этот протокол

# Integrated Services



# Differentiated Services

Определение классов на всем оборудовании для используемого трафика.

Например – выделяем трафик телефонии - голос чувствителен к latency и jitter и назначаем максимальный приоритет

Трафик электронной почты или YouTube можно выделить в менее приоритетный трафик и т.д.

# Differentiated Services

Обработка трафика:

1. Classification (разбивка на классы трафика – Class of Service)
2. Metering
3. Coloring
4. Policing
5. Queuing
6. Dropper
7. Shaper and scheduling
8. Marking
9. Serialization

# Differentiated Services

Классификация и маркировка трафика происходит на пограничных устройствах

Следующие устройства доверяют метке и передают трафик по заданному CoS

DffServ-Domain – зона доверия.



# 3

## CLASSIFICATION AND MARKING



# CLASSIFICATION AND MARKING

Способы работы с классификацией трафика:

1. Behavior Aggregate – довериться метке IP DSCP
2. Interface-based
3. MultiField – анализ поля заголовков пакета(MAC, IP и т.д.)

# DSCP

3 бита	1 бит	1 бит	1 бит	1 бит	1 бит
Precedence	Delay	Througput	Relia bility	0	0



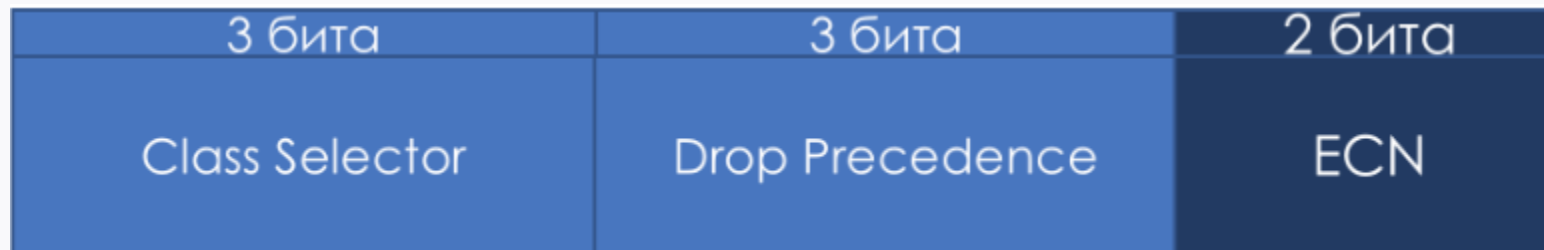
3 бита	1 бит	1 бит	1 бит	1 бит	1 бит
Precedence	Delay	Througput	Relia bility	Cost	0



TOS

6 бит	2 бита
DSCP	Currently Unused

# DSCP



No.	Time	Source	Destination	Protocol	Length	Info
→ 1	0.000000	172.16.1.1	172.16.2.2	ICMP	114	Echo (ping) request
← 2	0.000859	172.16.2.2	172.16.1.1	ICMP	114	Echo (ping) reply
3	0.000968	172.16.1.1	172.16.2.2	ICMP	114	Echo (ping) request
4	0.001345	172.16.2.2	172.16.1.1	ICMP	114	Echo (ping) reply

▶ Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface

▶ Ethernet II, Src: aa:bb:cc:00:72:00 (aa:bb:cc:00:72:00), Dst: aa:bb:cc:00:82:10 (aa:bb:cc:00:82:10)

▼ Internet Protocol Version 4, Src: 172.16.1.1, Dst: 172.16.2.2

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 100
- Identification: 0x001e (30)
- ▶ Flags: 0x00
- Fragment offset: 0
- Time to live: 255
- Protocol: ICMP (1)
- Header checksum: 0x6057 [validation disabled]
- [Header checksum status: Unverified]
- Source: 172.16.1.1
- Destination: 172.16.2.2
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

▶ Internet Control Message Protocol

# DSCP

- DF – Default Forwarding(BE) – стандартная пересылка
- AF – Assured Forwarding – гарантированная пересылка( Steaming, конференц-связь, игры)
- EF – Expedited Forwarding – экстренная пересылка(телефония)
- CS – Class Selector – для обратной совместимости. Сейчас сохранились только CS6/CS7. исключает отбрасывание и задержку. Но допустима малая полоса пропускания

DSCP Class	DSCP Value Bin	Decimal Value Dec	Drop Probability	Equivalent IP Precedence Value
DF (CS0)	000 000	0		0
CS1	001 000	8		1
AF11	001 010	10	Low	1
AF12	001 100	12	Medium	1
AF13	001 110	14	High	1
CS2	010 000	16		2
AF21	010 010	18	Low	2
AF22	010 100	20	Medium	2
AF23	010 110	22	High	2
CS3	011 000	24		3
AF31	011 010	26	Low	3
AF32	011 100	28	Medium	3
AF33	011 110	30	High	3
CS4	100 000	32		4
AF41	100 010	34	Low	4
AF42	100 100	36	Medium	4
AF43	100 110	38	High	4
CS5	101 000	40		5
EF	101 110	46		5
CS6	110 000	48		6
CS7	111 000	56		7

# DSCP

DF – нетребовательный трафик — получает внимание по остаточному принципу

AF – необходимо обеспечить полосу, в ущерб задержкам и потерям.

EF – гарантия задержек, джиттера и отсутствия потерь.

CS6, CS7 – недопустимы потери и задержки, но малая пропускная способность. Например служебный трафик

# MultiField

На основе различных критериев присваиваем определенный класс трафика

Критерии на основе:

- Internal: QoS groups (locally significant to a router)
- Layer 1: Physical interface, subinterface, or port
- Layer 2: MAC address and 802.1Q/p Class of Service (CoS) bits
- Layer 2.5: MPLS Experimental (EXP) bits
- Layer 3: Differentiated Services Code Points (DSCP), IP Precedence (IPP), and source/destination IP address
- Layer 4 – tcp/udp
- Layer 7 – Next Generation Network-Based Application Recognition (NBAR2)

# MultiField

```
ip access-list extended ICMP_ACL  
  permit icmp any any
```

```
ip access-list extended TCP_ACL  
  permit tcp any any
```

```
ip access-list extended OTHER_ACL  
  permit ip any any
```

# MultiField

```
class-map match-all TCP_CM  
  match access-group name TCP_ACL
```

```
class-map match-all OTHER_CM  
  match access-group name OTHER_ACL
```

```
class-map match-all ICMP_CM  
  match access-group name ICMP_ACL
```

# MultiField

```
policy-map ADMISSION_CONTROL
```

```
  class ICMP_CM
```

```
    set ip dscp ef
```

```
  class TCP_CM
```

```
    set ip dscp af11
```

```
  class OTHER_CM
```

```
    set ip dscp default
```

# MultiField

```
interface Ethernet0/1  
  service-policy input ADMISSION_CONTROL
```

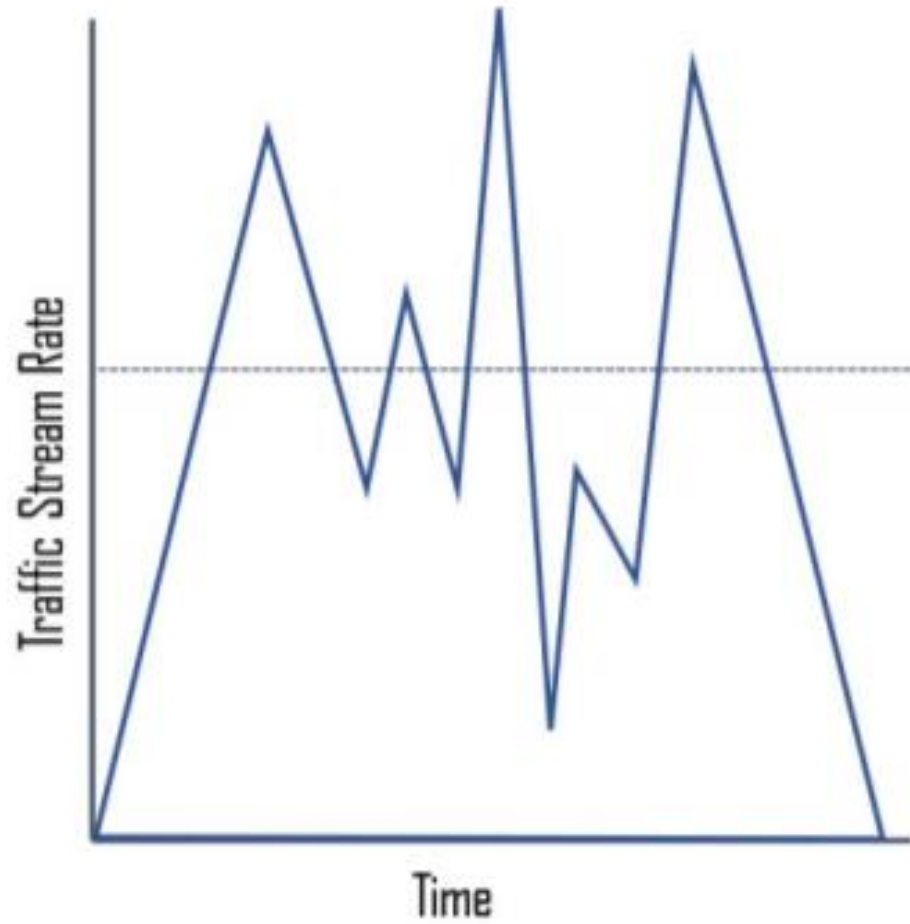


4

Ограничение трафика



# Policing



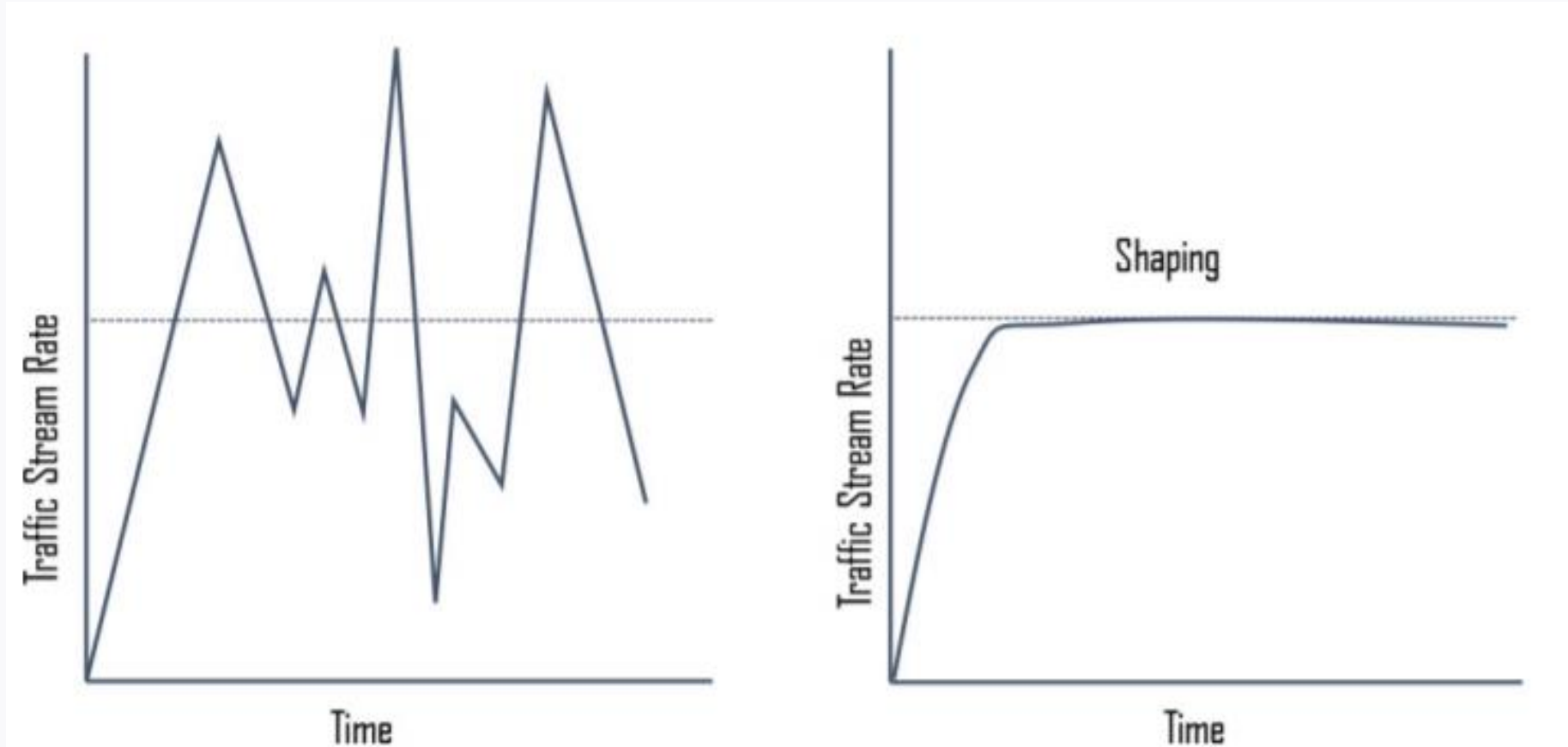
# Policing

Два метода работы:

1. Hard Policing – отбрасывает все\* что выходит за границы
2. Soft Policing – помещает трафик в другой класс, более низкий класс

\* На самом деле дает немного выйти за границу

# Shaping



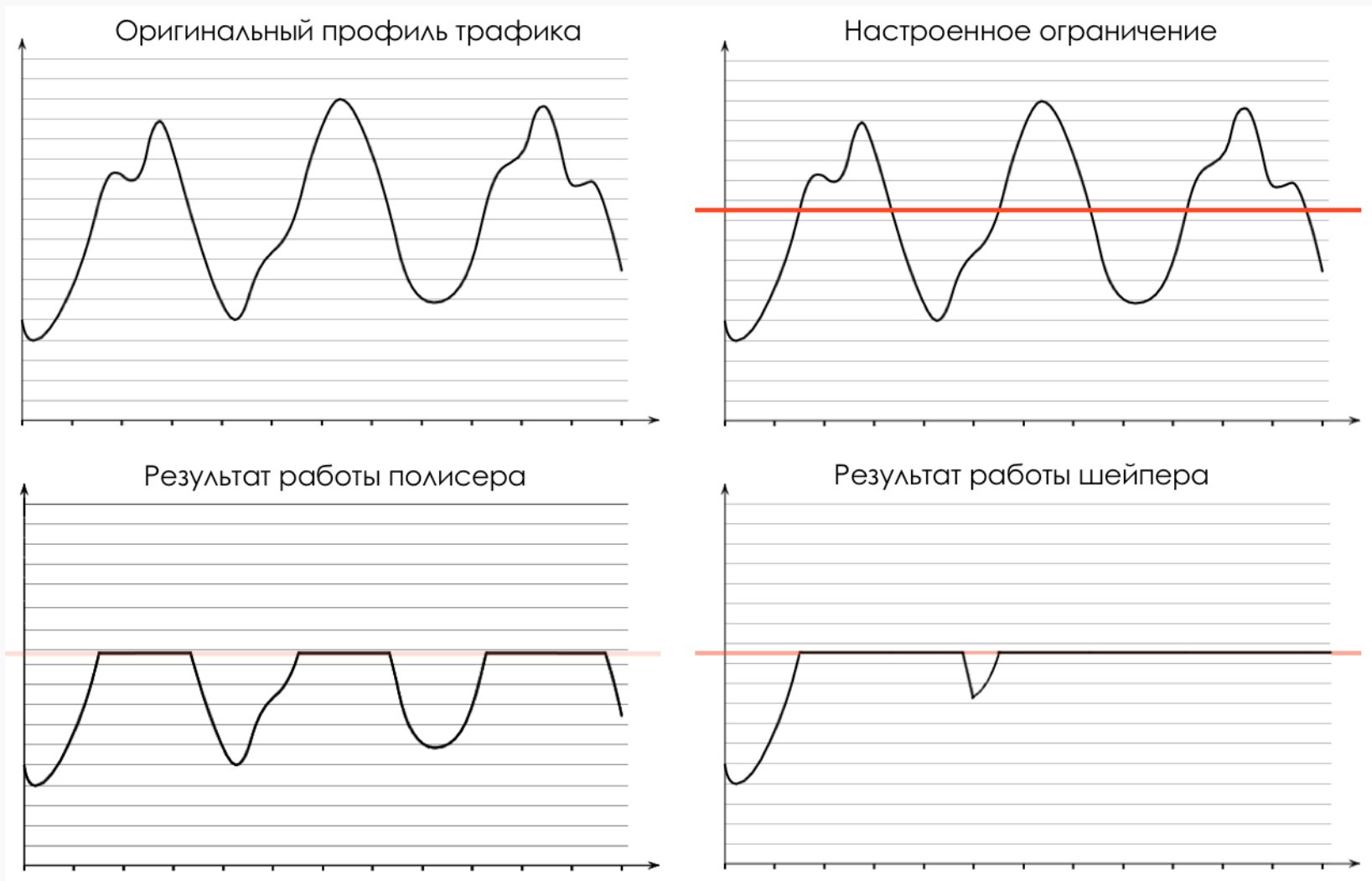
# Shaping

Создается буфер в котором хранится трафик

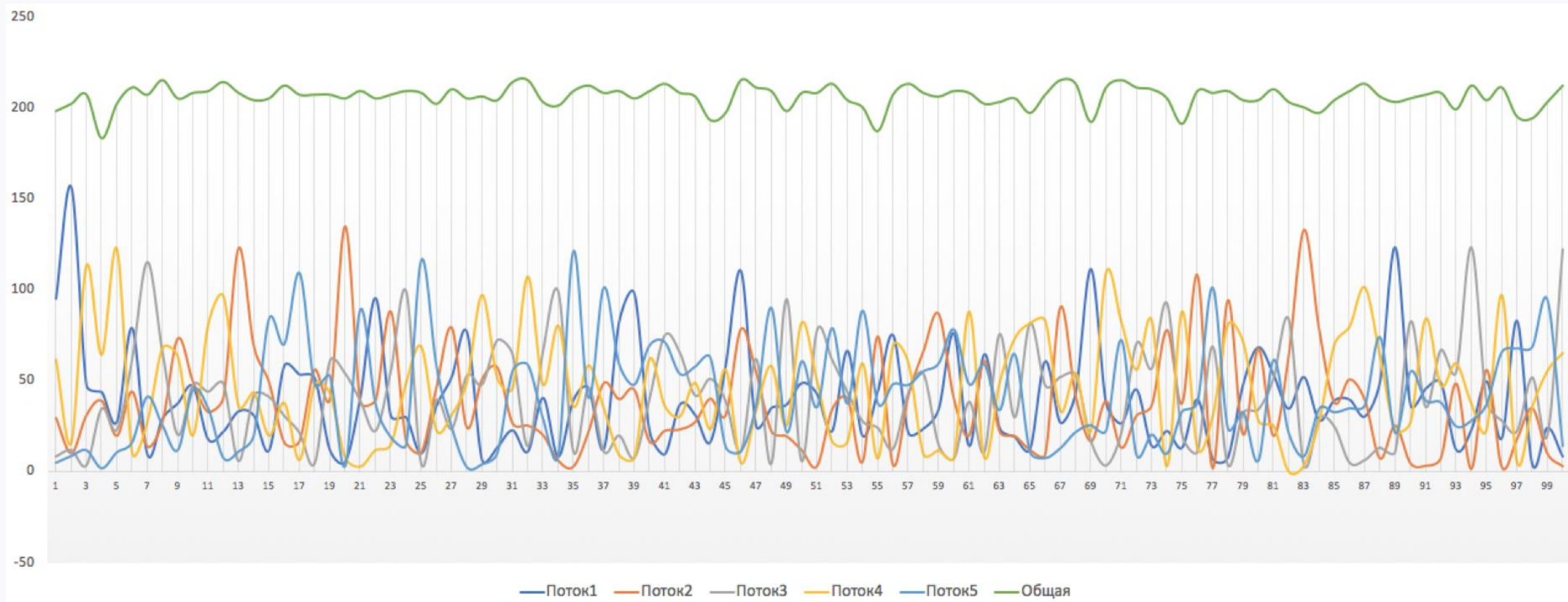
Подходит для трафика не чувствительного к задержкам, но критичному к потерям

Никак не влияет на маркировку пакета

# Policing/Shaping



# Shaping



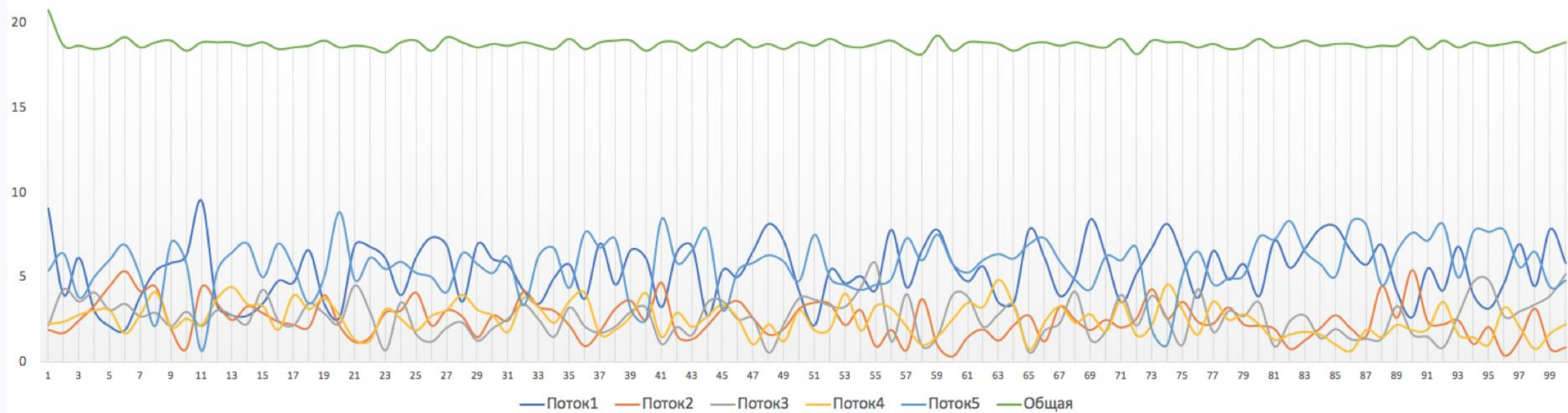
# Shaping

```
class-map match-all ALL_CM  
  match any
```

```
policy-map SHAPING  
  class ALL_CM  
    shape average 20000000
```

```
interface Ethernet0/2  
  service-policy output SHAPING
```

# Shaping



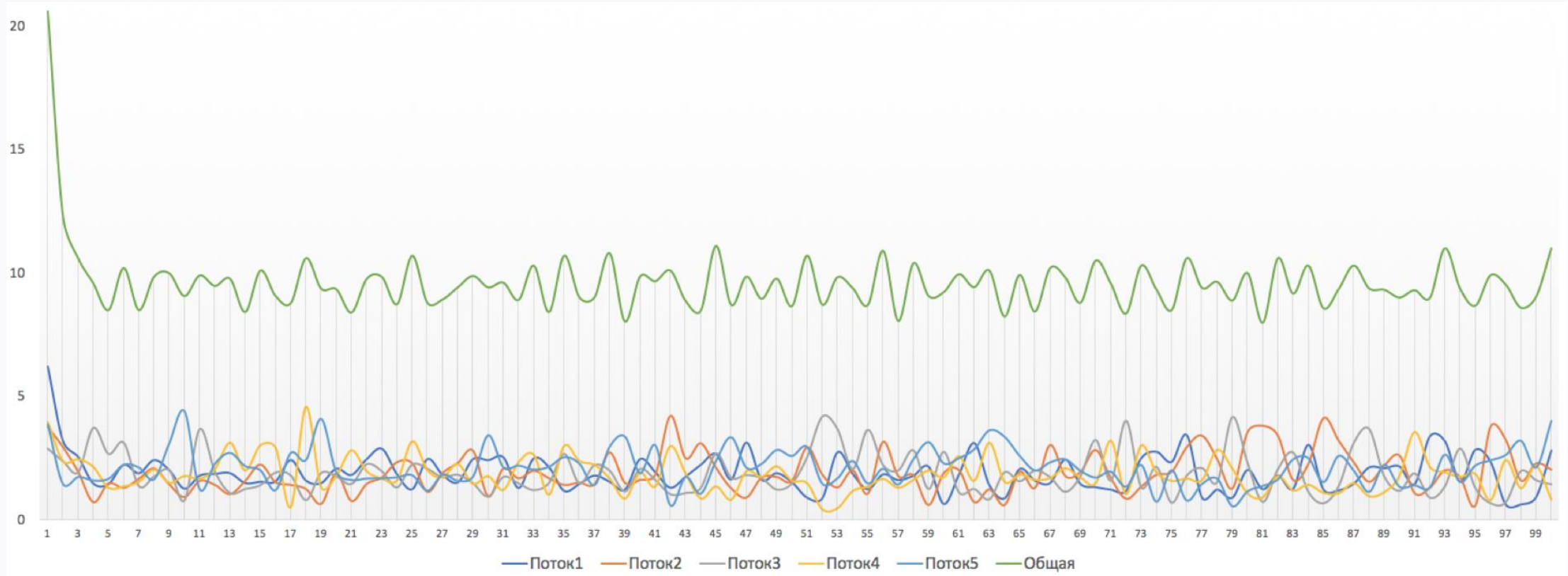
# Policing

```
policy-map ADMISSION_CONTROL  
  class TCP_CM  
    police cir 10000000 bc 1875000 conform-action transmit exceed-action  
drop
```

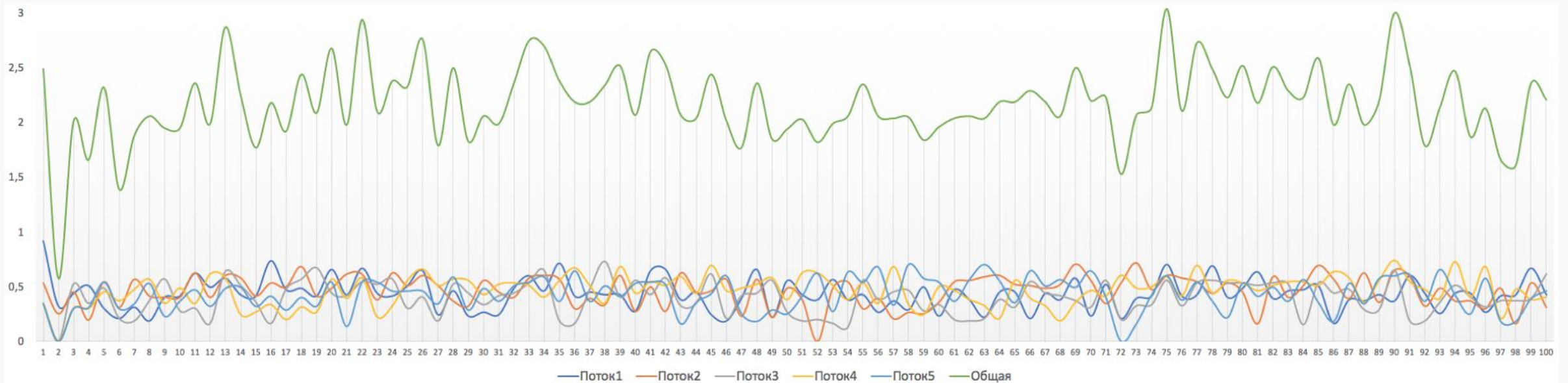
```
interface Ethernet0/1  
  service-policy input ADMISSION_CONTROL
```

средняя разрешённая скорость - CIR (10Мб/с)  
разрешённый всплеск Bc (1 875 000 байтов около 14,6 МБ)

# Policing



# Policing



police cir 10000000 bc 10000 conform-action transmit exceed-action drop

# Policing

Cir – Committed Information Rate – гарантированная средняя скорость(б/сек)

CBS(Вс) – Committed Burst Size – разрешенный максимальный размер всплеска(байт)

$CBS = CIR \text{ (бит в секунду)} * 1,5 \text{ (секунды)} / 8 \text{ (бит в байте)}$



Заполните, пожалуйста,  
опрос о занятии по ссылке в чате



# До новых встреч!

## Приходите на следующие занятия



Кулиничев Алексей

Администратор Сетей

[Santchous42@yandex.ru](mailto:Santchous42@yandex.ru)