Методы инспекции пакетов и анализа трафика

Лекция 1
Эволюция методов анализа трафика

Фицов Вадим Владленович

ст.преп. кафедры ИКС

Цели дисциплины

Методы инспекции пакетов и анализа трафика

Цель дисциплины:

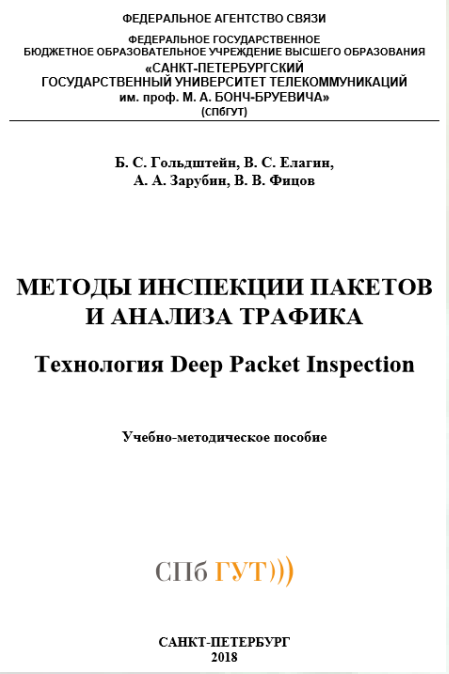
- Получить представление о современных системах контроля пакетного трафика в мультисервисных сетях. .

Компетенции:

- **способность проводить работы по управлению потоками трафика на сети.**

- **собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи и их элементов .**

- **знать принципы эксплуатации сетей связи, современные направления развития телекоммуникационных сетей и систем, основные методы анализа, особенности реализации услуг, используемые системы сигнализации и протоколы**


ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Б. С. Гольдштейн, В. С. Елагин,
А. А. Зарубин, В. В. Фицов

МЕТОДЫ ИНСПЕКЦИИ ПАКЕТОВ
И АНАЛИЗА ТРАФИКА

Технология Deep Packet Inspection

Учебно-методическое пособие

СПб ГУТ)))

САНКТ-ПЕТЕРБУРГ
2018

Литература:

1. Методы инспекции пакетов и анализа трафика. Технология Deep Packet Inspection
[Электронный ресурс] : учебно-методическое пособие / Б. С. Гольдштейн [и др.] – СПб. : СПбГУТ, 2018. - 60 с. : ил., цв.ил.

2. Гольдштейн Б. С., Соколов Н.А., Яновский Г.Г. Сети связи.
учебник для вузов [Текст] : учебник для вузов / СПб. : БХВ-Петербург, 2014. - 400 с.

3. **Гольдштейн, Б. С. Сети связи пост-NGN [Электронный ресурс] / Б. С. Гольдштейн, А. Е. Кучерявый.** - СПб. : БХВ-Петербург, 2014. - 160 с. : ил. - ISBN 978-5-9775-3251-8 : Б. ц.

4. **http://iks.sut.ru (разделы: COPM, DPI)**

Темы лекций

1. Эволюция методов анализа трафика

2. Понятие и назначение DPI
3. Возможности технологии DPI
4. Применение DPI в целях СОРМ

5. Особенности использования DPI оператором связи.

6. Принцип работы DPI

7. Архитектура DPI

8. Алгоритм работы системы DPI в целом

9. Политики обслуживания в PCRF

10. Мониторинг трафика сети с применением DPI

- Анализ трафика на основе
-адресации и транспортных портов (SPI).

- Дифференцированное обслуживание.
- LPI
- MPI
- Middle boxes
- DPI

Методы классификации:

1. Системы дифференцированного обслуживания
2. Анализ по портам
3. Облегченный анализ пакетов (Lightweight Packet Inspection)
4. Средний анализ пакетов (MPI)
5. Глубокого анализа пакетов (Deep Packet Inspection)
6. URL фильтрация
7. Технологии Data Mining

Тренды Интернет трафика

Выводы:

- По разным источникам ежегодный рост объемов трафика составляет около 25-35%
- Все типы трафика увеличивают объёмы
- Три основных типа трафика: P2P, онлайн видео и WEB браузинг
- Стремительно растёт доля онлайн видео, видео сервисы получают резкое развитие за счет онлайн кинотеатров (Netflix, VK, IVI и т.д.) и поддержки онлайн видео телевизорами и телевизионными приставками.
- Существенно увеличивается доля трафика видео-звонков и конференций

История развития DPI

Модель развития DPI

Технологии инспекции трафика развивались последовательно, каждая последующая наследовала часть предыдущих механизмов и добавляла свои….

Уровень	SPI	Port based (Firewall)	MPI и LPI	DPI	Модель OSI
7					Приложения
6					Представления
5					Сеансовый
4					Транспортный
3					Сетевой
2					Канальный

1.Анализ трафика на основе
- адресации и транспортных
портов (SPI).

11

Типовая идентификация трафика

Используемые порты

Proxy – DNS имя

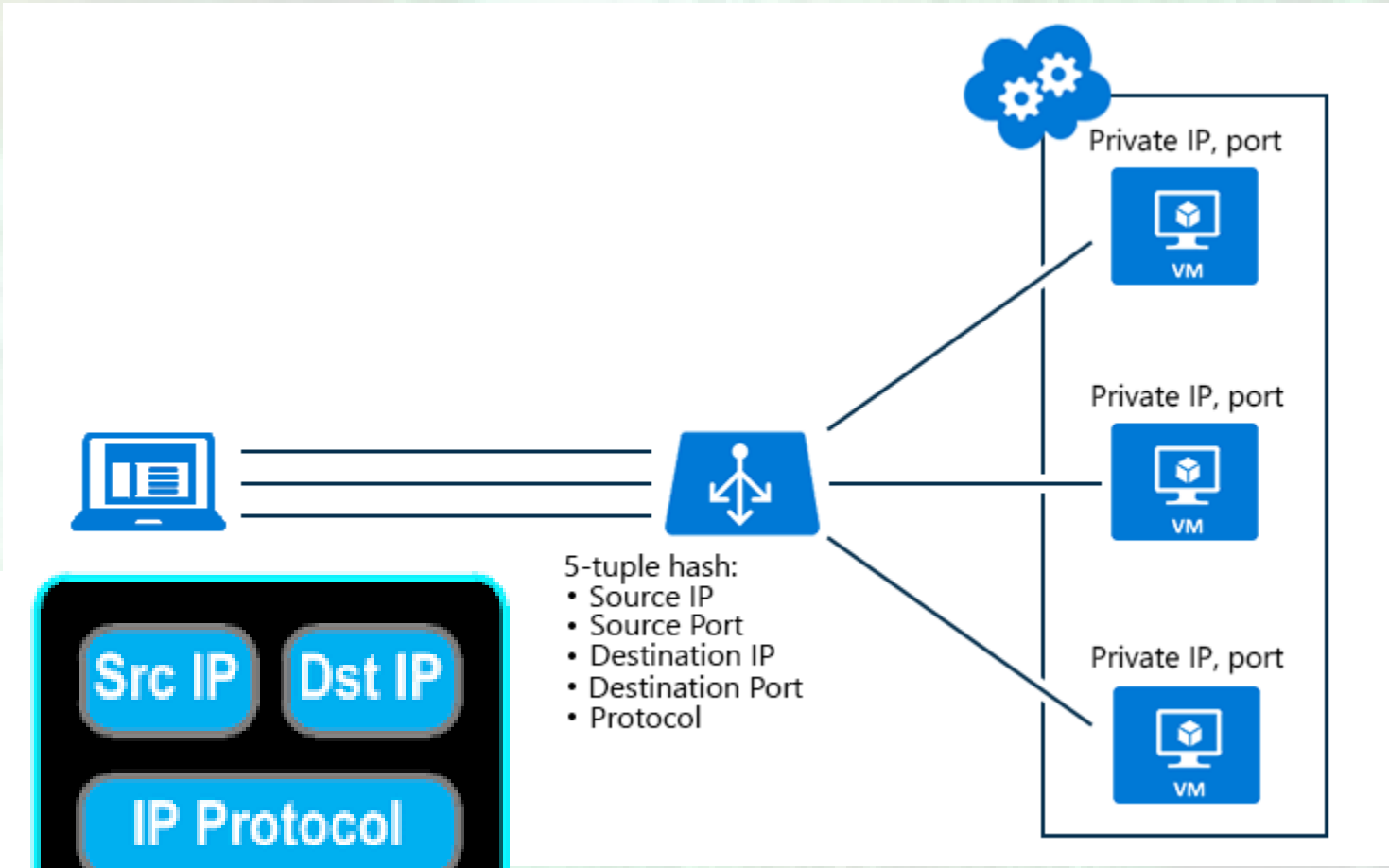
Протокол/ID (TCP/UDP/…)

IP адреса (SRC/DST)

MAC-адреса

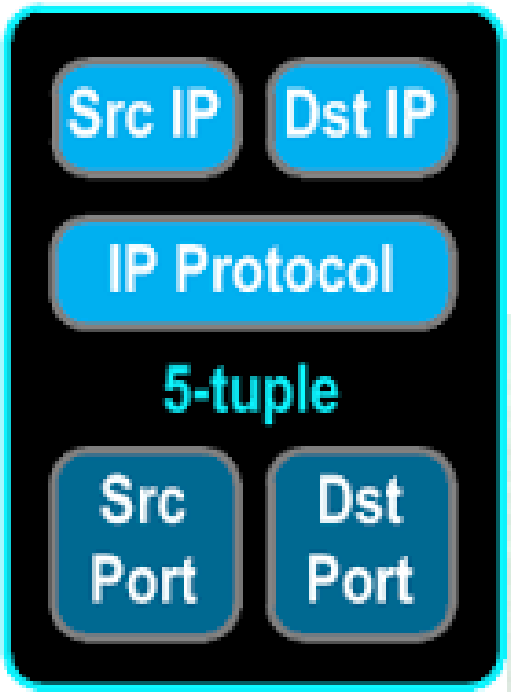
Основные идентификаторы управления трафиком в коммутаторах, маршрутизаторах, брандмауэрах позволяющие настроить ACL или QoS

7 tuples (кортеж 7)

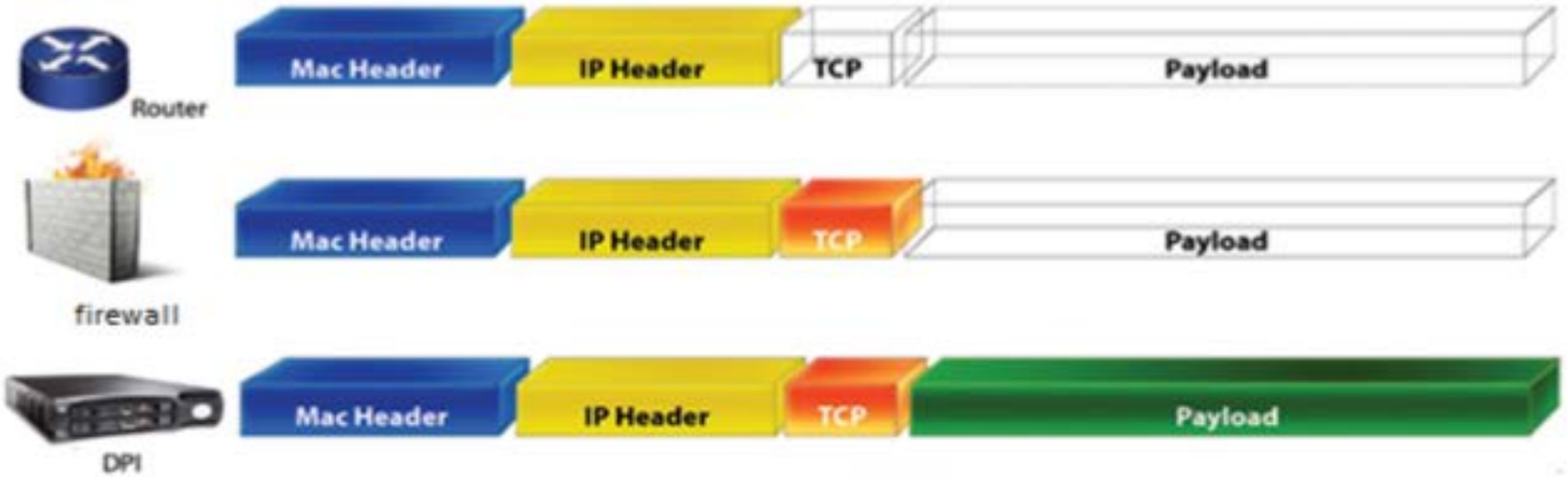


Network-Layer Metadata

Transport-Layer Metadata



13


Router
Mac Header
IP Header
TCP
Payload
firewall
Mac Header
IP Header
TCP
Payload
DPI
Mac Header
IP Header
TCP
Payload

Параметры фильтрации:

- IP адреса назначения и отправления
- MAC адреса назначения и отправления
- порт назначения
- длина кадра
- протокол
- количество пакетов подлежащих анализу
- интерфейс ПК анализатора
- интервал ожидания последующего пакета

15

Параметры фильтрации:

- время начала и конца анализа пакетов
- полный HEX-код каждого кадра
- количество собранных пакетов в соответствии с фильтром
- график распределения задержки пакетов (jitter-histogramm)

16

Анализ:

- распределение по типам протоколов

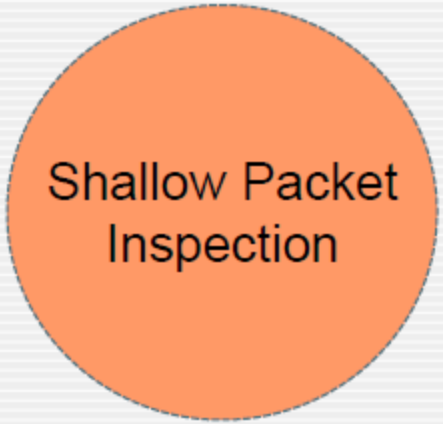
(%, кол-во пакетов, кол-во байт, скорость)

- распределение по длине кадров
- расчет скорости для каждого протокола
- построение графиков (пакетов/с, бит/с)
- список сайтов к которым обращаются HTTP запросы
- распределение количества пакетов по IP адресам
- обнаружение udp multicast

17

История развития DPI

Слабый анализ пакетов



Shallow Packet Inspection – технология анализа трафика, основывающаяся исключительно на заголовках пакета (не анализирует содержимое полезной нагрузки пакета).

Это первая реализация технологии инспектирования трафика. Менее требовательна к ресурсам, чем MPI и DPI, за счёт чего, может обрабатывать гораздо большие объемы трафика с высокой точность определения.

Технология широко распространена, на её основе работает большинство брандмауэров операционных систем, маршрутизаторов (ACL) и т.д.

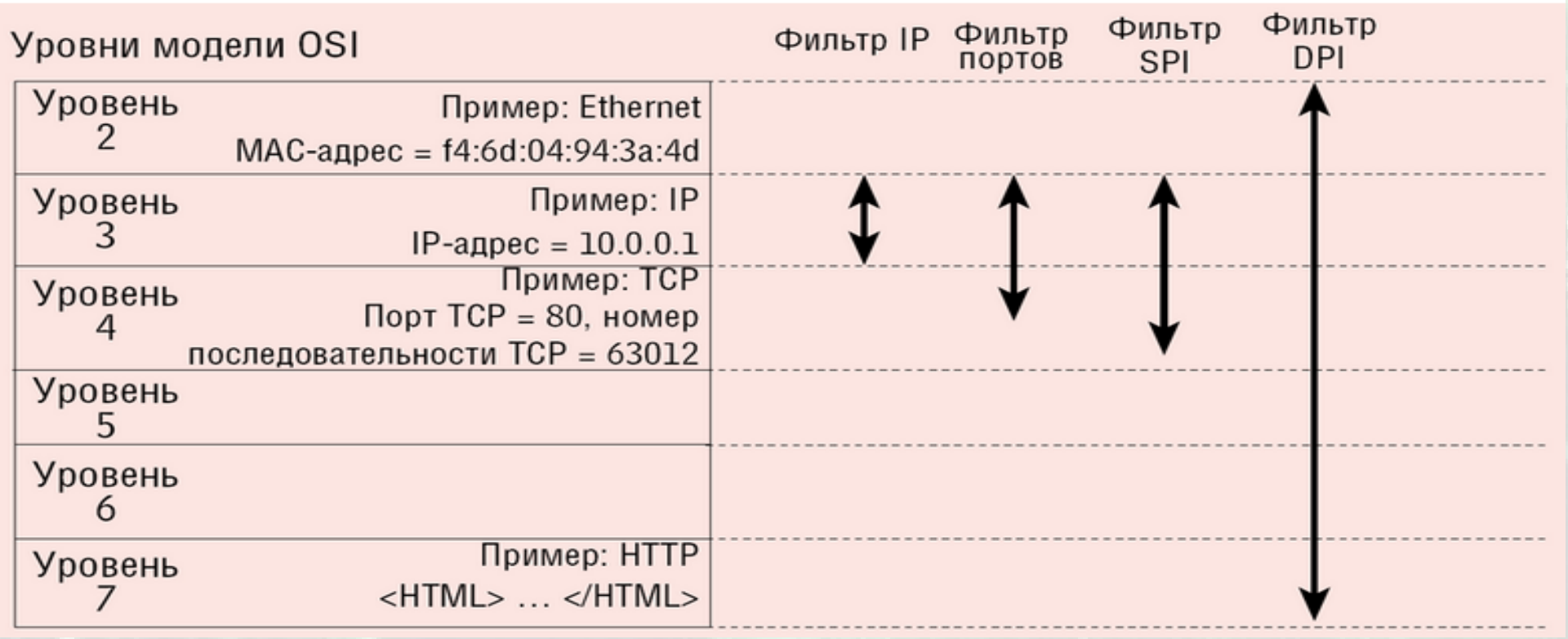
Примечание: не путать с технологией stateful packet inspection – технология проверки трафика на корректность.

SPI

- журнал событий,
- трансляция адресов (Network Address Translation, NAT),
- конечная точка VPN,
- блокирует абсолютно весь трафик.

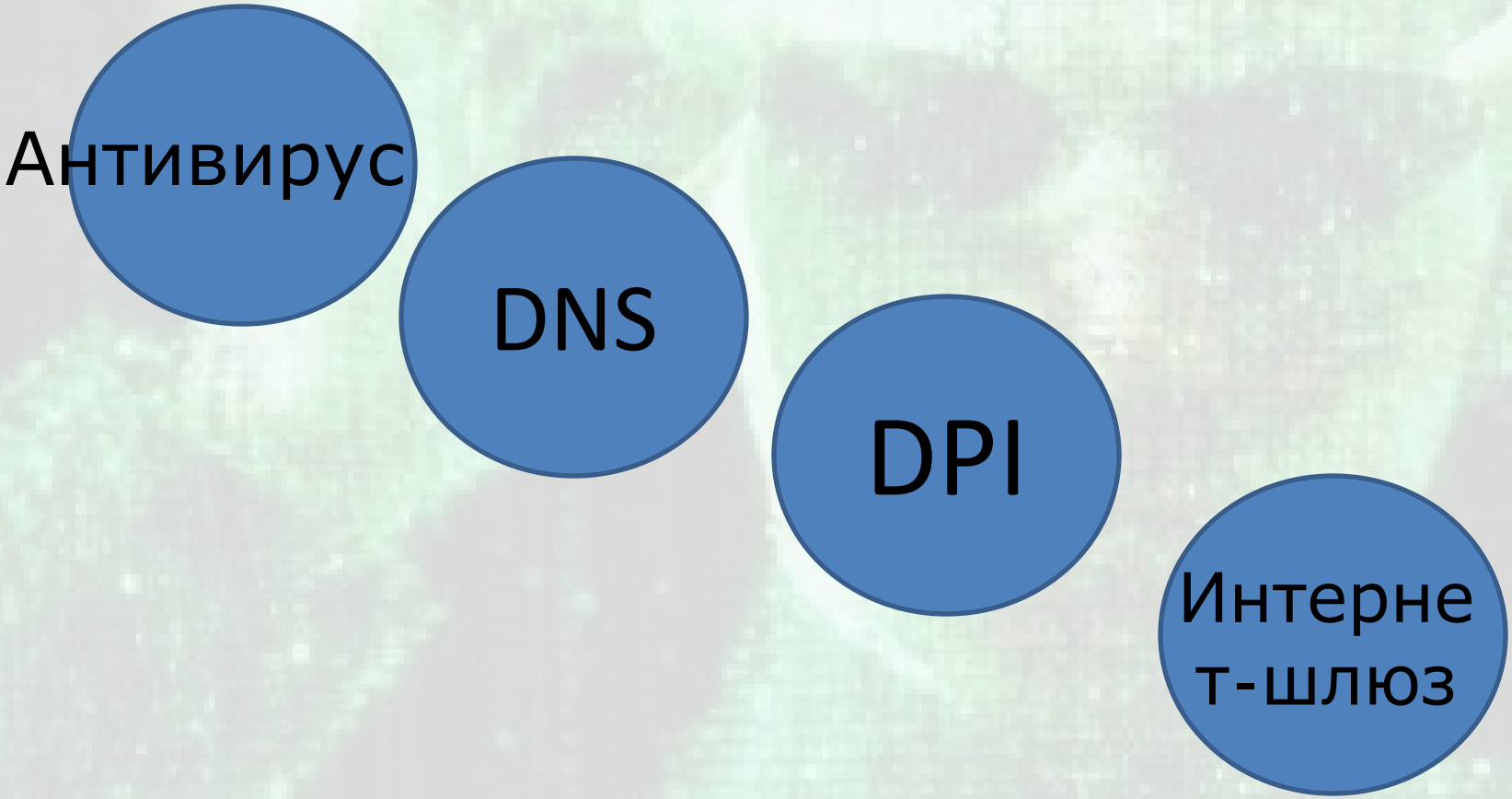
19

SPI (Shallow Packet Inspection)
-технология анализа трафика, основывающаяся на заголовке пакета (не анализирует содержимое полезной нагрузки пакета)



Access Control List, ACL - «разрешить/запретить»

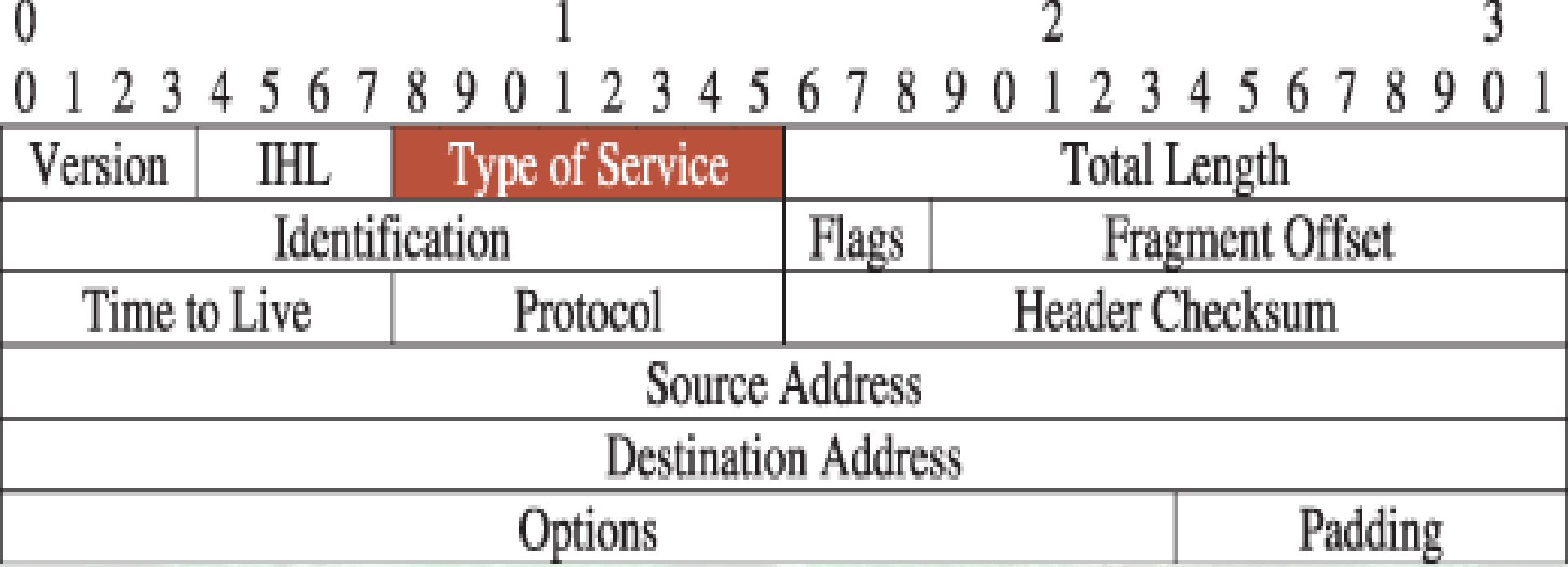
Типы систем фильтрации



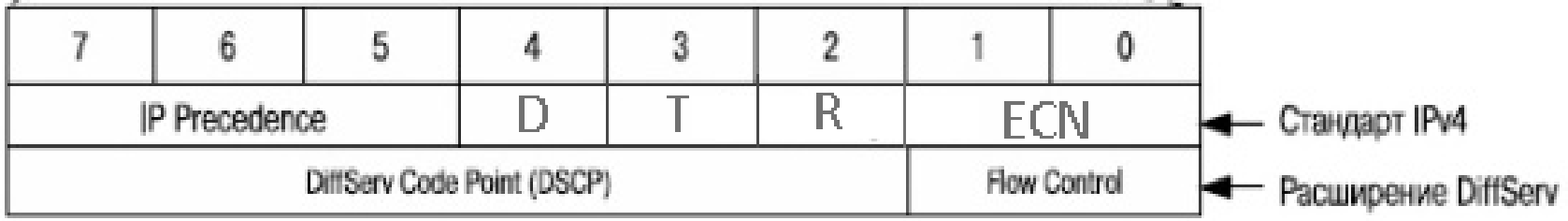
2. Дифференцированное обслуживание

Рекомендации ITU-T регулирующие QoS

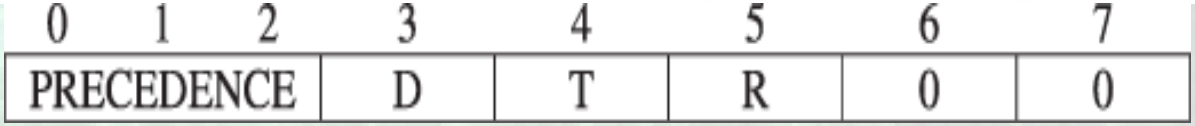
E.800	Термины качества обслуживания (QoS) и управлении им.
G.1000	Определение качества услуг связи, в различных структурах.
Y.1540	Параметры скорости, точности, надежности и доступности передачи IP-пакетов к сквозным IP-услугам и IP-услугам типа «точка–точка»
Y.1541	Классы QoS для SLA.


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding


Версия Длина
Байт ToS
Общая длина
Идентификация
Смещение
Время жизни
Протокол
Контрольная сумма заголовка
Адрес источника
Адрес приемника
Данные


7 6 5 4 3 2 1 0
IP Precedence
D
T
R
ECN
Стандарт IPv4
DiffServ Code Point (DSCP)
Flow Control
Расширение DiffServ

RFC-791


0 1 2 3 4 5 6 7
PRECEDENCE
D
T
R
0
0

Классические методы маркировки

DS5	DS4	DS3	DS2	DS1	DS0	ECN	ECN

Код DSCP — 6 бит (DS5-DS0)

ECN – явн. увед. о пер.(2 бита)

Рис.5 Структура поля DiffServ

Метка	EXP	S	TTL
20	3	1	8

Метка

EXP – поле эксп. битов

S – ср. подд. Иер. Стр. ст. меток

TTL – время жизни

Рис.6 Заголовок метки MPLS

TPID	Priority	CFI	VID
16	3	1	12

TPID – ид. пр. маркировки

Priority – приоритет

CFI – инд. канон. формата

VID – идент. виртуальной сети

Рис.7 Структура метки VLAN

- IP
- VLAN
- MPLS
- DPI

- Управление доступом
- Классификация трафика
- Организация очередей
- Маркировка пакетов

Характеристики сети	Классы QoS					
	0	1	2	3	4	5
Задержка доставки пакета	100 мс	400 мс	100 мс	400 мс	1 с	Н
Джиттер	50 мс	50 мс	Н	Н	Н	Н
Коэффициент потери пакетов	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	Н

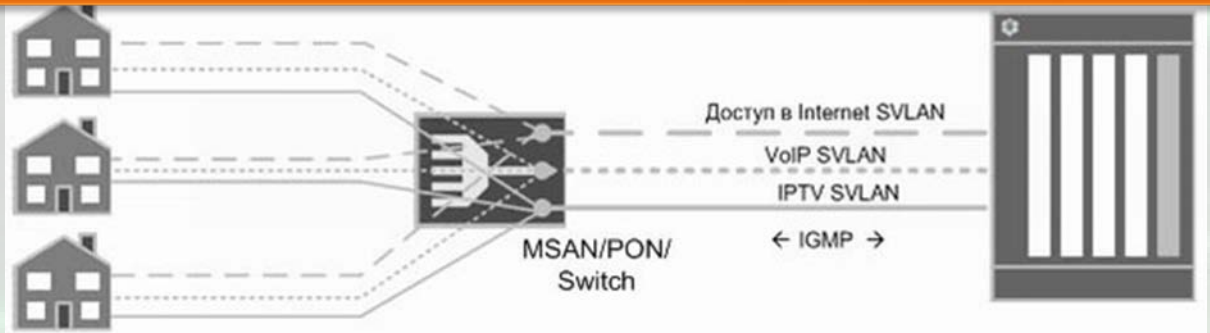
Y.1541

DIFFSERV – ДИФФЕРЕНЦИРОВАННОЕ ОБСЛУЖИВАНИЕ

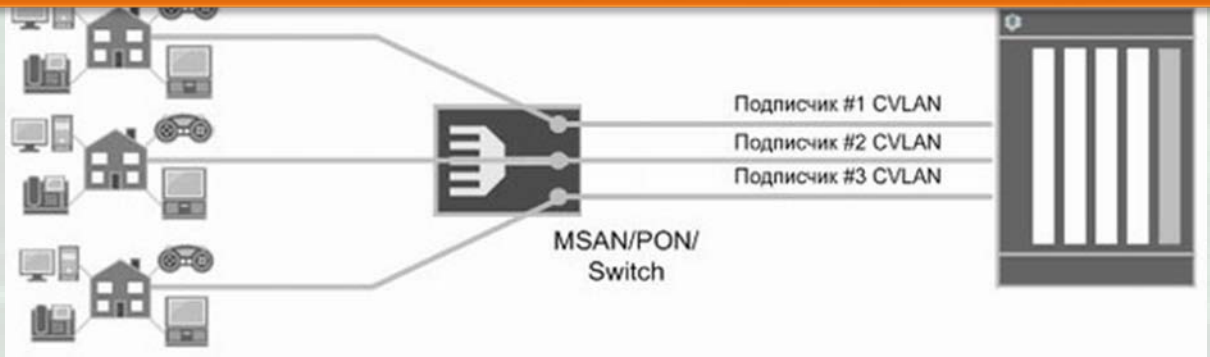
Особенности:	разделение трафика по классам, для каждого из которых определяется свой уровень QoS
	управление формированием трафика (классификация пакетов, маркировка, управление интенсивностью)
	управление политикой (распределение ресурсов, политика отбрасывания пакетов)

РАЗЛИЧНЫЕ МОДЕЛИ VLAN

Сервисный VLAN (S-VLAN) - каждая услуга находится в своем VLAN



Клиентский VLAN (C-VLAN) - каждый абонент находится в своем VLAN



ПРИМЕНЕНИЕ VLAN

Способы организации VLAN

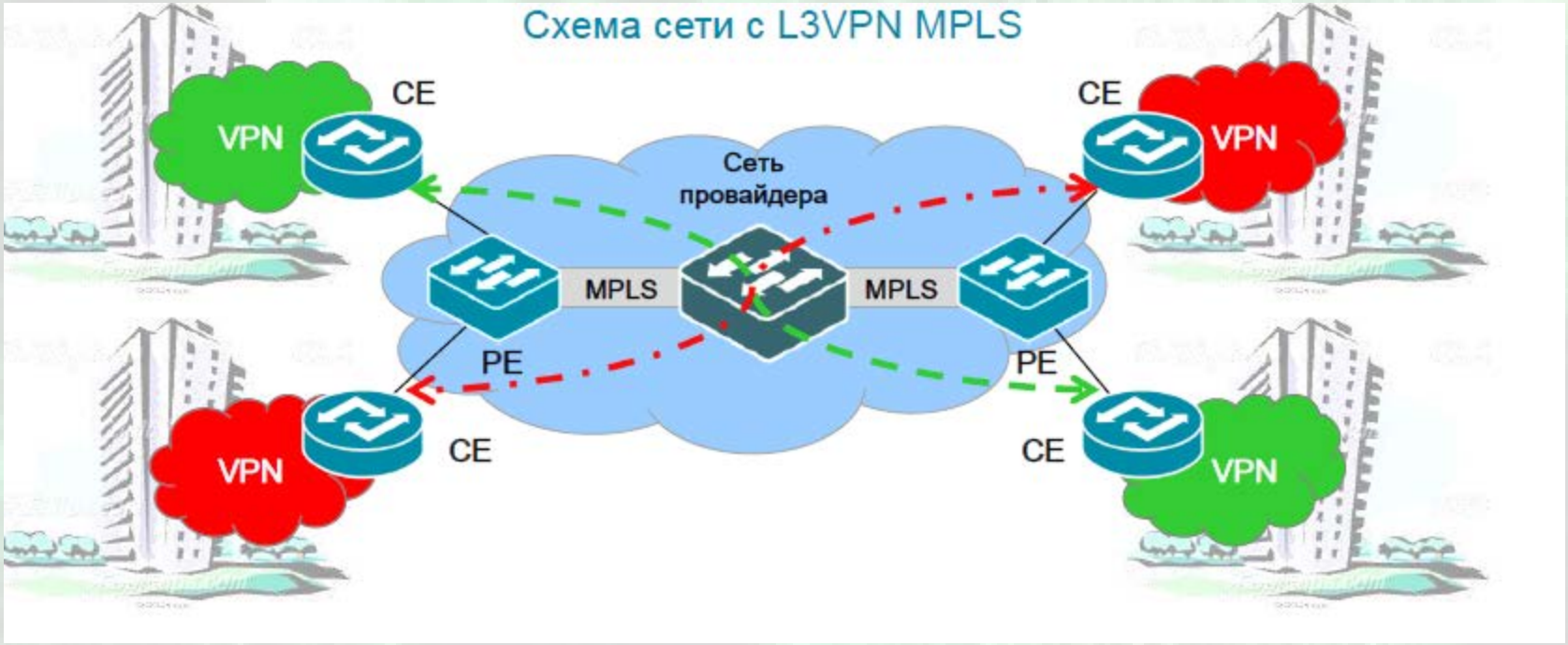
- На основе портов
- На основе MAC-адресов
- На основе протоколов сетевого уровня

Обеспечения QoS

- Классификация трафика
- Маркирование трафика
- Управление очередями
- Резервирование и профилирование

ТЕХНОЛОГИИ VLAN И MPLS

MPLS (Multiprotocol Label Switching) — многопротокольная коммутация по меткам



Коммутация каналов пропускной способностью до 10 Гбит/с

Применение технологии MPLS на уровне ядра и агрегации

30

Provider Backbone Bridges (IEEE 802.1ah)

PBB – Eth in Eth

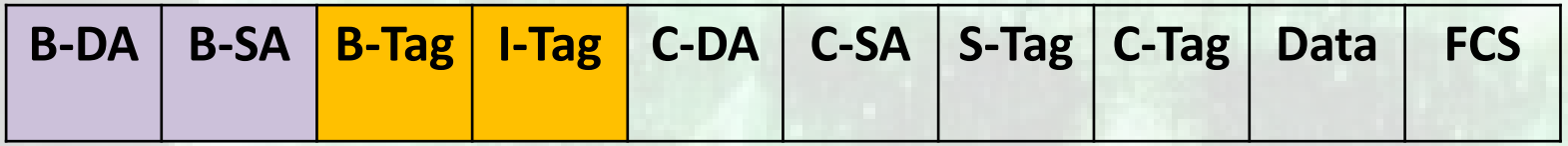


Рис. Структура заголовка PBB

- **B-DA - магистральный адрес получателя**
- **B-SA - магистральный адрес отправителя**
- **B-Tag - магистральный тег виртуальной сети**
- **I-Tag - тег экземпляра сервиса**
- C-DA - пользовательский адрес получателя
- C-SA - пользовательский адрес отправителя
- S-Tag - тег виртуальной сети провайдера
- C-Tag - тег виртуальной сети пользователя
- Data - данные
- FCS - контрольная последовательность кадра

Network Service Header (NSH)

Base Header
Service Path Header
Mandatory Context Header
Mandatory Context Header
Mandatory Context Header
Mandatory Context Header
Optional Variable Length Context Headers

Рис. Структура заголовка сетевой службы

- **Base Header – базовый заголовок**
- Service Path Header – заголовок пути обслуживания
- Mandatory Context Header – обязательный контекстный заголовок
- Optional Variable Length Context Headers - необязательная переменная длина контекстных заголовков

NSH. Base Header

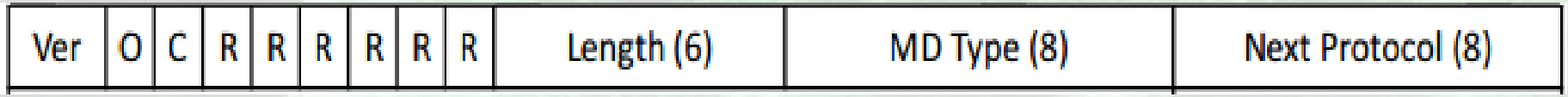


Рис. Структура базового заголовка NSH

- Ver– номер версии
- Флаги-биты (0, C, R)
- Length– общая длина NSH
- MD Type – тип NSH
- Next Protocol – следующий протокол

Cisco vPath

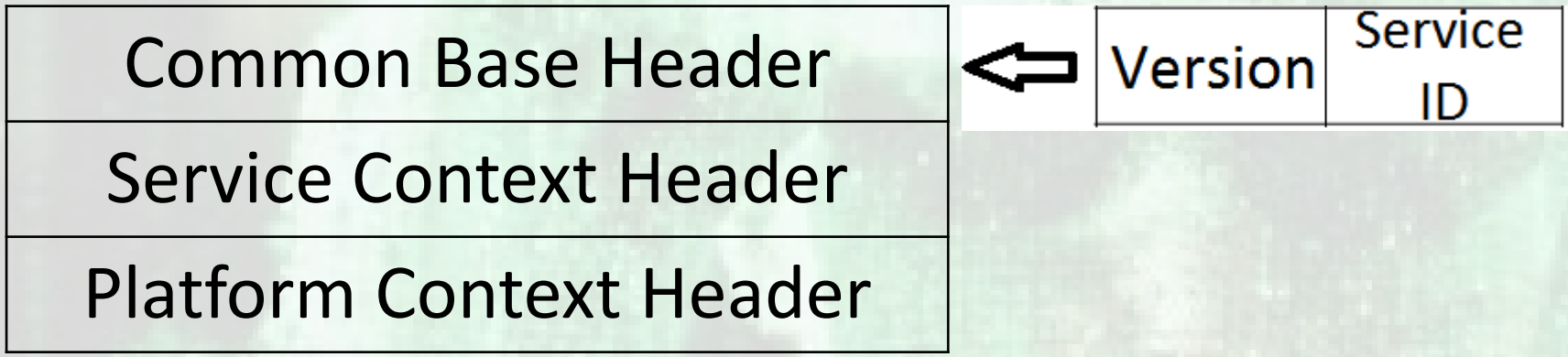


Рис. Структура заголовка vPath

- Common Base Header – общий базовый заголовок
- Service Context Header – сервисный заголовок
- Platform Context Header – платформенный заголовок

OpenFlow

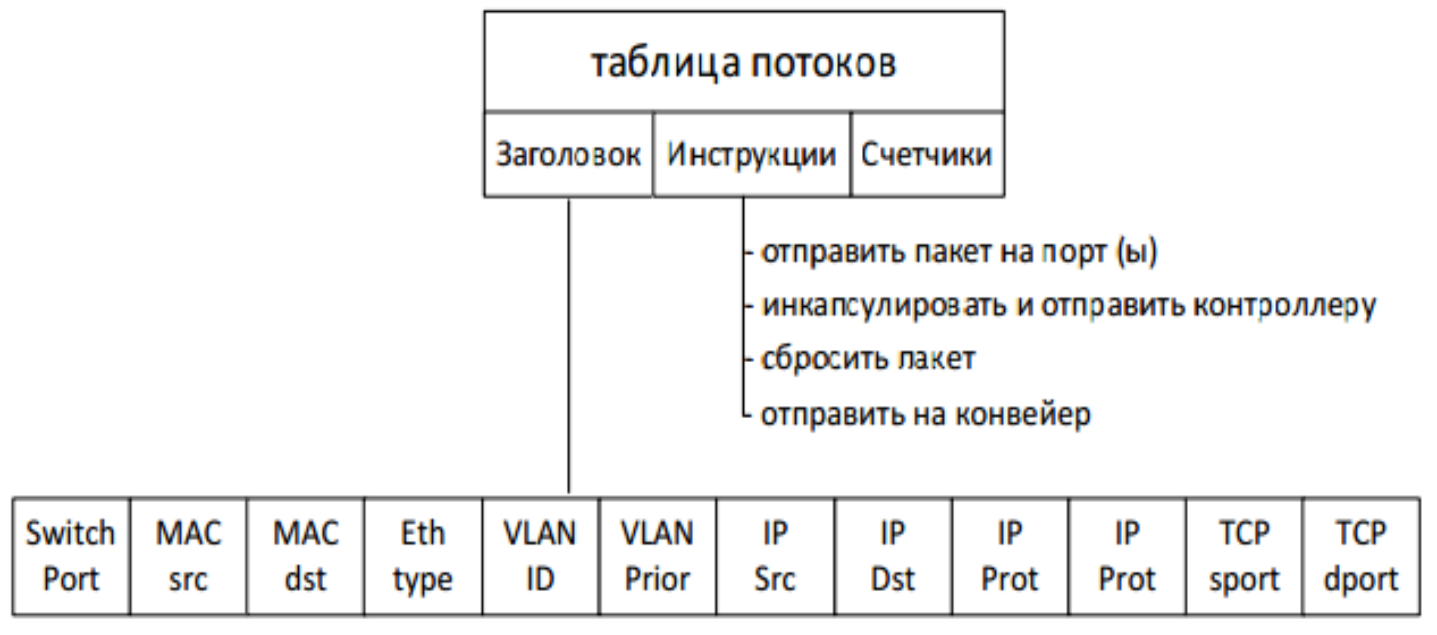


Рис. Таблица потоков и структура заголовка OpenFlow

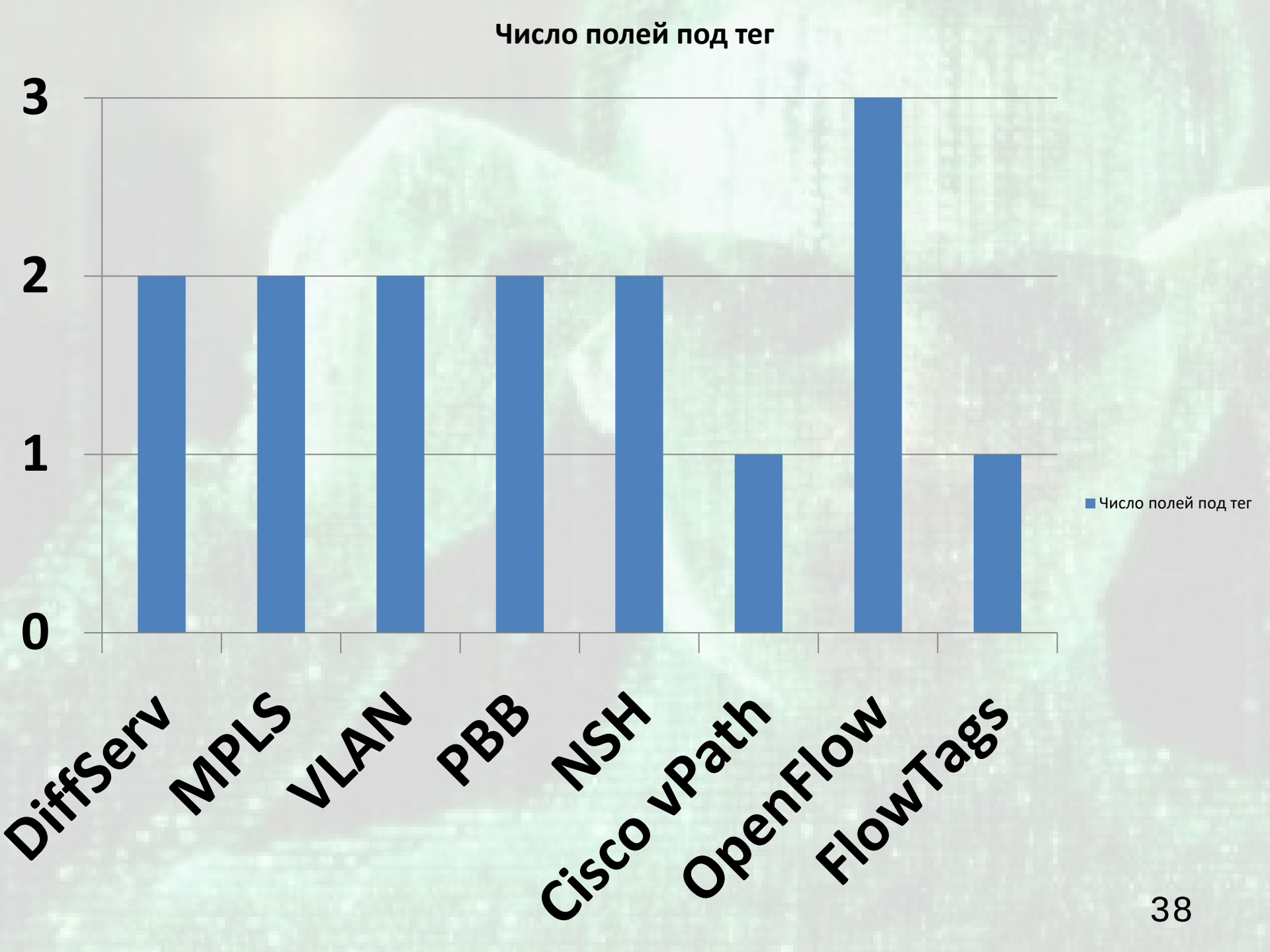
- FlowTags – расширение для OpenFlow, 2013

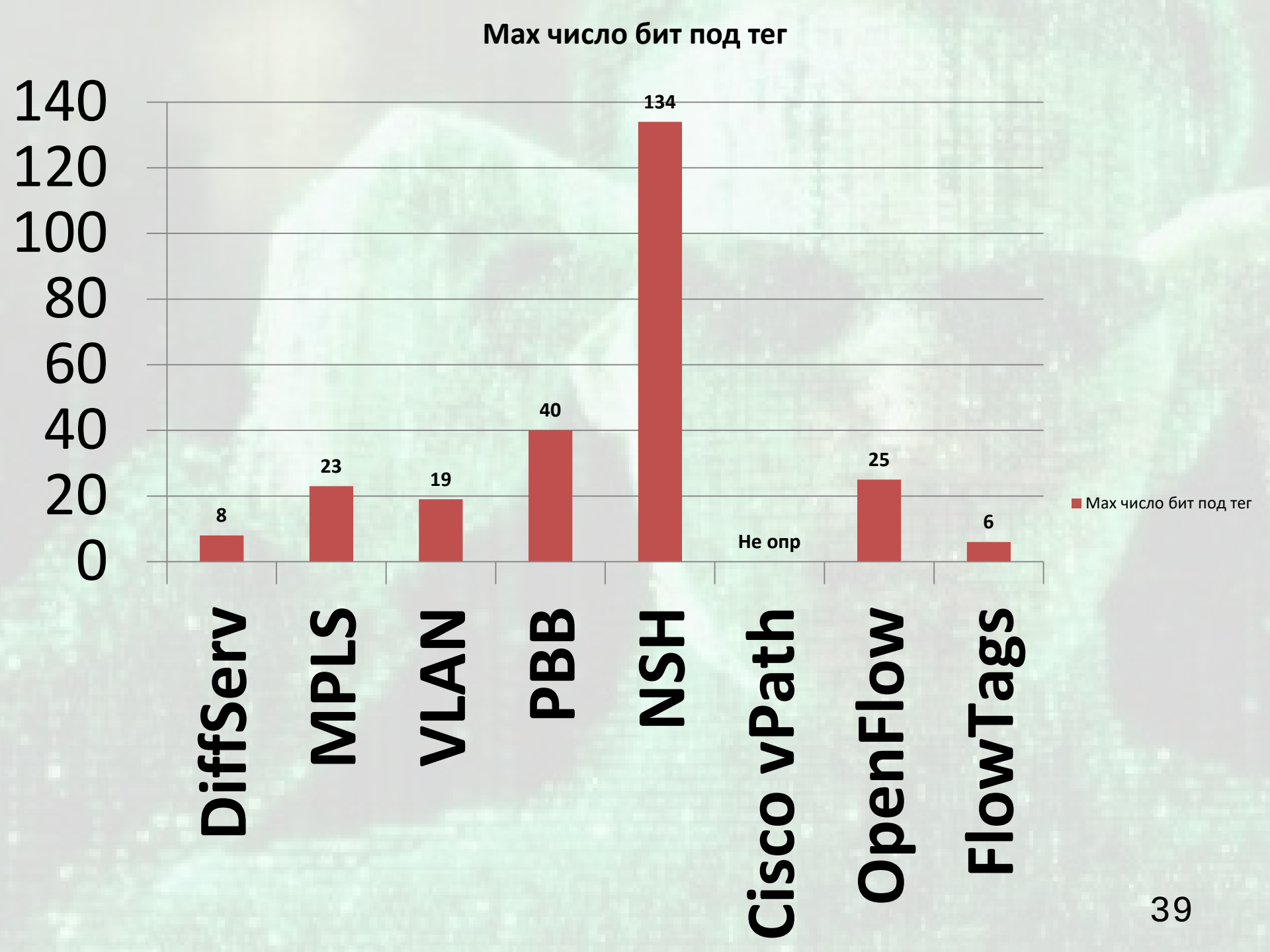
Сравнение методов маркировки

Методы/ критерии	Число полей под тег	Название полей под тег	Число бит в каждом поле	Max число бит под тег	Flow*	Инструкции (действия с потоком)
DiffServ	2	DSCP	6	8	-	-
		ECN	2			
MPLS	2	Метка	20	23	-	-
		EXP	3			
VLAN	2	TPID	16	19	-	-
		Priority	3			

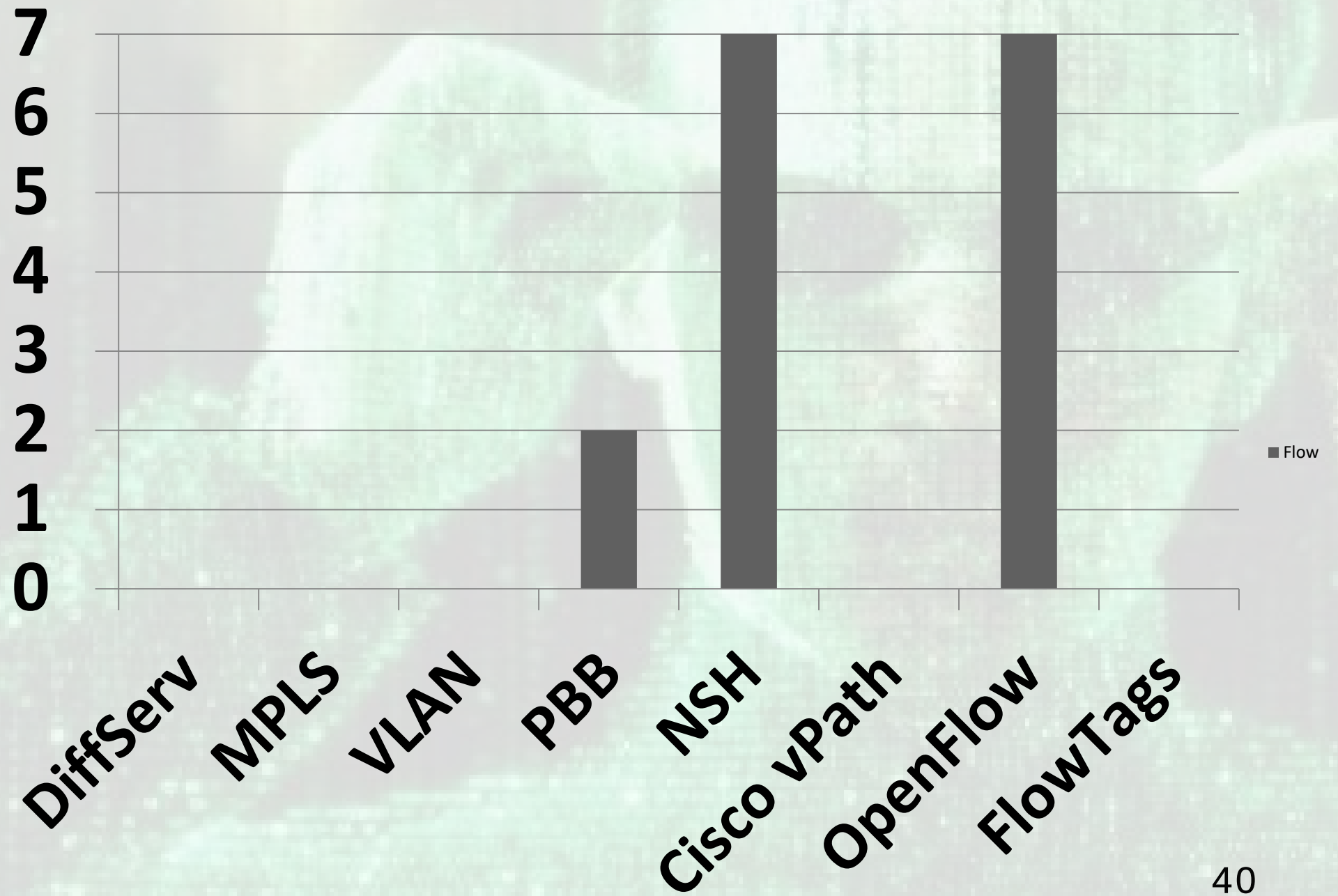
Сравнение методов маркировки

PBB	2	B-Tag	16	40	1, 2	-
		I-Tag	24			
NSH	2	Reserve	6	134	1-7	-
		Context Headers	128			
Cisco vPath	1	Service ID	Не определено	Не определено	-	-
OpenFlow	3	VLAN ID	16	25	1-7	+
		VLAN Priority	3			
		ToS	6			
FlowTags	1	ToS/DSCP	6	6	-	+


Число полей под тег
3
2
1
0
DiffServ
MPLS
VLAN
PBB
NSH
Cisco vPath
OpenFlow
FlowTags
Число полей под тег


Max число бит под тег
140
120
100
80
60
40
20
0
8
23
19
40
134
Не опр
25
6
DiffServ
MPLS
VLAN
PBB
NSH
Cisco vPath
OpenFlow
FlowTags
Max число бит под тег

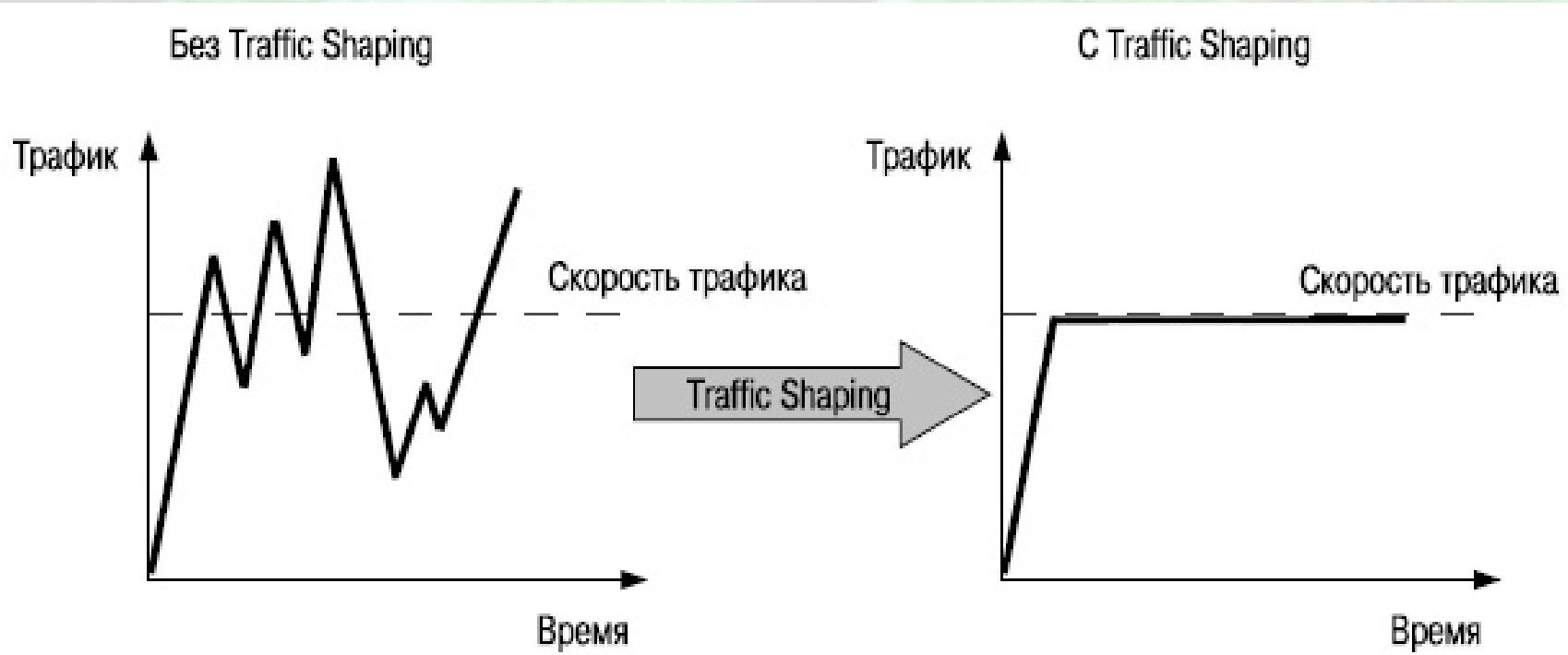
Передача данных о потоке



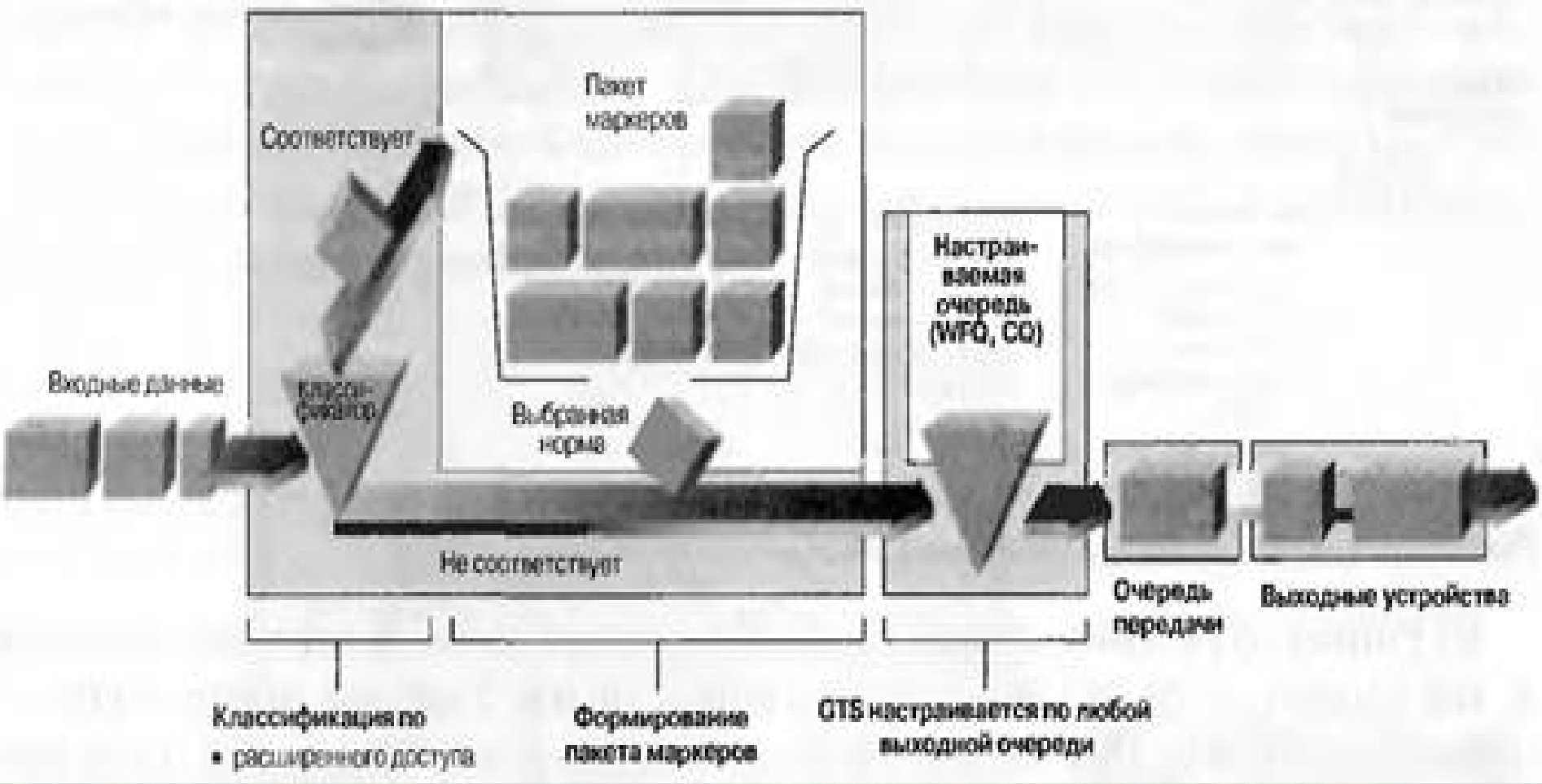
Правила обработки очередей

- **FIFO** (First In, First Out) – первый пришел – первый ушел;
- **WFQ** (Weighted Fair Queuing) – механизм взвешенной справедливой буферизации – ограниченная пр. сп. на выходе узла между потоками;
- **CBQ** (Class-Based Queuing) – механизм классификации потоков по классу обслуживания – в разных очередях. Каждой очереди выделяется доля пр. сп.
- **CBWFQ** (Class-Based Weighted Fair Queuing) – справедливое, взвешенное управление очередями на основе классов –классы по критериям, (ACL, входящий интерфейс, протокол и др.)
- **LLQ** (Low-Latency Queuing) – разновидность механизма CBWFQ - выделенная очередь для чувствительного к задержке, такого как голос или видео;


Без Traffic Policing
Трафик
Скорость трафика
Время
Traffic Policing
С Traffic Policing
Трафик
Скорость трафика
Время


Без Traffic Shaping
Трафик
Скорость трафика
Время
Traffic Shaping
С Traffic Shaping
Трафик
Скорость трафика
Время

фрагментация и чередование пакетов LFI



LPI

44

Методы классификации:

1. Системы дифференцированного обслуживания
2. Анализ по портам
3. Облегченный анализ пакетов (Lightweight Packet Inspection)
4. Средний анализ пакетов
5. Глубокого анализа пакетов (Deep Packet Inspection)
6. URL фильтрация
7. Технологии Data Mining

45

Анализ результатов исследования алгоритма PortLoad

	Точность по определению приложения		Точность по определению категории приложения	
Классификатор	сессии	байты	сессии	байты
Port-based	19,57%	25,12%	15,95%	23,89%
PortLoad	74,24%	97,83%	73,88%	97,45%

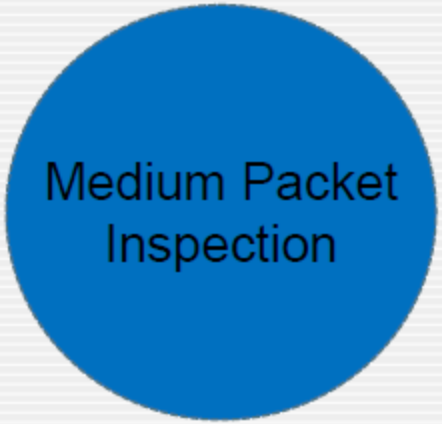
Классификатор	Среднее время(мкс)	Среднее время (в сравнении с port-based)
L7-filter	211,4	85,2
Port-based	2,48	1,0
PortLoad	6,99	2,8

PortLoad - анализ первых неск. байт данных

MPI

История развития DPI

Средний анализ пакетов



Medium Packet Inspection – технология анализа трафика, основывающаяся на инспектировании сессий и сеансов связи инициированных приложением, но устанавливаемых шлюзом-посредником. Как правило, название технологии MPI замещается обозначением «application proxy».

Частично анализирует содержимое пакетов по предопределенным правилам. Не используются сложные методы анализа (сигнатурный и т.д.)

Так же является одной из форм брандмауэра.

MPI позволяет заблокировать
- flash-файлов
-картинок с определённых интернет сервисов
(на уровне представления OSI)

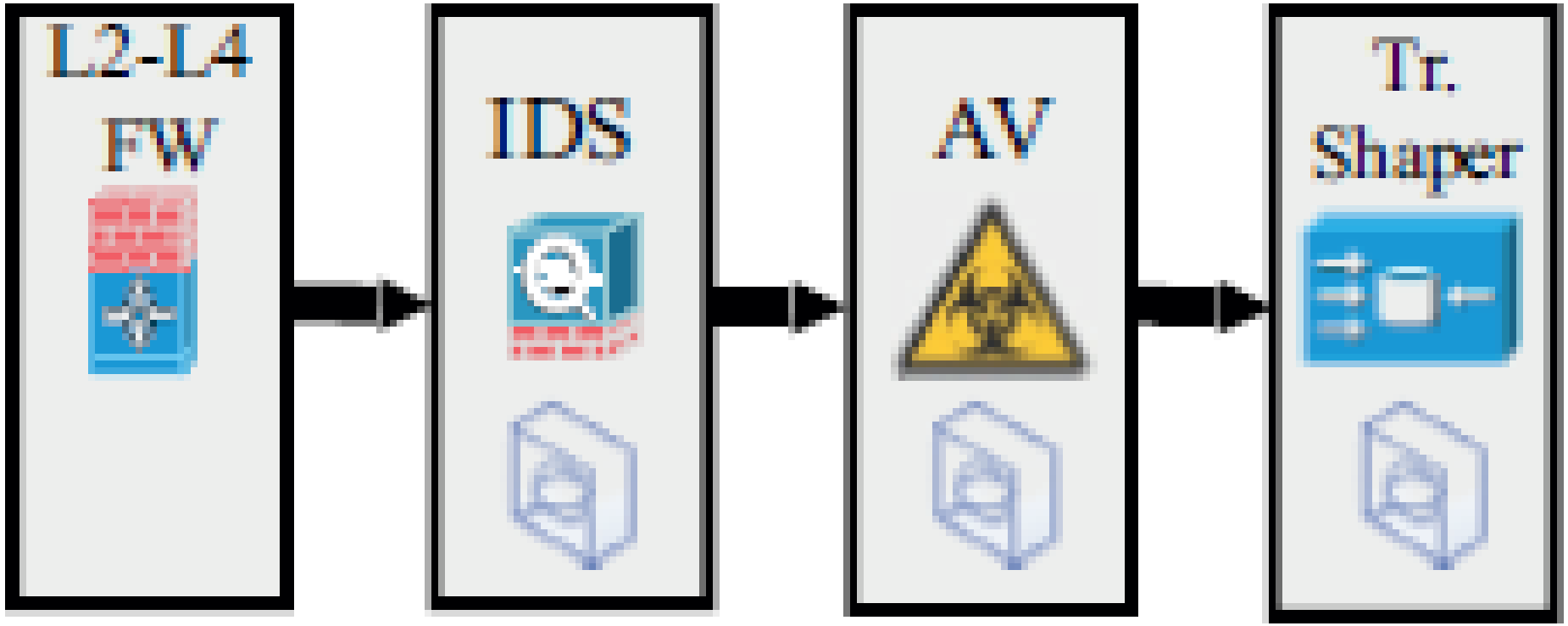
или заблокировать
-часть команд (на уровне приложения OSI) в
отдельных протоколах.

Набор протоколов, как правило, очень ограничен.

49

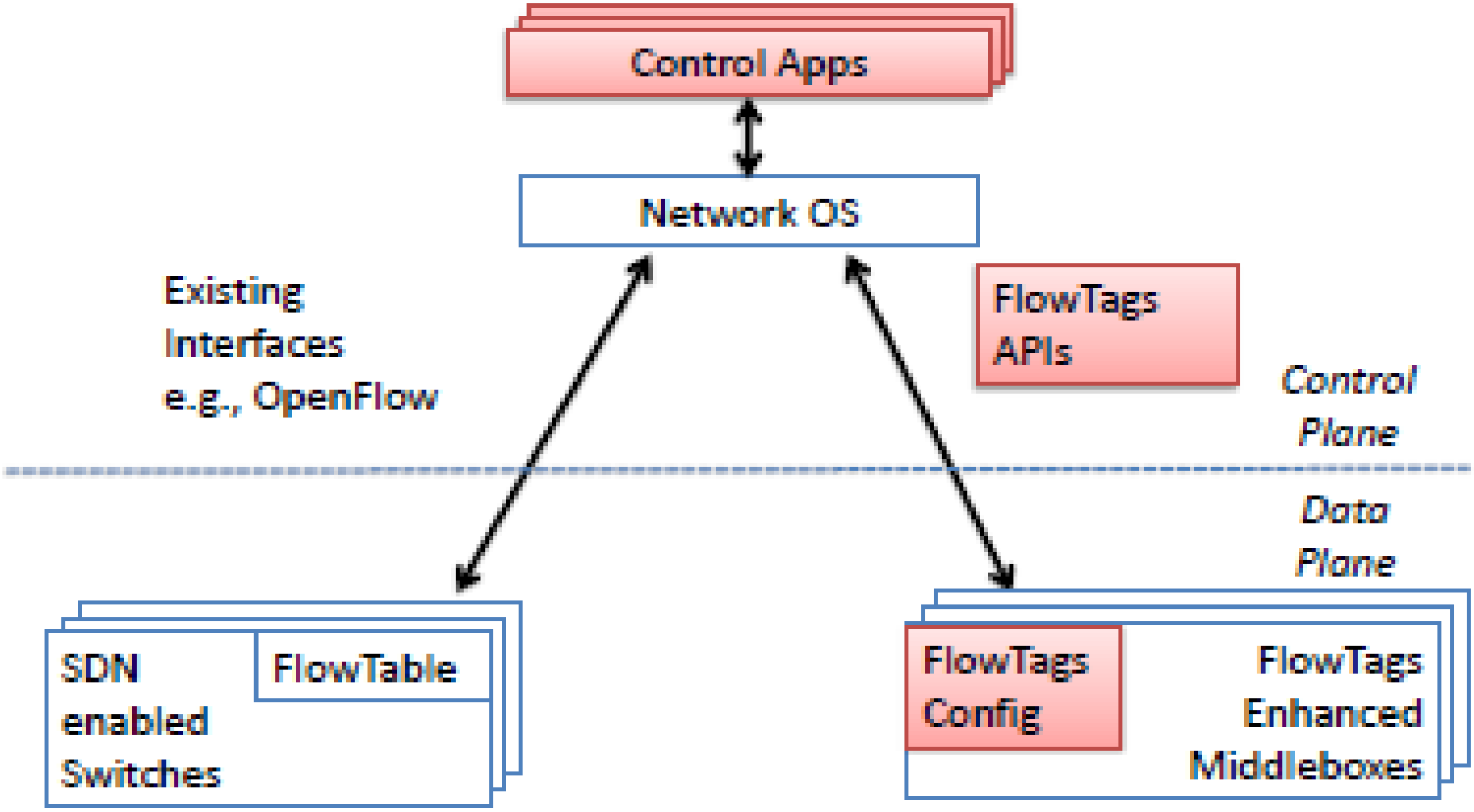
Middle Boxes

Middlebox – система обнаружения вторжений(IDS), антивирус/антиспам, traffic shaper и др.



51

Архитектура SDN-сети с расширением FlowTags



DPI

Определение DPI и DPP

Deep Packet Inspection (сокр. DPI) — совокупное название технологии, позволяющей проводить накопление, анализ, классификацию, контроль и модификацию сетевых пакетов в зависимости от их содержимого в реальном времени.

Определение DPI и DPP

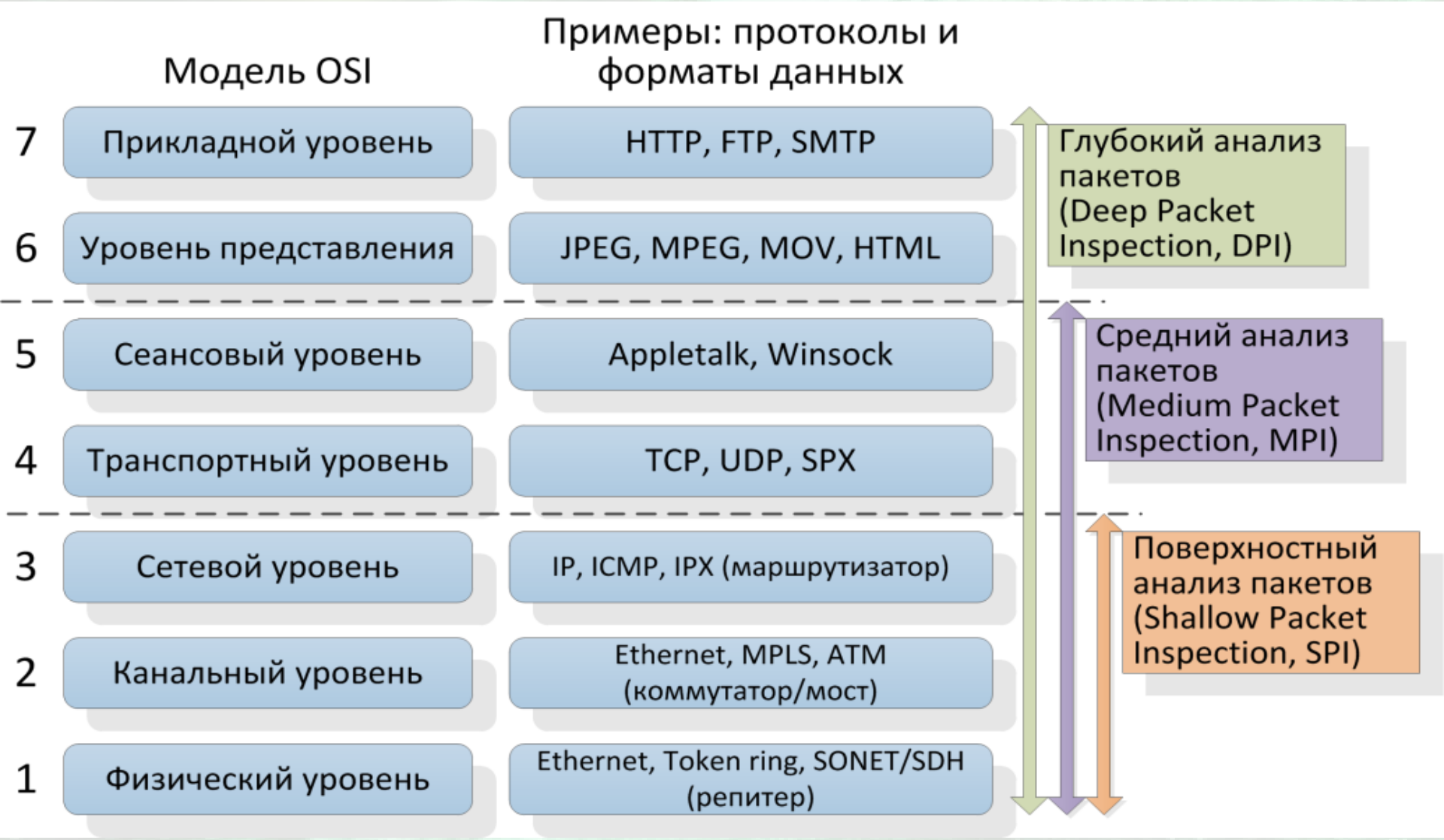
Иногда употребляют более узкий термин — DPP (Deep Packet Processing), который подразумевает такие действия над пакетами, как модификация, фильтрация или перенаправление.

Сегодня оба термина — DPI и DPP — часто используются как взаимозаменяемые.

История развития DPI

Модель развития DPI

Технологии инспекции трафика развивались последовательно, каждая последующая наследовала часть предыдущих механизмов и добавляла свои….


Модель OSI
Примеры: протоколы и форматы данных
7
Прикладной уровень
HTTP, FTP, SMTP
6
Уровень представления
JPEG, MPEG, MOV, HTML
5
Сеансовый уровень
Appletalk, Winsock
4
Транспортный уровень
TCP, UDP, SPX
3
Сетевой уровень
IP, ICMP, IPX (маршрутизатор)
2
Канальный уровень
Ethernet, MPLS, ATM (коммутатор/мост)
1
Физический уровень
Ethernet, Token ring, SONET/SDH (репитер)
Глубокий анализ пакетов (Deep Packet Inspection, DPI)
Средний анализ пакетов (Medium Packet Inspection, MPI)
Поверхностный анализ пакетов (Shallow Packet Inspection, SPI)

57

Многоликий DPI

Современные решения использующие технологию DPI

Отличие DPI систем от брандмауэра

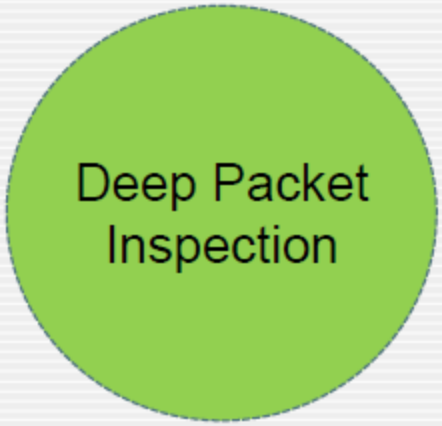
- DPI система анализирует не только заголовки пакетов, но и полное содержимое трафика на уровнях модели OSI со второго и выше.
- DPI система может принимать решение не только по содержимому пакетов, но и по косвенным признакам, присущим каким-то определённым сетевым программам и протоколам. Для этого может использоваться статистический анализ (например статистический анализ частоты встречи определённых символов, длины пакета и т.д.).
- DPI система в отличии от брандмауэра применяет различные модели действий над трафиком (классификация, ограничение полосы, приоритезация, маркировка, кэширование и т.д.)

Модель OSI и DPI

Уровень	Модель OSI	Назначение	Объект управления	Возможность обработки Proxy	Возможность обработки Брандмауэр	Возможность обработки DP
7	Прикладной	Доступ приложений к сетевым службам	Данные	Частично (application-level proxy)		Да
6	Представления	представление и кодирование данных	Данные	Частично (application-level proxy)		Да
5	Сеансовый	Управление сеансом связи	Данные	Да (application-level proxy)	Да (Stateful Packet Inspection)	Да
4	Транспортный	Соединение т-т, контроль передачи данных	Блоки	Да (application-level proxy)	Да	Да
3	Сетевой	Маршратизация, управление потоками данных	Пакеты	Да (transparent - level proxy)	Да (Stateless)	Да
2	Канальный	MAC- управление доступом к середе (коммутация), LLC - Контроль логической связи (формирование кардров)	Кадры		Да	Да
1	Физический	Физическая среда (битовые протоколы передачи данных)	Биты			

История развития DPI

Глубокий анализ пакетов



Технология DPI возникла из-за необходимости анализировать, контролировать и управлять передаваемым трафиком. Технология DPI получила развитие, прежде всего, из-за стремительного роста вычислительных способностей чипов (процессоров), их быстродействия.

Внедрение DPI

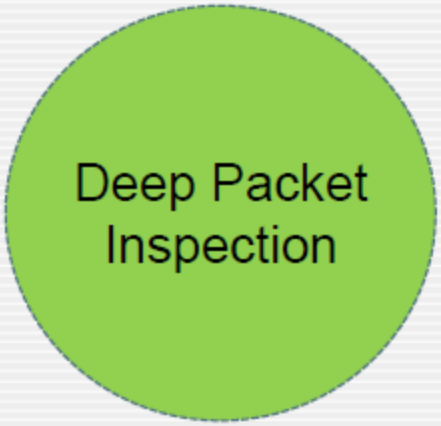
Три основных причины внедрения DPI

Внедрение DPI

Основные направления применения DPI систем управления трафиком

История развития DPI

Поколения DPI систем



В некоторых источниках встречается информация о поколении DPI систем управления трафиком. Отмечается два поколения таких устройств:

- Первое поколение: было приспособлено для решения более узких задач и имело только сигнатурный механизм анализа.
- Второе поколение: более универсальные и масштабируемые устройства с анализом имеющим эвристический и поведенческий механизмы, имеющие в своём составе инструменты классификации и управлениями политиками.

Иногда разделяют по поколениям исходя из производительности устройств: 1-ое поколение до 10Гибит/с, второе от 10 до 100 и третье поколение более 100.

Типовая идентификация трафика

Используемые порты

Proxy – DNS имя

Протокол/ID (TCP/UDP/…)

IP адреса (SRC/DST)

MAC-адреса

Основные идентификаторы управления трафиком в коммутаторах, маршрутизаторах, брандмауэрах позволяющие настроить ACL или QoS

DPI средства управления трафиком

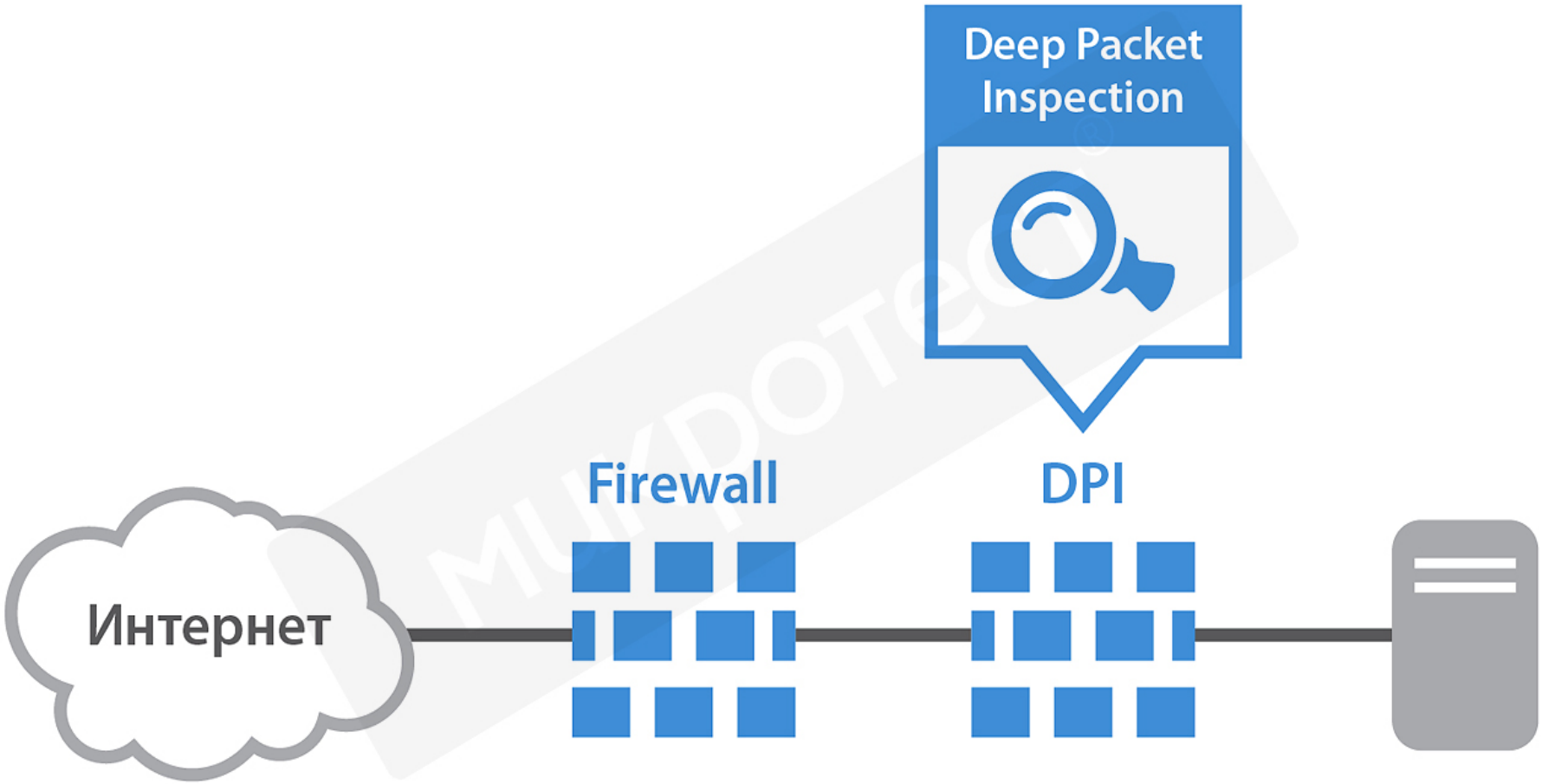
DPI средства управления трафиком

Инструмент контроля с расширенными политиками

Помимо стандартных инструментов контроля/управления трафиком – ACL и QoS, DPI системы управления трафиком имеют их расширенный функционал – политики. Политики основаны на динамическом изменении правил в зависимости от времени, объемов того или иного трафика, поведения трафика и т.д.

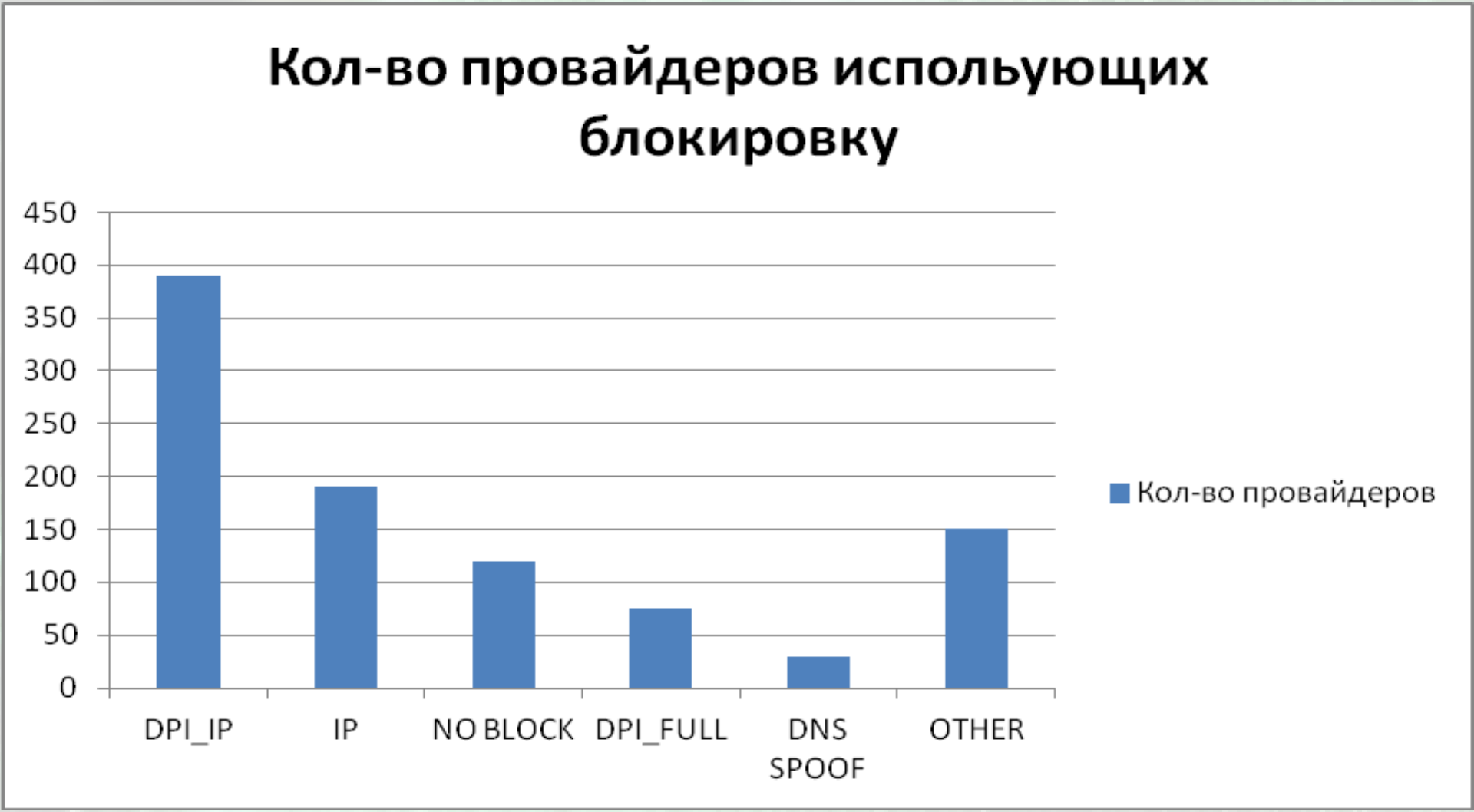
Политики контроля и обработки правил могут создаваться и изменяться как администратором системы, так и быть загруженными от производителя.

Возможно применение политик на географически разобщенный кластер устройств.



68

2015


Кол-во провайдеров испольующих блокировку
450
400
350
300
250
200
150
100
50
0
DPI_IP
IP
NO BLOCK
DPI_FULL
DNS SPOOF
OTHER
Кол-во провайдеров

69

Проблема шифрования

Обработка ***неизвестностного*** трафика

выявление ***P2P*** трафика

Спасибо за внимание.

Вопросы?

Ст. преп. каф. Инфокоммуникационных систем СПбГУТ,

Фицов Вадим Владленович,