

IPv6-трафик в сетях

IPv4

П.О. Ковалёв, Е.В. Хазанкин

Celebrating New Year 2016 with 10% IPv6!



Projection of IPv6 %-age of IPv6-Enabled Web Browsers (**courtesy Google**) in World Wide

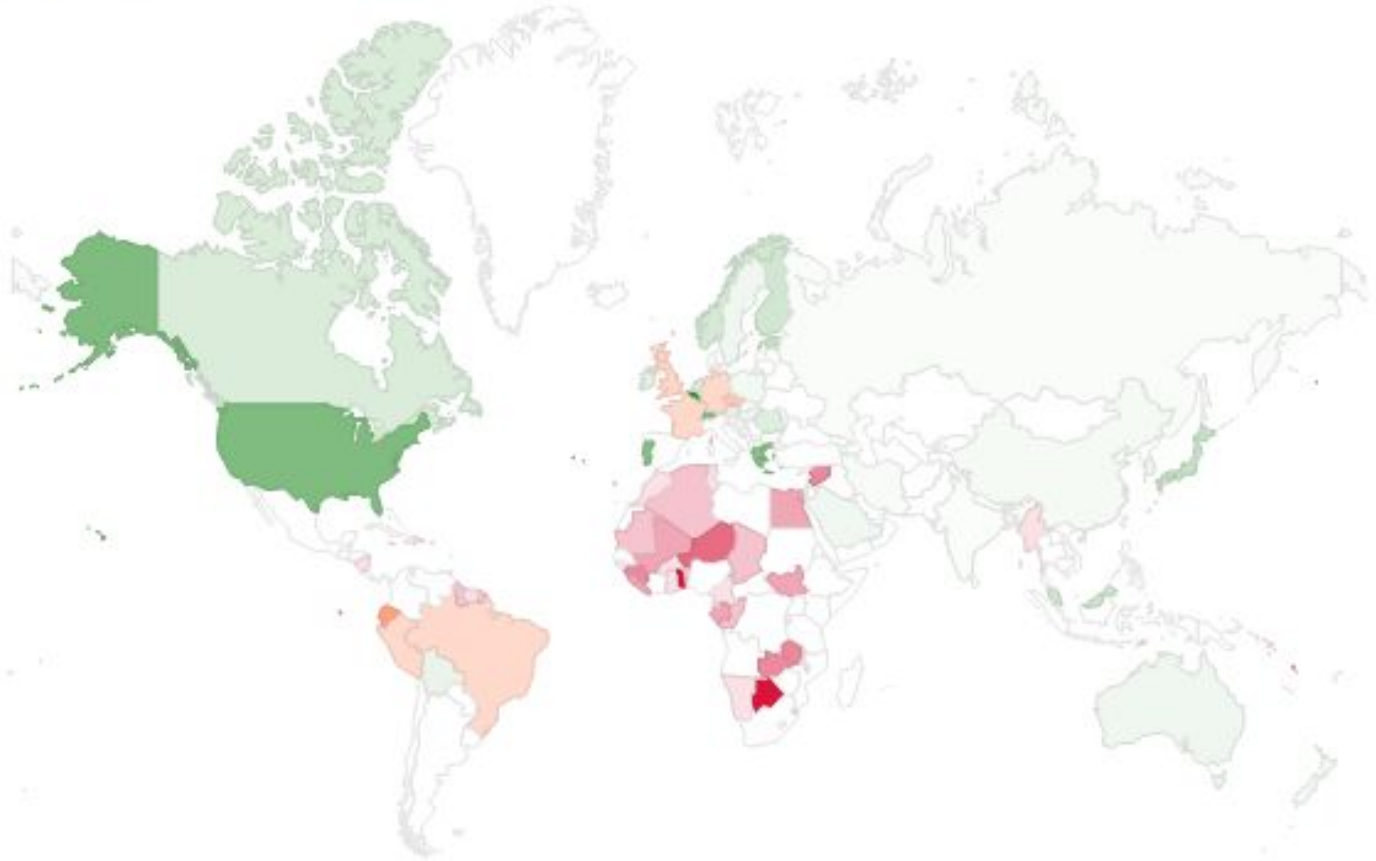
World Wide Projection ~15% (April 11, 2017)

Celebrating New Year 2016 with 10% IPv6!

IPv6 Adoption

Per-Country IPv6 adoption

Per-Country IPv6 adoption



Internet Peering Ecosystem

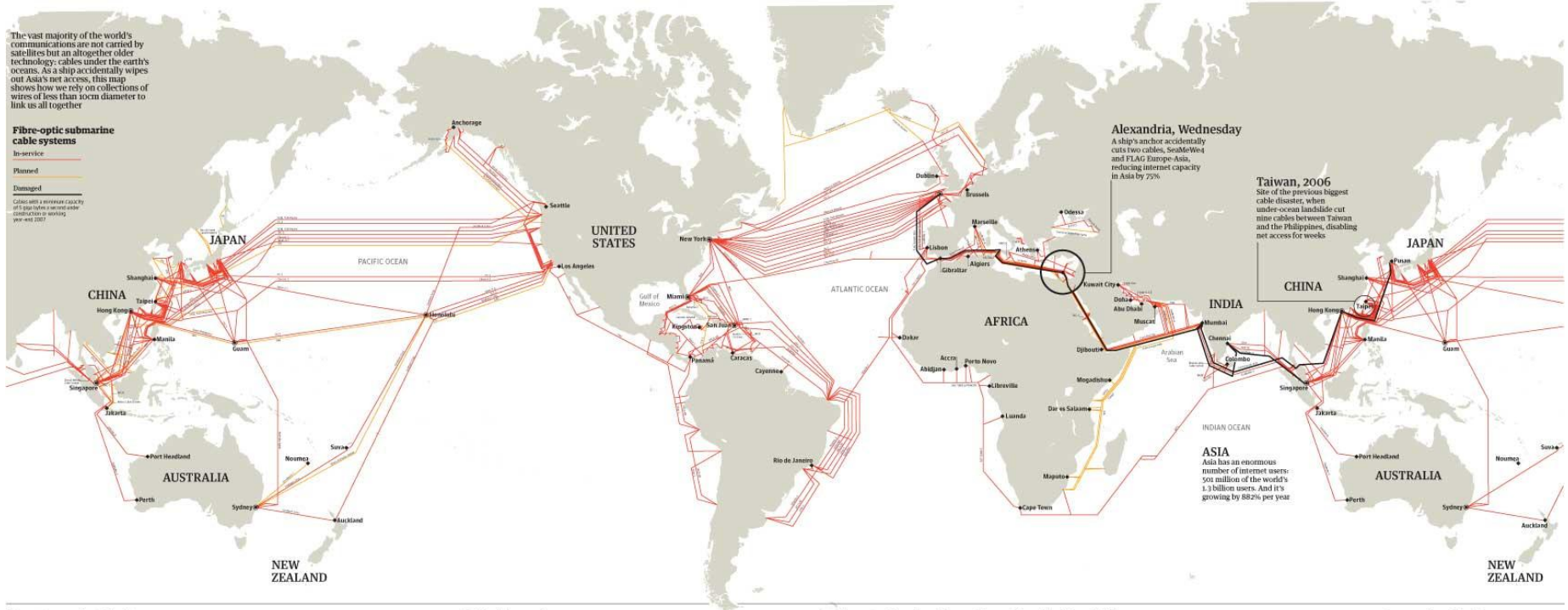
The internet's undersea world

The vast majority of the world's communications are not carried by satellites but an altogether older technology: cables under the earth's oceans. As a ship accidentally wipes out Asia's net access, this map shows how we rely on collections of wires of less than 1cm diameter to link us all together

Fibre-optic submarine cable systems

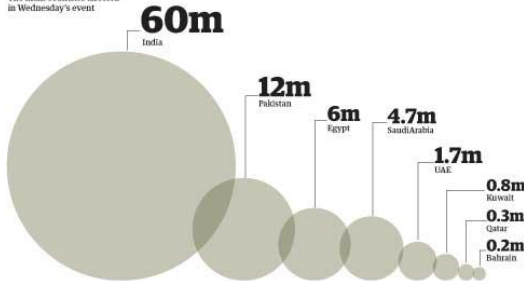
In-service
Planned
Damaged

Cables with a minimum capacity of 100 Gbps are marked under construction or pending (year-end 2007)



Internet users affected by the Alexandria accident

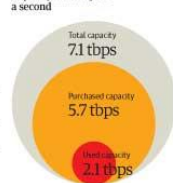
The main countries affected in Wednesday's event



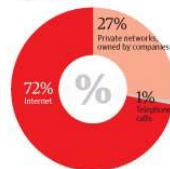
World cable capacity

Submarine cable operators light (turn on) capacity on their systems to sell bandwidth to other carriers. Carriers buy extra capacity, mainly to hold in reserve. On the trans-Atlantic route 80% of the bandwidth is purchased, but only 29% is used

Capacity in terbytes a second



What makes up "used capacity"?



The longest submarine cables

The SeaMeWe-3 system from Norden in Germany to Rango, South Korea connects 30 different countries with 30 landing points

SeaMeWe-3	39,000 km
Southern Cross	30,500 km
China-US	30,476 km
FLAG Europe-Asia	28,000 km
South America-1	25,000 km

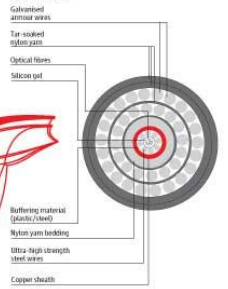
The world's cables in bandwidth

The first intercontinental telephony submarine cable system, TAT-1, connected North America to Europe in 1958 and had an initial capacity of 640,000 bytes per second. Since then, total trans-Atlantic cable capacity has soared to over 7 trillion bps

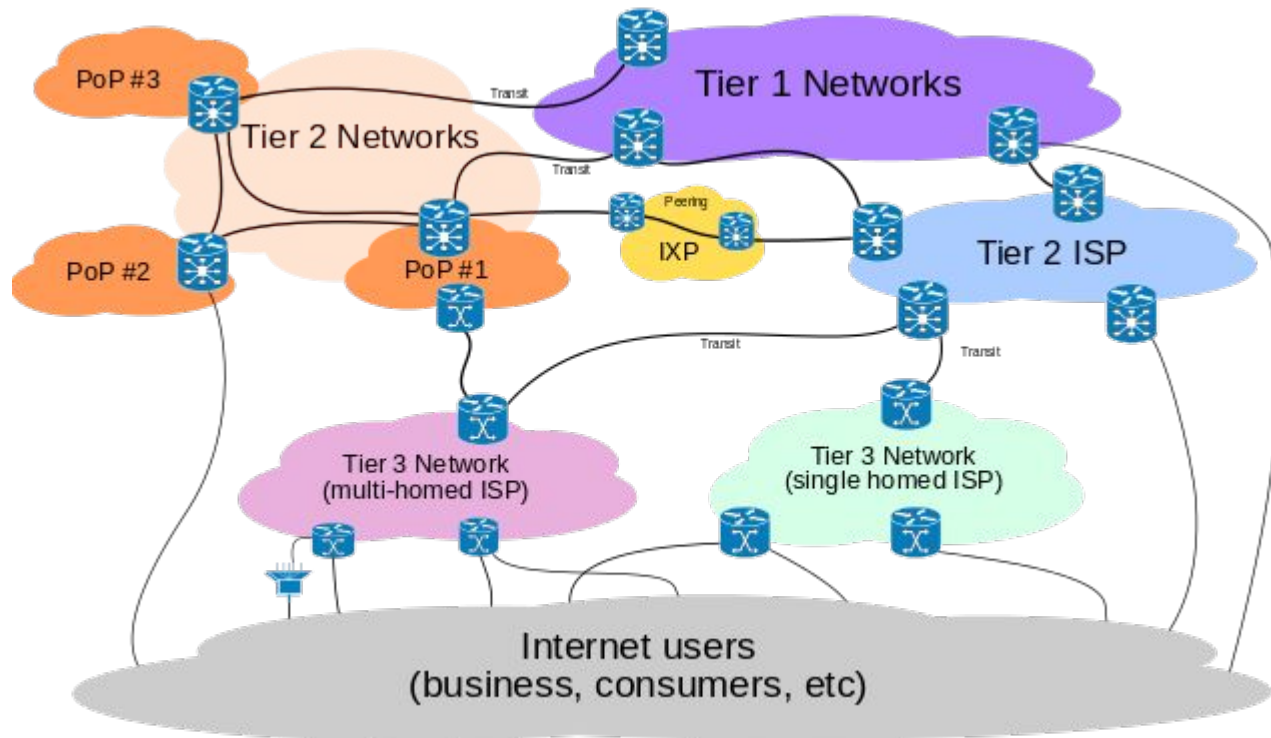


Cross-section of a cable

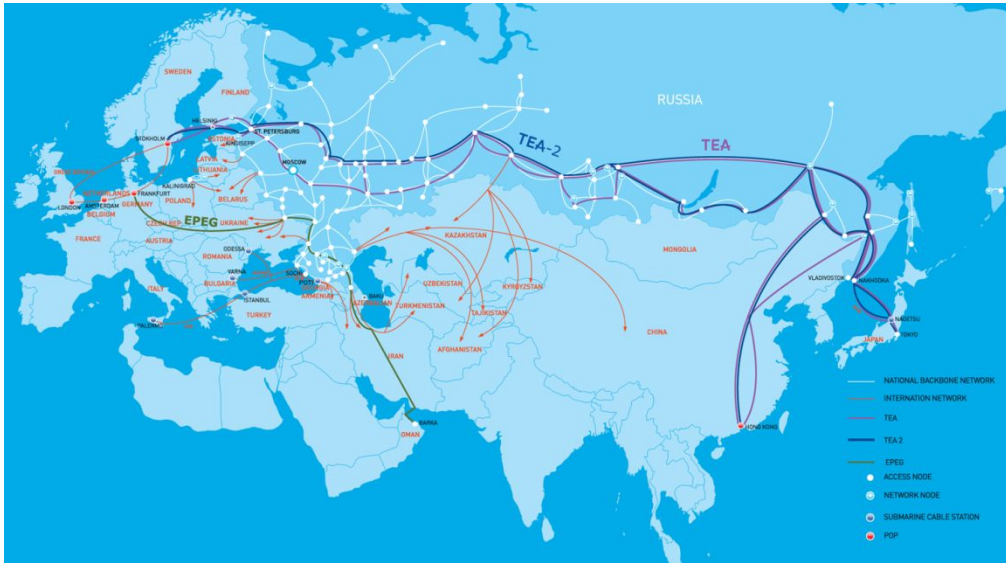
Cables of this strength are typically 60 mm in diameter and weigh over 10,000 kilograms a kilometer. In deeper waters, lighter and less insulated cables are used



Internet Peering Ecosystem



Runet Peering Ecosystem



Каким образом IPv6-трафик присутствует в IPv4-

IPv4 Header

Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
Time to Live	Protocol	Header Checksum		
Source Address				
Destination Address				
Options			Padding	

Legend

- Field's Name Kept from IPv4 to IPv6
- Fields Not Kept in IPv6
- Name and Position Changed in IPv6
- New Field in IPv6

IPv6 Header

Version	Traffic Class	Flow Label		
Payload Length		Next Header	Hop Limit	
Source Address				
Destination Address				

Каким образом IPv6-трафик присутствует в IPv4-

Dual stack



IPv6 host



IPv6 host

Идеальный мир



Dual-stack host



IPv6 host



IPv4 host

Реальный мир



Dual-stack host



IPv6 host



IPv4 host

Еще более реальный мир

Redefining Flow Label in IPv6 and MPLS Headers for End to End QoS in Virtual Networking for Thin Client

Mohammad Aazam¹, Adeel M. Syed², Eui-Nam Huh³
Innovative Cloud and Security Lab, Department of Computer Engineering
Kyung Hee University, Suwon, South Korea.
²Bahria University, Islamabad, Pakistan
¹aazam@ieee.org
²adeelmuzaffar@gmail.com
³johnhuh@khu.ac.kr

Abstract— Applications that require timeliness such as; video conferencing, Voice over IP (VoIP), Video-on-Demand (VoD) etc., require quantified and well managed Quality of Service (QoS). For this, the flow label field in IPv6 header and the Label field in MPLS header should be used for efficient QoS provisioning. In this paper, flow label specifications were first investigated and then a new structure is proposed for QoS provisioning. The 20-bit field in IPv6 as well as MPLS is meant to provide QoS, other than labeling or identification purpose. But its usage is not standardized and defined that how these 20-bits must effectively be used to provide maximum possible QoS in a better way. This paper discusses it by proposing portions for QoS by explicitly specifying bandwidth, delay, and packet loss. By keeping the QoS parameters open in this way, it would be easy for a flow to decide what to reserve and how much to reserve. After that, mapping of flow label with class fields of IPv6 and MPLS is presented. In virtual networks, specially for Thin client, service quality degradation is a major issue, when IPv4-IPv6 virtual networks co-exist. This is also where this redefinition can come very handy.

Keywords—Flow label; IPv6; MPLS; QoS; virtual networking; Thin client

is considered to be the best available and most efficient combination of protocols on layer 2 and layer 3 for routing of packets. So, the same specification of label field can be used with both these protocols to allow the stability in QoS for a particular flow, throughout the communication, from MAC to the network layer. A 'flow' can be defined as a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling for QoS by the intermediate routers [8]. The flow is uniquely identified within the network by the flow label and its source address. All packets belonging to one flow should be treated within the network in the same way. The usage of the flow label is not completely specified within the RFCs [8] and [9]. However the flow label field can be defined as a 20-bit field that may be used by a source to label sequences of packets for which it requests special handling by the routers, such as non-default quality of service or real-time service [8]. During our studies [15, 16], it was realized that in virtual networking environment, when IPv4 and IPv6 coexist, it incurs some reasonable amount of signaling overhead, due to which, service quality degrades. Since, redefinition of flow label for end to end QoS is the main concern of this paper and

Многообразие механизмов

Dual-stack

Dual-stack

Dual-stack lite

Tunneling

6in4

6to4

6a44

GRE tunneling

ISATAP

Teredo

6rd

LISP

IPv6 over MPLS

и другие

Translation

NAT64

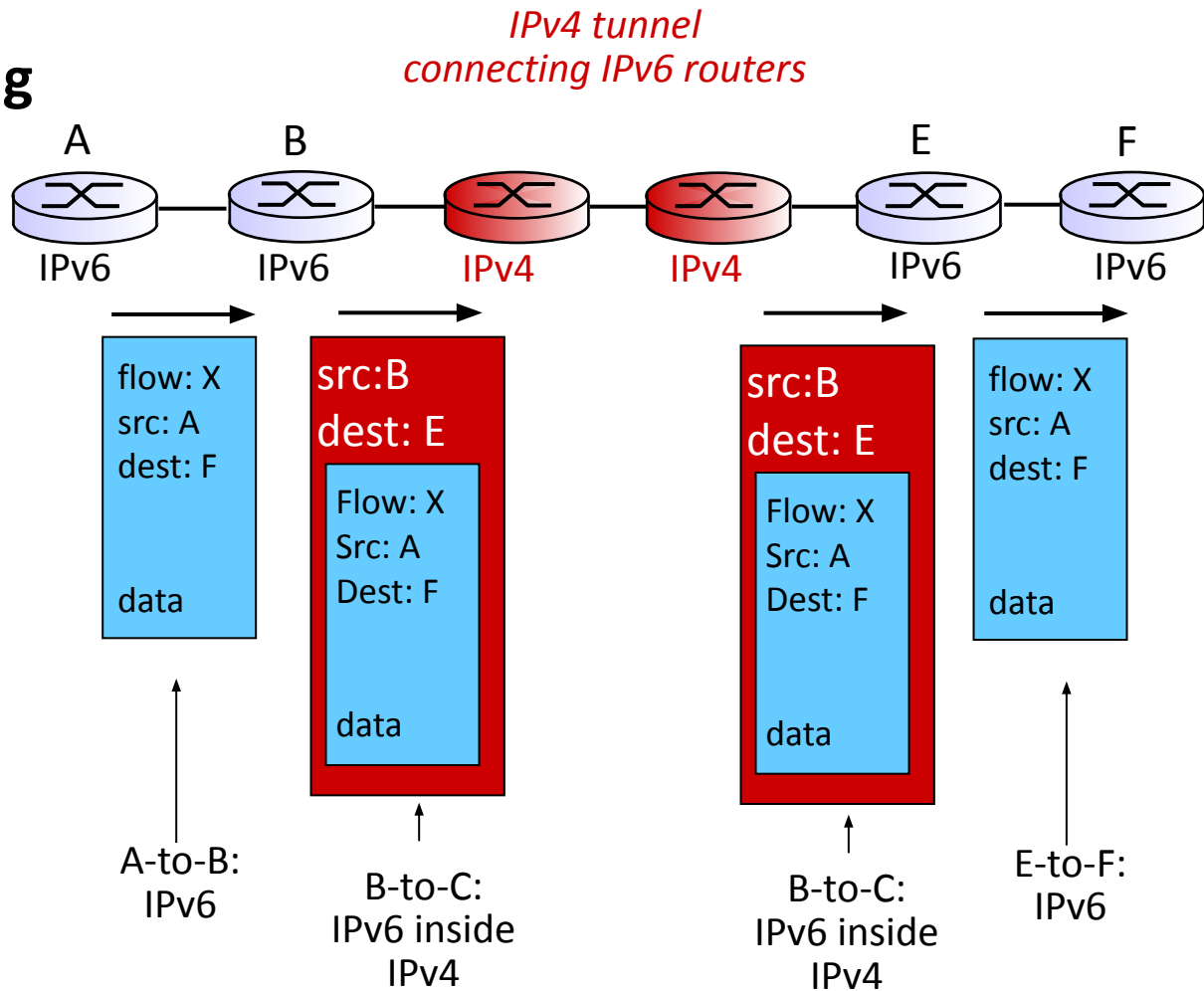
Некоторые из этих механизмов инкапсулируют IPv6-пакеты внутри IPv4-пакетов.

Есть желание посмотреть, что на самом деле передается внутри IPv4-пакета (вложенный внутри IPv6-пакет – тоже часть IPv6-трафика, который необходимо учитывать при анализе). Каким образом может быть инкапсулирован IPv6 в IPv4?

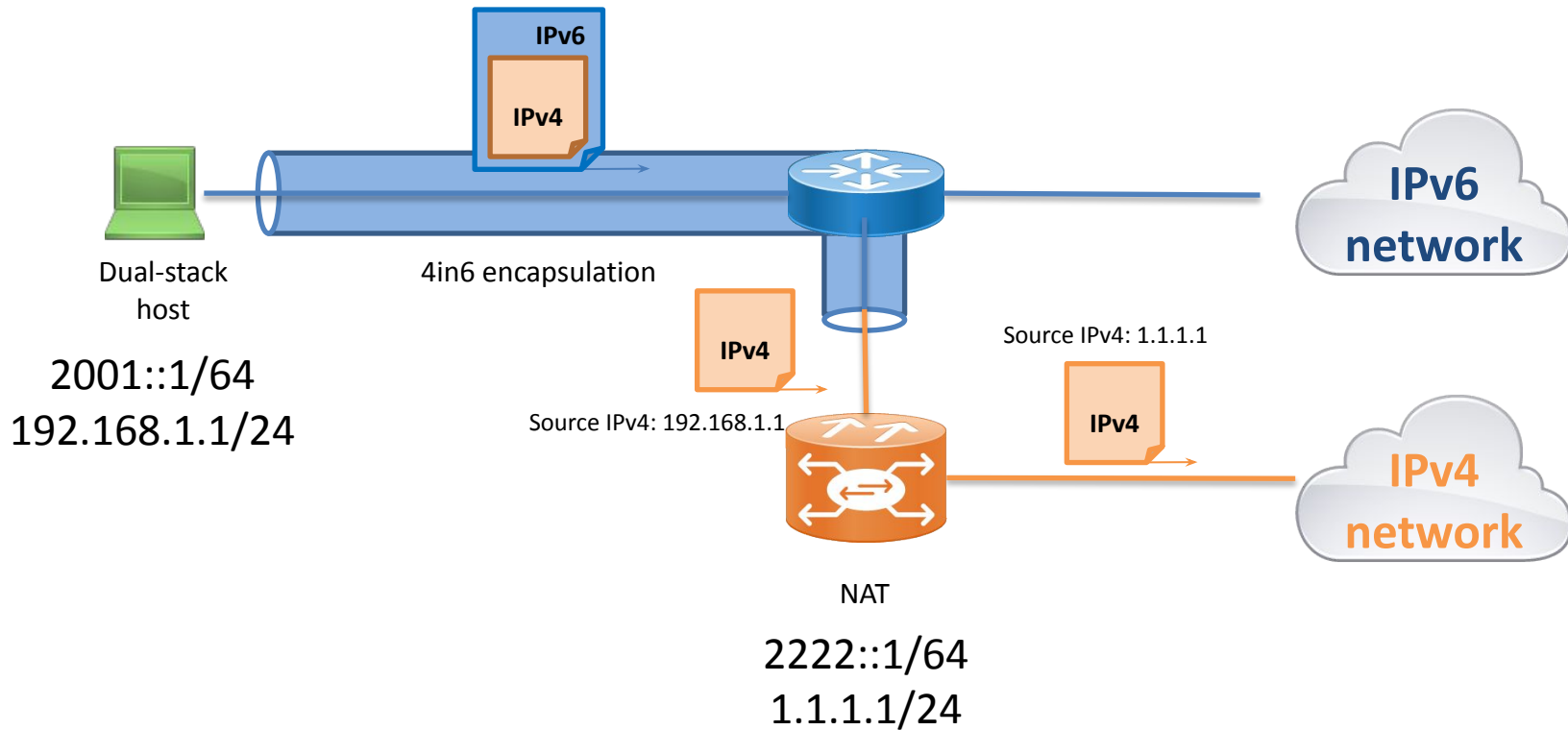


Каким образом IPv6-трафик присутствует в IPv4-

Tunneling



Обзор Dual-stack lite

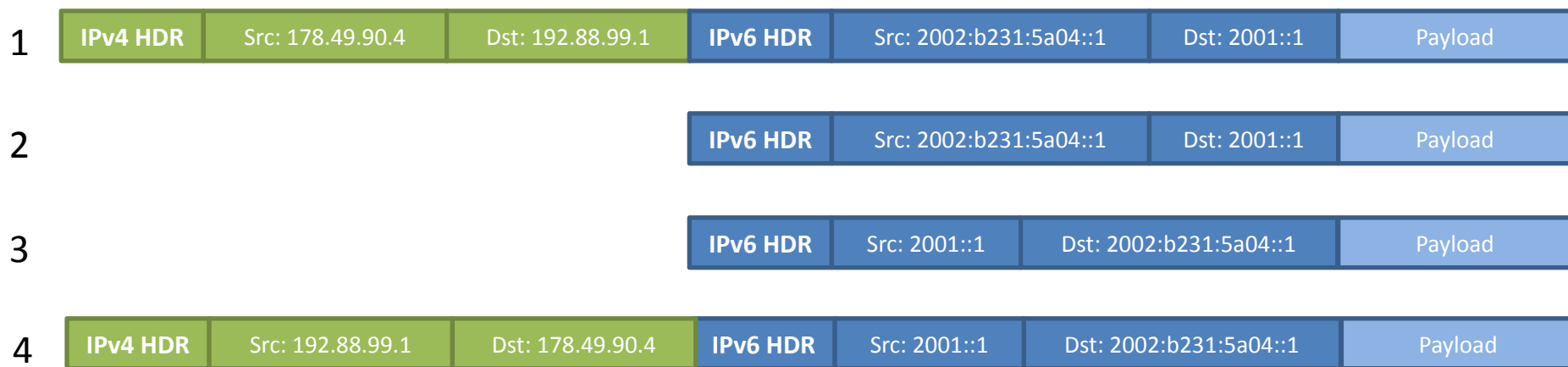
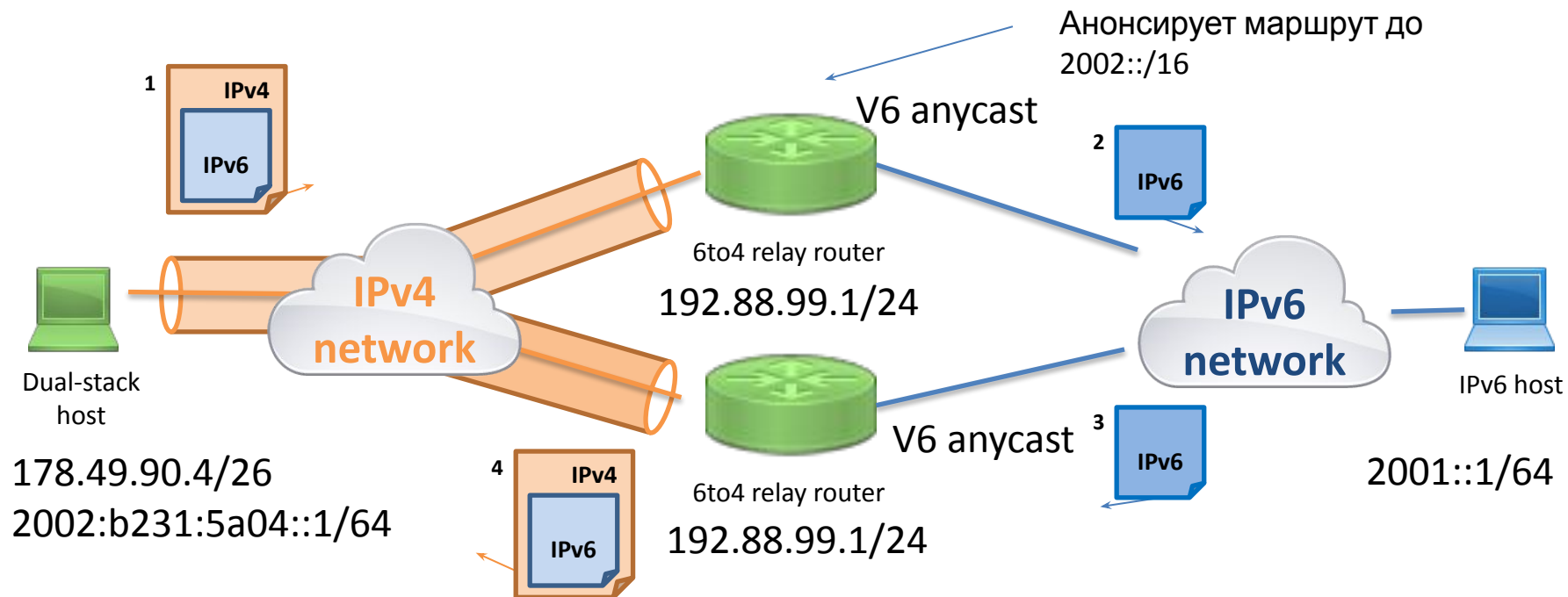


Заполняется таблица трансляции на NAT:

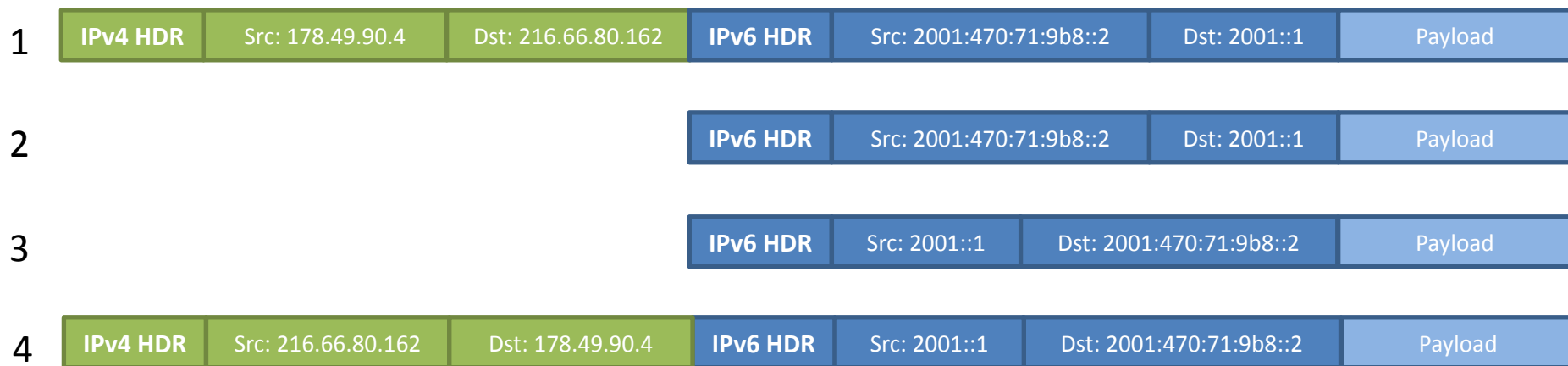
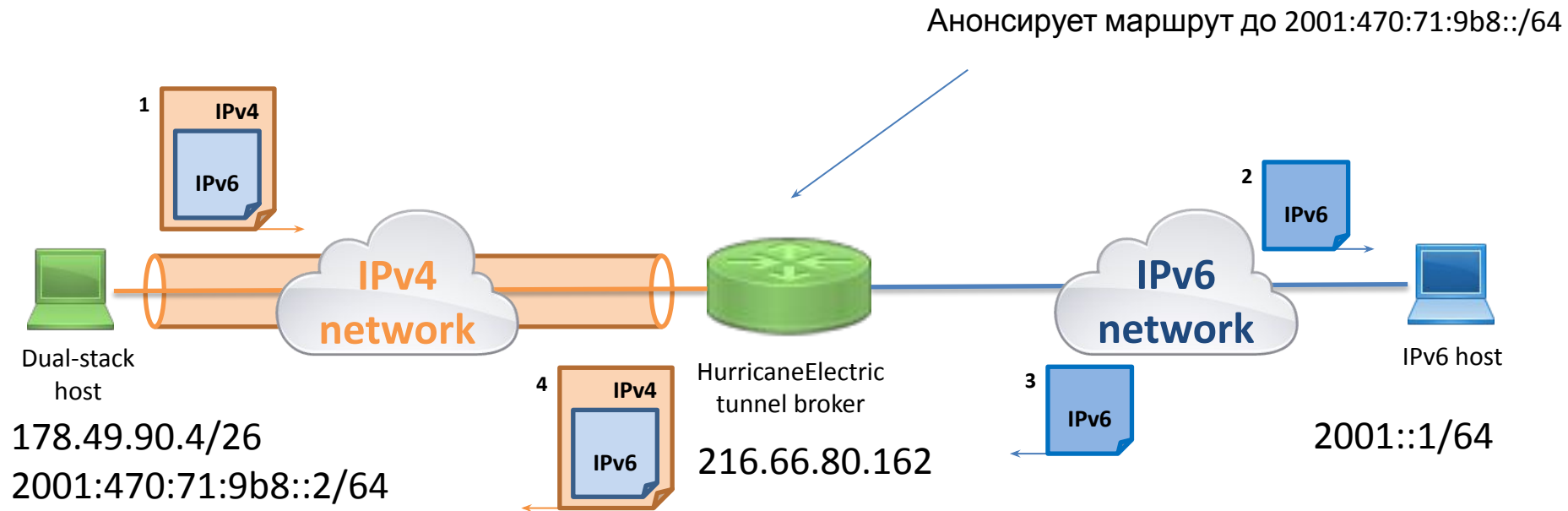
`192.168.1.1:XXXX == 1.1.1.1:YYYY` (классический NAT44)

IPv4-пакет с IP `192.168.1.1` пришел от `2001::1`

Обзор 6to4



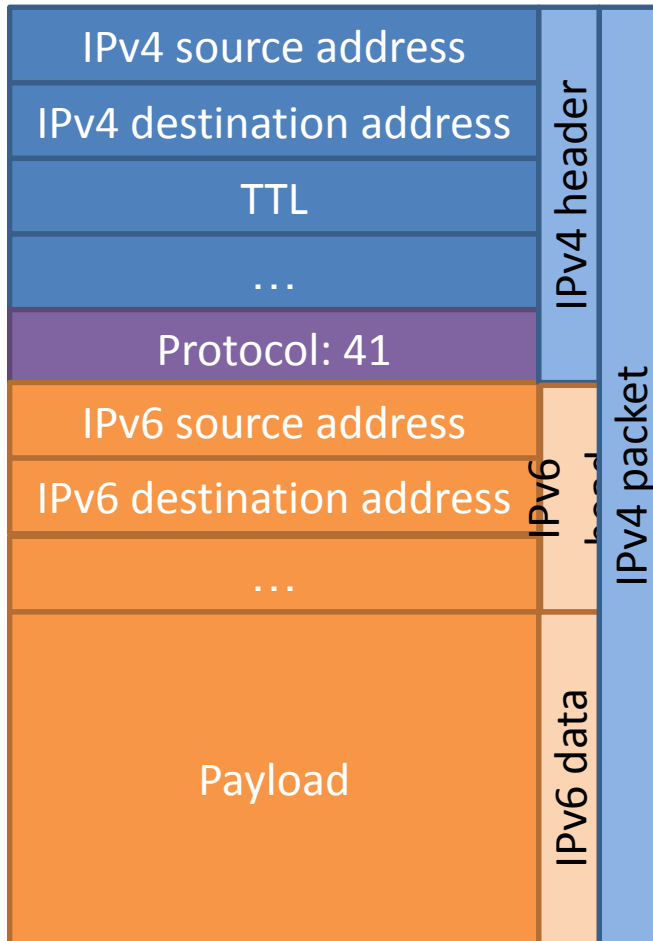
Обзор



Способы инкапсуляции IPv6 в IPv4

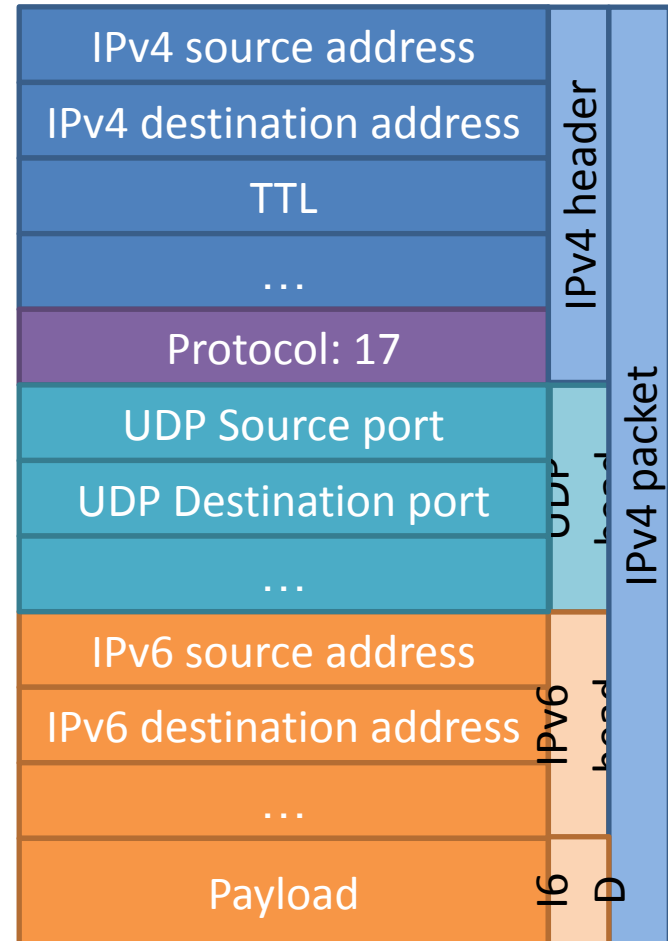
Protocol 41

6to4, 6in4, ISATAP
Easily filtered



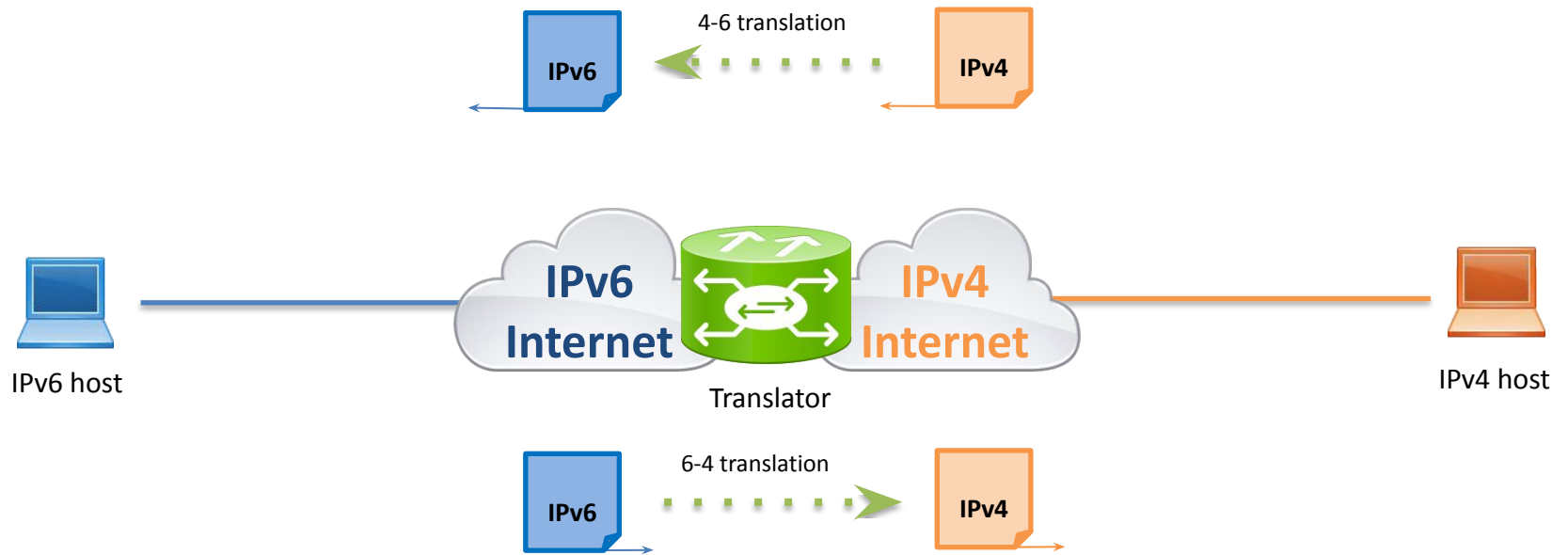
UDP

Teredo, 6a44
Less susceptible to filtering

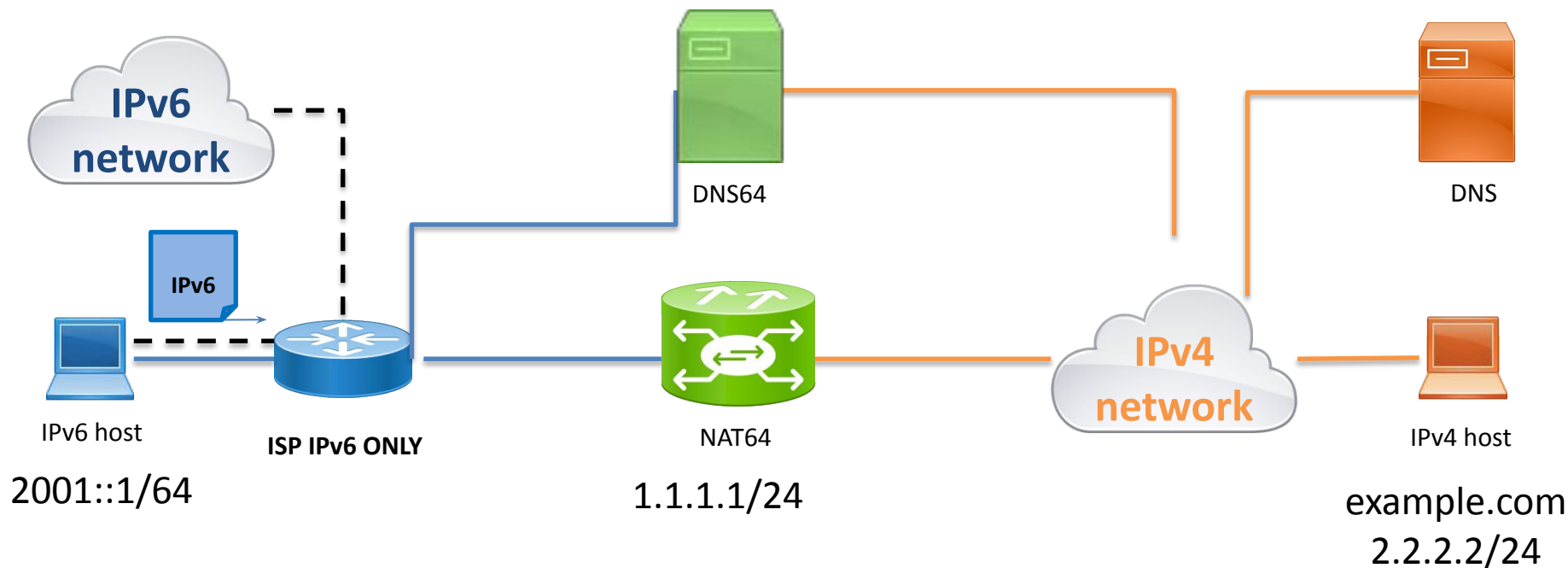


Каким образом IPv6-трафик присутствует в IPv4-

Translation



Обзор



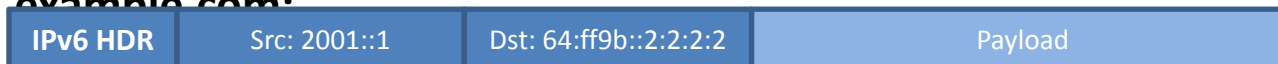
1

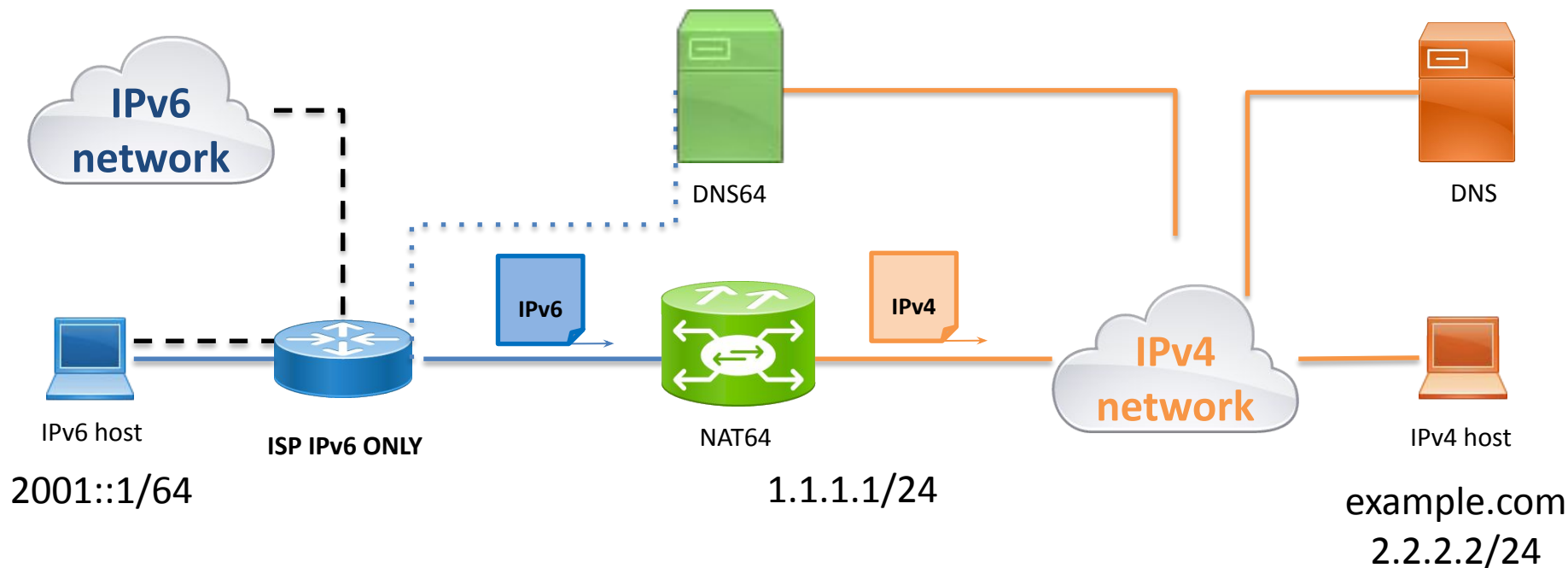
DNS64 ask IPv4 DNS:
example.com A: 2.2.2.2
example.com AAAA: none

DNS64 answer IPv6 host:
example.com A: 2.2.2.2
example.com AAAA: 64:ff9b::2:2:2:2

2

IPv6 host 2001::1 отправляет пакет для example.com:





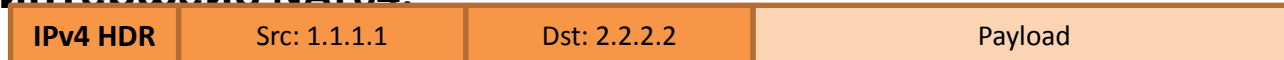
3

Заполняется таблица трансляции на NAT64:

[2001::1]:8080 == 1.1.1.1:8080

4

Согласно RFC6145 заголовок IPv6 **конвертируется** в IPv4. Пакет IPv6 превращается в IPv4 и высылается через IPv4 интерфейс NAT64:



Monitoring of Tunneled IPv6 Traffic Using Packet Decapsulation and IPFIX

By Martin Elich, Matej Gregr and Pavel Celeda

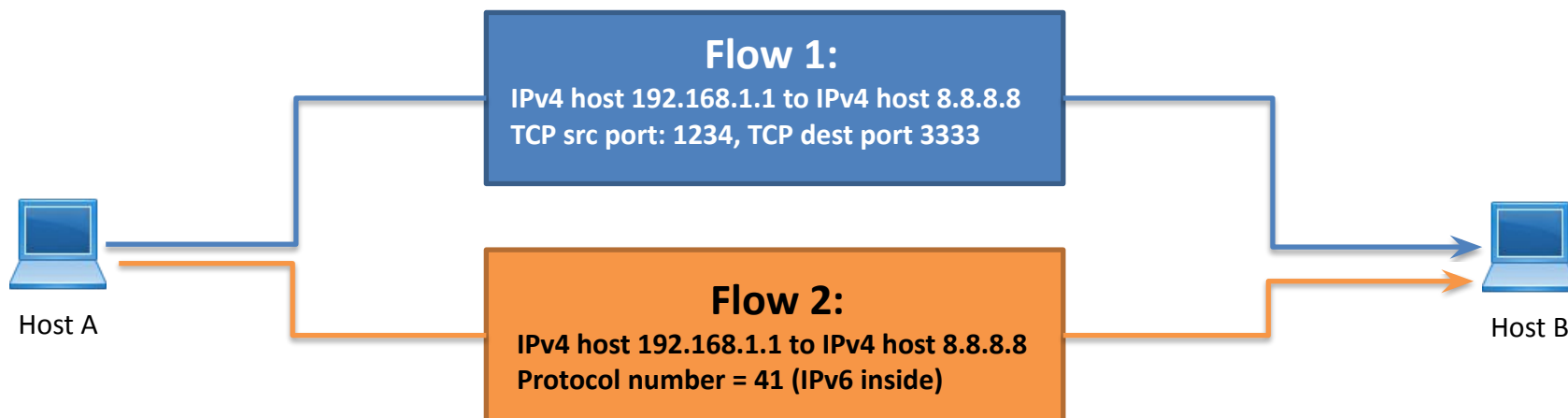
Internet Protocol Flow Information Export

Протокол IETF, определяющий стандарт экспорта информации о **потоках данных** с различных сетевых устройств.

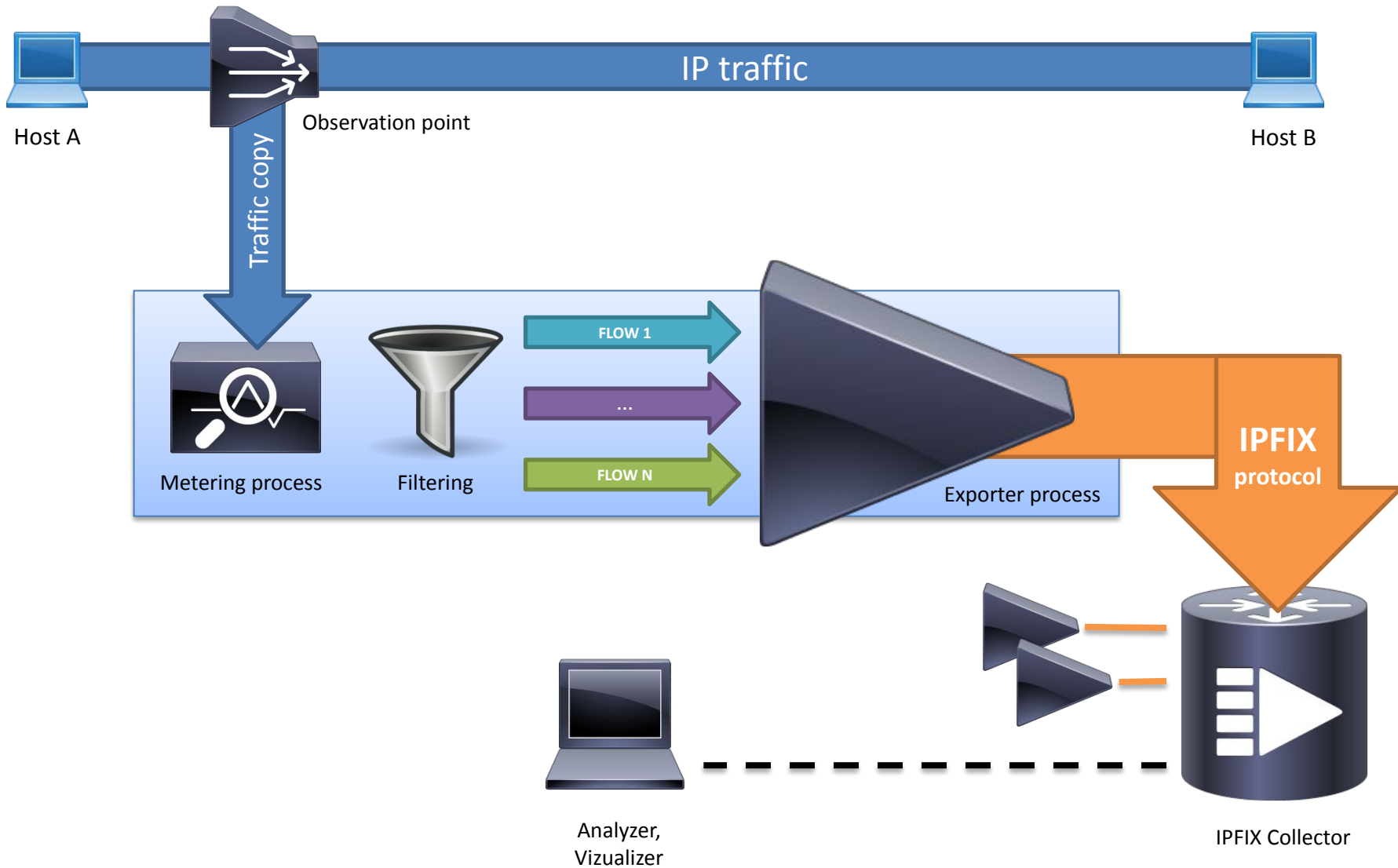
Основан на протоколе Cisco NetFlow v9.

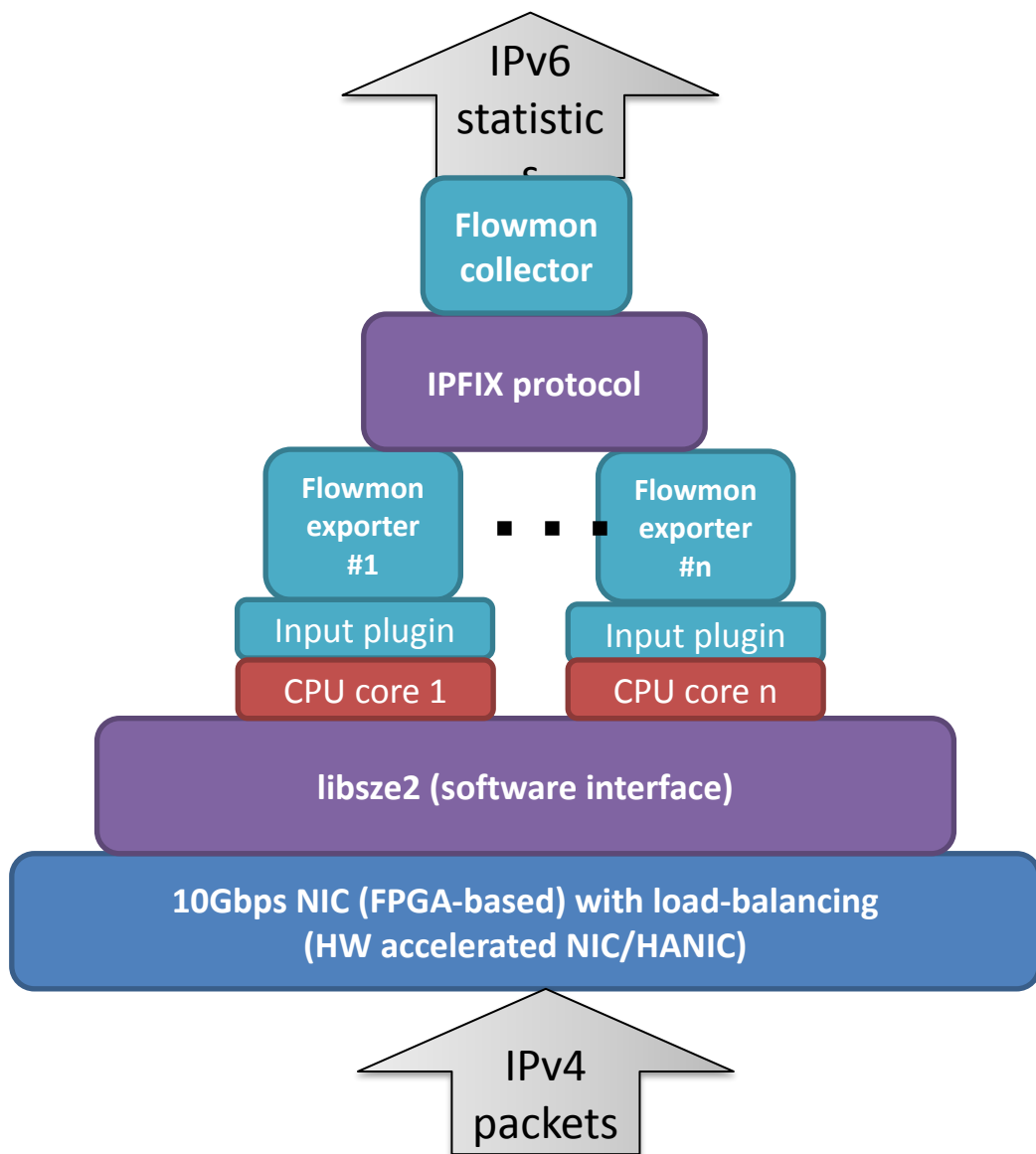
Информация о потоках данных может использоваться в таких задачах, как:

- Мониторинг трафика, учет использования сетевых ресурсов
- Анализ трафика
- Обнаружение/предотвращение вторжений



Кратко о





Получение статистики по IPv6-трафику, инкапсулированному в IPv4 (разбор некоторых туннелей)

Сборщик IPFIX (в данном случае Flowmon) собирает итоговую статистику по потокам со всех экспортеров и презентует ее пользователю в том или ином виде

Информация о потоке передается сборщику при помощи протокола IPFIX.

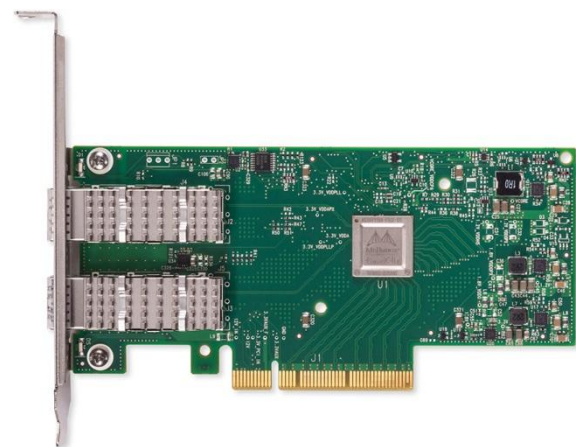
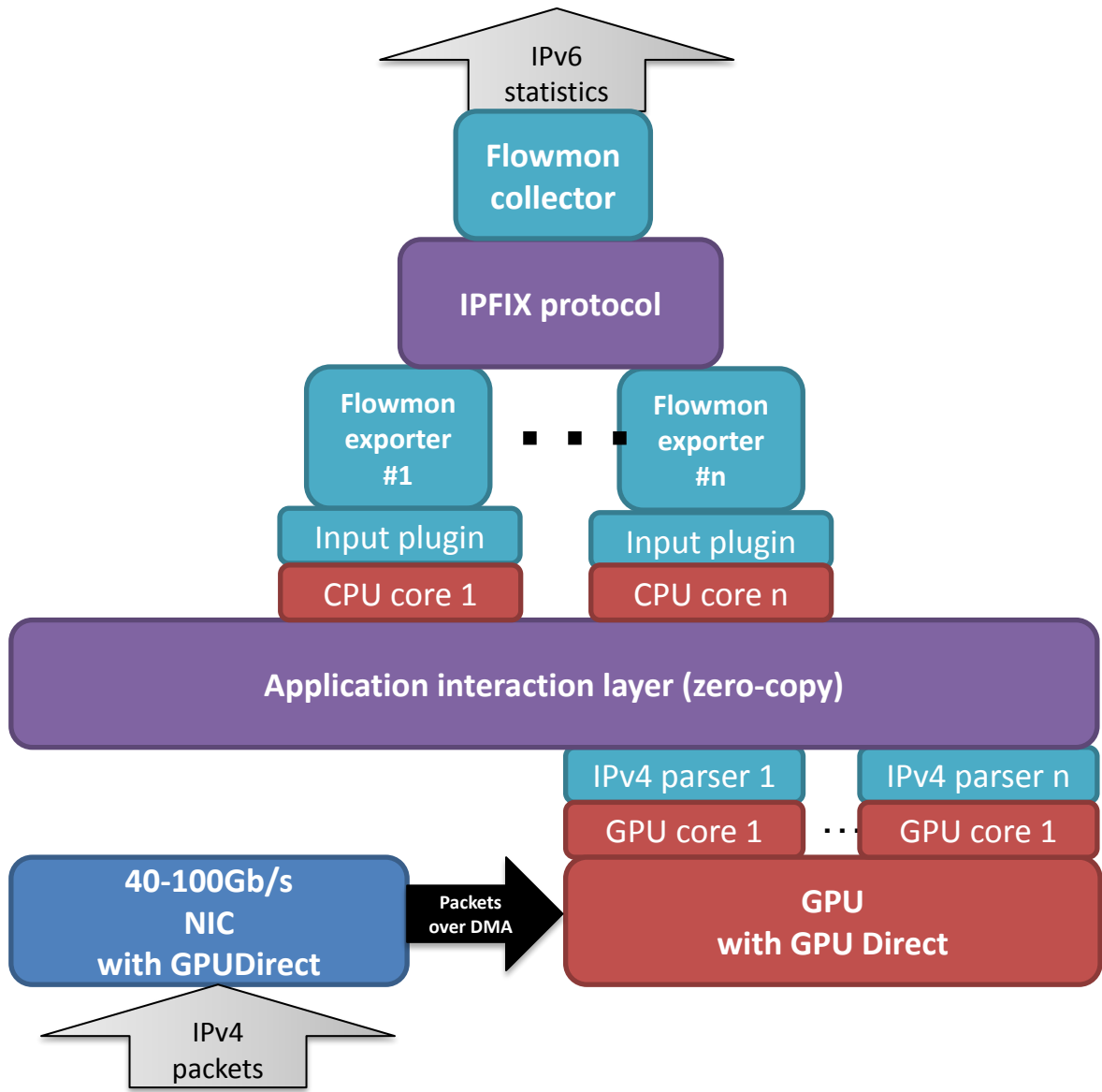
При обнаружении IPv6-пакета внутри IPv4, IPv6-пакет декапсулируется из IPv4, на основании информации в заголовке IPv6 пакет сопоставляется определенному потоку.

Пакеты распределяются по обработчикам
На каждом ядре сидит экспортер с самописным плагином для обнаружения IPv6 в v4
(реализовано обнаружение Teredo, ISATAP, 6to4)

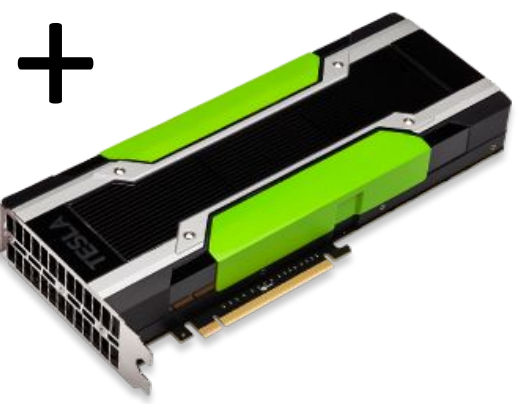
В сети практически нет информации по библиотеке Skoree всего, с ее помощью делается zero-copy

Для каждого принятого пакета ставит timestamp
Некоторым образом получает хэш заголовка пакета
Далее согласно хэшу пакеты распределяются по обработчикам

Варианты новой высокопроизводительной

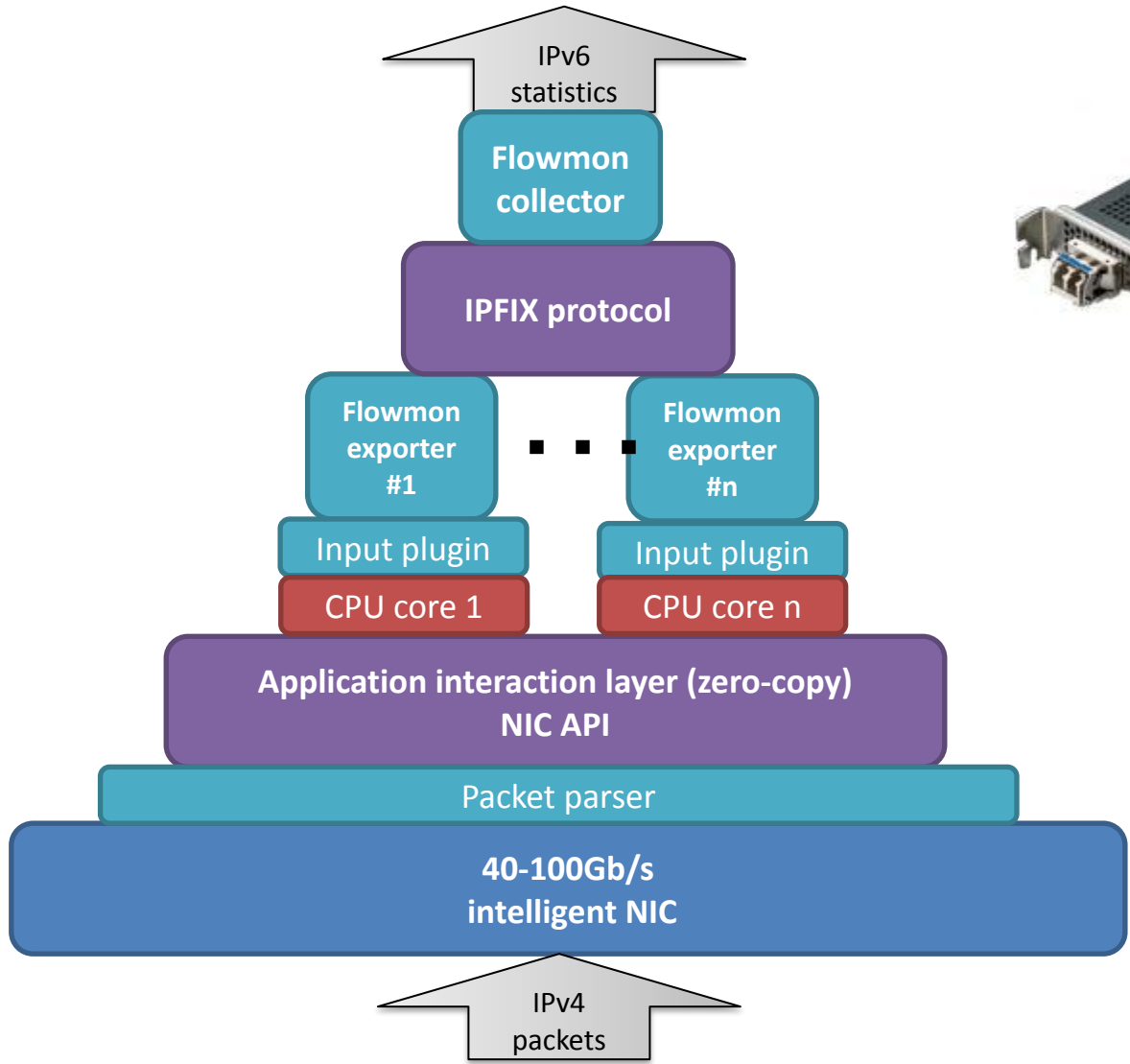


Mellanox ConnectX-4 LX

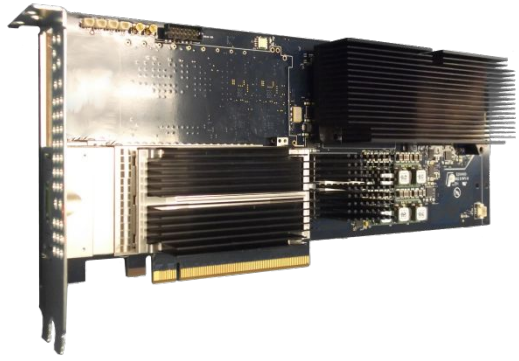


Nvidia Tesla Kepler GPU

Варианты новой высокопроизводительной



Napatech NT100-E3-1-PTP



Accolade ANIC-100K

- RFC 7059 - A Comparison of IPv6-over-IPv4 Tunnel Mechanisms
- RFC 4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC 6145 - IP/ICMP Translation Algorithm
- RFC 6146 - Stateful NAT64
- RFC6147 - DNS64

**Спасибо за
внимание**