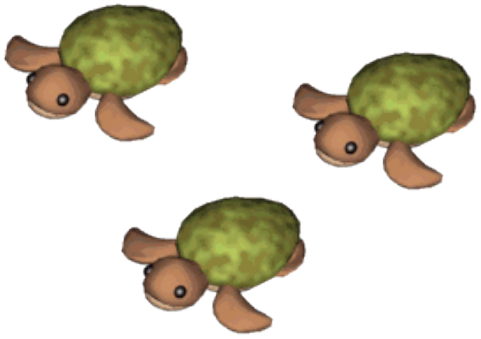
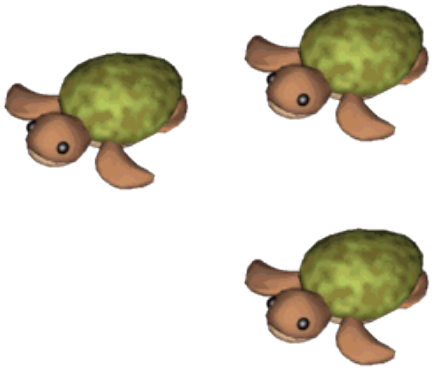
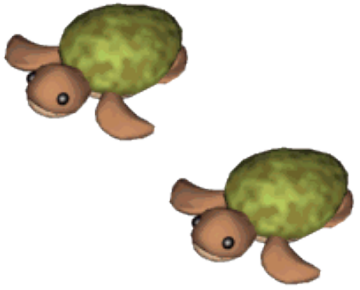



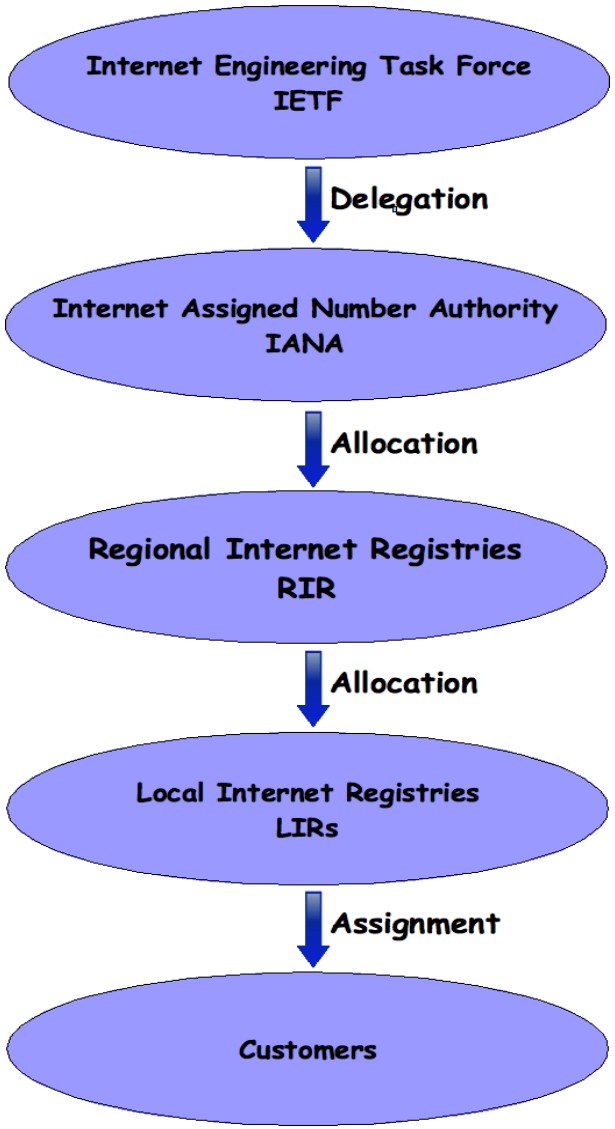

IPv6

Jen Linkova aka Furry
Openwall, Inc
furry@openwall.com

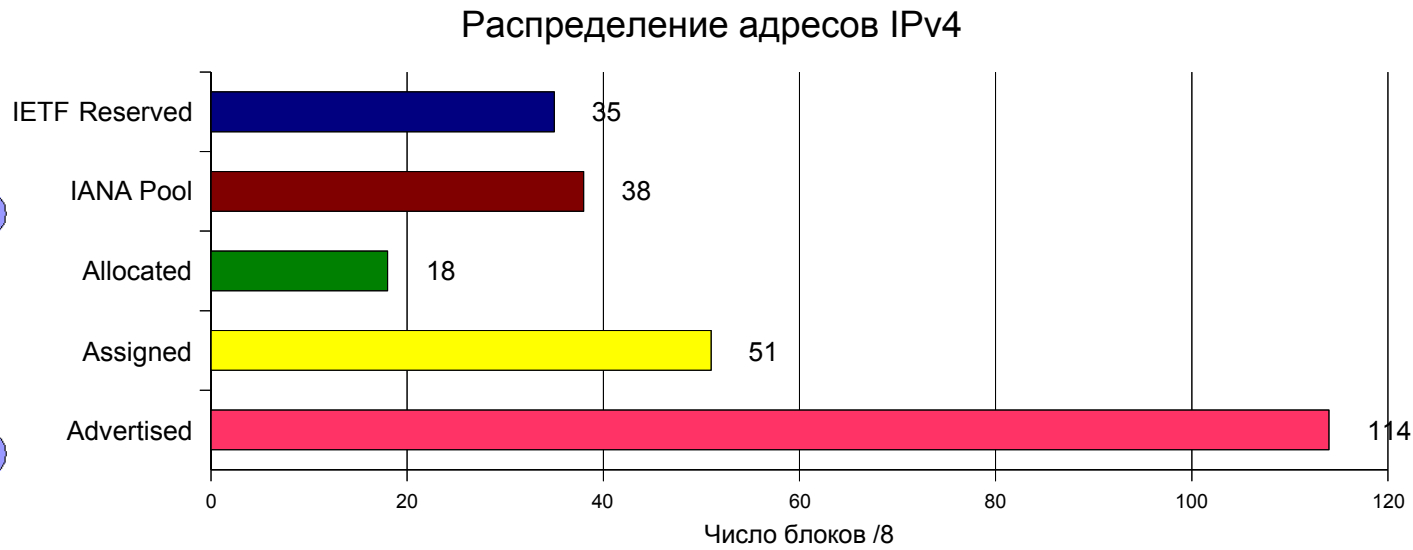




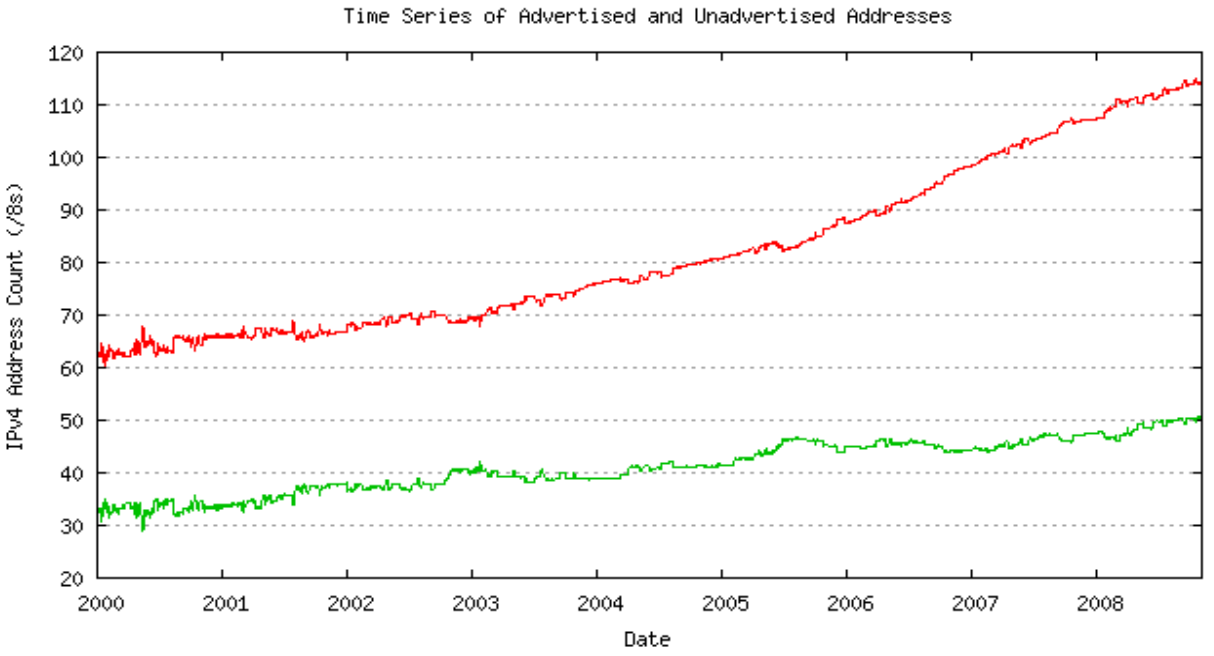
Распределение адресов в мире IPv4

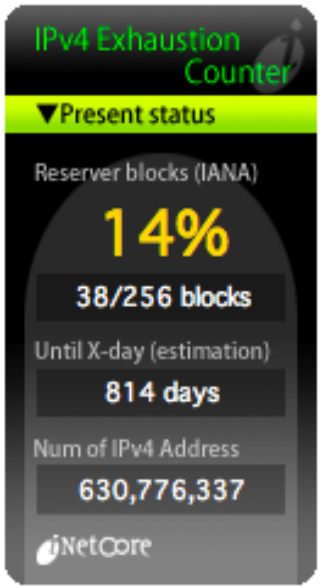


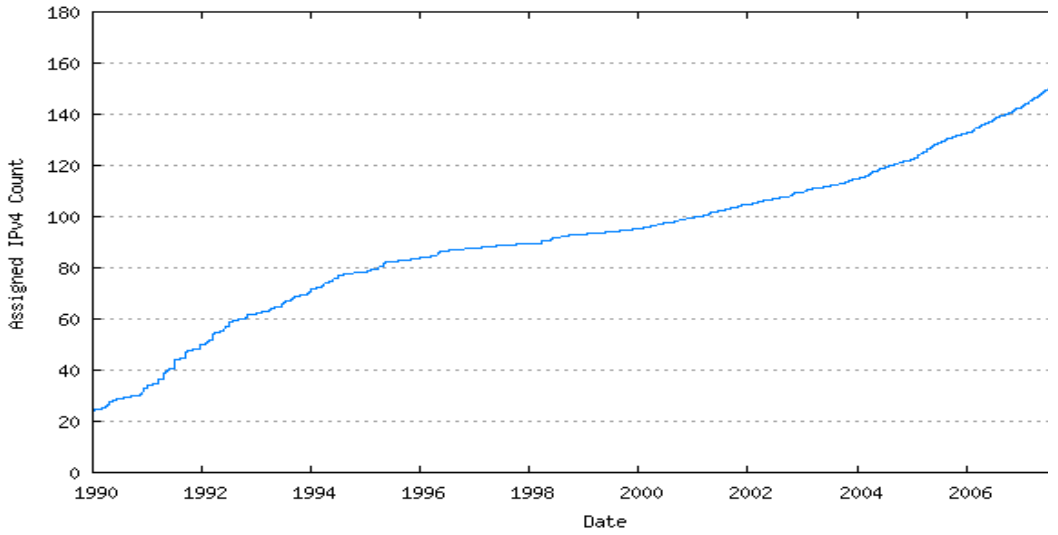
- длина адреса - 32 бита
- 4 294 967 296 адреса
- 256 блоков /8

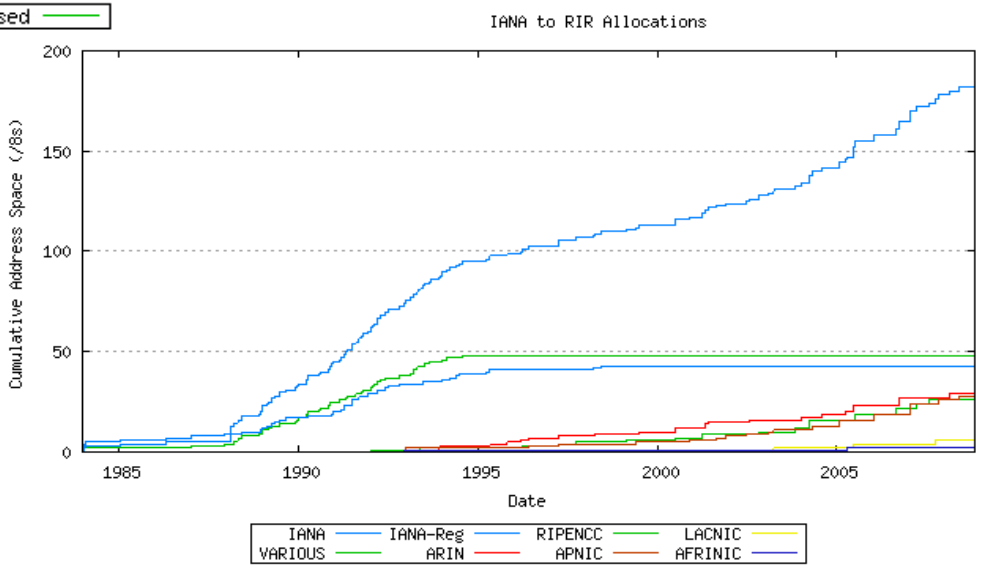


Три вида лжи: ложь, наглая ложь и статистика?









Источник: «IPv4 Address Report», http://www.potaroo.net/tools/ipv4/

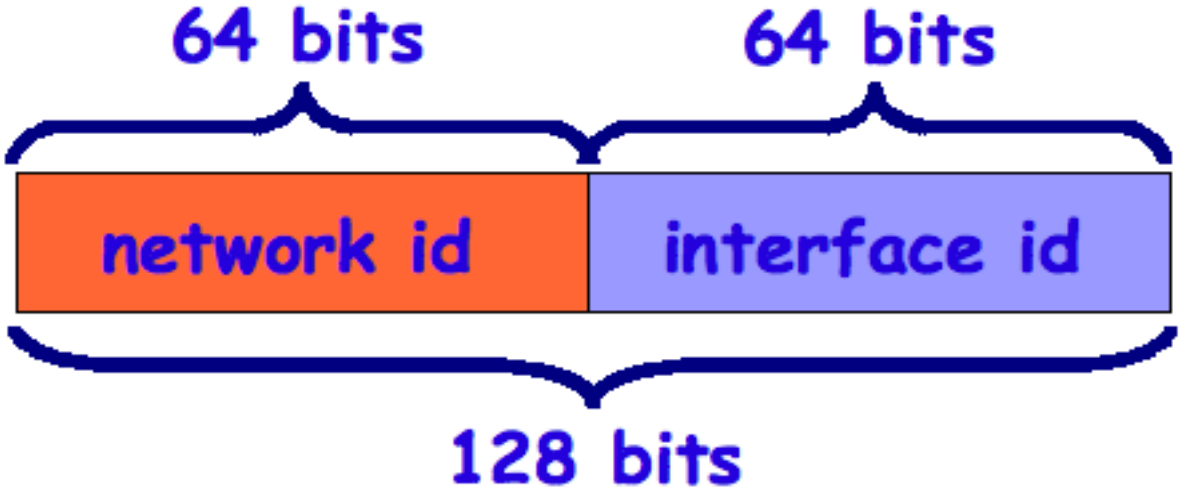
Меньше тратить.....

- Изменение политики выделения адресов для LIR (/19, /20, /21...)
- Трансляция адресов (NAT, NAPT):
  - нарушает принцип сквозной прозрачности
  - влияет на работу протоколов
  - создает иллюзию безопасности

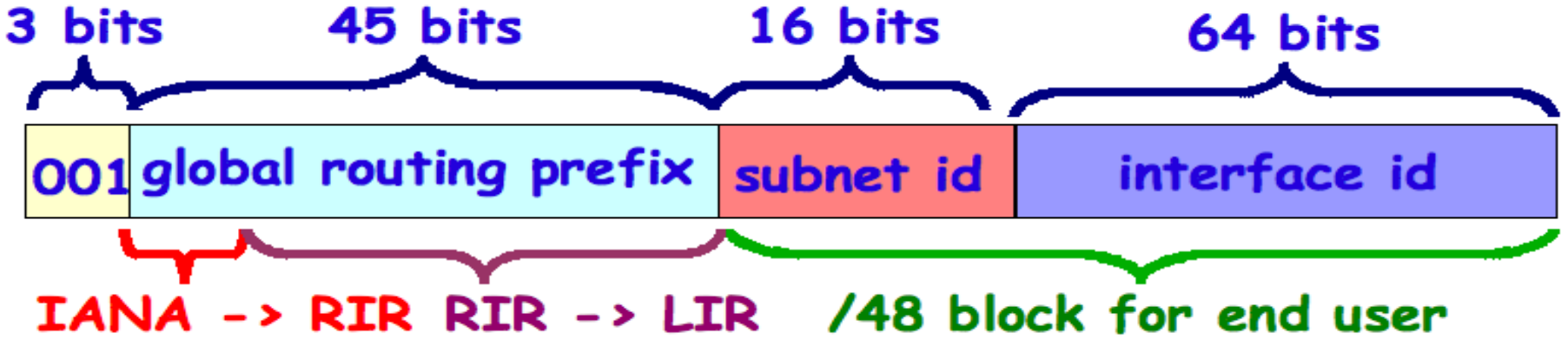
См. документы

- *RFC 2775 «Internet Transparency»*
- *RFC 3027 «Protocol Complication with the IP Network Address Translator»*
- *RFC 2993 «Architectural Implications of NAT»*
- *Internet-Draft «Security implication of Network Address Translators»*

..или больше получать? ;-)



- 340 282 366 920 938 463 463 374 607 431 768 211 456 адресов
- в каждой подсети до 2^64 узлов
- не требуется дробление на подсети переменного размера
- на каждом уровне иерархии выделяется ОДИН префикс



Достаточно ли?

- **Допустим**, что…
  - каждые 18 месяцев RIR запрашивают новый блок
- **Тогда...**
  - Блок выделенный IETF для RIRs (1/8 всего пространства) закончится в 2158 году
  - Будет доступно еще более 5/8 пространства адресов (префиксы 000 и 111 – специальные адреса)

Источник: David Conrad, General Manager, IANA, 2007 год
http://www.iana.org/about/presentations/conrad-buenosaires-citel-060913.pdf

Формат записи адреса IPv6

X:X:X:X:X:X:X:X

где X принимает значения от 0x0000 до 0xFFFF

- 2001:0DB8:0000:0000:0008:8000:0000:417A
- 2001:DB8:0:0:8:8000:0:417A
- 2001:DB8::8:8000:0:417A
- 2001:DB8:0:0:8:8000::417A
- 2001:db8::8:8000:417A

Несколько примеров

- loopback адрес

  0:0:0:0:0:0:0:1 или ::1

- неопределенный (unspecified)

  0:0:0:0:0:0:0:0 или ::

- Специальная форма записи: IPv4-mapped

  0:0:0:0:0:FFFF:192.0.2.1

  ::FFFF:192.0.2.1

Где ошибка?

2001:0DB8:0000:0000:FFFF:0CA0:0000:0000

1)2001:DB8::FFFF:CA0:0:0

2)2001:db8:0:0:FFFF:0CA0:0:0

3)2001:DB8::FFFF:CA0:0:0

4)2001:db8::FFFF:ca0::

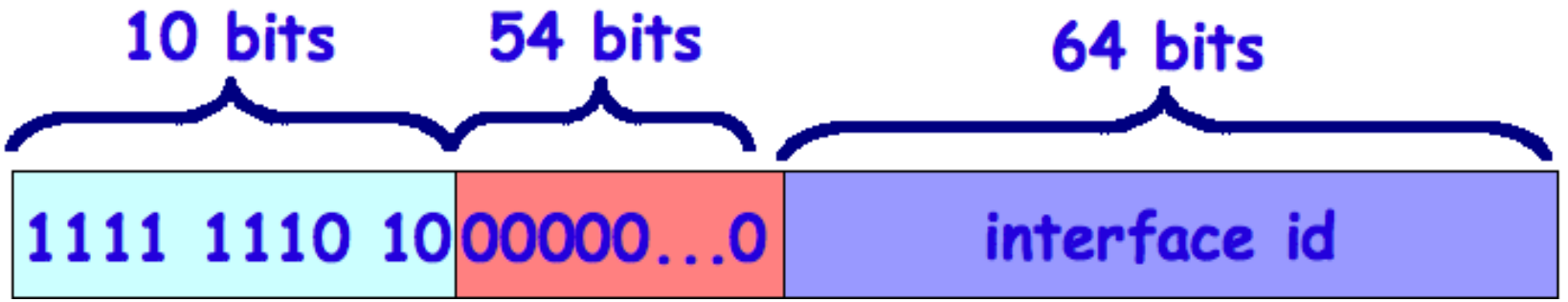
5)2001:db8:0:0:FFFF:CA0::

6)2001:db8::FFFF:CA:0:0

Типы адресов IPv6

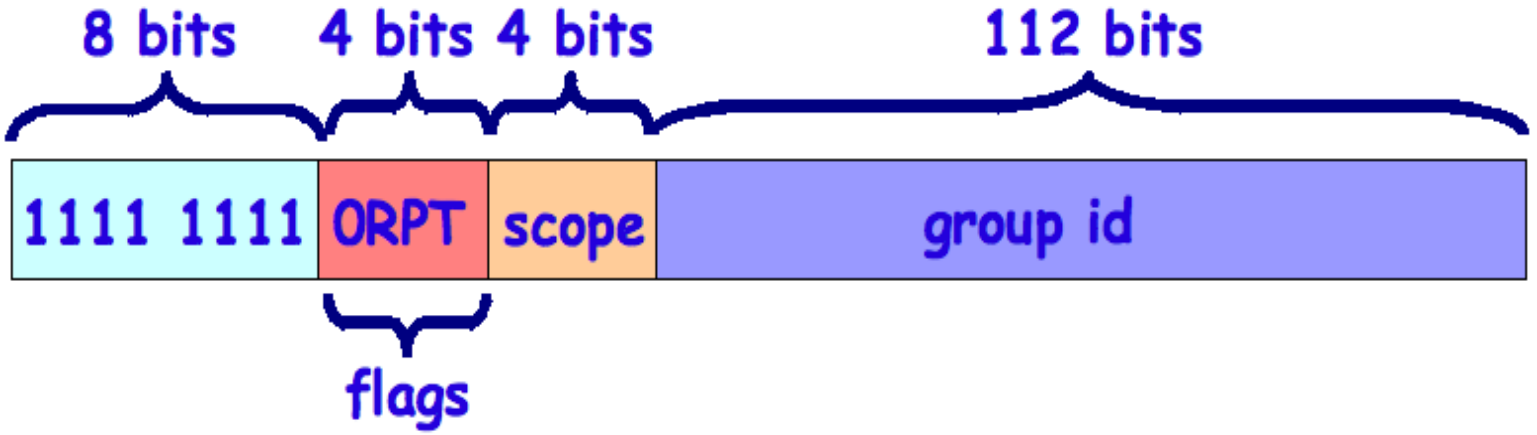
Тип адреса	Бинарный префикс	Префикс
unspecified	000...0 (128 бит)	::/128
loopback	0000...01 (128 бит)	::1/128
link-local unicast	1111 1110 10	FE80::/10
multicast	1111 1111	FF00::/8
Global unicast	все остальное	

Link-local (внутриканальные) адреса



- Блок FE80::/10
- Аналог блока 169.254.0.0/16
- Адрес назначается автоматически
- Область действия - канал!
- Обеспечивает
  - взаимодействие «ненастроенных» узлов
  - работу служебных протоколов

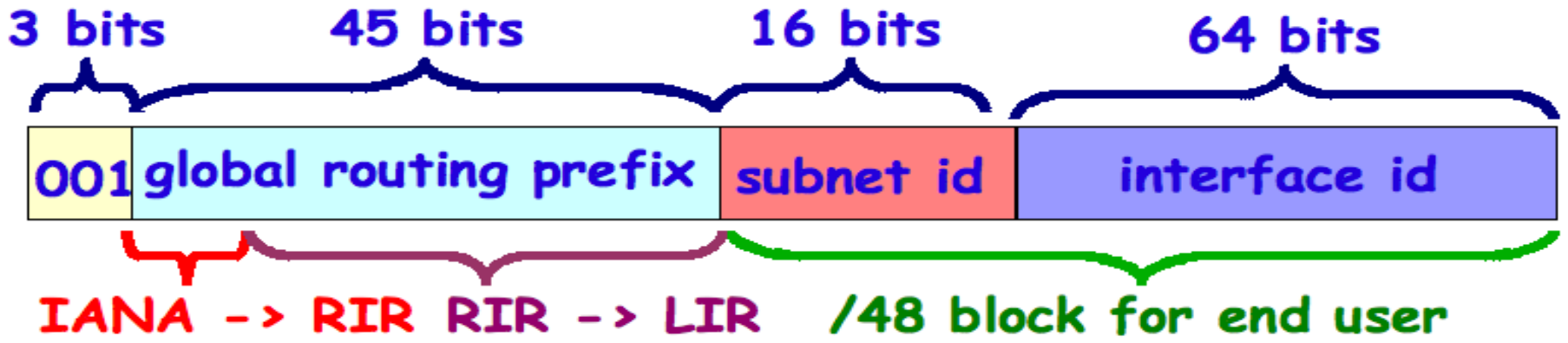
Multicast (групповые) адреса



- Флаг T=0 – глобально выделенный (общепринятый) адрес, T=1 – временно занятый
- Scope – область действия адреса
  - 1 – интерфейс
  - 2 – канал
  - 5 – сайт
  - 14 – Интернет
- Group ID:
  - 1 – все узлы (scope = 1,2)
  - 2 – все маршрутизаторы (scope = 1,2,5)
  - 101 – все NTP-серверы
- Пример:
  - FF02::101 – все NTP-серверы на данном канале
  - FF02::2 – все маршрутизаторы на данном канале
  - FF05::101 – все NTP-серверы сайта
-

Global Unicast

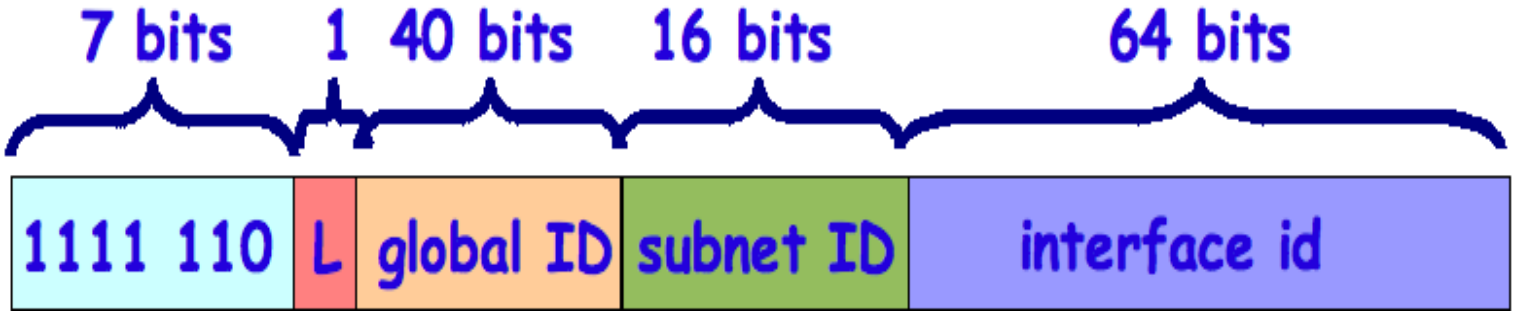
Тип адреса	Бинарный префикс	Префикс
unspecified	000...0 (128 бит)	::/128
loopback	0000...01 (128 бит)	::1/128
Ipv4-mapped	000...01111111111111111(96 бит)	::FFFFF/96
ULA	1111 110	FC00::/7
Исп. RIRs	001	2000::/3
Global unicast	все остальное	



Unique Local Unicast Addresses (ULA)

- Блок FC00::/7 (RFC4193)
- Адреса для внутреннего использования
- С высокой степенью вероятности – уникальные
- Не должны выходить за пределы административной зоны
- Известный префикс – легко фильтровать

Формат ULA



L = 1 префикс выделен локально (самостоятельно)
L = 0 возможно использование в дальнейшем

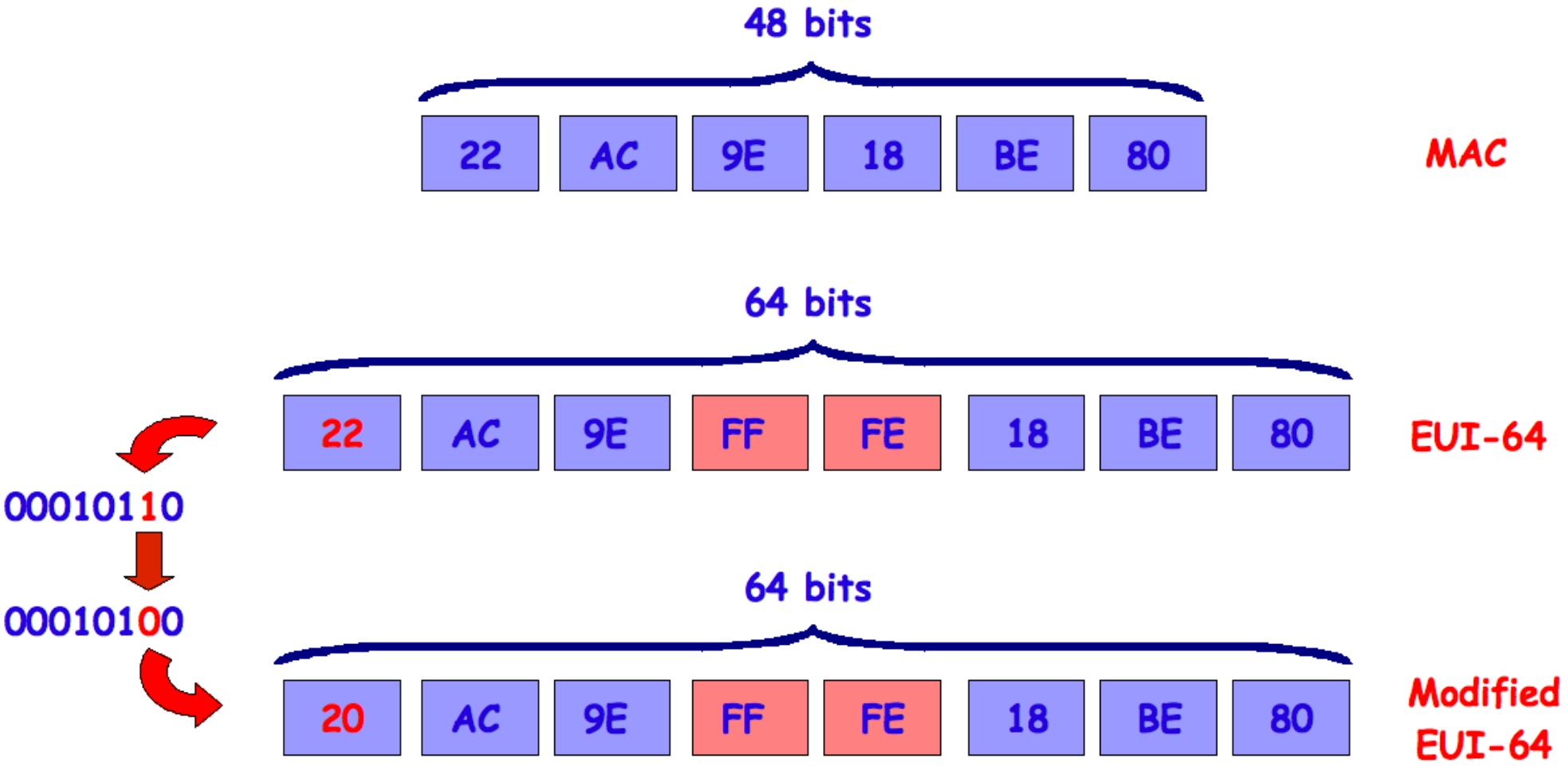
Global ID уникальный идентификатор данного префикса
Subnet ID идентификатор подсети

Генератор случайного Global ID:
1)получить текущее время (64-битное значение)
2)Взять EUI-64 interface ID (получить из MAC)
3)Сцепить результаты 1 и 2
4)Вычислить SHA-1 digest и взять 40 младших битов как Global ID

Идентификатор интерфейса Вариант настройки

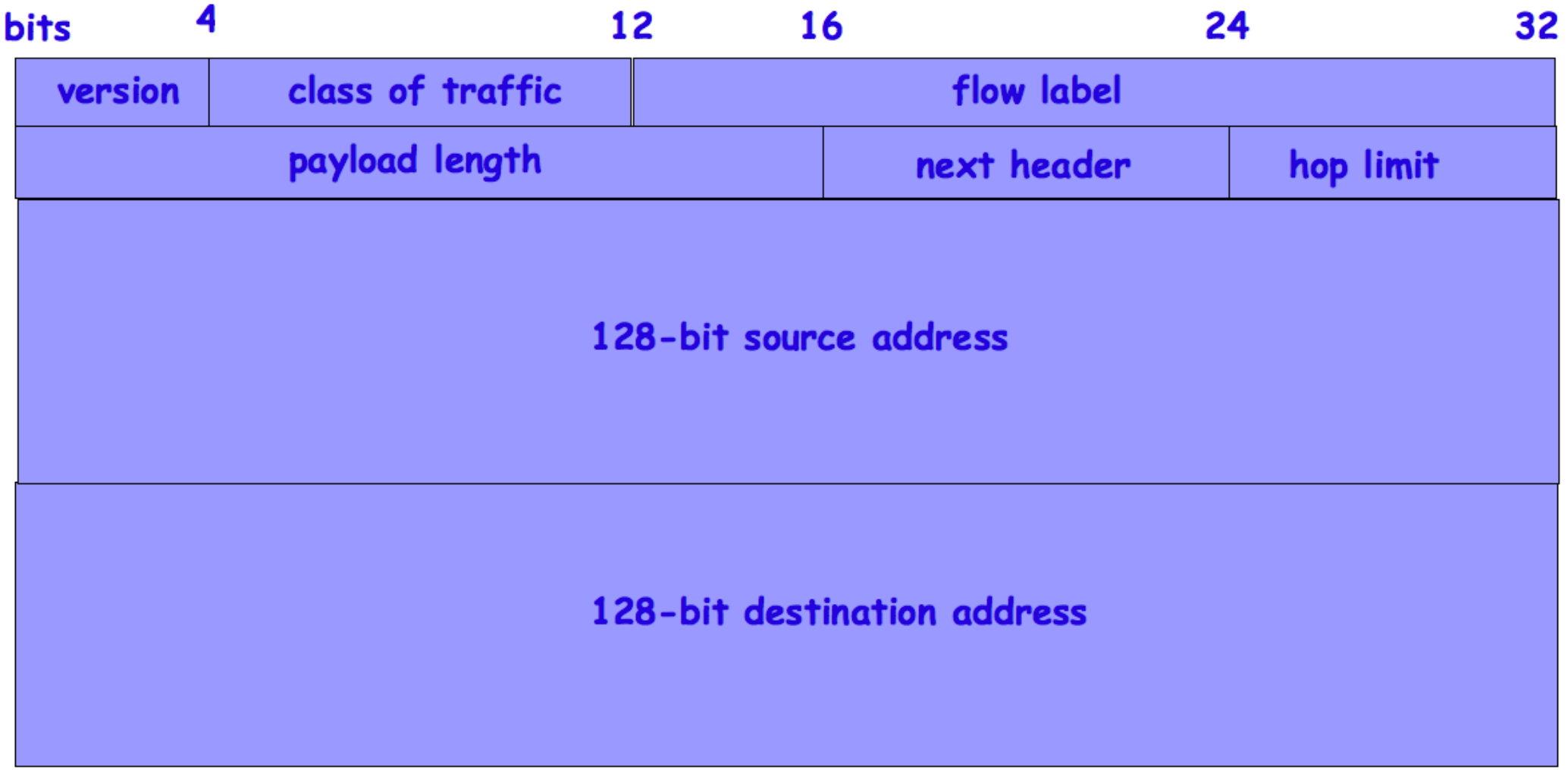
- Ручная настройка
- Автоматическая настройка (формат модифицированного EUI-64 на основе MAC-адреса)
- DHCPv6
- Псевдо-случайное число
- Отпечаток криптографического ключа

Extended Unique Identifier EUI-64



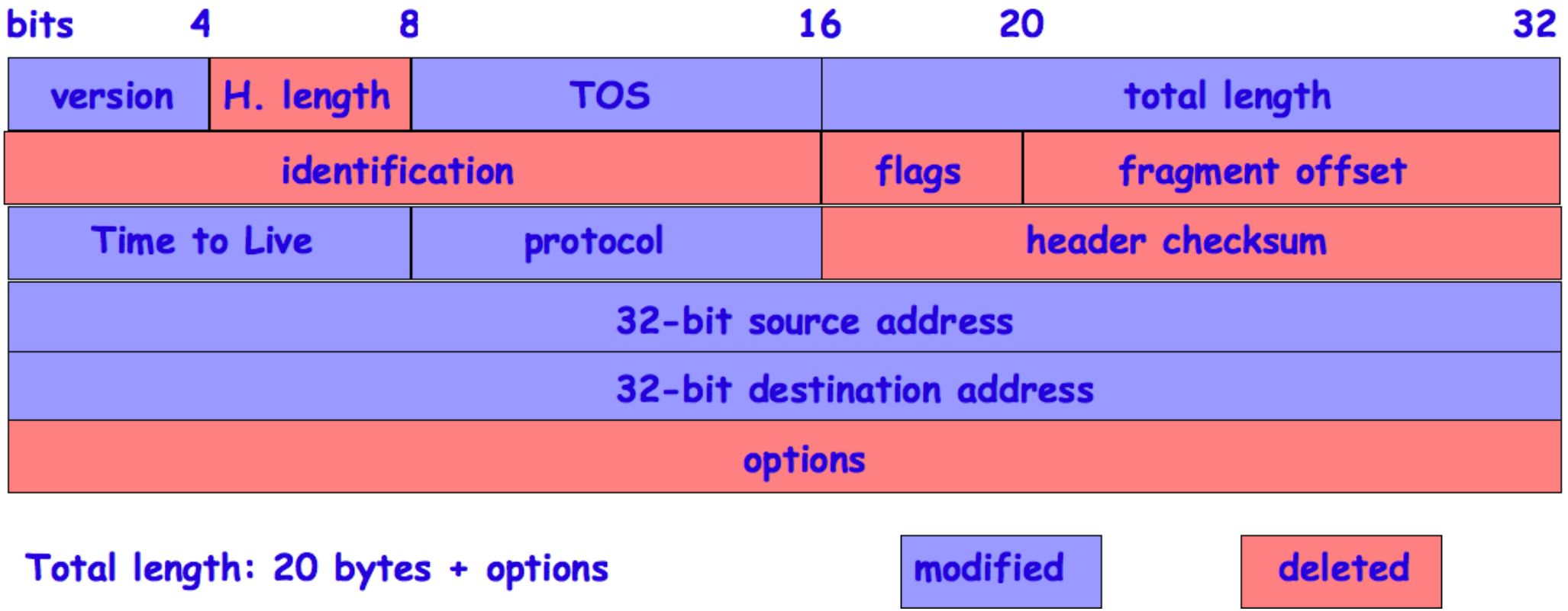
Пример: ::1 – глобально назначенный EUI-64, но локально назначенный MEUI-64

Заголовок IPv6



Total length: 40 bytes

Заголовок IPv4



Total length: 20 bytes + options

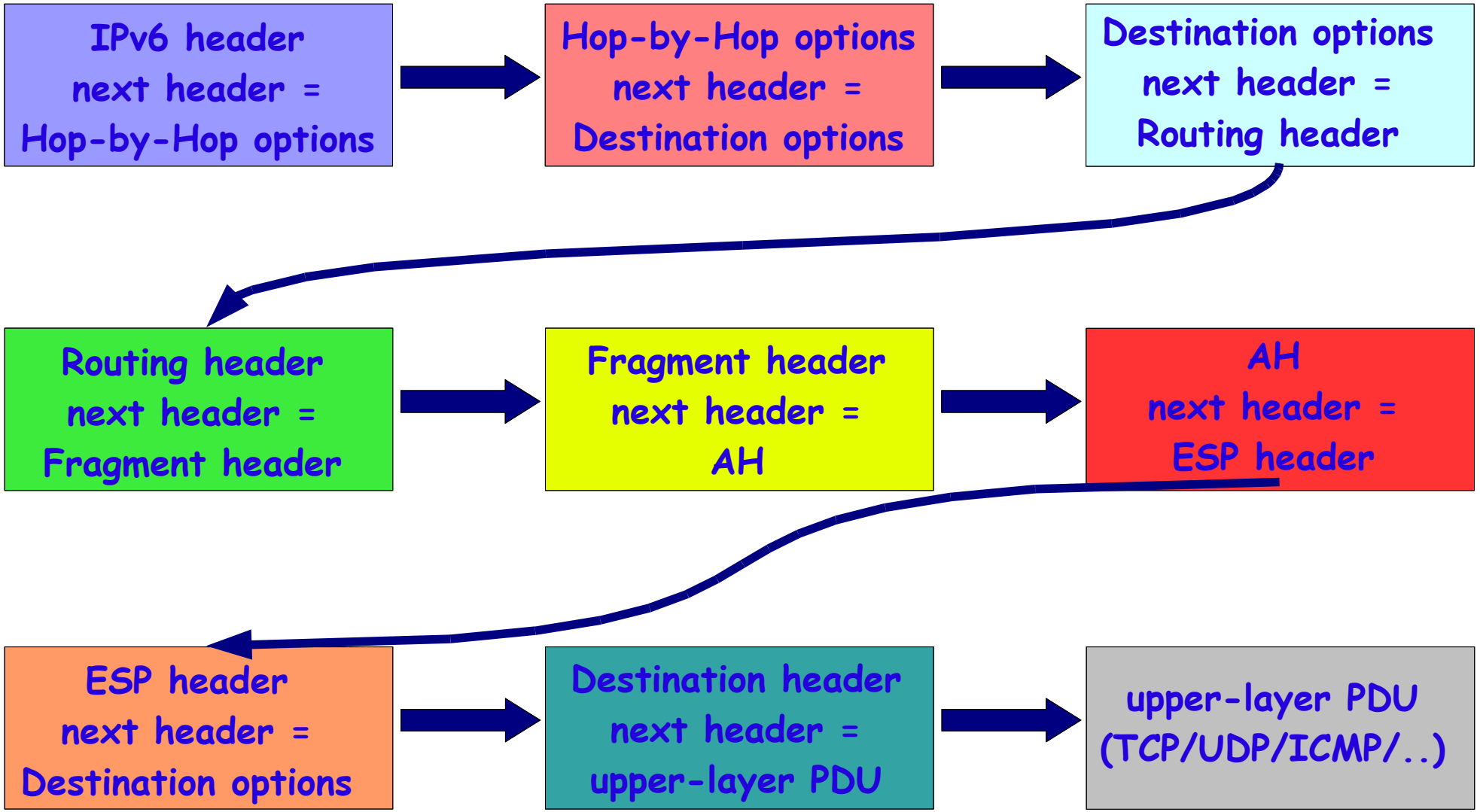
modified

deleted

Отличия заголовка IPv6

- Фиксированная длина
- Все необязательные параметры и опции – в заголовках расширения
- Нет контрольной суммы
- Поле длины не учитывает заголовок
- Поле TTL переименовано в соответствии с функцией

Заголовки расширения

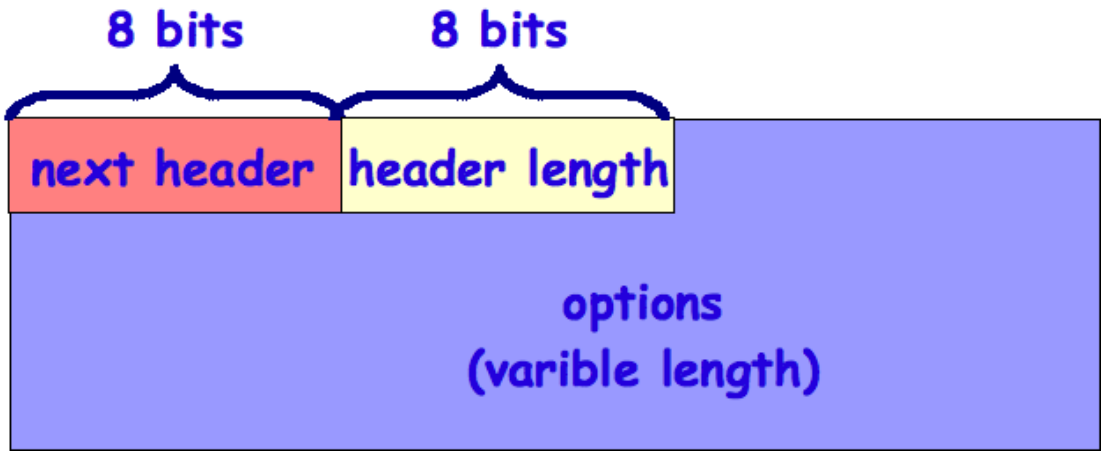


Обработка заголовков расширения

- Все (кроме Hop-by-Hop options) обрабатываются **адресатом**!
- Неопознанный заголовок – отбрасывание пакета
- Порядок заголовков – рекомендован, но необязателен (исключение - Hop-by-Hop)
- Специальный код заголовка 59 «no next header»

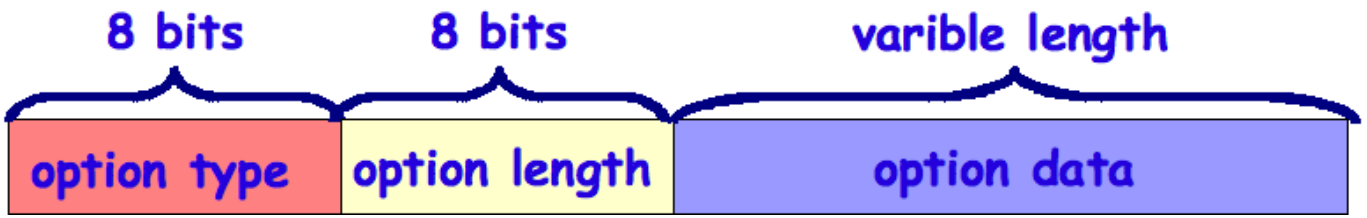
Заголовки опций

- Деление на Hop-by-hop и Destination удобно:
  - обработка промежуточными узлами
  - шифрование
  - фрагментация
- Hop-by-Hop options: для промежуточных узлов
- Destination options: для получателя *(или того, кто указан в поле Destination address!)*
- Произвольное число опций переменной длины



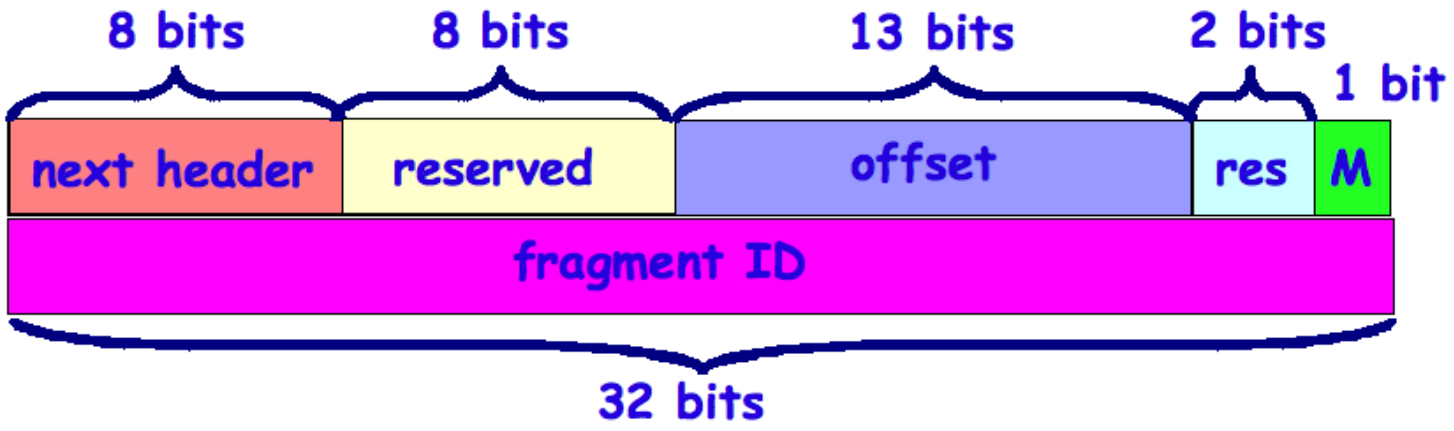
TLV-кодирование опций (type-length-value)

- Type: идентификатор опции
- Два старших бита типа: реакция на неизвестную опцию:
  - 00 – продолжить обработку
  - 01 – отбросить пакет
  - 10 – отбросить и отправить ICMPv6
  - 11 – отбросить и отправить ICMPv6 если адрес получателя не групповой
- Третий бит типа: меняется ли (1) или нет (0) опция при передаче пакета
- Length: длина данных в октетах



Заголовок фрагментации

- Offset: смещение (в 8-байтных единицах) от начала фрагментируемой части
- M: флаг последнего фрагмента
  - 0 – последний фрагмент
  - 1 – есть дальнейшие фрагменты



Уровень управления в IPv6

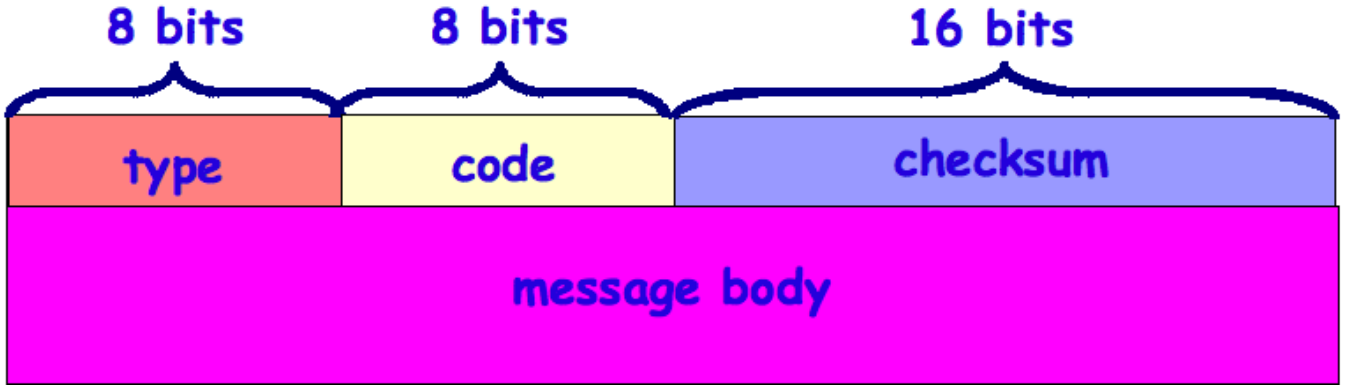
- Управляющие протоколы в сетях IPv4:
  - ARP (для случая Ethernet)
  - ICMP
  - IGMP
- Управляющий протокол в сетях IPv6:

ICMPv6

(номер протокола 58)

ICMPv6

- Type:
  - 0 – 127: сообщения об ошибках
  - 128 – 255: информационные сообщения
- Сообщение об ошибке содержит максимальную часть исходного пакета
- Не фрагментируются!
- Не высылаются в ответ на сообщения об ошибке и на широковещательные/групповые запросы



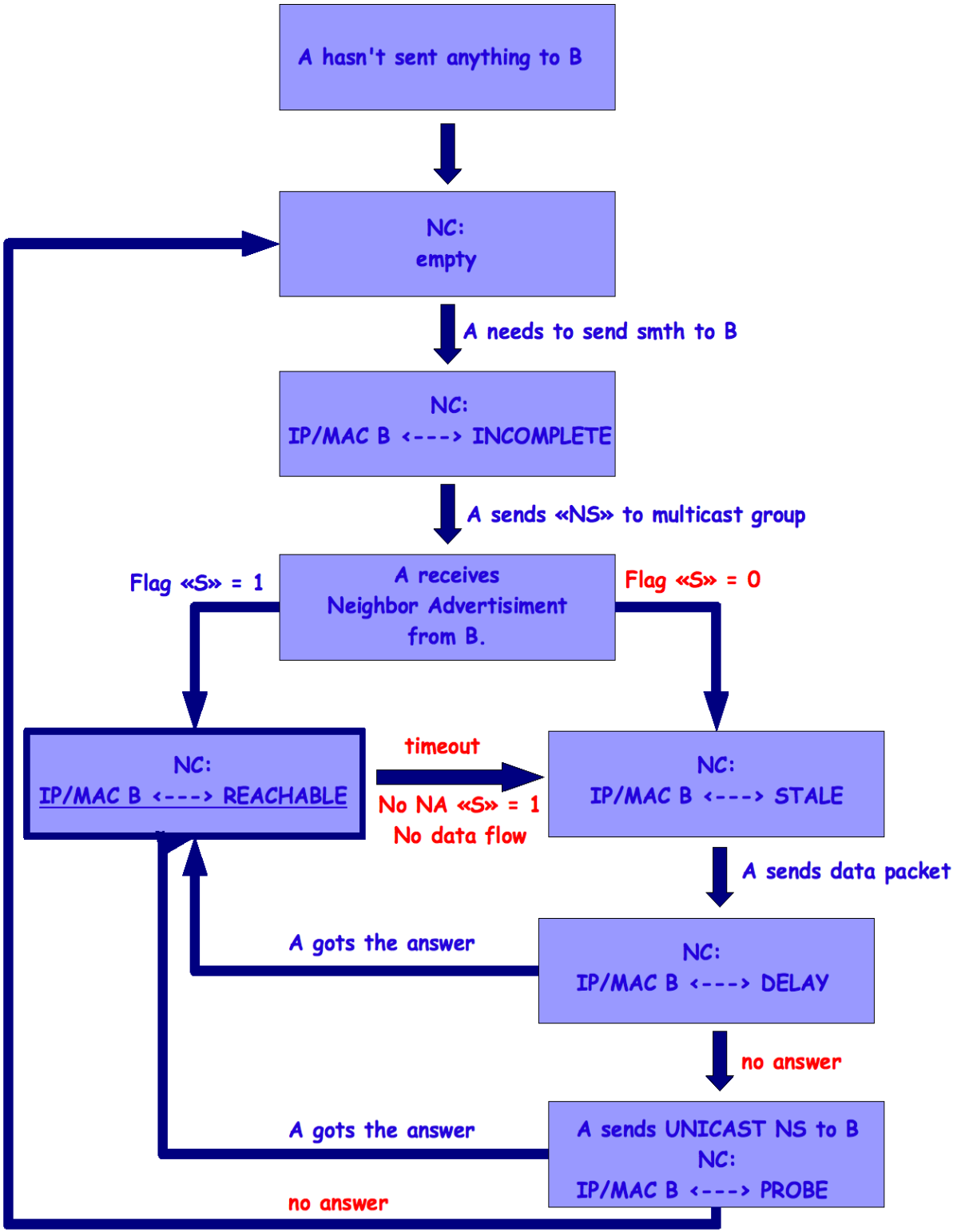
Роль мультикаста для IPv6 огромна!

- Узел IPv6 **обязан** поддерживать multicast!
- Широковещание = группа «все узлы канала»
  - *примечание: желательна поддержка IGMP snooping/GMRP на коммутаторах*
- Узлы с «близкими» IP-адресами входят в группу искомого узла *(solicited-node multicast address)*
  - *на 1 интерфейсе всего одна группа при правильной настройке адресов*
- Адрес группы:
  - глобальный префикс **FF02**::1:FF00:0:/104
  - младшие 24 бита адреса узла

Пример: узел 2001:db8::1:20cd:f345:5432:51d8 входит в группу FF02::1:FF00:0:32:51d8

Neighbor Discovery (ND)

- Подмножество ICMPv6
- Использует multicast (в отличие от ARP)
- Запрос информации: *neighbor solicitation (NS)*
- Выдача информации: *neighbor advertisement (NA)*
  - *флаг S=1 – ответ на запрос NS*
  - *флаг S=0 – «добровольный» анонс*
- Хранение информации:
  - *neighbor cache (NC)*
  - *destination cache (DC)*
- *Связь с более высокими уровнями!*


A hasn't sent anything to B
NC:
empty
A needs to send smth to B
NC:
IP/MAC B <---> INCOMPLETE
A sends «NS» to multicast group
A receives
Neighbor Advertisiment
from B.
Flag «S» = 1
Flag «S» = 0
NC:
IP/MAC B <---> REACHABLE
timeout
No NA «S» = 1
No data flow
NC:
IP/MAC B <---> STALE
A sends data packet
A gots the answer
NC:
IP/MAC B <---> DELAY
no answer
A gots the answer
A sends UNICAST NS to B
NC:
IP/MAC B <---> PROBE
no answer

ND-proxy

- На NS запрос может отвечать адресат или ND-proxy. Как избежать конфликта?
- NA содержит флаг «O» (override)
  - ND-proxy: O=0 (REACHABLE -> STALE)
  - адресат: O=1 (обновляет NC)

Достоинства ND

- Взаимодействие с вышележащими протоколами
- Контроль состояния соседей *(neighbor unreachability detection, NUD)*
- Уменьшение задержки при начала диалога

Anycast

- **Задача:** обеспечить обращение клиентов к любому серверу из группы (например, DNS, SMTP)
- Все устройства группы имеют одинаковый **anycast** IPv6 адрес
  - клиент в том же сегменте: флаг «O»=0 в NA
  - клиент в других сегментах: маршрутизация

Настройка IPv6 узла

- Настройка IPv6 адреса:
  - настройка идентификатора интерфейса
    - вручную
    - автоматически (напр. на основе MAC)
  - настройка префикса сети
    - вручную
    - автоматически
    - **известный префикс (link-local, FE80::/10)**
  - настройка доп. параметров (маршруты)

Автонастройка интерфейса

- MAC превращается в modified EUI-64
  - *возможны другие варианты (см. далее)*
- Как избежать конфликта?
  - совпадение MAC
  - совпадение адресов при иных методах
- Механизм ND позволяет найти владельца заданного адреса
- Вариация ND: Duplicate Address Detection (DAD)

Duplicate Address Detection

1. Узел X пытается назначить на интерфейс I адрес A
2. X вступает в группы:
    1. FF02::1
    2. FF02::1:FF00:0:A' *(«все узлы с адресом A»)*
3. X наблюдает за NS для адреса A с адреса :: (в фоне)
4. X отправляет NS для адреса A *(src ip = ::)*
5. Узлы с адресом A отвечают NA *(флаг S = 0)* на адрес FF02::1
6. До истечения timeout произошло событие 3 или 5 – **адрес занят!**
7. Отсутствие событий 3 и 5 – **адрес свободен**

Процедура повторяется несколько раз!

Для любого (не только автоматического) адреса!

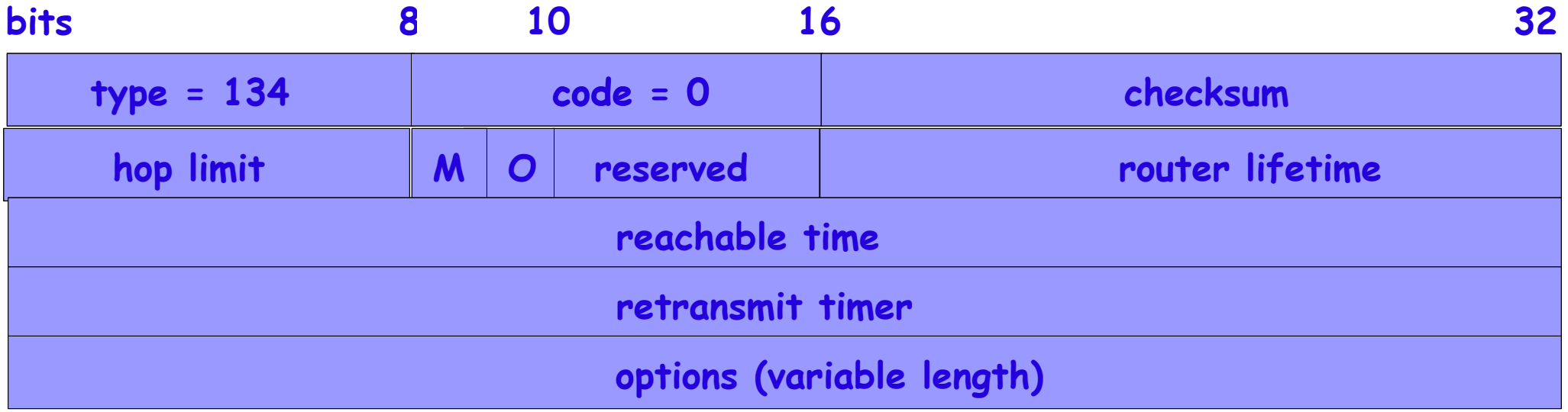
StateLess Address Auto Configuration (SLAAC)

- Link-local адреса + DAD = возможность взаимодействия на данном сегменте!
- Дальнейшие задачи:
  - настройка глобальных префиксов
  - поиск маршрутизатора по умолчанию
  - заполнение таблицы маршрутизации
- Вся информация доступна маршрутизаторам!
- Можно ли ее запросить?

Обнаружение маршрутизаторов

- Поиск маршрутизатора аналогичен поиску соседа
- Существует группа «все маршрутизаторы канала» FF02::2
- Клиент может отправить запрос «Router Solicitation», RS
- Маршрутизатор анонсирует себя при помощи «Router Advertisiment», RA

Формат сообщения RA



Src IP = link-local, Dst IP = адрес, с которого отправили RS или FF02::1

- Флаги M,O говорят о возможности получения адресов (M) и доп. параметров (O) по протоколу DHCPv6
- Router lifetime (секунды) – период использования маршрутизатора как маршрутизатора по умолчанию (0 – не использовать вовсе/удалить!)
- Reachable time (миллисекунды) – timeout для записи в NC (переход от Reachable к Stale)
- Retransmit timer (миллисекунды) – интервал между сообщениями NS

Что можно передать в RA?

Дополнительная информация передается в разделе options

- Список префиксов для SLAAC и их параметров
  - длина префикса
  - время жизни
  - назначение (настройка адреса или таблицы маршрутизации)
- MTU каналов
- Link-layer адрес маршрутизатора (для обновления NC)

Несогласованные значения на разных маршрутизаторах – путь к нестабильности!

ND: меры безопасности

- ND работает в пределах канала
- Сообщения ND не должны маршрутизироваться
- Маршрутизация уменьшает TTL
- TTL < 255 может говорить о маршрутизации *(однако «0-1=255»!!)*
- **Generalized TTL Security Mechanism (GTSM)** (RFC5082)

Атаки на ND

- Возможна подмена ответа (NA)
- Как убедиться в подлинности ответа NA?
- Подпись сообщения?
- Симметричная криптография неустойчива к кражам ключа на одном узле
- Асимметричная криптография: распределение ключей. Как убедиться, что ключ именно данного узла, а не злоумышленника?

Дайте мне точку опоры..

- Масштабируемый способ распределения ключей
- Присоединение открытого ключа к сообщению
- Проверка отпечатка ключа
- IPv6 адрес идентифицирует узел!
- Связь адрес <-> отпечаток ключа

Создание Cryptographically Generated Address

- сгенерировать пару ключей для узла;
- вычислить идентификатор интерфейса как отпечаток открытого ключа;
- составить адрес из префикса подсети и идентификатора интерфейса;
- внести ключи в настройки узла;
- назначит адрес интерфейсу узла;
- распространить сведения о новом адресе в сети (DNS, etc)

Отпечаток ключа (адрес) можно менять время от времени, добавляя случайный параметр!

Проверка CGA

- Проверка соответствия адреса и приложенного ключа
- Проверка подписи сообщения;

Необходимо расширить формат сообщений ND для передачи параметров CGA и открытого ключа

Расширение получило название SEcure ND (SEND)

SEND: Защита автонастройки

- CGA можно использовать если известен IP
- В случае RA адрес маршрутизатора неизвестен (злоумышленник может разослать RA)
- Применяется выдача маршрутизаторам сертификатов, подписанных УЦ
- Корневой сертификат распространяется на клиентские устройства

Big Brother is watching you!

- Получение идентификатора интерфейса из MAC адреса – постоянный идентификатор
- Перемещение пользователя (дом-работа-интернет-кафе-отпуск-командировка):
  - смена префикса сети
  - идентификатор узла остается постоянным!
- Возможность нежелательной идентификации!

Обеспечение privacy

- Задача: менять идентификатор узла
- Условие: сохранить SLAAC
- Требуется уникальность в пределах канала, а не глобально
- Адрес может быть случайным
- Проверка с помощью DAD (как для любого адреса)
- Обнаружение дубликата – создание нового адреса!

Default Address Selection

- Многообразие методов настройки адреса
- Противоречивые требования
- Легкость идентификации в корп. среде
- Сохранение privacy в Internet
- Более одного адреса на интерфейсе (+link-local)
- Выбор адреса зависит от адреса назначения!

См. RFC5220 «Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules»

Фрагментация

Фрагментация – зло!

- Нагрузка на устройства (фрагментация, сборка, промежуточная сборка)
- Снижение производительности при потере фрагментов
- Коллизии при сборке

- **Причины фрагментации:**
  - изменения MTU на пути следования (!туннели!)
  - реализации стека TCP/IP

Блокировка PMTUD – бесследное исчезновение пакетов

Фрагментация в IPv6

Только сквозная (end to end)!

- Нет аналога DF-бита
- Мин. MTU = 1280 байт
- Пакет > MTU отбрасывается, отправляется ICMPv6

Варианты:

- Фрагментация до размера 1280 байт (1232 байта полезной нагрузки)
- PMTUD и сохранение значения MTU в Destination Cache (DC)
- Связь приложения и уровня IPv6 через API (напр. сокеты Беркли, RFC3542)

Опция	Смысл
IPV6_USE_MIN_MTU	Использовать минимальный MTU (1280 байт)
IPV6_PATHMTU	Запросить приближение PMTU для подключенного сокета
IPV6_RECVPATHMTU	Разрешить возврат приближения PMTU из вызова *recvfrom()*
IPV6_DONTFRAG	Запретить фрагментацию исходящих пакетов сокета

IPv6 и DNS

Новый тип RR: запись типа AAAA

furry:~ furry$ dig www.kame.net aaaa

www.kame.net. IN AAAA 2001:200::8002:203:47ff:fea5:3085

Обратная зона:

- Домен ipv6.arpa
- Гранулярность делегирования – полубайт (1 символ в записи адреса)

Адрес 2001:db8::20:219f:bd8c:17af

f.a.7.1.c.8.d.b.f.9.2.1.0.2.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ipv6.arpa. PTR

Следует использовать $ORIGIN

Миграция

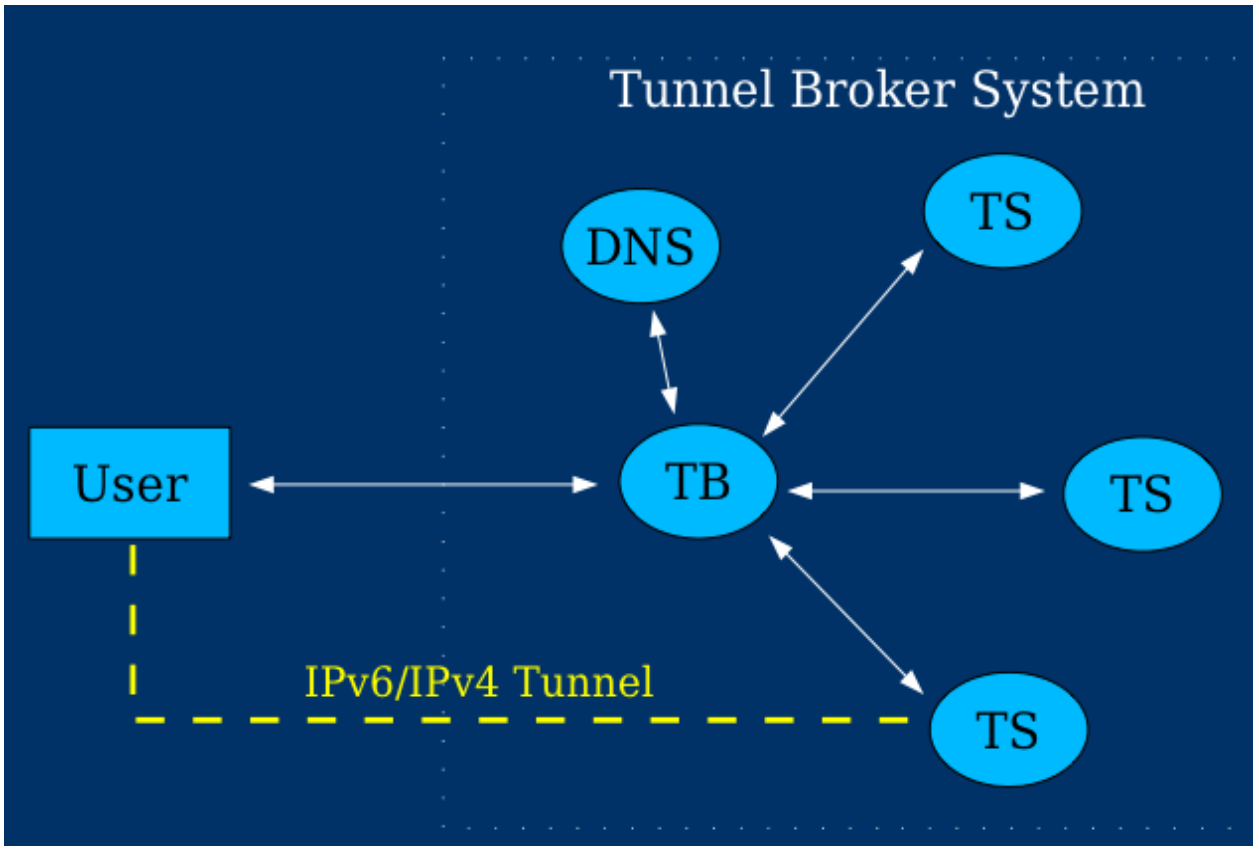
- Двойной стек IPv6+IPv4 на одном узле
  - уже сегодня IPv6 активирован на рабочих станциях
  - Windows: при наличии глобального IPv6 адреса – будет работать через него.
  - Дополнительная угроза безопасности!
- Объединение IPv6 облаков: туннели
- Подключение IPv6 сети к IPv4: трансляция адресов

Туннели

- 6to4 – наиболее распространен, требует наличия у концов туннеля публичных IPv4 адресов
- Teredo – инкапсуляция IPv6 в IPv4 & UDP
  - Поддерживает NAT-T
  - узлы получают глобальные IPv6 адреса
  - клиент-relay-сервер
  - включен в Vista по умолчанию (**teredo.ipv6.microsoft.com**)
- Угроза безопасности!!

Туннельные брокеры

- обширный список (с протоколами)
  http://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers
- Часто - web-интерфейс

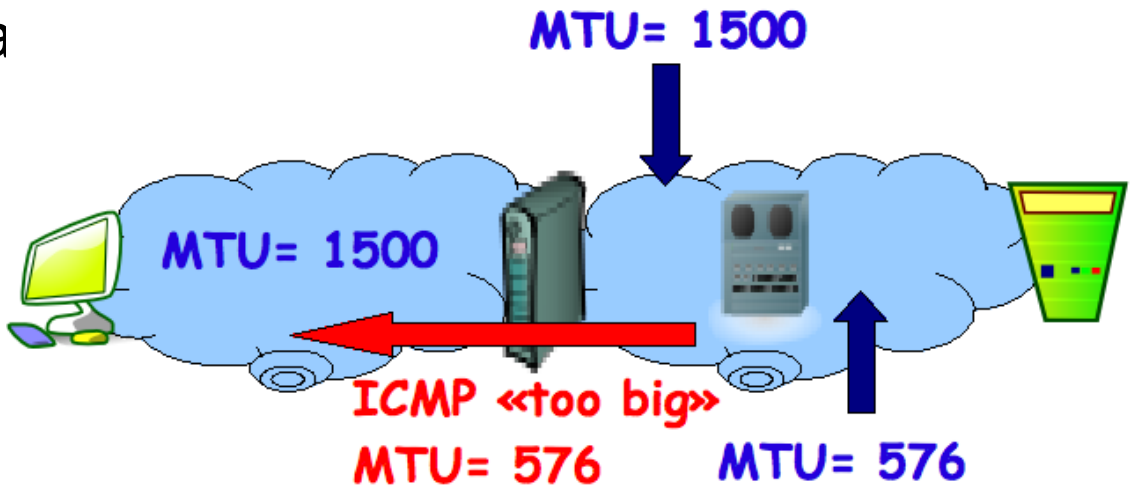


Трасляция адресов: NAT64

- http://tools.ietf.org/html/draft-bagnulo-behave-nat64-02
- Трансляция заголовков в соотв. с Stateless IP/ICMP Translation Algorithm (SIIT)
- IPv6 адреса отображаются в диапазон IPv4 адресов
- IPv4 адреса представляются как Pref64::IPv4

Фрагментация и NAT64

- Минимальное MTU в IPv4: 68 байт
- Минимальное MTU в IPv6: 1280 байт
- IPv4 - устройство может потребовать уменьшения MTU ниже порога 1280 байт
- IPv6 - узел может:
- уменьшить MTU
- включить Fragment hea



Преимущества IPv6

- Нет дробления адресного пространства
- Сквозная адресация, NAT не нужен
- Фрагментация только сквозная
- Стандартные механизмы на основе группового вещания, а не широковещания
- Механизмы обеспечения безопасности
- Единая система управления (ICMPv6)
- Автоматическая настройка
- Модульный заголовок

Немного о мифологии *«Неасилил, многа букф»*

- use DNS!
- «короткие адреса» при ручной настройке
- сокращенная нотация (много подсетей – можно выбрать короткие)

Сравним:

furry:~ furry$ dig www.ipv6porn.co.nz aaaa

www.ipv6porn.co.nz. 3324 IN AAAA 2002:3cea:4c32::1 (17 знаков)

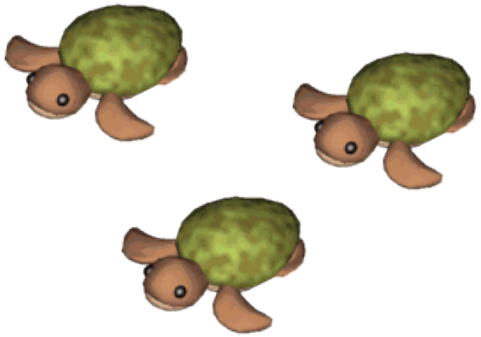
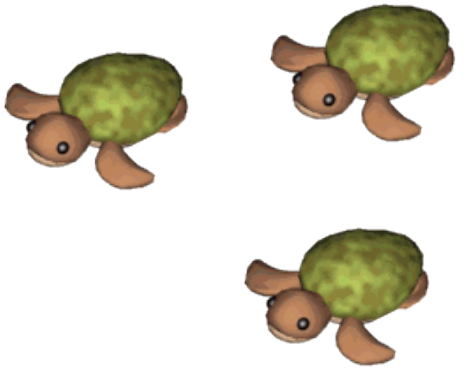
www.ipv6porn.co.nz. 3324 IN AAAA 2001:388:f000::285 (18 знаков)

furry:~ furry$ dig www.ipv6porn.co.nz a

www.ipv6porn.co.nz. 10000 IN A 60.234.76.50 (12 знаков)

Немного о мифологии
«Нам это не надо»

- Внутри ЛВС возможно стихийное возникновение IPv6 элементов.
- Безопаснее контролировать, нежели ликвидировать последствия
- Наблюдается рост числа внедрений - следует подготовиться

?