ИНФОРМАТИКА

УДК 004.057.4

ПОДХОДЫ К ИЗМЕНЕНИЮ МЕХАНИЗМОВ МАРШРУТИЗАЦИИ В СЕТЕВЫХ СТРУКТУРАХ

А.В. Воруев, В.Д. Левчук, С.М. Колаиб

Гомельский государственный университет им. Ф. Скорины

APPROACHES TO CHANGE OF ROUTING MECHANISMS IN NETWORK STRUCTURES

A.V. Varuyeu, V.D. Liauchuk, S.M. Kolaib

F. Scorina Gomel State University

В 2019 году в качестве альтернативы действующей IP-системе предложен новый подход оптимизации сетевого трафика, предполагающий сегментирование глобальных сетевых структур с уникальной идентификацией сервисов и IP-заголовком переменной длины. В статье рассматриваются способы организации глобальной маршрутизации. Проводится анализ текущей ситуации по распределению IP-пространств.

Ключевые слова: *системы агрегированной адресации NewIP, IPv4, IPv6, туннелирование IPv4-IPv6, преобразование адресов NAT, сегментная маршрутизация.*

In 2019, a new approach to optimizing network traffic was proposed as an alternative to the current IP system. It involves the segmentation of global network structures with a unique identification of services and a variable-length IP header. Ways of organizing global routing are considered in the article. The analysis of the current situation on the distribution of IP-spaces is carried out.

Keywords: *aggregated addressing systems NewIP, IPv4, IPv6, IPv4-IPv6 tunneling, NAT, segment routing.*

Введение

Стек протокола TCP/IP на базе системы адресации IPv4 обеспечивает задачи по оптимизации продвижения сетевого трафика с 1972 года. При всех инвестициях, которые были вложены в модернизацию данного протокола, очевидно, что изменение структуры пользовательского и служебного трафика IP-сетей, увеличение его объема в последние годы и необходимость обеспечения кибербезопасности в локальных и глобальных сетевых структурах создали необходимость внедрения новой концепции маршрутизации сетевого трафика.

Действующая иерархическая модель перераспределения сетевого трафика ограничена производительностью ключевых узлов связи.

Маршрутизируемый протокол – это сетевой протокол, обеспечивающий продвижение трафика между независимыми сегментами сетевых структур [1]. Адрес сетевого уровня должен

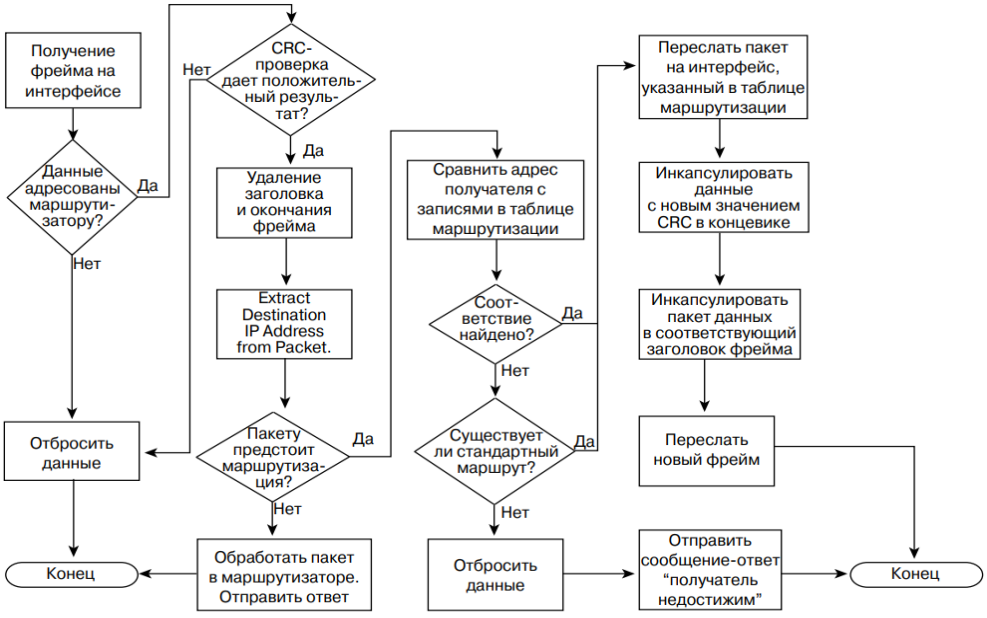

Рисунок 0.1 – Процесс трансформации данных в маршрутизаторе

предоставлять достаточное количество информации для доставки пакета от одного сетевого узла другому. Протокол предопределяет форматы полей внутри пакета. Подразумевается, что пакеты передаются от одной конечной системы другой без дополнительного преобразования (рисунок 0.1). Маршрутизируемый протокол использует таблицу маршрутизации для пересылки пакетов на всех промежуточных узлах ретрансляции. Участок передачи данных должен быть моногенным, то есть использовать единую версию протокола адресации.

Используемый в глобальных сетевых структурах, протокол IP не отвечает за установку соединений, не является надежным и позволяет реализовать только негарантированную доставку данных.

1 Иерархическая маршрутизация IP

Формальная структура продвижения трафика в IP-сетях основана на иерархии последовательного поиска сети назначения, в которой находится узел назначения трафика (рисунок 1.1).

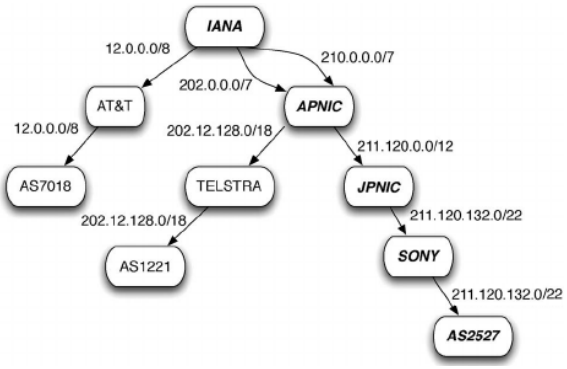

Рисунок 1.1 – Иерархическая соподчиненность автономных зон IPv4

Когда трафик находится в пределах смежных сетей (условно локальный тип трафика), его обслуживание обеспечивает одно устройство или группа ближайших устройств. Эта группа входит в автономную зону местного провайдера. Общая структура автономных зон, обеспечивающих IP-трафик Беларуси, включает 132 элемента (рисунок 1.2).

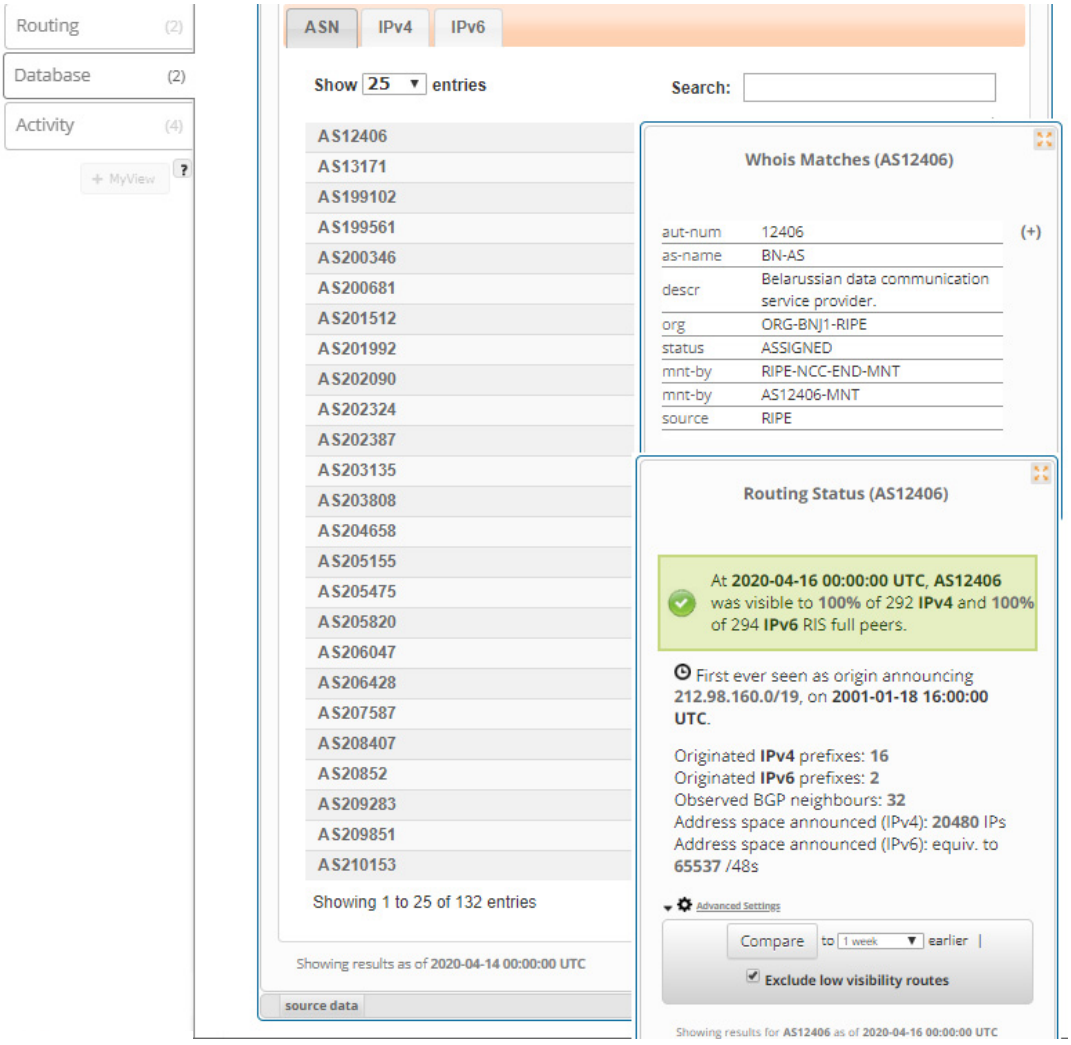

Рисунок 1.2 – Перечень ASN Database https://stat.ripe.net/BY

Участок автономной зоны передачи данных предполагает работу с IP-моногенным трафиком. Другими словами, прозрачность автономной зоны при прохождении IPv4 или IPv6 трафика обеспечивается на уровне операционных систем узлов трансляции и межузловыми связями.

Доступность узла назначения для трафика обоих типов должна поддерживаться локальной операционной системой, операционной системой узла «точки разграничения» на границе между сетью провайдера и сетью назначения, а также тарифным планом провайдера для этого абонента.

2 Трансляция адресов

Коммерческое применение IP-адресации столкнулось с критическими прогнозами по масштабированию адресного пространства одновременно с утверждением ее в качестве стандарта.

Предложенное решение, зафиксированное в RFC1918, заключалось в отсекании «тупиковых сетей» от общей иерархии маршрутов методом изоляции их адресных пространств. Роль посредников в продвижении IP-трафика между изолированными оконечными устройствами и остальной сетью играют трансляторы сетевых адресов (network address translator).

Изолированная сеть становится отдельным IP-слоем с собственной структурой иерархии маршрутов. При появлении трафика, который должен быть направлен в другую сеть, транслятор осуществляет преобразование адресного поля и становится источником вновь сформированного запроса для внешней сети (рисунок 2.1).

На рисунке 2.1 Inside – внутренняя тупиковая сеть с «частной» (private) адресацией; Outside – «публичные» (public) адреса, расположенные во внешней сети; Inside local IP address – IP-адрес, который был назначен узлу во внутренней сети, не входящий в диапазон глобальной маршрутизации; Inside global IP address – адрес, назначаемый пакету данных транслятором из глобально адресного пространства, предоставляемого провайдером [2].

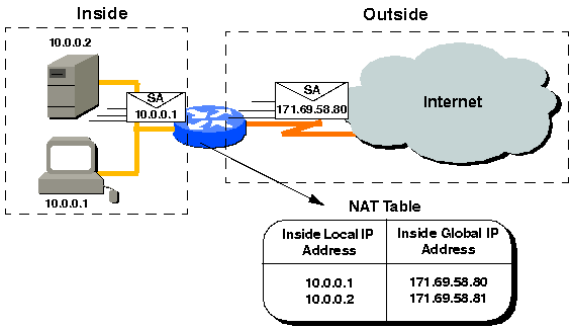

Рисунок 2.1 – Роль устройства трансляции адресов

Неизбежным недостатком реализации такого подхода стали временные издержки и изменение структуры информационной безопасности. В такой среде установить соответствие между источником IP-данных и получателем на стороне отправки данных достаточно сложно. Следствием стало сворачивание целого направления IP-сервисов.

Тем не менее, технология NAT останется промышленным стандартом до момента завершения использования системы адресации IPv4.

3 Интеграция IPv6

Параллельно с развитием технологии трансляции адресов реализовывался комплекс мер по переводу IP-сетей на систему адресации IPv6 с более широкой емкостью адресного поля. Увеличение размера IP-адреса с 32 до 128 бит не только решает проблему дефицита адресного пространства, но и позволяет добиться IP-моногенности на траектории всего маршрута между источником данных и пунктом назначения. Структура иерархии остается неизменной (рисунок 3.1). Дополнительная нагрузка на содержание таблиц маршрутизации и трансляцию трафика возлагается на провайдеров.

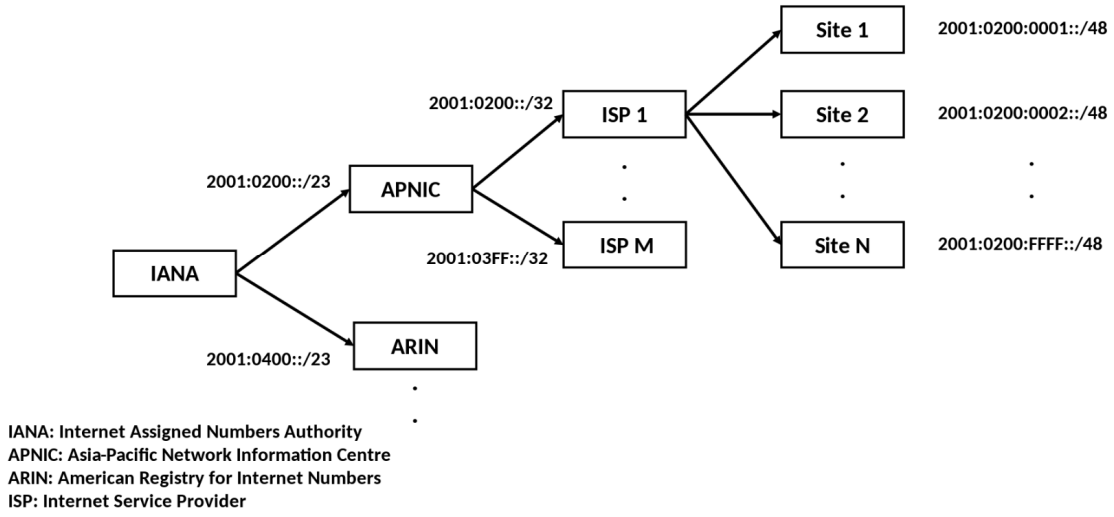

Рисунок 3.1 – Иерархическая соподчиненность IPv6

После реализации указа Президента РБ №350 от 21 сентября 2019 года по обязательной поддержке адресации IPv6 для провайдеров стеки протоколов IPv6 и IPv4 должны использоваться параллельно (этот режим называется dual stack), с постепенным увеличением доли трафика IPv6, по сравнению с IPv4 в общей доле IP трафика страны.

Агрегируемый глобальный IPv6-адрес Unicast является глобально уникальным и аналогичен IPv4-адресу Unicast Public. Используется префикс 2000::/3. Поэтому, как правило, адресное пространство IPv6, полученное в аренду, равно /48 (более $1{,}2 \cdot 10^{24}$ адресов узлов). Такой адресный пул может быть дополнительно разделен на 65536 подсетей (рисунок 3.2).

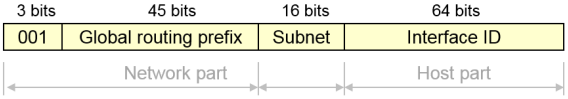

Рисунок 3.2 – Структура IPv6-адреса

Провайдеры Беларуси начали резервировать диапазоны IPv6 в 2004 году. На текущий момент для провайдеров Беларуси выделены следующие диапазоны IPv6 адресов 2001:67c:18a8::/48, 2001:67c:2268::/48, 2001:67c:57c::/48, 2001:7f8:5a::/48, 2001:7f8:8b::/48, 2a00:1760::/29, 2a00:6440::/32, 2a00:c820::/29, 2a01:6e40::/32, 2a02:2208::/29, 2a02:bf0::/32, 2a02:d240::/29, 2a02:e300::/29, 2a03:3000::/29, 2a03:5be0::/32, 2a03:9120::/32, 2a03:9b60::/32, 2a03:c740::/32, 2a04:2e80::/29, 2a04:9b40::/29, 2a04:cc40::/29, 2a06:1280::/29, 2a06:4800::/29, 2a07:200::/29, 2a0a:7d80::/29, 2a0a:eac0::/29, 2a0a:f240::/29, 2a0b:8680::/29, 2a0c:b1c0::/29, 2a0d:2d00::/32.

Размер объединенного адресного поля, охватываемого этими диапазонами, составляет более $1{,}1 \cdot 10^{31}$ адресов узлов, что более чем необходимо для коммерческой практики на ближайшие годы.

Довольно большой объем трафика переводится на использование адресов формата Link-Local с префиксом FE80::/10. Условное подобие в модели IPv4 можно найти при использовании Unicast Private адресов, хотя принципы назначения и использования адресов Link-Local уникальны для IPv6. Такой подход сказывается на различии в подходах к реализации программной части приложений для работы в локальных, глобальных и межузловых сетях. В качестве попутного положительного свойства данный подход помогает скрывать от возможных кибератак операционные системы ретранслирующих узлов, поскольку они не участвуют в общем поле адресации домена маршрутизации (рисунок 3.3).

Другими словами, окно возможностей у технологии достаточно широкое, наряду с поддержкой со стороны технического сообщества. При этом внедрение IPv6 в действующих сетях идет медленно. Технические проблемы внедрения IPv6 наглядно демонстрирует факт задержек и проволочек в ее практическом применении в течение 24 лет после утверждения стандарта.

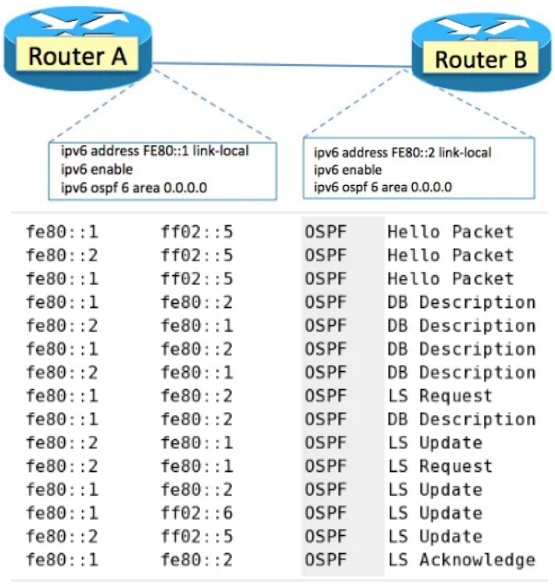

Рисунок 3.3 – Локализация трафика между соседними устройствами на траектории маршрута в глобальной сети [3]

4 Обходы требования по IP-моногенности

Поскольку в глобальных сетевых структурах невозможно достигнуть синхронного единообразия в подходах в работе операционных систем узлов связи, то поддержка протоколов обновленной адресации будет внедряться в разное время и, возможно, неполнофукционально.

Например, в случае неудовлетворительных результатов текущей интеграции Dual Stack и / или полного перехода трафика провайдера в режим передачи данных IPv6 (что будет вероятной практикой для вновь создаваемых сетевых подключений) системный администратор сети для объединения сетевых сред IPv6 через сеть IPv4 сможет использовать решения IPv4-IPv6 туннелирования. Пример таких переходных зон поддержки протоколов представлен на рисунке 4.1 [4]. В используемом примере, используется разрыв непрерывного поля адресации IPv6 (IP-разрыв).

Для решения задач IPv4-IPv6 туннелирования необходимо наличие эффективной связи между сегментами сети с помощью средств второго IP-протокола. На участке Сегмента 3 достаточно объявить туннель IPv6 over IPv4. Для доставки IPv6 трафика задействуется канал IPv4. По условиям примера после прохождения тоннеля все клиенты IPv6 смогут реализовать полноценную двустороннюю связь.

Следует особо подчеркнуть, что при инкапсуляции туннелируемого трафика пакет-носитель IPv4 добавляет свои адресные данные поверх

Протокол IP	Сегмент 1	Сегмент 2	Сегмент 3	Сегмент 3			Сегмент 4	Сегмент 5
IPv4	+	+	+	+	+	+	-	-
IPv6	+	+	+	+	-	+	+	+

Рисунок 4.1 – Пример карты сети с разным уровнем поддержки IPv4/IPv6

Протокол	Сегмент 1	Сегмент 2	Сегмент 3	Сегмент 3			Сегмент 4	Сегмент 5
OSPFv2	+	+	+	+	+	+	-	-
OSPFv3	+	+	+	+	-	+	+	+

Рисунок 4.2 – Разрывы в работе версий протокола OSPF

Протокол	Сегмент 1	Сегмент 2	Сегмент 3	Сегмент 3			Сегмент 4	Сегмент 5
OSPFv2	+	+	+	+	+	+	-	-
OSPFv3	+	+	+	+			+	+

Рисунок 4.3 – Расширение зоны действия протокола OSPFv3

передаваемого пакета IPv6. Поскольку размер итогового сетевого пакета (после инкапсуляции) не должен превышать ограничение MTU в 1500 байт. Для этого необходимо на стороне отправителя уменьшить поле блока данных на размер внедряемых служебных данных, который на иллюстрируемом примере составляет 24 байта.

На рисунке 4.2 показаны участки, доступные для работы версий протокола OSPF до настройки туннелирования.

Как можно видеть из рисунка OSPFv2 работает только в зоне адресов IPv4, а OSPFv3 – в зоне адресов IPv6. После построения туннелей картина немного меняется (рисунок 4.3).

Поскольку для работы протоколов динамической маршрутизации необходим сбор служебных данных о топологии сети с целью поиска оптимального маршрута продвижения IP-пакетов, то параллельная работа двух версий протокола OSPF может увеличить нагрузку на каналы связи. Каждая из версий протокола OSPF рассылает сообщения канального уровня, описывающие маршрутизаторы и сети, которые вместе образуют базу данных состояния каналов (LSDB) на каждом маршрутизирующем устройстве.

Следует учесть, что данные для построения LSDB собираются на канальном уровне, а основная работа версий протоколов идет на сетевом уровне. Поэтому есть возможность оптимизировать служебный трафик.

В случае любой архитектуры тоннелей необходимо снижение размера параметра MTU IP-пакета, что повлияет на конечную скорость передачи трафика дополнительно.

Таким образом, сам принцип моногенности IP-трафика может выполняться не на всем участке сети от источника трафика до пункта назначения, а лишь на тех участках, где происходит первичный и последующие этапы туннелирования данных.

Учитывая, что механизм туннелирования снижает зависимость от параметра TTL как максимального количества шагов пересылки, данный тип решения фактически является необъявленным техническим стандартом в современных условиях.

5 Сегментная маршрутизация и модификация IP-адресации

На текущий момент большое число видов сеансов связи между приложениями предъявляют различные сетевые требования [5]. Например, приложения реального времени предпочитают сетевые траектории с малой задержкой и низким джиттером, а приложения с большими данными предпочитают туннели с высокой пропускной способностью и низкими показателями потери пакетов. Решение состоит в том, чтобы позволить сетевым процессам управлять развитием сети и определять архитектуру сети. В частности, приложение предъявляет требования (к задержке, пропускной способности и скорости потери пакетов). Контроллер собирает информацию, такую как топология сети, использование полосы пропускания и информацию о задержке, и вычисляет явный путь, который удовлетворяет требованиям обслуживания (рисунок 5.1).

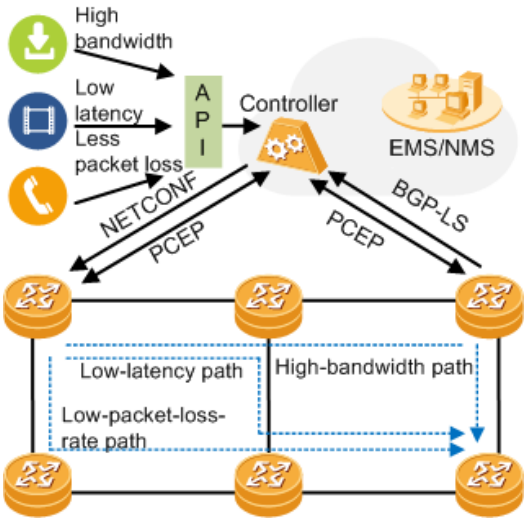

Рисунок 5.1 – Сервисно-управляемая сеть

Сегментная маршрутизация используется для простого определения явного пути. Узлы должны просто поддерживать информацию о сегментной маршрутизации, чтобы адаптироваться к требованиям сервиса в режиме реального времени.

Сегментная маршрутизация (Segment Routing, SR) – это протокол, предназначенный для пересылки пакетов данных в сети на основе исходных маршрутов. Маршрутизация сегмента MPLS – это маршрутизация сегмента на основе плоскости пересылки MPLS, которая также называется маршрутизацией сегмента. Маршрутизация сегментов разделяет сетевой путь на несколько сегментов и назначает идентификатор сегмента (SID) каждому сегменту и узлу пересылки сети. Сегменты и узлы расположены последовательно (список сегментов) для формирования пути пересылки.

Рост сегмента IoT-устройств, которые генерируют большой поток данных в направлении мобильного получателя (смартфон или другое автономное устройство пользователя) может потребовать многократное изменение маршрута доставки данных.

Частный случай, когда операционная система устройства автоматически переключается между поставщиком услуг связи, приведет к изменению IP-адреса абонента во время работы.

То есть IP-моногенность не выдерживается уже не по типу IP-адреса, а по его принадлежности провайдеру. Изменение геопозиции получателя в траектории доставки данных может привести к пересчету принадлежности к единой автономной зоне. Непрерывность сеанса связи в таких условиях не может быть обеспечена традиционными алгоритмами.

Критическая чувствительность к задержкам и разрывам в связи у современных приложений проиллюстрирована на рисунке 5.2.

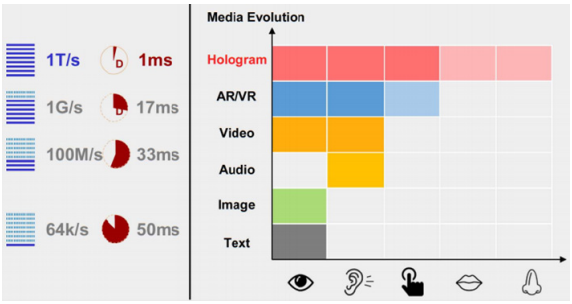

Рисунок 5.2 – Требования к полосе пропускания и задержкам контента разных типов

Протокол NewIP, предлагаемый специалистами компании Huawei, предоставляет более эффективные механизмы адресации и управления трафиком, а также решает проблему организации взаимодействия разнотипных сетей в условиях роста фрагментации глобальной сети [6].

Например, для IoT сетей желательно использование коротких адресов для экономии памяти и ресурсов, промышленные сети частично избавляются от IP-адресации для улучшения обмена данными, спутниковые сети не могут использовать фиксированную адресацию из-за постоянного перемещения узлов. Частично проблемы пытаются решить при помощи протокола 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks), но без динамической адресации он малоэффективен.

В новой технологии предлагается использование IP-адреса переменной длины, способствующего организации обмена данными между различными типами сетей. Для абстрагирования сервисов от IP-адресов предусмотрена возможность отказа от указания адреса источника или адреса назначения. В частности, этот режим предлагается для экономии ресурсов при отправке данных с датчика, т. к. не предполагается изменение адресата.

Допускается определение разной семантики адресов (рисунок 5.3). Например, помимо классического формата IPv4/IPv6, можно использовать вместо адреса уникальные идентификаторы сервиса. Идентификаторы обеспечивают привязку на уровне обработчиков и сервисов, не привязываясь к местоположению серверов и устройств, а также их потенциально переменной адресацией сетевого уровня. Идентификаторы сервисов позволяют обойтись без DNS и маршрутизировать запрос к ближайшему обработчику, соответствующему указанному идентификатору. Например, датчики в умном доме могут отправлять статистику определённому сервису вообще без определения его адреса в классическом понимании.

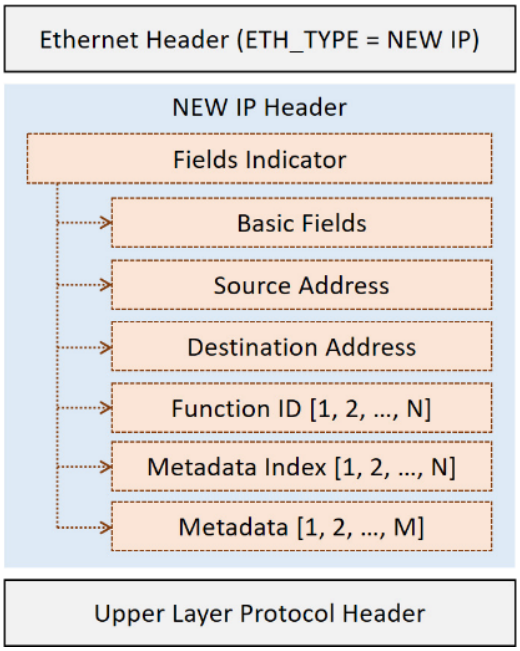

Рисунок 5.3 – Структура заголовка NewIP

В результате программный код оконечного устройства получит возможность гибко взаимодействовать напрямую (т. е. без устройств-посредников облачного и / или туманного типа вычислений), формируя направлено-адресуемый трафик сетевого уровня.

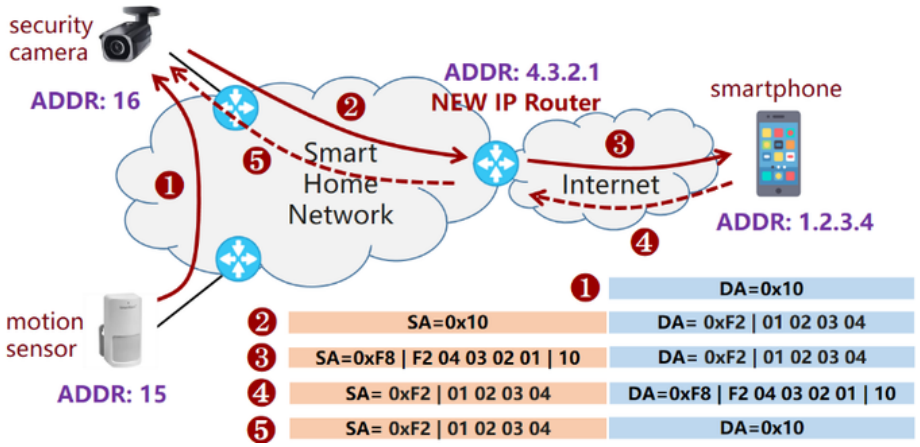

Рисунок 5.4 – Структура заголовка NewIP

На рисунке 5.4 в первом запросе от датчика движения отсутствует поле Source Address, поскольку устройство данного типа не предполагает обратного управления. Эти данные относятся к инициирующим событиям. На шаге 2 камера безопасности отправляет поток удаленному устройству Smartphone. Обеспечение ретрансляции трафика на данном шаге реализовано устройством NewIPRouter и внешней сетевой средой Internet. Таким образом, снижается нагрузка на устройство-источник при сохранении прямой уникальной идентификации адресата.

В шагах 3 и 4 можно увидеть функцию NewIP, аналогичную NAT по трансляции заголовка во внешний адрес, но с существенной оговоркой: удаленное устройство Smartphone имеет полную информацию об устройстве и уникальном идентификаторе сервиса, породившем информационный поток.

Заключение

Председатель IETF (Internet Engineering Task Force) Алисса Купер заявила, что развитие Интернета достигается с помощью модульных и слабо связанных строительных блоков, что является преимуществом Интернета.

Точка зрения Председателя IETF показывает, что сложившийся порядок технической анархии устраивает исполнительных лиц без учета мнения пользователей и разработчиков приложений.

Доклад Oxford Information Laboratory для стран-участников Северного Атлантического Альянса содержит предостережения о возможности внедрения разработчиками NewIP неких функций «нисходящего контроля над Интернет», что будет иметь последствия для безопасности и прав человека.

На собрании IETF в ноябре 2019 года представитель Huawei заявил, что NewIP представляет собой нисходящую общую архитектуру, дающую возможность тесно связать приложения с сетью, что и является первоначальным замыслом интернет-дизайна.

Разработка NewIP была предназначена только для удовлетворения технических требований быстрорастущего цифрового мира и не включала какой-либо механизм управления в структуру проекта. В то же время Huawei также отметила, что исследования и инновации в области новой информационной сети открыты для ученых и инженеров по всему миру, и они могут участвовать в этом и вносить в него свой вклад.

ЛИТЕРАТУРА

1. *Программа сетевой академии Cisco CCNA 1 и 2*: вспомогат. Руководство; пер. с англ. – 3-е изд., испр. и доп. – М. и др.: Вильямс. – 2007. – 1156 с.

2. *Cisco IOS Network Address Translation* (NAT). – Режим доступа: http://staff.ustc.edu.cn/~james/cisco/nat/60.html. – Дата доступа: 13.04.2020.

3. *Understanding IPv6*: *Link-Local* “*Magic*”. – Режим доступа: https://www.networkingwithfish.com/understanding-ipv6-link-local-magic/. – Дата доступа: 13.04.2020.

4. *Инкапсуляция магистрального трафика центра обработки данных* / А.В. Воруев, О.М. Демиденко, В.Д. Левчук, П.Л. Чечет // Проблемы физики, математики и техники. – 2018. – № 1 (34). – С. 88–93.

5. *New IP Technologies. Huawei Tech. Co., Ltd*. – Режим доступа: https://support.huawei.com/enterprise/en/doc/EDOC1000173015?section=j003. – Дата доступа: 13.04.2020.

6. *Huawei развивает протокол NEW IP, нацеленный на использование в сетях будущего*. – Режим доступа: https://www.opennet.ru/opennews/art.shtml?num=52648. – Дата доступа: 13.04.2020.

Поступила в редакцию 04.11.2020.