Independent Submission
Request for Comments: 8799
Category: Informational
ISSN: 2070-1721

B. Carpenter
Univ. of Auckland
B. Liu
Huawei Technologies

July 2020

Limited Domains and Internet Protocols

Ограниченные домены и протоколы Internet

Аннотация

Наблюдается четкая тенденция к изменению поведения и семантики сетей в соответствии с определенными наборами требования, применяемыми в ограниченной части Internet. Правила, принятые по умолчанию параметры, стиль управления сетями и требования безопасности могут существенно отличаться в таких ограниченных областях. В этом документе рассмотрены примеры таких областей (их называют также контролируемыми средами), отмечены новые решения и описана связанная с этим таксономия. Кратко рассматривается также стандартизация протоколв для ограниченных доменов. В заключение показана необходимость четкого определения «принадлежности к ограниченным ддоменам» и механизмов, позволяющих узлам безопасно подключаться к домену и находить других членов домена, включая граничные узлы.

Документ является результатом исследований авторов и прошел обсуждение и консультации в рамках IETF, но не выражает согласованного мнения IETF.

Оглавление

1. Введение

По мере продолжающегося роста и диверсификации сети Internet с реальной перспективой прямого и косвенного подключения десятков миллиардов узлов, наблюдается заметная тенденция к заданию требований, поведения и семантики на сетевом и локальном уровне. Однако термин «локальный» здесь имеет особое значение. Во многих случаях он может относится к физической или географической области - узлы одного здания, отдельный кампус, данное транспортное средство. В иных случаях это может быть множество пользователей или узлов, распределенных

в более широкой области, но собранных в одну виртуальную сеть через Internet, или одна физическая сеть, работающая параллельно Internet. Ниже это рассматривается более подробно. В документе такие сети названы «ограниченными доменами». Подобная ситуация может возникнуть и в изолированной от Internet сети, но это здесь не рассматривается. Однако следует помнить, что совместимость нужна и в изолированной сети.

Некоторые люди опасаются раздела Internet по политическим или языковым границам с помощью механизмов блокировки свободного перемещения информации. Эта не является темой данного документа, которые не рассматривает механизмы фильтрации (см. [RFC7754]) и не применяется к протоколам, которые предназначены для применения во всей сети Internet. Здесь обсуждаются лишь домены с определенными техническими требованиями.

Термин «домен» в этом документе не относится к доменным именам DNS, хотя в некоторых случаях ограниченный домен может случайно совпадать с доменом DNS. В частности при конфигурации DNS с расщепленным горизонтом (split horizon) [RFC6950] раздел может проходить по краю ограниченного домена. Недавнее предложение определить периметры внутри DNS [DNS-PERIMETER] также может рассматриваться как механизм ограниченного домена.

Другим термином, который используется в ином контексте, является «контролируемая среда» (controlled environment). Например в [RFC8085] этот термин служит для обозначения границ области действия, в которой может применяться определенная туннельная инкапсуляция. Конкретным примером является инкапсуляция GRE-in-UDP [RFC8086], в которой четко указано: «контролируемая среда предъявляет менее строгие требования, нежели Internet.» Например, трафик без контроля перегрузок может быть приемлемым в контролируемой среде. Эта же фраза может применяться для обозначения области действия протоколов QoS[1] [RFC6398]. Это не обязательно тот случай, где протоколы будут отказывать (fail) за пределами контролируемой среды, но они могут работать неоптимально. В этом документе предполагается, что на практике термины «ограниченный домен» и «контролируемая среда» означают одно и то же. Термин «управляемая сеть» (managed network) используется аналогичным образом, например, в [RFC6947]. В контексте защищенной групповой адресации определен термин «домен интерпретации для группы» (group domain of interpretation) [RFC6407].

Еще больше определений типов доменов имеется в документах о маршрутизации, таких как [RFC4397], [RFC4427], [RFC4655]. Понятие ограниченного домена используется весьма широко в разных аспектах технологий Internet.

Требования ограниченных доменов зависят от варианта развертывания. Правила, принятые по умолчанию значения, поддерживаемые опции могут меняться в широких пределах. Стиль управления может меняться от полного отсутствия до автоматизированного управления в распределенном или централизованном варианте, а также в разных комбинациях перечисленного. Могут меняться и требования по безопасности и конфиденциальности.

В этом документе рассматриваются и анализируются некоторые последствия отмеченной тенденции и ее возможное влияние на идею универсального взаимодействия в Internet. Во-первых, приведены примеры вариантов и технических решений для ограниченных доменов с основным вниманием к Internet-уровню стека протоколов. В приложении приведена таксономия свойст ограниченных доменов. На этом фоне рассматривается проблема универсальности стандартов Internet в плане области действия и применимости. Отмечено, что некоторые протоколы, хотя и требуют стандартизации и совместимости, должны быть ограниченными в применении. Это предполагает необходимость формализации и обеспечения механизмов защиты для ограниченных доменов и принадлежности к ним. Документ не предлагает устройства таких механизмов, но задает некоторые функциональные требования.

Документ является результатом исследований авторов и прошел процедуры обсуждения и консультаций в IETF, но не является выражением согласованной точки зрения IETF.

2. Текущие отказы в Internet

Сегодня в Internet нет четкой концепции ограниченных доменов. В результате этого некоторые протоколы и функции не работают на определенных путях. Прежний анализ этой проблем концентрировался на потере «прозрачности» Internet [RFC2775], [RFC4924] или ответственности промежуточных узлов за такую потерю [RFC3234], [RFC7663], [RFC8517]. К сожалению проблемы возникают как в прикладных протоколах, так и в фундаментальных механизмах. Например, в Internet нет прозрачности для заголовков расширения IPv6 [RFC7872], а механизм Path MTU Discovery не обеспечивал надежности в течение многих лет [RFC2923], [RFC4821]. Фрагментация IP также ненадежна [FRAG-FRAGILE] и отмечены проблемы согласования TCP MSS [IPV6-USE-MINMTU].

С точки зрения безопасности широкое применение межсетевых экранов на границах сетей, воспринимаемых людьми, но неизвестных протоколам, ведет к различным отказам на прикладных уровнях. Имее реальный опыт и рекомендации, гарантированно при эффективного boundaries that are perceived by humans but unknown to protocols results in arbitrary failure modes as far as the application layer is concerned. There are operational recommendations and practices that effectively guarantee arbitrary failures in realistic scenarios [IPV6-EXT-HEADERS].

Задаваемые административно (например, правилами фильтрации в маршрутизаторах) подвержены утечкам, вызванным человеческими ошибками, особенно в случаях, когда ограниченный трафик домена представляется граничным маршрутизаторам обычным трафиком. Эта форма утечки становится значительно менее вероятной, если узлы должны быть явно настроены на обработку данного протокола ограниченного домена (например, за счет установки обработчика конкретного протокола).

Исследования ненадежности фрагментации IP [FRAG-FRAGILE] и фильтрации заголовков расширения IPv6 [RFC7872] убедительно показывают потерю прозрачности по меньшей мере для некоторых протокольных элементов и промежуточные устройства играют здесь свою роль. В двух следующих параграфах рассмотрены некоторые среды приложений, требующие свойств протоколов, которые невозможно или не следует поддерживать в масштабе Internet.

3. Примеры требований ограниченного домена

В этом разделе описаны примеры, в которых требования различных ограниченных доменовможно легко идентифицировать на основе приложения или технических решений. Спосок, естественно, не является полным и упорядочен по масштабам от меньшего к юольшему.

[1]Quality-of-service - качество обслуживания.

1. *Домашняя сеть*. Это обычно неуправляемая сеть созданная не специалистом. Сеть должна работать с «устройствами из коробки» от производителя и обеспечивать по умолчанию адекватный уровень защиты. Может потребоваться удаленный доступ. Требования и применимые принципы описаны в [RFC7368].

2. *Сеть небольшого офиса*. Иногда такие сети практически не отличаются от домашних, если те, кто отвечает за сеть не имеют или почти не имеют специальных знаний. Однако требования безопасности и конфиденциальности могут заметно отличаться. В некоторых случаях такие сети могут создаваться профессионалами с соблюдением рекомендаций по выбору и настройке оборудования, но оставаться без управления. Может требоваться удаленный доступ.

3. *Сеть транспортного средства*. Такие сети создаются производителями транспортных средств и могут включать устройства, добавленные владельцем или оператором транспортного средства. К элементам сети предъявляются высокие требования по надежности и производительности, оказывающие влияние на безопасность людей. Для некоторых функций может требоваться удаленный доступ, тогда как к другим он должен быть полностью запрещен. Требуется связь с другими транспортными средствами, дорожной инфраструктурой и внешними источниками данных. Примеры рассмотрены в [IPWAVE-NETWORKING].

4. *Сети SCADA[1] и другие сети, работающие в реальном масштабе времени*. Эти сети предъявляют конкретные требования, включая жесткие показатели работы в режиме реального времени. Множество примеров таких сетей рассмотрено в [RFC8578]. Одним из примеров является сеть строительных служб, разработанная специально для строительства конкретного здания, но с использованием стандартных компонентов. В любой момент может потребоваться добавление в сеть новых устройств. Отдельные части могут предъявлять высоркие требования к надежности, связанные с безопасностью людей. Может требоваться удаленный доступ к некоторым функциям при полном запрете доступа к другим. Крайним случаем является сеть, используемая для приложений виртуальной или дополненной реальности с высокими требованиями к задержкам.

5. *Сети датчиков*. Два предыдущих случая включают датчики, но некоторые сети могут быть осознанно ограничены датчиками, а также сбором и обработкой их сигналов. Они могут размещаться в отдаленных или труднодоступных местах и устанавливаться неспециалистами.

6. *Сети IoT[2]*. Этот термин очень гибок и охватывает многие инновационные типы сетей, включая специализированные (ad hoc) сети, формируемые спонтанно, и некоторые приложения 5G, представляется разумным считать, что пограничные сети IoT будут предъявлять специальные требования и использовать протоколы, которые полезны лишь в конкретном домене и из соображений безопасности не могут применяться для работы через Internet.

7. *Сети устройств с ограниченными возможностями*. Важным подклассом сетей IoT являются сети устройств с ограниченными возможностями [RFC7228], в которых узлы ограничены по энергопотреблению и пропускной способности, что требует использования очень экономных протоколов.

8. *Устойчивые к задержкам сети* могут состоять из сравнительно изолированных доменов, быть ограниченными по питанию (например, размещаться в глубоком космосе) и подключаться лишь периодически с очень большой задержкой в соединениях [RFC4838].Понятно, что требования к протоколам для таких сетей специфичны.

9. *Традиционные сети предприятий и кампусов* могут иметь значительную протяженность и включать множество сайтов со своим подключением к Internet. Интересно, что в рамках IETF такой вариант давно существующих сетей не анализировался в общем виде, за исключениям случаев, связанных с развертыванием IPv6 (например, [RFC7381]).

10. *Неприемлемые стандарты*. В корпоративных сетях могут возникать ситуации, когда решение, подходящее для Internet может приводить к локальным отказам или быть слишком сложным. Примером могут быть сложности, вызванные такими механизмами как ICE[3] [RFC8445], не оправданными внутри сети. Кроме того, ICE в некоторых случаях невозможно использовать по причине неизвестности адресов-кандидатов до организации соединения, в результате чего может требоваться иное локальное решение [RFC6947].

11. *Управляемые распределенные сети сервис-провайдеров и предприятий*, такие как соединения «точка-точка» на уровне L2 (Ethernet и т. п.) с использованием псевдопроводов, многоточечные L2 Ethernet VPNs, использующие услуги VPLS[4], или Ethernet VPN (EVPN) и L3 IP VPN. Обычно они характеризуются соглашениями об уровне обслуживания я части доступности, потери пакетов и, возможно, групповых служб. Это отличается от предыдущего случая тем, что используются такие сети в основном на инфраструктурах MPLS, требования к которым четко заданы IETF.

12. *ЦОД и хостинг*. Высокие требования к производительности, безопасности и приватности. Большое число независимых сетей «арендаторов», наложенных на общую инфраструктуру.

13. *Сети CDN[5]*, состоящие из распределенных ЦОД и путей между ними, простирающихся на тысячи километров. Множество подключений к Internet.

14. *Крупные сети Web*. Небольшой класс общеизвестных сетей, объединяющих в себе аспекты распределенных корпоративных сетей, ЦОД и CDN. Они имеют свои транснациональные сети в обход традиционных опереторов. Кодобно CDN, они имеют множество соединений с Internet, обычно предлагая свои услуги в каждой стране.

Еще три аспекта, хоть и не привязаны к конкретным типам сетей, сильно зависят от концепции ограниченных доменов.

[1]Supervisory Control And Data Acquisition - диспетчерское управление и сбор данных.
[2]Internet-of-Things - Internet вещей.
[3]Interactive Connectivity Establishment - интерактивная организация соединений.
[4]Virtual Private LAN Service - виртуальная частная ЛВС.
[5]Content Delivery Network - сеть доставки содержимого.

1. Многие из перечисленных типов сетей могут включать соединения через Internet на основе методов VPN[1]. Поэтому можно утверждать, что ограниченные домены могут перекрываться между собой с использованием методов виртуализации. Как отмечено выше, для использования в конкретном домене могут быть приспособлены те или иные методы туннелирования и инкапсуляции.

2. В сетях на основе намерений (intent-based) домены настраиваются и управляются в соответствии с абстрактной политикой, называемой намерением (Intent), для обеспечения подобающей работы сети [IBN-CONCEPTS]. Какие бы технологии не использовались для поддержки этого, они будут применяться в границах домена, даже если поддерживаемые доменом службы доступны глобально.

3. «Нарезка» сетей (network slicing) является формой виртуальной сети, состоящей из управляемого набора ресурсов, взятого из более крупной сети [ENHANCED-VPN]. Предполагается, что этот подход станет значимым в сетях 5G [USER-PLANE-PROTOCOL]. Какие бы технологии не применялись для «нарезки», потребуется четкое определение границ каждого «среза» в более крупном домене.

Хотя желание использовать общие решения и стандарты очевидно, это становится все трудней обеспечить с учетом широко меняющихся требований, перечисленных выше. Тем не менее, имеется тенденция при создании новых протоколов и расширений задаваться вопросом, как это будет работать через открытую сеть Internet. Здесь предлагается несколько иной подход - считать некоторые протоколы и расширения не предназначенными для работы через Internet. Требования и семантика таких протоколов имеют существенные ограничения (в отмеченном смысле).

Принято считать, что протоколы, предназначенные для ограниченного применения, имеют много шансов оказаться используемыми (возможно, некорректно) в других ситуациях, включая открытую сеть Internet. Это верно и означает, что ограниченное применение протокола не означает снижения требований к его устройству и безопасности. Фактически, протоколы ограниченного применения являются более сложными и предъявляют более высокие требования к безопасности, как будет показано ниже.

Тем не менее, разнообразие ограниченных доменов с особыми характеристиками вероятно приведет к появлению конкретных стандартов (включая ad hoc) для различных типов доменов. Будут предприняты попытки охватить каждый сектор рынка, но рынок потребует стандартизации решений в каждом секторе. Кроме того, будут приняты решения, которые фактически будут работать лишь в ограниченных доменах. История RSVP [RFC2205] показывает, что стандарт, созданный для работы через открытую сеть Internet, на деле этого не может. В общем случае больше нельзя считать, что протоколы, созданные по классическим правилам Internet, смогут реально работать во всей сети. Однако «открытая сеть Internet» должна оставаться универсальным средством соединения. Устранение этого конфликта является сложной задачей.

4. Примеры ограниченных доменов

В этом разделе перечислены примеры ограниченных доменов, которые были предложены или определены. Здесь намеренно не включены разные технологические решения L2, которые по определению применяются в разных доменах. Тем не менее, следует отметить, что с учетом недавних разработок, таких как TRILL[2] [RFC6325] и [SPB[3]], домены L2 могут быть очень большими.

1. *Дифференцированные услуги*. Механизм [RFC2474] позволяет сети назначать 6-битовые значения кодов обслуживания DSCP[4] с локальной значимостью каждому пакету IP. Имеются рекомендации по выделению кодов для управления поведением очередей на этапе пересылки, однако в целом эти коды предназначены для классификации, кондиционирования и (пере)маркировки пакетов на границах домена (если нет междоменного соглашения о маркировке пакетов).

2. *Интегрированные услуги*. Хотя этот механизм и не является неотъемлемой частью RSVP [RFC2205], многие годы эксплуатации показали, что интегрированные услуги можно эффективно реализовать лишь в ограниченном домене с подобающей настройкой оборудования и ресурсов.

3. *Виртуализация сетевых функций*. Как отмечено в [RFC8568], эта базовая концепция является темой продожающихся исследований систем, где виртуализованные сетевые функции организованы как часть распределенной системы. Такая организация функций с неизбежностью ведет к использованию того или иного домена с ограничениями, несмотря на то, что междоменная организация (оркестровки) тоже является предметом исследований.

4. *Цепочки сервисных функций (SFC[5])*. Этот метод [RFC7665] предполагает, что сетевые службы представляют собой цепочки отдельных сервисных функций внутри конкретного домена SFC (например, 5G). Как отмечено в RFC: «Возможно потребуется применять определенные функции на границе домена SFC, например, для предотвращения утечки информации SFC». Для инкапсуляции пакетов, проходящих через цепочку функций, применяются заголовки NSH[6] [RFC8300]: «Предполагаемая область действия NSH - один домен провайдера».

5. *Квитанции FAST*[7] сопровождают пакет, позволяя тому проходить через сеть или запрашивать конкретную сетевыую услугу [FAST]. «Билеты» имеют значение лишь в конкретном домене.

6. *Наложенные виртуальные сети ЦОД*. Общим требованием ЦОД, где размещается оборудование множества арендаторов (клиентов), является предоставление каждому клиенту защищенной частной сети, но при этом сети всех клиентов должны работать на основе общей физической инфраструктуры. В [RFC8151] описаны различные варианты решений, а также рассмотрены разрабатываемые спецификации. Включены также ситуации, где сеть арендатора физически разделена между несколькими ЦОД, но должна представляться пользователям как единый защищенный домен.

---

[1] Virtual private network - виртуальная частная сеть.
[2] Transparent Interconnection of Lots of Links - прозрачные соединения между большим числом каналов.
[3] Shortest Path Bridging - мост через кратчайший путь.
[4] Differentiated Services Code Point - код дифференцированного обслуживания.
[5] Service Function Chaining.
[6] Network Service Header - заголовок сетевой службы.
[7] Firewall and Service Ticket - квитанция (билет) для межсетевых экранов и служб.

7. *Сегментная маршрутизация*. Этот метод «ведет пакет через упорядоченный список инструкций, называемых сегментами» [RFC8402]. Семантика инструкция является локаотной для домена сегментной маршрутизации или даже для одного узла. Технически эти сегменты или инструкции представляются как метки MPLS или адреса IPv6, обеспечивающие их сементическую интерпретацию в домене.

8. *Автономные сети*. Как указано в [REF-MODEL], автономная сеть является также доменом безопасности, в котором агенты автономных служб используют автономную плоскость (уровень) управления [ACP]. These agents manage technical objectives, which may be locally defined, subject to domain-wide policy. Thus, the domain boundary is important for both security and protocol purposes.

9. *Домовые сети*. Как показано в [RFC7368], домашние сети имеют свои требования к протоколам, отличающиеся от требований корпоративных сетей и Internet в целом. Это включает протокол HNCP[1] [RFC7788], а также решение [HOMENET-NAMING] для именования и обнаружения.

10. *Творческое использование свойств IPv6*. Протокол IPv6 обеспечивает большую по сравнению с IPv4 гибкость.

    - Метки потоков, например, [RFC6294].
    - Заголовки расширений, например, для сегментной маршрутизации [RFC8754] или маркировки OAM[2] [IPV6-ALT-MARK].
    - Значимые биты адресов, например, [EMBEDDED-SEMANTICS]. Сегментная маршрутизация использует адреса IPv6 в качестве идентификаторов сегментов с локальной значимостью [RFC8402].
    - При использовании сегментной маршрутизации для программирования сети [SRV6-NETWORK] заголовки расширений IPv6 могут применяться взамен более сложной локальной функциональности.

    Заголовки расширений особенно интересны, поскольку их наличие является основной «точкой продажи» IPv6, однако новые заголовки практически невозможно размернуть в масштабе Internet [RFC7045] [RFC7872]. Следует отметить, что фильтрация заголовков считается важной проблемой безопасности [IPV6-EXT-HEADERS]. Прозводители и операторы стремятся гибко определять заголовки расширения для использования в ограниченных или специализированных доменах, например, [IPV6-SRH], [BIGIP], [APP-AWARE]. Предусмотрены также локально значимые поэтапные (hop-by-hop) опции, понятные маршрутизаторам внутри домена, но не внешним устройствам (например, [IN-SITU-OAM]).

11. *Детерминированные сети* (DetNet). Архитектура [RFC8655] и инкапсуляция [DETNET-DATA-PLANE] нацелены на поддержку потоков с экстемально низкими потерями данных и ограниченной задержкой, но лишь в части сети, понимающей DetNet. Как и для дифференцированных услуг концепция является фундаментальной.

12. *Домены обеспечения* (PvD). Архитектура [RFC7556] позволяет хостам, подключенным к нескольким сетям, явно узнавать детали услуг, предоставляемых каждой сетью.

13. *Область действия адресов*. Отметим, что некоторые адреса, в частности IPv6, имеют явно ограниченную область действия. Например локальные для канала адреса (link-local) действуют лишь на одном физическом соединении [RFC4291], а уникальные локальные адреса [RFC4193] ограничены слабо определенной областью локального сайта. Были определены также локальные для сайта адреса (site-local), но их сочли устаревшими по причине нечеткости концепции сайта [RFC3879]. Групповые адреса также явно ограничены в области действия [RFC4291].

14. В качестве примера прикладного уровня можно указать потоковые службы, такие как инфраструктура IPTV, которые основаны на стандартных протоколах, но не предоставляют глобального доступа.

Все перечисленные варианты доступны лишь в определенных доменах. Тем не менее, все они явно рассчитаны для реализации с оборудованием множества компаний в тысячах или миллионах сетевых доменов, поэтому стандартизация взаимодействия будет полезной. Этот аргумент может показаться не соответствующим приватным или фирменным реализациям, но они имеют тенденцию становиться фактическими стандартами в случае успеха, поэтому аргументы данного документа остаются применимыми.

5. Область действия протоколов в ограниченных доменах

Одним из следствий развертывания доменов с ограничениями в Internet является разработка, расширение и настройка некоторых протоколов так, что они будут корректно работать лишь между конечными системами таких доменов. Это в той или иной степени поощряется некоторыми имеющимися стандартами и назначением кодов для экспериментального или локального применения. В любом случае предотвратить эти процессы не удастся. Кроме того, поддержка таких направлений, как цепочки сервисных функций, сегментная маршрутизация детерминированные сети, в рамках IETF фактически поощряет развертывание ограниченных доменов. Если же IoT[3] станет реальностью, к Internet будут подключены миллионы граничных сетей, содержащих совершенно новые типы устройств, и каждая из таких сетей будет ограниченным доменом.

Поэтому следует обсудить вопросы стандартизации некоторых протоколов и расширений для взаимодействия внутри ограниченных доменов. Для таких протоколов не требуется поддержка взаимодействия через всю сеть Internet. Здесь возможные разные варианты при наличии множества доменов, использующих такие протоколы.

A. Если домен разделен на две части, связанные через Internet непосредственно на уровне IP (т. е. без туннельной инкапсуляции), протокол ограниченного домена независимо от своей специальной природы, если он использует стандартные форматы IP и не блокируется межсетевыми экранами. Простым примером является использование специального номера порта для протокола не-IETF.

   Такой протокол можно считать междоменным, поскольку сеть Internet прозрачна для него, даже если протокол имеет смысл лишь в ограниченном домене. Это не вносит ничего нового в архитектуру Internet.

[1] Home Network Control Protocol - протокол управления домашней сетью.
[2] Operations, Administration, and Maintenance - эксплуатация, администрирование и обслуживание.
[3] Internet of Things - Internet вещей.

B. Если протокол ограниченного домена не соответствует стандартным форматам IP (например, включает нестандартный заголовок расширения IPv6), он не сможет работать между парой доменов, соединенных напрямую через Internet на уровне IP.

   Такие протоколы можно называть внутридоменными и сеть Internet «непрозрачна» для них.

C. Если для протокола ограниченного домена явно указана непригодность за пределами домена, ни один из вариантов A и B не применим. Единственным решением будет создание общего виртуального домена. Например, можно использовать туннельную инкапсуляцию для создания общего виртуального домена. На границе домена все пакеты такого протокола должны отбрасываться.

D. Если протокол ограниченного домена имеет специфические для доменов варианты, реализации в разных доменах могут оказаться несовместимыми при соединении доменов по варианту C. Протокол при таком соединении может приводить к непредсказуемым отказам. Простым примером является любой протокол, использующий выделенный для эсперименотов номер порта. Связанные с этим вопросы рассматриваются в [RFC5704], включая достаточно сложный вариант использования Transport MPLS.

В качестве распространенного примера рассмотрим дифференцированные услуги [RFC2474]. Пакет с любым значением в 6 битах поля DSCP[1] имеет корректный формат для варианта A. Однако семантика кодов DSCP имеет локальную значимость, поэтому применим также вариант D. Фактически дифференцированные услуги могут поддерживаться через границы доменов лишь при наличии соответствующего соглашения между операторами. В иных случаях для полноценного взаимодействия нужны специальные функции на шлюзе. Более подробно это рассмотрено в [RFC2474] и [RFC8100].

В качестве провокационного примера рассмотрим предложенное в [IPV6-SRH] смягчение ограничений [RFC8200], позволяющее вставлять заголовки расширения в пакеты IPv6 «на лету». Если это делать так, чтобы измененные пакеты никогда не покидали ограниченный домен, применим вариант C. Если семантика вставляемых заголовков определена локально, применим также вариант D. В обоих случаях работа Internet за пределами ограниченного домена не нарушается. Однако внутри домена узлы должны понимать вариант протокола. Если вариант не стандартизован в виде формальной версии в учетом всех обстоятельств, предусмотренных [RFC6709], все узлы должны быть нестандартными для понимания варианта протокола. Для случая вставки заголовков расширения IPv6 это означает несоответствие [RFC8200] внутри домена даже при полном соответствии стандарту самих вставляемых заголовков. Помимо проблемы формального соответствия такие отклонения могут значительно усложнять отладку. Возможное практическое влияние такой вставки заголовков рассмотрено в [IN-FLIGHT-IPV6].

Отмеченное в разделе 4 (п. 5) предложение FAST также дает интересный пример. Семантика квитанций FAST [FAST] имеет ограниченную область действия. Однако они разработаны так, что в принципе могут передаваться через Internet в форме стандартизованных опций IPv6 hop-by-hop или даже в заголовках расширения IPv4 [IPV4-EXT-HEADERS]. Вопрос надежности использования таких вариантов в открытой сети Internet остается неясным [IPV6-EXT-HEADERS].

Мы пришли к выводу, что разумно явно определять протоколы ограниченных доменов как стандарты или фирменные механизмы при условии указания применимых вариантов, перечисленных выше, и четкого определения домена. Пока все относящиеся к делу стандарты выполняются за пределами домена, четко определенный протокол ограниченного домена не должен оказывать вредного влияния на сеть Internet. Однако, как указано ниже, нужны механизмы поддержки операций определения принадлежности к домену.

Отметим, что этот вывод не является рекомендацией к отказу от обычной цели, заключающейся в том, что стандартизованные протоколы должны действовать глобально и обеспечивать взаимодействие через открытую сеть Internet. Это лишь признание фактов несоответствия этой цели.

6. Функциональные требования ограниченных доменов

Учитывая то, что протоколы ограниченных доменов определялись в прошлом и несомненно будут определяться впредь, следует рассмотреть, как протокол может узнать о домене, где он работает, и как могут быть идентифицированы граничные ущлы домена. Как показывает описанная в Приложении A таксономия, домены имеют множество аспектов. Тем не менее, можно определить некоторые базовые свойства и функции, которые будут полностью или частично применимы во многих случаях.

Сегодня ограниченные домены создаются по сути путем тщательной настройки граничных маршрутизаторов и межсетевых экранов. Если домен имеет один или несколько адресных префиксов, назначение адресов хостам тоже нужно тщательно контролировать. Эти методы подвержены ошибкам и сочетание ошибок настройки с принятой по умолчанию маршрутизацией может приводить к выходу нежелательного трафика за пределы домена. Поэтому мы предполагаем, что домены следует по возможности создавать и поддерживать автоматически с минимальным участием человека в настройке. Далее рассмотрены требования к автоматическому созданию и поддержке домена.

Во-первых, создание топологического плана (карты) данного домена (физического или виртуального) позволяет четко определить границу домена. Однако сама по себе граница не имеет технического значения. На деле важна принадлежность узлов к домену и факт размещения узлов на границе между доменом и остальной частью Internet. Таким образом, важна идентификация не самой границы, а узлов, имеющих интерфейсы внутрь домена и наружу. Внутри домена передающему узлу нужно понимать, расположен адресат внутри или вне домена, а принимающим - получен пакет от внешнего или внутреннего узла. Граничным узлам следует различать свои внутренние и внешние интерфейсы (как физические, так и виртуальные).

Чтобы подчеркнуть важность идентификации границы домена, отметим проблему детерминированных сетей [RFC8557], где «все еще недостаточно четко определены границы домена, в котором может быть оганизован детерминированный путь». Это замечание можно обобщить.

С учетом отмеченного можно указать некоторые базовые функциональные требования. Основное допущение заключается в том, что операции управления принадлежностью к домену следует защищать криптографически, поскольку без этого домен не может быть надежно защищен от атак.

[1] Differentiated Services Code Point - код дифференцирования услуг.

1. *Идентификация домена*. Домен должен иметь уникальный проверяемый идентификатор, фактически это будет открытый ключ домена. Без этого невозможно обеспечить безопасность работы домена и принадлежности к нему. Владелец соответствующего секретного ключа будет привязкой доверия для домена.
2. *Вложенность*. Домены могут быть вложенными (см. приведенный выше пример «нарезки сетей»).
3. *Наложение*. Узлы и каналы могут входить в несколько доменов (см. упомянутый выше случай PvD).
4. *Выбор для узла*. Узел должен иметь возможность определить домены, к которым он может присоединиться и применяемые для этого интерфейсы.
5. *Безопасная регистрация*. Узел должен иметь возможность зарегистрироваться в данном домене, используя безопасную идентификацию, и получить ссответствующие свидетельства (предоставление полномочий) для выполнения операций в домене. На узлах с несколькими физическими или виртуальными интерфейсами может потребоваться отдельная регистрация для каждого интерфейса.
6. *Отзыв*. Узел должен иметь возможность отозвать регистрацию в данном домене.
7. *Динамическое членство*. Узлам может предоставляться возможность временного выхода (отключения) из домена (регистрация сохраняется, но принадлежность к домену прекращается).
8. *Роль*, предполагающее предоставление прав выполнять некие действия. Узел должен иметь проверяемую роль. В простейшем случае узлы делятся по ролям на внутренние и граничные. В граничных узлах роли интерфейсов могут различаться (например, внешние и внутренние).
9. *Проверка партнеров*. Узел должен иметь возможность проверки принадлежности своего партнера к домену.
10. *Проверка роли*. Узлу слудует обеспечивать возможность проверки роли партнера. В частности, следует обеспечивать возможность нахождения граничных узлов (с интерфейсом в Internet).
11. *Данные домена*. В домене с требованиями по управления узлам должна обеспечиваться возможность получить правила и/или конфигурационные данные домена. Это включает, например, пакеты, которые не должны покидать домен.

Эти требования могут стать основой для последующего анализа и разработки решения.

Другой вопрос связан с использованием в пакетах того или иного индикатора принадлежности к домену или определением такой принадлежности по адресам IP. С этим связана криптограическая аутентификация пакетов и вопрос требует отдельного исследования.

7. Вопросы безопасности

Как отмечено выше, протоколы, предназначенные для ограниченного применения, могут попадать в открытую часть Internet, поэтому ограниченности применния протокола не является основанием для пренебрежения вопросами защиты. Фактически, ограниченное применение протокола усложняет разработку средств его защиты.

Зачастую периметр домена с ограничениями является также границей защиты. В частности, периметр является границей доверия и полномочий доступа к определенным возможностям. Например, сегментная маршрутизация [RFC8402] явно использует для концепцию «домена доверия». Внутри периметра протоколы или свойства ограниченного домена могут быть полезны, но за пределами домена они могут становиться ненужными или вредными.

Граница служит также для обеспечения конфиденциальности и приватности рабочих параметров, которые оператор не хочет раскрывать. Отметим, что это не связано с защитой конфиденциальности отдельных пользователей домена.

Модель безопасности для протокола с ограниченной областью применения должна поддерживать границу и, в частности, смену модели доверия на этой границе. Обычно для этого требуются «свидетельства» (credentials) подписанные уполномоченным органом домена.

8. Взаимодействие с IANA

Этот документ не требует действий со стороны IANA.

9. Литература

[ACP] Eckert, T., Behringer, M., and S. Bjarnason, "An Autonomic Control Plane (ACP)", Work in Progress[1], Internet-Draft, draft-ietf-anima-autonomic-control-plane-27, 2 July 2020, <https://tools.ietf.org/html/draft-ietf-anima-autonomic-control-plane-27>.

[APP-AWARE] Li, Z., Peng, S., Li, C., Xie, C., Voyer, D., Li, X., Liu, P., Liu, C., and K. Ebisawa, "Application-aware IPv6 Networking (APN6) Encapsulation", Work in Progress, Internet-Draft, draft-li-6man-app-aware-ipv6-network-02, 2 July 2020, <https://tools.ietf.org/html/draft-li-6man-app-aware-ipv6-network-02>.

[BIGIP] Li, R., "HUAWEI - Big IP Initiative", 2018, <https://www.iaria.org/announcements/HuaweiBigIP.pdf>.

[DETNET-DATA-PLANE] Varga, B., Farkas, J., Berger, L., Malis, A., and S. Bryant, "DetNet Data Plane Framework", Work in Progress[2], Internet-Draft, draft-ietf-detnet-data-plane-framework-06, 6 May 2020, <https://tools.ietf.org/html/draft-ietf-detnet-data-plane-framework-06>.

[DNS-PERIMETER] Crocker, D. and T. Adams, "DNS Perimeter Overlay", Work in Progress, Internet-Draft, draft-dcrocker-dns-perimeter-01, 11 June 2019, <https://tools.ietf.org/html/draft-dcrocker-dns-perimeter-01>.

[1]Опубликовано в RFC 8994. *Прим. перев.*
[2]Опубликовано в RFC 8938. *Прим. перев.*

[EMBEDDED-SEMANTICS] Jiang, S., Qiong, Q., Farrer, I., Bo, Y., and T. Yang, "Analysis of Semantic Embedded IPv6 Address Schemas", Work in Progress, Internet-Draft, draft-jiang-semantic-prefix-06, 15 July 2013, <https://tools.ietf.org/html/draft-jiang-semantic-prefix-06>.

[ENHANCED-VPN] Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Enhanced Virtual Private Networks (VPN+) Service", Work in Progress, Internet-Draft, draft-ietf-teas-enhanced-vpn-06, 13 July 2020, <https://tools.ietf.org/html/draft-ietf-teas-enhanced-vpn-06>.

[FAST] Herbert, T., "Firewall and Service Tickets", Work in Progress, Internet-Draft, draft-herbert-fast-04, 10 April 2019, <https://tools.ietf.org/html/draft-herbert-fast-04>.

[FRAG-FRAGILE] Bonica, R., Baker, F., Huston, G., Hinden, R., Troan, O., and F. Gont, "IP Fragmentation Considered Fragile", Work in Progress[1], Internet-Draft, draft-ietf-intarea-frag-fragile-17, 30 September 2019, <https://tools.ietf.org/html/draft-ietf-intarea-frag-fragile-17>.

[HOMENET-NAMING] Lemon, T., Migault, D., and S. Cheshire, "Homenet Naming and Service Discovery Architecture", Work in Progress, Internet-Draft, draft-ietf-homenet-simple-naming-03, 23 October 2018, <https://tools.ietf.org/html/draft-ietf-homenet-simple-naming-03>.

[IBN-CONCEPTS] Clemm, A., Ciavaglia, L., Granville, L., and J. Tantsura, "Intent-Based Networking - Concepts and Definitions", Work in Progress[2], Internet-Draft, draft-irtf-nmrg-ibn-concepts-definitions-01, 9 March 2020, <https://tools.ietf.org/html/draft-irtf-nmrg-ibn-concepts-definitions-01>.

[IN-FLIGHT-IPV6] Smith, M., Kottapalli, N., Bonica, R., Gont, F., and T. Herbert, "In-Flight IPv6 Extension Header Insertion Considered Harmful", Work in Progress, Internet-Draft, draft-smith-6man-in-flight-eh-insertion-harmful-02, 30 May 2020, <https://tools.ietf.org/html/draft-smith-6man-in-flight-eh-insertion-harmful-02>.

[IN-SITU-OAM] Bhandari, S., Brockners, F., Pignataro, C., Gredler, H., Leddy, J., Youell, S., Mizrahi, T., Kfir, A., Gafni, B., Lapukhov, P., Spiegel, M., Krishnan, S., and R. Asati, "In-situ OAM IPv6 Options", Work in Progress[3], Internet-Draft, draft-ietf-ippm-ioam-ipv6-options-02, 13 July 2020, <https://tools.ietf.org/html/draft-ietf-ippm-ioam-ipv6-options-02>.

[IPV4-EXT-HEADERS] Herbert, T., "IPv4 Extension Headers and Flow Label", Work in Progress, Internet-Draft, draft-herbert-ipv4-eh-01, 2 May 2019, <https://tools.ietf.org/html/draft-herbert-ipv4-eh-01>.

[IPV6-ALT-MARK] Fioccola, G., Zhou, T., Cociglio, M., Qin, F., and R. Pang, "IPv6 Application of the Alternate Marking Method", Work in Progress[4], Internet-Draft, draft-ietf-6man-ipv6-alt-mark-01, 22 June 2020, <https://tools.ietf.org/html/draft-ietf-6man-ipv6-alt-mark-01>.

[IPV6-EXT-HEADERS] Gont, F. and W. LIU, "Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers", Work in Progress[5], Internet-Draft, draft-ietf-opsec-ipv6-eh-filtering-06, 2 July 2018, <https://tools.ietf.org/html/draft-ietf-opsec-ipv6-eh-filtering-06>.

[IPV6-SRH] Voyer, D., Filsfils, C., Dukes, D., Matsushima, S., Leddy, J., Li, Z., and J. Guichard, "Deployments With Insertion of IPv6 Segment Routing Headers", Work in Progress, Internet-Draft, draft-voyer-6man-extension-header-insertion-09, 19 May 2020, <https://tools.ietf.org/html/draft-voyer-6man-extension-header-insertion-09>.

[IPV6-USE-MINMTU] Andrews, M., "TCP Fails To Respect IPV6_USE_MIN_MTU", Work in Progress, Internet-Draft, draft-andrews-tcp-and-ipv6-use-minmtu-04, 18 October 2015, <https://tools.ietf.org/html/draft-andrews-tcp-and-ipv6-use-minmtu-04>.

[IPWAVE-NETWORKING] Jeong, J., "IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", Work in Progress[6], Internet-Draft, draft-ietf-ipwave-vehicular-networking-16, 7 July 2020, <https://tools.ietf.org/html/draft-ietf-ipwave-vehicular-networking-16>.

[REF-MODEL] Behringer, M., Carpenter, B., Eckert, T., Ciavaglia, L., and J. Nobre, "A Reference Model for Autonomic Networking", Work in Progress[7], Internet-Draft, draft-ietf-anima-reference-model-10, 22 November 2018, <https://tools.ietf.org/html/draft-ietf-anima-reference-model-10>.

[RFC2205] Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, DOI 10.17487/RFC2205, September 1997, <https://www.rfc-editor.org/info/rfc2205>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <https://www.rfc-editor.org/info/rfc2474>.

[RFC2775] Carpenter, B., "Internet Transparency", RFC 2775, DOI 10.17487/RFC2775, February 2000, <https://www.rfc-editor.org/info/rfc2775>.

[RFC2923] Lahey, K., "TCP Problems with Path MTU Discovery", RFC 2923, DOI 10.17487/RFC2923, September 2000, <https://www.rfc-editor.org/info/rfc2923>.

[RFC3234] Carpenter, B. and S. Brim, "Middleboxes: Taxonomy and Issues", RFC 3234, DOI 10.17487/RFC3234, February 2002, <https://www.rfc-editor.org/info/rfc3234>.

[1] Опубликовано в RFC 8900. *Прим. перев.*
[2] Опубликовано в RFC 9315. *Прим. перев.*
[3] Опубликовано в RFC 9486. *Прим. перев.*
[4] Опубликовано в RFC 9343. *Прим. перев.*
[5] Опубликовано в RFC 9288. *Прим. перев.*
[6] Опубликовано в RFC 9365. *Прим. перев.*
[7] Опубликовано в RFC 8993. *Прим. перев.*

[RFC3879] Huitema, C. and B. Carpenter, "Deprecating Site Local Addresses", RFC 3879, DOI 10.17487/RFC3879, September 2004, <https://www.rfc-editor.org/info/rfc3879>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/info/rfc4193>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4397] Bryskin, I. and A. Farrel, "A Lexicography for the Interpretation of Generalized Multiprotocol Label Switching (GMPLS) Terminology within the Context of the ITU-T's Automatically Switched Optical Network (ASON) Architecture", RFC 4397, DOI 10.17487/RFC4397, February 2006, <https://www.rfc-editor.org/info/rfc4397>.

[RFC4427] Mannie, E., Ed. and D. Papadimitriou, Ed., "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4427, DOI 10.17487/RFC4427, March 2006, <https://www.rfc-editor.org/info/rfc4427>.

[RFC4655] Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <https://www.rfc-editor.org/info/rfc4655>.

[RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, DOI 10.17487/RFC4821, March 2007, <https://www.rfc-editor.org/info/rfc4821>.

[RFC4838] Cerf, V., Burleigh, S., Hooke, A., Torgerson, L., Durst, R., Scott, K., Fall, K., and H. Weiss, "Delay-Tolerant Networking Architecture", RFC 4838, DOI 10.17487/RFC4838, April 2007, <https://www.rfc-editor.org/info/rfc4838>.

[RFC4924] Aboba, B., Ed. and E. Davies, "Reflections on Internet Transparency", RFC 4924, DOI 10.17487/RFC4924, July 2007, <https://www.rfc-editor.org/info/rfc4924>.

[RFC5704] Bryant, S., Ed., Morrow, M., Ed., and IAB, "Uncoordinated Protocol Development Considered Harmful", RFC 5704, DOI 10.17487/RFC5704, November 2009, <https://www.rfc-editor.org/info/rfc5704>.

[RFC6294] Hu, Q. and B. Carpenter, "Survey of Proposed Use Cases for the IPv6 Flow Label", RFC 6294, DOI 10.17487/RFC6294, June 2011, <https://www.rfc-editor.org/info/rfc6294>.

[RFC6325] Perlman, R., Eastlake 3rd, D., Dutt, D., Gai, S., and A. Ghanwani, "Routing Bridges (RBridges): Base Protocol Specification", RFC 6325, DOI 10.17487/RFC6325, July 2011, <https://www.rfc-editor.org/info/rfc6325>.

[RFC6398] Le Faucheur, F., Ed., "IP Router Alert Considerations and Usage", BCP 168, RFC 6398, DOI 10.17487/RFC6398, October 2011, <https://www.rfc-editor.org/info/rfc6398>.

[RFC6407] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, DOI 10.17487/RFC6407, October 2011, <https://www.rfc-editor.org/info/rfc6407>.

[RFC6709] Carpenter, B., Aboba, B., Ed., and S. Cheshire, "Design Considerations for Protocol Extensions", RFC 6709, DOI 10.17487/RFC6709, September 2012, <https://www.rfc-editor.org/info/rfc6709>.

[RFC6947] Boucadair, M., Kaplan, H., Gilman, R., and S. Veikkolainen, "The Session Description Protocol (SDP) Alternate Connectivity (ALTC) Attribute", RFC 6947, DOI 10.17487/RFC6947, May 2013, <https://www.rfc-editor.org/info/rfc6947>.

[RFC6950] Peterson, J., Kolkman, O., Tschofenig, H., and B. Aboba, "Architectural Considerations on Application Features in the DNS", RFC 6950, DOI 10.17487/RFC6950, October 2013, <https://www.rfc-editor.org/info/rfc6950>.

[RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", RFC 7045, DOI 10.17487/RFC7045, December 2013, <https://www.rfc-editor.org/info/rfc7045>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/info/rfc7228>.

[RFC7368] Chown, T., Ed., Arkko, J., Brandt, A., Troan, O., and J. Weil, "IPv6 Home Networking Architecture Principles", RFC 7368, DOI 10.17487/RFC7368, October 2014, <https://www.rfc-editor.org/info/rfc7368>.

[RFC7381] Chittimaneni, K., Chown, T., Howard, L., Kuarsingh, V., Pouffary, Y., and E. Vyncke, "Enterprise IPv6 Deployment Guidelines", RFC 7381, DOI 10.17487/RFC7381, October 2014, <https://www.rfc-editor.org/info/rfc7381>.

[RFC7556] Anipko, D., Ed., "Multiple Provisioning Domain Architecture", RFC 7556, DOI 10.17487/RFC7556, June 2015, <https://www.rfc-editor.org/info/rfc7556>.

[RFC7663] Trammell, B., Ed. and M. Kuehlewind, Ed., "Report from the IAB Workshop on Stack Evolution in a Middlebox Internet (SEMI)", RFC 7663, DOI 10.17487/RFC7663, October 2015, <https://www.rfc-editor.org/info/rfc7663>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <https://www.rfc-editor.org/info/rfc7665>.

[RFC7754] Barnes, R., Cooper, A., Kolkman, O., Thaler, D., and E. Nordmark, "Technical Considerations for Internet Service Blocking and Filtering", RFC 7754, DOI 10.17487/RFC7754, March 2016, <https://www.rfc-editor.org/info/rfc7754>.

[RFC7788] Stenberg, M., Barth, S., and P. Pfister, "Home Networking Control Protocol", RFC 7788, DOI 10.17487/RFC7788, April 2016, <https://www.rfc-editor.org/info/rfc7788>.

[RFC7872] Gont, F., Linkova, J., Chown, T., and W. Liu, "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World", RFC 7872, DOI 10.17487/RFC7872, June 2016, <https://www.rfc-editor.org/info/rfc7872>.

[RFC8085] Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage Guidelines", BCP 145, RFC 8085, DOI 10.17487/RFC8085, March 2017, <https://www.rfc-editor.org/info/rfc8085>.

[RFC8086] Yong, L., Ed., Crabbe, E., Xu, X., and T. Herbert, "GRE-in-UDP Encapsulation", RFC 8086, DOI 10.17487/RFC8086, March 2017, <https://www.rfc-editor.org/info/rfc8086>.

[RFC8100] Geib, R., Ed. and D. Black, "Diffserv-Interconnection Classes and Practice", RFC 8100, DOI 10.17487/RFC8100, March 2017, <https://www.rfc-editor.org/info/rfc8100>.

[RFC8151] Yong, L., Dunbar, L., Toy, M., Isaac, A., and V. Manral, "Use Cases for Data Center Network Virtualization Overlay Networks", RFC 8151, DOI 10.17487/RFC8151, May 2017, <https://www.rfc-editor.org/info/rfc8151>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8300] Quinn, P., Ed., Elzur, U., Ed., and C. Pignataro, Ed., "Network Service Header (NSH)", RFC 8300, DOI 10.17487/RFC8300, January 2018, <https://www.rfc-editor.org/info/rfc8300>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[RFC8445] Keranen, A., Holmberg, C., and J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal", RFC 8445, DOI 10.17487/RFC8445, July 2018, <https://www.rfc-editor.org/info/rfc8445>.

[RFC8517] Dolson, D., Ed., Snellman, J., Boucadair, M., Ed., and C. Jacquenet, "An Inventory of Transport-Centric Functions Provided by Middleboxes: An Operator Perspective", RFC 8517, DOI 10.17487/RFC8517, February 2019, <https://www.rfc-editor.org/info/rfc8517>.

[RFC8557] Finn, N. and P. Thubert, "Deterministic Networking Problem Statement", RFC 8557, DOI 10.17487/RFC8557, May 2019, <https://www.rfc-editor.org/info/rfc8557>.

[RFC8568] Bernardos, CJ., Rahman, A., Zuniga, JC., Contreras, LM., Aranda, P., and P. Lynch, "Network Virtualization Research Challenges", RFC 8568, DOI 10.17487/RFC8568, April 2019, <https://www.rfc-editor.org/info/rfc8568>.

[RFC8578] Grossman, E., Ed., "Deterministic Networking Use Cases", RFC 8578, DOI 10.17487/RFC8578, May 2019, <https://www.rfc-editor.org/info/rfc8578>.

[RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/info/rfc8754>.

[SPB] "IEEE Standard for Local and metropolitan area networks - Bridges and Bridged Networks", DOI 10.1109/IEEESTD.2018.8403927, IEEE 802.1Q-2018, July 2018, <https://ieeexplore.ieee.org/document/8403927>.

[SRV6-NETWORK] Filsfils, C., Camarillo, P., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "SRv6 Network Programming", Work in Progress[1], Internet-Draft, draft-ietf-spring-srv6-network-programming-16, 27 June 2020, <https://tools.ietf.org/html/draft-ietf-spring-srv6-network-programming-16>.

[USER-PLANE-PROTOCOL] Homma, S., Miyasaka, T., Matsushima, S., and D. Voyer, "User Plane Protocol and Architectural Analysis on 3GPP 5G System", Work in Progress, Internet-Draft, draft-ietf-dmm-5g-uplane-analysis-03, 3 November 2019, <https://tools.ietf.org/html/draft-ietf-dmm-5g-uplane-analysis-03>.

Приложение A. Таксономия ограниченных доменов

В этом приложении рассмотрена таксономия ограниченных доменов, включая:

- домен как целое;
- отдельные узлы;
- границы доменов;
- топологию доменов;
- технологии доменов;
- подключение доменов к Internet
- модели безопасности, доверия и конфиденциальности;
- рабочие операции.

[1]Опубликовано в RFC 8986. *Прим. перев.*

A.1. Домен как целое

- Почему домен существует (например, человеческий выбор, административные правила, организационные требования, технические требования, такие как операционное разделение с целями масштабирования)?
- Если есть специальные требования, они относятся к L2, L3 или вышележащему уровню?
- Где находится домен в спектре от полностью управляемого людьми до совершенно автономного?
- Если домен управляемый, какой стиль применяется (ручная или автоматизированная настройка, автоматическое управление (orchestration))?
- Имеется ли модель политики (намерения, правила настройки конфигурации)?
- Используется в домене контролируемый, платный или свободный доступ?

A.2. Отдельные узлы

- Являются члены домена полными узлами или только интерфейсами узлов?
- Являются узлы постоянными членами домена или возможно подключение и отключение?
- Являются узлы физическими или виртуальными устройствами?
- Являются виртуальные устройства обычными (общего назначения) или специализированными (функции, приложения, пользователи)?
- Являются узлы ограниченными в возможностях (батареи и т. п.)?
- Устройства устанавливаются «из коробки» или требуют предварительной настройки?

A.3. Граница домена

- Как задается или идентифицируется граница домена?
- Граница домена фиксирована или является динамической?
- Являются граничные узлы специальными или можно применять любое устройство?

A.4. Топология

- Является домен частью другого домена L2 или L3?
- Перекрывается ли домен с другими доменами (может ли узел входить в несколько доменов)?
- Модем соответствует физической топологии или использует виртуальную (наложенную)?
- Ограничен домен зданием, кампусом, транспортным средством или является распределенным?
- Распределенный домен имеет соединения через частные сети или Internet?
- В плане адресации IP домен является локальным для канала, локальным для сайта или глобальным?
- Соответствует ли область индивидуальной и групповой адресации границам домена?

A.5. Технология

- Какие применяются протоколы маршрутизации или иные механизмы пересылки (например, MPLS или не-IP)?
- Если домен является наложенным, какой применяется метод (L2VPN, L3VPN и т. п.)?
- Есть ли специфические требования QoS?
- Какова задержка на каналах - обычная или очень большая?
- Имеются ли в домене мобильные узлы? Является ли вся сеть мобильной?
- Какие специфические технологии применимы (например, из числа описанных в разделе 4)?

A.6. Подключение к Internet

- Является подключение к Internet постоянным или прерывистым (отсутствие подключения не считается)?
- Блокируется ли трафик на входе или выходе?
- Какой трафик разрешен (allow), входящий или исходящий?
- Какой трафик преобразуется, входящий или исходящий?
- Нужен ли защищенный или привилегированный удаленный доступ?
- Разрешает ли домен непривилегированные удаленные сессии?

A.7. Модель безопасности, доверия и приватности

- Требуется ли контроль полномочий для членов домена?
- Имеют ли все узлы домена одинаковый уровень доверия?
- Является ли трафик аутентифицированным?
- Шифруется ли трафик?

- Что спрятано от внешнего мира?

A.8. Работа

- Играет ли домен важную роль в обеспечении безопасности людей?
- Требования к надежности обычны или нужно 99,999%?
- Работает ли домен в условиях опасной среды?
- Имеются ли специфические требования к установке?
- Доступ для обслуживания - просто, сложно или невозможно?
- Возможно ли обновление программ и микрокода?

A.9. Использование таксономии

Эта таксономия может применяться при разработке и анализе для конкретного типа ограниченного домена. В настоящем документе она является лишь основой для рассмотрения области действия протоколов, применяемых в ограниченных доменах, и механизмов требуемых для безорасного определения принадлежности к домену и свойств домена.

Благодарности

Полезные замечания предоставили Amelia Andersdotter, Edward Birrane, David Black, Ron Bonica, Mohamed Boucadair, Tim Chown, Darren Dukes, Donald Eastlake, Adrian Farrel, Tom Herbert, Ben Kaduk, John Klensin, Mirja Kuehlewind, Warren Kumari, Andy Malis, Michael Richardson, Mark Smith, Rick Taylor, Niels ten Oever и другие.

Участники работы

Sheng Jiang

Huawei Technologies

Q14, Huawei Campus

No. 156 Beiqing Road

Hai-Dian District, Beijing

100095

China

Email: jiangsheng@huawei.com

Адреса авторов

Brian Carpenter

The University of Auckland

School of Computer Science

University of Auckland

PB 92019

Auckland 1142

New Zealand

Email: brian.e.carpenter@gmail.com

Bing Liu

Huawei Technologies

Q14, Huawei Campus

No. 156 Beiqing Road

Hai-Dian District, Beijing

100095

China

Email: leo.liubing@huawei.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru