Internet Engineering Task Force (IETF)
Request for Comments: 8994
Category: Standards Track
ISSN: 2070-1721

T. Eckert, Ed.
Futurewei USA
M. Behringer, Ed.

S. Bjarnason
Arbor Networks

May 2021

An Autonomic Control Plane (ACP)

Автономная плоскость управления

Аннотация

Автономным (самоуправляемым) функциям для взаимодействия нужна плоскость управления, которая зависит от некой адресации и маршрутизации. Такой автономной плоскости управления (Autonomic Control Plane или ACP) в идеале следует быть самоуправляемой и максимально независимой от конфигурации. В этом документе определена такая плоскость управления, предназначенная прежде всего для работы с автономными функциями. Она также служит отдельным виртуальным каналом (virtual out-of-band channel) для взаимодействий OAM через сеть, который обеспечивает автоматически настраиваемый, поэтапно (hop-by-hop) аутентифицируемый и шифрованный обмен данными с автоматической настройкой IPv6 даже в ненастроенной или некорректно настроенной сети.

Статус документа

Документ содержит проект стандарта Internet (Standards Track).

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc8994.

Авторские права

Copyright (c) 2021. Авторские права принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К этому документу применимы права и ограничения, перечисленные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (http://trustee.ietf.org/license-info), на момент публикации данного документа. Прочтите упомянутые документы внимательно, поскольку в них описаны права и ограничения, относящиеся к данному документу. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

Оглавление

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение (информационное)

Автономные сети (Autonomic Networking) - это концепция самоуправления - автономные функции самостоятельно настраиваются и согласуют параметры и настройки через сеть. В документе Autonomic Networking: Definitions and Design Goals [RFC7575] рассмотрены основные идеи и цели разработки самоуправляемых (автономных) сетей. Анализ пробелов в части таких разработок приведён в документе General Gap Analysis for Autonomic Networking [RFC7576]. Эталонная архитектура сетей с самоуправлением в рамках IETF представленв в документе A Reference Model for Autonomic Networking [RFC8993].

Для функций самоуправления нужна соответствующая коммуникационная инфраструктура, которая должна быть защищённой, отказоустойчивой и пригодной для всех автономных функций. В разделе 5 [RFC7575] описана такая инфраструктура, названная автономной плоскостью управления (Autonomic Control Plane или ACP). Для лучшего понимания её следовало бы назвать автономной коммуникационной инфраструктурой для OAM и управления (Autonomic communications infrastructure for OAM and control), но для согласованности документов здесь применяется термин ACP.

Сегодня плоскостями управления и OAM в сетях IP обычно являются размещённые в основной полосе каналы управления и/или сигнализации и трафик управления зависит от таблиц маршрутизации и пересылки, безопасности,

правил, QoS и, возможно, других параметров, которые обеспечиваются с помощью тех же протоколов управления и контроля. Некорректные настройки, включая побочные эффекты и взаимозависимости, могут нарушать работу OAM и управления, особенно доступ к удалённому управлению затронутым ошибками узлом, а также могут осложнять доступ ко многим другим узлам, на пути к которым упомянутый узел размещается.

Пример отказа при управлении по основному каналу в результате внесённых оператором ошибок в конфигурации, приведён в разделе III.B.15 (стр. 8) [FCC].

> … инженеры почти сразу поняли, что неверно диагностировали проблему. Однако им не удалось проблему решить путём восстановления канала, поскольку нужные инструменты управления полагались на те же пути, которые были только что отключены.

Традиционно для решения этой проблемы или по меньшей мере восстановления используются физически отделённые (out-of-band) сети управления. В худшем случае персонал направляется на сайт для доступа через отдельные порты управления (служебный порт, последовательная консоль, порт Ethernet-управления). Однако оба варианты недёшевы.

С расширением автоматизации сетей централизованным системам управления и распределенным агентам служб в сети требуется плоскость управления, независимая от конфигурации управляемой сети, чтобы избежать влияния на их работу внесённых в конфигурацию сети изменений.

В этом документе описано модульное решение для самоформирующейся, самоуправляемой и самозащищающейся плоскости ACP, представляющей собой виртуальную отдельную (out-of-band) сеть с максимальной независимостью от конфигурации, адресации и маршрутизации, чтобы избежать проблем самозависимости современных сетей IP при работе по основным (in-band) каналам той же физической сети, для управления которой она служит. Устройство ACP рассчитано на максимально возможное сочетание устойчивости отдельных (out-of-band) сетей управления с низкой стоимостью традиционного управления сетями IP по основному каналу (in-band). Детали решения описаны в разделе 6. Создание ACP (нормативный раздел).

В полностью автономной сети без унаследованных функций и протоколов управление и/или поддержки плоскость данных будет просто плоскостью пересылки для пакетов «данных» IPv6, которые отличаются от пакетов управления и поддержки, пересылаемых ACP. В такой сети не будет неавтономного управления узлами и неавтономной плоскости управления.

Протоколы маршрутизации будут встроены в ACP как автономные функции через различные автономные агенты служб, использующие функции ACP вместо отдельной реализации каждого протокола - обнаружения, автоматической организации аутентифицированных шифрованных соединений локальных и удалённых партнёров для трафика управления и поддержки, общих сеансовых и представительских функций протокола управления и поддержки.

При добавлении функциональности ACP на узлах без автономных функций управления и поддержки (неавтономные узлы или узлы без самоуправления), ACP лучше абстрагировать как специальный экземпляр виртуальной маршрутизации и пересылки (Virtual Routing and Forwarding или VRF) - виртуальный маршрутизатор, а имеющуюся плоскость управления считать частью плоскости данных, чтобы избежать применения для этого случая особой терминологии.

Подобно плоскости пересылки для пакетов «данных», функциями неавтономного управления и поддержки можно управлять (использовать их) через ACP. Такая терминология согласуется с имеющимися документами, такими как Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance (OAM) [RFC8368].

В автономных и неавтономных экземплярах плоскость ACP создаётся так, она может работать без плоскости данных. ACP также работает при наличии любой настроенной (возможно, некорректно) неавтономной системы управления и поддержки в плоскости данных.

ACP выполняет одновременно несколько задач, указанных ниже.

1. Взаимодействие автономных функций через ACP и прямой поддержкой функций самоуправляемых сетей, как описано в [RFC8993]. Например, протокол GRASP ("GeneRic Autonomic Signaling Protocol (GRASP)" [RFC8990]) работает через ACP и использует её как «подложку защищённого транспорта».
2. Контроллер или система управления сетью может использовать ACP для защищённой загрузки сетевых устройств в удалённых точках, даже когда сеть (плоскость данных) к ним ещё не настроена. Настройка загрузки, зависящая от плоскости данных, не требуется. Пример процесса защищённой загрузки представлен в Bootstrapping Remote Secure Key Infrastructure (BRSKI) [RFC8995].
3. Оператор может применять ACP для доступа к удаленным устройствам с использованием таких протоколов, как SSH (Secure SHell) или NETCONF (Network Configuration Protocol) даже в ненастроенной или некорректно настроенной сети.

В разделе 3 эти задачи рассмотрены на примерах использования ACP, раздел 4 задаёт требования, а раздел 5 содержит обзор устройства ACP. Нормативная часть документа начинается с раздела 6, где задана спецификация ACP. В разделе 7 описана поддержка ACP в коммутаторах (L2), а раздел 8 посвящён интеграции с узлами и сетями, не поддерживающими ACP. Остальные разделы не являются нормативными. В разделе 10 описаны преимущества ACP, раздел 9 содержит эксплуатационные рекомендации, в Приложении A приведены дополнительные сведения и рассмотрены возможные расширения, которые не были применены в спецификации, но считаются важными. Реализация Приложения A не требуется для создания полной и совместимой реализации ACP.

ACP обеспечивает защищённую связность IPv6 и может применяться для защищённых соединений не только в самоуправлении, как требует для ACP [RFC7575], но и для традиционного (централизованного) управления. ACP можно реализовать и использовать без других компонентов автономных сетей, требуется лишь GRASP. ACP полагается на протокол GRASP с незапрашиваемым обнаружением локальных каналов (Discovery Unsolicited Link-Local или DULL, параграф 6.4) для автоматического поиска соседей ACP и включает экземпляр ACP GRASP для обнаружения служб клиентами ACP (параграф 6.9), в том числе для поддержки сертификатов ACP.

В [RFC8368] описано, как можно использовать ACP автономно для обеспечения защищённой и стабильной связности автономных и неавтономных приложений OAM, в частности, на современных неавтономных узлах и/или в сетях. Документ также объясняет, как существующие управляющие решения могут применять ACP вместе с традиционными моделями управления, когда следует применять ACP и как можно объединить ACP с системами OAM, поддерживающими лишь IPv4.

Объединение ACP с BRSKI[1] [RFC8995] ведёт к автономной сетевой инфраструктуре (Autonomic Network Infrastructure или ANI) [RFC8993], обеспечивающей автономную связность с защищённой автоматической (zero-touch) загрузкой из BRSKI. Сама инфраструктура ANI не создаёт автономной сети, но позволяет организовать более или менее автономные сети на своей основе, используя централизованную автоматизацию в стиле SDN (см. Software-Defined Networking (SDN): Layers and Architecture Terminology [RFC7426]) или распределенную автоматизацию через автономные агенты сервиса (Autonomic Service Agent или ASA) и/или автономные функции (Autonomic Functions или AF). Дополнительные сведения можно получить из [RFC8993].

1.1. Применимость и область действия

Используемые в этом параграфе термины приведены в разделе 2. Термины и сокращения (информационный раздел).

Устройство ACP, заданное этим документом, считается применимым ко всем типам «профессионально управляемых» сетей: сервис-провайдеры, ЛВС, городские (Metropolitan Area Network или MAN/Metro), распределенные (Wide Area Network или WAN), корпоративные информационные (Enterprise Information Technology или IT), технологические (Operational Technology или OT) сети. ACP может работать с оборудованием сетевого (L3) и канального L2 уровня, таким как мосты (см. раздел 7. Поддержка ACP на коммутаторах и портах L2 (нормативный)). Поэтапная (hop-by-hop) аутентификация, защита целостности и конфиденциальности, применяемая в ACP, может согласовываться, поэтому ACP можно распространить на среды с разными предпочтительными протоколами. Минимальные требования этого документа нацелены на обеспечения максимальной совместимости, задавая поддержку опций в зависимости от типа устройств - IPsec (см. Security Architecture for the Internet Protocol [RFC4301]) или защита транспорта дейтаграмм (Datagram Transport Layer Security или DTLS, см. параграф 6.8.4. ACP по протоколу DTLS).

Реализация ACP включает код инфраструктуры открытых ключей (Public Key Infrastructure или PKI) для сертификатов ACP, в том числе EST (см. Enrollment over Secure Transport [RFC7030]), GRASP, UDP, TCP, защита транспортного уровня (Transport Layer Security или TLS, см. параграф 6.1. Требования к использованию TLS). Дополнительные сведения в части защищенности и надёжности GRASP и EST, применяемого в защищённых каналах ACP (таких как IPsec и DTLS) и экземплярах пересылки и маршрутизации пакетов IPv6 с помощью RPL приведены в документе RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks [RFC6550] (отдельно от маршрутизации и пересылки пользовательских пакетов в плоскости данных).

В ACP применяется только IPv6, чтобы избежать сложностей работы с двойным стеком (IPv6 и IPv4). Тем не менее, ACP можно интегрировать без изменений с сетевыми устройствами, поддерживающими лишь IPv4. Плоскость данных менять не потребуется и она может по-прежнему работать лишь с IPv4. Для таких устройств протокол IPv6 будет дополнительной областью реализации, требуемой лишь для ACP.

Выбор протоколов для ACP основан в первую очередь на широком применении и поддержке в сетях и устройствах, хорошо известных свойствах защиты и требованиях к расширяемости. ACP является попыткой создать комбинацию имеющихся технологий и протоколов для построения широко применимого оперативного решения по управлению сетями с минимальным риском.

Протокол RPL был выбран потому, что у него менее жёсткие требования к размеру таблиц маршрутизации по сравнению с другими протоколами с автономно настраиваемыми областями. Опыт реализации больших сетей IoT[2] служит основой для широкого развёртывания RPL. Выбранный в ACP профиль RPL не использует каких-либо специфических для этого протокола функций плоскости данных (заголовки расширения IPv6), делая его реализацию исключительно программным требованием плоскости управления.

GRASP является единственным совершенно новым протоколом в ACP и его выбор обусловлен отсутствием другого протокола, обеспечивающего требуемые для ACP функции. Протокол GRASP был разработан специально для этого.

ACP подходит для устройств с ограничениями в части CPU и памяти, а также сетей, ограниченных по скорости и надёжности, но этот документ не пытается определить максимальные ограничения для устройств и сетей применительно к ACP. RPL и DTLS для защищённых каналов ACP уже делают ACP подходящим решением для сред с ограничениями. Поддержка устройств с ограничениями в этой спецификации условна и неполна, поскольку для надёжного транспорта GRASP (параграф 6.9.2. ACP как защищённая транспортная подложка для GRASP) заданы лишь TCP и TLS. В Приложении A.8 обсуждаются будущие стандарты и подходящие расширения и вариации ACP, которые могут лучше соответствовать ожиданиям и отличать от положенных в основу текущего решения, включая лучшую поддержку устройств с ограничениями.

2. Термины и сокращения (информационный раздел)

Этот документ служит нормативной спецификацией поведения узлов ACP, а также разъяснением контекста с помощью описания требований, преимуществ, архитектуры и аспектов работы. Нормативные разделы помечены и используют ключевые слова BCP 14. Информативные разделы тоже помечены, но ключевых слов не используют.

Далее в документе использующие ACP системы называются узлами (node). Обычно такой узел является физическим устройством (сетевое оборудование), но может быть и виртуализованной системой. Поэтому в документе они не называются устройствами, если текст не относится именно к физическом системам.

Ниже указаны используемые в документе термины (в алфавитном порядке). Вводимые документом термины объясняются при первом использовании, а в список включены лишь для полноты.

[1] Bootstrapping Remote Secure Key Infrastructure - инфраструктура ключей защиты удалённой загрузки.
[2] Internet of Things - Интернет вещей.

ACP - Autonomic Control Plane

Автономная плоскость управления - автономная (самоуправляемая) функция, определённая в этом документе. Она обеспечивает защищённую, автоматизированную (zero-touch), транзитивную (через всю сеть) связность IPv6 для всех узлов в одном домене ACP, а также экземпляр GRASP, работающий через соединения ACP IPv6. Основным назначением ACP является использование в качестве компонента ANI для обеспечения работы автономных сетей (Autonomic Network), а также в в простых сетях ANI (без автономных функций) или полностью самостоятельно.

ACP address - адрес ACP

Адрес IPv6, назначенный узлу ACP. Хранится в поле acp-node-name сертификата ACP.

ACP address range or set - диапазон или набор адресов ACP

Адрес ACP может предполагать диапазон или набор адресов, которые узел может назначать для разных целей. Диапазон или набор выводится узлом из формата адреса ACP, называемого субсхемой адресации.

ACP certificate - сертификат ACP

Сертификат отождествления локального устройства (Local Device IDentity или LDevID), соответствующий профилю Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [RFC5280] и содержащий поле acp-node-name, используемое ACP для выяснения его адреса ACP, а также выведения и криптографической оценки его принадлежности к домену ACP. В контекте ANI сертификат ACP называют также сертификатом ANI, в контексте AN - сертификатом AN.

ACP connect interface - интерфейс соединения ACP

Интерфейс на узле ACP, обеспечивающий доступ к не поддерживающим ACP узлам без использования защищённого канала ACP. См. параграф 8.1.1. Контроллер или NMS без поддержки ACP.

ACP domain - домен ACP

Набор узлов с сертификатами ACP, которые позволяют им проверить подлинность друг друга в качестве членов домена ACP. См. параграф 6.2.3. Проверка принадлежности к домену ACP.

ACP loopback interface - петлевой интерфейс ACP

Петлевой (loopback) интерфейс в ACP VRF с адресом ACP. См. параграф 6.13.5.1. Петлевые интерфейсы ACP.

ACP network - сеть ACP

Сеть ACP включает все узлы, имеющие доступ к ACP. Это набор активно или транзитивно соединённых узлов домена ACP, а также всех узлов, имеющих доступ к ACP данного домена через граничные узлы ACP.

ACP (ULA) prefix(es) - префикс(ы) ACP (ULA)

Префиксы IPv6 /48, используемые в ACP. В нормальном или простом случае ACP имеет один уникальный локальный префикс (Unique Local Address или ULA), см. параграф 6.11. Адресация внутри ACP. Таблица маршрутизации ACP может включать множество префиксов ULA, если применяется опция rsub для создания нескольких префиксов ULA (6.2.2. AcpNodeName в сертификате ACP). ACP может также включать иные (не ULA) префиксы, если они настроены на интерфейсах ACP connect (8.1.1. Контроллер или NMS без поддержки ACP).

ACP secure channel - защищённый канал ACP

Канал, аутентифицированный с помощью сертификатов ACP, обеспечивающий защиту целостности и конфиденциальности путём шифрования. Такие каналы организуются между (обычно) смежными узлами ACP для передачи трафика ACP VRF по основному каналу (in-band) через те же соединения и пути, что и трафик данных, но с изоляцией от него и защитой.

ACP secure channel protocol - протокол защищённого канала ACP

Протокол для создания защищённого канала ACP, например, Internet Key Exchange Protocol version 2 (IKEv2) с IPsec или DTLS.

ACP virtual interface - виртуальный интерфейс ACP

Интерфейс в ACP VRF, отображенный на один или несколько защищённых каналов ACP (6.13.5. Интерфейсы ACP).

acp-node-name field - поле имени узла ACP

Информационное поле в сертификате ACP, где хранятся относящиеся к ACP сведения: имя домена ACP, адрес узла ACP IPv6, а также необязательные атрибуты роли узла.

AN - Autonomic Network

Автономная (самоуправляемая) сеть в соответствии с [RFC8993]. Основными её компонентами являются ANI, автономные функции и намерения (Intent).

(AN) Domain Name

Полное доменное имя (Fully Qualified Domain Name или FQDN) в поле acp-node-name сертификата домена (6.2. Домен, сертификат и сеть ACP).

ANI (nodes/network) - Autonomic Network Infrastructure

Автономная сетевая инфраструктура (ANI) является инфраструктурой для обеспечения работы автономных сетей. Она включает ACP, BRSKI и GRASP. Каждая автономная сеть включает ANI, но не каждой ANI требуется включать автономные функции помимо ANI (и Intent). Сеть ANI без других автономных функций может, например, поддерживать защищённую автоматическую (zero-touch) загрузку и стабильную связность для сетей SDN (см. [RFC8368]).

ANIMA - Autonomic Networking Integrated Model and Approach - модель и подход для автономных сетей

ACP, BRSKI и GRASP являются спецификациями рабочей группы IETF ANIMA.

ASA - Autonomic Service Agent

Автономный агент службы - программные модули, работающие в устройстве ANI. Компоненты, образующие ANI (BRSKI, ACP, GRASP), также описываются как агенты ASA.

autonomic function - автономная функция

Функция и/или служба в автономной сети (AN), состоящая из одного или нескольких агентов ASA на одном или нескольких узлах ANI.

BRSKI - Bootstrapping Remote Secure Key Infrastructure [RFC8995]

Протокол, расширяющий EST для защищённой автоматической загрузки в сочетании с ACP. Узлы ANI используют ACP, BRSKI, GRASP.

CA - Certification Authority.

Удостоверяющий центр - орган, выпускающий цифровые сертификаты. CA применяет свой секретный ключ для подписывания выданных сертификатов. Доверяющая сторона применяет открытый ключ CA для проверки подписи.

CRL - Certificate Revocation List

Список отозванных сертификатов нужен для отмены действия сертификата до завершения срока.

data plane - плоскость данных
Контрапункт ACP VRF на узле ACP. Служит для пересылки пользовательского трафика в неавтономных узлах и/или, а также для выполнения функций неавтономных плоскостей управления и/или поддержки. На узле полностью автономной сети плоскость данных управляется через автономные функции и намерения (раздел 1).

device - устройство
Физическая система или узел.

enrollment - зачисление
Процесс, посредством которого узел аутентифицирует себя в сети с исходным отождествлением, которое часто называют сертификатом IDevID (Initial Device IDentity), и получает от сети соответствующее отождествления (идентификатор), которое часто называют сертификатом LDevID, и сертификаты одной или нескольких привязок доверия. В ACP сертификат LDevID называют сертификатом ACP.

EST - Enrollment over Secure Transport [RFC7030]
Стандартный протокол IETF для зачисления узла с сертификатом LdevID. Протокол BRSKI основан на EST.

GRASP - GeneRic Autonomic Signaling Protocol
Расширяемый протокол сигнализации, требуемый в ACP для обнаружения соседей. ACP также обеспечивает защищённую транспортную подложку для экземпляра ACP GRASP, который работает по защищённым каналам ACP для поддержки BRSKI и других автономных функций, NOC и/или OAM (см. [RFC8990]).

IDevID
Сертификат Initial Device IDentity X.509, установленный производителем нового оборудования. Сертификат IDevID содержит сведения для отождествления узла в контексте его производителя и/или изготовителя, такие как модель и/или тип и серийный номер (см. [AR8021]). Сертификат IDevID не может быть идентификатором узла для ACP, поскольку он не предоставлен владельцем сети и не может напрямую указывать домен ACP, к которому относится.

In-band - по основному каналу (для управления или сигнализации)
Трафик управления и/или сигнализация плоскости управления в том же канале с использованием тех же ресурсов сети, таких как маршрутизаторы и/или коммутаторы и сетевые каналы, которыми он управляет. In-band-управление является стандартным механизмом поддержки и сигнализации в сетях IP. По сравнению с отдельными каналами (out-of-band) механизмы in-band не требуют дополнительных физических ресурсов, но могут создавать циклические зависимости, влияющие на работу (см. раздел 1).

Intent - намерения
Язык правил для автономной сети в соответствии с [RFC8993].

Loopback interface - петлевой интерфейс
См. ACP loopback interface.

LDevID
Local Device IDentity - это сертификат X.509, установленный при зачислении в сеть. Сертификат домена в ACP является сертификатом LDevID (см. [AR8021]).

management - управление, поддержка
Используется в этом документе как синоним OAM.

MASA (служба) - Manufacturer Authorized Signing Authority
Уполномоченный производителем орган подписания. Производитель и/или изготовитель или полномочная облачная служба в Internet, используемая как часть протокола BRSKI.

MIC - Manufacturer Installed Certificate
Установленный производителем сертификат. Синоним IDevID в некоторых документах (здесь не применяется).

native interface - естественный интерфейс
Интерфейс, существующий на узле без настройки уже работающего узла. На физических узлах это обычно физические интерфейсы, на виртуальных - их эквивалент.

NOC - Network Operations Center
Центр сетевых операций.

node - узел
Система, поддерживающая ACP в соответствии с этим документом. Узел может быть виртуальным или физическим. Физические узлы называют устройствами.

Node-ID - идентификатор узла
Идентификатор узла ACP внутри ACP, может быть 64- (6.11.3. Субсхема адресации ACP Zone (ACP-Zone)) или 78-битовым (6.11.5. Субсхемы ACP Vlong (ACP-Vlong-8 и ACP-Vlong-16)) адресом ACP.

OAM - Operations, Administration, and Management
Эксплуатация, администрирование, управление (включая мониторинг).

Operational Technology (OT) - технологическая сеть
«Оборудование или программа, выделенные для обнаружения или инициирования изменений в физических процессах путём прямого мониторинга и/или управления физическими устройствами, такими как клапаны, насосы и т. п.» [OP-TECH]. В большинстве современных систем сети OT отделены от сетей IT.

out-of-band (management) network - сеть (управления) по отдельному каналу
Вторичная (вспомогательная) сеть, применяемая для управления основной сетью. Оборудование основной сети подключено к сети out-of-band через выделенные порты управления на оборудовании первичной сети. Исторически чаще всего применялись последовательные (консольные) порты управления, но в современном оборудовании часто имеются порты Ethernet, предназначенные лишь для управления. Сеть out-of-band обеспечивает доступ к управлению первичной сетью независимо от состояния последней (см. раздел 1).

out-of-band network, virtual - виртуальная сеть out-of-band
ACP можно называть сетью out-of-band для управления и поддержки, поскольку эта плоскость управления пытается обеспечить преимущества (физически) отдельной сети при работе по основному каналу (in-band) физической сети (см. раздел 1).

root CA - root Certification Authority
Корневой удостоверяющий центр. CA для которого могут применяться процедуры обновления ключа коревого CA (параграф 4.4 в [RFC7030]).

RPL
Протокол маршрутизации IPv6 Routing Protocol для сетей со слабым питанием и потерями (Low-Power and Lossy Networks) [RFC6550]. Этот протокол применяется в ACP.

registrar (ACP, ANI/BRSKI) - регистратор

Регистратор ACP - это человек или программа, организующая зачисление узлов ACP по сертификатам ACP. Узлы ANI используют BRSKI, поэтому регистраторов ANI называют ещё регистраторами BRSKI. Для узлов ACP без ANI этот документ не задаёт механизмов регистрации (см. 6.11.7. Регистраторы ACP). Обновление и иное обслуживание (например, отзыв) сертификатов ACP могут выполнять не только регистраторы. Для обновления сертификатов ACP требуется поддержка EST (см. 6.2.5. Поддержка сертификата и привязки доверия). BRSKI является расширением EST, поэтому регистраторы ANI/BRSKI легко могут поддерживать обновление сертификатов ACP в дополнение к начальному зачислению.

RPI - RPL Packet Information

Информация пакета RPL - заголовок расширения для использования с RPL. Не применяется с RPL в ACP (см. 6.12.1.13. Информационный пакет RPL).

RPL - Routing Protocol for Low-Power and Lossy Networks

Протокол маршрутизации, применяемый в ACP (см. 6.12. Маршрутизация в ACP).

sUDI - secured Unique Device Identifier

Защищённый уникальный идентификатор устройства - синоним IDevID в иных документах (здесь на применяется).

TA - Trust Anchor

Привязка доверия - сущность, которой доверяют в плане проверки пригодности сертификатов. Сведения в TA, такие как самоподписанные сертификаты TA, настраиваются на узле ACP в процессе зачисления (см. параграф 6.1.1 в [RFC5280]).

UDI - Unique Device Identifier

Уникальный идентификатор устройства. В контексте этого документа - незащищённые идентификационные данные узла, обычно включающие хотя бы модель и/или серийный номер устройства, зачастую в формате производителя (см. sUDI и LDevID).

ULA (Global ID prefix)

Уникальный локальный адрес (Unique Local Address) - адрес IPv6 из блока fc00::/7, определеного в Unique Local IPv6 Unicast Addresses [RFC4193]. ULA является в IPv6 преемником приватных адресов IPv4 (Address Allocation for Private Internets [RFC1918]). Адреса ULA имеют существенные отличия от приватных адресов IPv4, важно для применений в ACP, такие как локально назначаемый префикс Global ID, занимающий первые 48 битов адреса ULA (параграф 3.2.1 в [RFC4193]). В этом документе такие префиксы называются префиксами ULA.

(ACP) VRF

ACP в этом документе моделируется как экземпляр виртульной маршрутизации и пересылки (Virtual Routing and Forwarding). Это значит, что ACP базируется на «виртуальных маршрутизаторах», имеющих отдельную таблицу пересылки IPv6, с которой связаны виртуальные интерфейсы ACP, и соответствующую таблицу маршрутизации IPv6, отделённые от плоскости данных. В отличие от VRF на MPLS/VPN PE (BGP/MPLS IP Virtual Private Networks (VPNs) [RFC4364]) и LISP xTR (The Locator/ID Separation Protocol (LISP) [RFC6830]), ACP VRF не имеет каких-либо специальных функций, ориентированных на ядро, и/или протоколов маршрутизации и/или отображения, используемых разными экземплярами VRF. В фирменной продукции VRF, подобные ACP VRF, могут называть ещё VRF-lite.

(ACP) Zone

Зона ACP - это набор узлов ACP, использующих одно значение поля зоны в своих адресах ACP в соответствии с параграфом 6.11.3. Субсхема адресации ACP Zone (ACP-Zone). Зоны служат механизмом поддержки структурированной адресации ACP внутри одного префикса ULA /48.

Ключевые слова **должно** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

3. Примеры использования ACP (информационный раздел)

В этом разделе обобщены примеры использования, которые предназначены для поддержки ACP. Для их понимания и связи с более широким кругом применения автономных сетей следует прочесть Autonomic Networking Use Case for Distributed Detection of Service Level Agreement (SLA) Violations [RFC8316].

3.1. Инфраструктура для автономных функций

Для работы автономных функций нужна стабильная инфраструктура и всем автономным функциям следует использовать одну инфраструктуру для минимизации сложности сети. Таким образом, требуется лишь один механизм обнаружения, один механизм защиты и по одному экземпляру других процессов, нужных автономным функциям.

3.2. Безопасная начальная загрузка через незащищённую сеть

Сегодня для начальной загрузки нового узла обычно требуется полная и корректная настройка, адресация и защита всех узлов между ним и контролирующим узлом, таким как контроллер SDN (см. [RFC7426]). Начальная загрузка и настройка узлов выполняется кольцами вокруг контроллера - сначала настраивается и загружается ближайшее кольцо, затем следующее и т. д. Без консольного доступа (например, через отдельную сеть) сегодня невозможно обеспечить защищённый доступ к устройствам до настройки всей сети на пути к ним.

С ACP защищённая начальная загрузки новых устройств и новых сетей может происходить без настройки устройств на пути. Когда все устройства на пути поддерживают ACP и механизм автоматической (zero-touch) загрузки, такой как BRSKI, можно запустить ACP в сети ненастроенных устройств без вмешательства оператора и/или системы обеспечения. ACP также предоставляет дополнительную защиту для любых механизмов начальной загрузки благодаря шифруемому обнаружению (ACP GRASP) регистраторов и других серверов начальной загрузки с помощью посредников, подключённых к загружаемым узлам. Шифрование ACP скрывает участников процесса (заявитель и регистратор), осложняя поиск жертвы для атаки. Можно также использовать сертификат ACP для сквозного шифрования связи при загрузке между посредниками и серверами. Отметим, что начальная загрузка здесь включает не только первый шаг, который может быть обеспечен BRSKI (ключи защиты),но и последующие атапы, где загружаются конфигурации.

3.3. Постоянная доступность независимо от плоскости данных

Сегодня для наиболее важных протоколов плоскости управления и OAM используется плоскость данных сети. Это часто ведёт к нежелательным зависимостям между плоскостью управления и OAM с обной стороны и плоскостью данных - с другой. Все эти плоскости будут работать, как ошибается, лишь при корректной настройке пересылки и плоскости управления для плоскости данных.

На связность плоскости данных могут влиять ошибки и отказы. Примеры включают ошибки в настройке, которые делают серверы AAA[1] недоступными или блокируется доступ администратора к устройству, проблемы маршрутизации и адресации могут делать устройства недоступными, отключение интерфейсов, через которые работают сеансы управления может безвозвратно лишить администратора доступа к устройству. Традиционно устранение таких проблем достигается лишь за счёт отдельных (out-of-band) каналов доступа через консольный порт или порт Ethernet для управления.

Зависимости плоскости данных влияют и на приложения в NOC, такие как контроллеры SDN. Некоторые изменения в сети сложно реализовать, поскольку они могут влиять на доступность устройств. Примеры включают смену адресов или масок, маршрутизации или политики безопасности. Сегодня для таких изменений требуется разработки точного плана поэтапной (hop-by-hop) настройки.

Отметим, что конкретные функции плоскости управления для плоскости данных часто зависят от возможности пересылать пакеты управления через плоскость данных. Пакеты проверки живучести и сигнализация протоколов маршрутизации передаются через плоскость данных для проверки доступности, сигнальные пакеты IPv4 служат для маршрутизации IPv4, а сигнальные пакеты IPv6 - для маршрутизации IPv6.

При соответствующей реализации (см. параграф 6.13.2. Адресация на защищённых каналах) ACP обеспечивает доступность независимо от плоскости данных. Это позволяет плоскостям управления и OAM работать более надёжно.

- Для протоколов плоскости поддержки (management) ACP обеспечивает функциональность виртуальных отдельных каналов (Virtual out-of-Band или VooB), предоставляя связность со всеми узлами независимо от конфигурации плоскости данных, а также таблиц маршрутизации и пересылки.
- Протоколам плоскости управления (control) ACP позволяет работать даже при временных отказах плоскости данных и во время переходных процессов, таких как смена маршрутизации, которые хотя бы временно могут влиять на плоскость управления. Это особенно важно для автономных агентов служб, которые могут влиять на связность плоскости данных.

В документе Using Autonomic Control Plane for Stable Connectivity of Network OAM [RFC8368] примеры использования ACP рассмотрены более подробно и описано применение ACP в сетевой практике.

4. Требования (информационный раздел)

Ниже указаны требования информационного характера для проектирования ACP, основанные на рассмотренных в разделе 3 примерах. Требования к ACP, указанные в нормативных разделах соответствуют или превосходят их.

ACP1
ACP следует обеспечивать отказоустойчивую связность, независимо от настройки адресации, конфигурации и маршрутизации. На этом основаны требования 2 и 3, имеющие также самостоятельную ценность.

ACP2
Адресное пространство ACP должно быть отделено от адресов плоскости данных. Это обеспечит трассировку, упростит отладку, отделит от плоскости данных и защиты инфраструктуры (фильтрация по адресам).

ACP3
Адресное пространство ACP должно управляться автономно. Это упростит начальную загрузку и (автономную) настройку, повысит отказоустойчивость (администратор не сможет легко нарушить работу сети). Для этого в данном документе применяется схема ULA [RFC4193].

ACP4
ACP должна быть универсальной, т. е. применимой для всех функций и протоколов ANI. Клиентов ACP недопустимо привязывать к конкретным приложениям или транспортным протоколам.

ACP5
В ACP должна обеспечиваться защита. Проходящие через ACP сообщение должны аутентифицироваться (исходить от доверенных узлов) и настоятельно рекомендуется шифровать их.

Разъяснение требования ACP4. В полностью автономной сети (AN) все надавно написанные агенты служб (ASA) могут взаимодействовать с каждым другим агентом исключительно через GRASP и если бы это было единственным требованием к ACP, не требовась бы связность на уровне IPv6 между узлами, хватило бы GRASP. Тем не менее, поскольку ACP требуется также поддерживать неавтономные сети, очень важно обеспечивать связность IPv6 через ACP для работы любых протоколов транспортного и прикладного уровня.

ACP работает в поэтапном режиме (hop-by-hop), поскольку такое взаимодействие можно организовать на основе адресов IPv6 link-local, которые автономны и не зависят от конфигурации (требование ACP1). Может потребоваться связность ACP через узлы, не относящиеся к ACP, например, для соединения узлов ACP через Internet. Это возможно, но вызывает зависимость от стабильной и отказоустойчивой маршрутизации через узлы без ACP (см. параграф 8.2).

5. Обзор (информационный раздел)

Когда узел имеет сертификат ACP (6.2.1. Сертификаты ACP) и ACP активна (9.3.5. Включение ACP и ANI на уровне узла), узел будет создавать свою плоскость ACP без настройки, как указано ниже.

1. Узел создаёт экземпляр VRF или похожий виртуальный контекст для ACP.
2. Узел назначает себе адрес (префикс) ULA IPv6 (6.11. Адресация внутри ACP), взятый из поля acp-node-name (6.2.2. AcpNodeName в сертификате ACP) в своём сертификате ACP (6.2.1. Сертификаты ACP), на петлевом (loopback) интерфейсе (6.11. Адресация внутри ACP) и соединяет этот интерфейс с ACP VRF.

[1]Authentication, Authorization, and Accounting - проверка подлинности и полномочий, учёт.

3. Узел создаёт список кандидатов в партнеры-соседи и типов каналов-кандидатов для организации смежности. Это происходит автоматически для всех кандидатов link-local (6.4. Обнаружение соседей с помощью DULL GRASP) через все естественные интерфейсы (9.3.4. Какие интерфейсы включать автоматически?). Если кандидат в партнёры обнаружен через несколько интерфейсов, будет создаваться 1 смежность на интерфейс. Если узел ACP имеет несколько интерфейсов, подключённых к той же подсети, в которой он служит коммутатором L2 для плоскости данных, он применяет методы ACP с коммутацией L2 (см. раздел 7).
4. Для каждой записи списка кандидатов в соседи узел согласует защищённый туннель с использованием типа канала-кандидата (см. 6.6. Выбор канала).
5. Узел проверяет подлинность партнёра при организации защищённого канала и разрешает ему стать частью ACP в соответствии с параграфом 6.2.3. Проверка принадлежности к домену ACP.
6. Отказ при аутентификации кандидата в партнёры ведёт к дросселированию (throttle) попыток соединения, пока этот кандидат не будет обнаружен (см. 6.7. Проверка кандидата в соседи ACP).
7. Каждый созданный защищённый канал отображается на виртуальный интерфейс ACP, который помещается в ACP VRF (см. 6.13.5.2. Виртуальные интерфейсы ACP).
8. На каждом узле запускается облегченный протокол маршрутизации (6.12. Маршрутизация в ACP) для анонсирования доступности адреса (префикса) петлевого интерфейса ACP через плоскость ACP.
9. На этом завершается создание ACP с защищёнными поэтапными (hop-by-hop) туннелями, автоматической адресацией и маршрутизацией. Узел становится участником ACP.

Примечания.

- Ни одна из указанных выше операций (кроме настраиваемых явно) не отражается в конфигурации узла.
- Системы управления сетью без ACP (network management systems или NMS) и контроллеры SDN нужно явно настраивать для соединения с ACP.
- Для дополнительных партнерских соединений ACP через облака L3 без ACP требуется явная настройка (8.2. Соединение островков ACP через сети L3 без ACP (удалённые соседи)).

Схема ACP приведена на рисунке 1.

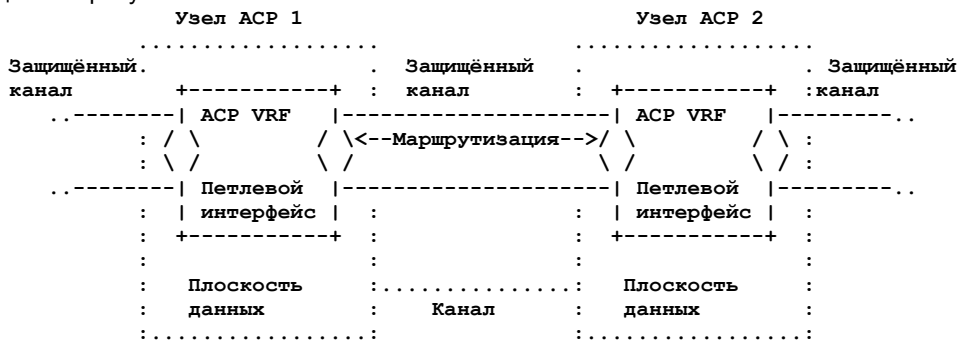

Рисунок 1. ACP VRF и защищённые каналы.

Полученная в результате наложенная сеть обычно основана исключительно на поэтапных (hop-by-hop) туннелях. Это обусловлено адресацией link-local на каналах IPv6, не требующей настройки для соединения, что позволяет создавать ACP даже через ненастроенные узлы или при наличии в плоскости данных проблем адресации или маршрутизации.

6. Создание ACP (нормативный раздел)

В этом разделе описаны компоненты и этапы создания ACP. Плоскость ACP автоматически создаёт себя, что делает её «неразрушимой» при большинстве изменений в плоскости данных, включая ошибки в настройке маршрутизации, адресации, NAT, межсетевых экранов или иных фильтров трафика, которые непреднамеренно или иначе с неизбежностью влияют на трафик плоскости управления, такой как команды оператора через интерфейс (CLI) или сессии NETCONF на контроллере, через которые вносятся изменения в плоскость данных.

Физические ошибки в соединениях между узлами ACP также не прервут работу ACP. Пока имеется переходный (транзитивный) физический путь между узлами, ACP следует обеспечивать восстановление за счёт работы через все интерфейсы узлов ACP и автоматического определения пути между ними.

Атаки на сеть с использованием некорректных адресных и маршрутных сведений в плоскости данных не будут влиять на ACP. Даже повреждённые узлы ACP будут иметь существенно меньший фронт атак, потому что только очень немногие конфигурации ACP или интерфейсов (up/down) могут влиять на ACP, а в зависимости от конкретного устройства и таких атак можно избежать (см. 9.3. Включение и отключение ACP и ANI и 11. Вопросы безопасности).

Узел ACP может быть маршрутизатором, коммутатором, контроллером, хостом NMS или иным узлом с поддержкой IPv6. Узел изначально **должен** иметь свой сертификат ACP, а также (пустую) таблицу соседей (6.3. Таблица смежности ACP). После этого узел может запустить поиск соседей ACP для построения плоскости ACP, как описано ниже.

6.1. Требования к использованию TLS

Ниже приведены требования к TLS при использовании протокола компонентами ACP. Такие компоненты включают поддержку сертификатов ACP через EST (6.2.5. Поддержка сертификата и привязки доверия), соединения TLS для точек распространения CRL (CRL Distribution Point или CRLDP) или ответчиков OCSP (Online Certificate Status Protocol) (6.2.3. Проверка принадлежности к домену ACP) и ACP GRASP (6.9.2. ACP как защищённая транспортная подложка для GRASP). На узлах ANI эти требования относятся и к BRSKI.

Протокол TLS **должен** соответствовать документу Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) [RFC7525], **требуется** поддержка TLS 1.2 (The Transport Layer Security (TLS) Protocol Version 1.2 [RFC5246]), а применять более старые версии TLS **недопустимо**. **Следует** поддерживать TLS 1.3 (The Transport Layer Security (TLS) Protocol Version 1.3 [RFC8446]). Выбор TLS 1.2 в качестве наименьшей версии для ACP основан на ожидаемой в настоящее время и весьма вероятной доступности для широкого класса узлов ACP, у которых может не быть гибкого стека TCP/IP.

В TLS **должны** поддерживаться алгоритмы TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 и TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 и **недопустимо** предлагать симметричное шифрование или хэширование с ключами короче 384 битов. При поддержке TLS 1.3 **должен** предлагаться TLS_AES_256_GCM_SHA384 и **можно** предлагать TLS_CHACHA20_POLY1305_SHA256.

В TLS **должно** включаться расширение Supported Elliptic Curves, которое **должно** поддерживать кривые NIST P-256 (secp256r1(22)) и P-384 (secp384r1(24)) из документа Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier [RFC8422]. Кроме того, клиентам TLS 1.2 **следует** передавать расширение ec_point_format с единственным элементом uncompressed.

6.2. Домен, сертификат и сеть ACP

ACP полагается на групповую безопасность. Домен ACP - это группа узлов, доверяющих друг другу в операциях ACP, таких как создание защищённых каналов «точка-точка» между членами домена ACP по протоколам IPsec и т. п. Для аутентификации и предоставления полномочий другому узлу ACP с доступом в домен ACP каждому члену ACP нужен ключевой материал - узел ACP **должен** иметь сертификат LDevID и сведения об 1 или нескольких привязках доверия (TA), требуемые для проверки принадлежности к домену ACP (6.2.3. Проверка принадлежности к домену ACP).

Задание ключей вручную через общие секреты не подходит для домена ACP, поскольку требует иметь один общий секрет для всех имеющихся и будущих членов домена ACP, чтобы соответствовать ожиданиям автономной организации партнерских (peer-to-peer) защищённых каналов между любыми членами домена ACP. Такой общий секрет привёл бы к слабости защиты. Асимметричный ключевой материал (открытые ключи) без сертификатов не обеспечивает механизма аутентификации принадлежности к домену ACP в автономной партнерской манере для имеющихся и будущих членов домена ACP.

Сертификат LDevID далее называется сертификатом ACP. TA - это сертификат корневого CA в домене ACP domain.

ACP не требует конкретных механизмов предоставления ключевого материала узлу ACP. Требуется лишь соответствие параграфу 6.2.1. Сертификаты ACP, в частности, наличие acp-node-name, указанного в параграфе 6.2.2. AcpNodeName в сертификате ACP, в сертификате домена, а также в сертификатах кандидатов в партнёры ACP. Варианты зачисления и предоставления рассмотрены в приложении A.2. Начальная загрузка BRSKI (ANI).

В этом документе термин ACP часто применяется в тех местах, где документы по автономным сетям [RFC7575] и [RFC8993] применяют слово «автономный» (autonomic). Причина заключается в том, что упомянутые документы рассматривают лишь полностью автономные сети и узлы, но поддержка ACP не требует других компонентов автономной сети за исключением зависимости от GRASP и обеспечения защиты и транспорта для GRASP. Поэтому слово «автономный» могло бы создать путаницу для операторов, заинтересованных лишь в ACP.

В [RFC7575] автономный домен (autonomic domain) определён как набор автономных узлов. Узлам ACP не требуется быть полностью автономными, но когда это так, домен ACP является автономным доменом. В [RFC8993] сертификат домена (domain certificate) определён как сертификат, применяемый в автономном домене. Сертификат ACP является таким сертификатом домена, когда узлы ACP являются (полностью) автономными узлами. Сетью ACP в этом документе называется сеть, созданная активными узлами ACP в домене ACP. Сеть ACP может включать не только узлы ACP, как указано в параграфе 8.1. ACP Connect.

6.2.1. Сертификаты ACP

Сертификаты ACP **должны** быть совместимыми с [RFC5280] сертификатами X.509 v3 [X.509].

Узлы ACP **должны** поддерживать обработку сертификатов ACP, TA и сертификатов цепочек сертификации (далее сертификаты) с открытыми ключами RSA и эллиптических кривых (Elliptic Curve Cryptography или ECC).

Узлам ACP **недопустимо** поддерживать сертификаты с открытыми ключами RSA с модулем короче 2048 битов или групп с порядком менее 256 битов. Они **должны** поддерживать сертификаты с открытым ключом RSA с модулем 2048 битов и **могут** поддерживать более длинные ключи RSA. **Должны** поддерживаться сертификаты с открытым ключом ECC, использующие кривые NIST P-256, и **следует** поддерживать кривые P-384 и P-521.

Узлам ACP **недопустимо** поддерживать сертификаты с открытыми ключами RSA с модулем короче 2048 битов или ECC из групп с порядком менее 256 битов. **Должны** поддерживаться сертификаты подписей RSA с открытым ключом 2048 битов и **могут** поддерживаться такие сертификаты с более длинным ключом. **Должны** поддерживаться сертификаты ECDSA, использующие кривые NIST P-256, и **следует** поддерживать кривые P-384 и P-521.

Узлы ACP **должны** поддерживать сертификаты RSA с подписями RSA и дайджестом содержимого SHA-256, а также **следует** поддерживать дайджесты SHA-384 и SHA-512 в таких подписях. Такие же требования применимы к подписям сертификатов ECDSA (Elliptic Curve Digital Signature Algorithm) и дополнительно узлы ACP **должны** поддерживать подписи ECDSA в сертификатах ECDSA.

В сертификатах ACP **следует** применять ключ и подпись RSA, когда такой сертификат предназначен для использования лишь при аутентификации ACP. Сертификат ACP **может** использовать ключ ECC и подпись ECDSA, если этот сертификат предназначен лишь для аутентификации и проверки полномочий в ACP и ANI.

Все протоколы защиты каналов, применяемые для ACP в соответствии с этим документом или его расширениями, **должны** поддерживать аутентификацию (например, подпись), начиная с этих типов сертификатов. Дополнительные сведения приведены в [RFC8422].

Выбор алгоритмов обусловлен тем, что в 2020 г. RSA применялся все еще чаще ECC, поэтому для RSA указан уровень **должен**. ECC обеспечивает эквивалентную защиту с более коротким (логарифмически) ключом (см. [RFC8422]). Это

может давать преимущества, особенно при ограниченной пропускной способности или наличии узлов с ограничениями в сети ACP/ANI. Некоторые функции ACP, такие как партнерские отношения GRASP через ACP, требуют сквозной аутентификации каждого с каждым, поэтому ECC можно надёжно применять в ACP лишь в тех случаях, когда его **должны** поддерживать все узлы ACP. Подписи RSA должны поддерживаться и для сертификатов ECC, поскольку сами CA могут ещё не поддерживать ECC.

Сертификат ACP **следует** применять при каждой аутентификации между узлами с сертификатами ACP (узлы ACP и NOC), где полномочия предоставляются лишь членам домена ACP, например, сквозная защита между узлом ACP и NOC/OAM, а также между ASA и ASA. Проверка принадлежности к домену описана в параграфе 6.2.3. Использование этой проверки стандартизовано здесь для создания защищённых поэтапных каналов ACP (6.8. Протоколы защищённых связей (каналов)) и для ACP GRASP (6.9.2. ACP как защищённая транспортная подложка для GRASP) через TLS.

Для проверки принадлежности к домену ACP требуется минимальное числ0 элементов в сертификате, как описано в параграфе 6.2.3. Отождествление узла в ACP передаётся в поле acp-node-name, как указано в параграфе 6.2.2.

Для применения алгоритма Диффи-Хеллмана на эллиптических кривых (Elliptic Curve Diffie-Hellman или ECDH) напрямую с ключом в сертификате ACP сертификаты с ключами ECC должны указывать поддержку ECDH, если присутствует расширение X.509 v3 keyUsage, должен быть установлен бит keyAgreement. Отметим, что эта опция не требуется ни для одного из требуемых этим документом шифров и может не поддерживаться некоторыми CA.

Остальные поля сертификата ACP заполняются в соответствии с [RFC5280]. Коль скоро они соответствуют [RFC5280], любое иные поля сертификата ACP можно установить по желанию оператора домена ACP через подходящего регистратора ACP и/или процедуры ACP CA. Например, другие поля могут потребоваться для целей, отличающихся от предусмотренных для сертификата ACP (скажем, элементы SubjectName).

В остальном сертификаты ACP могут следовать рекомендациям [CABFORUM].

Для диагностики и рабочих задач полезно скопировать идентифицирующие устройство поля сертификата IDevID узла в сертификат ACP, например, атрибут serialNumber (параграф 6.2.9 в [X.520]) в поле субъекта кодирования отличительного имени. Отметим, что это не serial-number из сертификата (см. также параграф 2.3.1 в [RFC8995]). Это можно сделать, например, если допустимо передать serialNumber по протоколу обнаружения на канальном уровне (Link Layer Discovery Protocol или LLDP) [LLDP], поскольку, как передаваемая через LLDP информация, сведения из сертификата ACP могут извлечь соседние узлы без дальнейшей аутентификации и применить их как для полезной диагностики, так и для вредоносных атак. Извлечение сертификата ACP возможно с помощью (неудачной) попытки создать защищённый канал ACP, а serialNumber обычно содержит сведения о типе устройства, которые могут способствовать более быстрому обнаружения действующих эксплойтов или атак на устройство.

Отметим, что здесь нет намерения ограничить проверку полномочий в ACP или автономных сетях, использующих ACP, просто проверкой принадлежности к домену ACP, заданной в этом документе. Проверка может быть расширена или изменена дополнительными требованиями. Такие проверки полномочий могут в будущем использовать и требовать наличия дополнительных элементов в сертификатах или правилах, а также дополнительных сертификатов. Дополнительная проверка атрибута использования расширенного ключа id-kp-cmcRA рассмотрена в параграфе 6.2.5. Поддержка сертификата и привязки доверия, а также в Certificate Management over CMS (CMC) Updates [RFC6402] и приложении A.9.5. Назначение роли.

6.2.2. AcpNodeName в сертификате ACP

```
acp-node-name = local-part "@" acp-domain-name
local-part = [ acp-address ] [ "+" rsub extensions ]
acp-address = 32HEXDIG / "0" ; HEXDIG из Приложения B.1 к [RFC5234]
rsub = [ <subdomain> ] ; <subdomain> из параграфа 3.5 в [RFC1034]
acp-domain-name = <domain> ; из параграфа 3.5 в [RFC1034]
extensions = *( "+" extension )
extension  = 1*etext  ; определение будущего стандарта.
etext      = ALPHA / DIGIT /  ; Printable US-ASCII
             "!" / "#" / "$" / "%" / "&" / "'" /
             "*" / "-" / "/" / "=" / "?" / "^" /
             "_" / "`" / "{" / "|" / "}" / "~"

routing-subdomain = [ rsub "." ] acp-domain-name
```

Рисунок 2. ACP Node Name ABNF.

Например, адрес ACP fd89:b714:f3db:0:200:0:6400:0000, домен ACP с именем acp.example.com и расширение rsub area51.research дают в результате

```
acp-node-name      = fd89b714f3db0000020000064000000
                     +area51.research@acp.example.com
acp-domain-name    = acp.example.com
routing-subdomain  = area51.research.acp.example.com
```

Поле acp-node-name на рисунке 2 - это определение ABNF (Augmented BNF for Syntax Specifications: ABNF [RFC5234]) для ACP Node Name. Сертификат ACP **должен** содержать эту информацию. Он **должен** включать поле otherName в расширение X.509 Subject Alternative Name, а в otherName **должно** содержаться AcpNodeName, как указано в параграфе 6.2.2.1. Модуль ASN.1 AcpNodeName .

Соответствующие этой спецификации узлы **должны** быть способны получить свой адрес ACP через сертификат домена и в этом случае их собственный сертификат ACP **должен** иметь поле 32HEXDIG acp-address. Регистр символов в поле acp-address значения не важен, поскольку поле имеет тип ABNF HEXDIG. Рекомендуется использовать в поле acp-address строчные буквы. Соответствующие этой спецификации узлы **должны** быть способны аутентифицировать узлы как членов домена ACP или партнёров по защищённому каналу ACP, когда они имеют поле acp-address=0, и как членов домена ACP (не не партнёров по защищённому каналу ACP), когда поле acp-address отсутствует в AcpNodeName (см. 6.2.3. Проверка принадлежности к домену ACP).

Поле acp-domain-name служит для указания домена ACP, через который узлы ACP проверяют подлинность и полномочия друг друга, например, для создания защищённых каналов ACP между собой (6.2.3. Проверка принадлежности к домену ACP). В acp-domain-name следует указывать FQDN домена Internet, принадлежащего сетевой администрации ACP и в идеале зарезервированного для ACP. В этой спецификации оно служит именем для ACP, которое в идеале является уникально глобальным. Когда имя acp-domain-name уникально в глобальном масштабе, конфликты адресов ACP в разных доменах ACP возможны лишь в результате конфликтов хэш-значений ULA (6.11.2. Базовая схема адресации ACP). Используя разные acp-domain-name, операторы могут различать ACP даже при совпадении TA.

Для сохранения простоты кодирования другие языки для acp-domain-name не рассматриваются. Значение acp-node-name не предназначено для конечных пользователей. Не предусмотрено защиты от выбора оператором любого доменного имени для ACP, даже если тот не владеет доменом. Имя домена служит лишь в качестве хэш-затравки для ULA и операторской диагностики. Поэтому оператору, у которого есть домен лишь на отличном от английского языке (internationalized), следует иметь возможность выбора любой уникальной строки 7-битовых символов ASCII для представления в acp-domain-name доменного имени на другом языке.

Строку routing-subdomain можно создать из acp-node-name и применять для создания хэша ULA (6.11.2. Базовая схема адресации ACP). Наличие rsub позволяет реализовать в одном домене ACP несколько префиксов ULA /48 (см. примеры в A.6. CA, домены и маршрутные субдомены).

Необязательное поле расширения служит для стандартизации будущих расширений этой спецификации и **должно** игнорироваться в случае непонимания.

Ниже указаны и обоснованы принятые варианты кодирования.

1 Формат.

1.1 Требуется включить rsub в local-part. Если в формат включено лишь поле routing-subdomain как доменная часть acp-node-name, rsub и acp-domain-name нельзя отделить друг от друга при определении в процессе проверки принадлежности к домену ACP, какая часть является acp-domain-name, а какая служит лишь для создания отличающегося префикса ULA.

1.2 Если acp-address и rsub отсутствуют в AcpNodeName, local-part будет иметь формат "++extension(s)". Два символа + требуются для того, чтобы узел мог однозначно увидеть отсутствие acp-address и rsub.

2 Причины выбора описанного здесь кодирования доменного имени и адреса ACP.

2.1 Поле acp-node-name служит идентификатором ACP для узла. Оно включает компоненты, требуемые для идентификации ACP узла как изнутри, так и извне ACP.

2.2 Для ручной и автоматизированной диагностики, а также управления устроствами и ACP требуется иметь понятное человеку и пригодное для машинного разбора стандартное представление acp-node-name в одну строку. Например, системы инвентаризации и другие backend-системы всегда идентифицируют элемент по уникальной строке, а не по комбинации нескольких полей, которая потребовалась бы в ином случае.

2.3 Если кодирование отличалось бы от такой строки, пришлось бы задать другое стандартное кодирование, чтобы представить этот формат (стандартное кодирование в строку) для применения операторам.

2.4 Адреса вида <local>@<domain> стали предпочтительным форматом для идентификаторов элементов во многих системах, включая большинство идентификаторов в web и мобильных приложениях, таких как многодоменные системы с единым входом.

3 Совместимость.

3.1 Следует обеспечить возможность применения сертификата ACP в качестве сертификата LDevID в системах, используемых помимо ACP. Поэтому информационные элементы, требуемые для ACP, следует кодировать так, чтобы минимизировать возможность несовместимости с другими приложениями. Например, атрибуты поля субъекта часть используются отличными от ACP приложениями, поэтому их не следует занимать новыми значениями ACP.

3.2 Элементам не следует требовать дополнительного кодирования и/или декодирования ASN.1, поскольку библиотеки для доступа к сведениям из сертификатов, особенно во встраиваемых устройствах, могут не поддерживать расширенное декодирование ASN.1 сверх предопределённых обязательных полей. Поля subjectAltName и otherName уже используются с одним строковым параметром для нескольких otherName (см. Extensible Messaging and Presence Protocol (XMPP): Core" [RFC6120], "Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI) [RFC7585], Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name [RFC4985], Internationalized Email Addresses in X.509 Certificates [RFC8398]).

3.3 Элементам, требуемым для ACP, следует минимизировать риск ошибочной интерпретации при ином применении сертификатов LDevID. Их недопустимо трактовать как адреса электронной почты, поэтому применение опций otherName и rfc822Name в сертификатах будет неуместным.

Подробное описание поля subjectAltName приведено в параграфе 4.2.1.6 [RFC5280].

6.2.2.1. Модуль ASN.1 AcpNodeName

Приведённый ниже модуль ASN.1 нормативно задаёт структуру AcpNodeName. Эта спецификация использует определения ASN.1 из документа New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX) [RFC5912] с нотацией 2002 ASN.1. В [RFC5912] обновлены нормативные документы, использовавшие старую нотацию ASN.1.

```
ANIMA-ACP-2020
  { iso(1) identified-organization(3) dod(6)
    internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-anima-acpnodename-2020(97) }
```

```
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
  OTHER-NAME
  FROM PKIX1Implicit-2009
    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-mod(0)
      id-mod-pkix1-implicit-02(59) }

  id-pkix
  FROM PKIX1Explicit-2009
    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-mod(0)
      id-mod-pkix1-explicit-02(51) } ;

  id-on OBJECT IDENTIFIER ::= { id-pkix 8 }

  AcpNodeNameOtherNames OTHER-NAME ::= { on-AcpNodeName, ... }

  on-AcpNodeName OTHER-NAME ::= {
      AcpNodeName IDENTIFIED BY id-on-AcpNodeName
  }

  id-on-AcpNodeName OBJECT IDENTIFIER ::= { id-on 10 }

  AcpNodeName ::= IA5String (SIZE (1..MAX))
   -- AcpNodeName в соответствии с этим документом передаёт
   -- поле acp-node-name, заданное ABNF в параграфе 6.2.2

END
```

Рисунок 3. Модуль ASN.1 AcpNodeName.

6.2.3. Проверка принадлежности к домену ACP

Ниже указаны этапы проверки принадлежности к домену ACP на основании сертификата кандидата в партнёры.

1. Проверяется владение партнёром секретным ключом, соответствующим открытому ключу в сертификате. Эта проверка выполняется с помощью применяемого протокола защищённых связей, например, как описано в параграфе 2.15 Internet Key Exchange Protocol Version 2 (IKEv2) [RFC7296].

2. Проверяется путь для сертификата партнёра в соответствии с разделом 6 в [RFC5280] по отношению к одной из привязок доверия (TA), связанных с сертификатом ACP узла ACP (6.2.4. Привязки доверия). Это включает проверку срока действия сертификатов в пути.

3. Если в сертификате партнёра указан ответчик CRLDP ([RFC5280], параграф 4.2.1.13) или OCSP ([RFC5280], параграф 4.2.2.1), сертификат партнёра **должен** быть действительным в соответствии с этими механизмами, когда они доступны. Проверка OCSP для сертификата партнёра через ACP должна быть успешной, этот партнёр должен отсутствовать в списке CRL, полученном от CRLDP. Эти механизмы недоступны, когда узел ACP не имеет связности (ACP или иной) для получения текущего списка CRL, не имеет доступа к ответчику OCSP, а протокол защищённой связи также не может передать CRL и проверить OCSP.

   Повторные попытки узнать об отзыве через OCSP или CRL **следует** предпринимать с использованием отсрочки, как описано в 6.7. Проверка кандидата в соседи ACP. Когда узел ACP узнает о недействительности партнерского сертификата ACP, для которого проверка 3 была пропущена в процессе создания защищённого канала ACP, защищённый канал ACP к этому партнёру **должен** быть закрыт, даже если он является единственным соединением для доступа CRL/OCSP. Это относится ко всем защищённым каналам ACP к данному партнёры, если их больше 1. Соединение по защищённому каналу ACP **должно** повторяться периодически на случай обретения соседом нового, действительного сертификата.

4. Проверяется синтаксическая корректность поля acp-node-name в сертификате партнёра и совпадение acp-domain-name в acp-node-name из этого сертификата со значением в сертификате данного узла ACP (с приведением символов к нижнему регистру).

При организации защищённого канала ACP выполняется ещё одна проверка сертификата кандидата в партнёры.

5. Поле acp-address присутствует в AcpNodeName сертификата и имеет форму 32HEXDIG или 0 (Рисунок 2).

Технически защищённые каналы ACP можно организовать лишь с узлами, имеющими acp-address. Правило 5 гарантирует учёт этого при проверке принадлежности к домену ACP.

Узлы без поля acp-address могут использовать свой сертификат домена ACP лишь для аутентификации защищённого канала без ACP. Это включает, например, узлы NMS, которым разрешено взаимодействовать с ACP через ACP connect (параграф 8.1)

Особый случая значения 0 в поле acp-address сертификата ACP предназначен для узлов, которые могут и должны определять свой адрес ACP с помощью механизма, отличающегося от получения из поля acp-address в сертификате ACP. Таким узлам ACP разрешена организация защищённых каналов ACP. Механизмы определения адреса ACP такими узлами выходят за рамки этой спецификации, но такая возможность включена, чтобы любой узел ACP мог создать защищённые каналы ACP в соответствии с правилом 5.

Необязательное поле rsub в AcpNodeName не связано с проверкой принадлежности к домену ACP, поскольку оно служит лишь для структурирования маршрутизации и адресации внутри ACP, а не ручной взаимной проверки подлинности и полномочий (отсюдя название субдомен маршрутизации - routing subdomain).

- Этапы 1 - 4 представляют собой стандартную проверку сертификата и аутентификацию секретного ключа в соответствии с [RFC5280], а также протоколов защищённой связи (таких как IKEv2 [RFC7296]) при использовании сертификатов.
- За исключением открытого ключа, этапы 1 - 4 не проверяют какие-либо заданные заранее элементы отождествления сертификата, такие как префикс доменного имени web-сервера, который часто кодируется в общем имени сертификата. Этап 5 является эквивалентом для AcpNodeName.
- На этапе 4 выполняются стандартные проверки CRL и OCSP, усовершенствованные для случая отсутствия связности и ограниченной функциональности протоколов защищенной связи.
- Этапы 1 - 4 разрешают создание любых защищённых соединений между членами одного домена ACP за исключением защищённых каналов ACP.
- Этап 5 включает дополнительную проверку наличия адреса ACP, требуемого для защищённого канала ACP.
- Таким образом, этапы 1 - 5 разрешают создание защищённого канала ACP.

Для краткости в оставшейся части документа этот процесс указывается лишь как аутентификация без упоминания проверки полномочий.

6.2.3.1. Проверка часов и времени

Узел ACP с часами (realtime), в которых он уверен, **должен** проверять временные метки при проверке принадлежности к домену ACP, например, проверять срок действия сертификата на этапе 1 и соответствующее время на этапе 4 для сведений об отзыве (например, signingTimes в подписях Cryptographic Message Syntax (CMS)).

Узел ACP без таких часов **может** пропускать проверку временных меток, если он не знает текущего времени. Таким узлам ACP **следует** определять текущее время защищённым способом, например, по протоколу NTP через ACP. Проверка временных меток пропускается лишь до момента определения текущего времени. При отсутствии защищённого механизма такой узел ACP **может** использовать при проверке принадлежности к домену ACP текущее время, определённое незащищённым путём.

Узнать текущее время незащищённым способом **можно**, например, по протоколу NTP (Network Time Protocol Version 4: Protocol and Algorithms Specification [RFC5905]) через тот же адрес IPv6 link-local, который используется для ACP с соседними узлами ACP. Узлам ACP, предоставляющим NTP без защиты по своим адресам link-local, **следует** сначала запустить NTP через ACP и получать время NTP через ACP только из доверенных источников. Детали таких процедур NTP выходят за рамки этой спецификации.

Помимо проверки принадлежности к домену, ACP не зависит от знания текущего времени, но оно может требоваться для протоколов и служб, использующих ACP (например, для записи событий в системный журнал.

6.2.4. Привязки доверия

Узлам ACP нужны сведения о привязках доверия (TA) в соответствии с параграфом 6.1.1 (d) в [RFC5280], обычно в форме одного или нескольких сертификатов TA для проверки пути в соответствии с правилом 2 параграфа 6.2.3. Сведения о TA **должны** предоставляться узлу ACP (вместе с сертификатом домена ACP) регистратором ACP при начальном зачислении узла-кандидата ACP. Узлы ACP **должны** также поддерживать обновление сведений о TA через EST, как описано в параграфе 6.2.5. Поддержка сертификата и привязки доверия.

Требуемые сведения о TA могут состоять из одного или нескольких сертификатов, необходимых для обновления сертификатов CA, как указано в параграфе 4.4 Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP) [RFC4210]).

Путь к сертификату - это цепочка сертификатов, начинающаяся с сертификата ACP (лист и/или конечный элемент), за которым могут следовать сертификаты CA, и заканчивающаяся данными о TA, которыми обычно служат 1 или несколько самоподписанных сертификатов TA. Удостоверяющий центра (CA), подписавший сертификат ACP, называется назначающим CA. При отсутствии промежуточных CA назначающим CA служит TA. Путь проверки сертификатов подтверждает, что TA, связанная с ACP разрешает сертификат напрямую или опосредованно через один или несколько промежуточных CA.

Отметим, что у разных узлов ACP могут быть разные промежуточные CA на пути сертификации и даже разные TA. Набор TA для домена ACP должен быть согласованным для всех членов ACP, чтобы любой узел ACP мог проверить подлинность любого другого узла ACP. Протоколы, используемые на этапах 1 - 3 при проверке принадлежности к домену ACP должны поддерживать обмен не только сертификатам узлов ACP но и промежуточными TA.

Для проверки принадлежности к домену ACP узлы ACP **должны** поддерживать проверку пути сертификации без промежуточных CA или с одним таким CA. **Следует** поддерживать 2 промежуточных CA и 2 TA (для смены TA).

Сертификаты для ACP **должны** выдаваться лишь узлам, которым разрешено входить в домен ACP. Когда подписывающий CA полагается на регистратора ACP, он **должен** подписывать только сертификаты с acp-node-name от доверенных регистраторов ACP. При этом может применяться любой имеющийся CA, не знающий формата acp-node-name.

Эти требования могут быть выполнены за счёт использования частной TA домена ACP или с помощью соглашений между вовлечёнными сторонами (регистратор и CA). Применение общественных CA выходит за рамки документа.

Один владелец может управлять несколькими независимыми доменами ACP с одним набором TA. При этом регистраторы должны знать, в какой плоскости ACP нужно регистрировать узел.

6.2.5. Поддержка сертификата и привязки доверия

Узлы ACP **должны** поддерживать обновление своего сертификата и данных о TA через EST и **могут** поддерживать иные механизмы. Требования для TLS указаны в параграфе 6.1. Требования к использованию TLS. Сеть ACP **должна** иметь хотя бы 1 узел ACP с функциональностью сервера EST, чтобы можео было использовать обновление по EST.

Узлу ACP **следует** помнить параметры GRASP O_IPv6_LOCATOR сервера EST, на котором он последний раз обновлял свой сертификат ACP. **Следует** обеспечивать возможность установки этих параметров сервера EST регистратором ACP (6.11.7. Регистраторы ACP), который исходно зачислил устройство ACP с его сертификатом ACP. При использовании BRSKI (см. [RFC8995]) локатор IPv6 для регистратора BRSKI из соединения BRSKI TLS **следует** запоминать и применять при следующем обновлении через EST, если этот регистратор также объявляет себя сервером EST через GRASP на своём адресе ACP (6.2.5.1. Цель GRASP для сервера EST).

Сервер EST **должен** представить сертификат, прошедший проверку членства в домене ACP, при организации соединения TLS (правила 1 - 4 из параграфа 6.2.3, но без правила 5, поскольку это не создание защищённого канала ACP). Сертификат сервера EST **должен** также включать атрибут расширенного использования ключа id-kp-cmcRA [RFC6402], а клиент EST **должен** проверять его наличие.

Дополнительная проверка поля расширенного применения ключа id-kp-cmcRA гарантирует, что клиенты не станут жертвами подставного сервера EST. Хотя таким незаконным серверам EST не следует иметь возможность поддержки запросов на подпись сертификата (они не могут получит ответ на подпись от действительного CA), они могут представить поддельный сертификат CA клиентам EST, которым нужно обновить просроченные сертификаты CA.

Отметим, что серверам EST, поддерживающим несколько доменов ACP, потребуется отдельный сертификат для каждого домена ACP и нужно отвечать по разным транспортным адресам (IPv6 и/или порт TCP). Это легко автоматизировать на сервере EST, если CA позволяет регистраторам запрашивать для себя сертификаты с расширенным использованием ключа id-kp-cmcRA.

6.2.5.1. Цель GRASP для сервера EST

Узлы ACP, являющиеся серверами EST, **должны** анонсировать свои услуги в ACP сообщениями GRASP Flood Synchronization (M_FLOOD). Определение этих сообщений дано в параграфе 2.8.11 [RFC8990], а на рисунке 4 представлен пример.

```
[M_FLOOD, 12340815, h'fd89b714f3db0002000000064000001', 210000,
    [["SRV.est", 4, 255 ],
    [O_IPv6_LOCATOR,
         h'fd89b714f3db0002000000064000001', IPPROTO_TCP, 443]]
]
```

Рисунок 4. Пример цели GRASP SRV.est.

Формат определения цели в CDDL (см. Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures [RFC8610]) приведён на рисунке 5.

```
flood-message = [M_FLOOD, session-id, initiator, ttl,
                 +[objective, (locator-option / [])]]
                             ; См. пример выше о объяснения ниже
                             ; для initiator и ttl.

objective = ["SRV.est", objective-flags, loop-count,
                                      objective-value]

objective-flags = sync-only  ; Как в [RFC8990].
sync-only       = 4          ; M_FLOOD требует лишь синхронизации.
loop-count      = 255        ; Рекомендуется при отсутствии механизма
                             ; определения диаметра сети.
objective-value = any        ; Резерв для будущих расширений.
```

Рисунок 5. Определение GRASP SRV.est.

Имя SRV.est указывает, что целью служит сервер EST, соответствующий [RFC7030], поскольку est - зарегистрированное имя службы (Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry [RFC6335]) для [RFC7030]. Поле objective-value при его наличии **должно** игнорироваться. Совместимое с прежними версиями расширение [RFC7030] **можно** указать в objective-value. Опции обновления сертификата, не совместимые с [RFC7030], **должны** использовать другие objective-name. Нераспознанные поля objective-value (или их части при непонятной структуре) **должны** игнорироваться.

Сообщения M_FLOOD **должны** передаваться периодически. По умолчанию **следует** использовать интервал 60 секунд, оператору **следует** иметь возможность изменения периода, но не **следует** делать его меньше 60 секунд. Частота передачи **должна** быть такой, чтобы общее число периодических M_FLOOD от всех источников не вызывало значительного трафика в ACP. Для параметра ttl **следует** устанавливать значение в 3,5 раза больше периода, чтобы можно было отбросить до 3 последовательных сообщений, прежде чем анонс будет сочтён просроченным. В приведённом выше примере установлено ttl = 210000 мсек, т. е. 3,5 + 60 секунд. Когда анонсировавший эти параметры неожиданно «умирает» сразу после отправки M_FLOOD, получатели особзнают это через 210 секунд. Если получатель попытается подключиться к неработающей службе до истечения этого интервала, он столкнётся с отказом, который послужит индикацией недоступности экземпляра сервиса, и выберет иной экземпляр (из другого анонса GRASP).

Цели SRV.est **следует** анонсировать лишь в случаях, когда узел ACP знает, что он может связаться с CA для обновления EST и/или смены ключей в домене ACP (см. 11. Вопросы безопасности).

6.2.5.2. Обновление

При обновлении узлу **следует** соединяться с запомненным сервером, а при неудаче - с узнанным от GRASP. Сервер, с которого удалось обновить сертификат, **следует** запомнить для последующего обновления. Запоминание и предпочтение сервера последнего обновления обеспечивает привязку, которая может помочь при диагностике, а также обеспечивает некоторую защиту от скомпрометрированных членов ACP, анонсирующих ложные данные в GRASP.

Обновление сертификатов **следует** запускать по истечении 50% срока действия сертификата домена, чтобы у сетевых операций было достаточно времени для поиска и устранения проблем, препятствующих своевременному обновлению сертификата домена, а также для обеспечения продолжения работы частей сети, из которых недоступны CA.

6.2.5.3. Списки отзыва сертификатов (CRL)

Узлу ACP **следует** поддерживать отзыв сертификата через списки CRL (Certificate Revocation List) по протоколу HTTP с одной или несколькими точками распространения CRL (CRL Distribution Point или CRLDP). CRLDP **должны** указываться в сертификате домена. Если CRLDP URL использует адрес IPv6 (адрес ULA при использовании заданных в этом документе правил), узел ACP будет соединяться с CRLDP через ACP. Если CRLDP использует доменное имя, узел ACP будет связываться с CRLDP через плоскость данных.

Обычно для CRLDP применяются доменные имена, но для ACP не задана поддержка DNS. Поиск в DNS через плоскость данных не только может вызывать проблемы безопасности, но и не указывает, предназначен ли распознанный адрес для доступа через ACP. Поэтому применение адреса IPv6 вместо имени DNS эффективней, поскольку указывает доступность CRLDP через ACP.

Доступ к CRLDP через ACP можно обеспечить, разместив службы на узле с ACP или подключившись к узлу через интерфейс ACP connect (см. параграф 8.1).

При использовании частной инфраструктуры PKI для сертификатов ACP может потребоваться знать CRL, например, для запрета анализа операционной практики домена путём отслеживания роста CRL. В этом случае можно выбрать HTTPS для защиты конфиденциальности, особенно при доступности CRL в плоскости данных. Для проверки подлинности и полномочий **следует** использовать сертификаты ACP и проверку принадлежности к домену ACP (параграф 6.2.3). CRLDP **может** пропускать проверку CRL при аутентификации партнёра, чтобы разрешить извлечение CRL узлам ACP с отозванным сертификатом ACP, что может помочь (бывшему) узлу ACP быстрее узнать об отзыве своего сертификата. Однако это может нарушать требование знать списки (need-to-know). Узлы ACP **могут** поддерживать операции CRLDP по протоколу HTTPS.

6.2.5.4. Срок действия

Срок действия сертификата может быть короче обычного (1 год), поскольку обновление сертификатов полностью автоматизировано через ACP и EST. Основным фактором, сдерживающим сокращение срока действия, является нагрузка на серверы EST и CA. Поэтому рекомендуется поддерживать сертификаты ACP через цепочку CA, где производительности назначающего CA достаточно для управления краткосрочными сертификатами. Пример реализации этого приведён в параграфе 9.2.4. Регистраторы ACP с суб-CA. См. также Support for Short-Term, Automatically Renewed (STAR) Certificates in the Automated Certificate Management Environment (ACME) [RFC8739].

При достаточно коротком сроке действия сертификатов, например, несколько часов, отзыв сертификатов может не требоваться, что позволяет упростить инфраструктуру поддержки сертификатов.

В Приложении A.2 рассмотрена оптимизация поддержки сертификатов при использовании BRSKI [RFC8995].

6.2.5.5. Повторное зачисление

Узел ACP может определить, что срок действия его сертификата ACP закончился, после продолжительного выключения или отсоединения. В этом случае узел ACP **следует** заново зачислить в роли кандидата ACP. В этой роли узел поддерживает TA и цепочку сертификатов, связанные с сертификатом ACP, исключительно для повторного зачисления и пытается (или ждёт) повторного зачисления с новым сертификатом ACP. Детали этого зависят от механизмов и протоколов, применяемых регистраторами ACP. Использование регистраторов и ваучеров в разъяснено в параграфе 6.11.7. Регистраторы ACP и [RFC8995]. Когда предполагается использование ACP без BRSKI, приведённые ниже сведения о BRSKI и ваучерах можно опустить.

При использовании BRSKI (т. е. на узлах ACP, являющихся узлами ANI) повторно зачисляемый узел-кандидат в ACP пытается регистрироваться как кандидат в узлы ACP (поручительство BRSKI), но вместо применения сертификата IDevID узла ACP ему **следует** сначала попытаться использовать свой сертификат домена ACP в аутентификации BRSKI TLS. Регистратор BRSKI **может** принять этот сертификат после завершения его срока исключительно для повторного зачисления. Использование сертификата домена ACP узлом позволяет регистратору BRSKI узнать acp-node-name узла, чтобы назначить те же адресные данные ACP этому узлу в новом сертификате ACP.

Если регистратор BRSKI отвергает применение старого сертификата ACP повторное зачисление узла-кандидата ACP **должно** предпринять попытку регистрации с использованием сертификата IDevID, как задано в BRSKI, при создании соединения TLS.

При попытке соединения BRSKI со старым сертификатом ACP или сертификатом IDevID кандидату на повторное зачисление в ACP **следует** аутентифицировать регистратора BRSKI в процессе организации соединения TLS на основе имеющихся сведений о цепочке сертификатов TA, связанных со старым сертификатом ACP. Кандидату на повторное зачисление в ACP **следует** возвращаться к запросу ваучера у регистратора BRSKI лишь при отказе аутентификации в процессе организации соединения TLS. В качестве меры против атак с попыткой заставить узел ACP забыть прежний (просроченный) сертификат и TA узлу ACP следует чередовать попытки повторного зачисления с использованием старого ключевого материала, сертификата IDevID и запроса ваучера.

При использовании отличных от BRSKI механизмов повторного зачисления сертификата ACP принципы остаются теми же. Кандидат на повторное зачисление в ACP пытается аутентифицировать любые партнерские узлы регистратора ACP, используя протоколы повторного зачисления и/или механизмы с имеющейся цепочкой сертификатов и/или сведениями TA, и предоставляет имеющийся сертификат ACP и другие отождествления (такие как сертификат IDevID), требуемые регистратором.

Сохранение имеющихся сведений о TA особенно важно при использовании механизмов повторного зачисления без аутентификации регистратора ACP (таких как ваучер в BRSKI) и внедрение отказов для сертификата может сделать плоскость ACP уязвимой для удалённых атак с возвратом узла ACP в состояние «утенка» (duckling). Где он принимает повторное зачисление в любой сети, к которой подключается. Поэтому **следует** поддерживать (просроченный) сертификат ACP и ACP TA и пытаться использовать их как возможное свидетельство для повторного зачисления, пока не получен новый ключевой материал.

При использовании BRSKI или иных протоколов и/или механизмов с поддержкой ваучеров, сохранение сведений о TA позволяет упростить повторное зачисление просроченных сертификатов ACP, особенно в средах где повторное получение ваучера в течение срока действия узла ACP может быть затратным или нежелательным по иной причине.

6.2.5.6. Сертификаты с отказом

Сертификат ACP считается отказавшим, если узел ACP, для которого выпущен сертификат, может определить, что сертификат отозван (или явно не обновлён) или (без явной локальной диагностики) узел ACP не может связаться с другими узлами того же домена ACP, используя этот сертификат ACP. Чтобы определённо связать отказ в соединении с сертификатом ACP, следует проверить принадлежность партнёра к домену (6.2.3. Проверка принадлежности к домену ACP), а диагностика соединения должна исключить другие причины отказа. Такие отказы могут возникать при создании или обновлении соединения по защищённому каналу ACP или ином применении сертификата ACP, например при соединении TLS с сервером EST для обновления сертификата домена ACP.

Примеры отказа сертификатов, которые узел ACP может обнаружить лишь по отказу в соединении, включают отзыв или завершение срока действия сертификата домена или любого из его сертификатов подписи, когда сам узел ACP не может обнаружить это напрямую. Сведения об отзыве или синхронизация часов могут быть доступны лишь через ACP, но узел ACP не может создать защищённый канал ACP, поскольку партнёры ACP отвергают сертификат домена узла.

Узлам ACP **следует** поддерживать возможность обнаружения отказов сертификата ACP и в этом случае переходить к роли кандидата на повторное зачисление в ACP, как описано в параграфе 6.2.5.5. Повторное зачисление.

6.3. Таблица смежности ACP

Чтобы знать, с какими узлами организовывать каналы ACP, каждый узел ACP поддерживает таблицу смежности. Эта таблица содержит сведения о смежных узлах ACP, включая, как минимум, Node-ID (идентификатор узла внутри ACP, см. параграфы 6.11.3 и 6.11.5), интерфейс, через который обнаружен сосед (от GRASP, как описано ниже), адрес IPv6 link-local соседа на данном интерфейсе и сертификат (включая acp-node-name). Узел ACP **должен** поддерживать эту таблицу смежности, которая служит для определения соседей, с которыми организовано соединение ACP.

Когда следующий узел ACP не является прямым соседом (нет канала к этому узлу), информация в таблице смежности **может** быть добавлена путём настройки, например, можно указать Node-ID и IP-адрес (см. 8.2. Соединение островков ACP через сети L3 без ACP (удалённые соседи).

Таблица смежности может содержать сведения о действительности и доверии к сертификату соседнего узла ACP. Однако последующие шаги всегда **должны** начинаться с проверки принадлежности к домену ACP для партнёра (см. 6.2.3. Проверка принадлежности к домену ACP). Таблица смежности содержит сведения о соседях ACP в целом, независимо от их домена и статуса доверия. Следующий шаг определяет узлы, с которыми следует организовать соединения ACP.

6.4. Обнаружение соседей с помощью DULL GRASP

Обнаружение незапрошенных локальных каналов (Discovery Unsolicited Link-Local или DULL) GRASP - это ограниченное подмножество GRASP для работы в области незащищённых локальных соединений. Формальное определение приведено в параграфе 2.5.2 [RFC8990]. В ACP применяется 1 экземпляр DULL GRASP для каждого интерфейса L2 на узле ACP для обнаружения кандидатов в соседи ACP, смежных на канальном уровне. Если не внесено изменений правилами, как отмечено выше (п. 2 в разделе 5), естественные интерфейсы (например, физические интерфейсы на физических узлах) **следует** автоматически инициализировать в состояние, где возможно автоматическое обнаружения ACP, и любые естественные интерфейсы с соседями ACP могут войти в ACP, даже если они в остальном не настроены. Приём пакетов на таких ненастроенных интерфейсах **должен** ограничиваться так, чтобы сначала работали лишь SLAAC (IPv6 Stateless Address Autoconfiguration [RFC4862]) и DULL GRASP, а затем - только последующая организация защищённых каналов ACP, но не иной ненужный трафик (например, нет других ответчиков транспортного стека IPv6 link-local).

Отметим, что использование группового адреса IPv6 link-local (ALL_GRASP_NEIGHBORS) предполагает необходимость использовать MLDv2 (см. Multicast Listener Discovery Version 2 (MLDv2) for IPv6 [RFC3810]) для анонсирования желания получать пакеты по этому адресу. Иначе DULL GRASP может работать некорректно в присутствии коммутаторов с отслеживанием MLD (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches [RFC4541]), которые не поддерживают или не ACP или ACP не включён на них, поскольку эти коммутаторы не будут пересылать пакеты DULL GRASP. Коммутаторы, не поддерживающие отслеживание MLD, должны работать как обычные мосты L2 для групповых пакетов IPv6, чтобы протокол DULL GRASP мог работать.

Обнаружение ACP **не следует** разрешать по умолчанию на интерфейсах, не являющихся естественными. В частности, его **недопустимо** запускать в ACP через виртуальные интерфейсы ACP. В параграфе 9.3 даны ненормативные предложения по управлению ACP на уровне интерфейса, в параграфе 8.2.2 - детали о туннелях, а в разделе 7 описано расширения ACP на устройствах, работающих (также) как мосты L2.

> Примечание. Если узел ACP реализует BRSKI для зачисления своего сертификата ACP (A.2. Начальная загрузка BRSKI (ANI)), приведённые выше соображения применимы и к обнаружению GRASP для BRSKI. Каждый экземпляр DULL GRASP для ACP тогда применяется для обнаружения посредников начальной загрузки по протоколу BRSKI, когда у узла нет сертификата домена. Обнаружение соседей ACP выполняется лишь при наличии у узла сертификата. Поэтому узлу никогда не требуется одновременно искать прокси начальной загрузки и соседа ACP.

Узел ACP анонсирует себя возможным партнёрам ACP с помощью цели AN_ACP. Эта цель синхронизации предназначена для лавинной рассылки по одному каналу в сообщении GRASP Flood Synchronization (M_FLOOD). В соответствии со структурой сообщения локатор с адресом IP link-local, номером протокола IP и порта будет распространяться вместе с целью лавинной рассылки. Неформальльный пример сообщения приведён на рисунке 6.

```
[M_FLOOD, 12340815, h'fe80000000000000c0011001feef0000', 210000,
  [["AN_ACP", 4, 1, "IKEv2" ],
   [O_IPv6_LOCATOR,
        h'fe80000000000000c0011001feef0000', IPPROTO_UDP, 15000]]
  [["AN_ACP", 4, 1, "DTLS" ],
   [O_IPv6_LOCATOR,
        h'fe80000000000000c0011001feef0000', IPPROTO_UDP, 17000]]
]
```

Рисунок 6. Пример цели GRASP AN_ACP.

Формальное определение CDDL представлено на рисунке 7.

```
flood-message = [M_FLOOD, session-id, initiator, ttl,
                 +[objective, (locator-option / [])]]

objective = ["AN_ACP", objective-flags, loop-count,
                                        objective-value]

objective-flags = sync-only ; как в [RFC8990]
sync-only =  4    ; M_FLOOD требует ограничить синхронизацию
loop-count = 1    ; операциями на локальном канале

objective-value = method-name / [ method, *extension ]
method = method-name / [ method-name, *method-param ]
method-name = "IKEv2" / "DTLS" / id
extension = any
method-param = any
id = text .regexp "[A-Za-z@_$]([-.]*[A-Za-z0-9@_$])*"
```

Рисунок 7. Определение GRASP AN_ACP.

Поле objective-flags указывает синхронизацию, loop-count имеет значение 1, поскольку это операция link-local.

В приведённом примере **рекомендуемый** период передачи цели составляет 60 секунд. Значение ttl = 210000 мсек указывает, что цель может кэшироваться узлами ACP даже при потере двух сообщений из трёх в процессе передачи.

Случайное значение session-id служит для предотвращения петель (отличает сообщение от его предшествующего экземпляра). В DULL это поле не имеет смысла, но указано в соответствии со спецификацией GRASP.

Отправитель **должен** указываться адресом IPv6 link-local на передающем интерфейсе узла ACP. Поле method-name в параметре objective-value является строкой, указывающей протокол, доступный на указанном или предполагаемом локаторе. Это протокол, поддерживаемый узлом для согласования защищённого канала. На рисунке 6 указан протокол IKEv2 для согласования защищённого канала IPsec.

Параметр method-param позволяет передавать зависящие от метода параметры. Эта спецификация не определяет method-param для IKEv2 или DTLS. Значения method-param для этих двух методов, непонятные узлу ACP **должны** игнорироваться им. Параметр extension позволяет задать независимые от метода параметры. Данная спецификация не задаёт расширений. Непонятные узлу ACP расширения **должны** игнорироваться им.

Параметр locator-option необязателен и требуется лишь в случаях, когда протокол защищённого канала не предложен на общеизвестном порту или такой порт не задан.

IKEv2 является фактическим протоколом для согласования соединений IPsec, поэтому GRASP указывает IKEv2, а не IPsec. Указание IPsec могло бы означать использование устаревшей верии IKE (v1) (The Internet Key Exchange (IKE) [RFC2409]). Для IKEv2 в IANA выделен порт 500, но на рисунке 6 кандидат в соседи ACP предлагает согласовать защищённый канал ACP через IKEv2 на порту 15000 (исключительно для демонстрации возможности указания в GRASP номера порта, не выделенного IANA). Для порта UDP в DTLS не задан принятый по умолчанию номер и порт всегда назначается узлом. Детали применения защищённых каналов DTLS приведены в параграфе 6.8.4.

При включении локатора это **должен** быть O_IPv6_LOCATOR и адрес IPv6 **должен** совпадать с адресом инициатора (это требования DULL для минимизации DoS-атак третьей стороны).

Заданные этим документом методы защиты каналов используют для objective-value значения IKEv2 и DTLS. Естественный IKEv2 и GRE-IKEv2 не различаются, поскольку согласование происходит исключительно по IKEv2. Узлу, поддерживающему более одного метода для защищённого канала, требуется лавинно рассылать несколько вариантов цели AN_ACP, чтобы каждый метод мог сопровождаться своей опцией locator-option. Для этого можно использовать 1 сообщение GRASP M_FLOOD, как показано на рисунке 6.

Основным назначением DULL GRASP является обнаружение адресов IPv6 link-local кандидатов в партнёры ACP в подсетях. Сигнализация о поддерживаемом варианте защищённого канала предназначена в основном для диагностики, но может потребоваться и для обнаружения, когда у протокола нет общеизвестного транспортного адреса, например, как в случае DTLS.

Отметим, что узел, являющийся одновременно узлом ACP и BRSKI Join Proxy может распространять цель AN_ACP и BRSKI в одном сообщении M_FLOOD, поскольку GRASP допускает в одном сообщении несколько целей. Это может быть непрактично, если операции ACP и BRSKI реализованы в разных программных модулях и/или ASA.

Результатом обнаружения является адрес IPv6 link-local у соседа, а также поддерживаемые им протоколы защищённого канала (и нестандартный порт протокола). Они сохраняются в таблице смежности ACP (6.2.3. Проверка принадлежности к домену ACP), которая затем управляет построением ACP с этим соседом.

Отметим, что в описанную цель DULL GRASP намеренно не включён сертификат ACP узла ACP, хотя это могло быть полезным для диагностики и упрощения защищённого обмена параметрами защиты в протоколах создания безопасного канала ACP (6.8. Протоколы защищённых связей (каналов)). Причина в том, что сообщения DULL GRASP передаются периодически по групповым адресам через подсети IPv6, а включение полного сертификата может приводить к фрагментации групповых пакетов IPv6 DULL GRASP из-за большого размера, что весьма нежелательно.

6.5. Выбор кандидатов в соседи ACP

Узел ACP определяет, с каким из других узлов в таблице смежности ACP ему следует пытаться организовать соединение ACP. Это происходит на основе сведений, хранящихся в таблице смежности ACP. ACP организуется исключительно между узлами одного домена, включая все субдомены маршрутизации. В приложении A.6 указано, чем отличаются соединения через такие субдомены.

Результатом процесса выбора соседей ACP служит список смежных или заданных в конфигурации автономных соседей, к которым следует организовать канал ACP, как описано ниже.

6.6. Выбор канала

Чтобы избежать атак, начальное обнаружение кандидатов в партнёры ACP не может включать согласование без защиты. Чтобы не изобретать велосипед, следующим шагом после определения адреса кандидата является организация защищённой связи с соседом на основе общеизвестного метода.

Из вариантов применения очевидно, что не все типы узлов ACP можно и нужно соединять напрямую и не каждый узел поддерживает все возможные механизмы. Например, устройства IoT с ограниченным размером кода могут поддерживать лишь DTLS, поскольку такой код уже применяется ими для сквозной защиты, а недорогие потолочные (in-ceiling) коммутаторы L2 могут поддерживать лишь MacSec (Media Access Control Security, 802.1AE [MACSEC]), поскольку это реализовано в их микросхемах. Только гибким шлюзам может потребоваться поддержка обоих этих механизмов, а может и других. Отметим, что поддержку MacSec не требует ни один из профилей ACP в этой спецификации и MacSec лишь упоминается как интересный протокол для защищённого канала. Отметим также, что модель защиты разрешает и требует проверку подлинности и полномочий в режиме «каждый с каждым» для всех узлов ACP, поскольку для защищённых каналов применяется не только поэтапная, но и сквозная аутентификация.

Для поддержки расширяемого выбора протоколов защищённых каналов без обязательного для реализации протокола (mandatory-to-implement или MTI) узел ACP **должен** пробовать все поддерживаемые им протоколы защищённого канала ACP, которые анонсированы кандидатом в соседи ACP через параметры GRASP AN_ACP (из называют возможными протоколами защищённого канала ACP).

Чтобы гарантировать предсказуемость выбора протокола и отсутствие блокировки, введены правила, указанные ниже.

- Узел ACP может инициировать разные возможные протоколы защиты канала ACP последовательно или параллельно в соответствии со своей политикой, но он **должен** выступать ответчиком для всех параллельно.
- После того как первое соединение защищённого канала ACP с конкретным адресом партнёра IPv6 пройдёт аутентификацию, оба партнёра знают сертификаты друг друга, поскольку эти сертификаты ACP применяются всеми протоколами защиты канала для взаимной аутентификации. Партнёр с большим Node-ID в AcpNodeName его сертификата ACP принимает роль решающего (Decider), а другой - роль последующего (Follower). Решающий узел выбирает применяемый для защиты канала протокол.
- Последователь (Follower) становится пассивным и не пытается в дальнейшем инициировать соединения протокола защиты канала ACP с Decider и не считает ошибкой закрытие защитного канала решающим узлом. Decider становится активной стороной, продолжая организацию защищённого канала с последователем. Процесс завершается, когда Decider достигает «лучшего» (с его точки зрения) варианта организации защищённого канала ACP с Follower.
- Партнёр с acp-address = 0 в своём AcpNodeName принимает роль Follower при взаимодействии с узлом, где acp-address отличен от 0 (отметим, что эта спецификация на задаёт полностью поведение при согласовании защищённого канала ACP для узлов с 0 в поле адреса ACP, задавая совместимость с такими узлами ACP).

В простом примере партнёр ACP Node 1 пытается создать соединение IPsec через IKEv2 с Node 2. Аутентификация IKEv2 завершается успешно. Node 1 имеет меньший адрес ACP и становится Follower, а Node 2 - Decider. IKEv2 может не быть предпочтительным протоколом защитного канала ACP для Node 2 (Decider) и тот продолжит попытки создания защищённого канала с более предпочтительным протоколом (например, DTLS/UDP). Если предпочтительное соединение ACP с Decider успешно, соединение IPsec закрывается. Если у Node 2 нет предпочтения перед IPsec или другие попытки соединения с Node 1 не удаются, Node 2 сохранит соединение IPsec и будет использовать его. Решающему узлу **не следует** передавать реальные пакеты данных через защищённый канал, пока он не решил его применять. Последователь **может** задержать привязку защищённого канала ACP к виртуальному интерфейсу ACP, пока не увидит первый пакет данных от Decider (но не более 5 секунд), чтобы избежать ненужной привязки защищённого канала, который будут вскоре разорван решающим узлом. Ниже последовательность этапов в примере показана более подробно и каждый этап помечен в форме [<номер>{:<соединение>}], чтобы легче было понять, к какому из двух соединений относится этап - инициированному узлом Node 1 или узлом Node 2.

[1] Node 1 передаёт сообщение GRASP AN_ACP, анонсируя себя.

[2] Node 2 передаёт сообщение GRASP AN_ACP, анонсируя себя.

[3] Node 2 получает [1] от Node 1.

[4:C1] В результате [3] Node 2 инициирует защищённый канал к Node 1 со своим предпочтительным протоколом. Соединение C1.

[5] Node 1 получает [2] от Node 2.

[6:C2] В результате [5] Node 1 инициирует защищённый канал к Node 2 со своим предпочтением. Соединение C2.

[7:C1] Node 1 и Node 2 аутентифицируют сертификаты друг друга в C1 как действительных партнёров ACP.

[8:C1] В сертификате Node 1 значение ACP Node-ID меньше, чем у Node 2, поэтому Node 1 считает себя последователем (Follower), а Node 2 - решающим (Decider) в соединении C1. Соединение C1 завершено.

[9] Node 1 не предпринимает других попыток соединения с Node 2 (Decider), известным из [2], поскольку он знает из [8:C1] о своей роли последователя.

[10:C2] Node 1 и Node 2 аутентифицируют сертификаты друг друга в соединении C2 (как в [7:C1]).

[11:C2] В сертификате Node 1 значение ACP Node-ID меньше, чем у Node 2, поэтому Node 1 считает себя последователем (Follower), а Node 2 - решающим (Decider) в соединении C2, но C2 и C1 относятся к одной паре узлов и это уже не имеет значения, поскольку роли Decider и Follower уже распределены [8:C1].

[12:C2] Node 2 (Decider) закрывает C1, Node 1 принимает это, поскольку является последователем (из [8:C1]).

[13] Node 2 (Decider) и Node 1 (Follower) начинают обмен данными через соединение C2, которое становится защищённым каналом для ACP.

Все эти согласования происходят в контексте интерфейса L2. Decider и Follower создают соединения ACP между собой на каждом интерфейсе L2 между ними. Автономному узлу **недопустимо** предполагать, что сосед с тем же адресом L2 или IPv6 link-local на другом интерфейсе L2 является тем же узлом. Это можно определить лишь после проверки сертификата вслед за успешной попыткой организации защищённого соединения.

Решающему узлу **не следует** подавлять попытки организации конкретного соединения по защищённому каналу ACP на интерфейсе L2 на основании отказа для этого типа защищённого канала ACP с партнёром с тем же сертификатом ACP через другой интерфейс L2 interface. Различаться могут не только поддерживаемые типы защищённого канала ACP на разных интерфейсах L2 одного узла ACP, но и условия ошибок для разных интерфейсов L2. Отказ от такой «оптимизации» попыток соединения может повысить отказоустойчивость при наличии ошибок.

6.7. Проверка кандидата в соседи ACP

Независимо от выбранного протокола защищённого канала подлинность кандидатов в соседи ACP требуется проверять по сертификату домена. Это означает, что любой протокол защищённого канала **должен** поддерживать аутентификацию по сертификатам, которая позволяет проверить принадлежность к домену ACP, как указано в параграфе 6.2.3. При отказе попытка соединения прерывается и записывается ошибка. Повторные попытки **должны** дросселироваться. По умолчанию **рекомендуется** двухкратное увеличения интервала с начальным значением (initial retransmission time или IRT) 10 секунд и максимальным (maximum retransmission time или MRT) - 640 секунд.

Отказу при аутентификации соседа ACP в роли ответчика протокола аутентификации защиты **недопустимо** влиять на попытки узла ACP организовать соединение в роли инициатора. Это правило предназначено для повышения отказоустойчивости при создании защищённого канала. В параграфе 6.6 описано, как обрабатываются конфликты при одновременных попытках создать защищённый канал.

6.8. Протоколы защищённых связей (каналов)

В этом параграфе описано, как узлы ACP организуют защищённые соединения для данных с автоматически найденными или настроенными партнёрами ACP. В параграфе 6.4 описано автоматическое обнаружение соседей в подсети IPv6, а в параграфе 8.2 - настройка партнёров, которые не являются соседями в подсети IPv6.

В параграфе 6.13.5.2 описано сопоставление защищённых каналов с виртуальными интерфейсами подсети IPv6 в ACP. Простым примером является отображение каждого защищённого канала ACP на свой виртуальный интерфейс ACP «точка-точка» (6.13.5.2.1. Виртуальные интерфейсы ACP "точка-точка"). Когда в одной подсети имеется несколько партнёров ACP, это ведёт к созданию множества виртуальных интерфейсов ACP «точка-точка» в базовую сеть IPv6. Это можно оптимизировать с помощью «множественных» виртуальных интерфейсов ACP (6.13.5.2.2. Виртуальные интерфейсы ACP с множественным доступом), но сложность оптимизации может превысить преимущества.

6.8.1. Общие соображения

За счёт выбора каналов (6.6. Выбор канала) ACP может поддерживать расширяемый набор протоколов защищённой связи, не требующий поддержки одного MTI в масштабе сети. Узлам ACP необходимо реализовать протоколы, нужные лишь для взаимодействия с кандидатами в партнёры, а не со всеми узлами домена ACP. Примеры приведены в параграфе 6.8.5. Профили защищённых каналов ACP.

Уровень защиты на каждом этапе (hop) сети ACP должен быть согласованным для всей сети, чтобы не возникало «слабых звеньев», которые могут стать объектами атак. При взломе защищённого канала на одном соединении он может использоваться для передачи и/или получения пакетов всей сети ACP. Поэтому, несмотря на возможность применять разные протоколы защиты, их минимальный уровень безопасности должен быть сопоставимым.

Протоколы защищённых каналов не обязаны поддерживать произвольную связность сетевого уровня (L3) между партнёрами, но могут пользоваться тем, что стандартным вариантом для защищённых каналов ACP служит смежность L2. Поэтому зависящие от L2 механизмы могут быть приспособлены в качестве протоколов защищённых каналов.

Механизмы L2, такие как радио-технологии со строгим шифрованием или [MACSEC], могут предоставлять эквивалентное шифрование, а протокол защищённой связи ACP может требоваться лишь для проверки принадлежности к домену ACP партнёров и/или устройств и/или вывода ключа из механизма L2. Механизмы, использующие лишь такую базовую защиту L2 для автоматического обнаружения и связи с партнёрами ACP, возможны и желательны для предотвращения дублирования шифрования, но они не заданы этим документом.

Надёжная физическая защита каналов может устанавливаться тем, где недоступна криптографическая защита. Поскольку не существует защищённого механизма автоматического обнаружения строгой физической защиты между парой узлов, такую защиту можно применять лишь при явной настройке в конфигурации и такая конфигурация может стать направлением атаки. Поэтому документ указывает для ACP (параграф 8.1) лишь явно настраиваемый механизм без какого-либо протокола защищённого канала для случаев, когда соединение и подключённые к нему узлы имеют надёжную физическую защиту.

6.8.2. Общие требования

Аутентификация партнёров в протоколе защищённой связи **должна** использовать сертификат ACP, как указано в параграфе 6.2.3. Поскольку автообнаружение кандидатов в партнёры ACP через GRASP (6.4. Обнаружение соседей с помощью DULL GRASP), заданное в этом документе, не применяет сертификат ACP соседа, а узлы ACP могут (ещё) не иметь другой связности с сетью для извлечения сертификата, протокол защищённой связи **должен** применять механизм прямой передачи сертификата, не полагаясь на указанный механизм, такой как передача для сертификата лишь хэш-значения и/или URL.

Протокол защищённой связи **должен** использовать Forward Secrecy (внутренне или как часть профила протокола защищённой связи).

Поскольку данные (payload) ACP от унаследованных протоколов внутри ACP и рассылаемые лавинно сведения ACP GRASP не шифруются, протоколу защищённого канала ACP нужна конфиденциальность. Симметричное шифрование данных защищённого канала **должно** применять схемы, считающиеся надёжными с защитой не хуже, чем при ключах размером 256 битов, такие как AES-256. Поддержка NULL-шифрования **недопустима**.

Протоколы защищённых связей обычно сигнализируют лишь о сертификате конечного элемента (например, сертификате ACP) и всех возможных промежуточных CA для выполнения взаимной проверки подлинности. Привязки доверия (TA) должны быть известны обеим сторонам и пользоваться доверием, поэтому их сертификаты не требуются для взаимной аутентификации. Тем не менее, для использования при организации защищённого канала ACP **следует** предоставлять возможность включения сертификата TA в сигнализацию для облегчения поиска неполадок (см. 9.1. Диагностика ACP и BRSKI). Включение сертификатов TA может быть неприемлемо в системах, полагающихся на модели защиты, где содержимое сертификатов TA считается конфиденциальным и приемлема лишь передача хэша содержимого. Узлам ACP **следует** иметь механизм выбора условий передачи сертификата TA в предположении её возможности для конкретного протокола защищённого канала.

Защищённый канал ACP **должен** немедленно разрываться при завершении срока действия или отзыве любого из сертификатов в цепочке аутентификации соседа. Это может быть нестандартным поведением для протокола защищённого канала, поскольку аутентификация сертификатов может влиять в протоколе лишь на организацию защищённого канала и не может повторно проверяться в течение срока действия защищённого соединения при отсутствии этого требования.

При указании дополнительного протокола защищённой связи для защищённых каналов ACP, помимо указанных в этом документе, всех опций протокола, не требуемых для поддержки устройств, которые предполагаются способными поддерживать ACP, **следует** избегать, чтобы не возникало лишних сложностей при реализации. Например, определения протоколов защиты часто включают устаревшие и/или внутренние опции защиты, которые нужны лишь для совместимости с имеющимися устройствами, которые невозможно обновить до предпочитаемых в данное время опций защиты. Такие устаревшие и/или внутренние опции не требуется поддерживать, когда протокол защищённой связи впервые задаётся для ACP. Это укрепляет «слабое звено» и упрощает реализацию ACP.

6.8.3. ACP по протоколу IPsec

Узел ACP анонсирует свою способность поддерживать IPsec с согласованием через IKEv2 в качестве защищённого канала ACP, используя objective-value = IKEv2 в цели GRASP AN_ACP.

Применение IPsec и IKEv2 в ACP предписывает профиль с небольшим набором опций из текущих стандартов (Standards Track) применения IPsec (Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH) [RFC8221]) и IKEv2 (Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2) [RFC8247]). Эти опции обеспечивают строгие свойства защиты и могут исключать устаревшие и отменённые алгоритмы, поскольку не требуется совместимость с унаследованным оборудованием для защищённых каналов ACP. Любая совместимость с устаревшими версиями расширила бы фронт атак и усложнила реализацию, не обеспечивая преимуществ.

6.8.3.1. Естественная защита IPsec

Узел ACP с естественной поддержкой IPsec **должен** применять IPsec в туннельном режиме с согласованием через IKEv2 и данными (payload) IPv6 (например, ESP Next Header 41). Для инкапсуляции **должны** применяться свой и партнерский адреса IPv6 link-local. Заданные вручную ключи **недопустимы** (см. 6.2. Домен, сертификат и сеть ACP). Селекторы трафика (TS) имеют вид

```
TSi = (0, 0-65535, :: - FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF)
TSr = (0, 0-65535, :: - FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF)
```

Туннельный режим IPsec требуется потому, что ACP будет маршрутизировать и/или пересылать по защищённым каналам ACP пакеты, полученные от любого другого узла ACP, а не только свои пакеты. В транспортном режиме IPsec (без дополнительной инкапсуляции заголовка в данные ESP) возможно лишь передавать пакеты, созданные самим узлом ACP, поскольку адреса IPv6 в ESP должны совпадать с адресами во внешнем заголовке IPv6.

6.8.3.1.1. RFC 8221 (IPsec/ESP)

Реализации ACP IPsec **должны** соответствовать [RFC8221] и обновляющим его документам. Приведённые в этом параграфе и выше требования изменяют и переопределяют требования указанного документа.

Заголовок аутентификации IP (Authentication Header или AH) применять **недопустимо** (не обеспечивается конфиденциальность).

Для требуемых алгоритмов шифрования ESP из раздела 5 в [RFC8221] заданы дополнительные рекомендации:

- ENCR_NULL AH применять **недопустимо** (не обеспечивается конфиденциальность);
- ENCR_AES_GCM_16 является единственным MTI для шифрования ESP в ACP через IPsec/ESP (уже указан как **обязательный** в [RFC8221]);
- **можно** поддерживать ENCR_AES_CBC с AUTH_HMAC_SHA2_256_128 (как алгоритм шифрования ESP) и ENCR_AES_CCM_8, если какой-то алгоритм превосходит ENCR_AES_GCM_16 по производительности, его **следует** поддерживать;
- ENCR_CHACHA20_POLY1305 **следует** поддерживать с производительностью не ниже ENCR_AES_GCM_16, **можно** поддерживать алгоритм и при более низкой производительности.

IKEv2 указывает порядок предлагаемых алгоритмов. Алгоритмы **следует** упорядочивать по производительности. Выбирается первый алгоритм, указанные обеими сторонами.

- Не задаются требования к взаимодействию с унаследованным оборудованием в защищённых каналах ACP, поэтому достаточно одного алгоритма MTI для IPsec в защищённых каналах ACP, чтобы обеспечить совместимость и применять самые лёгкие реализации.
- ENCR_AES_GCM_16 является режимом аутентифицированного шифрования со связанными данными (Authenticated Encryption with Associated Data или AEAD), поэтому не требуется дополнительный алгоритм аутентификации ESP, что упрощает требования к MTI для ACP с IPsec.

- Не задаётся требований к MTI для поддержки ENCR_AES_CBC, поскольку предполагается, что алгоритм ENCR_AES_GCM_16 реализуем в системах с аппаратным ускорением с меньшими затратами и/или большей производительностью, нежели ENCR-AES_CBC.

- Алгоритм ENCR_CHACHA20_POLY1305 обязателен в [RFC8221], поскольку его целевым применением является резервирование (откат) при обнаружении слабых мест в AES. К сожалению, в настоящее время нет способа автоматически распространить через ACP правило для запрета использования алгоритмов на базе AES, поэтому данное преимущество ENCR_CHACHA20_POLY1305 ещё не может быть полностью реализовано в ACP. В результате алгоритм остаётся лишь рекомендуемым. Замена AES на этот алгоритм с возможным падением производительности может сделать ACP неработоспособной. Поэтому к данному алгоритму предъявляется требование производительности, чтобы он стал эффективным резервом защиты для AES в ACP, как только политика перехода на него или предпочтение станет доступным в среде ACP.

[RFC8221] разрешает ключи размером 128 или 256 битов для AES. Этот документ указывает, что **должны** поддерживаться лишь 256-битовые ключи AES.

При обновлении [RFC8221] реализации ACP должны будут решить вопрос совместимости с устаревшими системами.

6.8.3.1.2. RFC 8247 (IKEv2)

В [RFC8247] даны базовые рекомендации по обязательным для реализации (MTI) шифрам, проверке целостности, псевдослучайным функциям и механизмам Diffie-Hellman. Эти рекомендации и рекомендации последующих документов применимы и к ACP. Поскольку IKEv2 на защищённых каналах ACP достаточно реализовать в программах плоскости управления, а не специализированных микросхемах (Application-Specific Integrated Circuit или ASIC), а на узлах ACP с поддержкой IKEv2 не предполагается ограничений пространства кода и в имеющихся реализациях IKEv2 предполагается поддержка рекомендаций [RFC8247], этот документ не пытается упростить рекомендации для ACP.

В [IKEV2IANA] приведены имена параметров IANA IKEv2, используемые в тексте.

Узлы ACP, поддерживающие IKEv2, **должны** соответствовать [RFC8247] с изменениями, представляющими заявление политики, разрешённое [RFC8247].

Для сигнализации цепочки сертификатов ACP (включая TA), как требует параграф 6.8.2, можно применять в IKEv2 содержимое X.509 Certificate - Signature. Это обязательно в соответствии с параграфом 3.6 в [RFC7296].

Узлам ACP **следует** настроить IKEv2 для использования лишь сертификата ACP и TA при работе в качестве ответчика IKEv2 с адресом IPv6 link-local и номером порта, указанным в анонсах DULL GRASP AN_ACP (см. параграф 6.4).

При получении от партнёра CERTREQ без указания какого-либо из сертификатов TA этого узла ACP, узлу ACP **следует** игнорировать CERTREQ и продолжить передачу своей цепочки сертификатов, включающей его TA, в соответствии с параграфом 6.8.2. Это не приведёт к успеху взаимной аутентификации, но поможет в диагностике.

Отметим, что с IKEv2 отказ при аутентификации приведёт лишь к тому, что ответчик получит цепочку сертификатов от инициатора, но не наоборот. Поскольку организация защищённого канала симметрична (см. параграф 6.7), каждый невредоносный сосед ACP будет пытаться подключиться как инициатор, что позволит ему получить диагностические сведения о сертификате соседа.

В IKEv2 узлы ACP идентифицируются по их адресам ACP. **Должны** применяться идентификационные данные IKEv2 ID_IPv6_ADDR, которые **должны** содержать адрес ACP. Если партнерский сертификат ACP включает адрес ACP 32HEXDIG в acp-node-name (не 0), адрес в идентификационных данных IKEv2 **должен** совпадать с ним. В параграфе 6.2.3 приведены дополнительные сведения для случая отсутствия адреса ACP или значения в acp-node-name.

При аутентификации IKEv2 **должен** применяться метод 14 (Digital Signature) для сертификатов ACP, этот метод может использоваться с сертификатами RSA и ECDSA указанными объектом ASN.1 AlgorithmIdentifier.

Для Digital Signature **должен** поддерживаться хэш SHA2-512 в дополнение к SHA2-256.

Должен поддерживаться обмен ключами IKEv2 Diffie-Hellman группы 19 (256-битовое случайное значение ECP). Причина этого заключается в том, что ECC обеспечивает уровень безопасности, аналогичный обмену ключами с конечным полем (модульное возведение в степень - MODP), при более коротком ключе, поэтому предпочтительней при отсутствии иных соображений.

6.8.3.2. IPsec с инкапсуляцией GRE

В сетевых устройствах высокопроизводительные виртуальные интерфейсы чаще реализуются на основе инкапсуляции GRE, нежели «естественных» ассоциаций IPsec (без какой-либо инкапсуляции, заданной IPsec). Для таких устройств организация защищённых каналов ACP на основе GRE с защитой IPsec.

Требования для ESP/IPsec/IKEv2 с GRE такие же, как для IPsec (6.8.3.1. Естественная защита IPsec) за исключением согласования транспортного режима и следующего протокола GRE (47). GRE позволяет избежать туннельного режима. Селекторы трафика имеют вид

```
TSi = (47, 0-65535, Initiator-IPv6-LL-addr ... Initiator-IPv6-LL-addr)
TSr = (47, 0-65535, Responder-IPv6-LL-addr ... Responder-IPv6-LL-addr)
```

Если инициатор и ответчик поддерживают IPsec на основе GRE, это будет предпочтительней естественного режима IPsec, поскольку IKEv2 согласует транспортный режим (как задано профилем IPsec на базе GRE) в отличие от туннельного при естественном IPsec (см. параграф 1.3.1 в [RFC7296]). Трафик IPv6 ACP передаётся через GRE в соответствии с IPv6 Support for Generic Routing Encapsulation (GRE) [RFC7676].

6.8.4. ACP по протоколу DTLS

Этот документ определяет использование ACP через DTLS в предположении, что это, вероятно, первое транспортное шифрование, поддерживаемое некоторыми классами устройств с ограничениями - DTLS обычно применяется в таких устройствах, а IPsec - нет. Пространство кода в таких устройствах может быть ограничено, чтобы поддерживать требования сверх минимальных.

Узел ACP анонсирует свою способность поддерживать DTLS версии 1.2 (Datagram Transport Layer Security Version 1.2 [RFC6347]), совместимую с требованиями этого документа, как протокол защищённого канала ACP в GRASP с помощью objective-value = DTLS в цели AN_ACP (6.4. Обнаружение соседей с помощью DULL GRASP).

Для работы ACP через UDP и DTLS применяется локально заданный порт UDP, анонсируемый кандидату в партнёры как параметр цели GRASP AN_ACP. Этот порт может быть связан с любой новой версией DTLS, если она может согласовать соединение DTLS 1.2 при наличии партнёра, поддерживающего лишь DTLS 1.2.

Все узлы ACP, поддерживающие DTLS как протокол защищённого канала, **должны** следовать рекомендациям по реализации DTLS и соображениям безопасности из BCP 195 [RFC7525], за исключением версии DTLS. Узлы ACP, поддерживающие DTLS, **должны** поддерживать DTLS 1.2 и **недопустима** поддержка более старых версий DTLS.

В отличие от IPsec, не предпринимается попыток упростить требования BCP 195 [RFC7525], поскольку предполагается, что DTLS будет использовать лишь программные реализации, где повторное использование широко распространённых реализаций важнее возможности минимизировать сложности реализаций с аппаратным ускорением, важной для IPsec.

DTLS 1.3 [TLS-DTLS13] совместима с DTLS 1.2 (см. раздел 1 в [TLS-DTLS13]). Реализация DTLS, поддерживающая DTLS 1.2 и DTLS 1.3 соответствует приведённым выше требованиям согласования DTLS 1.2 при наличии партнёра, поддерживающего лишь DTLS 1.2, но использует DTLS 1.3, когда оба партнёра поддерживают эту версию.

Версия 1.2 является MTI для DTLS в этой спецификации по указанным ниже причинам.

- Имеется обширный опыт применения DTLS 1.2 на широком спектре целевых устройств ACP.
- Микрокод мелких встраиваемых устройств ACP может долгое время не поддерживать новую версию.
- В DTLS 1.3 внесены существенные изменения, такие как иной уровень записи, требующий времени на реализацию и развёртывание, особенно на устройствах низкого уровня с ограниченным пространством кода.
- Обновление имеющегося BCP [RFC7525] для DTLS 1.2 может занять столько же времени, как обретение опыта для более новых версий DTLS.
- Нет существенных преимуществ DTLS 1.3 над DTLS 1.2, важных в контексте опций ACP для DTLS. Например, повышение производительности сигнализации при организации сессии в DTLS 1.3 не важно для ACP с учётом длительного срока работы защищённых каналов ACP и того, что соединения DTLS организуются в основном на локальном канале (малое значение RTT).

Тем не менее, новые версии DTLS, такие как DTLS 1.3, предъявляют более строгие требования к защите, а стандарты IETF обычно требуют применять последнюю версию стандартных протоколов. Поэтому рекомендуется поддерживать в реализациях ACP все более новые версии DTLS, которые все ещё могут согласовываться в DTLS 1.2.

Помимо этой простой настройки DTLS, не требуется дополнительной настройки сессии или иной защитной ассоциации. Как только сессия DTLS заработает, партнёры ACP смогут обмениваться пакетами IPv6 ACP в качестве содержимого транспортного соединения DTLS. Любые заданные DTLS механизмы ассоциаций защиты, такие как смена ключей, применяются как и в других приложениях, полагающихся только на DTLS.

6.8.5. Профили защищённых каналов ACP

Как отмечено в начале параграфа 6.6, не т единого механизма защиты каналов, заданного для всех узлов ACP. Вместо этого данный параграф определяет два профиля ACP - базовый (baseline) и ограниченный (constrained) для узлов ACP которые вносят такие требования.

Узел ACP с поддержкой базового профиля должен естественным путём поддерживать IPsec и может поддерживать IPsec через GRE. Узел ACP с поддержкой ограниченного профиля, не способный поддерживать IPsec, должен поддерживать DTLS. Узел ACP, соединяющий область узлов с ограничениями с областью узлов ACP с базовым профилем, должен поддерживать IPsec и DTLS (оба профиля).

Пояснение. Не все типы узлов ACP могут или требуют создавать прямые соединения с каждым другим, а также не способны поддерживать или предпочитать все возможные механизмы защиты каналов. Например, устройства IoT с ограниченным пространством кода могут поддерживать только DTLS, поскольку этот код уже имеется на них для сквозной защиты, а высокопроизводительные маршрутизаторы ядра могут не захотеть поддерживать DTLS, поскольку возможно исполнение IPsec в аппаратных ускорителях, но им потребуется поддерживать DTLS на путях пересылки со слабыми CPU, используемых в критически важных операциях плоскости управления. Не возникает проблемы развёртывания одной плоскости ACP через такие узлы, поскольку имеются также подходящие шлюзы ACP с достаточной поддержкой множества механизмов защиты каналов, чтобы соединяться с областями узлов ACP с более ограниченным набором протоколов защиты канала. На границе между областями IoT и высокопроизводительными сетями ядра маршрутизаторы общего назначения в качестве шлюзов, способные поддерживать множество протоколов защиты канала, уже стали нормой.

Естественный режим IPsec с туннелями обеспечивает наименьшие затраты на инкапсуляцию. GRE может быть предпочтительней для унаследованных реализаций, поскольку в прошлом виртуальные интерфейсы, требуемые для ACP в сочетании с защищёнными каналами, чаще реализовались с помощью GRE, нежели естественного IPsec.

Узлам ACP требуется указывать набор поддерживаемых механизмов защиты ACP в документации, а также следует объявлять поддерживаемые в соответствии с приведёнными выше требованиями профили.

6.9. GRASP в ACP

6.9.1. GRASP как базовый сервис ACP

В ACP **должен** запускаться внутренний экземпляр GRASP, являющийся ключевой частью услуг ACP. Фундаментальной функцией GRASP для ACP является способность обнаруживать сервис в масштабе ACP (используя цели в GRASP).

ACP обеспечивает индивидуальную маршрутизацию IP на основе протокола RPL (6.12. Маршрутизация в ACP).

В ACP не применяется групповая маршрутизация IP и не предоставляются базовые групповые услуги IP (обработка групповых сообщений GRASP link-local описана в параграфе 6.9.2). Вместо этого ACP обеспечивает обнаружение служб со помощью механизмов обнаружения, анонсирования и согласования цели в экземпляре ACP GRASP (службы являются формой цели). Эти механизмы используют поэтапную (hop-by-hop) надёжную лавинную рассылку сообщений GRASP M_DISCOVERY для обнаружения и M_FLOOD - для анонсирования услуг. Более подробно это описано в Приложении A.5. Распространение информации ACP и групповая передача.

6.9.2. ACP как защищённая транспортная подложка для GRASP

В терминологии GRASP [RFC8990] ACP является подложкой защиты и транспорта для экземпляра GRASP, запущенного внутри ACP (ACP GRASP). Это значит, что ACP отвечает за то, что этот экземпляр GRASP передаёт сообщения только через виртуальные интерфейсы ACP GRASP. При каждом добавлении или удалении такого интерфейса ACP в результате создания или закрытия защищённого канала ACP это нужно указать запущенному в ACP экземпляру GRASP. ACP может работать даже при отсутствии активных соседей ACP. Плоскость ACP создаётся при наличии у узла сертификата домена и продолжает существовать, даже когда соседи перестают работать. В таких случаях агенты ASA, использующие экземпляр GRASP на том же узле, по-прежнему должны иметь возможность обнаруживать цели друг друга. Когда ACP не существует, агенты ASA, использующие экземпляр ACP GRASP через API, **должны** продолжать работу и **должны** быть способны понимать, что ACP нет и, следовательно, экземпляр ACP GRASP не может работать.

Работа ACP в качестве подложки защиты и транспорта для GRASP показана на рисунке 8.

Индивидуальные сообщения GRASP внутри ACP всегда используют адрес ACP. Адреса link-local из ACP VRF **недопустимо** применять внутри целей. Индивидуальные сообщения GRASP внутри ACP доставляются через TLS, требования описаны в параграфе 6.1. Требования к использованию TLS. При взаимной аутентификации TLS должна выполняться проверка принадлежности к домену ACP, описанная в параграфе 6.2.3.

Групповые сообщения GRASP link-local нацелены на конкретные виртуальные интерфейсы ACP (6.13.5. Интерфейсы ACP), но ACP передаёт их на виртуальные интерфейсы ACP GRASP, основанные на соединениях TCP с адресами соседей IPv6 link-local через базовый виртуальный интерфейс ACP. Если у виртуального интерфейса ACP GRASP есть не меньше 2 соседей, групповые сообщения GRASP link-local реплицируются во все соединения TCP с соседями.

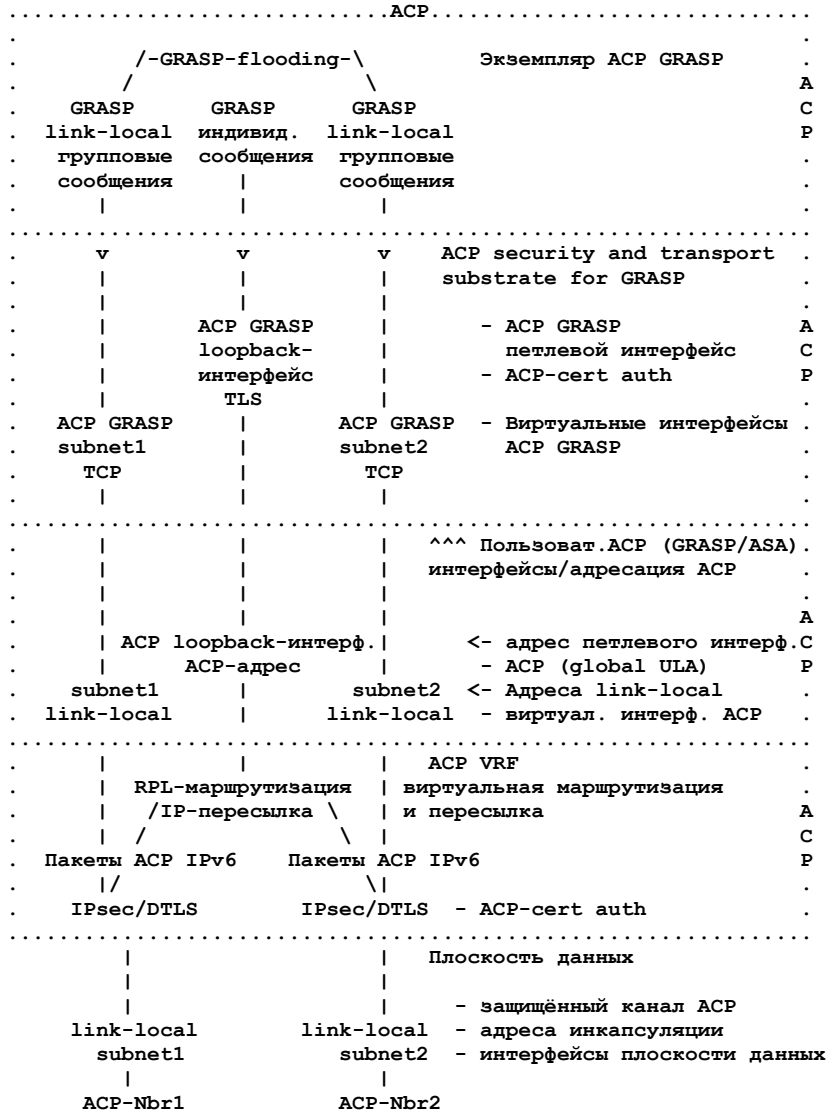

Рисунок 8. ACP как подложка защиты и транспорта для GRASP.

Соединения TCP и TLS для GRASP в ACP используют выделенный IANA порт TCP для GRASP (7017). По сути, предполагается применение транспортного стека TLS для соединений с адресами ACP (например, глобальные адреса) и TCP для соединений с адресами link-local на виртуальных интерфейсах ACP. Последние применяются лишь для лавинной рассылки сообщений GRASP.

6.9.2.1. Обсуждение

Инкапсуляция TCP для сообщений GRASP M_DISCOVERY и M_FLOOD на локальном канале применяется из-за того, что эти сообщения рассылаются в лавинном режиме возможно через несколько интервалов (hop) всем узлам ACP, а один канал даже с временными потерями (например, Wi-Fi или Powerline) может снизить вероятность передачи без потерь так, что приложения захотят повысить частоту отправки этих сообщений. Такое сокращение периода отправки дейтаграмм увеличит трафик и издержки на обработку в ACP по сравнению с надёжным поэтапным (hop-by-hop) повтором передачи, обеспечиваемым TCP без возникновения дубликатов GRASP.

Протокол TLS требуется для нелокальной индивидуальной передачи GRASP, поскольку обязательные аутентификация и шифрование с защищённых каналах ACP защищают лишь от внешних атак, скомпрометированные члены ACP, которые (ещё) не обнаружены и не удалены (например, через отзыв или завершение срока действия сертификата) могут быть опасны. Если бы партнерские соединения GRASP применяли лишь TCP, скомпрометированные члены ACP могли бы пассивно прослушивать соединения, проходящие через них (MITM[1]), или перехватывать и изменять сообщения. TLS не позволяет полностью исключить проблемы, связанные со скомпрометированными членами ACP, но существенно осложняет такие атаки.

Прослушивание и/или подмена скомпрометированным узлом ACP по-прежнему возможны, поскольку в модели ACP и GRASP поставщик и потребитель цели изначально не имеют уникальных сведений (таких, как отождествление) о другой стороне, которые позволили бы различить скомпрометрированных партнёров. Скомпрометированный узел ACP может просто анонсировать цель, фильтровать исходную цель GRASP при участии в MITM-атаке и действовать как посредник прикладного уровня. Это требует от скомпрометированного узла ACP понимания семантики согласования GRASP для выступления в роли посредника без обнаружения, но в среде ACP такая семантика может быть открыта и даже стандартизована.

Соединения GRASP TLS работают также, как любая передача трафика ACP через защищённые каналы ACP. Это ведёт к двойной аутентификации и шифрованию, обеспечивая перечисленные ниже преимущества.

- Методы защиты канала, такие как IPsec, могут обеспечивать дополнительную защиту от атак (например, атак со сбросом).
- Метод защиты канала может применять аппаратное ускорение, но выигрыш от этого невелик.
- Модель защиты для ACP GRASP не отличается от защиты другого трафика ACP, просто применяется ещё один уровень защиты от внутренних атак, который важен с учётом роли GRASP в ACP.

6.10. Разделение контекста

Контекст ACP отделен от обычной плоскости данных на узле и включает для каналов ACP пересылку и маршрутизацию IPv6, а также все требуемые функции верхних уровней ACP.

В классических сетевых системах VRF является одним из логических вариантов реализации ACP. Если это разрешено программной архитектурой системы, логический контейнер или экземпляр виртуальной машины будет предпочтительным для разделения контекста, минимизируя общие компоненты. Контекст для ACP требуется создавать автоматически при начальной загрузке узла. По возможности, его следует защитить от непреднамеренного изменения при настройке конфигурации (плоскости данных).

Разделение контекста повышает уровень защиты, поскольку плоскость ACP недоступна из таблиц маршрутизации и пересылки плоскости данных. Ошибки настройки плоскости данных не будут влиять на ACP.

6.11. Адресация внутри ACP

Описанные выше каналы обычно связывают лишь два соседних узла, а для взаимодействия через несколько узлов (hop) в ACP нужна действительная адресация и маршрутизация в масштабе сети. Каждый узел ACP создаёт петлевой (loopback) интерфейс с уникальным в масштабе сети ACP адресом (префиксом) в контексте ACP (6.10. Разделение контекста). Этот адрес можно применять и в другом виртуальном контексте.

С представленным здесь алгоритмом все узлы в одном субдомене маршрутизации имеют один префикс ULA /48. И наоборот, ULA Global ID из разных доменов вряд ли будут конфликтовать, так что две сети ACP можно объединить, если политика разрешает это. Вопросы слияния доменов рассмотрены в параграфе 10.1. Свойства самовосстановления.

Каналы внутри ACP применяют лишь адреса IPv6 link-local, поэтому каждому узлу ACP нужен лишь один маршрутизируемый адресный префикс.

6.11.1. Фундаментальные концепции автономной адресации

- Использование. Автономные адреса служат исключительно для функций самоуправления внутри домена доверия и не применяются для пользовательского трафика. Взаимодействие с объектами вне домена доверия происходит в другом пространстве адресов, например, по обычным маршрутизируемым адресам (плоскость данных в этом документе).
- Разделение. Автономное пространство адресов отделено от пользовательского пространства и других областей адресации. Это продиктовано требованиями отказоустойчивости.
- Только шлейфовые адреса. Маршрутизируемые адреса имеют лишь петлевые интерфейсы ACP (возможно, интерфейсы, настроенные для ACP connect, 8.1. ACP Connect), все прочие (виртуальные интерфейсы ACP) используют лишь адреса IPv6 link-local. Применение адресации IPv6 link-local описано в Using Only Link-Local Addressing inside an IPv6 Network [RFC7404].
- Использование ULA. Для петлевых интерфейсов узлов ACP применяются ULA с установленным (1) битом L (параграф 3.1 в [RFC4193]). Отметим, что случайное хэш-значени для петлевого адреса ACP использует определение из параграфа 6.11.2. Базовая схема адресации ACP, а не из параграфа 3.2.2 в [RFC4193].

[1]Man in the middle - атака с перехватом при участии человека.

- Нет внешних соединений. Адреса не обеспечивают доступа в Internet. Если узлу нужны внешние соединения, ему следует параллельно применять управляемую традиционным способом систему адресации.

- Адреса в ACP являются постоянными, а временные адреса, определённые в Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6 [RFC8981], не поддерживаются.

- Адреса ACP не считаются чувствительными в плане приватности, поскольку узлы ACP не предполагаются в качестве пользовательских хостов, поэтому адреса ACP не указывают конечных пользователей или группы. Все узлы ACP размещаются в одном (возможно, федеративном) административном домене. Для трафика ACP узлы предполагаются хостами-кандидатами или транзитными узлами. Нет транзитных узлов с меньшими правами знать отождествления других хостов в ACP. Поэтому адреса ACP не обязаны быть псевдослучайными, как описано в Security and Privacy Considerations for IPv6 Address Generation Mechanisms [RFC7721]. Поскольку адреса не распространяются недоверенным (не ACP) узлам и остаются внутри домена (доверия), они не считаются объектами атак со сканированием.

В ACP применяется лишь адресация IPv6 по ряду причин, перечисленных ниже.

- Простота, надёжность, расширяемость. Если бы поддерживались протоколы сетевого уровня, каждому потребовался бы свой набор защитных ассоциаций, таблица маршрутизации, процесс и т. п.

- Автономные функции не требуют IPv4. Автономные функции и агенты служб - это новые концепции и могут строиться изначально на основе IPv6. Совместимость с прежними версиями не требуется.

- Протоколам OAM не требуется IPv4. ACP пожет поддерживать протоколы OAM и соответствующие протоколы (SNMP, TFTP, SSH, SCP, RADIUS, Diameter, NETCONF и т. п.) доступны в IPv6. Взаимодействие ACP с OAM на основе IPv4 рассмотрено в [RFC8368].

Дополнительное рассмотрение причин выбора адресации и маршрутизации для ACP приведено в параграфе 6.13.5.1. Петлевые интерфейсы ACP.

6.11.2. Базовая схема адресации ACP

Базовая схема адресации ULA для узлов ACP показана на рисунке 9.

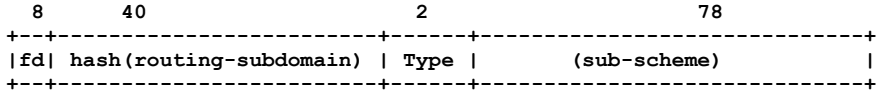

Рисунок 9. Базовая схема адресации ACP.

Первые 48 битов соответствуют схеме ULA, заданной в [RFC4193], с добавлением поля Type.

fd

Указывает локально определённый адрес ULA.

hash(routing-subdomain)

40-битовое поле ULA Global ID (термин из [RFC4193]) для адреса ACP, передаваемого в acp-node-name сертификата ACP, содержит первые 40 битов хэш-значения SHA-256 субдомена маршрутизации из того же acp-node-name. В примере из параграфа 6.2.2 субдомен маршрутизации - это area51.research.acp.example.com, а ULA Global ID - 89b714f3db.

При создании нового субдомена маршрутизации для имеющейся автономной сети **должно** выбираться значение rsub, не создающее конфликтов результирующего хэш-значения субдомена маршрутизации с существующими маршрутными субдоменами автономной сети. Это гарантирует отсутствие конфликтов между адресами ACP, созданными регистраторами для разных субдоменов маршрутизации.

Для поддержки расширяемости узлам ACP при нормальной работе **не следует** предполагать, что ULA Global ID является хэш-значением субдомена маршрутизации. Хэш-функция выполняется лишь в процессе создания сертификата. При использовании BRSKI регистратор BRSKI создаёт registrar acp-node-name в ответ на сообщение EST Certificate Signing Request (CSR) Attributes Request от заявителя.

Организация связности между разными ACP (разные acp-domain-name) выходит за рамки этой спецификации. Если это будет происходить на основе будущих расширений, потребуется выбирать rsub во всех субдоменах маршрутизации этих автономных систем так, чтобы не возникало конфликтов хэш-значений. Например, большая корпорация с приватной привязкой доверия (TA) может создать автономные сети, которые исходно не связаны, с возможностью их последующего объединения. С учётом такой возможности легко выбрать rsub, чтобы не было конфликтов.

Type

Это поле позволяет применять разные субсхемы адресации в соответствии с требованием обновляемости. Назначение и поддержка типов предоставляется IANA.

(sub-scheme)

Субсхема может просто указывать диапазон или набор адресов, выделенных узлу. Это называется диапазоном (набором) адресов ACP и разъяснено для каждой субсхемы ниже.

Причины использования нескольких субсхем адресации и работа с ними описаны в параграфе 6.11.7. Регистраторы ACP и Приложении A.1. Схемы адресного пространства ACP. Сводка субсхем приведена в таблице 1

Таблица 1. Субсхемы адресации.

Тип	*Имя*	*Биты F*	*Z*	*Биты V*	*Префикс*
0	ACP-Zone	-	0	1	/127
0	ACP-Manual	-	1	-	/64
1	ACP-Vlong-8	0	-	8	/120
1	ACP-Vlong-16	1	-	16	/112
2	Резерв на будущее				
3					

Биты F (бит формата, 6.11.5. Субсхемы ACP Vlong (ACP-Vlong-8 и ACP-Vlong-16)) и Z (6.11.4. Субсхема ручной адресации ACP (ACP-Manual)) задают кодирование, как описано ниже. Число битов V указывает размер адресов, выделенных узлу ACP, а префикс указывает размер префикса, анонсируемого узлом ACP в RPL.

6.11.3. Субсхема адресации ACP Zone (ACP-Zone)

Эта субсхема указывается значениями Type = 0 и Z = 0.

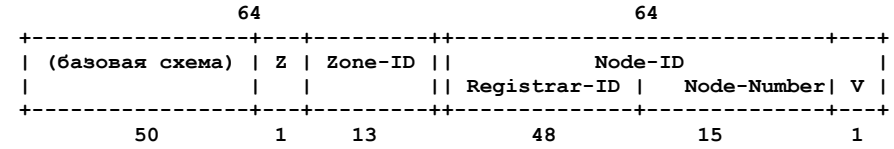

Рисунок 10. Субсхема адресации ACP Zone.

Type

Должно быть 0.

Z

Должно быть 0.

Zone-ID

Значение для зоны сети.

Node-ID

Уникальное значение для каждого узла.

64-битовое поле Node-ID для узла должно быть уникальным в домене ACP и задаётся, как указано ниже.

Registrar-ID (48 битов)

Уникальное для домена значение, указывающее регистратора ACP, назначившего Node-ID для узла. Для этого может применяться 1 или несколько уникальных в домене идентификаторов регистратора ACP (см. параграф 6.11.7.2. Выделение уникального адреса/префикса).

Node-Number

Число, делающее значение Node-ID уникальным. Это могут быть последовательные значения, выделяемые регистратором ACP, который владеет Registrar-ID.

V (1 бит)

Бит виртуализации

0 - указывает саму плоскость (базовая система узла ACP);

1 - указывает необязательный контекст «хоста» узла ACP (см. ниже).

В субсхеме адресации ACP-Zone адрес ACP в сертификате имеет поле V, содержащее только 0.

Набор адресов ACP на узле включает адреса с любыми значениями Zone-ID и V, поэтому никаие два узла в одной плоскости ACP и с одним хэшем субдомена маршрутизации не могут иметь одинаковые Node-ID в субсхема адресации ACP-Zone, отличаясь, например, лишь Zone-ID.

Бит виртуализации (V) в этой субсхеме позволяет легко добавлять ACP в имеющиеся системы, не вызывая проблем в пространстве номеров портов между службами ACP и имеющейся системы. V=0 указывает маршрутизатор ACP (базовая система автономного узла), а V=1 - хост с имеющимися транспортными конечными точками, которые могут конфликтовать с транспортными конечными точками, используемыми маршрутизатором ACP. Хост ACP может, например, иметь виртуальный интерфейс P2P (точка-точка) с адресом с V=0 в качестве маршрутизатора для ACP. В зависимости от устройства программ агентов ASA, выходящего за рамки этой спецификации, он может использовать адрес с V=0 или V=1. Размещение бита V в конце адреса позволяет анонсировать 1 префикс для каждого узла ACP. Например, в сети 20 000 узлов ACP это позволяет избежать 20 000 дополнительных маршрутов в таблице.

Рекомендуется применять только Zone-ID = 0, если это не предназначено для использования в сочетании с практикой частичного или поэтапного внедрения ACP, как описано в параграфе 9.4. Частичное или поэтапное внедрение.

Примечание. Зоны и Zone-ID, заданные здесь, не связаны с зонами и zone_id в IPv6 Scoped Address Architecture [RFC4007]. Адреса зон ACP не ограничены областью действия (т. е. доступны не только внутри зоны, как в [RFC4007]) и доступны из всей плоскости ACP. Идентификатор zone_id является индексом зоны с локальной значимостью на узле [RFC4007], а ACP Zone-ID служит идентификатором для зоны ACP, уникальным в рамках ACP.

6.11.4. Субсхема ручной адресации ACP (ACP-Manual)

Эта субсхема указывается значениями Type = 0 и Z = 1.

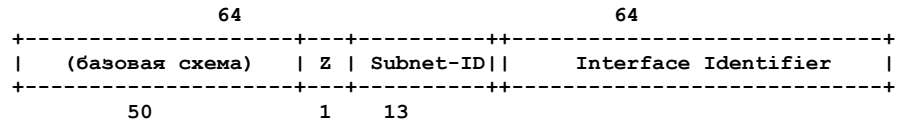

Рисунок 11. Субсхема адресации ACP Manual.

Type

Должно быть 0.

Z

Должно быть 1.

Subnet-ID

Настроенный идентификатор подсети.

Interface Identifier

Идентификатор интерфейса в соответствии с [RFC4291].

Эта субсхема указывает назначение подсетей «вручную», когда другие схемы не подходят. Она применяется в основном на подсетей ACP (8.1.1. Контроллер или NMS без поддержки ACP). Этот режим означает, что значение Subnet-ID должно быть быть выделено уже имеющимся, неавтономным механизмом. В каждой сети, применяющей эту субсхему, должно устанавливаться уникальное значение Subnet-ID (если не применяется anycast).

Бит Z служит для различения субсхем Zone и Manual без добавления ещё одного бита в базовую схему, что позволяет субсхемам Vlong (6.11.5. Субсхемы ACP Vlong (ACP-Vlong-8 и ACP-Vlong-16)) иметь 1 дополнительный бит.

Адреса субсхемы Manual **не следует** использовать в сертификатах ACP. Любому способному строить защищённые каналы ACP узлу, которому политика регистратора разрешает создавать такие каналы, **следует** получать адрес (префикс) ACP от иной (не ручной) субсхемы адресации ACP. Узел, который не может (не разрешено) участвовать в

защищённых каналах ACP, может подключаться к ACP через интерфейсы ACP connect на граничных узлах ACP (8.1. ACP Connect) без создания защищённого канала ACP. В его сертификате ACP **должно** быть опущено поле acp-address для указания применимости сертификата ACP лишь отличными от ACP защищёнными каналами, такими как сквозные транспортные соединения через ACP или плоскость данных.

Управление адресами подсетей ACP connect выполняется традиционными методами и имеющимися протоколами IPv6 (см. 8.1.3. Автонастройка), поэтому V-биты при адресации узлов ACP не применяются в этой субсхеме.

6.11.5. Субсхемы ACP Vlong (ACP-Vlong-8 и ACP-Vlong-16)

Эта субсхема адресации применяется при значении Type = 1 в базовой схеме.

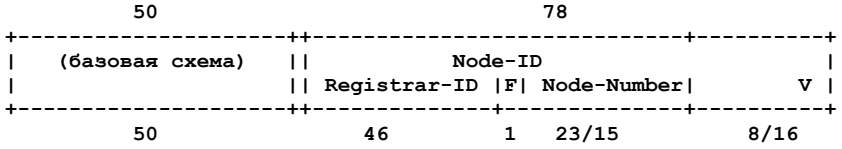

Рисунок 12. Субсхема адресации ACP Vlong.

В этой субсхеме отсутствует поле Zone-ID (6.11.3. Субсхема адресации ACP Zone (ACP-Zone)), чтобы представлять более крупные сети с плоской маршрутизацией (например, IoT) и 8 421 376 Node-Number ($2^{23} + 2^{15}$). Она также позволяет использовать до 2^{16} (65 536) виртуализованных адресов на узле, которые могут служить для адресации программных компонентов на узле ACP.

Поля похожи на применяемые в субсхеме Zone (6.11.3. Субсхема адресации ACP Zone (ACP-Zone)) с уточнениями.

F

Бит, определяющий формат последующих битов.

V

Биты виртуализации (8 при F=0, 16 при F=1), задаваемые узлом ACP. В адресе ACP сертификата ACP (6.2.2. AcpNodeName в сертификате ACP) все биты V имеют значение 0.

Registrar-ID

Для максимизации Node-Number и V поле Registrar-ID сокращено до 46 битов. Можно применять 1 или несколько идентификаторов регистраторов ACP для домена (см. 6.11.7.2. Выделение уникального адреса/префикса).

Node-Number

Значение Node-Number уникально для каждого узла ACP и может иметь 2 формата - 23 бита при F=0, и 15 при F=1. Для каждого формата Node-Number используется своё пространство номеров.

Формат адреса при F=0 предназначен для узлов ACP «общего назначения» которые обычно имеют ограниченное число (меньше 256) клиентов ACP (ASA и/или автономные функции или унаследованные службы), которым нужны отдельные виртуальные (V) адреса. Адреса с F=1 предназначены для узлов ACP, которые служат краевыми (8.1.1. Контроллер или NMS без поддержки ACP) или имеют большое число клиентов, требующих отдельных виртуальных (V) адресов, например, большие контроллеры SDN с модульной контейнерной архитектурой программ (8.1.2. Программные компоненты).

В субсхеме адресации Vlong адреса ACP в сертификате имеют поле V, заполненное нулями. Адрес ACP для узла может иметь любое значение поля V.

6.11.6. Другие субсхемы адресации ACP

Для определения других субсхем адресации нужно собрать опыт применения описанных здесь схем, которые были разработаны для обеспечения достаточной гибкости при организации ACP в разных ситуациях. Это привело к достаточно гибкому использования адресного пространства. Субсхема Zone предназначена для оптимизированной маршрутизации в больших сетях за счёт резервирования битов для Zone-ID, субсхемы Vlong позволяют выделять 8- или 16-битовые адреса внутри отдельных узлов ACP и оба адресных пространства поддерживают распределенное выделение адресов узлов без координации за счёт резервирования битов для поля Registrar-ID в адресах.

6.11.7. Регистраторы ACP

Регистраторы ACP отвечают за зачисление узлов-кандидатов ACP с сертификатами ACP и соответствующими привязками доверия, а также за включение поля acp-node-name в сертификат ACP. Это поле содержит имя домена ACP и префикс адреса ACP для узла ACP, который должен оставаться неизменным в течение срока жизни узла ACP.

Наличие субсхем адресации ACP позволяет домену ACP иметь несколько распределенных регистраторов ACP, которые не обязаны координировать назначение адресов. Регистраторы ACP могут также служить суб-CA и в этом случае они могут выдавать сертификаты ACP независимо от (общих) TA (кроме обновления своих сертификатов).

Регистраторы ACP являются агентами регистрации PKI (PKI registration authorities или RA), расширенными обработкой связанных с сертификатами ACP полей. Они запрашивают сертификаты для узлов ACP у CA с помощью любого подходящего механизма (это выходит за рамки документа, но этот механизм должен BRSKI для регистраторов ANI). Только узлам, являющимся доверенными в соответствии с указанными здесь требованиями к регистраторам, могут быть предоставлены свидетельства, необходимые для выполнения этой функций RA (такие как свидетельство регистратора ACP для подключения к CA в таком качестве).

6.11.7.1. Использование BRSKI или иных механизмов и протоколов

Регистраторы ACP могут применять любые протоколы и механизмы при условии, что полученный сертификат ACP и сертификаты TA могут использоваться другими членами домена для проверки принадлежности к домену ACP, описанной в параграфе 6.2.3. Проверка принадлежности к домену ACP, и соответствия поля acp-node-name требованиям к адресации ACP, приведённым в трёх следующих параграфах.

Регистратором ACP может быть лицо, принимающее решение о зачислении кандидата в ACP и последующей организации (оркестровке) зачисления сертификата ACP и связанной TA через команды или web-интерфейс на узле-кандидате в ACP и TA для генерации и подписывания сертификата ACP, а также настройки сертификата и TA на узле.

В настоящее время для регистраторов ACP определён лишь протокол BRSKI [RFC8995]. При использовании BRSKI узлы ACP называются узлами ANI, а регистраторы ACP - регистраторами BRSKI или ANI. Спецификация BRSKI не задаёт обработки поля acp-node-name, поскольку правила не зависят от BRSKI, но в равной мере применяются к любым протоколам и механизмам, которые может использовать регистратор ACP.

6.11.7.2. Выделение уникального адреса/префикса

Регистратора ACP недопустимо выделять адресные префиксы ACP узрам ACP по имени acp-node-name, которое может вызывать конфликты с префиксами ACP других узлов ACP в том же домене ACP. Это включает префиксы, выделенные одним регистратором ACP разным узлам ACP, и префиксы, выделенные другими регистраторами ACP для того же домена ACP.

Для выделения уникальных адресов регистратор ACP должен имет 1 или несколько 46-битовых идентификаторов (Registrar-ID), уникальных в домене ACP. назначение Registrar-ID регистраторам ACP может происходить с помощью механизмов OAM в сочетании с некой базой данных и/или оркестровкой выделения.

Регистраторы ACP, работающие на узлах с глобально уникальными адресами EUI[1]-48 MAC, могут использовать младшие 46 битов этих адресов в качестве уникального Registrar-ID без какой-либо внешней сигнализации и/или настройки (два старших бита V и U, не задаются однозначно, но функциональны). Этот подход привлекателен для распределенных реализаций облегчённых регистраторов ACP без централизованного администрирования. Механизма проверки уникальности MAC-адреса не существует и реализациям следует применять дополнительные внешние (offline) сведения для принятия допущений об уникальности адресов. Это может быть, например, сведения о продукции или микросхемах сетевых адаптеров (Network Interface Controller или NIC), гарантирующие наличие глобально уникального адреса EUI-48 MAC.

Когда устройство-кандидат в ACP (заявитель в BRSKI) зачисляется в домен ACP, регистратору ACP нужно выделить узлу уникальный адрес ACP и обеспечить включение в сертификат ACP поля acp-node-name (6.2.2. AcpNodeName в сертификате ACP) с подобающей информацией - именем домена ACP, адресом ACP и т. д. Если регистратор ACP применяет BRSKI, он сообщает поле ACP acp-node-name заявителю в атрибутах EST CSR (см. параграф 5.9.2 в [RFC8995]).

6.11.7.3. Правила субсхем адресации

Регистратор ACP выбирает для узла-кандидата ACP уникальный префикс адреса из подходящей субсхемы адресации ACP - префикс субсхемы Zone (6.11.3. Субсхема адресации ACP Zone (ACP-Zone)) или Vlong (6.11.5. Субсхемы ACP Vlong (ACP-Vlong-8 и ACP-Vlong-16)). Назначенный префикс адреса ACP, закодированный в поле acp-node-name сертификата ACP, указывает узлу ACP сведения о его адресе ACP. Субсхема адресации задаёт размер префикса - /127 для Zone, /120 или /112 для Vlong. Первый адрес из этого префикса является адресом ACP, а остальные адреса предназначены для иных применений узлом ACP, как описано в параграфах для субсхем Zone и Vlong. Сам префикс адреса ACP передаётся узлом ACP в протокол маршрутизации ACP (6.12. Маршрутизация в ACP) для обеспечения доступности IPv6 через ACP.

Выбор субсхемы адресации и размер префикса Vlong определяется политикой регистратора ACP. Это может быть политика для домена ACP, узла ACP или типа узлов ACP. Например, в BRSKI регистратор ACP знает сертификат IDevID узла-кандидата ACP, который обычно содержит атрибут serialNumber поле субъекта кодирования отличительного имени, которое часто указывает производителя и тип устройства и может служить для управления правилами выбора подходящей субсхемы адресации для узла или класса узлов.

Регистраторам ACP по умолчанию **следует** выделять адреса субсхемы Zone с Zone-ID = 0.

Регистраторам ACP, знающим сертификат IDevID устройства-кандидата ACP, следует поддерживать выбор субсхемы Zone или Vlong для узлов ACP на основе атрибута serialNumber [X.520] в поле субъекта кодирования отличительного имени в сертификате IDevID например по идентификатору продукции (Product Identifier или PID), который указывает тип продукции, или полному атрибуту serialNumber. PID, например, может указывать узлы, которые позволяют использовать специализированные агенты ASA, требующие несколько адресов, или неавтономные VM для служб и такие узлы могут получать адреса ACP по схеме Vlong.

В простой схеме выделения регистратор ACP постоянно (даже при перезагрузке) помнит используемый идентификатор Registrar-ID и для каждой субсхемы регистрации (Zone с Zone-ID = 0, Vlong с префиксом /112, Vlong с префиксом /120) - следующее значение Node-Number, доступное для выделения, и увеличивает значение Node-Number при следующем зачислении узла ACP. В этой простой схеме выделения регистратор ACP не будет повторно использовать префиксы адресов ACP от узлов ACP, которые больше не используются.

Если регистратор не может запомнить выделенные адреса, необходимо использовать новое значение поля Register-ID в адресах ACP или определять выделенные адреса ACP по доступности узлов ACP, которая может показывать не все узлы ACP. Неотслеживаемые адреса ACP можно вернуть отзывая или не обновляя сертификаты для них и потом использовать эти адреса в новых сертификатах (например, с новым Registrar-ID). Отметим, что такая стратегия может потребовать координации между регистраторами.

6.11.7.4. Сохранение адреса/префикса

Когда сертификат ACP обновляется или его ключи меняются с EST или иным механизмом, адрес (префикс) ACP в поле acp-node-name **должен** сохраняться за исключением ситуаций, когда проблемы безопасности или нарушения требования к уникальности адресов существуют или предполагаются регистратором ACP.

Адресную информацию ACP **следует** поддерживать даже при обновлении или смене ключей регистратор ACP не совпадает с зачислившим ранее сертификат ACP (см., например, 9.2.4. Регистраторы ACP с суб-CA). Адресную информацию ACP **следует** поддерживать также при завершении срока или отказе сертификата ACP (см. 6.2.5.5. Повторное зачисление и 6.2.5.6. Сертификаты с отказом).

[1]Extended Unique Identifier - расширенный уникальный идентификатор.

6.11.7.5. Дополнительные детали

В параграфе 9.2. Регистраторы ACP приведены дополнительные сведения о регистраторах ACP - требуемые взаимодействия и параметры, обновление и ограничения сертификатов, применение суб-CA и централизованное управление политикой.

6.12. Маршрутизация в ACP

После установки адресов ULA на всех автономных элементах следует запустить протокол маршрутизации в контексте ACP. Этот протокол распространяет созданные ULA для обеспечения доступности. Использование контекста ACP исключает конфликты с таблицами маршрутизации плоскости данных, а также защищает ACP от несоответствия конфигурации и некорректных маршрутных обновлений.

Организация плоскости маршрутизации происходит автоматически и строго в соответствии с ACP, поэтому явной настройки не требуется. Все маршрутные обновления автоматически защищаются при передаче, поскольку каналы ACP шифруются, а маршрутизация работает только в контексте ACP.

Протоколом маршрутизации внутри ACP служит RPL [RFC6550], обоснование выбора приведено в Приложении A.4. Выбор протокола маршрутизации (RPL).

Смежность RPL организуется через каналы ACP в одном домене, включая его субдомены маршрутизации, как описано в Приложении A.6. CA, домены и маршрутные субдомены.

6.12.1. Профиль ACP RPL

Далее описан профиль RPL, который узлы ACP должны поддерживать по умолчанию. Формат описания заимствован из [ROLL-APPLICABILITY].

6.12.1.1. Обзор

Информационный пакет RPL (RPL Packet Information или RPI), описанный в параграфе 11.2 [RFC6550], определяет элементы (artifact), требуемые или полезные при пересылке пакетов, маршрутизируемых протоколом RPL. Этот профиль не использует RPI для большей совместимости с аппаратно ускоренными плоскостями пересылки, которые зачастую не поддерживают заголовки Hop-by-Hop, применяемые для RPI, а также для исключения издержек на заголовки RPI в линии и расходов на их добавление и/или удаление.

6.12.1.1.1. Один экземпляр

Чтобы избежать RPI, профиль ACP RPL использует простую таблицу маршрутизации и пересылки на основе префиксов получателей. Для этого в профиле применяется только один экземпляр RPL instanceID. Этот экземпляр instanceID может содержать лишь граф DODAG[1], поэтому таблица маршрутизации и пересылки может учитывать лишь 1 класс обслуживания (best effort в направлении первичного NOC/корня) и не может создавать оптимизированные пути маршрутизации для достижения целей задержки или энергопотребления между любой парой узлов.

Такой выбор является компромиссом. Рассмотрим сеть с несколькими NOC в разных местах. Лишь один из этих NOC станет корнем DODAG. Трафик к другим NOC и от них передаётся через DODAG (дерево кратчайших путей) с корнем в первичном NOC. В зависимости от топологии это может оказаться неоптимальным решением с точки зрения задержки и минимизации ресурсов на сетевом пути, но считается приемлемым с учётом того, что трафик ACP включает «только» пакеты управления и поддержки (см. Приложение A.9.4. Усовершенствование RPL).

Использование одного instanceID/DODAG не создаёт критическую точку отказа, поскольку DODAG перенастраивается при обнаружении отказов пересылки в плоскости данны, включая выбор другого корня при отказе основного.

Преимущество этого профиля, особенно в сравнении с другими IGP, состоит в том, что здесь не рассчитываются маршруты для узлов, доступных через тот же интерфейс, что и корень DODAG. Поэтому такой профиль RPL может работать с гораздо большим числом узлов ACP при том же объёме расчётов и занимаемой памяти, нежели другие протоколы, особенно на узлах, являющихся листьями топологии или близких к таким листьям.

6.12.1.1.2. Повторное схождение

В профилях RPL с пакетами RPI (6.12.1.13. Информационный пакет RPL) эти пакеты также служат для запуска повторного схождения (reconvergence) при ошибочной маршрутизации (например, петли), обнаруживаемой из данных RPI. Это помогает минимизировать сигнальный трафик RPL, особенно в сетях без стабильной топологии и с медленными каналами. Профиль ACP RPL вместо этого полагается на быстрое повторное сведение DODAG за счёт распознавания смены состояния канала (down/up) с использованием сигнализации, описанной в параграфе 6.12.1.7. Ремонт DODAG. Поскольку предполагается, что каналы ACP в основном надежны (или имеют защиту от потерь на канальном уровне) и нет описанного в параграфе 6.12.1.7 «растяжения», петли, вызываемые потерей сигнальных пакетов RPL, скорей всего, будут чрезвычайно редкими.

Кроме того, в RPL возможно множество механизмов предотвращения временных петель, которые **рекомендуется** применять в профиле ACP RPL - объекты DIO (DODAG Information Object) **следует** передавать 2 или 3 раза для информирования потомков о потере последнего предка. Метод из параграфа 8.2.2.6 в [RFC6550] (Detaching) следует предпочитать методу из параграфа 8.2.2.5 (Poisoning), поскольку он разрешает локальную связность. Узлам **следует** выбирать несколько предков (по возможности, не менее 3) и передавать DAO параллельно всем родителям.

Неисправные туннели ACP можно быстро обнаруживать с помощью механизмов протокола защищённого канала, таких как обнаружение «мертвых» партнёров в IKEv2. Это может служить заменой функции LLN ETX[2], которая не применяется в этом профиле. Об отказе туннеля ACP следует сразу сообщать плоскости управления RPL для выбора другого родителя.

6.12.1.2. Экземпляры RPL

Применяется единственный экземпляр RPL, по умолчанию установлено RPLInstanceID = 0.

[1]Destination-Oriented Directed Acyclic Graph - ориентированный на получателя направленный ациклический граф.
[2]Low-power and Lossy Network's Expected Transmission Count - счётчик ожидаемых передач с сети с потерями и слабым питанием.

6.12.1.3. Режим с сохранением и без сохранения

Для RPL **должен** поддерживаться режим (Mode of Operation или MOP) 2, «Сохранение режима операций без поддержки групповой передачи» ("Storing Mode of Operations with no multicast support). Реализации **могут** поддерживать режим 3 «… с поддержкой групповой передачи» (... with multicast support) как надмножество режима 2. Корень указывает режим в потоке DIO.

6.12.1.4. Политика DAO

Политика DAO заключается в энергичной (aggressive), упреждающей (proactive) поддержке состояния DAO.

- Применяется флаг K в незапрошенном DAO для указания замены предшествующих сведений (для DAO-ACK).
- Такие сообщения DAO повторяются DAO-RETRIES (3) раз с интервалом DAO-ACK_TIME_OUT (256 мсек).

6.12.1.5. Метрика пути

Применяется счётчик интервалов Hop Count в соответствии с Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks [RFC6551]. Отметим, что счётчик нужен лишь для диагностики и не применяется в Objective Function.

6.12.1.6. Предметная функция

Objective Function (OF)

Применяется Objective Function Zero (OF0) (Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL) [RFC6552]). Контейнеры метрики не используются.

rank_factor

Определяется скоростью канала - LOW_SPEED_FACTOR (5) для скорости не выше 100 Мбит/с, иначе HIGH_SPEED_FACTOR (1). Это простое ранжирование каналов на «низкоскоростные» или IoT, которые обычно используют скорость не выше 100 Мбит/с, и «инфраструктурные» со скоростями 1 Гбит/с и выше. С учётом того, что выбор пути в ACP основан лишь на достижимости, а не на оптимизации стоимости, не предпринимается попыток «тонкой настройки» пути.

6.12.1.7. Ремонт DODAG

Глобальный ремонт

Предполагается стабильность каналов и рангов (метрики),поэтому не возникает необходимости в периодическом перестроении DODAG. Версия DODAG инкрементируется лишь при катастрофических событиях (например, по команде администратора).

Локальный ремонт

При обнаружении обрыва канала узел ACP передаёт No-Path DAO для всех целей, которые были доступны через этот канал. При восстановлении канала узел ACP проверяет, предоставляет ли этот канал лучшего предка (родителя). Если это так, узел ACP рассчитывает новый ранг и передаёт новое сообщение DIO с анонсом ранга. Затем он передаёт DAO с новым путём к себе.

При использовании виртуальных интерфейсов ACP с множественным доступом, локальный ремонт может напрямую инициироваться прерыванием связи с партнёром (6.13.5.2.2. Виртуальные интерфейсы ACP с множественным доступом).

stretch_rank

Не предоставляется (не растягивается).

Data-Path Validation

Не используется.

Trickle

Не используется.

6.12.1.8. Групповая передача

Групповая передача ещё не применяется, но может быть использована выбранным режимом работы.

6.12.1.9. Безопасность

Защита RPL [RFC6550] на используется, достаточно защиты ACP. Поскольку каналы ACP уже имеют средства защиты конфиденциальности и целостности, дополнительная защита на уровне RPL была бы избыточной.

6.12.1.10. Коммуникации P2P

Не используются.

6.12.1.11. Настройка адреса IPv6

Каждый узел ACP (узел RPL) анонсирует префикс IPv6, охватывающий адреса, выделенные узлу ACP в AcpNodeName. Размер префикса зависит от субсхемы acp-address - /127 для Zone, /112 или /120 для Vlong (см. параграф 6.11).

Каждый узел ACP **должен** установить маршрут в «чёрную дыру» (black hole) или null-маршрут, если у него имеется неиспользуемая часть адресного пространства ACP, выделенного ему в AcpNodeName. Это переопределяется более длинными префиксами для интерфейсов в соответствии с фактически используемыми адресами. Например, при наличии у узла адресов ACP-Vlong-8 он устанавливает «черную дыру» /120. Тогда при использовании лишь адреса ACP (первый в диапазоне), например, он установит этот адрес с префиксом /128 на петлевом интерфейсе ACP (6.13.5.1. Петлевые интерфейсы ACP). Ни один из более длинных префиксов не анонсируется в RPL.

Для адресов ACP-Manual на узле ACP, например, в подсетях ACP connect (8.1.1. Контроллер или NMS без поддержки ACP) узел анонсирует префикс подсети /64.

6.12.1.12. Административный параметр

Административное предпочтение (Administrative Preference) (параграф 3.2.6 в [RFC6550], чтобы стать корнем) указывается полем DODAGPreference в сообщении DIO.

```
Явно заданный «корень»:  0b100
Регистратор ACP (по умолчанию):  0b011
```

```
ACP connect (не регистратор):  0b010
По умолчанию:  0b001
```

6.12.1.13. Информационный пакет RPL

RPI не требуется в профиле ACP RPL по указанным ниже причинам.

Одной из опций RPI является заголовок заданной источником маршрутизации RPL (Source Routing Header или SRH) (An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL) [RFC6554]), который не требуется, поскольку профиль ACP RPL использует режим с сохранением (storing), где каждый узел пересылки (hop) имеет сведения о следующем узле (next-hop) для пересылки.

Упрощённый заголовок RPL Option (The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams [RFC6553]) также не требуется в этом профиле, поскольку применяется 1 экземпляр RPL и проверка пути данных также не производится.

6.12.1.14. Неизвестные получатели

Поскольку RPL минимизирует размер таблицы маршрутизации и пересылки, префиксы, доступные через тот же интерфейс, что и корень RPL, известны не каждому узлу ACP. Поэтому трафик на неизвестный адрес можно увидеть лишь в корне RPL. Корню RPL **следует** иметь безопасные механизмы для оперативного обнаружения и фиксации (log) таких пакетов.

Поскольку это требование дополнительно ограничивает функциональность плоскости данных корня RPL, оно не применяется к «обычным» узлам, не настроенным на выполнение специальных функций (т. е. административный параметр из параграфа 6.12.1.12 имеет значение 0b001). Если сеть ACP деградирует до состояния, когда ни один узел не может быть задан корнем, регистратором или узлом ACP connect, возможно, что корень RPL (и ACP в целом) не сможет обнаружить трафик к неизвестным получателям. Однако при отсутствии узлов с административным предпочтением, отличным от 0b001, маловероятна возможность получить диагностические сведения из ACP, поэтому обнаружение трафика к неизвестным получателям в любом случае не будет действенным.

6.13. Общие вопросы ACP

Поскольку каналы по умолчанию организуются между соседями, полученная в результате наложенная сеть использует поэтапное (hop-by-hop) шифрование. Каждый узел расшифровывает входящий трафик ACP и шифрует трафик для своих соседей ACP. Маршрутизация рассмотрена в параграфе 6.12. Маршрутизация в ACP.

6.13.1. Производительность

Этот документ не задаёт требований к производительности реализаций ACP, поскольку они зависят от предполагаемого использования. Ожидается, что полностью автономный узел с широким набором агентов ASA может потребовать высокой производительности пересылки в ACP, например, для телеметрии. Реализации ACP, поддерживающие лишь традиционное применение или стиль SDN, могут выиграть при более низкой производительности ACP, особенно при использовании ACP лишь для критических операций, например, при недоступности плоскости данных. Устройство ACP, заданное этим документом, рассчитано на поддержку широкого спектра вариантов производительности и разрешает программные реализации с потенциально малой производительностью и варианты с высокой производительностью (см. [RFC8368]).

6.13.2. Адресация на защищённых каналах

Для независимости от адресации и маршрутизации плоскости данных в защищённых каналах ACP, найденных GRASP, применяются адреса IPv6 link-local для связи между соседями[1].

Чтобы избежать влияния интерфейса и адреса IPv6 (link-local), применяемого для каналов ACP, при настройке плоскости данных, это требуется учитывать при реализации. Если интерфейс IPv6 с адресом link-local используется совместно с плоскостью данных, для него нужно исключить возможность перенастройки или отключения путём настройки конфигурации. Вместо совместного использования интерфейса и адреса IPv6 link-local можно применять отдельный (виртуальный) интерфейс с отдельным адресом IPv6 link-local. Например, интерфейс ACP может работать через отдельный MAC-адрес базового интерфейса L2 (Ethernet). Дополнительные детали и варианты приведены в Приложении A.9.2. Варианты исключения зависимости от плоскости данных IPv6.

Отметим, что другие (не идеальные) реализации могут создавать дополнительные, нежелаемые зависимости от плоскости данных, например, общий код и конфигурация протоколов защищённого канала (IPsec и/или DTLS).

6.13.3. MTU

Значение MTU для защищённых каналов ACP **должно** задаваться локально на основе MTU базового канала за вычетом издержек на инкапсуляцию в защищённом канале.

Протоколам защищённого канала ACP не требуется определять MTU, поскольку они организуются на основе смежности L2 и значения MTU на обеих сторонах соединения L2 предполагаются согласованными. Расширения ACP, где, например, применяется туннелирование ACP, должны рассмотреть вопрос согласованности MTU. Это проблема туннелей, а не работы ACP через туннель. Транспортные стеки, работающие через ACP, могут применять обычный механизм PMTUD (Path MTU Discovery). Поскольку в ACP надёжность преобладает над производительностью, **можно** ожидать предпочтения минимального IPv6 MTU (1280 октетов), чтобы избежать ошибок реализации PMTUD и проблем несоответствия MTU на базовых каналах.

6.13.4. Несколько каналов между узлами

Если два узла соединены несколькими каналами, ACP следует организовать через каждый канал, но возможно использование для ACP лишь части каналов. Наличие канала ACP на каждом соединении имеет много преимуществ (например, более быстрое восстановление при отказе соединения) и более точно отражает физическую топологию.

[1] В параграфе 8.2 заданы расширения для настройки защищённых каналов в форме туннелей через плоскость данных, поэтому такие каналы зависят от неё.

Использование части каналов (например, одного) снижает расход ресурсов узла, поскольку для каждого канала ACP нужно сохранять состояние. Схема согласования (6.6. Выбор канала) позволяет решающему узлу (Decider - узел с большим адресом ACP) сбрасывать все каналы ACP кроме желаемых к узлу Follower, а тот не будет пытаться повторить организацию защищённых каналов со своей стороны, пока Decider не появится с неизвестным ранее анонсом GRASP (например, на другом канале или с другим адресом, сообщаемым в GRASP).

6.13.5. Интерфейсы ACP

Концептуально ACP VRF имеет два типа интерфейсов - петлевые (ACP loopback interface), которым назначаются адреса ACP ULA и виртуальные (ACP virtual interface), которые сопоставляются с защищёнными каналами ACP.

6.13.5.1. Петлевые интерфейсы ACP

Для автономных операций ACP, описанных в разделах 6 и 7, узел ACP использует первый адрес из N-битового префикса ACP, выделенного узлу, N = (128 - число битов V в адресе ACP). Этот адрес с префиксом N или больше назначается петлевому (loopback) интерфейсу.

Другие адреса из префикса узел ACP может использовать по своему усмотрению. Автономные операции ACP не требуют дополнительных глобальных адресов IPv6, они могут применяться для агентов ASA и неавтономных функций. Компоненты ACP, которые не полностью автономны, такие как интерфейсы ACP (Рисунок 14), также могут вводить дополнительные глобальные адреса IPv6 на других типах интерфейсов в ACP.

Применение петлевых интерфейсов для глобальных адресов является обычной практикой для маршрутизаторов, например, в соединениях внутреннего BGP (Internal BGP или IBGP) с BGP4 (A Border Gateway Protocol 4 (BGP-4) [RFC1654]) или более ранними версиями протокола. ACP принимает и автоматизирует эту практику.

Петлевой интерфейс для описанного выше применения в ACP - это интерфейс, поведение которого соответствует разделу 4 (второй абзац) Default Address Selection for Internet Protocol Version 6 (IPv6)" [RFC6724]. Пакеты, переданные хостом узла с петлевого интерфейса ведут себя, как будто они «закольцованы» интерфейсом, т. е. они выглядят как переданные loopback-интерфейсом, затем принятые узлом и переданные в направлении адресата. Термин loopback only указывает такое поведение, а не фактическое название типа интерфейса, выбранного в фактической реализации. Петлевым интерфейсом для использования с ACP может быть виртуальной и/или программной конструкцией, не связанной с оборудованием, или аппаратным интерфейсом, работающим в петлевом режиме (loopback mode). Петлевому интерфейсу, используемому для ACP, **недопустимо** иметь соединения с другими узлами.

Ниже приведён список причин выбора loopback-адресов для ACP, основанный на архитектуре адресации IPv6 и общих проблемах.

1. Адреса IPv6 назначаются интерфейсам, а не узлам. IPv6 следует модели IPv4 в том, что префикс подсети связывается с одним каналом, см. параграф 2.1 в IP Version 6 Addressing Architecture [RFC4291].
2. Реализации IPv6 обычно не позволяют назначать один глобальный адрес IPv6 нескольким интерфейсам в одном экземпляре VRF.
3. Глобальные адреса, назначенные интерфейсам, соединённым с другими узлами (внешние интерфейсы), могут не быть стабильными, поскольку на любом из таких интерфейсов может возникнуть отказ по внешним для узла причинам. Это может сделать назначенные интерфейсу адреса непригодными.
4. Если отказ в подсети не отключает (down) интерфейс и не делает его адреса непригодными, это может привести к недоступности интерфейса, поскольку кратчайший путь к узлу может проходить через другой узел той же подсети, который может считать подсеть работающей, даже если это не так.
5. Многие реализации служб OAM на маршрутизаторах не могут работать более чем с одним адресом партнёра, зачастую потому, что уже предполагают возможность использования петлевого адреса, особенно для обеспечения стабильного адреса при отказах на внешних интерфейсах или каналах.
6. Даже при поддержке приложением нескольких адресов партнёра, оно может использовать лишь один адрес в каждый момент для соединения с наиболее распространёнными транспортными протоколами TCP и UDP. Хотя в TCP Extensions for Multipath Operation with Multiple Addresses [RFC6824]/[RFC8684] эта проблема решена, это может быть недостаточно широко реализовано службами OAM в маршрутизаторах.
7. Для полностью автономного назначения глобальных адресов подсетям, соединённым с другими узлами, каждый узел должен иметь достаточно большое адресное пространство префикса (порядка максимального числа подсетей, к которым узел может присоединяться), а затем узлу придётся договариваться со смежными узлами в этих подсетях, какое пространство адресов применять для каждой подсети.
8. Использовать глобальные адреса для подсетей между узлами не требуется, если эти подсети лишь соединяют маршрутизаторы (как защищённые каналы ACP), поскольку они могут взаимодействовать с удалёнными узлами через свои глобальные loopback-адреса. Поэтому назначение глобальных адресов для этих внешних подсетей расточительно для адресного пространства, а также без нужды увеличивает размер таблиц маршрутизации и пересылки, что крайне нежелательно, особенно для ACP, поскольку здесь требуется минимизировать на уровне узла издержки ACP VRF.
9. По этим причинам субсхемы адресации ACP не рассматривают адреса ACP для подсетей, соединяющих узлы ACP.

Отметим, что в Segment Routing Architecture [RFC8402] введён термин Node-SID для указания сегментов префикса IGP, идентифицирующих конкретный маршрутизатор, например, на loopback-интерфейсе. Префикс петлевого адреса ACP можно по аналогии называть идентификатором узла ACP (ACP Node Identifier).

6.13.5.2. Виртуальные интерфейсы ACP

Любая защищённая связь ACP с другим узлом ACP сопоставляется с виртуальным интерфейсом одним из описанных ниже способов. Это не зависит от выбранного протокола защиты (IPsec, DTLS, иной стандартный или нестандартный протокол).

Отметим, что все приведённые здесь соображения предполагают защищённые связи «точка-точка». Отображения множественных защищённых связей, такие как The Group Domain of Interpretation [RFC6407], выходят за рамки документа.

6.13.5.2.1. Виртуальные интерфейсы ACP "точка-точка"

В этом варианте каждый защищённый канал ACP отображается на свой виртуальный интерфейс «точка-точка». Если физическая подсеть имеет более двух узлов с поддержкой ACP (в одном домене), такой подход к реализации ведёт к полносвязной (full mesh) сети виртуальных интерфейсов ACP между узлами.

Когда протокол защищённого канала видит, что партнёр не работает, ему **следует** сообщить о разрыве связи для запуска восстановления RPL DODAG (6.12.1.7. Ремонт DODAG).

6.13.5.2.2. Виртуальные интерфейсы ACP с множественным доступом

При более совершенном подходе ACP создаёт один виртуальный интерфейс ACP с множественным доступом для всех защищённых каналов ACP к поддерживающим ACP узлам, доступным через одну базовую (физическую) подсеть. Групповые пакеты IPv6 link-local, переданные на виртуальный интерфейс ACP с множественным доступом, реплицируются в каждый защищённый канал ACP, сопоставленный с этим интерфейсом. Индивидуальный пакет IPv6, направленный на виртуальный интерфейс ACP с множественным доступом, передаётся в защищённый канал ACP, относящийся к соседу ACP, который является next hop в таблице пересылки ACP, используемой для адресата пакета.

Когда протокол защищённого канала видит, что партнёр по защищённому каналу, отображенному на виртуальный интерфейс ACP с множественным доступом, не работает, ему **следует** сообщить о разрыве связи для запуска восстановления RPL DODAG (6.12.1.7. Ремонт DODAG).

Не требуется, чтобы все узлы ACP одной подсети с множественным доступом использовали один тип виртуальных интерфейсов ACP. Это определяется локальным решением узла.

Узлы ACP **должны** выполнять стандартные операции IPv6 через виртуальные интерфейсы ACP, включая SLAAC [RFC4862] для назначения адреса IPv6 link-local виртуальному интерфейсу ACP и ND (Neighbor Discovery for IP version 6 (IPv6) [RFC4861]) для определения адреса IPv6 link-local сопоставленного с защищённым каналом ACP, отображённым на виртуальный интерфейс ACP. Это не зависит от типа виртуального интерфейса ACP.

Рекомендуется применять оптимистическое обнаружение дубликатов адресов (Optimistic Duplicate Address Detection или DAD) в соответствии с Optimistic Duplicate Address Detection (DAD) for IPv6 [RFC4429], поскольку вероятность дубликатов между узлами ACP крайне мала, поскольку адрес может формироваться из глобально уникального идентификатора, назначенного локально (например, EUI-48 или EUI-64, см. ниже).

Узлы ACP **могут** снижать число групповых пакетов IPv6 link-local от ND за счёт определения адреса IPv6 link-local для соседа по защищённому каналу ACP из других источников, таких как адрес отправителя в групповых сообщениях RPL, с отказом от передачи сообщений Neighbor Solicitation.

Адрес IPv6 link-local виртуального интерфейса ACP можно вывести из подходящего локального источника, например адреса EUI-48 или EUI-64 на узле. **Недопустима** зависимость этого от чего-либо, что может подвергнуться атаке из плоскости данных, например, от адреса IPv6 link-local базового физического интерфейса, который может быть атакован через SLAAC, или параметров заголовка инкапсуляции защищённого канала, которые не защищены.

Адрес канального уровня для виртуального интерфейса ACP - это адрес, применяемый для базового интерфейса, через который организован защищённый туннель (обычно адрес Ethernet). Поскольку индивидуальные пакеты IPv6, отправляемые виртуальному интерфейсу ACP, передаются не по адресу получателя на канальном уровне, в в защищённый канал ACP, поле адреса канального уровня **следует** игнорировать при получении, запоминая вместо него защищённый канал ACP из которого было получено сообщение.

Виртуальные интерфейсы ACP с множественным доступом предпочтительней в реализации, когда базовый интерфейс относится к (широковещательной) подсети с множественным доступом, поскольку он отражает множественный доступ в базовой подсети виртуальным интерфейсам ACP. Это упрощает, например, организацию служб с пониманием топологии внутри ACP VRF, как будто они работают на естественных интерфейсах с множественным доступом.

Следует также сравнивать виртуальные интерфейсы «точка-точка» и с множественным доступом в плане эффективности лавинной рассылки групповых сообщений link-local.

Рассмотрим ЛВС с 3 соседями - Алиса, Боб и Кэрол. Пусть ACP GRASP Алисы хочет передать групповое сообщение GRASP link-local Бобу и Кэрол. Если ACP у Алисы эмулирует ЛВС как виртуальные интерфейсы «точка-точка» (один для Боба, второй для Кэрол), ACP GRASP Алисы будет передавать две копии групповых сообщения GRASP - одну Бобу, другую Кэрол. Если ACP Алисы эмулирует ЛВС как многоточечный виртуальный интерфейс, ACP GRASP Алисы будет передавать этому интерфейсу 1 пакет, а многоточечный виртуальный интерфейс ACP будет реплицировать пакет в каждый защищённый канал (Бобу и Кэрол). Результат в обоих случаях одинаков. Различие возникает, когда Боб и Кэрол получают пакеты. Если они используют виртуальные интерфейсы ACP «точка-точка», их экземпляр GRASP будет пересылать пакет от Алисы друг другу как часть процедуры лавинной рассылки GRASP. Эти пакеты не нужны и будут отброшены GRASP при получении как дубликаты (по GRASP Session ID). Если же ACP Боба и Кэрол эмулируют виртуальный интерфейс с множественным доступом, дублирования не будет, поскольку процедура лавинной рассылки GRASP не реплицирует пакеты в интерфейс, откуда пакет принят.

Отметим, что групповые сообщения GRASP link-local не передаются напрямую как групповые сообщения IPv6 link-local UDP виртуальным интерфейсам ACP, а вместо этого передаются виртуальным интерфейсам ACP GRASP, которые размещаются над виртуальными интерфейсами ACP для добавления надёжности TCP групповым сообщениям GRASP link-local. Тем не менее, эти виртуальные интерфейсы ACP GRASP выполняют такую же репликацию сообщений и так же влияют на лавинную рассылку (6.9.2. ACP как защищённая транспортная подложка для GRASP).

RPL поддерживает операции и корректное построение таблиц маршрутизации в подсетях с множественным доступом без широковещания (non-broadcast multi-access или NBMA). Такие системы широко применяются для радиодоступа. При использовании подсетей NBMA **недопустимо** представлять их виртуальными интерфейсами ACP с множественным доступом, поскольку реплики групповых сообщений IPv6 link-local не будут доставлены всем соседям в

сети NBMA, что приведёт к отказу лавинной рассылки сообщений GRASP. Взамен каждый защищённый канал ACP с таким интерфейсом **должен** представляться как виртуальный интерфейс ACP «точка-точка» (A.9.4. Усовершенствование RPL).

Нужно соблюдать осторожность при создании виртуальных интерфейсов ACP с множественным доступом для защищённых каналов ACP между узлами ACP в разных доменах или субдоменах маршрутизации. Например, если будущие междоменные правила ACP определить как «одноранговые» (peer-to-peer) это упростит создание виртуальных интерфейсов ACP «точка-точка» для таких междоменных защищённых каналов.

7. Поддержка ACP на коммутаторах и портах L2 (нормативный)

7.1. Зачем? (преимущества ACP на коммутаторах L2)

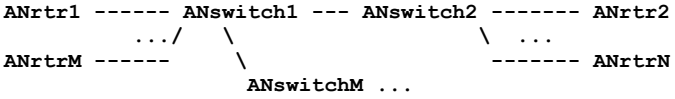

Рисунок 13. Топология с коммутаторами L2 ACP.

Рассмотрим большую ЛВС L2 с маршрутизаторами ANrtr1 — AnrtrN, соединёнными через некую топологию коммутаторов L2. Примерами могут служить сети больших организаций с ядром L2, сети IoT или широкополосные сети агрегирования, где часто применяется многоуровневая топология с коммутацией L2.

Если используемый в ACP протокол обнаружения работает на уровне подсети, каждый маршрутизатор ACP будет видеть все прочие маршрутизаторы ACP в ЛВС как соседей и образуется полносвязная (full mesh) сеть каналов ACP. Если все или часть коммутаторов AN автономны и применяют тот же протокол обнаружения, они также войдут в полносвязную сеть.

Полная связность соединений ACP может создавать проблемы для расширения. Число защищённых связей в протоколах защищённых каналов вряд ли сможет произвольно увеличиваться, особенно при использовании аппаратного ускорения операций шифрования и расшифровки. Другие операции ACP (такие как маршрутизация) также потребуют расширения с ростом числа прямых соседей ACP. Маршрутизатора ACP с 4 физическими интерфейсами достаточно в ЛВС с сотнями соседей, подключённых через коммутаторы. Введение такого нового, непредсказуемого фактора масштабирования усложняет поддержку ACP на произвольных платформах в произвольных средах.

Можно легко обеспечить предсказуемые требования к росту числа соседей ACP, если в аналогичной топологии коммутаторы L2 с поддержкой ACP могут ограничить рассылку сообщений обнаружения, чтобы маршрутизаторы и коммутаторы ACP находили лишь физически подключённые коммутаторы ACP L2 в качестве кандидатов в соседи ACP. При наличии такого механизма обнаружения ACP и защищённые связи будут расширяться пропорционально числу физических интерфейсов, а не числу потенциальных соседей, «подключённых к ЛВС», и топология ACP будет соответствовать физической топологии, что иногда может быть полезно для операций управления или ASA.

Пусть в приведённом выше примере ANswitch1 и ANswitchM поддерживают ACP, а ANswitch2 не поддерживает. Желаемая топология ACP будет получаться при наличии у ANrtr1 и ANrtrM соединения ACP лишь с ANswitch1 и полносвязных соединениях ACP между ANswitch1, ANrtr2 и AnrtrN. ANswitch1 также имеет соединения ACP с ANswitchM, а ANswitchM - с кем-либо, расположенным за ним.

7.2. Как? (на уровне порта L2 DULL GRASP)

Для поддержки ACP на коммутаторах L2 или коммутирующих портах L2 устройства L3, необходимо, чтобы эти порты L2 для реализации ACP выглядели как интерфейсы L3. В первую очередь это связано с созданием отдельного экземпляра/домена DULL GRASP для каждого такого порта L2. Поскольку GRASP имеет выделенный групповой адрес IPv6 link-local (ALL_GRASP_NEIGHBORS), этого достаточно, чтобы все пакеты для этого адреса извлекались на уровне порта и передавались данному экземпляру DULL GRASP. Аналогично, групповые пакеты IPv6 link-local, переданные экземпляром DULL GRASP, должны отправляться лишь в на порт L2 для этого экземпляра DULL GRASP (вместо лавинной рассылки через все порты VLAN, к которой относится порт).

Когда порты/интерфейсы, через которые предполагается работа ACP в понимающем ACP коммутаторе L2 или маршрутизирующем устройстве L2/L3, являются портами моста L2, пакеты на адрес ALL_GRASP_NEIGHBORS **недопустимо** передавать между ними. При использовании отслеживания MLD, ему **должна** быть запрещена передача через мост (bridging) пакетов для группового адреса IPv6 ALL_GRASP_NEIGHBORS.

На гибридных коммутаторах L2/L3 одному интерфейсу L3 VLAN назначается множество портов L2. С упомянутыми выше расширениями для DULL GRASP плоскость ACP может просто работать на интерфейсах L3 VLAN, поэтому не требуется дополнительной (аппаратной) пересылки для работы ACP на портах L2. Это обеспечивается тем, что протоколы защищённых каналов ACP используют лишь индивидуальные пакеты IPv6 link-local и эти пакеты будут передаваться корректному порту L2 в направлении партнёра логикой VLAN на устройстве.

Этого достаточно при организации виртуальных интерфейсов ACP P2P для каждого партнёра ACP. Когда желательно создать виртуальные интерфейсы ACP с множественным доступом (параграф 6.13.5.2.2), **требуется** объединять не все защищённые каналы ACP на одном интерфейсе L3 VLAN, а только каналы на одном порту L2.

При использовании тегов VLAN описанная выше логика применяется лишь к пакетам GRASP без тегов. Для обнаружения соседей ACP через GRASP **следует** принимать и передавать пакеты без тегов VLAN. В гибридных коммутаторах L2/L3, каждая сеть VLAN будет создавать смежности ACP лишь через порты, где нет тегов VLAN.

В результате простая логика заключается в том, что защищённые каналы ACP будут работать через те же интерфейсы L3, которые имеются в плоской сети с мостами (bridged) через все маршрутизаторы, но полной связности каналов ACP не возникает и соседями становятся лишь узлы ACP, подключённые по защищённым каналам через порт L2, поскольку работа DULL GRASP разделена по портам.

Например, на рисунке 13 ANswitch1 может запустить отдельные экземпляры DULL GRASP на портах к ANrtr1, ANswitch2 и AnswitchI, даже если эти три порта в плоскости данных будут в той же сети VLAN (ЛВС) и выполнять коммутацию L2 между этими портами. ANswitch1 будет выполнять между этими портами маршрутизацию ACP L3.

Описание в предыдущем абзаце специально предназначено для иллюстрации того, что на гибридных устройствах L3/L2, распространённых в корпоративных сетях, IoT и широкополосном агрегировании извлечение пакета GRASP происходит лишь 1 раз (по адресу Ethernet), равно как вставка группового пакета GRASP link-local на порт L2, которая работает с портами L2 на уровне аппаратной пересылки. Остальные операции относятся полностью к плоскости управления ACP и организации защищённых каналов через интерфейс L3. Предполагается, что это упростит поддержку ACP на уровне портов L2 в таких гибридных устройствах.

В устройства без смешения портов/интерфейсов L2 и интерфейсов L3 (для завершения транспортных соединений) детали реализации могут отличаться. Логичней и проще рассматривать и использовать каждый порт L2 как отдельную подсеть L3 для всех операций ACP. Тот факт, что для ACP нужна лишь групповая и индивидуальная передача IPv6 link-local, должен максимально упростить поддержку ACP на устройствах L2 любого типа.

Общей проблемой ACP в сетях с коммутацией L2 является взаимодействие с протоколом связующего дерева (Spanning Tree Protocol или STP). Без дополнительного усовершенствования L2 плоскость ACP будет работать лишь через активную топологию STP и при изменении дерева работа ACP будет прерываться с повторным схождением. В идеале партнёрство ACP **следует** организовывать лишь через порты, которые заблокированы в STP, чтобы работа ACP не зависела от STP и могла продолжаться при изменении топологии STP, когда повторное схождение может быть достаточно долгим. Описанных выше простых вариантов для этого недостаточно.

8. Поддержка элементов, не понимающих ACP (нормативный раздел)

8.1. ACP Connect

8.1.1. Контроллер или NMS без поддержки ACP

ACP может применяться системами управления, такими как контроллеры или хосты NMS, для подключения к устройствам (или иным типам узлов). Для этого хосту NMS нужен доступ в ACP. Плоскость ACP - это наложенная сеть с самозащитой, по умолчанию предоставляющая доступ лишь доверенным автономным системам. Поэтому традиционные (не ACP) не имеют по умолчанию NMS доступа в ACP, как и другие внешние узлы.

Если хост NMS не является автономным, т. е. не поддерживает автономного согласования ACP, его можно ввести в ACP путём явной настройки. Для поддержки соединений со смежными устройствами, не являющимися узлами ACP, узлу ACP **следует** поддерживать ACP connect (иногда называется автономным соединением autonomic connect).

ACP connect - это настроенный на уровне интерфейса обход для подключения доверенных узлов, не относящихся к ACP. Узел ACP, на котором настраивается ACP connect, называется краевым узлом ACP. Через ACP connect плоскость ACP становится доступной для узлов не-ACP (таких, как системы NOC) без поддержки на нихх обнаружения или организации защищённых каналов ACP. Это называют естественным (native) доступом в ACP, поскольку для систем NOC интерфейс выглядит как обычный сетевой интерфейс без защищённого канала ACP, инкапсулирующего трафик.

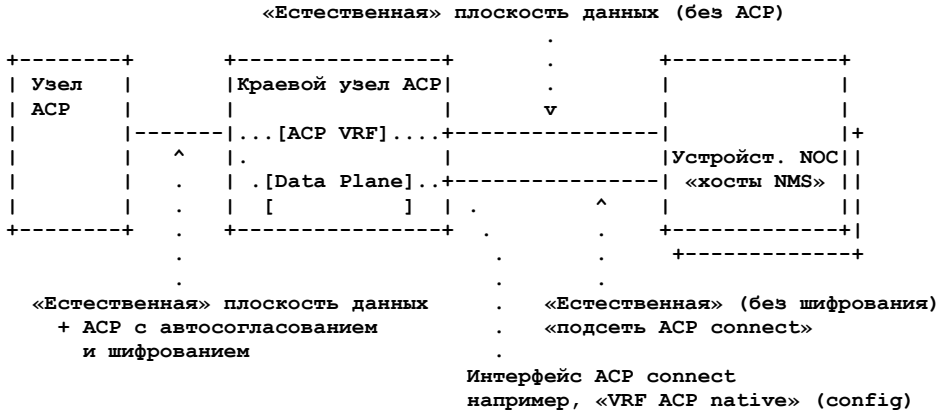

Рисунок 14. ACP Connect.

ACP connect влияет на безопасности, все системы и процессы, подключённые через ACP connect, получают доступ ко всем узлам ACP в плоскости ACP без дополнительной аутентификации. Таким образом, интерфейс ACP connect и подключённые к нему системы NOC должны контролироваться или защищаться физически. По этой причине описанные здесь механизмы явно не включают опций, позволяющих подключить маршрутизатор не-ACP через интерфейс ACP с маршрутизацией внутрь ACP.

Наличие физического контроля и/или защиты означает, что злоумышленники не могут получить доступ к физическому устройству, поддерживающему граничный узел ACP, физическим интерфейсам и каналам ACP, а также физическим устройствам, поддерживающим NOC. В простом случае граничный узел ACP и устройство NOC размещаются в помещении с контролируемым доступом, таком как NOC, куда злоумышленники попасть не могут.

Интерфейс ACP обеспечивает исключительный доступ только к плоскости ACP. Этого может быть недостаточно для многих хостов NMS. Им потребуется второй интерфейс «плоскости данных» вне ACP для связи между хостом NMS и администраторами, службами Internet или для прямого доступа к плоскости данных. В документе Using Autonomic Control Plane for Stable Connectivity of Network OAM [RFC8368] более подробно рассмотрены способы интеграции ACP в смешанную среду NOC.

На интерфейсе ACP connect **следует** использовать адрес/префикс IPv6 из субсхемы Manual (6.11.4. Субсхема ручной адресации ACP (ACP-Manual)), позволяющий оператору настроить, например, лишь Subnet-ID и автоматически получить оставшуюся часть адреса/префикса. **Не следует** использовать префикс, который маршрутизируется за пределы ACP, чтобы адреса чётко указывали, используются ли они внутри ACP.

Префикс ACP connect для подсетей **должен** распространяться краевым узлом ACP в протокол маршрутизации ACP (RPL). Хост NMS **должен** подключаться к префиксам из таблицы маршрутизации ACP через интерфейс ACP connect. В простом случае, где ACP использует лишь 1 префикс ULA и все подсети ACP имеют охватываемые им префиксы, хост NMS может полагаться на [RFC6724] для определения маршрутов с наибольшим совпадением префикса к разным своим интерфейсам, ACP и плоскости данных. С [RFC6724] хост NMS будет выбирать интерфейс ACP connect для всех адресов из ACP, поскольку любые адресаты в ACP будут давать максимальное совпадение с адресом интерфейса ACP. Если интерфейс ACP connect хоста NMS использует иной префикс или в ACP применяется несколько префиксов ULA, хосту NMS потребуются (статические) маршруты к интерфейсам ACP для этих префиксов.

Когда краевой узел ACP получает пакет от интерфейса ACP connect, он **должен** пересылать пакет в ACP лишь при наличии в нем адреса отправителя IPv6 от этого интерфейса (это иногда называют пересылкой по обратному пути - Reverse Path Forwarding или RPF). Это правило фильтрации **можно** изменить административно. Расширение доступности узлов не-ACP таким способом может создавать проблемы безопасности для ACP.

Для ограничения влияния ACP connect на безопасность поддерживающим такой интерфейс узлам **следует** реализовать механизм защиты, позволяющий настраивать и/или использовать интерфейсы ACP лишь на узлах, явно предназначенных для такого развёртывания (физически защищённые места, такие как NOC). Например, регистратор может запретить возможность включения ACP connect на устройствах в процессе зачисления и это можно будет изменить лишь при повторном зачислении (A.9.5. Назначение роли).

Граничным узлам ACP **следует** иметь опцию настройки для запрета пакетов с заголовками RPI (6.12.1.13. Информационный пакет RPL) через интерфейс ACP connect. Эти заголовки выходят за рамки профиля RPL в данной спецификации, но могут применяться в будущих расширениях.

8.1.2. Программные компоненты

В предыдущем параграфе предполагалось, что краевой узел ACP и устройства NOC являются разными физическими устройствами, а интерфейс ACP является физическим сетевым соединением. Здесь рассматривается случай, когда эти компоненты являются программами на одном физическом устройстве.

Механизм ACP connect может служить для соединения ACP не только с внешними физическими системами (хосты NMS), но и с приложениями, контейнерами, виртуальными машинами. На практике одним из возможных путей решения проблем безопасности внешнего интерфейса ACP connect является совместное размещение краевого узла ACP и хоста NMS, сделав один контейнером или виртуальной машиной внутри другого. В этом случае незащищённая внешняя подсеть ACP становится внутренней виртуальной подсетью на том же устройстве. В конечном итоге это ведёт к созданию хоста NMS с полной поддержкой ACP при минимальном воздействии на программную архитектуру хоста NMS. Такой подход не ограничивается хостами NMS и может также применяться к устройствам, содержащим одну или несколько виртуальных сетевых функций (VNF), - внутренней виртуальной подсети, соединяющей out-of-band-интерфейсы VNF с краевым маршрутизатором ACP (VNF).

Основное требование состоит в том, что программные компоненты должны разрешать доступ в ACP и могут разрешать доступ в плоскость данных. Как и в физическом решении для хостов NMS, это можно реализовать через 2 внутренних виртуальных сети - одна для подключения к ACP (может быть контейнером или виртуальной машиной), другая (другие) - к плоскости данных.

Такое «внутреннее» применение ACP connect не следует считать обходом, поскольку в этом случае можно организовать корректную модель безопасности - не требуется полагаться на непроверяемые внешние механизмы защиты, как в случае с внешними хостами NMS. Вместо этого может выполняться организация (оркестровка) ACP, виртуальных подсетей и программных компонентов доверенными программами, которые можно считать частью ANI (или даже расширенной ACP). Эти программные компоненты отвечают за обеспечение доступа к виртуальной подсети лишь доверенных программных компонентов, а к виртуальной подсети ACP и плоскости данных - ещё более доверенные (поскольку через них возможны утечки между ACP и плоскостью данных). Такое доверие можно организовать, например, в помощью криптографии, такой как подписи программных пакетов.

8.1.3. Автонастройка

Краевым узлам ACP, хостам NMS и программным компонентам, предназначенным, как описано выше, для соединения через виртуальные интерфейсы, **следует** поддерживать SLAAC [RFC4862] в подсети ACP connect и автоматическую настройку маршрутов в соответствии с Default Router Preferences and More-Specific Routes [RFC4191].

Краевой узел ACP действует как маршрутизатор для ACP в подсети ACP connect, предоставляя настраиваемый (автоматически) префикс для подсети ACP connect и создаваемые (автоматически) маршруты из ACP к хостам NMS и/или программным компонентам. Краевой узел ACP использует опцию маршрутной информации (Route Information Option или RIO) из [RFC4191] для анонсирования агрегированных префиксов для адресных префиксов ACP (с номинальными сроками действия RIO). Кроме того, краевой узел ACP применяет RIO для анонсирования принятого по умолчанию маршрута (::/0) со сроком действия 0.

Эти RIO позволяют подключать хосты типа C с ACP через подсеть ACP connect на одном интерфейсе и другую сеть (плоскость данных или сеть NMS) на том же или другом интерфейсе хоста типа C, полагаясь на маршрутизаторы, отличные от краевого узла ACP. RIO гарантируют, что эти хосты будут маршрутизировать краевому ACP узлу лишь префиксы, применяемые в ACP.

Хосты типа A и B игнорируют RIO и будут считать узел ACP своим маршрутизатором по умолчанию для всех адресатов. Этого достаточно, когда хосту типа A или B нужно лишь соединение с ACP, но не с другими сетями. Подключение хоста типа A или B к ACP и другим сетям требует явной настройки маршрута для префикса ACP на хосте или комбинированном интерфейсе ACP и плоскости данных на краевом узле ACP (8.1.4. Комбинированный интерфейс ACP и плоскости данных (VRF Select)).

Агрегированный префикс означает, что краевому узлу ACP нужно анонсировать лишь префикс ULA /48, используемый в ACP, а не фактические маршруты /64 (сбсхема Manual), /127 (субсхема Zone), /112 мом /120 (субсхема Vlong) реальных узлов ACP. Если интерфейсы ACP настроены с отличными от ULA префиксами, эти префиксы невозможно агрегировать без дополнительной настройки политики на краевом узле ACP. Это объясняет приведённую выше

рекомендацию применять префиксы ACP ULA для интерфейсов ACP connect для сокращения списка префиксов, анонсируемых через [RFC4191] хостам NMS и программным компонентам.

Краевой узел ACP с адресом ACP Vlong **может** выделять подсети из скоего префикса /112 или /120 интерфесам ACP connect для исключения необходимости неавтономной настройки и/или предоставления адресных префиксом таким интерфейсам ACP connect.

8.1.4. Комбинированный интерфейс ACP и плоскости данных (VRF Select)

Использование двух физических и/или виртуальных подсетей (и интерфейсов) для хостов NMS (8.1.1. Контроллер или NMS без поддержки ACP) или программ (8.1.2. Программные компоненты) может казаться усложнённым, например, с унаследованными хостами NMS, поддерживающими лишь 1 интерфейс IP, или недостаточным для поддержки хостов типа A или B [RFC4191] (8.1.3. Автонастройка).

Для обеспечения единой подсети ACP и плоскости данных узлу ACP требуется демультиплексировать пакеты от хостов NMS в ACP VRF и плоскость данных. Это иногда называют выбором VRF (VRF select). Если адреса ACP VRF не перекрываются с адресами IPv6 в плоскости данных (перекрытия следует избегать), эта функция может использовать адрес получателя IPv6. Проблема состоит в выборе адреса источника на хостах NMS в соответствии с [RFC6724].

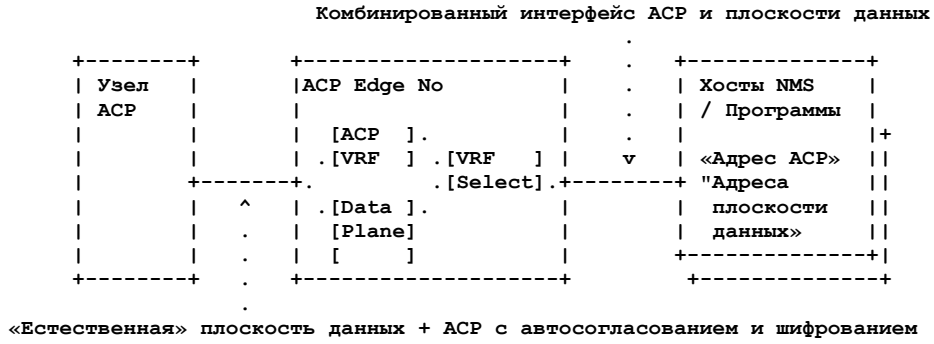

Рисунок 15. VRF Select.

Рассмотрим простой случай, где ACP использует лишь 1 префикс ULA, а префикс ACP IPv6 для комбинированного интерфейса ACP и плоскости данных охватывается этим префиксом ULA. Краевой узел ACP анонсирует префикс ACP IPv6 и 1 или несколько префиксов для плоскости данных. Без дополнительной настройки правил на хостах NMS, они могут выбрать свои адреса ACP как адреса отправителя для получателей ULA в плоскости данных в соответствии с правилом 8 (раздел 5 в [RFC6724]). Краевой узел ACP может передать пакет плоскости данных, но адрес отправителя из ACP не следует применять для плоскости данных и обратные пакеты могут не прийти. Если ACP передаёт несколько префиксов ULA или не являющийся ULA префикс ACP, выбор адреса отправителя становится более проблематичным.

С раздельными подсетями ACP connect и плоскости данных, а также анонсами префиксов [RFC4191], которые маршрутизируются через интерфейс ACP будет применяться выбор адреса отправителя по правилу 5 (адрес выходного интерфейса) из раздела 5 в [RFC6724], чтобы указанные выше проблемы не возникали даже в более сложных случаях множества префиксов ULA и других (не-ULA) префиксов в таблице маршрутизации ACP.

Чтобы достичь такого же поведения с комбинированным интерфейсом ACP connect и плоскости данных, краевой узел ACP должен вести себя как два отдельных маршрутизатора на интерфейсе - один (маршрутизатор/адрес) IPv6 link-local для достижимости ACP, другой - для достижимости плоскости данных. Анонсы маршрутизаторов (Router Advertisement или RA) для обоих описаны в параграфе 8.1.3 - для ACP анонсируется префикс ACP с опцией префикса [RFC4191], маршрутизируемой через ACP, и нулевым сроком действия для отмены этого next hop как принятого по умолчанию маршрутизатора. Для плоскости данных анонсируются префиксы вместе с параметрами принятого по умолчанию маршрутизатора плоскости данных.

В результате выбор адреса источника по правилу 5.5 из раздела 5 в [RFC6724] может приводить к корректному поведению выбора адреса источника хостами NMS без дополнительной настройки, что и при отдельных интерфейсах ACP connect и плоскости данных на хосте. Как указано в правиле 5.5 из раздела 5 в [RFC6724], это **может** происходить лишь потому, что от хостов IPv6 не требуется отслеживать информацию next-hop. Если хост NMS не делает этого, предпочтительным методом подключения будут раздельные интерфейсы ACP connect и плоскости данных. Хостам, реализующим First-Hop Router Selection by Hosts in a Multi-Prefix Network [RFC8028], следует (вместо может) реализовать правило 5.5 из раздела 5 в [RFC6724], поэтому для хостов предпочтительно поддерживать [RFC8028].

Краевые узлы ACP **могут** поддерживать комбинированный интерфейс ACP и плоскости данных.

8.1.5. Использование GRASP

GRASP можно и следует применять на интерфейсах ACP connect, особенно в архитектурно корректных решениях, когда протокол служит для подключения программ (например, ASA или унаследованных приложений NMS) к ACP.

С учётом того, что ACP служит защитной транспортной подложкой для GRASP, требования состоят в том, чтобы устройства, подключённые через ACP были защищены так же (или лучше), как узлы ACP, не применяющие ACP connect, и чтобы на них работали лишь программы, защищённые так же (или лучше), заведомо не вредоносные, и подобающим образом спроектированные для изоляции ACP от внешнего оборудования.

Различия в безопасности заключаются в том, что криптографическая защита каналов ACP заменяется требованием физической защиты и/или контроля сетевых соединений между краевым узлом ACP и NMS или другим хостом, доступным через интерфейс ACP (см. 8.1.1. Контроллер или NMS без поддержки ACP).

При использовании комбинированного интерфейса ACP и плоскости данных, нужно следить, чтобы краевые узлы ACP пересылали лишь сообщения GRASP, принятые от программ или хостов NMS и предназначенные для домена ACP GRASP. В настоящее время не определено подложки для защиты и транспорта GRASP помимо ACP, поэтому не задано, какие программы и хосты NMS могут участвовать в двух разных доменах GRASP через одну подсеть (домены ACP и плоскости данных). Сейчас предполагается, что все пакеты GRASP на комбинированном интерфейсе ACP и

плоскости данных относятся к домену GRASP ACP. В них **следует** использовать адреса ACP IPv6 для программ и хостов NMS. Адреса IPv6 link-local программ и хостов NMS (для сообщений GRASP M_DISCOVERY и M_FLOOD) предполагаются относящимися к пространству адресов ACP.

8.2. Соединение островков ACP через сети L3 без ACP (удалённые соседи)

Не все узлы в сети могут поддерживать ACP. Если между узлами ACP имеются устройства L2, не поддерживающие ACP, плоскость ACP будет работать через них, поскольку она основана на IP. Однако автономное обнаружение соседей ACP через DULL GRASP предназначено лишь для работы через соединения L2, а этого недостаточно для создания соединений ACP через устройства L3 без поддержки ACP.

8.2.1. Настроенный удалённый сосед ACP

На узле ACP удалённые соседи задаются явно. Параметры такого «соединения» показаны ниже в форме ABNF. Синтаксис не является нормативным (нет стандарта для настройки) лишь иллюстрирует параметры, указывая необязательные.

```
connection = method "," local-addr "," remote-addr [ "," pmtu ]
method =    "any"
           / ( "IKEv2" [ ":" port ] )
           / (  "DTLS"  [ ":"  port ] )
port = 1*DIGIT
local-addr  = [ address  [ ":" vrf  ] ]
remote-addr =   address
address =  "any"
           / IPv4address / IPv6address  ; Из [RFC5954]
vrf = system-dependent ; Имя VRF для локального адреса
```

Рисунок 16. Параметры для удалённых соседей ACP.

Явная настройка удалённого партнёра в соответствии ABNF обеспечивает все сведения для организации защищённого канала без организации туннеля к партнёру и запуска DULL GRASP в нем. Конфигурация включает все параметры, которые иначе пришлось бы передавать через DULL GRASP - локальный адрес, удалённый (партнерский) локатор и метод. Отличия от локального обнаружения через DULL GRASP перечислены ниже.

- Адреса могут быть IPv4 или IPv6 и обычно являются глобальными динамическими адресами.
- Можно указать VRF (где находится local-addr) для организации соединения. Если параметр vrf не задан, предполагается принятый по умолчанию экземпляр VRF на узле. В DULL GRASP под VRF подразумевается интерфейс, через который работает DULL GRASP.
- Если для локального адреса задано значение any, используемый при организации безопасного канала локальный адрес определяется выбором адреса источника ([RFC6724] для IPv6). На стороне ответчика прослушиваются все адреса узла в выбранном экземпляре VRF.
- Указание порта нужно лишь для методов, где порт не задан по умолчанию (например, DTLS).
- Если для удалённого адреса задано значение any, соединение будет лишь ответчиком. Это концентратор (hub), который может использоваться несколькими удалёнными партнёрами для одновременного соединения без необходимости знать и настраивать адреса. Примером служит сайт-хаб для сайтов-лучей, доступных через Internet.
- Параметр pmtu следует делать настраиваемым, чтобы преодолеть проблемы и ограничения определения MTU для пути (Path MTU Discovery или PMTUD).
- IKEv2/IPsec для удалённых партнёров следует поддерживать необязательные процедуры для работы через NAT (NAT Traversal или NAT-T).

8.2.2. Туннельный удалённый сосед ACP

Между удалёнными партнёрами ACP задаётся имеющийся туннель IP-in-IP, GRE и т. п., а представляющие туннель виртуальные интерфейсы настраиваются для поддержки ACP (ACP enable). Это активирует адреса IPv6 link-local и DULL для туннеля. В результате туннель служит для обычного обнаружения кандидата в соседи ACP по смежности L2 с помощью DULL и защищённый канал организуется, как описано выше.

Для туннелируемого удалённого соседа ACP нужны 2 инкапсуляции - настроенный туннель и защищённый канал в этом туннеле. Это делает механизм менее желательным, нежели настройка удалённого партнёра. Преимуществом туннеля является простота реализации, поскольку не требуется менять функциональность ACP, просто работа выполняется через виртуальный (туннельный) интерфейс вместо естественного. Туннель может обеспечивать PMTUD, а защищённый канал не делает этого. Туннельный механизм может не работать через некоторые межсетевые экраны, а защищённому каналу они не мешают.

Туннелирование с незащищённой инкапсуляцией в среднем повышает риск MITM-атак «на понижение (downgrade) в пути. В таких случаях MITM фильтрует пакеты для всех вариантов защищённого канала ACP, кроме наименее защищённых, чтобы атаковать их. Узлам ACP, поддерживающим туннельное соседство, **следует** обеспечивать настройку туннельных интерфейсов для ограничения или явного выбора протоколов защищённого канала ACP (если узел ACP поддерживает более одного такого протокола).

8.2.3. Заключение

Удалённые соседи менее «нерушимы» нежели смежные по L2 соседи ACP, использующие адреса link-local, поскольку они зависят от операций плоскости данных, таких как маршрутизация и глобальная адресация. Тем не менее, эти варианты могут быть очень важны для развёртывания ACP, особенно при необходимости соединять «островки» через Internet. Реализациям **следует** поддерживать хотя бы туннельных соседей ACP через протокол GRE, который сегодня представляется наиболее распространенным для туннелей между маршрутизаторами.

9. Операции ACP (информационный раздел)

В следующих параграфах описаны важные эксплуатационные аспекты ACP. Этот текст не является нормативным, поскольку он не влияет на взаимодействие между компонентами ACP, но он включает рекомендации и/или требования к внутренним моделям работы, полезным или требуемым для достижения желаемых результатов применения ACP (см. 3. Примеры использования ACP (информационный раздел)).

- В параграфе 9.1 описаны рекомендуемые возможности диагностики узлов ACP оператором.
- В параграфе 9.2 приведено общее описание требований к работе регистратора ACP, параметров конфигурации и конкретных аспектов, влияющих на выбор варианта развёртывания. Рассмотрена модель, где регистраторы ACP имеют свой суб-CA для более распределенного варианта развёртывания регистраторов ACP, а также даны рекомендации по централизованному управлению правилами работы регистраторов ACP.
- В параграфе 9.3 описано предлагаемое поведение узла ACP и операционные интерфейсы (опции настройки) для управления ACP в так называемых устройствах зелёного (не настроенные ранее) и коричневого (заранее настроенные) поля.

Рекомендации и предложения этого раздела основаны на опыте эксплуатации с коммерчески доступными предстандартными реализациями ACP.

9.1. Диагностика ACP и BRSKI

Хотя ACP и ANI в целом устраняют многие ошибки ручной настройки за счёт автоматизации, важно обеспечить хорошую диагностику и для них. Базовая стандартизованная диагностика требует поддержки моделей (YANG), представляющих полное состояние (авто)настройки и работы для всех компонентов: GRASP, ACP и применяемой ими инфраструктуры, такое как TLS/DTLS, IPsec, сертификаты, TA, время, VRF и т. д. Это необходимо, но недостаточно.

Простое представление состояний компонентов не позволяет операторам быстро предпринимать действия, пока они не понимают, как интерпретировать данные, что может означать необходимость глубокого понимания всех компонентов и их взаимодействий в ACP/ANI. Поддержка диагностики должна помогать быстро получить ответы на ожидаемые вопросы операторов, такие как: «ACP работает корректно?» или «Почему нет соединения ACP с известным соседом?». В современных подходах к управлению сетями логика ответов на такие вопросы чаще всего встроена в централизованные программы диагностики, использующие упомянутые выше модели данных. Хотя такой подход возможен для использующих ANI компонентов, его недостаточно для диагностики самих ANI, как указано ниже.

- Для разработки логики выявления общих проблем нужен опыт работы с компонентами ANI. Определение своего анализа каждой системой управления неэффективно.
- При некорректной работе ANI удалённая диагностика может стать недоступной из-за отсутствия связности. Поэтому в ANI следует иметь локально доступные средства диагностики на самих узлах.
- Некоторые операции сложно или невозможно контролировать в реальном масштабе времени, например, проблемы с начальной загрузкой в сети при отсутствии возможности подключить локальную диагностику. Поэтому важно определить, как собрать (log) диагностику локально для последующего извлечения. В идеале такие записи должны быть энергонезависимыми, чтобы они сохранялись при отключении питания, например, когда устройство, которое не удалось запустить автоматически (zero-touch) передаётся для диагностики в более подходящее место.

Простейшей формой диагностики для ответа на вопросы, подобные приведённым выше, является последовательное представление имеющих отношение к делу сведений в порядке зависимости, где первый неожиданный и/или неработающий элемент является наиболее вероятной причиной отказа, или просто регистрация и/или выделение такого элемента. Примеры приведены ниже.

Вопрос. Может ли ACP воспринимать соединения от соседей?

- Проверяется корректность настройки рабочего состояния ACP/ANI (9.3. Включение и отключение ACP и ANI).
- Выглядит ли системное время правдоподобным? Может быть это устанавливаемое по умолчанию время в результате отказа батареи в часах? Проверка сертификатов зависит от корректности времени.
- Есть ли на узле ключевой материал, такой как сертификаты домена, TA и т. п.?
- Если ключевого материала нет и ANI включена, проверяется состояние BRSKI (не детализировано в примере).
- Проверяется действительность сертификата домена.
  - Проверяется ли сертификат в TA?
  - Сертификат не отозван?
  - Была ли успешна последняя попытка получить CRL (актуальны ли сведения CRL)?
  - Действителен ли сертификат? Начало действия сертификата в прошлом, а завершение в будущем?
  - Есть ли в сертификате корректно сформированное поле acp-node-name?
- Удалось ли создать ACP VRF?
- Включена ли ACP на одном или нескольких интерфейсах, которые включены и работают?

Если все указанные проверки прошли, ACP следует работать локально и нужно проверить связи с соседями ACP.

Вопрос. Почему узел не создал работающее соединение ACP с соседом по интерфейсу?

- Интерфейс физически активен? У него есть адрес IPv6 link-local?
- На интерфейсе разрешена плоскость ACP?

- Удаётся ли передать сообщения DULL GRASP на интерфейс? (Есть ли ошибки канального уровня?)
- Принимаются ли сообщение DULL GRASP на интерфейсе? Если нет, проблемы могут быть связаны с промежуточными устройствами L2, плохо отслеживающими MLD. Следует провести диагностику, например, устройства MLD, запрашивающего адрес IPv6 и MAC.
- Видна ли цель ACP в каком-либо сообщении DULL GRASP от интерфейса? Диагностика поддерживаемых методов защиты канала.
- Известен ли MAC-адрес соседа с целью ACP? Если нет, проверяется состояние SLAAC/ND.
- Когда была последняя попытка организовать защищённый канал ACP к соседу?
- Если такая попытка была неудачно проверяются указанные ниже условия.
  - Один из участников закрыл соединение из-за отказа при проверке сертификата принадлежности к домену?
  - Если соединение закрыл сосед, нужна диагностика протокола защиты канала.
  - Если причину выяснить не удалось, нужно исследовать локальны причины.
    - У соседей нет общего протокола защиты канала (это невозможно при соответствии данной спецификации, требующей поддержки IPsec).
    - Проверка сертификата принадлежности к ACP (6.2.3. Проверка принадлежности к домену ACP) завершилась отказом?
      - Сертификат соседа на подписан напрямую или опосредовано одной из точек TA. Выполняется диагностика TA it (сожно узнать, кому принадлежит устройство).
      - Сертификат соседа относится к другому домену (или домена в нем нет). Проверяется acp-domain-name и, возможно, другие сведения из сертификата.
      - Сертификат соседа отозван или не может быть аутентифицирован OCSP.
      - Срок действия сертификата соседа истёк или ещё не начался.
  - Есть ли другие проблемы соединения, например IKEv2/IPsec, DTLS?

Вопрос. Работает ли ACP по защищённым каналам корректно?

- Есть ли один или несколько активных соседей ACP с защищёнными каналами?
- Работает ли RPL для ACP?
- Есть ли в таблице маршрутизации ACP принятый по умолчанию маршрут к корню?
- Есть ли маршрут для каждого прямого соседа ACP, недоступного через виртуальный интерфейс ACP к корню?
- Работает ли ACP GRASP?
- Кэширована ли хотя бы одна цель SRV.est (для поддержки обновления сертификатов)?
- Есть ли в кэше хотя бы одна цель регистратора BRSKI (если BRSKI поддерживается)?
- Нормально ли работает BRSKI-прокси на всех интерфейсах, где работает ACP?

Эти списки не являются полными, но они иллюстрируют принцип и возможность наличия разных проблем, начиная от обычных операций (сосед в другом домене ACP) и заканчивая проблемами поддержки свидетельств (срок действия сертификатов), явными защитными действиями (отзыв) или неожиданными проблемами связности (промежуточное оборудование L2). Показана возможность диагностики ANI путём пассивного наблюдения за рабочим состоянием компонентов, включая историю, кэширование и/или учёт событий. Для надёжной диагностики этого может быть недостаточно.

Компоненты ACP и BRSKI учитывают требования безопасности, но не пытаются обеспечить диагностику для построения самой сети. Ниже приведены два примера.

1. BRSKI не позволяет соседнему устройству идентифицировать сертификат IDevID у заявителя. Это может делать лишь выбранный регистратор BRSKI, но распространение сведений о нежелательных заявителях узлам от регистраторов BRSKI может быть затруднено.
2. LLDP распространяет сведения об узлах, такие как модель, тип, имя программы или интерфейса, число соединений с прямыми соседями. Эти сведения зачастую полезны или необходимы для диагностики сети. Однако их можно считать небезопасными, поскольку информация передаётся без защиты все соседям.

«Заинтересованная смежная сторона» всегда может определить сертификат IDevID заявителя BRSKI, действуя как посредник или регистратор BRSKI. Поэтому сертификат IDevID заявителя BRSKI не предназначен для защиты, его можно запросить и он не передаётся без запроса (как в LLDP), чтобы другие наблюдатели в сети могли определить, кто является «заинтересованной смежной стороной».

9.1.1. Диагностика партнёра по защищённому каналу

При взаимной проверке подлинности сертификатов не требуется явно передавать сертификаты TA, поскольку для проверки цепочки сертификации достаточно их хэш-значений. При организации защищённого канала ACP это ведёт к ограничению диагностики в случае отказа из-за несоответствия TA. Поэтому параграф 6.8.2 рекомендует включать сертификат TA в сигнализацию защищённого канала. Следует делать это без изменения протоколов защищённой связи, применяемых ACP. В [RFC7296] это не упоминается, но и не запрещено.

Одним из распространённых случаев, когда диагностика за счёт передачи TA кандидата в партнёры очень полезна, является среда с множеством арендаторов, такая как офисный центр, где разные арендаторы организуют свои сети и

ACP. Каждому арендатору предоставляется предположительно автономная связность L2 через инфраструктуру здания. В таких средах часто наблюдаются ошибки, в результате которых устройство получает связность L2 с сетью не того арендатора. Хотя это не влияет на ACP, это может сказаться на плоскости данных. Поэтому важно иметь возможность диагностики такой нежелательной связности из ACP, чтобы любые автономные и неавтономные механизмы настройки плоскости данных могли подобающим образом обрабатывать такие интерфейсы. Сведения из TA партнёра могут помочь при устранении таких неполадок.

Другим примером служит преднамеренная или нечаянная реактивация оборудования, такого как взятые со склада резервные устройства с истекшим сертификатом TA.

Ещё один случай связан со слияниями или приобретениями, когда узлы ACP не представлены должным образом точкам TA ранее раздельных ACP. Это предполагает, что имена доменов ACP уже согласованы и отказ при проверке принадлежности к домену ACP связан лишь с TA.

Четвёртый пример связан с наличием нескольких регистраторов для одной плоскости ACP без корректной организации общей точки TA. Это может возникать при поддержке регистраторами CA, настроенных как TA, а промежуточный CA.

9.2. Регистраторы ACP

Как описано в параграфе 6.11.7. Регистраторы ACP, механизм адресации ACP предназначен для облегчённых, распределенных и некоординируемых регистраторов ACP, предоставляющих адресные префиксы ACP узлам-кандидатам в ACP путём зачисления их по сертификатам ACP в домен ACP с помощью подходящего механизма и/или протокола (не обязательно автоматизированного). В этом параграфе приведено неформальное описание деталей и вариантов для регистраторов ACP.

9.2.1. Взаимодействие регистраторов

В этом параграфе обсуждаются и обобщаются взаимодействия с другими элементами, требуемые регистратором ACP.

В простых экземплярах сети ACP не требуется центрального компонента NOC, помимо TA. Обычно это корневой CA. Можно установить 1 или некоординируемых самостоятельно регистраторов ACP с описанным ниже взаимодействием.

Для оркестровки автоматического зачисления узлов кандидатов в ACP регистратор ACP может полагаться на ACP и применять прокси для доступа к узлу-кандидату, что позволяет обойтись минимальными, имеющимися настроенными (заранее) сетевыми службами на узле-кандидате. BRSKI определяет BRSKI-прокси, который можно приспособить для разных протоколов, которые заявители и/или узлы-кандидаты ACP могут применять, например, BRSKI через CoAP (Constrained Application Protocol) или посредничество для NETCONF.

Для доступа к точке TA, не связанной с ACP, регистратор ACP использует плоскость данных. ACP и плоскость данных в регистраторе ACP могут (по умолчанию это следует делать) быть полностью изолированы на сетевом уровне. Доступ к обеим транспортным сетям нужен лишь таким приложениям, как регистраторы ACP.

При неавтономном зачислении сначала нужно настроить плоскость данных между регистратором ACP и узлом-кандидатом в ACP. Это включает регистратор ACP и узел-кандидат. Затем можно использовать любой подходящий протокол между регистратором и узлом-кандидатом для обнаружения другой стороны с последующим соединением и зачислением (настройкой) кандидата в ACP по сертификату ACP. Например, для этого может служить протокол NETCONF Zero Touch (Secure Zero Touch Provisioning (SZTP) [RFC8572]). BRSKI с дополнительными механизмами обнаружения тоже подходит для узлов-кандидатов, пытающихся зачислить себя в ACP через сеть без поддержки ACP, например, Internet.

Когда узел-кандидат в ACP, такой как заявитель BRSKI, использует защищённую начальную загрузку, он не будет доверять конфигурации и/или зачислению через сеть, пока ему не представлен ваучер (A Voucher Artifact for Bootstrapping Protocols [RFC8366]) подтверждающий подлинность сети в части владения узлом. Регистратору ACP потребуется метод получения такого ваучера через сеть или иным путём (offline) от агентства MASA (Manufacturer Authorized Signing Authority). Протоколы BRSKI и NETCONF Zero Touch имеют возможность предоставления ваучера узлу-кандидату в ACP.

Регистратор ACP может применять EST для отзыва сертификатов ACP и/или выступать как точка распространения CRL. Узлу, оказывающему такие услуги, не нужно выполнять (начальное) зачисление, но от него требуется описанная выше связность, как от регистратора ACP (через ACP с узлами ACP и через плоскость данных с TA и иными источниками CRL).

9.2.2. Параметры регистратора

Взаимодействия регистраторов ACP, описанные в параграфах 6.11.7 и 9.2.1, зависят от указанных ниже параметров.

- URL для TA и свидетельства, чтобы регистратор ACP мог разрешить TA подписывать сертификаты узлов ACP.
- Имя домена ACP.
- Registrar-ID для использования. По умолчанию это может быть MAC-адрес регистратора ACP.
- Следующие пригодные Node-ID для субсхем Zone (Zone-ID 0) и Vlong (/112 и /120) при восстановлении. Эти идентификаторы нужны лишь при восстановлении после отказа. Могут потребоваться иные механизмы для запоминания идентификаторов в резервном месте или восстановления от известных узлов ACP.
- Правила предоставления сертификатов (например, сертификата домена) узлам-кандидатам ACP на основе сертификата IDevID как в BRSKI. Регистратор ACP может создавать «белые» или «черные» списки на основе атрибута serialNumber [X.520] в поле кодирования субъекта отличительного имени в его сертификате IDevID.
- Правила выбора типа адресного префикса для устройства-кандидата ACP, вероятно на основе тех же данных.
- Для BRSKI или иного механизма с ваучерами - параметры для определения способа извлечения ваучеров для конкретного типа защищённой загрузки узла-кандидата в ACP (например, MASA URL), пока эти сведение не получены автоматически, например, из сертификата IDevID узла-кандидата в ACP (как задано в BRSKI).

9.2.3. Отзыв и ограничения сертификатов

Когда узел ACP обновляет сертификат и/или меняет его ключи, он в конечном итоге может сделать это через другого регистратора (например, сервер EST), нежели тот, от которого был получен сертификат ACP, например, по причине ухода того регистратора ACP. Регистратор ACP, через которого выполнено обновление или смена ключей, по умолчанию доверяет acp-node-name из текущего сертификата ACP узла ACP и поддерживает эту информацию, чтобы узел ACP сохранял свой адресный префикс ACP. При обновлении или смене ключей через EST текущий сертификат ACP узла ACP указывается в процессе согласования TLS. Этому простому сценарию присущи два ограничения.

1. Регистратор ACP не может напрямую назначать сертификаты узлам, поэтому нуждается в действующем подключении к TA.
2. Восстановление от скомпрометированного регистратора ACP затруднено. При компрометации регистратора ACP он может внедрить, например, конфликтующее значение acp-node-name и таким образом создать возможность атаки других узлов ACP через протоколо маршрутизации ACP.

Даже при обнаружении такого злонамеренного регистратора ACP решение проблемы может быть сложным из-за того, что потребуется идентифицировать все ложные сертификаты ACP, выданные через скомпрометированного регистратора ACP. Без дополнительного централизованного отслеживания выданных сертификатов это невозможно.

9.2.4. Регистраторы ACP с суб-CA

В ситуации, когда любое из двух указанных выше ограничений является проблемой, регистраторы ACP могут также быть суб-CA. Это снимает необходимость подключения к TA при каждом зачислении узла ACP и снижает потребность в подключении такого регистратора ACP к TAЮ требуя её лишь для обновления своего сертификата. Регистратор ACP будет применять свой (суб-CA) сертификат при зачислении и подписывании сертификатов узлов ACP, поэтому потребуется лишь отозвать сертификат суб-CA скомпрометированного регистратора ACP. Можно также дождаться завершения срока действия сертификата суб-CA и не обновлять его, когда этот срок достаточно короток.

Поскольку при проверке принадлежности к домену ACP проверяется цепочка доверия для сертификата ACP узла ACP, это включает и проверку сертификата подписи, который является скомпрометированным и/или отозванным сертификатом суб-CA. Поэтому включить в домен ACP узел ACP, зачисленный скомпрометированным и обнаруженным регистратором ACP, не получится.

Узлы ACP, зачисленные скомпрометированным регистратором ACP, автоматически не смогут организовать каналы ACP и обновить сертификат домена ACP через EST, поэтому вернутся в состояние кандидата в ACP и будут пытаться получить новый сертификат ACP от регистратора ACP, например, через BRSKI. В результате регистраторы ACP со связанным суб-CA упрощают изоляцию и решение проблем со скомпрометированными регистраторами.

Отметим, что регистраторы ACP с функциональностью суб-CA могут также более легко контролировать срок действия сертификатов ACP, поэтому могут служить как инструмент создания краткосрочных сертификатов и больше не полагаться на CRL, тогда как сертификаты этих суб-CA могут быть более долгосрочными и отзываемыми через CRL.

9.2.5. Централизованное управление политикой

При использовании нескольких регистраторов ACP без координации некоторые расширенные операции могут быть сложнее, чем с одной отказоустойчивой системой (backend) управления политикой. Примеры приведены ниже.

- Решение о включении узла-кандидата ACP в домен ACP. Это может быть решением, которое не нужно принимать заранее, чтобы политика для атрибута serialNumber в поле субъекта кодирования отличительного имени могла быть загружена в каждый регистратор ACP. Может оказаться лучше решать этот вопрос в реальном масштабе времени, включая возможное участие человека в NOC.
- Отслеживание всех зачисленных узлов ACP и сведений об их сертификатах, например, для поддержки отзыва сертификатов отдельных узлов ACP.
- Потребность в более гибких правилах в отношении типа адресного префикса и даже конкретного префикса, назначаемого узлу-кандидату в ACP.

Эти и другие операции можно было бы упростить введением централизованной системы управления политикой (Policy Management System или PMS) и смены поведения регистраторов ACP, чтобы они запрашивали у PMS любые решения о политике в процессе зачисления узлов-кандидатов в ACP и/или обновления сертификатов узлов ACP (например, выделяемый префикс ACP). Точно так же регистратор ACP будет сообщать PMS любую соответствующую информацию о смене состояния, например, при успешном зачислении сертификата на узле-кандидате ACP.

9.3. Включение и отключение ACP и ANI

Как для ACP, так и для BRSKI требуется достаточная работоспособность интерфейсов для поддержки передачи и приёма их пакетов. В узлах, где интерфейсы по умолчанию включены (например, без настройки конфигурации), как в большинстве коммутаторов L2, поведение будет меняться не столь сильно, как в большинстве устройств L3 (например, маршрутизаторов), где интерфейсы по умолчанию отключены. Однако почти во всех сетевых устройствах настройка конфигурации с физическим отключением интерфейсов ведёт к нарушению работы ACP.

В этом параграфе рассматривается предлагаемая модель работы для включения и отключения интерфейсов и узлов ACP/ANI с минимизацией риска прерывания работы ACP в результате действий оператора, а также минимизацией неожиданностей для оператора, когда активируется поддержка ACP/ANI в программах узла.

9.3.1. Фильтрация пакетов, не относящихся к ACP/ANI

Всякий раз, когда в этом документе упоминается включение интерфейса для ACP (или BRSKI), требуется лишь разрешение интерфейсу передавать и принимать данные, необходимые для работы ACP (или BRSKI), но не иные пакеты данных. Если плоскость данных явно не настроена и не разрешена, все пакеты, не требуемые для ACP/BRSKI, следует фильтровать на входе и выходе.

Протоколы BRSKI и ACP требуют на интерфейсах лишь операции IPv6 link-local и DULL GRASP. Операции IPv6 link-local означают минимальную сигнализацию для автоматического назначения адреса IPv6 link-local и взаимодействия с соседями через него - SLAAC [RFC4862] и ND [RFC4861]. Когда устройство является заявителем BRSKI, оно может также требовать на интерфейсе соединений TCP/TLS с посредниками BRSKI. При наличии у интерфеса ключевого материала и работе ACP требуется поддержка пакетов DULL GRASP и пакетов, необходимых для механизмов организации защищённых каналов, например, пакетов IKEv2 и IPsec ESP или DTLS по адресу IPv6 link-local соседа ACP на интерфейсе. Нужны также пакеты TCP/TLS для функций BRSKI-прокси при поддержке BRSKI.

9.3.2. Состояние admin down

В большинстве сетевых устройств интерфейсы имеют хотя бы два состояния - up (включён) и down (отключён). Имена состояний могут зависеть от конкретного устройства, например, down иногда называют shutdown, а up - no shutdown. Состояние down отключает все операции интерфейса на физическом уровне. Состояние up разрешает на интерфейсе работу всех возможных служб L2/L3 и может автоматически включать некоторые службы. Чаще всего операциями L2/L3 оправляют те или иные опции на уровне узла или интерфейса, но все они становятся доступными лишь в состоянии интерфейса, отличном от down. Поэтому самым простым способом деактивировать на интерфейсе все операции L2/L3 является перевод интерфейса с состояние down. Физическое отключение интерфейса во многих случаях является побочным эффектом, но иногда может быть важно само по себе (9.3.2.2. Быстрое распространение состояний и диагностика).

Распространённой проблемой при удалённом управления является прерывание оператором или контроллером SDN своей связности с уделенным узлом через конфигурацию, влияющую на настройку управляющего соединения с этим узлом. Плоскости ACP, как таковой, не следует иметь выделенной конфигурации, кроме упомянутого выше включения ACP на узлах с заранее настроенной плоскостью данных (brownfield). Это исключает конфигурации, не способные различать ACP и плоскость данных как источники ошибок в настройке, которые будут влиять на ACP, даже будучи нацеленными лишь на плоскость данных. Единственным распространенным типом команд, которые имеют такой побочный эффект, являются команды административного отключения интерфейса - down. Когда такая команда применяется к интерфейсу, через который ACP обеспечивает доступ для удалённого управления, это разрывает управляющее соединение через ACP, как отмечено выше, поскольку команда down обычно влияет на физический уровень,а не только на службы плоскости данных.

Для обеспечения устойчивости ACP/ANI к таким ошибкам оператора этот документ рекомендует разделить состояние down на admin down, где работа на физическом уровне сохраняется и ACP/ANI могут использовать интерфейс, и physical down. Существующие down-конфигурации будут отображаться на состояние admin down, которое имеющиеся службы L2/L3 не будут отличать от физического отключения. Для блокировки передачи и приёма каких-либо пакетов данных можно автоматически организовать фильтрацию пакетов, как описано в параграфе 9.3.1.

Примером трафика ANI (но не ACP), который следует разрешать даже в состоянии admin down, является трафик зачисления BRSKI между заявителем и посредником BRSKI.

Для перевода в состояние physical down при необходимости могут быть введены дополнительные опции (см. ниже). Эти опции следует снабжать дополнительными проверками для снижения риска ввода команд, приводящих к прерыванию работы ACP без автоматического восстановления. Примеры проверок включают запрет ввода опции из управляющего соединения (NETCONF/SSH), проходящего через сам интерфейс (не отключить себя) или применение опции после дополнительного подтверждения.

В последующих параграфах рассмотрены важные аспекты введения состояния admin down.

9.3.2.1. Безопасность

Интерфейсы отключают физически (или оставляют в принятом по умолчанию состоянии down) из соображений безопасности. Описанное выше состояние admin down также обеспечивает высокий уровень безопасности, поскольку оно разрешает лишь операции ACP/ANI, которые хорошо защищены. В конечном итоге безопасность развёртывания зависит от того, является ли admin down приемлемой заменой физическому отключению.

Необходимость доверять защите операций ACP/ANI нужно сравнивать с эксплуатационными преимуществами. Рассмотрим типовой пример клиентского оборудования (customer premises equipment или CPE), установленного там, где нет специалиста по сетям. Пользовательские порты устройств находятся в состоянии physical down, если явно не задано иное. В случае ошибочной конфигурации восходящее соединение (uplink) может быть некорректно подключено к этому порту. Устройство оказывается отключённым от сети и диагностика со стороны сети становится невозможной. Если же все порты находятся в состоянии admin down, плоскость ACP (но не плоскость данных) по-прежнему будет формироваться автоматически. Диагностика с сетевой стороны становится возможной и действия оператора могут восстановить работу uplink-порта или передать на сайт инструкцию по подключению через иной порт. С точки зрения безопасности атаковать можно лишь ACP/ANI, поскольку все прочие функции фильтруются на интерфейсе admin down.

9.3.2.2. Быстрое распространение состояний и диагностика

Состояние physical down на многих сетевых интерфейсах (например, Ethernet) передаётся другой стороне. Это ведёт к быстрой реакции протокола L2/L3 на той стороне. Состояние admin down будет давать такой же (быстрый) результат.

Насколько известно, перевод интерфейсов в состояние physical down, всегда является результатом действий оператора и никогда не происходит в результате действий автономных служб L2/L3 на узлах. Поэтому одним из вариантов является прекращение зависимости оператора от распространения состояний интерфейсов через канал подсети или физический уровень. Это может оказаться невозможным, когда каждая сторона управляется своим оператором, но в таких случаях маловероятна работа ACP по каналу и перевод интерфейса в состояние physical down остаётся хорошим решением.

В идеале быстрое распространение физического состояния заменяется быстрым распространением программно-управляемого состояния. Например, цель DULL GRASP admin-state можно использовать для автоматической настройки сессии BFD ("Bidirectional Forwarding Detection (BFD)" [RFC5880]) между двумя сторонами канала, которая будет распространять состояние up, а не admin down.

Переход в состояние physical down можно также использовать для диагностики проблем в кабелях при отсутствии более простых методов. Это сложней автоматической диагностики соседей, поскольку требует координации удалённого доступа (вероятно) к обеим сторонам канала, чтобы понять, вызовет ли переключения up/down такую же реакцию на удалённой стороне.

В параграфе 9.1 описано, как LLDP и диагностику через GRASP можно использовать для диагностики соседей, что может избавить от необходимости применять physical down для такой диагностики, если оба соседа поддерживают ACP/ANI.

9.3.2.3. Диагностика каналов на нижнем уровне

Состояние physical down служит для диагностики проблем на нижних уровнях, когда высокоуровневые службы (например, IPv6) не работают. Канала Ethernet особенно подвержены проблемам с соединениями, если они не поддерживают автоматического определения скорости (10/100/1000 Мбит/с), MDI-X и разъемы (когда интерфейс поддерживает несколько типов среды). Потребность в диагностике на нижних уровнях можно исключить при использовании автоматической настройки каналов. В дополнение к состоянию physical down диагностика на нижних уровнях Ethernet или других интерфейсов включает создание на интерфейсах иных состояний, таких как внутренние и внешние физические петли (loopback) или отключение передачи всех пакетов для отражения при рефлектометрии и/или измерении длины кабеля. Все эти варианты нарушают работу ACP.

Когда на работающем канале нужна такая диагностика, но канал критически важен для работы ACP, агенты ASA на обоих узлах могут выполнить согласованную диагностику, автоматически завершающуюся предопределённым способом без зависимости от внешнего ввода, обеспечивая восстановление работы канала.

9.3.2.4. Вопросы энергопотребления

Энергопотребление интерфейса в состоянии physical down может быть существенно меньше по сравнению с admin down, например на оптических интерфейсах для длинных линий. Включение интерфейсов, например, для проверки доступности также может потреблять дополнительную энергию. Это может сделать такие интерфейсы не подходящими для работы только в ACP, когда не требуется передачи в плоскости данных.

9.3.3. Включение ACP и ANI на уровне интерфейса

Опция ACP enable на уровне интерфейса разрешает на нем операции ACP, начиная с автоматического обнаружения соседей ACP через DULL GRASP. Опция ANI enable на уровне интерфейса узла, поддерживающего BRSKI и ACP запускает операции с заявителями BRSKI, когда на узле нет сертификата домена. На узлах ACP/BRSKI может потребоваться поддержка лишь опции ANI enable (без ACP enable).

Если это не переопределено глобальными параметрами конфигурации (параграф 9.3.4), любая из команд ACP enable и ANI (сокращённо ACP/ANI enable") заменят состояние down на интерфейсе состояним admin down.

9.3.4. Какие интерфейсы включать автоматически?

Параграф 6.4 требует автоматической установки ACP enable на естественных интерфейсах, но не на прочих (напомним, что естественными считаются интерфейсы, существующие без дополнительной настройки, такие как физические интерфейсы в физических устройствах). В идеале ACP enable автоматически устанавливается на всех интерфейсах, обеспечивающих дополнительную связность, которая позволяет достичь большего числа узлов в домене ACP. Лучший набор таких интерфейсов невозможно определить автоматически, поэтому выбор естественных интерфейсов является хорошим приближением.

Рассмотрим домен ACP из узлов ACP, транзитивно соединённых через естественные интерфейсы. Созданы туннели в плоскости данных между узлами, не являющимися прямыми соседями, и для этих туннелей установлено ACP enable. Протокол ACP RPL видит эти туннели как один интервал пересылки (hop). Маршруты в ACP будут использовать этот интервал как подходящий элемент пути для соединения смежных с туннелем областей. В результате фактические поэтапные (hop-by-hop) пути, используемые для трафика в ACP, могут ухудшаться. Кроме того, корректность пересылки в ACP становится зависимой от корректной пересылки в плоскости данных, включая QoS, фильтрацию и другую защиту на пути, по которому проходит туннель. По этой причине ACP/ANI enable не следует устанавливать автоматически на неестественных интерфейсах.

Если туннель связывает две ранее разделённые области ACP, он явно будет полезен для ACP. Туннель в плоскости данных может работать через узлы без ACP и обеспечивать дополнительную связность для уже подключённой сети ACP. Преимущество такой избыточности в ACP необходимо сопоставлять с проблемами, связанными с плоскостью данных. Если туннель соединяет две раздельные области ACP, сколько туннелей может потребоваться для достаточно надёжного соединения этих областей ACP? Между какими узлами? Это стандартные вопросы организации туннелирования, не связанные с ACP, и для них нет единого автоматизируемого решения. Вместо автоматической установки ACP enable для таких интерфейсов может потребоваться решение, основанное на цели применения неестественного интерфейса, и ACP enable потребуется установить в сочетании с механизмом, который создаёт и настраивает неестественный интерфейс.

В дополнение к явной установке ACP/ANI enable для неестественных интерфейсов требуется также задать стоимость канала ACP RPL, чтобы избежать проблем привлечения в канал излишнего трафика, как описано выше.

Даже естественные интерфейсы могут быть неспособны автоматически выполнять BRSKI или ACP, поскольку они могут требовать дополнительных действий оператора для своей работы. Примеры включают интерфейсы DSL, требующие свидетельств PPPoE (Point-to-Point Protocol over Ethernet), или мобильные интерфейсы, требующие свидетельств с SIM-карты. Какой би механизм ни применялся для обеспечения нужной конфигурации устройства для включения интерфейса, его можно расширить для решения вопроса об установке ACP/ANI enable.

Цель автоматической установки ACP/ANI на (любых) интерфейсах состоит в устранении ненужных «касаний» к узлу, чтобы сделать работу узла максимально близкой к zero-touch в части ACP/ANI. При наличии неизбежных действий, таких как создание и/или настройка неестественного интерфейса или предоставление свидетельств естественному интерфейсу ACP/ANI enable следует добавлять как часть такого действия. Если ошибочное «касание» легко исправить(без создания другого дорогостоящего касания), по умолчанию не следует включать ANI/ACP, а при сложном

или дорогом исправлении (например, параметры на SIM-карте, отправленное в далёкое место) следует по умолчанию включать ACP/ANI.

9.3.5. Включение ACP и ANI на уровне узла

Команда на уровне узла ACP/ANI enable [up-if-only] включает ACP или ANI на узле (ANI = ACP + BRSKI). Без этого набора команд все команды ACP/ANI enable на уровне интерфейсов игнорируются. После выполнения команды ACP/ANI будет работать на интерфейсах, гда задано ACP/ANI enable. Установка ACP/ANI enable на уровне интерфейса выполняется автоматически (по умолчанию) или явным действием оператора, как описано в параграфе 9.3.4.

Если использована опция up-if-only поведение интерфейсов с состоянии down не меняется и ACP/ANI будет работать лишь на интерфейсах, где задано ACP/ANI enable и интерфейс находится в состоянии up. При отсутствии этой опции интерфейсы в состоянии down с ACP/ANI enable перейдут в состояние admin down.

9.3.5.1. Узлы с настроенной плоскостью данных

Настроенными (brownfield) узлами называют те, на которых уже настроена плоскость данных.

Глобальное выполнение ACP/ANI enable [up-if-only] на каждом узле является единственной командой, требуемой для создания ACP в сети уже настроенных (brownfield) узлов, когда у них уже есть сертификаты домена. При использовании BRSKI (ANI enable), для предоставления этих сертификатов требуется установить один регистратор BRSKI, который также может служить CA для сети. Это простейший способ запустить ACP/ANI в имеющейся сети.

Необходимость явного включения ACP/ANI особенно важна для узлов brownfield, поскольку иначе обновление программ может внести поддержку ACP/ANI. Автоматическое включение ACP/ANI в сетях, где оператор не желает применять ACP/ANI (скорее просто не слышал об этом) может сильно раздражать оператора, особенно при смене состояния down на admin down.

Автоматическая установка ANI на brownfield-узлах, где оператор не знает о работе BRSKI и MASA может создать серьёзную проблему безопасности, хоть это и маловероятно. Если атакующий может выдать себя за оператора, регистрируясь в таком качестве на узле MASA, или иным путём получить ваучеры, то при достаточном физическом доступе в сеть, чтобы заявители регистрировались у него, злоумышленник сможет получить доступ к ACP и далее через ACP - к плоскости данных. В сетях, где оператор явно разрешает ANI, этого не может случиться, поскольку оператор будет создавать регистратор BRSKI, который обнаружит попытки атак, и оператор настраивал бы свой регистратор с MASA. Узлы, требующие ваучеров владения, не подвержены такой атаке (см. [RFC8995]). Отметим, что при глобальном ACP enable не возникает риска таких атак, поскольку они зависят от какого-либо механизма для предварительного предоставления сертификатов домена устройствам.

9.3.5.2. Заранее не настроенные узлы

Узлами ACP greenfield считаются узлы, которые не имеют предварительной конфигурации и могут использовать начальную загрузку через сеть для присоединения к ACP. Для поддержки таких узлов описанную в документе плоскость ACP нужно объединить с протоколом начальной загрузки и/или механизмом, который будет зачислять узлы с ключевым материалом ACP - сертификатом ACP и TA. Для узлов ANI таим механизмом служит BRSKI.

Когда такой узел включается и обнаруживает отсутствие конфигурации (greenfield), он включает протоколы и/или механизмы начальной загрузки. После зачисления ключевого материала ACP состояние greenfield завершается и запускается ACP. При использовании BRSKI состояние узла отражает это установкой ANI enable при определении состояния greenfield в момент включения питания.

Узлам ACP greenfield, интерфейсы которых при отсутствии ACP будут в состоянии down, **следует** установить все естественные интерфейсы в состояние admin down и разрешать лишь трафик плоскости данных, требуемый для протоколов и/или механизмов начальной загрузки.

Состояние ACP greenfield завершается зачислением ключевого материала ACP (сертификат и TA) или обнаружением разрешения прервать операции ACP greenfield.

Узлы ACP, поддерживающие работу с нуля (greenfield), **могут** пожелать обеспечивать совместимость с прежними формами настройки и/или обеспечения, особенно в случаях развёртывания ACP лишь на части узлов. Таким узлам ACP **следует** наблюдать попытки обеспечения или настройки узла с помощью интерфейсов и/или методов, которые традиционно указывают физическое владение узлом, такие как подключение последовательного или USB-порта для консольного доступа или носителя USB с конфигурацией начальной загрузки. Когда такая операция замечена до завершения зачисления ключевого материала ACP, узлу **следует** перейти в состояние, в котором он находился бы при запрете ACP/ANI во время загрузки. Это прерывает операции ACP greenfield.

Когда узел ACP разрешает параллельно автоматическое зачисление ACP или не-ACP и/или протоколы и механизмы начальной загрузки, следует соблюдать осторожность, чтобы не прервать какой-либо протокол или механизм до того, как другие зарегистрировали ключевой материал ACP или продвинулись до точки разрешённого прерывания операций ACP greenfield. Узлы ACP greenfield с надёжной защитой могут не разрешать прерывание операций ACP greenfield даже при физическом доступе.

Узлам, заявляющим поддержку операций ANI с нуля (greenfield), **не следует** разрешать параллельно с BRSKI какой-либо протокол или механизм зачисления или начальной загрузки, который допускает доверие при первом использовании (Trust On First Use или TOFU, Opportunistic Security: Some Protection Most of the Time [RFC7435]) через интерфейсы, отличные от тех, которые традиционно показывают физическое владение узлом. Считается, что протоколы и механизмы с опубликованной аутентификацией по имени пользователя и паролю страдают от TOFU. Защита протоколов и механизмов начальной загрузки требованием ваучера [RFC8366] может служить для предотвращения TOFU.

Таким образом, цель поддержки ACP greenfield заключается в возможности разрешить удалённое автоматизированное зачисление ключевого материала ACP и, следовательно, автоматическую начальную загрузку в ACP, а также запретить TOFU в процессе начальной загрузки с возможностью исключения (для совместимости с прежними механизмами) начальной загрузки через интерфейсы, традиционно указывающие физическое владение узлом.

9.3.6. Отмена ANI/ACP enable

Отключение ANI/ACP путём отмены (undo) ACP/ANI enable создаёт риск для надёжной работы ACP, если это сделано по ошибке или без соответствующих полномочий. На это можно повлиять с помощью дополнительного (будущего) свойства в сертификате (например, в поле расширения acp-node-name). В развёртывании ANI, предназначенном для удобства, отключение может быть разрешено без дополнительных ограничений. В развёртывании ANI, считающемся критическим, требуется больше проверок. Одним из наиболее контролируемых вариантов был бы запрет этих команд , пока сертификат домена не отозван или его обновление не было отвергнуто. Настройка этого варианта была бы параметром регистраторов BRSKI. Пока узел не получил сертификат домена, для отмены ANI/ACP enable не следует устанавливать дополнительных ограничений.

9.3.7. Заключение

Команды ACP/ANI enable [up-if-only] на уровне узла разрешают работу ACP/ANI. Это автоматически разрешено лишь на устройствах ANI greenfield, в иных случаях требуется явная настройка.

Если опция up-if-only не задана, интерфейсы со включённым ACP/ANI рассматривают состояние down как admin down, а не physical down. В состоянии admin-down все пакеты, не относящиеся к ACP/ANI, фильтруются, но физический уровень продолжает работать для операций ACP/ANI.

(Новые) команды, приводящие к физическому прерыванию (physical down, loopback) интерфейсов с поддержкой ACP/ANI, следует создавать так, чтобы максимально защитить непрерывность или восстановление ACP.

Команды ACP/ANI enable на уровне интерфейса управляют операциями на интерфейсе. Этот режим включён по умолчанию на естественных интерфейсах и настраивается явно на прочих интерфейсах.

Отключение ACP/ANI enable глобально или на уровне интерфейса следует выполнять с дополнительными проверками для предотвращения нежелательных перебоев в работе ACP. Уровень контроля может быть параметром на уровне домена в сертификатах домена.

9.4. Частичное или поэтапное внедрение

Субсхема адресации Zone (параграф 6.11.3) позволяет поэтапно внедрять ACP в сети, где ACP может развёртываться по периметру, но не в ядре, соединяющем эти края. В таких случаях каждая краевая сеть, такая как сеть кампуса или предприятия, имеет отдельную (disjoint) плоскость ACP, которой выделен один или несколько уникальных Zone-ID. Узлы ACP, зарегистрированные в конкретной зоне ACP получают адреса по субсхеме Zone, например, посредством создания для каждой такой зоны одного или нескольких регистраторов ACP с Zone-ID. Все регистраторы для этих зон ACP должны получить сертификаты ACP от CA на основе общего набора TA и общего имени домена ACP.

Эти зоны ACP могут создаваться сначала как отдельные сети без соединений между собой и/или могут быть соединены через сеть ядра без ACP с помощью различных неавтономных методов работы. Например, каждая отдельная зона ACP может иметь краевой узел в форме L3 VPN PE (MPLS или IPv6 L3VPN), где создаётся полная, неавтономная VPN ядра ACP с использованием ACP VRF и обмена маршрутами от этих ACP VRF через неавтономные протоколы маршрутизации VPN.

Хотя такая установка возможна с любой субсхемой адресации ACP, субсхема Zone проще в настройке и расширяема для любых протоколов маршрутизации VPN, поскольку каждой зоне ACP требуется лишь указать один или несколько адресных префиксов /64 зоны ACP в VPN ядра ACP в отличие от маршрутов к каждому узлу ACP, как требуют другие субсхемы адресации ACP.

Отметим, что неавтономная VPN ядра ACP требует дополнительных расширений для распространения сообщений GRASP, когда желательно обнаружение GRASP через зоны. Например, можно создать на каждом граничном маршрутизаторе зоны туннель ACP к концентратору GRASP. Этот концентратор можно реализовать на прикладном уровне и запустить в сети NOC. Он будет распространять анонсы GRASP между зонами ACP и/или генерировать аносы GRASP для служб NOC.

Такое частичное развёртывание может оказаться достаточным и может развиваться, чтобы стать автономным за счёт будущих стандартных или нестандартных расширений, например, разрешая распространять сообщения GRASP через L3VPN с использованием, скажем, групповой рассылки L3VPN.

Такие частичные развёртывания можно объединить в полностью автономную плоскость ACP (при подходящей поддержке ACP в ядре) без замены криптографического материала, поскольку сертификаты узлов ACP получены из одной ACP.

9.5. Конфигурация и ACP (заключение)

Для ACP нет желательной конфигурации и все параметры, которые нужно настраивать для поддержки ACP, являются ограничениями решения, но они требуются лишь в тех случаях, когда не все компоненты являются автономными. Когда это необходимо, применяются имеющиеся механизмы настройки, такие как CLI или модели данных YANG (The YANG 1.1 Data Modeling Language [RFC7950]). Наиболее важные примеры таких конфигураций указаны ниже.

- Когда узлы ACP не поддерживают автономный способ получения сертификатов ACP, например, BRSKI, сертификат требуется настраивать с помощью имеющихся механизмов, выходящих за рамки этой спецификации. В современных маршрутизаторах обычно имеется набор таких механизмов.
- Для управления сертификатами нужны функции PKI. Обнаружение таких функций через ACP автоматизировано (6.2.5. Поддержка сертификата и привязки доверия), а их настройка - нет.
- Когда узлы без поддержки ACP, такие как имеющиеся NMS, нужно физически подключать к ACP, применяемый для подключения узел ACP нужно настроить в соответствии с параграфом 8.1. ACP Connect. Можно также организовать подключение ACP и плоскости данных сети через одно физическое соединение (параграф 8.1.4).
- Когда начальная загрузка устройств неавтономна, нужна явная настройка для включения ACP (параграф 9.3).

- Когда требуется расширять ACP через отличные от L2 интерфейсы, ACP в соответствии с этим документом не может автоматически обнаруживать кандидатов в соседи и их нужно настраивать (параграф 8.2).

Когда ACP работает, дополнительную настройку плоскости данных надёжней выполнять через ACP, поскольку адресация и связность (маршрутизация) ACP не зависит от плоскости данных. Для этого методу настройки нужно лишь разрешить работу через ACP VRF, например, с использованием NETCONF, SSH или иного метода.

ACP также обеспечивает дополнительную защиту за счёт применения поэтапного (hop-by-hop) шифрования для таких операций настройки. Некоторые традиционные методы настройки (например, SNMP, TFTP, HTTP) могут не использовать сквозного шифрования и большинство методов настройки со сквозной защитой по-прежнему легко позволяет пассивно наблюдать на процессом настройки (например, транспортные потоки, номера портов, адреса IP).

ACP можно и следует использовать как транспорт для упомянутых выше неавтономных элементов ACP, но в этом случае требуется применять осторожность как при настройке плоскости данных без ACP. Ошибки в настройке могут привести к отсоединению настраиваемого элемента, например, в результате некорректной настройки удалённого соседа ACP, через которого осуществляется доступ к настраиваемому узлу ACP.

10. Заключение - преимущества (информационный раздел)

10.1. Свойства самовосстановления

ACP поддерживает самовосстановление, как указано ниже.

- Новые соседи автоматически присоединяются к ACP после успешной проверки и становятся доступными через ACP по их уникальным адресам ULA.
- При любом изменении топологии протокол маршрутизации ACP будет автоматически принимать эти изменения и продолжать обеспечивать доступность для всех узлов.
- ACP отслеживает действительность сертификатов партнёров и разрывает защищённые каналы ACP по истечении срока действия сертификата партнёра. Когда используются краткосрочные сертификаты с временем действия порядка периода обновления OCSP/CRL, это позволяет удалять недействительных партнёров (чей сертификат не обновлён) с той же скоростью, что и при использовании OCSP/CRL. Такие же преимущества могут быть достигнуты при использовании CRL/OCSP, периодическом обновлении сведений об отзыве, а также разрыве защищённых каналов, когда (длительный) сертификат партнёра отозван. Однако в целях упрощения от реализаций ACP не требуется поддержка этих усовершенствований.

ACP обеспечивает стойкость к разделению и слиянию сетей. Практически все операции ACP выполняются через локальный канал, где разделение сети не оказывает влияния. Узлы аутентифицируют друг друга по сертификатам домена для организации ACP локально. Адресация внутри ACP не меняется и протокол маршрутизации в обеих частях ACP приведёт к двум работающим (но разделённым) ACP.

Имеется несколько важных зависимостей. Списки CRL могут стать недоступными при разделении сети. Это можно решить подходящим правилом не отключать сразу же соседей при недоступности CRL. Кроме того, регистратор ACP или CA могут стать недоступными при разделении. Это может задержать обновление сертификатов, срок действия которых завершается в будущем, и помешать зачислению новых узлов при разделении сети.

Решения ACP с высокой устойчивостью к отказам могут создаваться с использованием регистраторов ACP со встроенными суб-CA, как указано в параграфе 9.2.4. Пока в отделившейся сети имеется один или несколько таких регистраторов ACP, будет продолжаться зачисление новых кандидатов в ACP до завершения срока действия сертификата суб-CA у регистратора ACP. Поскольку адресация ACP основывается на уникальных Registrar-ID, последующее слияние разделённых частей сети не вызовет проблем с адресацией ACP, заданной при разделении.

После разделения сети слияние просто восстановит предыдущее состояние, сертификаты будут обновлены, CRL станут доступны и новые узлы смогут зачисляться везде. Поскольку все узлы используют одну TA, слияние будет беспрепятственным.

При слиянии двух сетей с разными TA от узлов ACP потребуется доверие к объединению TA. Когда хэш-значения субдоменов маршрутизации различаются, адресация не будет перекрываться. Перекрытие возможно лишь случайно в случае маловероятного совпадения 40-битовых хэш-значений SHA-256 (см. 6.11. Адресация внутри ACP). Отметим, что полные механизмы слияния сетей выходят за рамки этой спецификации.

Для реализаций ACP очень важна способность работать через отключённые административно интерфейсы. При невозможности этого взамен можно запросить у оператора явное переопределение действий по отключению интерфейсов, через которые работает ACP, особенно если известно, что отключение ACP оторвёт оператора от узла. Например, административные действия по отключению могут включать проверку зависимостей, чтобы увидеть, не отключат ли эти действия транспортное соединение в результате (при использовании принятой по умолчанию маршрутизации RPL пересылка пакетов будет симметричной, поэтому это можно проверить фактически).

10.2. Самозащита

10.2.1. Извне

Как указано в разделе 6. Создание ACP (нормативный раздел), ACP работает на основе защищённых каналов между узлами, которые взаимно аутентифицируют друг друга по сертификатам домена. Сами каналы защищены стандартными методами шифрования, такими как DTLS или IPsec, которые обеспечивают дополнительную аутентификацию при создании, целостность и конфиденциальность данных внутри ACP, а также защиту от повторного использования (replay). Атакующий не сможет войти в ACP, пока у него нет действительного сертификата ACP. Злоумышленник в пути без действительного сертификата ACP не сможет внедрить пакеты в ACP, поскольку каналы ACP защищены. Он не сможет и расшифровать трафик ACP без взлома шифрования. Он может лишь пытаться анализировать поведение шифрованного трафика ACP.

Степень влияния скомпрометированных узлов на работу ACP зависит от реализации узлов ACP и их повреждений. Когда атакующий получил лишь административные права для удалённой настройки узлов ACP, он может нарушить работу ACP с помощью одного или нескольких параметров конфигурации, чтобы отключить узел (9.3. Включение и отключение ACP и ANI) или настройки неавтономных опций ACP, если это поддерживается повреждёнными узлами ACP (8. Поддержка элементов, не понимающих ACP (нормативный раздел)). Внедрение или извлечение трафика на повреждённом узле ACP возможно лишь при поддержке этим узлом ACP connect (8.1. ACP Connect) и злоумышленник может контролировать трафик на одном из интерфейсов узла ACP, например, имея физический доступ к узлу ACP.

ACP также служит защитой (за счёт аутентификации и шифрования) для протоколов, связанных с OAM, которые могут не иметь опций защиты стека или в которых реализация или развёртывание опций защиты не удались по причине ограничений производителя, продукции или клиента. Это включает протоколы SNMP (An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks [RFC3411]), NTP [RFC5905], PTP (Precision Time Protocol [IEEE-1588-2008]), DNS (DNS Extensions to Support IP Version 6 [RFC3596]), DHCPv6 (Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [RFC3315]), syslog (The BSD Syslog Protocol [RFC3164]), RADIUS (Remote Authentication Dial In User Service (RADIUS) [RFC2865]), Diameter (Diameter Base Protocol [RFC6733]), TACACS (An Access Control Protocol, Sometimes Called TACACS [RFC1492]), IPFIX (Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information [RFC7011]), NetFlow (Cisco Systems NetFlow Services Export Version 9 [RFC3954]) и другие. Не все приведённые ссылки указывают на последние версии протоколов, но указанные версии применяются широко.

Защита на основе защищённых поэтапных соединений ACP для этих и других протоколов является лишь временной мерой, конечная цель состоит в сквозном шифровании с использованием сертификата домена и опора на защищённые каналы ACP предназначена прежде всего для надёжной связности без участия пользователя (zero-touch), а не для обеспечения безопасности.

Оставшийся вектор атак включает атаки непосредственно на базовые протоколы ACP напрямую или через отказ в обслуживании. Однако, благодаря построению ACP на основе адресов IPv6 link-local, удалённые атаки из плоскости данных невозможны, поскольку в плоскости данных нет возможностей удалённо передавать пакеты IPv6 link-local. Единственным исключениям являются интерфейсы ACP connect, требующие большей физической защиты. Адреса ULA доступны лишь из контекста ACP и поэтому недостижимы из плоскости данных. Кроме того, протоколы ACP следует реализовать так, чтобы быть устойчивым к атакам и не потреблять избыточных ресурсов даже при атаке.

10.2.2. Изнутри

Модель защиты ACP основана на доверии всех членов группы узлов, имеющих сертификаты ACP одного домена, поэтому атаки со стороны скомпрометированного члена группы создают наибольшие проблемы.

Члены группы должны быть защищены от злоумышленников, чтобы их нельзя было легко скомпрометировать или использовать как посредников для атаки на другие устройства через ACP. Например, функциям плоскости управления (транспортные порты) следует быть доступными лишь из ACP, а не из плоскости данных. Это особенно относится к функциям плоскости управления, где отсутствует сквозной защищённый транспорт, а ACP обеспечивает автоматическую надёжную связность и защиту от атак. Защиту от всех возможных векторов атак обычно проще обеспечить на устройствах, программы которых изначально создавались с ACP, нежели в унаследованных программных системах, где плоскость ACP добавлена в качестве ещё одной функции.

Как отмечено выше, для трафика через ACP следует по возможности обеспечивать сквозное шифрование. Это включает трафик GRASP, EST и BRSKI внутри ACP. Такая защита минимизирует MITM-атаки со стороны скомпрометированных членов группы ACP. Такой злоумышленник не может перехватить или изменить коммуникации, но способен фильтровать их, что неизбежно в любых обстоятельствах.

Дополнительные сведения о предотвращении и обработке атак со стороны скомпрометированных узлов приведены в Приложении A.9.8. Предотвращение и обработка атак от скомпрометированных устройств.

10.3. Представление для администратора

Плоскость ACP является самоформирующей, самоуправляемой и самозащищающейся, поэтому она минимально зависит от администратора сети. В частности, поскольку она (предположительно) не зависит от конфигурации, возможности ошибок настройки для самой ACP ограничены. У администратора может быть возможность включить или отключить ACP полностью, но детальная настройка недоступна ему. Это значит, что плоскости ACP недопустимо отражаться в конфигурации узлов за исключением возможности её включить или выключить (да и это нежелательно).

Хотя настройка невозможна (за исключением описанной в разделе 8 и параграфе 9.2), администратору должна обеспечиваться полная видимость ACP и всех параметров плоскости для случаев поиска неполадок. Поэтому в ACP должны поддерживаться все опции отображения и отладки, как и для других сетевых функций. В частности, NMS или контроллер должны иметь возможность обнаружить ACP и отслеживает её состояние. Эта видимость операций ACP должна быть чётко отделена от видимости операций плоскости данных, чтобы автоматизированным системам не приходилось иметь дело в аспектами ACP, если это им не нужно явно.

Благодаря самозащите ACP, узлы без поддержки ACP или не имеющие действительного сертификата домена, не могут подключиться к ACP. Это значит, что по умолчанию возможности подключения лишены традиционные контроллеры и NMS. В параграфе 8.1.1. Контроллер или NMS без поддержки ACP описано, как они могут организовать подключение.

11. Вопросы безопасности

Набор узлов ACP с сертификатами ACP из одного домена ACP и включённой функциональностью ACP автоматически «строят себя» - ACP автоматически организуется между соседними узлами ACP. Обеспечивается также самозащита - защищённые каналы ACP аутентифицируются и шифруются. Для этого не требуется настройка.

Свойство самозащиты не включает обхода неавтономных элементов, как описано в разделе 8. Самозащита ACP от внешних и, в меньшей степени, от внутренних атак описана в параграфе 10.2.

Однако безопасность ACP зависит от множества факторов, перечисленных ниже.

- Использование сертификатов домена зависит от работы поддерживающей инфраструктуры PKI. При её компрометации защита ACP также будет скомпрометирована. Обычно это контролирует администратор сети.

- Узлы ACP получают свои сертификаты от регистраторов ACP. Регистраторы ACP критически важны для безопасности ACP. Процедуры и протоколы для регистраторов ACP выходят за рамки спецификации, как указано в параграфе 6.11.7.1, заданы лишь требования для сертификатов ACP.

- Каждый регистратор ACP (для зачисления сертификатов ACP) и сервер ACP EST (для обновления сертификатов ACP) важен для безопасности и его протоколы также важны для защиты. Те и другие должны быть защищены от атак, подобно CA и их протоколам. Враждебный регистратор может зачислить вредоносные узлы в сеть ACP (если CA предоставляет это регистратору) или нарушить маршрутизацию ACP, например, допуская дубликаты адресов ACP на узлах ACP по их сертификатам ACP.

- Узлы ACP, являющиеся узлами ANI полагаются на BRSKI как протокол для регистраторов ACP. К узлам ACP типа ANI применимы соображения безопасности для BRSKI, обеспечивающего автоматическое, защищённое зачисление сертификатов ACP.

- BRSKI и, возможно, другие варианты протокола регистратора ACP требуют, чтобы узлы имели IDevID (на основе X.509 v3). IDevID являются опцией регистраторов ACP для безопасного отождествления узлов-кандидатов в ACP, которые следует зачислить в домен ACP.

- Чтобы IDevID надёжно идентифицировали узлы, которым они назначены, узлы должны (1) использовать аппаратную поддержку, такую как модуль TPM для защиты от извлечения и/или клонирования секретного ключа IDevID и (2) апаратную или программную инфраструктуру для запрета исполнения неразрешённых программ с целью защиты от вредоносного использования IDevID.

- Как и IDevID, сертификаты ACP должны быть в равной степени защищены от извлечения и других злоупотреблений той же инфраструктурой узла ACP. Эта инфраструктура защиты IDevID и сертификата ACP полезна независимо от применяемого регистратором ACP протокола (BRSKI или иной).

- Для обновления сертификатов ACP нужна поддержка EST, поэтому соображения безопасности из [RFC7030], связанные с обновлением сертификатов, заменой ключей и обновлением TP применимы и к ACP. Вопросы безопасности EST, отличные от применяемых при взаимной аутентификации сертификатов, не применимы. Не рассматриваются также вопросы безопасности начального развёртывания через EST, за исключением узлов ACP типа ANI, поскольку в BRSKI применяется EST.

- Вредоносный узел ACP может объявить себя сервером EST через GRASP в ACP, если на узле могут быть выполнены враждебные программы. Поэтому CA следует аутентифицировать только заведомо доверенные серверы EST, такие как узлы с аппаратной защитой от враждебных программ. Когда регистраторы применяют свой сертификат ACP для аутентификации по отношению к CA, атрибут расширенного использования ключей id-kp-cmcRA [RFC6402] позволяет CA определить, что узлу ACP разрешено выступать при зачислении как регистратору ACP. Без такого взаимодействия с CA враждебный сервер EST может привлекать узлы ACP, пытающиеся обновить свой ключевой материал, но они не смогут обновить действительный сертификат ACP. Узел ACP, пытающийся использовать враждебный сервер EST, может после этого обратиться к другому серверу EST и зарегистрировать отказ злонамеренного сервера EST.

- Враждебный узел ACP на пути может фильтровать действительные анонсы сервера EST через ACP, но такие узлы в равной мере могут фильтровать любой трафик ACP, включая трафик самого EST. Однако для любой атаки нужна возможность выполнения вредоносной программы на повреждённом узле ACP.

- При отсутствии возможности внедрить враждебный код атакующий может исказить настройку узла ACP, поддерживающего функциональность сервера EST, и попытаться настроить вредоносный CA. Это не позволит обновить сертификаты ACP, но может привести к DoS-атаке, если враждебный узел станет сервером EST и заставит узлы ACP пытаться обновить свои сертификаты ACP через повреждённый узел. Этой проблемы можно избежать, если реализация сервера EST может проверять полномочия настроенного CA обновлять сертификаты ACP для узлов. Такая возможность зависит от протокола между сервером EST и CA, который выходит за рамки этого документа.

Атаки на зависимости ACP от PKI и сертификатов можно минимизировать разными аппаратными и программными компонентами, включая TPM для IDevID и сертификатов ACP, запреты на выполнение недоверенных программ, аспекты функциональности сервера EST для ACP избавляющие от повреждений на уровне конфигурации.

Поскольку партнёры выбирают один из взаимно поддерживаемых протоколов защищённого канала ACP с помощью подхода, описанного в параграфе 6.6, организация защищённого канала ACP подвержена MITM-атакам с понижением. Последствия такой атаки могут быть обнаружены с помощью дополнительных механизмов, описанных в Приложении A.9.9. Как вариант, могут быть разработаны новые выбора протокола механизмы защиты канала.

Модель безопасности ACP, заданная в этом документе, рассчитана на использование частной инфраструктуры PKI. TA в приватных PKI обеспечивают защиту от злонамеренно созданных сертификатов ACP при доступе в ACP. Такие атаки могут создавать фиктивные сертификаты ACP с корректными на вид AcpNodeNames, но эти сертификаты не пройдут проверку пути сертификации при контроле принадлежности к домену ACP (п. 2 в параграфе 6.2.3).

В ACP нет защиты от подмены адреса отправителя. Это означает, что злоумышленник с доступом в ACP, может подделать все адреса в ACP и сообщения от любого узла. Новым протоколам и службам, работающим через ACP следует применять сквозную аутентификацию внутри ACP. Это уже делает GRASP в соответствии с этим документом.

Плоскость ACP предназначена для автоматизации современного управления сетями и управления будущими одноранговыми и распределенными сетями. Любой член ACP может передавать пакеты ACP IPv6 другим членам ACP и анонсировать через ACP GRASP услуги всем членам ACP без зависимости от централизованных компонентов.

В ACP применяется проверка подлинности и полномочий партнёров по сертификатам ACP. Такая модель защиты необходима для поддержки автономной специализированной связности «каждый с каждым» между узлами ACP. Защита инфраструктуры обеспечивается пошаговой (hop-by-hop) аутентификацией и шифрованием без привлечения третьей стороны. Для любых служб, где подходит эта полностью автономная модель безопасности одноранговых групп

(например, для защиты протоколов маршрутизации в плоскости данных), сертификат ACP можно применять без изменений.

Эта модель безопасности ACP рассчитана прежде всего для отражения внешних, а не внутренних атак. Для защиты от атак с подменой адресов со стороны скомпрометированных узлов ACP на пути в новой сигнализации ACP применяется сквозное шифрование внутри ACP - GRASP через ACP с применением TLS. Такое же поведение ожидается от всех не унаследованных протоколов и служб, применяющих ACP. Поскольку групповые ключи не используются, не возникает риска получения повреждёнными узлами доступа к трафику от других узлов ACP со сквозным шифрованием.

Атаки со стороны повреждённых узлов ACP на ACP сложнее атак на плоскость данных, благодаря автоматической настройке ACP и отсутствию параметров конфигурации, которые можно было бы злонамеренно применить для нарушения или прерывания работы ACP. Это исключает настройку обходных путей в поддержку неавтономных элементов.

Смягчение атак от скомпрометированных членов ACP возможно с помощью стандартных механизмов автоматизированного управления сертификатами, включая отзыв и отказ от обновления краткосрочных сертификатов. В этой спецификации не предусмотрена дальнейшая оптимизация заданных для ACP механизмов (но см. Приложение A.9.8. Предотвращение и обработка атак от скомпрометированных устройств).

Службам верхнего уровня, созданным с применением сертификатов ACP, не следует полагаться лишь на недифференцированную групповую защиту, если другая модель подходит больше или лучше защищена. Например, централизованная настройка сети полагается на модель защиты, где лишь немногим особо доверенным узлам разрешено настраивать плоскость данных узлов сети (CLI, NETCONF). Это можно сделать с помощью сертификатов ACP путём их разделения и введения ролей (A.9.5. Назначение роли).

Операторам и разработчикам программ обеспечения необходимо знать как обеспечения и конфигурация сетевых устройств влияют на возможности оператора и обеспечивающих программ удалённо обращаться к узлам сети. При использовании ACP большинство проблем обеспечения и настройки, вызывающих потери связности для удалённого обеспечения и настройки можно предотвратить (см. раздел 6). Остаётся лишь несколько проблем, таких как явное физическое отключение устройства (9.3.2. Состояние admin down).

Многие аспекты ACP разработаны с учётом безопасности и эти вопросы рассмотрены в тексте документа.

Адреса IPv6, используемые узлами ACP учитываются в сертификате домена для узла, как описано в параграфе 6.2.2. Это позволяет проверить владение партнёром адресом IPv6 при аутентификации соединений по сертификату домена.

ACP служит подложкой защиты (и транспорта) для GRASP внутри ACP, т. е. протокол GRASP защищён не только от атак извне, но и от атак со стороны скомпрометированных внутренних узлов, полагаясь не только на поэтапную защиту каналов ACP, но и на сквозную защиту для сообщений GRASP (параграф 6.9.2).

ACP обеспечивает защищённое, отказоустойчивое автоматическое (zero-touch) обнаружение серверов EST для обновления сертификатов (6.2.5. Поддержка сертификата и привязки доверия).

ACP обеспечивает расширяемую, автоматически настраиваемую поэтапную (hop-by-hop) защиту инфраструктуры ACP путём согласования протоколов поэтапной защиты каналов (6.6. Выбор канала).

Плоскость ACP разработана для минимизации атак извне путём сокращения зависимости от операцией и конфигурации не-ACP (плоскость данных) на узле (6.13.2. Адресация на защищённых каналах).

В сочетании с BRSKI плоскость ACP обеспечивает отказоустойчивое полностью автоматизированное (zero-touch) сетевое решения для краткосрочных сертификатов, которые могут быть обновлены или заново зачислены даже после непреднамеренного истечения срока действия (например, при прерывании связности). См. Приложение A.2.

Поскольку защищённые каналы ACP могут сохраняться долго, а сертификаты могут быть краткосрочными, защищённые каналы, созданные, например, с применением IPsec, требуется разрывать по истечении срока действия сертификата (6.8.5. Профили защищённых каналов ACP).

В параграфе 7.2 описан способ реализации маршрутизируемой топологии ACP, работающей, фактически, в большом домене мостов при использовании маршрутизаторов L3/L2, работающих в плоскости данных на уровне L2. В этом случае плоскость ACP гораздо сильнее подвержена атакам других узлов, «крадущих» адреса L2, чем в случае реальной маршрутизации, особенно при включении в сеть мостов недоверенных устройств, таких как хосты. Это общая проблема ЛВС L2. Устройства L2/L3 зачастую уже имеют ту или иную форму защиты портов (port security) для предотвращения этого. Они полагаются на протокол обнаружения соседей (Neighbor Discovery Protocol или NDP) или обучения DHCP для связывания порта или адреса MAC с адресом IPv6 и блокировки адресов отправителей MAC/IPv6 от некорректных портов. Этот тип функций нужно включать для предотвращения DoS-атак, в частности, на ACP. Аналогично экземпляр GRASP DULL должен убедиться, что адрес IPv6 в locator-option соответствует адресу отправителя IPv6 в заголовке пакета DULL GRASP.

12. Взаимодействие с IANA

Этот документ определяет автономную плоскость управления (Autonomic Control Plane).

Для модуля ASN.1 ANIMA-ACP-2020 агентство IANA выделило значение id-mod-anima-acpnodename-2020 = 97 в реестре SMI Security for PKIX Module Identifier (1.3.6.1.5.5.7.0). Для otherName/AcpNodeName агентство IANA выделило значение id-on-AcpNodeName = 10 в реестре SMI Security for PKIX Other Name Forms (1.3.6.1.5.5.7.8).

Агентство IANA зарегистрировало указанные в таблице 2 имена в субреестре GRASP Objective Names реестра GeneRic Autonomic Signaling Protocol (GRASP) Parameters.

Таблица 2. Имена целей GRASP.

Название цели	***Документ***
AN_ACP	RFC 8994 (параграф 6.4)
SRV.est	RFC 8994 (параграф 6.2.5)

В этом документе выбран странно выглядящий формат SRV.<service-name>", чтобы эти имена целей соответствовали будущему упрощению реестра целей GRASP. Сегодня каждое имя в реестре целей GRASP должно явно выделяться IANA. Впредь можно будет считать, что этот тип имён целей включается в реестр автоматически для той же службы, для которой регистрируется <service-name> в соответствии с [RFC6335]. Это разъяснение является информационным и не влияет на запрошенную регистрацию.

Агентство IANA создало реестр Autonomic Control Plane (ACP) с субреестром ACP Address Type (Таблица 3).

Таблица 3. Исходные значения субреестра ACP Address Type.

Значение	***Описание***	***Документ***
0	Субсхемы адресации ACP Zone и ACP Manual	RFC 8994 (параграфы 6.11.3 и 6.11.4)
1	Субсхема адресации ACP Vlong	RFC 8994 (параграф 6.11.5)
2-3	Не выделены	

Значения в субреестре ACP Address Type представляют собой числа от 0 до 3 в паре с именем (строка). Новые значения **должны** выделяться по процедуре Standards Action, заданной в Guidelines for Writing an IANA Considerations Section in RFCs [RFC8126].

13. Литература

13.1. Нормативные документы

[IKEV2IANA] IANA, "Internet Key Exchange Version 2 (IKEv2) Parameters", <https://www.iana.org/assignments/ikev2-parameters>.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <https://www.rfc-editor.org/info/rfc3810>.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005, <https://www.rfc-editor.org/info/rfc4191>.

[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>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC5954] Gurbani, V., Ed., Carpenter, B., Ed., and B. Tate, Ed., "Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261", RFC 5954, DOI 10.17487/RFC5954, August 2010, <https://www.rfc-editor.org/info/rfc5954>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <https://www.rfc-editor.org/info/rfc6550>.

[RFC6551] Vasseur, JP., Ed., Kim, M., Ed., Pister, K., Dejean, N., and D. Barthel, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks", RFC 6551, DOI 10.17487/RFC6551, March 2012, <https://www.rfc-editor.org/info/rfc6551>.

[RFC6552] Thubert, P., Ed., "Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6552, DOI 10.17487/RFC6552, March 2012, <https://www.rfc-editor.org/info/rfc6552>.

[RFC6553] Hui, J. and JP. Vasseur, "The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams", RFC 6553, DOI 10.17487/RFC6553, March 2012, <https://www.rfc-editor.org/info/rfc6553>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/info/rfc7030>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/info/rfc7525>.

[RFC7676] Pignataro, C., Bonica, R., and S. Krishnan, "IPv6 Support for Generic Routing Encapsulation (GRE)", RFC 7676, DOI 10.17487/RFC7676, October 2015, <https://www.rfc-editor.org/info/rfc7676>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8221] Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 8221, DOI 10.17487/RFC8221, October 2017, <https://www.rfc-editor.org/info/rfc8221>.

[RFC8247] Nir, Y., Kivinen, T., Wouters, P., and D. Migault, "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 8247, DOI 10.17487/RFC8247, September 2017, <https://www.rfc-editor.org/info/rfc8247>.

[RFC8422] Nir, Y., Josefsson, S., and M. Pegourie-Gonnard, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier", RFC 8422, DOI 10.17487/RFC8422, August 2018, <https://www.rfc-editor.org/info/rfc8422>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/info/rfc8610>.

[RFC8990] Bormann, C., Carpenter, B., Ed., and B. Liu, Ed., "GeneRic Autonomic Signaling Protocol (GRASP)", RFC 8990, DOI 10.17487/RFC8990, May 2021, <https://www.rfc-editor.org/info/rfc8990>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

13.2. Дополнительная литература

[AR8021] IEEE, "IEEE Standard for Local and metropolitan area networks - Secure Device Identity", IEEE 802.1AR, <https://1.ieee802.org/security/802-1ar>.

[CABFORUM] CA/Browser Forum, "Certificate Contents for Baseline SSL", November 2019, <https://cabforum.org/baseline-requirements-certificate-contents/>.

[FCC] FCC, "June 15, 2020 T-Mobile Network Outage Report", A Report of the Public Safety and Homeland Security Bureau Federal Communications Commission, PS Docket No. 20-183, October 2020, <https://docs.fcc.gov/public/attachments/DOC-367699A1.docx>.

[IEEE-1588-2008] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", DOI 10.1109/IEEESTD.2008.4579760, IEEE 1588-2008, July 2008, <https://standards.ieee.org/standard/1588-2008.html>.

[IEEE-802.1X] IEEE, "IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control", DOI 10.1109/IEEESTD.2010.5409813, IEEE 802.1X-2010, February 2010, <https://standards.ieee.org/standard/802_1X-2010.html>.

[LLDP] IEEE, "IEEE Standard for Local and metropolitan area networks: Station and Media Access Control Connectivity Discovery", DOI 10.1109/IEEESTD.2016.7433915, IEEE 802.1AB-2016, March 2016, <https://standards.ieee.org/standard/802_1AB-2016.html>.

[MACSEC] IEEE, "IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security", DOI 10.1109/IEEESTD.2006.245590, IEEE 802.1AE-2006, August 2006, <https://standards.ieee.org/standard/802_1AE-2006.html>.

[NOC-AUTOCONFIG] Eckert, T., Ed., "Autoconfiguration of NOC services in ACP networks via GRASP", Work in Progress, Internet-Draft, draft-eckert-anima-noc-autoconfig-00, 2 July 2018, <https://tools.ietf.org/html/draft-eckert-anima-noc-autoconfig-00>.

[OP-TECH] Wikipedia, "Operational technology", October 2020, <https://en.wikipedia.org/w/index.php?title=Operational_technology&oldid=986363045>.

[RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, DOI 10.17487/RFC1112, August 1989, <https://www.rfc-editor.org/info/rfc1112>.

[RFC1492] Finseth, C., "An Access Control Protocol, Sometimes Called TACACS", RFC 1492, DOI 10.17487/RFC1492, July 1993, <https://www.rfc-editor.org/info/rfc1492>.

[RFC1654] Rekhter, Y., Ed. and T. Li, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 1654, DOI 10.17487/RFC1654, July 1994, <https://www.rfc-editor.org/info/rfc1654>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[RFC2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, DOI 10.17487/RFC2315, March 1998, <https://www.rfc-editor.org/info/rfc2315>.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, DOI 10.17487/RFC2409, November 1998, <https://www.rfc-editor.org/info/rfc2409>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC3164] Lonvick, C., "The BSD Syslog Protocol", RFC 3164, DOI 10.17487/RFC3164, August 2001, <https://www.rfc-editor.org/info/rfc3164>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <https://www.rfc-editor.org/info/rfc3315>.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, DOI 10.17487/RFC3411, December 2002, <https://www.rfc-editor.org/info/rfc3411>.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", STD 88, RFC 3596, DOI 10.17487/RFC3596, October 2003, <https://www.rfc-editor.org/info/rfc3596>.

[RFC3954] Claise, B., Ed., "Cisco Systems NetFlow Services Export Version 9", RFC 3954, DOI 10.17487/RFC3954, October 2004, <https://www.rfc-editor.org/info/rfc3954>.

[RFC4007] Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "IPv6 Scoped Address Architecture", RFC 4007, DOI 10.17487/RFC4007, March 2005, <https://www.rfc-editor.org/info/rfc4007>.

[RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, DOI 10.17487/RFC4210, September 2005, <https://www.rfc-editor.org/info/rfc4210>.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, DOI 10.17487/RFC4364, February 2006, <https://www.rfc-editor.org/info/rfc4364>.

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006, <https://www.rfc-editor.org/info/rfc4429>.

[RFC4541] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, DOI 10.17487/RFC4541, May 2006, <https://www.rfc-editor.org/info/rfc4541>.

[RFC4604] Holbrook, H., Cain, B., and B. Haberman, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", RFC 4604, DOI 10.17487/RFC4604, August 2006, <https://www.rfc-editor.org/info/rfc4604>.

[RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, DOI 10.17487/RFC4607, August 2006, <https://www.rfc-editor.org/info/rfc4607>.

[RFC4610] Farinacci, D. and Y. Cai, "Anycast-RP Using Protocol Independent Multicast (PIM)", RFC 4610, DOI 10.17487/RFC4610, August 2006, <https://www.rfc-editor.org/info/rfc4610>.

[RFC4985] Santesson, S., "Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name", RFC 4985, DOI 10.17487/RFC4985, August 2007, <https://www.rfc-editor.org/info/rfc4985>.

[RFC5790] Liu, H., Cao, W., and H. Asaeda, "Lightweight Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Version 2 (MLDv2) Protocols", RFC 5790, DOI 10.17487/RFC5790, February 2010, <https://www.rfc-editor.org/info/rfc5790>.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://www.rfc-editor.org/info/rfc5880>.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <https://www.rfc-editor.org/info/rfc5905>.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <https://www.rfc-editor.org/info/rfc5912>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <https://www.rfc-editor.org/info/rfc6120>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC 6335, DOI 10.17487/RFC6335, August 2011, <https://www.rfc-editor.org/info/rfc6335>.

[RFC6402] Schaad, J., "Certificate Management over CMS (CMC) Updates", RFC 6402, DOI 10.17487/RFC6402, November 2011, <https://www.rfc-editor.org/info/rfc6402>.

[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>.

[RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, DOI 10.17487/RFC6554, March 2012, <https://www.rfc-editor.org/info/rfc6554>.

[RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012, <https://www.rfc-editor.org/info/rfc6724>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, DOI 10.17487/RFC6733, October 2012, <https://www.rfc-editor.org/info/rfc6733>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <https://www.rfc-editor.org/info/rfc6763>.

[RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, DOI 10.17487/RFC6824, January 2013, <https://www.rfc-editor.org/info/rfc6824>.

[RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013, <https://www.rfc-editor.org/info/rfc6830>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/info/rfc7011>.

[RFC7404] Behringer, M. and E. Vyncke, "Using Only Link-Local Addressing inside an IPv6 Network", RFC 7404, DOI 10.17487/RFC7404, November 2014, <https://www.rfc-editor.org/info/rfc7404>.

[RFC7426] Haleplidis, E., Ed., Pentikousis, K., Ed., Denazis, S., Hadi Salim, J., Meyer, D., and O. Koufopavlou, "Software-Defined Networking (SDN): Layers and Architecture Terminology", RFC 7426, DOI 10.17487/RFC7426, January 2015, <https://www.rfc-editor.org/info/rfc7426>.

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <https://www.rfc-editor.org/info/rfc7435>.

[RFC7575] Behringer, M., Pritikin, M., Bjarnason, S., Clemm, A., Carpenter, B., Jiang, S., and L. Ciavaglia, "Autonomic Networking: Definitions and Design Goals", RFC 7575, DOI 10.17487/RFC7575, June 2015, <https://www.rfc-editor.org/info/rfc7575>.

[RFC7576] Jiang, S., Carpenter, B., and M. Behringer, "General Gap Analysis for Autonomic Networking", RFC 7576, DOI 10.17487/RFC7576, June 2015, <https://www.rfc-editor.org/info/rfc7576>.

[RFC7585] Winter, S. and M. McCauley, "Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)", RFC 7585, DOI 10.17487/RFC7585, October 2015, <https://www.rfc-editor.org/info/rfc7585>.

[RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016, <https://www.rfc-editor.org/info/rfc7721>.

[RFC7761] Fenner, B., Handley, M., Holbrook, H., Kouvelas, I., Parekh, R., Zhang, Z., and L. Zheng, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", STD 83, RFC 7761, DOI 10.17487/RFC7761, March 2016, <https://www.rfc-editor.org/info/rfc7761>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8028] Baker, F. and B. Carpenter, "First-Hop Router Selection by Hosts in a Multi-Prefix Network", RFC 8028, DOI 10.17487/RFC8028, November 2016, <https://www.rfc-editor.org/info/rfc8028>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8316] Nobre, J., Granville, L., Clemm, A., and A. Gonzalez Prieto, "Autonomic Networking Use Case for Distributed Detection of Service Level Agreement (SLA) Violations", RFC 8316, DOI 10.17487/RFC8316, February 2018, <https://www.rfc-editor.org/info/rfc8316>.

[RFC8366] Watsen, K., Richardson, M., Pritikin, M., and T. Eckert, "A Voucher Artifact for Bootstrapping Protocols", RFC 8366, DOI 10.17487/RFC8366, May 2018, <https://www.rfc-editor.org/info/rfc8366>.

[RFC8368] Eckert, T., Ed. and M. Behringer, "Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance (OAM)", RFC 8368, DOI 10.17487/RFC8368, May 2018, <https://www.rfc-editor.org/info/rfc8368>.

[RFC8398] Melnikov, A., Ed. and W. Chuang, Ed., "Internationalized Email Addresses in X.509 Certificates", RFC 8398, DOI 10.17487/RFC8398, May 2018, <https://www.rfc-editor.org/info/rfc8398>.

[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>.

[RFC8572] Watsen, K., Farrer, I., and M. Abrahamsson, "Secure Zero Touch Provisioning (SZTP)", RFC 8572, DOI 10.17487/RFC8572, April 2019, <https://www.rfc-editor.org/info/rfc8572>.

[RFC8684] Ford, A., Raiciu, C., Handley, M., Bonaventure, O., and C. Paasch, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 8684, DOI 10.17487/RFC8684, March 2020, <https://www.rfc-editor.org/info/rfc8684>.

[RFC8739] Sheffer, Y., Lopez, D., Gonzalez de Dios, O., Pastor Perales, A., and T. Fossati, "Support for Short-Term, Automatically Renewed (STAR) Certificates in the Automated Certificate Management Environment (ACME)", RFC 8739, DOI 10.17487/RFC8739, March 2020, <https://www.rfc-editor.org/info/rfc8739>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

[RFC8992] Jiang, S., Ed., Du, Z., Carpenter, B., and Q. Sun, "Autonomic IPv6 Edge Prefix Management in Large-Scale Networks", RFC 8992, DOI 10.17487/RFC8992, May 2021, <https://www.rfc-editor.org/info/rfc8992>.

[RFC8993] Behringer, M., Ed., Carpenter, B., Eckert, T., Ciavaglia, L., and J. Nobre, "A Reference Model for Autonomic Networking", RFC 8993, DOI 10.17487/RFC8993, May 2021, <https://www.rfc-editor.org/info/rfc8993>.

[ROLL-APPLICABILITY] Richardson, M., "ROLL Applicability Statement Template", Work in Progress, Internet-Draft, draft-ietf-roll-applicability-template-09, 3 May 2016, <https://tools.ietf.org/html/draft-ietf-roll-applicability-template-09>.

[SR] Wikipedia, "Single-root input/output virtualization", September 2020, <https://en.wikipedia.org/w/index.php?title=Single-root_input/output_virtualization&oldid=978867619>

[TLS-DTLS13] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Work in Progress[1], Internet-Draft, draft-ietf-tls-dtls13-43, 30 April 2021, <https://tools.ietf.org/html/draft-ietf-tls-dtls13-43>.

[X.509] ITU-T, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, October 2016, <https://www.itu.int/rec/T-REC-X.509>.

[X.520] ITU-T, "Information technology - Open Systems Interconnection - The Directory: Selected attribute types", ITU-T Recommendation X.520, October 2016, <https://www.itu.int/rec/T-REC-X.520>.

Приложение A. Основы и будущее (информационный раздел)

В этом приложении приведены базовые сведения об аспектах нормативных разделов этого документа или связанных механизмах, таких как BRSKI (конкретный выбор делает ACP), а также рассмотрены возможные расширения ACP.

A.1. Схемы адресного пространства ACP

Этот документ определяет субсхемы адресации Zone, Vlong, Manual прежде всего для поддержки назначения адресных префиксов через распределенные, потенциально не согласованные регистраторы ACP, как указано в параграфе 6.11.7. Требуется 48/46-битовый идентификатор, чтобы эти регистраторы ACP могли назначать не конфликтующие префиксы адресов. Такое решение не оставляет достаточно битов для одновременной поддержки большого числа узлов (Node-ID), больших префиксов локальных адресов на каждом узле и достаточно большого набора битов для указания зоны маршрутизации. В результате субсхемы Zone и Vlong 8/16 пытаются поддерживать все свойства через раздельные префиксы.

В сетях, предполагающих всегда полагаться на централизованную систему PMS, как описано в параграфе 9.2.5, можно сохранить 48/46-битовые Registrar-ID. Такие вариации механизмов адресации ACP могут быть введены в будущих работах различными способами. При введении нового otherName можно было бы создать несовместимые вариации ACP, где можно изменить каждый аспект устройства ACP, включая выбор адресации. Если вместо этого задать новую субсхему адресации, она может быть совместимой с текущей спецификацией ACP. Такие сведения, как размер префикса зоны и префикса, выделенного самому узлу ACP, можно кодировать в поле расширения acp-node-name.

Отметим, что явно заданная субсхема назначения адресов вручную (Manual) всегда предпочтительней для предоставления узлам ACP простого способа запрета некорректной неавтономной настройки любых неручных адресных пространств ACP и, следовательно, предотвращения влияния таких неавтономных операций на корректную маршрутизацию для любых неручных адресов ACP, назначенных по сертификатам ACP.

A.2. Начальная загрузка BRSKI (ANI)

BRSKI описывает, как узлы с сертификатом IDevID можно безопасно автоматическим (zero-touch) регистрировать по их сертификату LDevID для поддержки ACP. BRSKI также применяет ACP для поддержки автоматической (zero-touch) начальной загрузки через сети без каких-либо требований к конфигурации транзитных узлов (например, DHCP, пересылка DNS, организация сервера). Это включает ненастроенные в остальном сети, как указано в параграфе 3.2. Поэтому BRSKI в сочетании с ACP обеспечивает защищённое и автоматическое (zero-touch) решения для управления целыми сетями. Узлы, поддерживающие такую инфраструктуру (BRSKI и ACP) зазывают узлами ANI (Autonomic Networking Infrastructure, см [RFC8993]). Узлы, которые не поддерживают сертификат IDevID и имеют лишь (незащищённый) уникальный идентификатор устройства (Unique Device Identifier или UDI) от производителя или узлы, производитель которых не поддерживает MASA могут использовать будущую версию BRSKI со сниженной защитой.

[1]Опубликовано в RFC 9147. *Прим. перев.*

При использовании BRSKI для предоставления сертификата домена (зачисления), регистратор BRSKI (выступающий как расширенный сервер EST) должен включать закодированный в otherName/AcpNodeName адрес ACP и имя домена для зачисляемого узла (заявитель) в свой отклик на запрос атрибутов заявителя EST CSR, обязательный в BRSKI.

CA в сети ACP недопустимо менять otherName/AcpNodeName в сертификатах. Поэтому узлы ACP могут найти свои адреса ACP и домен по этому полю в сертификатах домена как для себя, так и для других узлов.

Применение BRSKI вместе с ACP может дополнительно упростить обслуживание и обновление сертификатов домена. Можно, не полагаясь на CRL, сделать срок действия сертификатов очень коротким, например, в несколько часов. Когда узлу не удаётся подключиться к ACP в течение срока действия сертификата, он не сможет подключиться к ACP для обновления сертификата (просто используя EST), но может обновить его как зачисленный заявитель с истекшим сроком через прокси начальной загрузки BRSKI. Для этого требуется лишь признание регистратором BRSKI просроченных сертификатов домена и выполнение заявителем аутентификации TLS для начальной загрузки BRSKI с использованием сертификата домена, прежде чем вернуться к применению сертификата IDevID для BRSKI. Этот механизм может сделать CRL ненужными, поскольку регистратор BRSKI в сочетании с CA не будет обновлять отозванные сертификаты - потребуется лишь список Do-not-renew (не обновлять) у регистратора BRSKI или CA.

В отсутствие BRSKI или менее защищённых вариантов предоставление сертификатов может включать одно или несколько действий или нестандартную автоматизацию. Производители узлов обычно поддерживают предоставление сертификатов узлам через PKCS #7 (PKCS #7: Cryptographic Message Syntax Version 1.5 [RFC2315]) и могут поддерживать предоставление через фирменные модели по протоколу NETCONF (Network Configuration Protocol (NETCONF) [RFC6241]). Если такие узлы поддерживают NETCONF Zero Touch [RFC8572], это можно комбинировать с автоматическим (zero-touch) предоставлением сертификатов узлам. Однако без эквивалентной интеграции соединений NETCONF через ACP, как в BRSKI, эта комбинация не сможет поддерживать автоматическую начальную загрузку через ненастроенную сеть.

A.3. Выбор протокола обнаружения соседей ACP

В этом приложении обосновывается выбор GRASP DULL в качестве протокола обнаружения смежных на уровне L2 узлов в качестве кандидатов в соседи ACP. Рассматривались также варианты GRASP, mDNS, LLDP.

A.3.1. LLDP

LLDP и более ранний протокол Cisco CDP (Cisco Discovery Protocol) являются примерами протоколов обнаружения L2, которые завершают свои сообщения на портах L2. Если бы эти протоколы были выбраны для обнаружения соседей ACP, процесс обнаружения также завершался бы на портах L2. Это помешало бы созданию ACP через коммутаторы без поддержки ACP, поддерживающие LLDP или CDP. LLDP имеет расширения, использующие разные MAC-адреса, и это можно было бы применить для обнаружения в ACP, но требуемая дополнительная стандартизация в IEEE и определение профиля для такого изменённого варианта LLDP показались требующими слишком большой работы по сравнению с преимуществами от использования имеющегося протокола LLDP для этой очень простой задачи.

A.3.2. mDNS и поддержка L2

Протокол Multicast DNS (mDNS) (Multicast DNS [RFC6762]) с записями о ресурсах DNS Service Discovery (DNS-SD) , определёнными в DNS-Based Service Discovery [RFC6763] был основным претендентом на роль протокола обнаружения в ACP. Поскольку протокол основан на групповой адресации IP link-local, он работает на уровне подсети и встречается в коммутаторах L2. Авторы документа не знают реализаций mDNS, завершающих свои сообщения mDNS на портах L2 вместо уровня подсети. При использовании mDNS как протокола обнаружения в ACP на коммутаторе (L3)/L2 с поддержкой ACP, как описано в разделе 7, это потребовалось бы реализовать. Вполне вероятно, что завершение соединений mDNS может применяться только ко всем сообщениям mDNS от такого порта, что затем потребует программной пересылки всех не относящихся к ACP сообщений mDNS для поддержки поддержки прежней функциональности mDNS, не связанной с ACP. Таким образом, добавление поддержки ACP на таких коммутаторах L2 с mDNS может создать проблемы возвращения к прежней функциональности mDNS на этих узлах. С учётом низкой производительности программной пересылки во многих коммутаторах L2, это могло сделать поддержку ACP на таких коммутаторах L2 рискованной.

A.3.3. Почему DULL GRASP?

LLDP не подошёл из-за отмеченных выше проблем, а MDNS не был выбран с учётом приведённых соображений для L2 mDNS и указанных ниже обстоятельств.

Если mDNS ещё нет на узле, его реализация потребует больше работы по сравнению с реализацией DULL GRASP, а если применять имеющуюся реализацию mDNS, вероятно потребуется больший объем кода, нежели для отдельной реализации DULL GRASP или общей реализации DULL GRASP и GRASP в ACP.

A.4. Выбор протокола маршрутизации (RPL)

В этом приложении приведены мотивы выбора RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks [RFC6550]) в качестве принятого по умолчанию (в этой спецификации единственного) протокола маршрутизации для ACP. Выбор и приведённый выше профиль были основаны на предстандартной реализации ACP, успешно развёрнутой в действующих сетях. Требования к маршрутизации в ACP указаны ниже.

- Самоуправление. Плоскость ACP должна создаваться автоматически, без участия человека, поэтому протокол маршрутизации также должен работать автоматически. RPL является простым протоколом с самоуправления, который не требует зон или областей. Он также самостоятельно настраивается, поскольку конфигурация передаётся как часть протокола (параграф 6.7.6 в [RFC6550]).
- Расширяемость маршрутизации. ACP создаётся в целом домене, которым может быть сеть большого предприятия или сервис-провайдера. Поэтому протокол маршрутизации должен поддерживать сотни тысяч узлов в идеальном варианте без разделения на зоны или области. RPL обеспечивает такую возможность, основанную на широком применении заданных по умолчанию маршрутов.

- Малое потребление ресурсов. ACP поддерживает традиционную инфраструктуру сети, поэтому работает в дополнение к традиционным протоколам. ACP и особенно протокол маршрутизации должны потреблять немного ресурсов памяти и CPU. В частности, на граничных узлах, где мало таких ресурсов, их потребление следует минимизировать. RPL создаёт дерево DODAG, где основным потребителем ресурсов является корень DODAG. Чем ближе граница сети, тем меньше состояний нужно поддерживать. Это подходит для типового устройства сетей. Кроме того, все изменения ниже общего предка сохраняются ниже родительского узла.

- Поддержка неструктурированного пространства адресов. В ANI адреса узлов служат идентификаторами и могут назначаться без учёта топологии. Кроме того, узлы могут перемещаться в топологии без смены адреса. Поэтому протокол маршрутизации должен поддерживать неструктурированное пространство адресов. Протокол RPL разработан для мобильных специализированных (ad hoc) сетей без допущений о топологической привязке адресов.

- Модульность. Для сохранения первоначальной реализации небольшой с возможностью позднее добавлять более сложные методы, крайне желательно, чтобы протокол маршрутизации имел простую базовую функциональность, но при необходимости мог импортировать функциональные модули. RPL обладает такими свойствами с концепцией «целевой функции», которая служит подключаемым модулем для маршрутизации.

- Расширяемость. Поскольку концепция ANI является новой, вполне вероятны изменения в её работе со временем. RPL позволяет добавлять целевые функции, которые могут менять способ создания деревьев DAG протоколом маршрутизации.

- Поддержка множества топологий. В будущем может потребоваться поддержка нескольких деревьев DODAG для разных задач с использованием различных целевых функций. RPL позволяет создавать несколько параллельных DODAG, это может служить для создания нескольких топологий для доступа к разным корням.

- Отсутствие требования к оптимизации пути. RPL не обязательно рассчитывает оптимальный путь между двумя узлами. Сегодня ACP этого не требует, поскольку работает в основном с нечувствительными к задержкам контурами обратной связи. В будущем могут потребоваться иные схемы оптимизации, но RPL можно расширить (см. выше).

A.5. Распространение информации ACP и групповая передача

Групповая передача IP не применяется в ACP, поскольку в ANI это не требуется и нужно лишь для анонсирования и обнаружения служб. Применение групповой передачи IP потребовало бы разработки решения по автоматической (zero-touch) настройке конфигурации для ASM (Any Source Multicast - исходная форма групповой передачи IP из Host extensions for IP multicasting [RFC1112]), что было бы достаточно сложно и необоснованно. Одним из аспектов сложности, для которого в документах IETF не предпринималось попыток решения, является автоматический выбор маршрутизаторов на роль «точек встречи независимой от протокола групповой передачи в разреженном режиме» (PIM Sparse Mode (PIM-SM) Rendezvous Point (RP), см. Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised) [RFC7761]). Другим аспектом сложности является реализация MLD (Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast [RFC4604]), PIM-SM и Anycast-RP (Anycast-RP Using Protocol Independent Multicast (PIM) [RFC4610]). Если такие реализации уже имеются в проукции, они скорей всего будут привязаны к ускоренной пересылке, потребляющей аппаратные ресурсы, что сложно оправдать затратами лишь на обнаружение служб.

Будущие агенты ASA могут потребовать высокопроизводительной репликации данных в сети. В этом случае будет оправдано применение групповой передачи IP. Такие ASA могут применять обнаружение служб ACP GRASP и тогда им для репликации потребуется не ASM, а лишь SSM (Source-Specific Multicast for IP [RFC4607]). SSM можно просто включить в плоскости данных (или даже в обновлении ACP) без какой-либо настройки свех включения на всех узлах и для этого нужна лишь простая версия MLD (Lightweight Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Version 2 (MLDv2) Protocols [RFC5790]).

Протоколы маршрутизации IGP на основе протокола состояния канала (Link State Protocol или LSP) обычно имеют механизм лавинной рассылки информации и такой механизм может служить для лавинной рассылки целей GRASP путём задания их как информации IGP. Это могло бы быть оптимизацией для будущих версий ACP с протоколом маршрутизации на основе LSP. Однако такой механизм не будет легко работать для сообщений GRASP M_DISCOVERY, для которых применяется интеллектуальная (ограниченная) лавинная рассылка не через всю ACP, а лишь узлу, где найден ответчик. Предполагается, что многие будущие службы в ASA будут иметь лишь несколько потребляющих ASA, а для этого метод M_DISCOVERY эффективней лавинной рассылки через весь домен.

Поскольку в ACP применяется RPL, желательным расширением будет использование имеющегося в RPL понятия DODAG (дерево распространения без петель) для повышения эффективности лавинной рассылки GRASP для M_FLOOD и M_DISCOVERY. В параграфе 6.13.5 указано, как это будет полезно для интерфейсов NBMA. В настоящее время это не задано в документе, поскольку ещё не совсем понятно, как будет влиять на лавинную рассылку GRASP время схождения RPL DODAG и сколь сложно будет лавинной рассылке GRASP получить доступ к дереву DODAG.

A.6. CA, домены и маршрутные субдомены

Имеется много решений по установке ACP с подобающим использованием CA, домена и элементов rsub в acp-node-name сертификата домена. Эти варианты обобщены здесь, поскольку они описаны в разных частях документа. Рассмотрены также возможные и желаемые расширения.

Домен ACP - это множество всех узлов ACP которые могут аутентифицировать друг друга, как принадлежащих к одной сети ACP путём проверки принадлежности к домену ACP (6.2.3. Проверка принадлежности к домену ACP). GRASP в ACP работает через все транзитивно соединённые узлы ACP в домене. Элемент rsub в acp-node-name разрешает применение адресов из разных префиксов ULA. Одним из вариантов использования является сведение множества физических сетей, которые исходно разделены и имеют один домен ACP с разными субдоменами маршрутизации, чтобы все узлы могли взаимно доверять сертификатам ACP (независимо от rsub) и могли позднее объединиться в непрерывную сеть ACP. Одним из примеров такого решения является ACP для регионов, соединённых через ядро без поддержки ACP, скажем, по причине отсутствия решения с ACP для маршрутизаторов ядра. Конфигурации ACP

connect, определённые в этом документе, могут служить для расширения и соединения этих островков ACP с NOC и слияния в одну плоскость ACP, когда появятся нужные решения для маршрутизаторов ядра.

Отметим, что RPL расширяется очень хорошо. Не требуется использовать множество субдоменов маршрутизации для расширения доменов ACP, как это требовалось бы при использовании других протоколов маршрутизации. Они рассмотрены лишь в качестве вариантов по упомянутым выше причинам.

Если нужно создать домена ACP, которым по умолчанию не разрешено соединяться между собой, просто используются разные элементы domain в acp-node-name. Эти элементы могут быть произвольными, в том числе иерархическими - домены example.com и research.example.com будут раздельными, если оба значения указаны в элементах domain в acp-node-name соответствующих сертификатов.

Не требуется иметь разные CA для разных доменов ACP, оператор может предоставлять один CA для подписывания сертификатов множества доменов ACP, которым не разрешено соединяться между собой, поскольку проверка смежности в ACP включает сравнение domain.

Если несколько независимых сетей используют одно имя домена, но в каждой используются свои CA, эти сети не образуют одного домена ACP, поскольку CA различаются. Поэтому не возникает проблемы выбора доменного имени, которое может использовать кто-то ещё. Тем не менее, настоятельно рекомендуется выбирать для доменов имена, которые с большой вероятностью будут уникальны. Рекомендуется использовать доменные имена, содержащие имя домена в DNS, принадлежащего назначающей организации, и уникальный в рамках организации префикс, например, acp.example.com в домене example.com.

A.7. Намерения для ACP

Намерения (Intent) - это компонент архитектуры автономных сетей (Autonomic Networks) [RFC8993], позволяющий операторам задавать правила для сети. Применимость намерений достаточно широка и гибка, возможным применением является лавинная рассылка политики через ACP GRASP и её интерпретация каждым узлом ACP.

Одной из проблем будущих определений для намерений является проблема циклических зависимостей при выражении намерений для самой плоскости ACP. Например, намерения могут указывать желание собрать ACP из всех доменов, имеющих общий родительский домен (не полагаясь на решение rsub для субдоменов маршрутизации, заданное в документе) - узлам ACP из доменов example.com, access.example.com, core.example.com, city.core.example.com следует создать одну плоскость ACP.

Если у каждого домена имеется свой источник намерений, тогда намерения должны просто разрешать добавление TA и доменных имён партнерских доменов в параметры проверки принадлежности к домену ACP (6.2.3. Проверка принадлежности к домену ACP), чтобы узлы из этих отдельных доменов воспринимались как партнёры ACP.

Если намерения исходят лишь из одного домена, они, скорей всего, не сработают, поскольку другие домены не создадут соединений ACP между собой, независимо от использования одного или разных CA, в результате проверки принадлежности к домены ACP.

Если домены используют общий CA, они могут изменить настройку ACP, чтобы разрешить соединения ACP между узлами ACP с разными acp-domain-name, но лишь для распространения ограниченных сведений, таких как намерения (Intent), но не для организации полной связности ACP, в частности, не будет маршрутизации RPL и передачи произвольных сведений GRASP, пока правила Intent не позволят делать это через границы доменов.

Этот тип подхода, когда ACP сначала разрешает работу Intent и лишь потом настраивает остальную часть связности ACP на основе политики Intent, можно также использовать для включения правил Intent, которые будут ограничивать функциональность ACP внутри домена, если никакая политика не будет мешать распространению Intent, например, для ограничения доступности через ACP некоторых типов узлов или мест их размещения.

A.8. Адаптация концепций ACP для других сред

Плоскость ACP, заданная в этом документе, очень подробно описывает выбор опций, обеспечивающих совместимость реализаций. Принятый выбор может быть не лучшим, но концепции ACP можно применить для производных решений.

ACP задаёт применение ULA и вывод префикса по имени домена, чтобы не требовалось выделять адреса для развёртывания ACP. Плоскость ACP будет одинаково работать с любым префиксом IPv6 /48, а не только с ULA. Этот префикс может быть просто параметром регистраторов ACP (например, при использовании BRSKI) для зачисления сертификатов домена вместо вывода регистратором ACP префикса ULA /48 из имени домена автономной сети (AN).

В некоторых решениях уже может быть схема автоматической адресации, выведенная, например, из уникальных идентификаторов устройств (скажем, MAC). В этих случаях выделение адресов через поле адресных сведений ACP, описанное в документе, может быть нежелательно. Сертификат может просто служить для указания домена ACP, а поле адреса можно опустить. Единственное исправление, которое потребуется для оставшегося способа работы ACP, заключается в задании другого элемента в сертификате домена для распределения между двумя партнёрами ролей Decider и Follower при организации защищённого канала. Отметим, что в будущих работах адрес ACP может служить для аутентификации принадлежности адреса устройству. Если применяемый устройством адрес ACP выводится из имеющегося постоянного локального идентификатора (такого как MAC-адрес), будет полезно внести его в сертификат.

ACP определяется как отдельный экземпляр VRF, поскольку предназначена для поддержки хорошо управляемых сетей с широким набором конфигураций. Поэтому надёжная, не нарушаемая настройками связность может быть получена от самой плоскости данных. В решениях, где все функции, влияющие на транзитную связность (включая защиту), автоматизированы, неразрушаемы и устойчивы к отказам, можно было бы исключить потребность ACP быть отдельным экземпляром VRF. Рассмотрим простой пример системы, в которой нет отдельной плоскости данных, а её роль играет ACP. Добавление BRSKI делает её полностью автономной сетью (AN), за исключением того, что не поддерживается автоматическая адресация оборудования. Это можно исправить, добавив решение на основе Autonomic IPv6 Edge Prefix Management in Large-Scale Networks [RFC8992].

TCP/TLS как протоколы, обеспечивающие надёжность и безопасность GRASP в ACP могут не оказаться предпочтительными в сетях с ограничениями. Например, протокол CoAP/DTLS (Constrained Application Protocol) может

быть лучше, если он уже применяется, поскольку это снизит размер кода для ACP на устройствах с ограничениями. Поэтапная надёжность для сообщений ACP GRASP может быть обеспечена для поддержки таких протоколов, как DTLS, путём добавления такого же типа согласования, какой определён в этом документе для защищённых каналов ACP. В будущих расширениях ACP для поддержки устройств с ограничениями могут быть созданы сквозные соединения GRASP для выбора их транспортного протокола путём указания поддерживаемых протоколов (например, TLS/DTLS) в параметрах GRASP из цели GRASP, через которую обнаруживается конечная точка.

RPL - протокол маршрутизации в ACP - явно не оптимизирует кратчайшие пути и скорейшее схождение. Варианты ACP могут воспользоваться иным протоколом или разработать усовершенствованные профили RPL.

Такие изменения, как используемый протокол маршрутизации, создание ACP в VRF (как предложено выше) или как фактической плоскости данных, могут автоматически выбираться в реализации для поддержки нескольких вариантов путём их выведения из будущих параметров сертификатов. Параметры в сертификатах следует ограничивать набором, который нужно менять не чаще, чем сертификат обновляется, или обеспечить возможность предоставления этих параметров до активации варианта ACP на узле. С помощью BRSKI это можно сделать, например, в виде дополнительной сигнализации сразу после зачисления сертификата, по-прежнему применяя соединение BRSKI TLS и не задавая дополнительных требований к нему.

Протоколы защиты канала, включая их инкапсуляцию, легко добавляются в решения ACP. Защищённые поэтапные (hop-by-hop) каналы ACP на сетевом уровне легко заменить сквозной защитой в сочетании с другими мерами защиты инфраструктуры. Во всех будущих сетевых OAM следует применять сквозную защиту. При использовании сертификатов домена она не будет зависеть от услуг, предоставляемых защищёнными каналами ACP.

A.9. Дополнительные (будущие) варианты

A.9.1. Автоматическое агрегирование маршрутов

Маршрутизация в ACP в соответствии с этой спецификацией использует лишь стандартный механизм оптимизации маршрутов RPL, например, сохраняя лишь маршруты, не ведущие к корню RPL. Известно, что это работает для сетей с 20000 и более узлов. Автоматическое агрегирование маршрутов для префиксов ULA /48 (при использовании rsub в acp-node-name) и префиксов на основе Zone-ID не предусмотрено. Автоматическое назначение Zone-ID и автоматическое агрегирование моршрутов можно организовать, например, путём настройки границ зоны, анонсирования через GRASP в зоны параметров зон (Zone-ID и префикс ULA /48) и автоматического агрегирования маршрутов на границе зоны. Узлы будут назначать Zone-ID и, возможно, даже префикс /48 на основе анонсов GRASP.

A.9.2. Варианты исключения зависимости от плоскости данных IPv6

Как описано в параграфе 6.13.2, ACP зависит от плоскости данных при адресации IPv6 link-local на интерфейсах. Использование отдельного MAC-адреса для ACP позволяет полностью изолировать ACP от плоскости данных совместимым с этой спецификацией способом. Это также будет идеальным вариантом при использовании виртуализации ввода-вывода с одним корнем (single-root input/output virtualization или SR-IOV, см. [SR]) в реализации ACP, поскольку разные интерфейсы SR-IOV используют свои MAC-адреса.

Если дополнительные адреса MAC недоступны, можно отделить ACP через разные точки демультиплексирования. Один интерфейс подсети может иметь свои интерфейсы IPv6 для ACP и плоскости данных, что позволит разделить их адреса link-local и интерфейс ACP не будет доступен для настройки из плоскости данных. Это тоже совместимо со спецификацией и не препятствует совместимости.

Вариантом, требующим дополнительной спецификации, является применение Ethertype, отличного от 0x86DD (IPv6) при инкапсуляции пакетов IPv6 для ACP. Это похоже на подход, применяемый для аутентификации пакетов IP в [IEEE-802.1X] с использованием Ethertype (0x88A2) расширяемого протокола аутентификации в ЛВС (Extensible Authentication Protocol over Local Area Network или EAPoL) .

Отметим, что в случае узлов ANI приведённые выше соображения применимы в равной степени к инкапсуляции пакетов BRSKI, включая применение GRASP для BRSKI.

A.9.3. ACP API и рабочие модели (YANG)

В будущих работах следует определить модель данных YANG [RFC7950] или внутренние API узлов для мониторинга и управления ACP. В такие модели и API необходимо включить поддержку таблицы смежности ACP (6.3. Таблица смежности ACP) и ACP GRASP.

A.9.4. Усовершенствование RPL

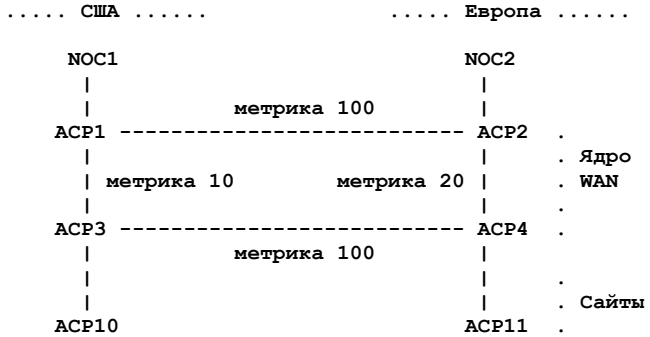

Рисунок 17. Двойной NOC.

Заданный в этом документе профиль RPL создаёт единственный путь через связующее дерево (spanning-tree) к корню (обычно регистратор в NOC). При наличии нескольких NOC маршрутизация к некорневым NOC может быть неоптимальной (Рисунок 17). Предположим, что узел ACP1 становится корнем RPL. Трафик между ACP11 и NOC2

пойдёт через ACP4-ACP3-ACP1-ACP2 вместо ACP4-ACP2, поскольку рассчитанное RPL дерево DODAG и маршруты будут кратчайшими путями к корню RPL. Чтобы преодолеть эти ограничения, можно оптимизировать изменения и/или расширения RPL для нескольких NOC. Это требует использования особенностей (artifact) плоскости данных, включая инкапсуляцию и декапсуляцию IP-in-IP на маршрутизаторах ACP, а также обработку заголовков IPv6 RPI. В качестве варианта можно использовать записи таблицы маршрутизации (Src, Dst).

Лавинная рассылка сообщение ACP GRASP может быть дополнительно ограничена и, следовательно, оптимизирована использованием её лишь на каналах, являющихся частью RPL DODAG.

A.9.5. Назначение роли

ACP connect является явным механизмом «утечки» трафика ACP (например, в NOC). Поэтому возможны угрозы безопасности при использовании ACP connect на скомпрометированных узлах ACP. Одним из простых решений является задание расширения в информационном поле сертификата ACP, указывающего возможность настройки ACP connect на данном узле. Это можно сделать аналогично управлению возможностью узла становиться регистратором.

Связывание разрешённых «ролей» узла ACP с сертификатом ACP обеспечивает достаточно надёжную защиту от ошибочной настройки, но может потребовать изменения кода.

Ещё одна интересная роль, которую можно задать в сертификате, - это узел NOC. Это позволит разрешать некоторые типы соединений (например, OAM TLS) только инициаторам и ответчикам NOC.

A.9.6. Автономный транзит L3

В этой спецификации ACP может организовывать автономную связность лишь через узлы L2 и требует неавтономной настройки для туннелей через узлы L3. В будущих работах следует определить механизмы для автоматического туннелирования ACP через сети L3. Вариант звезды (hub-and-spoke) позволит создавать туннели через Internet в облако или центральный экземпляр ACP. Одноранговый (peer-to-peer) механизм туннелирования будет соединять островки ACP через инфраструктуру L3VPN.

A.9.7. Диагностика

В параграфе 9.1 описаны варианты диагностики, которые можно применять без изменения внешних, влияющих на взаимодействие характеристик реализации ACP. Можно улучшить диагностику ACP с помощью дополнительных сигнальных расширения, как указано ниже.

1. Оценка приемлемости LLDP в качестве рекомендуемой функциональности для устройств ANI с целью улучшения диагностики и, при положительном решении, выбор информационных элементов для сигнализации (отметим, что такие сведения передаются без защиты). Это может включать новые элементы информации.
2. Вместо LLDP можно определить диагностическую цель DULL GRASP для переноса этих сведений.
3. Сертификаты IDevID заявителей BRSKI следует включать в выбранный незащищённый вариант диагностики. Это может быть нежелательно,если раскрытие сведений об устройстве считается серьёзной проблемой безопасности (например, возможность получить сведения для атаки на основании модели устройства).
4. Следует предоставлять более широкий набор диагностических сведений по защищённым каналам ACP с использованием одноэтапного (single-hop) механизма GRASP или определения топологии в масштабе сети.

A.9.8. Предотвращение и обработка атак от скомпрометированных устройств

Скомпрометированные узлы ACP создают наибольший риск для работы сети. Ниаболее распространёнными типами компрометации являются утечка свидетельств, применяемых для управления и настройки устройств и программ, включая изменение свидетельств доступа, но не изменение программ. В любом случае большей части современного сетевого оборудования следует иметь инфраструктуру для защиты загрузки и программ, поэтому атаки с использованием вредоносного ПО организовать сложнее. Наиболее важным аспектом защиты от этих типов атак является отказ от методов доступа к конфигурации по имени пользователя и паролю в пользу основанных на сертификатах свидетельств, которые выдаются лишь узлам, где очевидна невозможность утечки секретных ключей. Это ограничивает неожиданное распространение свидетельств.

Если требуется поддерживать основанные на паролях свидетельства для настройки устройств, их недопустимо делать настраиваемыми локально, предоставляя и проверяя их лишь удалённо (через такие протоколы, как RADIUS или Diameter), и не должно быть локальной конфигурации, позволяющей изменить эти механизмы аутентификации. В идеале следует выполнять автоматическую настройку через ACP (см. [NOC-AUTOCONFIG]).

Без физического доступа к скомпрометированному устройству злоумышленники с доступом к конфигурации не должны иметь возможность разорвать связность ACP, даже если они способны разрывать или иначе (подмена адресов) воздействовать на связность плоскости данных через настройку. Для достижения этого необходимо исключать для ACP предоставление параметров конфигурации, позволяющих включать и отключать интерфейсы. Например, может быть конфигурация ACP блокирующая текущую конфигурацию ACP, пока не будет сброса к заводским настройкам.

С помощью таких мер действительная администрация имеет хорошие шансы сохранить доступ к узлам ACP, обнаруживать вредоносные конфигурации (например, путём отслеживания из центра) и должным образом реагировать. Основной реакцией является отзыв или изменение сертификатов, разрыв имеющихся вредоносных сеансов управления и исправление конфигурации. Обеспечение автоматического завершения сеансов управления с недействительными свидетельствами без возможности восстановить их, скорей всего, требует дополнительной работы. Лишь в случае невозможности выполнить такие действия потребуется отозвать или завершить срок действия сертификата ACP и считать узел отключённым, пока проблема не будет решена (для этого может потребоваться физический доступ к узлу).

Без расширений скомпрометированные узлы ACP можно удалить из ACP лишь по мере распространения сведений CRL/OCSP об отзыве или завершении срока (без удаления) краткосрочных сертификатов. Будущие расширения ACP могут, например, использовать лавинное распространение GRASP для инициированных обновления CRL/OCSP или явную индикацию удаления сертификатов домена для скомпрометированных узлов.

A.9.9. Обнаружение атак с понижением на защищённый канал ACP

Ниже описан механизм защиты от атак на понижение без добавления нового специализированного механизма защищённого канала GRASP. Механизм полагается на запуск GRASP после организации протокола защищённого канала для проверки, не был ли организованный вариант защищённого канала результатом MITM-атаки с понижением.

Участники MITM-атаки могут инициировать атаки на снижение версии для защищённого канала ACP путём фильтрации и/или изменения сообщений DULL GRASP и/или фактических пакетов данных в защищённом канале. Например, если в какой-то момент трафик DTLS легче расшифровать, чем трафик IKEv2, MITM-атака может фильтровать все пакеты IKEv2, чтобы вынудить узлы ACP применять DTLS (в предположении, что эти узлы поддерживают DTLS и IKEv2).

В случаях, когда такие MITM-атаки не способны внедрить вредоносный трафик (но способны трафик расшифровать), атаки с понижением можно обнаружить после организации защищённого канала, например, с использованием описанного ниже типа механизма.

После организации защищённого канала два партнёра ACP согласуют с помощью принятого (ещё не задан) механизма GRASP протокол защиты канала ACP, который им следует выбрать (в отсутствие MITM-атаки). Это согласование будет указывать опции защищённого канала ACP, анонсированные DULL GRASP каждого из партнёров, затем последует анонс предпочтительного протокола защиты канала от партнёра ACP, ставшего решающим (Decider) при организации канала, т. е. партнёра ACP выбирающего протокол для использования. Если этот выбранный протокол отличается от выбранного фактически, это говорит о наличии MITM-атаки или похожей проблемы (например, межсетевого экрана, препятствующего использованию конкретного протокола). Это обнаружение может обеспечить варианты смягчения последствий, такие как запись в системный журнал и последующие расследования.

Благодарности

Эта работа стала результатом проекта Autonomic Networking компании Cisco Systems, начатого в начале 2010 г. В ACP внесли свой вклад и идеи множество людей, включая (в алфавитном порядке) Ignas Bagdonas, Parag Bhide, Balaji BL, Alex Clemm, Yves Hertoghs, Bruno Klauser, Max Pritikin, Michael Richardson, Ravi Kumar Vadapalli. Отдельная благодарность Brian Carpenter, Elwyn Davies, Joel Halpern и Sheng Jiang за их подробные рецензии.

Большое спасибо Ben Kaduk, Roman Danyliw и Eric Rescorla за их рецензии SEC AD, Russ Housley и Erik Kline за рецензии, а также Valery Smyslov, Tero Kivinen, Paul Wouters, Yoav Nir за обзор параметров IPsec и IKEv2 и способствование в понимании этих и других протоколов защиты. Спасибо Carsten Bormann за помощь в CBOR/CDDL. Комментарии, отзывы и предложение предоставили также Rene Struik, Benoit Claise, William Atwood, Yongkang Zhang.

Участники работы

Все, что связано с GRASP, включая код проверки, текст документа и технические сведения

Brian Carpenter
School of Computer Science
University of Auckland
PB 92019
Auckland 1142
New Zealand
Email: brian.e.carpenter@gmail.com

RPL и все, что связано с BRSKI и начальной загрузкой, включая код проверки, текст документа и технические сведения

Michael C. Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca
URI: http://www.sandelman.ca/mcr/

Выбор и текст о технологии RPL

Pascal Thubert
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
06254 Mougins - Sophia Antipolis
France
Phone: +33 497 23 26 34
Email: pthubert@cisco.com

Адреса авторов

Toerless Eckert (editor)
Futurewei Technologies Inc. USA
2330 Central Expy
Santa Clara, CA 95050
United States of America
Email: tte+ietf@cs.fau.de

Michael H. Behringer (editor)
Email: michael.h.behringer@gmail.com

Steinthor Bjarnason
Arbor Networks
2727 South State Street, Suite 200
Ann Arbor, MI 48104
United States of America
Email: sbjarnason@arbor.net

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru