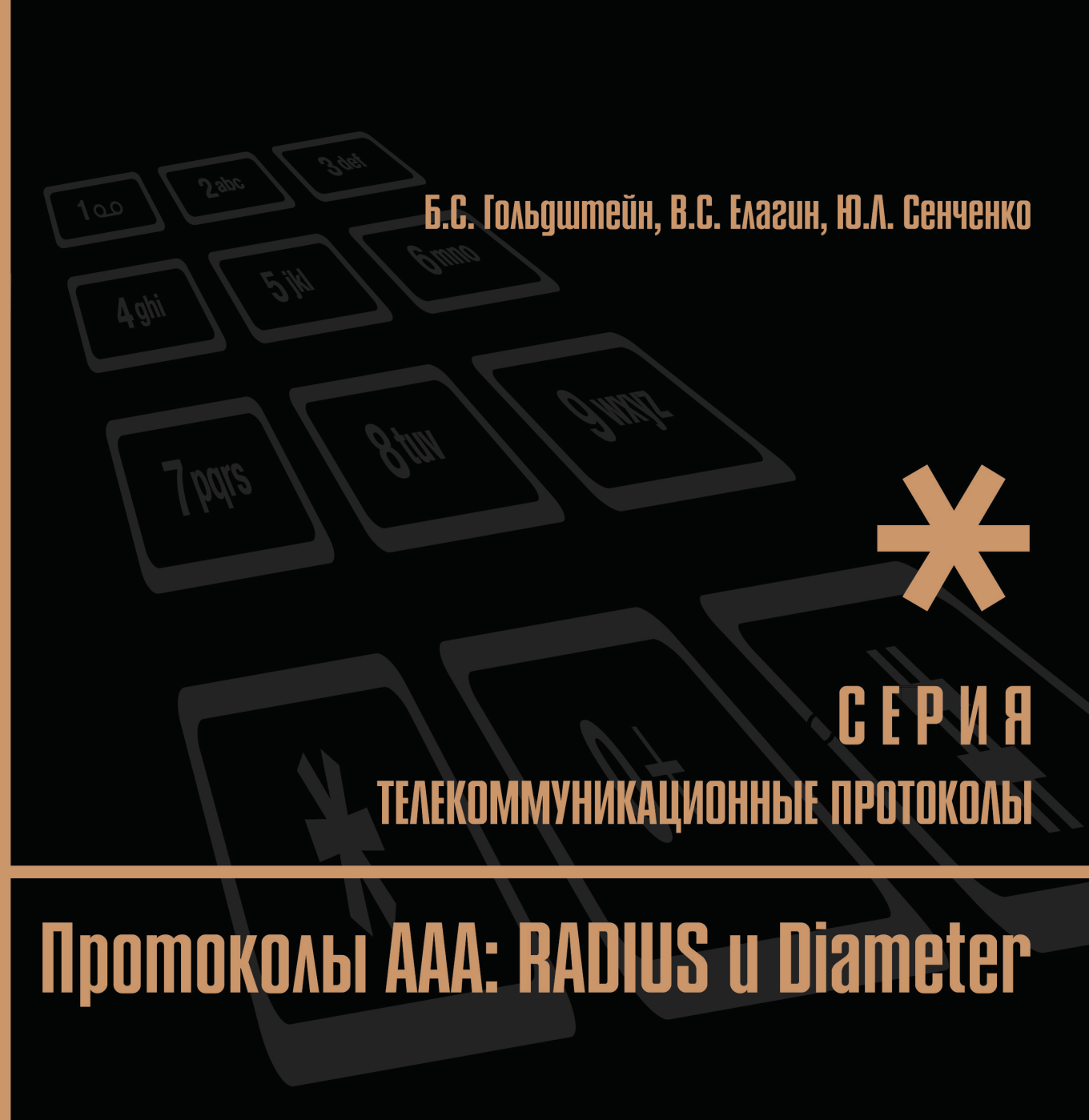

Б.С. Гольдштейн, В.С. Елагин, Ю.Л. Сенченко

СЕРИЯ

ТЕЛЕКОММУНИКАЦИОННЫЕ ПРОТОКОЛЫ

Протоколы AAA: RADIUS и Diameter

Б. С. Гольдштейн, В. С. Елагин, Ю. Л. Сенченко

Серия
«Телекоммуникационные протоколы ЕСЭ РФ»

Протоколы AAA: RADIUS и Diameter

Книга 9

Санкт-Петербург
«БХВ-Петербург»
2014

УДК 621.395
Г63
ББК 32.88

Б. С. Гольдштейн, В. С. Елагин, Ю. Л. Сенченко
Протоколы AAA: RADIUS и Diameter. Серия «Телекоммуникационные протоколы». Книга 9 – СПб.: БХВ-Петербург, 2014. – 352 с.: ил.

ISBN 978-5-9775-3052-1

Рассматриваются протоколы и процедуры аутентификации, авторизации и учета AAA (Authentication, Authorization, Accounting) в современных сетях мобильной и фиксированной связи. AAA обеспечивают управление доступом к любым сетям связи и играют ключевую роль всюду, где требуется представить конечному пользователю счет за предоставленные инфокоммуникационные услуги, включая традиционную телефонию, широкополосный доступ, услуги маршрутизации, услуги шлюза и т.п. Важность AAA-операций все более возрастает по мере распространения сетей NGN/IMS. Книга содержит подробные сведения о двух наиболее распространенных сегодня AAA-протоколах.

Серия «Телекоммуникационные протоколы»

ISBN 978-5-9775-3052-1

Издательство «БХВ-Петербург», 190005, Санкт-Петербург, Измайловский пр., 29

Содержание

Глава 3. Протокол Diameter 145

Предисловие

«*Когда денег нет, то лучше еще, чем уже*» подметил композитор Никита Богословский. Определение границы между *еще* и *уже* для того или иного пользователя той или иной инфокоммуникационной услугой в современных сетях связи осуществляется средствами AAA. Триединый термин AAA обозначает действия по *аутентификации*, *авторизации* и *учету* (*Authentication, Authorization, Accounting*). Важность AAA-операций все более возрастает по мере распространения сетей NGN/IMS, хотя функции AAA обеспечивают управление доступом к любым сетям связи и играют ключевую роль всюду, где требуется представить конечному пользователю счет за предоставленные инфокоммуникационные услуги. Речь идет обо всех сетевых услугах, включая традиционную телефонию, широкополосный доступ, услуги маршрутизации, услуги шлюза и т.п.

Все три составляющие AAA тесно связаны. Например, учет использования ресурса с целью выставления счета не имеет смысла, если субъект, которому предоставляется услуга, не может быть достоверно идентифицирован, то есть *аутентифицирован*. После того как субъект установлен, следует определить, доступ к каким ресурсам и на каких условиях (параметры качества обслуживания, виды услуг, виды носителей) может быть ему предоставлен. Процедура *авторизации* позволяет применять правила доступа к ресурсам в соответствии с соглашением с Оператором. Выставление счетов за услуги в большинстве случаев основывается на информации о количестве и типе потребленных абонентом ресурсов и длительности этого потребления. Сбор такого рода информации осуществляется в рамках процедур *учета*.

Настоящая книга посвящена двум протоколам, созданным и повсеместно используемым для обеспечения функций AAA, – протоколам RADIUS и Diameter.

Главной телекоммуникационной услугой на протяжении большей части XX века являлась традиционная телефонная связь, местная, междугородная и международная.

Декадно-шаговые и координатные АТС, соединявшие абонентов с помощью электромеханических контактов, практически исключали понятие мошенничества (фрода) в его сегодняшнем понимании, так как абонент идентифицировался исключительно физической линией, подведенной к месту установки стационарного телефонного аппарата. Таким образом, аутентификация при доступе к сети выполнялась непосредственно подключением на кроссе АТС, а счет за услуги выставлялся владельцу линии. Авторизация как таковая также была элементарна, так как абоненту была доступна только услуга телефонной связи. Если абонент не оплачивал услуги связи в соответствии с условиями договора, его линия физически блокировалась. Учет длительности разговоров осуществлялся первоначально только на междугородных станциях – АМТС – с помощью процедуры АОН, а несколько позже – и на АТС – тоже с помощью дополнительно устанавливаемого оборудования учета стоимости.

Появление цифровых АТС несколько усложнило AAA-процедуры в ТфОП. Аутентификация, как и раньше, производилась на основе анализа номера абонентской линии, по которой поступал вызов. Однако, в отличие от предшественников, в цифровых АТС действовала полноценная процедура авторизации. Предоставление дополнительных услуг, таких как переадресация или автоматическая побудка, требовало создания профиля абонента, в котором фиксировались правила доступа к подобным услугам. При каждом запросе система обращалась к профилю и выполняла проверку прав абонента, и дальнейшее обслуживание зависело от результатов проверки. Появилось и встроенное программное обеспечение учета стоимости услуг связи, являющееся неотъемлемой частью программного обеспечения цифровых АТС.

Ситуация радикально изменилась с появлением Интернет-технологий. Первым популярным способом доступа в Интернет стал Dial-Up (коммутируемый доступ через модем по двухпроводной телефонной линии). Заключая договор с Интернет-провайдером, абонент получал логин и пароль, по которым система могла аутентифицировать его запрос подключения к сети. Учитывая, что точек доступа к сети, называемых также *NAS (Network Access Server)*, могло быть много, а хранить параметры абонентов удобнее в единой, а не распределенной базе данных, IETF специфицировала в RFC 2058 протокол RADIUS *(Remote Authentication Dial In User Service)*, определявший формат взаимодействия NAS и специального сервера, который выполнял проверку параметров аутентификации по базе данных Интернет-провайдера. Чуть позже, в середине 1997 года, спецификации этого протокола были пересмотрены в RFC 2138, а затем еще раз – в 2000 году – в RFC 2865 [67]. Простейший (и уже постепенно уходящий) пример использования RADIUS при доступе dial-up в Интернет показан на рис. 1.

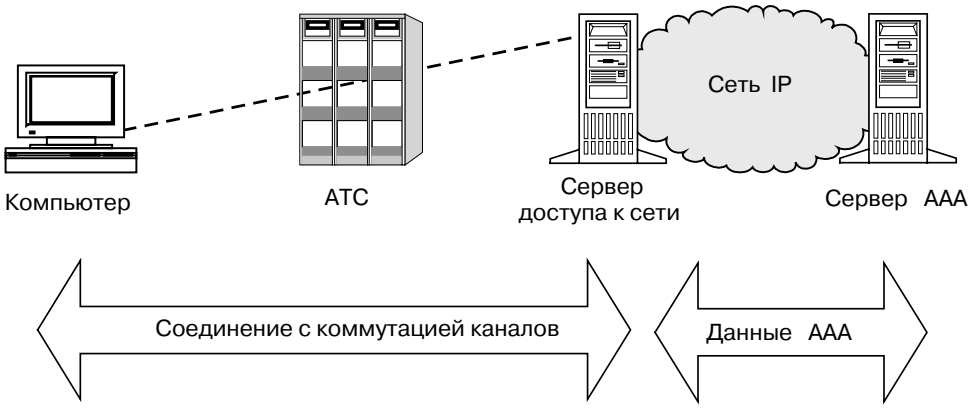

Рис. 1. Функции AAA в доступе dial-up через ТфОП

Помимо аутентификации, появление Интернет привнесло необходимость развития систем учета Интернет-провайдеров. Выставление счетов пользователям выполнялось на основе информации о продолжительности доступа к сети и объема данных, переданных в рамках Интернет-сессии. Эту информацию было целесообразно накапливать централизованно, что потребовало разработки протокола передачи такого рода информации от NAS на сервер учета. IETF доработал существующую версию RADIUS, создав в январе 1997 года протокол RADIUS Accounting RFC 2059 [66], который, как и RADIUS, был дважды переработан в RFC 2139 и RFC 2866 в середине 1997 и в 2000 годах, соответственно. Согласно этому протоколу, в момент начала сессии NAS отправляет на сервер учета сообщение, сигнализирующее о необходимости начала отсчета времени. В конце сессии NAS отправляет еще одно сообщение, уведомляющее об окончании сессии и об объеме переданной информации, предоставляя серверу учета необходимые данные для формирования счетов. Протоколы RADIUS и RADIUS Accounting рассматриваются подробно в главе 2.

Эволюция сетей связи, выражающаяся в усложнении сетевого и пользовательского оборудования, в увеличении количества услуг, в новом уровне угроз защите информации, а также в необходимости обеспечения согласованного качества обслуживания, привела к тому, что разработанный без учета всех этих факторов протокол RADIUS в силу своих ограничений стал во многих случаях неприменимым для решения задач AAA в рамках новых инфокоммуникационных реалий. Это побудило IETF стандартизировать новый AAA-протокол, что и было вскоре сделано:

в RFC 3588 [25] в конце 2003 года появилась первая версия базового протокола Diameter, рассматриваемого в главе 3.

Одним из отличий протокола Diameter от RADIUS является то, что стандартизация практических приложений, работающих на основе базового протокола Diameter, ведется в рамках отдельных RFC, каждый из которых, по сути, представляет собой отдельный стандарт. Глава 4 посвящена рассмотрению приложения кредитного контроля Diameter [53] – одному из наиболее распространенных на сегодня Diameter-приложений, которое позволяет на основе стандартизированных механизмов выполнять контроль расходования ресурсов мультисервисной сети в режиме реального времени по принципу предварительного резервирования.

Де-факто, последователем протокола RADIUS является не базовый протокол Diameter, а рассматриваемое в главе 5 Diameter-приложение сервера доступа к сети [38], так как именно оно описывает процедуры взаимодействия сервера доступа к сети NAS и AAA-сервера при обслуживании пользователей, запрашивающих доступ к сетевым ресурсам. В силу того что, по понятным причинам, единовременный переход на новый AAA-протокол невозможен, большое внимание в главе 5 уделяется задачам преобразования протоколов RADIUS и Diameter для обеспечения совместимости существующего и нового оборудования.

Традиционная для книг этой серии глава 6 охватывает вопросы реализации и тестирования протоколов AAA, а в главе 7 рассматриваются вопросы реализации законного перехвата сообщений – COPM (которым посвящена отдельная книга этой же серии [8]) – для протоколов RADIUS и Diameter.

Обсуждение материала, содержащегося в главах 2-7, требует согласования понятийного аппарата и краткого обзора процедур AAA без привязки к конкретной реализации протокола. Основные определения и описание обобщенной AAA-архитектуры приводятся в главе 1.

Авторы пользуются случаем выразить благодарность за помощь в подготовке этой книги сотрудникам Научно-технических центров НТЦ Протей, НТЦ Аргус и НТЦ Севентест, профессорам и преподавателям, а также аспирантам и студентам кафедры систем коммутации и распределения информации СПбГУТ им. проф. М.А. Бонч-Бруевича, коллегам из отдела системных исследований НИИТС, специалистам сертификационного центра ЛО ЦНИИС и инженерам ведущих зарубежных компаний, с которыми изучались, обсуждались и тестировались спецификации протоколов, рассматриваемых в этой книге.

Глава 1. Архитектура AAA

Согласно традиции, сложившейся в книгах этой серии «Телекоммуникационные протоколы», в первой главе предпринимается попытка осмыслить основные идеи AAA, договориться об общем понимании терминов и подходов к протоколам AAA. Все три составляющие архитектуры AAA уже давно укрепились в современных телекоммуникационных сетях. *Аутентификация, авторизация и учет* в том или ином виде всегда сопровождают каждую попытку доступа к любым инфокоммуникационным услугам, будь то доступ в Интернет, традиционный телефонный вызов ТфОП, роуминг в сетях мобильной связи, заказ VAS, etc. Реализация функций AAA в разных сетях связи принимает разнообразные формы. В телефонных сетях ТфОП она предстает в виде определения исходящего направления и номера абонентской линии в телефонной станции, запрос пары «логин – пароль» используется в случае доступа пользователя в Интернет, в Интеллектуальных сетях (IN) для этого используется номер карточки предоплаты определенной услуги и т.п.

Конвергенция вышеупомянутых сетей и услуг связи побудила IETF, начиная с 2000 года, приступить к выпуску ряда документов [51], [18], [27], [9], [32] и др. с описанием архитектуры, протоколов и систем взаимодействия AAA. Представлению основных концепций и описанию базовой архитектуры AAA и посвящена эта глава. Основные идеи реализации архитектуры построения систем аутентификации, авторизации и учета (AAA) представлены в документе RFC 2903.

Перед тем как перейти непосредственно к рассмотрению протоколов AAA, приведем определения терминов, входящих в аббревиатуру AAA, согласно RFC 2989. Как уже упоминалось во введении, *Аутентификация* – это верификация идентификационной информации, предъявляемой в форме имени из обоюдно согласованного пространства имен. *Авторизация* – это выяснение того, может ли

некое право, такое как право доступа к определенному ресурсу, быть предоставлено предъявителю определенного набора данных. *Учет* – это сбор информации об использовании ресурса с целью анализа, контроля, выставления счетов или распределения стоимости.

1.1. Аутентификация

Перефразируя приведенное выше определение, можно сказать, что *аутентификация* – это процедура, состоящая из двух операций. Первая операция заключается в предоставлении аутентифицируемой стороной некой информации, которая позволяет аутентифицирующей стороне выполнить проверку достоверности переданной идентификационной информации. Вторая операция представляет собой проверку, выполняемую аутентифицирующей стороной. Бытовым примером процедуры аутентификации является предъявление паспорта при входе в вагон поезда дальнего следования. Железнодорожный билет содержит имя и фамилию человека, который имеет право проезда по данному билету из пункта А в пункт Б. Для того чтобы пропустить пассажира в вагон, проводник должен быть уверен, что предъявитель билета действительно является тем человеком, имя которого указано в билете. Фактически, имя и фамилия в билете являются идентификационной информацией пассажира, требующей подтверждения, аутентифицируемой стороной выступает потенциальный пассажир, а аутентифицирующей – проводник вагона поезда. Для выполнения процедуры аутентификации, то есть проверки достоверности предъявленной информации о личности пассажира, последний показывает аутентифицирующей стороне паспорт с собственной фотографией. В случае схожести фотографии в паспорте и лица предъявителя аутентифицирующая сторона принимает на веру то, что имя и фамилия, указанные в паспорте, принадлежат предъявителю, а, значит, железнодорожный билет дает право проезда в поезде именно этому пассажиру.

Для корректности изложения следует добавить, что идентификационная информация, подлежащая верификации, должна обладать свойством уникальности, чтобы процедура аутентификации имела смысл. Возвращаясь к примеру с железнодорожным билетом, предположим, что в билете указан пассажир Сергей Кузнецов или Иван Смирнов. Такая совокупность имени и фамилии (как, впрочем, значительное число сочетаний имен и фамилий в большой стране) не является уникальной, таким образом, процедура аутентификации с предъявлением пас-

порта не позволит проводнику удостовериться, что в поезд садится именно тот Сергей Кузнецов или Иван Смирнов, для которого был приобретен билет. Для этого помимо имени и фамилии в билеты добавляется номер паспорта, который обеспечивает уникальность идентификации пассажира. По существу, имя и фамилия являются избыточными идентификаторами пассажира, так как критерию уникальности удовлетворяет как совокупность данных имя+фамилия+номер паспорта, так и один номер паспорта.

Выделяют следующие виды аутентификации:

– аутентификация клиента;

– аутентификация сообщения;

– взаимная аутентификация.

Приведенный пример с железнодорожным билетом можно отнести к категории аутентификации клиента, когда обслуживающая система проверяет аутентичность пользователя, желающего получить доступ к ее ресурсам. Под категорию аутентификации клиента подпадает также аутентификация устройства без привязки к личности пользователя. В мире телекоммуникаций аутентификация устройств является распространенным явлением – именно такой вид аутентификации используется в сетях мобильной связи, а также в сетях некоторых Интернет-провайдеров. В мобильной сети аутентификация устройства выполняется на основе карты SIM, вставляемой в мобильный телефон. «Зашитые» в SIM-карту ключи позволяют сети выполнить процедуру аутентификации и удостовериться в том, что претендующий на использование сетевых ресурсов мобильный аппарат действительно принадлежит владельцу средств, внесенных на счет в биллинговой системе. Проблема в данном случае состоит в том, что аутентификация устройства не позволяет провести аутентификацию пользователя. Если каким-либо образом подключенный к сети телефон попадет в чужие руки, ресурсы мобильной сети станут автоматически доступны новому обладателю мобильного устройства, так как он не будет отличим для сети от его предыдущего владельца в силу отсутствия аутентификации пользователя. Незаконное использование может продолжаться до тех пор, пока владелец не заявит администрации сети об утере мобильного устройства и необходимости его отключения. Отметим, что для выполнения такого рода операции по телефону пользователю придется пройти аутентификацию, чтобы сотрудники Оператора убедились в его праве на отключение соответствующего устройства от сети. Аутентификация в данном случае будет проведена в виде ответа на секретный вопрос.

Еще одним примером аутентификации устройства является аутентификация сетевой карты по ее MAC-адресу в сети некоторых Интернет-провайдеров. Фактически, провайдеру безразлично, кто из обитателей квартиры пользуется Интернет-доступом, главное, чтобы MAC-адрес устройства совпадал с допустимым для данного кабельного подключения.

Аутентификация сообщений в наши дни является не менее серьезной задачей, нежели аутентификация клиента. К примеру, при удаленной торговле на бирже важной является не только аутентичность клиента, пытающегося продать или купить акции, пользуясь ресурсами своего счета, но и аутентичность команды, которую передает данный клиент по сети. Если на пути следования запроса от клиента к электронной бирже сообщение передается в открытом виде, злоумышленник может поменять команду клиента на выгодную для себя (или невыгодную для клиента). Таким образом, клиенту будет нанесен ущерб в виде потери времени или денег за счет покупки не тех бумаг, которые интересовали его в момент совершения сделки. Более того, операция может быть изменена на противоположную, и бумаги будут не куплены, а проданы. Во избежание мошенничества подобного рода (называемого «*человек посередине*» – *Man In The Middle* – *MITM*) в современных телекоммуникационных сетях применяется процедура аутентификации сообщения, именуемая также процедурой обеспечения целостности информации. Для обеспечения целостности сообщения отправитель выполняет операцию хеширования передаваемых данных и некоторого секретного слова, известного только ему и получателю сообщения (бирже), после чего передает сообщение, добавляя в его конец получившуюся на выходе хэш-функции последовательность. Получатель сообщения выполняет аналогичную операцию над полученными данными, и, в случае совпадения с переданным результатом, верифицирует целостность информации. Если по пути следования сообщения оно будет изменено злоумышленником, получатель на выходе хэш-функции получит результат, отличный от того, который добавлен к сообщению отправителем, и поймет, что тело сообщения подверглось модификации.

Взаимная аутентификация – это аутентификация не только сервером клиента, но и клиентом сервера, либо, в конфигурации peer-to-peer, взаимная аутентификация взаимодействующих узлов. Взаимная аутентификация необходима в окружении, где клиент не может доверять идентификатору сервера, либо равноправный узел не может доверять идентификатору равноправного узла. Примером взаимной аутентификации является аутентификация пользователем сайта, который требует введения логина и пароля для аутентификации пользователя.

Так как логин и пароль являются для пользователя «чувствительной» информацией, за которой могут охотиться Интернет-мошенники, перед аутентификацией клиент хочет быть уверен, что сайт является именно тем сайтом, за который он себя выдает. В данном примере аутентификация будет выполнена с помощью подписанного сертификата, который пользователь принимает от сайта перед тем, как выполнить аутентификацию. В силу того, что настоящая книга посвящена протоколам AAA, здесь отсутствует детальное рассмотрение механизмов аутентификации клиентов, сообщений и взаимной аутентификации. Вместо этого предлагается обсудить аутентификационные модели, которые позволят читателю понять место AAA-протокола в инфраструктуре AAA инфокоммуникационной сети.

1.1.1. Двусторонняя модель

Двусторонняя модель аутентификации имеет место в случаях, когда процедура аутентификации выполняется непосредственно участниками диалога без привлечения третьей стороны. Примером двусторонней аутентификации является аутентификация при удаленном доступе к оборудованию (например, по протоколу SSH). При поступлении запроса аутентификации аутентифицирующая сторона выполняет аутентификацию локально, на основе хранящейся в данном узле информации. Для выполнения аутентификации при удаленном доступе к серверу взаимодействие с третьей стороной не требуется, так как обычно параметры клиентов конфигурируются непосредственно на аутентифицирующем узле.

1.1.2. Трехсторонняя модель

Двусторонняя модель аутентификации не может лежать в основе больших распределенных сетей – для выполнения аутентификации в этом случае каждый элемент такой сети должен обладать всей полнотой информации о пользователях, для того чтобы иметь возможность выполнить аутентификацию любого подключающегося клиента. Например, в двусторонней модели сеть Wi-Fi хотспотов должна состоять из точек доступа, каждая из которых хранит учетные записи всех пользователей в сети. Понятно, что данная модель является менее эффективной, чем трехсторонняя, при которой точки доступа из приведенного примера будут не более чем передатчиками аутентификационной информации к единому хранилищу, которое содержит всю необходимую для аутентификации любого пользователя информацию. Трехсторонняя модель (рис. 1.2) аутентификации характеризуется следующим набором компонентов:

a) поставщик аутентификационной информации – пользователь, желающий аутентифицироваться в сети;

b) сервер доступа к сети, который является шлюзом между пользователем и сетью. Сервер доступа к сети получает от пользователя информацию аутентификации и передает ее на AAA-сервер для выполнения процедуры аутентификации;

c) AAA-сервер – элемент, содержащий информацию, достаточную для проведения аутентификации пользователя. Он выполняет проверку учетных данных пользователя по запросу сервера доступа к сети. Если запрос завершается успешно, то есть пользователь действительно является тем, за кого себя выдает, AAA-сервер дает серверу доступа к сети команду предоставить пользователю сетевой доступ в соответствии с его полномочиями (которые определяются при процедуре авторизации, речь о которой в следующем параграфе).

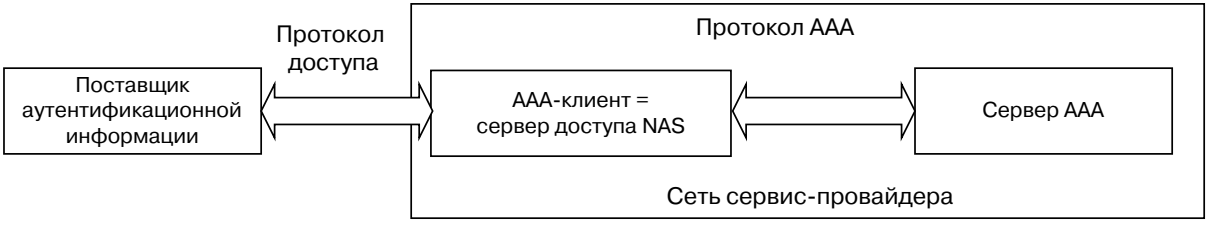

Рис. 1.1. Трехсторонняя модель аутентификации

Следует отметить различную природу протоколов передачи аутентификационной информации на участке между пользователем и сервером доступа к сети (NAS). Пользователь не является (AAA-клиентом). В первом случае обмен данными происходит в большинстве случаев до получения IP-адреса (так как IP-адрес является ресурсом сети, доступ к которому может быть предоставлен только после аутентификации и авторизации пользователя). Кроме того, передача данных на сервер сетевого доступа выполняется в режиме без посредников, так как точка подключения к сети, как правило, является сервером следующего перехода по отношению к поставщику аутентификационной информации и не требует каких-либо посредников для передачи информации. Совокупность этих факторов является причиной того, что протокол передачи аутентификационной информации до сервера сетевого доступа работает поверх функций второго уровня семиуровневой модели OSI.

В отличие от участка пользователь – сервер доступа к сети, участок сервер доступа к сети – AAA-сервер в большинстве случаев (в случаях одного домена) является защищенным, поэтому обмен аутентификационной информацией между сервером сетевого доступа и AAA-сервером проходит, как правило, поверх транспортного протокола UDP, TCP или SCTP, требующего получения IP-адреса. Именно информационный обмен на данном участке лежит в зоне ответственности AAA-протоколов – предмета, которому посвящена большая часть настоящего издания. Наиболее распространенными AAA-протоколами сегодня являются протоколы RADIUS и Diameter.

1.2. Авторизация

Авторизация – вторая «A» в аббревиатуре – процедура, значение которой часто недооценивается либо вообще не воспринимается как некое самостоятельное действие, так как во многих случаях авторизация выполняется либо одновременно с аутентификацией, либо одновременно с учетом. Тем не менее, авторизация имеет важное значение в обеспечении функций AAA, поэтому ей посвящены отдельные RFC [34], [33], [35], описывающие, соответственно, инфраструктуру авторизации, примеры приложений авторизации и требования к авторизации.

Как следует из определения, приведенного в начале главы, авторизация – это определение полномочий доступа к некоторым ресурсам.

Аутентификация позволяет только убедиться, что претендующее на ресурсы лицо или устройство является именно тем, за кого себя выдает. После того как личность претендующего достоверно установлена, начинается процесс авторизации, то есть определения, какая часть ресурсов может быть предоставлена данному пользователю. Фактически, авторизация имеет место в любой сети, а если рассматривать шире, в процессе получения доступа к любой услуге, в рамках которой пользователю предлагаются как минимум два вида ресурсов.

Рассмотрим уже упоминавшийся пример с поездом дальнего следования. Предположим, что в поезде дальнего следования предоставляется только одна услуга – проезд в купейном вагоне. В этом случае аутентификация и авторизация фактически происходят одновременно в рамках аутентификации: если личность пассажира подтверждается, он автоматически имеет право на доступ к ресурсу – проезд в купейном вагоне.

Предположим, далее, что в билет может быть включен ужин в вагоне-ресторане. В данном случае уже не обойтись без процедуры авторизации. После входа в вагон и начала следования проводник проверит по билету, имеет ли право данный пассажир на ужин. Это уже будет процедура авторизации в чистом виде, в полном соответствии с приведенным определением.

Рассмотрим другой пример – билет в парк аттракционов, в который включен трехразовый прокат на любых аттракционах парка. Посетитель парка, купивший билет, будет предъявлять его контролеру, который поставит на нем отметку о посещении аттракциона, после чего предоставит посетителю доступ к ресурсу – откроет калитку и пропустит посетителя в кресло аттракциона «американские горки» или, к примеру, на колесо обозрения. В данном примере аутентификация не имеет места – контролеру безразлично имя или фамилия посетителя, важно только одно – наличие права пользования аттракционом, то есть билет, а также наличие на билете не более двух отметок о посещении «его» аттракциона. Процесс проверки билета представляет собой процесс авторизации, однако в этом случае авторизация совмещена с учетом – при проверке контролер ставит на билете отметку об использовании одного из трех посещений, то есть, фактически, ведет учет использования ресурса.

Как следует из предисловия к RFC 2904, утвержденной в 2000 году, целью создания инфраструктуры, представленной в этой RFC, было введение единой архитектуры и терминологии, подходящих для обсуждения большого числа приложений. На рис. 1.2 представлены базовые концептуальные элементы такой инфраструктуры:

- пользователь, желающий получить доступ к услуге или ресурсу;
- домашняя организация пользователя, с которой у него заключено соглашение. Эта организация проверяет, имеет ли данный пользователь право доступа к требуемому ресурсу или услуге. Этот элемент является хранилищем информации, которая может быть неизвестна сервис-провайдеру (к примеру, лимит средств на счете);
- AAA-сервер сервис-провайдера, который авторизует доступ к услуге на основе соглашения с домашней организацией пользователя;
- оборудование услуги, которое непосредственно предоставляет услугу. Это может быть сервер доступа к сети, принтер, маршрутизатор или другое оборудование.

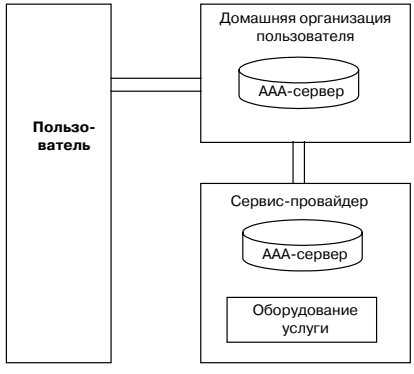

Рис. 1.2. Соглашения об обслуживании

Двойными линиями на рисунке изображены соглашения об обслуживании, такие как соглашение об уровне обслуживания SLA или простые договоры о взаимодействии, на основе которых выполняются процедуры авторизации.

В простейшем случае домашняя организация пользователя и сервис-провайдер являются единой сущностью, то есть находятся в рамках одного домена. Более сложным случаем является роуминг, когда пользователь уходит из домашнего домена к сервис-провайдеру, имеющему свой собственный AAA-сервер. Рассмотрим возможные последовательности обмена сообщениями авторизации в случаях одного домена, после чего рассмотрим случай роуминга.

1.2.1. Обмен сообщениями внутри одного домена

1.2.1.1. Агентская последовательность

В агентской последовательности AAA-сервер сервис-провайдера выступает в качестве агента между пользователем и услугой. AAA-сервер получает запрос пользователя и перенаправляет информацию авторизации вместе с информацией конфигурации на оборудование услуги. В модели агентской последовательности на рис. 1.3 пользователь отправляет запрос на AAA-сервер сервис-провайдера (шаг 1), который применит политику, относящуюся к данному абоненту и запрашиваемой услуге. AAA-сервер отправляет запрос к оборудованию услуги, и оборудование услуги организует ее предоставление (шаг 2). Оборудование услуги затем

отвечает AAA-серверу, что для данного пользователя услуга подготовлена (шаг 3). AAA-сервер отвечает пользователю, что услуга подключена и тот может использоваться ею (шаг 4).

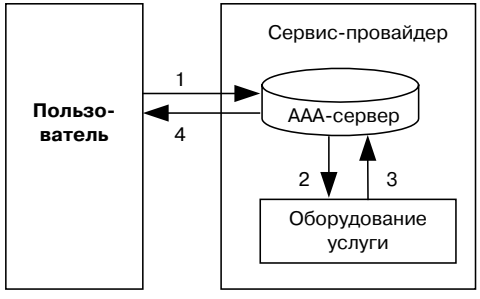

Рис. 1.3. Агентская последовательность

1.2.1.2. Последовательность с опросом

Последовательность с опросом (рис. 1.4) используется в приложениях удаленного доступа, в Mobile-IP окружении и в некоторых приложениях, обеспечивающих качество обслуживания. Пользователь отправляет запрос на оборудование услуги (шаг 1), которое перенаправляет его на AAA-сервер сервис-провайдера (шаг 2). AAA-сервер выполняет обработку запроса и передает соответствующий ответ на оборудование услуги (шаг 3), которое устанавливает услугу и уведомляет пользователя о готовности (шаг 4).

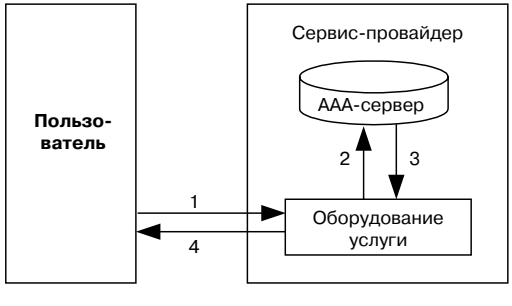

Рис. 1.4. Последовательность с опросом

1.2.1.3. Последовательность с билетом

Последовательность с билетом (рис. 1.5) подразумевает получение пользователем билета от AAA-сервера сервис-провайдера, подтверждающего его право пользования услугой (шаги 1,2). Пользователь прикладывает к запросу, отправляемому на оборудование услуги, полученный билет (шаг 3). Оборудование услуги на основе этого билета выполняет верификацию запроса и отвечает подтверждением пользователю (шаг 4).

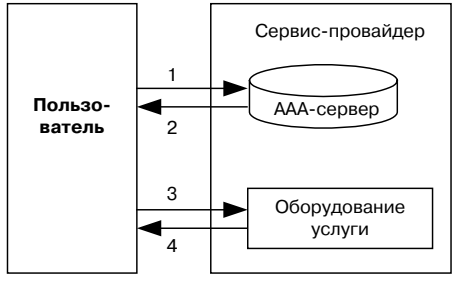

Рис. 1.5. Последовательность с билетом

1.2.2. Обмен сообщениями между разными доменами – роуминг

Во многих случаях организация, аутентифицирующая и авторизующая пользователя, и организация, предоставляющая услугу, не совпадают. Данная ситуация рассматривается как роуминг, когда пользователь домашней сети уходит в гостевую сеть и запрашивает услугу оттуда.

В роуминговых сценариях применяются те же последовательности обмена сообщениями, что и в сценариях с одним доменом – агентская последовательность, последовательность с опросом и последовательность с билетом. Для простоты изображения сгруппируем AAA-сервер и оборудование услуги сервис-провайдера в один логический элемент. Описанные последовательности для случая роуминга представлены на рис. 1.6, 1.7 и 1.8.

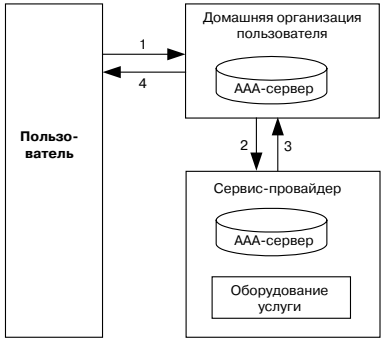

Рис. 1.6. Агентская последовательность (роуминг)

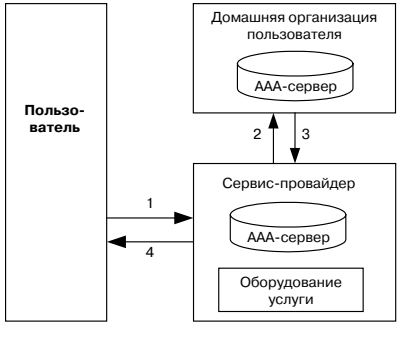

Рис. 1.7. Последовательность с опросом (роуминг)

Рис. 1.8. Последовательность с билетом (роуминг)

1.2.2.1. Распределенная услуга

Предоставление конкурентоспособного обслуживания во многих случаях требует комбинирования услуг от нескольких сервис-провайдеров. Примером может служить пользователь, требующий обеспечения определенного уровня качества обслуживания на пути сообщений, пересекающих сети нескольких сервис-провайдеров Интернет. Услуга, предоставляемая более чем одним сервис-провайдером, считается распределенной.

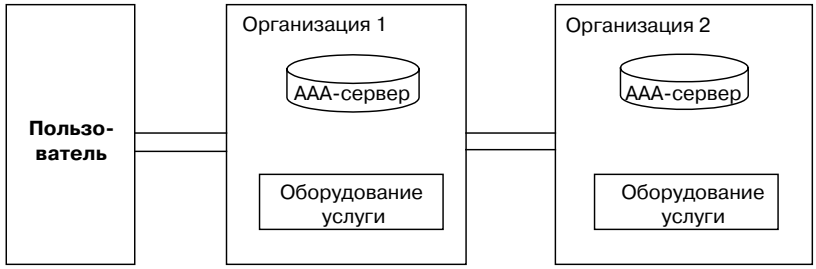

Рис. 1.9. Распределенная услуга

Соглашения между элементами рис. 1.9 подразумевают передачу запроса аутентификации и авторизации пользователя первой организации на обработку, после чего запрос должен быть передан второй организации. Следует отметить, что последовательности обмена сообщениями при обработке запроса первой и второй организациями могут различаться. К примеру, первая может использовать последовательность с опросом, в то время как вторая – агентскую последовательность (рис. 1.10).

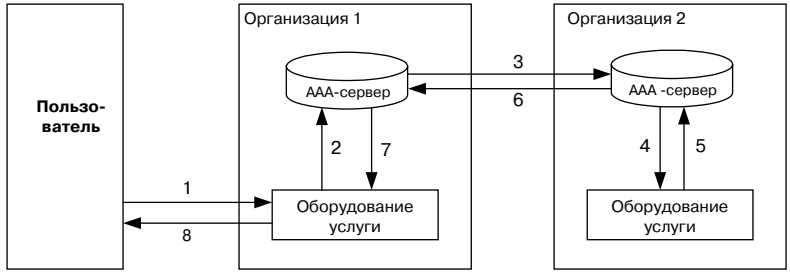

Рис. 1.10. Возможная последовательность обработки запроса

1.2.2.2. Роуминговая распределенная услуга

На рис. 1.11 показана комбинация роуминговой и распределенной услуги.

Новым элементом на этом изображении является Суперорганизация, предназначение которой заключается в выполнении аутентификации и авторизации пользователей для организаций, предоставляющих услуги. Фактически, эта организация является брокером, или продавцом услуг всех взаимодействующих организаций.

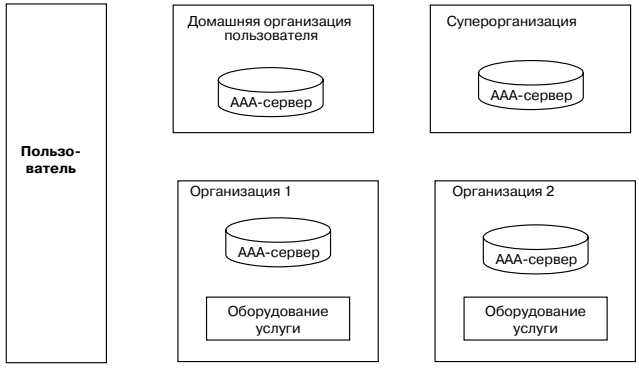

Рис. 1.11. Роуминговая распределенная услуга

1.3. Учет

Если слова «аутентификация» и «авторизация» в русском и английском языках начинаются на одну и ту же букву – «А», то перевод английского слова «Accounting» нарушает эту аналогию: в русском языке для обозначения последней составляющей AAA принято использовать слово «учет». Понятие учета является широким и охватывает несколько видов деятельности, причем различные стандартизующие структуры определяют его по-разному. IETF, к примеру, определяет учет как сбор информации об использовании ресурса с целью анализа, контроля, выставления счетов или распределения стоимости. 3GPP же считает учетом процесс распределения стоимости между домашним окружением, обслуживающей сетью и пользователем.

Поскольку материал этой книги базируется на документах IETF, мы будем придерживаться IETF-интерпретации и пользоваться терминологией IETF. Кроме того, распределение стоимости является в большей степени организационной, а не технической задачей, в то время как сбор информации об использовании ресурса является преимущественно технической и стандартизируемой задачей. Несмотря на расхождения некоторых других относящихся к учету определений, 3GPP и IETF, тем не менее, одинаково определяют стандарты для выполнения сходных операций, что естественно в условиях конвергенции сетей и использования одного и того же набора протоколов для выполнения сходных задач.

RFC 2975, специфицирующая основные понятия процедур учета, а также формулирующая определения основных относящихся к учету терминов, была утверждена IETF в 2000 году. Целью ее создания была выработка универсальных требований к приложениям учета, которые можно было бы использовать при последующем создании универсального протокола учета и разработке универсальных механизмов обеспечения защиты информации. Согласно RFC 2975:

Биллинг – совокупность действий, нужных для приготовления счета.

Аудит – акт верификации корректности этой совокупности действий.

Промежуточный учет – данные об использовании ресурсов во время сессии пользователя. Это может быть полезно в случае перезагрузки устройства или возникновения сетевой проблемы, которая препятствует генерации итоговой записи учета по всей сессии.

Учет в пределах одного домена – сбор информации об использовании ресурса в пределах административного домена при пользовании ресурсом в рамках этого домена. В процессе учета в пределах одного домена информация учета, как правило, не пересекает административных границ.

Междоменный учет – сбор в рамках одного домена информации об использовании ресурса в рамках другого домена. В случае междоменного учета информация учета, как правило, пересекает административные границы.

Учет в режиме реального времени – обработка информации учета использования ресурса внутри определенного временного окна. Временные ограничения накладываются, как правило, для ограничения финансового риска.

Сервер учета – получает информацию учета от устройств и преобразует ее в сессионные записи. Сервер учета может также отвечать за доставку сессионных записей заинтересованным сторонам.

1.3.1. Архитектура системы управления учетом

Управление учетной информацией подразумевает взаимодействие между устройствами сети, сервером учета и сервером биллинговой системы. Устройства сети собирают информацию об использовании ресурсов в форме измерений и пересылают эту информацию на сервер учета. Как правило, пересылка выполняется посредством протокола учета, хотя устройства могут генерировать сессионные записи самостоятельно.

Далее сервер учета обрабатывает полученную от устройств сети учетную информацию,что включает в себя суммирование данных промежуточного учета, детектирование дублирующихся записей, генерацию сессионных записей.

Обработанная информация учета затем пересылается на биллинг-сервер, который, как правило, выполняет функции оценки стоимости и генерации счетов, но может также осуществлять аудит, распределение стоимости, анализ тенденций развития или планирование емкости сети.

Одной из функций сервера учета является разделение внутридоменных и междоменных событий и соответствующая маршрутизация трафика. Для сессионных записей, содержащих NAI [10], решение может приниматься на основе анализа доменной части NAI. Отсутствие доменной части подразумевает принадлежность события внутридоменному учету.

Внутридоменные события учета, как правило, передаются на локальный биллинг-сервер, в то время как междоменные события маршрутизируются на серверы учета в других административных доменах.

Принятие решения о маршрутизации событий учета часто возлагается на прокси-сервер. Устройства сети обычно передают события учета на такой прокси, который либо трансформирует их в сессионные записи, либо перенаправляет пакеты в другие домены. В случае если прокси-сервер не является доверенным устройством, на него возлагаются только функции пересылки записей учета без генерации сессионных записей. В силу того, что протоколы учета, как правило, поддерживают функции обеспечения защиты дата-объекта, это позволяет получателям удостовериться, что пакет не был модифицирован, и его содержимое не попало в руки злоумышленников, и генерировать сессионные записи самостоятельно.

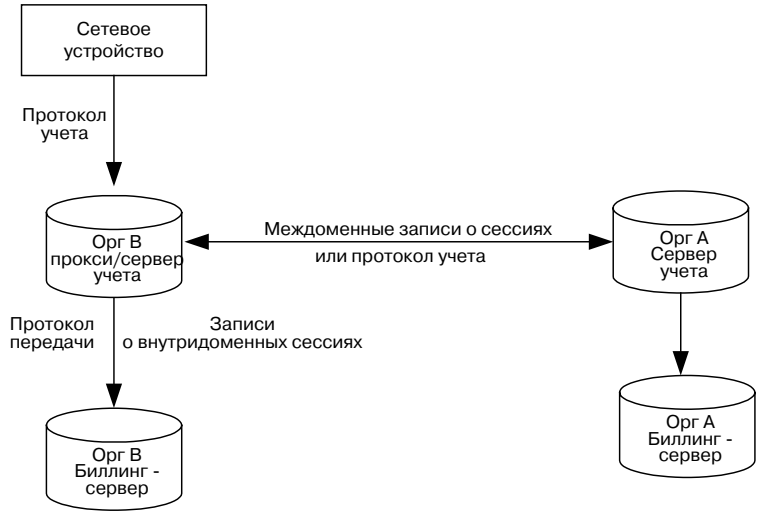

Рис. 1.12. Внутридоменный и междоменный учет

1.3.2. Обеспечение надежности учета

Учитывая, что повреждение информации учета может привести к потерям Оператора, а также стать причиной выставления некорректных счетов пользователям, особое внимание уделяется вопросам обеспечения надежности протоколов учета. Наиболее существенными факторами, влияющими на доставку информации учета, являются:

– потери пакетов;

– нарушение работы серверов учета;

– нарушение работы сетевого оборудования;

– перезагрузка устройств сети.

Возможность преодоления негативного воздействия этих факторов является важным требованием к протоколам учета. Обеспечение надежности передачи учетной информации производится с помощью следующих механизмов.