БИБЛИОГРАФИЧЕСКИЙ СПИСОК
1. *Костюк В.И.* Основы построения АСУ: Учебное пособие для вузов. ─ М.: Сов. радио, 1977.
2. *Гибмаш Е.А.* Повышение качества проектирования АСУТП // Приборы и системы. ─ М.: 2002. ─ №6.
3. *Гнеденко Б.В., Коваленко И.Н.* Введение в теорию массового обслуживания. ─ М.: Наука, 1966.
4. *Севостьянов Б.А.* Эргодическая теорема для марковских процессов и ее приложение к телефонным линиям с отказами. – В кн.: Теория вероятностей и ее применение. ─ М.: 1957. Вып. 1. Т.2.
5. *Саати Т.Л.* Элементы теории массового обслуживания и ее приложения. ─ М.: Сов. радио, 1971.
6. *Цвиркун А.Д.* Структура сложных систем. ─ М., 1975.

УДК 621.39

А.В. Анисимов

ХАРАКТЕРИСТИКИ КАЧЕСТВА УДАЛЕННОГО ДОСТУПА

Беспроводные сети доступа к WAP (Wireless Application Protocol) являются средством организации доступа абонентов сотовой связи к WAP-ресурсам Интернет. Необходимым компонентом для решения этой задачи является RADIUS (Remote Authentication Dial-In User Service). Информационные документы Интернет-RFC содержат технические спецификации и стандарты RADIUS. На основе этих стандартов создаются сервера управления учетными записями и сессиями пользователей, в названии которых, как правило, используются производные от термина RADIUS. Качество доступа (качество услуги ─ QoS) к WAP-ресурсам при эксплуатации в глобальных сетях определяется, в том числе, и технологией обработки RADIUS пакетов пользователей. Подобная обработка включает в себя добавление/изменение атрибутов по заданным условиям, пересылку пакетов на другие RADIUS-сервера, параллельный форвардинг RADIUS-пакетов на несколько серверов.

Показатели качества служат основой для разработки архитектуры сервера. Требования высокой производительности, надежности и минимизации потерь данных при отказах представляют собой основные показатели качества. Архитектура сервера, позволяющая оптимальным образом настроить систему под конкретные требования, рассматривается как показатель качества с позиций адаптации системы к задачам потребителей сетевых услуг. В настоящей статье приводятся характеристики серверов, которые определяют качество доступа к информационным ресурсам.

Процедура работы по протоколу RADIUS выполняется пользователем, запрашивающим услугу, сервером доступа (NAS – Network Access Server), обеспечивающим услугу, и RADIUS сервером. Сервис, обеспечиваемый NAS пользователям, предоставляется в форме сеанса, который носит название сессия. Стандарт, используемый при организации сессий, разработан 3GPP (3rd Generation Partnership Project), которая утвердила определенный IETF протокол Session Initiation Protocol (SIP) в качестве основы для сетей мобильной связи. IETF (Internet Engineering Task Force) ─ международное сообщество, которое занима-

ется развитием протоколов и архитектуры Интернет. Механизм управления сессиями основывается на клиент-серверной модели, в которой NAS сервер выступает в роли клиента, а радиус-аккаунтинг (accounting) сервер в роли сервера, выполняющего учет используемого сервиса. Сессия, реализуемая по протоколу RADIUS, инициируется пользователем, который запрашивает услугу путем обращения к серверу. Транзакции в обратном направлении не предусмотрены. Процедура аутентификации, завершается выдачей в ответном пакете максимальной длительности сессии (session timeout). По истечении времени сервер доступа обязан текущую сессию разорвать. Для характеристик качества существенным является возможность организация множества одновременных сессий.

Сессии реализуются на основе протокола UDP. Этот протокол характеризуется неизменностью параметров (адресов, портов, интерфейсов) отправителя и получателя на протяжении всей сессии. Эффективность функционирования RADIUS сервера, которая определяется также протоколом аутентификации, зависит от организации диалога между клиентом и сервером, в ходе которого проверяется имя пользователя и пароль. С помощью этого стандарта осуществляется разработка протоколов по передаче информации, необходимой для аутентификации. Аутентификация может осуществляться в соответствии со стандартом IEEE 802.11. Частным случаем использования данного стандарта является открытая аутентификация, выполняемая посредством обмена сообщениями запроса аутентификации и подтверждения аутентификации. Решение задачи обеспечения качества информационных процессов реализуется путем других способов аутентификации, например аутентификации с общим ключом. Аутентификация с общим ключом является таким методом аутентификации стандарта IEEE 802.11, при котором выполняется настройка у абонента статического ключа шифрования. Абонент посылает запрос аутентификации с общим ключом (Authentication Request). В результате этого запроса присылается подтверждение, содержащее псевдослучайный Challenge Text (испытательный текст). В ответ на это абонент шифрует Challenge Text своим статическим ключом, полученным на основе секретного WEP-ключа и произвольного вектора, инициализации и снова повторяет запрос аутентификации. WEP (Wired Equivalent Privacy) ─ это протокол шифрования трафика. Зашифрованный испытательный текст (Encrypted Challenge Text) вместе с вектором инициализации подвергается обратному преобразованию. При этом используется секретный WEP-ключ и открытый вектор инициализации. При расшифровке ключа, то есть совпадении полученного текста с оригинальным испытательным текстом, аутентификация проходит успешно и клиенту отправляется подтверждение доступа (Confirm Success). Стандартами для форматов и протоколов обмена пакетами служат документы из серии пронумерованных информационных документов Интернет-RFC, которые содержат технические спецификации и стандарты. Основные составные части службы идентификации удаленных пользователей описываются RFC от IETF:

- RFC 2865 Remote Authentication Dial-In User Service (RADIUS) [1];
- RFC 2866 RADIUS Accounting [2];
- RFC 2882 RADIUS Extended [4].

Концепция RADIUS состоит в обеспечении удаленного доступа через коммутируемое телефонное соединение. Эта технология включает в себя и доступ к

серверам виртуальных частных сетей (Virtual Private Network), а также в точки доступа беспроводных локальных сетей (Wireless LAN).

Концепция службы идентификации удаленных пользователей реализуется в том, что сервер доступа, в роли которого выступает клиент RADIUS (сервер VPN или точка доступа беспроводной локальной сети) отсылает серверу RADIUS параметры доступа пользователя (Credentials ─ настройки безопасности и права доступа), а также параметры соответствующего соединения. Для этого клиент использует соответствующий формат, называемый RADIUS-Message. При получении параметров доступа сервер начинает проверку, в ходе которой он аутентифицирует и авторизует запрос клиента RADIUS, а затем пересылает ему ответ: RADIUS-Message-response.

В соответствии с RFC 2865 и RFC 2866 определены следующие типы сообщений:

- Запрос доступа (Access-Request) ─ запрос клиента RADIUS, с которого начинается собственно аутентификация и авторизация попытки доступа в сеть.
- Доступ разрешен (Access-Accept) ─ ответ на запрос доступа клиенту RADIUS, в котором сообщается, что попытка соединения была успешно аутентифицирована и авторизована.
- Доступ не разрешен (Access-Reject) ─ ответ сервера RADIUS означает, что попытка доступа к сети не удалась.
- Вызов запроса (Access-Challenge) ─ сервер RADIUS передает его в ответ на запрос доступа;
- Запрос учета (Accounting-Request) ─ клиент RADIUS отсылает для ввода учетной информации после получения разрешения на доступ.
- Ответ учета (Accounting-Response) ─ сервер RADIUS реагирует на запрос учета и подтверждает факт обработки запроса учета.

Сообщение RADIUS всегда состоит из заголовка и атрибутов, каждый из которых содержит ту или иную информацию о попытке доступа: например, имя и пароль пользователя, запрашиваемые услуги и IP-адрес сервера доступа. Задачей, решаемой при помощи атрибутов RADIUS, прежде всего, является транспортировка информации между клиентами, серверами и прочими агентами RADIUS. Познакомиться с атрибутами MRADIUS можно путем обращения к RFC 2865 [1], RFC 2866[2], RFC 2867 [3], RFC 2868 [5], RFC 2869 [6] и RFC 3162 [8].

Конфигурация между сервером доступа к сети (NAS) и сервером аутентификации (RADIUS) предусматривает конфигурацию интерфейсов. Основной файл конфигурации должен содержать корневой элемент RADIUS, включающий в себя описание компонентов системы. Такими компонентами являются интерфейсы, источники данных, соединения с базой данных, алгоритмы обработки пакетов.

Каждый интерфейс описывается с помощью элемента RADIUS в установленном формате.

Интерфейс включает в себя элементы описания серверов. Все серверные интерфейсы реализованы на протоколе, основанном на RADIUS протоколе, с использованием соответствующих принципов ограничения доступа. Поэтому для каждого клиента должна быть зарегистрирована учетная запись, содержащая IP-адрес и secret, используемый для шифрования поля аутентификации. К каждому серверному интерфейсу подключаются интерфейсы. Пакет, поступивший в

серверное соединение, передается на обработку в интерфейсы. Обработка на интерфейсах запускается последовательно и выполняется в отдельных потоках. Число потоков соответствует размеру пула. Таким образом, оптимальной можно считать конфигурацию, в которой число потоков в пуле сервера соответствует количеству интерфейсов обработки.

Интерфейс обработки в результате выполнения действий над пакетом может сформировать ответ, который будет отправлен серверу. В серверах RADIUS может быть использован расширенный протокол аутентификации (Extensible Authentication Protocol, EAP), который изначально задумывался как дополнение к PPP для поддержки различных механизмов аутентификации доступа к сети. При этом механизм аутентификации применяется во время фазы установления соединения. Такими протоколами являются протоколы аутентификации CHAP, MS-CHAP и MS-CHAPv2. Протокол аутентификации должен обеспечивать верификацию соединения путем выполнения заранее определенной последовательности сообщений. Эти сообщения должны отсылаться в указанной очередности. При использовании EAP в процессе установления соединения специальный механизм не определяется. На этапе аутентификации реализуется специальная схема аутентификации – схема EAP.

В процессе аутентификации сервер генерирует ключ PMK (Pairwise Master Key), который передается клиенту. EAP позволяет осуществлять обмен сообщениями клиент – сервер RADIUS, который может учитывать особенности различных соединений. Этот протокол включает в себя собственно запросы, а также соответствующие ответы. Информация, определяющая аутентификацию, размещается в запросе. В результате достигается возможность выполнения аутентификации с помощью подключенных модулей с обеих сторон соединения: от клиента и от сервера. При установке библиотечного файла EAP как на клиенте, так и на сервере, то можно изменить схему аутентификации в зависимости от характера информационного обмена.

Идентификация в RADIUS осуществляется при использовании атрибута “secret”. Этот атрибут используется как средство шифрования пароля пользователя. Кроме того, применяется алгоритм хэширования MD5. В RFC 2865 отмечается недостаточная надежность подобного шифрования по сравнению с другими методами. Однако существует большое количество применений, в которых подобных средств защиты достаточно.

Существенным для процедуры идентификации является время, на которое выполняется идентификация. Например, в случае предоставления услуги временного типа, когда идентификация используется для единичного доступа фактор времени несущественный.

Однако если аутентификация относится к доступу с существенным параметром времени, например мобильному доступу в Интернет, существенным является возможность оценки длительности сессии. При достижении лицевого счета отметки блокирования доступа к услуге, должны запускаться внешние скрипты, блокирующие доступ.

Характеристики качества RADIUS серверов ─ это не только выполнение аккаунтинга, но и работа в режиме RADIUS Proxy, как это определено в стандарте RADIUS. При работе в этом режиме выполняется прием запроса от NAS и пересылки его другому серверу. Стандартная процедура предусматривает такую последовательность действий:

• NAS посылает пакеты Accounting-Request RADIUS серверу.

• RADIUS сервер протоколирует пакет Accounting-Request, добавляет атрибут Proxy-State после имеющихся в пакете атрибутов Proxy-State, обновляет атрибут Request Authenticator и пересылает запрос удаленному серверу.

• Удаленный сервер протоколирует пакет Accounting, копирует поступившие все атрибуты Proxy-State, не меняя их порядка, в пакет ответа и передает ответ Accounting-Response RADIUS серверу.

• RADIUS серверу удаляет из пакета последний атрибут Proxy-State, обновляет значение атрибута Response Authenticator и пересылает пакет Accounting-Response серверу NAS.

Сервер RADIUS в стандартном исполнении может пересылать пакеты, передавая повторные пакеты по мере получения, или передавать пакеты от своего имени, модифицируя атрибуты пакета. При решении вопросов повышения качества обслуживания эта стандартная процедура может модифицироваться. Например, проксирование может осуществляется в режиме форвардинга. и не ставится в зависимость от получения ответа от сервера, которому пересылается пакет. Дополнительно к стандартным функциям, Сервер RADIUS может быть дополнен механизмом управления сессиями, определяющий условия одновременного существования сессий и методы устранения конфликтов.

Эффективность проксирования может быть обеспечена параллельной пересылкой неограниченному количеству Radius-серверов. Данная реализация пересылки не соответствует стандартному Radius-проксированию, но позволяет реализовать параллельную процессы в сети, что повышает производительность при реализации доступа.

Если интерфейс никогда не возвращает ответа серверу, то он может использоваться только совместно с другими интерфейсами обработки.

Рассмотренные характеристики серверов, определяющие качество доступа к информационным ресурсам имеют количественную оценку при рассмотрении конкретных программных продуктов, представленных на рынке.

Количественные оценки эффективности доступа к информационным услугам могут быть получены при совместном рассмотрении аппаратной организации каналов связи, интенсивности запросов и рассмотренных в настоящей статье информационных процессов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Rigney C., Willens S., Rubensand A., Simpson W.* "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.
2. *Rigney C.* "RADIUS Accounting". RFC 2866, June 2000.
3. *Aboba B., Mitton D., Zorn G.* "RADIUS Accounting Modifications for Tunnel Protocol Support", RFC 2867 , June 2000.
4. *Mitton D.* "Extended RADIUS Practices", RFC 2882, July 2000.
5. *Goyret I., Zorn G., Leifer D., Rubens A., Holdrege M., Shriver J.* "RADIUS Attributes for Tunnel Protocol Support " RFC 2868, June 2000.
6. *Rigney C., Willats W., Calhoun P.* RADIUS Extensions" RFC 2869, June 2000.
7. *Rigney C., Rubens A., Simpson W., and Willens S.* "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.
8. *Aboba D., Mitton B., Zorn G.* "RADIUS and IPv6" RFC 3162, August 2001.