УДК 621.391:681.5

ВИКОРИСТАННЯ ПРОТОКОЛУ DIAMETER У КОМП'ЮТЕРНИХ МЕРЕЖАХ ІЗ РЕАЛІЗАЦІЄЮ АРХІТЕКТУРИ AAA

DOI 10.36994/2788-5518-2021-01-01-15[15]

Буренко А.М., *Державний університет телекомунікацій, Київ, Україна.* burenko333@gmail.com

Анотація. *У статті розглянуто роботу протоколу Diameter, як прямого наступника протоколу RADIUS. Обидва використовуються у комп'ютерних мережах з реалізацією архітектури AAA. Крім того, у роботі досліджено вміст пакету повідомлення Diameter, його будову та принципи передачі. Організацію з'єднань та сесій користувачів.*

Архітектура AAA використовується для реалізації гнучких політик безпеки у комп'ютерних мережах. AAA дозволяє проводити автентифікацію, авторизацію та облік дій користувача.

Найпопулярнішим протоколом AAA зараз залишається RADIUS, проте, через наявність серйозних недоліків, йому на зміну прийшов Diameter, який усуває певні проблеми попередника та реалізує власні додаткові інструменти, що роблять його перспективною заміною RADIUS.

Diameter використовує звичну нам модель «клієнт-сервер», проте, будь-який хост може бути клієнтом або сервером. У новому протоколі описано декілька видів вузлів – агентів, кожен із яких має своє специфічне призначення: relay, proxy, redirect, translation. Останній вид агента дозволяє реалізувати часткову зворотну сумісність RADIUS та Diameter.

Повідомлення Diameter має набір полів, які унікально ідентифікують з'єднання та сесію між клієнтом і сервером. Але, ідентифікатор з'єднання може змінюватись у процесі передачі повідомлення між агентами.

На відміну від RADIUS, при конфігурації Diameter не потрібно вручну вказувати адресу сервера. Diameter реалізує можливості динамічного виявлення однорангових вузлів, що є ще однією його перевагою, оскільки спрощує його впровадження у великих комп'ютерних мережах.

Після виявлення однорангового вузла, на основі транспортного протоколу TCP або SCTP (у RADIUS – UDP) відбувається встановлення фізичного з'єднання та логічного сеансу зв'язку між вузлами. Сесія описує процес взаємодії між клієнтом та сервером та має унікальний ідентифікатор Session-Id.

Оскільки Diameter – протокол із відстеженням стану, то у ньому реалізовано механізм перевірки використання користувачем з'єднання, що робить його ще більш гнучким для використання та допомагає ефективніше розподіляти навантаження на сервер та використовувати виділені для клієнтів ресурси.

Ключові слова: *AAA, автентифікація, авторизація, облік, протокол, RADIUS, Diameter.*

---

[15] Буренко А.М.
Інфокомунікаційні та комп'ютерні технології, № 1 (01), 2021

USING THE DIAMETER PROTOCOL IN COMPUTER NETWORKS WITH AAA ARCHITECTURE IMPLEMENTATION

Andrii Burenko, *State University of Telecommunications, Kyiv, Ukraine. burenko333@gmail.com*

Abstract*. The article considers the operation of the Diameter protocol as a direct successor of the RADIUS protocol. Both are used in computer networks implementing the AAA architecture. In addition, the content of the Diameter message packet, its structure and transmission principles are studied. Organize user connections and sessions.*

The AAA architecture is used to implement flexible security policies in computer networks. AAA allows authentication, authorization and accounting of user actions.

The most popular AAA protocol now remains RADIUS, but due to serious shortcomings, it has been replaced by Diameter, which eliminates certain problems of its predecessor and implements its own additional tools that make it a promising replacement for RADIUS.

Diameter uses the usual "client-server" model, however, any host can be a client or a server. The new protocol describes several types of nodes - agents, each of which has its own specific purpose: relay, proxy, redirect, translation. The latter type of agent allows for partial backward compatibility of RADIUS and Diameter.

The Diameter message has a set of fields that uniquely identify the connection and session between the client and the server. However, the connection ID may change as the message is transmitted between the agents.

Unlike RADIUS, you do not need to manually specify a server address when configuring Diameter. Diameter realizes the possibility of dynamic detection of peers, which is another advantage because it simplifies its implementation in large computer networks.

Once a peer is detected, a physical connection and a logical communication session between the nodes are established based on the TCP or SCTP transport protocol (in RADIUS - UDP). The session describes the process of interaction between the client and the server and has a unique identifier Session-Id.

Because Diameter is a status-tracking protocol, it implements a mechanism to verify user usage of a connection, making it even more flexible to use and helping to more efficiently distribute workloads to the server and utilize resources allocated to clients.

Keywords: *AAA, authentication, authorization, accounting, protocol, RADIUS, Diameter.*

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА DIAMETER В КОМПЬЮТЕРНЫХ СЕТЯХ С РЕАЛИЗАЦИЕЙ АРХИТЕКТУРЫ AAA

Буренко А.М., *Государственный университет телекоммуникаций, Киев, Украина. burenko333@gmail.com*

Аннотация. *В статье рассмотрена работа протокола Diameter, как прямого преемника протокола RADIUS. Оба используются в компьютерных сетях с реализацией архитектуры AAA. Кроме того, в работе исследованы содержание пакета сообщение Diameter, его строение и принципы передачи. Организацию соединений и сессий пользователей. Архитектура AAA используется для реализации гибких политик безопасности в компьютерных сетях. AAA позволяет проводить аутентификацию, авторизацию и учет действий пользователя.*

Самым популярным протоколом AAA сейчас остается RADIUS, однако, из-за наличия серьезных недостатков, ему на смену пришел Diameter, который устраняет некоторые проблемы предшественника и реализует собственные дополнительные инструменты, которые делают его перспективной заменой RADIUS. Diameter использует привычную нам модель «клиент-сервер», однако, любой хост может быть клиентом или сервером. В новом протоколе описано несколько видов узлов - агентов, каждый из которых имеет свое специфическое назначение: relay, proxy, redirect, translation. Последний вид агента позволяет реализовать частичную обратную совместимость RADIUS и Diameter. Сообщение Diameter имеет набор полей, которые уникально идентифицируют соединения и сессию между клиентом и сервером. Но, идентификатор соединения может изменяться в процессе передачи сообщения между агентами. В отличие от RADIUS, при конфигурации Diameter не нужно вручную указывать адрес сервера. Diameter реализует возможности динамического обнаружения одноранговых узлов, что является еще одним его преимуществом, поскольку упрощает его внедрение в крупных компьютерных сетях. После обнаружения одноранговой узла, на основе транспортного протокола TCP или SCTP (в RADIUS - UDP) происходит установление физического соединения и логического сеанса связи между узлами. Сессия описывает процесс взаимодействия между клиентом и сервером и имеет уникальный идентификатор Session-Id. Поскольку Diameter - протокол с отслеживанием состояния, то в нем реализован механизм проверки использования пользователем соединения, что делает его еще более гибким для использования и помогает эффективно распределять нагрузку на сервер и использовать выделенные для клиентов ресурсы.

Ключевые слова: *AAA, аутентификация, авторизация, учет, протокол, RADIUS, Diameter.*

Вступ

Сучасні комп'ютерні мережі часто піддаються впливу зловмисників з метою отримання конфіденційної чи комерційної інформації, облікових даних користувачів, несанкціонованого доступу до обладнання та ін. Багато компаній та постачальників послуг зв'язку для запобігання вищевказаних небезпек розгортають сервіси AAA на базі своєї мережевої інфраструктури.

AAA (з англ. Authentication, Authorization, Accounting) – загальне поняття, яке описує три основні процеси, що забезпечують захист даних у інформаційних системах: автентифікацію, авторизацію та облік.

Автентифікація – визначення персони та співставлення із даними облікового запису у системі безпеки.

Авторизація – співставлення визначеної персони із дозволеними вповноваженнями (перевірка рівня доступу).

Облік – журналювання дій користувача, що пройшов автентифікацію та авторизацію.

Для реалізації архітектури AAA існує декілька протоколів: TACACS, TACACS+, TACACS, RADIUS, Diameter. На сьогодні, найпопулярнішим та найпоширенішим є протокол RADIUS (Remote Access Dial-In User Service). Але

оскільки RADIUS має певні недоліки, то як логічне продовження, що усуває частину проблем, було розроблено Diameter.

Поверхневий огляд протоколу RADIUS

RADIUS – протокол типу «клієнт-сервер» (описано у RFC 2865 та 2866). Клієнт RADIUS зазвичай являє собою сервер NAS (Network Access Server), яким можуть виступати FTP, POP, WWW, PRO□Y та ін. Сервер RADIUS – процес-демон на комп'ютері з ОС Windows NT або UNI□. Клієнт передає відомості про користувача зазначеним серверам RADIUS і виконує різні дії в залежності від отриманої відповіді. Сервери RADIUS приймають запити підключення користувачів, виконують автентифікацію користувачів і повертають дані про конфігурацію, необхідні для обслуговування користувача клієнтом. Сервер RADIUS може діяти як проміжний для інших серверів RADIUS або серверів автентифікації іншого типу.

Згідно із специфікацією, RADIUS це:

- протокол на базі UDP (порт 1812 для автентифікації, 1813 для обліку);
- підтримує автентифікацію PAP, CHAP, EAP;
- протокол без відстеження стану (stateless);
- надає більше 50 пар атрибут/значення з можливістю створювати специфічні для виробника пари;
- підтримує архітектуру AAA;
- облікові дані можуть зберігатись локально або на зовнішніх джерелах (БД SQL, Kerberos, LDAP, Active Directory).

Запити від користувачів обробляються наступним чином (Рис. 1):

1. Користувач/пристрій відправляє запит на NAS. У свою чергу, NAS надсилає повідомлення Access-Request на сервер RADIUS, запитуючи авторизацію. У даному повідомленні міститься інформація для ідентифікації користувача за обліковими даними (як правило – логін та пароль), але може містити і додаткову необхідну інформацію (IP-адреса, номер телефону та ін.)
2. RADIUS-сервер перевіряє правильність інформації використовуючи наступні схеми перевірки: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) або EAP (Extensible Authentication Protocol).
3. Після перевірки RADIUS-сервер повертає NAS одну із відповідей:

- Access-Reject – доступ відхилено;
- Access-Challenge – необхідна додаткова інформація (напр. пін-код, другий пароль та ін.);
- Access-Accept – доступ надано.

Після отримання користувачем доступу до ресурсу, NAS відправляє на RADIUS-сервер запит Accounting-Request-Start, який сигналізує, що почався сеанс користувача. Коли настає кінець сесії, NAS відправляє повідомлення Accounting-Request-Stop із наданням інформації про тривалість сеансу,

кількість переданих пакетів та іншу інформацію, пов'язану із доступом користувача до мережі.

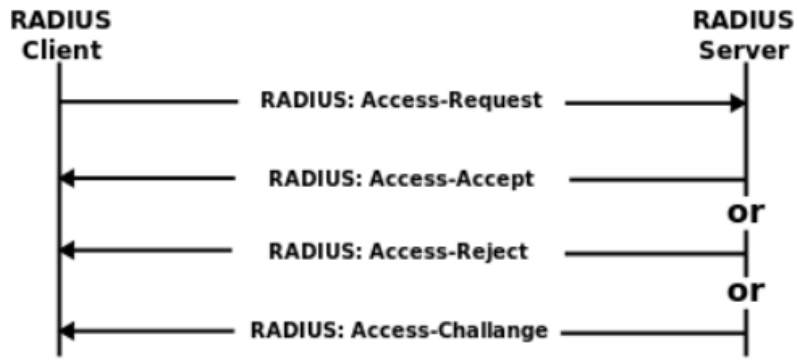

Рис. 1. Запити від користувачів та можливі варіанти відповідей RADIUS-сервера

Враховуючи всі свої можливості та переваги, RADIUS, все ж, має недоліки, а саме:

- недостатній рівень безпеки в деяких реалізаціях. У разі використання декількох проміжних серверів RADIUS, усі вони мають можливість переглядати дані автентифікації, що передаються через них;
- в основний редакції не має можливості відкликання ресурсів після того як авторизація була проведена. У деяких випадках ця проблема вирішується виробником RADIUS-сервера самостійно;
- RADIUS – це протокол без підтримки станів. Він не зберігає транзакційної інформації і не використовує її у наступних сеансах;
- RADIUS не завжди має достатній рівень масштабованості.

Базовий протокол Diameter

Оскільки протокол RADIUS має об'єктивні недоліки (викладені у попередньому розділі), йому на зміну прийшов Diameter (RFC 3588 та 6733). Вже із назви стає зрозуміло, що це не цілком новий протокол для забезпечення архітектури AAA, а логічне продовження та покращення RADIUS, покликане в першу чергу для подолання деяких його обмежень.

Diameter бере суть архітектури AAA із RADIUS і визначає набір досить узагальнених повідомлень, які служать його базовим ядром. Наразі, новий протокол широко використовується у архітектурі IMS (IP Multimedia Subsystem).

У якості транспорту, Diameter використовує TCP (порт 3868) та підтримує TLS, DTLS або IPSec шифрування. Оскільки новий протокол виступає покращенням RADIUS, то він має часткову зворотну сумісність, що полегшує перехід. Крім того, важливим удосконаленням, порівняно із RADIUS, є підтримка моделей зі збереженням та без збереження стану (stateful/stateless).

Diameter має однорангову архітектуру (Peer-To-Peer), і кожен хост, який реалізує даний протокол, може виступати або клієнтом, або сервером, у залежності від мережевої інфраструктури:

Diameter-клієнт – це мережевий пристрій, що безпосередньо обробляє трафік користувача. Зазвичай, це NAS.

Diameter-сервер – вузол, що обробляє запити клієнта. Він виконує автентифікацію, на основі інформації, отриманої від клієнта (напр. логін та пароль). У випадку успішної автентифікації, сервер відправляє клієнту відповідь, що включає авторизацію (повноваження користувача).

На перший погляд, описана вище структура має вигляд традиційної клієнт-серверної, проте, це не так. Іноді, вузол, що сервером, може виступати у ролі клієнта. Крім того, у протоколі чітко визначено ще один тип вузла – Diameter-агент. Їх є три види:

- *relay agent (агент ретранслятор)* – перенаправляє повідомлення відповідному адресату, в залежності від інформації у повідомленні. Такий агент може бути корисним при об'єднуванні запитів із різних регіонів у певну область, що усуває необхідність кропіткого налаштування NAS при зміні Diameter-сервера;
- *proxy agent (проксі агент)* – також перенаправляє повідомлення, але може змінювати вміст повідомлення, надавати додаткові служби, застосовувати правила для різних повідомлень та виконувати функції адміністрування для різних областей;
- *redirect agent (агент перенаправлення)* – виступає у ролі централізованого «сховища» конфігурацій для інших Diameter-серверів. При отриманні повідомлення, переглядає власну таблицю маршрутизації та повертає відповідь разом із інформацією про перенаправлення відправнику. Такий функціонал корисний, оскільки усуває необхідність списку маршрутизації на інших Diameter-вузлах.

З огляду на те, що Diameter є удосконаленням RADIUS, існує ще один спеціальний агент –*translation agent (агент трансляції)*, який реалізує сумісність із RADIUS шляхом перетворення повідомлення одного AAA-протоколу у інший. Такий агент корисний тоді, коли у компанії/провайдера фізичні пристрої не сумісні на рівні AAA-протоколів.

Структура повідомлень Diameter

Diameter-повідомлення є повідомленням у класичному розумінні та складається із заголовку (Рис. 2) та корисного навантаження. Корисне навантаження (Рис. 3) представляється у вигляді заголовку AVP (Attribute-Value Pair) – пара атрибут-значення.

Поля:

- version – версія протоколу;
- message length – довжина повідомлення;

• command flags – прапорець, який вказує на тип службової інформації повідомлення;

• command code – код команди, що передається у повідомленні;

• application-id – вказівник типу додатка (може бути додаток автентифікації, додаток обліку чи специфічний додаток виробника);

• hop-by-hop identifier – ідентифікатор запиту в рамках з'єднання. Має такий самий і у повідомленні-відповіді, але може змінюватись агентами при необхідності;

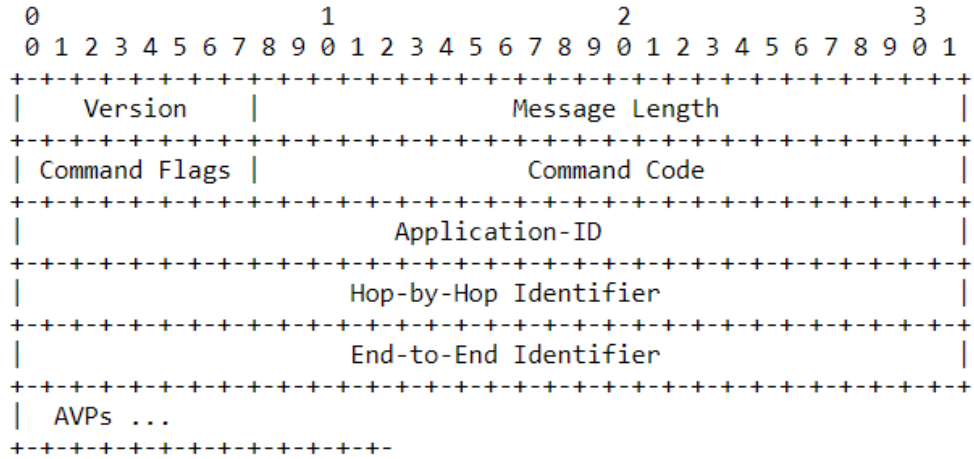

Рис. 2. Формат заголовку Diameter-повідомлення

• end-to-end identifier – ідентифікатор запиту, який має бути унікальним у рамках сесії і не може бути змінений агентами.

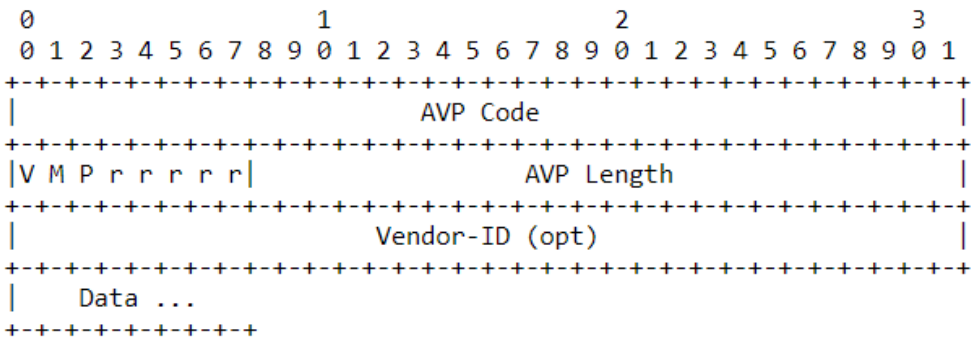

Рис. 3. Структура AVP-заголовку

• AVP code – код AVP у поєднанні з полем Vendor-Id однозначно ідентифікує атрибут. Номери AVP від 1 до 255 зарезервовані для повторного використання атрибутів RADIUS без встановлення поля Vendor-Id. Номери AVP 256 і вище використовуються для Diameter.

• AVP flags – інформує одержувача, як потрібно обробляти кожен атрибут. Новим додаткам DIAMETER не слід визначати додаткові біти прапора AVP.

• AVP length – вказує кількість октетів у цьому AVP, включаючи поле коду AVP, поле довжини AVP, поле прапорів AVP, поле ідентифікатора виробника (якщо воно є) та поле даних AVP. Якщо повідомлення надійшло з недійсною довжиною атрибута, воно повинно бути відхилене.

Виявлення однорангового вузла

Одним із покращень протоколу Diameter, на відміну від RADIUS, є відсутність необхідності ручного налаштування місцезнаходження AAA-серверу на NAS для передачі запитів від користувачів. Diameter дозволяє знаходити однорангові вузли. Окрім ручного налаштування, яке має підтримуватись усіма Diameter-вузлами, для динамічного виявлення можуть підтримуватись два параметри – SRVLOC та DNS. У цьому полягає концепція, що Diameter-вузлам потрібно повідомляти, які додатки вони підтримують, а також необхідний рівень безпеки.

Знайшовши одноранговий вузол, Diameter-вузол може записати його місцезнаходження та конфігурацію маршрутизації у таблиці:

• Peer Table – використовується вручну, для зберігання адрес хостів відомих Diameter-вузлів. Також, записи містять інформацію про метод виявлення вузла (динамічно чи статично) та інформацію про захист.

• Peer Routing Table – має чотири стовпці: Real Name та Application Name, що визначають критерії вибору для маршрутизації повідомлень. Третій стовпець – дія, яку необхідно виконати для цільового повідомлення (може бути PRO□Y, RELAY, REDIRECT або LOCAL). Дія LOCAL означає, що повідомлення необхідно обробити локально, без пересилки на інші сервери. Четвертий стовпчик посилається на запис у Peer Table, щоб визначити реального адресата хоста адресата.

З'єднання і сесія

Після виявлення однорангового вузла, необхідно створити фізичне з'єднання з ним. Для цього Diameter використовує TCP або SCTP, які забезпечують надійнішу передачу, ніж це було у RADIUS. Протокол Diameter явно визначає, що Diameter-вузол, як мінімум, повинен встановлювати з'єднання з двома одноранговими вузлами у кожній області, які виступають як первинні (primary) і вторинні контакти (secondary contact). Природно, що при необхідності могли б бути встановлені додаткові з'єднання.

Сесія – логічне з'єднання між двома Diameter-вузлами і може пересікати декілька фізичних з'єднань. Сесія описує взаємодію між Diameter-клієнтом та Diameter-сервером протягом певного проміжку часу. Кожна сесія асоціюється із Session-Id, який унікальний глобально та протягом усієї сесії (Рис. 4). Крім того, Session-Id використовується для ідентифікації кожної конкретної сесії при подальшому обміні інформацією.

Ініціювання сесії відбувається як і у більшості клієнт-серверних моделей. Diameter-клієнт передає повідомлення auth-request Diameter-серверу, у якому

міститься Session-Id. Варто зазначити, що пари AVP (описані вище) залежать від додатків і не визначені у базовому протоколі.

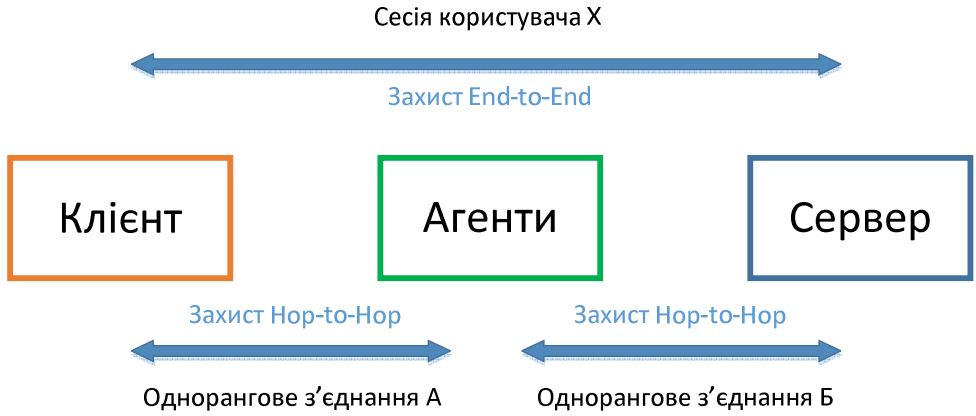

Рис. 4. Diameter з'єднання та сесія

Після прийому повідомлення auth-request Diameter-сервер може включити у відповідь Authorization-Lifetime AVP. Ця пара AVP використовується для вказання кількості часу у секундах, який потрібен Diameter-клієнту для повторної авторизації. Після закінчення ліміту часу і допустимого Auth-Grace-Period, Diameter-сервер буде видаляти сесію зі свого списку сесій і звільняти всі ресурси, виділені для неї.

Під час сесії, Diameter-сервер може ініціювати запит повторної автентифікації або авторизації. Це необхідно для перевірки того, чи продовжує користувач використання сесії. Якщо відповідь негативна, то сервер видаляє сесію та припиняє виділення ресурсів для неї.

Повідомлення про завершення сесії використовується тільки для служб автентифікації та авторизації, і тільки тоді коли сесія підтримувалась. Для служб обліку використовується повідомлення про припинення обліку.

Завершення сесії може ініціюватись як клієнтом, так і сервером. Якщо необхідно припинити сесію Diameter-клієнту, то він передає повідомлення серверу повідомлення Session-Termination-Request. У цьому повідомленні міститься AVP Termination-Cause, яка описує причину завершення сесії. Diameter-сервер зі свого боку, якщо бачить, що сесію треба завершити, відправляє клієнту повідомлення Abort-Session-Request. Це може бути у випадку, якщо клієнт вийшов за межі наданого кредиту часу або з адміністративною метою. Проте, в залежності від політик та сценаріїв використання, Diameter-агент може не дозволити закрити сесію, навіть попри повідомлення від серверу.

Висновки

Описаний у статті протокол Diameter є логічним продовженням та удосконаленням протоколу RADIUS, який активно використовується у наш час у різних топологіях комп'ютерних мереж для реалізації безпекових принципів

архітектури AAA. Проте, об'єктивно, RADIUS має масу недоліків, які, власне, і покликаний усунути Diameter. Для підсумку, нижче наведена таблиця (Табл. 1) порівняння двох протоколів AAA описаних у статті:

Таблиця 1

Порівняння протоколів Diameter та RADIUS

	Diameter	RADIUS
Транспортний протокол	TCP/SCTP	UDP
Захист	Hop-to-Hop, End-to-End	Hop-to-Hop
Підтримувані агенти	Relay, Proxy, Redirect, Translation	Поведінку агента можна реалізувати на сервері
Можливості по узгодженню	Узгоджує підтримувані додатки та рівень безпеки	Не підтримується
Виявлення вузлів	Статична конфігурація, динамічне виявлення	Статична конфігурація
Повідомлення ініціації сервера	Підтримується	Не підтримується
Максимальний розмір даних атрибутів	16 777 215 октетів	255 октетів
Підтримка сторонніх виробників	Підтримка сторонніх атрибутів та повідомлень	Підтримка тільки сторонніх атрибутів

Література

1. C. Rigney. S. Willens, A. Rubens, W. Simpson, Remote Authentication Dial In User (RADIUS), RFC 2865, June 2000.
2. P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, Diameter Base Protocol, RFC 3588, September 2003.
3. Дж. Лиу, С. Джианг, Х. Лин, «Введение в Diameter. AAA-протокол следующего поколения» [Електронний ресурс] : https://www.ibm.com/developerworks/ru/library/wi-diameter/#artrelatedtopics
4. С.А. Владимиров, «Организация услуг на сети доступа» [Електронний ресурс]: http://www.opds.spbsut.ru/data/_uploaded/mu/tad/vlsa-sad-lec/Lec_4_Organizacia_uslug.pdf

References

1. C. Rigney. S. Willens, A. Rubens, W. Simpson, Remote Authentication Dial In User (RADIUS), RFC 2865, June 2000.
2. P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, Diameter Base Protocol, RFC 3588, September 2003.
3. J. Liu, S. Jiang, H. Lin, «Introduction to Diameter. Next generation AAA protocol» [Electronic resource] : https://www.ibm.com/developerworks/ru/library/wi-diameter/#artrelatedtopics

4. S.A. Vladimirov, «Organizatsiya uslug na seti dostupa» [Electronic resource]: http://www.opds.spbsut.ru/data/_uploaded/mu/tad/vlsa-sad-lec/Lec_4_Organizacia_uslug.pdf