Flat Layer Radius Model: Reducing Authentication Delay in eduroam

Rajashree Sokasane[1], Kyungbaek kim[1],

[1] Distributed Network & System Laboratory,
Department of Electronics & Computer Engineering,
Chonnam National University
77 Yongbong-ro, Buk-gu, Gwangju, Korea

Abstract. Eduroam is a secure worldwide wireless network which allows users to access the Internet with their own credentials at visiting institution during roaming. We focused on authentication delay of RADIUS based tree structure in eduroam. In a tree structure, all authentication traffic flows through the whole tree hierarchy even though a user is only of interest to the information of a leaf RADIUS server, and it causes long authentication delay. In this paper, the flat layer RADIUS server model is proposed in order to improve the performance of the authentication process. In the flat layer RADIUS server model, an authentication request is directly forwarded to the target RADIUS server by referring a domain mapping table which has mappings between domain names and contact points of RADIUS servers. By using the Flat Layer RADIUS server model we can reduce the authentication delay as well as we can avoid single points of failures.

Keywords: eduroam, Wi-Fi roaming, RADIUS, Hash Table.

1 Introduction

Wi-Fi Technology has become increasingly popular due to its flexibility and mobility. A user can access to the Internet by establishing a connection with a Wi-Fi access point. However, in order to use Wi-Fi connections users needs to pass through authentication process because of various reasons such as privacy and management. For example, Wi-Fi access points run by an educational institute should be accessible only to faculties, students and staffs of the institute.

The Wi-Fi authentication process is basically supported by an individual access point with WPA (Wi-Fi Protected Access) and WPA-PSK (pre shared key) [2]. Moreover, for an enterprise the Wi-Fi authentication process is managed by network servers such as RADIUS (Remote Access Dial-In User Service) server [1], and a user can access multiple Wi-Fi access points with a same authentication key or credential which is registered on a RADIUS server.

Furthermore, in order to expand the coverage of availability of Wi-Fi connectivity, RADIUS servers can exchange the information of users' authentication keys or credentials. A representative example is eduroam [5] which is a secure roaming system between educational institutes. The goal of eduroam is allowing a user of an educational institute A to connect any Wi-Fi access points deployed in different educational institute B by using the authentication key or credential issued by the institute A.

The authentication process of eduroam is based on the tree structured RADIUS servers. However, the tree structured RADIUS approach has some room for improvements. Some of the issues of the tree structure based RADIUS approach are: all authentication traffic flows through the whole tree hierarchy even though a user is only of interest to the information of a leaf RADIUS server of the tree, and it causes long authentication delay. The authentication delay becomes much longer when the tree structured RADIUS servers are spread over WAN (Wide Area Network). Another issue of the tree structured RADIUS servers is that having a chain of intermediate systems introduces single points of failure.

In this paper, a flat layer RADIUS server model is proposed in order to improve the performance of the authentication process of an eduroam-like Wi-Fi access point sharing service. The flat layer RADIUS server model is a domain mapping based RADIUS structure. An authentication request is directly forwarded to the target RADIUS server by referring the domain mapping table which has mappings between domain names and contact points of RADIUS servers. To evaluate the performance and feasibility of the proposed flat layer RADIUS server model, the authentication delay is measured on various RADIUS structures which are composed of modified open-source based RADIUS servers connected over an emulated network.

The remainder of this paper is structured as fallows. Section 2 provides background of eduroam and RADIUS server. Section 3 describes the proposed flat layer RADIUS server in detail. Section 4 presents the results of the implementation based evaluations. Finally, Section 5 covers conclusion and discussions.

2 Background

In this section we give an overview of the eduroam, authentication process and each related protocol, such as Remote Authentication Dial-In User Service (RADIUS).

2.1 Eduroam

The eduroam originally proposed by TERENA (Trans-European Research and Education Networking Association). The eduroam allows students, researchers and staff from home institutions to obtain Internet connectivity when visiting to other other institutions. The eduroam principle[7] is based on the fact that the user's authentication is done by the user's home institution, whereas the authorization decision allowing access to the network resources is done by the visited network. In eduroam the most secure encryption and authentication standards are used, which gives an access to authorized users only [7].

The eduroam is based on hierarchical structured RADIUS proxy servers and IEEE802.1X. Fig. 1 shows an example of the RADIUS proxy tree in eduroam. When a user accesses an access point (AP) in the network of visited institution, authentication information is transmitted from visited institution to user's home institution through RADIUS proxy tree [5]. If the authentication is successful, the user can use the network of visited institution.

When a user tries to log on to the wireless network of a visited eduroam-enabled institution, the user's authentication request has been sent to the user's home institution. This process is done via a hierarchical system of RADIUS servers. The user's home institution verifies the user's credentials and sends to the visited institution (via the RADIUS servers) the result of such verification.

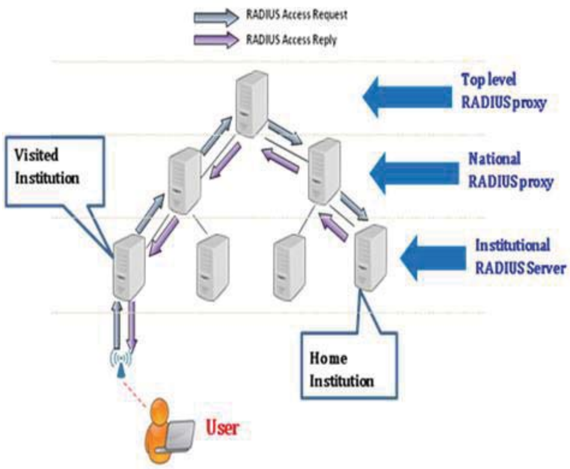

Fig. 1. RADIUS based tree structure in eduroam

2.2 RADIUS server

A RADIUS server is a mechanism for regulating access to a computer network by users [8]. It makes sure that they are authorized. The RADIUS server checks the passwords entered by the users and grants or denies access as appropriate as shown in Fig. 2. It also keeps a record of network usage. RADIUS is a networking protocol that provides centralized AAA (Authentication, Authorization and Accounting) [8] management for computers to connect and use a network service [6].

Authentication is the process of determining the identity of a user. The most common form of authentication is by user name and password. Other forms use digital certificates, digital signatures, etc.

Authorization is the process of determining which service(s) a user is permitted to use and to what extent. It requires that the identity of the user be previously established by authentication process.

Accounting is the process of keeping track of network usage. It records the date and time of the start of each user's session, its duration and the number of bytes transferred.

RADIUS can act as a proxy or RADIUS client which is able to forward a request to another server in different domain. To support this function, the roaming user sends its identity with specific format (userid@realm), when a RADIUS server in visited domain receives an AAA request for a user name containing a realm; the server will reference table/files of configured realms. If the realm is known, the server will then forward the request to the configured home server for that domain. A proxying capability is used to give service to roaming user whenever they move, such as in eduroam [9].

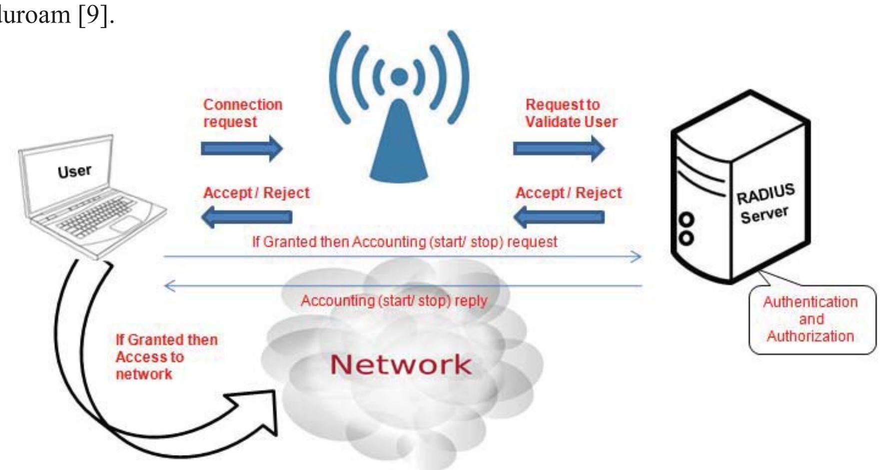

Fig. 2. RADIUS Server Work Flow

3 Flat Layer RADIUS Server Model

Although eduroam is a secure roaming system between research and educational institutions; it has some disadvantages especially with its RADIUS based tree structure. Every authentication traffic flows through the whole hierarchy [4] even though it is only of interest to a leaf RADIUS server that causes long authentication delay. As a result of RADIUS based tree structure the upper level RADIUS are used more frequently, and considered more important than lower level RADIUS. If the upper level RADIUS proxy has some failure then we cannot reach up to the RADIUS with requested domain; and also having a chain of intermediate systems introduces single points of failure.

To overcome those issues, we proposed domain mapping based flat layer RADIUS structure instead of RADIUS based tree structure. In flat layer RADIUS server model, each RADIUS is directly communicate with each other, i.e. without using any intermediate RADIUS proxy servers. By using this Flat Layer RADIUS server model we can reduce authentication delay as well as avoid single point's failure.

In flat layer RADIUS server model, each RADIUS server maintains a domain mapping table with mappings between domain name and other RADIUS. For this we must take for granted that each RADIUS server in a network has known about other RADIUS servers. With the flat layer RADIUS server model, an authentication request is forwarded directly to a destination RADIUS by referring the domain mapping table with the requested name.

For example, consider an eduroam like Wi-Fi access point sharing system has four RADIUS servers namely R1, R2, R3 and R4. Like Fig. 3, in this case each RADIUS server has a domain mapping table with tuples like (R1, jnu.ac.kr), (R2, snu.ac.kr), (R3, knu.ac.kr), (R4, cnu.ac.kr).

If request arises at R1 for user@knu.ac.kr then R1 is directly connected to the R3. In this case there is no need to use R2 as intermediate RADIUS proxy to connect with R3; I.e. Path for authentication is R1 → R3 instead of R1 → R2 →R3. Authentication takes place on R3 and response is forwarded to R1. By using this Flat Layer RADIUS server model, it is not needed to travel through unnecessary RADIUS proxies; we can directly communicate with the RADIUS which is corresponding to the requested domain.

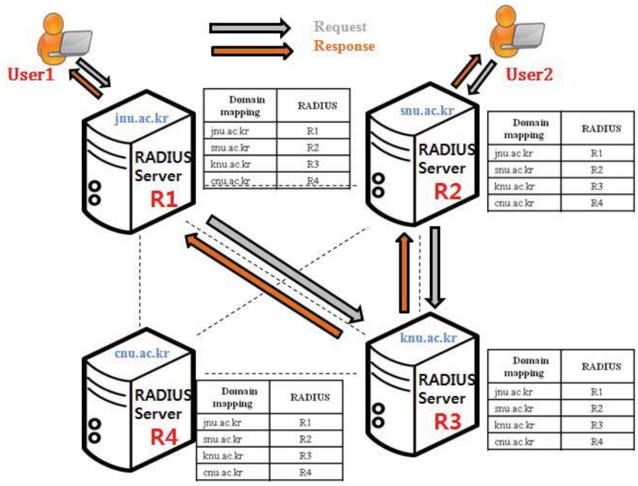

Fig. 3. RADIUS based flat layer structure

4 Evaluation

To evaluate performance of Flat layer RADIUS server model we compared Flat layer RADIUS server model with RADIUS based tree structure in eduroam.

4.1 Evaluation settings

We used an open source based freeRADIUS (version 2.1.8) on ubuntu (version 10.04.4) as RADIUS servers.

According to the structure of RADIUS servers, we can apply different configurations of connectivity of RADIUS servers. For considering WAN (Wide Area Network) connectivity between RADIUS servers we emulate network links between each RADIUS servers and 100ms delay.

We compared Flat layer RADIUS server model with RADIUS based tree structure models (three hops away and two hops away models) in eduroam.

In Fig. 4 RADIUS R1, R3 and R4 work as RADIUS proxy and R2 works as RADIUS server. When request arises at R1, it checks whether requested realm is found for processing on it, if not then request is forwarded to next RADIUS (R3) for further process. When request arises at R3 (here R3 also works as RADIUS proxy) it checks whether requested realm is found for processing on it, if not then request is forwarded to next RADIUS (R4) for further process. When request arises at R4 (here R4 also works as RADIUS proxy) it checks whether requested realm is found for processing on it, if not then request is forward to next RADIUS R2. When request arises at R2 it checks for requested realm, if requested realm founds then it check user's validity. If the requested user is valid then sending access accept response back to the user.

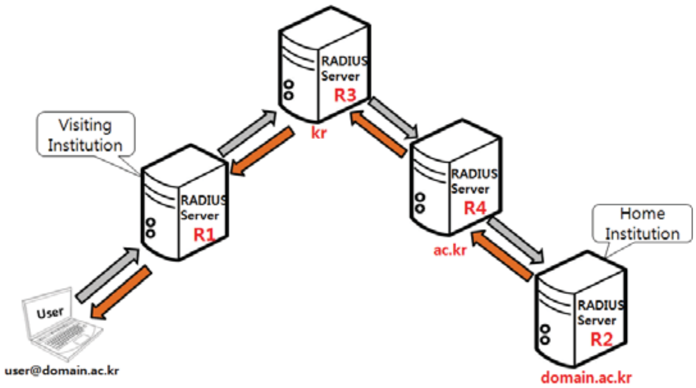

Fig. 4. RADIUS based tree structure with three hops away

Fig. 3 illustrates flat layer RADIUS server model and Fig. 4 illustrates RADIUS based tree structure - three hops away. In the both structures, we requested for same domain. In flat layer RADIUS server model the path for authentication is R1 → R3, whereas RADIUS based tree structure – with three hops away the path for authentication is R1 → R3 → R4 → R2.

If we compare flat layer RADIUS server model with RADIUS based tree structure - two hops away. In this case we consider R4 is our destination RADIUS in tree structure - two hops away. In both structure we requested for same domain. In flat layer RADIUS server model the path for authentication is R1 → R4, whereas RADIUS based tree structure – with two hops away the path for authentication is R1 → R3 → R4.

In case of tree structure (three hops away and two hops away) we need intermediate RADIUS proxy to forward the request to a destination RADIUS, however in case of flat layer RADIUS server model the request forwarded directly to the destination RADIUS without using any intermediate RADIUS.

We have measured authentication time which includes request forwarding process, authentication process, and response forwarding process and network latency.

Request forwarding is a process in which the request is processed and decided to forward it to next device for further processing.

Authentication process is a process in which authentication takes place on the basis of requested user credential.

Response forwarding process is a process in which reply of authentication (Access-Accept / Access-Reject) is forwarded to user.

Network latency is a time required for forwarding request or response from one to other RADIUS server.

Authentication time is defined as the time involved in an authentication phase of security protocol.

4.2 Results

Table 1 AUTHENTICATION TIME (μs)

	Tree structure 3 hops away	**Tree structure 2 hops away**	**Flat Layer RADIUS model**
Request Forwarding Process	1155	711	273
Authentication Process	330	237	242
Response Forwarding Process	559	278	134
Network latency	620823	402997	201330

Table 2 REQUEST PROCESSING TIME

Process/machine	Time in μs
Request Forwarding	357
Authentication	270
Response Forwarding	162

From Table 1 it is observed that the dominant delay for the whole authentication time is the network latency. It has clearly observed from Table 1 that flat layer RADIUS server model takes less authentication time than RADIUS based tree structures. Also, it is observed that the authentication time increases most likely in linear along with the depth of the tree structure. In particular, the authentication time of 3 hops away tree structure exhibits 3 times more delay than the flat layer RADIUS server model.

From Table 2 it is observed that the request forwarding process takes more time than the response forwarding process. Specifically, the request forwarding time is almost twice of the response forwarding time. During the request forwarding process, a RADIUS request is matched to the domain mapping table in order to find out the next RADIUS server to which the request is forwarded. This process takes place on every node along with the path of the RADIUS request. On the other hand, the response process is relatively simpler than the request process. When a RADIUS request reaches at the destination RADIUS server, it is authenticated on that particular server and the server response in forwarded to user. The response forwarding process simply forwards the response along with the opposite path of the RADIUS request. Consequently, the response forwarding process takes about twice less time than the request forwarding process.

5 Conclusion and discussion

In this paper we presented the flat layer RADIUS server model, in which each RADIUS server in a network has known about each other RADIUS servers and each RADIUS server maintains a domain mapping table with mappings between domain name and other RADIUS. The experimental results demonstrate that the network delay is the dominant factor of the whole authentication time of RADIUS request, and the flat later RADIUS server model is promising to make edurom-like services more scalable than RADIUS based tree structure. Also, through the detail results, it is observed that the request forwarding process takes more time than the response forwarding process. That is, to reduce the authentication delay of RADIUS request, it is better to improve the performance of the request forwarding process.

In a flat layer RADIUS server cluster, if one new RADIUS server is added then we have to modify domain mapping tables of all existing RADIUS servers. To support this, we need a manager which keeps current domain mapping table in dynamic situation where RADIUS servers join and leave at their will. Currently we are developing the manager to handle such situation.

Acknowledgements

This research was supported by the MSIP(Ministry of Science, ICT&Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2013-H0301-13-3005) supervised by the NIPA(National IT Industry Promotion Agency).

References

1. L. Phifer , "Using RADIUS For WLAN Authentication, Part I "
2. Wikipedia. http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
3. Y. Watanabe, H. Goto, H. Sone, "Resource Access Control for Wireless LAN Roaming Systems", in Proceedings of International Symposium on Applications and the Internet, 2008 p. 281-284.
4. K. Wierenga, L. Florio, "eduroam: Past, Present and Future", Computational Method in Science and Technology, vol. 11, pp. 169-173, 2005
5. Yoshinori MIYAMOTO, Yasuhiro YAMASAKI, Hideaki GOTO Hideaki SONE "Optimization System of IP Address Using Terminal ID in eduroam" in Proceedings of 2011 IEEE/IPSJ International Symposium on Applications and the Internet.
6. Wikipedia. http://en.wikipedia.org/wiki/RADIUS
7. eduroam. https://www.eduroam.org
8. RADIUS. http://www.wifi.keller.com/CNIT107HW7.html
9. L. Florio, K. Wierenga, "eduroam, providing mobility for roaming users."
10. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification", IEEE Std. 802.11, 1997.