International Journal of Multimedia and Ubiquitous Engineering
Vol.9, No.2 (2014), pp.161-168
http://dx.doi.org/10.14257/ijmue.2014.9.2.16

Reduce Authentication Delay in Eduroam Using Flat Layer Approach

Rajashree Sokasane and Kyungbaek Kim

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

Abstract

Eduroam is a Wi-Fi roaming system which allows a user of a domain to access wireless resources in another domain with the unique credential of the user managed in the original domain. Eduroam employs a hierarchical tree structure of RADIUS servers to provide a scalable authentication procedure over wide area networks. However, the tree structure of RADIUS servers causes long latency of remote authentication procedures, and the single point of failures can be issued. In this paper, we propose a flat layer approach to build a network of RADIUS servers in order to reduce the delay of remote authentication procedures and eliminate the concern of the single point of failures. In the flat layer approach, each RADIUS server knows the information of all the other RADIUS servers through a domain mapping table. The domain mapping table is updated whenever the membership of the network of RADIUS servers is changed. To make the updating operation of domain mapping tables more efficient and faster, DHT based broadcasting approach is used. Through an implementation based evaluation, we show that our flat layer approach is efficient and viable in practice.

Keywords: *eduroam, Wi-Fi roaming, RADIUS server, Domain mapping table, Distributed Hash Table*

1. Introduction

Eduroam is a secure roaming system between educational institutes. Eduroam provides secure wireless access for roaming and stationary end-users that just works everywhere: "*Open your laptop and be online*" [11]. Eduroam allow its domain user(s) to access wireless resources in another domain with the same credentials used with the original domain; to use Wi-Fi roaming facility, users needs to pass through an authentication process. The authentication process in eduroam is based on the hierarchical tree structured RADIUS servers over wide area networks. However, hierarchical tree structure approach in eduroam causes long latency of remote authentication procedure, and also issues the single point failures. In order to reduce the delay of remote authentication procedure and to avoid the single point failure problem we propose a flat layer approach to build RADIUS server network in eduroam.

In the flat layer approach, each domain in the network knows the every other domain information in the network through the domain mapping table. Domain mapping table needs to be updated, either a new member joins the network or existing one leaves the network. If new node (RADIUS server) joins the network then domain mapping table present on all other nodes in the network needs to be updated with new node domain information. One of the nodes in the network is responsible to broadcast the information of join/leave node operation to all other nodes in the network to update their domain mapping table with latest

ISSN: 1975-0080 IJMUE

membership updates. With this simple broadcasting approach in the network, update operation may take much time to update all domain mapping tables in the network.

In order to update the domain mapping tables more efficient and faster, DHT based broadcasting approach is used. In DHT based broadcasting approach, multiple nodes are responsible to broadcast information of join/leave node operation over the network. DHT is dynamically managing the nodes, which are responsible for broadcasting the information of join/leave node operation.

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

2. Background

2.1. Eduroam

The eduroam originally proposed by TERENA (Trans-European Research and Education Networking Association). 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]. Eduroam provides the most secure encryption and authentication standards. Eduroam gives an access to its authorized users only [7]. After successful authentication, the user can get access to the network of visited institution. Figure 1 shows an example of the RADIUS proxy tree in eduroam.

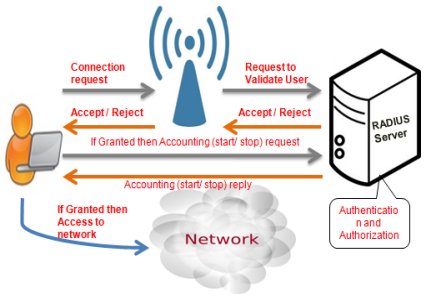

Figure 1. Hierarchical tree structure of RADIUS in eduroam

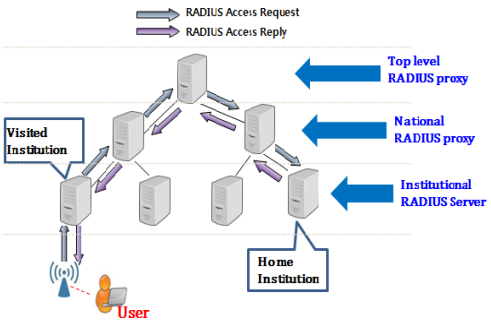

Figure 2. Authentication in a RADIUS Server

2.2. RADIUS server

A RADIUS server is uses as authentication server in eduroam. A RADIUS server makes sure that they are authorized. Figure 2 shows how authentication request is handled by RADIUS server. A RADIUS server is a mechanism for regulating access to a computer network by users [8]. RADIUS is a networking protocol that provides centralized AAA management for computers to connect and use a network service [8, 6]. The RADIUS server checks the login credentials such as user name and password entered by the users and grants or denies access as appropriate. It also keeps a record of network usage. A proxying capability of RADIUS server is used to give service to roaming user whenever they move, such as in eduroam [9]. To support this function, the roaming user sends its identity with specific format like userid@realm.

3. Flat Layer Approach

The aim of eduroam is to enable a quick and easy way to obtain a secure access to the Internet for their registered user [7]. Although eduroam is a secure roaming system between research and educational institutions; existing tree structure approach in eduroam has some limitations. Existing tree structure approach in eduroam causes long authentication delays [4] and it is self-configurable in case of join/leave node operation takes place in the network. In order to overcome these limitations we proposed flat layer approach with eduroam.

3.1. Domain Mapping based Flat Layer Approach

In domain mapping based flat layer approach, we used domain mapping table to map domain information of existing nodes in the network. In domain mapping based flat layer approach, each node (RADIUS server) in the network is directly communicate with each other, *i.e.*, without using any intermediate node (RADIUS proxy servers). With this functionality of domain mapping based flat layer approach, we can reduce authentication delay.

In domain mapping based flat layer approach, each RADIUS server maintains a domain mapping table with mappings between domain name and RADIUS server associated with it. For this we must take for granted that each node in the network knows about every other node. With the domain mapping based flat layer approach, an authentication request is forwarded directly to a destination node by referring the domain mapping table with the requested domain name. Figure 3 shows an overview of domain mapping based flat layer approach.

For example, consider an eduroam like Wi-Fi access point sharing system has four RADIUS servers namely R1, R2, R3 and R4. Like Figure 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.

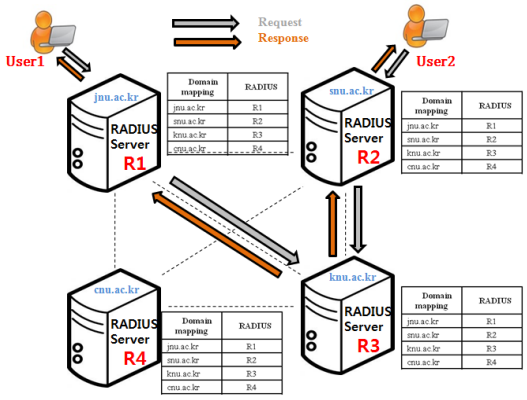

Figure 3. Overview of Domain Mapping based Flat Layer Approach

3.2. Update operation in Flat Layer Approach

In this section we focus on the updating operation of domain mapping table, with broadcasting in flat layer approach. In existing tree structure approach of eduroam, if join/leave node operation takes place in the network then it is not dynamically managed by the system. In the flat layer approach, join/leave node operation is automatically handled by the system with broadcasting latest membership information. Figure 4 shows simple broadcasting approach. With simple broadcasting approach, if new node sends the join request to one of the nodes in network then that node broadcast the new nodes domain information, to all the other nodes in the network. In simple broadcasting approach, only one node in the network is responsible to broadcast the latest membership information to all the other nodes in the network. If the number of nodes in the network is large then simple broadcasting may lead to overhead. With simple broadcasting approach, the nodes take much time to update their domain mapping tables with latest membership information; it may cause for bottleneck.

In order to make the updating operation of domain mapping table more efficient and faster, we used DHT based broadcasting approach. Figure 5 shows how update operation takes place with DHT based broadcasting approach. In DHT based broadcasting approach, if join/leave node operation takes place in the network then all other nodes in the network need not to update with latest membership information; rather the node(s) associated with the join/leave node needs the update. In DHT based broadcasting approach, multiple nodes take responsibility to broadcast latest membership information. DHT is dynamically managing the nodes that are responsible to broadcast the latest membership information over the network. The maintenance cost of flat layer approach with DHT based broadcasting is lower than that of with simple broadcasting. Latest membership information updating operation in eduroam is easily handled with the help of DHT based broadcasting approach.

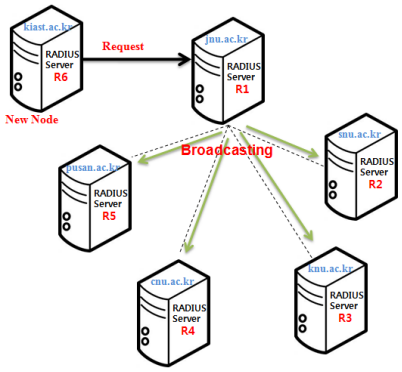

Figure 4. Simple Broadcasting

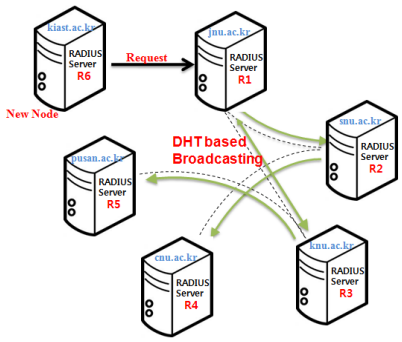

Figure 5. DHT based Broadcasting

4. Implementation and Evaluation

To evaluate performance of flat layer approach with eduroam, we compared domain mapping based flat layer approach with tree structure approach in eduroam.

4.1. Implementation

We implemented a proxy server for a RADIUS server to support join/leave updating operation in eduroam with flat layer approach. A proxy server processes the incoming join/leave requests and sends related messages to all RADIUS servers in the flat layer

network. When the RADIUS server gets a join/leave node request, the proxy server processes the request and modifies configuration files of the RADIUS server, *e.g.*, proxy.conf and clients.conf, to keep them up-to-date with latest membership changes. A proxy server takes responsibility of configuring domain mapping tables automatically, presenting on all RADIUS servers in the network with latest domain information.

4.2. Evaluation

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 Figure 6 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.

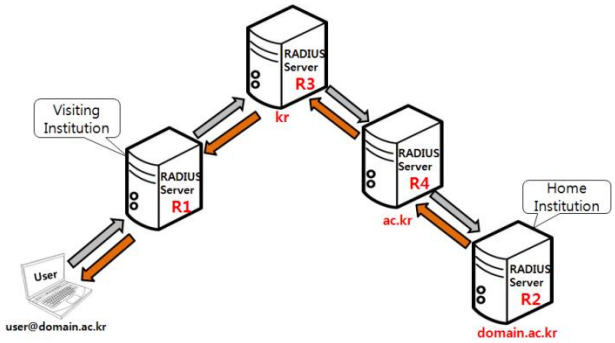

Figure 6. Hierarchical tree structure of RADIUS with three hops away

Figure 3 illustrates overview of domain mapping based flat layer approach and Figure 6 illustrates hierarchical tree structure of RADIUS server - three hops away. In 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 hierarchical tree structure of RADIUS server - 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 process* 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.

4.3. 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 approach to build RADIUS server network for eduroam; in which each RADIUS server in a network has known about each other RADIUS servers by using domain mapping table. In order to maintain up-to-date domain information of every domain in the network, we need to update domain mapping table after every join/leave node operation takes place in the network. With simple broadcasting approach, we keep all domains up-to-date with latest membership information; but it may lead us to problems like overhead and bottleneck.

To avoid such problems and to keep all domains up-to-date with latest membership information more efficiently, we used DHT based broadcasting approach. DHT based broadcasting approach, is more efficient and faster than simple broadcasting, while handling updating operation in flat layer approach of eduroam.

Acknowledgements

This research was supported by the MSIP(Ministry of Science, ICT&Future Plan-ning), 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] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access.
[3] Y. Watanabe, H. Goto and H. Sone, “Resource Access Control for Wireless LAN Roaming Systems”, in Proceedings of International Symposium on Applications and the Internet, **(2008)**, pp. 281-284.
[4] K. Wierenga and L. Florio, “eduroam: Past, Present and Future”, Computational Method in Science and Technology, vol. 11, **(2005)**, pp. 169-173.
[5] Y. Miyamoto, Y. Yamasaki, H. Goto and H. Sone, “Optimization System of IP Address Using Terminal ID in eduroam”, in Proceedings of 2011 IEEE/IPSJ International Symposium on Applications and the Internet, **(2011)**.
[6] 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)**.
[11] http://www.eduroam.ua.ac.be/.
[12] R. Sokasane and K. Kim, “Flat Layer Radius Model: Reducing Authentication Delay in eduroam”, in Proceedings of the 2nd International Conference on Smart Media and Applications, **(2013)**.