Central Authentication Server for a Wireless Ad-Hoc Network

Ganesh Gupta[1]**, Dr. Vivek Jaglan**[2]**, Dr. Ashok K Raghav**[3]

[1]Research Scholar, ASET, Amity University Haryana, Gurugram, India
[2]Department of Computer Science, ASET, Amity University Haryana, Gurugram, India
[3]Director Industrial Research & Training, Amity University Haryana, Gurugram, India
[1]ggupta@ggn.amity.edu, [2]vjaglan@ggn.amity.edu, [3]akraghav@ggn.amity.edu

Abstract- **The purpose of this research is to examine the field of authentication and authorization for ad-hoc wireless users connected to Central Authentication Server. The topic has gained certain popularity over the last decade because of the constant growth of Ad-hoc wireless users. The paper defines AAA protocols idea, authentication protocols and security standards. The practice explains by steps the implementation in to the private network of the RADIUS protocol that was chosen as an AAA protocol.**

This central authentication system will authenticate the users using their username and password which they created before in the server and according to that username and password they can connect to the network and they will be authenticated by central RADIUS Server. Hence a new user can access all the services anytime anywhere.

Keywords— RADIUS,CHAP,PAP,AAA,VLAN etc.

I. Introduction

RADIUS Server is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

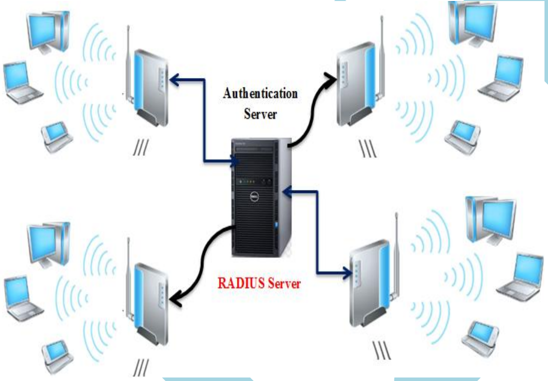

Figure 1: Central Authentication Server

RADIUS allows an organization to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing an organization to set up a policy that can be applied at a single administered network point.[1]

Having a central service also means that it's easier to track usage for billing and for keeping network statistics. Created by Livingston (now owned by Lucent), RADIUS is a de facto industry standard used by a number of network product companies and is a proposed IETF standard.

II. Principal of RADIUS Server Authentication

RADIUS is an AAA protocol that manages network access. AAA stands for Authentication, Authorization and Accounting.

It uses two packet types to manage the full AAA process

1. Access-Request: it manages authentication and authorization.

2. Accounting-Request: It manages an accounting. Authentication and authorization .

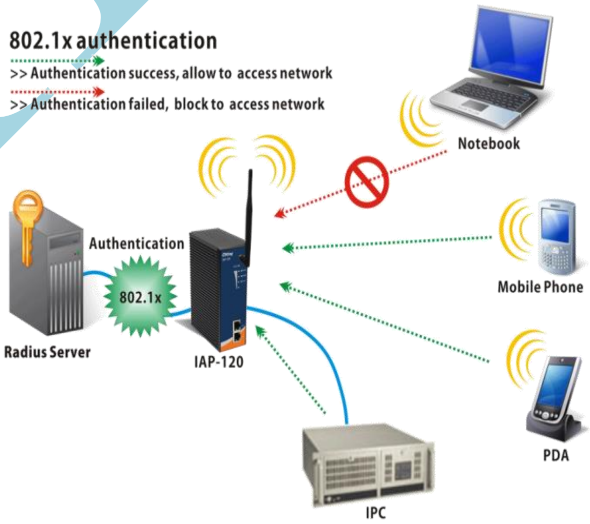
802.1x authentication
>> Authentication success, allow to access network
>> Authentication failed, block to access network
Notebook
Authentication
802.1x
Mobile Phone
Radius Server
IAP-120
PDA
IPC

Figure 2: Authentication Proces

Authentication Steps [2]

1. The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS

2. The NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access

3. The RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP or EAP. The user's proof of identification is verified.

4. The RADIUS server then returns one of three responses to the NAS.

Access Reject

The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive user account

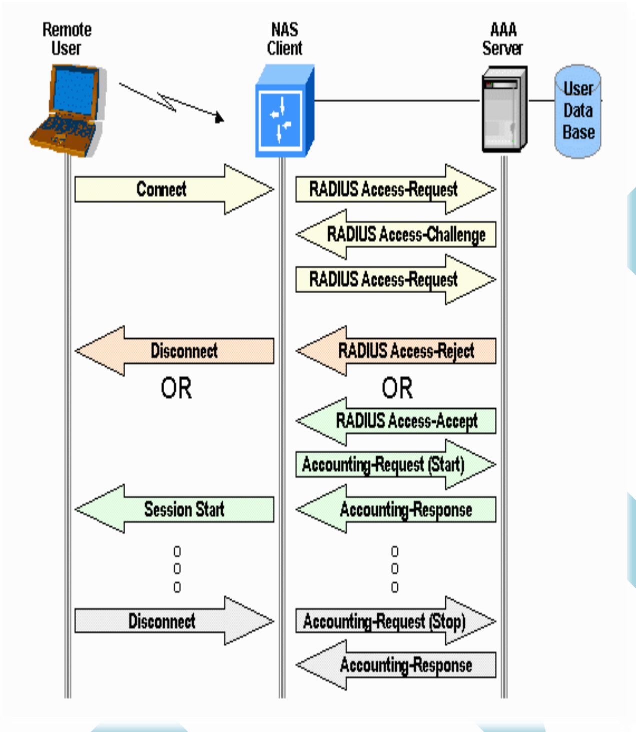

Figure 3: How RADIUS works

Access Challenge

It Requests additional information from the user such as a secondary password, PIN, token, or card. Access Challenge is also used in more complex authentication dialogs where a secure tunnel is established between the user machine and the Radius Server in a way that the access credentials are hidden from the NAS.

Access Accept

The user is granted access. Once the user is authenticated, the RADIUS server will often check that the user is authorized to use the network service requested. A given user may be allowed to use a company's wireless network, but not its VPN service, for example. Again, this information may be stored locally on the RADIUS server, or may be looked up in an external source such as LDAP or Active Directory.

III. Advantage and Disadvantage of RADIUS Server

Advantage :[5]

1) All user can access wireless using username and password

2) No need to add MAC address of the User to Router for wireless access

3) We can Limited access time for users e.g. : 3 hour per day

4) Enhanced reporting and tracking based on client usernames even more so when tied into an LDAP backend such as Active Directory.

5) Ability to direct Faculty into one User Profile and Students into another based on LDAP membership and/or RADIUS attribute return. This allows you to place restrictions on the Student User Profile/VLAN (if desired) while keeping Faculty members unrestricted.

Disadvantage :

1) If users are connecting to the wireless network for the first time it need to install certificate of the server for windows users it would be difficult

2) High speed server to respond for all the users

IV. Analyzing Centralized System

A centralized management system allows one to create, manage system, user privileges, authentication, and security within hosting environment far more efficiently than by using local user accounts and individual server management.

TABLE 1. Benefits of Centralized Authentication System

Benefits	**Description**
Simplicity	It is a powerful simple model for managing user account and associated right
Cost effective	A single central model manages the service provider therefore cost reduces on operation.
Single Set of tools	A Single central server maintains active directory to serve as a solution provider where one can get all tools in single set.
Central data Store	A single design for server management means that we can process all recent change from one central data store.
Global Security	Operation benefits are also realized through defining and managing a global security policy including security lockdown process.
Automatic Security deployment	Automatic centralize deployment of security policies minimizes the error of manually lockdown risks.
Increases Overall Efficiency	Cost effectiveness and central data store increases the overall efficiency of this model.

Using centralized management reduces operational complexity, improves security, and lowers risk through consistent policy application. One can use the centralized user database in future and can connect to the other branch as well.

V. CONCLUSION

As from the last some decades it has been seen a growing the usage of wireless technology and people are using PSK (pre shared Key) for all users which is not a secure method or they are using the MAC address filtering to secure wireless network. Implementation of Central authentication server for wireless network necessary to use from recorded information which we have in the server and the user can use that username password for wireless authentication.

The RADIUS server is an open source server (freely available) and it we can have track of the users, and we can add limitation on access time of the user daily or hourly.

REFERENCES

[1] Daniel Szilagyi, Arti Sood and Tejinder Singh, "RADIUS: A REMOTE AUTHENTICATION DIAL-IN USER SERVICE," River Academic Journal, vol. 5, number 2, pp. 1–12, 2009.

[2] B Adida. "Cosign: Secure, intra-institutional web authentication. "http://weblogin.org/ , August,2012.

[3] Penn.CoSign "Troubleshooting" https://www.upenn.edu/ computing/resources/category/web/article/cosign troubleshooting , April,2013.

[4] https://technet.microsoft.com/en-us/library/cc539020.aspx

[5] Eric Geier." Low-cost RADIUS servers for Wi-Fi security" https://www.networkworld.com/article/2160360/servers/low-cost-radius-servers-for-wi-fi-security.html, Sept. 2012.

[6] AJndress, Jason "The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice" 2011.

[7] Z.Dennis.Choosing an SSO strategy. http://www. mutuallyhuman.com/blog/2013/05/09/choosing-an-sso-strategy-saml-vs-oauth2/ (2013, May).

[8] Foursquare. Connect to foursqure. https:/ /developer.foursquare.com/overview/auth , January 2014