# An Analytical and Experimental Study of AAA Model with Special Reference to RADIUS and TACACS+

Arun Pratap Singh Sikarwar
M.Tech. (Network Management & Info. Security)
School of Computer Science & IT
Devi Ahilya University, Indore, India

Preeti Saxena
Reader,
School of Computer Science & IT
Devi Ahilya University, Indore, India.

## ABSTRACT
A significant growth is observed in network technology during last few decades. Several kinds of information services are delivered using the networks. Additionally, both legitimate and malicious users are accessing the services. Moreover, the network is always vulnerable to different kinds of security issues. Therefore the domain of security is an essential aspect of the study, research, and development. For that purpose, the efforts are made to design effective security protocols. During effective security protocol design, the authentication, authorization, and accounting of network access are a key concern. The ability of network security design is well known as AAA model. This presented work investigates about the two popular network security protocols namely RADIUS and TACACS+ to deploy AAA model. Evaluation and comparison of both the security techniques and simulation methodologies are involved in the presented work.

## Keywords
AAA Model, TACACS+, RADIUS, Comparative study, performance analysis, implementation.

## 1. INTRODUCTION
A rapid advancement in communication technology is found in recent years. New users of communication networks are also increasing day by day. In order to deal with the newly generated crowd in network services new and enhance infrastructure is required. Not only QoS is important in the network but the security and privacy are also a major concern. Network security is a domain where it deals with the understanding, controlling and managing the risk of an infrastructure and their assets. Network security has a number of properties to satisfy. The availability, integrity, authentication, confidentiality, and non-repudiation ensure the security. The RADIUS (Remote Authentication Dial- in User Service) and TACACS + (Terminal Access Controller Access-Control System Plus) are key areas of investigation, design, and implementation.

RADIUS and TACACS + are the most prominent network security protocols to deploy AAA model. The AAA is an abbreviation of Authentication, Authorization, and Accounting. AAA model is basically used for securing the network infrastructure such as Internet service provider and enterprise network. AAA has become valuable because it enables the network and service provider to manage the access of the network, network devices, and the distributable services. In addition of that, it offers the tracking and monitoring of network infrastructure by supporting the auditing of the logs [1]. The components of AAA model are [2]:

- **Authentication –**Authentication is a process of verifying and validating the identity of a user. Before providing access to any resource such as device or service in a network, basically, it is required to validate the end user. In most of the authentication systems, a password is required to verify and validate the identity of the user. These days for more secure credentials OTP (one-time password) and biometric systems are used frequently.
- **Authorization –** Authorization is the process of assigning privileges to the users. A significant amount of services are offered in a network infrastructure and a large number of users are available to use them. Different levels of users or authorities need different privileges. Authorization is also included for providing different privileges to service consumers along with authentication.
- **Accounting –** Accounting is a more effective part of the entire network technology. The accessible services, devices, and processes need to keep to track information about the end user and their activity. Therefore some kinds of logs are maintained to make it accountable and auditable for both the ends i.e. consumer and service provider.

The presented work implemented AAA model using the RADIUS and TACACS+ protocols. Additionally, their experimental outcomes are demonstrated by using their comparative performance study. Further, the detailed literature about both the protocols and their simulation environment are presented. In addition of that, the comparative performance study is also reported.

Section 2 provides literature survey. Section 3 demonstrates the utility of AAA model, additionally, the overview of both the protocols are provided. Further, in section 4 the required network configuration and comparative study of both the protocols are provided. Final section 5 draws the conclusion of the work performed. In addition, it includes suggestion and future research directions.

## 2. LITERATURE SURVEY
The recent research work and contributions relevant to AAA model implementation and their deployment for improving the network security is presented here.

The advantage to adopting 802.1 x authentications for network access control is obvious. It is an ideal and low-cost scheme to provide port-based network access control. ***Jiange Zhang et al*** [3]analyzed 802.1x protocol, EAP protocol and RADIUS protocol, and constructed AAA which is based on 802.1 x authentications at the end. Using software the messages of the whole authentication process had been captured. According to AAA mechanism, they analyzed EAP messages and RADIUS messages details. The analysis of these messages provides technology strongly for particular research. The suggested improvement can lead to important value for research and application.

***Jindrich Jelinek et al*** [4] described issues of experiments with the model of the enhanced RADIUS protocol simulated in

Colored Petri Nets. The model simulated the distributed network topology with one supplicant and several RADIUS servers. Experiments showed that the enhanced RADIUS protocol could be a solution of the problem with authentication of a client if its home realm is not reachable and some else realms know the identity of the client. The model of the protocol and the experiments were realized in CPN Tools.

***Gabriel-CătălinCristescu et al*** [5] presented a solution related to the authentication, authorization, and accounting of the users intending to get access to the Internet through a secured network. The RADIUS protocol was used to encapsulate the packets of the PAP, CHAP, MSCHAPv1, and MSCHAPv2 legacy authentication protocols, while the MD4, MD5, salted MD5 and SHA-1 hashing algorithms were used to provide an enhanced security for the user passwords.

In Internet and text documents tons of vital information is available these days. This side-information is available in documents as beginning information, the links within the documents, user access behavior from Internet logs, or different non-textual characteristics which are embedded into the text document. The side-information is employed in document clustering of such documents bunch. This information can embody noisy information as well; therefore it is tough to use it with efficiency. According to literature, some equivalent correct algorithms are required to use such information in document clustering to avoid noise from the extracted clusters. The paper presented properly dominated ways to perform the mining method to optimize the benefits got from mistreatment of this side-information. ***Nisha Bawaria et al*** [6] tried to improve the planning of AAA algorithm to accommodate high security and efficiency of the system.

***Daniel Granlund et al [7]*** presented a scalability study of AAA support in mobile heterogeneous access networks. The study was done with respect to the server and network load related to AAA processes using the RADIUS protocol. Technologies such as IEEE 802.11, CDMA 2000 and UMTS which all support the RADIUS protocol for AAA handling are discussed and analyzed in their work. Typical performance data are gathered and presented with a theoretical study for achieving an overview of the parameters that will affect the performance and scalability of the network. Also, they developed guidelines for network design in order to achieve the desired performance for a given number of users. Results of study represented that the main bottleneck of the AAA procedure is not necessarily the AAA server CPU power. Aside from the cases with a high proportion of computationally intensive Wi-Fi sign-on with strong encryption, performance issues may be caused by AAA server network connection bandwidth, and RAM memory. In cases where a high number of users reside in the same user database, database performance becomes a significant issue. In order to achieve better performance, CPU load balancing over several servers may be performed.

## 3. BACKGROUND

The section provides the discussion about the basic features and capabilities of both the protocols for designing the AAA model.

### 3.1 AAA Model

Basically, the AAA is a security technique deployed in a large network. For deploying the security model RADIUS and TACACS+ servers are used. These security servers are connected through various networking devices such as Routers, Switches, Firewalls and various servers. In any ISP's and Enterprise network, there are many employees (such as, network admin, network Engineers, network managers.) who need to access these network devices and servers. They are the actual users of these devices but they are not directly clients of AAA server. Whenever and wherever the employees need to access any network device they require to get authentication and authorization by AAA Server.

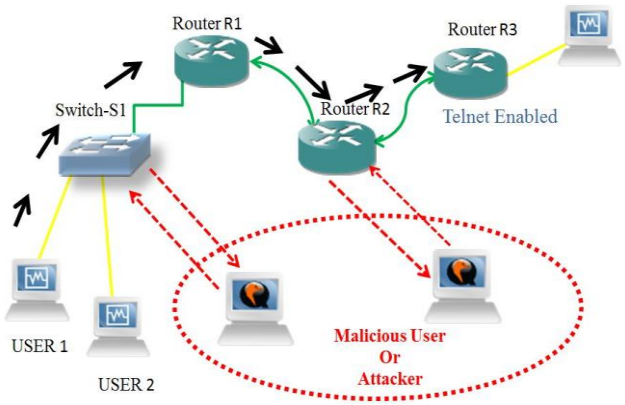


**Figure 1: Why AAA?**

Figure 1 shows the requirement of AAA model. The diagram depicts the connection of users through the Routers and switches. Additionally, users can extend the network for connection to the network and gain access to the network devices and services. On the other hand, as an initial process, authentication provides a way of identifying the user. Therefore user enters a valid user ID and a valid password to grant access. The authentication is based on each user having a unique set of criteria for gaining access. The AAA server verifying and validating user by matching user's authentication credentials with the credentials previously stored in the database. If the credentials match successfully, the user is granted access to the network devices and services, otherwise, authentication fails and network access is denied. Once a user gets authenticated by AAA server and gained access of network device or service user may try to issue some commands. The authorization process determines whether the user has the authority to issue such commands or not. The authorization is the process of enforcing policies and assigning privileges and determining what types of activities, or services a user is permitted. Usually, process authorization takes place within the context of the authentication process. Once the system has authenticated a user, the user may be assigned privileges for different types of access rights or activity.

The final step in the AAA framework is an accounting. The accounting measures the resources, a user consumes during the access. This can include the amount of system time or the amount of data a user has sent and/or received during the session. Accounting is performed by keeping a log of session statistics and usage information. Accounting can be used for the purpose of security audit, resource utilization, authorization control, billing, trend analysis, and capacity planning activities. Figure 2 shows working of user authentication and authorization process. First, the user requests to authenticate through the intermediate devices. In response to the request, the server asks for user credentials. These credentials passed by the user are verified using the server database. If the information is available in the database, the server responses and provides the access for services otherwise the error message is generated.

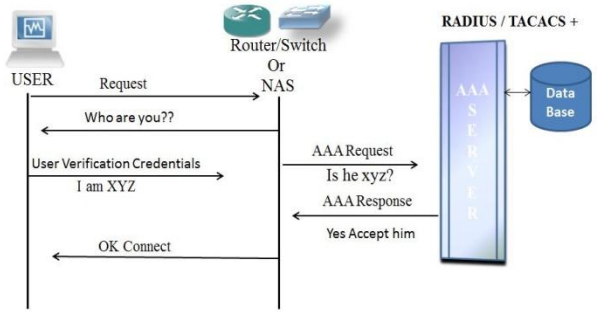


**Figure 2: Working of AAA server**

## 3.2 RADIUS

The RADIUS protocol is also known as Remote Authentication Dial-In User Service. RADIUS was developed by Livingston Enterprises. It is frequently used by Internet service providers and enterprises. The protocol helps to manage access to Internet or internal networks, wireless networks, and integrated e-mail services. RADIUS is a client/server protocol that runs in the application layer, and use UDP as transport. That is also used for deploying AAA security. RADIUS encrypts only the user's password as it travels from the RADIUS client to RADIUS server. Therefore, it is vulnerable to different types of attacks. This protocol may use for embedded network devices such as routers, switches. The reasons behind its use include:

- The embedded devices cannot work with a large number of users with unique authentication.
- RADIUS facilitates centralized user administration, which is important in various applications. Many ISPs have millions of users. Users are added and deleted continuously, and user authentication updated continuously. Therefore centralized administration is an operational requirement of such system.
- RADIUS provides protection against a sniffer and active attacker. Other remote authentication protocols offer irregular, insufficient or non-existent protection. LDAP natively provides no protection against sniffing or active attackers.

Figure 3 depicts the user authentication through Network Access Server (NAS) and RADIUS Protocol. A Point to Point Protocol (PPP) is used for communication between the end user and NAS. In order to authenticate the user, the NAS contacts a Network Policy Server (NPS) using RADIUS protocol. A NAS operates as a client of a server that supports the RADIUS protocol. Servers that support the RADIUS protocol are generally referred to as the RADIUS servers. The RADIUS client passes user information to designated RADIUS server and then acts on the responses received from the RADIUS server.

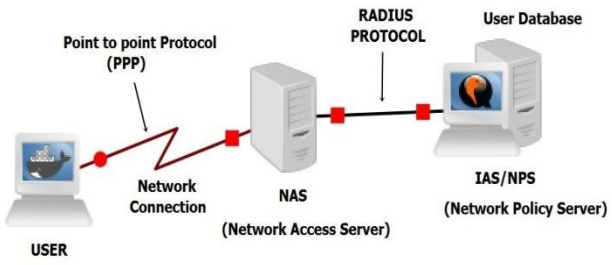


**Figure 3: NAS authenticating user by contacting NPS using RADIUS Protocol**

## 3.3 TACACS+

TACACS+ is also termed as Terminal Access Controller Access-Control System Plus. This protocol is developed by Cisco. The protocol is used for handling authentication and related services, for networked access control through a centralized server. The protocol uses TCP (transmission control protocol). Authentication, authorization, and accounting components of the AAA model can be isolated and taken care on discrete servers. Additionally, TACACS+ encrypts all the data mentioned above and therefore does not have the vulnerabilities [8].

The TACACS+ protocol allows access to network services to control and administrate on a more effective manner. Remote users who want to connect to the network can be first evaluated using user database. A policy is present that controls not only what devices a user can access, but also what services a user can access. If user's account is compromised that account can be disabled immediately. Accounting offers audit trail that helps to track what services the user accessed. During the implementation of TACACS+, it is considered that servers that are running TACACS+ can compromise with an attacker. Thus TACACS+ servers should not run any other application. This minimizes the chances of server compromise. TACACS+ servers should be limited to the devices or clients that need to communicate with the server for authentication. If an attacker wants to gain access, he should not be able to connect to TACACS+ server from any device. It is must to have access control on the routers and also required to apply additional security such as TCP wrappers.

# 4. SIMULATION

This section provides the details about the implementation and simulation for the proposed comparative study.

## 4.1 System Configuration

The simulation is carried out in Windows environment on a quad core machine with 2.7 G Hz speed and 12 GB of RAM.

## 4.2 Simulation Setup

The network is configured and experimentation is performed using four virtual machines running VMware Workstation version 12. The first machine has Windows Server 2012 platform and Radius Server Configured. The implementation requires to utilize the Active Directory and to configure the Network Policy Server. The second machine is running Ubuntu 12.04. This machine is used to configure TACACS + Server. The third machine is used with the Kali Linux installation. This machine is used for demonstrating utilization of the protocols. This machine in other terms is used for the testing purpose. Finally on the fourth machine the Windows -7 is installed. This machine is working as a Remote VPN client. All These machines are needed to be connected therefore required to develop network topology with loopback network adapter. Thus the network is configured and simulated using GNS-3 network simulator.

## 4.3 Network Design on GNS-3

The simulation of assumed network is performed using GNS-3. That is a discrete event simulator and works as the real-time network. Network design consists of CISCO 3745 Routers and CISCO Ether Switch Routers. Additionally two autonomous systems AS10 and AS100 are configured. The routing protocols are required to enable network services. The EIGRP protocol is used as an interior routing protocol and BGP is used for exterior routing. Main machine and virtual machines are connected to network topology designed on GNS-3 simulator using a cloud

and a loopback network adaptor. These machines are under the same administration (AS10). The network communication among main machine and other virtual machines has been established after the implementation. Routers and switches are the RADIUS and TACACS + clients in this experimental environment

### *4.3.1 RADIUS Configuration on CISCO Router*

Figure 4 shows the complex network design for RADIUS simulation. It includes multiple administrative authority, Virtual local area network (VLANs), Virtual private networks (VPNs) and Cisco routers and switches that are RADIUS clients. Before configuring RADIUS, it is assumed that Router is pre-configured for IP Addresses and Routing. Configuration commands to enable AAA Service and RADIUS are listed here.

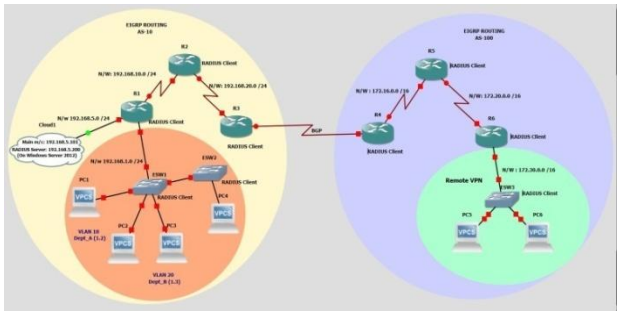

**Figure 4: RADIUS Simulation**

Router> enable

Router# configuration terminal

Router(config)# aaa new-model

Router(config)# aaa group server radius script

Router(config-sg-radius)# server-private 192.168.5.200 key password

Router(config-sg-radius)# exit

Router(config)# aaa authentication login default group scsit

Router(config)# aaa authorization exec default group scsit

Router(config)# line vty 0 4

Router(config-line)# transport input telnet ssh

Router(config-line)# login authentication default

***Note:*** Here "scsit" is a radius group name, "192.168.5.200" is server IP and "password" is a secrete key.

### *4.3.2. TACACS+ Configuration on CISCO Router*

Figure 5 shows the complex network design for TACACS+ simulation. The similar assumption is made as previously defined during the TACACS+ configuration. Configuration commands to enable AAA service and TACACS + are as follows:

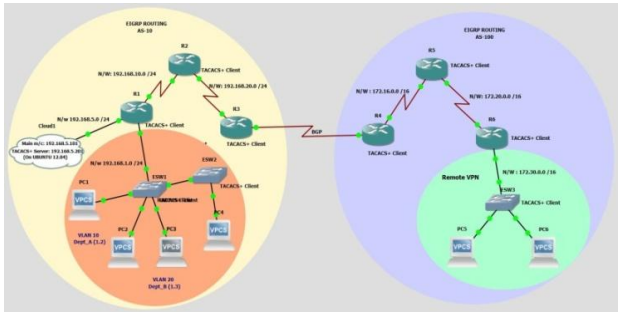

**Figure 5: TACACS + simulation**

Router> enable

Router# configuration terminal

Router(config)#tacacs-server host 192.168.5.201

Router(config)#tacacs-server key testing123

Router(config)# aaa new-model

Router(config)# aaa authentication login default group tacacs+ local none

Router(config)# aaa authorization exec default group tacacs+ local none

Router(config)# aaa authorization commands 0 default group tacacs+ local none

Router(config)# aaa authorization commands 15 default group tacacs+ local none

Router(config)# aaa accounting exec default start-stop group tacacs+

Router(config)# aaa accounting commands 0 default start-stop group tacacs+

Router(config)# aaa accounting commands 15 default start-stop group tacacs+

**Note:** Here "192.168.5.201" is TACACS+ server IP and "testing123" is a super secrete key.

## 5. COMPARISION OF RADIUS AND TACACS+

RADIUS was intended to verify, validate and log dial-up remote users to access a network, and TACACS+ is used most commonly for administrator access to network elements such as routers, switches, firewall, and servers. The names of the protocol also indicate the same. RADIUS stands for Remote Access Dial-In User Service, and TACACS+ stands for Terminal Access Controller Access Control Service Plus.

The principal operational difference between RADIUS and TACACS+ is that the Authorization process is separate from authentication process in TACACS+, whereas RADIUS combines both Authentication and Authorization. Though this may seem like a small detail, it makes a world of difference when implementing administrator AAA in a network environment.

Since the RADIUS does not separate out authentication and authorization functionality, it can include privilege information in the authentication reply; however, it can only provide the privilege level, which reveals different things to different vendors. Since there is no standard between vendor implementations of RADIUS authorization, each vendor's attributes often conflict, resulting in inconsistent results. Regardless of the possibility that the information was consistent, the administrator would still need to manage the privilege level for commands on each device. This will quickly become unmanageable.

RADIUS accounting does not log the commands issued by the administrator. It only logs the start, stop, and interim records of that session. This signifies that if two or more administrators logged in simultaneously, there is no way to determine which administrator issued which commands.

TACACS+ is a standard protocol developed by the U.S. Department of Defense and has been reengineered over the years by Cisco Systems. Authentication and authorization functions are separate in TACACS+ protocol, so it enables additional flexibility and granular access controls on who can execute which commands on specified devices. Every single command issued by a user is first sent to the central TACACS+

server. The server checks the command against an accredited list of commands for that user or group. TACACS+ can define policies based on user, device type, location, or time of day. The TACACS+ can use local users or groups configured in Active Directory or LDAP to control access to devices in the network. This provides Single Sign-On capability, which increases security, simplifies management, and makes it easier for users.

RADIUS permits use of same shared secretes by multiple users. All clients of the same RADIUS group holds the same shared secrete that can be treated as a single client. It is vulnerable to attacks. However, TACACS+ permits each client to have its own secrete key which enables protection against attacks.

RADIUS is inadequate for heterogeneous network and administrator AAA. It can still be used for the administrator but only if there is a homogeneous network environment or authorization and accounting is not required. RADIUS is basically developed for subscriber AAA. If AAA server required deploying in a heterogeneous network environment or accounting and authorization policies are required for network devices, TACACS+ is the best option. TACACS + is specially designed for administrator AAA. Table 1 shows the differences between the two protocols.

**Table 1: RADIUS vs. TACACS+**

| S.N | RADIUS | TACACS + |
|---|---|---|
| 1 | Less secure – only runs an MD5 hash on the password in access request packet. | More secure - Encrypts the entire packet including username, password, and other attributes. |
| 2 | Combines authentication and authorization | Separates all 3 elements of AAA, making it more flexible |
| 3 | No command authorization | Command authorization |
| 4 | Authorization on per group basis | Authorization on per user and per group basis |
| 5 | Requires each network device to contain authorization configuration | Central management for authorization configuration |
| 6 | No command accounting | Full command accounting |
| 7 | No multiprotocol support | Offers multiprotocol support |
| 8 | Uses same shared secret for many clients. | Each client has its own secrete key |
| 9 | UDP- Connectionless UDP ports 1645/1646, 1812/1813 | TCP- Connection oriented TCP port 49 |
| 10 | Minimal vendor support for authorization | Supported by most major vendors |

# 6. CONCLUSION

The RADIUS and TACACS+ protocols are studied for their experimental utilization and the application level analysis. In the investigation it is found that both the protocols help to deploy the AAA model of security. For deploying the secure and effective security, the TACACS+ is much effective then the RADIUS protocol. Additionally, TACACS+ is worldwide acceptable for different secure server installation. The key highlights of the proposed analysis are described as:

- TACACS+ should be deployed in a fully-trusted, internal network to increase security and simplify management.
- TACACS+ permits to set access policies by user, device, location, or time of the day
- TACACS+ includes per-command authorization and accounting.
- RADIUS uses the same shared secrete for many clients which make it vulnerable to attacks.

Both the protocols are effective and acceptable for different applications and their utilities. But still some limitations exist in both the AAA models. In near future, the work will be extended to discover the facts and the techniques that help to overcome the limitation in protocols. In addition of that, the authentication process is required to be more complicated using second authentication options, such as bio-metric systems or user attribute based authentication and authorization techniques.

# 7. REFERENCES

[1] Daniel Granlund, "Secure and Scalable Roaming Support in Heterogeneous Access Networks", Thesis, Mobile Systems Department of Computer Science and Electrical Engineering Luleå University of Technology, January 2011

[2] Hasan, A., Jahnert, J., Zander, S. and Stiller, B., "Authentication, Authorization, Accounting and Charging for the Mobile Internet" Mobile Summit (September 2001).

[3] Jiange Zhang, Yuanbo Guo, Yue Chen, Jun Ma, "Research of AAA messages Based on 802.1x Authentication", Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 19-20 Dec. 201,Chongqing, China, IEEE

[4] Jindrich Jelinek and Pavel Satrapa, Jiri Fiser, "Experimental Issues of the Model of the Enhanced RADIUS Protocol", IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM), 2015

[5] Gabriel-Cătălin Cristescu, Victor Croitoru, Vlad Sorici, "Implementing an AAA-RADIUS Solution Based on Legacy Authentication Protocols", 12th International Symposium on Electronics and Telecommunications (ISETC), 2016, Timisoara, Romania, 27-28 Oct. 2016, IEEE

[6] Nisha Bawaria, Kamlesh Namdeo, Pankaj Richhariya, "High-Performance AAA Security for Cloud Computing in Hierarchical Model", International Journal of Computer Applications (0975 – 8887) Volume 132 – No.15, December 2015

[7] Daniel Granlund, Christer Åhlund, "A Scalability Study of AAA Support in Heterogeneous Networking Environments with Global Roaming Support", 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011, 16-18 Nov. 2011, Changsha, China IEEE

[8] The Advantages of TACACS+ for Administrator Authentication, TACACS.net document, 2011, available at http://www.tacacs.net/docs/TACACS_Advantages.pdf.