International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 2 ǁ February 2023 ǁ PP. 56-63

External Server Based Authentication Using Tacacs Server

[1] A.Koteswara Rao, [2]Shaik Taj Mahaboob, [3]K.Ravindra Reddy
1 M.Tech Student, 2Assistant Professor, 3Assistant Professor (Adhoc)
akoteswararao9@gmail.com
1Electronics and Communication Engineering,
JNTUA College of Engineering Pulivendula, Andhra Pradesh, India.

Abstract: *The requirement for administering Network Access Servers (NAS) expanded along with the use of remote access. Additionally, the requirement for user and password management as well as control over per-user basis has grown to be crucial. A security protocol known as the Terminal Access Controller Access Control System (TACACS) provides centralized authority for verifying users attempting to access a router or NAS.TACACS, a new version of the protocol, was recently created to increase security by offering independent authentication, authorization, and accounting, or simply AAA, for validating and logging information about the respective users.*

Key words— *Classification, Authentication, Authorization, and Accounting (AAA), Terminal Access Controller Access Control System (TACACS), Network Access Servers (NAS), and TACACS (AAA).*

Date of Submission: 24-01-2023 Date of acceptance: 07-02-2023

I. Introduction

Considering the length and breadth of the TACACS, which by default utilizes Port 49 or UDP, is described in RFC 8907. TACACS forces a client to accept a username and password and then sends a request to the TACACS authentication server, also known as TACACSD. It will produce a response indicating whether to approve or reject an authentication request. TIP will then decide whether or not to provide access based on the response. These decision-making processes are referred to as "opened up," and the TACACSD's administrators control the data and algorithms utilized to make choices.

Extended TACACS, commonly referred to as XTACACS, uses various extra features that increase the robustness of the TACACS protocol.It separates the duties of authentication, authorisation, and accounting, even requiring that they be handled by distinct servers andtechnologies.

1.1Tacacs

The Cisco ACS server and client communicate with one another via the TACACS protocol. 49 was the TCP port number chosen for greater stability. TACACS and RADIUS servers have nearly supplanted TACACS and XTACACS in all networks. TACACS is a completely new protocol and is not compatible with those of existing protocols. Unlike RADIUS, which utilises UDP for transmission control, TACACS uses TCP. RADIUS does not have to fix transmission issues like packet loss and time-out since it employs UDP, a connection-less protocol. RADIUS encrypts user passwords, but all other user-related information, such as usernames, authorizations, and accounting, is transferred in clear text and is therefore more susceptible to security breaches. TACACS, in contrast, encrypts all user-related data, making it less susceptible to assaults.

1.2Features of TACACS

1.2.1 Full Implementation of TACACS Protocol

Any TACACS client vendor, including Cisco, Fortigate, Aruba, Juniper, Citrix, and others, is compatible with the TACACS protocol.
Additionally, TACACS authorisation and accounting characteristics of any arbitrary nature are provided.

1.2.2 Configuration based on policies

Depending on the established regulations, each request may be handled in a variety of ways. Each authentication and/or accounting request may be handled differently depending on its request attributes, sender address, and user name pattern.
With a few mouse clicks, let's say that the scenario "authenticate all requests from 192.168.1.3 against Active Directory, and utilise internal database for all other customers" is set up.

1.2.3. Interoperability
RADIUS feature databases can be expanded with vendor-specific characteristics. H323 Cisco and Quintum characteristics are supported at the server core level.

1.2.4.Built-in User Accounts Management
Using the database, you may create, change, and remove user accounts. The administration interface may be used to manage passwords, access policies, double login prevention, MAC address authentication, and limited logon hours.

1.2.5.Multiple Accounting Consumers
Accounting RADIUS data are being logged in many methods at the same time. SQL data storage, simple files, and distant RADIUS servers all work. Advanced approaches, like as data caching in MS Message Queue, improve system scalability and fault tolerance.TACACS employs central administration of AAA, which means that the data is stored in a single, secure database that is easier to maintain than scattered data across several devices. Being client-server systems, TACACS and RADIUS both enable effective exchange of AAA information.

1.2.6Authentication
Verifies the user's identity, whether they are a legitimate user, and their eligibility for accessing the network. The TACACS employs an authentication database to store user data, preventing network intrusion.

1.2.7Authorization
It specifies which resources and services must be made available to the authorised user. Controlling resources and services offered to a user via the network is possible with authorization. Additionally, the network manager has the ability to regulate the use of specific instructions. Without authentication, the next step cannot be completed.

1.2.8Accounting
It keeps time and record-keeping on the user and his network activity. This functions as a connection time and resource use audit trial or billing. Accounting may be done without following the other two processes. authentication and authorization.

2. A Comprehensive study of authentication and confidentiality for tacacs server

There may be a large number of top features for routers according to study [1], but the actual challenge is understanding when, how, and why to employ each function. Most networking issues may be resolved with Cisco equipment in a variety of methods, some of which may be more efficient than others. The main issue for a network engineer is determining which solution is most appropriate for our specific circumstance. Unfortunately, the text outlining a specific feature or command provides very little to address the queries that were raised, even after selecting a specific feature. Anyone who has used Cisco routers, regardless of how long or how briefly, has had to ask others for things like router configuration files that can demonstrate how to resolve a certain issue.

The author of article [2] researched how to identify a user in TACACS using the TELNET option. A TELNET option that was created to make it easier to prevent multiple logins is described in the section below. The target hosts are intended for TAC connections for TAC users, although any two users that are in agreement for the connection may utilise it.

The author of [3] explored public key infrastructure, access control, and authentication in networks. Access control prevents unauthorised resource viewing, destruction, or tampering. Additionally, they guarantee anonymity, privacy, and the absence of illegal disclosure. Access control, authentication, and public key infrastructure explains the elements of access control, provides a framework for their implementation, and examines legal issues that impact control systems. It has been revisited and updated with the knowledge from this field. It scans information systems and IT infrastructures for threats, weaknesses, and dangers and considers how to handle them.

The author of [4] suggests the TACACS access control scheme. TACACS assigns a username and password before sending a message to the TACACSD or TACACS Daemon authentication server. TACACSD responds with a decision on whether to accept or reject the authentication request. The TIP will then decide whether to grant access or not based on the reply. In this approach, the process of decision-making is "opened up," and the person in charge of the TACACS has control over the algorithms and information that are utilised to make judgments.

This research [5] studied about TACACS and RADIUS server. TACACS is more reliable than RADIUS since it uses TCP. In contrast to RADIUS, which does not provide external authorisation of commands, TACACS offers more control over the instructions that are used to authorise. TACACS is more secure since every packet is encrypted, as opposed to RADIUS, which just encrypts passwords.

S.no	Author Name	Title	Method

1.	V. Ravi	Formal ways to validate authentication in TACACS+ protocol	Commercial routers used TACACS+ and RADIUS protocols to support the AAA services
2.	R. Pradeep	Formal Verification of Authentication and Confidentiality for TACACS+ Security Protocol Using Scyther	AAA services officially validate by using TACACS which is confirmed by Scyther tool
3.	T. Dahm	The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol	TACACS protocol is used to wireless devices with centralised servers
4.	Gabriel	AAA-RADIUS Solution Implementation Based on Legacy Authentication Protocols	AAA-RADIUS system is implemented using the Alcatel-Lucent 8950 AAA software
5.	Toni Janevskil	Integrated AAA System for PLMN-WLAN Interworking	The WLAN Gateway handles the WLAN service with the help of AAA services
6.	Zhang Jiange	Research of AAA messages Based on 802.1x Authentication	Analyses of EAP and RADIUS with AAA mechanism

3. Methodology

The TACACS client is referred to as Network Access Device (NAD) or Network Access Server in this implementation (NAS). The NAS will communicate with the TACACS server through a CONTINUE message to acquire a username prompt. After the user inputs their username and the NAS contacts the TACACS server once more to acquire a password prompt and continue message for the user to see, the password entry is delivered to the TACACS server. TACACS utilises TCP for transportation. The TACACS server port 49 is designated to handle traffic. The article makes extensive use of the session. In the TACACS server, a session is any individual authentication process, authorization exchange, or accounting exchange. An arbitrary number of packets are traded during an authentication session. The term "session" refers to a functional concept that is maintained between the TACACS client and server and is not always associated with a specific user or their actions.

3.1Header of a TACACS packet

The TACACS ID is a 12-byte header that is included in all TACACS transmissions. This header is always transmitted in plain text is shown in figure 3.1

Figure 3.1 TACACS Header Format

3.1.1TACACS Packet Body

The packet header contains a definition of the various TACACS body types. The remainder will discuss the TACACS body types' contents. Any variable-length data fields that aren't in use MUST have a length value of zero. If the credentials entered are genuine, the server can react with reply messages; if not, it can reply with a REJECT message. The link responds with an ERROR message if it isn't functioning properly. When in accounting mode, the client will send the server a REQUEST message, and the server will reply with a response message confirming receipt of the record.

3.1.2Encryption

The body of the packet could be encrypted. The encryption method that is allowed in order to enable "The Draft's" backwards compatibility Both the client and the server are aware of the secret key that powers the encryption key mechanism.

3.1.3 Encoding Text

With the exception of some particular restrictions for user and data fields used for passwords, all text that appears in TACACS should be ASCII-US.

3.1.4 Packet body for START authentication

The action for doing authentication is shown in the authentication start packet body. All values are legal values. Assorted authentication methods include ASCII, PAP, and CHAP.

3.1.5 Body of the authentication reply packet

Current status of the authentication is provided. Additionally, only legal values are used. FAIL, GETDATA, GETUSER, GETPASS, RESTART, ERROR, and FOLLOW are among the several statuses is shown in figure 1.

3.1.6 CONTINUE Authentication Packet Body
As a response to the server msg with a REPLY packet, the user typed this or the client gave it for the user. The bit-mapped flags that affect the action are contained in it, fig 3.1.7

3.1.7 Abandoning a session of authentication
The ABORT flag in the CONTINUE message can be used by the client to end a session. When the flag is set, a section of the message's payload may include an ASCII explanation for terminating the session. A no REPLY message is issued and the session is ended**.**

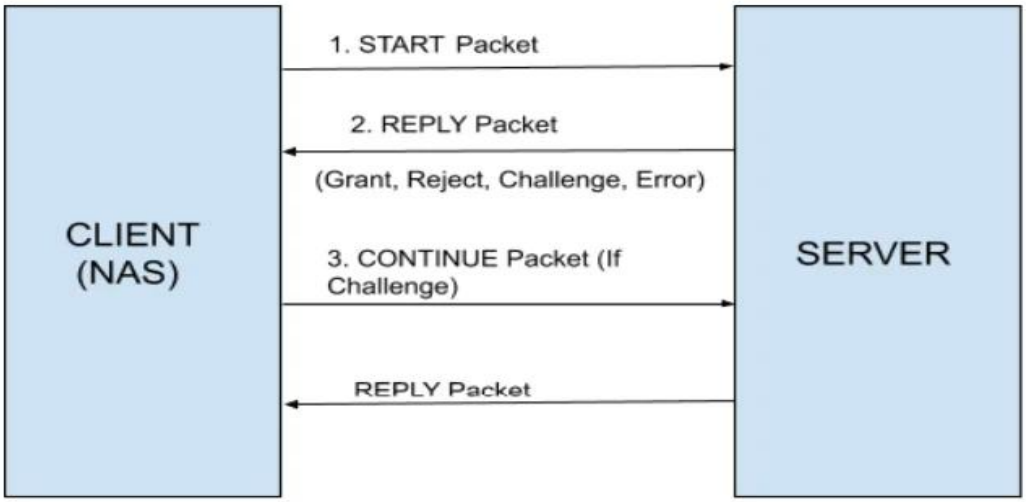


Fig 3.1.7:Authentication Flow

3.1.8 Authorization
A REQUEST and a RESPONSE are the two messages that make up the authorisation session. The REQUEST message includes a collection of variable parameters that describe the options and services of authorization that will be offered, as well as a fixed field that indicates how the user was processed or authenticated is shown in fig 3.1.8

3.1.9 Request for Authorization Packet Body
This demonstrates how the user's information will be obtained by the client using an authentication technique. Some of the components utilized by the authentication mechanism of the authorization request packet body include NOTSET, NONE, and KRB5. A client's local user database is referred to as LOCAL. Guest login with ARAP is not the same as guest authentication.

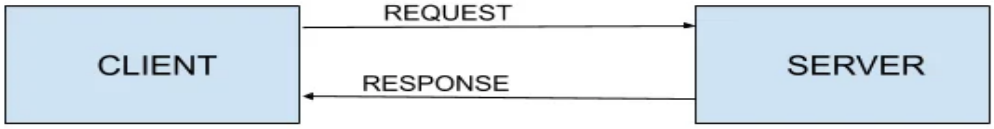


Fig 3.1.8:Authorization Flow

3.1.10 Accounting
The accounting TACACS technique for authorisation is identical, as is the format of the packet, which has a fixed and extensible section. The extensible portion employs the same value-pairs of characteristics as the fixed portion and even adds some more. Bit-mapped flags like FLAG START, FLAG STOP, and FLAG WATCHDOG are included in this, fig 3.1.10

3.1.11Accounting PACKAGE BODY
The accounting message's response informs the user that the server's accounting function has been finished. Only after the record has reached the necessary levels of relieving and security will the server's response be marked as successful. This can be set to SUCCESS, ERROR, or FOLLOW is shown in fig 3.1.10

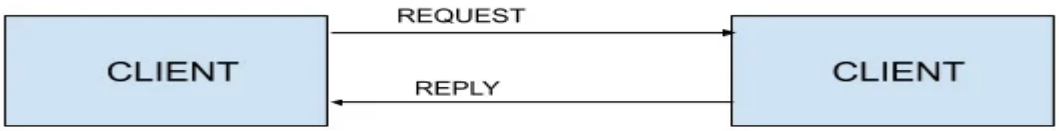


Fig 3.1.10:Accounting Flow

3.1.12 Pairs of Attribute-Value

TACACS is designed to be an expandable protocol. There are several qualities for typical use cases for authorization and accounting that customers should be required to utilise when offering assistance for the corresponding use cases. These attributes are not fixed. All of the Boolean characteristics were encoded with "True" or "False," respectively.

3.1.13 Attributes of Authorization

This key objective is to offer service and describe service characteristics that indicate whether a request is for authorisation or accounting. Current examples of this variable's values are "slip," "tty-server," "connection," "shell," "ppp," "system," and "firewall." This attribute should always be included. A protocol's subset is a service. PPP NCP is an example, with the current values for "lcp," "http," "login," and "unknown" and Cmd.

3.1.14 Accounting Characteristics

These characteristics are unique to TACACS accounting. These come before any properties of permission section when they are listed among the arguments. Start and stop values for the same event should match task ID, for example. Until it sends a stop record, the client is not permitted to reuse a task ID is shown in fig: 3.1.14.

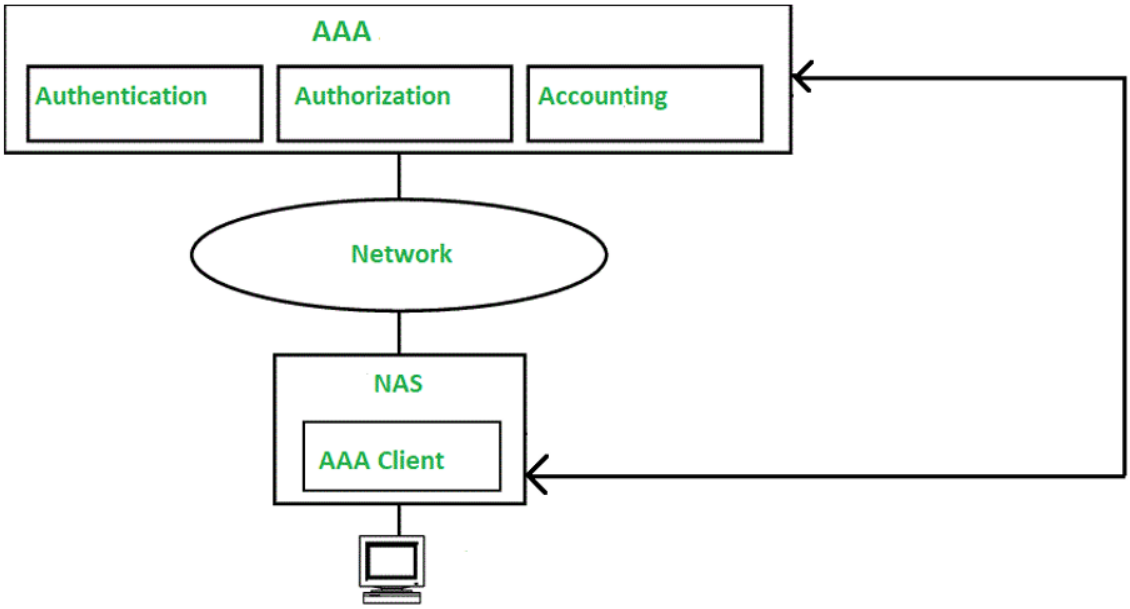


Fig3.1.14: Flow chart of AAA Authentication

3.1.15 Priority Levels

TACACS uses systems of extendable characteristics to enable greater authorization. Privilege levels is a scheme built on the protocol. Privilege levels are values from 0 to 15 that, in sequence, reflect the degree of privilege that is a superset of the level below it.

4 Results and discussion

The below figures are the experimental outputs Is shown in fig: 4

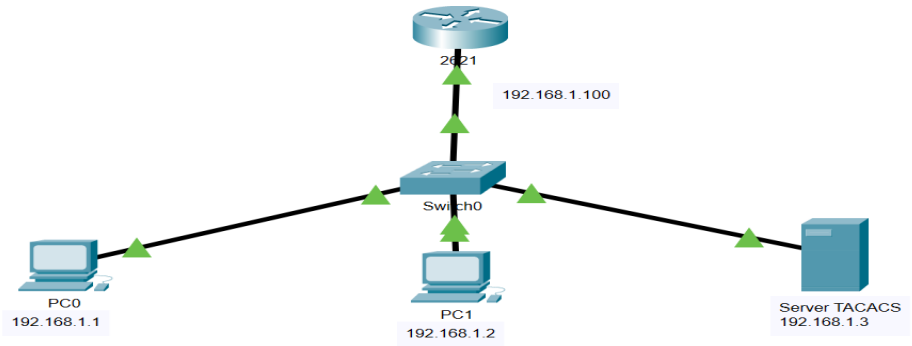


Fig4: With TACACS server

Login using Router with user1

```
User Access Verification

Username:
Username: admin
Password:
% Login invalid

Username: user1
Password:
Router>
```

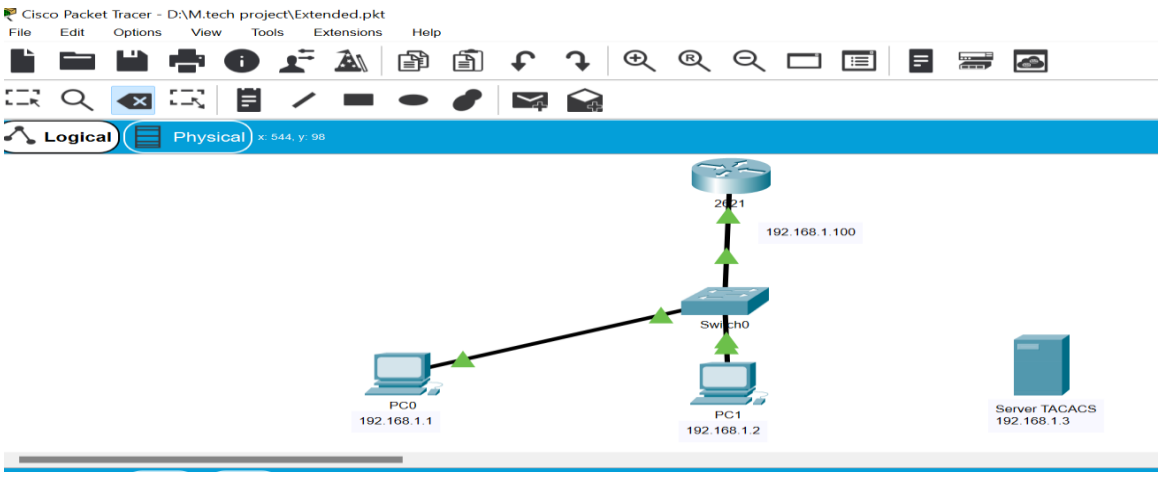
Login using Router with user2

```
User Access Verification

Username:
Username:
Username: user2
Password:
Router>
```

4.1 If Tacacs server failure

Proper configuration of a Cisco router will allow it to local authentication if the connection to TACACS fails. However, a situation can occur where the connection fails after the user is successfully authenticated. This may prevent the user from performing basic commands such as logout. To account for this situation, modify the aaa statements in the config of your Cisco router.



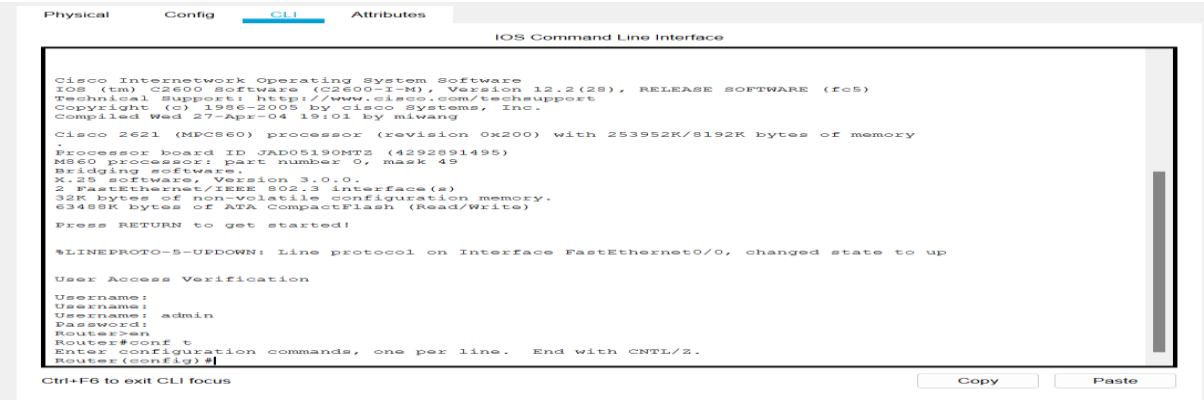


Fig 4.1: Without TACACS server.

With TACACS server is shown in fig: 4

Login mode	TACACS
User name for PC0	user1
Password for PC0	user1
User name for PC1	user2
Password for PC1	user2

Without TACACS server is shown in fig: 4.1

Login mode	Router
User name	admin
Password	cisco

5. Advantages, Disadvantages and applications

Advantages:

1. TACACS uses authentication and progressive recording function with pass-words in run-time.
2. Transmission control protocol is employed, in addition with AAA for better performance.
3. It supports Kerberos secret key authentication.
4. All the packets in AAA are encrypted, while only passwords are encrypted in other servers.
5. It uses AAA which is more secure for authorizing users.
6. AAA will maintain accounting of details of the users like time and date, making even more robust compared to other servers.

Disadvantages:

It is an open standard server.

1. Not accepts pass-words prompt while changing of password or during the in-process tokens of pass-word.
2. It uses both TCP and UDP.
3. It uses port number 49.

Applications:

1. Network devices like switches and router are accessed for admin,
2. Networks where authorization requires,
3. Authenticating networks,
4. Networks where centralized validation requires.

6. Conclusion

We have implemented the TACACS server in packet tracer, we obtained a better result than the existing systems. We analyzed the AAA performance, with TACACS server. We can finally conclude that TACACS is best when it comes security because it uses Authentication, Authorization and Accounting (AAA) for even more robust security than the existing RADIUS server.

The TACACS server was incorporated in Cisco Packet Tracer, and the results were superior to those of the previous systems. Using the TACACS server, we examined the AAA performance. Finally, we can state that TACACS employs Authentication, Authorization, and Accounting (AAA) for even stronger protection, making it the greatest security option available.

TACACS is currently one of the best server protocols, but TACACS can be implemented with multiple protocols other than internet protocols (IPs). In further implementations TACACS can be implemented on multiple protocols and can yield better same results.

Reference

[1]. Kevin Dooley and Ian Brown (2003). Cookbook for Cisco. Page 137 of O'Reilly Media. ISBN 9781449390952. Archived on 2016-06-24 from the original.

[2]. Brian Anderson (December 1984). Telnet option for "TACACS User Identification". Task Force for Internet Engineering. On August 12, 2014, the original version was archived. obtained on February 22, 2014.

[3]. Bill Ballad, Tricia Ballad, and Erin Banks (2011). Access Control, Authentication, and Public Key Infrastructure. Pages 278–280 in Jones & Bartlett Learning. ISBN 9780763791285.Finest, Craig

[4]. (July 1993). "An Access Control Protocol, Occasionally Known as TACACS." Task Force for Internet Engineering. On February 22, 2014, the original version was archived. obtained on February 22, 2014.

[5]. "TACACS and RADIUS Comparison," page 5. 14 January 2008. Cisco. On September 7, 2014, the original version was archived. Obtainable as of September 9, 2014.

[6]. "Formal ways to validate authentication in TACACS+ protocol" by Ravi V, Dr. Sunitha N. R, and Pradeep R

[7]. Formal Verification of Authentication and Confidentiality for TACACS Security Protocol Using Scyther by Pradeep R, Sunitha N.R, and Ravi V IEEE - 45670

[8]. Ota, T. Dahm Medway, D.C. The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol, Gash D. Carrel L. Grant, RFC 8907.

[9]. Victor CROITORU and Gabriel-Cătălin CRISTESCU "AAA-RADIUS Solution Implementation Based on Legacy Authentication Protocols" 978-1-5090-3748-3/16/$31.00 ©2016 IEEE

[10]. Aleksandar Tudzarov, Toni Janevski, Meri Janevska, PervojeStojanovski, DuskoTemkov, GoceStojanov, DuskoKantardziev, Mine Pavlovski, and Tome Bogdanov Serbia and Montenegro, Nis, September 28–30, 2005, "Integrated AAA System for PLMN-WLAN Interworking"

[11]. "Research of AAA messages Based on 802.1x Authentication" by Jiange Zhang, Yuanbo Guo, Yue Chen, and Jun Ma. 978-1-47--/1/$31.00 201IEEE

[12]. Feng Jian, "Design and Implementation of RADIUS Client Based on Finite State Machine," Pacific-Asia Conference on Circuits, Communications and System, July 2009, pp. 3-4.

[13]. International Conference on Computer Application and System Modeling (ICCASM 2010), pp. 1-2, October 2010. X. Chen and J. Hu, "Design and Implementation of VoIP Prepaid Service Based on RADIUS."

[14]. Ravi.V, Dr. Sunitha N.R, Pradeep.R "Formal methods to verify authentication in" 10.1109/ICECIT.2017.8453431.

[15]. http://info.internet.isi.edu/in-notes/rfc/files/rfc927.txt.

[16]. https://www.cisco.com/c/en/us/support/docs/security-vpn/remoteauthentication-dial-user-service-radius/13838-10.html