SERVER BASED AUTHENTICATION USING TACACS SERVER

A. Koteswara Rao, PG Scholar,Department of Electronics and Communication Engineering JNTUA College of Engineering Pulivendula, Andhra Pradesh, India. Email: akoteswararao9@gmail.com
K. Ravindra Reddy, Assistant Professor Department of Electronics and Communication Engineering JNTUA College of Engineering Pulivendula, Andhra Pradesh, India
Shaik Taj Mahaboob, Assistant Professor Department of Electronics and Communication Engineering JNTUA College of Engineering Pulivendula, Andhra Pradesh, India

Abstract: As the use of remote access has expanded, so too has the need for Network Access Servers (NAS). In addition to managing user access and passwords, it is now crucial to be able to control access on a per-user basis. A security protocol known as the (TACACS) provides centralized authority for verifying users set to access a router. TACACS, is a advanced 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. This new protocol offers a more secure way of managing access to devices on a network, providing an extra layer of security for your data.

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

1. Introduction

A TACACS server is an authentication server used in networking. It is a part of the Remote Authentication Dial-In User Service (RADIUS) protocol. The TACACS server is the key to controlling access to a network. It can be used in multiple ways, but the most preffered use is to authorize users before they are permit entry to the network. This allows administrators to keep track of who is accessing the network and what they are doing. The 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 that are utilized to make choices. This allows for a top level of flexibility and security for TACACSD.
XTACACS is a more robust form of TACACS that uses separate servers for authentication, authorisation, and accounting. This makes the protocol more reliable and efficient.

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

The best routers for your business may not be the most popular ones on the market. According to a recent study, [1] there are a number of top features for routers, 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. Network engineers have to constantly determine the best solution for their 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.

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 [11]

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 [12]
3.	T. Dahm	(TACACS+) Protocol	TACACS protocol is used to wireless devices with centralised servers [13]
4.	Gabriel	AAA-RADIUS Solution Implementation Based on Legacy Authentication Protocols	AAA-RADIUS system is implemented using the Alcatel-Lucent 8950 AAA software [14]
5.	Toni Janevskil	Integrated AAA System for PLMN-WLAN Interworking	The WLAN Gateway handles the WLAN service with the help of AAA services [15]
6.	Zhang Jiange	Research of AAA messages Based on 802.1x Authentication	Analyses of EAP and RADIUS with AAA mechanism [16]

Table 2.1: Comprehensive study and Review table for tacacs server

The author of article [2] How to identify a user in TACACS using the TELNET option A TELNET option has been created to make it easier to identify users in TACACS. 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 article [3] Public key infrastructure is a secure way to exchange information over an insecure network. The public key cryptography system is a way to encrypt and decrypt data using 2keys- a private key and a public key, the private key must be kept confidential and the public key can be split with anyone. This system is very secure, as even if someone obtains the public key, they cannot decrypt the data without the private key. Access control prevents unauthorised resource viewing, destruction, or tampering. Additionally, they guarantee anonymity, privacy, and the absence of illegal disclosure. An in-depth exploration of access control, authentication, and public key infrastructure, this guide has been updated with the latest knowledge from the field. It covers how to scan information systems and IT infrastructures for threats, weaknesses, and dangers, and provides guidance on 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 either to accept or reject the request for authentication. If your authentication is successful, you will be granted access to the requested resource. The TIP will then decide whether to allow access or not based on the reply. In this approach, the action of controlling is "opened up," and the person in charge of the TACACS has control over the data and information that are utilised to make judgments.

This research [5] studied about the reliability of TACACS and RADIUS servers. TACACS was found to be more reliable than RADIUS, as 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 was also found to be more secure, as every packet is encrypted, whereas RADIUS just encrypts passwords.

- NAS, Tacacs Process and Tacacs host are frequently used and described in below table 2.2, in this paper

Term	**Description**
NAS	The E Series router is a network access server that provides connections to a single user, to a network or subnetwork, and to interconnected networks.

	In reference to TACACS, the NAS is the device that provides authentication and authorization services.
TACACS Process	TACACS is a security server program that provides AAA services using the TACACS protocol. This program processes authentication, authorization, and accounting requests from users and systems to provide secure access to network resources. It is widely used by organizations to protect their networks from unauthorized users or malicious activities.
TACACS Host	The security server on which the TACACS process is running is also known as a TACACS server. This server is responsible for authorizing users and providing authentication. Without this server, your network would be at risk for unauthorized access.

Table 2.2: Above terms are used frequently in this chapter.

3. Methodology

The protocol that TACACS employs is all that this paper is capable of describing.

- Client

A client is the one who provides connectivity for services, it is just a device. Clients normally provide a graphical user interface for character mode and allow users to login or telnet to some other host. Clients can sometimes support access services of different protocols.

- Server

Server receives request of a certain protocol, and responds accordingly by using the model of algorithm configured in the document.

- packet

All use the packet of words for this document referring to packets of protocol if not mentioned explicitly.

Here is a workflow that illustrates the AAA authentication process

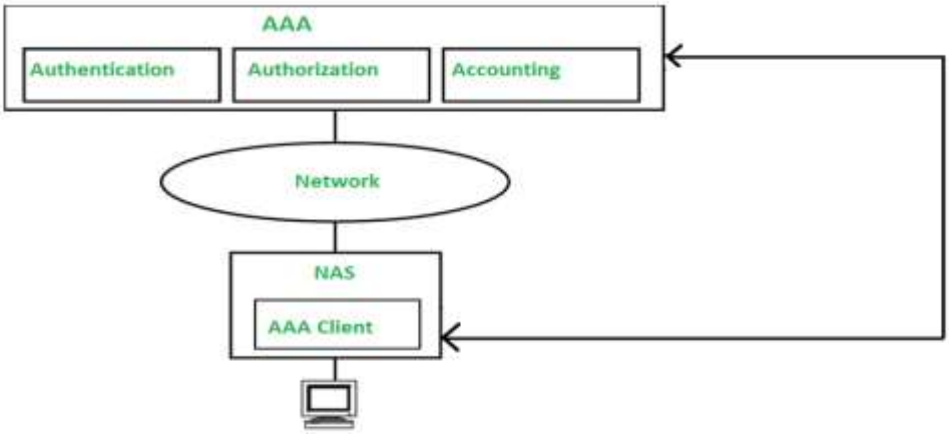

Fig 2.3: Structural flow of AAA

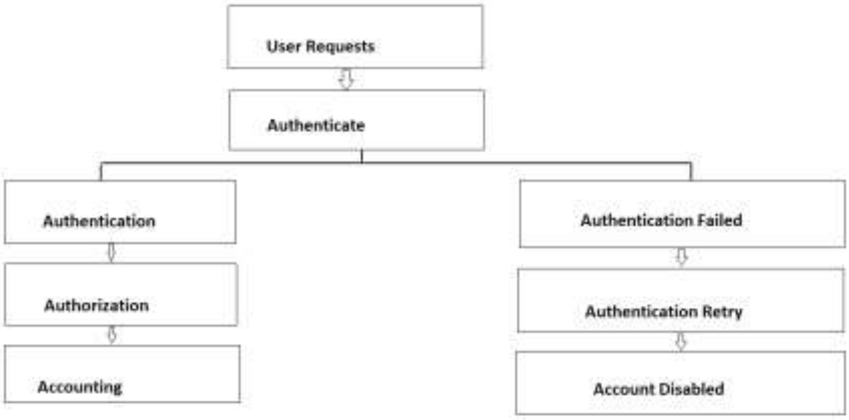

Fig 3: AAA authentication flow chart

3.1 User Requests: The process of gaining access to a network resource begins when a user requests access. This can be done in a variety of ways, such as through a web browser or an application. Once the request is made, the network resource will determine whether or not to grant access. If the request is approved, the user can able to allow the resource.

3.2 Authenticate: The authentication process begins when the network device requests the user's login credentials. The device then sends the login credentials to a centralized authentication server, such as a TACACS server, for verification is shown in fig:4

3.3 Authentication: The authentication server verifies the user's login credentials and sends a response back to the network device, indicating whether the login was successful or not.

3.4 Authorization: If the user's login was successful, the network device requests authorization from the authentication server to determine the user's level of access to the requested resource. The authorization server then checks the user's permissions and sends a response back to the network device, indicating the level of access that the user has.

3.5Accounting: Once the user has been authenticated and authorized, the network device logs all activities performed by the user on the network. This helps to maintain a record of all user activities on the network, which can be used for auditing, compliance, and troubleshooting purposes.

3.6 Authentication Failed: If the user's login credentials are not valid, the authentication server sends acknowledge back to the network device reflets that the login failed. The user will then need to provide valid credentials to try again. The user is then prompted to enter their login credentials again.

3.7 Authentication Retry: If the user's login credentials are not valid, the network device may prompt the user to try again or provide additional authentication information, such as a token or a biometric identifier.

3.8 Account Disabled: If the user's account has been disabled, the authentication server will response back to network device indicating that the account is disabled, and the user will not able to approach the resource network.

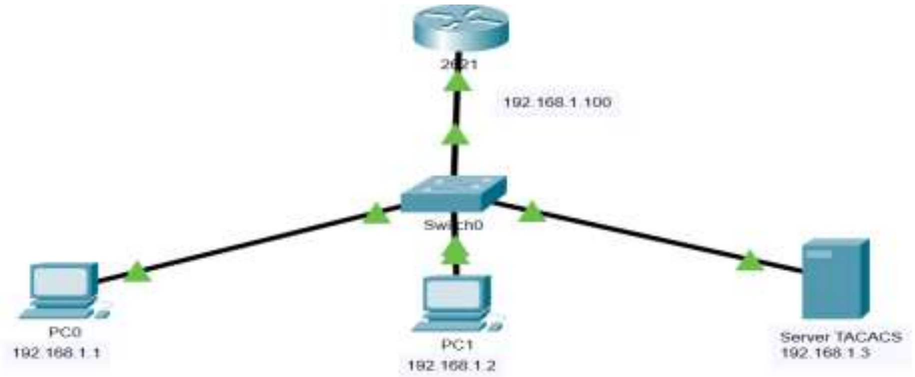

Fig 4 : Server based authentication using with TACACS server

3.9 If TACACS server failure

If a Cisco router is properly configured, it can perform local authentication if the connection to TACACS fails. However, there may be a situation where the connection fails after the user successfully authenticates. This may prevent the user from performing basic commands such as logging out. To address this situation, modify the aaa statements in your Cisco router configuration is shown in fig 5.

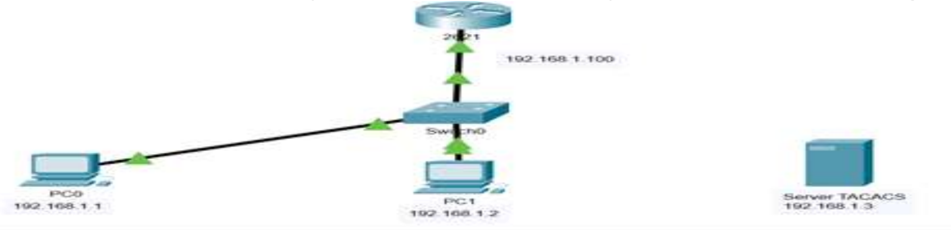

Fig 5 : Server based authentication using without TACACS server

Summary of Accounting Packets

In the context of TACACS, accounting mention the process of tracking and logging user activity on a network, such as logins, logouts, and system configuration changes. When accounting is enabled, TACACS servers receive accounting packets from network devices, which contain information about user activity.

Here is a summary of accounting packets in TACACS:

Start Packet: The start packet will sent by a network device to the TACACS server when a user begins a new session or starts a new activity, such as logging in or configuring a network device. The start packet includes information about the user's identity, the device they are using, and the type of activity they are performing.

Stop Packet: The stop packet can able to sent by a network device to the TACACS server when a user ends a session or completes an activity. The stop packet includes information about the duration of the session or activity, the amount of data transferred, and any errors that occurred during the session.

Interim Packet: The interim packet sent to the TACACS server periodically during a user's session or activity. The interim packet includes information about the user's activity, such as data transferred.

Watchdog Packet: The watchdog packet is sent by the TACACS server to a network device to verify that the device is still active and responsive. If the network device fails to respond to the watchdog packet, the TACACS server assumes that the device is offline and terminates the user's session.

The accounting packets are essential for monitoring and auditing user activity on a network and can be used for troubleshooting and security purposes. By analyzing accounting data, network administrators can detect and prevent unauthorized access, identify security threats, and optimize network performance.

List of Protocols With statistical value	OSPF statistical value	STATIC statistical value	RIP statistical value	With TACACS by using AAA Process	Without TACACS statistical value
Source	Router	Router	Server	Router	Pc
Destination	PC	PC	PC	Pc	Router
Min time taken to delivery	12ms	10ms	14ms	0ms	0ms
Max time taken to delivery	18ms	18ms	16ms	2ms	1ms
Average Time taken to delivery	30ms	28ms	30ms	2ms	1ms
Packet loss	0 loss	0 loss	0 loss	0 loss	0 Loss

Fig 3.2: Statistical values for Tacacs server

TACACS is a protocol used for centralized (AAA) services in computer networks. It was originally developed by Cisco Systems, but is now an open standard.

Advantages of TACACS:

- Enhanced security: TACACS uses a separate authentication and authorization process, which increases security compared to other protocols like RADIUS.
- Granular access control: TACACS provides granular access control, allowing administrators to specify which commands or actions a user can perform.
- Centralized management: TACACS allows centralized management of user accounts, providing a single point of administration for network access.
- Detailed accounting: TACACS provides detailed accounting of user activity, including authentication attempts, command usage, and system events.
- Customizable: TACACS allows for customizable authentication and authorization policies based on specific user roles, locations, and other criteria.

Disadvantages of TACACS:

- Complexity: TACACS can be complex to configure and maintain, requiring specialized knowledge and expertise.
- Cost: TACACS solutions may require expensive hardware and software, making it less cost-effective than other authentication protocols.
- Network latency: TACACS may introduce network latency, which can impact the performance of network applications.

Applications of TACACS:

- Network security: TACACS is commonly used to provide secure authentication and authorization for network devices, such as firewalls, switches and routers.
- Access control: TACACS used to control access to sensitive information and resources, such as financial data or confidential documents.
- Compliance: TACACS provides detailed accounting information, which can be used for compliance and auditing purposes, such as tracking changes made to network configurations.

- Identity management: TACACS can be used in conjunction with identity management systems, such as Active Directory or LDAP, to provide a more centralized management of user accounts and access control policies. This allows for a more streamlined process when it comes to granting and revoking access to systems and applications.

Challenges of TACACS:

TACACS is a protocol used to authenticate and authorize network users. While TACACS provides several advantages over other authentication protocols, it also poses some challenges. Here are some of the challenges for TACACS:

Encryption: TACACS is the latest version of TACACS that uses encryption to secure communication between the TACACS server and the network device. However, the older TACACS protocol does not provide encryption, leaving authentication and authorization information vulnerable to interception and tampering.

Compatibility: TACACS is not as widely adopted as other authentication protocols, such as RADIUS (Remote Authentication Dial-In User Service). As a result, some network devices may not support TACACS, making it difficult to implement a uniform authentication solution across the network.

Scalability: As network infrastructure grows, the number of TACACS clients also increases. This can pose challenges for TACACS servers, which may not be able to handle the increased load of authentication requests.

Configuration: TACACS servers and clients require extensive configuration, which can be time-consuming and complex. This complexity can increase the likelihood of misconfiguration, leading to authentication and authorization failures.

Maintenance: TACACS servers and clients require regular maintenance to ensure they remain secure and up-to-date. This includes patching vulnerabilities, upgrading software, and monitoring logs for suspicious activity. Failing to maintain TACACS infrastructure can lead to security breaches and unauthorized access.

Overall, while TACACS provides some advantages over other authentication protocols, it also poses several challenges that network administrators must consider when implementing a TACACS solution.

Conclusion

In conclusion, TACACS is a powerful (AAA) protocol that provides enhanced security, granular access control, centralized management, detailed accounting, and customization options. It is commonly used for network security, access control, compliance, and identity management purposes. TACACS can be complex to configure and maintain, but offers a robust solution for businesses that need to tightly control access to their networks.

REFERENCES

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

[2] Anderson, Brian (December 1984). "TACACS User Identification Telnet Option". Internet Engineering Task Force. Archived from the original on 12 August 2014. Retrieved 22 February 2014.

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

[4] Finseth, Craig (July 1993). "An Access Control Protocol, Sometimes Called TACACS". Internet Engineering Task Force. Archived from the original on 22 February 2014. Retrieved 22 February 2014.

[5] "TACACS and RADIUS Comparison". Cisco. 14 January 2008. Archived from the original on 7 September 2014. Retrieved 9 September 2014.

[6] 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.

[7] 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.

[8] 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

[9] (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.

[10] "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.

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

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

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

[14] 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

[15] Aleksandar Tudzarov, Toni Janevski, Meri Janevska, Pervoje Stojanovski, Dusko Temkov, Goce Stojanov, Dusko Kantardziev, Mine Pavlovski, and Tome Bogdanov Serbia and Montenegro, Nis, September 28–30, 2005, "Integrated AAA System for PLMN-WLAN Interworking"

[16] "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

[17] 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.

[18] 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."

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

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

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