CCNA Security v2.0 Chapter 3 Exam Answers

itexamanswers.net/ccna-security-v2-0-chapter-3-exam-answers.html

February 9, 2016

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. A user complains about not being able to gain access to a network device configured with AAA. How would the network administrator determine if login access for the user account is disabled?

- **Use the show aaa local user lockout command.***
- Use the show running-configuration command.
- Use the show aaa sessions command.
- Use the show aaa user command.

The show aaa local user lockout command provides an administrator with a list of the user accounts that are locked out and unable to be used for authentication. This command also provides the date and timestamp of the lockout occurrence.

2. When a method list for AAA authentication is being configured, what is the effect of the keyword local?

- The login succeeds, even if all methods return an error.
- It uses the enable password for authentication.
- **It accepts a locally configured username, regardless of case***
- It defaults to the vty line password for authentication.

In defining AAA authentication method list, one option is to use a preconfigured local database. There are two keywords, either of which enables local authentication via the preconfigured local database. The keyword local accepts a username regardless of case, and the keyword local-case is case-sensitive for both usernames and passwords.

3. Which solution supports AAA for both RADIUS and TACACS+ servers?

- **Implement Cisco Secure Access Control System (ACS) only.***
- RADIUS and TACACS+ servers cannot be supported by a single solution.

- Implement a local database.
- Implement both a local database and Cisco Secure
- Access Control System (ACS).

Cisco Secure Access Control System (ACS) supports both TACACS+ and RADIUS servers. Local databases do not use these servers.

4. What difference exists when using Windows Server as an AAA server, rather than Cisco Secure ACS?

- Windows Server requires more Cisco IOS commands to configure.
- Windows Server only supports AAA using TACACS.
- **Windows Server uses its own Active Directory (AD) controller for authentication and authorization.***
- Windows Server cannot be used as an AAA server.

The Cisco IOS configuration is the same whether communicating with a Windows AAA server or any other RADIUS server.

5. When using 802.1X authentication, what device controls physical access to the network, based on the authentication status of the client?

- the router that is serving as the default gateway
- the authentication server
- **the switch that the client is connected to***
- the supplicant

The devices involved in the 802.1X authentication process are as follows:
The supplicant, which is the client that is requesting network access
The authenticator, which is the switch that the client is connecting and that is actually controlling physical network access
The authentication server, which performs the actual authentication

6. Because of implemented security controls, a user can only access a server with FTP. Which AAA component accomplishes this?

- accounting
- accessibility
- auditing
- **authorization***
- authentication

One of the components in AAA is authorization. After a user is authenticated through AAA, authorization services determine which resources the user can access and which operations the user is allowed to perform.

7. Why is authentication with AAA preferred over a local database method?

- **It provides a fallback authentication method if the administrator forgets the username or password.***
- It uses less network bandwidth.
- It specifies a different password for each line or port.
- It requires a login and password combination on the console, vty lines, and aux ports.

The local database method of authentication does not provide a fallback authentication method if an administrator forgets the username or password. Password recovery will be the only option. When authentication with AAA is used, a fallback method can be configured to allow an administrator to use one of many possible backup authentication methods.

8. What is a characteristic of TACACS+?

- TACACS+ uses UDP port 1645 or 1812 for authentication, and UDP port 1646 or 1813 for accounting.
- TACACS+ is backward compatible with TACACS and XTACACS.
- TACACS+ is an open IETF standard.
- **TACACS+ provides authorization of router commands on a per-user or per-group basis.***

The TACACS+ protocol provides flexibility in AAA services. For example, using TACACS+, administrators can select authorization policies to be applied on a per-user or per-group basis.

9. Refer to the exhibit. Router R1 has been configured as shown, with the resulting log message. On the basis of the information that is presented, which two statements describe the result of AAA authentication operation? (Choose two.)

```
R1(config)# enable algorithm-type scrypt
R1(config)# enable secret 9 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
R1(config)# username Admin algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case enable
R1(config)# aaa local authentication attempts max-fail 1
R1(config)# exit
R1#
Apr 26 22:37:32.259: %SYS-5-CONFIG_I: Configured from console by Admin on console
R1#
Apr 26 22:44:05.971: %AAA-5-USER_LOCKED: User Admin locked out on authentication
failure
R1#
```


- **The locked-out user stays locked out until the clear aaa local user lockout username Admin command is issued.***

- The locked-out user stays locked out until the interface is shut down then re-enabled.
- The locked-out user is locked out for 10 minutes by default.
- The locked-out user should have used the username admin and password StrongPa55word.
- **The locked-out user failed authentication.***

The aaa local authentication attempts max-fail command secures AAA user accounts by locking out accounts that have too many failed attempts. After the condition is reached, the user account is locked. The user account in effect stays locked out until the status is cleared by an administrator.

10. A user complains about being locked out of a device after too many unsuccessful AAA login attempts. What could be used by the network administrator to provide a secure authentication access method without locking a user out of a device?

- **Use the login delay command for authentication attempts.***
- Use the login local command for authenticating user access.
- Use the aaa local authentication attempts max-fail global configuration mode command with a higher number of acceptable failures.
- Use the none keyword when configuring the authentication method list.

The login delay command introduces a delay between failed login attempts without locking the account. This provides a user with unlimited attempts at accessing a device without causing the user account to become locked and thus requiring administrator intervention.

11. Which debug command is used to focus on the status of a TCP connection when using TACACS+ for authentication?

- **debug tacacs events***
- debug tacacs
- debug tacacs accounting
- debug aaa authentication

The debug tacacs events command displays the opening and closing of a TCP connection to a TACACS+ server, the bytes that are read and written over the connection, and the TCP status of the connection.

12. Which characteristic is an important aspect of authorization in an AAA-enabled network device?

- The authorization feature enhances network performance.
- **User access is restricted to certain services.***
- User actions are recorded for use in audits and troubleshooting events.

- A user must be identified before network access is granted.

Authorization is the ability to control user access to specific services. Authentication is used to verify the identity of the user. The accounting feature logs user actions once the user is authenticated and authorized.

13. What is the result of entering the aaa accounting network command on a router?

- **The router collects and reports usage data related to network-related service requests.***
- The router outputs accounting data for all EXEC shell sessions.
- The router provides data for only internal service requests.
- The router outputs accounting data for all outbound connections such as SSH and Telnet.

The three parameters that can be used with aaa accounting are:
network- runs accounting for all network-related service requests, including PPP
exec- runs accounting for all the EXEC shell session
connection – runs accounting on all outbound connections such as SSH and Telnet

14. What is a characteristic of AAA accounting?

- **Possible triggers for the aaa accounting exec default command include start-stop and stop-only.***
- Accounting can only be enabled for network connections.
- Accounting is concerned with allowing and disallowing authenticated users access to certain areas and programs on the network.
- Users are not required to be authenticated before AAA accounting logs their activities on the network.

AAA accounting enables usage tracking, such as dial-in access and EXEC shell session, to log the data gathered to a database, and to produce reports on the data gathered. Configuring AAA accounting with the keyword Start-Stop triggers the process of sending a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. AAA accounting is not limited to network connection activities. AAA accounting is in effect, if enabled, after a user successfully authenticated. Allowing and disallowing user access is the scope of AAA authorization.

15. Which authentication method stores usernames and passwords in ther router and is ideal for small networks.

- local AAA over TACACS+
- server-based AAA over TACACS+

- **local AAA***
- local AAA over RADIUS
- server-based AAA over RADIUS
- server-based AAA

16. Which component of AAA allows an administrator to track individuals who access network resources and any changes that are made to those resources?

- **accounting***
- accessibility
- authentication
- authorization

One of the components in AAA is accounting. After a user is authenticated through AAA, AAA servers keep a detailed log of exactly what actions the authenticated user takes on the device.

17. Which two features are included by both TACACS+ and RADIUS protocols? (Choose two.)

- 802.1X support
- separate authentication and authorization processes
- SIP support
- **password encryption***
- **utilization of transport layer protocols***

Both TACACS+ and RADIUS support password encryption (TACACS+ encrypts all communication) and use Layer 4 protocol (TACACS+ uses TCP and RADIUS uses UDP). TACACS+ supports separation of authentication and authorization processes, while RADIUS combines authentication and authorization as one process. RADIUS supports remote access technology, such as 802.1x and SIP; TACACS+ does not.

18. Which server-based authentication protocol would be best for an organization that wants to apply authorization policies on a per-group basis?

- SSH
- RADIUS
- ACS
- **TACACS+***

TACACS+ is considered to be more secure than RADIUS because all TACACS+ traffic is encrypted instead of just the user password when using RADIUS.

19. Refer to the exhibit. Which statement describes the configuration of the ports for Server1?

```
Rtr1(config)# aaa new-model
Rtr1(config)# radius server Server1
Rtr1(config-radius-server)# address ipv4 192.168.1.101 auth-port 1812 acct-port 1813
Rtr1(config-radius-server)# key RADIUS-Pa55w0rd
Rtr1(config-radius-server)# exit
```


- The configuration using the default ports for a Cisco router.
- The configuration of the ports requires 1812 be used for the authentication and the authorization ports.
- The configuration will not be active until it is saved and Rtr1 is rebooted.
- **The ports configured for Server1 on the router must be identical to those configured on the RADIUS server.***

Cisco routers, by default, use port 1645 for the authentication and port 1646 for the accounting. In the configuration output, the configuration of the RADIUS authentication and authorization ports must match on both router Rtr1 and Server1.

20. True or False?
The single-connection keyword prevents the configuration of multiple TACACS+ servers on a AAA-enabled router.

- **false***
- true

The single-connection keyword enhances TCP performance by maintaining a single TCP connection for the entire duration of a session. The keyword does not prevent the configuration of multiple TACACS+ servers.

21. Why would a network administrator include a local username configuration, when the AAA-enabled router is also configured to authenticate using several ACS servers?

- Because ACS servers only support remote user access, local users can only authenticate using a local username database.
- A local username database is required when configuring authentication using ACS servers.
- **The local username database will provide a backup for authentication in the event the ACS servers become unreachable.***
- Without a local username database, the router will require successful authentication with each ACS server.

The local username database can serve as a backup method for authentication if no ACS servers are available.

22. Which authentication method stores usernames and passwords in the router and is ideal for small networks?

- **local AAA***
- server-based AAA
- server-based AAA over TACACS+
- local AAA over TACACS+
- local AAA over RADIUS
- server-based AAA over RADIUS

In a small network with a few network devices, AAA authentication can be implemented with the local database and with usernames and passwords stored on the network devices. Authentication using the TACACS+ or RADIUS protocol will require dedicated ACS servers although this authentication solution scales well in a large network.

23. What device is considered a supplicant during the 802.1X authentication process?

- **the client that is requesting authentication***
- the switch that is controlling network access
- the router that is serving as the default gateway
- the authentication server that is performing client authentication

The devices involved in the 802.1X authentication process are as follows:
The supplicant, which is the client that is requesting network access
The authenticator, which is the switch that the client is connecting to and that is actually controlling physical network access
The authentication server, which performs the actual authentication

24. What protocol is used to encapsulate the EAP data between the authenticator and authentication server performing 802.1X authentication?

- SSH
- MD5
- TACACS+
- **RADIUS***

Encapsulation of EAP data between the authenticator and the authentication server is performed using RADIUS.

Download PDF File below:

[sociallocker id=”54558″]

ITexamanswers.net – CCNA Security v2.0 Chapter 3 Exam Answers.pdf

745.42 KB 2152 downloads

...

Download

[/sociallocker]