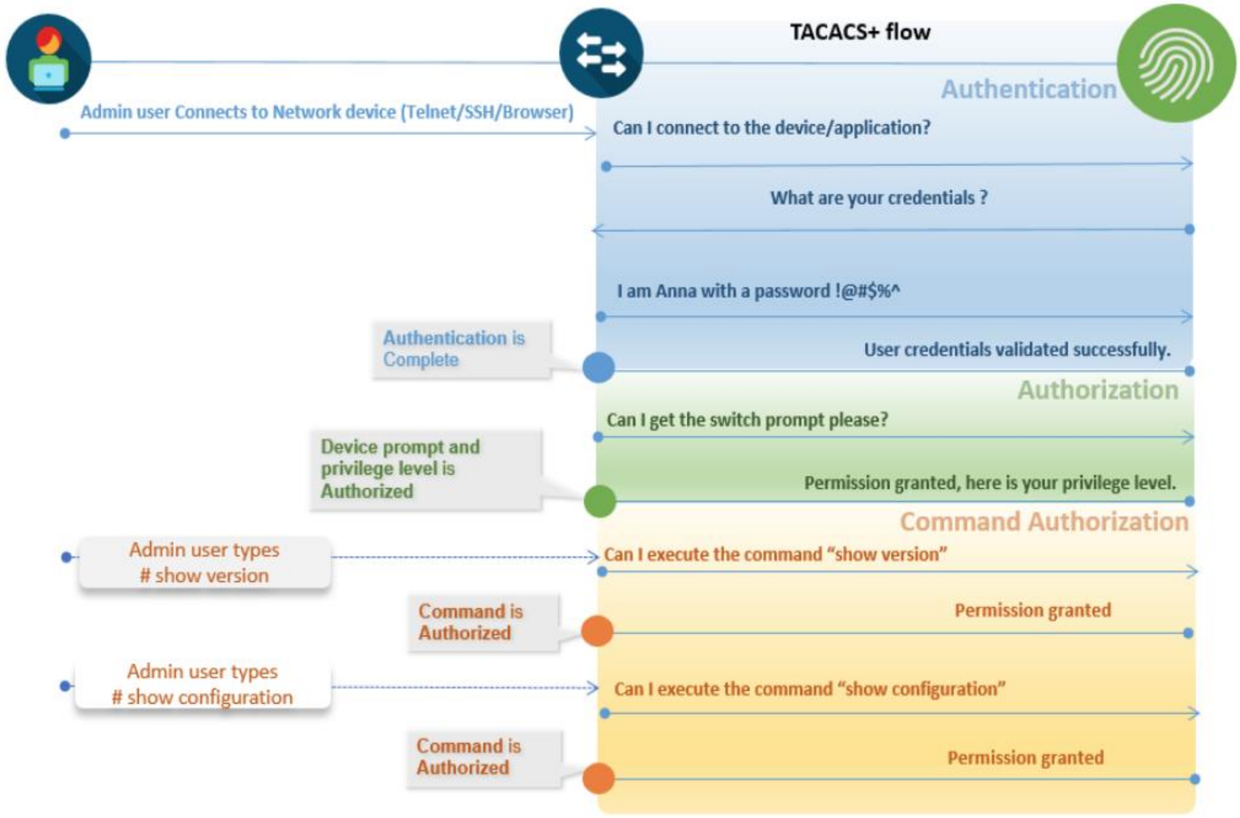
AAA Options:

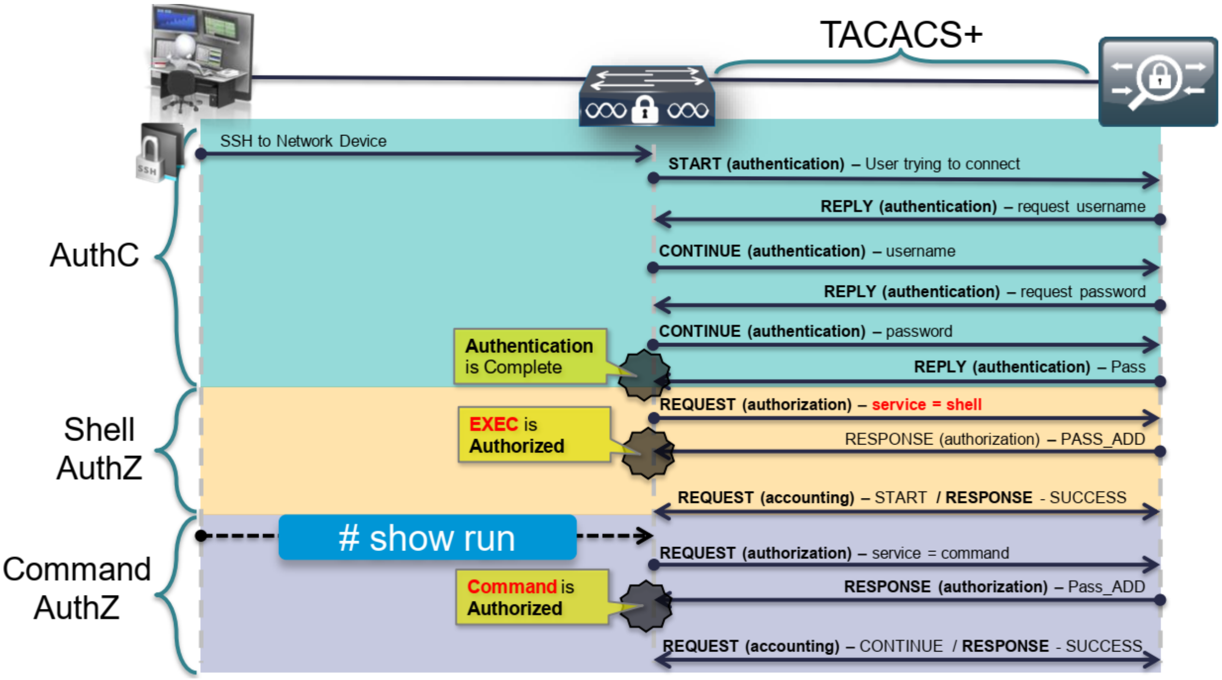
- Cisco Identity Services Engine (ISE) provides a number of ways to implement AAA.
- Two main protocols used by Cisco Identity Services Engine are TACACS and RADIUS.

AAA with TACACS+:

- TACACS+ stands for Terminal Access Controller Access Control System Plus.
- Terminal Access Controller Access-Control System is a protocol set created.
- The TACACS protocol Intended was for controlling the access to UNIX terminals.
- Cisco created a new protocol called TACACS+ used for the Device Administration.
- TACACS+ is Cisco proprietary protocol that is use to deliver AAA security services.
- TACACS+ provides centralized acceptance of user to take access control of devices.
- TACACS+ provides to control authorization of device commands per-user or group.
- Terminal Access Controller Access Control System Plus offers multiprotocol support.
- TACACS+ encrypts entire body of the packet but leaves a standard TACACS+ header.
- Terminal Access Controller Access Control System Plus (TACACS+) separates AAA.
- TACACS+ uses TCP port 49 to communicate between TACACS+ client and server.
- Cisco switch authenticating & authorizing administrative access to switch's IOS CLI.
- The Cisco switch is the TACACS+ client, and Cisco Secure ISE is the TACACS+ server.
- TACACS+ is it's the ability to separate authentication, authorization and accounting.
- This is why TACACS+ protocol is so commonly used for the Device Administration.
- Device need to authenticate once, but authorize many times during single session.
- A router or switch may need to authorize a user's activity on a per-command basis.
- TACACS+ protocol is designed to accommodate that type of authorization need.

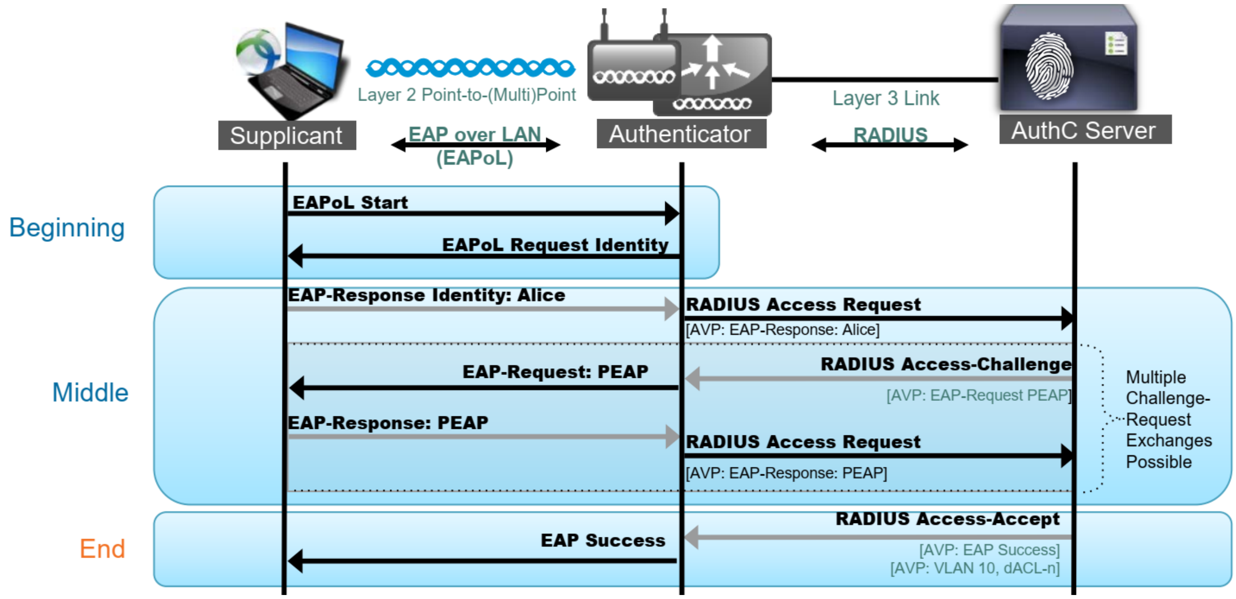
RADIUS	TACACS+
RADIUS uses UDP	TACACS+ uses TCP
Uses ports 1812/1645 for authentication Uses ports 1813/1646 for accounting	TACACS+ uses TCP port 49
RADIUS encrypts passwords only	TACACS+ encrypts the entire communication
RADIUS combines authentication and Authorization	TACACS+ treats Authentication, Authorization, and Accountability differently
RADIUS is an open protocol	TACACS+ is Cisco proprietary protocol
RADIUS is a light-weight protocol consuming less resources	TACACS+ is a heavy-weight protocol consuming more resources
RADIUS is limited to privilege mode	TACACS+ supports 15 privilege levels
Mainly used for Network Access	Mainly used for Device Administration

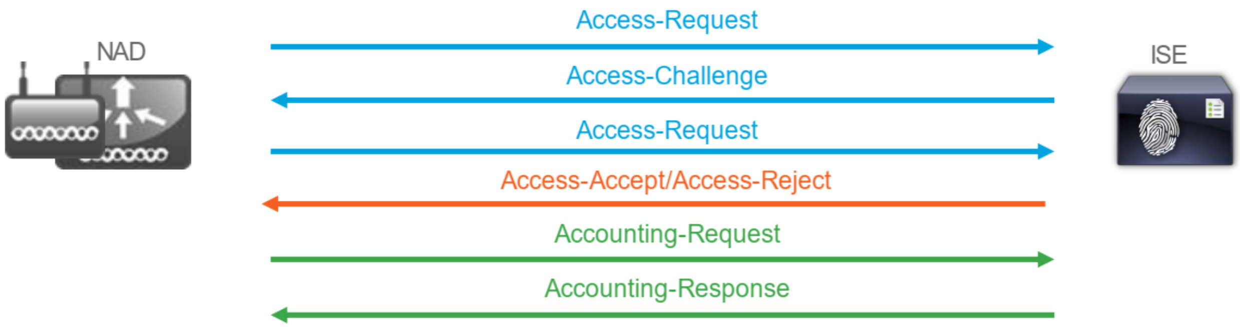

TACACS+ flow
Admin user Connects to Network device (Telnet/SSH/Browser)
Authentication
Can I connect to the device/application?
What are your credentials ?
I am Anna with a password !@#$%^
Authentication is Complete
User credentials validated successfully.
Authorization
Can I get the switch prompt please?
Device prompt and privilege level is Authorized
Permission granted, here is your privilege level.
Command Authorization
Admin user types # show version
Can I execute the command "show version"
Command is Authorized
Permission granted
Admin user types # show configuration
Can I execute the command "show configuration"
Command is Authorized
Permission granted


TACACS+
SSH to Network Device
START (authentication) – User trying to connect
REPLY (authentication) – request username
CONTINUE (authentication) – username
REPLY (authentication) – request password
CONTINUE (authentication) – password
REPLY (authentication) – Pass
AuthC
Authentication is Complete
REQUEST (authorization) – service = shell
RESPONSE (authorization) – PASS_ADD
Shell AuthZ
EXEC is Authorized
REQUEST (accounting) – START / RESPONSE - SUCCESS
# show run
REQUEST (authorization) – service = command
RESPONSE (authorization) – Pass_ADD
Command AuthZ
Command is Authorized
REQUEST (accounting) – CONTINUE / RESPONSE - SUCCESS

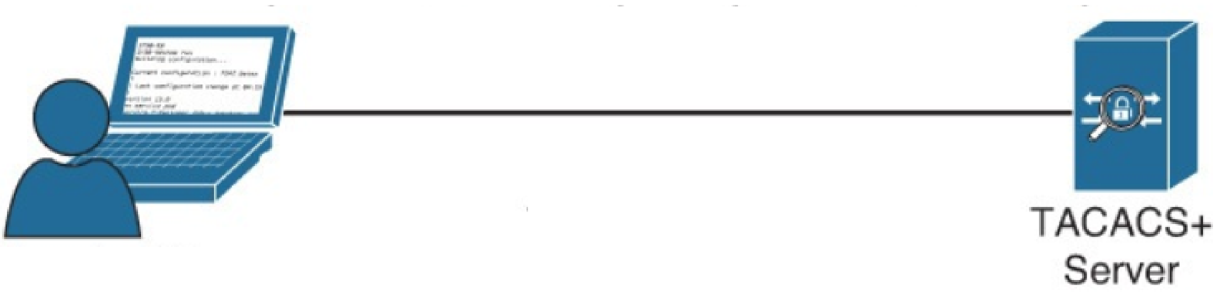
AAA with RADIUS:

- RADIUS is a term, which is stand for Remote Authentication Dial in User Service.
- Remote Access Dial in User Service (RADIUS) is an open standard protocol use for.
- RADIUS use for communication between any vendor AAA client and Cisco ISE server.
- RADIUS is a security protocol that secures the network against unauthorized access.
- RADIUS clients run on routers & send authentication request to a centralized server.
- RADIUS Server contains network service access information and user authentication.
- RADIUS does not allow the users to control which commands can be executed or not.
- RADIUS is not as useful for Cisco Router or Cisco Switch or Cisco Firewall management.
- RADIUS does not allow users to control which commands can be executed on a router.
- Remote Authentication Dial in User Service (RADIUS) does not support multiprotocol.
- RADIUS encrypts password of the access-request packet only from Client to the server.
- RADIUS Protocols uses UDP as a transport protocol while TACACS+ Protocols uses TCP.
- RADIUS Protocol combines authentication and authorization processes into one packet.
- It uses port number 1812 for authentication and authorization and 1813 for accounting.
- It uses port number 1645 for authentication and authorization and 1646 for accounting.

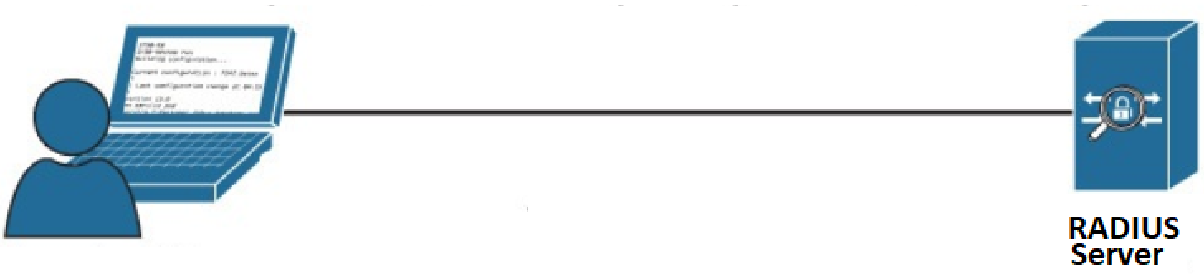




TACACS+ and RADIUS Packets:



TACACS + Packets			
→	Start	Authentication	User trying to connect
←	Reply	Authentication	Ask client for username
→	Continue	Authentication	Bring username to server
←	Reply	Authentication	Ask Client for Password
→	Continue	Authentication	Bring Password to server
←	Reply	Authentication	Authentication Pass/Fail Status
→	Request	Authorization	Request for service = shell
←	Response	Authorization	Authorization success /Fail
→	Request	Accounting	Request for Start-exec
←	Response	Accounting	Record Received



RADIUS Packets			
→	Access	Request	Access request
←	Access	Accept	With Authorization
→	Accounting	Request	To start accounting
←	Accounting	Response	Accounting Response to client
→	Accounting	Request	To stop accounting
←	Accounting	Response	Accounting Response to client