AAA
– Authentication, Authorization, and Accounting

AAA Terminology

- **Authentication**: verifies a user’s identity, usually with a username and password
- **Authorization**: determines what services a user can access
- **Accounting**: keeps a record of a user’s actions
- **ACS**: Access Control Server
- **AAA session**: Period of time a user is connected to the router/network through AAA

Local vs. Remote Authentication

Local

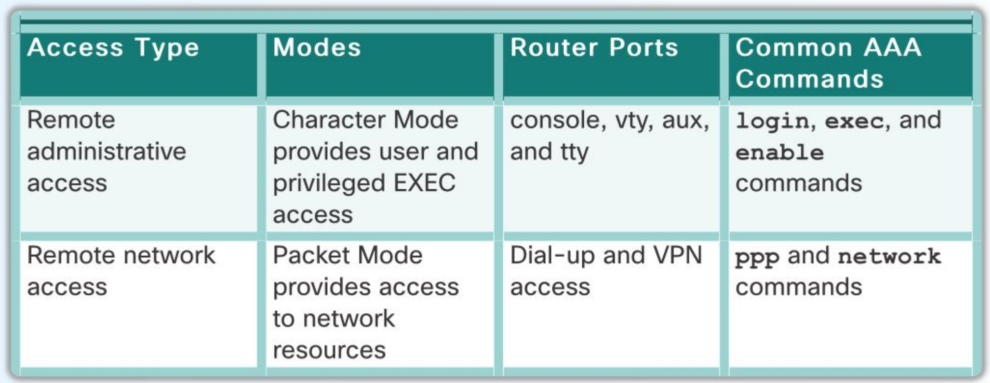
- Uses the usernames and passwords created on the device
- Simpler to set up
- Does not scale well
- More difficult to make modifications across devices

Remote

- Checks login credentials against a database stored on a server
- More difficult to set up
- Scales easily
- Changes to the server affect all connected devices

AAA Access Modes

- Different methods to request AAA services
- Most AAA commands apply to both modes
- Character mode: user directly connects to the router, which then authenticates the user
- Packet mode: user goes through the router to a server, which then authenticates the user



Access Type	Modes	Router Ports	Common AAA Commands
Remote administrative access	Character Mode provides user and privileged EXEC access	console, vty, aux, and tty	**login**, **exec**, and **enable** commands
Remote network access	Packet Mode provides access to network resources	Dial-up and VPN access	**ppp** and **network** commands

Authorization

- Uses privilege levels or views to determine what a user can and cannot do
- Occurs after authentication
- Performed immediately without further action from the user

Accounting

- Generates a start message when a user is authenticated and a stop message when the session is over
- Collects data used for billing, auditing, or forensics
- Can include information such as who entered which commands at what time, system error messages, packet/byte counts, etc.

Authentication Config

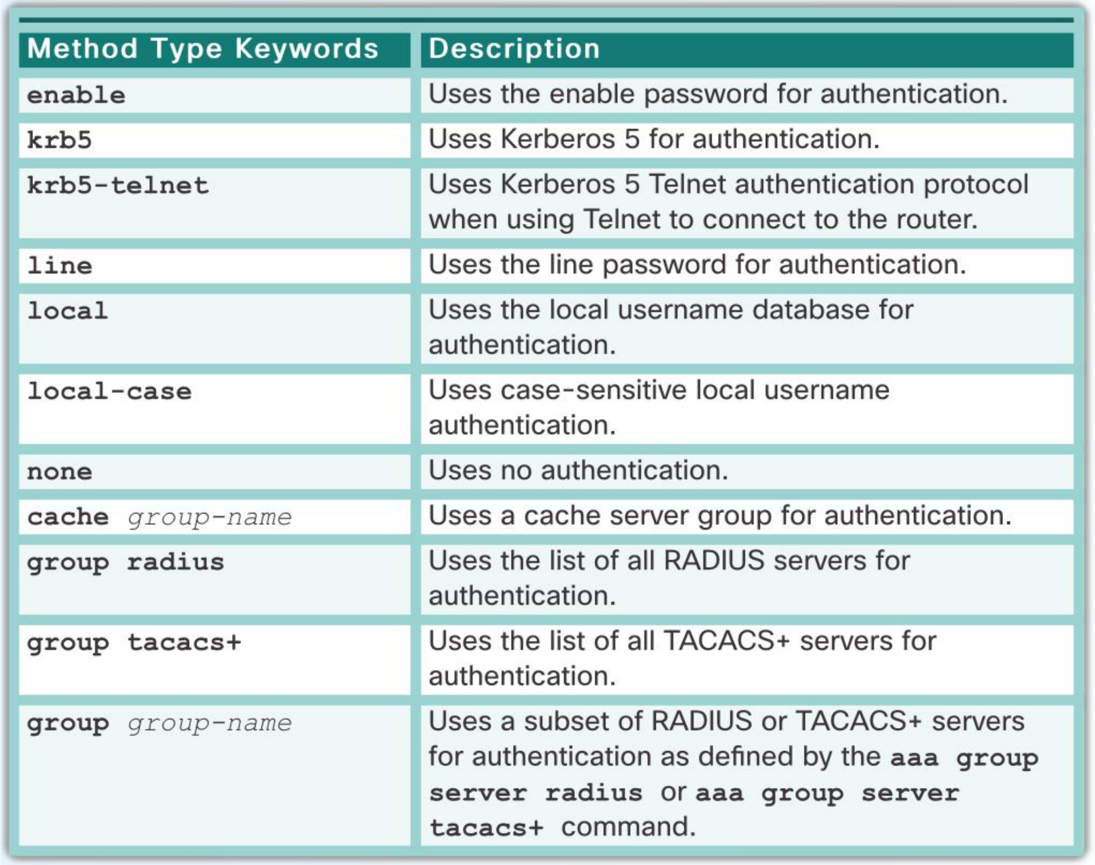
- A list is created with 1-4 authentication methods (TACACS+, RADIUS, local, enable, etc.)
- The list is applied to vty lines
- When a user attempts to login, the router uses the methods in the order entered to attempt to authenticate the user
- If an error occurs, the router tries the next method
- If a user is denied access, the process stops without attempting the next method

The “Default” List

- Default list has only the method “local”, but can be edited
- Automatically applied to all interfaces/lines after AAA is enabled
- If the default list is edited, those edits automatically apply to all interfaces/lines
- If an interface/line has a different list applied, it overrides the default

Authentication Methods

Note: Not all methods are available in Packet Tracer



Method Type Keywords	Description
enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
krb5-telnet	Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
cache *group-name*	Uses a cache server group for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Authentication Server Protocols

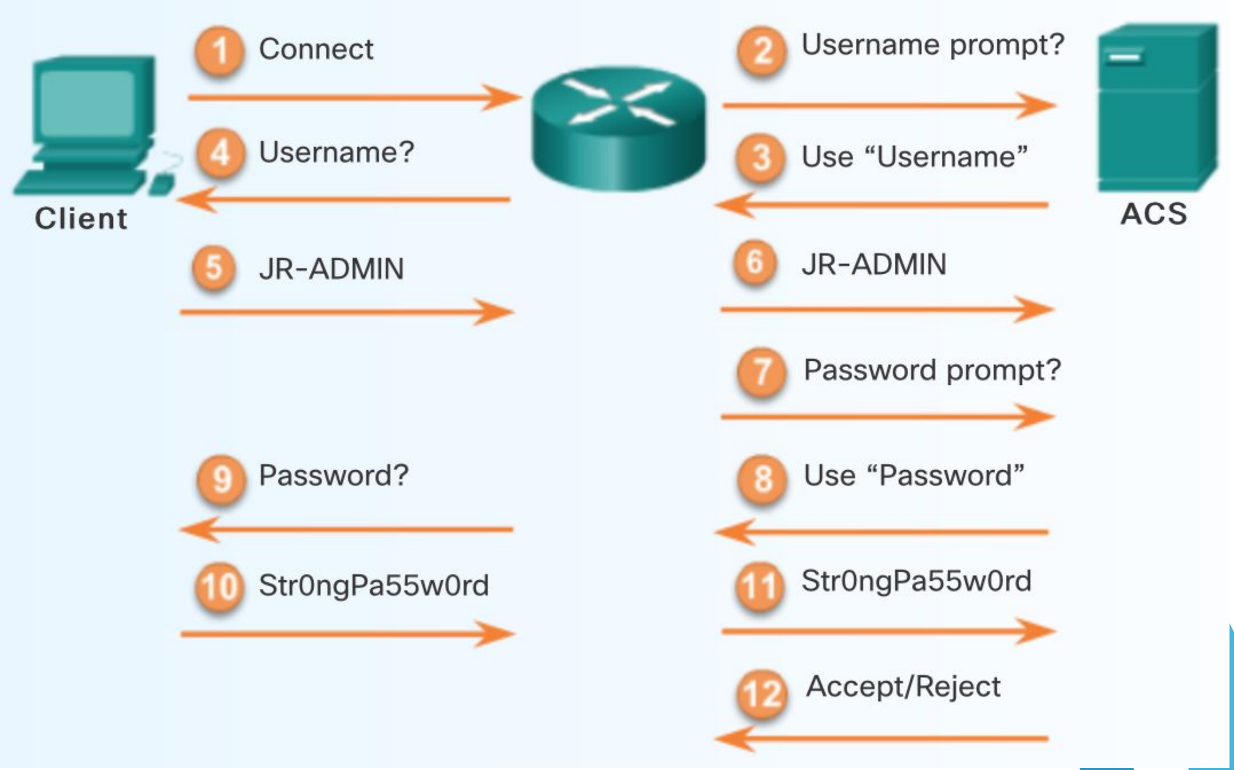
TACACS+

- Incompatible with its predecessors TACACS and XTACACS
- Separates authentication and authorization
- Encrypts all communication
- Utilizes TCP port 49

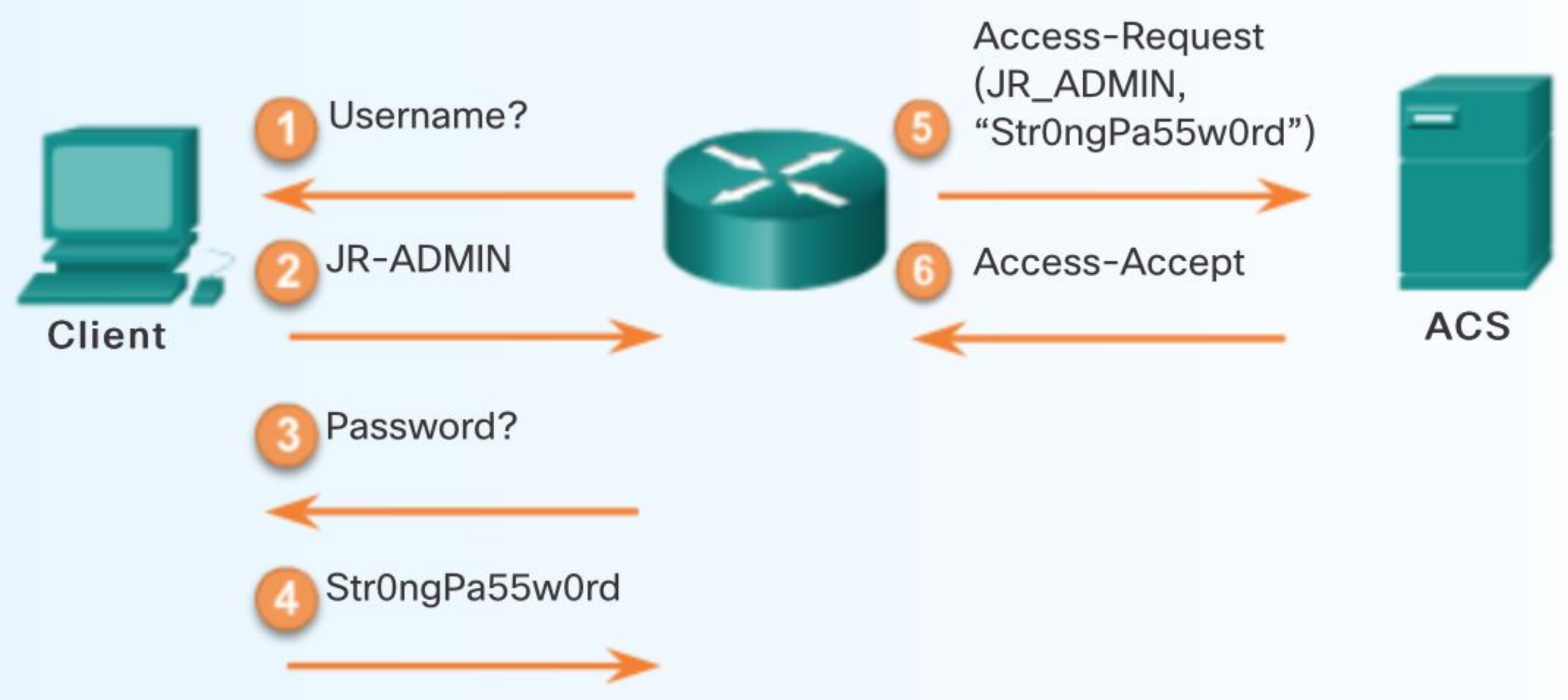
RADIUS

- Uses proxy servers for scalability
- Combines authentication and authorization as one process
- Encrypts only the password
- Utilizes UDP (port numbers vary)
- Supports remote-access technologies, 802.1X, and Session Initiation Protocol (SIP)

TACACS+ Authentication



RADIUS Authentication



1 Username?

2 JR-ADMIN

3 Password?

4 Str0ngPa55w0rd

5 Access-Request (JR_ADMIN, “Str0ngPa55w0rd”)

6 Access-Accept

Cisco Secure ACS

- Type of server located on an end device
- Can use TACACS+ and RADIUS
- Uses a GUI
- Centralizes authentication
- Offers scalability, security, flexibility, integration, 3rd party support, and several levels of access control

Accounting Configuration

- Uses a method list like the authentication command
- Can specify whether a start and stop message is recorded for each user session, only a stop message, or none
- Outside of Packet Tracer, it can be used to log exec sessions, network sessions, and/or outbound connections
- Within PT, it can only be used to log exec sessions

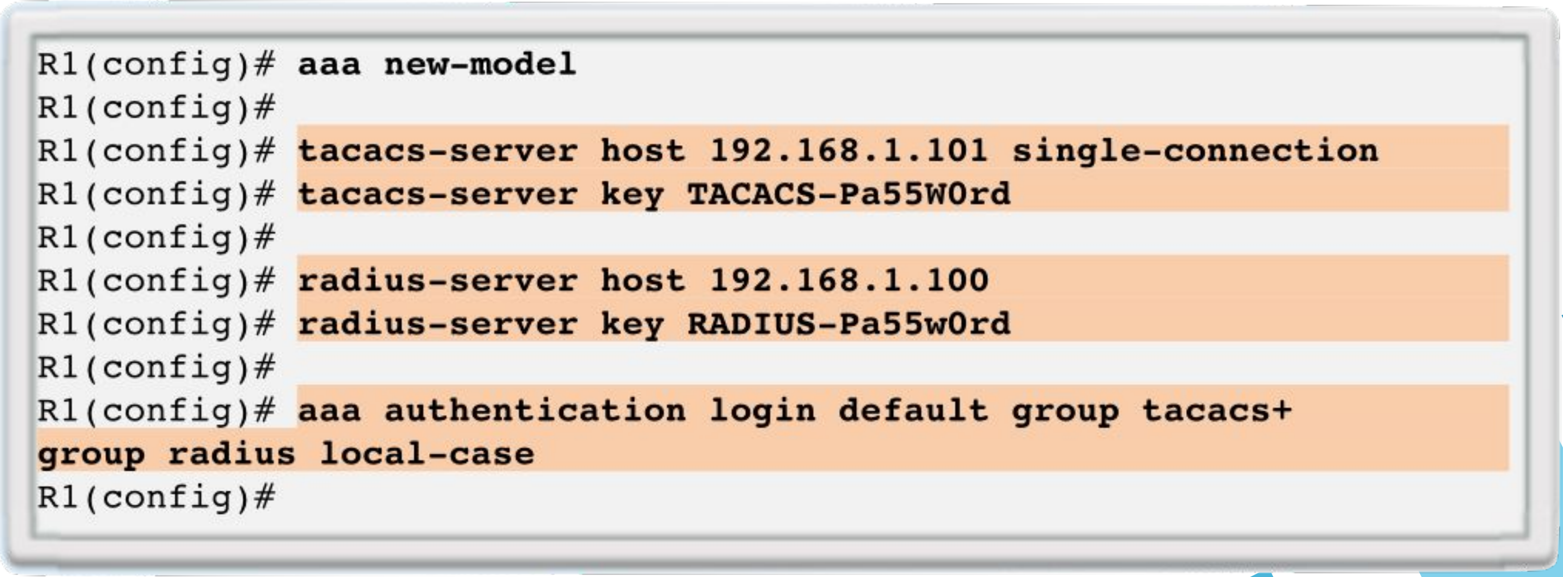
AAA Configuration

Step Description	Placement	Command	Category	Notes
enable AAA	router config	aaa new-model	requirement	
configure a list of authentication methods	router config	aaa authentication [enable/login/ppp] [default/other list name] [methods]	requirement	1-4 methods can be used possible methods: enable, local, group radius, group tacacs+, group [group name] (method explanations: http://goo.gl/tFYu9W) additional options outside of Packet Tracer default list uses local authentication on all lines add "none" as the last method to allow access even if other methods deny it (for use only when testing)
apply a list to lines	line config	login authentication [list name]	requirement	
lock out accounts with excessive login failures	router config	aaa local authentication attempts max-fail [attempts]	optional	after the set number of failed attempts has been reached, the connection is dropped and the account is locked until unlocked by an administrator
show locked out users	anywhere	do show aaa local user lockout	optional	
reset locked out users	router config	clear aaa local user lockout [all/username]	optional	

AAA Configuration (cont.)

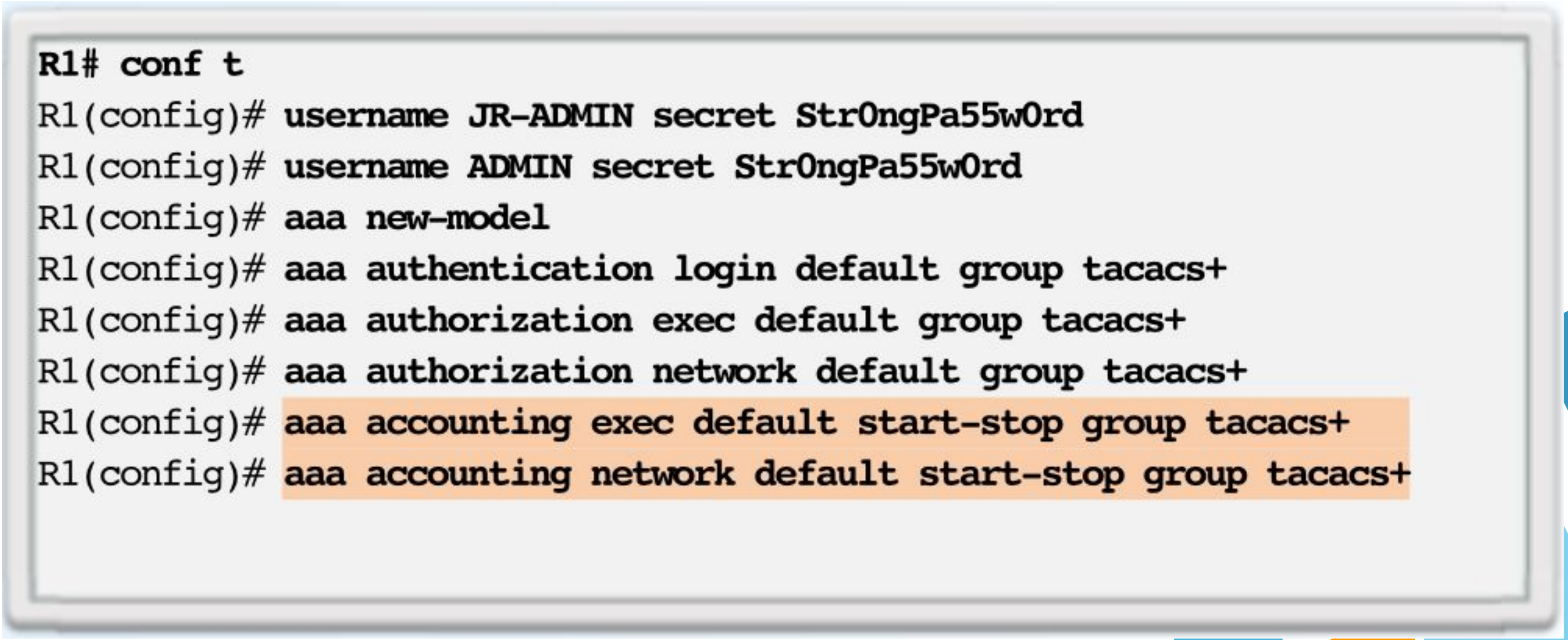
Step Description	Placement	Command	Category	Notes
show info on logged in users	anywhere	do show aaa sessions	optional	
show more info on a specific user's aaa session	anywhere	do show aaa user [all/session id]	optional	the session ID can be found using the "do show aaa sessions" command
add a TACAS+ server	router config	tacacs-server host [ip address]	optional	repeat the command to add multiple servers add "single-connection" to the end of the command for enhanced performance (only if instructed to)
add a RADIUS server	router config	radius-server host [ip address]	optional	repeat the command to add multiple servers
add a server key	router config	[tacacs-server/radius-server] key [password]	optional	must be the same key on the router and server
configure a list of authorization methods	router config	aaa authorization [network/exec] [default/other list name] [methods]	optional	must have a user with full rights before authorization is configured methods: group, if-authenticated, local, none
configure accounting	router config	aaa accounting exec [default/other list name] [none/start-stop/stop-only] group [radius/tacas+]	optional	additional options outside of Packet Tracer

AAA Server Config Example



```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs-server host 192.168.1.101 single-connection
R1(config)# tacacs-server key TACACS-Pa55W0rd
R1(config)#
R1(config)# radius-server host 192.168.1.100
R1(config)# radius-server key RADIUS-Pa55w0rd
R1(config)#
R1(config)# aaa authentication login default group tacacs+
group radius local-case
R1(config)#
```

AAA Config Example



```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ngPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default group tacacs+
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
R1(config)# aaa accounting exec default start-stop group tacacs+
R1(config)# aaa accounting network default start-stop group tacacs+
```

Packet Tracer Lab

CCNA 3.6.1.2

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash