CCS6224
Network Security

Lecture 2
Authentication, Authorization, Accounting (AAA)

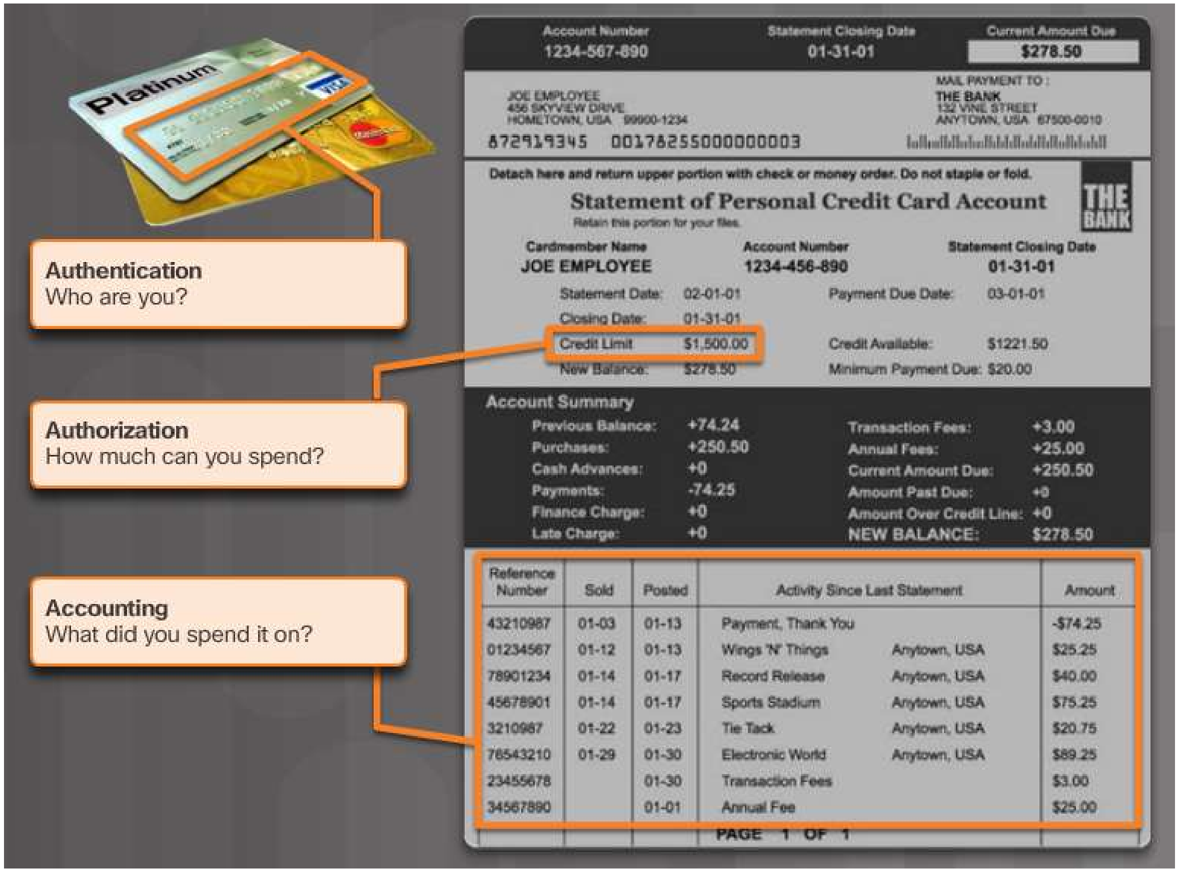
Simple Authentication

- The simplest form of authentication is passwords.
- Password-only logins are very vulnerable to brute-force attacks, and do not provide accountability.
- The local database method provides additional security, because an attacker is required to know a username and a password. It also provides more accountability, because the username is recorded when a user logs in.
- A better solution is to have all devices refer to the same database of usernames and passwords from a central server.

AAA Components

- Authentication- Users and administrators must prove that they are who they say they are. Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods.
- Authorization- After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform.
- Accounting and auditing- Accounting records what the user does, including what is accessed, the amount of time the resource is accessed, and any changes that were made.

AAA Components



Authentication
Who are you?

Authorization
How much can you spend?

Accounting
What did you spend it on?

Account Number	Statement Closing Date	Current Amount Due
1234-567-890	01-31-01	$278.50

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99900-1234

MAIL PAYMENT TO :
THE BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

872919345 00178255000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

THE BANK

Statement of Personal Credit Card Account

Retain this portion for your files.

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	01-31-01

Statement Date:	02-01-01	Payment Due Date:	03-01-01
Closing Date:	01-31-01		
Credit Limit	$1,500.00	Credit Available:	$1221.50
New Balance:	$278.50	Minimum Payment Due:	$20.00

Account Summary

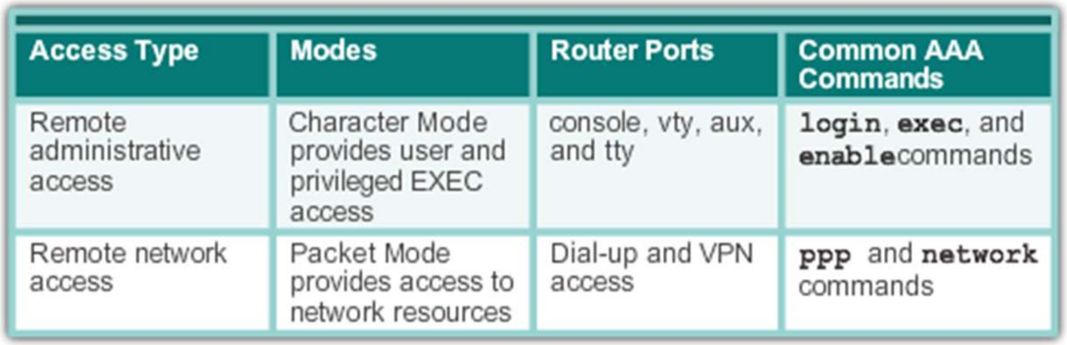
Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	$278.50

Reference Number	Sold	Posted	Activity Since Last Statement		Amount
43210987	01-03	01-13	Payment, Thank You		-$74.25
01234567	01-12	01-13	Wings 'N' Things	Anytown, USA	$25.25
78901234	01-14	01-17	Record Release	Anytown, USA	$40.00
45678901	01-14	01-17	Sports Stadium	Anytown, USA	$75.25
3210987	01-22	01-23	Tie Tack	Anytown, USA	$20.75
76543210	01-29	01-30	Electronic World	Anytown, USA	$89.25
23455678		01-30	Transaction Fees		$3.00
34567890		01-01	Annual Fee		$25.00

PAGE 1 OF 1

Authentication Modes

› AAA can be used to authenticate users for ***administrative access*** or to authenticate users for ***remote network access***. These two access methods use different modes to request AAA services.



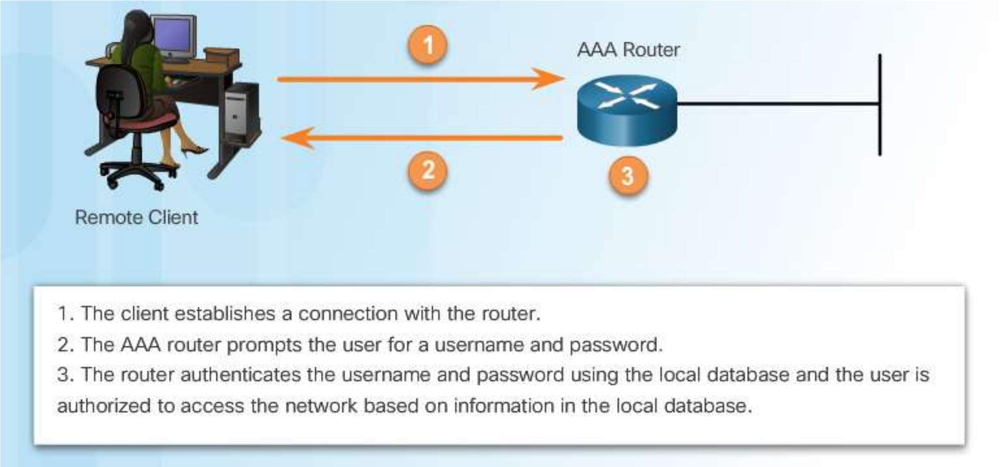
Access Type	Modes	Router Ports	Common AAA Commands
Remote administrative access	Character Mode provides user and privileged EXEC access	console, vty, aux, and tty	**`login`**, **`exec`**, and **`enable`**commands
Remote network access	Packet Mode provides access to network resources	Dial-up and VPN access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

- ➢ **Local AAA Authentication** - Uses a local database for authentication. This method stores usernames and passwords locally in the router, and users authenticate against the local database.

- ➢ **Server-Based AAA Authentication** - The server-based method uses an external database server resource that leverages RADIUS or TACACS+ protocols.

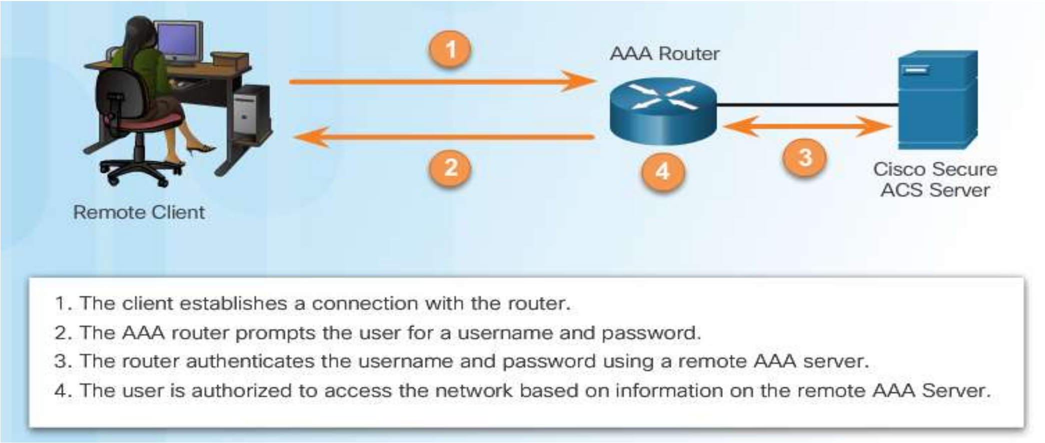
Authentication Modes

Local



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is authorized to access the network based on information in the local database.

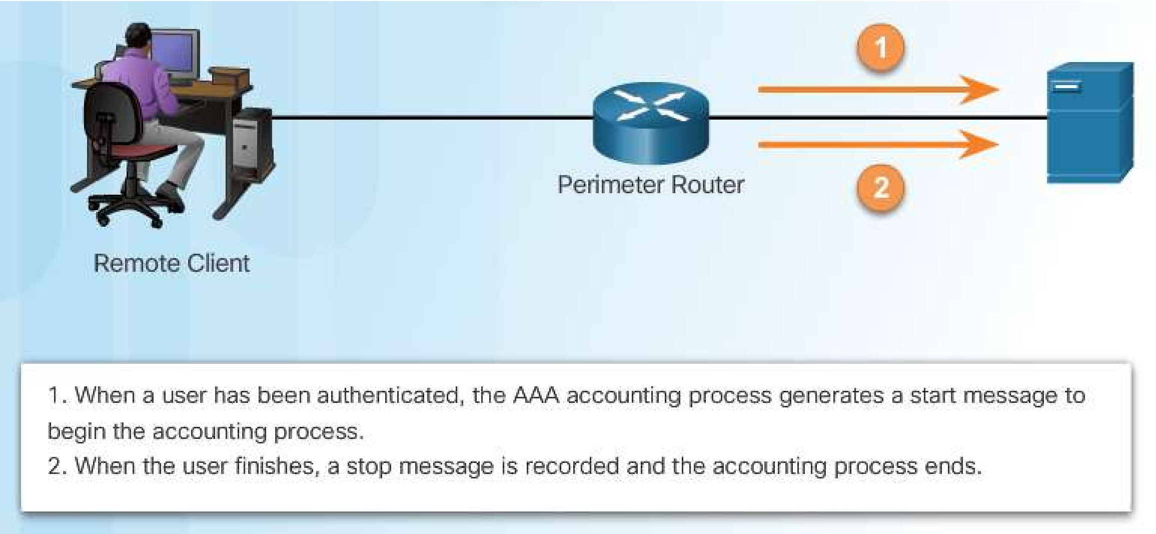
Server-based



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server.
4. The user is authorized to access the network based on information on the remote AAA Server.

Accounting

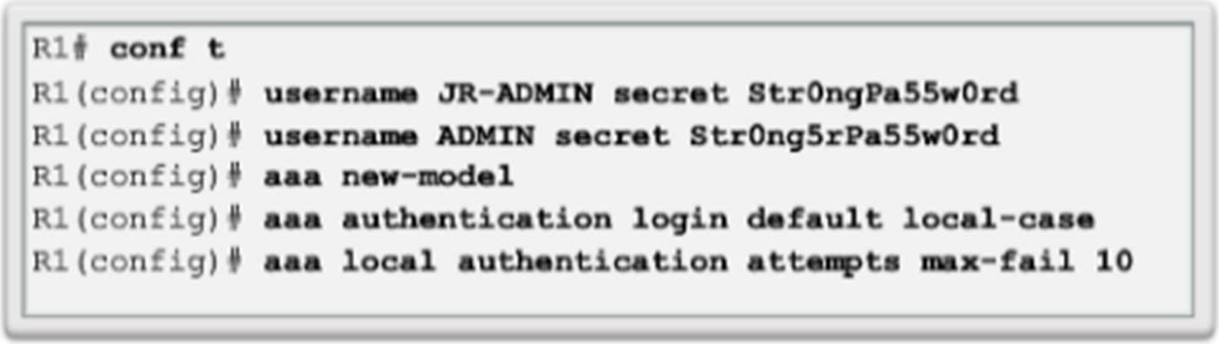
- Types of accounting information: Network, connection, systems, command, resource, etc.
- Accounting collects and reports usage data so that it can be employed for purposes such as auditing or billing.



1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded and the accounting process ends.

Configuring Local AAA Authentication with CLI Authenticating Administrative Access

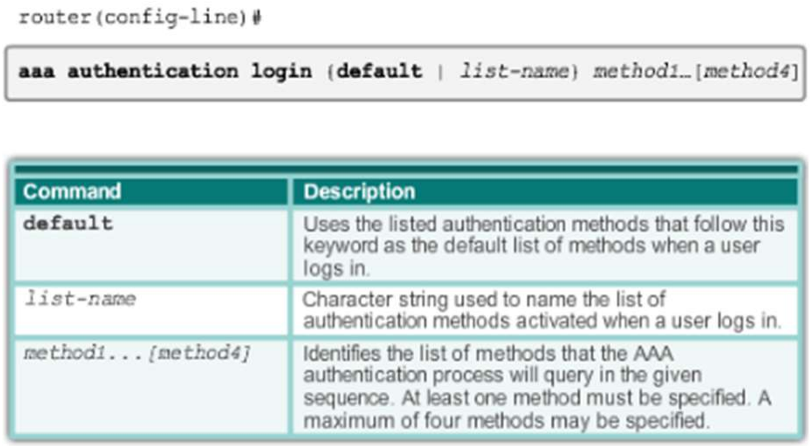
- Configuring local AAA services to authenticate administrator access (character mode access) requires a few basic steps:
- Step 1. Add usernames and passwords to the local router database for users that need administrative access to the router.
- Step 2. Enable AAA globally on the router.
- Step 3. Configure AAA parameters on the router.
- Step 4. Confirm and troubleshoot the AAA configuration.



```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case
R1(config)# aaa local authentication attempts max-fail 10
```

Authentication Methods

- To enable AAA, use the **`aaa new-model`** global configuration mode command.
- To configure authentication on vty ports, the auxiliary port, or the console port, define a named list of authentication methods and then apply that list to the various interfaces.
- To define a named list of authentication methods, use the **`aaa authentication login`** command.



```
router(config-line)#
aaa authentication login {default | list-name} method1…[method4]
```

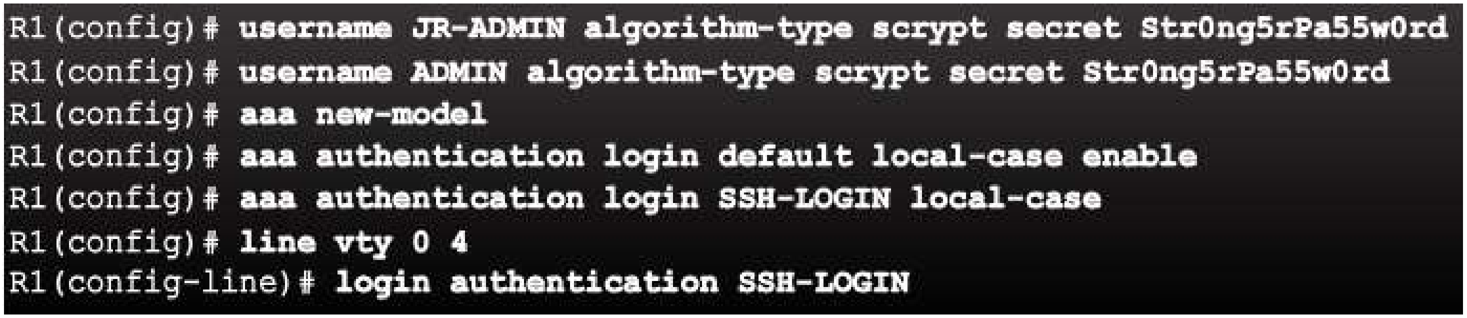
Command	Description
`default`	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
`list-name`	Character string used to name the list of authentication methods activated when a user logs in.
`method1...[method4]`	Identifies the list of methods that the AAA authentication process will query in the given sequence. At least one method must be specified. A maximum of four methods may be specified.

Authentication Methods

- To configure authentication, define a named list of authentication methods, and then apply that list to the various interfaces.
- To define a named list of authentication methods, use the **`aaa authentication login`** command.
- To enable local authentication using a preconfigured local database, use the **`local`** or **`local-case`** (case-sensitive) keyword.
- To specify that a user can authenticate using the enable password, use the **`enable`** keyword.
- A minimum of one method and a maximum of four methods can be specified for a single method list. When a user attempts to log in, the first method listed is used.

Authentication Methods

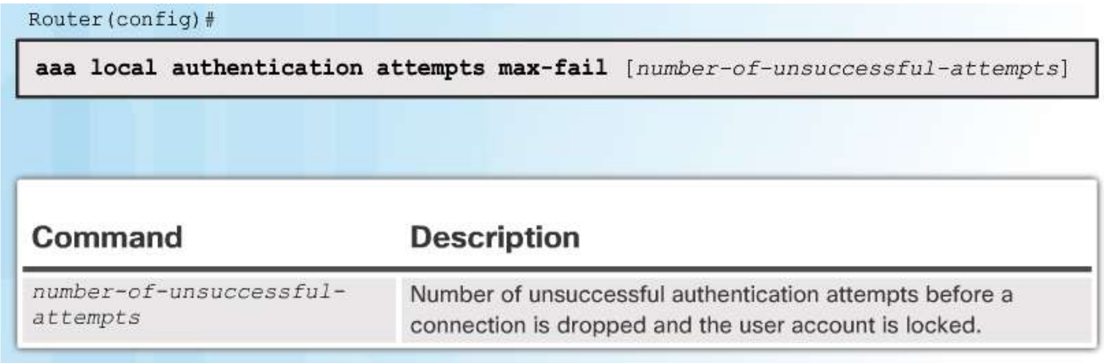
- The defined list of authentication methods must be applied to specific interfaces or lines. Different method lists can be applied to different interfaces and lines.
- To enable a specific list name, use the login authentication *list-name* command in line configuration mode.
- To assign multiple authentication methods to the default list, use the command aaa authentication login default *method1*…[*method2*].



```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
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 authentication login SSH-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication SSH-LOGIN
```

Refine the Authentication Configuration

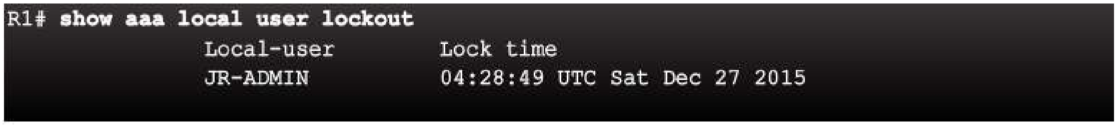
- Additional security can be implemented on the line using the **`aaa local authentication attempts max-fail`** *`number-of-unsuccessful-attempts`* command in global configuration mode.



```
Router(config)#
aaa local authentication attempts max-fail [number-of-unsuccessful-attempts]
```

Command	Description
number-of-unsuccessful-attempts	Number of unsuccessful authentication attempts before a connection is dropped and the user account is locked.

- This command secures AAA user accounts by locking out accounts that have excessive failed attempts.
- To show locked out users

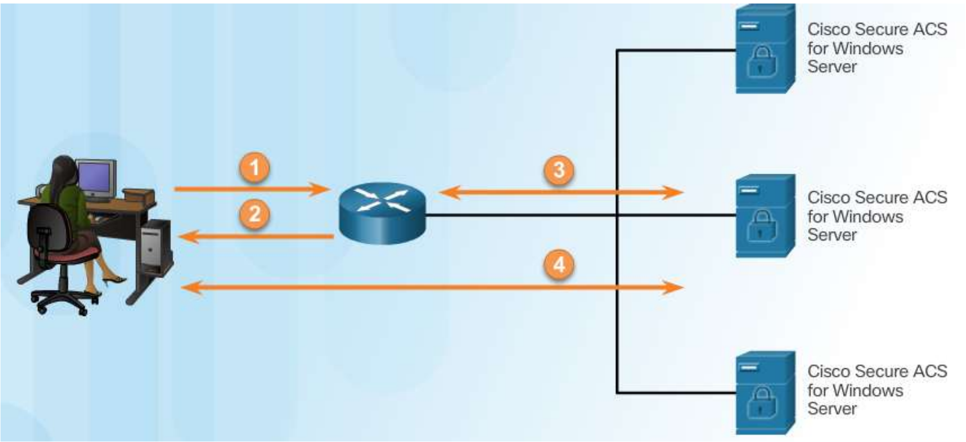


```
R1# show aaa local user lockout
               Local-user        Lock time
               JR-ADMIN          04:28:49 UTC Sat Dec 27 2015
```

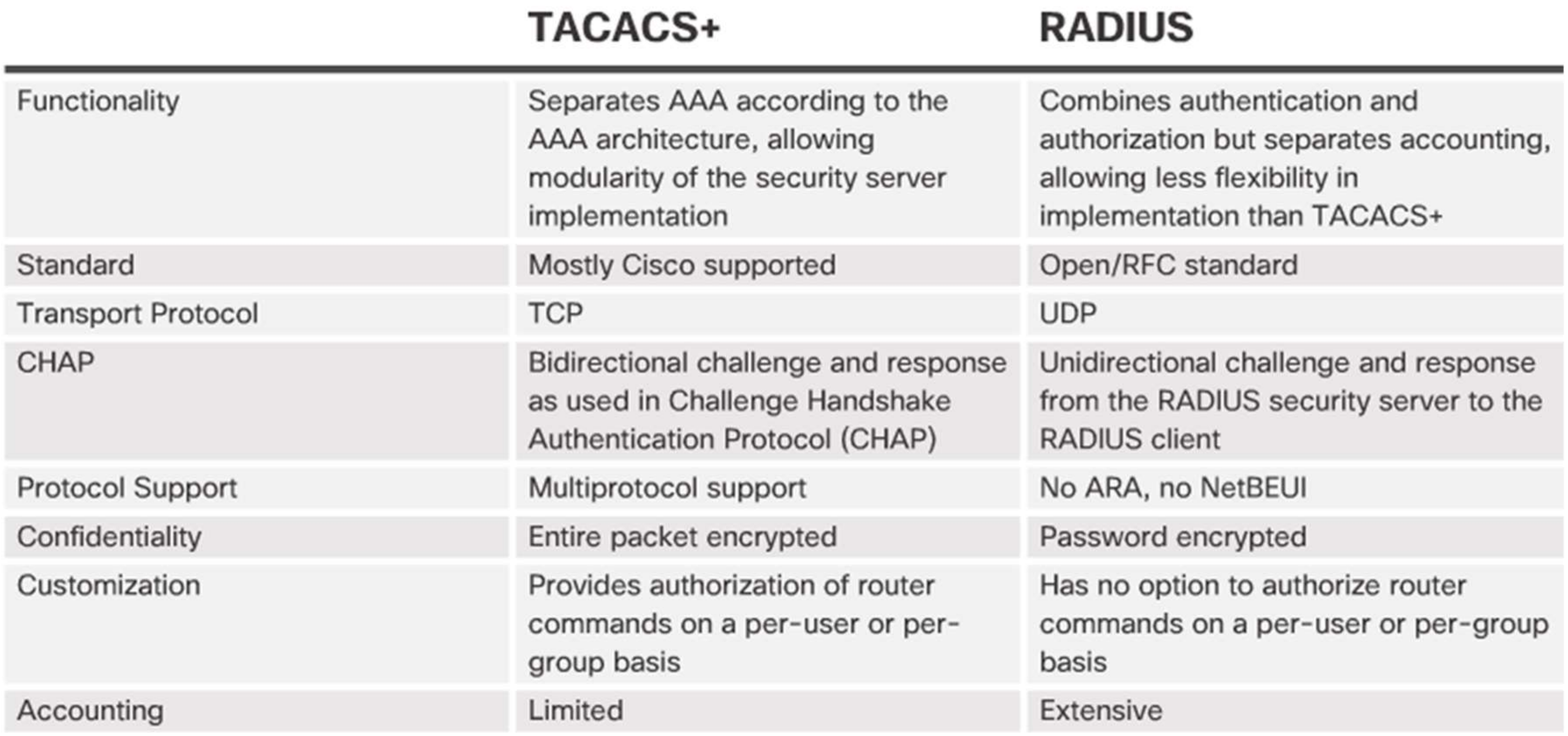
Server-based AAA

Server-based authentication:

1. User establishes a connection with the router.
2. Router prompts the user for a username and password.
3. Router passes the username and password to the Cisco Secure ACS (server or engine)
4. The Cisco Secure ACS authenticates the user.

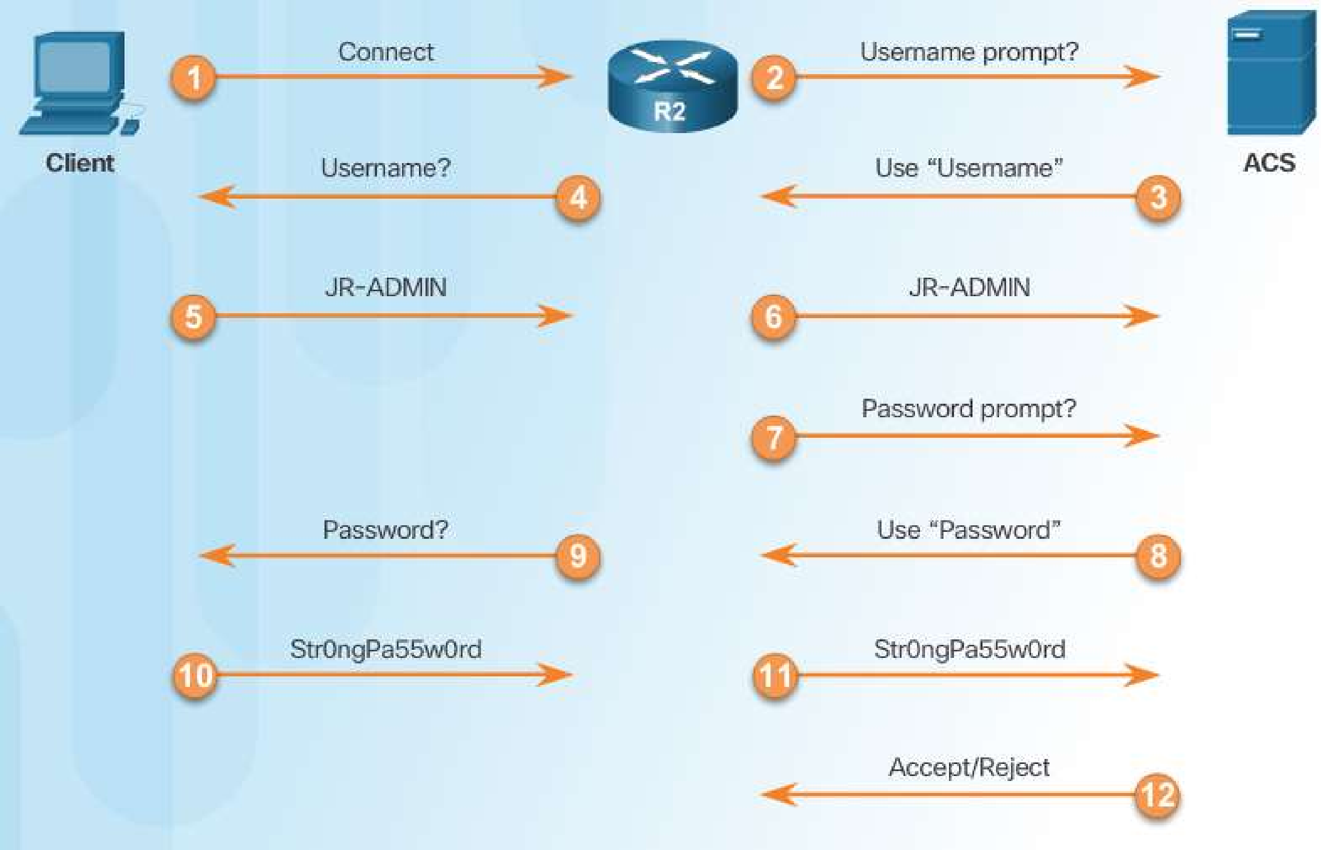

Cisco Secure ACS for Windows Server
1
2
3
4
Cisco Secure ACS for Windows Server
Cisco Secure ACS for Windows Server

Server-Based AAA Communication Protocols

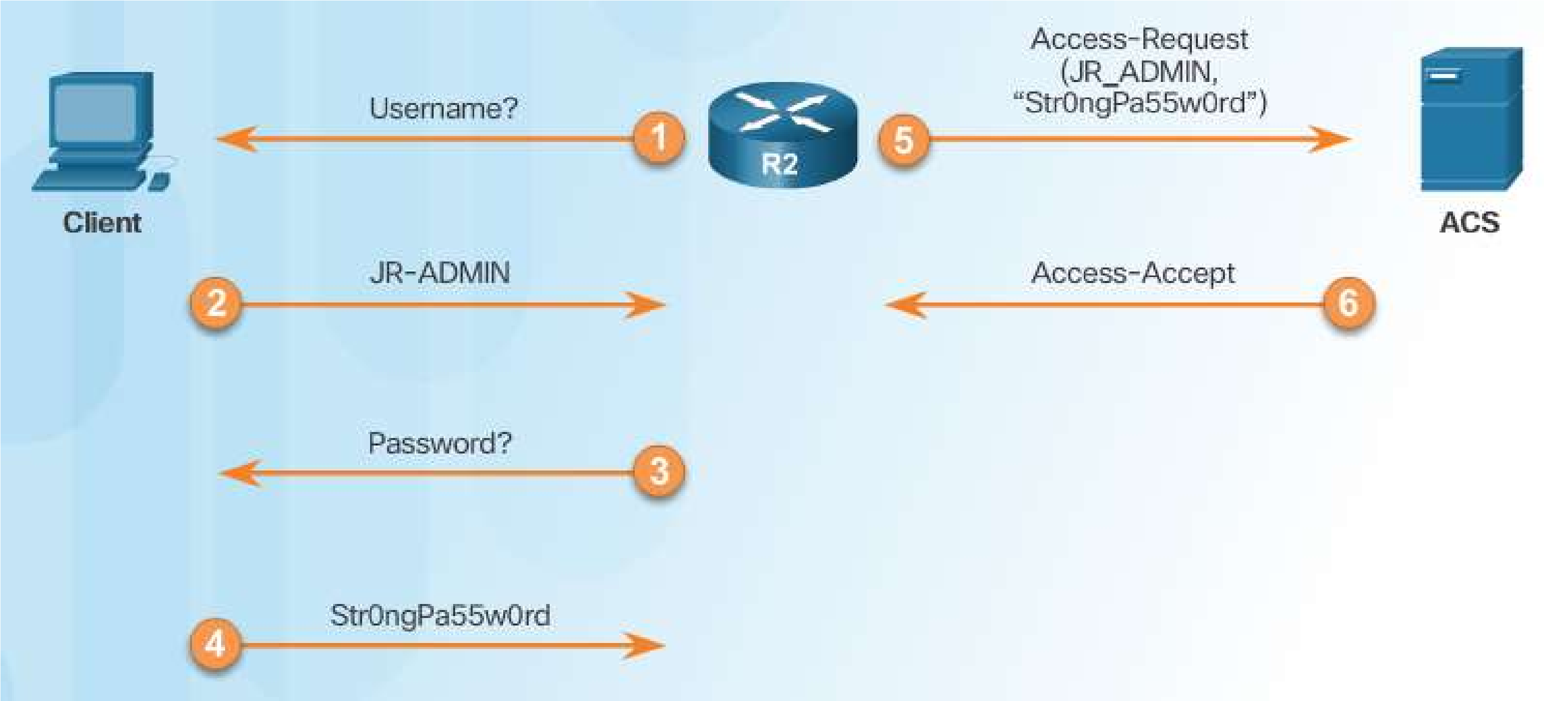


	TACACS+	RADIUS
Functionality	Separates AAA according to the AAA architecture, allowing modularity of the security server implementation	Combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+
Standard	Mostly Cisco supported	Open/RFC standard
Transport Protocol	TCP	UDP
CHAP	Bidirectional challenge and response as used in Challenge Handshake Authentication Protocol (CHAP)	Unidirectional challenge and response from the RADIUS security server to the RADIUS client
Protocol Support	Multiprotocol support	No ARA, no NetBEUI
Confidentiality	Entire packet encrypted	Password encrypted
Customization	Provides authorization of router commands on a per-user or per-group basis	Has no option to authorize router commands on a per-user or per-group basis
Accounting	Limited	Extensive

TACACS+ Authentication

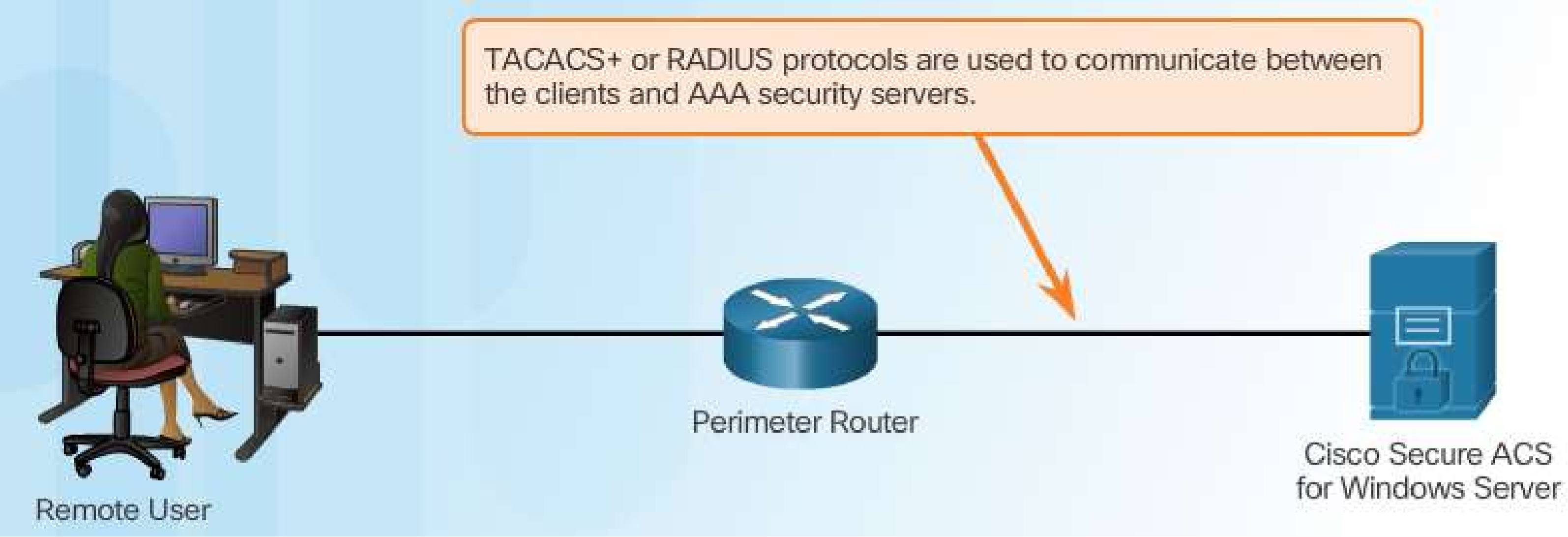


RADIUS Authentication



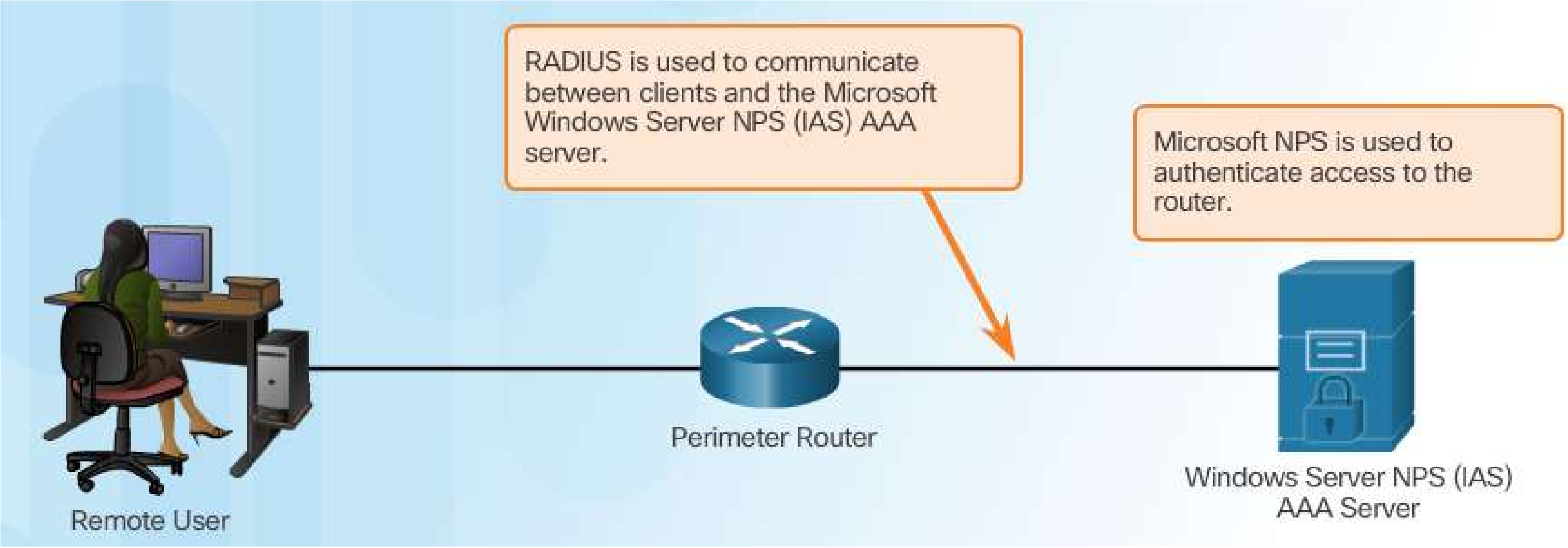
Integration of TACACS+ and ACS

Cisco Secure ACS



TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.

Integration of AAA with Active Directory

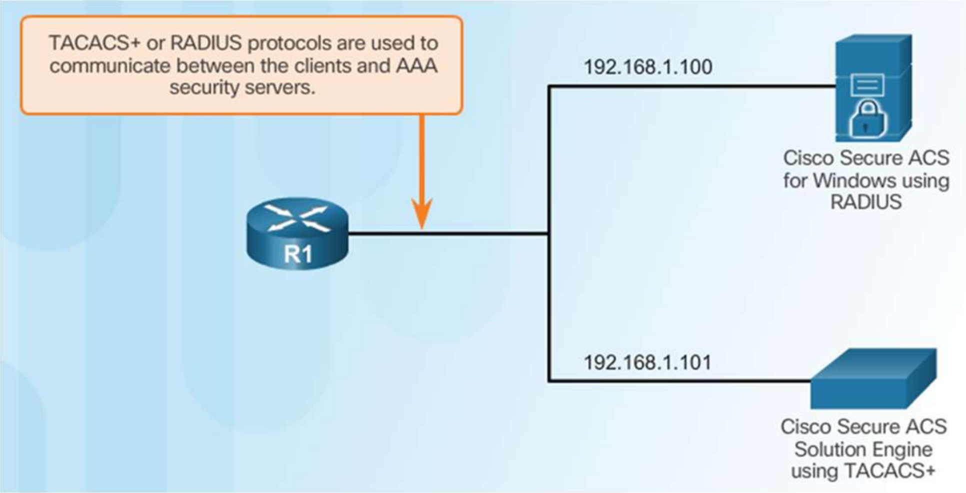


RADIUS is used to communicate between clients and the Microsoft Windows Server NPS (IAS) AAA server.

Microsoft NPS is used to authenticate access to the router.

Configuring Server-Based Authentication

1. Enable AAA.
2. Specify the IP address of the ACS server.
3. Configure the secret key.
4. Configure authentication to use either the RADIUS or TACACS+ server.

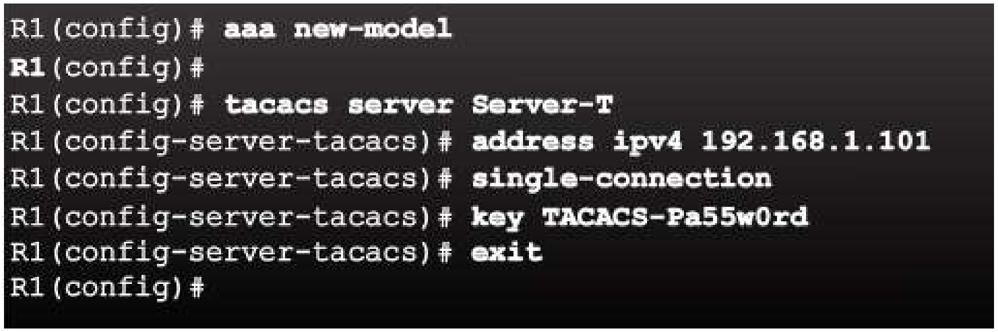


TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.

R1
192.168.1.100
Cisco Secure ACS for Windows using RADIUS
192.168.1.101
Cisco Secure ACS Solution Engine using TACACS+

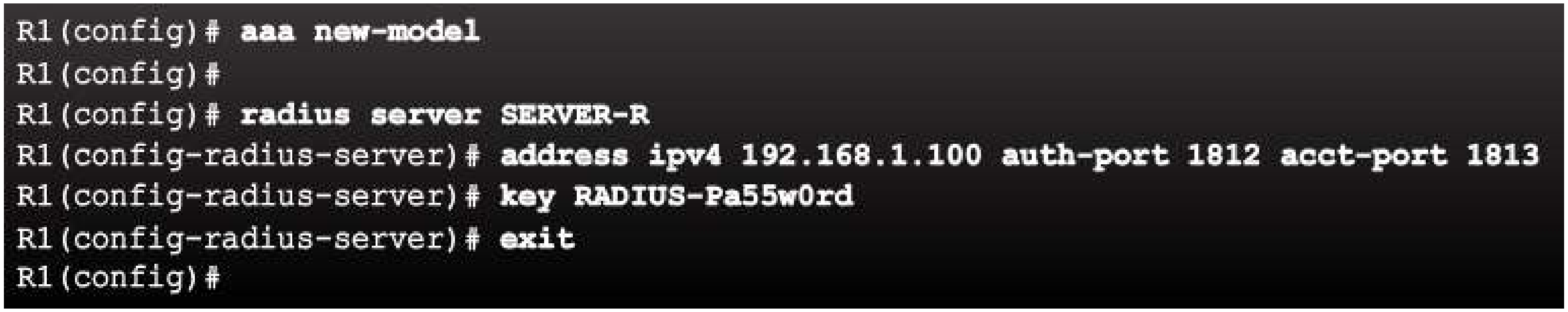
Configuring Server-Based Authentication

- Configuring a AAA TACACS+ server



```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs server Server-T
R1(config-server-tacacs)# address ipv4 192.168.1.101
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key TACACS-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)#
```

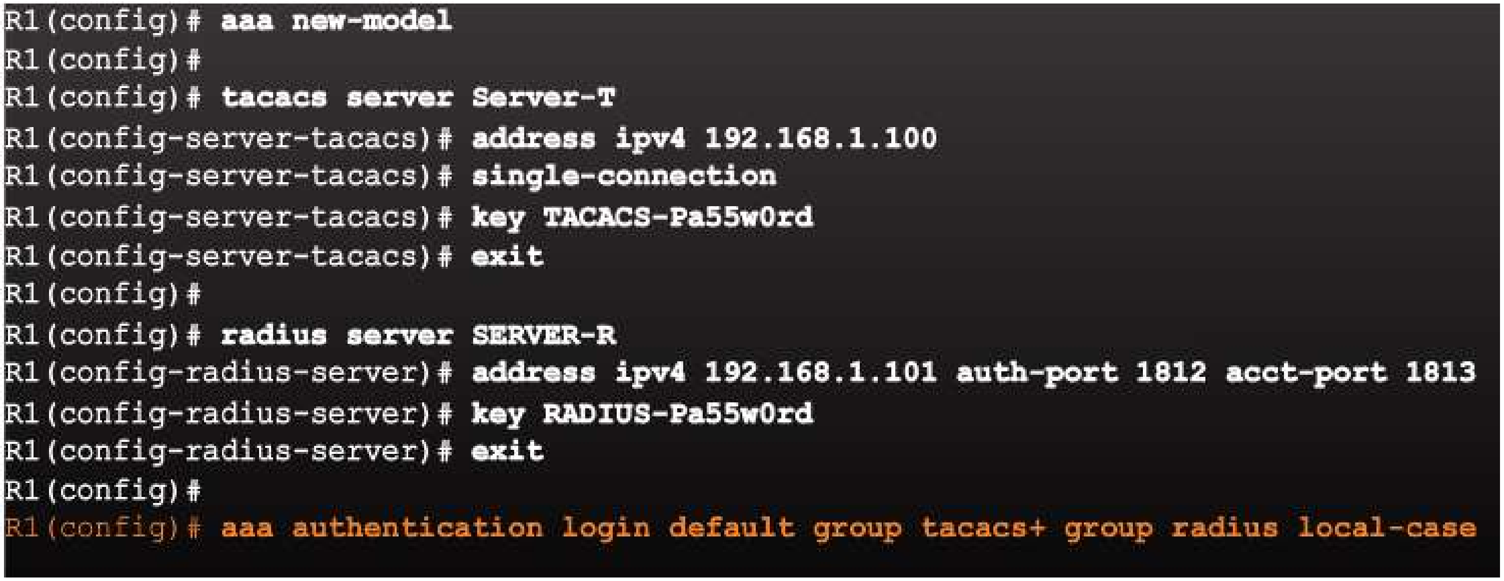
- Configuring a AAA RADIUS server



```
R1(config)# aaa new-model
R1(config)#
R1(config)# radius server SERVER-R
R1(config-radius-server)# address ipv4 192.168.1.100 auth-port 1812 acct-port 1813
R1(config-radius-server)# key RADIUS-Pa55w0rd
R1(config-radius-server)# exit
R1(config)#
```

Configure Authentication to Use the AAA Server

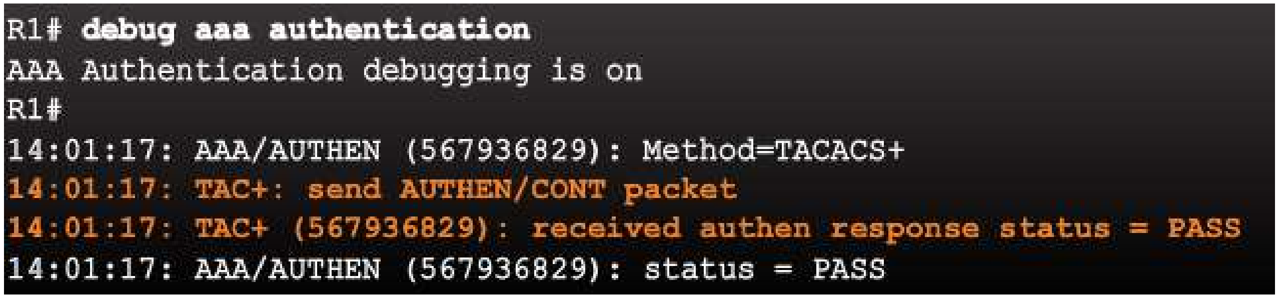
Configure Server-Based AAA Authentication



```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs server Server-T
R1(config-server-tacacs)# address ipv4 192.168.1.100
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key TACACS-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)#
R1(config)# radius server SERVER-R
R1(config-radius-server)# address ipv4 192.168.1.101 auth-port 1812 acct-port 1813
R1(config-radius-server)# key RADIUS-Pa55w0rd
R1(config-radius-server)# exit
R1(config)#
R1(config)# aaa authentication login default group tacacs+ group radius local-case
```

Monitoring Authentication Traffic

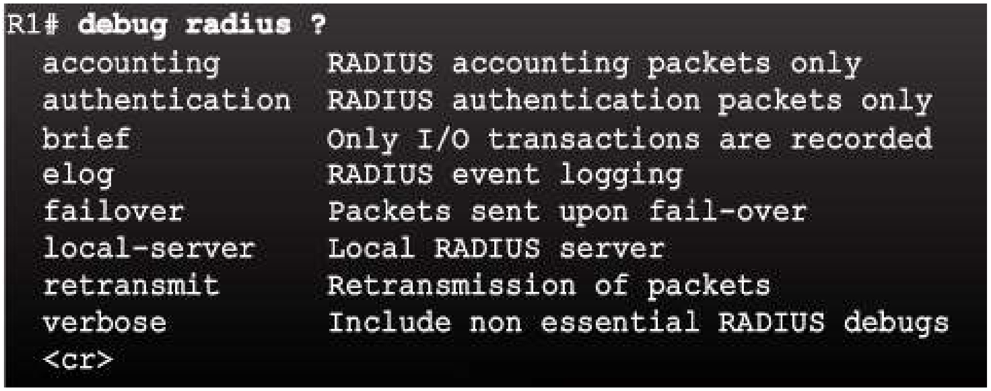
Debugging Server-Based AAA Authentication



```
R1# debug aaa authentication
AAA Authentication debugging is on
R1#
14:01:17: AAA/AUTHEN (567936829): Method=TACACS+
14:01:17: TAC+: send AUTHEN/CONT packet
14:01:17: TAC+ (567936829): received authen response status = PASS
14:01:17: AAA/AUTHEN (567936829): status = PASS
```

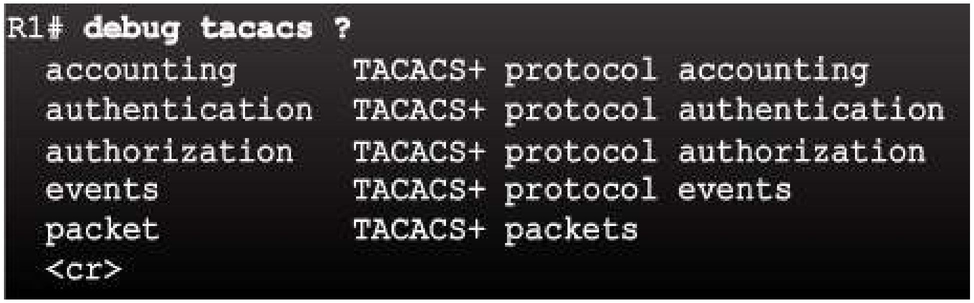
Debugging TACACS+ and RADIUS

Troubleshooting RADIUS



```
R1# debug radius ?
  accounting      RADIUS accounting packets only
  authentication  RADIUS authentication packets only
  brief           Only I/O transactions are recorded
  elog            RADIUS event logging
  failover        Packets sent upon fail-over
  local-server    Local RADIUS server
  retransmit      Retransmission of packets
  verbose         Include non essential RADIUS debugs
  <cr>
```

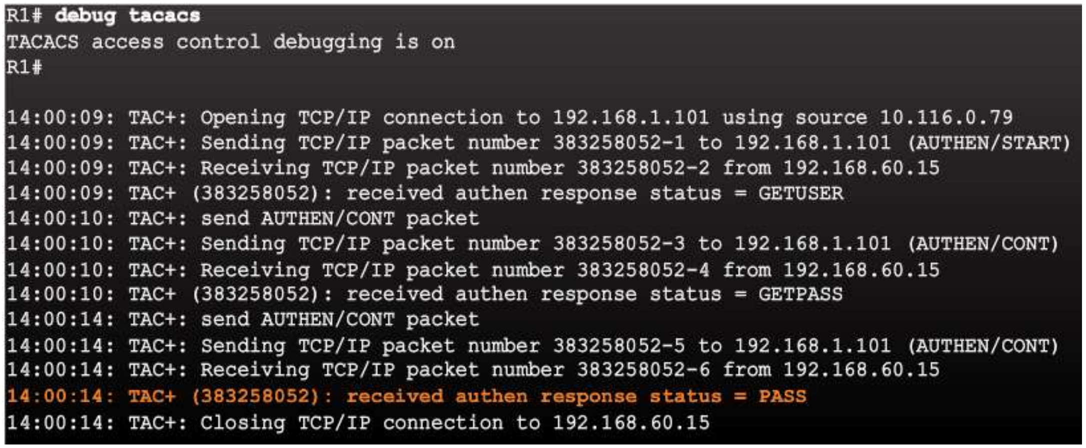
Troubleshooting TACACS+



```
R1# debug tacacs ?
  accounting      TACACS+ protocol accounting
  authentication  TACACS+ protocol authentication
  authorization   TACACS+ protocol authorization
  events          TACACS+ protocol events
  packet          TACACS+ packets
  <cr>
```

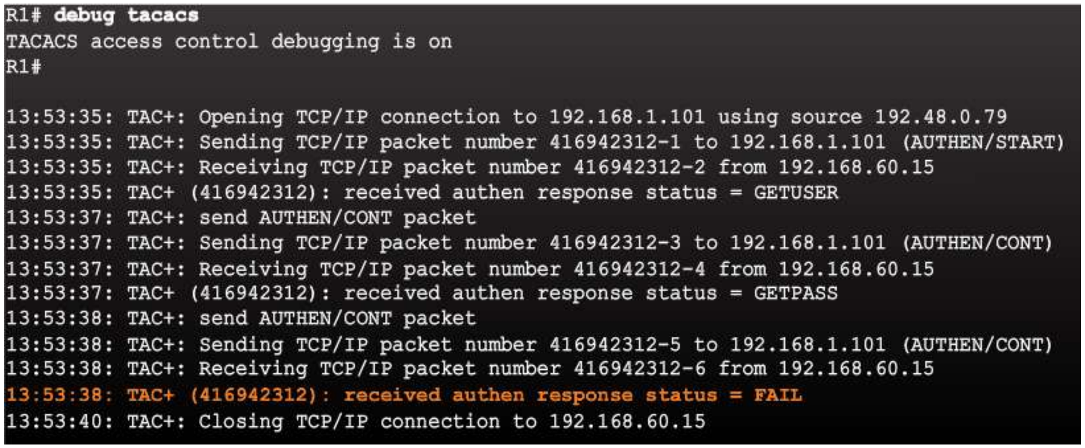
Debugging TACACS+ Example

Authentication Success



```
R1# debug tacacs
TACACS access control debugging is on
R1#

14:00:09: TAC+: Opening TCP/IP connection to 192.168.1.101 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.1.101 (AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.1.101 (AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.1.101 (AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

Authentication Failure



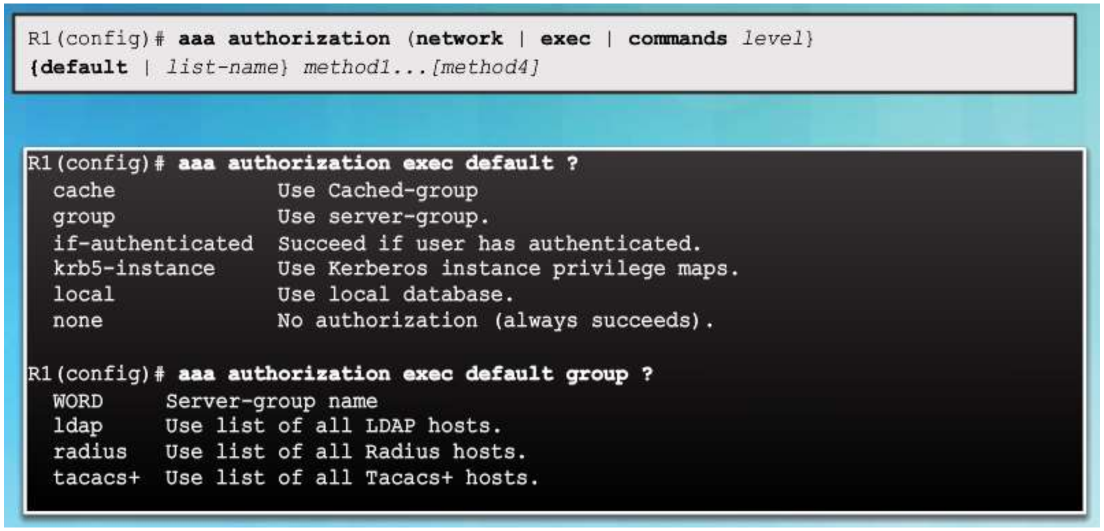
```
R1# debug tacacs
TACACS access control debugging is on
R1#

13:53:35: TAC+: Opening TCP/IP connection to 192.168.1.101 using source 192.48.0.79
13:53:35: TAC+: Sending TCP/IP packet number 416942312-1 to 192.168.1.101 (AUTHEN/START)
13:53:35: TAC+: Receiving TCP/IP packet number 416942312-2 from 192.168.60.15
13:53:35: TAC+ (416942312): received authen response status = GETUSER
13:53:37: TAC+: send AUTHEN/CONT packet
13:53:37: TAC+: Sending TCP/IP packet number 416942312-3 to 192.168.1.101 (AUTHEN/CONT)
13:53:37: TAC+: Receiving TCP/IP packet number 416942312-4 from 192.168.60.15
13:53:37: TAC+ (416942312): received authen response status = GETPASS
13:53:38: TAC+: send AUTHEN/CONT packet
13:53:38: TAC+: Sending TCP/IP packet number 416942312-5 to 192.168.1.101 (AUTHEN/CONT)
13:53:38: TAC+: Receiving TCP/IP packet number 416942312-6 from 192.168.60.15
13:53:38: TAC+ (416942312): received authen response status = FAIL
13:53:40: TAC+: Closing TCP/IP connection to 192.168.60.15
```

Server-Based AAA Authorization and Accounting

- Authorization allows and disallows authenticated users access to certain areas and programs on the network.
- The TACACS+ protocol allows the separation of authentication from authorization.
- The RADIUS protocol does not separate authentication from authorization.
- A router can be configured to restrict the user to performing only certain functions after successful authentication.
- Authorization can be configured for both character mode (exec authorization) and packet mode (network authorization).

AAA Authorization Configuration with CLI

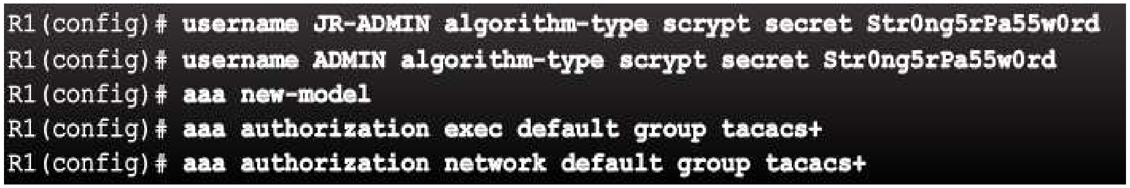
Authorization Method Lists



```
R1(config)# aaa authorization {network | exec | commands level}
{default | list-name} method1...[method4]
```

```
R1(config)# aaa authorization exec default ?
  cache              Use Cached-group
  group              Use server-group.
  if-authenticated   Succeed if user has authenticated.
  krb5-instance      Use Kerberos instance privilege maps.
  local              Use local database.
  none               No authorization (always succeeds).

R1(config)# aaa authorization exec default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
```

AAA Authorization Example

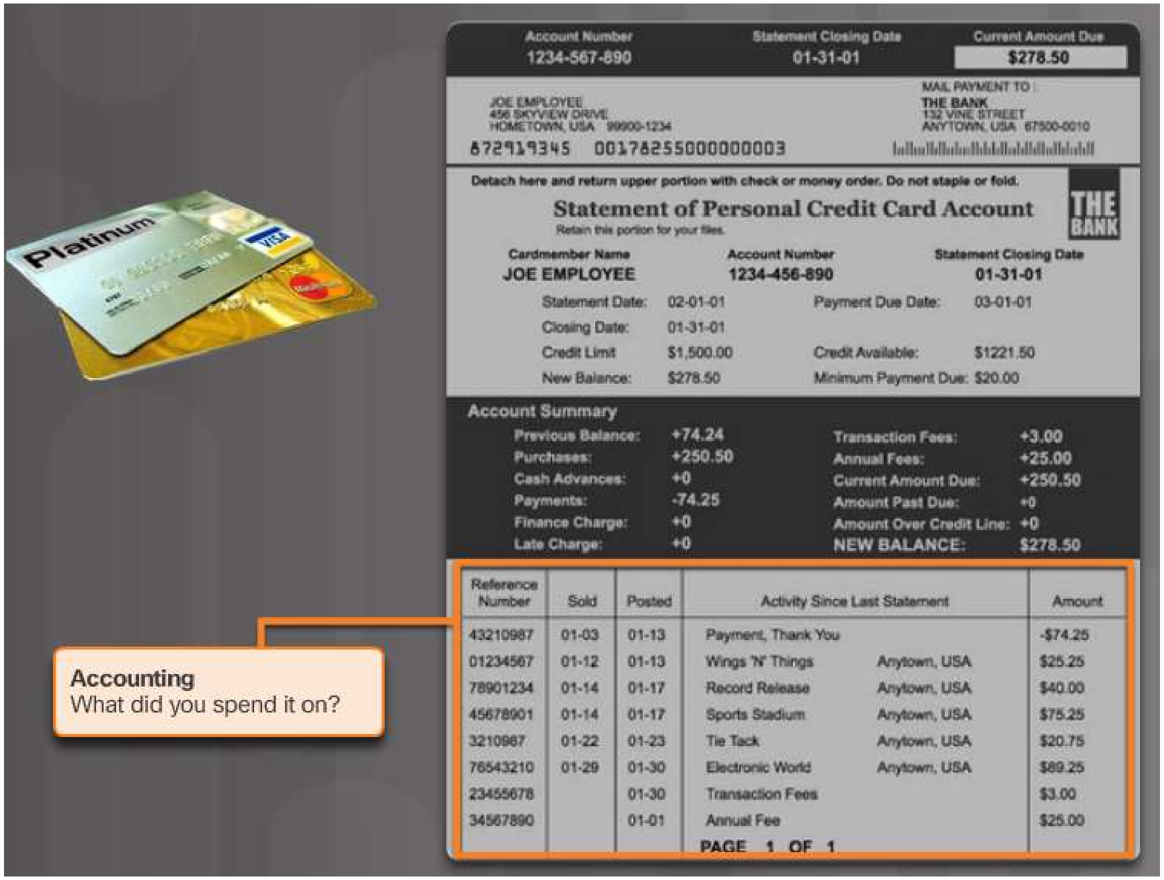


```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
```

Server-Based AAA Accounting

- Companies often must track resources that individuals or groups use.
- AAA accounting enables usage tracking, such as dial-in access, to log the data gathered to a database, and to produce reports on the data gathered.
- One security issue (addressed by accounting) is the creation of a user list and the time of day a user dialed into the system.
- Another reason to implement accounting is to create a list of changes occurring on the network, the user that made the changes, and the exact nature of the changes.

Server-based AAA Accounting


Platinum
VISA
THE BANK

Accounting
What did you spend it on?

Account Number	Statement Closing Date	Current Amount Due
1234-567-890	01-31-01	$278.50

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99900-1234

MAIL PAYMENT TO :
THE BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

872919345 00178255000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

Statement of Personal Credit Card Account

Retain this portion for your files.

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	01-31-01

Statement Date:	02-01-01	Payment Due Date:	03-01-01
Closing Date:	01-31-01		
Credit Limit	$1,500.00	Credit Available:	$1221.50
New Balance:	$278.50	Minimum Payment Due:	$20.00

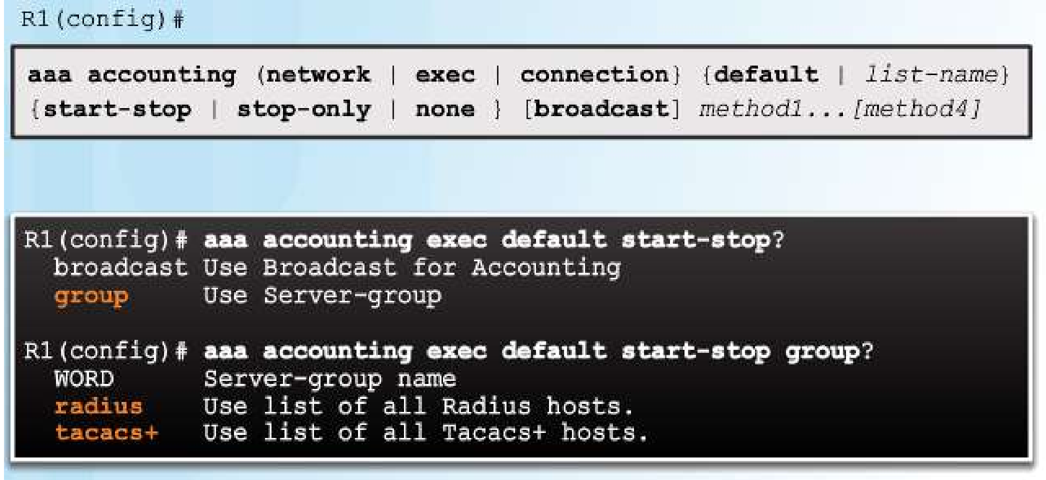
Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	$278.50

Reference Number	Sold	Posted	Activity Since Last Statement		Amount
43210987	01-03	01-13	Payment, Thank You		-$74.25
01234567	01-12	01-13	Wings 'N' Things	Anytown, USA	$25.25
78901234	01-14	01-17	Record Release	Anytown, USA	$40.00
45678901	01-14	01-17	Sports Stadium	Anytown, USA	$75.25
3210987	01-22	01-23	Tie Tack	Anytown, USA	$20.75
76543210	01-29	01-30	Electronic World	Anytown, USA	$89.25
23455678		01-30	Transaction Fees		$3.00
34567890		01-01	Annual Fee		$25.00
			PAGE 1 OF 1		

AAA Accounting Configuration with CLI

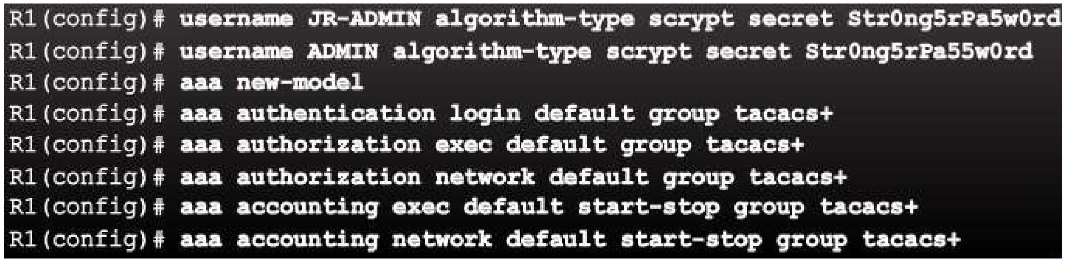
Accounting Method Lists



```
R1(config)#

aaa accounting {network | exec | connection} {default | list-name}
{start-stop | stop-only | none } [broadcast] method1...[method4]
```

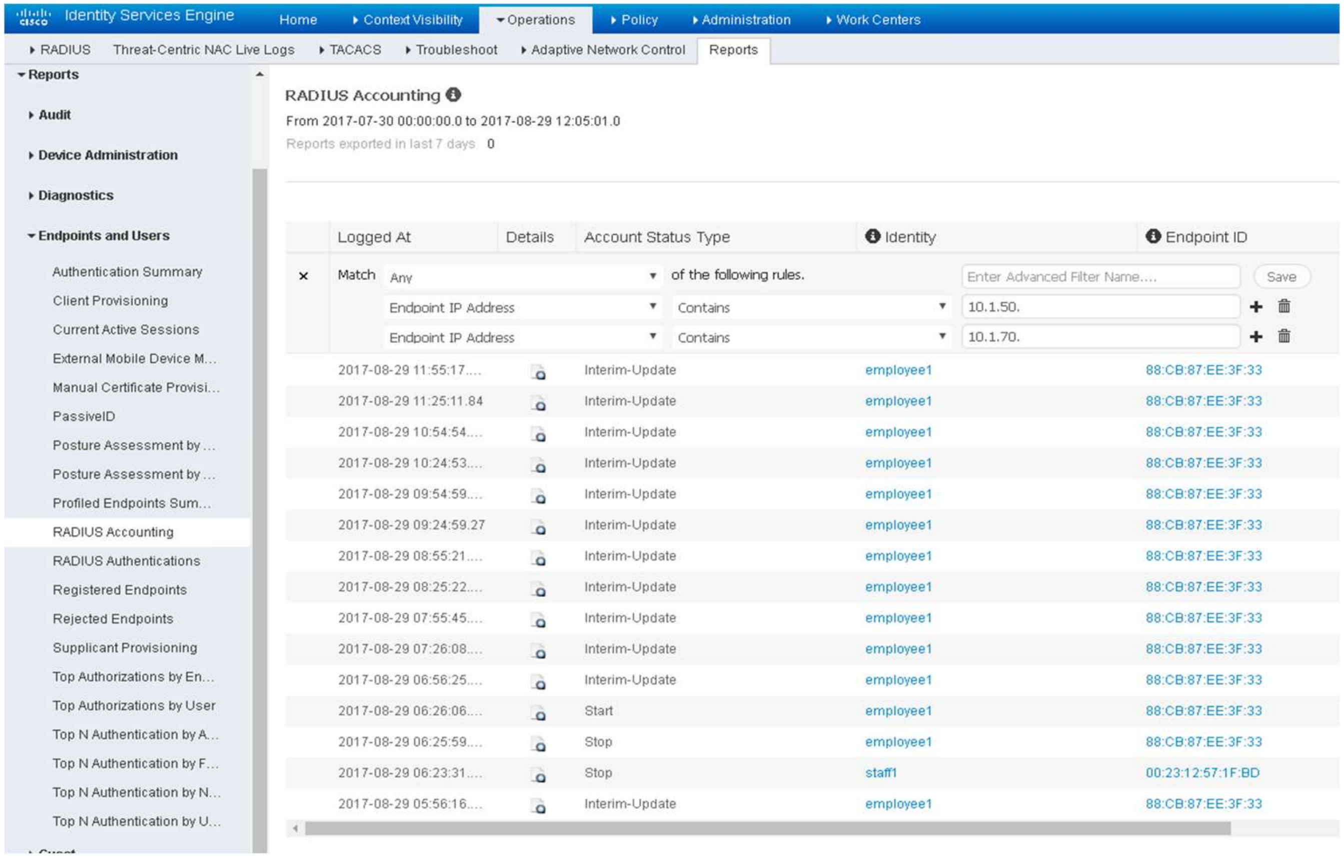
```
R1(config)# aaa accounting exec default start-stop?
  broadcast Use Broadcast for Accounting
  group     Use Server-group

R1(config)# aaa accounting exec default start-stop group?
  WORD      Server-group name
  radius    Use list of all Radius hosts.
  tacacs+   Use list of all Tacacs+ hosts.
```

AAA Accounting Example



```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa5w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
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+
```

Accounting Logs (Cisco ISE)



RADIUS Accounting

From 2017-07-30 00:00:00.0 to 2017-08-29 12:05:01.0

Reports exported in last 7 days 0

Match Any of the following rules.

Enter Advanced Filter Name.... Save

Endpoint IP Address Contains 10.1.50.

Endpoint IP Address Contains 10.1.70.

Logged At	Details	Account Status Type	Identity	Endpoint ID
2017-08-29 11:55:17....		Interim-Update	employee1	88:CB:87:EE:3F:33
2017-08-29 11:25:11.84		Interim-Update	employee1	88:CB:87:EE:3F:33
2017-08-29 10:54:54....		Interim-Update	employee1	88:CB:87:EE:3F:33
2017-08-29 10:24:53....		Interim-Update	employee1	88:CB:87:EE:3F:33
2017-08-29 09:54:59....		Interim-Update	employee1	88:CB:87:EE:3F:33
2017-08-29 09:24:59.27		Interim-Update	employee1	88:CB:87:EE:3F:33
2017-08-29 08:55:21....		Interim-Update	employee1	88:CB:87:EE:3F:33
2017-08-29 08:25:22....		Interim-Update	employee1	88:CB:87:EE:3F:33
2017-08-29 07:55:45....		Interim-Update	employee1	88:CB:87:EE:3F:33
2017-08-29 07:26:08....		Interim-Update	employee1	88:CB:87:EE:3F:33
2017-08-29 06:56:25....		Interim-Update	employee1	88:CB:87:EE:3F:33
2017-08-29 06:26:06....		Start	employee1	88:CB:87:EE:3F:33
2017-08-29 06:25:59....		Stop	employee1	88:CB:87:EE:3F:33
2017-08-29 06:23:31....		Stop	staff1	00:23:12:57:1F:BD
2017-08-29 05:56:16....		Interim-Update	employee1	88:CB:87:EE:3F:33

Summary

- The AAA protocol provides a scalable framework for enabling administrative access.
- AAA controls who is allowed to connect to the network, what they are allowed to do, and tracks records of what was done.
- In small or simple networks, AAA authentication can be implemented using the local database.
- In larger or complex networks, AAA authentication should be implemented using server-based AAA.
- AAA servers can use RADIUS or TACACS+ protocols to communicate with client routers.
- The Cisco ACS can be used to provide AAA server services.
- Local AAA and server-based AAA authentication can be configured using the CLI or CCP.