Computer Security

Labs

Mahmoud Abdel-Salam
Faculty of Computer and Information
Mansoura university
IT department
mahmoud20@mans.edu.eg

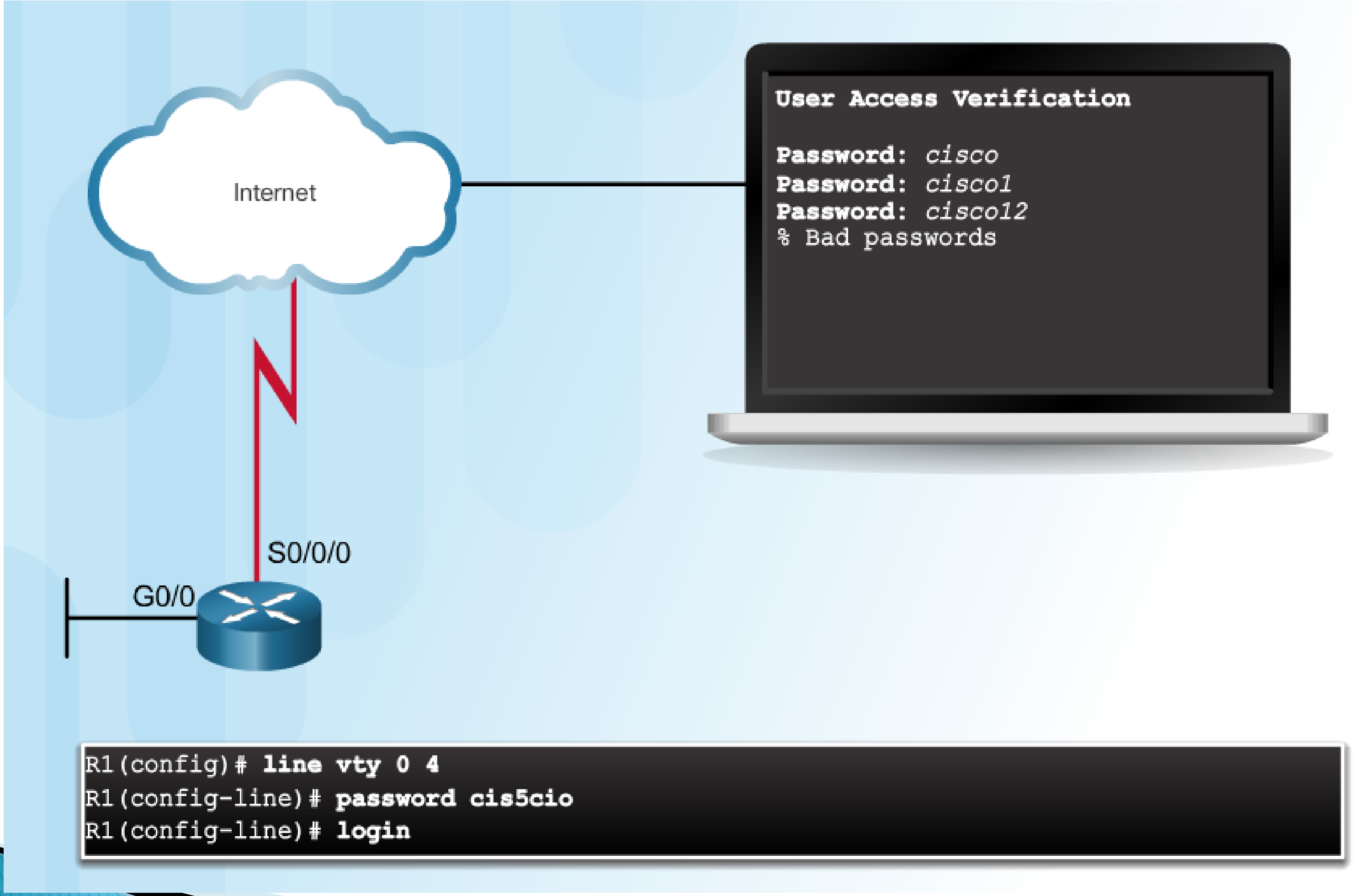
Outlines

- AAA protocol
- Dot 802.1x port authentication protocol.
- Firewall examples.

AAA

Authentication without AAA

Telnet is Vulnerable to Brute-Force Attacks



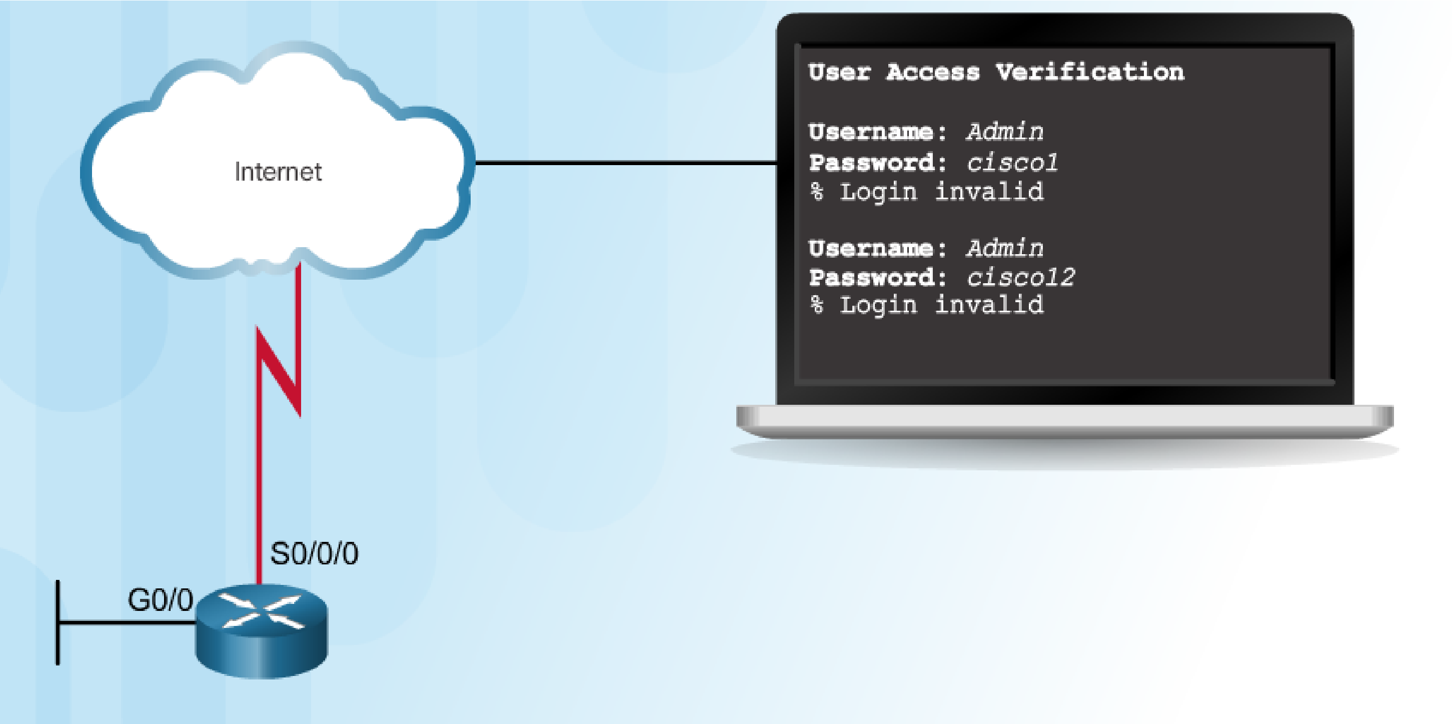
```
User Access Verification

Password: cisco
Password: cisco1
Password: cisco12
% Bad passwords
```

```
R1(config)# line vty 0 4
R1(config-line)# password cis5cio
R1(config-line)# login
```

Authentication without AAA (Cont.)

SSH and Local Database Method



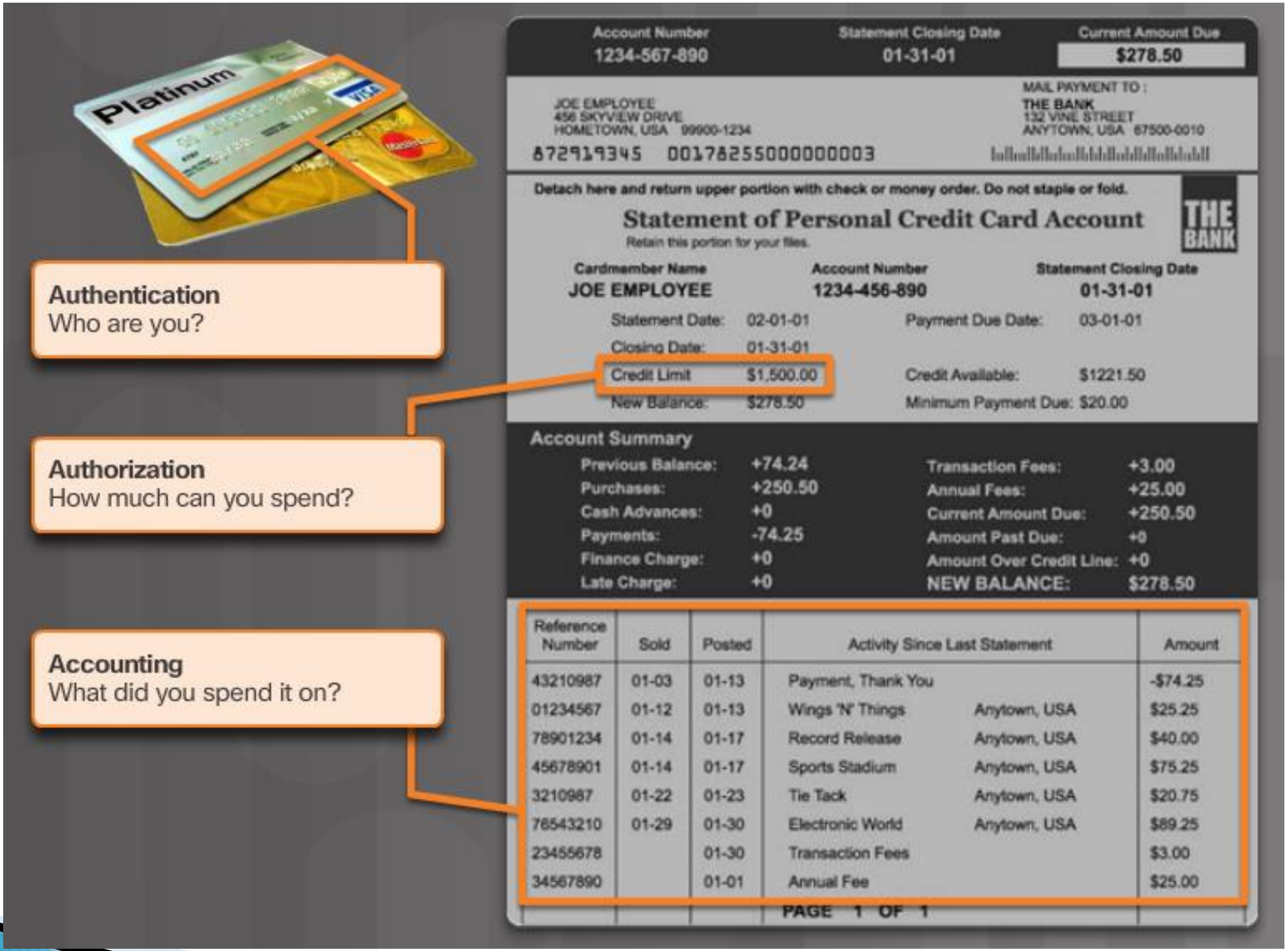
```
User Access Verification

Username: Admin
Password: cisco1
% Login invalid

Username: Admin
Password: cisco12
% Login invalid
```

```
R1(config)# ip domain-name cisco-academy.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

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 0017825500000003

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

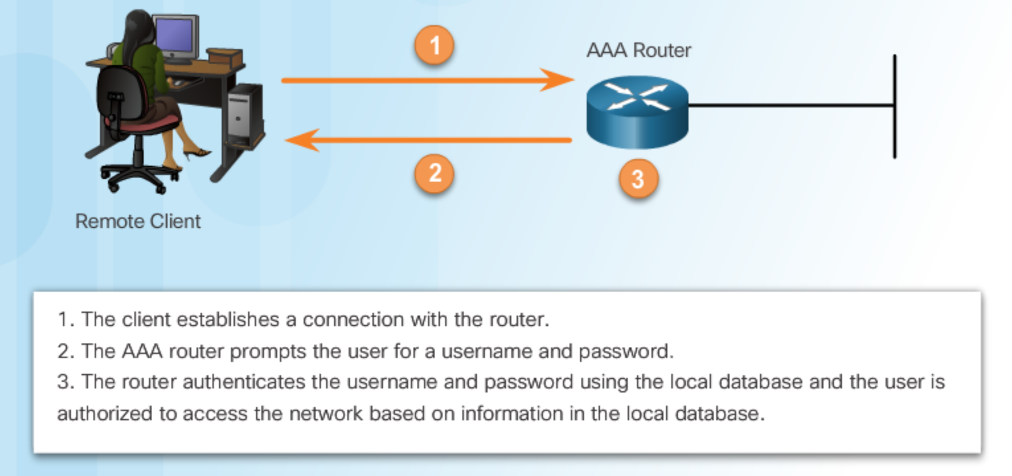
Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	$278.50

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

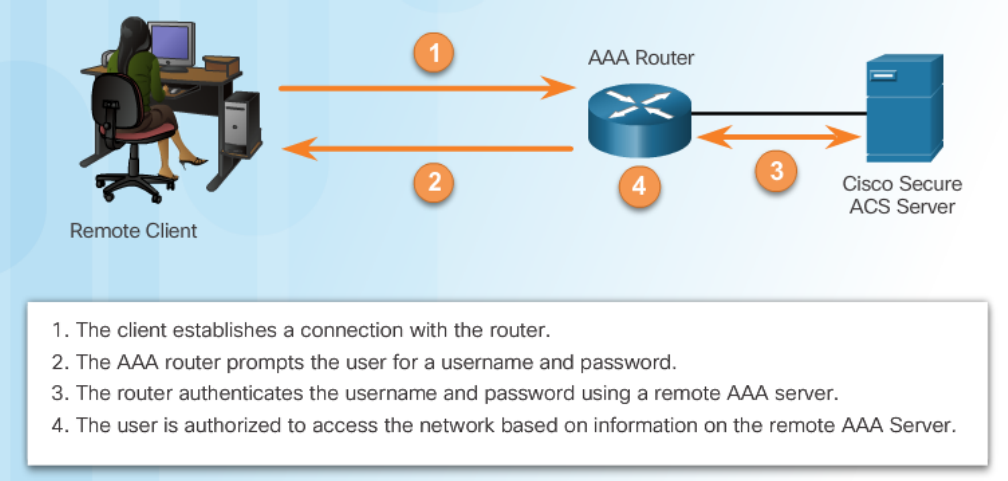
Authentication Modes

Local AAA
Authentication



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.

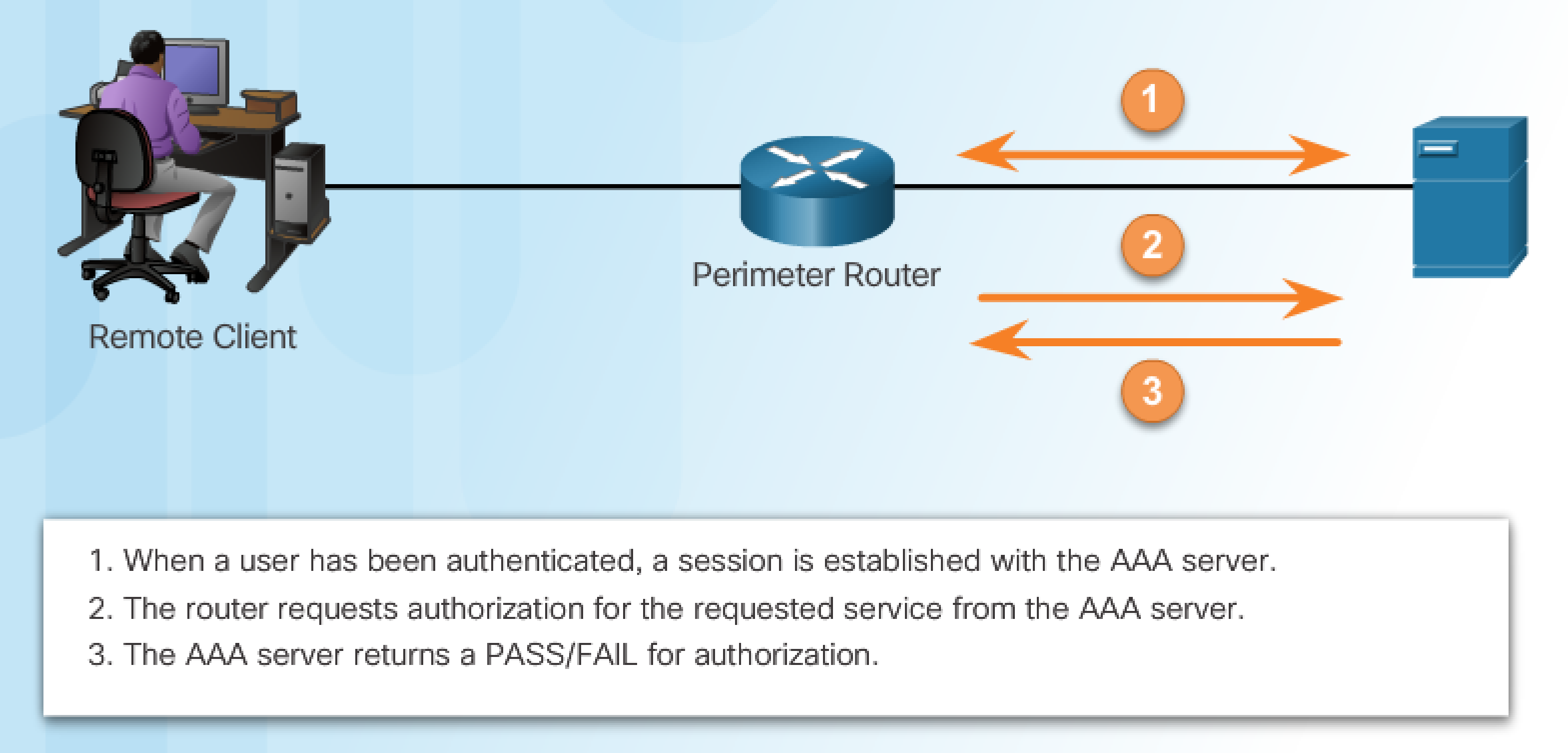
Server-Based
AAA Authentication



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.

Authorization

AAA Authorization



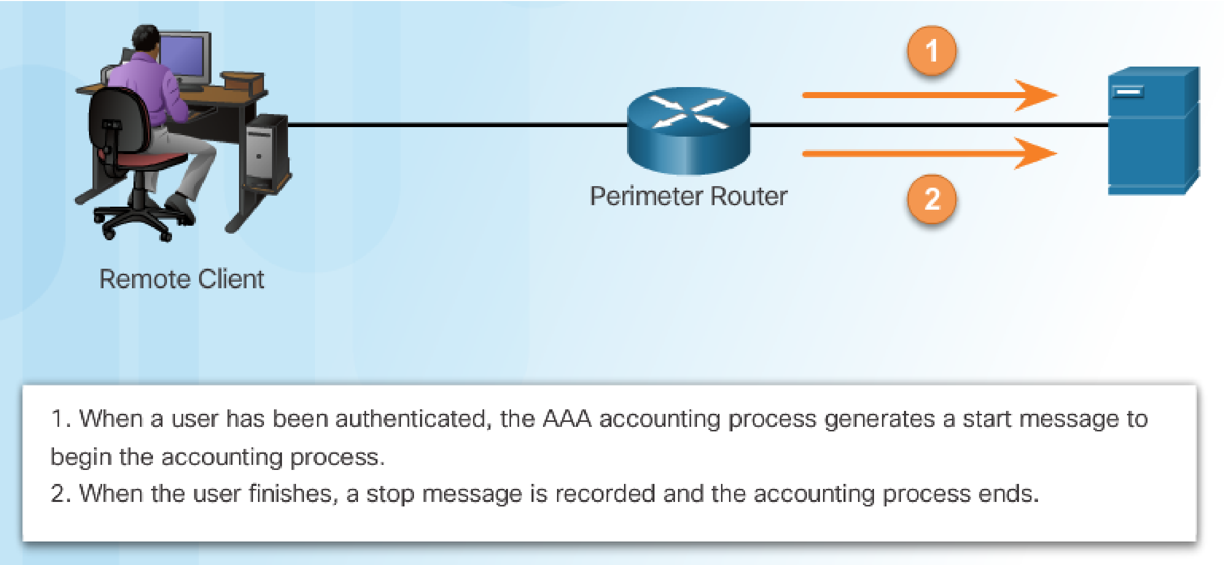
1. When a user has been authenticated, a session is established with the AAA server.
2. The router requests authorization for the requested service from the AAA server.
3. The AAA server returns a PASS/FAIL for authorization.

Accounting

Types of accounting information:

- Network
- Connection
- EXEC
- System
- Command
- Resource

AAA Accounting

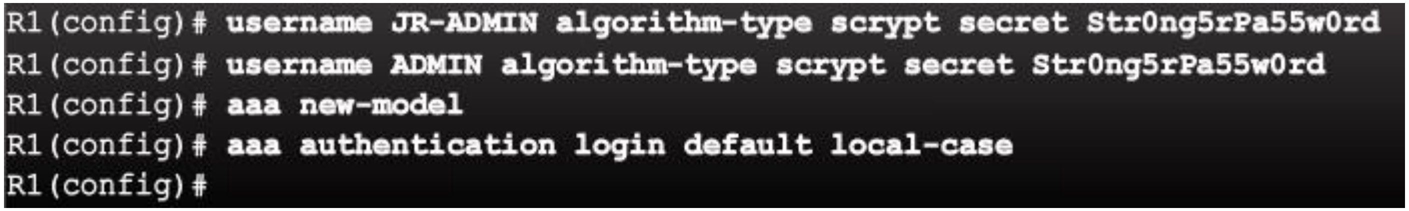


1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded and the accounting process ends.

Local AAA Authentication

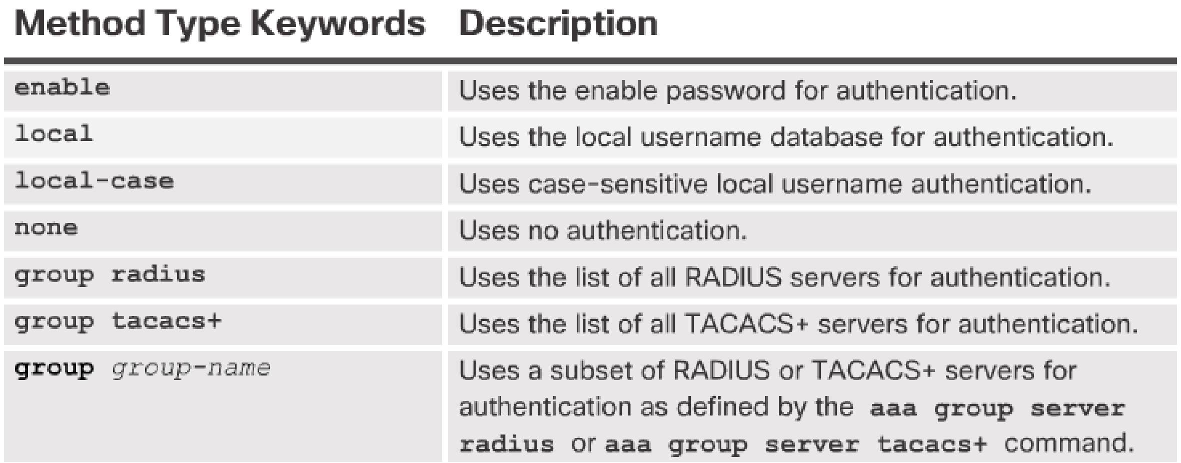
Authenticating Administrative Access

1. Add usernames and passwords to the local router database for users that need administrative access to the router.
2. Enable AAA globally on the router.
3. Configure AAA parameters on the router.
4. Confirm and troubleshoot the AAA configuration.

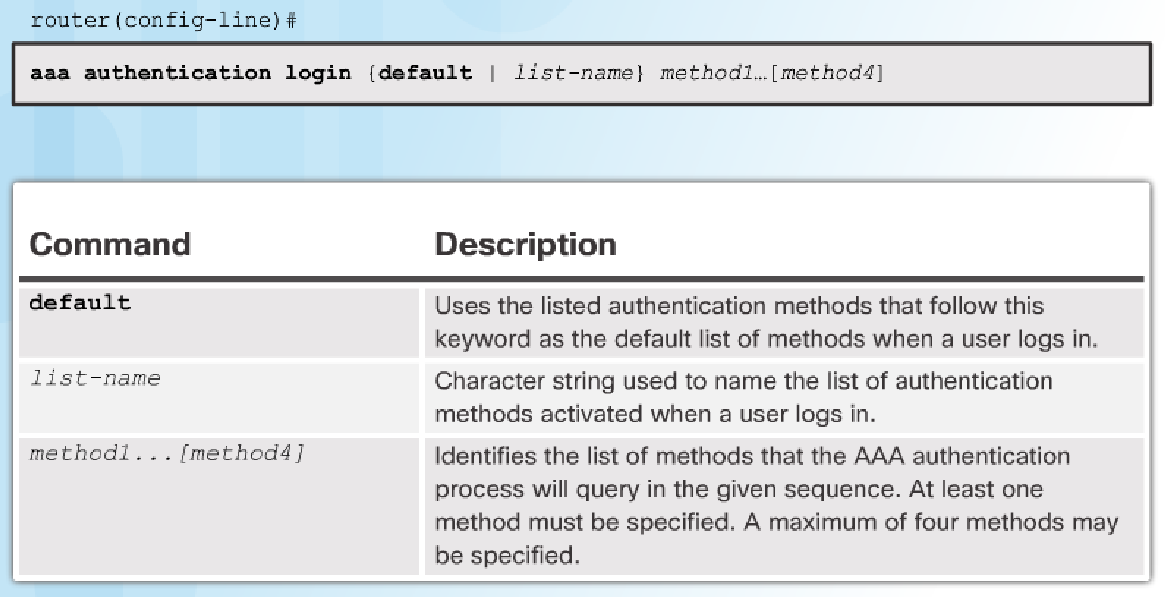


```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case
R1(config)#
```

Authentication Methods



Method Type Keywords	Description
`enable`	Uses the enable password for authentication.
`local`	Uses the local username database for authentication.
`local-case`	Uses case-sensitive local username authentication.
`none`	Uses no 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.

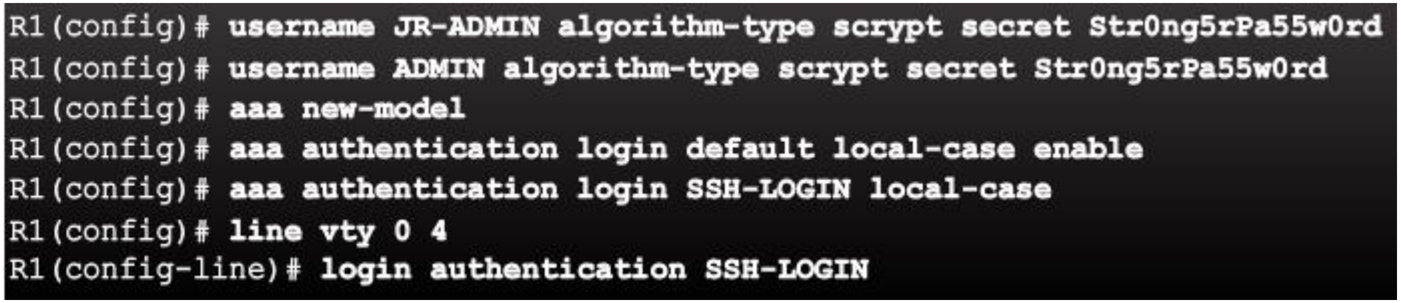


```
router(config-line)#
aaa authentication login {default | list-name} method1…[method4]
```

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.

Default and Named Methods

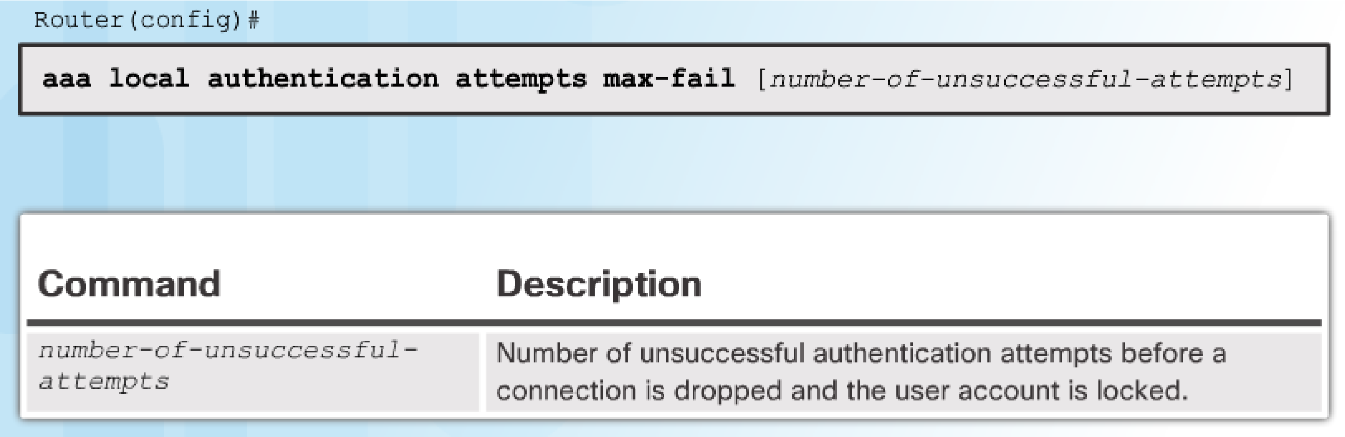
Example Local AAA Authentication



```
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
```

Fine-Tuning the Authentication Configuration

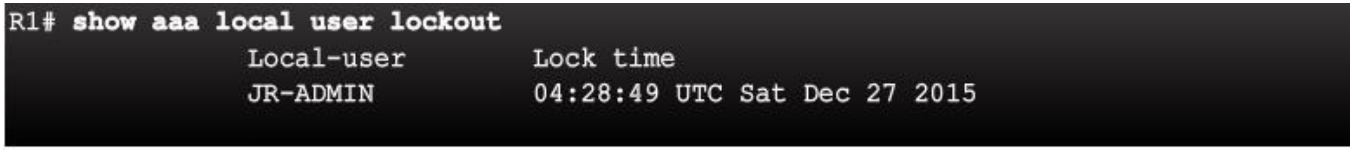
Command Syntax



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

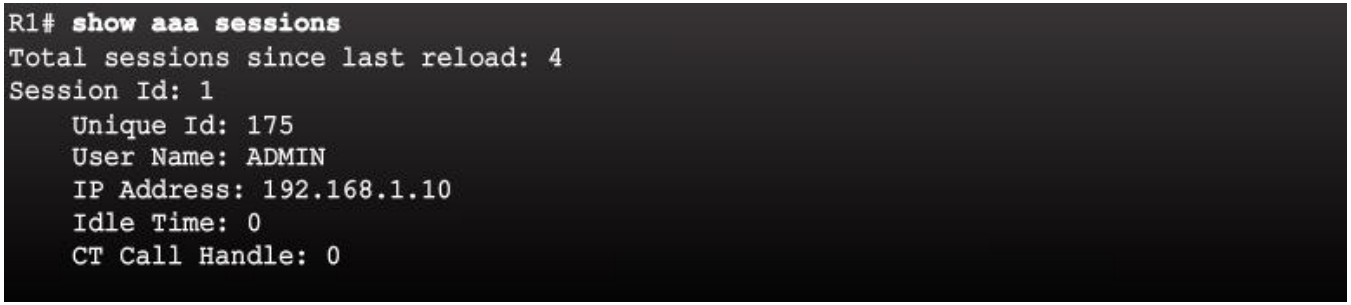
Command	Description
number-of-unsuccessful-attempts	Number of unsuccessful authentication attempts before a connection is dropped and the user account is locked.

Display Locked Out Users



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

Show Unique ID of a Session

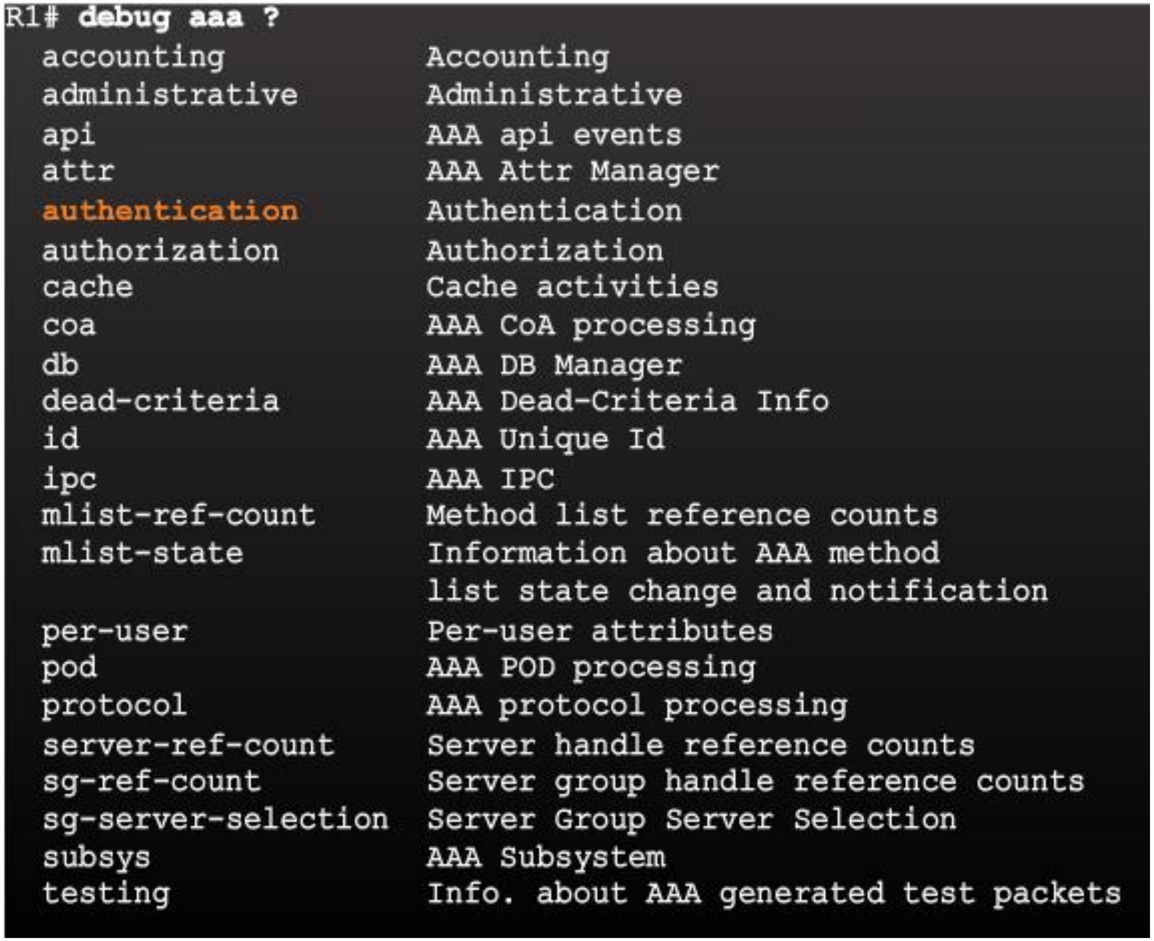


```
R1# show aaa sessions
Total sessions since last reload: 4
Session Id: 1
    Unique Id: 175
    User Name: ADMIN
    IP Address: 192.168.1.10
    Idle Time: 0
    CT Call Handle: 0
```

Troubleshooting Local AAA Authentication

Debug Options

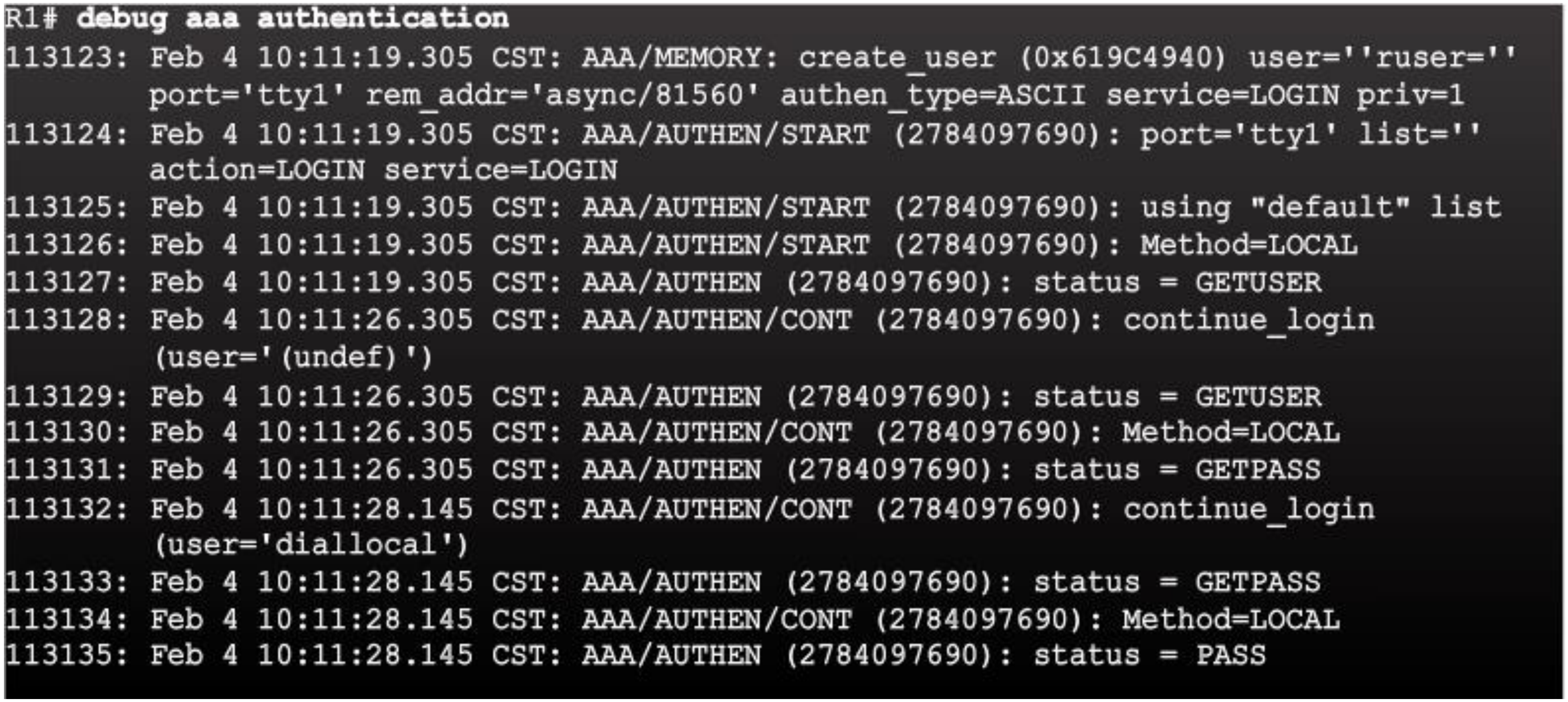
Debug Local AAA Authentication



```
R1# debug aaa ?
  accounting              Accounting
  administrative          Administrative
  api                     AAA api events
  attr                    AAA Attr Manager
  authentication          Authentication
  authorization           Authorization
  cache                   Cache activities
  coa                     AAA CoA processing
  db                      AAA DB Manager
  dead-criteria           AAA Dead-Criteria Info
  id                      AAA Unique Id
  ipc                     AAA IPC
  mlist-ref-count         Method list reference counts
  mlist-state             Information about AAA method
                          list state change and notification
  per-user                Per-user attributes
  pod                     AAA POD processing
  protocol                AAA protocol processing
  server-ref-count        Server handle reference counts
  sg-ref-count            Server group handle reference counts
  sg-server-selection     Server Group Server Selection
  subsys                  AAA Subsystem
  testing                 Info. about AAA generated test packets
```

Debugging AAA Authentication

Understanding Debug Output



```
R1# debug aaa authentication
113123: Feb 4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user=''ruser=''
        port='tty1' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113124: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): port='tty1' list=''
        action=LOGIN service=LOGIN
113125: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): using "default" list
113126: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): Method=LOCAL
113127: Feb 4 10:11:19.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113128: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): continue_login
        (user='(undef)')
113129: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113130: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113131: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETPASS
113132: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): continue_login
        (user='diallocal')
113133: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = GETPASS
113134: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113135: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = PASS
```