CCNA Security

Chapter Three

Authentication, Authorization, and Accounting

Lesson Planning

- This lesson should take 3-6 hours to present
- The lesson should include lecture, demonstrations, discussion and assessment
- The lesson can be taught in person or using remote instruction

Major Concepts

- Local Authentication
- Enhancements to Local Authentication
- Describe the purpose of AAA and the various implementation techniques
- Implement AAA using the local database
- Implement AAA using TACACS+ and RADIUS protocols
- Implement AAA Authorization and Accounting

Lesson Objectives

Upon completion of this lesson, the successful participant will be able to:

1. Describe the importance of AAA as it relates to authentication, authorization, and accounting
2. Configure AAA authentication using a local database
3. Configure AAA using a local database in SDM
4. Troubleshoot AAA using a local database
5. Explain server-based AAA
6. Describe and compare the TACACS+ and RADIUS protocols

Lesson Objectives

7. Describe the Cisco Secure ACS for Windows software
8. Describe how to configure Cisco Secure ACS for Windows as a TACACS+ server
9. Configure server-based AAA authentication on Cisco Routers using CLI
10. Configure server-based AAA authentication on Cisco Routers using SDM
11. Troubleshoot server-based AAA authentication using Cisco Secure ACS
12. Configure server-based AAA Authorization using Cisco Secure ACS
13. Configure server-based AAA Accounting using Cisco Secure ACS

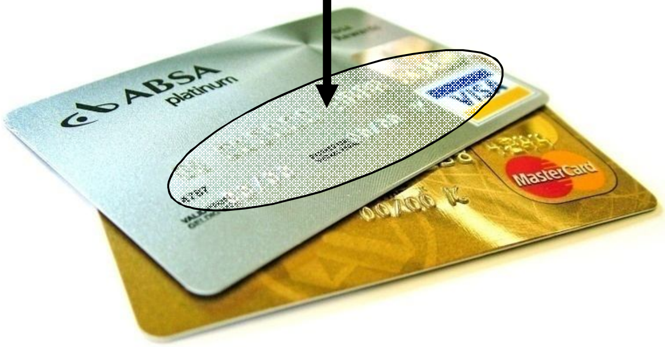
AAA Access Security

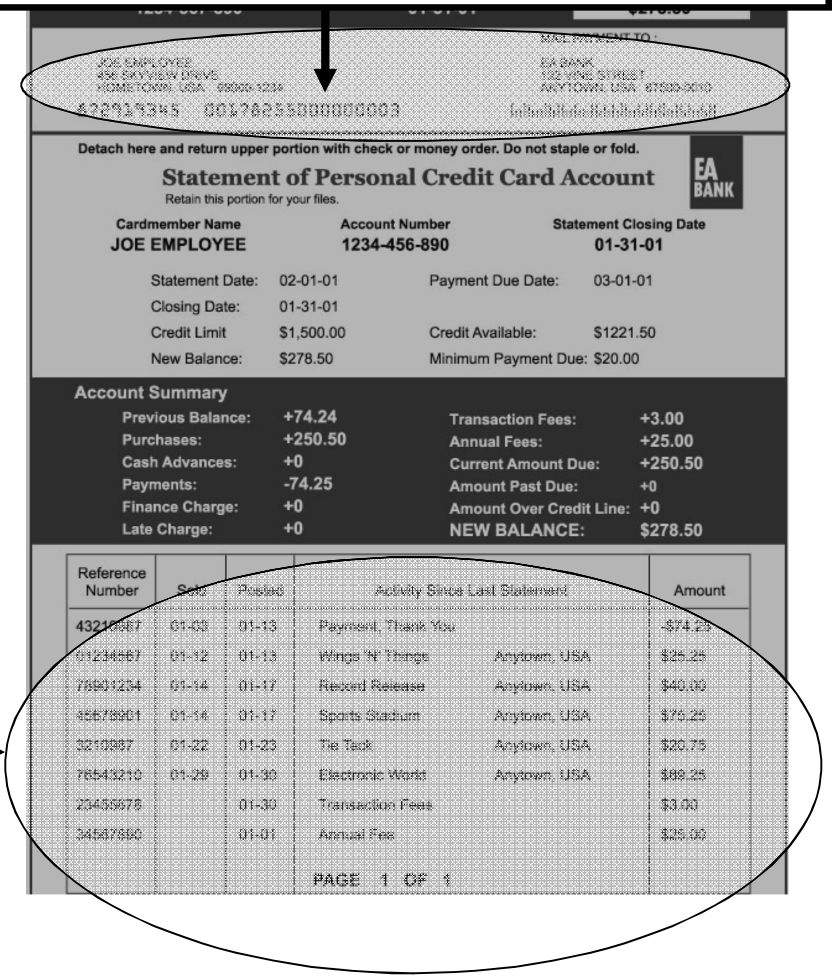
Authorization

which resources the user is allowed to access and which operations the user is allowed to perform?

Authentication

Who are you?





MAIL PAYMENT TO :

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA [illegible]

EA BANK
132 VINE STREET
ANYTOWN, USA [illegible]

A22919345 001782550000003

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.

EA BANK

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
23456678		01-30	Transaction Fees		$3.00
34567890		01-01	Annual Fee		$25.00

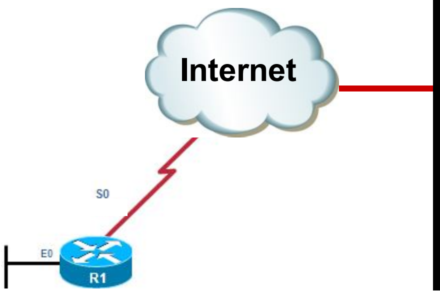
PAGE 1 OF 1

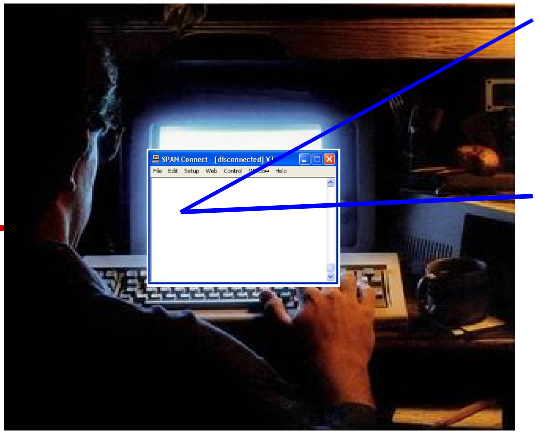
Accounting

What did you spend it on?

Authentication – Password-Only

Password-Only Method





```
User Access Verification

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

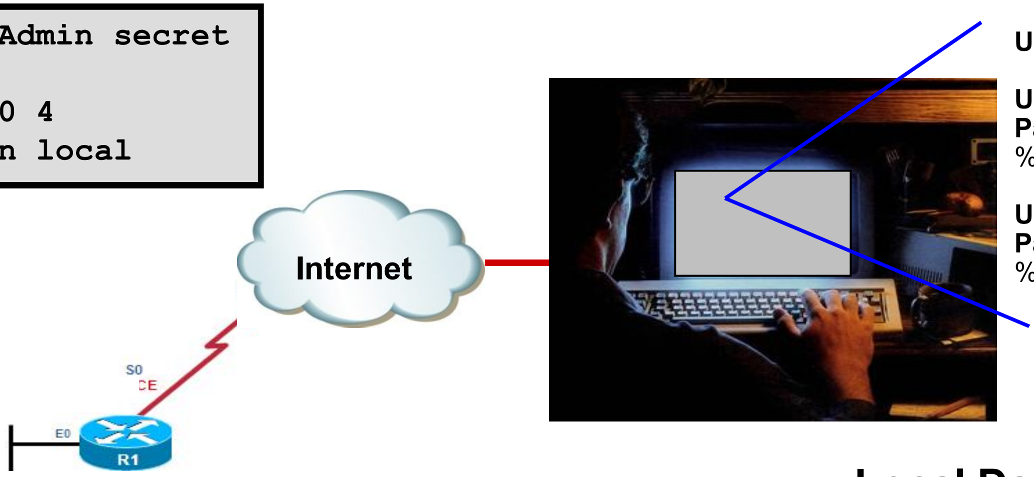
```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

- Uses a login and password combination on access lines
- Easiest to implement, but most unsecure method
- Vulnerable to brute-force attacks
- Provides no accountability

Authentication – Local Database

- Creates individual user account/password on each device
- Provides accountability
- User accounts must be configured locally on each device
- Provides no fallback authentication method

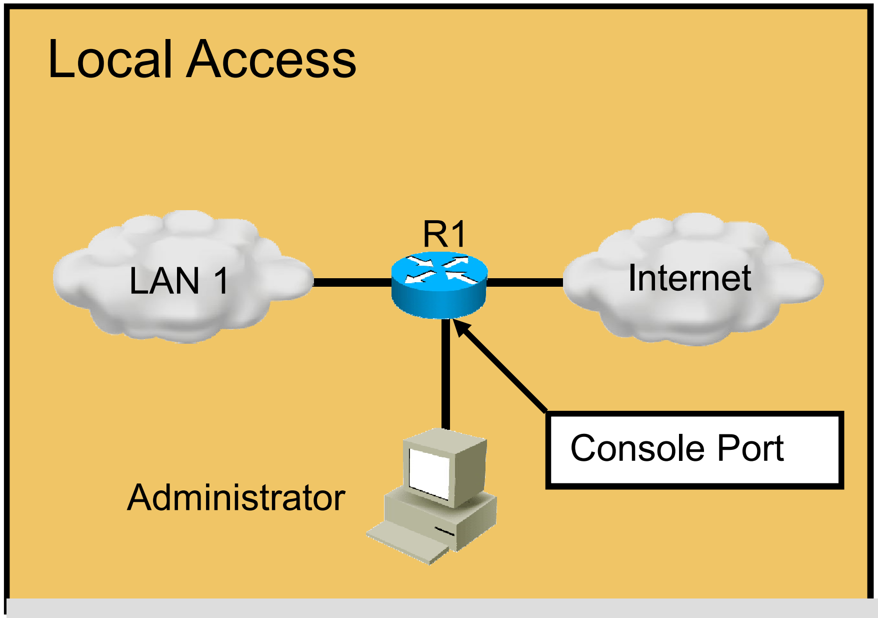
```
R1(config)# username Admin secret
Str0ng5rPa55w0rd
R1(config)# line vty 0 4
R1(config-line)# login local
```



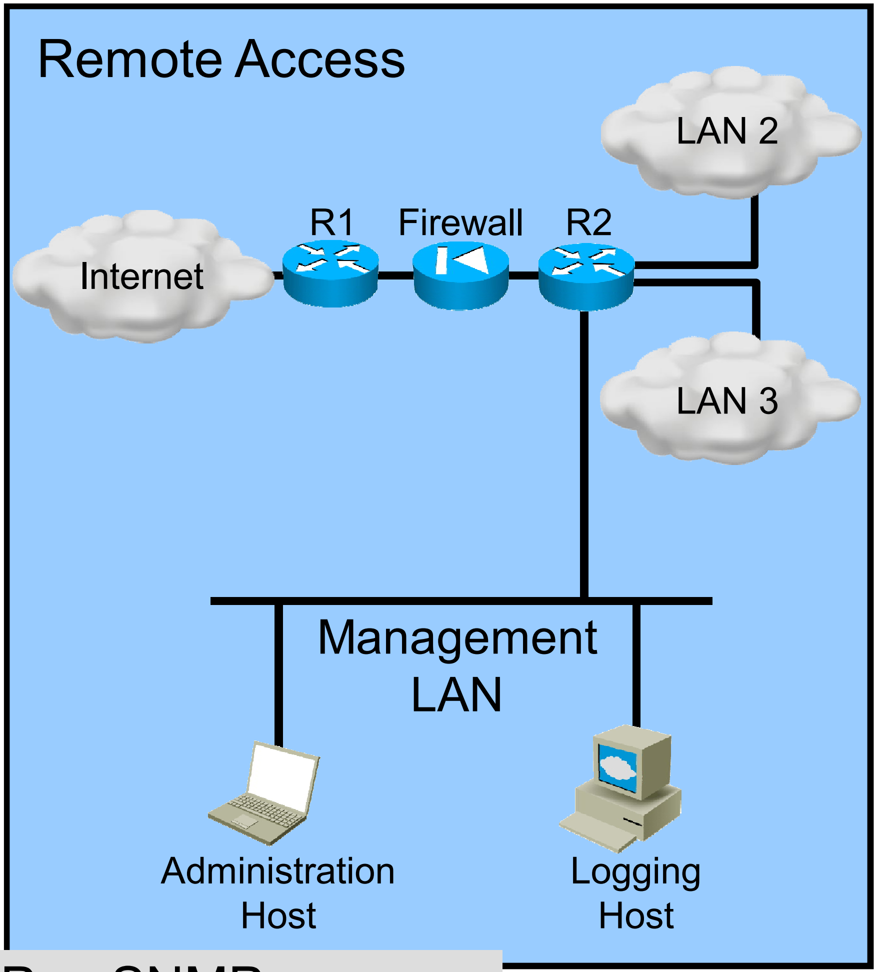
```
User Access Verification

Username: Admin
Password: cisco1
% Login invalid

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

Local Database Method

Local Versus Remote Access



Requires a direct connection to a console port using a computer running terminal emulation software

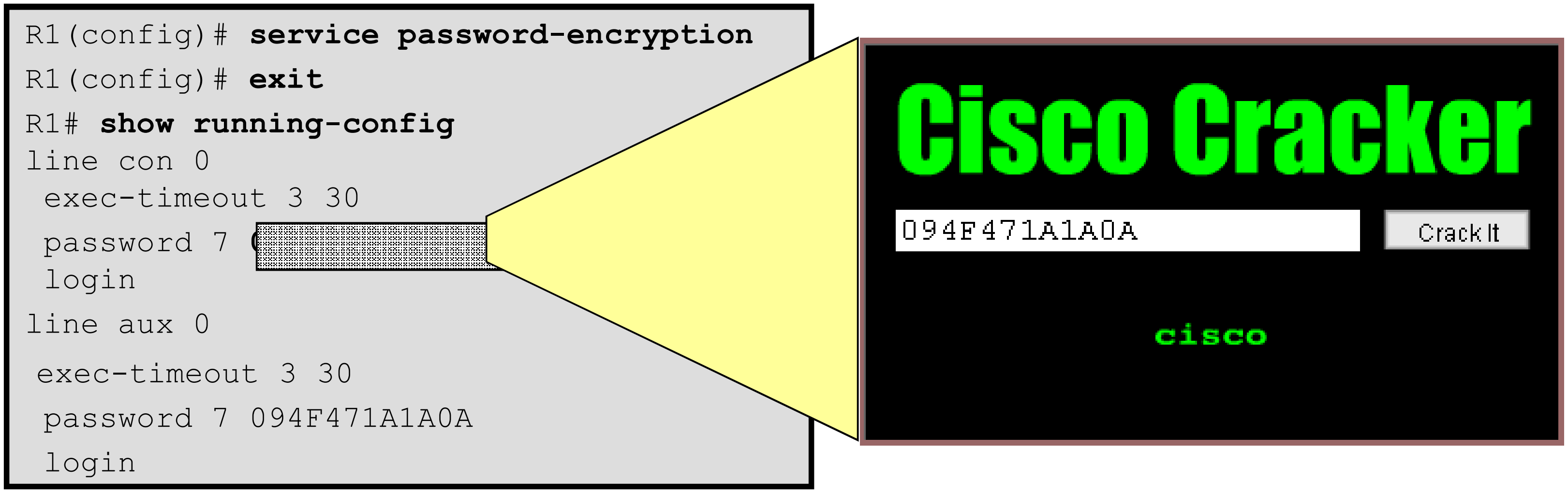


Uses Telnet, SSH HTTP or SNMP connections to the router from a computer

Password Security

To increase the security of passwords, use additional configuration parameters:

- Minimum password lengths should be enforced
- Unattended connections should be disabled
- All passwords in the configuration file should be encrypted



```
R1(config)# service password-encryption
R1(config)# exit
R1# show running-config
line con 0
 exec-timeout 3 30
 password 7
 login
line aux 0
 exec-timeout 3 30
 password 7 094F471A1A0A
 login
```

Cisco Cracker

094F471A1A0A

cisco

Passwords

An acceptable password length is 10 or more characters

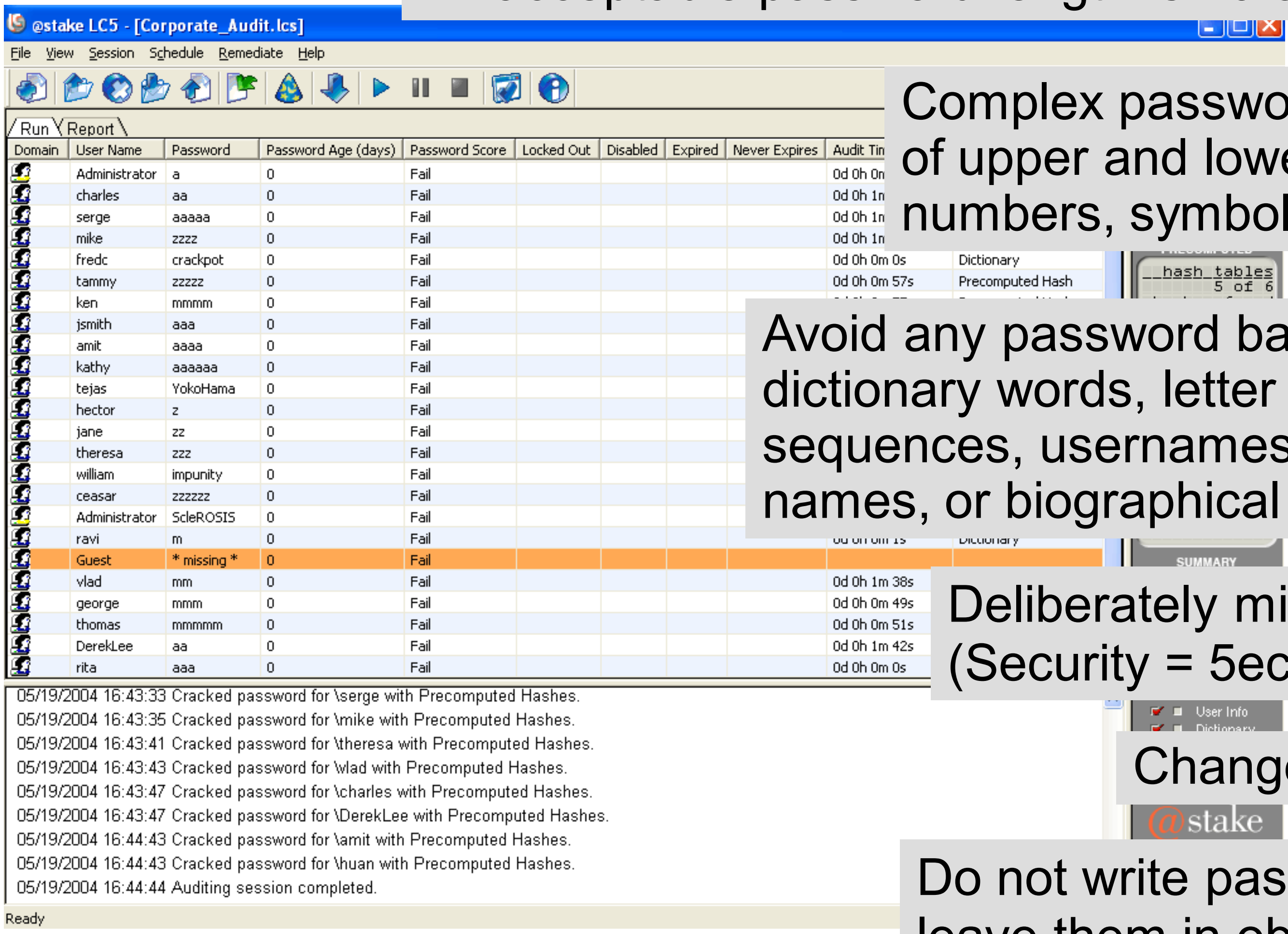
Complex passwords include a mix of upper and lowercase letters, numbers, symbols and spaces

Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, or biographical information

Deliberately misspell a password (Security = 5ecur1ty)

Change passwords often

Do not write passwords down and leave them in obvious places



Domain	User Name	Password	Password Age (days)	Password Score	Locked Out	Disabled	Expired	Never Expires	Audit Tin	
	Administrator	a	0	Fail					0d 0h 0m	
	charles	aa	0	Fail					0d 0h 1m	
	serge	aaaaa	0	Fail					0d 0h 1m	
	mike	zzzz	0	Fail					0d 0h 1m	
	fredc	crackpot	0	Fail					0d 0h 0m 0s	Dictionary
	tammy	zzzzz	0	Fail					0d 0h 0m 57s	Precomputed Hash
	ken	mmmm	0	Fail						
	jsmith	aaa	0	Fail						
	amit	aaaa	0	Fail						
	kathy	aaaaaa	0	Fail						
	tejas	YokoHama	0	Fail						
	hector	z	0	Fail						
	jane	zz	0	Fail						
	theresa	zzz	0	Fail						
	william	impunity	0	Fail						
	ceasar	zzzzzz	0	Fail						
	Administrator	ScleROSIS	0	Fail						
	ravi	m	0	Fail					0d 0h 0m 1s	Dictionary
	Guest	* missing *	0	Fail						
	vlad	mm	0	Fail					0d 0h 1m 38s	
	george	mmm	0	Fail					0d 0h 0m 49s	
	thomas	mmmmm	0	Fail					0d 0h 0m 51s	
	DerekLee	aa	0	Fail					0d 0h 1m 42s	
	rita	aaa	0	Fail					0d 0h 0m 0s	

```
05/19/2004 16:43:33 Cracked password for \serge with Precomputed Hashes.
05/19/2004 16:43:35 Cracked password for \mike with Precomputed Hashes.
05/19/2004 16:43:41 Cracked password for \theresa with Precomputed Hashes.
05/19/2004 16:43:43 Cracked password for \vlad with Precomputed Hashes.
05/19/2004 16:43:47 Cracked password for \charles with Precomputed Hashes.
05/19/2004 16:43:47 Cracked password for \DerekLee with Precomputed Hashes.
05/19/2004 16:44:43 Cracked password for \amit with Precomputed Hashes.
05/19/2004 16:44:43 Cracked password for \huan with Precomputed Hashes.
05/19/2004 16:44:44 Auditing session completed.
```

Access Port Passwords

```
R1(config)# enable secret cisco
```

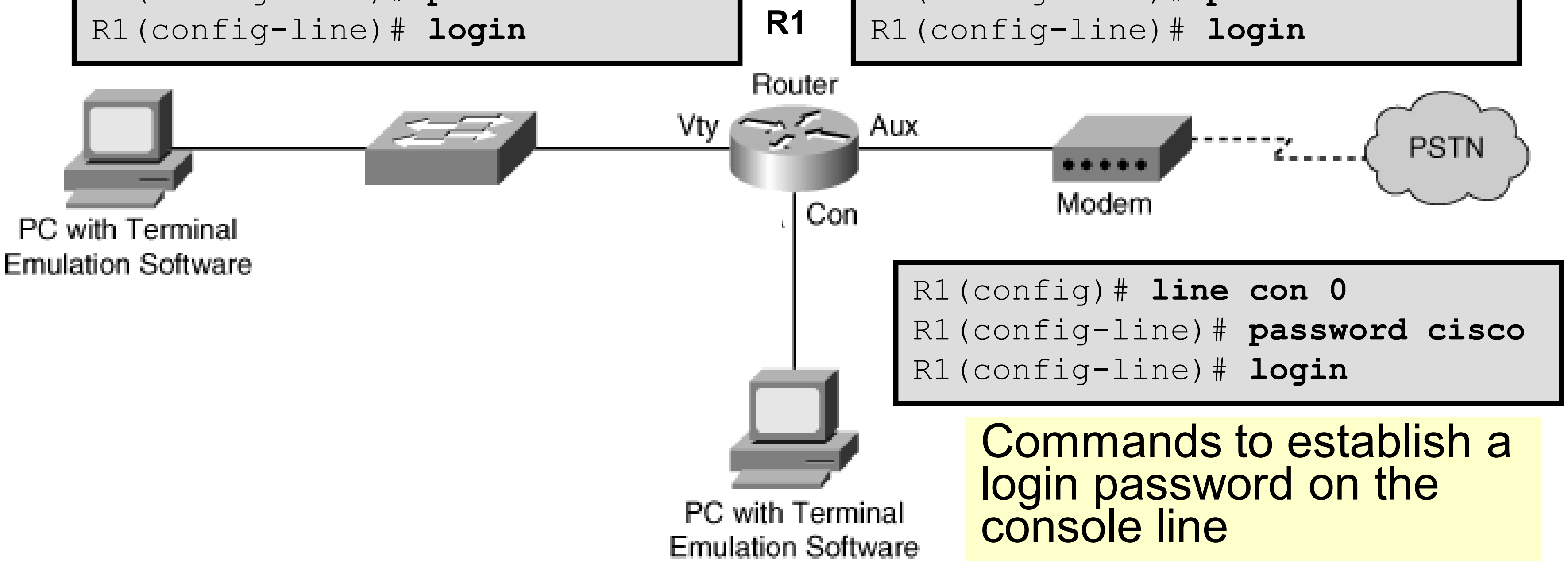
Command to restrict access to privileged EXEC mode

Commands to establish a login password on incoming Telnet sessions

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

Commands to establish a login password for dial-up modem connections

```
R1(config)# line aux 0
R1(config-line)# password cisco
R1(config-line)# login
```


R1
Router
Vty
Aux
Con
Modem
PSTN
PC with Terminal Emulation Software
PC with Terminal Emulation Software

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

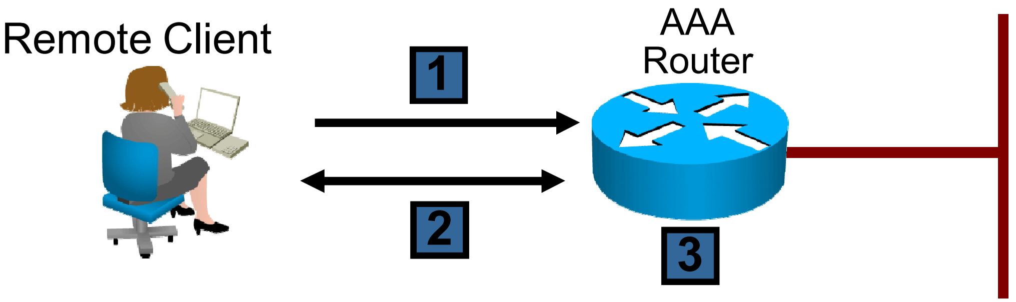
Commands to establish a login password on the console line

Creating Users

```
username name secret {[0]password|5encrypted-secret}
```

Parameter	Description
name	This parameter specifies the username.
0	(Optional) This option indicates that the plaintext password is to be hashed by the router using MD5.
password	This parameter is the plaintext password to be hashed using MD5.
5	This parameter indicates that the encrypted-secret password was hashed using MD5.
encrypted-secret	This parameter is the MD5 encrypted-secret password that is stored as the encrypted user password.

Self-Contained AAA Authentication



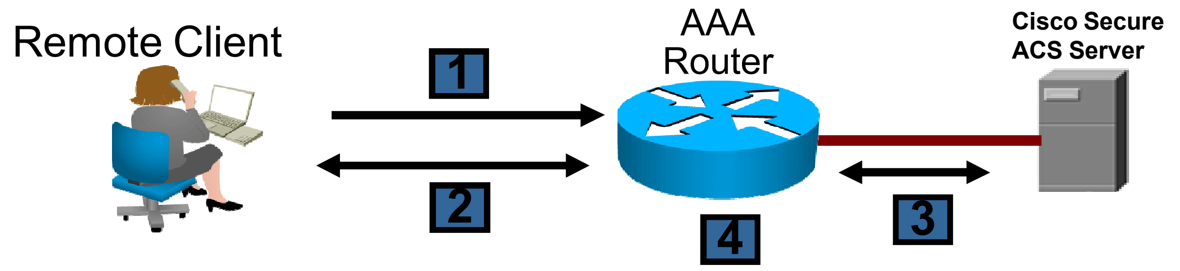
Self-Contained AAA

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.

- Used for small networks
- Stores usernames and passwords locally in the Cisco router

Server-Based AAA Authentication

- Uses an external database server
    - Cisco Secure Access Control Server (ACS) for Windows Server
    - Cisco Secure ACS Solution Engine
    - Cisco Secure ACS Express
- More appropriate if there are multiple routers

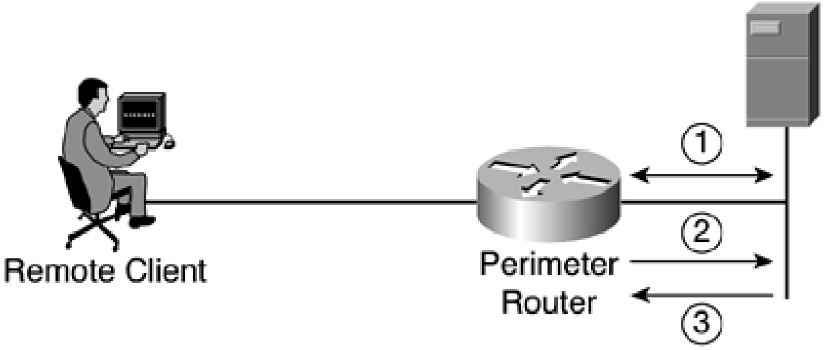


Server-Based AAA

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.

AAA Authorization

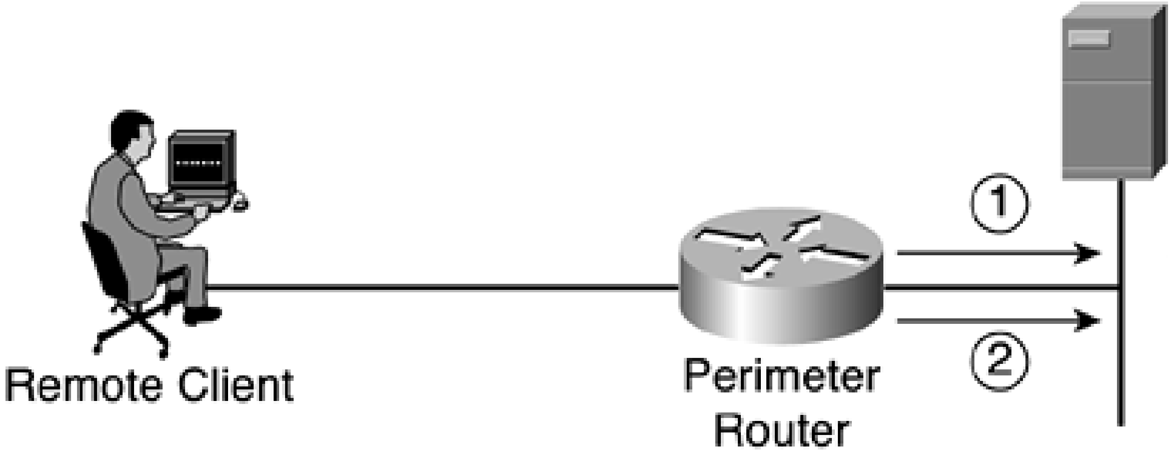
- Typically implemented using an AAA server-based solution
- Uses a set of attributes that describes user access to the network



1. When a user has been authenticated, a session is established with an 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.

AAA Accounting

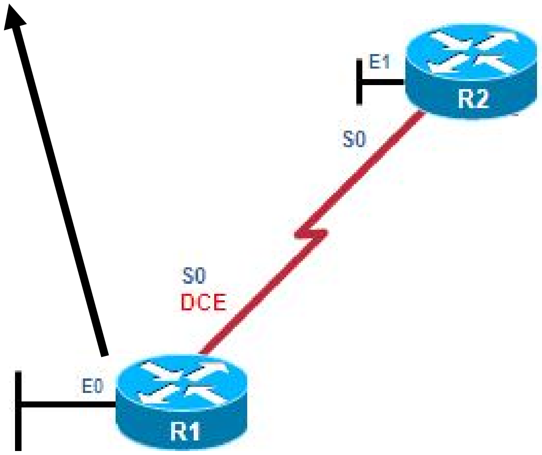
- Implemented using an AAA server-based solution
- Keeps a detailed log of what an authenticated user does on a device



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 ending the accounting process.

Local AAA Authentication Commands

```
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
```



To authenticate administrator access (character mode access)

1. Add usernames and passwords to the local router database
2. Enable AAA globally
3. Configure AAA parameters on the router
4. Confirm and troubleshoot the AAA configuration

Additional Commands

- aaa authentication enable

  Enables AAA for EXEC mode access

- aaa authentication ppp

  Enables AAA for PPP network access

AAA Authentication Command Elements

```
router(config)#
```

```
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
password-expiry	Enables password aging on a local authentication list.
method1 [*method2...*]	Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods.

Method Type Keywords

Keywords	Description
enable	Uses the enable password for authentication. This keyword cannot be used.
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.

Additional Security

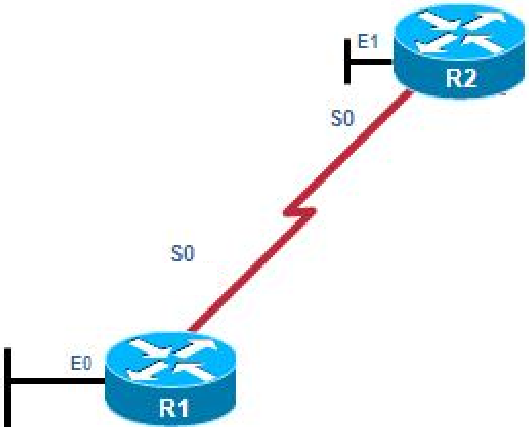
```
router(config)#
```

```
aaa local authentication attempts max-fail [number-of-
  unsuccessful-attempts]
```

```
R1# show aaa local user lockout

                    Local-user            Lock time
                    JR-ADMIN              04:28:49 UTC Sat Dec 27 2008
```

```
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
```

Sample 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 enable
R1(config)# aaa authentication login TELNET-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
```

Troubleshooting

- The **`debug aaa`** Command
- Sample Output

The debug aaa Command

```
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

R1# debug aaa
```

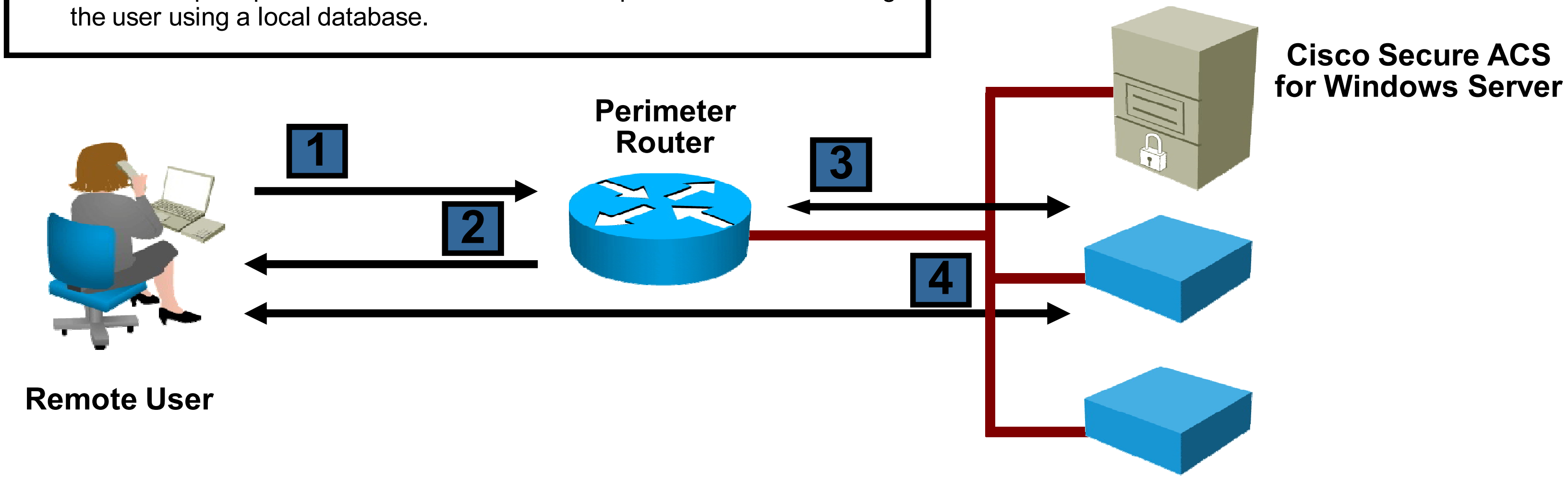
Sample Output

```
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
```

Local Versus Server-Based Authentication

Local Authentication

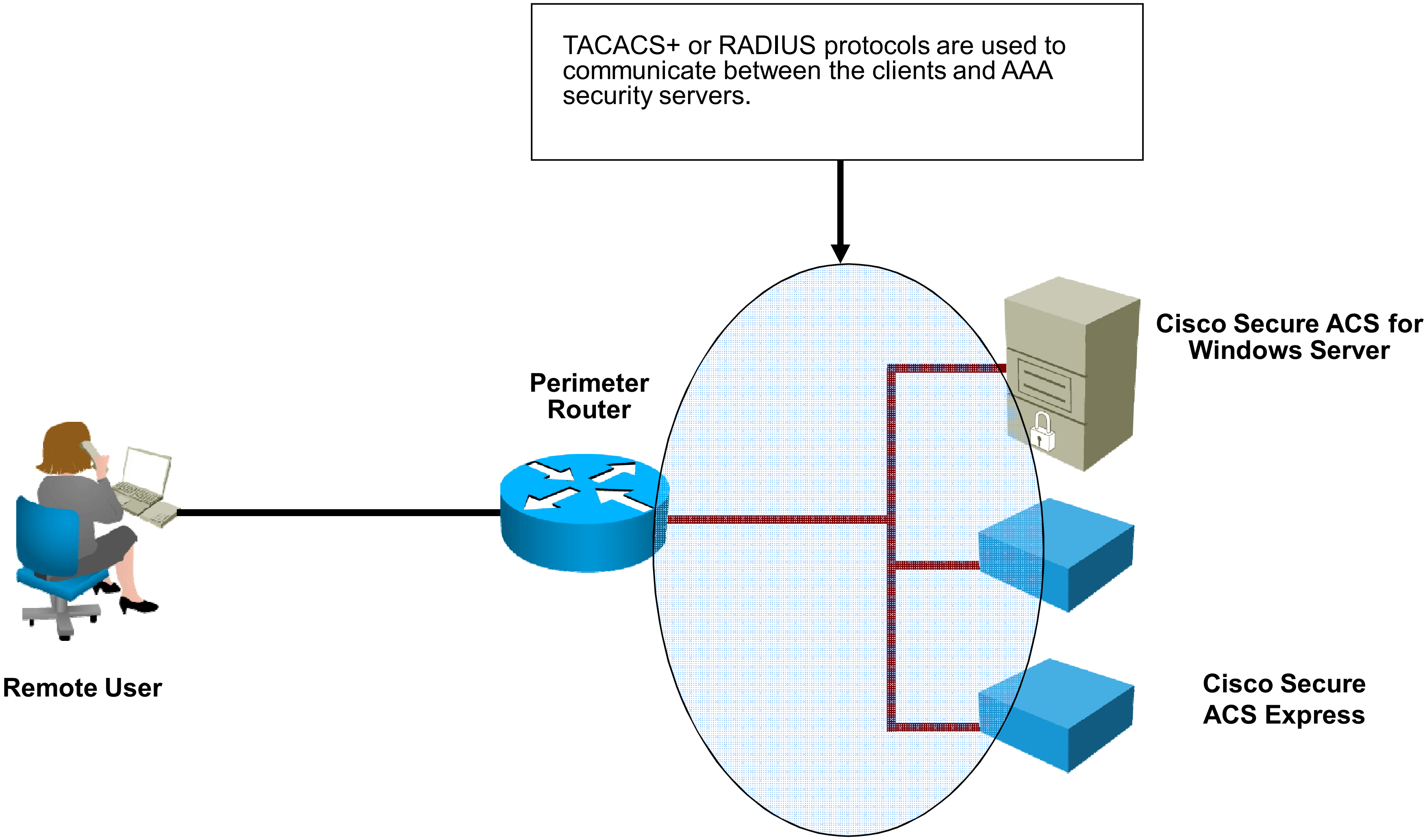
1. The user establishes a connection with the router.
2. The router prompts the user for a username and password authenticating the user using a local database.



Server-Based Authentication

1. The user establishes a connection with the router.
2. The router prompts the user for a username and password.
3. The router passes the username and password to the Cisco Secure ACS (server or engine).
4. The Cisco Secure ACS authenticates the user. The user is authorized to access the router (administrative access) or the network based on information found in the Cisco Secure ACS database.

Overview of TACACS+ and RADIUS



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

TACACS+/RADIUS Comparison

	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
Confidentiality	Limited	Extensive

AAA Authorization Commands

```
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 group tacacs+
R1(config)# aaa authentication login TELNET-LOGIN local-case
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
R1(config-line)# ^Z
```

- To configure command authorization, use:

  aaa authorization *service-type* **{default |** *list-name***}** *method1* **[***method2***] [***method3***] [***method4***]**

- Service types of interest include:

commands *level*	For exec (shell) commands
exec	For starting an exec (shell)
network	For network services. (PPP, SLIP, ARAP)

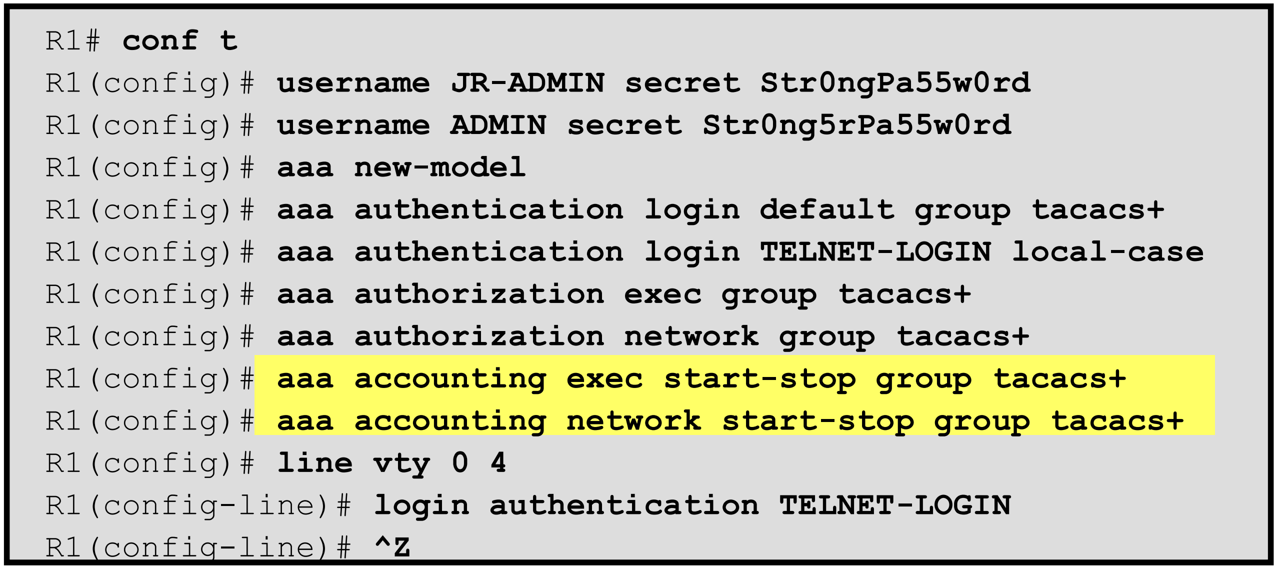
AAA Accounting Overview

- Provides the ability to track usage, such as dial-in access; the ability to log the data gathered to a database; and the ability to produce reports on the data gathered
- To configure AAA accounting using named method lists:

  aaa accounting {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **wait-start** | **stop-only** | **none**} [*method1* [*method2*]]

- Supports six different types of accounting: **network**, **connection**, **exec**, **system**, **commands** *level*, and **resource**.

AAA Accounting Commands



```
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 group tacacs+
R1(config)# aaa authentication login TELNET-LOGIN local-case
R1(config)# aaa authorization exec group tacacs+
R1(config)# aaa authorization network group tacacs+
R1(config)# aaa accounting exec start-stop group tacacs+
R1(config)# aaa accounting network start-stop group tacacs+
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
R1(config-line)# ^Z
```

- **aaa accounting exec default start-stop group tacacs+**
  Defines a AAA accounting policy that uses TACACS+ for logging both start and stop records for user EXEC terminal sessions.
- **aaa accounting network default start-stop group tacacs+**
  Defines a AAA accounting policy that uses TACACS+ for logging both start and stop records for all network-related service requests.

Cisco
Learning
Institute