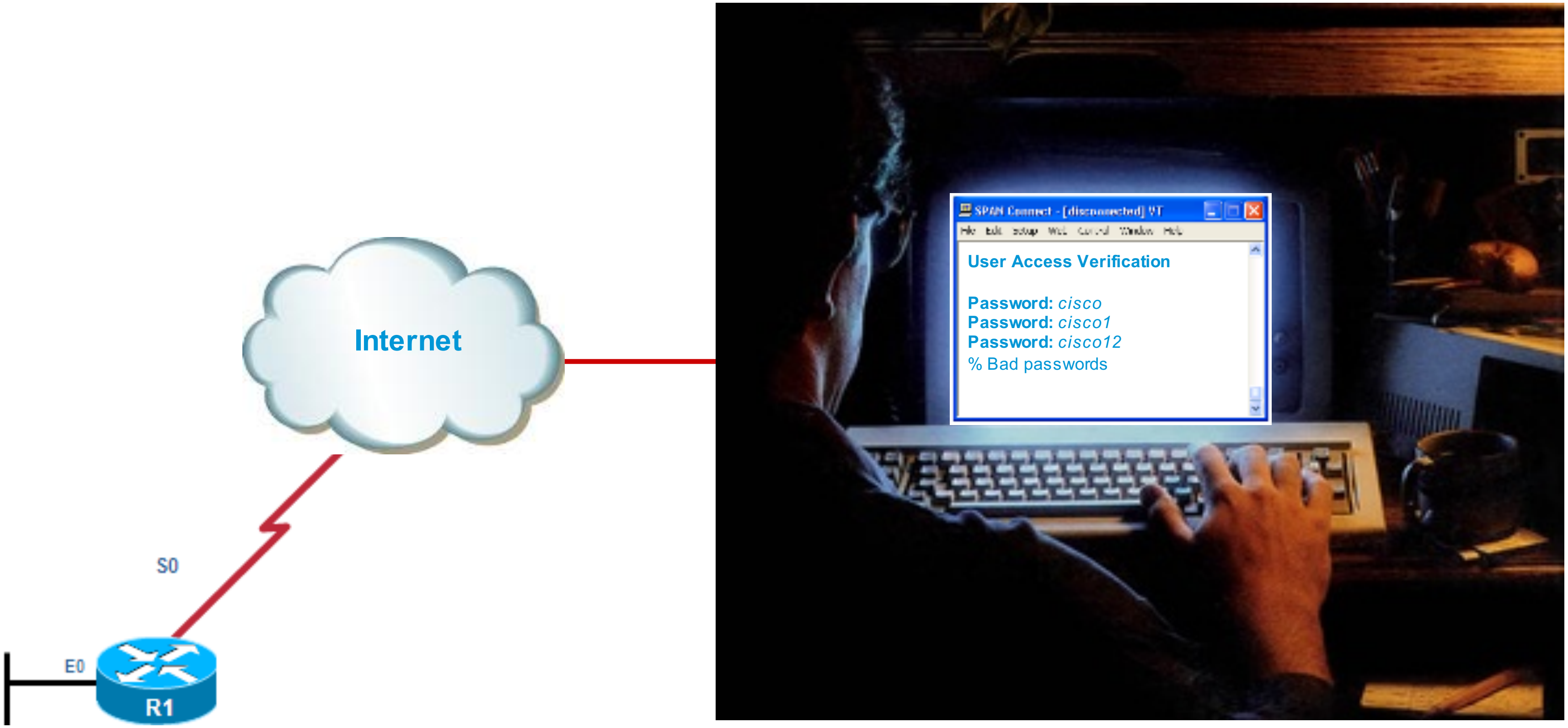
Authentication, Authorization, and Accounting

Managing Administrative Access

- Managing administrative infrastructure access is crucial.
- Methods:
  - Password only
  - Local database
  - AAA Local Authentication (self-contained AAA)
  - AAA Server-based

Access Type	Modes	Network Access Server Ports	Common AAA Command Element
Remote administrative access	Character Mode (line or EXEC mode)	tty, vty, auxiliary, and console	**`login`**, **`exec`**, and **`enable`** commands
Remote network access	Packet (interface mode)	Dial-up and VPN access including asynchronous and ISDN (BRI and PRI)	**`ppp`** and **`network`** commands

Password Only Method



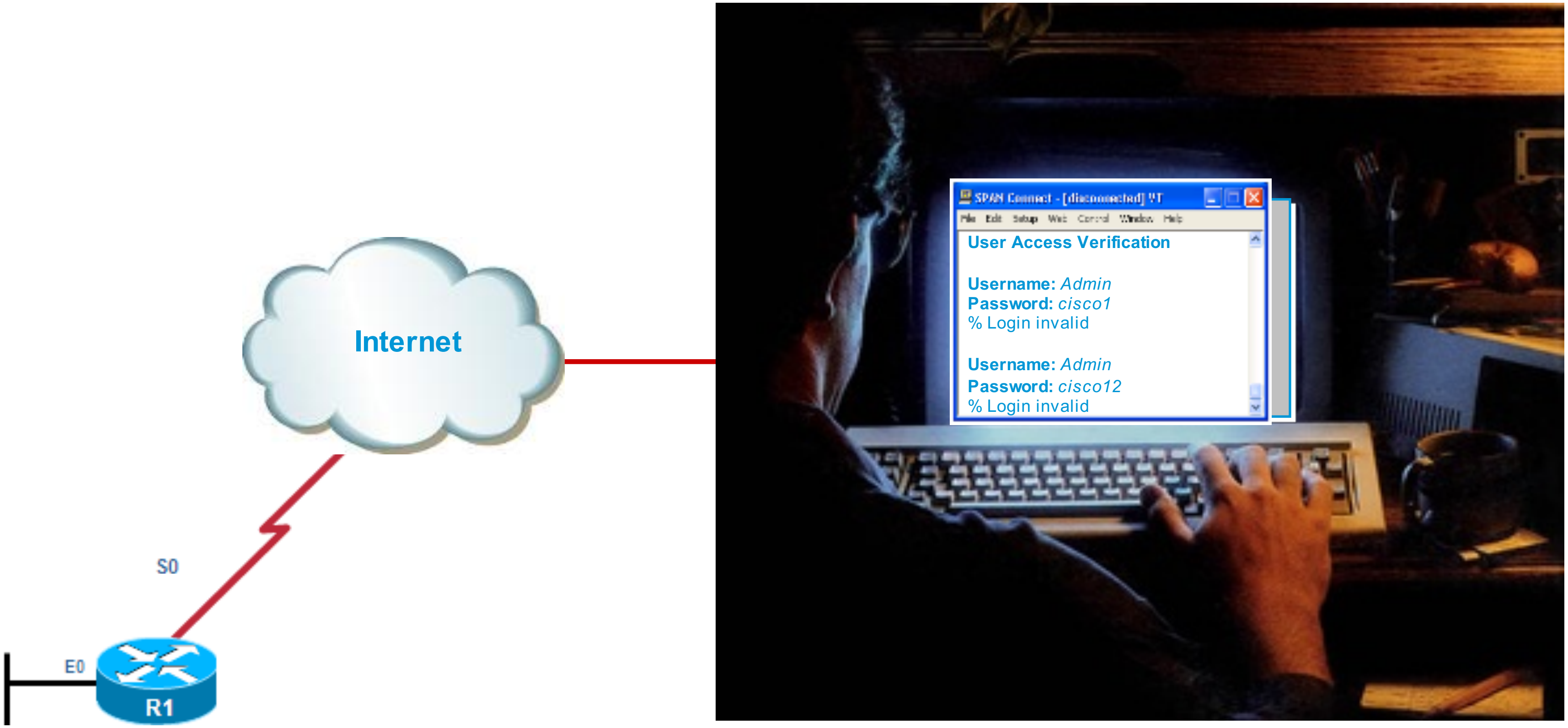
User Access Verification

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

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

- User EXEC mode or privilege EXEC mode password access is limited and does not scale well.

Local Database Method


Internet
S0
E0
R1
SPAN Connect - [disconnected] VT
File Edit Setup Web Control Window Help

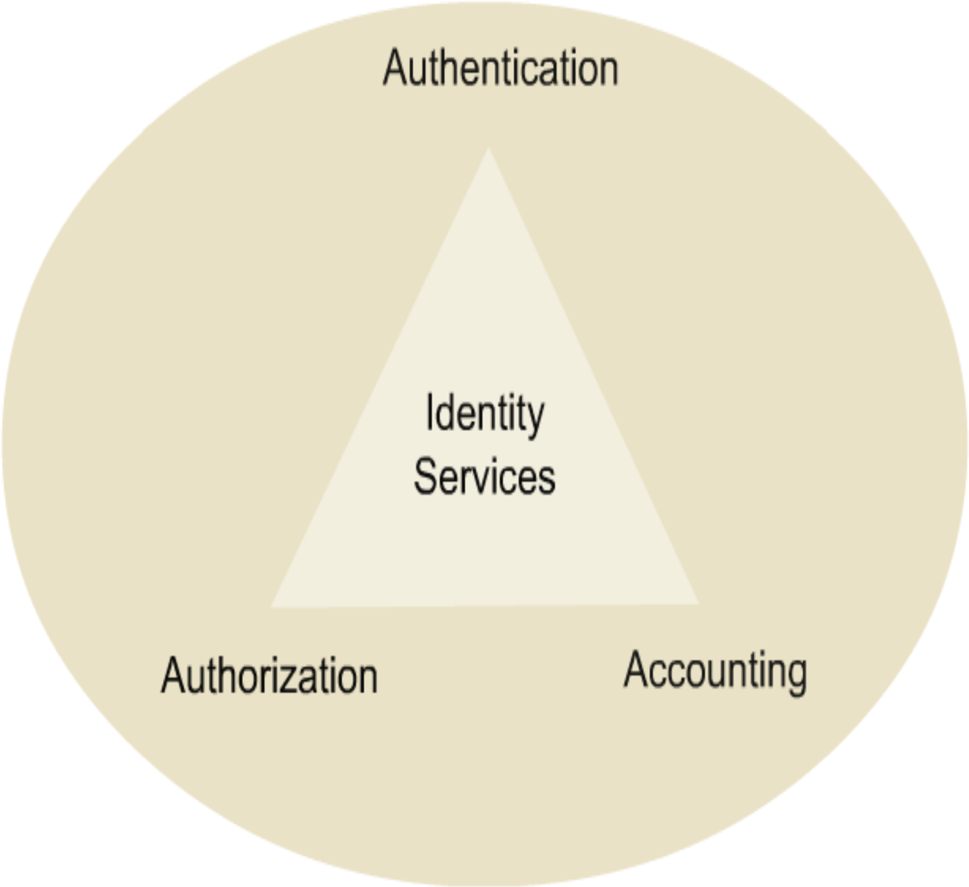
```
User Access Verification

Username: Admin
Password: cisco1
% Login invalid

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

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

- It provides greater security than a simple password.
- It’s a cost effective and easily implemented security solution.

Local Database Method

- The problem is this local database has to be replicated on several devices …
  - A better scalable solution is to use AAA.



AAA Security Services

- AAA is an architectural framework for configuring:

Authentication - Who is allowed access?

Authorization - What are they allowed to do?

Accounting - What did they do?

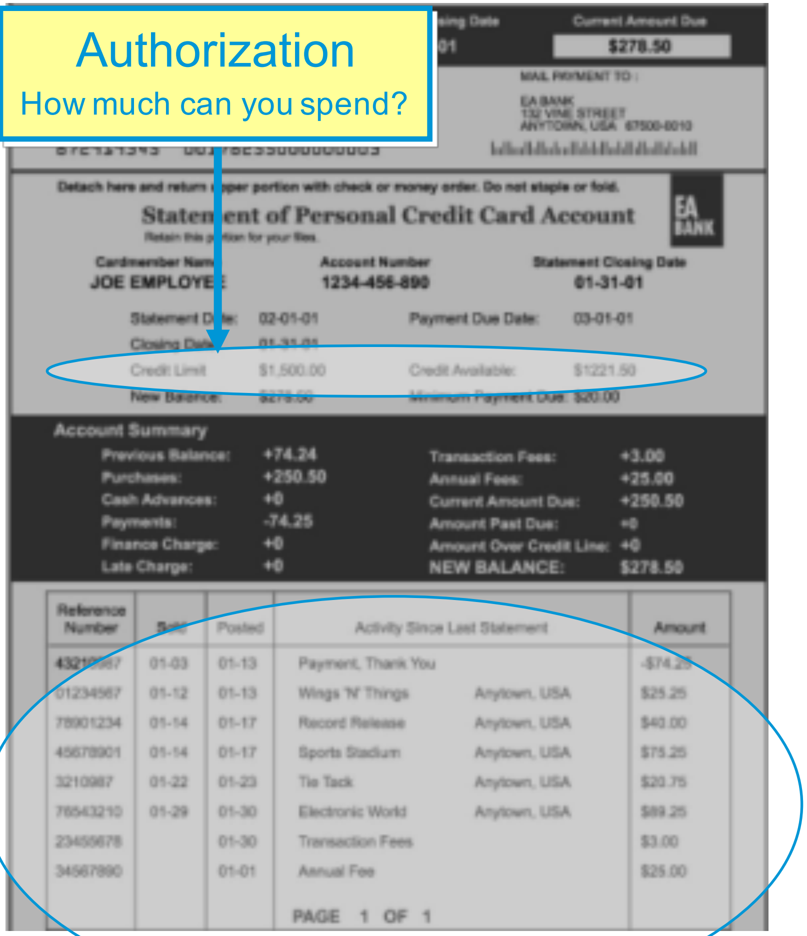
AAA Security Services

Authentication

Who are you?

Authorization

How much can you spend?



sing Date | Current Amount Due
01 | $278.50

MAIL PAYMENT TO :

EA BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

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

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

PAGE 1 OF 1

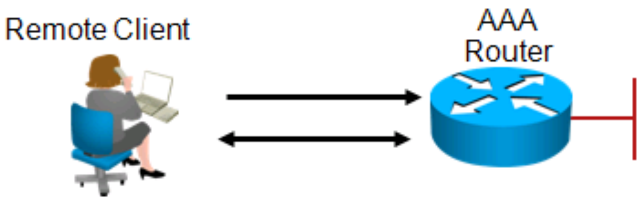
Accounting

What did you spend it on?

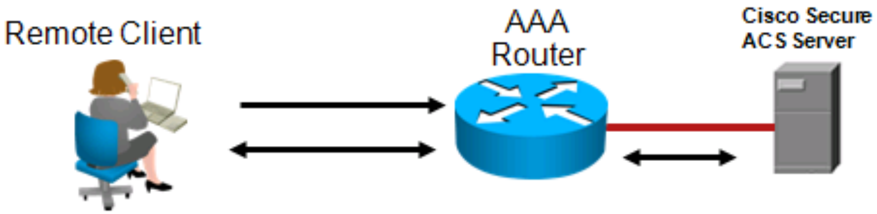
AAA Authentication Methods

- Cisco IOS routers can implement AAA using either:

Local username and password database



Cisco Secure Access Control Server (ACS)



AAA Local Authentication

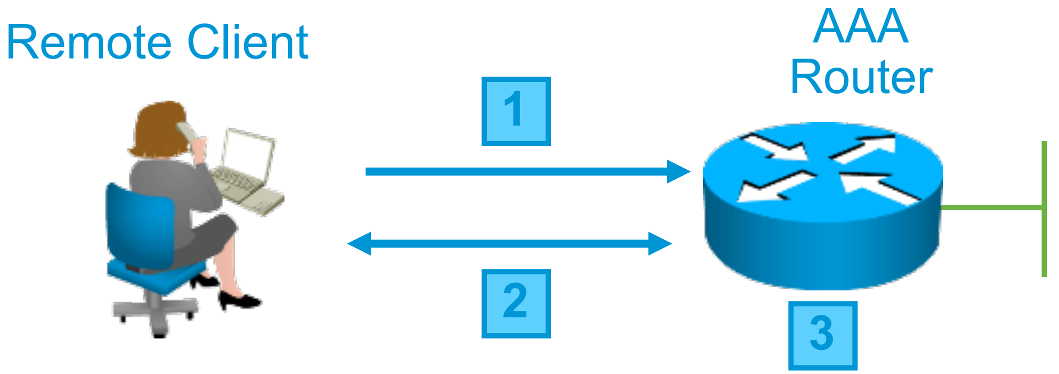
- Also called “Self-contained AAA”, it provides the method of identifying users:
  - Includes login and password dialog, challenge and response, messaging support, …
- It’s configured by:
  - Defining a “named” list of authentication methods.
  - Applying that list to various interfaces (console, aux, vty).
- The only exception is the default method list (“default”) which is automatically applied to all interfaces if no other method list is defined.

AAA Local Authentication

- The named or default authentication method defines:
  - The types of authentication to be performed.
  - The sequence in which they will be performed.
- It MUST be applied to a specific interface before any of the defined authentication methods will be performed.

AAA Local Authentication

- The client establishes a connection with the router.
- The AAA router prompts the user for a username and password.
- 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.

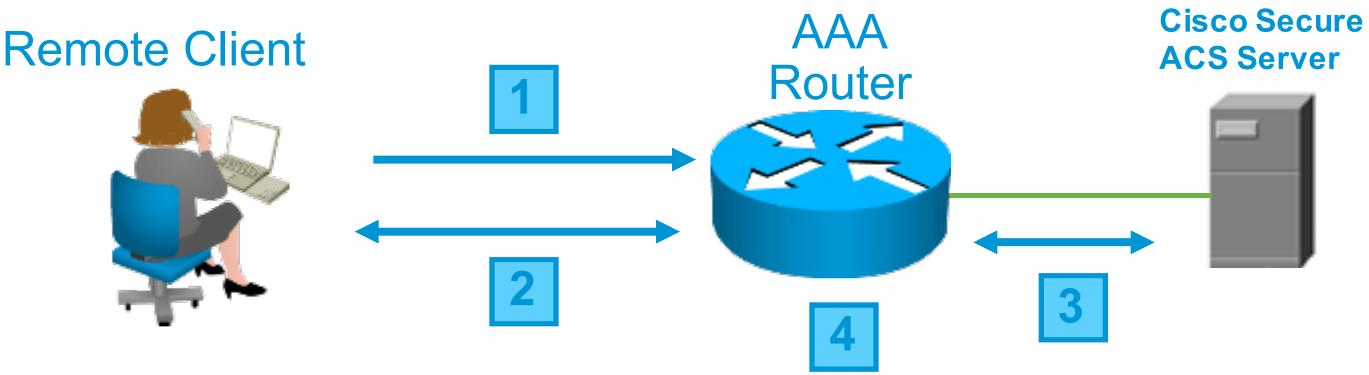


Server-Based AAA Authentication

- Using Cisco Access Control Server (ACS) is the most scalable because all infrastructure devices access a central server.
  - Fault tolerant because multiple ACS can be configured.
  - Enterprise solution.
- The actual server can be:
  - Cisco Secure ACS for Windows Server:
    - AAA services on the router contacts a Cisco Secure Access Control Server (ACS) system for user and administrator authentication.
  - Cisco Secure ACS Solution Engine:
    - AAA services on the router or NAS contact an external Cisco Secure ACS Solution Engine for user and administrator authentication.

Server-Based AAA Authentication

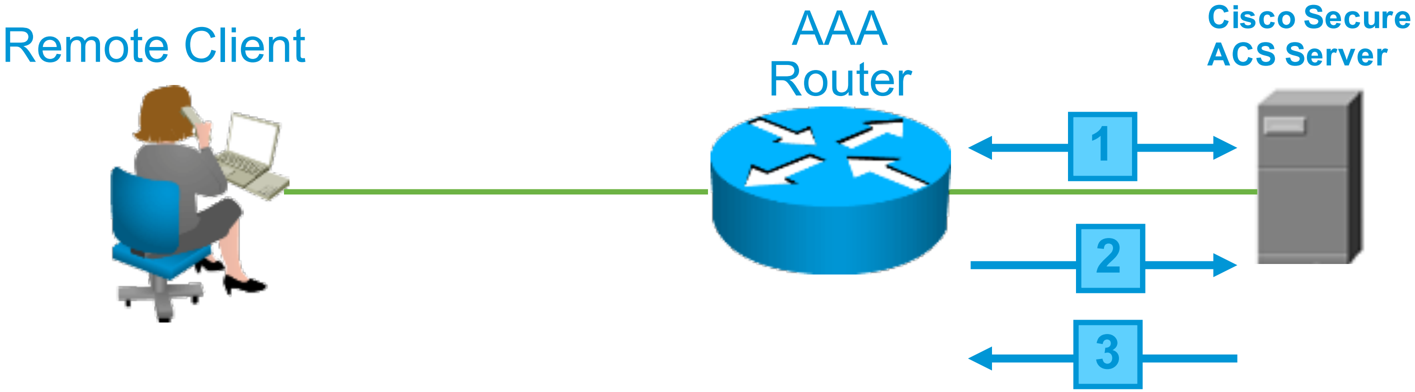
1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server.
4. The user is authorized to access the network based on information on the remote AAA Server.



Authorization

- Provides the method for remote access control.
  - Including one-time authorization or authorization for each service, per-user account list and profile, user group support, …
- Once a user has authenticated, authorization services determine which:
  - Resources the user can access.
  - Operations the user is allowed to perform.
    - E.g., “User ‘student’ can access host serverXYZ using Telnet only.”
- As with authentication, AAA authorization is configured by defining a “named” list of authorization methods, and then applying that list to various interfaces.

AAA Authorization

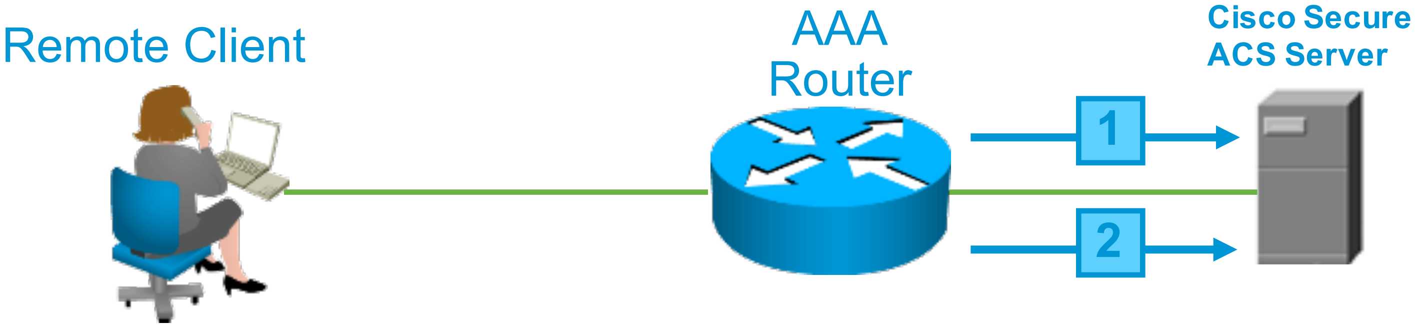


1. User has authenticated and a session has been established to the AAA server.
2. When the user attempts to enter privileged EXEC mode command, the router requests authorization from a AAA server to verify that the user has the right to use it.
3. The AAA server returns a “PASS/FAIL” response.

Accounting

- Provides the method for collecting and sending security server information.
- Used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands, number of packets / bytes, …
- With AAA accounting activated, the router reports user activity to the TACACS+ security server in the form of accounting records.
- Accounting is configured by defining a “named” list of accounting methods, and then applying that list to various interfaces.

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 logs out, a stop message is recorded and the accounting process ends.

AAA Benefits

- Increased flexibility and control of access configuration
- Scalability
- Multiple backup systems
- Standardized authentication methods
  - RADIUS, TACACS+ and Kerberos

AAA - Scalability

- AAA is typically implemented using a dedicated ACS server to store usernames / passwords in a centralized database.
- Information is centrally entered / updated unlike a local database which must be configured on every router.

CLI Local Authentication Configuration Steps

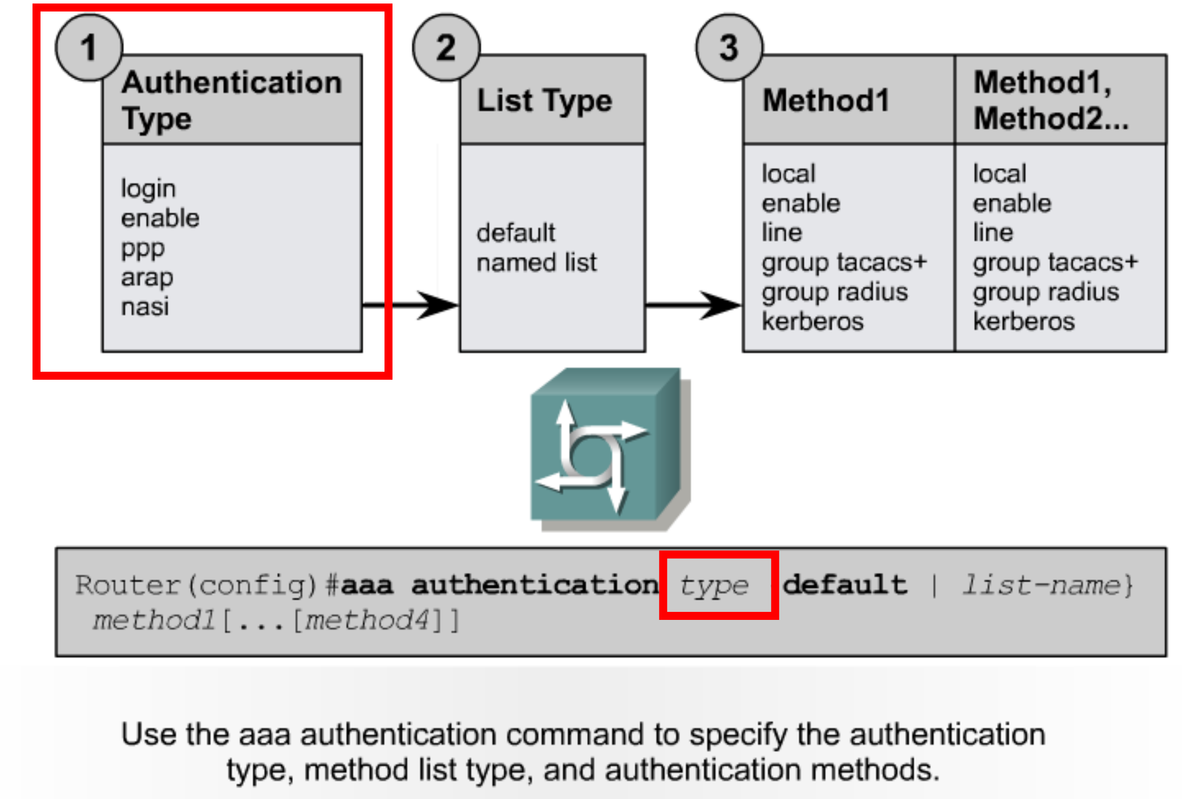
1. Enable AAA by using the global configuration command:
   - `aaa new-model`
2. Define the authentication method lists using:
   - `aaa authentication`
3. Apply the method lists to a particular interface or line (if required).

Enable AAA

- The **`aaa new-model`** command enables the AAA feature.
  - AAA commands can now be configured.
  - To disable AAA, use the **`no aaa new-model`** command.
- CAUTION:
  - Do not issue the command unless you are prepared to configure AAA authentication. Doing so could force Telnet users to authenticate with a username, even if no username database or authentication method is configured.

```
R1(config)#  aaa new-model
```

Configuring Authentication

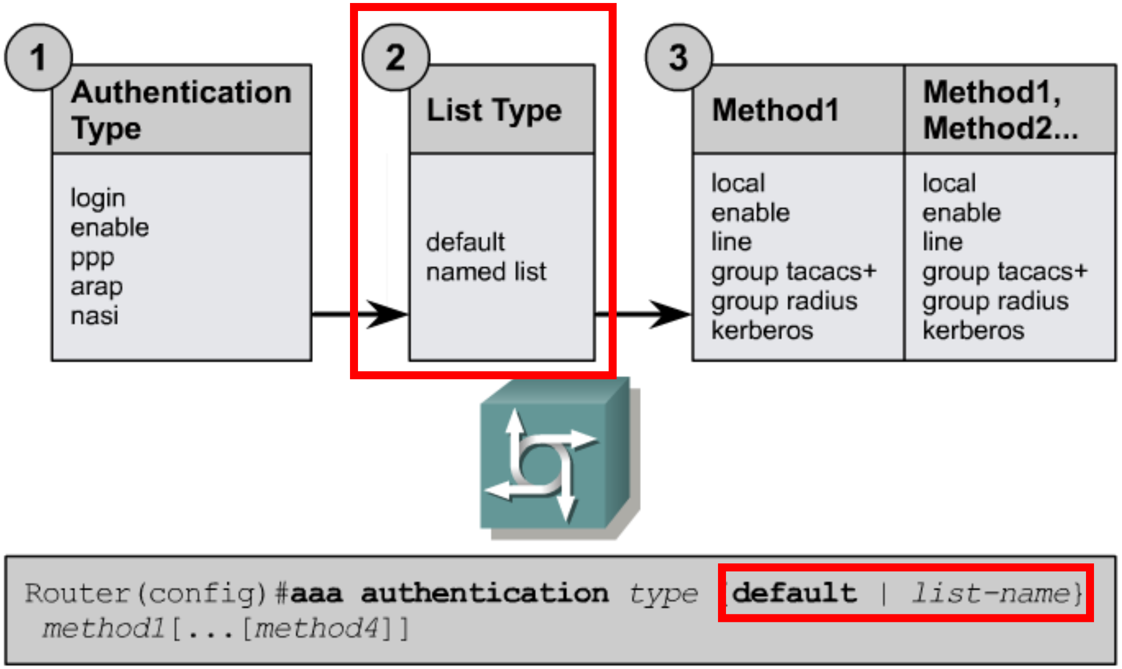


```
Router(config)#aaa authentication type default | list-name}
 method1[...[method4]]
```

Use the aaa authentication command to specify the authentication type, method list type, and authentication methods.

- Specify which type of authentication to configure:
  - Login - enables AAA for logins on TTY, VTYs, and con 0.
  - Enable - enables AAA for EXEC mode access.
  - PPP - enables AAA for logins on PPP (packet transfer).

Configuring Authentication

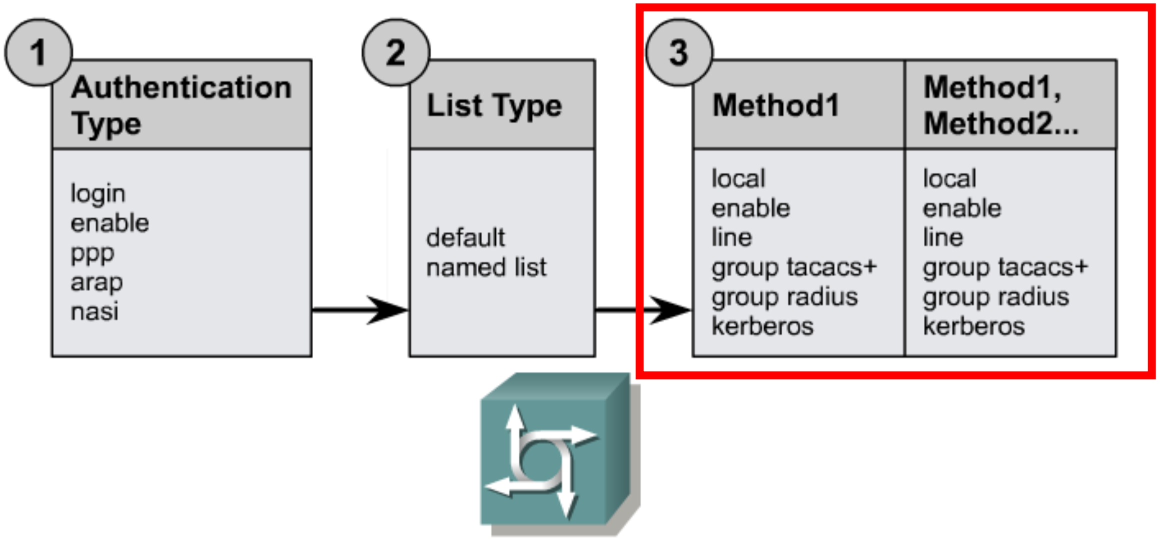


```
Router(config)#aaa authentication type {default | list-name}
 method1[...[method4]]
```

Use the aaa authentication command to specify the authentication type, method list type, and authentication methods.

- Default method list is automatically applied to all interfaces if no other method list is defined.
- Named lists must be applied to a specific interface before any of the defined authentication methods will be performed.

Configuring Authentication



1 Authentication Type

login
enable
ppp
arap
nasi

2 List Type

default
named list

3 Method1

local
enable
line
group tacacs+
group radius
kerberos

Method1, Method2...

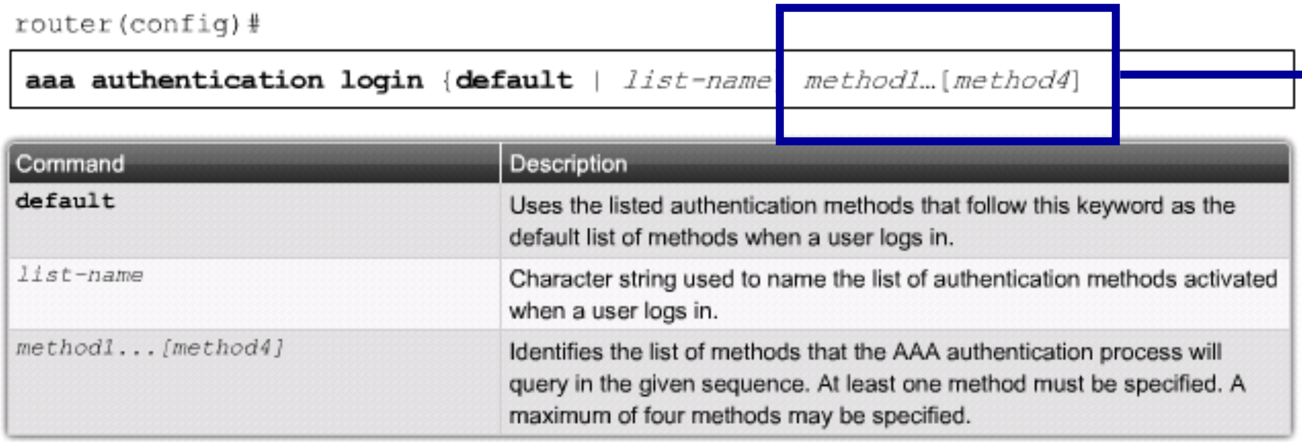
local
enable
line
group tacacs+
group radius
kerberos

```
Router(config)#aaa authentication type {default | list-name}
 method1[...[method4]]
```

Use the aaa authentication command to specify the authentication type, method list type, and authentication methods.

- Methods list the types of authentication to be performed and the sequence in which they will be performed, such as:
  - Pre-defined passwords (e.g., local, enable, or line)
  - Consulting a TACACS+ / RADIUS / Kerberos server(s)

Configure Authentication



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

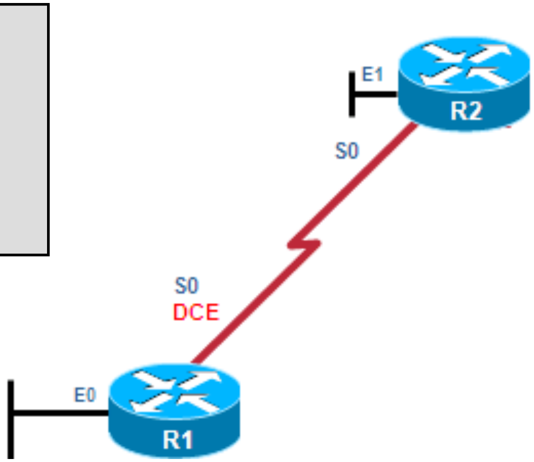
Command	Description
default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method1...[method4]	Identifies the list of methods 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.

Methods	Description
enable	Uses the enable password for authentication.
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.

Configuring Local AAA Authentication

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

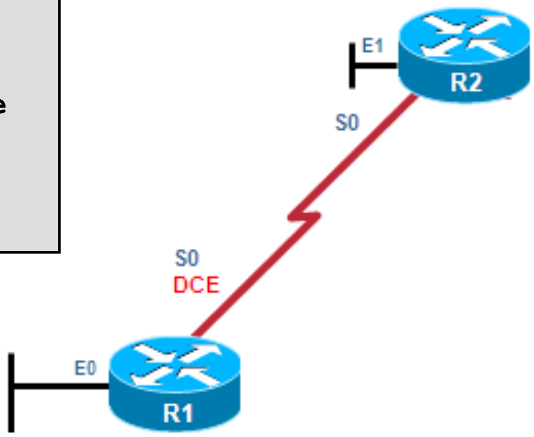
```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case
R1(config)# aaa local authentication attempts max-fail 10
```



Using a Named List

- A default list or a named list can be defined.
  - A default list is automatically applied to all interfaces if no other method list is defined.
  - A named list must be applied to a specific interface before any of the defined authentication methods will be performed.

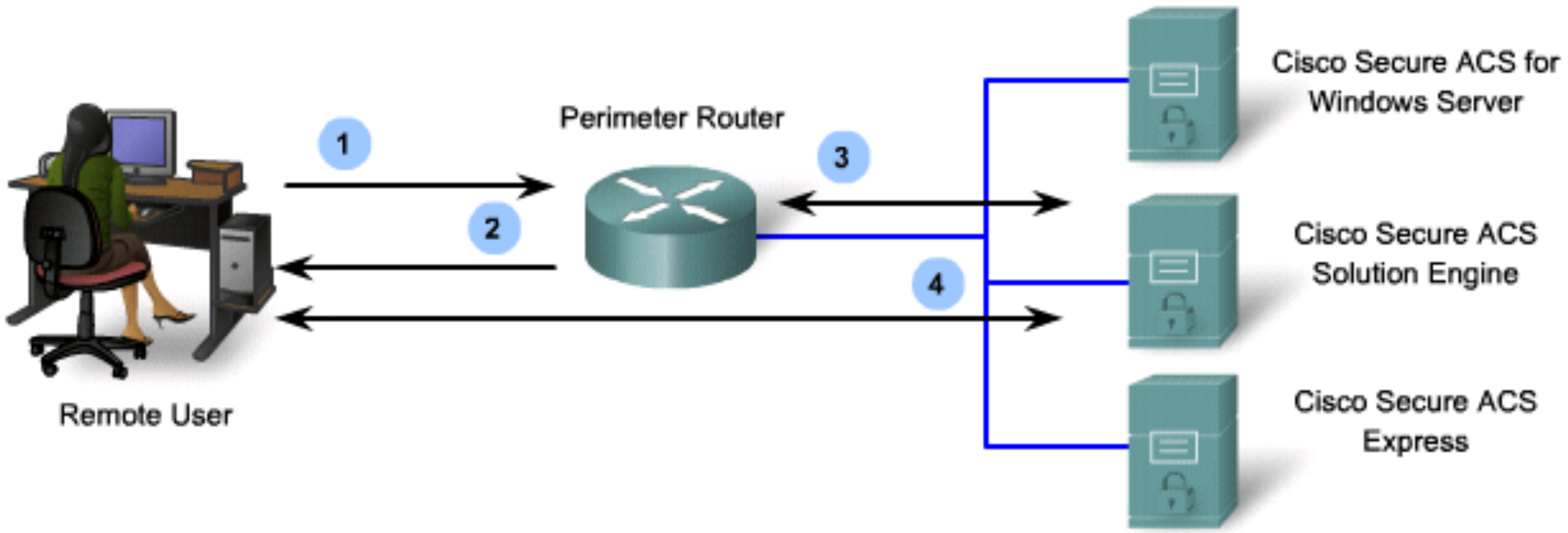
```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case enable
R1(config)# aaa authentication login TELNET-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
```



Troubleshooting AAA Authentication

```
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
```

Server-Based Solution

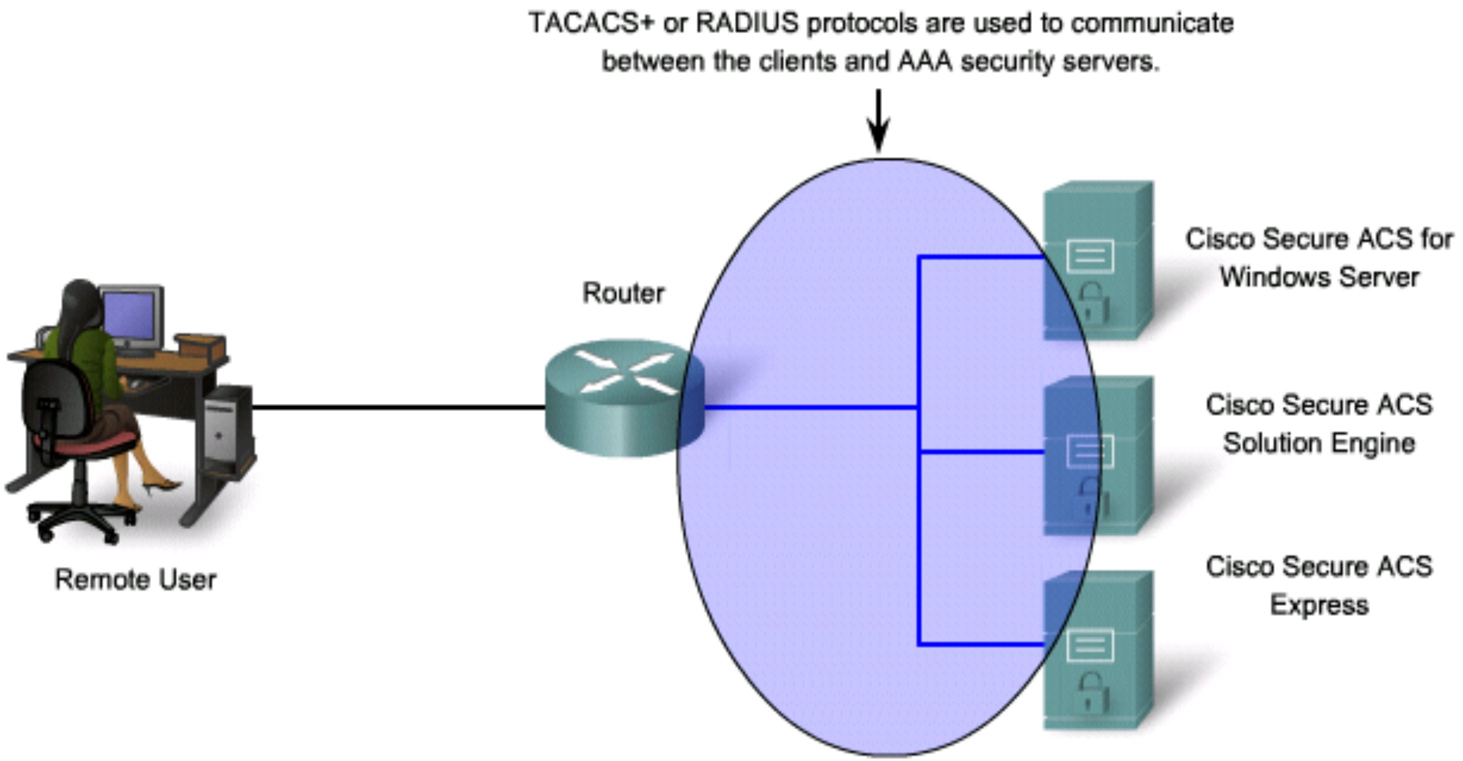

Remote User
Perimeter Router
1
2
3
4
Cisco Secure ACS for Windows Server
Cisco Secure ACS Solution Engine
Cisco Secure ACS Express

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.

TACACS+ and RADIUS

- The Cisco ACS family support:
  - Terminal Access Control Access Control Server Plus (TACACS+)
  - Remote Dial-in User Services (RADIUS) protocols


TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.
Router
Remote User
Cisco Secure ACS for Windows Server
Cisco Secure ACS Solution Engine
Cisco Secure ACS Express

TACACS+ and RADIUS

- Both protocols can be used to communicate between client and AAA servers.
- TACACS+ is considered the more secure protocol because all exchanges are encrypted.
- Radius only encrypts the user password.
  - It does not encrypt user names, accounting information, or any other information carried in the radius message.

TACACS+ vs. RADIUS

Feature	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 port 49	UDP port 1645 or 1812 for authentication UDP port 1646 or 1813 for accounting
CHAP	Bidirectional challenge and response as used in 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	Only the password is 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

Cisco Secure ACS

- Many enterprise-level authentication servers are on the market today including:
  - Funk's Steel-Belted RADIUS server
  - Livingston Enterprises' RADIUS Authentication Billing Manager
  - Merit Networks' RADIUS
  - Cisco Secure ACS for Windows Server (ACS)
- Cisco ACS is a single solution that offers AAA services using TACACS+ or RADIUS.

Cisco Secure ACS Benefits

Ease of use	- A web-based user interface simplifies the configuration for user profiles, group profiles, and ACS configuration.
Scalability	- ACS is built to provide large networked environments including redundant servers, remote databases, and database replication and backup services.
Extensibility	- Supports the authentication of user profiles that are stored in directories from leading directory vendors, including Sun, Novell, and Microsoft.
Management	- Active Directory support consolidates username and password management.
Administration	- Ability to group network devices together make it easier and more flexible to control the enforcement and changes for all devices in a network.
Product flexibility	- Cisco Secure ACS is available in three options: Cisco Secure ACS Solution Engine, Cisco Secure ACS Express, and Cisco Secure ACS for Windows.
Integration	- Tight coupling with Cisco IOS routers and VPN solutions.
Third-party support	- Cisco Secure ACS offers token server support for any one-time password (OTP) vendor that provides an RFC-compliant RADIUS interface, such as RSA, PassGo, Secure Computing, ActiveCard, Vasco, or CryptoCard.
Control	- Provides dynamic quotas to restrict access based on the time of day, network use, number of logged sessions, and the day of the week.

CLI Configuration Steps

1. Enable AAA by using the global configuration command:
   - **`aaa new-model`**
2. Configure security protocol parameters:
   - Server IP address and Key
3. Define the authentication method lists using:
   - **`aaa authentication`**
4. Apply the method lists to a particular interface or line (if required).
5. Optionally configure authorization using the global command:
   - **`aaa authorization`**
6. Optionally configure accounting using the global command:
   - **`aaa accounting`**

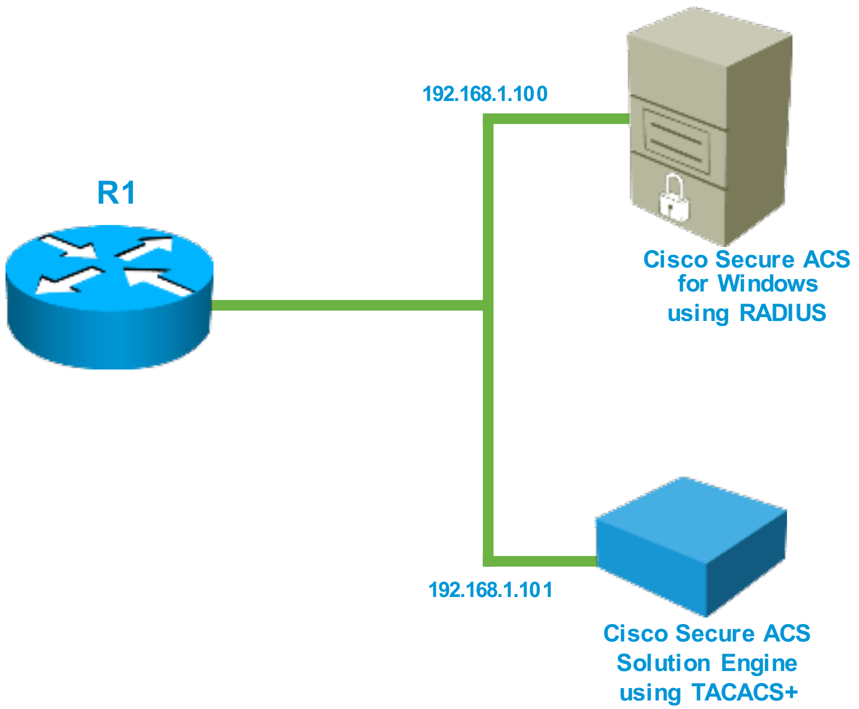
Server-Based AAA Authentication

1. Specify the location of the AAA server that will provide AAA services.
2. Configure the encryption key needed to encrypt the data transfer between the network access server and Cisco Secure ACS.

AAA Configuration Commands

Command	Description
tacacs-server host *ip-address* **single-connection**	- Indicates the address of the Cisco Secure ACS server and specifies use of the TCP single-connection feature of Cisco Secure ACS. - This feature improves performance by maintaining a single TCP connection for the life of the session between the network access server and the Cisco Secure ACS server, rather than opening and closing TCP connections for each session (the default).
tacacs-server key *key*	- Establishes the shared secret encryption key between the network access server and the Cisco Secure ACS server.
radius-server host *ip-address*	- Specifies a RADIUS AAA server.
radius-server key *key*	- Specifies an encryption key to be used with the RADIUS AAA server.

Configuring the AAA Server Parameters


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

```
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)#
```

Define Method Lists

```
R1(config)# aaa authentication login default ?
  enable         Use enable password for authentication.
  group          Use Server-group
  krb5           Use Kerberos 5 authentication.
  krb5-telnet    Allow logins only if already authenticated via Kerberos V
                 Telnet.
  line           Use line password for authentication.
  local          Use local username authentication.
  local-case     Use case-sensitive local username authentication.
  none           NO authentication.
  passwd-expiry  enable the login list to provide password aging support

R1(config)# aaa authentication login default group ?
  WORD     Server-group name
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

R1(config)# aaa authentication login default group
```

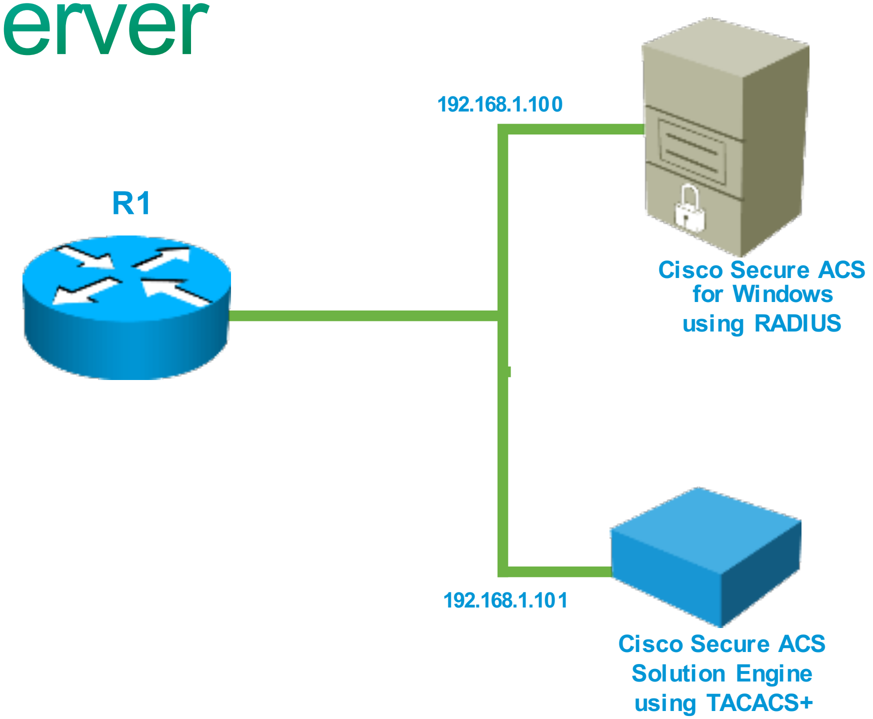
AAA Authentication Commands

```
R1(config)# aaa authentication login default group tacacs+ group radius local-case
```

Parameter	Description
`default`	• This command creates a default that is automatically applied to all lines and interfaces, specifying the method or sequence of methods for authentication.

`group` *`group-name`*
`group radius`
`group tacacs+`
	• These methods specify the use of an AAA server.
	• The group radius and group tacacs+ methods refer to previously defined RADIUS or TACACS+ servers.
	• The group-name string allows the use of a predefined group of RADIUS or TACACS+ servers for authentication (created with the aaa group server radius or aaa group server tacacs+ command).

Configuring the AAA Server



```
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)#
```