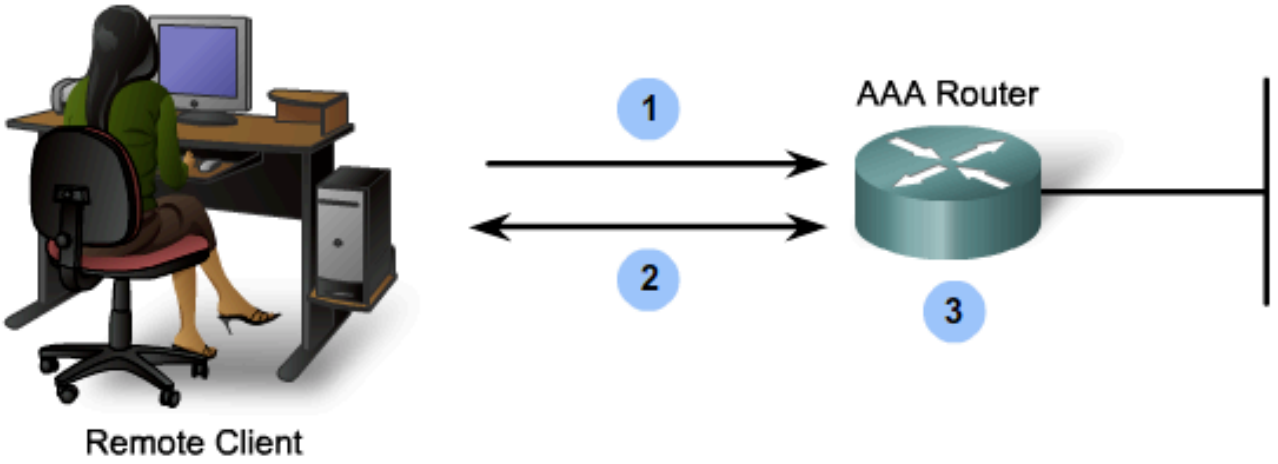
AAA

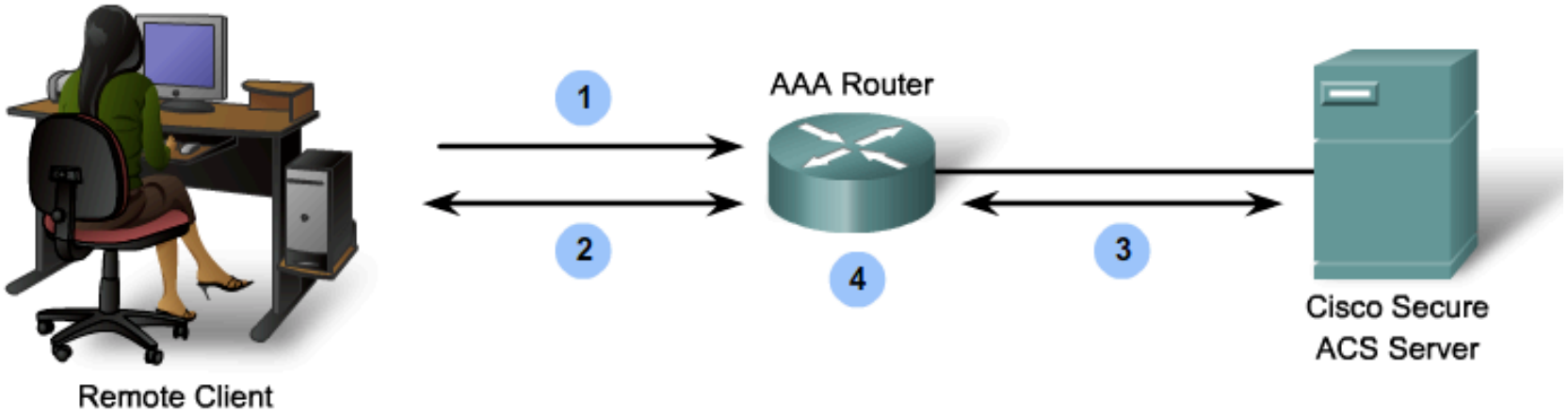
- A – Authentication
- A – Authorization
- A – Accountng
- Local database
- ACS to support AAA for Cisco Routers
- Server based AAA

Local Authentication



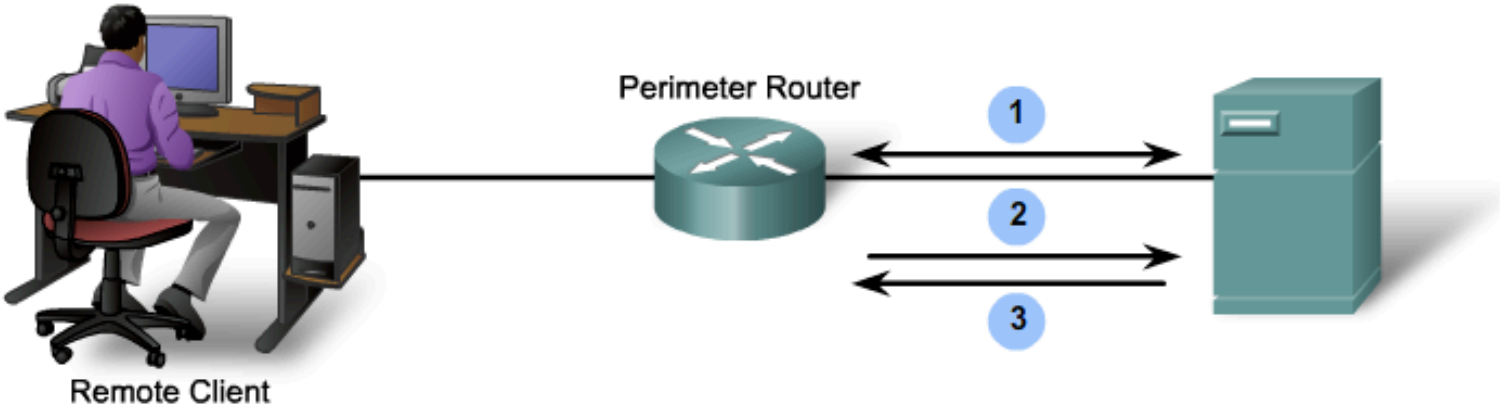
1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is authorized to access the network based on information in the local database.

Server Based Authentication



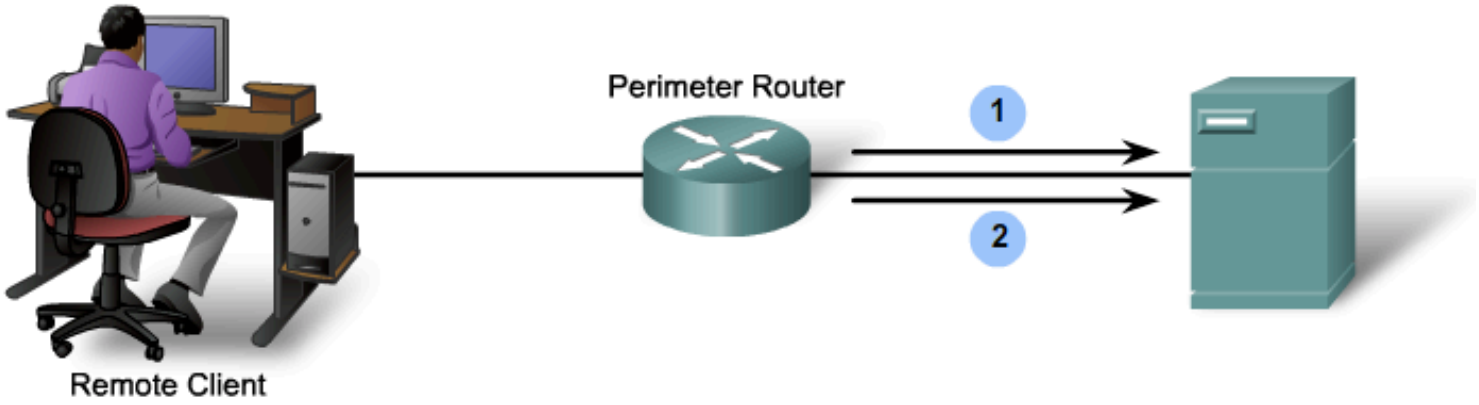
1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server.
4. The user is authorized to access the network based on information on the remote AAA Server.

Authorization



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.

Accounting

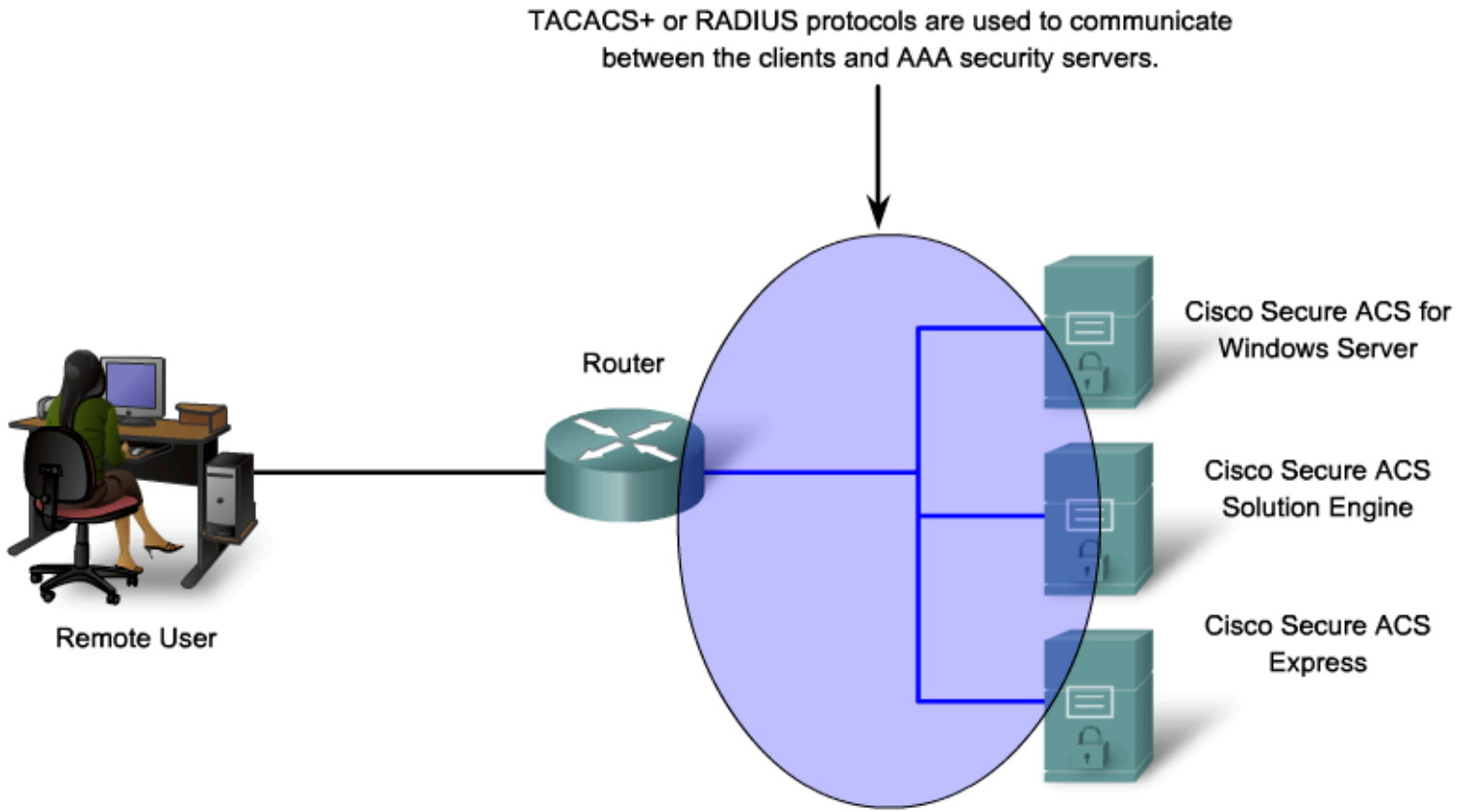


1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded and the accounting process ends.

Authentication Protocols

- TACACS+ Terminal Access Control Access Control Server Plus
- RADIUS Remote Access Dial In User Services

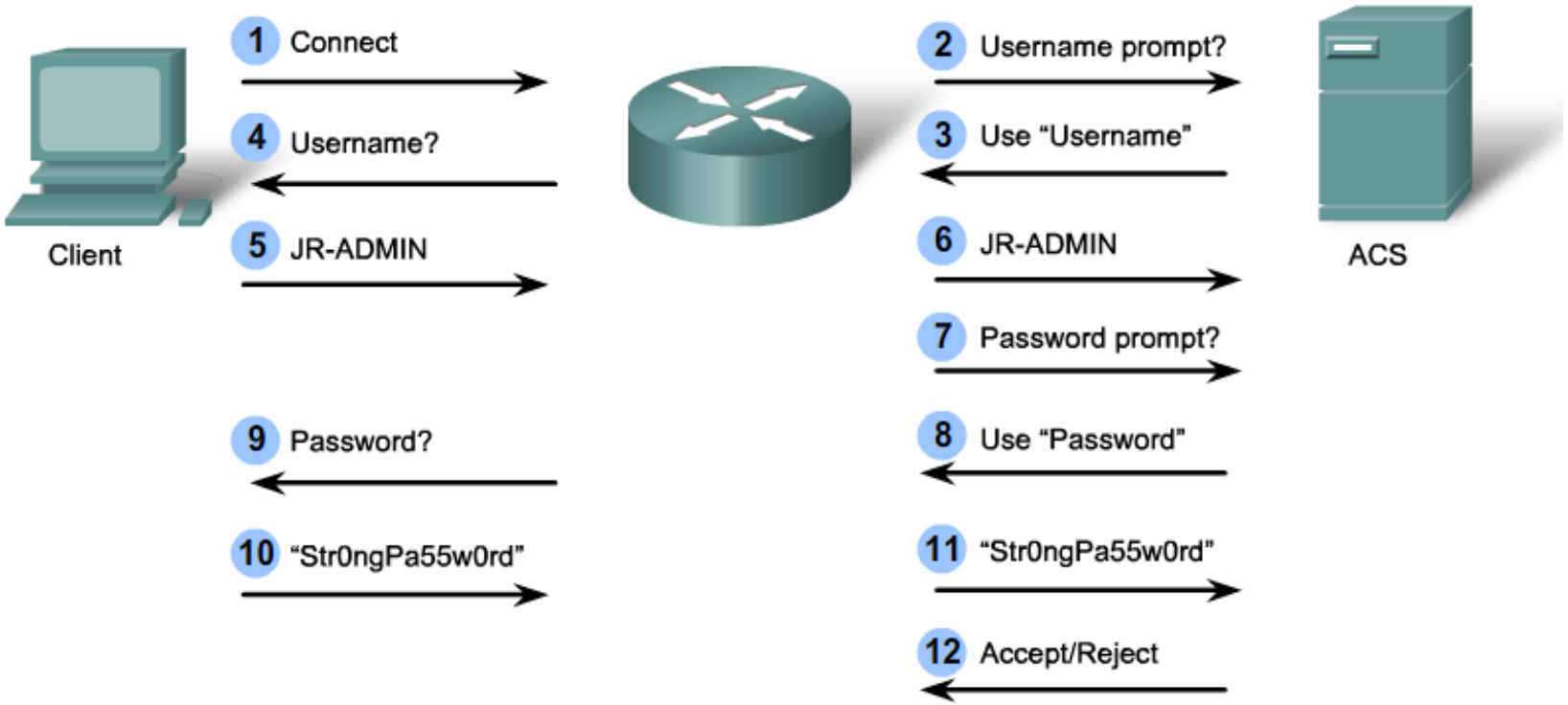
Authentication Protocols



TACACS+

- Is incompatible with TACACS and XTACACS
- Separates authentication and authorization
- Encrypts all communication
- Utilizes TCP port 49

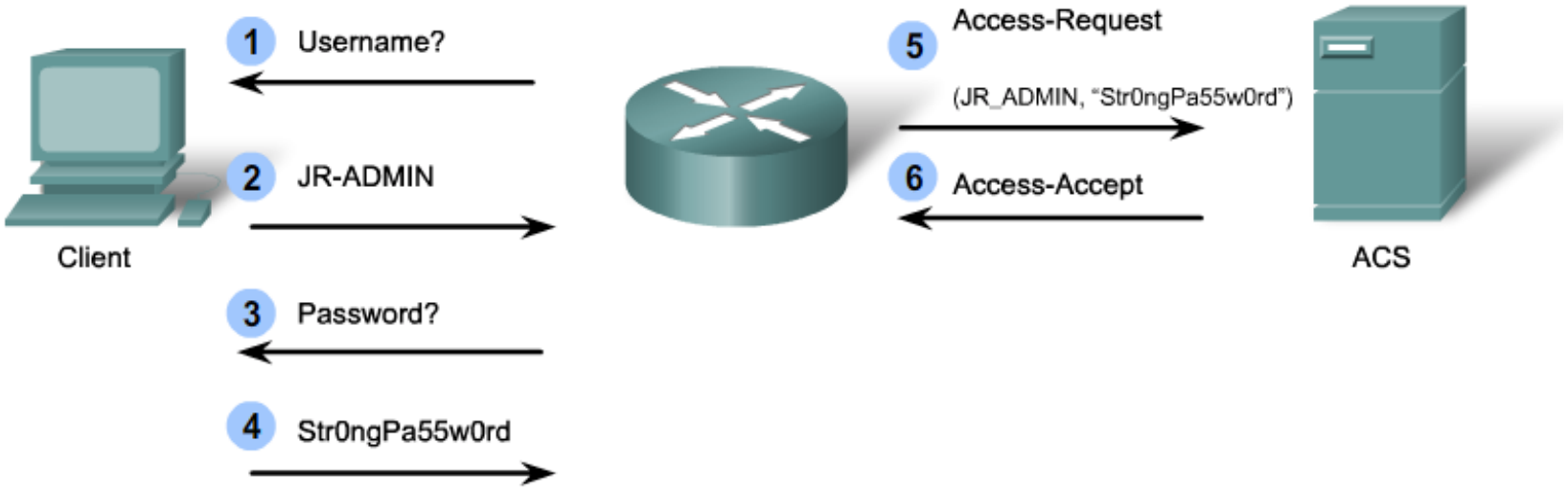
TACACS+


1 Connect
2 Username prompt?
3 Use "Username"
4 Username?
5 JR-ADMIN
6 JR-ADMIN
7 Password prompt?
8 Use "Password"
9 Password?
10 "Str0ngPa55w0rd"
11 "Str0ngPa55w0rd"
12 Accept/Reject
Client
ACS

RADIUS

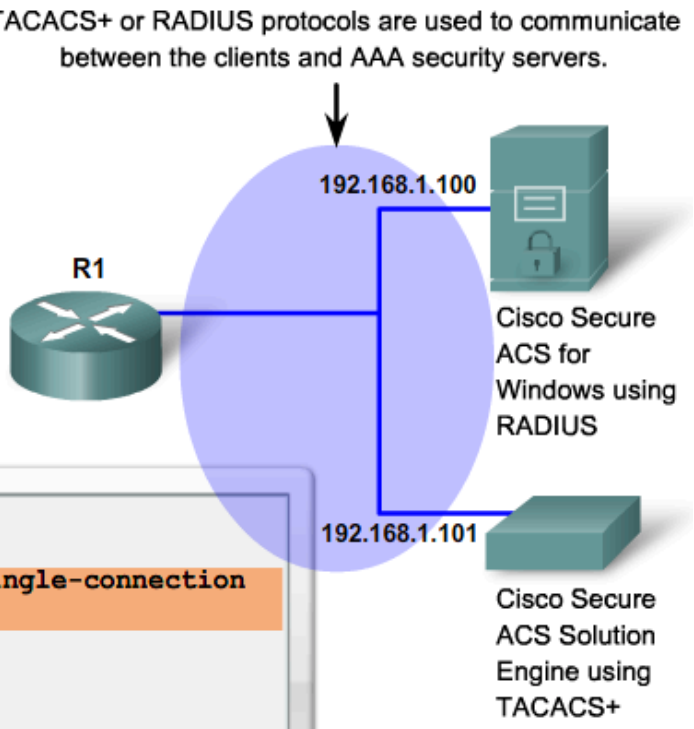
- Uses RADIUS proxy servers for scalability
- Combines RADIUS authentication and authorization as one process.
- Encrypts only the password
- Utilizes UDP

RADIUS


1 Username?
2 JR-ADMIN
3 Password?
4 Str0ngPa55w0rd
5 Access-Request
(JR_ADMIN, "Str0ngPa55w0rd")
6 Access-Accept
Client
ACS

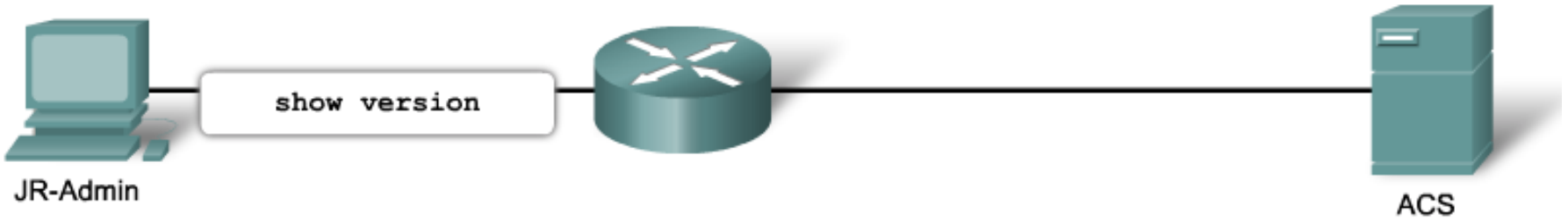
Configuration Authentication

Cisco.com



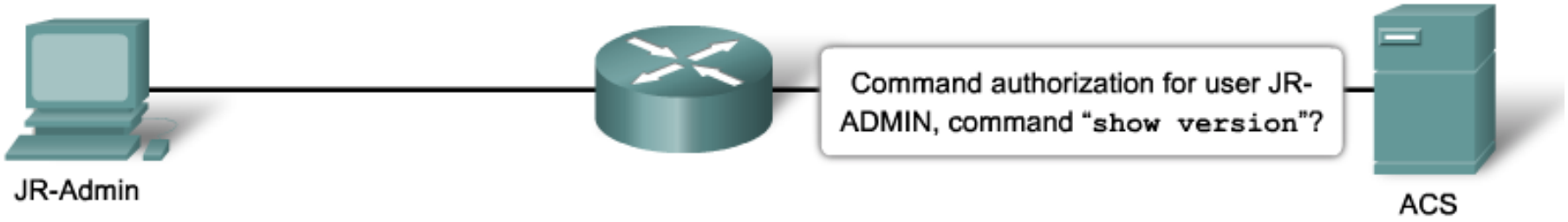

```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs-server host 192.168.1.101 single-connection
R1(config)# tacacs-server key TACACS+Pa55W0rd
R1(config)#
R1(config)# radius-server host 192.168.1.100
R1(config)# radius-server key RADIUS-Pa55w0rd
R1(config)#
R1(config)# aaa authentication login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

Authorization 1

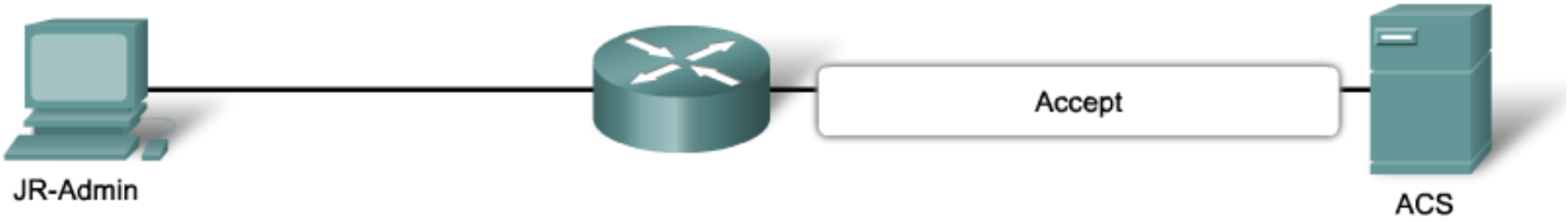


The JR-ADMIN has successfully Telneted and authenticated to the TACACS+ AAA ACS Server.

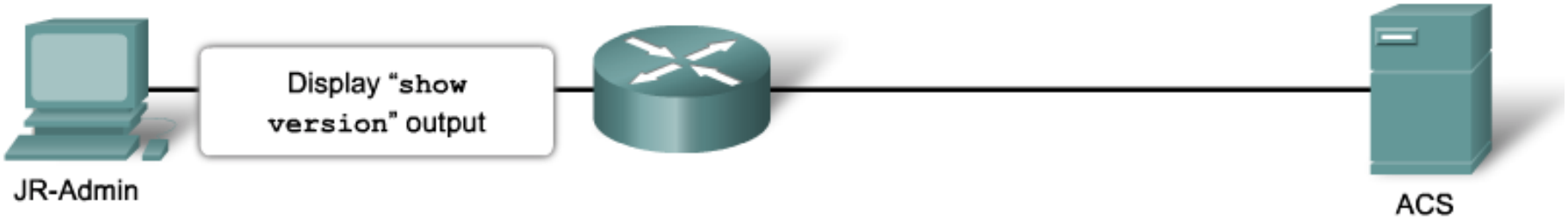
Authorization 2



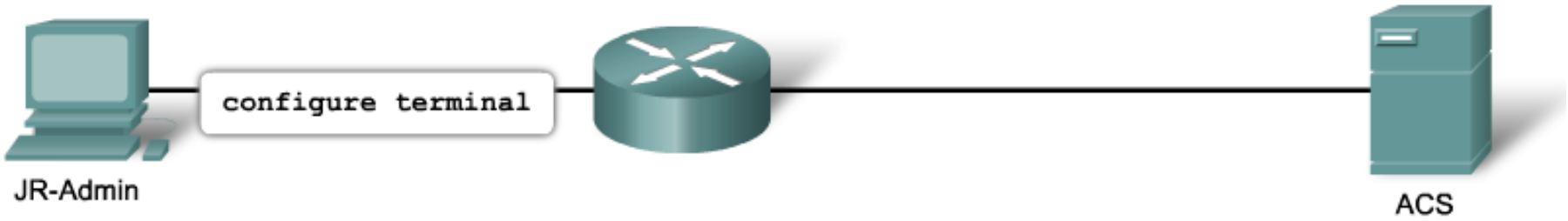
Authorization 3



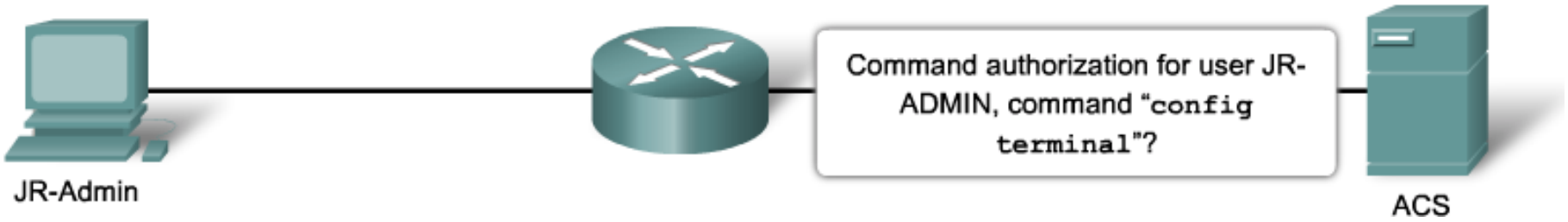
Authorization 4



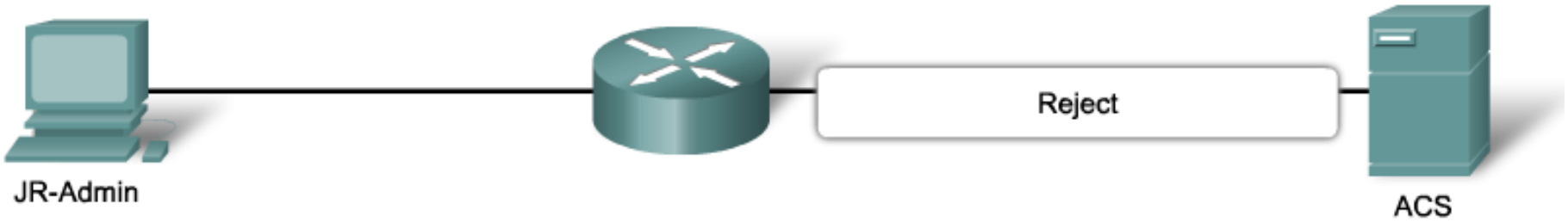
Authorization 5



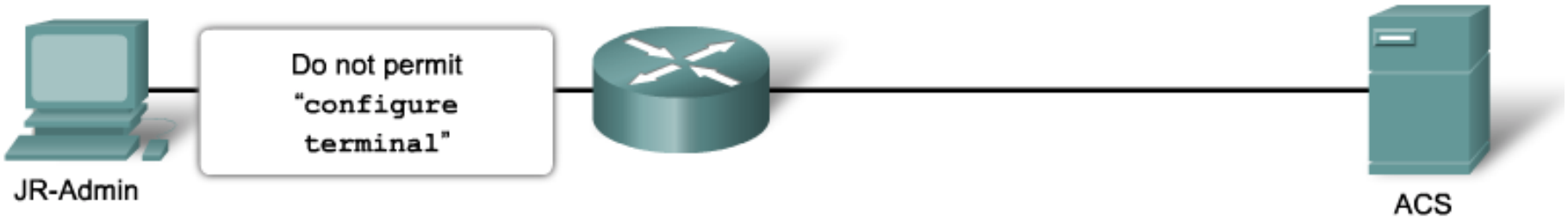
Authorization 6



Authorization 7



Authorization 8



Configuration Authorization


```
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 authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
```

Configuration

- When AAA authorization is not enabled, all users are allowed full access. After authentication is started, the default changes to allow no access. This means that the administrator must create a user with full access rights before authorization is enabled. Failure to do so immediately locks the administrator out of the system the moment the aaa authorization command is entered. The only way to recover from this is to reboot the router. If this is a production router, rebooting might be unacceptable. Be sure that at least one user always has full rights.

Configuration Accounting


```
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 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+
```