Computer Security

Labs

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

Outlines

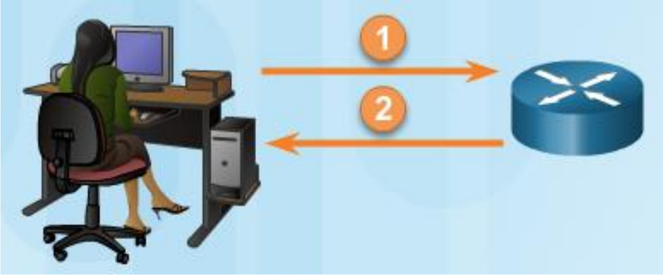
- Server- based AAA protocol
- Role-based CLI
- Firewall examples.

Server-Based AAA

Comparing Local AAA and Server-Based AAA Implementations

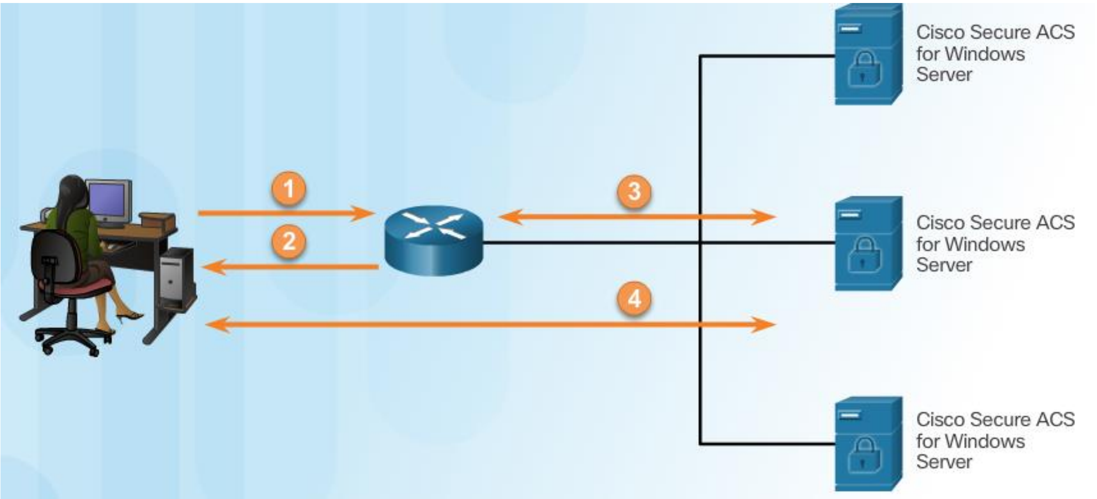
Local authentication:

1. User establishes a connection with the router.
2. Router prompts the user for a username and password, authentication the user using a local database.

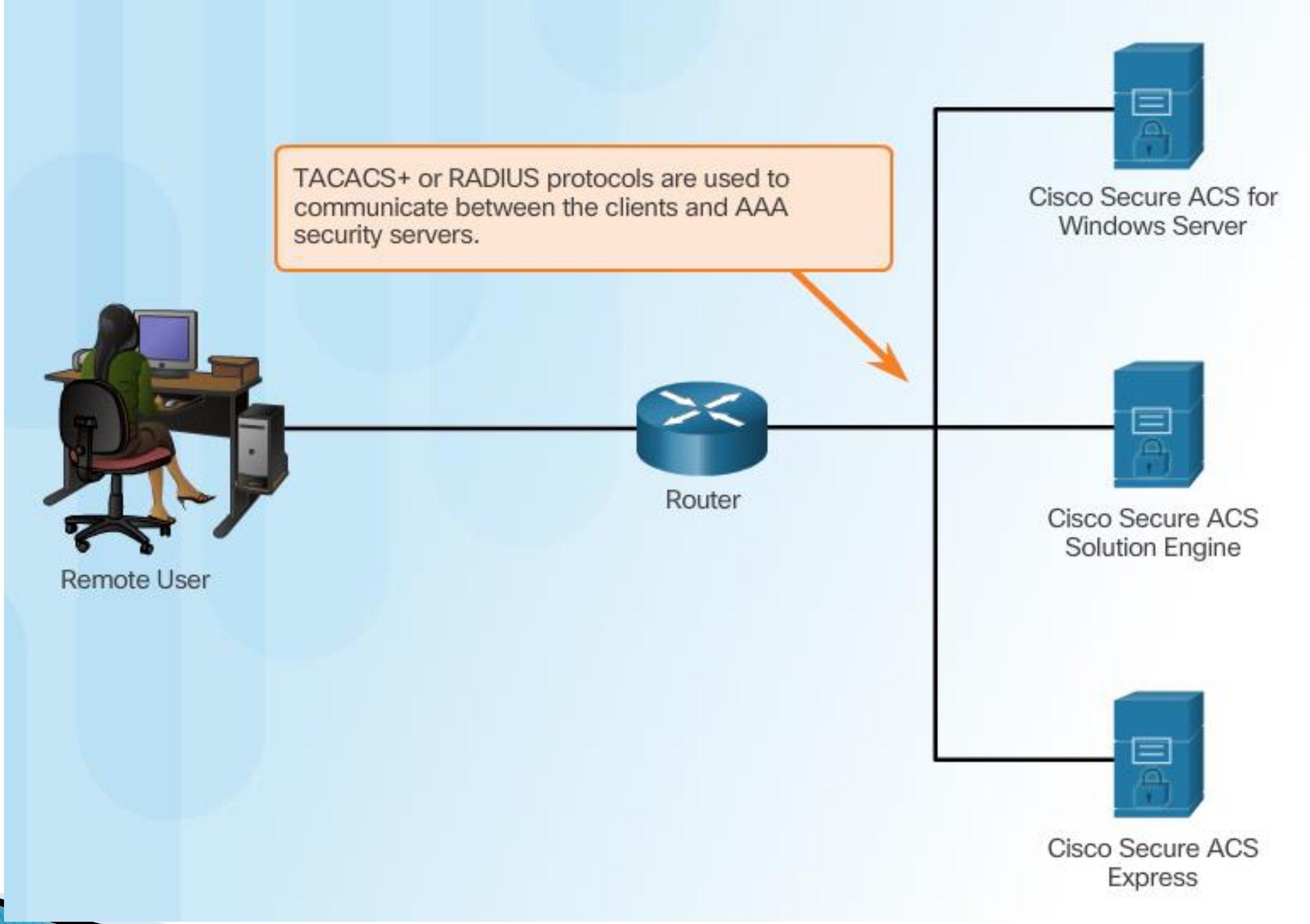


Server-based authentication:

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.


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

Introducing Cisco Secure Access Control System

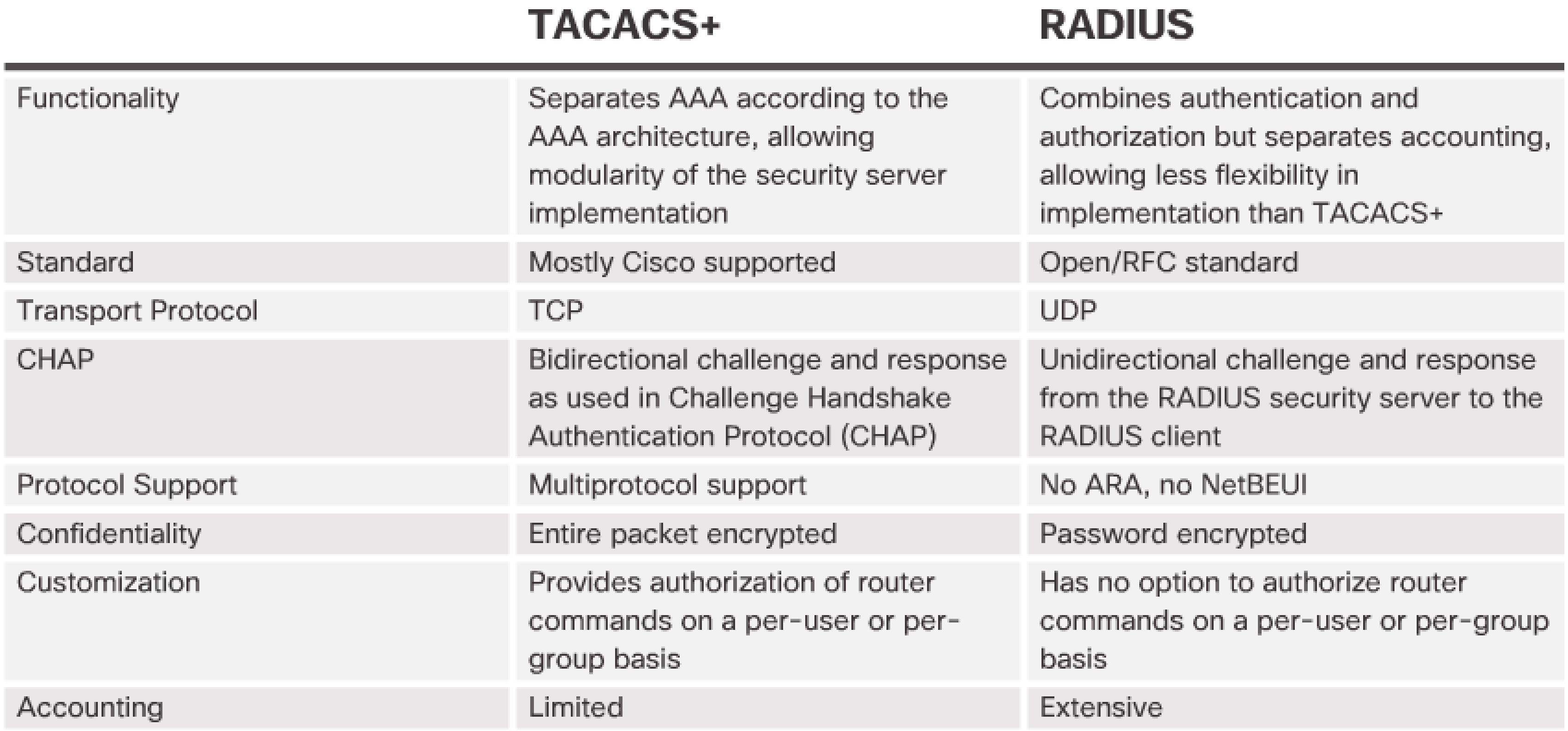


TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.

Remote User
Router
Cisco Secure ACS for Windows Server
Cisco Secure ACS Solution Engine
Cisco Secure ACS Express

Server-Based AAA Communication Protocols

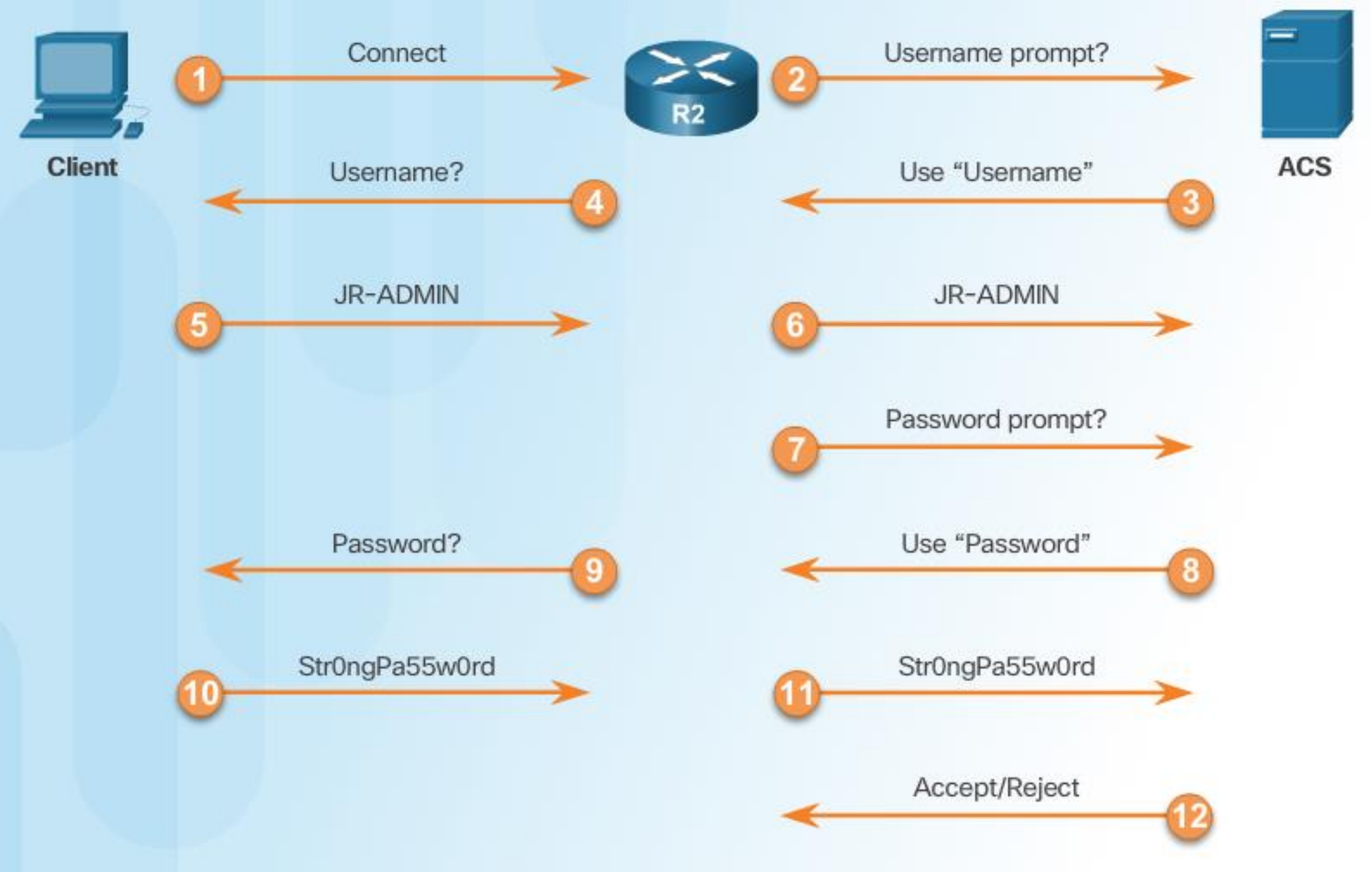
Introducing TACACS+ and RADIUS



	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

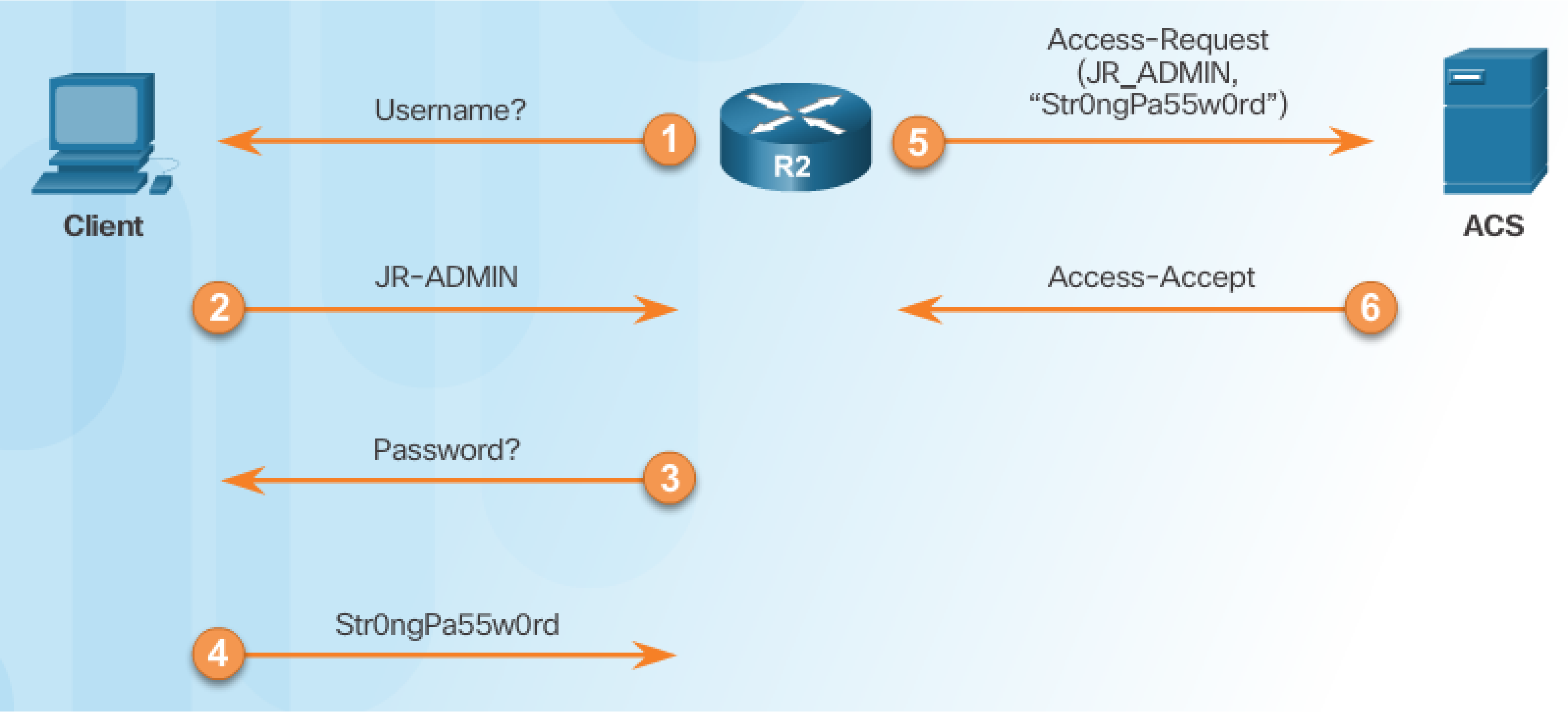
TACACS+ Authentication

TACACS+ Authentication Process



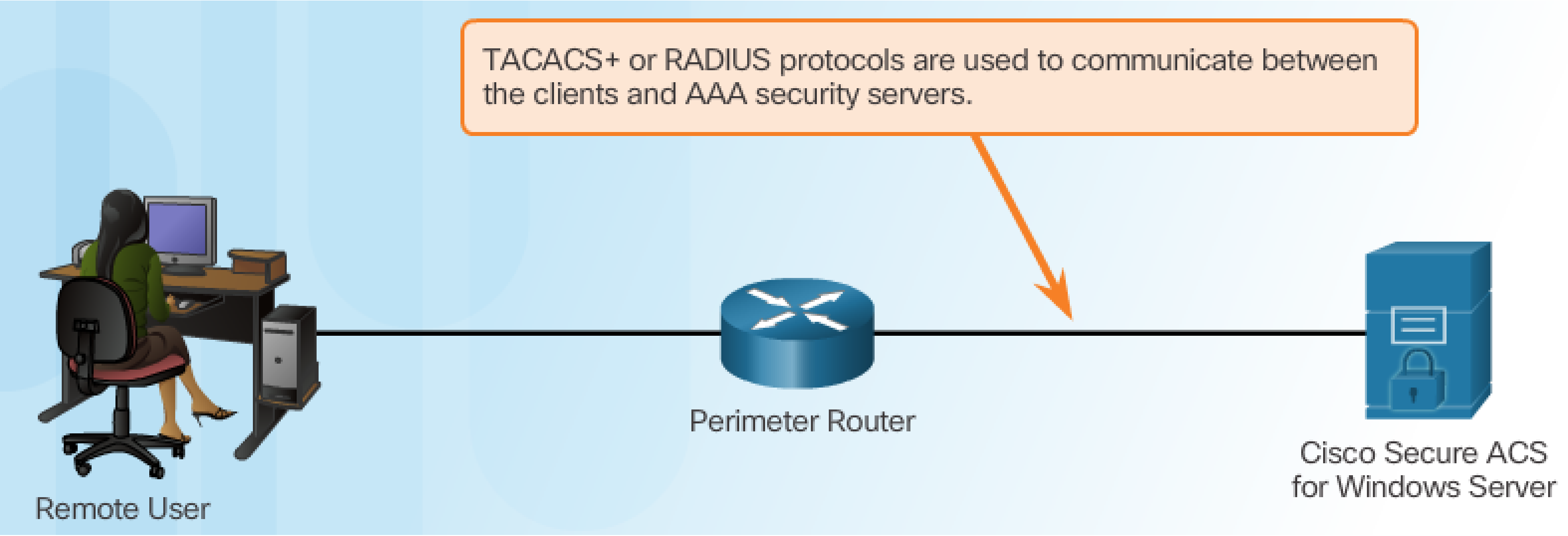
RADIUS Authentication

RADIUS Authentication Process



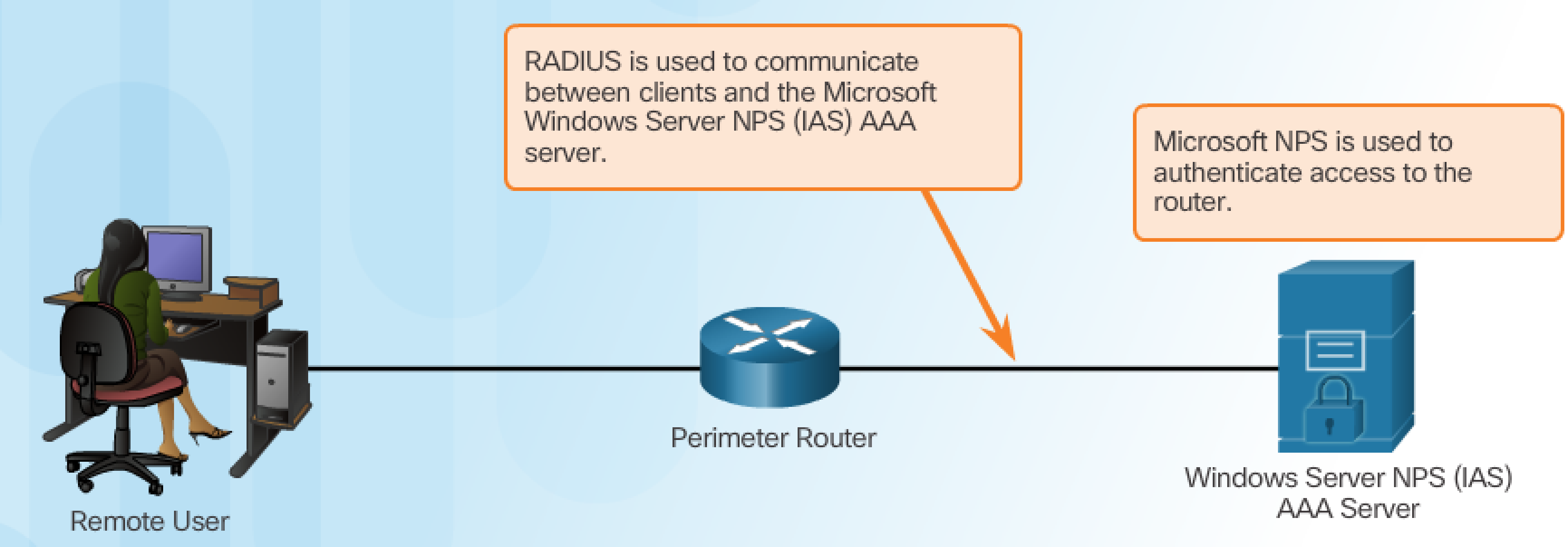
Integration of TACACS+ and ACS

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.

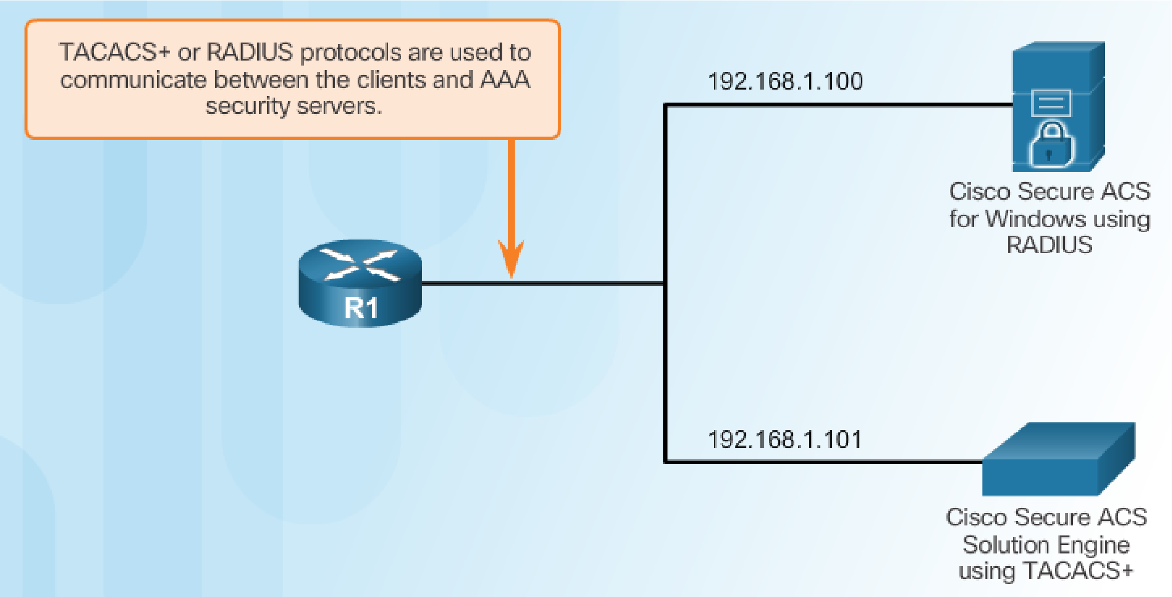
Server-Based AAA Authentication

Steps for Configuring Server-Based AAA Authentication with CLI

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.

Configuring the CLI with TACACS+ Servers

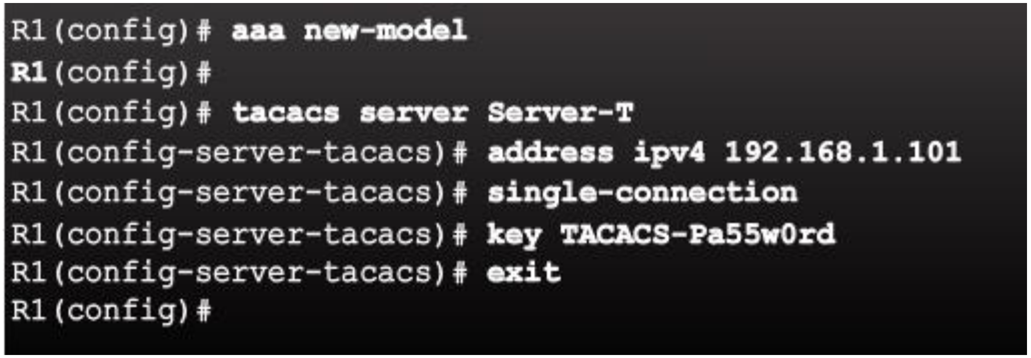
Server-Based AAA Reference Topology



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+

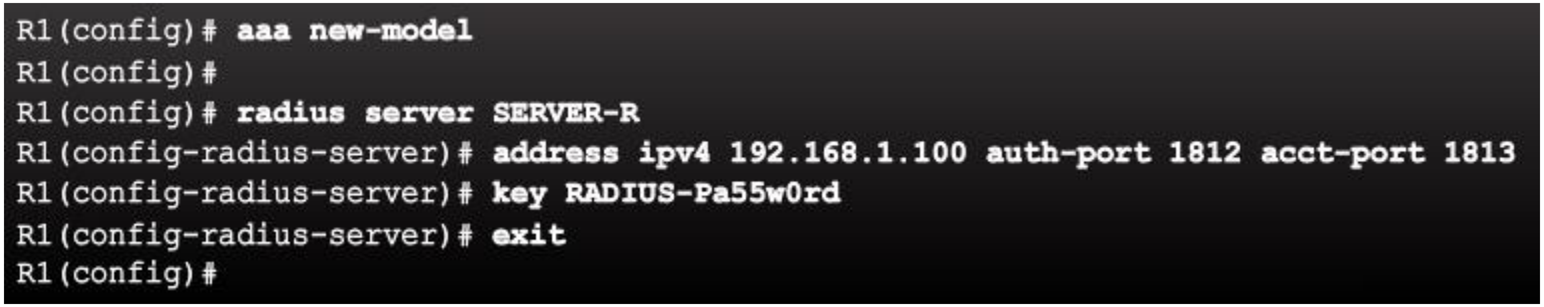
Configure a AAA TACACS+ Server



```
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 the CLI for RADIUS Servers

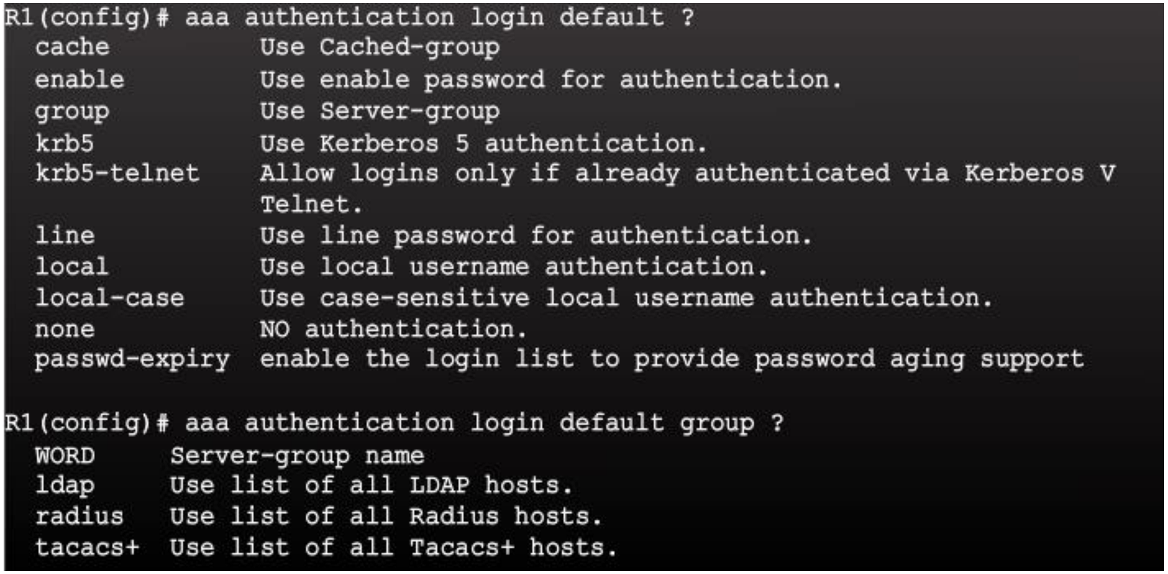
Configure a AAA RADIUS Server



```
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

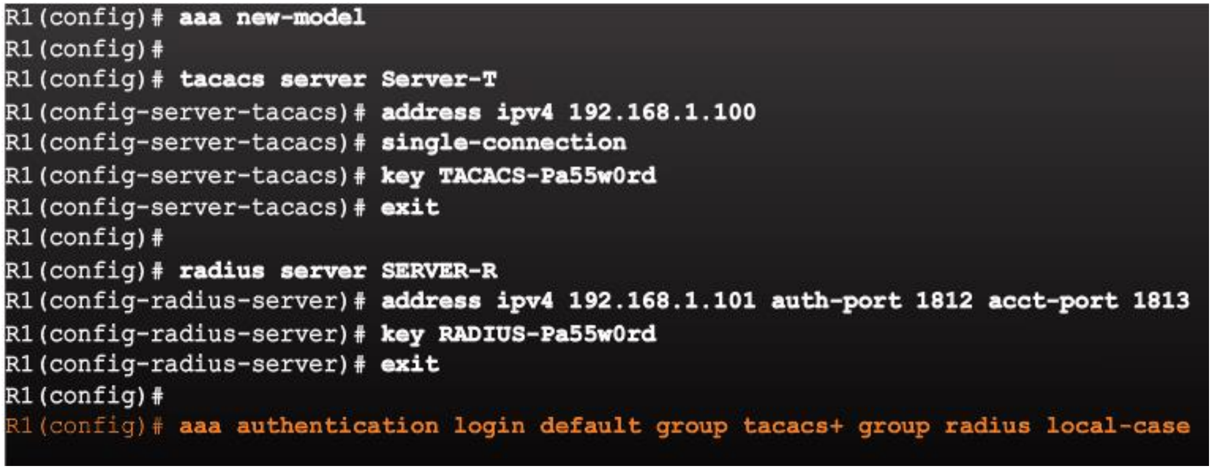
Command Syntax



```
R1(config)# aaa authentication login default ?
  cache          Use Cached-group
  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
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
```

Configure Server-Based AAA Authentication

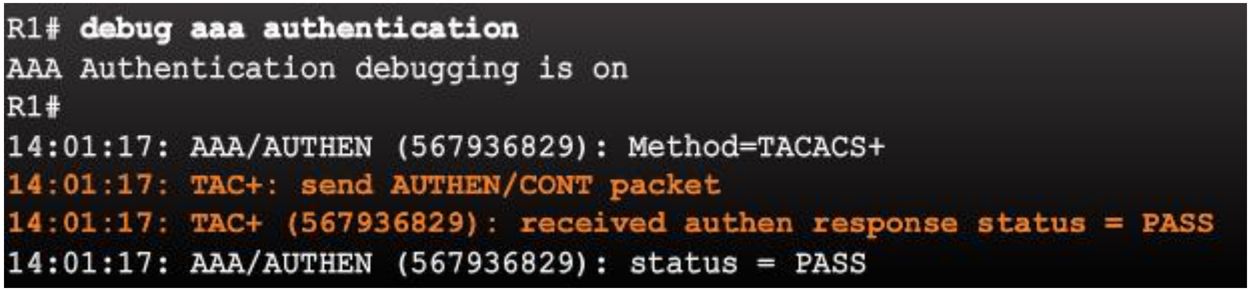


```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs server Server-T
R1(config-server-tacacs)# address ipv4 192.168.1.100
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key TACACS-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)#
R1(config)# radius server SERVER-R
R1(config-radius-server)# 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
```

Troubleshooting Server-Based AAA Authentication

Monitoring Authentication Traffic

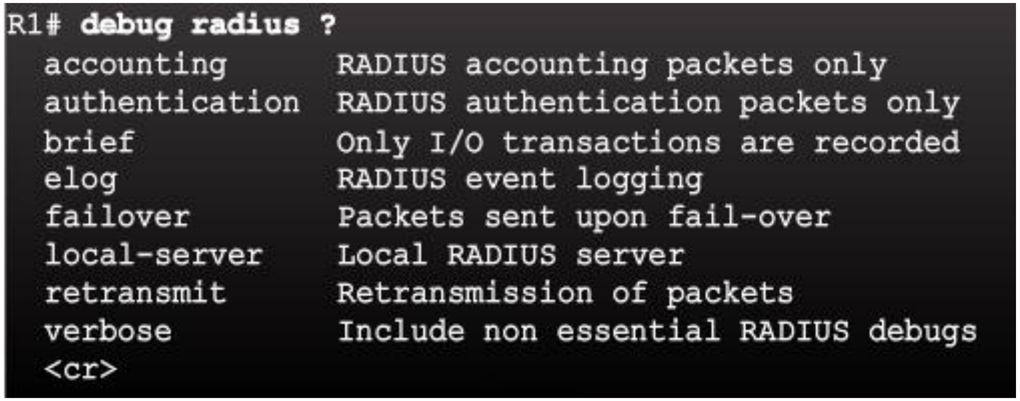
Troubleshooting Server-Based AAA Authentication



```
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
```

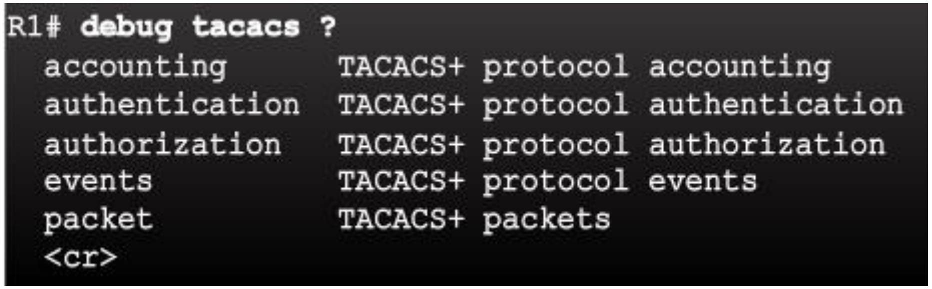
Debugging TACACS+ and RADIUS

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+

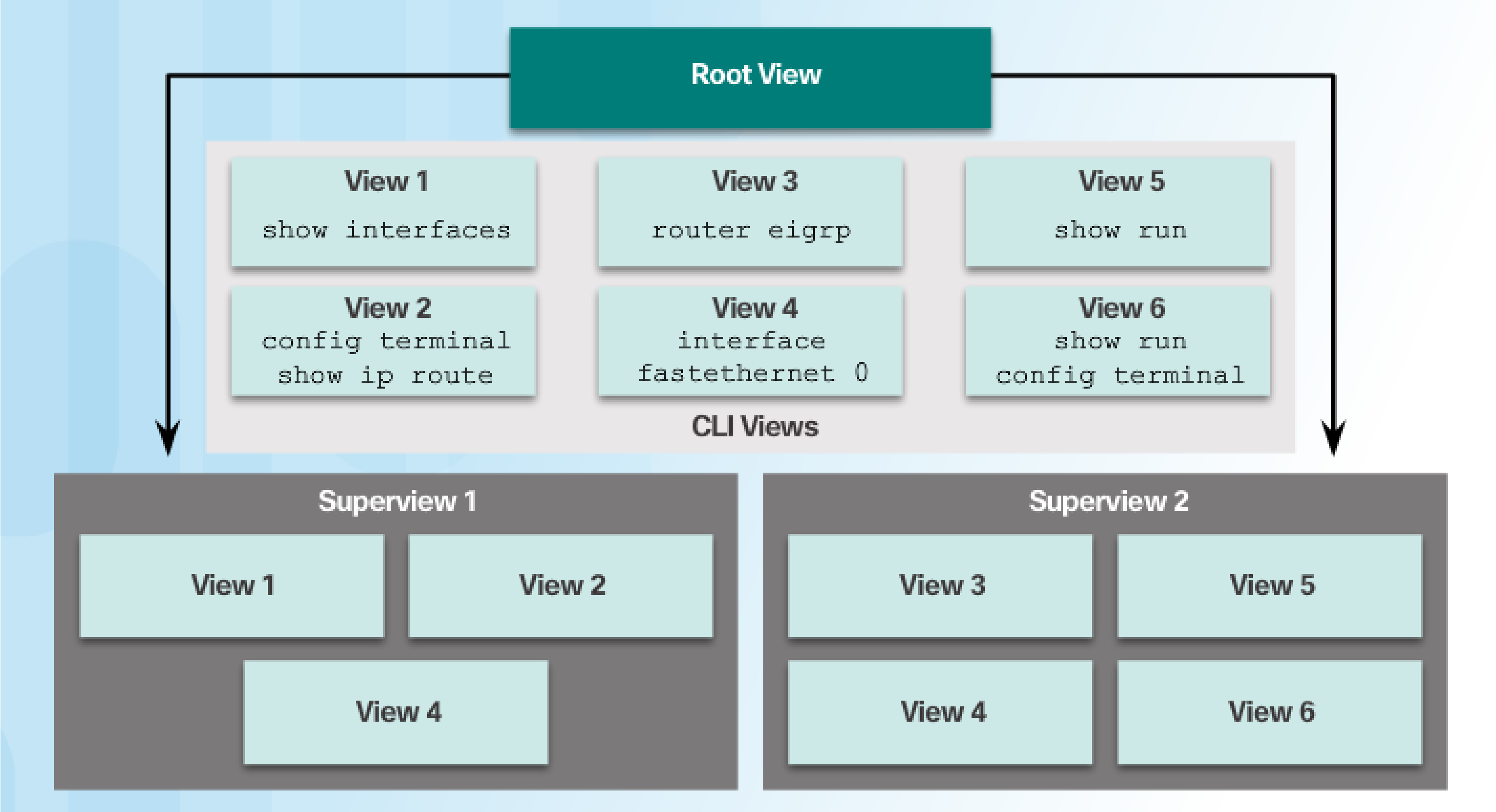


```
R1# debug tacacs ?
  accounting       TACACS+ protocol accounting
  authentication   TACACS+ protocol authentication
  authorization    TACACS+ protocol authorization
  events           TACACS+ protocol events
  packet           TACACS+ packets
  <cr>
```

Limitations of Privilege Levels

- No access control to specific interfaces, ports, logical interfaces, and slots on a router
- Commands available at lower privilege levels are always executable at higher privilege levels
- Commands specifically set at higher privilege levels are not available for lower privilege users
- Assigning a command with multiple keywords allows access to all commands that use those

Role-Based Views



Root View

View 1
show interfaces

View 3
router eigrp

View 5
show run

View 2
config terminal
show ip route

View 4
interface
fastethernet 0

View 6
show run
config terminal

CLI Views

Superview 1

View 1

View 2

View 4

Superview 2

View 3

View 5

View 4

View 6

Superviews contain Views but not commands. Two Superviews can use the same View.
For example, both Superview 1 and Superview 2 can have CLI View 4 placed inside.

Example

- View1
  - Ping
  - telnet
  - Show ip route
- View2
  - reload
  - Config t
- View3
  - Config t
  - Show run

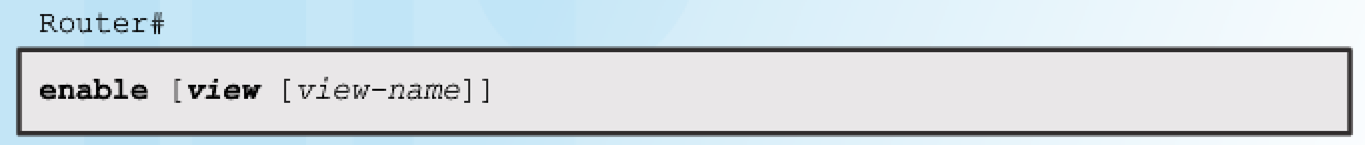
Views

- View4
  - Config t
  - router
  - copy running-config startup-config
- View5
  - Config t
  - interface
  - ping
- Ali → View1
- Ahmed → View2
- Sara → View3,4
- Nour → View 2,5

Permissions

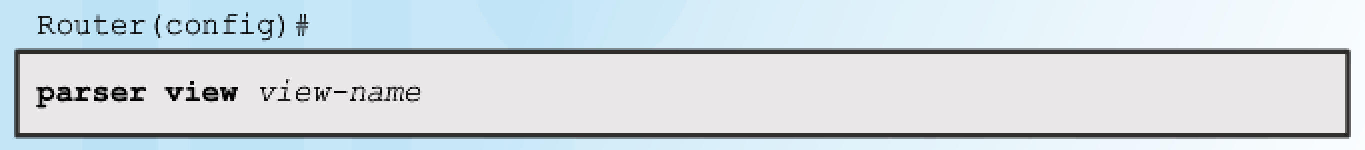
Configuring Role-Based Views

Step 1



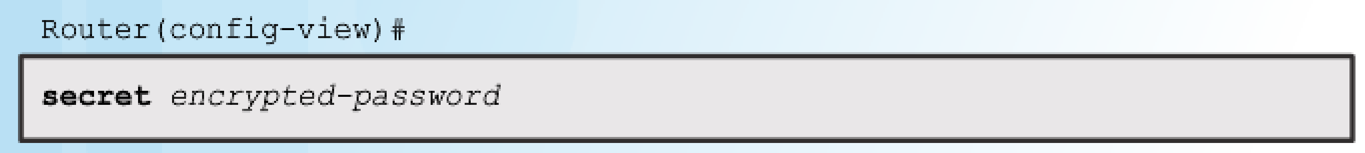
```
Router#
enable [view [view-name]]
```

Step 2



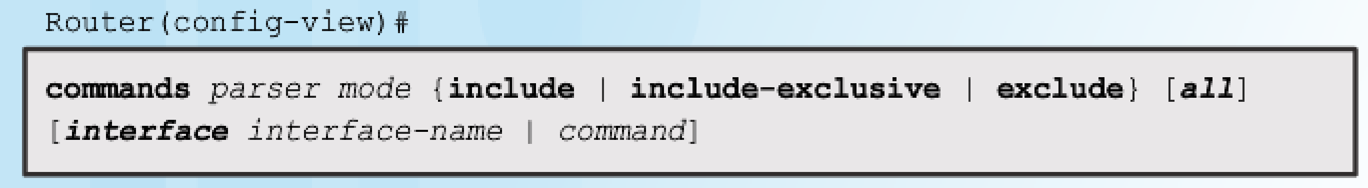
```
Router(config)#
parser view view-name
```

Step 3



```
Router(config-view)#
secret encrypted-password
```

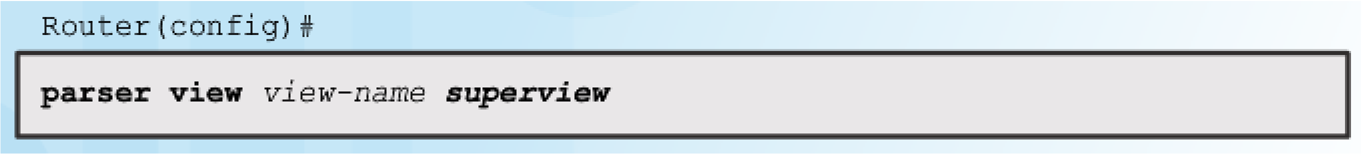
Step 4



```
Router(config-view)#
commands parser mode {include | include-exclusive | exclude} [all]
[interface interface-name | command]
```

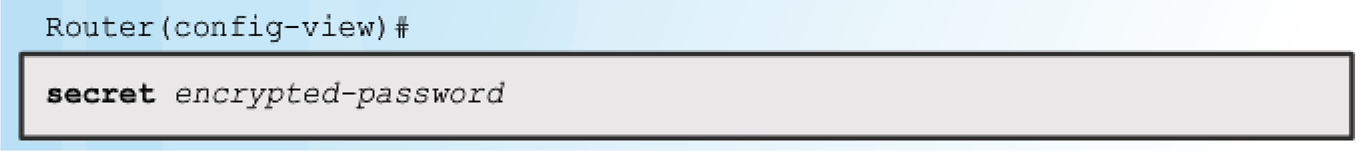
Configuring Role-Based CLI Superviews

Step 1



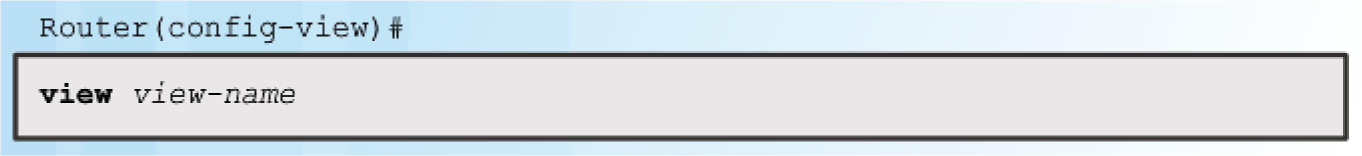
```
Router(config)#
parser view view-name superview
```

Step 2



```
Router(config-view)#
secret encrypted-password
```

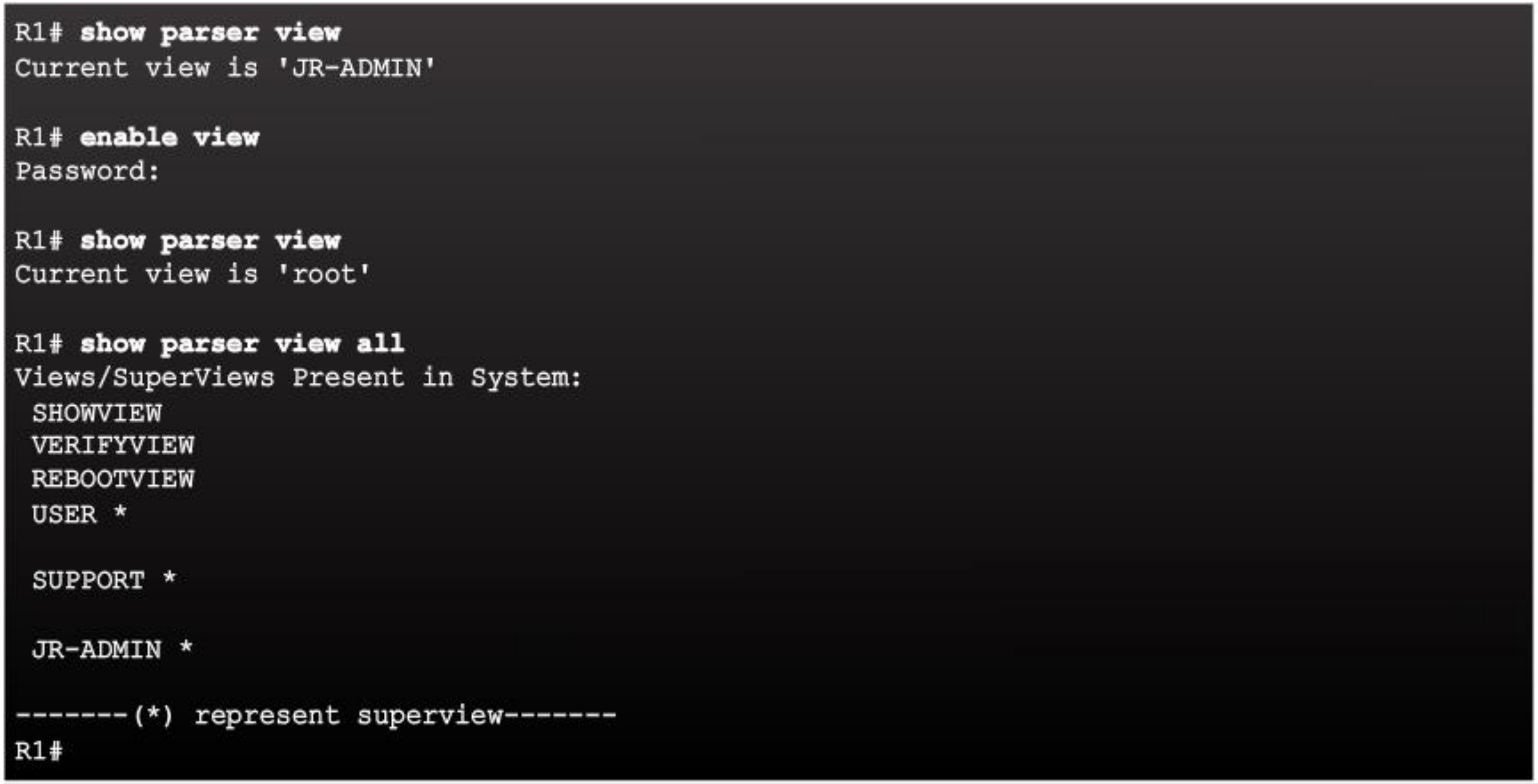
Step 3



```
Router(config-view)#
view view-name
```

Verify Role-Based CLI Views

Enable Root View and Verify All Views



```
R1# show parser view
Current view is 'JR-ADMIN'

R1# enable view
Password:

R1# show parser view
Current view is 'root'

R1# show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
 USER *

 SUPPORT *

 JR-ADMIN *

-------(*) represent superview-------
R1#
```