Some examples of configuring CLI views:

```
R1(config)# parser view SHOWVIEW
R1(config-view)# secret cisco
R1(config-view)# commands exec include show version
R1(config-view)# exit
R1#
R1(config)# parser view VERIFYVIEW
R1(config-view)# secret cisco5
R1(config-view)# commands exec include ping
R1(config-view)# exit
R1#
R1(config)# parser view CONFIGVIEW
R1(config-view)# secret cisco10
R1(config-view)# commands exec include configure terminal
R1(config-view)# commands configure include interface
R1(config-view)# exit
```

13

After configuration, you may verify available commands in the CLI view as follows:

```
R1> enable view SHOWVIEW
Password:
R1#
R1# ?
Exec commands:
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  show        Show running system information
R1#
R1# show ?
  parser      Display parser information
  version     System hardware and software status
```

By default, enable, exit and show parser commands are always available.

14

Optionally, superview can be configured, examples as follows:

Creating superviews USER, SUPPORT and ADMIN:

```
R1(config)# parser view USER superview
R1(config-view)# secret cisco
R1(config-view)# view SHOWVIEW
R1(config-view)# exit
R1#
R1(config)# parser view SUPPORT superview
R1(config-view)# secret cisco1
R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# exit
R1#
R1(config)# parser view ADMIN superview
R1(config-view)# secret cisco2
R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# view CONFIGVIEW
R1(config-view)# exit
```

15

You may also verify available commands in superviews as follows:

```
R1# enable view ADMIN
Password:
R1# ?
Exec commands:
  configure   Enter configuration mode
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  ping        Send echo messages
  show        Show running system information
R1# config t
R1(config)# ?
Configure commands:
  do-exec     To run exec commands in config mode
  end         Exit from configure mode
  exit        Exit from configure mode
  interface   Select an interface to configure
```

16

Lab Exercise 1B

1.2 Configure device access authorization using role-based CLI views.

9

Privilege level has the problem that commands at lower level are always available for higher privilege users. Thus a more flexible RBAC using views to define roles is developed.

Views allow you to pick and choose which commands are available according to roles, and are divided into 3 types:

- Root view: for creating views and superviews, similar as privilege level 15

- CLI view: for defining a set of available commands

- Superview (optional): for grouping CLI views, but not commands

10

To begin defining roles using views, enable root view in aaa new-model and then configure new CLI view as follows:

```
R1(config)# aaa new-model
R1(config)# exit
R1# enable view
Password:
R1#
R1# configure terminal
R1(config)# parser view VIEWNAME

R1(config-view)# secret viewpassword
R1(config-view)# commands exec include ...
R1(config-view)# commands exec exclude ...
R1(config-view)# commands exec include all ...
R1(config-view)# ...
R1(config-view)# exit
R1(config)#
```

1. Enable AAA to create views
2. Go to root view
3. Enter the same enable secret password
4. Create new CLI view
5. Password for new view
6. Pick and choose commands for view

Note: Only a maximum of 15 views can be created.

11

The parameters for you to pick and choose commands for CLI views are as follows:

```
commands parser-mode {include | include-exclusive | exclude}
[all] command
```

Parameter	Description
parser-mode	Specifies the mode in which the specified command exists (e.g. exec, configure).
include	Adds a command or an interface to the view and allows the same command or interface to be added to an additional view.
include-exclusive	Adds a command or an interface to the view and excludes the same command or interface from being added to all other views.
exclude	Excludes a command or an interface from the view; that is, users cannot access a command or an interface.
all	(Optional) Specifies a "wildcard" that allows every command in a specified configuration mode that begins with the same keyword or every subinterface for a specified interface to be part of the view.
command	Specifies a command that is added to the view.

12

Except for the five level 0 commands, all CLI commands are initially assigned to level 1 or level 15, but can be reconfigured to different custom privilege levels between 2 – 14 as follows:

To reconfigure command(s) to new privilege level:

```
R1(config)# privilege exec level level command-string
```

e.g.

```
R1(config)# privilege exec level 5 ping
```

For security, a password can be configured for the new privilege level; e.g.

```
R1(config)# enable secret level 5 cisco5
```

To reset command(s) to default privilege level:

```
R1(config)# privilege exec reset command-string
```

5

To run a command, a user must be at the same or higher privilege level as the command as shown below:

```
R1> show privilege
Current privilege level is 1
R1# ping 10.10.10.1
          ^
% Invalid input detected at '^' marker.

R1> enable 5
Password: <enter cisco5>
R1#
R1# show privilege
Current privilege level is 5
R1#
R1# ping 10.10.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1#
```

6

To simplify administration, privilege levels can be assigned to users directly so that they will enter at the assigned privilege level upon successful login.

An example of assigning 4 different users – USER, SUPPORT, JR-ADMIN and ADMIN – with different privilege levels to access the network device:

```
R1(config)# username USER privilege 1 secret cisco
R1(config)#
R1(config)# privilege exec level 5 ping
R1(config)# enable secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 secret cisco5
R1(config)#
R1(config)# privilege exec level 10 reload
R1(config)# enable secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 secret cisco10
R1(config)#
R1(config)# username ADMIN privilege 15 secret cisco123
```

7

If using AAA, privilege levels can also be assigned directly to users using the AAA authorization commands as follows:

```
R1(config)# aaa new-model
R1(config)# ...
R1(config)# aaa authentication login default group tacacs+
group radius local
R1(config)# aaa authorization exec default group tacacs+
group radius local
```

Correspondingly, users in AAA servers must be configured with appropriate privilege levels, e.g.

- For tacacs.net, in authorization.xml

```
<AutoExec>
    <Set>priv-lvl=5</Set>
</AutoExec>
```

- For freeRADIUS, in file 'users':

```
wendell   Cleartext-Password := "odom"
          cisco-avpair = "shell:priv-lvl=5"
```

8

ICT2203
Network Security

Lab 7.2 and 7.3 Notes:

Device Access Control with AAA – Authentication, Authorization and Accounting

2021-2022 Trimester 3

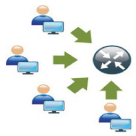
Lab Exercise 1A

1.1 Configure device access authorization using privilege level.

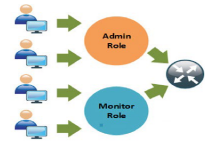
2

After successful authentication, users should not be given more access rights than necessary which brings us to the topic of authorization.

Theoretically, there are different access control models for implementing authorization.



Assigning rights directly to each user; e.g. privilege level



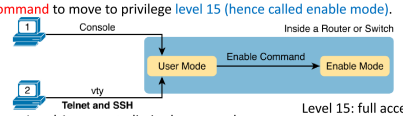
Assigning rights to roles which is then assigned to each user; e.g. CLI views

3

By default, authorization in Cisco devices is implemented using privilege levels in 3 pre-defined levels:

Privilege Level	Result
1	User level only (prompt is router>), the default level for login
15	Privileged level (prompt is router#), the level after going into enable mode
0	Seldom used, but includes five commands: disable, enable, exit, help, and logout

Upon login, users are placed at level 1 (user mode) , and can use enable command to move to privilege level 15 (hence called enable mode).



Level 1: access to limited commands; e.g. read-only commands like show

Level 15: full access to all commands

4

And here is a sample of exec log in tacacs.net server which can be found in c:\Users\All Users\TACACS.net\Logs\Accounting_...

A 'start' message is logged when the exec shell started:

```
<102> 2017-11-09 03:57:41 [192.168.1.200:43972]
11/09/2017 03:57:41 NAS_IP=192.168.1.200 Port=tty1
rem_addr=192.168.1.3 User=wendell Flags=Start task_id=25
timezone=UTC service=shell
```

A 'stop' message is logged when the exec shell ended:

```
<102> 2017-11-09 03:58:04 [192.168.1.200:32751]
11/09/2017 03:58:04 NAS_IP=192.168.1.200 Port=tty1
rem_addr=192.168.1.3 User=wendell Flags=Stop task_id=25
timezone=UTC service=shell disc-cause=1 disc-cause-ext=9
pre-session-time=5 elapsed_time=22 stop_time=731022330
```

25

Finally, AAA accounting is to have a record of what a user has done which is also crucial to security.

One useful type of accounting is 'exec' which provides information about user EXEC terminal session after login.

```
R1(config)# aaa new-model
R1(config)# ...
R1(config)# aaa authentication login default group tacacs+
group radius local
R1(config)# aaa authorization exec default group tacacs+
group radius local
R1(config)# aaa accounting exec default start-stop group
tacacs+ group radius
```

- start-stop: a start message is sent when session begins and a stop message is sent when session ends

21

In addition, you may use show parser view command to verify created views as follows:

```
R1# enable view
Password:
R1#
R1# show parser view
Current view is 'root'
R1#
R1# show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
 USER *
 SUPPORT *
 ADMIN *
-------(*) represent superview-------
R1#
```

17

In addition, TACACS+ (but not RADIUS) supports another useful type of accounting on commands which provide information about specific privilege level commands that a user issues.

```
R1(config)# aaa accounting exec default start-stop group
tacacs+ group radius
R1(config)# aaa accounting commands 15 default stop-only
group tacacs+
```

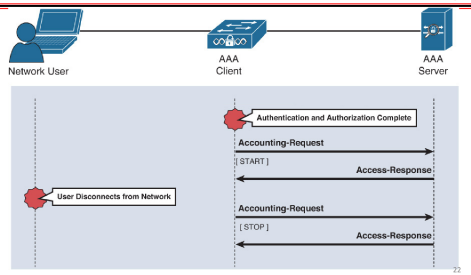
- stop-only: a stop message is sent when command is executed

A sample of commands log in tacacs.net:

```
<102> 2017-11-09 03:57:47 [192.168.1.200:44251]
11/09/2017 03:57:47 NAS_IP=192.168.1.200 Port=tty1
rem_addr=192.168.1.3 User=wendell Flags=Stop task_id=25
timezone=UTC service=shell priv-lvl=15 cmd=show
running-config <cr>
```

26

For RADIUS, accounting is done separately after authentication and authorization are completed as shown:



22

Similar as privilege levels, views can be assigned to users directly so that they will enter at the assigned views upon successful login.

Locally in network device:

```
R1(config)# username Wendell view ADMIN secret odom
```

or centrally using AAA servers:

```
R1(config)# aaa authentication login default group tacacs+
group radius local
R1(config)# aaa authorization exec default group tacacs+
group radius local
```

in tacacs.net:

```
<AutoExec>
    <Set>cli-view-name=ADMIN</Set>
</AutoExec>
```

in freeRADIUS 'users':

```
Wendell   Cleartext-Password := "odom"
          Service-Type = NAS-Prompt-User,
          cisco-avpair = "shell:cli-view-name=ADMIN"
```

18

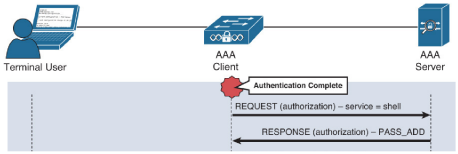
Here's a sample of exec log in freeRADIUS server which can be found at /var/log/freeradius/...

```
Thu Nov  9 13:00:56 2017
    Acct-Session-Id = "0000002F"
    User-Name = "wendell"
    Acct-Authentic = RADIUS
    Acct-Status-Type = Start
    NAS-Port = 1
    NAS-Port-Id = "tty1"
    NAS-Port-Type = Virt
    Service-Type = NAS-P
    NAS-IP-Address = 192
    Acct-Delay-Time = 0
    Event-Timestamp = "N
    Tmp-String-9 = "ai:"
    Acct-Unique-Session-
    Timestamp = 15102324
```

```
Thu Nov  9 13:07:28 2017
    Acct-Session-Id = "0000002F"
    User-Name = "wendell"
    Acct-Authentic = RADIUS
    Acct-Terminate-Cause = User-Request
    Acct-Session-Time = 392
    Acct-Status-Type = Stop
    NAS-Port = 1
    NAS-Port-Id = "tty1"
    NAS-Port-Type = Virtual
    Service-Type = NAS-Prompt-User
    NAS-IP-Address = 192.168.1.200
    Acct-Delay-Time = 0
    Event-Timestamp = "Nov  9 2017 13:07:28 UTC"
    Tmp-String-9 = "ai:"
    Acct-Unique-Session-Id = "f1e1339928a412881fcac9c442105e01"
    Timestamp = 1510232848
```

For TACACS+, authorization is done separately from authentication, whereas for RADIUS, authorization is done together with authentication.

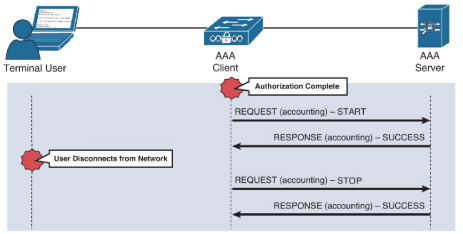
Specifically, TACACS+ authorization consists of a request and a response message to assign privilege level or view as shown:



In contrast, RADIUS authorization is done together with authentication in the same access-request and access-accept message in pg 33.

19

Similarly for TACACS+, accounting is done separately after authorization as shown:



24

Lab Exercise 2

2.1 Configure device access accounting using centralized AAA servers for storing logs.

20