Computer Security

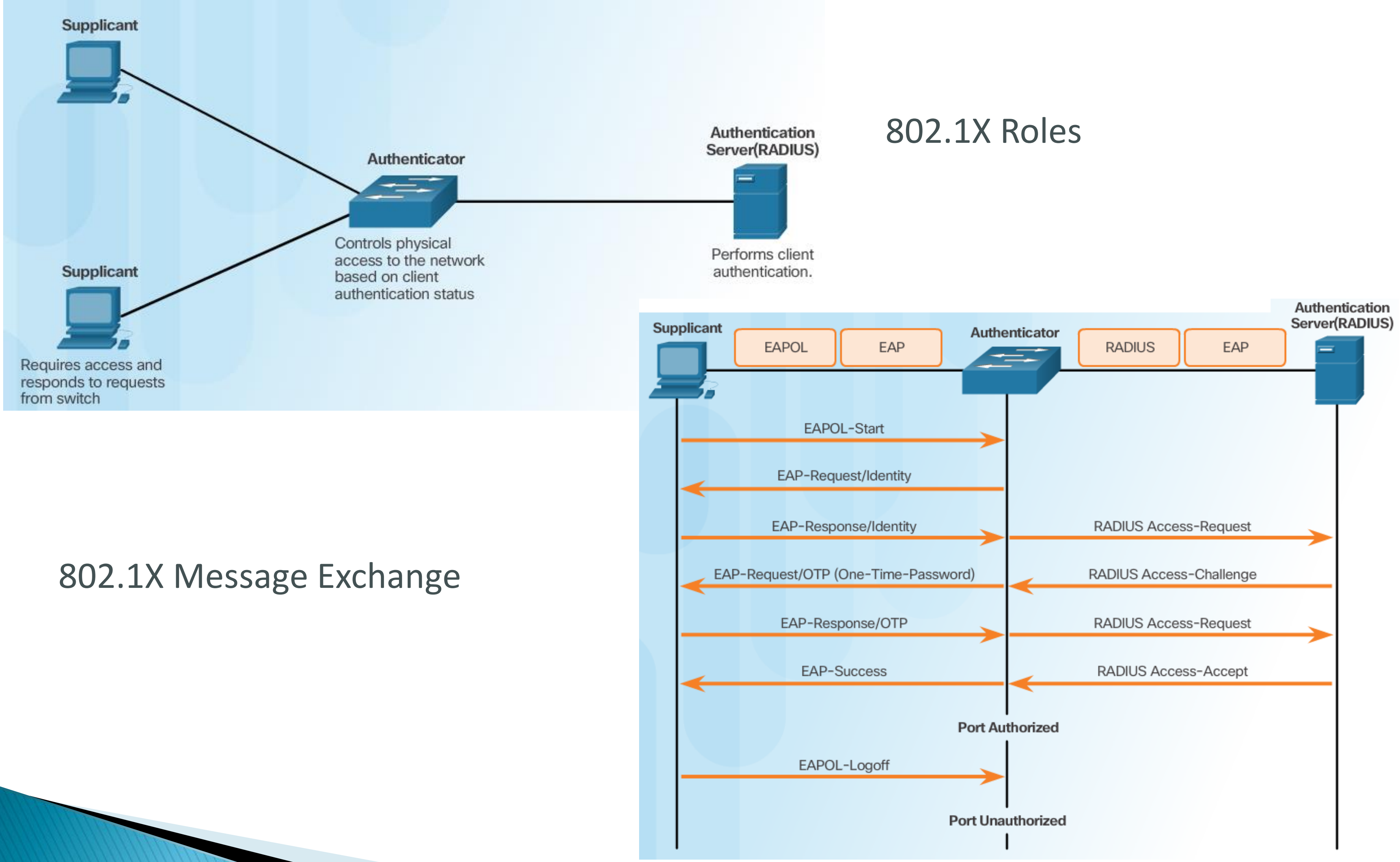
Labs

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

Outlines

- Switch-port security
- Dot 802.1x port authentication protocol.
- Privilege levels

Security Using 802.1X Port-Based Authentication

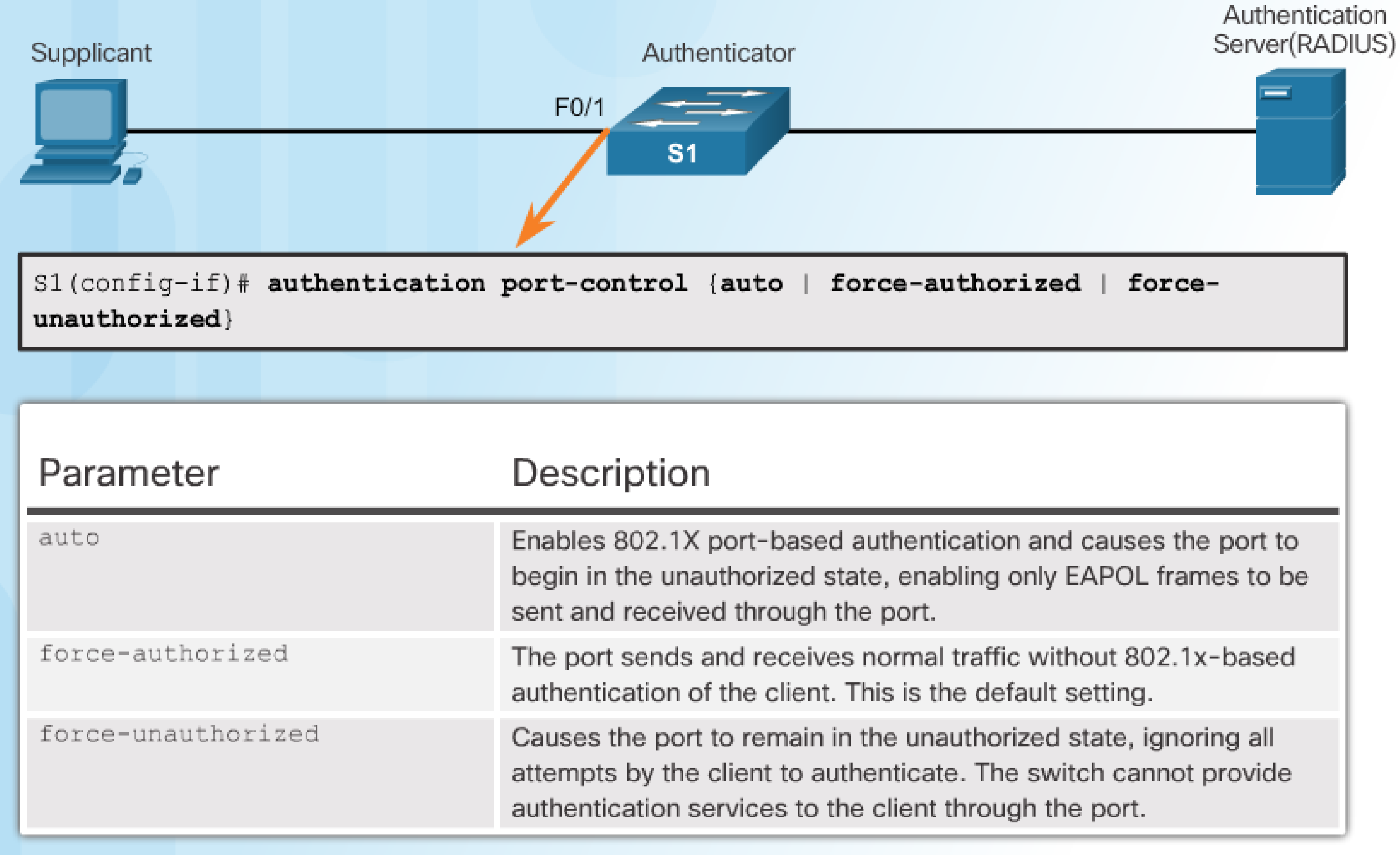


802.1X Roles

802.1X Message Exchange

802.1X Port Authorization State

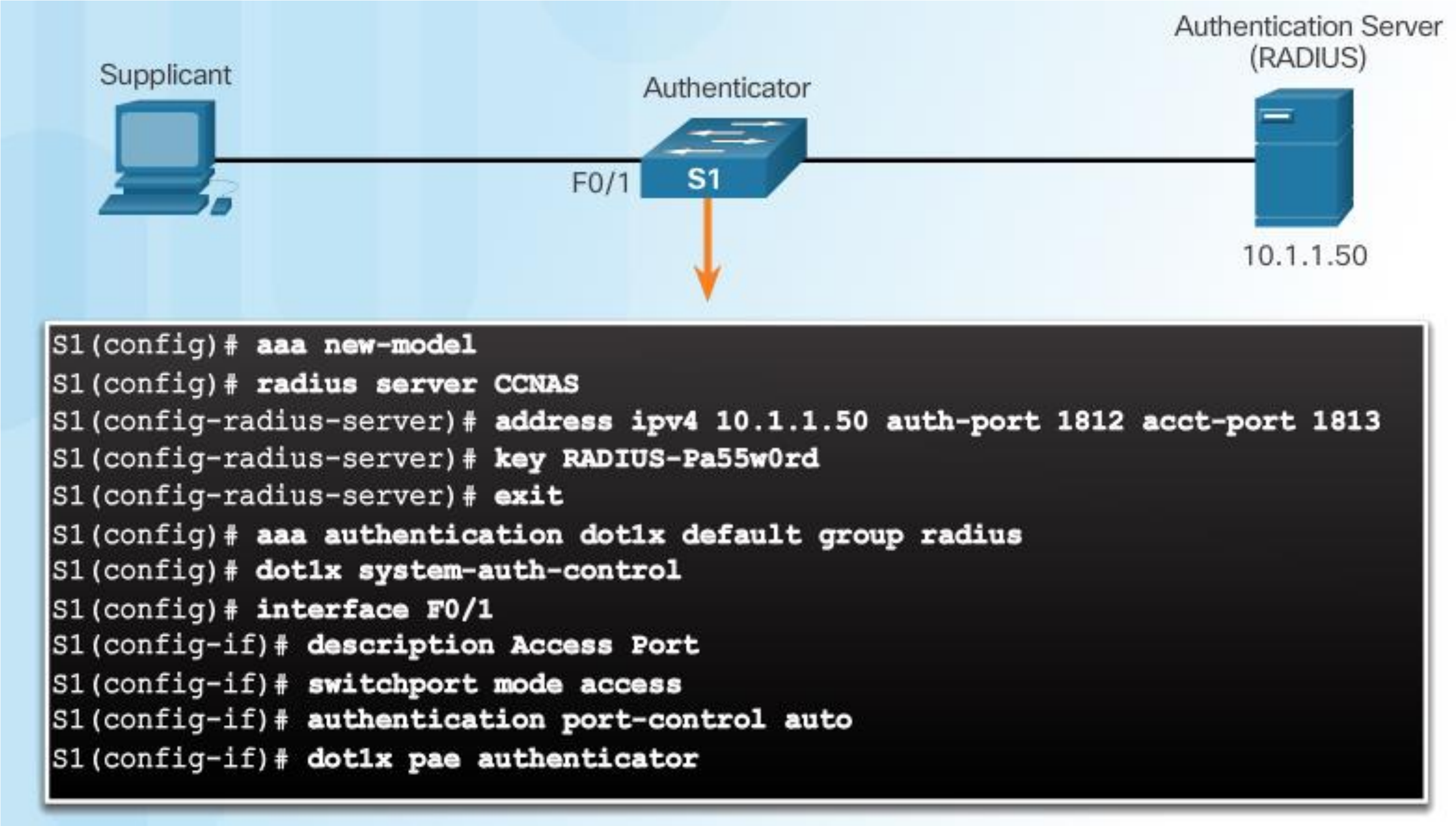
Command Syntax for dot1x port-control



```
S1(config-if)# authentication port-control {auto | force-authorized | force-unauthorized}
```

Parameter	Description
`auto`	Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, enabling only EAPOL frames to be sent and received through the port.
`force-authorized`	The port sends and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.
`force-unauthorized`	Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

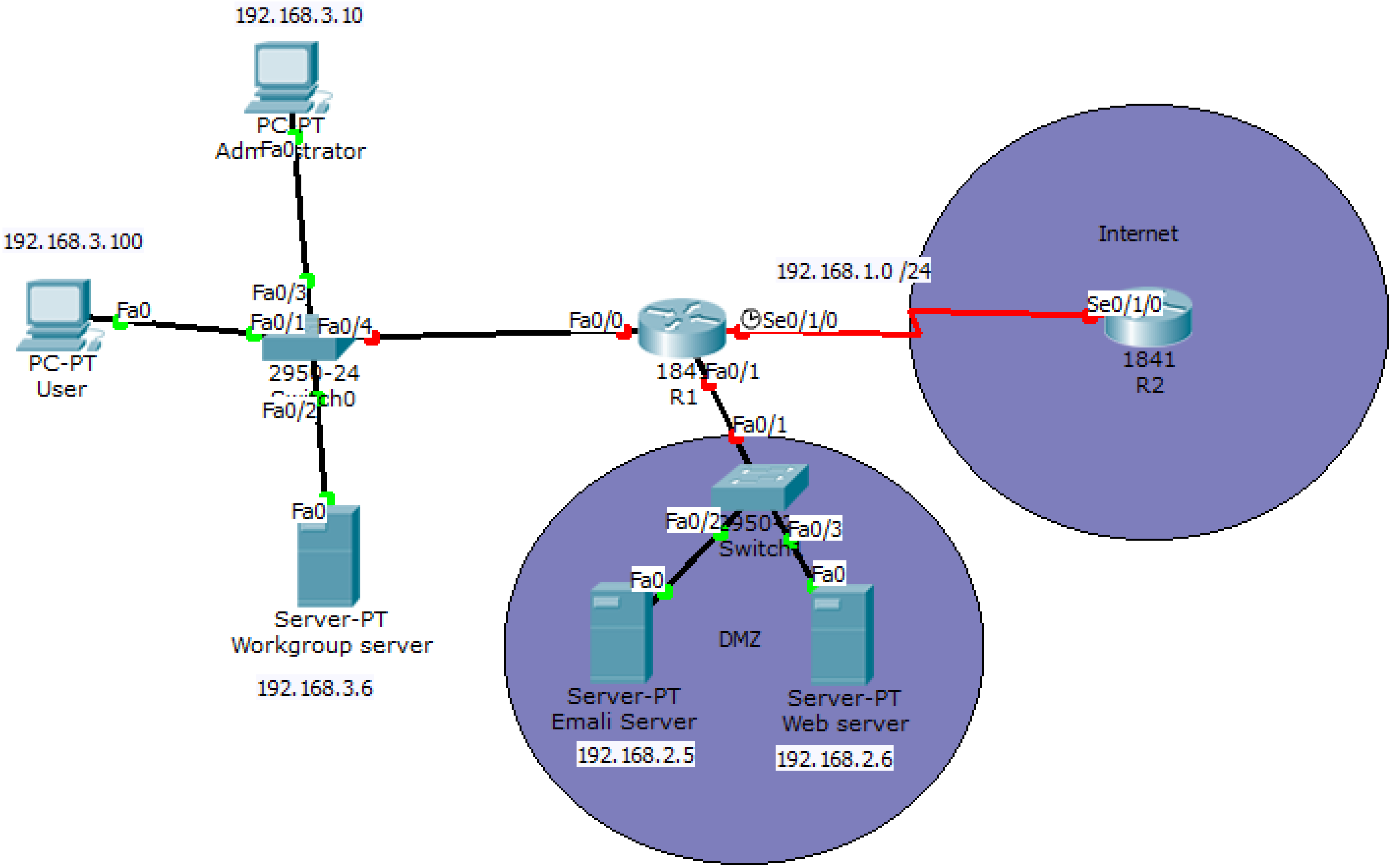
Configuring 802.1X



```
S1(config)# aaa new-model
S1(config)# radius server CCNAS
S1(config-radius-server)# address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
S1(config-radius-server)# key RADIUS-Pa55w0rd
S1(config-radius-server)# exit
S1(config)# aaa authentication dot1x default group radius
S1(config)# dot1x system-auth-control
S1(config)# interface F0/1
S1(config-if)# description Access Port
S1(config-if)# switchport mode access
S1(config-if)# authentication port-control auto
S1(config-if)# dot1x pae authenticator
```

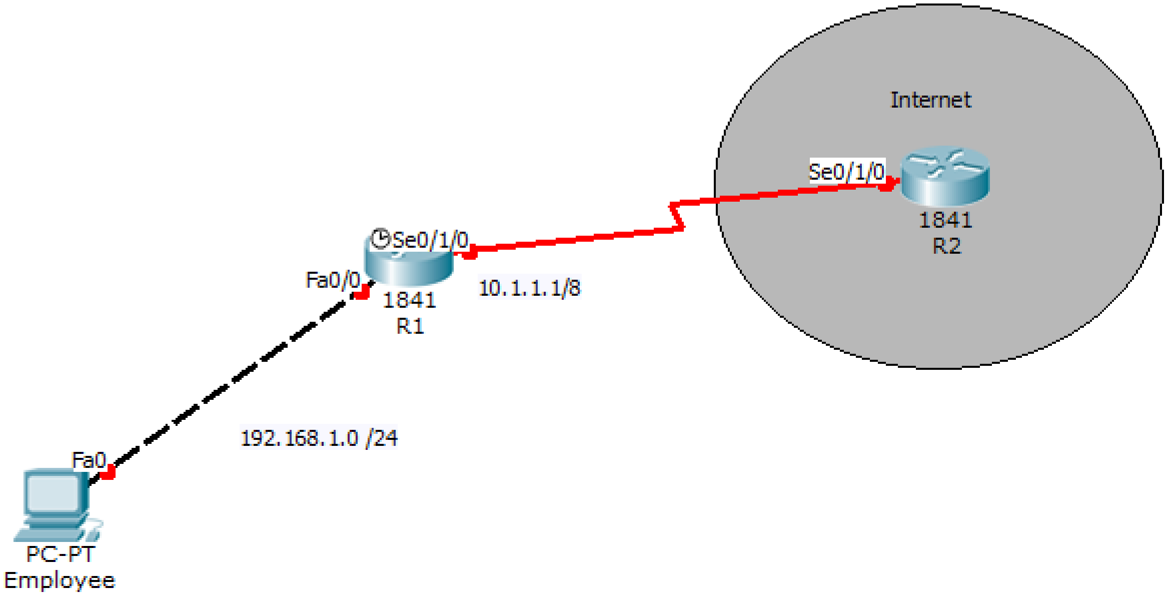
Established keyword Lab 2

- Create an extended named ACL called **RR**, applied incoming on the Fa0/0 interface, that denies the workgroup server outside access but permits the remainder of the LAN users outside access tcp sessions using the `established` ACL.

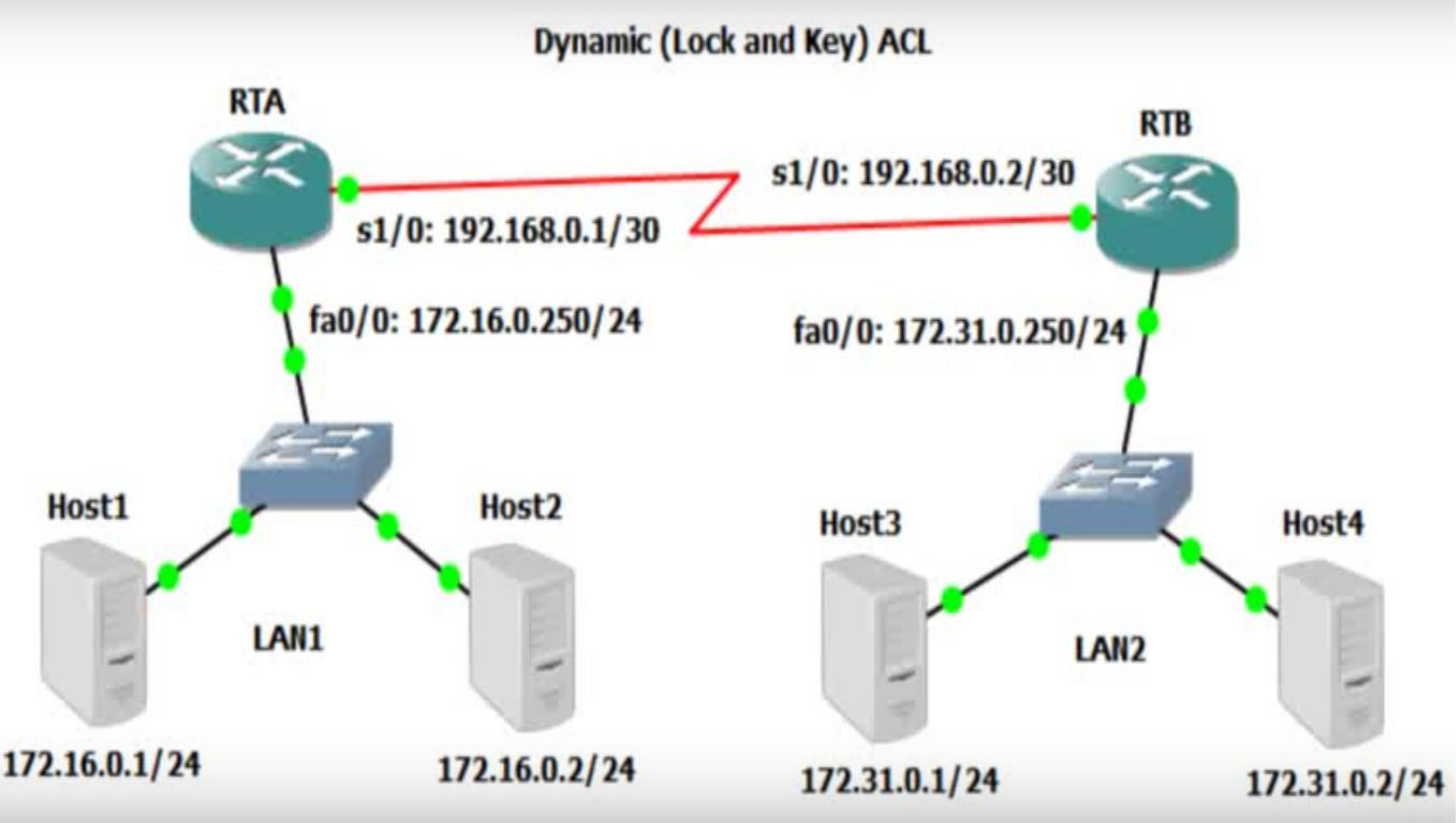


Time-based ACL Example

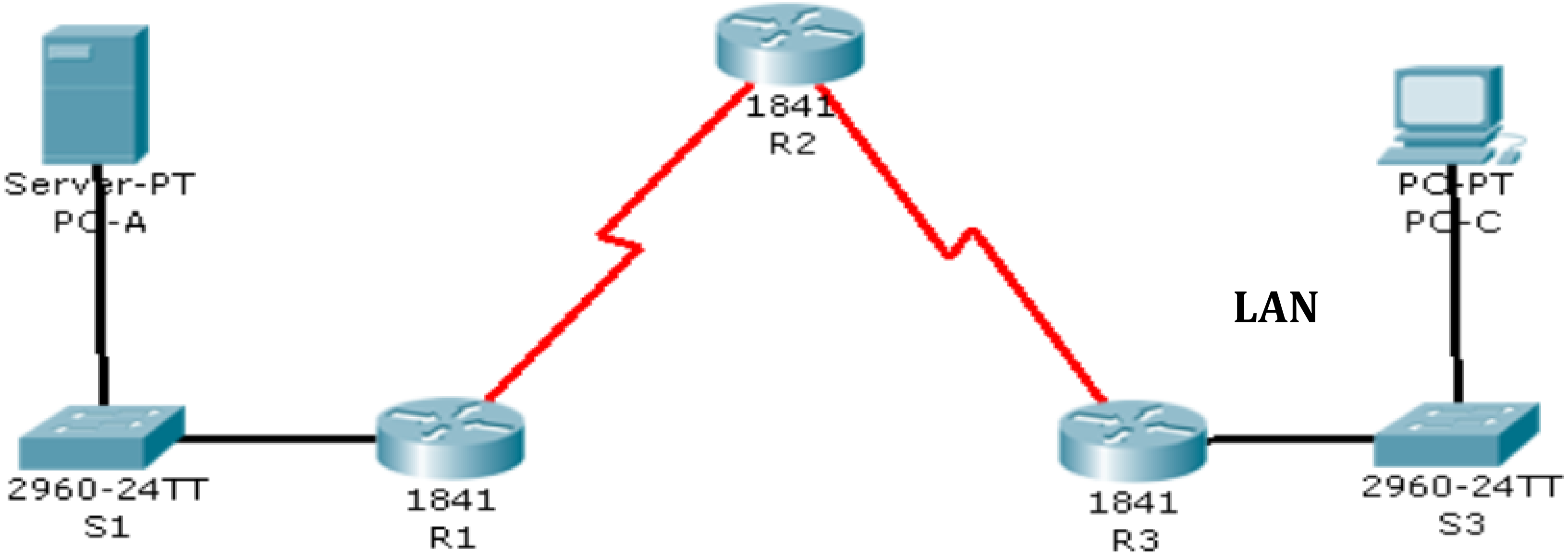
- Users are not allowed to access the Internet during business hours, except during lunch (12 p.m. to 1 p.m.) and after hours between 5 p.m. and 7 p.m.



Dynamic ACL firewall example



CBAC firewall example Lab2



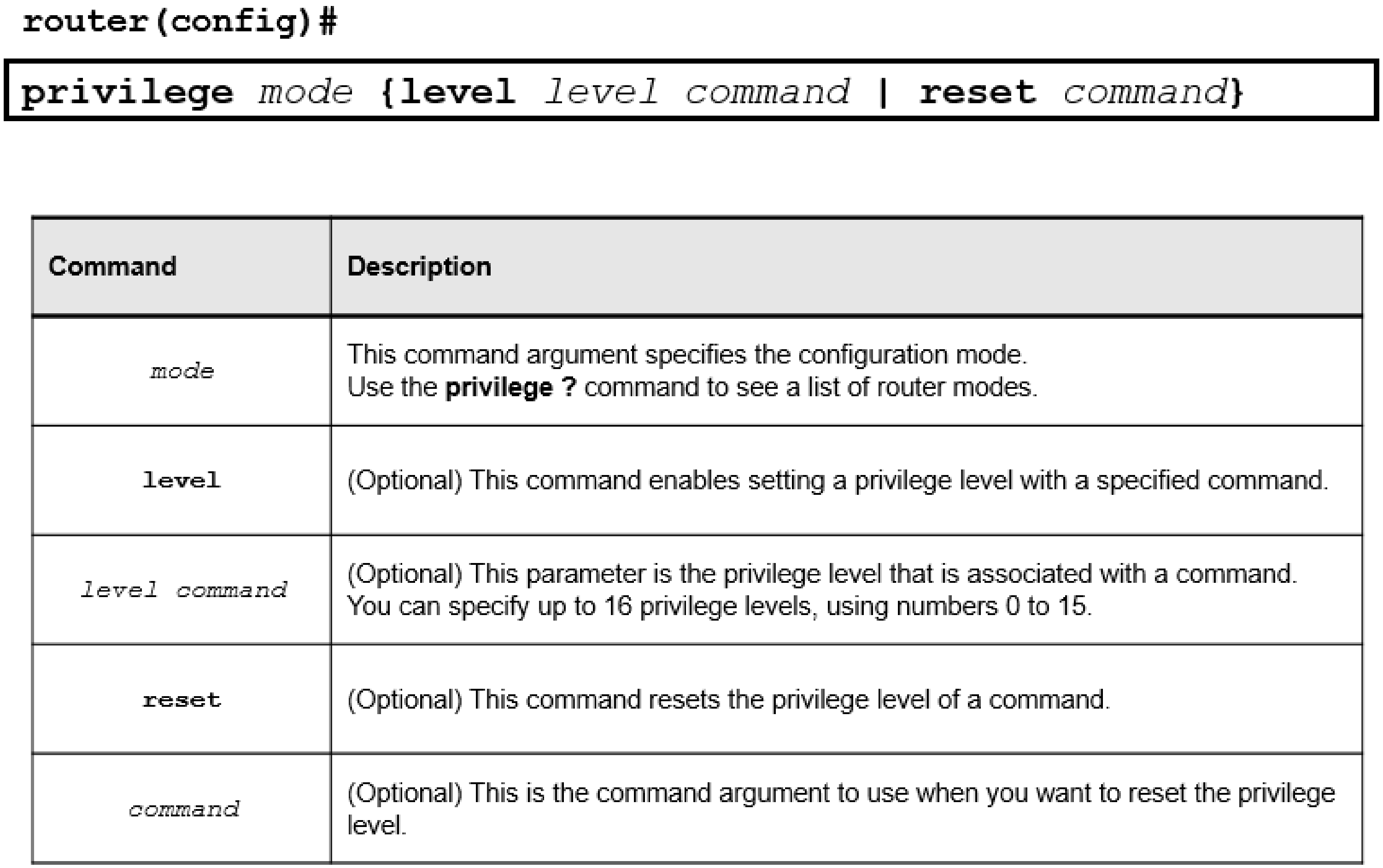
Limiting Command Availability

- Privilege levels determine who should be allowed to connect to the device and what that person should be able to do with it.
- The Cisco IOS software CLI has two levels of access to commands:
  - **User EXEC mode (privilege level 1)**
  - **Privileged EXEC mode (privilege level 15)**
- Cisco IOS software has two methods of providing infrastructure access and a more precise method of controlling access:
  - **privilege level**
  - **role-based CLI (View)**

Privilege Levels

- Level 0:
  - Predefined for **user-level access privileges.**
  - Seldom used, but includes five commands: **`disable`**, **`enable`**, **`exit`**, **`help`**, and **`logout`**
- Level 1(User EXEC mode):
  - The default level for **login with the router prompt Router>.**
  - A user cannot make any changes or view the running configuration file.
- Levels 2 –14:
  - May be **customized for user-level privileges.**
  - **Commands from lower levels may be moved up to a higher level**, or commands from higher levels may be moved down to a lower level.
- Level 15 (Privileged EXEC mode):
  - **Reserved for the enable mode privileges** (**`enable`** command).
  - Users can change configurations and view configuration files.

Privilege Levels Cont.

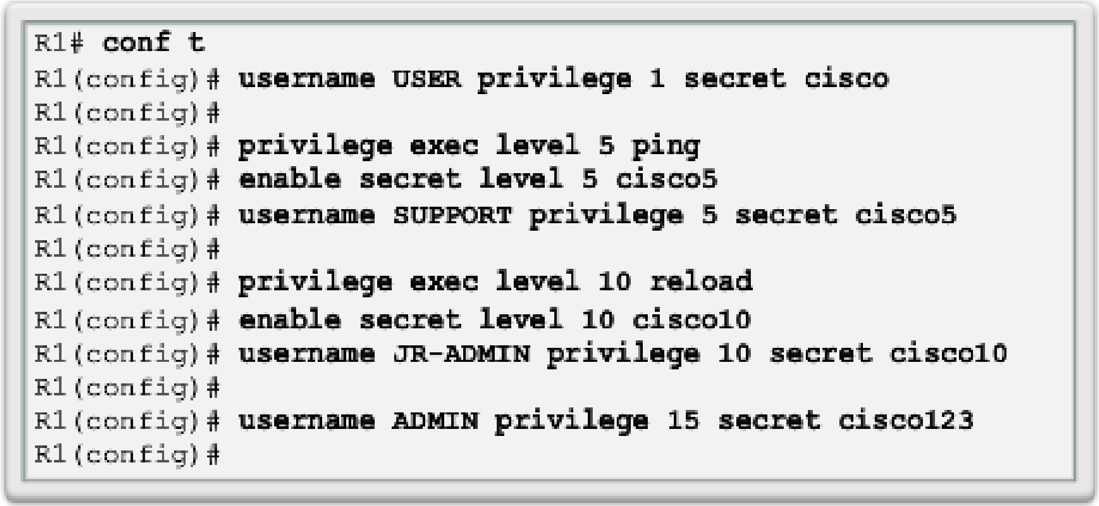


```
router(config)#
privilege mode {level level command | reset command}
```

Command	Description
mode	This command argument specifies the configuration mode. Use the **privilege ?** command to see a list of router modes.
level	(Optional) This command enables setting a privilege level with a specified command.
level command	(Optional) This parameter is the privilege level that is associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15.
reset	(Optional) This command resets the privilege level of a command.
command	(Optional) This is the command argument to use when you want to reset the privilege level.

Configuring Privilege Levels

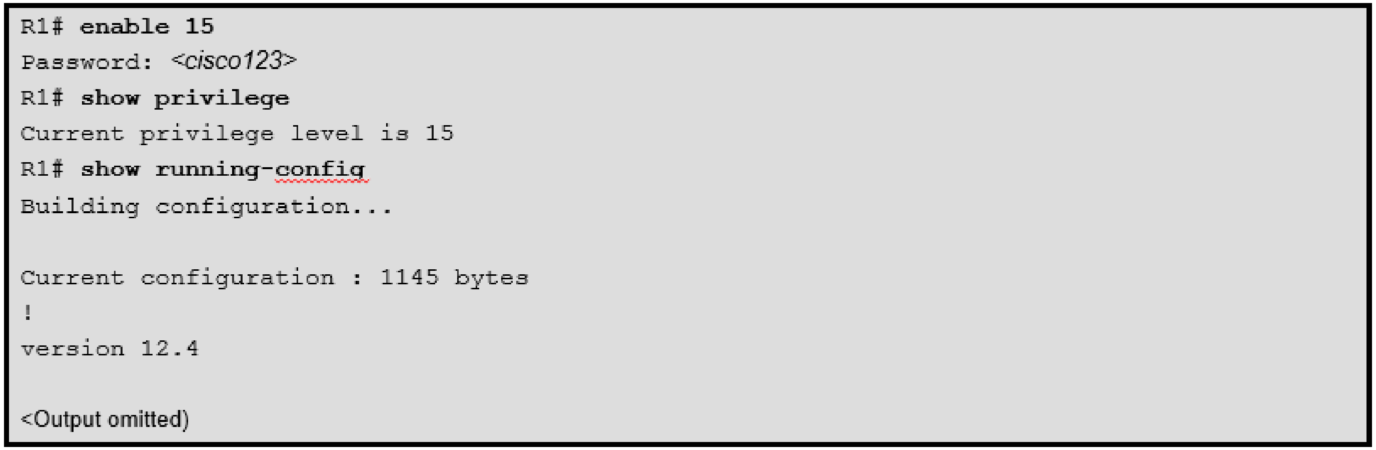
- To a user that is granted a specific privilege level, use the **`username`** *name* **`privilege`** *level* **`secret`** *password* global configuration mode command.



```
R1# conf t
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
R1(config)#
```

Assigning Privilege Levels

- To assign level 10 and the **`reload`** privileged EXEC mode command, use the following command sequence:
  - **`privilege exec level 10 reload`**
  - **`username NOUR privilege 10 secret cisco10`**
- **To access established privilege levels,** enter the **`enable`** *level* command from user mode, and enter the password that was assigned to the custom privilege level.



```
R1# enable 15
Password: <cisco123>
R1# show privilege
Current privilege level is 15
R1# show running-config
Building configuration...

Current configuration : 1145 bytes
!
version 12.4

<Output omitted)
```