| **Course: CSE 462**  **LAB 5 – Access Control List (Final Report)** |
| --- |

| **Student name** | *Pham Nguyen Bao Trang 2131220034*  *Nguyen Vu Phuong Trang 2131220008*  *Ha Quang Minh 1931220012* |
| --- | --- |
| **Student ID** |  |
| **Final Score** |  |

**Lab Exercise Submission**

Students are responsible for submitting the requested work files by the stated deadline for full marks. Late submissions will NOT be accepted.

**Objective:** This lab is to guide you how to work with Cisco router and ACL.

**NOTE:** *Students should read the guideline carefully before conducting Lab experiments and writing the final report.* **Students should write a final report in English.**

**- - - Good luck - - -**

**Students are required to perform the following tasks:**

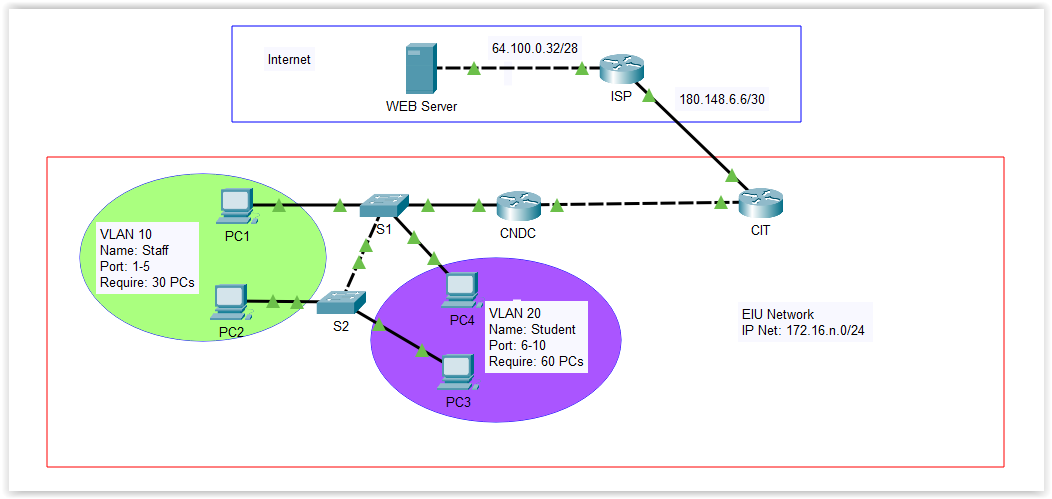
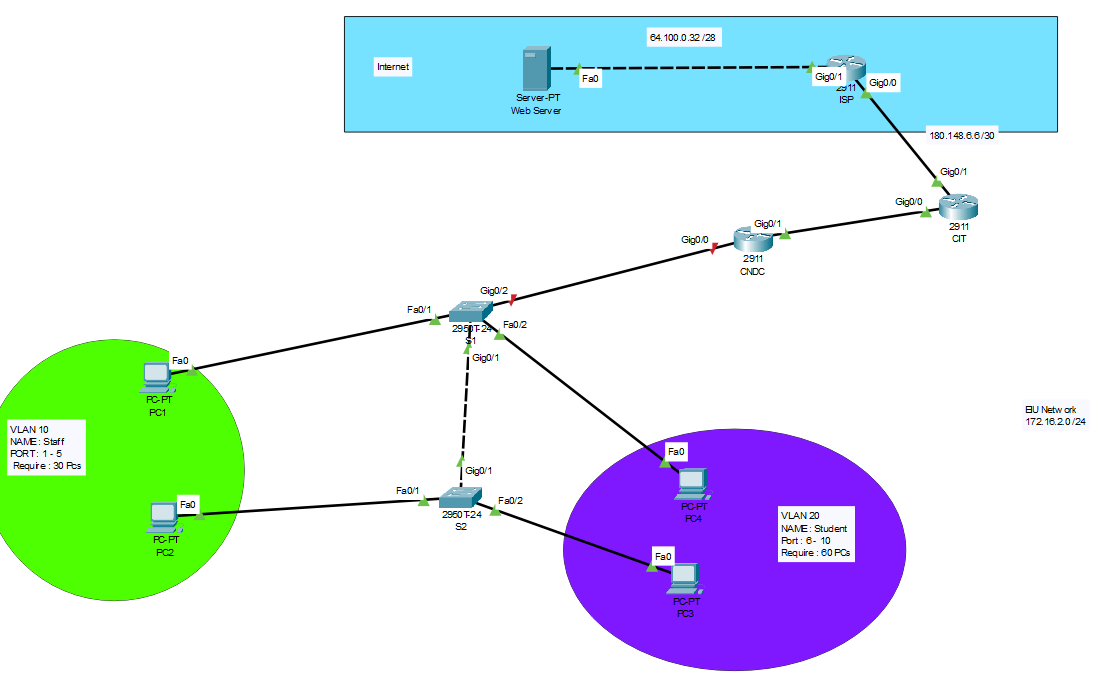


Figure 1. Network topology

****

**IP Addressing Table**

Fill the following table with the correct information from the above topology.

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| --- | --- | --- | --- | --- |
| CNDC  (R4) | gi0/0 |  |  |  |
| gi0/1 | 172.16.2.2 | 255.255.255.192 | 172.16.2.1 |
| CIT  (R5) | gi0/0 | 172.16.2.1 | 255.255.255.192 | 172.16.2.1 |
| gi0/1 | 180.148.6.9 | 255.255.255.252 | 180.148.6.9 |
| ISP  (R6) | gi0/0 | 180.148.6.10 | 255.255.255.252 | 180.148.6.9 |
| gi0/1 | 64.100.0.33 | 255.255.255.240 | 64.100.0.33 |
| S1  (S3) | fa0/1 |  |  |  |
| fa0/20 |  |  |  |
| fa0/7 |  |  |  |
| fa0/24 |  |  |  |
| S2  (S4) | fa0/1 |  |  |  |
| fa0/7 |  |  |  |
| fa0/20 |  |  |  |
| PC1  (Vlan 10) |  | 172.16.2.66 | 255.255.255.192 | 172.16.2.65 |

**Task 1: Answer the following questions:**

1. What is the purpose of using ACL (Access Control List) in a network?
2. What is the main difference between standard and extended ACL?

**Task 2: Perform Basic Device Configurations**

1. Assign IP address for all devices

### Router : CIT :

conf t

int g0/0

ip add 172.16.2.1 255.255.255.192

no shut

exit

int g0/1

ip add 180.148.6.9 255.255.255.252

no shut

exit

### 

### CNDC:

conf t

int g0/1

ip add 172.16.2.2 255.255.255.192  
 no shut

exit

### ISP:

conf t

int g0/0

ip add 180.148.6.10 255.255.255.252

no shut

exit

int g0/1

ip add 64.100.0.33 255.255.255.240

no shut

exit

### ✵ Enable SSH on all Routers

#### CIT

en

conf t

hostname CIT

ip domain-name mydomain.com

crypto key generate rsa

! Nhập độ dài khóa, ví dụ: 2048

2048

username admin privilege 15 secret 123

line vty 0 4

transport input ssh

login local

exit

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 3

write memory

#### CNDC

en

conf t

hostname CNDC

ip domain-name mydomain.com

crypto key generate rsa

! Nhập độ dài khóa, ví dụ: 2048

2048

username admin privilege 15 secret 123

line vty 0 4

transport input ssh

login local

exit

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 3

write memory

#### ISP

en

conf t

hostname ISP

ip domain-name mydomain.com

crypto key generate rsa

! Nhập độ dài khóa, ví dụ: 2048

2048

username admin privilege 15 secret 123

line vty 0 4

transport input ssh

login local

exit

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 3

write memory

1. **Create VLAN on switch S1, S2**

| Switch#conf t  Enter configuration commands, one per line. End with CNTL/Z.  Switch(config)#hostname S1  S1(config)#vlan 10  S1(config-vlan)#name Staff  S1(config-vlan)#vlan 20  S1(config-vlan)#name Student  S1(config-vlan)#exit  S1(config)# |
| --- |

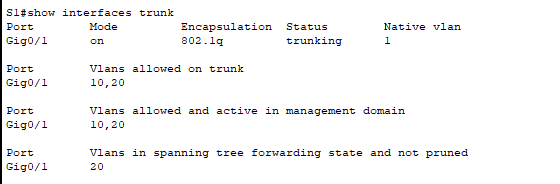
1. Assign ports to VLAN

| S1(config)#vlan 10  S1(config-vlan)#int range f0/1-5  S1(config-if-range)#switchport mode access  S1(config-if-range)#switchport access vlan 10  S1(config-if-range)#  S1(config-if-range)#exit  S1(config)#vlan 20  S1(config-vlan)#int range f0/6-10  S1(config-if-range)#switchport mode access  S1(config-if-range)#switchport access vlan 20  S1(config-if-range)#exit |
| --- |

1. **Configure trunk interface (802.1Q) between S1, S2**

| S1(config)#interface g0/1  S1(config-if)#switchport mode trunk  S1(config-if)#switchport trunk allowed vlan 10,20 |
| --- |

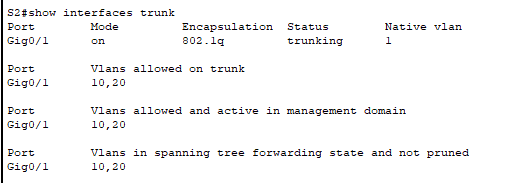
**Check : show interfaces trunk**



**Thiết lập trên S2**

| S2(config)#vlan 10  S2(config-vlan)#int range f0/1-5  S2(config-if-range)#switchport mode access  S2(config-if-range)#switchport access vlan 10  S2(config-if-range)#  S2(config-if-range)#exit  S2(config)#vlan 20  S2(config-vlan)#int range f0/6-10  S2(config-if-range)#switchport mode access  S2(config-if-range)#switchport access vlan 20  S2(config-if-range)#exit |
| --- |

| S2(config)#interface g0/1  S2(config-if)#switchport mode trunk  S2(config-if)#switchport trunk allowed vlan 10,20 |
| --- |



1. Allow VLAN on trunk interface
2. **Configure subinterface on Router CNDC for each VLAN using the 802.1Q encapsulation**

| CNDC(config)#int g0/0.10  CNDC(config-subif)# no shut  CNDC(config-subif)#no shut  CNDC(config-subif)#int g0/0.10  CNDC(config-subif)#encapsulation dot1q 10  CNDC(config-subif)#ip add 172.16.2.65 255.255.255.192  CNDC(config-subif)#exit  CNDC(config)#  CNDC(config)#interface g0/0.20  CNDC(config-subif)#encapsulation dot1q 20  CNDC(config-subif)#ip add 172.16.2.129  % Incomplete command.  CNDC(config-subif)#ip add 172.16.2.129 255.255.255.192  CNDC(config-subif)#exit |
| --- |

1. **Configure trunk interface on S1 which connects to Router CNDC**

**Remember :**

CNDC(config)#int g0/0

CNDC(config-if)#no shut

1. **Configure routing between routers in the topology.**

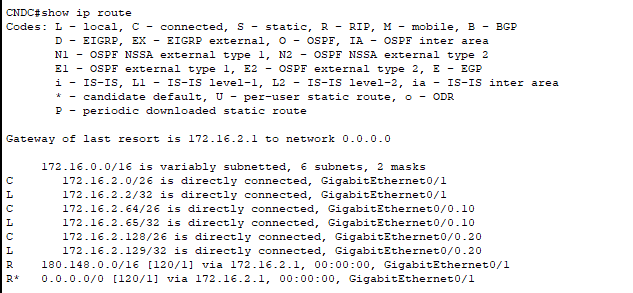
NOTE: ISP router does not neither run dynamic routing nor set a default route to customer network.

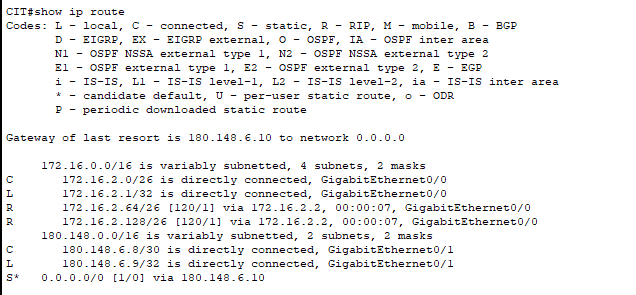
| CNDC(config)#router rip  CNDC(config-router)#ver 2  CNDC(config-router)#network 172.16.2.0  CNDC(config-router)#network 172.16.2.64  CNDC(config-router)#network 172.16.2.128 |
| --- |

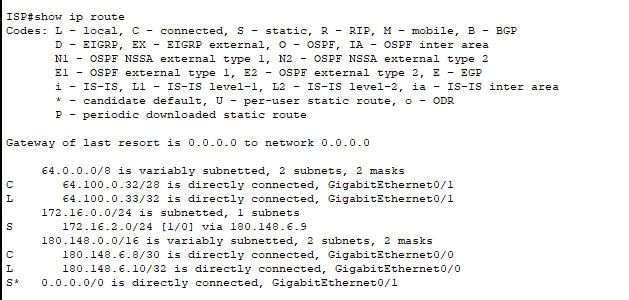
| CIT(config)#router rip  CIT(config-router)#ver 2  CIT(config-router)#network 172.16.2.0  CIT(config-router)#network 180.148.6.8  CIT(config-router)#ip route 0.0.0.0 0.0.0.0 180.148.6.10  CIT(config)#router rip  CIT(config-router)#network 180.148.6.8  CIT(config-router)#redistribute static |
| --- |

| ISP(config)#ip route 0.0.0.0 0.0.0.0 g0/1  %Default route without gateway, if not a point-to-point interface, may impact performance  ISP(config)#  ISP(config)#ip route 172.16.2.0 255.255.255.0 180.148.6.9 |
| --- |

1. Verify routing table in each router to make sure that it has all routes in the network

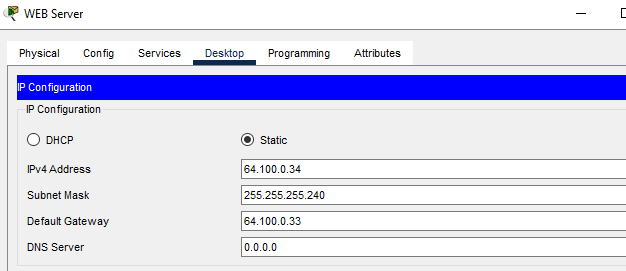






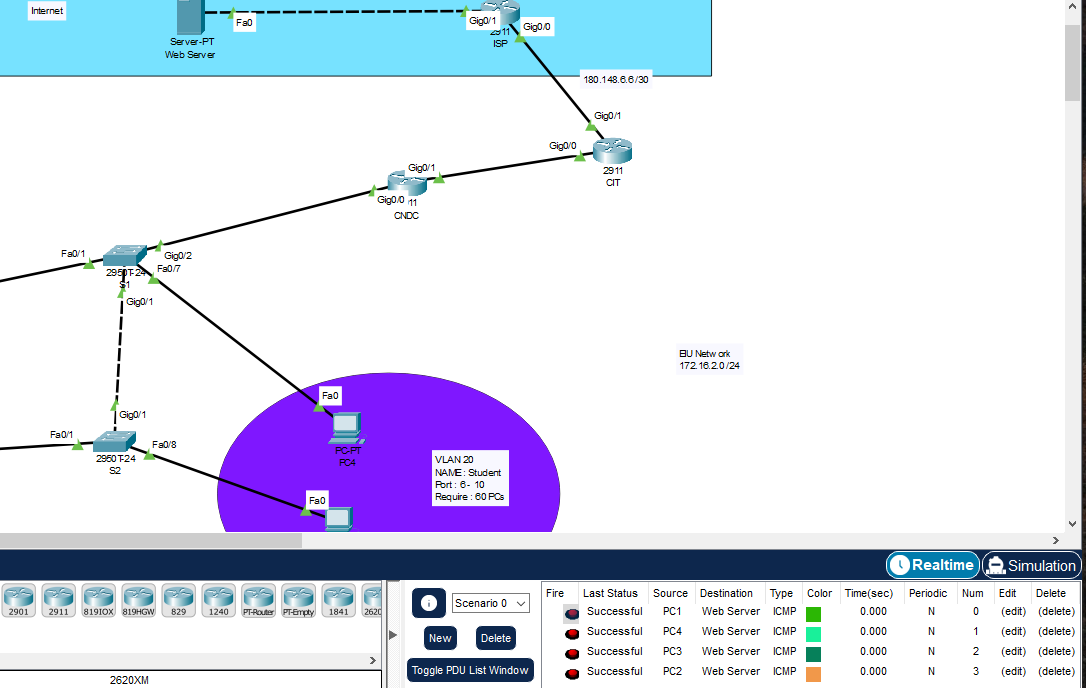
1. Verity the connection between PCs, Router and web server in the network.

**Remember :**



1. Make sure all computers can access to web service on Web server before doing task 3.

DONE



1. Make sure all computers can access SSH to all routers.

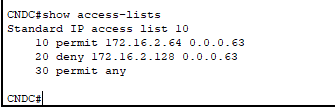
**Task 3: Configure a Standard ACL**

In this task, you are configuring a standard ACL. Users in Staff VLAN are permitted to access to ISP network; however, users in Student VLAN are prohibited from accessing ISP network.

**ANSWER:**

| CNDC(config)#access-list 10 permit 172.16.2.64 0.0.0.63  CNDC(config)#access-list 10 deny 172.16.2.128 0.0.0.63  CNDC(config)#access-list 10 permit any  CNDC(config)#int g0/0.10  CNDC(config-subif)#ip access-group 10 out |
| --- |

Check



**Task 4: Configure an Extended ACL**

Configure an extended ACL with the following requirement.

* Only users in Staff VLAN (10) are allowed to PING to CNDC and CIT Router; others are prohibited.
* Only users in Staff VLAN (10) are allowed to access web service on Web server; others are prohibited.

**ANSWER:**

| CNDC#conf t  Enter configuration commands, one per line. End with CNTL/Z.  CNDC(config)#access-list 100 permit icmp 172.16.2.64 0.0.0.63 host 172.16.2.1  CNDC(config)#access-list 100 permit icmp 172.16.2.64 0.0.0.63 host 172.16.3.1  CNDC(config)#  CNDC(config)#access-list 100 permit tcp 172.16.2.64 0.0.0.63 host 192.168.1.10 eq 80  CNDC(config)#  CNDC(config)#access-list 100 deny ip any any  CNDC(config)#  CNDC(config)#access-list 100 permit ip any any  CNDC(config)#  CNDC(config)#int g0/0.10  CNDC(config-subif)#ip access-group 100 in |
| --- |

**Task 5: Control Access to the VTY Lines with a Standard ACL**

Configure an ACL to permit hosts from VLAN Staff to access the VTY lines on CNDC and CIT. All other hosts are denied.

**ANSWER:**

| CNDC(config-line)#access-list 10 permit 172.16.2.64 0.0.0.63  CNDC(config)#no access-list 10 permit 172.16.2.64 0.0.0.63  CNDC(config)#access-list 10 permit 172.16.2.64 0.0.0.63  CNDC(config)#access-list 10 deny any  CNDC(config)#  CNDC(config)#access-list 10 permit 172.16.2.64 0.0.0.63  CNDC(config)#access-list 10 deny any  CNDC(config)#  CNDC(config)#line vty 0 4  CNDC(config-line)#access-class 10 in  CNDC(config-line)#login  CNDC(config-line)#exit  CNDC(config)# |
| --- |