DCN Project

Team members:

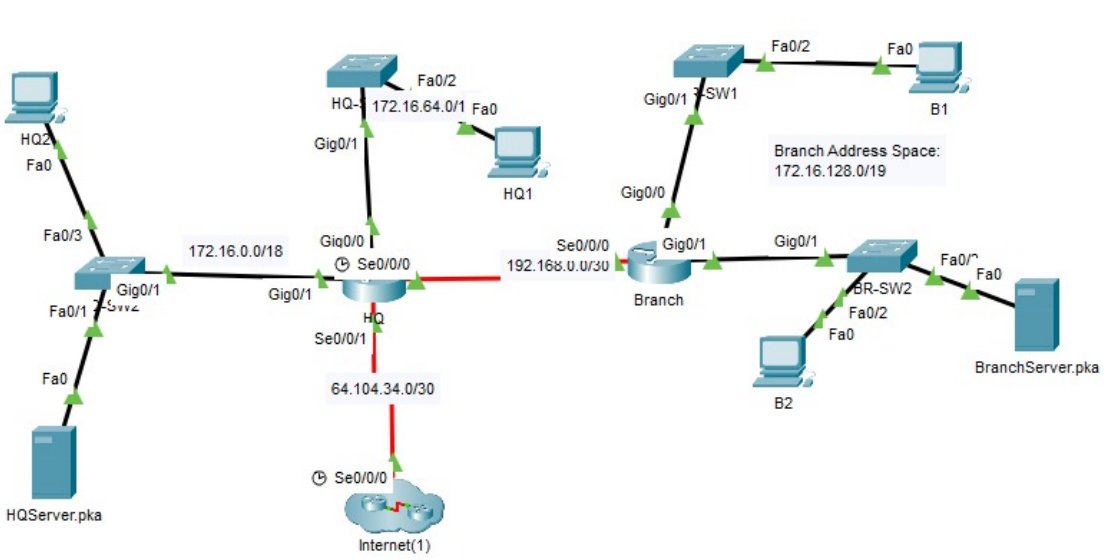
Binish Fatima Basathia
Mehdi Raza Khorasani
Ghani Haider

Address table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	G0/0	172.16.127.254	255.255.192.0	N/A
Untitled	G0/1	172.16.63.254	255.255.192.0	N/A
Untitled	S0/0/0	192.168.0.1	255.255.255.252	N/A
Untitled	S0/0/1	64.104.34.2	255.255.255.252	64.104.34.1
Branch	G0/0	172.16.159.254/20	255. 255.240.0	N/A
Untitled	G0/1	172.16.143.254/20	255.255.240.0	N/A
Untitled	S0/0/0	192.168.0.2	255.255.255.252	N/A
HQ1	NIC	172.16.64.1	255.255.192.0	172.16.127.254
HQ2	NIC	172.16.0.2	255.255.192.0	172.16.63.254
HQServer.pka	NIC	172.16.0.1	255.255.192.0	172.16.63.254
B1	NIC	172.16.128.1/20	255.255.240.0	172.16.143.254
B2	NIC	172.16.128.2	255.255.240.0	172.16.143.254
BranchServer.pka	NIC	172.16.128.1	255.255.240.0	172.16.143.254

When pinging Head Quarter's server, from denied client B1:

Topology



Task a

Divide 172.16.128.0/19 into two equal subnets for use on Branch.

Subnetting

Given IP address: 172.16.128.0/19
1111 1111. 1111 1111. 1110 0000. 0000 0000/19
Subnets required: 2
We use 1 bit from the host's MSB.
Subnet 1: xxxx xxxx. xxxx xxxx. xxx0 0000. 0000 0000/20
Subnet 2: xxxx xxxx. xxxx xxxx. xxx1 0000. 0000 0000/20
Subnet Mask: 255. 255.240.0

🚧 Subnet 1:
1010 1100. 0001 0000. 1000 0000. 0000 0000/20
Subnet ID: 172.16.128.0/20
First usable address: 172.16.128.1/20
Last usable address: 172.16.143.254/20
Broadcast address: 172.16.143.255/20

🚧 Subnet 2:
1010 1100. 0001 0000. 1001 0000. 0000 0000/20
Subnet ID: 172.16.144.0/20
First usable address: 172.16.144.1/20
Last usable address: 172.16.159.254/20
Broadcast address: 172.16.159.255/20

1. Assign the last usable address of the second subnet to the Gigabit Ethernet 0/0 interface.
   Address: 172.16.159.254/20
2. Assign the last usable address of the first subnet to the Gigabit Ethernet 0/1 interface.
   Address: 172.16.143.254/20
3. Document the addressing in the Addressing Table.
   Addressing Table updated.
4. Configure Branch with appropriate addressing

Task b

Configure B1 with appropriate addressing using the first available address of the network to which it is attached. Document the addressing in the Addressing Table.

First available address: 172.16.128.1/20
Subnet Mask: 255.255.240.0

Task c

Configure **HQ** and **Branch** with RIPv2 routing according to the following criteria:

- Advertise all three attached networks. Do not advertise the link to the Internet.
- Configure appropriate interfaces as passive.

Answer:

For Branch Router - task c

```
Branch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch(config)#
Branch(config)#router rip
Branch(config-router)#version 2
Branch(config-router)#passive-interface Gig0/0
Branch(config-router)#passive-interface Gig0/1
Branch(config-router)#network 172.16.0.0
Branch(config-router)#network 192.168.0.0
Branch(config-router)#no auto-summary
```

For HQ Router - task c

```
HQ#config t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#router rip
HQ(config-router)#version 2
HQ(config-router)#passive-interface Gig0/0
HQ(config-router)#passive-interface Gig0/1
HQ(config-router)#passive-interface Serial0/0/1
HQ(config-router)#network 172.16.0.0
HQ(config-router)#network 192.168.0.0
HQ(config-router)#no auto-summary
```

Task d

Set a default route on HQ which directs traffic to S0/0/1 interface. Redistribute the route to Branch.

Answer:

```
HQ(config-router)#ip route 0.0.0.0 0.0.0.0 Serial0/0/1
```

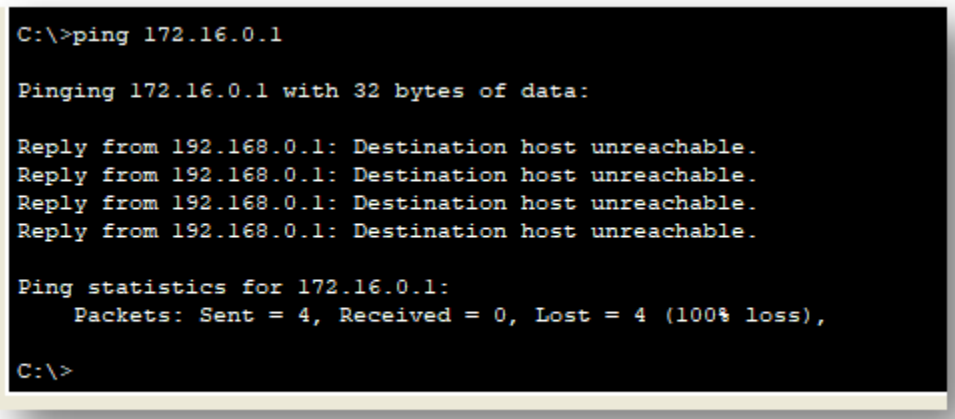
Task e

Design a named access list **HQServer** to prevent any computers attached to the Gigabit Ethernet 0/0 interface of the **Branch** router from accessing **pka**. All other traffic is permitted. Configure the access list on the appropriate router, apply it to the appropriate interface and in the appropriate direction.

Configuring the Access control list on the server:

```
HQ#config t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#ip access-list extended HQserver
HQ(config-ext-nacl)#deny ip 172.16.159.254 0.0.15.255 host 172.16.0.1
HQ(config-ext-nacl)#permit ip any any
HQ(config-ext-nacl)#end
HQ#
%SYS-5-CONFIG_I: Configured from console by console

HQ#enable
HQ#config t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#
HQ(config)#interface Se0/2/1
HQ(config-if)#ip access-group HQserver in
HQ(config-if)#end
HQ#
%SYS-5-CONFIG_I: Configured from console by console

HQ#show ip access-lists
Extended IP access list HQserver
    10 deny ip 172.16.144.0 0.0.15.255 host 172.16.0.1
    20 permit ip any any (31 match(es))
```

When pinging Head Quarter's server, from denied client B1:



Task f

Design a named access list **BranchServer** to prevent any computers attached to the Gigabit Ethernet 0/0 interface of the **HQ** router from accessing the **Branch S.** All other traffic is permitted. Configure the access list on the appropriate router, apply it to the appropriate interface and in the appropriate direction.

Configuring the Access control list on the server:

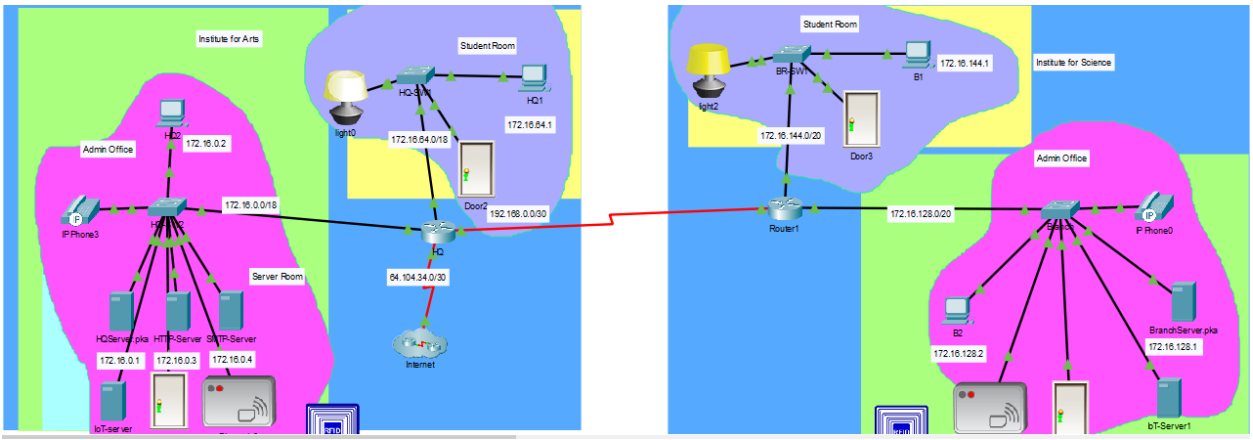
```
Branch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch(config)#ip access-list extended BranchServer
Branch(config-ext-nacl)#deny ip 172.16.127.254 0.0.63.255 host 172.16.128.1
Branch(config-ext-nacl)#permit ip any any
Branch(config-ext-nacl)#end
Branch#
%SYS-5-CONFIG_I: Configured from console by console

Branch#enable
Branch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch(config)#interface Se0/2/0
Branch(config-if)#ip access-group BranchServer in
Branch(config-if)#end
Branch#
%SYS-5-CONFIG_I: Configured from console by console

Branch#show ip access-lists
Extended IP access list BranchServer
    10 deny ip 172.16.64.0 0.0.63.255 host 172.16.128.1
    20 permit ip any any (15 match(es))
```

When pinging the Branch server, from denied client HQ1:

```
C:\>ping 172.16.128.1

Pinging 172.16.128.1 with 32 bytes of data:

Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.

Ping statistics for 172.16.128.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

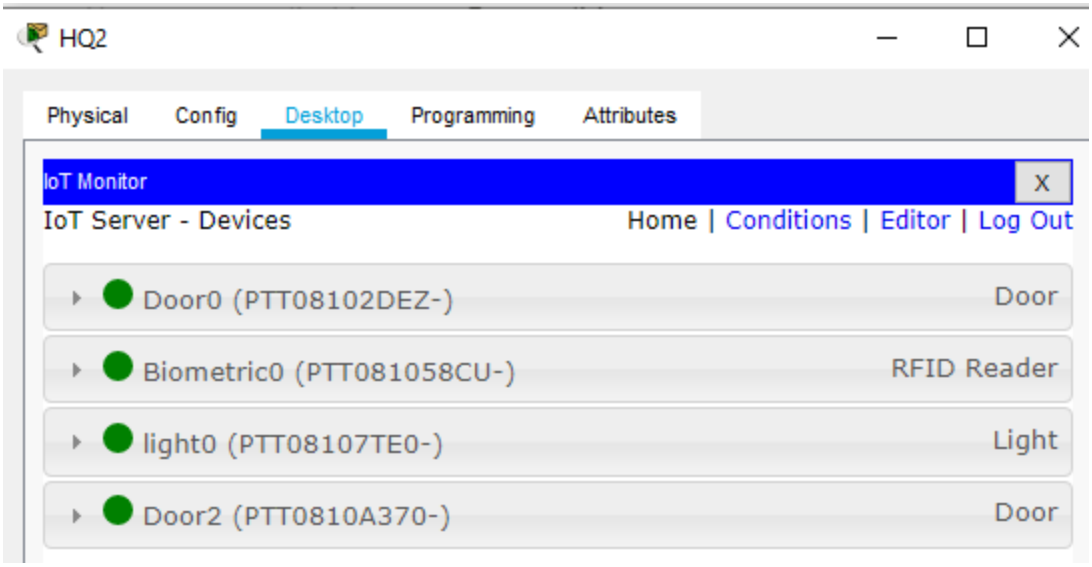
	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Failed	HQ1	BranchSer...	ICMP		0.000	N	0	(e

IOT devices in the network:



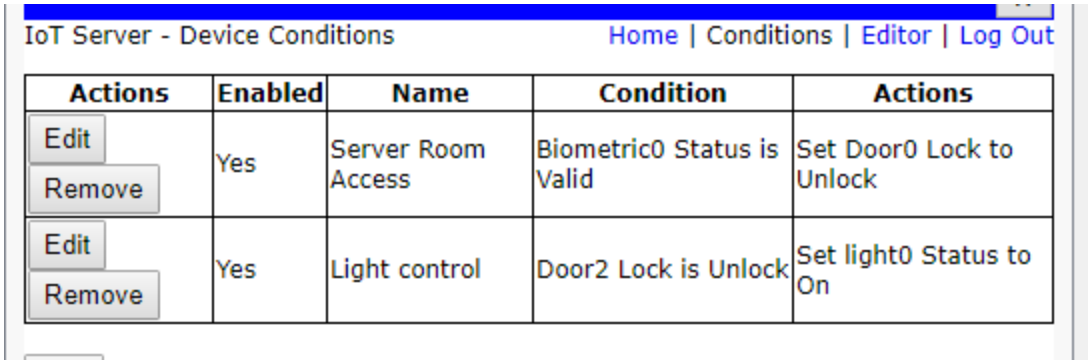
There are four IOT devices in each of the institutions:

- Door to the admin room
- Door to the students room
- Light in the students room
- Biometric scanner in the admin



The lock of the **door for the admin room** is *controlled* by the **biometric scanner**, this door unlocks when any authorized person enters the admin room (i.e. when

the biometric gives a valid reading). The PC in the admin room is used to control the IOT devices, in the entire institute. The **door for the students room** can be locked and unlocked from the admin room. The **light in the students room** is switched on whenever the lock of the door of the students room is unlocked. This is done using conditions:



IoT Server - Device Conditions Home | Conditions | Editor | Log Out

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Server Room Access	Biometric0 Status is Valid	Set Door0 Lock to Unlock
Edit Remove	Yes	Light control	Door2 Lock is Unlock	Set light0 Status to On

Video links:

here is the link to the demonstration videos.