CEP Project Proposal

Complex Engineering Problem

TAHA KHALEEL

FA17-BCE-052-B

Data Communication and Computer Networks

Date: 17 AUGUST 2020

Table of Contents

TOPOLOGY DIAGRAM:

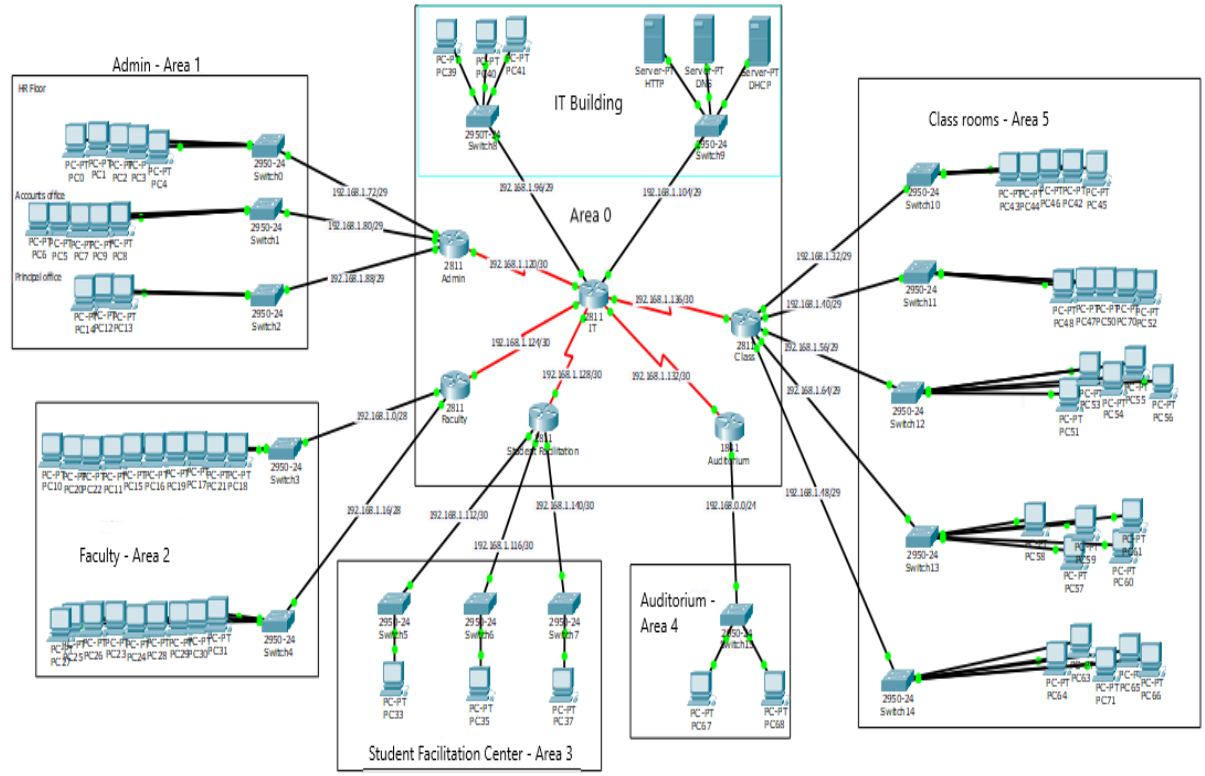


Figure 1 - Network Topology

IMPLEMENTATION DETAILS

First, devices such as routers, switches and PCs were placed and they were connected by different wires. For the connection between routers, a serial DCE wire was used for connections between a switch and a router, and a switch and a PC, straight through copper wire was used. There are three switches in Admin block where switch 1 and switch 2 are connected to 5 PCs each and switch 3 is connected to 3 PCs. There are 2 switches in Faculty block where switch 1 is connected to 10 PCs and switch 2 is connected to 9 PCs. Student Facilitation Centre has 3 switches and each switch is connected to a single host. Auditorium has a single switch connected to 2 hosts although it can support up to 200 hosts. Classroom Block has 5 switches and each switch is connected to 5 PCs. IT building has 2 switches where switch 1 is connected to 3 hosts and switch 2 is connected to 3 servers.

Each department has a router which is connected to IT building's router. The routers were assigned an IP address to Fast Ethernet and Serial connections by going to CLI global configuration mode.

After this, Multi area OSPF was assigned to all routers by assigned a network ID, wildmask and area. There are total 5 areas in this topology. Every area is connected to backbone area 0. Area 2 was assigned to networks 192.168.1.0 and 192.168.1.16 which are networks of Faculty building. Area 1 was assigned to networks 192.168.1.72 (HR office), 192.168.1.80 (Accounts office), 192.168.1.88 (Admin office). Area 3 was assigned to networks 192.168.1.112, 192.168.1.116, 192.168.1.140. Area 4 was assigned to network 192.168.0.0 and Area 5 was assigned to networks 192.168.1.32, 192.168.1.40, 192.168.1.48, 192.168.1.56 and 192.168.1.64.

Example of multi-area network of Area 1 is shown below. Here, it can be seen that it is connected to Area 0 (backbone area).

```
Routing for Networks:
  192.168.1.72 0.0.0.7 area 1
  192.168.1.80 0.0.0.7 area 1
  192.168.1.88 0.0.0.7 area 1
  192.168.1.120 0.0.0.3 area 0
Routing Information Sources:
  Gateway         Distance      Last Update
  192.168.1.122         110      00:17:59
  192.168.1.126         110      00:17:58
  192.168.1.134         110      00:17:58
  192.168.1.137         110      00:17:59
  192.168.1.138         110      00:17:58
  192.168.1.141         110      00:17:59
Distance: (default is 110)
```

Figure 2 - OSPF at Admin Building

After OSPF configuration, DHCP was configured on each router to assign IP addresses to Hosts in a network. For this, a separate pool was created for each network of each department. After giving a pool name, network IP address and subnet mask was assigned for each network, default router IP address was assigned and a DNS server IP address was assigned. After the configuration, each PC's IP address and default gateway was checked.

The backbone area connections are shown below. Here, network IDs shown are interfaces.

```
Routing for Networks:
  192.168.1.96 0.0.0.7 area 0
  192.168.1.104 0.0.0.7 area 0
  192.168.1.120 0.0.0.3 area 0
  192.168.1.128 0.0.0.3 area 0
  192.168.1.132 0.0.0.3 area 0
  192.168.1.136 0.0.0.3 area 0
  192.168.1.124 0.0.0.3 area 0
Routing Information Sources:
  Gateway         Distance      Last Update
  192.168.1.122         110      00:11:06
  192.168.1.126         110      00:11:05
  192.168.1.134         110      00:11:05
  192.168.1.137         110      00:11:05
  192.168.1.138         110      00:11:05
  192.168.1.141         110      00:11:05
Distance: (default is 110)
```

Figure 3 -OSPF at IT building

After implementation of DHCP, access control list was created. For each control list requirement, extended access control list was used to provide maximum security. To provide maximum security to Principal's office, extended ACL was created on each router of the topology to deny access to Principal office except the router of IT building because IT can access data of any department. Extended ACL was used on routers of each department as well as the router of Admin block because the access of HR and Accounts office to Principal office is also denied. Furthermore, access to HR and Accounts office is also denied by other networks except principal office. Hence, for every router except admin's router, access lists were created using the source IP address of the network of traffic source and destination network ID was used of Principals office, HR office and Accounts office. For admin's router, access-lists were created that denied network IDs of HR and Accounts office to have an access to Principal's office. Source network ID was used of HR and accounts office, and destination ID was used of Principal's office. Student facilitation centre, IT building and Faculty building were protected against any telnet request. For this, extended ACL was used. Extended ACL was created on each router in the topology except for Student Facilitation Centre router, Faculty Building router and IT building router. Each ACL implementation on each router was assigned source network ID of the interface from where traffic source is coming and destination host IP address was assigned of Student Facilitation Centre, Faculty Building and IT building along with eq telnet and tcp deny since telnet works on TCP. This denied any telnet request. Lastly, any other IP was permitted.

After implementation of ACLs, port security on each switch of the topology was created. For this, each switch's port was configured in mode access, port-security mode and maximum number of allowed MAC-addresses for each port was configured to 1, and the allowed MAC-address was assigned to that port. After this, violation of each port was configured to shutdown mode. If a rogue PC connects to a port, the port shuts down.

ADDRESSING SCHEME:

Router	*Interface*	*IP address*	*Subnet Mask*
IT	Fast Ethernet 0/0	192.168.1.97	255.255.255.248
	Fast Ethernet 0/1	192.168.1.105	255.255.255.248
	Serial0/1/0	192.168.1.121	255.255.255.252
	Serial0/1/1	192.168.1.125	255.255.255.252
	Serial0/2/0	192.168.1.129	255.255.255.252
	Serial0/2/1	192.168.1.133	255.255.255.252
	Serial0/3/0	192.168.1.137	255.255.255.252
Admin	Fast Ethernet 0/0	192.168.1.73	255.255.255.248
	Fast Ethernet 0/1	192.168.1.81	255.255.255.248
	Fast Ethernet 1/0	192.168.1.89	255.255.255.248
	Serial0/3/0	192.168.1.122	255.255.255.252
Faculty	Fast Ethernet 0/0	192.168.1.1	255.255.255.240
	Fast Ethernet 0/1	192.168.1.17	255.255.255.240
	Serial0/1/0	192.168.1.126	255.255.255.252
Student Facilitation Center	Fast Ethernet 0/0	192.168.1.113	255.255.255.252
	Fast Ethernet 0/1	192.168.1.117	255.255.255.252
	Fast Ethernet 1/0	192.168.1.141	255.255.255.252
	Serial0/3/0	192.168.1.130	255.255.255.252
Auditorium	FA0/0	192.168.0.1	255.255.255.0
	Serial0/1/0	192.168.1.134	255.255.255.252
Classrooms	Fast Ethernet 0/0	192.168.1.33	255.255.255.248
	Fast Ethernet 0/1	192.168.1.41	255.255.255.248
	Fast Ethernet 1/0	192.168.1.57	255.255.255.248
	Fast Ethernet 1/1	192.168.1.65	255.255.255.248
	Fast Ethernet 2/0	192.168.1.49	255.255.255.248
	Serial0/1/0	192.168.1.138	255.255.255.252

Table 1 - Addressing Scheme

ROUTING DETAILS:

Department	*Area*
Admin	1
Faculty	2
Student Facilitation Centre	3
Auditorium	4
Classrooms	5
IT	0

Table 2 - Area details

Area	*Network ID*
0	192.168.1.96
0	192.168.1.104
0	192.168.1.120
0	192.168.1.124
0	192.168.1.128
0	192.168.1.132
0	192.168.1.136
1	192.168.1.72
1	192.168.1.80
1	192.168.1.88
2	192.168.1.0
2	192.168.1.16
3	192.168.1.112
3	192.168.1.116
3	192.168.1.140
4	192.168.0.0
5	192.168.1.32
5	192.168.1.40
5	192.168.1.48
5	192.168.1.56
5	192.168.1.64

Table 3 - Area Network ID

CONNECTIVITY REPORT

The IP configurations can be shown below. These Ips were assigned using DHCP. The first IP configuration is of a host belonging to HR network, and the second IP configuration is of a host belong to Classroom network.

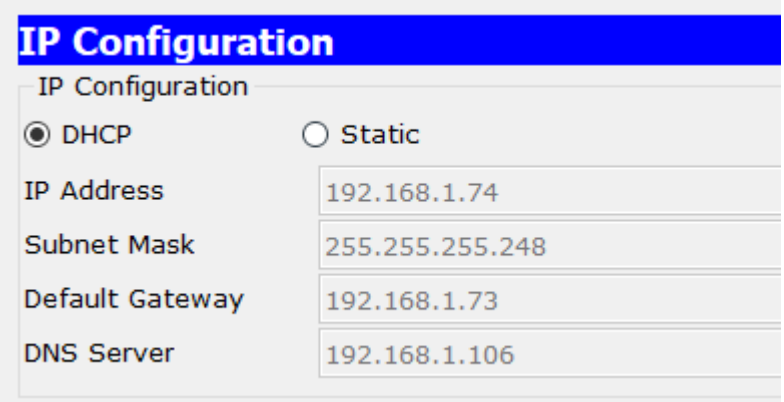


Figure 4 - IP Configuration

```
C>ipconfig /renew

   IP Address.....................: 192.168.1.36
   Subnet Mask....................: 255.255.255.248
   Default Gateway................: 192.168.1.33
   DNS Server.....................: 192.168.1.106
```

Figure 5- IP Configuration

The Multi area OSPFs are shown below. This is displayed using the command of *show ip route* on IT building's router. This router is connected to every other department's router. O IA represents Multi area OSPFs.

```
O IA 192.168.0.0/24 [110/65] via 192.168.1.134, 01:41:51, Serial0/2/1
     192.168.1.0/24 is variably subnetted, 20 subnets, 3 masks
O IA    192.168.1.0/28 [110/65] via 192.168.1.126, 01:41:51, Serial0/1/1
O IA    192.168.1.16/28 [110/65] via 192.168.1.126, 01:41:51, Serial0/1/1
O IA    192.168.1.32/29 [110/65] via 192.168.1.138, 01:41:51, Serial0/3/0
O IA    192.168.1.40/29 [110/65] via 192.168.1.138, 01:41:51, Serial0/3/0
O IA    192.168.1.48/29 [110/74] via 192.168.1.138, 01:41:51, Serial0/3/0
O IA    192.168.1.56/29 [110/65] via 192.168.1.138, 01:41:51, Serial0/3/0
O IA    192.168.1.64/29 [110/65] via 192.168.1.138, 01:41:51, Serial0/3/0
O IA    192.168.1.72/29 [110/65] via 192.168.1.122, 01:41:51, Serial0/1/0
O IA    192.168.1.80/29 [110/65] via 192.168.1.122, 01:41:51, Serial0/1/0
O IA    192.168.1.88/29 [110/65] via 192.168.1.122, 01:41:51, Serial0/1/0
C       192.168.1.96/29 is directly connected, FastEthernet0/0
C       192.168.1.104/29 is directly connected, FastEthernet0/1
O IA    192.168.1.112/30 [110/65] via 192.168.1.130, 01:41:51, Serial0/2/0
O IA    192.168.1.116/30 [110/65] via 192.168.1.130, 01:41:51, Serial0/2/0
C       192.168.1.120/30 is directly connected, Serial0/1/0
C       192.168.1.124/30 is directly connected, Serial0/1/1
C       192.168.1.128/30 is directly connected, Serial0/2/0
C       192.168.1.132/30 is directly connected, Serial0/2/1
C       192.168.1.136/30 is directly connected, Serial0/3/0
O IA    192.168.1.140/30 [110/65] via 192.168.1.130, 01:41:51, Serial0/2/0
```

Figure 6 - Multi area OSPF routes

Ping command was used to check connectivity between hosts after applying multi-area OSPF. The ping command was successful. Some examples are shown below

```
Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=2ms TTL=125
Reply from 192.168.0.2: bytes=32 time=2ms TTL=125
Reply from 192.168.0.2: bytes=32 time=12ms TTL=125
Reply from 192.168.0.2: bytes=32 time=5ms TTL=125

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 12ms, Average = 5ms
```

Figure 7 - Pinged from 192.168.1.36

```
Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=2ms TTL=125
Reply from 192.168.0.2: bytes=32 time=2ms TTL=125
Reply from 192.168.0.2: bytes=32 time=4ms TTL=125
Reply from 192.168.0.2: bytes=32 time=6ms TTL=125

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% l
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 6ms, Average = 3ms
```

Figure 8 - Pinged from 192.168.1.118

Access-list was created to deny telnet requests to Student Facilitation Centre, IT building and Faculty Building. It was also created to deny any IP request to Admin block. Example is shown below of a classroom network. This list was displayed using the command *show access-list*.

```
Extended IP access list 101
    10 deny tcp 192.168.1.32 0.0.0.7 host 192.168.1.1 eq telnet
    20 deny tcp 192.168.1.32 0.0.0.7 host 192.168.1.17 eq telnet
    30 deny tcp 192.168.1.32 0.0.0.7 host 192.168.1.117 eq telnet
    40 deny tcp 192.168.1.32 0.0.0.7 host 192.168.1.113 eq telnet (12 match(es))
    50 deny tcp 192.168.1.32 0.0.0.7 host 192.168.1.141 eq telnet
    60 deny tcp 192.168.1.32 0.0.0.7 host 192.168.1.105 eq telnet
    70 deny tcp 192.168.1.32 0.0.0.7 host 192.168.1.97 eq telnet
    90 deny ip 192.168.1.32 0.0.0.7 192.168.1.72 0.0.0.7
    100 deny ip 192.168.1.32 0.0.0.7 192.168.1.80 0.0.0.7
    110 deny ip 192.168.1.32 0.0.0.7 192.168.1.88 0.0.0.7 (4 match(es))
    120 permit ip any any
```

Figure 9 - An Access-list of a Classroom building router

A host of IP address 192.168.1.35 pinged all the networks (HR, Accounts Office and Principal Office) of admin building to see if the Access-list worked. Since it shows that Destination host unreachable, it means that access-lists are denying access to this host.

```
PC>ping 192.168.1.72

Pinging 192.168.1.72 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.72:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.80

Pinging 192.168.1.80 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.80:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.88

Pinging 192.168.1.88 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.88:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 10 - 192.168.1.35 pinging Admin Building networks

Since Principal office requires maximum security. It can't be accessed even by HR floor or Accounts office.

```
Pinging 192.168.1.88 with 32 bytes of data:

Reply from 192.168.1.73: Destination host unreachable.
Reply from 192.168.1.73: Destination host unreachable.
Reply from 192.168.1.73: Destination host unreachable.
Reply from 192.168.1.73: Destination host unreachable.

Ping statistics for 192.168.1.88:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 11 - Pinging Principal office from HR floor

```
PC>ping 192.168.1.88

Pinging 192.168.1.88 with 32 bytes of data:

Reply from 192.168.1.81: Destination host unreachable.
Reply from 192.168.1.81: Destination host unreachable.
Reply from 192.168.1.81: Destination host unreachable.
Reply from 192.168.1.81: Destination host unreachable.

Ping statistics for 192.168.1.88:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 12 - Pinging from Accounts office to Principal office

However, Principal's office can access any network in the topology.

```
Pinging 192.168.1.72 with 32 bytes of data:

Reply from 192.168.1.89: bytes=32 time=0ms TTL=255
Reply from 192.168.1.89: bytes=32 time=0ms TTL=255
Reply from 192.168.1.89: bytes=32 time=0ms TTL=255
Reply from 192.168.1.89: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.72:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.80

Pinging 192.168.1.80 with 32 bytes of data:

Reply from 192.168.1.89: bytes=32 time=1ms TTL=255
Reply from 192.168.1.89: bytes=32 time=0ms TTL=255
Reply from 192.168.1.89: bytes=32 time=0ms TTL=255
Reply from 192.168.1.89: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.1.0

Pinging 192.168.1.0 with 32 bytes of data:

Reply from 192.168.1.126: bytes=32 time=12ms TTL=253
Reply from 192.168.1.126: bytes=32 time=17ms TTL=253
Reply from 192.168.1.126: bytes=32 time=17ms TTL=253
Reply from 192.168.1.126: bytes=32 time=3ms TTL=253

Ping statistics for 192.168.1.0:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 17ms, Average = 12ms
```

Figure 13 - Principal office pinging other networks

IT building can access data of any department. No access-list is applied on IT building's router.

```
Pinging 192.168.1.72 with 32 bytes of data:

Reply from 192.168.1.122: bytes=32 time=1ms TTL=254
Reply from 192.168.1.122: bytes=32 time=2ms TTL=254
Reply from 192.168.1.122: bytes=32 time=1ms TTL=254
Reply from 192.168.1.122: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.1.72:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>ping 192.168.1.80

Pinging 192.168.1.80 with 32 bytes of data:

Reply from 192.168.1.122: bytes=32 time=9ms TTL=254
Reply from 192.168.1.122: bytes=32 time=1ms TTL=254
Reply from 192.168.1.122: bytes=32 time=7ms TTL=254
Reply from 192.168.1.122: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.1.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 9ms, Average = 4ms

PC>ping 192.168.1.88

Pinging 192.168.1.88 with 32 bytes of data:

Reply from 192.168.1.122: bytes=32 time=1ms TTL=254
Reply from 192.168.1.122: bytes=32 time=7ms TTL=254
Reply from 192.168.1.122: bytes=32 time=1ms TTL=254
Reply from 192.168.1.122: bytes=32 time=7ms TTL=254

Ping statistics for 192.168.1.88:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 7ms, Average = 4ms
```

Figure 14 - IT building pinging other networks

Port-security was implemented on all the ports of all switches. One of the port security can be shown below. The violation is shutdown mode.

```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)         (Count)
--------------------------------------------------------------------
        Fa0/1        1           1                0         Shutdown
        Fa0/2        1           1                0         Shutdown
        Fa0/3        1           1                0         Shutdown
        Fa0/4        1           1                0         Shutdown
        Fa0/5        1           1                0         Shutdown
        Fa0/6        1           1                0         Shutdown
        Fa0/7        1           1                0         Shutdown
        Fa0/8        1           1                0         Shutdown
        Fa0/9        1           1                0         Shutdown
       Fa0/10        1           1                0         Shutdown
--------------------------------------------------------------------
```

Figure 15 - Port security

No network can send telnet requests to Student facilitation centre, Faculty building and IT building. Access-lists were implemented on all routers except for the beforementioned routers. To verify this, telnet command was used by sending telnet requests.

```
PC>telnet 192.168.1.17
Trying 192.168.1.17 ...
% Connection timed out; remote host not responding
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...
% Connection timed out; remote host not responding
PC>telnet 192.168.1.113
Trying 192.168.1.113 ...
% Connection timed out; remote host not responding
PC>telnet 192.168.1.116
Trying 192.168.1.116 ...
% Connection timed out; remote host not responding
PC>telnet 192.168.1.117
Trying 192.168.1.117 ...
% Connection timed out; remote host not responding
PC>telnet 192.168.1.141
Trying 192.168.1.141 ...
% Connection timed out; remote host not responding
PC>telnet 192.168.1.97
Trying 192.168.1.97 ...
% Connection timed out; remote host not responding
PC>telnet 192.168.1.105
Trying 192.168.1.105 ...
% Connection timed out; remote host not responding
```

Figure 16 - HR being denied telnet requests

SERVERS OPERABILITY

DHCP SERVER:

DHCP Server is used to provide IP addresses to hosts of a network. Along with IP addresses, it also provides default gateway IP address and DNS IP address. For DHCP server configuration, all other services of the server were turned off and only DHCP service was turned on. After this, a pool name was provided to the server, default gateway, DNS server IP address, Start IP address and subnet masks was also assigned. Lastly, the pool was added to the server. Some of the pools are provided

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
Class5	192.168.1.49	192.168.1.106	192.168.1.50	255.255.255.248	6	0.0.0.0
Class4	192.168.1.65	192.168.1.106	192.168.1.66	255.255.255.248	6	0.0.0.0
Class3	192.168.1.57	192.168.1.106	192.168.1.58	255.255.255.248	6	0.0.0.0
Class2	192.168.1.41	192.168.1.106	192.168.1.42	255.255.255.248	6	0.0.0.0
Class1	192.168.1.33	192.168.1.106	192.168.1.34	255.255.255.248	6	0.0.0.0

Figure 17 - DHCP Pools

DNS SERVER:

DNS server is used to provide URL mapping from domain name to IP addresses. For DNS server, first we turned off all the other services in the server and only turned on DNS server. After this, name of the URL is provided such as www.google.com, and its IP address is assigned such as

192.168.1.107. 192.168.1.107 is the IP address of HTTP server. The DNS server gets HTML file from HTTP server by using this IP address.

No.	Name	Type	Detail
0	cep.com	A Record	192.168.1.107
1	cep1.com	A Record	192.168.1.107
2	www.google.com	A Record	192.168.1.107

Figure 18 - DNS addressing

HTTP SERVER:

HTTP server Is used to provide HTML file access to PCs. For this, first all the other services of the server were turned off and only HTTP service was turned on. Some of the files were already saved, and some were added.

File Manager

	File Name	Edit	Delete
1	cep1.html	(edit)	(delete)
2	copyrights.html	(edit)	(delete)
3	cscoptlogo177x...		(delete)
4	helloworld.html	(edit)	(delete)
5	image.html	(edit)	(delete)
6	index.html	(edit)	(delete)

Figure 19 - HTTP file manager

Figure 20 - Web browsing from a host

CHALLENGES

The initial challenge I faced was with the Access-list control configuration. It wasn't properly applying all the restrictions on the routers. If I applied telnet restriction, restriction to send packets to Principal office wasn't working and If I applied Principal office restriction, telnet restriction wasn't working properly. After some thinking, I made a single access-list for a single port which had restriction of access to Admin block as well as Telnet restriction instead of making a separate access-list for telnet and Admin block. It became functional after this implementation.

ALTERNATIVE METHOD

One possible alternative method is that we can implement DHCP by configuration on the router instead of a server.

COMMANDS

Commands for basic configuration on a router are listed below. The IP address and subnet masks were written according to the interfaces and networks.

enable
config term
int fa0/0 (it can be any according to interface)
ip address *ip-address subnet-mask*
no shutdown
int serial0/0 (it can be any according to interface)
ip address *ip-address subnet-mask*
clock rate 64000
no shutdown
exit

For multi area OSPF, following commands are used on each router. The router ospf 1 represents the process ID. Area-number was written according to the area. Network address is of the networks that are directly connected to a router. For instance, for area 1 that is Admin block, network addresses used were 192.168.1.72, 192.168.1.80 and 192.168.1.88 with wildmask of 0.0.0.7 for area 1 and 192.168.1.120 with wildmask of 0.0.0.3 for area 0.

enable
config term
router ospf 1
network network-address1 wildcard-mask area area-number
network network-address2 wildcard-mask area area-number
network network-address3 wildcard-mask area area-number
exit

For implementation of ACL for blocking access to Admin block by any department except for IT building, commands were used on the router near to traffic source. The source network address varies according to networks of a router. The addresses 192.168.1.88, 192.168.1.80, 192.168.1.72 are Admin block network IDs. The ID of access-list could be any access-list between 100 to 199. Access-list 101 is written as an example.

Access-list 101 deny ip source-network-address1 subnet-mask 192.168.1.88 0.0.0.7
Access-list 101 deny ip source-network-address2 subnet-mask 192.168.1.80 0.0.0.7
Access-list 101 deny ip source-network-address3 subnet-mask 192.168.1.72 0.0.0.7
Access-list 101 permit ip any any

After this command, interface of traffic was set

Int fa0/0 (is written according to interface)

Ip access-group *access-group-id* in

For implementation of ACL on Admin block, access-list commands used are listed below.

These commands were used to block access of HR office to Accounts office and Principal's office.

Access-list 101 deny ip 192.168.1.72 0.0.0.7 192.168.1.88 0.0.0.7
Access-list 101 deny ip 192.168.1.72 0.0.0.7 192.168.1.80 0.0.0.7
Access-list 101 permit ip any any
Int fa0/0
Ip access-group 101 in

These commands were used to block access of Accounts office to HR office and Principal's office:

Access-list 102 deny ip 192.168.1.80 0.0.0.7 192.168.1.72 0.0.0.7
Access-list 102 deny ip 192.168.1.80 0.0.0.7 192.168.1.88 0.0.0.7
Access-list 102 permit ip any any
Int fa0/1
Ip access-group 102 in

Commands used at Principal office were
No access-restriction was used on Principal's network except for restricting telnet requests. The commands used in global configuration mode are
Access-list 103 deny tcp 192.168.1.88 0.0.0.7 host 192.168.1.1 eq telnet
Access-list 103 deny tcp 192.168.1.88 0.0.0.7 host 192.168.1.17 eq telnet
Access-list 103 deny tcp 192.168.1.88 0.0.0.7 host 192.168.1.113 eq telnet
Access-list 103 deny tcp 192.168.1.88 0.0.0.7 host 192.168.1.117 eq telnet
Access-list 103 deny tcp 192.168.1.88 0.0.0.7 host 192.168.1.141 eq telnet
Access-list 103 deny tcp 192.168.1.88 0.0.0.7 host 192.168.1.97 eq telnet
Access-list 103 deny tcp 192.168.1.88 0.0.0.7 host 192.168.1.105 eq telnet
Access-list 103 permit ip any any
Int fa1/0
Ip access-group 103 in

The general commands to restrict Telnet requests are
Access-list *access-list-id* deny tcp *ip-address subnet-mask* host 192.168.1.1 eq telnet
Access-list *access-list-id* deny tcp *ip-address subnet-mask* host 192.168.1.1 eq telnet
Access-list *access-list-id* deny tcp *ip-address subnet-mask* host 192.168.1.1 eq telnet
Access-list *access-list-id* deny tcp *ip-address subnet-mask* host 192.168.1.1 eq telnet
Access-list *access-list-id* deny tcp *ip-address subnet-mask* host 192.168.1.1 eq telnet
Access-list *access-list-id* deny tcp *ip-address subnet-mask* host 192.168.1.1 eq telnet
Access-list *access-list-id* deny tcp *ip-address subnet-mask* host 192.168.1.1 eq telnet
Access-list *access-list-id* permit ip any any
Int fa0/0 (it is configured according to the interface)
Ip access-group *access-list-id* in

For **configuration of port security** of each port of each switch, the commands used are shown below. These commands are general where mac-address is different for every port according to the allowed host's mac-address.

enable
config term
int fa0/0 (changes depending upon interface)
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address mac-address
switchport port-security violation shutdown
exit

Other commands used to display different configuration were
Show ip route
Show access-list
Show port-security
Show ip protocols

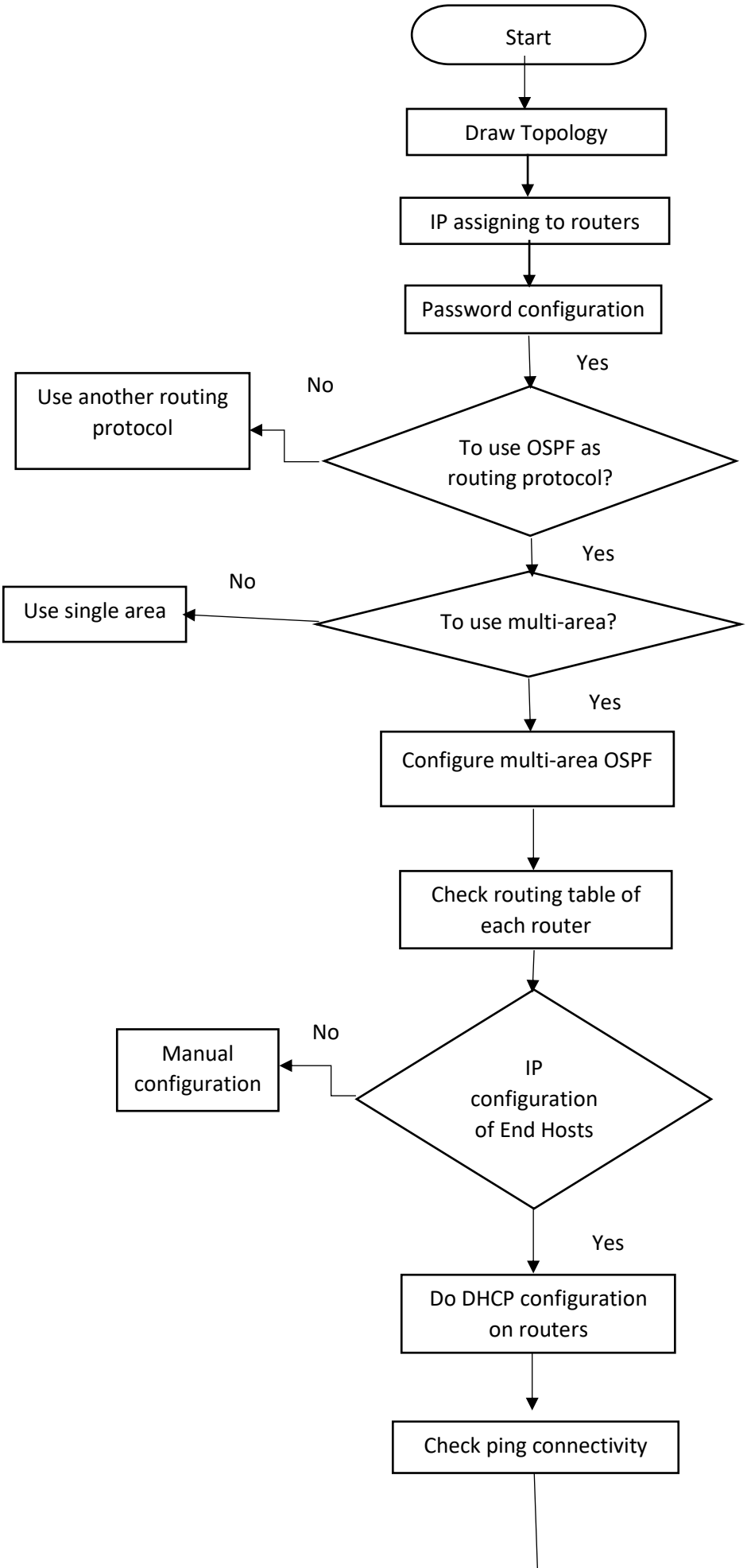
Commands for password configurations were used as following:

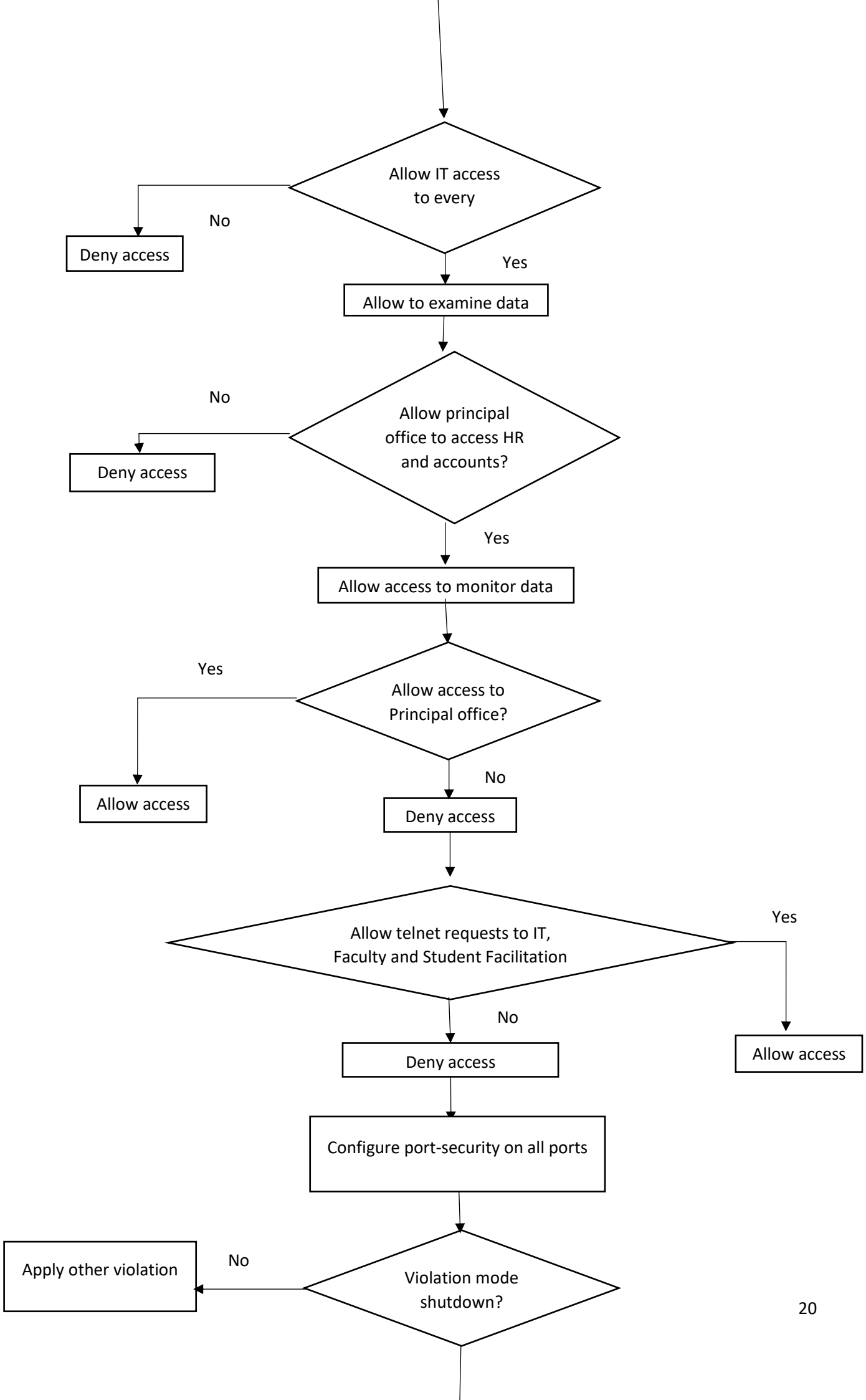
Enable
Config term
Enable password cisco
Exit

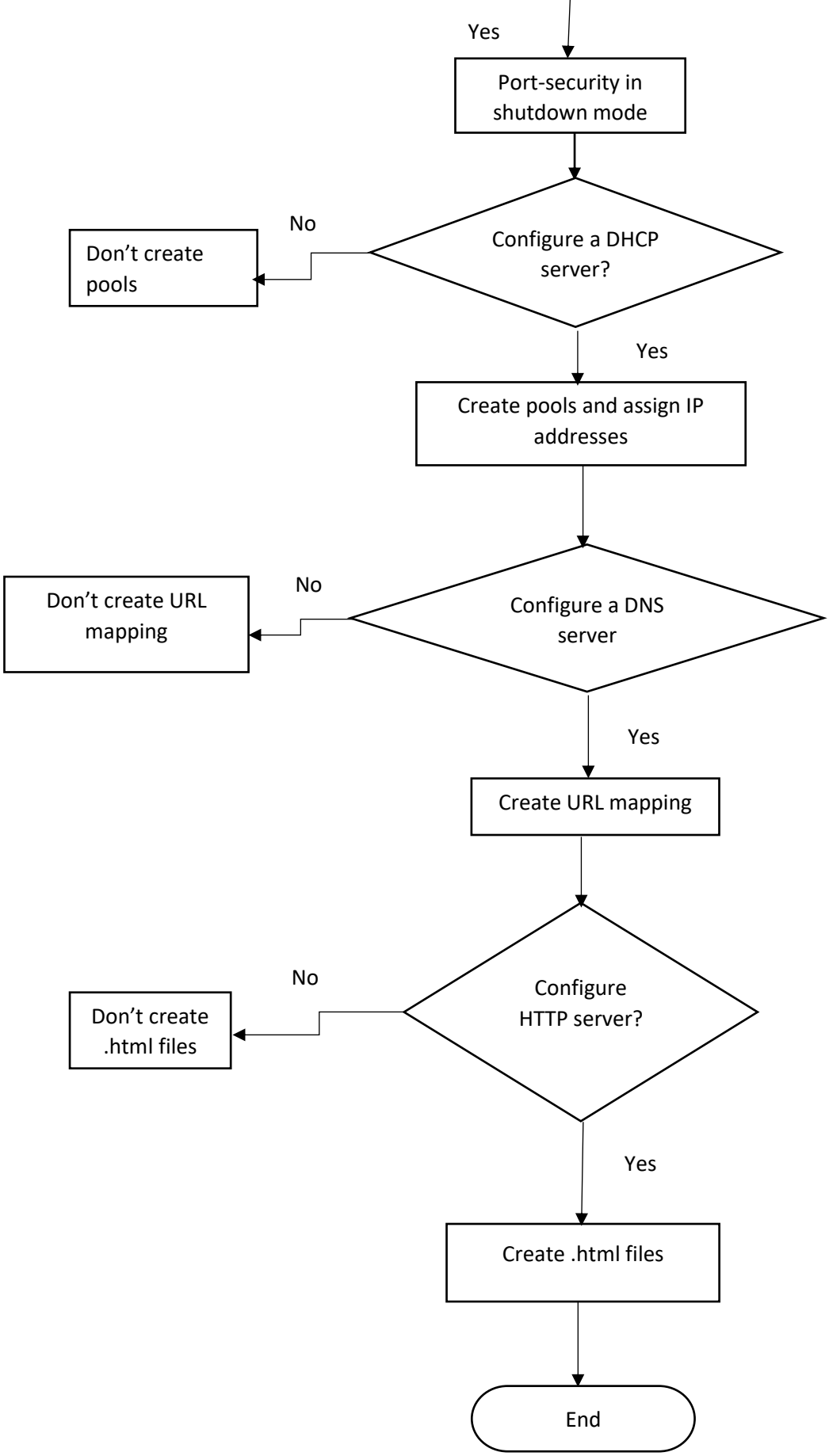
Enable
Config term
Line console 0
Password cisco
Login

Enable
Config term
Line vty 0 4
Password cisco
Login

FLOWCHART:


Start
Draw Topology
IP assigning to routers
Password configuration
Yes
No
Use another routing protocol
To use OSPF as routing protocol?
Yes
No
Use single area
To use multi-area?
Yes
Configure multi-area OSPF
Check routing table of each router
No
Manual configuration
IP configuration of End Hosts
Yes
Do DHCP configuration on routers
Check ping connectivity


Allow IT access to every
No
Deny access
Yes
Allow to examine data
No
Allow principal office to access HR and accounts?
Deny access
Yes
Allow access to monitor data
Yes
Allow access to Principal office?
Allow access
No
Deny access
Allow telnet requests to IT, Faculty and Student Facilitation
Yes
Allow access
No
Deny access
Configure port-security on all ports
Violation mode shutdown?
No
Apply other violation


Yes
Port-security in shutdown mode
Configure a DHCP server?
No
Don’t create pools
Yes
Create pools and assign IP addresses
Configure a DNS server
No
Don’t create URL mapping
Yes
Create URL mapping
Configure HTTP server?
No
Don’t create .html files
Yes
Create .html files
End