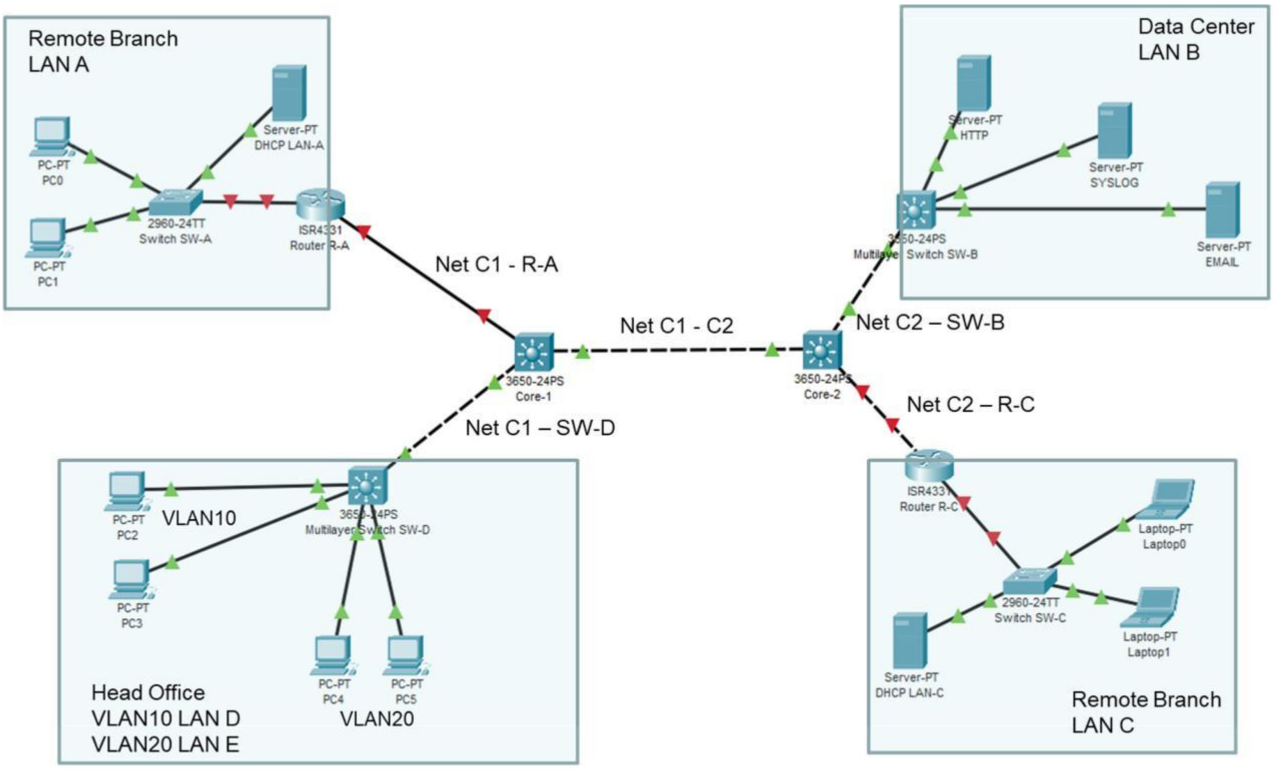
AMC Lab 3 Homework Deadline: 1.2.2021

Name: Rubaiya Kabir Pranti

QoS DiffServ Domain
for Enterprise IP Network



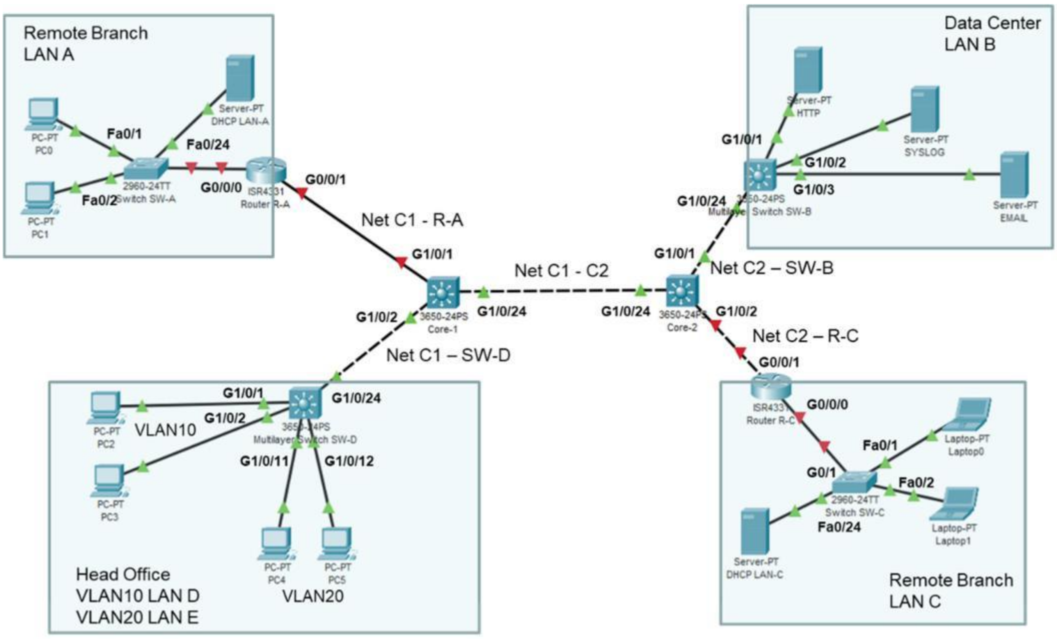
In this AMC lab you design and implement QoS for the enterprise network

Important Note: Write your answers in this PDF with red color
- with free Adobe Acrobat you may use
Comments/Notes Do not change the layout of this text
Do not use any other file format.
Do not create archive files

Homework / Preparation

Part 1: Correct your PT Topology and PT Configuration (if necessary)

Topology



Step 1: Network Addresses

Subnet Number	Subnet IP Address	Subnet Mask	Last Usable Host IP Address	Broadcast IP Address
LAN D (/24)	172.16.0.0	255.255.255.0	172.16.0.254	172.16.0.255
LAN E (/24)	172.16.1.0	255.255.255.0	172.16.1.254	172.16.1.255
LAN A (/26)	172.16.2.0	255.255.255.192	172.16.2.62	172.16.2.63
LAN C (/26)	172.16.2.64	255.255.255.192	172.16.2.126	172.16.2.127
LAN B (/27)	172.16.2.128	255.255.255.224	172.16.2.158	172.16.2.159
C1 – C2 (/30)	172.16.2.160	255.255.255.252	172.16.2.162	172.16.2.163
C1 – R-A (/30)	172.16.2.164	255.255.255.252	172.16.2.166	172.16.2.167
C1 – SW-D (/30)	172.16.2.168	255.255.255.252	172.16.2.170	172.16.2.171
C2 – SW-B (/30)	172.16.2.172	255.255.255.252	172.16.2.174	172.16.2.175
C2 – R-C (/30)	172.16.2.176	255.255.255.252	172.16.2.178	172.16.2.179

Step 2: Inter-Router/Switch Interfaces

Device	Interface	IP Address	Subnet Mask	Default Gateway
Core-1	G1/0/1	172.16.2.165	255.255.255.252	N/A
	G1/0/2	172.16.2.169	255.255.255.252	N/A
	G1/0/24	172.16.2.161	255.255.255.252	N/A
Core-2	G1/0/1	172.16.2.173	255.255.255.252	N/A
	G1/0/2	172.16.2.177	255.255.255.252	N/A
	G1/0/24	172.16.2.162	255.255.255.252	N/A
R-A	G0/0/0	172.16.2.62	255.255.255.192	N/A
	G0/0/1	172.16.2.166	255.255.255.252	N/A
SW-B	G1/0/24	172.16.2.174	255.255.255.252	N/A
	VLAN1	172.16.2.158	255.255.255.224	N/A
R-C	G0/0/0	172.16.2.126	255.255.255.192	N/A
	G0/0/1	172.16.2.178	255.255.255.252	N/A
SW-D	G1/0/24	172.16.2.170	255.255.255.252	N/A
	VLAN10	172.16.0.254	255.255.255.0	N/A
	VLAN20	172.16.1.254	255.255.255.0	N/A

Step 3: Host and Server Interfaces

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC-0	NIC	172.16.2.1	255.255.255.192	172.16.2.62
PC-1	NIC	172.16.2.2	255.255.255.192	172.16.2.62
DHCP-LAN A	NIC	172.16.2.61	255.255.255.192	172.16.2.62
HTTP-Server	NIC	172.16.2.129	255.255.255.224	172.16.2.158
SYSLOG-Ser.	NIC	172.16.2.130	255.255.255.224	172.16.2.158
EMAIL-Server	NIC	172.16.2.131	255.255.255.224	172.16.2.158
Laptop-0	NIC	172.16.2.65	255.255.255.192	172.16.2.126
Laptop-1	NIC	172.16.2.66	255.255.255.192	172.16.2.126
DHCP-LAN C	NIC	172.16.2.125	255.255.255.192	172.16.2.126
PC-2	NIC	172.16.0.1	255.255.255.0	172.16.0.254
PC-3	NIC	172.16.0.2	255.255.255.0	172.16.0.254
PC-4	NIC	172.16.1.1	255.255.255.0	172.16.1.254
PC-5	NIC	172.16.1.2	255.255.255.0	172.16.1.254

Part 2: DiffServ Service Engineering

Step 1: Service Description and DiffServ classes

a. Service 1 (network management):
SSH and OSPF network management traffic. SSH uses standard port. OSPF is not encapsulated in TCP or UDP, but OSPF has its own protocol number – directly encapsulated in IP.
Service 1 is DiffServ class AF11.

b. Service 2 (priority data):
Priority data traffic (HTTPS only) to the central host 172.16.2.129.
Service 2 is DiffServ class AF21.

c. Service 3 (normal data):
Syslog traffic, from any source routed to the Syslog server.
Service 3 is DiffServ class AF43.

d. Service 4 (background traffic):
Any traffic of any application, from any source routed to any destination.
Service 4 is DiffServ class BE.

Create a map of Service to DiffServ class to DSCP mapping

Service	DiffServ class	DSCP
Service 1	**AF11**	**10**
Service 2	**AF21**	**18**
Service 3	**AF43**	**38**
Service 4	**BE**	**0**

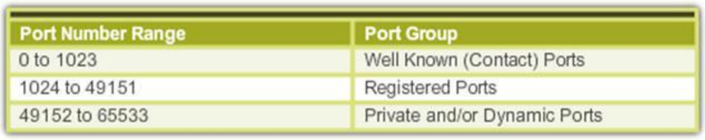
Step 2: Service IP flow match

Create a map which matches protocol, port (optional), Client and server IP address to Services

Service	Protocol	Client IP address	Client Port	Server IP address	Server Port
Service 1	**TCP/UDP**	**any**	**-**	**any**	**22**
	OSPF	**any**	**-**	**any**	**-**
Service 2	**TCP**	**any**	**-**	**172.16.2.129**	**443**
Service 3	**UDP**	**any**	**-**	**172.16.2.130**	**514**
Service 4	**IP**	**any**	**-**	**any**	**-**

Notes:

1. Service 1 needs two entries.
2. If "IP address" or "Port" can be more than one host, use "any" keyword for the parameter.
3. Some protocol(s) do not have port number(s).
4. Aside Well-known Port Numbers for defined protocols, corresponding shall clients use Dynamic Port Numbers.



Port Number Range	Port Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65533	Private and/or Dynamic Ports

Step 3: Extended ACL

a. The following commands of an extended ACL are given for router R1.
For each line, explain which IP flow is filtered

```
Line1:
R1(config)#access-list 101 permit icmp any 192.168.2.128 0.0.0.63 echo-reply
```

Protocol	**icmp**
Source IP range	**any**
Source Port (optional)	-
Destination IP range	**192.168.2.128 – 192.168.2.191**
Destination Port (optional)	-
Message Type	**echo-reply**

```
Line2:
R1(config)#access-list 101 permit tcp any host 192.168.2.129 eq 80
```

Protocol	**tcp**
Source IP range	**any**
Source Port (optional)	-
Destination IP range	**192.168.2.129**
Destination Port (optional)	**80**

```
Line3:
R1(config)#access-list 101 permit tcp any 192.168.1.0 0.0.0.255 eq 443
```

Protocol	**tcp**
Source IP range	**any**
Source Port (optional)	-
Destination IP range	**192.168.1.0-192.168.1.255**
Destination Port (optional)	**443**

```
Line4:
R1(config)#access-list 101 permit tcp host 192.168.3.3
                                              host 192.168.1.3 range 22 23
```

Protocol	**tcp**
Source IP range	**192.168.3.3**
Source Port (optional)	-
Destination IP range	**192.168.1.3**
Destination Port (optional)	**22-23**
Application(s)	**ssh and telnet (remote maintenance)**

b. Test ACL matches

1. ACLs walk through rules from top to bottom, execute the first hit of an ACL line and stop execution (no waterfall model). The sequence of rules is important.
2. ACLs also have an implicit deny default line at the end. In this extended ACL 101 for any IP encapsulated protocol like:

```
Implicit Line:
R1(config)#access-list 101 deny ip any any
```

Task b.1):

You apply the ACL 101 of a.). The ACL tests an HTTPS request to the Webserver 192.168.1.65 from the source IP address 10.0.0.1. In which line of the ACL 101 do you get a hit for such a packet?
Line 3

Task b.2):

You apply the ACL 101 of a.). The ACL tests an ICMP ping request from IP address 192.168.3.3 to destination 192.168.2.10. In which line of the ACL 101 do you get a hit for such a packet?
Line 1

Step 4: class-map

a. Configure a traffic class **myclass** which matches ACL 101 traffic from Step 3.

```
R1(config)#class-map match-any myclass
R1(config-cmap)#match access-group 101
R1(config-cmap)#exit
```

b. Configure one traffic class **high-class** for two IP flows:

- Any Email traffic (SMTP only) to the single destination IP address 172.16.2.131
- Any traffic of expedited forwarding DiffServ class

First create the required ACL with number 100, use port numbers instead of protocol names. Then create the class-map.

```
R1(config)#access-list 100 permit tcp any host 172.16.2.131 eq 25
R1(config)#class-map match-any high-class
R1(config-cmap)#match access-group 100
R1(config-cmap)#match ip dscp EF
R1(config-cmap)#exit
```

c. The traffic class **class-default** matches any unspecified traffic in a router. Which commands would create a class-default and this behavior?

```
R1(config)# class-map match-any   class-default
R1(config-cmap)#match any
R1(config-cmap)#match any would create a class-default and this behavior.
```

Step 5: policy-map

a. Configure a policy **mypolicy** for 3 classes

- class **high-class** gets 100 Mbps in periods of high load (CBWFQ scheduling)
- class **medium-class** gets 50 Mbps in periods of high load (CBWFQ scheduling) and is policed at 50 Mbps with best practice for Bc and Be (Tc = 4ms).
- class **low-class** gets 20 Mbps in periods of high load (CBWFQ scheduling).

The sequence of policy per class shall be according to the priority of classes.

```
R1(config)#policy-map mypolicy
R1(config-pmap)#class high-class
R1(config-pmap-c)#priority 100000   (in kbps)
R1(config-pmap-c)#class medium-class
R1(config-pmap-c)#police 50000000 25000 50000 conform-action exceed-action drop violate-action drop
R1(config-pmap-c#  bandwidth 50000 (in kbps)
R1(config-pmap-c)#class low-class

R1(config-pmap-c)#bandwidth 20000

R1(config-pmap-c)#end
```