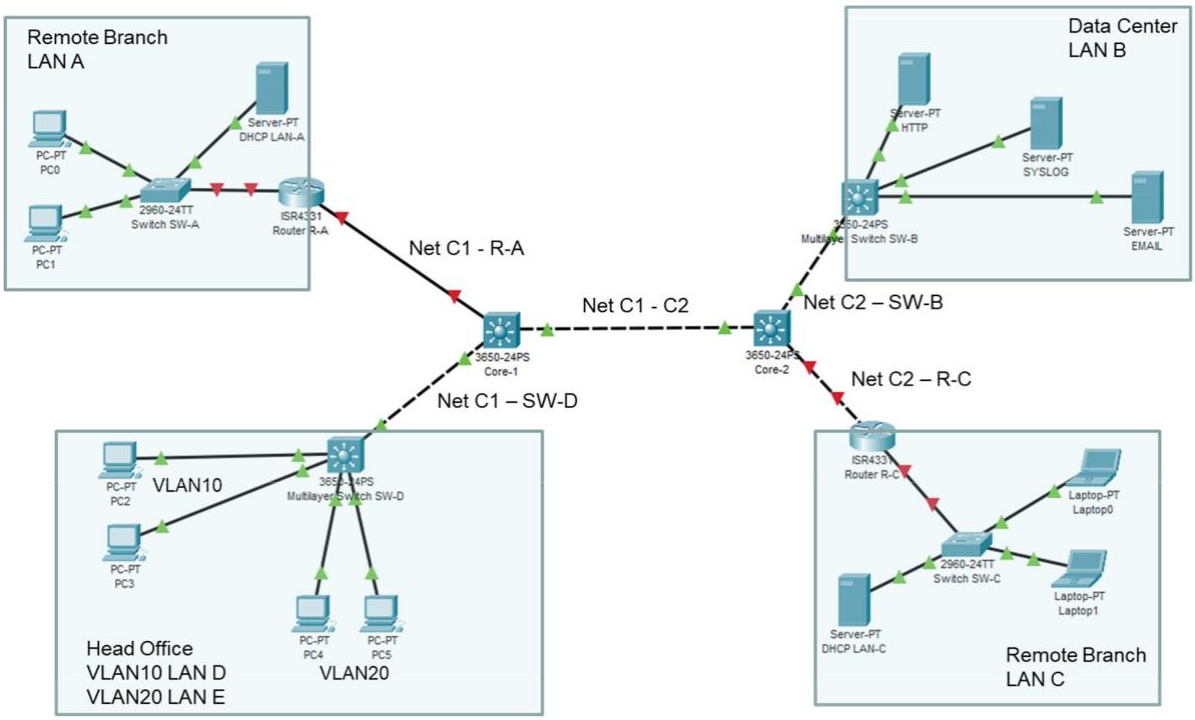
AMC Lab 3 Instruction Deadline: 8.2.2021

Name: Rubaiya Kabir Pranti

QoS DiffServ Domain
for Enterprise IP Network



Tasks:

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

Tasks **Enterprise Network PT Topology**

DiffServ DSCP Mapping

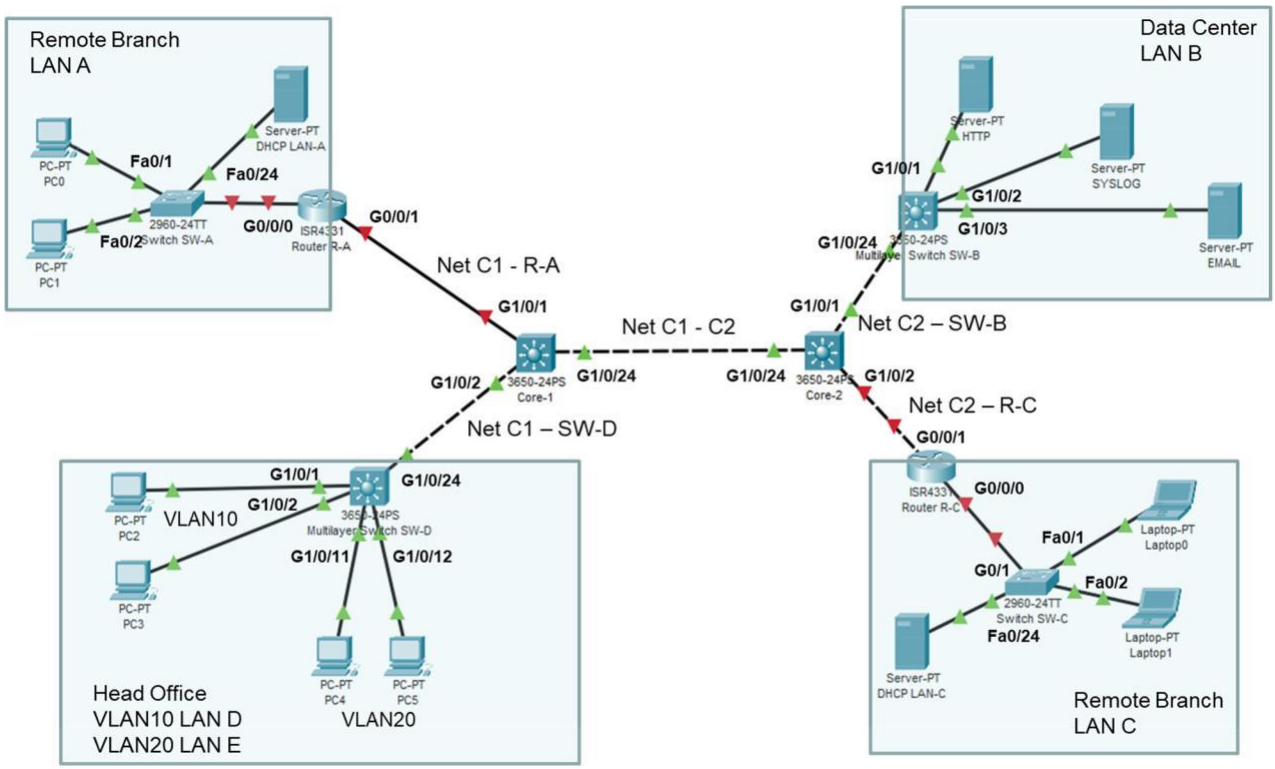
DiffServ Network Scheduling

Implement and Test DiffServ Domain

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

Task 1 – Enterprise Network PT Topology

Topology



Part 1: Baseline PT Topology

Step 1: Ensure correct PT Topology and Configuration

1. We continue with the PT Topology of AMC Default Lab2. Ensure, that your PT Topology is working correctly. Correct your PT Topology in necessary. The sample solution is given in Ilias.
2. You can check your configurations by some **show** commands in privileged EXEC context:

```
#show ip interface brief
#show interface gx/y/z
#show ip route
#show running-configuration
```

Step 2: Check Connectivity

You can check connectivity by pinging interfaces. From one sample PC (PC2 in LAN-D) you may ping any other of the 10 networks. The ping must be successful, correct your PT topology, if it is not working.

PC2 to SW-D (Default Gateway) works (y/n)? **yes**

PC2 to PC1 works (y/n)? **yes**

PC2 to PC0 (LAN-A) works (y/n)? **yes**

PC2 to SW-B works (y/n)? **yes**

PC2 to R-C works (y/n)? **yes**

PC2 to LAN-E works (y/n)? **yes**

PC2 to R-A works (y/n)? **yes**

PC2 to PC2 works (y/n)? **yes**

PC2 to HTTP Server (LAN-B) works (y/n)? **yes**

PC2 to Laptop0 (LAN-C) works (y/n)? **yes**

Task 2 – DiffServ DSCP Mapping

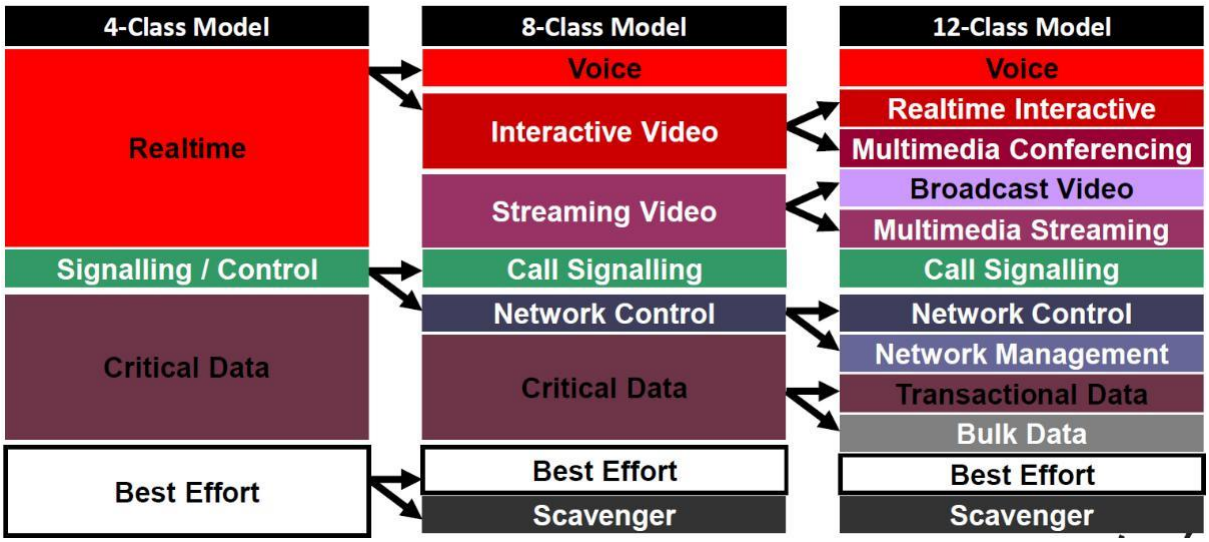
Part 1: Services and DiffServ Classes

List of Services

The following services shall be operated in your Enterprise network.

Service	Description	Requirement
Service1	Telephony with SIP signaling and RTP voice encapsulation	Minimum delay network scheduling for streaming media, guaranteed 8 Mbps streaming media throughput to and from any LAN. Peer-to-Peer RTP traffic is allowed. 800 kbps high priority Call Signaling Traffic per client LAN. Any SIP signaling traffic is pin-point routed to the central VoIP Call Server at IP address 172.16.2.130 in the Data Center
Service2	Websocket access to the HTTP Enterprise Server for Enterprise Resource Planning (ERP)	120 Mbps guaranteed ERP High-Throughput Transactional Data Traffic between any client LAN and the ERP Server (IP address 172.16.2.129).
Service3	Network Management traffic (Operations, Administration, and Maintenance (OAM)) using ICMP and SSH between Data Center connecting to any network device or client LAN.	Up to 10 Mbps guaranteed management traffic from any LAN to any other network device or LAN. Admins may be connected in any LAN.
Service4	Any other traffic	In minimum 40 Mbps throughput guaranteed on any link in periods of high load.

We follow the 12-Class DiffServ Model which separates 12 different service classes.



More detailed, we will use the Application to PHB to DSCP mapping proposed in RFC 4594 to select adequate PHB and DCSP values for different services.

EF: Expedited Forwarding

AF: Assured Forwarding

CSx: DiffServ Class Selector x, which maps to the IP Precedence (IPP) (e.g. CS1: IPP = 1, CS6: IPP = 6)

DF: Default Class, maps to BE

Application	L3 Classification		IETF
	PHB	DSCP	RFC
Network Control	CS6	48	RFC 2474
VoIP Telephony	EF	46	RFC 3246
Call Signaling	CS5	40	RFC 2474
Multimedia Conferencing	AF41	34	RFC 2597
Real-Time Interactive	CS4	32	RFC 2474
Multimedia Streaming	AF31	26	RFC 2597
Broadcast Video	CS3	24	RFC 2474
Low-Latency Data	AF21	18	RFC 2597
OAM	CS2	16	RFC 2474
High-Throughput Data	AF11	10	RFC 2597
Best Effort	DF	0	RFC 2474
Low-Priority Data	CS1	8	RFC 3662

22038

RFC 4594 Marking Recommendations

Step 1: Create Application to PHB to DSCP Mapping

1. Create a table with the mapping of Service Requirements to the per-hop-behavior (PHB) label and the DSCP values according to RFC 4594. This is a part of a Quality-of-Service document for any DiffServ QoS implementation.
2. Map Services or Sub-Services, if one service consists of several parts, to the appropriate PHB and DSCP of RFC 4594.
3. Define all mappings in sequence from Service 1 to Service 4.

   If more than one type of IP flow is used in one service, use one line per IP flow.

Service	Sub-Service Protocol and Server Port	PHB	DSCP
VOIP Telephony	protocol=RTP/UDP; port=16384-32767	EF	46
Call Signaling	protocol=UDP; port=5060/5061	CS5	40
ERP	protocol=TCP; port=80	AF11	10
OAM	protocol=ICMP; port=-	CS2	16
	protocol=TCP; port= 22		
Best Effort	protocol=IP; port= -	DF	0

Part 2: Edge and Core Routers

1. All devices in LANs are untrusted. Thus we have to create trusted traffic inside of our DiffServ domain. Check and classify which devices are edge routers (ingress, egress) and which devices are interior routers.
2. Check in the table which routers mark IP flows and which routers use defined network scheduling mechanisms.

Router	Router Classification	Marking	Defined Network Scheduling
R-A	edge router	*	*
SW-D	edge router	*	*
Core-1	interior router		*
Core-2	interior router		*
SW-B	edge router	*	*
R-C	edge router	*	*

Part 3: Identify IP Flows and create class-maps for Marking

Step 1: Display ACLs and class-maps

1. In upcoming tasks, you will work with ACLs and class-maps and create sample implementation at router R-A.
2. You can check these configurations by additional **show** commands in privileged EXEC context:

```
#show access-list
```

```
#show class-map
```

Step 2: Map PHB and DSCP to Marking Classes

We will have the following classes, predefined for your network.

1. Complete the table with the defined PHB and DSCP values.

Class	IP Flows	PHB	DSCP
VOIP	Telephony Streaming	EF	46
SIG	Telephony Signaling	CS5	40
ERP	ERP Data	AF11	10
OAM	OAM Data	CS2	16
class-default	Best Effort Data , any unmatched Data	DF	0

Step 3: Create a class-map for class SIG using ACL

1. Define a sample extended ACL **number 100** for Router R-A, interface g0/0/0 incoming traffic, to match SIP signaling traffic. Document the required ACL command here.
   SIG: access-list 100 permit udp host 172.16.2.62 host 172.16.2.130 eq 5060
2. Note the single SIP server host destination IP address and port number.
   host destination IP address=172.16.2.130 and port number=5060
3. Define the corresponding class-map SIG and record this class-map here:
   R-A(config)# class-map SIG
   R-A(config-cmap) #match access-group 100

Step 4: Create a class-map for class ERP using ACL

1. Define a sample extended ACL **number 101** for Router R-A, interface g0/0/0 incoming traffic, to match ERP traffic. Document the required ACL command here.
   access-list 101 permit tcp host 172.16.2.62 host 172.16.2.129 eq 80
2. Note the single HTTP server host destination IP address and port number.
   HTTP server host destination IP address=172.16.2.129 and port number=80
3. Define the corresponding class-map ERP and record this class-map here:
   R-A(config)# class-map ERP
   R-A(config-cmap) #match access-group 101

Step 5: Create a class-map for class OAM using ACL

1. **Note1:** Admins may be connected in any LAN and like to reach any device in the network.
2. **Note2:** All network devices and devices in LANs shall be reachable by ICMP and shall run an SSH server. This may require a detailed view into the source and destination ports, which are checked per ACL instruction line.
3. **Note3**: You may have more than one line per protocol in one ACL.
4. Define a sample extended ACL **number 102** for Router R-A, interface g0/0/0 incoming traffic, to match OAM traffic. Document the required ACL commands here.
   access-list 102 permit icmp any any
   access-list 102 permit tcp host 172.16.2.62 any eq 22
   access-list 102 permit tcp host 172.16.2.62 eq 22 any
5. Define the corresponding class-map OAM and record this class-map here:
   R-A(config)# class-map OAM
   R-A(config-cmap) #match access-group 102

Step 6: Create a class-map for class VOIP using NBAR

Network-Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications. When NBAR recognizes and classifies a protocol or application, the network can be configured to apply the appropriate quality of service (QoS) for that application or traffic with that protocol.
Note: NBAR uses the match command option **protocol** inside a class-map definition.

1. Define a class-map VOIP for Router R-A, using NBAR to match Voice-over-IP streaming traffic.
2. **Note**: Check the required protocol only.

   R-A(config)# class-map VOIP
   R-A(config-cmap) #match protocol rtp

Step 7: Check ACLs

1. Use the **show access-list** command at Router R-A to display ACLs.
2. Record which ACLs are defined.

R-A#sh access-list
Extended IP access list 100
10 permit udp host 172.16.2.62 host 172.16.2.130 eq 5060
Extended IP access list 101
10 permit tcp host 172.16.2.62 host 172.16.2.129 eq www
Extended IP access list 102
10 permit icmp any any
20 permit tcp host 172.16.2.62 any eq 22
30 permit tcp host 172.16.2.62 eq 22 any

Step 8: Check class-maps

1. Use the **show class-map** command at Router R-A to display class-maps.
2. Record which class-maps are defined.

R-A#sh class-map
Class Map match-any class-default (id 0)
Match any
Class Map match-all VOIP (id 1)
Match protocol rtp
Class Map match-all SIG (id 2)
Match access-group 100
Class Map match-all ERP (id 3)
Match access-group 101
Class Map match-all OAM (id 4)
Match access-group 102

From the displayed class-maps, which matching mechanism is used for class class-default?
As we know, system defines the default class by using the class class-default and by using match any mechanism.

Task 3 – DiffServ Network Scheduling

Part 1: Define Network Scheduling

Step 1: Map PHB and DSCP to Forwarding Classes

We will have the following classes, predefined for your network.

Note: Marking is only executed at ingress interfaces. Network scheduling must be executed at any forwarding network device interface. Execution of NBAR or Extended ACLs require higher computing power. It is less resource consuming just to check the DSCP field in IP packets. For this reason, we define new class-maps for forwarding purposes.

1. Complete the table with the defined PHB and DSCP values.

IP Flows	Class for Network Scheduling	PHB	DSCP
Telephony Streaming	PREMIUM	**EF**	**46**
Telephony Signaling	SIGNAL	**CS5**	**40**
OAM Data	HIGH	**CS2**	**16**
ERP Data	MEDIUM	**AF11**	**10**
Best Effort Data	class-default	**DF**	**0**

Step 2: Map Network Queueing Mechanism to Forwarding Classes

1. Define the network scheduling mechanism to meet the requirements of the **List of Services**.

Class for Network Scheduling	Network Scheduling Mechanism
PREMIUM	Priority Queueing
SIGNAL	CBWFQ
HIGH	CBWFQ
MEDIUM	CBWFQ
class-default	FIFO/ CBWFQ

Step 3: Create traffic matrix for bandwidth requirements

1. Each class requires some bandwidth according to the **List of Services**.
   - On some links aggregated bandwidth requirements must be calculated.
   - For bandwidth requirement calculation, note that only 2 LANs are connected to Multilayer Switch Core-2.
   - Take into account pin-point routing and peer-to-peer routing.
   - The link to the Data Center (LAN B) also has 8 Mbps bandwidth for VoIP media streaming.
   - Best effort traffic always gets a minimum of 40 Mbps on **any** link.

   Define the bandwidth requirements in kbps for each network link

	Service Bandwidth Requirement (in kbps)				
Class for Network Scheduling	**R-A to Core-1**	**R-C to Core-2**	**SW-D to Core-1**	**Core-1 to Core-2**	**SW-B to Core-2**
PREMIUM	8000	8000	16000	24000	8000
SIGNAL	800	800	1600	2400	3200
HIGH	10000	10000	20000	30000	10000
MEDIUM	120000	120000	240000	360000	480000
class-default	40000	40000	40000	40000	40000

Note: All throughput requirements are full duplex.

Part 2: Create policy-maps for Network Scheduling

1. In upcoming tasks, you will work with **sample policy-maps in router R-A.**
2. You can check these configurations by additional **show** commands in privileged EXEC context:

```
#show policy-map
#show policy-map interface <interface-id>
```

Step 1: Create a policy-map for class PREMIUM

1. Define a sample policy-map for class PREMIUM in router R-A for Link R-A to Core-1. Document this policy-map:
   R-A(config)# policy-map QOS (from task 4)
   R-A(config-pmap)#class PREMIUM
   R-A(config-pmap-c)# priority 8000

Step 2: Create a policy-map for class SIGNAL

1. Define a sample policy-map for class SIGNAL in router R-A for Link R-A to Core-1. Document this policy-map:
   R-A(config-pmap-c)#class SIGNAL
   R-A(config-pmap-c)# bandwidth 800

Step 3: Create a policy-map for class HIGH

1. Define a sample policy-map for class HIGH in router R-A for Link R-A to Core-1. Document this policy-map:
   R-A(config-pmap-c)#class HIGH
   R-A(config-pmap-c)# bandwidth 10000

Step 4: Create a policy-map for class MEDIUM

1. Define a sample policy-map for class MEDIUM in router R-A for Link R-A to Core-1. Document this policy-map:
   R-A(config-pmap-c)#class MEDIUM
   R-A(config-pmap-c)# bandwidth 120000

Step 5: Create a policy-map for class class-default

1. Define a sample policy-map for class class-default in router R-A, valid on any link. Document this policy-map:
   R-A(config-pmap-c)#class class-default
   R-A(config-pmap-c)# bandwidth 40000

Step 6: Check policy-maps

1. Use the show policy-map command to display policy-maps.
2. Record which policy-maps are defined.

Policy Map QOS
Class PREMIUM
Strict Priority
Bandwidth 8000 (kbps) Burst 200000 (Bytes)
Class SIGNAL
Bandwidth 800 (kbps) Max Threshold 64 (packets)
Class HIGH
Bandwidth 10000 (kbps) Max Threshold 64 (packets)
Class MEDIUM
Bandwidth 120000 (kbps) Max Threshold 64 (packets)
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)

Task 4 – Implement and Test DiffServ Domain

Part 1: Configure Edge Routers R-A and R-C

Step 1: Create class-maps for Marking all IP flows

1. Use class names and requirements of ACL or NBAR according to **Task2**.
2. Care about source and destination IP addresses and port numbers!

SIG: access-list 100 permit udp host 172.16.2.62 host 172.16.2.130 eq 5060
ERP: access-list 101 permit tcp host 172.16.2.62 host 172.16.2.129 eq 80
OAM: access-list 102 permit icmp any any
access-list 102 permit tcp host 172.16.2.62 any eq 22
access-list 102 permit tcp host 172.16.2.62 eq 22 any

Step 2: Create and activate policy-map MARK for Marking

1. Set the DSCP values in all classes according to **Task2**.

class-map:

```
class-map VOIP
match protocol rtp
class-map SIG
match access-group 100
class-map ERP
match access-group 101
class-map OAM
match access-group 102
class-map Class-default
match any
```

policy-map:

```
policy-map MARK
class VOIP
set ip dscp 46
class SIG
set ip dscp 40
class ERP
set ip dscp 10
class OAM
set ip dscp 16
class Class-default
set ip dscp 0
int g0/0/0
service-policy input MARK
```

```
R-A#sh policy-map
Policy Map MARK
Class VOIP
set ip dscp ef
Class SIG
set ip dscp cs5
Class ERP
set ip dscp af11
Class OAM
set ip dscp cs2
Class class-default
set ip dscp default
```

2. Overwrite DSCP values of incoming IP packets, even for BE traffic.

Step 3: Create class-maps for Forwarding all DSCP-marked IP flows

1. Use class names according to **Task3**.

class-map:

```
class-map PREMIUM
match ip dsp 46
class-map SIGNAL
match ip dscp 40
class-map HIGH
match ip dscp 16
class-map MEDIUM
match ip dscp 10
class-map Class-default
match any
```

output:

```
Class Map match-all PREMIUM (id 5)
Match ip dscp ef (46)
Class Map match-all SIGNAL (id 6)
Match ip dscp cs5 (40)
Class Map match-all HIGH (id 7)
Match ip dscp cs2 (16)
Class Map match-all MEDIUM (id 8)
Match ip dscp af11 (10)
```

Step 4: Create and activate policy-maps QOS for Forwarding

1. Apply the Network Scheduling Mechanisms with suitable Bandwidth calculation according to **Task3**.

policy-map:

```
policy-map QOS
class PREMIUM
priority 8000
class SIGNAL
bandwidth 800
class HIGH
bandwidth 10000
class MEDIUM
bandwidth 120000
class Class-default
bandwidth 40000
int g0/0/1
service-policy output QOS
```

```
Policy Map QOS
Class PREMIUM
Strict Priority
Bandwidth 8000 (kbps) Burst 200000 (Bytes)
Class SIGNAL
Bandwidth 800 (kbps) Max Threshold 64 (packets)
Class HIGH
Bandwidth 10000 (kbps) Max Threshold 64 (packets)
Class MEDIUM
Bandwidth 120000 (kbps) Max Threshold 64 (packets)
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)
```

Step 5: Check policy-maps

Check policy-map at router R-C.

R-C#sh policy-map
Policy Map MARK
Class VOIP
set ip dscp ef
Class SIG
set ip dscp cs5
Class ERP
set ip dscp af11
Class OAM
set ip dscp cs2
Class class-default
set ip dscp default

Policy Map QOS
Class PREMIUM
Strict Priority
Bandwidth 8000 (kbps) Burst 200000 (Bytes)
Class SIGNAL
Bandwidth 800 (kbps) Max Threshold 64 (packets)
Class HIGH
Bandwidth 10000 (kbps) Max Threshold 64 (packets)
Class MEDIUM
Bandwidth 120000 (kbps) Max Threshold 64 (packets)
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)

1. Record which policy-maps are implemented for BE traffic.

Class class-default
set ip dscp default
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)

----------R-C----------

SIG: access-list 100 permit udp host 172.16.2.126 host 172.16.2.130 eq 5060
ERP: access-list 101 permit tcp host 172.16.2.126 host 172.16.2.129 eq 80
OAM: access-list 102 permit icmp host 172.16.2.126 any
access-list 102 permit tcp host 172.16.2.126 any eq 22
access-list 102 permit tcp host 172.16.2.126 eq 22 any

INCOMING:

class-map:

class-map VOIP
match protocol rtp
class-map SIG
match access-group 100
class-map ERP
match access-group 101
class-map OAM
match access-group 102
class-map class-default
match any

policy-map:

```
policy-map MARK
class VOIP
set ip dscp 46
class SIG
set ip dscp 40
class ERP
set ip dscp 10
class OAM
set ip dscp 16
class Class-default
set ip dscp 0
int g0/0/0
service-policy input MARK
```

OUTGOING:

```
class-map PREMIUM
match ip dsp 46
class-map SIGNAL
match ip dscp 40
class-map HIGH
match ip dscp 16
class-map MEDIUM
match ip dscp 10
class-map Class-default
match any

policy-map QOS
class PREMIUM
priority 8000
class SIGNAL
bandwidth 800
class HIGH
bandwidth 10000
class MEDIUM
bandwidth 120000
class Class-default
bandwidth 40000
int g0/0/1
service-policy output QOS
```

Part 2: Configure Edge Routers SW-B and SW-D

Note1: Before applying NBAR, multiservice switches shall have Cisco Express Forwarding (CEF) enabled. CEF is switched-on by the command **ip cef** or **IP cef distributed** in privileged EXEC mode.

Note2: QoS shall be configured at router interface g1/0/24 instead of ingress switchport interfaces. Therefore, you configure one combined policy-map MARK_QOS

Step 1: Create combined class-maps for Marking and QoS Forwarding.

Class names shall be VOIP, SIG, ERP, OAM, and class-default according to **Task2**.

----------SW-D----------

```
SIG:  access-list 100 permit udp host 172.16.2.170 host 172.16.2.130 eq 5060
ERP: access-list 101 permit tcp host 172.16.2.170 host 172.16.2.129 eq 80
OAM: access-list 102 permit icmp host any any
        access-list 102 permit tcp host 172.16.2.170 any eq 22
        access-list 102 permit tcp host 172.16.2.170 eq 22 any

class-map VOIP
match protocol rtp
match ip dscp 46
class-map SIG
match access-group 100
match ip dscp 40
```

```
class-map ERP
match access-group 101
match ip dscp 10
class-map OAM
match access-group 102
match ip dscp 16
class-map class-default
match any
match ip dscp 0
```

output:

```
SW-D#sh class-map
Class Map match-any class-default (id 0)
Match any
Class Map match-all VOIP (id 1)
Match protocol rtp
Match ip dscp ef (46)
Class Map match-all SIG (id 2)
Match access-group 100
Match ip dscp cs5 (40)
Class Map match-all ERP (id 3)
Match access-group 101
Match ip dscp af11 (10)
Class Map match-all OAM (id 4)
Match access-group 102
Match ip dscp cs2 (16)
```

1. Care about source and destination IP addresses and port numbers!

Step 2: Create and activate policy-map MARK_QOS for Forwarding at interface g1/0/24

Apply the Network Scheduling Mechanisms with suitable Bandwidth calculation according to **Task3**.

policy-map:

```
policy-map MARK-QOS
class VOIP
priority 16000
set ip dscp 46
class SIG
bandwidth 1600
set ip dscp 40
class ERP
set ip dscp 10
bandwidth 240000
class OAM
bandwidth 20000
set ip dscp 16
class class-default
bandwidth 40000
set ip dscp 0

int g1/0/24
service-policy output MARK-QOS
```

Output:

```
SW-D#sh policy-map
Policy Map MARK_QOS
Class VOIP
Strict Priority
Bandwidth 16000 (kbps) Burst 400000 (Bytes)
set ip dscp ef
```

Class SIG
Bandwidth 1600 (kbps) Max Threshold 64 (packets)
set ip dscp cs5
Class ERP
Bandwidth 240000 (kbps) Max Threshold 64 (packets)
set ip dscp af11
Class OAM
Bandwidth 20000 (kbps) Max Threshold 64 (packets)
set ip dscp cs2
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)
set ip dscp default

In the same policy-map, set the DSCP values according to **Task2**.

1. Overwrite DSCP values of incoming IP packets, even for BE traffic.

----------SW-B----------

SIG: access-list 100 permit udp host 172.16.2.130 eq 5060 host 172.16.2.174
ERP: access-list 101 permit tcp host 172.16.2.129 eq 80 host 172.16.2.174
OAM: access-list 102 permit icmp host any any
access-list 102 permit tcp any eq 22 host 172.16.2.174
access-list 102 permit tcp any host 172.16.2.174 eq 22

Class-maps and policy-maps are same as SW-B configuration.

Output:

SW-B#sh class-map
Class Map match-any class-default (id 0)
Match any
Class Map match-all VOIP (id 1)
Match protocol rtp
Match ip dscp ef (46)
Class Map match-all SIG (id 2)
Match access-group 100
Match ip dscp cs5 (40)
Class Map match-all ERP (id 3)
Match access-group 101
Match ip dscp af11 (10)
Class Map match-all OAM (id 4)
Match access-group 102
Match ip dscp cs2 (16)

SW-B#sh policy-map
Policy Map MARK_QOS
Class VOIP
Strict Priority
Bandwidth 8000 (kbps) Burst 200000 (Bytes)
set ip dscp ef
Class SIG
Bandwidth 3200 (kbps) Max Threshold 64 (packets)
set ip dscp cs5
Class ERP
Bandwidth 480000 (kbps) Max Threshold 64 (packets)
set ip dscp af11

Class OAM
Bandwidth 10000 (kbps) Max Threshold 64 (packets)
set ip dscp cs2
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)
set ip dscp default

Part 3: Configure Core Routers Core-1 and Core-2

Note1: Before applying NBAR, multiservice switches shall have Cisco Express Forwarding (CEF) enabled. CEF is switched-on by the command **ip cef** or **IP cef distributed** in privileged EXEC mode.

Step 1: Create class-maps for Forwarding all DSCP-marked IP flows

1. Trust internal DSCP values.
2. Use class names according to **Task3**.

```
class-map PREMIUM
match ip dscp 46
class-map SIGNAL
match ip dscp 40
class-map HIGH
match ip dscp 16
class-map MEDIUM
match ip dscp 10
class-map class-default
match ip dscp 0

policy-map QOS11
class PREMIUM
priority 8000
class SIGNAL
bandwidth 800
class HIGH
bandwidth 10000
class MEDIUM
bandwidth 120000
class class-default
bandwidth 40000

int g1/0/1
service-policy output QOS11

policy-map QOS12
class PREMIUM
priority 16000
class SIGNAL
bandwidth 1600
class HIGH
bandwidth 20000
class MEDIUM
bandwidth 240000
class class-default
bandwidth 40000

int g1/0/2
service-policy output QOS12

policy-map QOS13
class PREMIUM
priority 24000
class SIGNAL
bandwidth 2400
class HIGH
shape average 30000000
class MEDIUM
bandwidth 360000
class class-default
bandwidth 40000
```

```
int g1/0/24
service-policy output QOS13

policy-map QOS21
class PREMIUM
priority 8000
class SIGNAL
bandwidth 3200
class HIGH
shape average 10000
class MEDIUM
bandwidth 480000
class class-default
bandwidth 40000

int g1/0/1
service-policy output QOS21

policy-map QOS22
class PREMIUM
priority 8000
class SIGNAL
bandwidth 800
class HIGH
bandwidth 10000
class MEDIUM
bandwidth 120000
class class-default
bandwidth 40000

int g1/0/2
service-policy output QOS22

policy-map QOS23
class PREMIUM
priority 24000
class SIGNAL
bandwidth 2400
class HIGH
shape average 30000000
class MEDIUM
bandwidth 360000
class class-default
bandwidth 40000

int g1/0/24
service-policy output QOS23
```

Step 2: Create and activate policy-maps for Forwarding

1. **Note:** Any forwarding interface at **core routers** must get rules for Forwarding.
   - Interface g1/0/1: Core-1: policy-map **QOS11** Core2: policy-map **QOS21**
   - Interface g1/0/2: Core-1: policy-map **QOS12** Core2: policy-map **QOS22**
   - Interface g1/0/24: Core-1: policy-map **QOS13** Core2: policy-map **QOS23**
2. Apply the Network Scheduling Mechanisms with bandwidth calculation from traffic matrix.
3. **For exercise purposes**:
   - Class **HIGH** on the link between Core-1 and Core-2, shall be **shaped** at average CIR in **addition**.
   - The shaped bandwidth shall be the same as required bandwidth for class HIGH on this link.

```
Core-1#sh class-map
Class Map match-any class-default (id 0)
Match any
Class Map match-all PREMIUM (id 1)
Match ip dscp ef (46)
Class Map match-all SIGNAL (id 2)
Match ip dscp cs5 (40)
Class Map match-all HIGH (id 3)
Match ip dscp cs2 (16)
Class Map match-all MEDIUM (id 4)
Match ip dscp af11 (10)

Core-1#sh policy-map
Policy Map QOS11
Class PREMIUM
Strict Priority
Bandwidth 8000 (kbps) Burst 200000 (Bytes)
Class SIGNAL
Bandwidth 800 (kbps) Max Threshold 64 (packets)
Class HIGH
Bandwidth 10000 (kbps) Max Threshold 64 (packets)
Class MEDIUM
Bandwidth 120000 (kbps) Max Threshold 64 (packets)
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)
Policy Map QOS12
Class PREMIUM
Strict Priority
Bandwidth 16000 (kbps) Burst 400000 (Bytes)
Class SIGNAL
Bandwidth 1600 (kbps) Max Threshold 64 (packets)
Class HIGH
Bandwidth 20000 (kbps) Max Threshold 64 (packets)
Class MEDIUM
Bandwidth 240000 (kbps) Max Threshold 64 (packets)
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)
Policy Map QOS13
Class PREMIUM
Strict Priority
Bandwidth 24000 (kbps) Burst 600000 (Bytes)
Class SIGNAL
Bandwidth 2400 (kbps) Max Threshold 64 (packets)
Class HIGH
Bandwidth 30000 (kbps) Max Threshold 64 (packets)
Traffic Shaping
Average Rate Traffic Shaping
CIR 30000000 (bps) Max. Buffers Limit 1000 (Packets)
Class MEDIUM
Bandwidth 360000 (kbps) Max Threshold 64 (packets)
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)
```

----------core-2----------

Core-2#sh policy-map
Policy Map QOS21
Class PREMIUM
Strict Priority
Bandwidth 8000 (kbps) Burst 200000 (Bytes)
Class SIGNAL
Bandwidth 3200 (kbps) Max Threshold 64 (packets)
Class HIGH
Bandwidth 10000 (kbps) Max Threshold 64 (packets)
Class MEDIUM
Bandwidth 480000 (kbps) Max Threshold 64 (packets)
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)
Policy Map QOS22
Class PREMIUM
Strict Priority
Bandwidth 8000 (kbps) Burst 200000 (Bytes)
Class SIGNAL
Bandwidth 800 (kbps) Max Threshold 64 (packets)
Class HIGH
Bandwidth 10000 (kbps) Max Threshold 64 (packets)
Class MEDIUM
Bandwidth 120000 (kbps) Max Threshold 64 (packets)
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)
Policy Map QOS23
Class PREMIUM
Strict Priority
Bandwidth 24000 (kbps) Burst 600000 (Bytes)
Class SIGNAL
Bandwidth 2400 (kbps) Max Threshold 64 (packets)
Class HIGH
Bandwidth 30000 (kbps) Max Threshold 64 (packets)
Class MEDIUM
Bandwidth 360000 (kbps) Max Threshold 64 (packets)
Class class-default
Bandwidth 40000 (kbps) Max Threshold 64 (packets)

Part 4: Save running-configurations

1. When you checked the correct implementation of the complete DiffServ Domain save your running configuration to the startup-configuration at any network device.
   Use the **copy running-config startup-config** command.
2. Save your PacketTracer file.

Part 5: Test DiffServ QoS Domain

Step 1: Close your PT file and restart your PT file

- By this step, all devices will reboot and all dynamic buffers and parameters will be reset.

Step 2: Check initial DSCP mapping in router R-A

1. At Router R-A display the policy-map statistics of interface g0/0/0. Record how many packets have been marked in different traffic classes:

- VOIP 0 packets
- SIG 0 packets
- ERP 0 packets
- OAM 0 packets
- class-default 30 packets (marked 0)

2. Display the Router R-A policy-map statistics of interface g0/0/1. Record how many packets have been scheduled in different traffic classes:

- PREMIUM 0 packets
- SIGNAL 0 packets
- HIGH 0 packets
- MEDIUM 0 packets
- class-default 3 packets

Step 3: Check DSCP mapping following some ICMP requests

1. From PC0 ping the server at IP address 172.16.2.130.
2. Display the Router R-A policy-map statistics of interface g0/0/1. Record how many packets have been scheduled in different traffic classes:

- HIGH 7 packets
- class-default 5 packets

3. Display the Multilayer Switch Core-2 policy-map statistics of interface g1/0/1. Record how many packets have been scheduled in different traffic classes:

- HIGH 6 packets – from g1/0/24 interface
- class-default 6 packets

Step 4: Check DSCP mapping following some HTTP requests

1. From Laptop0 use the Web Browser to request a Website from HTTP server at IP address 172.16.2.129.
2. Display the Router R-C policy-map statistics of interface g0/0/1. Record how many packets have been scheduled in different traffic classes:

- HIGH 0 packets
- MEDIUM 0 packets
- class-default 13 packets

3. Display the Multilayer Switch Core-2 policy-map statistics of interface g1/0/1. Record how many packets have been scheduled in different traffic classes:

- HIGH 5 packets
- MEDIUM 0 packets
- class-default 20 packets

4. Display the Multilayer Switch SW-B policy-map statistics of interface g1/0/24. Record how many packets have been scheduled in different traffic classes:

- HIGH 0 packets
- MEDIUM 0 packets
- class-default 22 packets

How many HTTP-Request have been sent to the HTTP-Server?

Not understandable from CLI

How many HTTP-Responses have been sent from the HTTP-Server?

Not understandable from CLI

Step 5: Demonstrate preemptive priority for VoIP

With the network devices in DN.Lab, you would have to demonstrate, that your DiffServ Domain is working correctly.

This final task cannot be performed in Packet Tracer and is skipped here.

In DN.Lab with different network devices, QoS has been implemented in above enterprise network. Specifically, the DiffServ architecture has been defined here for application of QoS.
The moto of enabling QoS here is to give priorities to distinguished traffic along the network. Additionally, to provide supportive bandwidth for particular links, to shape network traffic and so on.

In DiffServ Domain, DSCP (DiffServ Code Point) has been utilized as an indication of required QoS.
To implement the QoS in packet tracer, I have used two types of mapping. By using class-map, it's duty is to define/classify different traffic. And by policy-map, different traffic policies have been enabled.
Therefore, classification has been done here in routers of DN.Lab to prioritize one traffic from other which are represented by service classes through ACLs. Then marking is executed by mapping IP flows to service classes and by setting defined DSCP values to mark packets of IP flows. There is seen three types of routers in this Diffserv Domain which are ingress router, interior router and egress router.

In very first, R-A and R-C routers(ingress) have been configured where I used class map to classify IP Flows and policy map to set DSCP values for marking for **incoming traffic** from LAN A in ingress interface g0/0/0. After that, I again applied class map to match packets and policy map to implement PQ and CBWFQ (network scheduler algorithm) and other policies according to instructions for outgoing traffic at interface g0/0/1. This went same for other devices. However, to match IP flows, different extended ACLs (Access control Lists) were implemented in CLI as commands at very first before applying class maps and policy maps for edge routers. Not to mention, traffic shaping is also done between core1 and core2 through leaky bucket mechanism under policy-map.
After finishing required maps, policy-activation command was added to activate the policy to transmit packets successfully.

In short, router R-A, R-C, SW-B, SW-D have both interfaces called ingress and egress interface. For four of them, for incoming traffic, ingress interfaces were utilized for the purpose of matching traffic by ACLs and to classify traffic and to fix/set DSCP values. In egress interface, for outgoing traffic, they trusted the DSCP values at ingress ports and those traffic classes(ingress) were used by egress port and new queuing and scheduling mechanism had been used at egress ports. Lastly, the core routers, core1 and core2 had trusted the internal DSCP values and executed queueing and network scheduling parameters. Furthermore, cef (Cisco express forwading) was also activated for SW-B, SW-D,Core1 and Core2.

To demonstrate the preemptive priority for VoIP, we know that Priority Queueing(PQ) is used for preemptive priority that has been implemented here for the premium class called VOIP telephony. It has got strict priority over other service classes. The advantage for having PQ for VOIP is that it gets minimum delay and guranteed throughput.

Checkout

When you successfully finished this Lab

1. Save your results and answers **in this PDF file** and rename the file **AMC-Lab3-Results.pdf**.
2. Save the running configuration of **Router Core-2,** and of **Multilayer Switch SW-D** in one text file (**AMC-Lab3-Core-2_SW-D.txt**).
3. Upload these two files, **AMC-Lab3-Results.pdf** and **AMC-Lab3-Core-2_SW-D.txt** in Ilias.