

# CCNP ONT

## Cisco Router Challenge 130

### Outline

This challenge involves the configuration of a dial-peer.

### Objectives

The objectives of this challenge are to:

- Setup a dial-peer.

### Example

```
> enable
# config t
Router(config)# dial-peer ?
  cor          Class of Restriction
  hunt         Define the dial peer hunting choice
  outbound     Define the outbound options
  terminator   Define the address terminate character
  voice       Voice type
Router(config)# dial-p v ?
<1-2147483647> Voice dial-peer tag

Router(config)# dial-p voice 1 ?
  mmoip  Multi Media Over IP
  pots   Telephony
  voatm  Voice over ATM
  vofr   Voice over Frame Relay
  voip   Voice over IP

Router(config)# dial-p voice 1 pots

Router(config-dial-peer)# ?
DIALPEER configuration commands:
  answer-address  The Call Destination Number
  application     The selected application
  call-block     Incoming Call Blocking
  capacity       capacity update timer config
  carrier-id     Configure Carrier ID
  clid          Caller ID option
  corlist       set the Class of Restriction lists
  default       Set a command to its defaults
  description   Dialpeer specific description
  destination-pattern A full E.164 telephone number prefix
  digit-strip   Use digit strip option for the POTS digits replacement
  direct-inward-dial Use Called Number as final call destination
```

```

dnis-map          The name of a configured dnis-map
exit              Exit from dial-peer configuration mode
fax              Configure fax
forward-digits   Configure the destination digits forward of this
                 dialpeer
huntstop         Stop hunting on Dial-Peers
incoming         Incoming called number
information-type Information type for dialpeer
max-conn         Sets the maximum connections per peer, negation sets
                 to unlimited
no               Negate a command or set its defaults
numbering-type   The calling/called party numbering type
permission       set the call orig/term permission of this dialpeer
preference       Configure the preference order of this dialpeer
prefix           The pattern to be dialed before the dialed num
register         Register the E.164 number of this dial peer with
                 gatekeeper
resource         Resource allocation policy
session          The session [ target | protocol | transport ] for this
                 peer
shutdown         Change the Admin State of this peer to down (no->up)
supplementary-service Config supplementary service features
supported-language Language(s) supported by the peer
tgrep           TGREP config
tone            Generate tones
translate-outgoing Translation rule
translation-profile Translation profile
trunk-group-label Configure Trunk Group Label
trunkgroup       trunk groups associated with this peer
voice           Configure GATEWAY dial-peer for voice services
voice-class      Set Dial-peer voice class control parameters
Router(config-dial-peer)# destination-pattern ?
WORD A sequence of digits - representing the prefix or full telephone number
Router(config-dial-peer)# destination-pattern 11
Router(config-dial-peer)# port 1/1/1
Router(config-dial-peer)# exit

```

```

Router(config)# dial-p voice 2 voip

```

```

Router(config-dial-peer)# ?

```

```

DIALPEER configuration commands:

```

```

acc-qos          The Minimally Acceptable Quality of Service to be
                 used in getting to this peer
answer-address   The Call Destination Number
application       The selected application
call            Per Voip dial-peer Call configuration
call-block       Incoming Call Blocking
carrier-id       Configure Carrier ID
clid            Caller ID option
codec           The codec rate to be attempted in getting to this peer
corlist         set the Class of Restriction lists
default         Set a command to its defaults
description      Dialpeer specific description
destination-pattern A full E.164 telephone number prefix
dnis-map         The name of a configured dnis-map
dtmf-relay       Transport DTMF digits across IP link
exit            Exit from dial-peer configuration mode
expect-factor    Expectation Factor of voice quality
fax             Configure fax
fax-relay        fax-relay options
huntstop        Stop hunting on Dial-Peers
icpif           Calculated Planning Impairment Factor
incoming        Incoming called number

```

```

ip                Set ip packet options
max-conn          Sets the maximum connections per peer, negation sets
                  to unlimited
max-redirects    Configure the max number of redirects for this
                  dialpeer
modem             Modem commands through this peer
no               Negate a command or set its defaults
numbering-type   The calling/called party numbering type
permission       set the call orig/term permission of this dialpeer
playout-delay    Configure voice playout delay buffer
preference       Configure the preference order of this dialpeer
req-qos          The desired Quality of Service to be used in
                  getting to this peer

roaming          Use roaming server
rtp              RTP config
session         The session [ target | protocol | transport ] for this
                  peer

settle-call      Use settlement server
shutdown        Change the Admin State of this peer to down (no->up)
signal-type     The signaling type to be used when getting to this
                  peer

signaling        Signaling payload handling
snmp            Modify SNMP voice peer parameters
supplementary-service
tech-prefix     The H.323 gateway technology prefix
tone            Generate tones
translate-outgoing
translation-profile
trunk-group-label
trunkgroup      trunk groups associated with this peer
vad             Use VoiceActivityDetection as necessary option
voice           Configure GATEWAY dial-peer for voice services
voice-class     Set Dial-peer voice class control parameters

Router(config-dial-peer)# destination-pattern 22
Router(config-dial-peer)# session ?
  protocol      The session protocol to be used in getting to this peer
  target        The session target for this peer
  transport     The transport layer protocol used for this peer
Router(config-dial-peer)# sess target ?
  WORD          A string specifying the session target
Router(config-dial-peer)# session target ipv4:1.2.3.4

```

# Cisco Router Challenge 131

## Outline

This challenge involves the configuration of QoS (bandwidth and queue-limit).

## Objectives

The objectives of this challenge are to:

- Define QoS.
- Limit the bandwidth.
- Define a queue-limit.

## Example

```
> en
# config t

(config)# class-map ?
WORD          class-map name
match-all    Logical-AND all matching statements under this classmap
match-any     Logical-OR all matching statements under this classmap
(config)# class-map tayside
(config-cmap)#?
QoS class-map configuration commands:
description   Class-Map description
exit          Exit from QoS class-map configuration mode
match         classification criteria
no            Negate or set default values of a command
rename        Rename this class-map
(config-cmap)# exit
(config)# policy-map ankle
(config-pmap)# ?
QoS policy-map configuration commands:
class         policy criteria
description   Policy-Map description
exit          Exit from QoS policy-map configuration mode
no            Negate or set default values of a command
rename        Rename this policy-map
<cr>
(config-pmap)# class tayside
Router(config-pmap-c)# ?
QoS policy-map class configuration commands:
bandwidth     Bandwidth
exit          Exit from QoS class action configuration mode
fair-queue    Enable Flow-based Fair Queuing in this Class
no            Negate or set default values of a command
police        Police
priority      Strict Scheduling Priority for this Class
queue-limit   Queue Max Threshold for Tail Drop
random-detect Enable Random Early Detection as drop policy
service-policy Configure QoS Service Policy
set           Set QoS values
shape         Traffic Shaping
<cr>
(config-pmap-c)# bandwidth ?
<8-2000000>   Kilo Bits per second
percent       % of Available Bandwidth
(config-pmap-c)# bandwidth 128
(config-pmap-c)# queue-limit ?
<1-512>       Packets
(config-pmap-c)# queue-limit 21
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int s0
(config-if)# service-policy output ankle
```

The class map defines the traffic.

# Cisco Router Challenge 132

## Outline

This challenge involves the configuration of QoS (default-class).

## Objectives

The objectives of this challenge are to:

- Define QoS.
- Define a default class.

## Example

```
> en
# config t

(config)# class-map ?
WORD          class-map name
match-all    Logical-AND all matching statements under this classmap
match-any     Logical-OR all matching statements under this classmap
(config)# class-map tayside
(config-cmap)#?
QoS class-map configuration commands:
description   Class-Map description
exit          Exit from QoS class-map configuration mode
match         classification criteria
no            Negate or set default values of a command
rename        Rename this class-map
(config-cmap)# exit
(config)# policy-map ankle
(config-pmap)# ?
QoS policy-map configuration commands:
class         policy criteria
description   Policy-Map description
exit         Exit from QoS policy-map configuration mode
no           Negate or set default values of a command
rename        Rename this policy-map
<cr>
(config-pmap)# class tayside
Router(config-pmap-c)# ?
QoS policy-map class configuration commands:
bandwidth     Bandwidth
exit          Exit from QoS class action configuration mode
fair-queue    Enable Flow-based Fair Queuing in this Class
no            Negate or set default values of a command
police        Police
priority      Strict Scheduling Priority for this Class
```

```

queue-limit      Queue Max Threshold for Tail Drop
random-detect    Enable Random Early Detection as drop policy
service-policy   Configure QoS Service Policy
set              Set QoS values
shape            Traffic Shaping
<cr>
(config-pmap-c)# bandwidth ?
<8-2000000>      Kilo Bits per second
percent          % of Available Bandwidth
(config-pmap-c)# bandwidth 128
(config-pmap-c)# queue-limit ?
<1-512>          Packets
(config-pmap-c)# queue-limit 21
(config-pmap-c)# exit
(config-pmap)# class ?
WORD             class-map name
class-default    System default class matching otherwise unclassified
packets
(config-pmap)# class class-default
(config-pmap-c)# fair-queue
(config-pmap)# exit
(config)# int s0
(config-if)# service-policy output ankle

```

The class-default class does not have to be created before it is used in the policy-map. It supports any other traffic which does not match the class maps.

## Cisco Router Challenge 133

### Outline

This challenge allows the maximum bandwidth to be defined.

### Objectives

The objectives of this challenge are to:

- Define QoS.
- Define interesting traffic types with a class-map.

```

# config t
(config)# access-list 100 permit tcp host 165.246.68.4 host 200.194.252.5 eq echo
(config)# class-map Delaware
(config-cmap)# ?
QoS class-map configuration commands:
description    Class-Map description
exit           Exit from QoS class-map configuration mode
match          classification criteria
no             Negate or set default values of a command
rename         Rename this class-map
(config-cmap)# description testing

```

**(config-cmap)# match ?**

access-group	Access group
any	Any packets
class-map	Class map
cos	IEEE 802.1Q/ISL class of service/user priority values
destination-address	Destination address
discard-class	Discard behavior identifier
dscp	Match DSCP in IP(v4) and IPv6 packets
fr-de	Match on Frame-relay DE bit
fr-dlci	Match on fr-dlci
input-interface	Select an input interface to match
ip	IP specific values
mpls	Multi Protocol Label Switching specific values
not	Negate this match result
packet	Layer 3 Packet length
precedence	Match Precedence in IP(v4) and IPv6 packets
protocol	Protocol
qos-group	Qos-group
source-address	Source address

**(config-cmap)# match protocol ?**

arp	IP ARP
bgp	Border Gateway Protocol
bridge	Bridging
bstun	Block Serial Tunnel
cdp	Cisco Discovery Protocol
citrix	Citrix Traffic
compressedtcp	Compressed TCP
cuseeme	CU-SeeMe desktop video conference
custom-01	Custom protocol custom-01
custom-02	Custom protocol custom-02
custom-03	Custom protocol custom-03
custom-04	Custom protocol custom-04
custom-05	Custom protocol custom-05
custom-06	Custom protocol custom-06
custom-07	Custom protocol custom-07
custom-08	Custom protocol custom-08
custom-09	Custom protocol custom-09
custom-10	Custom protocol custom-10
dhcp	Dynamic Host Configuration
dls	Data Link Switching (Direct encapsulation only)
dns	Domain Name Server lookup
egp	Exterior Gateway Protocol
eigrp	Enhanced Interior Gateway Routing Protocol
exchange	MS-RPC for Exchange
fasttrack	FastTrack Traffic - KaZaA, Morpheus, Grokster...
finger	Finger
ftp	File Transfer Protocol
gnutella	Gnutella Traffic - BearShare, LimeWire, Gnutella...
gopher	Gopher
gre	Generic Routing Encapsulation
http	World Wide Web traffic
icmp	Internet Control Message
imap	Internet Message Access Protocol
ip	IP
ipinip	IP in IP (encapsulation)
ipsec	IP Security Protocol (ESP/AH)
ipv6	IPv6
irc	Internet Relay Chat
kazaa2	Kazaa Version 2
kerberos	Kerberos
l2tp	L2F/L2TP tunnel
ldap	Lightweight Directory Access Protocol
llc2	llc2

```

napster      Napster Traffic
netbios      NetBIOS
netshow      Microsoft Netshow
nfs          Network File System
nntp         Network News Transfer Protocol
notes        Lotus Notes(R)
novadigm     Novadigm EDM
ntp          Network Time Protocol
pad          PAD links
pcanywhere   Symantec pcANYWHERE
pop3         Post Office Protocol
pppoe        PPP over Ethernet
pptp         Point-to-Point Tunneling Protocol
printer      print spooler/lpd
qllc         qllc protocol
rcmd         BSD r-commands (rsh, rlogin, rexec)
rip          Routing Information Protocol
rsrb         Remote Source-Route Bridging
rsvp         Resource Reservation Protocol
rtp          Real Time Protocol
rtsplayer    RTSP players streaming protocol
secure-ftp   FTP over TLS/SSL
secure-http  Secured HTTP
secure-imap  Internet Message Access Protocol over TLS/SSL
secure-irc   Internet Relay Chat over TLS/SSL
secure-ldap  Lightweight Directory Access Protocol over TLS/SSL
secure-nntp  Network News Transfer Protocol over TLS/SSL
secure-pop3  Post Office Protocol over TLS/SSL
secure-telnet Telnet over TLS/SSL
smtp         Simple Mail Transfer Protocol
snapshot     Snapshot routing support
snmp         Simple Network Management Protocol
socks        SOCKS
sqlnet       SQL*NET for Oracle
sqlserver    MS SQL Server
ssh          Secured Shell
streamwork   Xing Technology StreamWorks player
stun         Serial Tunnel
sunrpc       Sun RPC
syslog       System Logging Utility
telnet       Telnet
tftp         Trivial File Transfer Protocol
vdolive     VDOLive streaming video
vofr         voice over Frame Relay packets
xwindows     X-Windows remote access

(config-cmap)# match protocol http
(config-cmap)# match protocol ftp
(config-cmap)# match protocol telnet
(config-cmap)# match access-list 100
(config-cmap)# exit
(config)# class-map VOICE
(config-cmap)# exit
(config)# class-map EXECTEST
(config-cmap)# exit
(config)# policy-map NEW
(config-pmap)# ?
QoS policy-map configuration commands:
class          policy criteria
description    Policy-Map description
exit           Exit from QoS policy-map configuration mode
no             Negate or set default values of a command
rename         Rename this policy-map
<cr>

```

```

(config-pmap)# description test
(config-pmap)# class Delaware
(config-pmap-c)# ?
QoS policy-map class configuration commands:
 bandwidth      Bandwidth
 exit           Exit from QoS class action configuration mode
 fair-queue     Enable Flow-based Fair Queuing in this Class
 no            Negate or set default values of a command
 police        Police
 priority      Strict Scheduling Priority for this Class
 queue-limit   Queue Max Threshold for Tail Drop
 random-detect Enable Random Early Detection as drop policy
 service-policy Configure QoS Service Policy
 set          Set QoS values
 shape        Traffic Shaping
 <cr>
(config-pmap-c)# police ?
 <8000-2000000000> Bits per second
 cir            Committed information rate

(config-pmap-c)# police 1000 ?
 <1000-512000000> Burst bytes
 bc            Conform burst
 conform-action action when rate is less than conform burst
 pir          Peak Information Rate
 <cr>
(config-pmap-c)# police 1000 500
(config-pmap-c-police)# ?
QoS Class Police configuration commands:
 conform-action action when rate is less than conform burst
 exceed-action  action when rate is within conform and conform + exceed burst
 exit          Exit from Police configuration mode
 no           Negate or set default values of a command
 violate-action action when rate is greater than conform + exceed burst
(config-pmap-c-police)# exit
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

# Cisco Router Challenge 69

## Outline

This challenge involves the configuration of CBWFQ.

## Objectives

The objectives of this challenge are to:

- Define CBWFQ.

## Example

```
> en
```

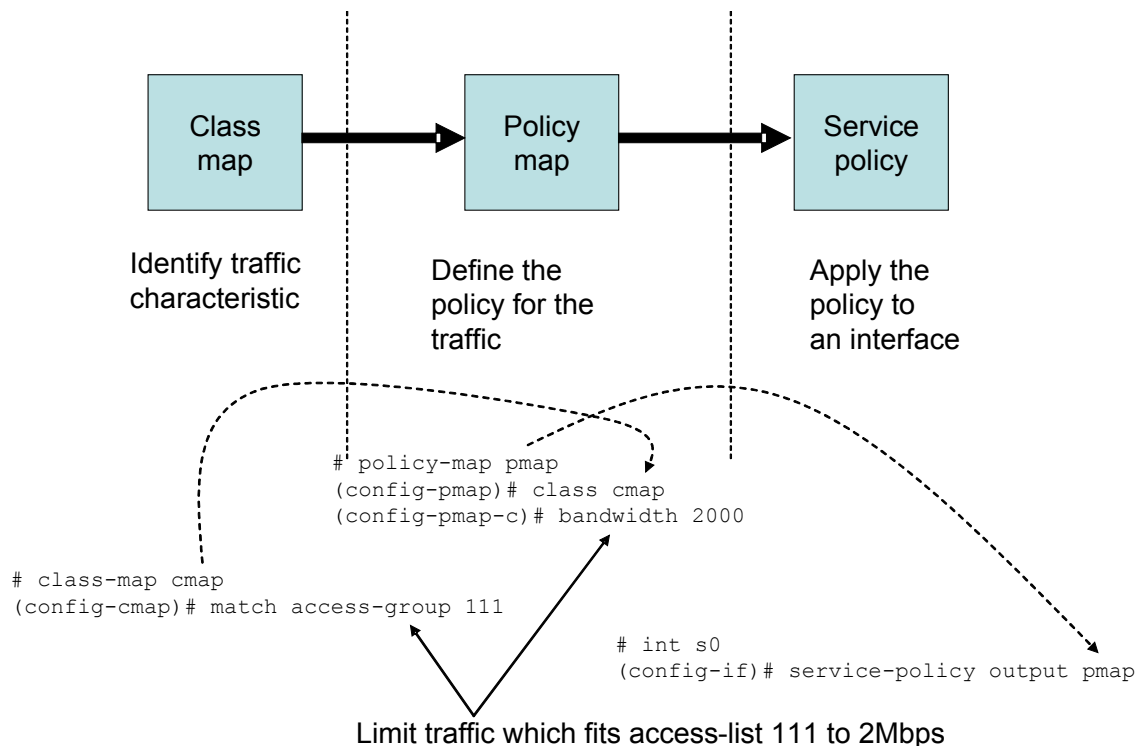
```

# config t
(config)# access-list 108 permit ip 162.78.102.0 0.0.255.255 247.226.90.0
0.0.255.255
(config)# class-map tayside
(config-cmap)# match access-group 108
(config-cmap)# exit
(config)# policy-map ankle
(config-pmap)# class tayside
(config-pmap-c)# bandwidth 128
(config-pmap-c)# queue-limit 21
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int s0
(config-if)# service-policy output ankle

```

### Explanation

The following shows an example of limiting all the traffic which fits access-list 111 to 2Mbps:



### Ref:

<http://www.netcraftsmen.net/welcher/papers/newqos121.html>

# Cisco Router Challenge 134

### Outline

This challenge involves the configuration of auto QoS on an interface.

## Objectives

The objectives of this challenge are to:

- Define CEF (Cisco Express Forwarding), as this is required for Auto QoS.
- Enable NBAR (Network Based Application Recognition), as this is required for Auto QoS.
- Define the bandwidth on an interface.
- Enable Auto QoS.

## Example

```
> en
# config t
(config)# ip cef
(config)# int s0
(config-if)# bandwidth ?
    <1-10000000> Bandwidth in kilobits
    inherit      Specify how bandwidth is inherited
(config-if)# bandwidth 256
(config-if)# ip nbar ?
    protocol-discovery Enable NBAR protocol discovery

(config-if)# ip nbar protocol ?
    <cr>
(config-if)# ip nbar protocol
(config-if)# auto ?
    qos Configure AutoQoS

(config-if)# auto qos ?
    voip Configure AutoQoS for VoIP

(config-if)# auto qos voip ?
    trust Trust the DSCP marking
    <cr>
(config-if)# auto qos voip
(config-if)# exit
(config)# exit
# sh ip nbar pr
Serial0/0

          Protocol                Input                Output
          Protocol                Packet Count         Packet Count
          Protocol                Byte Count           Byte Count
          Protocol                5 minute bit rate (bps)  5 minute bit rate
          (bps)
          -----
          bgp                      0                    0
          bgp                      0                    0
```

	0	0
citrix	0	0
	0	0
	0	0
cuseeme	0	0
	0	0
	0	0
custom-01	0	0
	0	0
	0	0
custom-02	0	0
	0	0
	0	0
custom-03	0	0
custom-04	0	0
	0	0
	0	0
custom-05	0	0
	0	0
	0	0
custom-06	0	0
	0	0
	0	0
custom-07	0	0
	0	0
	0	0
custom-08	0	0
	0	0
	0	0
custom-09	0	0
	0	0
	0	0
custom-10	0	0
	0	0
	0	0
dhcp	0	0
	0	0
	0	0
dns	0	0
	0	0
	0	0
egp	0	0
	0	0
	0	0
eigrp	0	0
	0	0
	0	0
exchange	0	0
	0	0
	0	0
fasttrack	0	0
	0	0
	0	0
finger	0	0
	0	0
	0	0

ftp	0	0
	0	0
	0	0
gnutella	0	0
	0	0
	0	0
gopher	0	0
	0	0
	0	0
gre	0	0
	0	0
	0	0
http	0	0
	0	0
	0	0
icmp	0	0
	0	0
	0	0
imap	0	0
	0	0
	0	0
ipinip	0	0
	0	0
	0	0
ipsec	0	0
	0	0
	0	0
irc	0	0
	0	0
	0	0
kazaa2	0	0
	0	0
	0	0
kerberos	0	0
	0	0
	0	0
l2tp	0	0
	0	0
	0	0
ldap	0	0
	0	0
	0	0
napster	0	0
	0	0
	0	0
netbios	0	0
	0	0
	0	0
netshow	0	0
	0	0
	0	0
nfs	0	0
	0	0
	0	0
nntp	0	0
	0	0
	0	0

notes	0	0
	0	0
	0	0
novadigm	0	0
	0	0
	0	0
ntp	0	0
	0	0
	0	0
pcanywhere	0	0
	0	0
	0	0
pop3	0	0
	0	0
	0	0
pptp	0	0
	0	0
	0	0
printer	0	0
	0	0
	0	0
rcmd	0	0
	0	0
	0	0
rip	0	0
	0	0
	0	0
rsvp	0	0
	0	0
	0	0
rtp	0	0
	0	0
	0	0
rtspplayer	0	0
	0	0
	0	0
secure-ftp	0	0
	0	0
	0	0
secure-http	0	0
	0	0
	0	0
secure-imap	0	0
	0	0
	0	0
secure-irc	0	0
	0	0
	0	0
secure-ldap	0	0
	0	0
	0	0
secure-nntp	0	0
	0	0
	0	0
secure-pop3	0	0
	0	0
	0	0

secure-telnet	0	0
	0	0
	0	0
smtp	0	0
	0	0
	0	0
snmp	0	0
	0	0
	0	0
socks	0	0
	0	0
	0	0
sqlnet	0	0
	0	0
	0	0
sqlserver	0	0
	0	0
	0	0
ssh	0	0
	0	0
	0	0
streamwork	0	0
	0	0
	0	0
sunrpc	0	0
	0	0
	0	0
syslog	0	0
	0	0
	0	0
telnet	0	0
	0	0
	0	0
tftp	0	0
	0	0
	0	0
vdolive	0	0
	0	0
	0	0
xwindows	0	0
	0	0
	0	0
unknown	0	0
	0	0
	0	0
Total	0	0
	0	0
	0	0

### **Explanation**

#### **Key facts:**

CCNP Objective: QoS Implementation Methods.

- **AutoQoS for the Enterprise** is the next generation of QoS generation, and uses NBAR for traffic discovery and classification. The basic Auto QoS is **Auto QoS VoIP**.
- For Auto QoS to work, **CEF** and **NBAR** must be enabled. Also the **bandwidth** must be correctly defined on the interface.
- AutoQoS automatically generate QoS commands.
- AutoQoS analyzes network traffic and tries to optimize the QoS through traffic classes that the AutoQoS Discovery method to create policies, which are applied to the interface(s).
- AutoQoS simplifies the configuration.
- AutoQoS uses **Classification** (This uses AutoQoS Discovery with NBAR to discover the requirements); **Policy generation** (This uses access-lists, class-maps and policy maps to optimize the setup); **Configuration** (This configures the required interfaces); **Monitoring and reporting** (This continually updates and reports on the operation); and **Consistency** (This allows for consistency across a range of devices).

## Cisco Router Challenge 135

### Outline

This challenge involves the configuration of QoS on VoIP traffic (H.323).

### Objectives

The objectives of this challenge are to:

- Define an ACL for VoIP (H.323).
- Define QoS on VoIP traffic.
- Define bit rate and a burst rate for the VoIP traffic.

### Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# police ?
<8000-2000000000> Bits per second
cir                Committed information rate

(config-pmap-c)# police 100 ?
<1000-512000000> Burst bytes
bc                Conform burst
```

```

conform-action    action when rate is less than conform burst
pir              Peak Information Rate
<cr>
(config-pmap-c)# police 100 500
(config-pmap-c-police)# exit
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

In this case VoIP is detected on TCP port 1720 and on UDP ports from 16384 to 32767:

```

(config)# access-list 100 udp any any range 16384 32000
(config)# access-list 100 tcp any any eq 1720

```

The main classification for VoIP are:

- **H.323**. TCP port 1720 is used for H.323 Host Call, and UDP ports from 16384 to 32767 for RTP (Realtime Transport Protocol). This is used in MS Messenger, and so on.
- **H.323 (Callserve)**. UDP port 1719 and TCP port 1720 are used for call signalling, and UDP ports from 5000 to 65535 for RTP (Realtime Transport Protocol). This is used in Callserve, and so on.
- **SIP**. TCP/UDP port 560 is used for signaling, and UDP ports from 16384 to 32767 for RTP (Realtime Transport Protocol). This is used in SIP, and so on.

## Cisco Router Challenge 136

### Outline

This challenge involves the configuration of QoS on VoIP traffic (SIP).

### Objectives

The objectives of this challenge are to:

- Define an ACL for VoIP (SIP).
- Define QoS on VoIP traffic.
- Define bit rate and a burst rate for the VoIP traffic.

### Example

```

> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 560
(config)# access-list 100 udp any any eq 560

(config)# class-map VOIP
(config-cmap)# match access-group 100

```

```

(config-cmap)# exit
(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# police ?
<8000-2000000000> Bits per second
cir Committed information rate

(config-pmap-c)# police 100 ?
<1000-5120000000> Burst bytes
bc Conform burst
conform-action action when rate is less than conform burst
pir Peak Information Rate
<cr>
(config-pmap-c)# police 100 500
(config-pmap-c-police)# exit
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

In this case VoIP is detected on TCP/UDP port 560 for the call setup and on UDP ports from 16384 to 32767 for the actual call traffic:

```

(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 560
(config)# access-list 100 udp any any eq 560

```

The main classification for VoIP are:

- **H.323.** TCP port 1720 is used for H.323 Host Call, and UDP ports from 16384 to 32767 for RTP (Realtime Transport Protocol). This is used in MS Messenger, and so on.
- **H.323 (Callserve).** UDP port 1719 and TCP port 1720 are used for call signalling, and UDP ports from 5000 to 65535 for RTP (Realtime Transport Protocol). This is used in Callserve, and so on.
- **SIP.** TCP/UDP port 560 is used for signaling, and UDP ports from 16384 to 32767 for RTP (Realtime Transport Protocol). This is used in SIP, and so on.

## Cisco Router Challenge 137

### Outline

This challenge involves the configuration of QoS on VoIP traffic (H.323).

### Objectives

The objectives of this challenge are to:

- Define an ACL for VoIP (H.323).
- Define QoS on VoIP traffic.
- Define bit rate and a burst rate for the VoIP traffic.

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# bandwidth ?
<8-2000000> Kilo Bits per second
percent      % of total Bandwidth
remaining    % of the remaining bandwidth
(config-pmap-c)# bandwidth 50
(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW
```

# Cisco Router Challenge 138

## Outline

This challenge involves the configuration of QoS on VoIP traffic (H.323).

## Objectives

The objectives of this challenge are to:

- Define an ACL for VoIP (H.323).
- Define QoS on VoIP traffic.
- Define bit rate and a burst rate for the VoIP traffic.

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# bandwidth ?
<8-2000000> Kilo Bits per second
percent      % of total Bandwidth
```

```

    remaining    % of the remaining bandwidth

(config-pmap-c)# bandwidth percent ?
    <1-100> Percentage <cr>
(config-pmap-c)# bandwidth percent 50
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

# Cisco Router Challenge 139

## Outline

This challenge involves the configuration of QoS on VoIP traffic (H.323).

## Objectives

The objectives of this challenge are to:

- Define an ACL for VoIP (H.323).
- Define QoS on VoIP traffic.
- Define bit rate and a burst rate for the VoIP traffic.

## Example

```

> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# priority ?
    <8-2000000> Kilo Bits per second
    percent    % of total bandwidth
(config-pmap-c)# priority 100
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

The main differences between the bandwidth and priority commands are:

### **bandwidth Command**

Maximum bandwidth guarantee	Yes
Minimum bandwidth guarantee	No

Built-in policer	No
Provides low latency	No

### **priority Command**

Maximum bandwidth guarantee	Yes
Minimum bandwidth guarantee	Yes
Built-in policer	Yes
Provides low latency	Yes

# Cisco Router Challenge 140

## Outline

This challenge involves the configuration of QoS on VoIP traffic (H.323).

## Objectives

The objectives of this challenge are to:

- Define an ACL for VoIP (H.323).
- Define QoS on VoIP traffic.
- Define bit rate and a burst rate for the VoIP traffic.

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# priority ?
<8-2000000> Kilo Bits per second
percent      % of total bandwidth
(config-pmap-c)# priority percent 50
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW
```

The main differences between the bandwidth and priority commands are:

## **bandwidth Command**

Maximum bandwidth guarantee	Yes
Minimum bandwidth guarantee	No
Built-in policer	No
Provides low latency	No

### **priority Command**

Maximum bandwidth guarantee	Yes
Minimum bandwidth guarantee	Yes
Built-in policer	Yes
Provides low latency	Yes

# Cisco Router Challenge 141

## Outline

This challenge involves the configuration of QoS for different class-maps.

## Objectives

The objectives of this challenge are to:

- Define access-lists for class-maps.

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# access-list 101 tcp any any eq 80

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# class-map DATA
(config-cmap)# match access-group 101
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# priority percent 60
(config-pmap-c)# exit
(config-pmap)# class DATA
(config-pmap-c)# priority percent 40
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int e0
```

```
(config-if)# service-policy output NEW
```

In this case 60% of the bandwidth will be allocated to VoIP traffic, and 40% to HTTP traffic. To recap the difference between the bandwidth and priority commands are:

#### **bandwidth Command**

Maximum bandwidth guarantee	Yes
Minimum bandwidth guarantee	No
Built-in policer	No
Provides low latency	No

#### **priority Command**

Maximum bandwidth guarantee	Yes
Minimum bandwidth guarantee	Yes
Built-in policer	Yes
Provides low latency	Yes

## **Cisco Router Challenge 142**

### Outline

This challenge involves the configuration of NBAR, which can be used to define interesting protocols.

### Objectives

The objectives of this challenge are to:

- Define NBAR parameters.

### Example

```
> en
# config t
(config)# ip nbar pdlm tftp://1.2.3.4/test.pdlm
(config)# ip nbar port-map http tcp 80 8080
(config)# ip nbar port-map ftp tcp 21
(config)# int s0
(config-if)# ip nbar protocol-discovery
```

```
Router# sh ip nbar port
port-map bgp          udp 179
port-map bgp          tcp 179
port-map citrix       udp 1604
port-map citrix       tcp 1494
port-map cuseeme      udp 7648 7649 24032
```

```

port-map cuseeme          tcp 7648 7649
port-map custom-01       udp 0
port-map custom-01       tcp 0
port-map custom-02       udp 0
port-map custom-02       tcp 0
port-map custom-03       udp 0
port-map custom-03       tcp 0
port-map custom-04       udp 0
port-map custom-04       tcp 0
port-map custom-05       udp 0
port-map custom-05       tcp 0
port-map custom-06       udp 0
port-map custom-06       tcp 0
port-map custom-07       udp 0
port-map custom-07       tcp 0
port-map custom-08       udp 0
port-map custom-08       tcp 0
port-map custom-09       udp 0
port-map custom-09       tcp 0
port-map custom-10       udp 0
port-map custom-10       tcp 0
port-map dhcp            udp 67 68
port-map dns             udp 53
port-map dns             tcp 53
port-map exchange       tcp 135
port-map fasttrack      tcp 1214
port-map finger         tcp 79
port-map ftp            tcp 21
port-map gnutella       tcp 6346 6347 6348 6349 6355 5634
port-map gopher         udp 70
port-map gopher         tcp 70
port-map http           tcp 80
port-map imap           udp 143 220
port-map imap           tcp 143 220
port-map irc            udp 194
port-map irc            tcp 194
port-map kerberos       udp 88 749
port-map kerberos       tcp 88 749
port-map l2tp           udp 1701
port-map ldap           udp 389
port-map ldap           tcp 389
port-map napster        tcp 6699 8875 8888 7777 6700 6666 6677 6688
4444 5555
port-map netbios        udp 137 138
port-map netbios        tcp 137 139
port-map netshow       tcp 1755
port-map nfs            udp 2049
port-map nfs            tcp 2049
port-map nntp           udp 119
port-map nntp           tcp 119
port-map notes          udp 1352
port-map notes          tcp 1352
port-map novadigm       udp 3460 3461 3462 3463 3464 3465
port-map novadigm       tcp 3460 3461 3462 3463 3464 3465
port-map ntp            udp 123
port-map ntp            tcp 123
port-map pcan anywhere  udp 22 5632

```

port-map pcan anywhere	tcp 65301 5631
port-map pop3	udp 110
port-map pop3	tcp 110
port-map pptp	tcp 1723
port-map printer	udp 515
port-map printer	tcp 515
port-map rcmd	tcp 512 513 514
port-map rip	udp 520
port-map rsvp	udp 1698 1699
port-map rtspplayer	tcp 554 7070
port-map secure-ftp	tcp 990
port-map secure-http	tcp 443
port-map secure-imap	udp 585 993
port-map secure-imap	tcp 585 993
port-map secure-irc	udp 994
port-map secure-irc	tcp 994
port-map secure-ldap	udp 636
port-map secure-ldap	tcp 636
port-map secure-nntp	udp 563
port-map secure-nntp	tcp 563
port-map secure-pop3	udp 995
port-map secure-pop3	tcp 995
port-map secure-telnet	tcp 992
port-map smtp	tcp 25
port-map snmp	udp 161 162
port-map snmp	tcp 161 162
port-map socks	tcp 1080
port-map sqlnet	tcp 1521
port-map sqlserver	tcp 1433
port-map ssh	tcp 22
port-map streamwork	udp 1558
port-map sunrpc	udp 111
port-map sunrpc	tcp 111
port-map syslog	udp 514
port-map telnet	tcp 23
port-map tftp	udp 69
port-map vdolive	tcp 7000
port-map xwindows	tcp 6000 6001 6002 6003

## Cisco Router Challenge 143

### Outline

This challenge involves the configuration of NBAR, and limit bandwidth for various protocols.

### Objectives

The objectives of this challenge are to:

- Define NBAR parameters.
- Define a traffic queue.

## Example

```
> en
# config t
(config)# ip nbar pdlm tftp://1.2.3.4/test.pdlm
(config)# ip nbar port-map http tcp 80 8080
(config)# ip nbar port-map ftp tcp 21
(config)# class-map cTest
(config-cmap)# match protocol http
(config-cmap)# match protocol ftp
(config-cmap)# match protocol telnet
(config-cmap)# exit
(config)# policy-map pTest
(config-pmap)# class cTest
(config-pmap-c)# bandwidth 512
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int s0
(config-if)# ip nbar protocol-discovery
```

This example a traffic queue of 512kbps is assigned for HTTP, FTP and TELNET traffic.

# Cisco Router Challenge 144

## Outline

This challenge involves matching for URL details.

## Objectives

The objectives of this challenge are to:

- Define match for URL

## Example

```
> en
# config t
(config)# class-map cTest
(config-cmap)# m pro http ?
  host  Server Host Name
  mime  Match MIME Type
  url   Match URL String
  <cr>
(config-cmap)# m pro http url ?
  WORD  Enter a string as the sub-protocol parameter
(config-cmap)# match protocol http url edinburgh*
(config-cmap)# exit
(config)# policy-map pTest
(config-pmap)# class cTest
(config-pmap-c)# bandwidth 512
```

```
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int s0
(config-if)# service-policy output pTest
```

This matches any URL with edinburgh, such as http://edinburghnights.com, http://tourist.com/edinburgh, and so on. The matching characters are:

*	Match zero or more characters
?	Match one character
	Or
( )	Match one choice in the parenthesis such as (gif   jpeg)
[]	Match in a range, such as jpeg[0-9]

## Cisco Router Challenge 145

### Outline

This challenge involves matching for HTTP host details.

### Objectives

The objectives of this challenge are to:

- Define match for URL host.

### Example

```
> en
# config t
(config)# class-map cTest
(config-cmap)# m pro http host ?
WORD Enter a string as the sub-protocol parameter
(config-cmap)# match protocol http host cisco*
(config-cmap)# exit
(config)# policy-map pTest
(config-pmap)# class cTest
(config-pmap-c)# bandwidth 512
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int s0
(config-if)# service-policy output pTest
```

This matches any host with cisco, such as cisco.com, and so on. The matching characters are:

*	Match zero or more characters
?	Match one character

	Or
( )	Match one choice in the parenthesis such as (gif   jpeg)
[]	Match in a range, such as jpeg[0-9]

## Cisco Router Challenge 146

### Outline

This challenge involves dropping packets which match a URL MIME details.

### Objectives

The objectives of this challenge are to:

- Define match for URL MIME types.

### Example

```
> en
# config t
(config)# class-map cTest
(config-cmap)# m pro http mime ?
WORD Enter a string as the sub-protocol parameter
(config-cmap)# match protocol http mime "*jpeg"
(config-cmap)# exit
(config)# policy-map pTest
(config-pmap)# class cTest
(config-pmap-c)# bandwidth 512
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int s0
(config-if)# service-policy output pTest
```

This matches any MIME type of jpeg. Other typical MIME types are gif, mp3, avi, and so on. The matching characters are:

*	Match zero or more characters
?	Match one character
	Or
( )	Match one choice in the parenthesis such as (gif   jpeg)
[]	Match in a range, such as jpeg[0-9]

## Cisco Router Challenge 147

### Outline

This challenge involves dropping packets which match URL details.

## Objectives

The objectives of this challenge are to:

- Define match for URL.

## Example

```
> en
# config t
(config)# class-map cTest
(config-cmap)# m pro http ?
  host    Server Host Name
  mime    Match MIME Type
  url     Match URL String
  <cr>
(config-cmap)# m pro http url ?
  WORD   Enter a string as the sub-protocol parameter
(config-cmap)# match protocol http url edinburgh*
(config-cmap)# exit
(config)# policy-map pTest
(config-pmap)# class cTest
(config-pmap-c)# ?
QoS policy-map class configuration commands:
bandwidth      Bandwidth
compression    Activate Compression
drop          Drop all packets
exit           Exit from QoS class action configuration mode
no            Negate or set default values of a command
police        Police
priority      Strict Scheduling Priority for this Class
queue-limit    Queue Max Threshold for Tail Drop
random-detect  Enable Random Early Detection as drop policy
service-policy Configure QoS Service Policy
set           Set QoS values
shape         Traffic Shaping
(config-pmap-c)# drop
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int s0
(config-if)# service-policy output pTest
```

# Cisco Router Challenge 148

## Outline

This challenge involves dropping packets which match HTTP host details.

## Objectives

The objectives of this challenge are to:

- Define match for URL host.

## Example

```
> en
# config t
(config)# class-map cTest
(config-cmap)# m pro http host ?
WORD Enter a string as the sub-protocol parameter
(config-cmap)# match protocol http host cisco*
(config-cmap)# exit
(config)# policy-map pTest
(config-pmap)# class cTest
(config-pmap-c)# drop
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int s0
(config-if)# service-policy output pTest
```

This matches any host with cisco, such as cisco.com, and so on. The matching characters are:

*	Match zero or more characters
?	Match one character
	Or
( )	Match one choice in the parenthesis such as (gif   jpeg)
[]	Match in a range, such as jpeg[0-9]

# Cisco Router Challenge 149

## Outline

This challenge involves dropping packets which match URL MIME details.

## Objectives

The objectives of this challenge are to:

- Define match for URL MIME types.

## Example

```

> en
# config t
(config)# class-map cTest
(config-cmap)# m pro http mime ?
WORD Enter a string as the sub-protocol parameter
(config-cmap)# match protocol http mime "*jpeg"
(config-cmap)# exit
(config)# policy-map pTest
(config-pmap)# class cTest
(config-pmap-c)# drop
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int s0
(config-if)# service-policy output pTest

```

# Cisco Router Challenge 150

## Outline

This challenge involves dropping packets which use the Fasttrack protocol (such as for KaZaA, Morpheus and Grokster)

## Objectives

The objectives of this challenge are to:

- Define match for Fasttrack file-transfer.
- Define the Drop action.

## Example

```

> en
# config t
(config)# class-map cTest
Router(config-cmap)# match protocol ?
arp                IP ARP
bgp                Border Gateway Protocol
bridge            Bridging
bstun             Block Serial Tunnel
cdp              Cisco Discovery Protocol
citrix           Citrix Traffic
compressedtcp    Compressed TCP
cuseeme          CU-SeeMe desktop video conference
custom-01        Custom protocol custom-01
custom-02        Custom protocol custom-02
custom-03        Custom protocol custom-03
custom-04        Custom protocol custom-04
custom-05        Custom protocol custom-05
custom-06        Custom protocol custom-06
custom-07        Custom protocol custom-07
custom-08        Custom protocol custom-08
custom-09        Custom protocol custom-09
custom-10        Custom protocol custom-10

```

dhcp	Dynamic Host Configuration
dlsw	Data Link Switching (Direct encapsulation only)
dns	Domain Name Server lookup
egp	Exterior Gateway Protocol
eigrp	Enhanced Interior Gateway Routing Protocol
exchange	MS-RPC for Exchange
fasttrack	FastTrack Traffic - KaZaA, Morpheus, Grokster...
finger	Finger
ftp	File Transfer Protocol
gnutella	Gnutella Traffic - BearShare, LimeWire, Gnutella...
gopher	Gopher
gre	Generic Routing Encapsulation
http	World Wide Web traffic
icmp	Internet Control Message
imap	Internet Message Access Protocol
ip	IP
ipinip	IP in IP (encapsulation)
ipsec	IP Security Protocol (ESP/AH)
ipv6	IPV6
irc	Internet Relay Chat
kazaa2	Kazaa Version 2
kerberos	Kerberos
l2tp	L2F/L2TP tunnel
ldap	Lightweight Directory Access Protocol
llc2	llc2
napster	Napster Traffic
netbios	NetBIOS
netshow	Microsoft Netshow
nfs	Network File System
nntp	Network News Transfer Protocol
notes	Lotus Notes(R)
novadigm	Novadigm EDM
ntp	Network Time Protocol
pad	PAD links
pcanywhere	Symantec pcANYWHERE
pop3	Post Office Protocol
pppoe	PPP over Ethernet
pptp	Point-to-Point Tunneling Protocol
printer	print spooler/lpd
qllc	qllc protocol
rcmd	BSD r-commands (rsh, rlogin, rexec)
rip	Routing Information Protocol
rsrb	Remote Source-Route Bridging
rsvp	Resource Reservation Protocol
rtp	Real Time Protocol
rtspplayer	RTSP players streaming protocol
secure-ftp	FTP over TLS/SSL
secure-http	Secured HTTP
secure-imap	Internet Message Access Protocol over TLS/SSL
secure-irc	Internet Relay Chat over TLS/SSL
secure-ldap	Lightweight Directory Access Protocol over TLS/SSL
secure-nntp	Network News Transfer Protocol over TLS/SSL
secure-pop3	Post Office Protocol over TLS/SSL
secure-telnet	Telnet over TLS/SSL
smtp	Simple Mail Transfer Protocol
snapshot	Snapshot routing support
snmp	Simple Network Management Protocol
socks	SOCKS
sqlnet	SQL*NET for Oracle
sqlserver	MS SQL Server
ssh	Secured Shell
streamwork	Xing Technology StreamWorks player
stun	Serial Tunnel

```

sunrpc      Sun RPC
syslog      System Logging Utility
telnet      Telnet
tftp        Trivial File Transfer Protocol
vdlive      VDOLive streaming video
vofr        voice over Frame Relay packets
xwindows    X-Windows remote access
(config-cmap)# match protocol fast ?
file-transfer File transfer stream
<cr>

(config-cmap)# match protocol fast file-transfer ?
WORD Enter a string as the sub-protocol parameter
(config-cmap)# match protocol fasttrack file-transfer "*"
(config-cmap)# exit
(config)# policy-map pTest
(config-pmap)# class cTest
(config-pmap-c)# drop
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int s0
(config-if)# service-policy output pTest

```

## Notes

Fasttrack matches traffic such as KaZaA, Morpheus, Grokster. It is also possible to apply other known peer-to-peer protocols such as:

```

(config-cmap)# match protocol napster
(config-cmap)# match protocol kazaa2
(config-cmap)# match protocol gnutella

```

# Cisco Router Challenge 151

## Outline

This challenge involves the configuration of QoS for RTP audio and video.

## Objectives

The objectives of this challenge are to:

- Define QoS for RRP audio and video.

## Example

```

> en
# config t

(config)# class-map AUDIO

```

```

(config-cmap)# match protocol rtp ?
  audio           Match voice packets
  payload-type    Match an explicit PT
  video           Match video packets
<cr>
(config-cmap)# match protocol rtp audio ?
<cr>
(config-cmap)# match protocol rtp payload- ?
  WORD            Enter a string as the sub-protocol parameter
(config-cmap)# match protocol rtp video ?
<cr>
(config-cmap)# match protocol rtp audio
(config-cmap)# exit
(config)# class-map VIDEO
(config-cmap)# match protocol rtp video
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class AUDIO
(config-pmap-c)# priority percent 60
(config-pmap-c)# exit
(config-pmap)# class VIDEO
(config-pmap-c)# priority percent 40
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

# Cisco ONT Test Unit 1

## Unit 1: Cisco VoIP Implementations

### Key facts

## Unit 1: Cisco VoIP Implementations

VoIP has the following benefits:

- Improved productivity.
- Access to new types of communication devices.
- Lower transmission costs.
- Consolidated costs.
- More efficient use of bandwidth/equipment.

The components of VoIP include:

- IP phone.
- Gateways.
- Multipoint control units.
- Application servers.
- Gatekeepers.

- Call agents.
- Video-end points.

Not available on this version.

## Cisco ONT Test Unit 2

### Key facts

#### Unit 2: IP Quality of Service

Not available on this version.

## Cisco ONT Test Unit 3

### Key facts

#### Unit 3: Classification, Marking and NBAR

Not available on this version.

## Cisco Router Challenge 152

## Outline

This challenge involves the configuration of Weighted Fair Queue (WFQ).

> CCNP ONT Area: Unit 4: Congestion Management and Queuing

## Objectives

The objectives of this challenge are to:

- Define WFQ CDT parameter.
- Define WFQ RDQ parameter.
- Define Hold-queue size.

## Example

```
> en
# config t

(config)# int s0
(config-if)# fair-queue ?
  <1-4096> Congestive Discard Threshold
  <cr>

(config-if)# fair-queue 1 ?
  <16-4096> Number Dynamic Conversation Queues
  <cr>

(config-if)# fair-queue 1 16 ?
  <0-1000> Number Reservable Conversation Queues
  <cr>

(config-if)# fair-queue 1 16 100

(config-if)# hold-time ?
  <0-4096> Queue length

(config-if)# hold-time 100 ?
  in   Input queue
  out  Output queue

(config-if)# hold-time 100 out ?
  <cr>

(config-if)# hold-time 100 out ?
```

Default are:

Congestive discard threshold 64 messages

Dynamic queues 256 queues

Reservable queues 0 queues

# Cisco Router Challenge 153

## Outline

This challenge involves the configuration of Class-based Weighted Fair Queue (CBWFQ).

> CCNP ONT Area: Unit 4: Congestion Management and Queuing

## Objectives

The objectives of this challenge are to:

- Define CBWFQ.

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# access-list 101 tcp any any eq 80

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# class-map DATA
(config-cmap)# match access-group 101
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# bandwidth 128
(config-pmap-c)# queue-limit 60
(config-pmap-c)# exit

(config-pmap)# class DATA
(config-pmap-c)# bandwidth 64
(config-pmap-c)# queue-limit 80
(config-pmap-c)# exit

(config-pmap)# class class-default
(config-pmap-c)# fair-queue 16
(config-pmap-c)# exit

(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW
```

Default are:

Congestive discard threshold 64 messages  
Dynamic queues 256 queues  
Reservable queues 0 queues

# Cisco Router Challenge 154

## Outline

This challenge involves the configuration of Class-based Weighted Fair Queue (CBWFQ).

> CCNP ONT Area: Unit 4: Congestion Management and Queuing

## Objectives

The objectives of this challenge are to:

- Define CBWFQ.

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# access-list 101 tcp any any eq 80

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# class-map DATA
(config-cmap)# match access-group 101
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# bandwidth percent 60
(config-pmap-c)# queue-limit 60
(config-pmap-c)# exit

(config-pmap)# class DATA
(config-pmap-c)# bandwidth percent 40
(config-pmap-c)# queue-limit 80
(config-pmap-c)# exit

(config-pmap)# class class-default
(config-pmap-c)# fair-queue 16
(config-pmap-c)# exit

(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW
```

# Cisco Router Challenge 155

## Outline

This challenge involves the configuration of Class-based Weighted Fair Queue (CBWFQ).

> CCNP ONT Area: Unit 4: Congestion Management and Queuing

## Objectives

The objectives of this challenge are to:

- Define CBWFQ.

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# access-list 101 tcp any any eq 80

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# class-map DATA
(config-cmap)# match access-group 101
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# bandwidth ?
<8-2000000> Kilo Bits per second
percent      % of total Bandwidth
remaining    % of the remaining bandwidth

(config-pmap-c)# bandwidth r ?
percent      % of the remaining bandwidth
(config-pmap-c)# bandwidth remaining percent 60
(config-pmap-c)# queue-limit 60
(config-pmap-c)# exit

(config-pmap)# class DATA
(config-pmap-c)# bandwidth remaining percent 40
(config-pmap-c)# queue-limit 80
(config-pmap-c)# exit

(config-pmap)# class class-default
(config-pmap-c)# fair-queue 16
(config-pmap-c)# exit
```

```
(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW
```

# Cisco Router Challenge 156

## Outline

This challenge involves the configuration of Low-Latency Queue (LLQ).

> CCNP ONT Area: Unit 4: Congestion Management and Queuing

## Objectives

The objectives of this challenge are to:

- Define LLQ

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# access-list 101 tcp any any eq 80

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# class-map DATA
(config-cmap)# match access-group 101
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# priority 50
(config-pmap-c)# exit

(config-pmap)# class DATA
(config-pmap-c)# bandwidth 50
(config-pmap-c)# exit

(config-pmap)# class class-default
(config-pmap-c)# fair-queue 16
(config-pmap-c)# exit

(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW
```

# Cisco Switch Challenge 69

## Outline

This challenge involves the configuration of Weighted RR (WRR).

> CCNP ONT Area: Unit 4: Congestion Management and Queuing

## Objectives

The objectives of this challenge are to:

- Enable QoS globally (mls qos).
- Define Layer 3 operation (no switchport).
- Define WRR.

## Example

```
> en
# config t
(config)# mls qos
(config)# int fa0/1
(config-if)# no switchport
(config-if)# mls ?
    qos    qos command keyword
(config-if)# mls qos ?
    cos          Configure interface COS parameters
    dscp-mutation Apply DSCP-DSCP map to DSCP trusted port
    monitor      Collect QoS statistics
    trust        Configure trust state of interface
(config-if)# mls qos trust ?
    cos          Classify by packet COS
    device       trusted device class
    dscp         Classify by packet DSCP
    ip-precedence Classify by packet IP precedence
    <cr>
(config-if)# mls qos trust cos
(config-if)# priority-queue ?
    out egress priority queue
(config-if)# priority-queue out

(config-if)# wrr-queue ?
    bandwidth    Configure WRR bandwidth
    cos-map      Configure cos-map for a queue id
    min-reserve  Configure min-reserve level

(config-if)# wrr-queue bandwidth ?
    <1-65536>   enter bandwidth weight for qid 1

(config-if)# wrr-queue bandwidth ?
```

```

<1-65536> enter bandwidth weight for qid 1

(config-if)# wrr-queue bandwidth ANY ?
<1-65536> enter bandwidth weight for qid 2

(config-if)# wrr-queue bandwidth ANY ANY ?
<1-65536> enter bandwidth weight for qid 3

(config-if)# wrr-queue bandwidth ANY ANY ANY ?
<1-65536> enter bandwidth weight for qid 4

(config-if)# wrr-queue cos-map ?
<1-4> enter cos-map queue id
(config-if)# wrr-queue cos-map 1 ?
<0-7> 8 cos values separated by spaces
(config-if)# wrr-queue cos-map 1 0 1 2 4
(config-if)# wrr-queue cos-map 3 4 5

```

# Cisco Router Challenge 157

## Outline

This challenge involves the configuration of PQ.

> CCNP ONT Area: Unit 4: Congestion Management and Queuing

## Objectives

The objectives of this challenge are to:

- Define PQ.
- Apply priority-list onto an interface.

## Example

```

> en
# config t
(config)# priority-list ?
<1-16> Priority list number

(config)# priority-list 1 ?
default      Set priority queue for unspecified datagrams
interface    Establish priorities for packets from a named interface
protocol     priority queueing by protocol
queue-limit  Set queue limits for priority queues

(config)# priority-list 1 queue-limit ?
<0-32767> High limit

(config)# priority-list 1 queue-limit 10 ?

```

```
<0-32767> Medium limit
(config)# priority-list 1 queue-limit 10 20 ?
<0-32767> Normal limit
(config)# priority-list 1 queue-limit 10 20 30 ?
<0-32767> Lower limit
(config)# priority-list 1 queue-limit 10 20 30 40
(config)# int e0
(config-if)# priority-group 1
```

## Cisco ONT Test Unit 4

### Key facts

#### Unit 4: Congestion Management and Queuing

Not available on this version.

## Cisco Router Challenge 158

### Outline

This challenge involves the configuration of CBWRED

> CCNP ONT Area: Unit 5: Congestion Avoidance, Policing, Shaping and Link Efficiency Mechanisms

### Objectives

The objectives of this challenge are to:

- Define CBWRED

### Example

```

> en
# config t
(config)# class-map VOIP
(config-cmap)# match ?
  access-group      Access group
  any                Any packets
  class-map         Class map
  cos               IEEE 802.1Q/ISL class of service/user priority values
  destination-address Destination address
  discard-class     Discard behavior identifier
  dscp              Match DSCP in IP(v4) and IPv6 packets
  fr-de             Match on Frame-relay DE bit
  fr-dlci           Match on fr-dlci
  input-interface  Select an input interface to match
  ip                IP specific values
  mpls              Multi Protocol Label Switching specific values
  not               Negate this match result
  packet            Layer 3 Packet length
  precedence        Match Precedence in IP(v4) and IPv6 packets
  protocol          Protocol
  qos-group         Qos-group
  source-address    Source address
(config-cmap)# match ip ?
  dscp              Match IP DSCP (DiffServ CodePoints)
  precedence        Match IP precedence
  rtp               Match RTP port nos
(config-cmap)# match ip p ?
  <0-7>             Enter up to 4 precedence values separated by white-spaces
  critical          Match packets with critical precedence (5)
  flash             Match packets with flash precedence (3)
  flash-override   Match packets with flash override precedence (4)
  immediate         Match packets with immediate precedence (2)
  internet          Match packets with internetwork control precedence (6)
  network           Match packets with network control precedence (7)
  priority          Match packets with priority precedence (1)
  routine           Match packets with routine precedence (0)
(config-cmap)# match ip precedence 3 4
(config-cmap)# exit
(config)# class-map DATA
(config-cmap)# match ip precedence 1 2
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# random-detect ?
  dscp              parameters for each dscp value
  dscp-based        Enable dscp-based WRED as drop policy
  exponential-weighting-constant weight for mean queue depth calculation
  prec-based        Enable precedence-based WRED as drop policy
  precedence        parameters for each precedence value
  <cr>
(config-pmap-c)# random-detect
(config-pmap-c)# random-detect prece ?
  <0-7>             IP precedence
  rsvp              rsvp traffic

(config-pmap-c)# random-detect prece 3 ?
  <1-4096>          minimum threshold (number of packets)

(config-pmap-c)# random-detect prece ANY ANY ?
  <1-4096>          maximum threshold (number of packets)

(config-pmap-c)# random-detect prece 10 20 30 ?

```

```

<1-65535> mark probability denominator
<cr>
(config-pmap-c)# random-detect prece 10 20 30

(config-pmap-c)# exit

(config-pmap)# class DATA
(config-pmap-c)# bandwidth 50
(config-pmap-c)# exit

(config-pmap)# class class-default
(config-pmap-c)# fair-queue
(config-pmap-c)# random-detect
(config-pmap-c)# exit

(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

This is CBWRED (Class-based Weighted Random Early Detection), where:

- **Minimum threshold.** When the queue is less than this value, no packets are dropped.
- **Maximum threshold.** When then the queue is greater than this value, all packets are dropped.
- **Mark Probability Denominator.** When the queue is between the minimum and maximum threshold values, the packets are dropped based on this probability.

Thus:

```
(config-pmap-c)# random-detect prece 10 20 30
```

Will not drop until there is a queue of 10, and will always drop when the queue is over 30. In-between 10 and 20, it will drop 30% of packets.

## Cisco Router Challenge 159

### Outline

This challenge involves the configuration of CBWRED (DSCP-based)

> CCNP ONT Area: Unit 5: Congestion Avoidance, Policing, Shaping and Link Efficiency Mechanisms

### Objectives

The objectives of this challenge are to:

- Define CBWRED using DSCP.

See the next challenge for tagging the traffic with the DSCP value.

### Example

```
> en
# config t
(config)# class-map VOIP
(config-cmap)# match ?
  access-group      Access group
  any                Any packets
  class-map         Class map
  cos               IEEE 802.1Q/ISL class of service/user priority values
  destination-address Destination address
  discard-class     Discard behavior identifier
  dscp              Match DSCP in IP(v4) and IPv6 packets
  fr-de            Match on Frame-relay DE bit
  fr-dlci          Match on fr-dlci
  input-interface  Select an input interface to match
  ip                IP specific values
  mpls             Multi Protocol Label Switching specific values
  not              Negate this match result
  packet           Layer 3 Packet length
  precedence        Match Precedence in IP(v4) and IPv6 packets
  protocol         Protocol
  qos-group        Qos-group
  source-address   Source address
(config-cmap)# match ip ?
  dscp      Match IP DSCP (DiffServ CodePoints)
  precedence Match IP precedence
  rtp       Match RTP port nos
(config-cmap)# match ip dscp ?
  <0-63> Differentiated services codepoint value
  af11   Match packets with AF11 dscp (001010)
  af12   Match packets with AF12 dscp (001100)
  af13   Match packets with AF13 dscp (001110)
  af21   Match packets with AF21 dscp (010010)
  af22   Match packets with AF22 dscp (010100)
  af23   Match packets with AF23 dscp (010110)
  af31   Match packets with AF31 dscp (011010)
  af32   Match packets with AF32 dscp (011100)
  af33   Match packets with AF33 dscp (011110)
  af41   Match packets with AF41 dscp (100010)
  af42   Match packets with AF42 dscp (100100)
  af43   Match packets with AF43 dscp (100110)
  cs1    Match packets with CS1(precedence 1) dscp (001000)
  cs2    Match packets with CS2(precedence 2) dscp (010000)
  cs3    Match packets with CS3(precedence 3) dscp (011000)
  cs4    Match packets with CS4(precedence 4) dscp (100000)
  cs5    Match packets with CS5(precedence 5) dscp (101000)
  cs6    Match packets with CS6(precedence 6) dscp (110000)
  cs7    Match packets with CS7(precedence 7) dscp (111000)
  default Match packets with default dscp (000000)
  ef     Match packets with EF dscp (101110)
(config-cmap)# match ip dscp af21 af22 af23 cs2
(config-cmap)# exit
(config)# class-map DATA
(config-cmap)# match ip ip dscp af11 af12 af13 cs1
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class VOIP
```

```

(config-pmap-c)# random-detect ?
dscp                parameters for each dscp value
dscp-based          Enable dscp-based WRED as drop policy
exponential-weighting-constant  weight for mean queue depth calculation
prec-based          Enable precedence-based WRED as drop policy
precedence          parameters for each precedence value
<cr>
(config-pmap-c)# random-detect
(config-pmap-c)# random-detect dscp ?
<0-63>              Differentiated services codepoint value
af11                Match packets with AF11 dscp (001010)
af12                Match packets with AF12 dscp (001100)
af13                Match packets with AF13 dscp (001110)
af21                Match packets with AF21 dscp (010010)
af22                Match packets with AF22 dscp (010100)
af23                Match packets with AF23 dscp (010110)
af31                Match packets with AF31 dscp (011010)
af32                Match packets with AF32 dscp (011100)
af33                Match packets with AF33 dscp (011110)
af41                Match packets with AF41 dscp (100010)
af42                Match packets with AF42 dscp (100100)
af43                Match packets with AF43 dscp (100110)
cs1                 Match packets with CS1(precedence 1) dscp (001000)
cs2                 Match packets with CS2(precedence 2) dscp (010000)
cs3                 Match packets with CS3(precedence 3) dscp (011000)
cs4                 Match packets with CS4(precedence 4) dscp (100000)
cs5                 Match packets with CS5(precedence 5) dscp (101000)
cs6                 Match packets with CS6(precedence 6) dscp (110000)
cs7                 Match packets with CS7(precedence 7) dscp (111000)
default            Match packets with default dscp (000000)
ef                 Match packets with EF dscp (101110)
rsvp                rsvp traffic
(config-pmap-c)# random-detect dscp af21 10 ?
<1-4096>           minimum threshold (number of packets)

(config-pmap-c)# random-detect dscp af21 10 20 ?
<1-4096>           maximum threshold (number of packets)

(config-pmap-c)# random-detect dscp af21 10 20 30 ?
<1-65535>         mark probability denominator
<cr>
(config-pmap-c)# random-detect dscp af21 10 20 30 ?
(config-pmap-c)# random-detect dscp af22 10 20 30 ?
(config-pmap-c)# random-detect dscp af23 10 20 30 ?
(config-pmap-c)# random-detect dscp cs2 10 20 30 ?

(config-pmap-c)# exit

(config-pmap)# class DATA
(config-pmap-c)# bandwidth 50
(config-pmap-c)# exit

(config-pmap)# class class-default
(config-pmap-c)# fair-queue
(config-pmap-c)# random-detect dscp-based
(config-pmap-c)# exit

(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

This is CBWRED (Class-based Weighted Random Early Detection), where:

- **Minimum threshold.** When the queue is less than this value, no packets are dropped.
- **Maximum threshold.** When then the queue is greater than this value, all packets are dropped.
- **Mark Probability Denominator.** When the queue is between the minimum and maximum threshold values, the packets are dropped based on this probability.

Thus:

```
(config-pmap-c)# random-detect prece 10 20 30
```

Will not drop until there is a queue of 10, and will always drop when the queue is over 30. In-between 10 and 20, it will drop 30% of packets.

## Cisco Router Challenge 160

### Outline

This challenge involves tagging traffic with the DSCP value.

> CCNP ONT Area: Unit 5: Congestion Avoidance, Policing, Shaping and Link Efficiency Mechanisms

### Objectives

The objectives of this challenge are to:

- Identify traffic, and tag.

### Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# access-list 101 tcp any any eq 80

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# class-map DATA
(config-cmap)# match access-group 101
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# set ?
```

```

atm-clp      Set ATM CLP bit to 1
cos          Set IEEE 802.1Q/ISL class of service/user priority
discard-class  Discard behavior identifier
dscp         Set DSCP in IP(v4) and IPv6 packets
fr-de       Set FR DE bit to 1
ip           Set IP specific values
mpls        Set MPLS specific values
precedence  Set precedence in IP(v4) and IPv6 packets
qos-group   Set QoS Group
(config-pmap-c)# set ip ?
dscp        Set IP DSCP (DiffServ CodePoint)
precedence  Set IP precedence
(config-pmap-c)# set ip dscp ?
<0-63>     Differentiated services codepoint value
af11       Match packets with AF11 dscp (001010)
af12       Match packets with AF12 dscp (001100)
af13       Match packets with AF13 dscp (001110)
af21       Match packets with AF21 dscp (010010)
af22       Match packets with AF22 dscp (010100)
af23       Match packets with AF23 dscp (010110)
af31       Match packets with AF31 dscp (011010)
af32       Match packets with AF32 dscp (011100)
af33       Match packets with AF33 dscp (011110)
af41       Match packets with AF41 dscp (100010)
af42       Match packets with AF42 dscp (100100)
af43       Match packets with AF43 dscp (100110)
cs1        Match packets with CS1(precedence 1) dscp (001000)
cs2        Match packets with CS2(precedence 2) dscp (010000)
cs3        Match packets with CS3(precedence 3) dscp (011000)
cs4        Match packets with CS4(precedence 4) dscp (100000)
cs5        Match packets with CS5(precedence 5) dscp (101000)
cs6        Match packets with CS6(precedence 6) dscp (110000)
cs7        Match packets with CS7(precedence 7) dscp (111000)
default    Match packets with default dscp (000000)
ef         Match packets with EF dscp (101110)
(config-pmap-c)# set ip dscp 46
(config-pmap-c)# exit

(config-pmap)# class DATA
(config-pmap-c)# set ip dscp 10
(config-pmap-c)# exit

(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

Note it is also possible to define:

```

(config-pmap-c)# set ip dscp EF
(config-pmap-c)# exit

(config-pmap)# class DATA
(config-pmap-c)# set ip dscp AF1
(config-pmap-c)# exit

```

which is the same as above.

For end-to-end QoS, the tagging is done at the first router which connects to the source of the traffic. In this way, all the devices on the way will read the DSCP tag, and route with the required QoS.

# Cisco Router Challenge 161

## Outline

This challenge involves tagging traffic with the Precedence value.

> CCNP ONT Area: Unit 5: Congestion Avoidance, Policing, Shaping and Link Efficiency Mechanisms

## Objectives

The objectives of this challenge are to:

- Identify traffic, and tag.

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# access-list 101 tcp any any eq 80

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# class-map DATA
(config-cmap)# match access-group 101
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# set ?
  atm-clp      Set ATM CLP bit to 1
  cos          Set IEEE 802.1Q/ISL class of service/user priority
  discard-class Discard behavior identifier
  dscp         Set DSCP in IP(v4) and IPv6 packets
  fr-de       Set FR DE bit to 1
  ip          Set IP specific values
  mpls        Set MPLS specific values
  precedence   Set precedence in IP(v4) and IPv6 packets
  qos-group    Set QoS Group
(config-pmap-c)# set ip ?
  dscp        Set IP DSCP (DiffServ CodePoint)
  precedence  Set IP precedence
(config-pmap-c)# set ip prec ?
<0-7>        IP precedence
```

```

<0-7>          Precedence value
critical        Set packets with critical precedence (5)
flash          Set packets with flash precedence (3)
flash-override Set packets with flash override precedence (4)
immediate      Set packets with immediate precedence (2)
internet       Set packets with internetwork control precedence (6)
network        Set packets with network control precedence (7)
priority       Set packets with priority precedence (1)
routine        Set packets with routine precedence (0)
(config-pmap-c)# set ip prec 5
(config-pmap-c)# exit

(config-pmap)# class DATA
(config-pmap-c)# set ip prec 1
(config-pmap-c)# exit

(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

Note it is also possible to define:

```

(config-pmap-c)# set ip dscp critical
(config-pmap-c)# exit

(config-pmap)# class DATA
(config-pmap-c)# set ip dscp priority
(config-pmap-c)# exit

```

which is the same as above.

For end-to-end QoS, the tagging is done at the first router which connects to the source of the traffic. In this way, all the devices on the way will read the DSCP tag, and route with the required QoS.

## Cisco Router Challenge 162

### Outline

This challenge involves compression the RTP header for a serial interface.

> CCNP ONT Area: Unit 5: Congestion Avoidance, Policing, Shaping and Link Efficiency Mechanisms

### Objectives

The objectives of this challenge are to:

- Define RTP header compression.

### Example

```

> en
# config t
(config)# int e0
(config-if)# ip ?
Interface IP configuration subcommands:
  access-group      Specify access control for packets
  accounting        Enable IP accounting on this interface
  address           Set the IP address of an interface
  audit            Apply IDS audit name
  auth-proxy        Apply authentication proxy
  authentication    authentication subcommands
  bandwidth-percent Set EIGRP bandwidth limit
  broadcast-address Set the broadcast address of an interface
  cef              Cisco Express Forwarding interface commands
  cgmp            Enable/disable CGMP
  dhcp            Configure DHCP parameters for this interface
  directed-broadcast Enable forwarding of directed broadcasts
  dvmrp          DVMRP interface commands
  flow            NetFlow related commands
  header-compression IPHC options
  hello-interval  Configures IP-EIGRP hello interval
  helper-address  Specify a destination address for UDP broadcasts
  hold-time       Configures IP-EIGRP hold time
  idle-group      Specify interesting packets for idle-timer
  igmp           IGMP interface commands
  information-reply Enable sending ICMP Information Reply messages
  inspect         Apply inspect name
  irdp           ICMP Router Discovery Protocol
  load-sharing    Style of load sharing
  local-proxy-arp Enable local-proxy ARP
  mask-reply     Enable sending ICMP Mask Reply messages
  mobile         Mobile IP support
  mrm           Configure IP Multicast Routing Monitor tester
  mroute-cache  Enable switching cache for incoming multicast packets
  mtu           Set IP Maximum Transmission Unit
  multicast      IP multicast interface commands
  nat           NAT interface commands
  nbar          Network-Based Application Recognition
  next-hop-self  Configures IP-EIGRP next-hop-self
  nhrp         NHRP interface subcommands
  ospf         OSPF interface commands
  pgm         PGM Reliable Transport Protocol
  pim         PIM interface commands
  policy       Enable policy routing
  proxy-arp    Enable proxy ARP
  rarp-server  Enable RARP server for static arp entries
  redirects   Enable sending ICMP Redirect messages
  rgmp        Enable/disable RGMP
  rip         Router Information Protocol
  route-cache Enable fast-switching cache for outgoing packets
  router      IP router interface commands
  rsvp       RSVP Interface Commands
  rtp        RTP parameters
  sap        Session Announcement Protocol interface commands
  security   DDN IP Security Option
  split-horizon Perform split horizon
  summary-address Perform address summarization
  tcp        TCP header compression and other parameters
  unnumbered Enable IP processing without an explicit address
  unreachable Enable sending ICMP Unreachable messages
  urd        Configure URL Rendezvousing

```

```

verify          Enable per packet validation
vrf             VPN Routing/Forwarding parameters on the interface
wccp           WCCP interface commands
(config-if)# ip rtp ?
  compression-connections  Maximum number of compressed connections
  header-compression       Enable RTP header compression
  priority                 Assign a priority queue for RTP streams
  reserve                 Assign a reserved queue for RTP streams
(config-if)# ip rtp header-compression
(config-if)# encapsulation ppp
(config-if)# ip rtp compression-connections ?
  <3-1000> Number of connections
(config-if)# ip rtp compression-connections 20

```

# Cisco Router Challenge 163

## Outline

This challenge involves compression the RTP header for a frame relay connection.

> CCNP ONT Area: Unit 5: Congestion Avoidance, Policing, Shaping and Link Efficiency Mechanisms

## Objectives

The objectives of this challenge are to:

- Define RTP header compression for a frame-relay connection.

## Example

```

> en
# config t
(config)# int s0
(config-if)# encapsulate ?
  atm-dxi      ATM-DXI encapsulation
  frame-relay  Frame Relay networks
  hdlc         Serial HDLC synchronous
  lapb        LAPB (X.25 Level 2)
  ppp         Point-to-Point protocol
  smds        Switched Megabit Data Service (SMDS)
  x25         X.25
(config-if)# encapsulate frame-relay

(config-if)# clock ?
  rate  Configure serial interface clock speed

(config-if)# clock rate ?
  Speed (bits per second)
  1200
  2400
  4800
  9600
  14400

```

19200  
28800  
32000  
38400  
56000  
57600  
64000  
72000  
115200  
125000  
128000  
148000  
192000  
250000  
256000  
384000  
500000  
512000  
768000  
800000  
1000000  
1300000  
2000000  
4000000  
8000000

<300-4000000> Choose clockrate from list above

**(config-if)# clock rate 1200**

**(config-if)# frame-relay ?**

accounting	Special accounting instruction
address-reg	ELMI address registration
broadcast-queue	Define a broadcast queue and transmit rate
class	Define a map class on the interface
congestion-management	Enable Frame Relay congestion management
de-group	Associate a DE group with a DLCI
fragment	Enable end-to-end fragmentation for all PVCs
fragmentation	Adaptive fragmentation
ifmib-counter64	Support IF-MIB's total packet/byte counts of Counter64 on FR if/subif when main interface's ifSpeed < 20 Mbps
interface-dlci	Define a DLCI on an interface/subinterface
interface-queue	configure PVC interface queueing
intf-type	Configure a FR DTE/DCE/NNI interface
inverse-arp	Enable/disable FR inverse ARP
ip	Frame Relay Internet Protocol config commands
lmi-n391dte	set full status polling counter
lmi-n392dce	LMI error threshold
lmi-n392dte	LMI error threshold
lmi-n393dce	set LMI monitored event count
lmi-n393dte	set LMI monitored event count
lmi-t392dce	set DCE polling verification timer
lmi-type	Use CISCO-ANSI-CCITT type LMI
local-dlci	Set source DLCI when LMI is not supported
map	Map a protocol address to a DLCI address
multicast-dlci	Set DLCI of a multicast group
policing	Enable Frame Relay policing
priority-dlci-group	Define a priority group of DLCIs
qos-autosense	enable QOS autosense
route	frame relay route for pvc switching
traffic-shaping	Enable Frame Relay Traffic Shaping
traps-maximum	set max traps FR generates at link up or when getting LMI Full Status message

**(config-if)# frame-relay map ?**

```

bridge   Bridging
bstun    Block Serial Tunnel
dlsw     Data Link Switching (Direct encapsulation only)
ip       IP
ipv6     IPV6
llc2     llc2
pppoe    PPP over Ethernet
qllc     qllc protocol
rsrb     Remote Source-Route Bridging
stun     Serial Tunnel

(config-if)# frame-relay map ip ?
A.B.C.D Protocol specific address

(config-if)# frame-relay map ip 1.2.3.4 ?
<16-1007> DLCI

(config-if)# frame-relay map ip 1.2.3.4 111 ?
broadcast      Broadcasts should be forwarded to this address
cisco          Use CISCO Encapsulation
compress       Enable TCP/IP and RTP/IP header compression
ietf           Use RFC1490/RFC2427 Encapsulation
nocompress     Do not compress TCP/IP headers
payload-compression Use payload compression
rtp            RTP header compression parameters
tcp           TCP header compression parameters
<cr>

(config-if)# frame-relay map ip 1.2.3.4 111 broadcast ?
cisco          Use CISCO Encapsulation
compress       Enable TCP/IP and RTP/IP header compression
ietf           Use RFC1490/RFC2427 Encapsulation
nocompress     Do not compress TCP/IP headers
payload-compression Use payload compression
rtp            RTP header compression parameters
tcp           TCP header compression parameters
<cr>

(config-if)# frame-relay map ip 1.2.3.4 111 broadcast rtp ?
header-compression Enable RTP/IP compression

(config-if)# frame-relay map ip 1.2.3.4 111 broadcast rtp header-compression ?
active         Always compress RTP headers
connections    Maximum number of compressed RTP connections
passive        Compress for destinations sending compressed RTP headers
<cr>

(config-if)# frame-relay map ip 1.2.3.4 111 b r header-compression

```

# Cisco Router Challenge 164

## Outline

This challenge involves compression the **TCP** header for an Ethernet interface.

> CCNP ONT Area: Unit 5: Congestion Avoidance, Policing, Shaping and Link Efficiency Mechanisms

## Objectives

The objectives of this challenge are to:

- Define TCP header compression.

## Example

```
> en
# config t
(config)# int e0
(config-if)# ip tcp ?
    adjust-mss                Adjust the mss of transit packets
    compression-connections  Maximum number of compressed connections
    header-compression        Enable TCP header compression
(config-if)# ip tcp header-compression
(config-if)# ip tcp compression-connections ?
    <3-256> Number of connections

(config-if)# ip tcp compression-connections 20
(config-if)# ip tcp header-compression
```

# Cisco Router Challenge 165

## Outline

This challenge involves multilink PPP (MLP) and Link Fragmentation (LFI).

> CCNP ONT Area: Unit 5: Congestion Avoidance, Policing, Shaping and Link Efficiency Mechanisms

## Objectives

The objectives of this challenge are to:

- Define a Dialer group.
- Define MLP and LFI.
- Apply to the BRI interface.

## Example

```
> en
# config t
(config)# int dialer0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# description test link
```

```

(config-if)# encapsulation ppp
(config-if)# ppp ?
  accm          Set initial Async Control Character Map
  accounting    Set PPP network accounting method
  acfc          Options for HDLC Address & Control Field Compression
  authentication Set PPP link authentication method
  authorization Set PPP network authorization method
  bridge        Enable PPP bridge translation
  caller        Caller option when no CLID is available
  chap          Set CHAP authentication parameters
  direction     Override default PPP direction
  dnis          Authentication via DNIS before LCP
  eap           Set EAP authentication parameters
  encrypt       Enable PPP encryption
  ipcp          Set IPCP negotiation options
  iphc          Set IPCP Header Compression control options
  lcp           PPP LCP configuration
  link          Set miscellaneous link parameters
  loopback      PPP loopback options
  max-bad-auth  Allow multiple authentication failures
  max-configure Number of conf-reqs sent before assuming peer is unable to
                respond
  max-failure   Number of conf-naks sent before assuming configuration is not
                converging
  max-terminate Number of term-reqs sent before assuming peer is unable to
                respond
  ms-chap       Set MS-CHAP authentication parameters
  ms-chap-v2    Set MS-CHAP-V2 authentication parameters
  multilink     Make interface multilink capable
  pap           Set PAP authentication parameters
  pfc           Options for Protocol Field Compression
  quality       Set parameters related to Link Quality Monitoring (LQM)
  reliable-link Use LAPB with PPP to provide a reliable link
  timeout       Set PPP timeout parameters
Router(config-if)# ppp authe ?
  chap          Challenge Handshake Authentication Protocol (CHAP)
  eap           Extensible Authentication Protocol (EAP)
  ms-chap       Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
  ms-chap-v2    Microsoft CHAP Version 2 (MS-CHAP-V2)
  pap           Password Authentication Protocol (PAP)
(config-if)# ppp authentication chap
(config-if)# dialer remote-name temp
(config-if)# dialer idle-timeout 100
(config-if)# dialer fast-idle 80
(config-if)# dialer string 2221111
(config-if)# dialer pool 1
(config-if)# dialer-group 1
(config-if)# ppp multilink
(config-if)# ppp multilink ?
  bap           Enable BACP/BAP bandwidth allocation negotiation
  fragment-delay Specify the maximum delay for each fragment
  fragmentation Enable/Disable multilink fragmentation
  idle-link     Do not transmit fragments over the lowest speed link
  interleave    Allow interleaving of small packets with fragments
  <cr> (config-if)# ppp multilink
(config-if)# ppp multilink interleave
(config-if)# ppp mu fragment-delay ?

```

```
<1-1000> Maximum delay in milliseconds
(config-if)# ppp multilink fragment-delay 20
(config-if)# exit
(config)# int bri0
(config-if)# dialer pool-member 1
```

# Cisco Router Challenge 166

## Outline

This challenge involves the policing of VoIP traffic for average bit rate and burst parameters.

## Objectives

The objectives of this challenge are to:

- Define an ACL for VoIP (SIP).
- Define QoS on VoIP traffic.
- Define bit rate and a burst rate for the VoIP traffic.

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 560
(config)# access-list 100 udp any any eq 560

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# police ?
<8000-2000000000> Bits per second
cir Committed information rate

(config-pmap-c)# police 1000 ?
<1000-512000000> Burst bytes
bc Conform burst
conform-action action when rate is less than conform burst
pir Peak Information Rate
<cr>

(config-pmap-c)# police 1000 5000 ?
<1000-512000000> Maximum burst bytes
conform-action action when rate is less than normal burst
<cr>

(config-pmap-c)# police 1000 5000 9000
(config-pmap-c-police)# ?
QoS Class Police configuration commands:
conform-action action when rate is less than conform burst
exceed-action action when rate is within conform and conform + exceed burst
exit Exit from Police configuration mode
```

```

no          Negate or set default values of a command
violate-action action when rate is greater than conform + exceed burst
(config-pmap-c-police)# exit
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

In this example the traffic flow is policed for an average rate of 1000 bits per second, a normal burst size of 5000 bytes, and an excess burst size of 9000.

# Cisco Router Challenge 167

## Outline

This challenge involves the traffic shaping.

## Objectives

The objectives of this challenge are to:

- Define traffic-shaping on an interface.

## Example

```

> en
# config t
(config)# int s0
(config-if)# traffic-shape ?
    adaptive      Enable Traffic Shaping adaptation to BECN
    fecn-adapt    Enable Traffic Shaping reflection of FECN as BECN
    group         configure token bucket: group <access-list> CIR (bps) [Bc (bits)
                  [Be (bits)]]
    rate          configure token bucket: CIR (bps) [Bc (bits) [Be (bits)]]
(config-if)# traffic-shape rate ?
    <8000-100000000> Target Bit Rate (bits per second)

(config-if)# traffic-shape rate 100 ?
    <0-100000000> bits per interval, sustained
    <cr>

(config-if)# traffic-shape rate 100 200 ?
    <0-100000000> bits per interval, excess in first interval
    <cr>

(config-if)# traffic-shape rate 100 200 300 ?
    <0-4096> Set buffer limit
    <cr>
(config-if)# traffic-shape rate 100 200 300
(config-if)# exit

(config)# int s1
(config-if)# traffic-shape ?
    adaptive      Enable Traffic Shaping adaptation to BECN
    fecn-adapt    Enable Traffic Shaping reflection of FECN as BECN

```

```

group          configure token bucket: group <access-list> CIR (bps) [Bc (bits)
               [Be (bits)]]
rate           configure token bucket: CIR (bps) [Bc (bits) [Be (bits)]]
(config-if)# traffic-shape rate ?
<8000-1000000000> Target Bit Rate (bits per second)

(config-if)# traffic-shape rate 100 ?
<0-1000000000> bits per interval, sustained
<cr>

(config-if)# traffic-shape rate 100 200 ?
<0-1000000000> bits per interval, excess in first interval
<cr>

(config-if)# traffic-shape rate 100 200 300 ?
<0-4096> Set buffer limit
<cr>
(config-if)# traffic-shape rate 100 200 300

```

# Cisco Router Challenge 168

## Outline

This challenge involves the traffic shaping by identifying streams with access-lists.

## Objectives

The objectives of this challenge are to:

- Define traffic-shaping on an interface from different flows.

## Example

```

> en
# config t
(config)# access-list 101 permit ip host 1.2.3.4 any any
(config)# access-list 102 permit ip host 1.2.3.5 any any

(config)# int s0

(config)# int s0
(config-if)# traffic-shape ?
adaptive      Enable Traffic Shaping adaptation to BECN
fecn-adapt    Enable Traffic Shaping reflection of FECN as BECN
group         configure token bucket: group <access-list> CIR (bps) [Bc (bits)
               [Be (bits)]]
rate          configure token bucket: CIR (bps) [Bc (bits) [Be (bits)]]

(config-if)# traffic-shape group ?
<1-2699> selecting Access list

(config-if)# traffic-shape group 101 ?
<8000-1000000000> Target Bit Rate (bits per second)

```

```
(config-if)# traffic-shape group 101 1000 ?
<0-1000000000> bits per interval, sustained
<cr>
(config-if)# traffic-shape group 101 1000
(config-if)# traffic-shape group 102 6000
```

This defines that the average rate for traffic from 1.2.3.4 will be 1000 bps, while it will be 6000 bps from 1.2.3.5. No other shaping will occur.

## Cisco Router Challenge 169

### Outline

This challenge involves using traffic shaping with frame relay. It detects the usage of the BECN bits to throttle back the flow.

### Objectives

The objectives of this challenge are to:

- Define traffic-shaping for congestion on a frame-relay interface.

### Example

```
> en
# config t
(config)# int s0
(config-if)# encapsulation frame-relay
(config-if)# traffic-shape ?
    adaptive      Enable Traffic Shaping adaptation to BECN
    fecn-adapt    Enable Traffic Shaping reflection of FECN as BECN
    group         configure token bucket: group <access-list> CIR (bps) [Bc (bits)
                  [Be (bits)]]
    rate         configure token bucket: CIR (bps) [Bc (bits) [Be (bits)]]
(config-if)# traffic-shape rate 1000000
(config-if)# traffic-shape adaptive ?
<1-1000000000> Lower Bound Target Bit Rate (bits per second)
(config-if)# traffic-shape adaptive 60000
(config-if)# traffic-shape fecn-adapt
```

This defines a committed information rate (CIR) of 60,000 bps, and an access rate of 1,000,000 bps.

FECN (Forward Explicit Congestion Notification)

BECN (Backward Explicit Congestion Notification)

### Definitions:

[http://searchnetworking.techtarget.com/sDefinition/0,,sid7\\_gci787381,00.html](http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci787381,00.html)

# Cisco Router Challenge 170

## Outline

This challenge involves class-based shaping, where the shaping profile can be defined in a policy-map.

> CCNP ONT Area: Unit 5: Congestion Avoidance, Policing, Shaping and Link Efficiency Mechanisms

## Objectives

The objectives of this challenge are to:

- Define class-based shaping.

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# access-list 101 tcp any any eq 80

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# class-map DATA
(config-cmap)# match access-group 101
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# shape ?
    adaptive      Enable Traffic Shaping adaptation to BECN
    average        configure token bucket: CIR (bps) [Bc (bits) [Be (bits)]],
                  send out Bc only per interval
    fecn-adapt     Enable Traffic Shaping reflection of FECN as BECN
    fr-voice-adapt Enable rate adjustment depending on voice presence
    max-buffers    Set Maximum Buffer Limit
    peak          configure token bucket: CIR (bps) [Bc (bits) [Be (bits)]],
                  send out Bc+Be per interval

(config-pmap-c)# shape average ?
    <8000-154400000> Target Bit Rate (bits per second), the value needs to be
                  multiple of 8000

(config-pmap-c)# shape average 8000 ?
    <256-154400000> bits per interval, sustained. Needs to be multiple of 128.
```

Recommend not to configure it, the algorithm will find out the best value

```
<cr>
(config-pmap-c)# exit
(config-pmap)# class DATA
(config-pmap-c)# shape average 80000 ?
(config-pmap-c)# exit
(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW
```

# Cisco Router Challenge 171

## Outline

This challenge involves CBWFQ with generic traffic shaping (GTS).

> CCNP ONT Area: Unit 5: Congestion Avoidance, Policing, Shaping and Link Efficiency Mechanisms

## Objectives

The objectives of this challenge are to:

- Define class-based shaping.
- Define bandwidth requirements.

## Example

```
> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# access-list 101 tcp any any eq 80

(config)# class-map VOIP
(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# class-map DATA
(config-cmap)# match access-group 101
(config-cmap)# exit

(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# shape ?
    adaptive      Enable Traffic Shaping adaptation to BECN
    average       configure token bucket: CIR (bps) [Bc (bits) [Be (bits)]],
                  send out Bc only per interval
```

```

fecn-adapt      Enable Traffic Shaping reflection of FECN as BECN
fr-voice-adapt  Enable rate adjustment depending on voice presence
max-buffers     Set Maximum Buffer Limit
peak           configure token bucket: CIR (bps) [Bc (bits) [Be (bits)]],
              send out Bc+Be per interval

(config-pmap-c)# shape average ?
<8000-154400000> Target Bit Rate (bits per second), the value needs to be
                multiple of 8000

(config-pmap-c)# shape average 800000 ?
<256-154400000> bits per interval, sustained. Needs to be multiple of 128.
                Recommend not to configure it, the algorithm will find out
                the best value

<cr>
(config-pmap-c)# bandwidth 512

(config-pmap-c)# exit

(config-pmap)# class DATA
(config-pmap-c)# shape peak ?
<8000-154400000> Target Bit Rate (bits per second), the value needs to be
                multiple of 8000
(config-pmap-c)# shape peak 300000 ?
(config-pmap-c)# bandwidth 256
(config-pmap-c)# exit

(config-pmap)# exit
(config)# int e0
(config-if)# service-policy output NEW

```

In this case the VOICE traffic will be given a bandwidth of 512 kbps, and an output which is shaped to 800,000 bps, whereas DATA will be given a bandwidth of 256 kbps, and a **peak** throughput of 300,000 bps.

## Cisco ONT Test Unit 5

### Key facts

#### Unit 5: Congestion Avoidance, Policing, Shaping, and Link Efficiency

Not available on this version.

## Cisco Router Challenge 172

## Outline

This challenge involves setting up a crypto map and applying it to an interface, with a QoS for a tunnel. It uses the **qos pre-classified** interface command which is a command that is restricted to tunnels, crypto maps, and is not available on normal interfaces.

## Objectives

The objectives of this challenge are to:

- Define a tunnel with a QoS service policy.
- Define a Crypto access-list, to identify the traffic to encrypt.
- Define IKE.
- Define a crypto map.
- Bind the ACL with the crypto map.
- Apply crypto map to E0.

## Example

```
> en
# config t
(config)# int tunnel1
(config-if)# ip 1.2.3.4 255.255.255.0

(config-if)# int tunnel1
(config-if)# crypto ?
  ipsec  Set IPsec parameters
  map    Assign a Crypto Map

(config-if)# crypto m ?
  WORD   Crypto Map tag
  <cr>

(config-if)# crypto m manchester

(config-if)# tunnel ?
  checksum          enable end to end checksumming of packets
  destination        destination of tunnel
  flow              flow options
  key               security or selector key
  mode              tunnel encapsulation method
  path-mtu-discovery Enable Path MTU Discovery on tunnel
  protection         Enable tunnel protection
  sequence-datagrams drop datagrams arriving out of order
  source            source of tunnel packets
  tos               set type of service byte
  ttl               set time to live
  udlr              associate tunnel with unidirectional interface

(config-if)# tunnel source e0
(config-if)# tunnel destination 1.2.3.4
```

```

(config-if)# qos ?
  pre-classify  Enable QOS classification before packets are tunnel
                 encapsulated

(config-if)# qos pre-classify
(config-if)# exit

(config)# hostname newhampshire
(config)# access-list 109 permit ip 50.93.142.0 0.0.255.255
        136.163.130.0 0.0.255.255
(config)# crypto isakmp enable
(config)# crypto isakmp policy 111
(config-isakmp)# ?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
(config-isakmp)# encryption?
  3des  Three key triple DES
  aes   AES - Advanced Encryption Standard.
  des   DES - Data Encryption Standard (56 bit keys).
(config-isakmp)# encryption des
(config-isakmp)# hash ?
  md5  Message Digest 5
  sha  Secure Hash Standard
(config-isakmp)# hash sha
(config-isakmp)# authentication ?
  pre-share  Pre-Shared Key
  rsa-encr   Rivest-Shamir-Adleman Encryption
  rsa-sig    Rivest-Shamir-Adleman Signature
(config-isakmp)# authentication pre-share
(config-isakmp)# group ?
  1  Diffie-Hellman group 1
  2  Diffie-Hellman group 2
  5  Diffie-Hellman group 5
(config-isakmp)# group 1
(config-isakmp)# exit
(config)# crypto isakmp identity hostname
(config)# crypto isakmp key test address 192.168.1.1
(config)# crypto ipsec transform-set finland esp-des
(config)# crypto map manchester 10 ipsec-isakmp
(config-crypto-map)# ?
Crypto Map configuration commands:
  default         Set a command to its defaults
  description     Description of the crypto map statement policy
  dialer          Dialer related commands
  exit            Exit from crypto map configuration mode
  match           Match values.
  no              Negate a command or set its defaults
  qos             Quality of Service related commands
  reverse-route   Reverse Route Injection.

```

```

set                               Set values for encryption/decryption
Router(config-crypto-map)# match ?
address Match address of packets to encrypt.

Router(config-crypto-map)# match address ?
<100-199> IP access-list number
<2000-2699> IP access-list number (expanded range)
WORD Access-list name
Router(config-crypto-map)# match address 109
Router(config-crypto-map)# set ?
identity Identity restriction.
isakmp-profile Specify isakmp Profile
peer Allowed Encryption/Decryption peer.
pfs Specify pfs settings
security-association Security association parameters
transform-set Specify list of transform sets in priority order
Router(config-crypto-map)# set peer 144.55.62.1
Router(config-crypto-map)# set transform-set ?
WORD Proposal tag
Router(config-crypto-map)# set transform-set finland
Router(config-crypto-map)# qos pre-classify
Router(config-crypto-map)# exit
Router(config)# int e0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# crypto map Manchester
Router(config-if)# service-policy out ptest
Router(config-if)# exit
Router(config)# exit

```

# Cisco Router Challenge 173

## Outline

This challenge involves define CoPP (Control plane policing).

## Objectives

The objectives of this challenge are to:

- Define CoPP.
- Apply the CoPP.

## Example

```

> en
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 560
(config)# access-list 100 udp any any eq 560

(config)# class-map VOIP

```

```

(config-cmap)# match access-group 100
(config-cmap)# exit
(config)# policy-map NEW
(config-pmap)# class VOIP
(config-pmap-c)# police ?
<8000-2000000000> Bits per second
cir Committed information rate

(config-pmap-c)# police 1000 ?
<1000-512000000> Burst bytes
bc Conform burst
conform-action action when rate is less than conform burst
pir Peak Information Rate
<cr>

(config-pmap-c)# police 9000 conform ?
drop drop packet
set-clp-transmit set atm clp and send it
set-dscp-transmit set dscp and send it
set-mps-exp-transmit set exp and send it
set-prec-transmit rewrite packet precedence and send it
set-qos-transmit set qos-group and send it
transmit transmit packet

(config-pmap-c)# police 9000 conform transmit ?
exceed-action action when rate is within normal and max burst
<cr>

(config-pmap-c)# police 9000 conform transmit exceed-action ?
drop drop packet
set-clp-transmit set atm clp and send it
set-dscp-transmit set dscp and send it
set-mps-exp-transmit set exp and send it
set-prec-transmit rewrite packet precedence and send it
set-qos-transmit set qos-group and send it
transmit transmit packet

(config-pmap-c)# police 9000 conform transmit exceed-action drop ?
violate-action action when rate is greater than max burst
<cr>
(config-pmap-c)# police 9000 conform transmit exceed drop
(config-pmap-c)# exit
(config-pmap)# exit
(config)# control-plane
(config-cp)# service-policy output NEW

```

# Cisco Router Challenge 174

## Outline

This challenge involves configuring telephony.

## Objectives

The objectives of this challenge are to:

- Define telephony settings.

## Example

```
> en
# config t

(config)# telephony-service
(config-telephony)# ?
Cisco IOS Telephony Service configuration commands:
  application      The selected application
  call-forward     Define E.164 telephone number for call forwarding
  create           create cnf for ethernet phone
  date-format      Set date format for IP Phone display
  default          Set a command to its defaults
  dialplan-pattern Define E.164 telephone number prefix
  directory        Define directory naming order
  dn-webedit       enable Edit DN through Web
  exit             Exit from telephony-service configuration mode
  ip               Define IP address and port for Telephony-Service/Fallback
  keepalive        Define keepalive timeout period to unregister IP phones
  load             Select the IP phone firmware load file
  max-conferences  Define max number of 3 party G.711 conferences
  max-dn           Maximum directory numbers supported
  max-ephones      Define max number of IP phones
  moh              Define music-on-hold filename
  mwi              Define IP address and port for MWI Server
  network-locale  Define ephone network locale
  no               Negate a command or set its defaults
  reset           reset ethernet phone
  restart          restart ethernet phone
  service          Service configuration in ITS
  time-format      Set time format for IP Phone display
  time-webedit     enable Edit Time through Web
  timeouts         Define timeout value for IP phone
  transfer-pattern Define valid call transfer destinations
  transfer-system  Define call transfer system: blind/consult and
                  local/end-to-end
  url              Define Ephone URL's
  user-locale      Define ephone user locale
  voicemail        Set the voicemail access number called when the MESSAGES IP
                  phone button is pressed
  web              define username for admin user
```

```
(config-telephony)# max-ep ?
```

```
<1-48> Maximum phones to support
```

```
(config-telephony)# max-ep 10 ?
```

```
<cr>
```

```
(config-telephony)# max-ephones 10
```

```
(config-telephony)# max-dn ?
```

```
<1-192> Maximum directory numbers supported
```

```
(config-telephony)# max-dn 10 ?
```

```
<cr>
```

```
(config-telephony)# max-dn 10
```

```

(config-telephony)# keepalive ?
  <10-65535> Time in seconds
(config-telephony)# keepalive 10

(config-telephony)# system message this is a Cisco IP phone

(config-telephony)# create ?
  cnf-files create XML cnf for ethernet phone
(config-telephony)# create cnf-files

(config-telephony)# ip ?
  source-address Define IP address and port for Telephony-Service/Fallback
(config-telephony)# ip source-address ?
  A.B.C.D Define IP source address
(config-telephony)# ip source-address 1.2.3.4 ?
  port Define tcp port for Telephony Service/CM FALLBACK
  <cr>
(config-telephony)# ip source-address 1.2.3.4 p ?
  <2000-9999> Specify the port: 2000 - 9999
  <cr>
(config-telephony)# ip source-address 192.168.0.1 port 2000

(config-telephony)# voicemail ?
  WORD voicemail access number
(config-telephony)# voicemail 5555

(config-telephony)# web ?
  admin define username for admin user
  customize define customization file name
(config-telephony)# web admin ?
  customer customer admin
  system system admin
(config-telephony)# web admin system ?
  name admin username
  password admin password
(config-telephony)# web admin system name ?
  WORD username for admin
(config-telephony)# web admin system name username test password pass

(config-telephony)# dn-webedit

(config-telephony)# time-webedit

```

# Cisco Router Challenge 175

## Outline

This challenge involves configuring telephony by creating directory numbers.

## Objectives

The objectives of this challenge are to:

- Define telephony settings.
- Define directory numbers.
- Define a call forwarding number on a non-answer.

### Example

```
> en
# config t

(config)# telephony-service
(config-telephony)# max-ephones 10
(config-telephony)# max-dn 10
(config-telephony)# keepalive 10
(config-telephony)# system message this is a Cisco IP phone
(config-telephony)# create cnf
(config-telephony)# ip source-address 192.168.0.1 port 2000
(config-telephony)# voicemail 5555
(config-telephony)# web admin system name username test password pass
(config-telephony)# exit

(config)# ephone-dn 1
(config-ephone-dn)# ?
Ephone DN configuration commands:
  application      The selected application
  call-forward     Define E.164 telephone number for call forwarding
  caller-id       Configure port caller id parameters
  cor             Class of Restriction on dial-peer for this dn
  default         Set a command to its defaults
  description     dn desc, for DN Qualified Display Name
  exit           Exit from ephone-dn configuration mode
  feed           set live feed multicast stream mode
  hold-alert     Set Call On-Hold timeout alert parameters
  huntstop       Stop hunting on Dial-Peers
  intercom       Define intercom/auto-call extension number
  loopback-dn    Define dn-tag to create loopback dn pair with this ephone-dn
  moh           set live-feed music-on-hold mode (with optional multicast)
  mwi           set message waiting indicator options (mwi)
  name          Define dn user name
  no            Negate a command or set its defaults
  number        Define E.164 telephone number
  paging        set audio paging mode
  preference     Preference for the attached dial-peer for the primary dn
                number
  transfer-mode  Define call transfer mode: blind vs. consult
  translate      Translation rule
(config-ephone-dn)# number 5501
(config-ephone-dn)# name fred
(config-ephone-dn)# call-forward noan 5503 timeout 10
(config-ephone-dn)# exit
(config)# ephone-dn 2
(config-ephone-dn)# number ?
WORD A sequence of digits - representing telephone number
```

```

(config-ephone-dn)# number 5502 ?
  no-reg      Set E164 not register
  secondary  secondary dn number
  <cr>
(config-ephone-dn)# number 5502

(config-ephone-dn)# name ?
  LINE user name, use quoted string if including spaces
(config-ephone-dn)# name bert

(config-ephone-dn)# call-forward ?
  all    forward all calls
  busy   forward call on busy
  noan   forward call on no-answer
(config-ephone-dn)# call-forward all ?
  WORD  A sequence of digits - representing E.164 number
(config-ephone-dn)# call-forward all 5504

```

# Cisco Router Challenge 176

## Outline

This challenge involves configuring telephony by creating an e-phone.

## Objectives

The objectives of this challenge are to:

- Define an e-Phone.
- Define telephony settings.
- Define directory numbers.
- Define a call forwarding number on a non-answer.

## Example

```

> en
# config t
(config)# ephone 1
(config-ephone)# ?
Ethernet phone configuration commands:
  button      define button to dn map
  default     Set a command to its defaults
  exit        Exit from ephone configuration mode
  keepalive   Define keepalive timeout period to unregister IP phone
  mac-address define ethernet phone MAC address
  no          Negate a command or set its defaults
  paging-dn   set audio paging dn group for phone
  reset       reset ethernet phone
  restart     restart ethernet phone

```

```

speed-dial      Define ip-phone speed-dial number
type            Define ip-phone type
username        define username to access ethernet phone from Web
vm-device-id   define voice-mail id string
(config-ephone)# mac-address ?
H.H.H   Mac address
<cr>
(config-ephone)# mac-address 1.2.3.4
(config-ephone)# type ?
7910      Cisco IP Phone 7910
7935      Polycom 7935
7940      Cisco IP Phone 7940
7960      Cisco IP Phone 7960
ata       ATA phone emulation for analog phone
cipc     Cisco IP
vgc-phone vg248 phone emulation for analog phone
(config-ephone)# type cipc
(config-ephone)# button ?
LINE     button-index:dn-index pairs example 1:2 2:5
(config-ephone)# button 1:1
(config-ephone)# exit

(config)# telephony-service
(config-telephony)# max-ephones 10
(config-telephony)# max-dn 10
(config-telephony)# keepalive 10
(config-telephony)# system message this is a Cisco IP phone
(config-telephony)# create test
(config-telephony)# ip source-address 192.168.0.1 port 2000
(config-telephony)# voicemail 5555
(config-telephony)# exit
(config)# ephone-dn 1
(config-ephone-dn)# number 5501
(config-ephone-dn)# name fred
(config-ephone-dn)# call-forward noan 5503 timeout 10
(config-ephone-dn)# exit
(config)# ephone-dn 2
(config-ephone-dn)# number 5502
(config-ephone-dn)# name bert
(config-ephone-dn)# call-forward all 5504

```

If Cisco IP Communicator is used to simulate Ethernet phones, then the type is **cipc**.

For button 1:2, assigns the first button to the second directory number.

## Cisco Switch Challenge 70

### Outline

This challenge involves configuring Auto QoS on a switch.

### Objectives

The objectives of this challenge are to:

- Define Auto QoS

### Example

```
> en
# config t
(config)# cdp run

(config)# int vlan 10

(config)# int vlan 10
(config-vlan)# exit
(config)# int vlan 20
(config-vlan)# exit

(config)# int fa0/1
(config-if)# cdp enable
(config-if)# switchport ?
  access          Set access mode characteristics of the interface
  block           Disable forwarding of unknown uni/multi cast addresses
  broadcast       Set broadcast suppression level on this interface
  encapsulation   Set trunking encapsulation when interface is in trunking mode
  host            Set port host
  mode            Set trunking mode of the interface
  multicast       Set multicast suppression level on this interface
  native         Set trunking native characteristics when interface is in
                 trunking mode
  nonegotiate     Device will not engage in negotiation protocol on this
                 interface
  port-security   Security related command
  priority        Set appliance 802.1p priority
  protected       Configure an interface to be a protected port
  pruning         Set pruning VLAN characteristics when interface is in trunking
                 mode
  trunk          Set trunking characteristics of the interface
  unicast         Set unicast suppression level on this interface
  voice          Voice appliance attributes
  <cr>

(config-if)# switchport access vlan 10
(config-if)# switchport voice ?
  vlan           Vlan for voice traffic

(config-if)# switchport voice vlan ?
  <1-4094>       Vlan for voice traffic
  dot1p         Priority tagged on PVID
  none          Don't tell telephone about voice vlan
  untagged      Untagged on PVID
(config-if)# switchport voice vlan 20
(config-if)# au ?
  qos           Configure AutoQoS

(config-if)# auto qos ?
```

voip Configure AutoQoS for VoIP

```
(config-if)# auto qos voip ?
  cisco-phone  Trust the QoS marking of Cisco IP Phone
  trust        Trust the COS marking
```

```
(config-if)# auto qos voip cisco-phone
(config-if)# exit
```

Note:

For Auto QoS VoIP, CDP needs to be enabled.

## Cisco Router Challenge 177

### Outline

This challenge involves configuring custom queueing.

### Objectives

The objectives of this challenge are to:

- Define custom queueing (CQ) for particular queues.
- Define byte count and packet limits for each queue.
- Apply the CQ onto an interface.

### Example

```
> en
# config t
(config)# queue-list ?
  <1-16> Queue list number
(config)# queue-list 1 ?
  default      Set custom queue for unspecified datagrams
  interface    Establish priorities for packets from a named interface
  lowest-custom Set lowest number of queue to be treated as custom
  protocol     priority queueing by protocol
  queue        Configure parameters for a particular queue
  stun         Establish priorities for stun packets
(config)# queue-list 1 protocol ?
  arp          IP ARP
  bridge       Bridging
  bstun        Block Serial Tunnel
  cdp          Cisco Discovery Protocol
  compressedtcp Compressed TCP
  dlsw         Data Link Switching (Direct encapsulation only)
  ip           IP
  ipv6         IPV6
  llc2         llc2
```

```

pad                PAD links
pppoe              PPP over Ethernet
qllc               qllc protocol
rsrb               Remote Source-Route Bridging
snapshot           Snapshot routing support
stun               Serial Tunnel
(config)# que 1 protocol ip ?
<0-16> queue number
(config)# queue-list 1 protocol ip 2 ?
fragments          Prioritize fragmented IP packets
gt                 Classify packets greater than a specified size
list               To specify an access list
lt                 Classify packets less than a specified size
tcp                Prioritize TCP packets 'to' or 'from' the specified port
udp                Prioritize UDP packets 'to' or 'from' the specified port
<cr>
(config)# queue-list 1 protocol ip 2 tcp ?
<0-65535>          Port number
bgp                Border Gateway Protocol (179)
chargen            Character generator (19)
cmd                Remote commands (rcmd, 514)
daytime            Daytime (13)
discard            Discard (9)
domain             Domain Name Service (53)
echo               Echo (7)
exec               Exec (rsh, 512)
finger            Finger (79)
ftp                File Transfer Protocol (21)
ftp-data           FTP data connections (20)
gopher             Gopher (70)
hostname           NIC hostname server (101)
ident              Ident Protocol (113)
irc                Internet Relay Chat (194)
klogin             Kerberos login (543)
kshell             Kerberos shell (544)
login              Login (rlogin, 513)
lpd                Printer service (515)
nntp               Network News Transport Protocol (119)
pim-auto-rp        PIM Auto-RP (496)
pop2                Post Office Protocol v2 (109)
pop3                Post Office Protocol v3 (110)
smtp                Simple MailTransport Protocol (25)
sunrpc             Sun Remote Procedure Call (111)
syslog             Syslog (514)
tacacs             TAC Access Control System (49)
talk               Talk (517)
telnet             Telnet (23)
time               Time (37)
uucp               Unix-to-Unix Copy Program (540)
whois              Nicname (43)
www                World Wide Web (HTTP, 80)
(config)# queue-list 1 protocol ip 2 tcp 22
(config)# queue-list 1 protocol ip 2 tcp telnet
(config)# queue-list 1 protocol ip 3 tcp pop3
(config)# queue-list 1 protocol ip 3 tcp smtp
(config)# queue-list 1 protocol ip 4 tcp www
(config)# queue-list 1 default 4

```

```

(config)# queue-list 1 queue 1 ?
    byte-count  Specify size in bytes of a particular queue
    limit        Set queue entry limit of a particular queue
(config)# queue-list 1 queue 1 limit ?
    <0-32767>    number of queue entries
(config)# queue-list 1 queue 1 limit 100
(config)# queue-list 1 queue 2 byte-count 1000
(config)# int s0
(config-if)# custom-queue-list 1

```

# Cisco Router Challenge 178

## Outline

This challenge involves configuring custom queuing using access-lists to define the traffic for each queue.

## Objectives

The objectives of this challenge are to:

- Define custom queuing (CQ) for particular queues.
- Define byte count and packet limits for each queue.
- Apply the CQ onto an interface.

## Example

```

> en
# config t
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# access-list 101 tcp any any eq 80

(config)# queue-list 1 protocol ip 2 ?
    fragments  Prioritize fragmented IP packets
    gt         Classify packets greater than a specified size
    list       To specify an access list
    lt         Classify packets less than a specified size
    tcp        Prioritize TCP packets 'to' or 'from' the specified port
    udp        Prioritize UDP packets 'to' or 'from' the specified port
    <cr>
(config)# queue-list 1 protocol ip 2 list 100
(config)# queue-list 1 protocol ip 3 list 101
(config)# queue-list 1 default 3
(config)# queue-list 1 queue 2 limit 100
(config)# queue-list 1 queue 3 byte-count 1000
(config)# int s0

```

```
(config-if)# custom-queue-list 1
```

# Cisco Router Challenge 179

## Outline

This challenge involves configuring priority queueing using access-lists to define the traffic for each queue.

## Objectives

The objectives of this challenge are to:

- Define priority queueing (PQ) for particular queues.
- Apply the PQ onto an interface.

## Example

```
> en
# config t
# config t
(config)# access-list 100 udp any any range 16384 32767
(config)# access-list 100 tcp any any eq 1720

(config)# access-list 101 tcp any any eq 80

(config)# priority-list ?
<1-16> Priority list number
(config)# priority-list ANY ?
default          Set priority queue for unspecified datagrams
interface        Establish priorities for packets from a named interface
protocol         priority queueing by protocol
queue-limit      Set queue limits for priority queues
(config)# priority-list 1 protocol ?
arp              IP ARP
bridge          Bridging
cdp             Cisco Discovery Protocol
clns            ISO CLNS
clns_es         ISO CLNS End System
clns_is        ISO CLNS Intermediate System
cmns           ISO CMNS
compressedtcp   Compressed TCP (VJ)
http           HTTP
ip             IP
llc2          llc2
pad           PAD links
pppoe         PPP over Ethernet
rsrb         Remote Source-Route Bridging
snapshot      Snapshot routing support
(config)# priority-list 1 protocol ip ?
```

high  
medium  
normal  
low

```
(config)# priority-list 1 protocol ip high ?  
fragments  Prioritize fragmented IP packets  
gt          Prioritize packets greater than a specified size  
list       To specify an access list  
lt         Prioritize packets less than a specified size  
tcp        Prioritize TCP packets 'to' or 'from' the specified port  
udp        Prioritize UDP packets 'to' or 'from' the specified port  
<cr>  
(config)# priority-list 1 protocol ip high list 100  
(config)# priority-list 1 protocol ip low list 101  
  
(config)# priority-list 1 queue-limit 20 40 60 80  
(config)# int e0  
(config-if)# priority-group 1
```

#### Note:

It is also possible to base the queue on protocols, such as:

```
(config)# priority-list 1 protocol ip low tcp 22  
(config)# priority-list 1 protocol ip high tcp www
```

To give a high priority for WWW traffic, and a low one for SSH.