Important : Un rapport doit être rendu au plus tard 15 jours après le TP.

Objectif :

- ☐ Configuration du DHCP, Call Manger Express (CME) et des téléphones IP
- ☐ Monter une plateforme de téléphonie IP entre deux sites distants
- ☐ Etudier le mécanisme de qualité de services (QoS) et en particulier le mécanisme DiffServ
- ☐ Comprendre les mécanismes de filtrage, classification des flux réseau
- ☐ Création de politique de services
- ☐ Connaître les principales commandes « Cisco » pour configurer les routeurs afin qu'ils supportent la QoS

Pré-requis :

- ☐ Protocole IP et adressage
- ☐ Routage statique

Le TP doit se dérouler en deux phases : simulation par « Packet Tracer » et implémentation par des vrais routeurs et câbles.

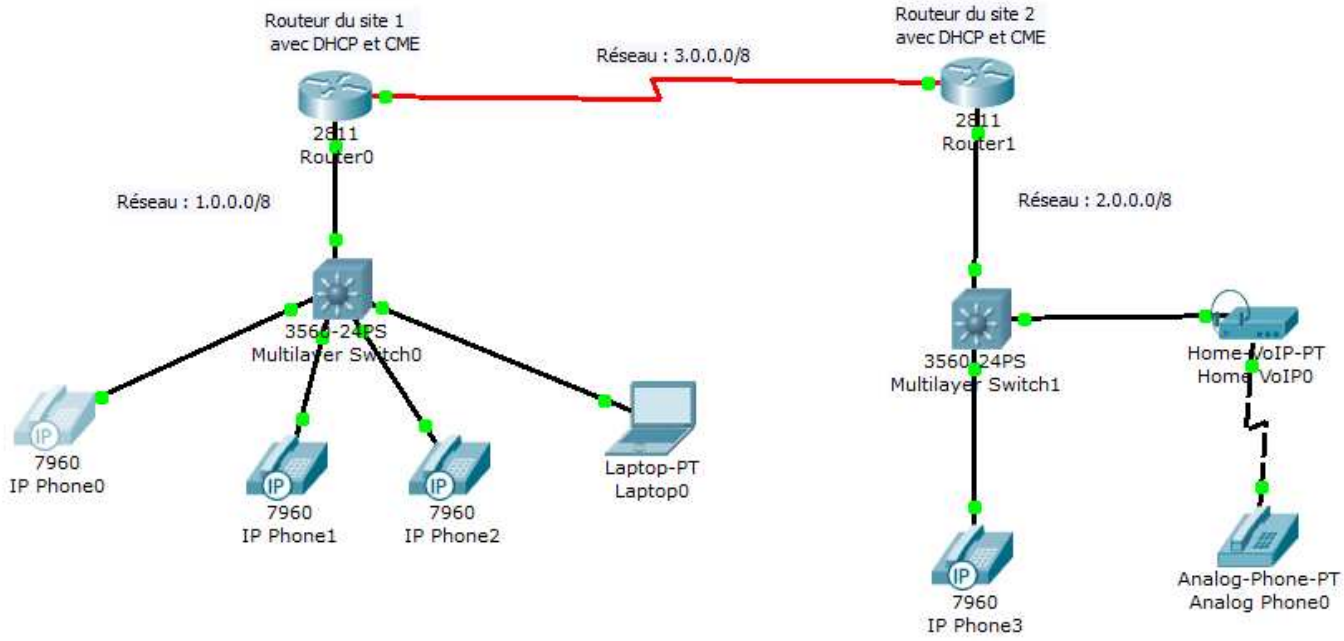


Figure 1. Topologie réseau

1. Configuration de base

Tâche 1 : configuration des informations IP sur les interfaces Ethernet d'un réseau

Étape 1 : configurez les informations IP sur les ordinateurs.
Configurez les informations IP suivantes sur les interfaces des routeurs 0 et 1 qui correspodent à deux sites différents 1 et 2 :

- **Routeur_du_site_1** – fastEthernet0/0 : Adresse IP : 1.1.1.1, masque de sous-réseau : 255.0.0.0,

- **Routeur_du_site_1 _** serial0/0/0 : Adresse IP : 3.0.0.1, masque de sous-réseau : 255.0.0.0

- **Routeur_du_site_2** – fastEthernet0/0 : Adresse IP : 2.1.1.1, masque de sous-réseau : 255.0.0.0,
- **Routeur_du_site_2 _** serial0/0/0 : Adresse IP : 3.0.0.2, masque de sous-réseau : 255.0.0.0

Accédez au routeur R0 (Routeur_du_site_1). Sous l'onglet ILC, saisissez le mode d'exécution privilégié en entrant la commande **enable**. Saisissez le mode de configuration globale en entrant la commande **config t**. Saisissez le mode de configuration pour la première **interface FastEthernet** en entrant la commande **interface fa0/0**. Configurez l'adresse IP suivant l'interface via la commande **ip address 1.1.1.1 255.0.0.0**. Activez l'interface en entrant la commande **no shutdown**. Quittez le mode de configuration en utilisant le raccourci clavier **Ctrl+z**.
Ensuite il faut configurer l'interface série via la commande **interface Serie 0/0/0.** Donner l'adresse IP à cette interface via la commande **ip address 3.0.0.1 255.0.0.0.** Il ne faut pas oublier le « **clock rate** » pour la synchronisation de la liaison.

Routeur_du_site_1(config)#interface serial 0/0/0
Routeur_du_site_1(config-if)#ip address 3.0.0.1 255.0.0.0
Routeur_du_site_1(config-if)#clockrate 56000
Routeur_du_site_1(config-if)#no shutdown

Il faut faire la même chose pour la configuration du routeur du site 2 (router 1).

Étape 2 : Configuration de service VOIP
Tâche 1 : Monter un serveur DHCP sur les deux routeurs (Routeur_du_site_1 et Routeur_du_site_2).
Les téléphone IP Cisco 7960 nécessite un serveur DHCP pour l'obtention de l'adresse IP. Accédez au routeur R0 (**Routeur_du_site_1**). Sous l'onglet ILC, saisissez le mode d'exécution privilégié en entrant la commande **enable**. Saisissez le mode de configuration globale en entrant la commande **config t**. Saisissez le mode de configuration pour créer le « pool DHCP » nommé VOICE1 pour le réseau 1.0.0.0 (VOICE2 dans le Routeur_du_site_2 pour le réseau 2.0.0.0). Exemple pour le premier pool DHCP :

Routeur_du_site_1(config)#ip dhcp pool VOICE1
Routeur_du_site_1(dhcp-config)#network 1.0.0.0 255.0.0.0
Routeur_du_site_1(dhcp-config)#default-router 1.1.1.1
Routeur_du_site_1(dhcp-config)#option 150 ip 1.1.1.1

Vous faites la même chose pour le deuxième pool « VOICE2 » dans le **Routeur_du_site_2**.

Tâche 2 : Configuration VLAN au niveau des Switchs Multi-Layers 3560 pour séparer le trafic
Pour séparer le flos VOIP dans les Switchs, il suffit de créer un VLAN au niveau des ports de Switch comme suit :

Switch0(config)#interface range fa0/1 – 5 # Configurer l'ensemble des interfaces du Switch
Switch0(config-if-range)#switchport mode access
Switch0(config-if-range)#switchport voice vlan 1 #Définir le VLAN pour les paquets VOIP#

Il faut répéter la tâche 3 pour le Swich1 du réseau 2.0.0.0/8.

Tâche 3 : Activer le gestionnaire de communication VOIP (Call Manager Express)
Pour la gestion de communication téléphonique et activer le VOIP dans le réseau, il faut configurer le serveur TFT ou le « Call Manager Express ». Ce serveur doit tourner sur le QoS_Router.

Routeur_du_site_1(config)#telephony-service #Pour configurer les services de téléphonie du routeur#
Routeur_du_site_1(config-telephony)#max-dn 5 #Définir le nombre maximum des numéros d'annuaires#
Routeur_du_site_1(config-telephony)#max-ephones 5 # Définir le nombre maximum de téléphones#
Routeur_du_site_1(config-telephony)#ip source-address 1.1.1.1 port 2000 #IP Address source#
Routeur_du_site_1(config-telephony)#auto assign 4 to 6 #Assigner de manière automatique l'extension des numéros au bouttons#
Routeur_du_site_1(config-telephony)#auto assign 1 to 5

Tâche 4 : Configurer le répertoire du téléphone IP
Cette tâche consiste à attribuer un numéro de téléphone aux IP phone 0, 1 et 2 dans le site 1 (IP Phone 3 et le téléphone analogique). Par conséquent, il faut configurer le Call Manager Express (CME) au niveau du routeur QoS_Router.

Routeur_du_site_1(config)#ephone-dn 1 #Définir le premier répertoire téléphonique (IP Phone 0)y#
Routeur_du_site_1(config-ephone-dn)#number 1101 #Attribuer un numéro téléphone à cette entrée#

Il faut répéter la tâche 4 pour l'IP Phone 1 et 2 avec l'attribution des numéros d'appels suivants : 1201, 1301 et 1401 (pour le Laptop0).

Tâche 5 : Répéter les tâches 3 et 4 pour configurer le Routeur_du_site_2
Pour le site 2 respectez la règle d'attribution des numéros d'appels pour faire la différence entre les deux sites 1 et 2. Les numéros d'appels des téléphones IP du site 1 commence par **1xxx** et **2xxx** pour le deuxième site.

Tâche 6 : Tester la configuration
Tout d'abord, il faut vérifier si tous les téléphones IP possèdent leurs adresses IP. Il suffit juste de passer le curseur sur le téléphone IP pour voir s'il possède une adresse IP et son numéro de ligne. Voir la figure ci-dessous. Vous pouvez lancer des appelles vers les différents numéros de téléphone.

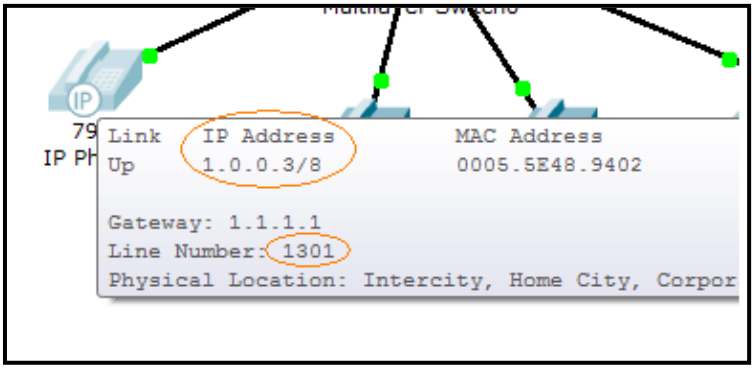


figure2. Test d'attribution d'adresse IP et de numéro d'appel au téléphone IP

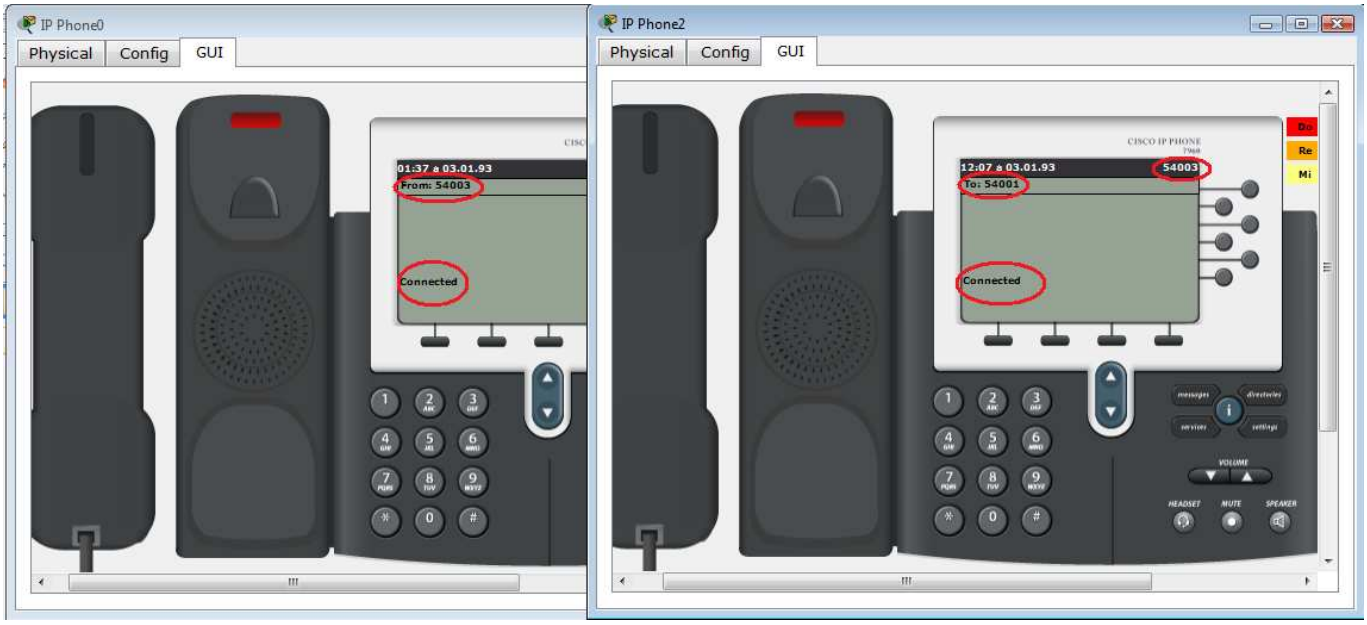


Figure3. Test d'appel téléphonique entre les deux téléphones IP 0 et 2

Nous constatons que les téléphones IP du site 1 n'arrivent pas à joindre les téléphones IP du site 2.

Il faut configurer les routeurs des deux sites 1 et 2 afin qu'ils puissent identifier les numéros d'appels du site distant en passant par le réseau WAN dont l'adresse réseau est : 3.0.0.0/8.
Sur le routeur du site 1 :

```
Routeur_du_site_1(config)#dial-peer voice 1 voip
Routeur_du_site_1(config-dial-peer)#destination-pattern 2…     #Destination commence par le n.o.2#
Routeur_du_site_1(config-dial-peer)#session target ipv4:3.0.0.2     #Passerelle Routeur_du_site_2#
```

Il faut faire la même chose pour le Routeur_du_site_2

Tâche 6 : Tester la configuration
Lancer un appel d'un téléphone IP du site 1 vers un autre téléphone IP du site 2.

Tâche 7 : Refaire les tâches 1 à 6 avec des vrai routeurs

Remarque :
1- À la fin du TP merci d'effacer la configuration de votre routeur avec la commande « **erase startup-config** ».
2- Si la configuration n'est pas une configuration d'usine, vous tapez **erase startup-config** suivi de **reload**). Nous allons utiliser celle-ci pour entrer simplement une première configuration qui :

- Donnez le nom que vous avez choisi au routeur ;
- Utilisez le mot cisco pour le « enable secret » et le *password* des consoles virtuelles, et n'importe quel autre mot de passe pour le « enable password » (le « enable secret » est le mot de passe du mode super-utilisateur (enable) qui est sauvé sous forme chiffrée, « enable password » est l'ancienne version du mot de passe sauvée sous forme non chiffrée qui ne sera utilisée que si l'on démarre le routeur avec une veille version de l'IOS) ;
- Configurez une des interfaces Ethernet du routeur avec l'adresse 1 de la plage d'adresses choisie pour votre réseau ;
- Ne configurez pas les autres interfaces ;
- Routez les datagrammes IP ;
- Ne démarrez aucun protocole de routage dynamique type RIP ou IGRP ;
- Ne démarrez pas le service SNMP.

3- Si vous travaillez sur le Switch intégré au routeur (HWIC-4ESW-POE), vous devez attribuer une adresse IP au VLAN créé ensuite associé cette adresse au serveur DHCP.
4- Pour analyser les paquets (en particulier de type ***SCCP***), il faut utiliser la commande du monitoring de port (à l'aide de la commande ***monitor session*** …). Cette commande permet d'orienter les paquets vers le port ou l'analyse des paquets sera effectuée.

Tâche 8 : Transfert d'appels

Le transfert d'appels est l'une des fonctionnalités principales utilisées dans la téléphonie. Elle permet, depuis le téléphone réceptionnant un appel établi, de rediriger ce dernier vers un tiers sans en interrompre la communication. La mise en place du transfert d'appels est une fonctionnalité directement disponible et ne demande donc aucun paramétrage. Le but étant ici d'analyser le comportement et les messages échangés entre les téléphones et le CallManager.

L'exécution d'un transfert d'appels s'effectue selon les opérations suivantes :

- Le téléphone IP Phone-0 établit une communication avec le téléphone IP Phone-1.
- Le téléphone IP Phone-1 active le mode de transfert par pression de la touche « Trnsfer » (disponible sous « more »)
- Le téléphone IP Phone-1 compose le numéro du téléphone IP Phone-3, vers lequel il souhaite transférer l'appel, et établit une communication.
- Le téléphone IP Phone-1 confirme l'option de transfert par nouvelle pression de la touche « Trnsfer » et l'appel est effectivement dévié.

Question 1 :

Réalisez le scénario ci-dessus à l'aide de votre architecture tout en capturant le trafic du téléphone émettant l'appel tout comme celui du téléphone déviant l'appel. Les captures sur les parties concernées peuvent s'effectuer en deux temps, avec les rôles des téléphones inversés.

a) Regardez d'abord le comportement du téléphone dont l'appel est transféré. Quels sont les messages qui effectuent le transfert de l'appel ? Est-ce que ces messages sont générés par le téléphone ou la CUCME (Cisco Unified Communications Manager Express) ?

b) Regardez maintenant le comportement du téléphone qui effectue le transfert. Décrivez la séquence des messages qui effectuent le transfert.

Tâche 9 : Hunting

L'option ephone-hunt permet la création d'un numéro de service qui, une fois appelé, redirige l'appel sur l'une des extensions inscrite dans une liste définie de numéros. L'appel sera redirigé de numéro en numéro tant qu'aucun correspondant ne décroche. Très utile en entreprise, cette fonctionnalité permet, par exemple, d'assigner plusieurs téléphones à répondre au numéro d'un service informatique.
Le paramétrage de cette option s'effectue selon les commandes ci-dessous.

```
Routeur_du_site_1(config)#ephone-hunt AA peer
Routeur_du_site_1(config-ephone-hunt)#pilot 1XXYY
Routeur_du_site_1(config-ephone-hunt)#list 1XXYY, 1XXYY, 1XXYY, 1XXYY, 1XXYY
Routeur_du_site_1(config-ephone-hunt)#final 1XXYY
Routeur_du_site_1(config-ephone-hunt)#hops BB
Routeur_du_site_1(config-ephone-hunt)#timeout CC
```

où

- AA représente le numéro d'extension hunt
- BB représente le nombre de sauts autorisés
- CC représente le temps d'attente, en secondes, entre chaque redirection d'appels
- XX représente le numéro de groupe
- YY représente un numéro de ligne

Le numéro de service est définit par « **pilot** ». Les extensions rattachées au numéro de service en question sont définies par l'option « **list** ». Une fois le nombre de saut (« **hops** ») maximum autorisé atteint, l'appel est redirigé vers le numéro final « **final** ». « **timeout** » définit le temps d'attente avant la prochaine redirection.
Remarque : Il est important de relever que les numéros de la liste sont appelés séquentiellement mais que cette séquence ne commence pas toujours par le premier numéro !
En fonction des instructions ci-dessus, paramétrez une extension hunt sur le numéro 80 de votre plage de numéros (1XX80). Définissez, les 2 premières extensions comme numéros de liste (1XX01 et 1XX02), la 3e extension comme numéro final, un nombre de sauts souhaités de 2 ainsi qu'un timeout de 5 secondes.

Question 2 :

a) Capturez le trafic émis lors de l'appel sur le numéro de service. Montrez la séquence des téléphones appelés.

b) Explique le mécanisme pour réaliser cette fonction. Que fait le CallManager ? Que font les télépones ?

Tâche 10 : Call-Park

La fonctionnalité du call-park permet la création d'une ligne de mise en attente. Très utile dans le but de faire patienter un correspondant, l'appel parqué réceptionnera la musique prévue à cet effet, contenue dans le fichier music-on-hold.au. L'ajout d'un appel en call-park s'effectue directement depuis les téléphones, à l'aide de la touche « Park ». Le téléphone ayant parqué l'appel se fait avertir de ce dernier à raison d'intervalles définie par l'option « timeout ».
Le paramétrage de cette option s'effectue selon les commandes ci-dessous.

```
Routeur_du_site_1(config)#ephone-dn AA
```

```
Routeur_du_site_1(config-ephone-dn)#number 1XXyy
Routeur_du_site_1(config-ephone-dn)#park-slot timeout BB limit CC
```

où

- AA représente le numéro d'extension
- BB représente le temps, en secondes, avant le prochain rappel
- CC représente le nombre de cycles de timeout autorisés
- XX représente le numéro de groupe
- YY représente un numéro de ligne

En fonction des instructions ci-dessus, paramétrez un call-park dans l'extention 55, sur le numéro de ligne 55. Le rappel de l'appel parqué doit s'effectuer toutes les 15 secondes pour un total maximal de 10.
La prise en compte du call-park par les téléphones nécessite une réinitialisation de ces derniers. Pour ce faire, utilisez la commande ci-dessous :

```
Routeur_du_site_1(config)#ephone XX
Routeur_du_site_1(config-ephone)#restart
```

où

- XX représente le numéro du téléphone physique à redémarrer

Question 3 :

Parquez un appel depuis le téléphone dont vous capturez le trafic et mettez en évidence les messages de rappel envoyés par le CallManager afin d'avertir le téléphone que l'appel est parqué.

Tâche 11 : Intercom

L'option d'Intercom vise à établir, à la pression d'un bouton et de manière directe, une communication entre deux ou plusieurs téléphones.
La configuration d'une liaison Intercom entre deux extensions, s'effectue selon les instructions ci-dessous.

```
Routeur_du_site_1(config)#ephone-dn AA
Routeur_du_site_1(config-ephone-dn)# number 1XXYY
Routeur_du_site_1(config-ephone-dn)# label Intercom
Routeur_du_site_1(config-ephone-dn)# name Intercom
Routeur_du_site_1(config-ephone-dn)# intercom 1XXZZ barge-in

Routeur_du_site_1(config)#ephone-dn BB
Routeur_du_site_1(config-ephone-dn)# number 1XXZZ
Routeur_du_site_1(config-ephone-dn)# label Intercom
Routeur_du_site_1(config-ephone-dn)# name Intercom
Routeur_du_site_1(config-ephone-dn)# intercom 1XXYY barge-in
```

où

- AA, BB représentent les numéros d'extension Intercom
- XX représente le numéro de groupe
- YY, ZZ représentent les numéros de lignes

Paramétrez, selon les instructions ci-dessus, une liaison Intercom entre les extensions 98 et 99. Les numéros de lignes utilisés seront similaires aux numéros d'extensions.
L'étape suivante consiste à l'attribution de ces extensions Intercom à deux téléphones Cisco, comme ligne secondaire.
Attribuez ces extensions aux téléphones possédant vos deux premières extensions (1XX01 et 1XX02).

Cisco 7960

```
Routeur_du_site_1(config)#ephone X
```

```
Routeur_du_site_1(config-ephone)#button 1:Y 2:BB
```

où

- AA, BB représentent les numéros d'extension Intercom
- X représente le numéro du téléphone
- Y représente le numéro d'extension déjà attribué au téléphone

Le modèle 7960 autorise l'attribution de 2 lignes sur 2 boutons différents tandis que le modèle 7906 intègre ses deux lignes sur un seul.
Un redémarrage des téléphones est nécessaire. Pour ce faire, utilisez la commande donnée précédemment.

Question 4 :

Mettez en évidence les messages transmis lors de l'établissement d'un Intercom.
Par quels états le téléphone passe-t-il ?

Tâche 12 : Conférence

Les conférences permettent une conversation téléphonique à plus de deux participants. Différents modes de conférences sont possibles (softwares, hardwares). Cette partie du laboratoire vise à étudier le mode de conférence le plus simple, déjà géré par CallManager, ne demandant donc pas de paramétrage.
La création d'une conférence s'effectue selon les opérations suivantes :

- Appel du premier participant
- Sélection de l'option « Confrn » (disponible sous « more »)
- Composition du numéro du deuxième participant
- Confirmation de la conférence par nouvel appui de « Confrn »

Question 5 :

a) Montrez la capture de trafic émis lors de l'établissement d'une conférence.
b) Quelle conséquence directe a la pression de la touche « Confrn » ?
c) Une fois la conférence démarrée, entre quelles adresses IP le flux média est-il échangé ? Que pouvez-vous en déduire ?

Tâche 13 : Administrer le CCME via une interface graphique

Dans cette partie, vous configurez le CCME pour qu'il puisse être administré via une l'interface web graphique.
La procèdure est la suivante :

Routeur_1(config)# ip http server

Routeur_1(config)# telephony-service
Routeur_1(config-telephony)# web admin system name <adminlogin> password <adminpassword>
Routeur_1(config-telephony)# dn-webedit
Routeur_1(config-telephony)# time-webedit

Lancez le navigateur à partir du PC, ensuite introduisez l'adresse IP du routeur. Une fenêtre d'authentification apparaisse et vous demande le login et mot de passe.

II- Qualité de Services IP

1. Génération et mesure du trafic réseau

Nous ajoutons deux machines PC1 et PC2 sur les sites 1 et 2 respectivement.

Nous considérons la concurrence entre deux trafics : UDP entre PC1 et PC2 et TCP entre Laptop0 et PC2.

- Le cas de « *Packet Tracer* » : vous pouvez utiliser l'outil « Traffic Generator » qui se trouve dans le bureau des PC/Laptop.
- Le cas des vrai routeurs/PC : vous pouvez générer et mesurer le trafic réseau de deux manières : l'utilisation des outils MGEN/TRPR ou les outils UDPMT/UDPTARGET pour le trafic UDP et TCPMT/TCPTARGET pour le trafic TCP.

Exemple de génération de trafic et de mesure (débit, gigue, pertes) avec MGEN/TRPR :

Syntaxe de la commande mgen: ***mgen input <scriptfile> [output <logfile>]***

Pour générer un trafic périodique de type UDP :

- 2 secondes après le démarrage, un flux nommé 1 en UDP avec comme IP de destination 172.30.2.2 sur le port 5000 un flux PERIODIC qui envoi 10 paquets de 1024 octets par seconde. Ce flux s'arrête au temps 11.0.
- Vous mettez les lignes suivantes dans le fichier ***source.mgn*** :
  2.0 ON 1 UDP DST 192.168.9.24/5000 PERIODIC [10.0 1024]
  11.0 OFF 1
- Pour lancer la génération : ***mgen input source.mgn***
- N'oubliez pas de lancer le serveur pour écouter les ports 5000 et 5001. Il suffit d'écrire un fichier *destination.mgn* qui contient la ligne suivante :
  0.0 LISTEN UDP 5000,5001
- Pour lancer la lecture : ***mgen input destination.mgn***
- Affichage graphique du trafic en temps réel ou à partir d'un fichier.
  mgen input destination.mgn | trpr mgen real | gnuplot
  trpr <nom_du_fichier_de_log mgen real | gnuplot –persist
- Les options de trpr :
  - *interarrival* affiche le temps entre le paquet courant et le dernier paquet reçu sur le même flux.
  - *loss* affiche la quantité de paquets perdus (valeur normée).
  - *history* N indique que le graphe affiche N secondes d'information.

Dans cette étape, il faut tester le trafic réseau dans le cas d'un seul flux périodique entre le PC1 et le PC2. Vous générez le trafic selon les scénarios donnés dans le tableau ci-dessous :

Taille des paquets en Octet	128		1024		8192	
Débit en paquet/seconde	50	1000	50	1000	50	1000

1- Calculer le débit, la gigue et le taux de perte des paquets. Analyser les résultats obtenus.
2- Ajouter un deuxième flux UDP entre le Laptop0 et le PC2 afin de créer une situation de concurrence avec le premier flux. Quelles sont les métriques d'évaluation pour savoir si le premier flux est perturbé par le second ? Quelles sont les remarques et les conclusions ?
3- La même chose que la question précédente, mais avec le deuxième flux de type TCP.
4- Quelle est la solution *la plus simple* pour assurer un traitement équitable entre les flux au niveau des files d'attente ? Est-ce que l'équité est assurée au niveau des paquets transmis ou au niveau des octets transmis ? Est-ce que cette solution permet de protéger le flux des perturbations éventuelles ?
5- Si nous connectons un autre réseau (172.30.20.0/24) au routeur 1, mais le trafic réseau venant du réseau (172.30.1.0/24) est prioritaire. Quelle est la solution la plus simple à mettre en place pour assurer cette condition ? Supposons que l'utilisation de plusieurs files d'attente différentes sur

l'interface de sortie permette de différencier le trafic venant des deux réseaux. Mettre en évidence cette solution. La commande « ***custom-queue-list*** » de configuration d'interface permet d'associer une liste de files d'attente (ex. ***custom-queue-list 1***). Ensuite la manipulation de cette liste par la commande « ***queue-list 1 interface Ethernet1/0 0*** »

2. Identification et filtrage de flux

Pour établir une qualité de service il faut tout d'abord identifier et sélectionner les flux qu'on veut différencier. Nous disposons de deux techniques de filtrage dans l'IOS du routeur qui sont basées sur l'utilisation d'ACLs (**Access Control List**) ou bien de **class-map**.

Access Control List : Une liste de contrôles d'accès est une collection d'instructions permettant d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :
-L'adresse d'origine, L'adresse de destination, Le numéro de port, Les protocoles de couches supérieures

Il existe 3 types de listes de contrôles d'accès : les ACLs standards, les ACLs étendues et les ACLs nommées.
Les **ACLs standards** utilisent des spécifications d'adresses simplifiées et autorisent ou refusent un ensemble de protocoles. C'est-à-dire en d'autres termes que l'on peut interdire par exemple à une machine l'accès à une autre machine ou à un autre réseau.
Les **ACLs étendues** utilisent des spécifications d'adresses plus complexes et autorisent ou refusent des protocoles précis. Ce type d'ACL utilise un filtrage bien plus spécifique - on peut selon nos besoins, interdire (ou permettre) des flux depuis et vers une autre machine (ou réseaux) suivant des critères tels que :
- Le type de protocole de niveau 4 (en l'occurrence TCP ou UDP).
- Le numéro de port utilisé.
- Ou même le type de l'application (ftp, telnet .....).
Les **ACLs nommées** peuvent être soit standards, soit étendues; elles n'ont pour but que de faciliter la compréhension et de connaître la finalité de l'ACL.

Paramètres d'une ACL :

Routeur# access-list *numéro { **permit** ou **deny** } protocole source destination opérateur (numéro de port)*

numéro : <1-99> : IP standard, <***100-199***> : IP étendu (des paquets IP qui transitent le routeur), …
protocole : IP, TCP, UDP, ICMP, GRE, IGRP
source : adresse source
destination : adresse destination
opérateur : lt *less than* (plus petit que), gt *greater than* (plus grand que), eq *equal (*egal à), neq *not equal (*différent de)
numéro de port : le numéro de port de l'application

Exemple : Pour filtrer les paquets TCP à destination du PC1 *172.30.2.2*, port 80, et quel que soit l'émetteur. Nous pouvons utiliser la commande suivante :
access-list 101 permit tcp 0.0.0.0 255.255.255.255 172.30.2.2 255.255.255.0 eq 80

1. Dans le but de protéger le flux TCP, limiter le débit du trafic UDP avec l'utilisation de la commande Cisco « *rate-limit* ». Cette méthode appelée CAR (Committed Access Rate) permet de limiter la bande passante sur l'interface de sortie d'un trafic particulier.
   La syntaxe de la cmd :
   rate-limit {input | output} [dscp* dscp-value*] [access-group [rate-limit]* acl-index*] bps burst-normal burst-max conform-action* conform-action ***exceed-action exceed-action
   Exemple : ***rate-limit output access-group 101 80000 8000 8000 conform-action transmit exceed-action drop***
2. Analyser le trafic réseau, ainsi que son impact sur le trafic VOIP.
3. Quelle est la limite de cette méthode?

3. Création d'une politique de qualité de service avec DiffServ

a) DiffServ (Differentiated Services)

Permet de marquer le trafic selon sa classe de priorité en utilisant le champ ToS (Type of Service) de 6 bit dans l'entête du paquet IP. Les valeurs de ce champ définissent un code pour classer les priorités appelé DSCP (Differentiated Services Code Point) autorisant **64** niveaux différents. Deux Classes de DSCP existent EF (Expedited Forwarding) et AF (Assured Forwarding) : EF définie un service premium alors que AF est constitué de quatre classes indépendantes, chacune comportant trois niveaux de priorités de rejet des paquets.

Type of Service (TOS)	X	X	X	X	X	X	X	0
	7	6	5	4	3	2	1	0
Differentiated Services (DS)	X	X	X	X	X	X	X	X

Figure 2. Le champ ToS dans l'entête IP

La notion **IP Precedence** est la technique de QoS la plus utilisée à cause de sa simplicité et de son interopérabilité avec les éléments du réseau. Elle utilise les **3 bits de poids fort du DSCP** ce qui assure la compatibilité avec la technique précédente, mais n'offre, par conséquent, que **8 niveaux de classifications**. Les valeurs **6 et 7** sont réservées pour **le contrôle du réseau et les protocoles de routage**. Il reste 6 niveaux de priorités. L'implémentation utilise généralement une priorité 5 pour la voix sur IP, 4 pour la vidéo et la visioconférence en général, 0 pour le trafic Best effort. Selon les RFC791/RFC1349 l'interprétation des valeurs attribuées au champ Tos et les recommandations en fonction de type de trafic réseau sont données dans les 2 tableaux suivants :

Bits	Meaning
7-5	IP Precedence: 111 Network Control 110 Internetwork Control 101 Critic/ECP 100 Flash Override 011 Flash 010 Immediate 001 Priority 000 Routine
4	1 = Low Delay; 0 = Normal Delay
3	1 = High Throughput; 0 = Normal Throughput
2	1 = High Reliability; 0 = Normal Reliability
1	1 = Minimise monetary cost (RFC 1349)
0	Must be 0

Trafic réseau	DSCP PHB	DSCP Décimale	IP Precedence
Voix (Voice)	EF	46	5
Vidéo	AF41	34	4
Contrôle voix	AF31	26	3
Données- High Priority1	AF21	18	2
Données- High Priority2	AF22	20	2
Données- High Priority3	AF23	22	2
Données – Medium Priority 1	AF11	10	1
Données – Medium Priority 2	AF12	12	1
Données – Medium Priority 3	AF13	14	1
Données – Best Effort	BE	0	0

Figure 3. Interprétation des valeurs du champ ToS et recommandation d'utilisation

AFxy Assured Forwarding (x=class, y=drop precedence) (RFC2597)
EF Expedited Forwarding (RFC 3246)

Classification du trafic réseau

L'utilisation du Modular QoS CLI (MQC) permet de réduire la complexité de configuration afin de créer des classes de services avec des politiques différentes. Une classe de trafic contient trois éléments essentiels : le nom de la classe, une série de commandes **match,** et comment évaluer ces commandes match.
Les commandes match sont utilisées pour spécifier divers critères de classification des paquets. Les paquets sont vérifiés pour déterminer s'ils appartiennent ou non à ces critères spécifiés par la commande match.
En utilisant la classification des paquets on peut par la suite partitionner notre réseau en plusieurs niveaux de priorités ou en classes de services (**class-map**).

Paramètres des class-map

routeur(config)#class-map *nom-de-la-classe*

On associe un nom à une class-map pour mieux la désigner par la suite

routeur(config)#class-map match-all *nom-de-la-classe*

On spécifie que TOUS les critères doivent être vérifiés pour que le paquet appartienne à la classe.

routeur(config)#class-map match-any *nom-de-la-classe*

On spécifie qu'AU MOINS un des critères doit être vérifié pour que le paquet appartienne à la classe.

routeur(config-cmap)#match access-group *numéro-de-l'ACL*

On spécifie que le paquet doit vérifier l'ACL correspondante pour qu'il appartienne à la classe.

routeur(config-cmap)#match any

On spécifie que tous les paquets seront dans cette classe.

routeur(config-cmap)#match {destination ou source}-address mac *adresse*

On spécifie que le paquet doit vérifier l'adresse MAC source ou destination pour qu'il appartienne à cette classe.

routeur(config-cmap)#match input-interface *nom-de-l'interface*

On spécifie que le paquet doit vérifier l'interface d'entrée indiquée pour qu'il appartienne à la classe.

routeur(config-cmap)#match ip dscp *valeur-du-ip-dscp*

Pour l'utilisation de DiffServ on a la possibilité de spécifier la valeur du **ip dscp** entre **0 et 63** pour que le paquet appartienne à la classe.

routeur(config-cmap)#match ip precedence *valeur-de-champs-TOS*

3 bits du champ TOS dans l'entête ip forment *l'IP precedence* utilisée pour la qualité de service. Dans un paquet reçu, si la valeur de ce champ est égale à la valeur indiquée ici alors le paquet appartient à cette classe.

routeur(config-cmap)#match protocol *protocole*

On spécifie le protocole suivant lequel les paquets appartiennent à la classe

Exemples :
Nous pouvons aussi assurer le filtrage et la classification des flux en fonction du protocole avec l'utilisation de la commande **class-map** et **match protocol** comme l'exemple suivant :

```
class-map match-any web-traffic
match protocol http
match protocol secure-http
match protocol ipsec
match protocol dns
```

A l'entrée du routeur, une vérification sur le type de trafic est effectuée pour établir une classification en fonction du protocole utilisé. Nous pouvons aussi établir une classification du trafic en fonction de l'URL avec la même commande voir l'exemple suivant :

```
class-map match-any scum
match protocol http url "*youtube*"
match protocol http url "*video.google*"
match protocol http url "*myspace*"
```

En outre, la commande **class-map** permet aussi de vérifier si les paquets entrant sont déjà marqués ou pas afin respecter la politique de QoS. L'exemple suivant, nous montre l'utilisation de la commande **class-map** avec la spécification ***« ip dscp »*** dans le but de détecter les paquets déjà marqués avec un dscp = af31 :

```
class-map match-all VOIP
match ip dscp af31
```

b) Création d'une politique de service

Maintenant qu'on a différencié le trafic on doit partager la bande passante de notre routeur. C'est pourquoi on doit utiliser des politiques de priorités (**policy-map**). C'est à partir du moment où on utilise les **policy-map**, qu'effectivement on met en place la Qualité de Service voulue.
Une policy-map contient trois éléments : le nom de la politique, les classes associées et les commandes de qualité de service.

Paramètres des Policy-map

routeur(config)#policy-map *nom-de-la-policy-map ;* On spécifie un nom pour la policy-map

routeur(config-pmap)#class *nom-de-la-classe*

On spécifie le nom de la classe sur laquelle on veut appliquer la politique de qualité de service

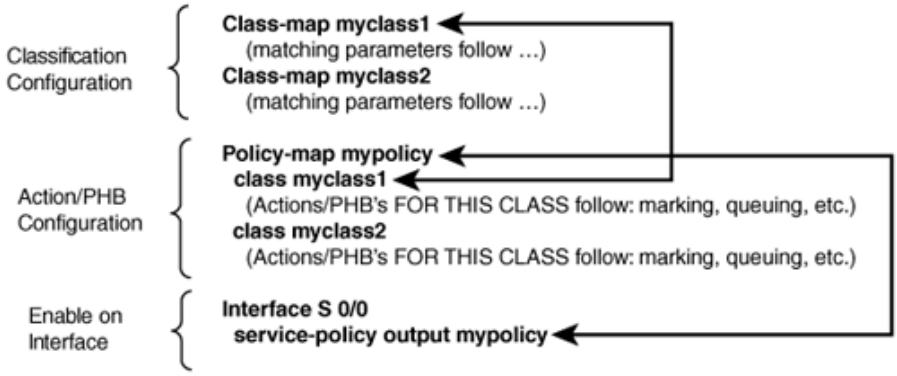
routeur(config-pmap-cmap)#bandwidth *debit en kbps ou pourcentage*

On spécifie la bande passante du routeur qu'on veut allouer à cette classe

routeur(config-pmap-cmap)#pritority *en kbps ou en percentage*

On spécifie pour la classe une bande passante avec un niveau de priorité élevé. Cette commande est en général utilisée pour le trafic temps réel.

Les commandes MQC et leurs corrélations sont montrées dans la figure suivante :



Exemple : Dans l'exemple suivant, une politique de QoS est créé pour attribuer 35% du débit sortant au trafic web.

```
policy-map inbound-internet
class web-traffic
bandwidth percent 35
```

Pour afficher la configuration actuelle du routeur il suffit d'utiliser les commandes suivantes :

```
show policy-map <policy-map-name>
show class-map <class-map-name>
show policy-map interface <interface>
show interface <interface>
```

Scénario 1 :

Nous allons configurer le routeur **R1** afin de différencier le trafic **VOIP** des autres trafics réseau.

Questions :

a. Est-il possible de filtrer les paquets avec la commande « **access-lists** » on se basant sur le champ DSCP? Si oui donner la commande qui permet de filtrer les paquets dont le DSCP est marqué "EF" (Expedited Forwarding).
b. Sur un routeur donné R1, comment peut-on marquer les paquets "SCCP" destinés ou originaire du routeur R1 pour leur attribuer un niveau de Precedence IP 6?

Scénario 2 :

Créer une classe de QoS qui possède trois niveaux de priorité : le premier niveau bénéficie de 30% de la bande passante (réservée pour le trafic VOIP), le deuxième niveau bénéficie de 10% de la bande passante (réservée pour le trafic WEB) et enfin le troisième niveau de 10% de la bande passante (réservée au trafic ICMP). Vous devrez mettre en place cette politique de QoS. Toutes les commandes et l'analyse des résultats doivent être prises en compte dans le rapport. Les étapes suivantes sont à titre indicatif :

1. Créez une ***extended access-list*** permettant d'identifier les paquets VOIP, WEB et ICMP grâce à leur numéro de port
2. Définissez une classe de trafic utilisant votre ***access-list*** avec la commande ***class-map*** afin de classifier les paquets
3. Affectez une réserve de bande passante aux paquets appartenant à votre classe de trafic avec la commande ***policy-map***
4. Affectez la politique de trafic aux sorties des interfaces avec la commande ***service-policy***
5. Testez cette configuration via la génération de trafic réseau ftp, web et ICMP

Remarque : La somme des réservations de la bande passante ne doit pas dépasser le seuil de 75%, car 25% de bande passante est réservée au trafic Best Effort et aussi au routage et à la gestion du réseau.

Scénario 3 :

Dans l'exercice précédent une différentiation entre le PC1 et le Laptop0 n'est pas considéré. Nous avons besoin effectuer cette différence car le PC1 qu'il doit avoir 2 fois plus de bande passante que le Laptop0. Changez la configuration pour pouvoir assurer ce service via l'utilisation d'***access-list***.

Scénario 4 :

Dans cette partie, le routeur R2 doit appliquer sa propre politique de service (sans prendre en considération la politique de service du routeur R1) sur les paquets déjà marqués afin d'augmenter la priorité (**AF21** et **AF11** pour les flux FTP dont la source est le **PC1** et **Laptop0** respectivement).

Remarque : Afin de convertir la notation de la classe AFxy en valeur décimale, vous pouvez utiliser la formule suivante **: « 8x + 2y = valeur décimale».**
Exemple pour la classe AF41 : (8*4)+(2*1) = 34