CTRL-TP: CGR 2017/2018 S1

# Consignes :

1. **Les documents papiers uniquement sont autorisés.**
2. Démarrer votre ordinateur et choisir le système **Ubuntu**
3. Utiliser votre login/mdp pour ouvrir votre session
4. Dans cet examen on vous demande de compléter la configuration du réseau dans le fichier CTRL-TP-CGR-17-18-S1.pkt disponible sur le site https://www.netacad.com/ dans le module 3IRC-17-18-CGR -> Fichier->CPE-FILES->CTRL-TP
5. Utiliser le simulateur « Packet Tracer v7 » pour la configuration du réseau (lancer dans un termina l la commande suivante : /softwares/INFO/pt/packettracer&)
6. Sauvegarder votre travail au fur et à mesure avec un nom de **fichier différent à chaque sauvegarde (exemple  ctr-tp-nom-v0, ctrl-tp-nom-v1, etc…)**
7. A la fin du contrôle il faut déposer le fichier packet tracer complété avec les configurations demandées sur le dépôt de fichiers ***Dépôt-CTRL-TP-S1*** (pour y accéder choisir « tâches » dans le menu gauche du module 3IRC-17-18-CGR ).
8. Durée conseillée : 2h

# Travail demandé

**Il est impératif de respecter le plan d’adressage IP indiqué dans la Figure-1 (indiqué également dans le fichier .pkt)**

## 1ère partie : Configurer le réseau de CPE (8 points):

1. Configurer les Switchs S1 et S2 comme suit :
   * Création des VLAN 10 et VLAN 20 sur les deux switchs
   * F0/1 à F0/10 en mode « access » dans le VLAN 10
   * F0/11 à F0/20 en mode  « access » dans le VLAN 20
   * F0/21 à Fa0/24 en mode « trunk » avec tous les vlans autorisés
2. Configurer R1 pour permettre le routage entre le VLAN 10 et le VLAN 20
3. Configurer R2 pour permettre le routage entre le VLAN 10 et le VLAN 20 également
4. Configurer HSRP sur R1 et R2 pour permettre la redondance de Gateway pour le VLAN 10 **et** le VLAN 20.
   * Vous devez optimiser votre configuration pour équilibrer la charge de routage entre R1 et R2
   * A ce stade de configuration tous les PCs du VLAN 10 doivent communiquer avec les PCs du VLAN 20
5. Configurer le routage RIPv2 entre R1, R2 et R3 : Le routeur R3 doit avoir dans sa table de routage une route RIP pour joindre le VLAN 10 et une autre route rip pour joindre le VLAN20

## 2ème partie : Configurer le réseau de l’INSA (8 points)

1. Configurer le switch S3 comme suit :
   1. Création des VLANs 160 et VLANs 161
   2. F0/1 à F0/10 en mode « access » dans le VLAN 160
   3. F0/11 à F0/20 en mode  « access » dans le VLAN 161
   4. F0/21 à Fa0/24 en mode « trunk » avec tous les VLANs autorisés
2. Configurer le switch S4 comme suit :
   1. Création des VLAN162 et VLAN163
   2. F0/1 à F0/10 en mode access dans le VLAN 162
   3. F0/11 à F0/20 en mode access dans le VLAN 163
   4. F0/21 à Fa0/24 en mode trunk avec tous les VLANs autorisés
3. Configurer le routeur R4 pour faire le routage entre les VAN160 et VLAN161
   1. A ce stade les PCs du VLAN160 doivent pouvoir communiquer avec les PCs du VLAN161
4. Configurer le routeur R5 pour faire le routage entre les VAN162 et VLAN163
   1. A ce stade les PCs du VLAN162 doivent pouvoir communiquer avec les PCs du VLAN163
5. Configurer OSPF sur les routeurs R3, R4, et R5 comme suit :
   1. R3 doit être le routeur désigné DR sur le segment LAN du Switch0 (Le réseau d’interconnexion entre les 3 routeurs)
   2. Les VLAN160 et VLAN161 sont dans la zone OSPF **1**
   3. Les VLAN162 et VLAN 163 sont dans la zone OSPF **2**
   4. Le réseau d’interconnexion entre les 3 routeurs (192.168.1.0**/29**) est dans la zone OSPF **0**
   5. R3 doit avoir dans sa table de routage 2 routes OSPF :
      1. La première route OSPF est vers le préfixe 160.1.0.0/23 (qui résume le VLAN160 et le VLAN161)
      2. La 2ème route OSPF est vers le préfixe 160.1.2.0/23 (qui résume le VLAN162 et le VLAN163)
   6. A ce stade tous les PCs des VLAN160, VLAN161, VLAN162, et VLAN163 doivent communiquer ensemble

## 3ème partie : Configurer la redistribution des routes (4 points)

1. Configurer la redistribution des routes entre le réseau de CPE et réseau de l’INSA pour permettre à tous les PCS des deux réseaux de communiquer ensemble

## 4ème partie (optionnelle : donnera un bonus de 3 points)

1. Sécuriser l’échange OSPF entre R3,R4 et R5 (Authentification)
2. Optimiser et sécuriser le routage OSPF sur R4 et R5 (commande network et Passive-interface)
3. Optimiser et sécuriser le routage RIP sur R1 et R2 (commande network et Passive-interface)
4. Implémenter un mécanisme de track avec HSRP (Avec Packet tracer seul le track d’une interface est possible)