CTRL-TP: CGR 2017/2018 S2

# 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-S2.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 terminal 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-S2***(pour y accéder choisir « tâches » dans le menu gauche du module 3IRC-17-18-CGR ).
8. Durée : 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 DMZ (8 points):

1. Configurer les Switchs S3 et S4 comme suit :
   * Création des VLAN 10 et VLAN 11 sur les deux switchs
   * F0/1 à F0/12 en mode « access » dans le VLAN 10
   * F0/13 à F0/24 en mode  « access » dans le VLAN 11
   * G0/1 et G0/2 en mode « trunk » avec tous les vlans autorisés
2. Configurer R4 et R5 pour permettre le routage entre le VLAN 10 et le VLAN 11
3. Configurer HSRP sur R4 et R5 pour permettre la redondance de Gateway pour le VLAN 10 **et** le VLAN 11.
   * Vous devez optimiser votre configuration pour équilibrer la charge de routage entre R4 et R5
   * A ce stade de configuration tous les PCs du VLAN 10 doivent communiquer avec les PCs du VLAN 11
4. Configurer le routage RIPv2 entre R3, R4, R5 et R6 : Le routeur R6 doit avoir dans sa table de routage une route RIP pour joindre le VLAN 10 et une autre route RIP pour joindre le VLAN11

## 2ème partie : Configurer le réseau des collaborateurs (8 points)

1. Configurer le switch S1 comme suit :
   1. Création des VLAN 40 et VLAN 50
   2. F0/1 à F0/12 en mode « access » dans le VLAN 40
   3. F0/13 à F0/24 en mode  « access » dans le VLAN 50
   4. G0/1 et G0/2 en mode « trunk » avec tous les vlans autorisés
2. Configurer le switch S2 comme suit :
   1. Création des VLAN 20 et VLAN 30
   2. F0/1 à F0/12 en mode « access » dans le VLAN 20
   3. F0/13 à F0/24 en mode  « access » dans le VLAN 30
   4. G0/1 et G0/2 en mode « trunk » avec tous les vlans autorisés
3. Configurer le routeur R1 pour faire le routage entre les VAN 40 et VLAN 50
   1. A ce stade les PCs du VLAN 40 doivent pouvoir communiquer avec les PCs du VLAN 50
4. Configurer le routeur R2 pour faire le routage entre les VAN 20 et VLAN 30
   1. A ce stade les PCs du VLAN 20 doivent pouvoir communiquer avec les PCs du VLAN 30
5. Configurer OSPF sur les routeurs R1, R2, et R3 comme suit :
   1. R3 doit être le routeur désigné DR sur le segment LAN du switch S5 (Le réseau d’interconnexion entre les 3 routeurs)
   2. Les VLAN 20 et VLAN 30 sont dans la zone OSPF **1**
   3. Les VLAN 40 et VLAN 50 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 172.16.0.0/22 (qui résume le VLAN 20 et le VLAN 30)
      2. La 2ème route OSPF est vers le préfixe 172.16.4.0/23 (qui résume le VLAN 40 et le VLAN 50)
   6. A ce stade tous les PCs des VLAN 20, VLAN 30, VLAN 40, et VLAN 50 doivent communiquer ensemble

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

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