Descriptif des épreuves:

Il s'agit ici de la résolution des épreuves pour le joueur 1. Elle est presque identique pour les autres joueurs, il suffit juste de modifier les adresses IP. Par exemple, 191.1.1.254 pour le joueur 1 devient 192.1.1.254 pour le joueur 2. Pour que les épreuves se déroulent normalement, il est important que la session serveur des organisateurs soit ouverte avant toutes les sessions clientes.

Pour connecter les sessions sur différents postes, l'utilisation du serveur barn-e-01 a été sélectionnée, mais s'est avérée ne pas convenir, potentiellement en raison des délais de transmissions entre le serveur et les machines utilisées. Parmi les solutions alternatives, on aurait pu créer un réseau privé, où une machine des organisateurs aurait servi de routeur d'un réseau local, tandis que les sessions clients et serveur aurait tourné sur les machines personnelles, ou encore créer directement un réseau physique entre les machines. Des applications comme PTBridge auraient ensuite relier les sessions Packet Tracer au réseau crée.

Partie I : Client

Le but de cette partie est d'atteindre la fin du réseau présenté afin d'accéder à des ressources indispensables pour continuer l'activité.

Épreuve 1 : Lancement d'un service DHCP

Le joueur peut tout d'abord accéder au *PC joueur* et remarquer qu'il ne dispose pas d'adresse IP. Il doit donc configurer un serveur DHCP pour mettre en place un adressage dynamique.
Pour cela il doit mettre en place le service dans : Server1 > Services (figure 1).

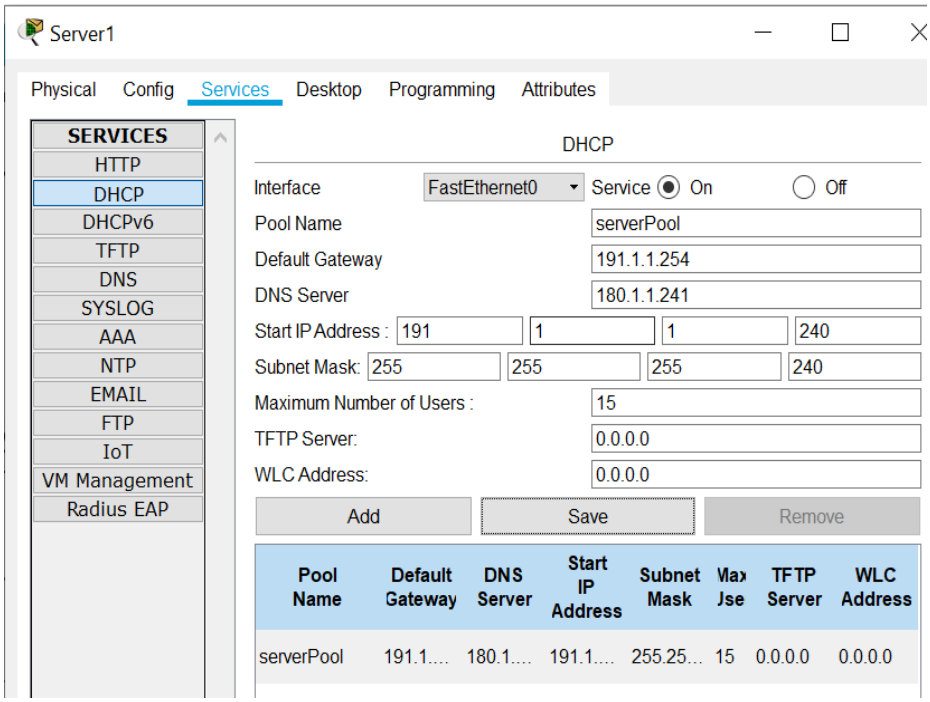

Figure 1 : Configuration du service DHCP pour le joueur 1

Il peut ensuite vérifier que le service est bien allumé, et il peut alors demander une adresse depuis le *PC joueur.* Pour cela il va dans : PC joueur > Desktop > IP Configuration (Figure 2).

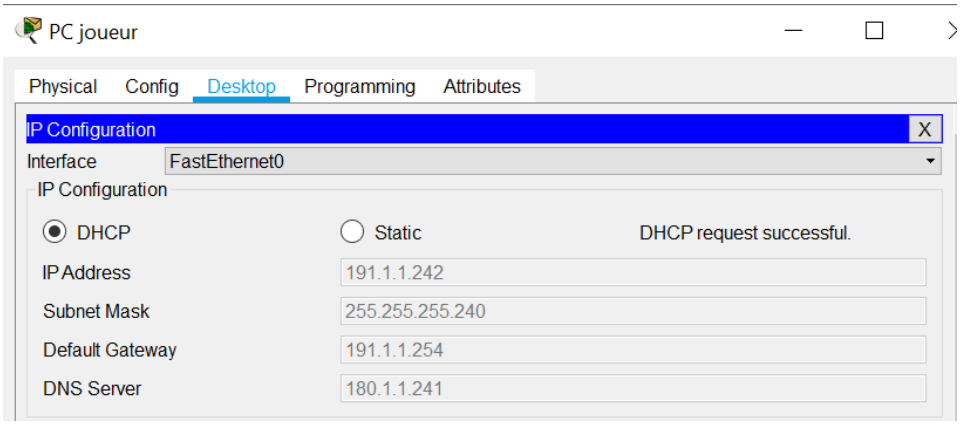

Figure 2 : Requête d'une adresse IP au serveur DHCP.

L'épreuve 1 est alors terminée, il peut donc passer à l'épreuve suivante.

Épreuve 2 : Configuration d'une interface d'un routeur et d'une route

Après l'épreuve 1 le joueur peut explorer le réseau en envoyant des « ping » aux différentes machines : 191.1.1.255 (Serveur1 : 191.1.1.241 et Router1 : 191.1.1.254), 191.2.1.254, 191.2.1.253 et 191.3.1.254. Les machines pourront être facilement identifier grâce à la construction des adresses IP donnée dans l'énoncé. En revanche, il n'arrivera pas à accéder à l'adresse 191.3.1.254, il sera donc bloqué et recevra la réponse de la figure 3.

```
C:\>ping 191.3.1.254

Pinging 191.3.1.254 with 32 bytes of data:

Reply from 191.2.1.253: Destination host unreachable.
Reply from 191.2.1.253: Destination host unreachable.
Reply from 191.2.1.253: Destination host unreachable.
Request timed out.

Ping statistics for 191.3.1.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 3 : Réponse aux pings sur les machines après le routeur 2

Il faudra donc qu'il tente un telnet sur l'adresse 191.2.1.253 pour prendre le contrôle du routeur, explorer ses configurations avec la commande **show running-config** et après donner une adresse à la seconde interface de se routeur et ajouter la route manquante (Figure 4).

```
C:\>telnet 191.2.1.253
Trying 191.2.1.253 ...Open
System Bootstrap, Version 12.1(3r)T2, R


Router>en
Password:
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet1/0
Router(config-if)#ip address 191.3.1.254 255.255.255.248
Router(config-if)#no shutdown

Router(config-if)#exit
Router(config)#
Router(config)#ip route 190.1.1.248 255.255.255.248 191.3.1.252
Router(config)#exit
Router#exit

[Connection to 191.2.1.253 closed by foreign host]
C:\>
```

Figure 4 : Configuration d'une interface de routeur et d'une route après un telnet sur l'adresse 191.2.1.253

L'interface FastEthernet1/0 permet de poursuivre dans le réseau et la route permet d'accéder au réseau d'écoute pour intercepter un message contenant des informations. En effet le message intercepté permettra d'obtenir la deuxième moitié d'un mot de passe (jhg2) dès qu'il sera montré au maître du jeu. Ce mot de passe servira à établir la connexion avec le multiuser. L'épreuve 2 et alors terminée.

Épreuve 2 bis : Interception d'un message

En découvrant le réseau 190.1.1.248 et les machines qui s'y trouve, le joueur doit comprendre qu'il doit écouter un échange de message entre *PC* et *Server 2*. Il doit alors configurer le Switch4. En revanche, il ne peut pas trouver l'adresse du switch il doit donc tenter un telnet sur les 6 adresses possibles du réseau. Il pourra donc prendre le contrôle de la machine 190.1.1.251 et entrer les lignes de commandes pour configurer les interfaces du Switch4 (Figure 5).

```
C:\>telnet 190.1.1.251
Trying 190.1.1.251 ...Open


Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#monitor session 1 source interface fastethernet0/1
Switch(config)#monitor session 1 source interface fastethernet0/2
Switch(config)#monitor session 1 destination interface fastethernet0/4
Switch(config)#exit
Switch#exit

[Connection to 190.1.1.251 closed by foreign host]
C:\>
```

Figure 5 : Configuration des interfaces du Switch4 pour le port mirroring

En prenant le contrôle du commutateur et en explorant sa configuration il pourra donc remarquer que les 4 premières interfaces FastEthernet sont actives mais seulement 3 sont reliées a des machines comme le montre la commande **show mac address-table**. Ainsi le joueur peut facilement identifier

que le Sniffer est connecté à l'interface FastEthernet0/4 et mettre cette dernière en destination. Avec les adresses mac il peut ensuite distinguer *Router3*, *PC* et S*erver 2*, il peut donc trouver les 2 interfaces à mettre en source. S'il n'arrive pas précisément à distinguer les interfaces à mettre en source il peut tout simplement mettre les 3 autres en sources après avoir trouvé celle du *Sniffer*. Il n'a plus qu'a allumer le *Sniffer* et lire les trames qu'il vient de détourner puis il pourra poursuivre sa progression dans le réseau.

Épreuve 3 : Configuration d'un VLAN

Une fois encore le joueur doit effectuer plusieurs pings jusqu'à tomber sur le même message que dans la figure 3 mais cette il s'agit d'une réponse provenant de l'adresse IP : 191.3.1.253, il devra donc également effectuer un telnet sur cette adresse. Une fois qu'il aura pris le contrôle du router il verra un message s'afficher lui indiquant ce qu'il doit faire. Il devra configurer l'interface du routeur donnant accès au VLAN 20 en s'inspirant de celle donnant accès au VLAN 10. Ainsi il écrira les commandes de la figure 6. Pour cette épreuve le joueur devra prêter attention à toutes les informations qu'il peut trouver non seulement dans la configuration du router mais également dans les notes qui se trouvent autours du réseau. Il devra également penser à explorer le VLAN 10 pour trouver l'adresse du *Server3* et la saisir dans le Web Browser du *PC joueur* pour obtenir la première moitié du mot de passe nécessaire pour établir la connexion avec le multiuser après avoir configurer le VLAN 20. Il pourra alors effectuer des pings sur les machines du côté serveur en suivant la même logique pour les adresses IP et tenter de prendre le contrôle de ces dernière pour pouvoir faire un ping de « broadcast » pour explorer plus facilement le réseau et également pour obtenir l'information cachée dans le « message of the day » de l'interface du router qui connecte le serveur et le joueur. Cette information lui permettra d'envoyer un mail pour pouvoir accéder à la deuxième partie du jeu. (Il est possible que le renvoi automatique du mail soit un peu long, il est donc préférable de « pinger » le serveur DNS : 180.1.1.241 et le serveur mail : 180.2.1.253 avant).

```
C:\>telnet 191.3.1.253
Trying 191.3.1.253 ...Open

Ce routeur donne acces a deux VLAN. Le premier contient des informations
necessaires pour continuer. Configurez l'acces au second VLAN depuis ce
routeur.



Router>en
Password:
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet1/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 191.4.20.254 255.255.255.252
Router(config-subif)#no shut
Router(config-subif)#exit
Router(config)#exit
Router#exit

[Connection to 191.3.1.253 closed by foreign host]
C:\>
```

Figure 6 : Commandes pour la configuration du VLAN 20

Figure 7: Message of the day

Partie II : Serveur

Le but de cette partie est d'explorer un réseau à l'aveugle (où il faudra donc progresser en observant la configuration des routeurs accessibles, ou bien en devinant les réseaux suivants à quelques occasions), ce afin d'atteindre une épreuve d'affrontement dans laquelle il faudra bloquer les autres joueurs pour se placer en premier. On a deux épreuves de ce type, la deuxième se débloquant une fois la première résolue.

Pour cette partie, seul le sous-réseau 19X.4.1.224 /27 prend en compte le numéro du joueur, car il s'agit du seul réseau à communiquer avec la partie commune du serveur. Les autres sous-réseaux utilisent des adresses en 191.

Le mail reçu à la fin de la partie client indique la marche à suivre pour commencer le début de la partie serveur. La connexion au serveur se fait via plusieurs points d'accès Wifi, eux-mêmes connecté à des emplacements différents du serveur. Pour commencer, on configure donc un point d'accès Wifi :

- Laptop - Physical : éteindre, enlever l'interface, ajouter le module WPC300N, rallumer

(Il faudra répéter les instructions suivantes à chaque changement de point d'accès)

- Laptop - Desktop - Wireless : Sélectionner la borne où se connecter (Wifi1 libre, mot de passe nécessaire pour les autres)

- Laptop - Config : Récupérer adresse IP dans cluster connecté, la rajouter dans Laptop

- Laptop - Desktop - Terminal : ping broadcast sur réseau local pour trouver adresse Gateway (+rajout dans Config)

- Ouverture accès multiserveur dans cluster connecté

Dans cette partie, on traitera chaque point d'accès comme une épreuve différente.

Connexion Wifi1 (pas de mot de passe) :

On explore un réseau contenant plusieurs serveurs. Parmi ceux-ci, deux contiennent des informations nécessaires pour progresser :

- Laptop - Desktop - Terminal : telnet 191.1.1.253 + enable(cisco) + sh runn : On identifie les réseaux connectés (puis ping broadcast 191.2.1.255) et les autres machines dans ce réseau

- Laptop - Desktop - Terminal : telnet 191.2.1.253 + ping broadcast 191.3.1.255 : déduction du réseau suivant

- Laptop - Desktop - Web : ouvrir chaque adresse du réseau 191.3.1.124/25
191.3.1.202 -> mot de passe wifi "WiFiAccess"
191.3.1.167 -> IV du déchiffrement final "20f255206a4d74e2da8200f4ceb90cba"

Connexion Wifi2 (mot de passe WiFiAccess) :

On répète le protocole d'exploration de l'épreuve précédente, en constatant que certains réseaux ne répondent pas à ce point d'accès. On met aussi à profit le programme du serveur mail, permettant de changer la réponse en fonction de l'objet des mails reçus.

- Laptop - Desktop - Terminal : telnet 191.4.1.254 + enable(cisco) + sh runn : On identifie les réseaux connectés (puis ping broadcast 191.5.1.255) et les autres machines dans ce réseau

- On répète l'étape précédente pour 191.5.1.253 et 191.6.1.251

- Laptop - Desktop - Web : ouvrir adresse 191.7.1.241 -> objet de mail "access"

- Laptop - Desktop - Mail : envoyer mail avec objet access : mot de passe "YouShallNotPass" en réponse

Connexion Wifi4 (mot de passe YouShallNotPass) :

Cette fois, on se reconnecte au même réseau que pour Wifi2, mais les machines accessibles ne sont plus les mêmes. On commence aussi à ajouter du chiffrement aux messages à récupérer (le logiciel Cyberchef a été utilisé pour coder et résoudre ces chiffrements et encodage).

- Laptop - Desktop - Terminal : telnet 191.9.1.254 + enable(cisco) + sh runn : On identifie les réseaux connectés (puis ping broadcast 191.5.1.255) et les autres machines dans ce réseau

- On répète l'étape précédente pour 191.10.1.253 et 191.6.1.250

- Laptop - Desktop - Web : ouvrir adresse 191.11.1.241 -> chiffrement base64 "QXplcnR5dWk=" du mot de passe Azertyui

Connexion Wifi5 (mot de passe Azertyui) :

Les méthodes d'explorations restent les mêmes que pour les épreuves précédentes. On fait de nouveau appel au serveur mail ainsi qu'au chiffrement.

- Exploration du réseau débloqué

- Laptop - Desktop - Terminal : telnet 191.13.1.253 + lecture du message of the day : chiffrement hexa "70617373776f7264" de l'objet de mail password

- Laptop - Desktop - Mail : envoyer mail avec objet password : chiffrement charcode (colon,32) "2f:3e:24:39:3i:31:39:3k:24:35:2c:35:3c:36:39:3h:3l:35" du mot de passe OnDiraitDeLelfique

Connexion Wifi6 (mot de passe OnDiraitDeLelfique)

Cette partie consiste en une simple exploration, avec un déchiffrement plus complexe.

- Exploration du réseau débloqué

- Laptop - Desktop - Web : ouvrir adresse 191.14.20.249 -> chiffrement hexa+base64 "NDUsNzAsNzMsNzQsNjUsNjksNmUsNjQsNjksNjQsNmUsNzQsNmIsNjksNmMsNmMsNjgsNjksNmQsNzMsNjUsNmMsNjY=" du mot de passe Epsteindidntkillhimself

Connexion Wifi3 (mot de passe Epsteindidntkillhimself) :

Pour cette épreuve, tout en récoltant des informations supplémentaires dans les serveurs, on va contourner un routeur qui bloquait la progression depuis Wifi2 avec une liste d'accès pour le débloquer.

- Exploration du réseau débloqué

- Laptop - Desktop - Web : ouvrir adresse 191.20.1.241 -> mot de passe telnet "C1SC0"

- Laptop - Desktop - Web : ouvrir adresse 191.20.1.241 -> 1ere partie du message du déchiffrement final "bc848746f80d211aee3a2c87e84b0d406"

- Laptop - Desktop - Terminal : telnet 191.21.1.254 + enable(C1SC0) : suppression de la liste d'accès 1 de l'interface fastEthernet0/0

Reconnexion Wifi2 :

L'accès étant été ouvert depuis Wifi3, on poursuit l'exploration du réseau. On récupère les dernières information relatives au déchiffrement final, puis on se connecte à un routeur, uniquement accessible depuis Wifi2, menant au premier affrontement.

- Exploration du réseau débloqué

- Laptop - Desktop - Web : ouvrir adresse 191.23.1.253 -> 2eme partie du message du déchiffrement final "a956f6be5de543284d54f170f993f83"

- Laptop - Desktop - Web : ouvrir adresse 191.24.1.241 -> clé du déchiffrement final "c5272bfc8aac476bae11f448e5dfdcecbae365b315d4d93133d97afbfc93c9553"
- Déchiffrement final (AES) : mot de passe telnet "FightToTheFinish"

- Laptop - Desktop - Terminal : telnet 191.21.1.250 (uniquement possible depuis Wifi2) + enable (FightToTheFinish) + sh runn: On identifie les réseaux

connectés (puis ping broadcast 180.X0.1.255) et les autres machines dans ce réseau

Affrontement 1 : VLAN

Chaque participant accède à l'affrontement depuis sa propre interface virtuelle, le premier doit fermer celle des autres avant d'être lui-même bloquer.

Une fois le premier affrontement terminé, la première place a été décidé, et les organisateurs révèlent le mot de passe telnet « NotAKnot », que les participants doivent utiliser pour débloquer le réseau au-delà du routeur 191.6.1.249. Celui-ci avait déjà été observé lors de l'exploration et contenait un message annonçant qu'il s'agirait de l'accès au deuxième affrontement. Cette nouvelle partie du réseau sera accessible exclusivement depuis Wifi2 et Wifi4.

Connexion Wifi2 :

On commence par simplement explorer le réseau accessible pour y lire le contenu d'un serveur.

- Exploration du réseau débloqué

- Laptop - Desktop - Web : ouvrir adresse 191.26.1.241 -> clé du déchiffrement final "929f13dd8ca95f55b5745cb2ca93e9012281fc9bd0a32f5f651d3d0417296715"

Connexion Wifi4 :

On doit de nouveau contourner un routeur pour permettre à Wifi2 de pouvoir l'emprunter.

- Exploration du réseau débloqué

- Laptop - Desktop - Web : ouvrir adresse 191.27.1.249 -> IV du déchiffrement final "8a1531f207f355cc51bf29ee20925fe1"

- Laptop - Desktop - Web : ouvrir adresse 191.28.1.226 -> IV du déchiffrement final "d35a2d1d9618e664316fe03ffec5c4da120c5ef2af2934788090c16259254204"

- Déchiffrement final (AES) : mot de passe telnet "AccessToSecondKnot"

- Laptop - Desktop - Terminal : telnet 191.21.1.254 + enable(AccessToSecondKnot) : Activation de l'interface FastEthernet 0/0

Connexion Wifi2 :

On passe par l'accès débloquer pour progresser vers l'affrontement final.

- Exploration du réseau débloqué

- Laptop - Desktop - Terminal : telnet 191.29.10.254 (uniquement possible depuis Wifi2) +
enable (cisco) + sh runn: On identifie les réseaux connectés (puis ping broadcast 181.1.1.255) et les autres machines dans ce réseau

Affrontement 2 : Liste d'accès

Pour cet affrontement, tous les joueurs arrivent sur le même réseau et se connecte au routeur de sortie depuis une même interface. Afin de bloquer les autres joueurs, le premier doit donc créer une liste d'accès sur cette interface qui ne laisserait le passage qu'à lui-même.

- Laptop - Desktop - Terminal : telnet 200.1.1.254 (uniquement possible depuis Wifi2)
enable (cisco)
configure terminal
access-list 1 permit 19X.4.1.224 0.0.0.31
interface fastethernet 0/0
ip access-group 1 in

Une fois cet affrontement terminé, le joueur en deuxième place a été décidé, et on peut mettre fin à l'activité.