R2.04 -- TP 2

Préambule

La plupart de nos TPs dans les deux ressources de réseaux, R2.04 et R2.05 seront réalisés en utilisant l'émulateur Kathará. Cet outil, conçu à l'Université Roma 3, nous permet de tester une configuration en réseau avant de la déployer.

Trouvez en /VM-ROOT/VirtualBox/ la machine virtuelle Debian11. Lorsque la machine virtuelle affiche son premier écran, choisissez l'option d'initialiser des nouvelles adresses MAC pour chaque interface réseau.

Votre VM s'affichera en mode plein écran, ce que vous cachera l'image sur votre machine physique. Pour jongler entre les deux vous pouvez utiliser CTRL (de droite) + h.

Choisissez, à l'intérieur de la VM Debian de démarrer le système d'exploitation Debian Linux. Une fois l'installation réalisée vous serez dans votre environnement de travail.

La première chose à faire sera d'ouvrir un terminal et de prendre les privilèges de `root` en utilisant la commande `su`. Tapez le mot de passe `iut`. Sur votre Desktop (dans le répertoire Bureau) créez un dossier appelé LabTP1. C'est dans ce répertoire que vous allez travailler lors de cette session de TP.

Exercice I : Découverte et configuration d'un lab Netkit

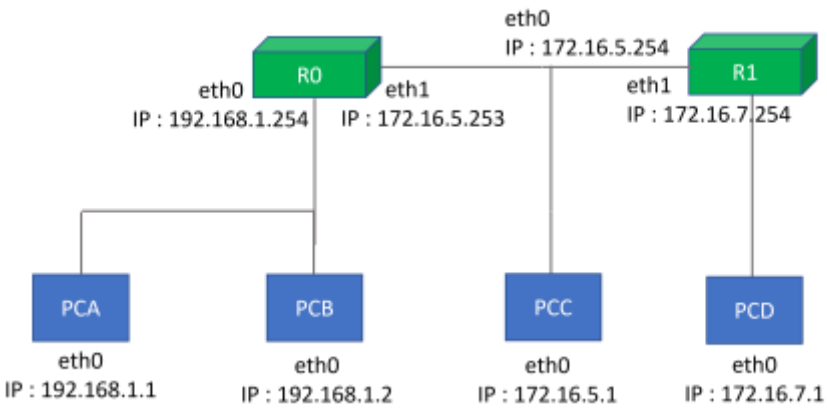
Lors de ce premier exercice, le but sera d'apprendre comment marche Kathará.

Les projets Kathará se structurent dans des labs. Un lab Kathará aura un fichier de configuration qui spécifie premièrement la topologie réseau : c'est-à-dire comment les machines se regroupent dans des domaines de collision différents, etc. Chaque machine manipulée par Kathará est une machine virtuelle, localisée dans un container Docker.

En soi, et par défaut, le lab Kathará sera isolé de la machine physique sur laquelle on fait fonctionner Kathrá. Mais, si on le souhaite (par exemple pour donner un accès Internet aux machines virtuelles dans le lab) on peut mettre en place un *pont* entre les deux.

Pour ce TP, nous avons la topologie suivante.

1. Quels sont les trois réseaux indiqués dans la figure ci-dessus ? Quelles machines font partie de



chaque domaine de collision ?

Le fichier qui indique, dans Kathará, la configuration de réseau, est un fichier nommé lab.conf. Dans ce fichier, on indique quelle interface de quel réseau fait partie de quel domaine de collision, on peut indiquer la configuration de chaque machine (capacité de mémoire, etc.), si elles utilisent des adresses IPv4 ou IPv6, et finalement on peut également réaliser un pont avec la machine physique.

Dans la figure ci-dessus, les machines R0 (interface eth0) et les machines PCA et PCB sont dans un même domaine de collision. Ceci est indiqué dans le fichier lab.conf. par le code suivant :

```
pca[0] = net0
pcb[0] = net0
r0[0] = net0
```

Ceci indique le fait que les interfaces eth0 et PCA, PCB et R0 sont dans un même domaine de collision, qu'on appelle net0 (mais on aurait pu l'appeler autrement aussi !) En Kathará, les interfaces sont nommées eth0 (indiquée par le [0] à côté des machines), puis eth1, eth2, etc.

Ne pas utiliser des majuscules dans le code de lab.conf, sauf s'il s'agit d'une instruction dédiée.

2. Pouvez-vous compléter le reste du contenu que nous devons mettre dans le fichier lab.conf ?

3. Dans le répertoire LabTP1, créez un fichier lab.conf et mettez le texte qui fera la configuration de la topologie ci-dessus. Sauvegardez le fichier.

4. Avec l'aide de votre terminal, allez dans le répertoire LabTP1. Tapez le mot kathara. Que voyez-vous ? Pouvez-vous identifier et taper l'instruction à taper pour démarrer le lab ? Quelle est l'instruction que vous venez de taper ? (Déboguez votre fichier si le démarrage ne réussit pas).

En dehors de l'instruction qui va démarrer votre lab, vous aurez également besoin de ces deux commandes : `kathara lclean` et `kathara wipe`, notamment lorsque vous devez redémarrer le lab (pour être sûrs d'avoir éteint toute trace de machine virtuelle restante avant de la rédémarrer).

5. Kathará va créer des terminaux pour chaque machine du lab. Sur le terminal correspondant à la machine R1, tapez une instruction, qui vous permettra de voir toutes les interfaces de cette machine avec leurs adresses IP. Quelle est cette instruction et quels sont les résultats ?

Normalement là nous avons un lab Kathará fonctionnel -- mais aucune machine n'a pas été configurée. Nous pourrions effectuer cette configuration à la main (sur chaque machine), mais dans ce cas-ci, la configuration sera temporaire seulement. Nous voulons, au contraire, que la configuration soit pérenne. Comme ça si on change la topologie (ce qui sera le cas plus tard, les machines commenceront en ayant les adresses et routeurs déjà mis en place).

Ceci se fait en Kathará en mettant en place des fichiers de startup pour chaque machine. Chaque fichier de startup porte le nom de la machine (tel qu'indiqué dans le fichier lab.conf) : la machine pca aura un fichier de configuration pca.startup, etc. Dans ce fichier nous mettrons toutes les instructions que nous

voulons faire exécuter sur la machine après son démarrage (par exemple les instructions ip address, ip route, nécessaire à la configuration et au routage).

6. Préparez les fichiers de configuration pour les machines « utilisateur » : PCA, PCB, PCC et PCD. Les fichiers s'appelleront : pca.startup, pcb.startup, pcc.startup et pcd.startup et seront mis dans le répertoire LabTP1. Les instructions mises dans ces fichiers s'exécuteront au démarrage du lab, avant la création des terminaux pour chaque machine.
   Dans chacun de ces fichiers de configuration, vous allez mettre en place des instructions qui configurent leurs adresses IP, qui activent ces adresses, et qui définissent un routeur par défaut pour chaque machine.

   Quels sont les routeurs par défaut de chaque machine ?

7. Préparez le fichier de configuration pour la machine R0 (r0.startup), selon la figure ci-dessus, tel que : les adresses IP soient configurées ; les interfaces (avec les adresses) soient activées ; et la machine R1 soit utilisée en tant que le routeur par défaut de R0. Quel est le contenu de ce fichier ?

8. Préparez le fichier de configuration pour la machine R1 (r1.startup), selon la figure ci-dessus, tel que : les adresses IP soient configurées ; les interfaces (avec les adresses) soient activées ; et tel que R0 soit le routeur utilisé par R1 pour envoyer des paquets au sous-réseau incluant PCA, PCB. Quel est le contenu du fichier r1.startup ?

9. Une fois les fichiers écrits, redémarrez votre lab. Faites des pings entre chaque paire de machines et déboguez votre configuration si besoin (n'oubliez pas à fermer le lab correctement à chaque fois avant de le redémarrer !)

10. Utilisez la commande ip en dehors de Kathará, dans un terminal sur votre machine virtuelle Debian, pour apprendre la configuration actuelle de la machine hôte, notamment par rapport à quelles interfaces réseau elle peut avoir, quelles adresses IP elle a, etc. Quelle est la configuration actuelle de votre machine ?

Exercice II : tcpdump et les captures Wireshark

Dans cet exercice nous allons analyser les échanges de messages à l'intérieur de Kathará. Ces machines n'ont pas un outil comme Wireshark installé là-dessus, qui pourrait analyser les trames échangées. Cependant, nous pouvons utiliser tcpdump.

1. Sur la machine PCB tapez les commandes suivantes :

   ```
   ip neigh flush all
   tcpdump -i eth0
   ```

   La première commande enlèvera le cache d'adresses MAC que PCB a pu garder pendant les échanges précédents. La deuxième commande mettra en place une capture des trames qui rentrent et sortent du PCB via son interface eth0.

2. Sur PCA faites un ping et un seul (en utilisant l'option -c 1 de la commande ping) vers PCB. Quelle commande avez-vous utilisé ?

3. Sur PCB, utilisez ensuite Ctrl+C pour arrêter la capture tcpdump. Regardez les messages capturés. Quels types de trames voyez-vous ?

4. Maintenant nous allons utiliser une commande de sauvegarde pour tcpdump, qui nous permettra ensuite d'analyser la capture en utilisant le logiciel Wireshark. Sur la machine PCC tapez la commande suivante :

   ```
   tcpdump -i eth0 -w /shared/capturepcc.pcap &
   ```

   Avec le & à la fin de la ligne, nous pouvons nous assurer que le logiciel marche en background, nous permettant de continuer à manipuler la machine.

5. Faites la même chose pour la machine PCD, pour laquelle les données seront sauvegardées dans le fichier capturepcd.pcap .

6. Utilisez la machine PCC pour faire un ping (et un seul) vers PCD. Ensuite utilisez la commande `fg` pour remettre tcpdump en foreground. Arrêtez ensuite la capture avec Ctrl+C. Remettez ensuite tcpdump en foreground de la machine PCD. Finalement arrêtez la capture sur cette machine-ci également.

7. Sur la machine hôte, trouvez les captures, qui seront sauvegardées dans le répertoire du lab. Utilisez Wireshark pour ouvrir les deux captures. Filtrez les paquets ping (rappelez-vous quel protocole encapsule ces messages). Ensuite regardez les adresses sources et destination des paquets ping dans les deux paquets. Que remarquez-vous ?

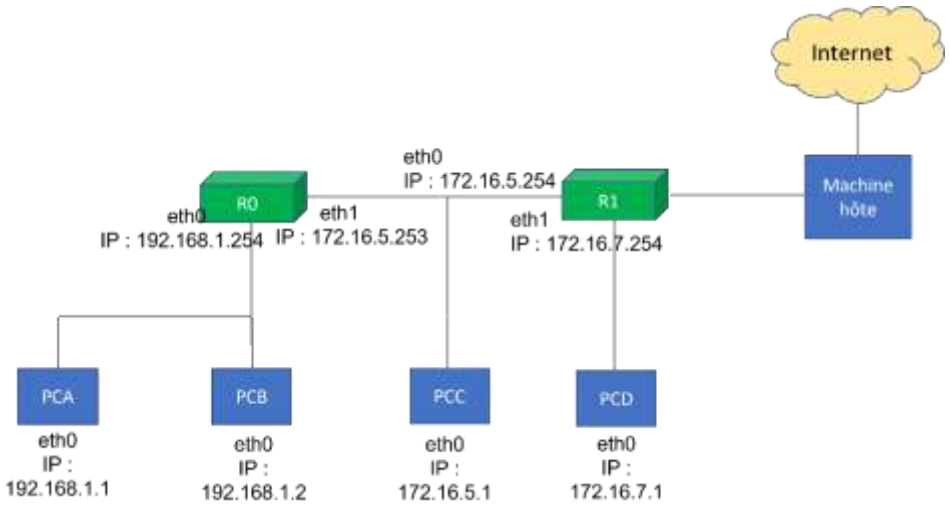
Exercice III : Connecter un lab à la machine hôte

Dans ce deuxième exercice nous allons nous poser la question de comment on peut faire en sorte que les machines puissent avoir accès à l'Internet. Ceci nécessitera des légères modifications à apporter à la configuration du lab et de votre machine.

1. Vous allez travailler sur le PCA. Envoyez un ping vers 8.8.8.8.
    a. Quel est la commande que vous avez utilisée et quel est le résultat ?

    b. Déboguez la situation en utilisant certaines instructions sur les machines PCA et R1, pour montrer où est le problème. Quelles instructions avez-vous tapé ? Quel est votre diagnostique ?

Jusqu'à ce point, notre lab Kathará existait (dans des containeurs) sur notre machine physique. Nous voulons désormais que les machines du lab soient également connectées à la machine hôte -- notamment nous voulons modifier la topologie tel que ci-dessous :



2. Pour connecter le routeur R1 et la machine hôte, nous aurons besoin qu'un pont (bridge) soit établi entre les deux. Modifiez le fichier de configuration du lab (lab.conf) pour ajouter la commande `r1[bridged] = true`.

3. Une fois le lab redémarré, utilisez la commande `ip` pour trouver les interfaces et les adresses IP de votre machine hôte là. Que voyez-vous si vous comparez vos résultats à ceux de l'exercice I, question 10 ?

4. Votre but sera de permettre au ping évoqué à la question 1 de réussir. Quelles modifications devez-vous faire ? Auxquels fichiers ?

5. Avez-vous réussi à faire marcher le routage ? Si c'est le cas, bravo, vous avez fini le TP. Sinon, qu'est-ce qu'il reste encore à faire ?