R2.04 -- TP 2

Préambule

La majorité de nos TPs pour les deux ressources de réseaux, R2.04 et R2.05, ainsi que la SAÉ 2.03 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_LAN. 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.

Vous aurez besoin de vérifier les interfaces de transmission (en cliquant sur l'icone de connectivité en bas à droite et en vous assurant que la première interface pointe vers eth0 et l'autre, vers eth1).

Par la suite, pour l'utilisation de Kathará vous aurez besoin de pouvoir rédiger des fichiers lab.conf et .startup. Pour pouvoir sauvegarder des fichiers, vous devez être root. Tapez la commande `su`. Tapez le mot de passe `iut`. La rédaction des fichiers Kathará se fera exclusivement en Nano. Kathará a du mal à traiter des fichiers écrits dans des éditeurs de type Notepad.

Pour le démarrage de Kathará, par contre, vous devez être non-root.

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.

Préambule : Découverte et configuration d'un lab Kathará

Ouvrez un navigateur. En root, positionnez-vous dans le répertoire LabTP1.

Tapez (en root) `nano lab.conf` . Cette commande va créer le fichier lab.conf et vous permettra de l'éditer, puis de le sauvegarder. Tapez le contenu suivant :

```
pca[0] = net0
pcb[0] = net1
r0[0] = net0
r1[0] = net 1
pcc[0] = net1
```

Puis, sauvegardez-le.

Dans le répertoire LabTP1, sans être en root, tapez `kathara lstart` (puis tapez non pour la question suivante). Kathará va créer des terminaux pour chaque machine du lab.

1. Tapez une commande qui vous permet de visualiser les configurations IP de toutes les interfaces de la machine R0. Quelle est la commande et quel est le résultat ?

   Commande :
   Résultat :

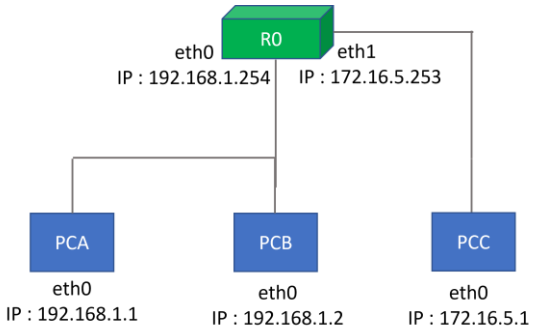
La commande `kathara lstart` n'a fait que démarrer le lab Kathará. Sauf que, dans l'absence de fichiers de startup, aucune configuration n'est réalisée.

2. Configurez, en ligne de commande, les adresses suivantes pour les 3 machines : 192.168.1.1 avec un CIDR de /24 pour PCA, 192.168.1.2 avec un CIDR de /24 pour PCB, 192.168.1.254 pour RO eth0, alors que l'interface eth1 de R0 aura l'adresse 172.16.5.253 avec un CIDR de /24. PCC aura l'adresse IP 172.16.5.1 avec un CIDR en /24.

3. Utilisez une commande qui vous permet de visualiser, sur PCA, toutes les interfaces actives. Quelle est la commande utilisée et quel est le résultat ?

   Commande :
   Résultat :

4. La topologie qu'on veut mettre en place est la suivante :



Normalement cela nous permet de faire un ping de PCA vers PCB.
Faites un ping de PCA vers PCB. Quelle est la commande à utiliser et quel est le résultat ?
Notez ces résultats dans votre cahier de débogage.

Commande :
Résultat :

5. Utiliser le cahier de débogage pour déboguer le problème. Dans un premier temps identifiez le problème : il s'agit d'un problème de ping entre deux machines situées dans un même réseau. Puis, trouvez les outils à potentiellement utiliser pour trouver le souci. Vous allez devoir vérifier l'adresse, le fait que l'interface est active, puis vérifier les fichiers de configurations Kathará. Faites en sorte que la topologie indiquée soit cohérente avec vos configurations.

6. Refaites un ping de PCA vers PCB. Après avoir modifié la configuration pour assurer qu'un ping puisse passer sans souci, configurez sur PCA une route par défaut via R0. Quelle est la commande à utiliser et sur quelle machine ? Quel est le résultat ?

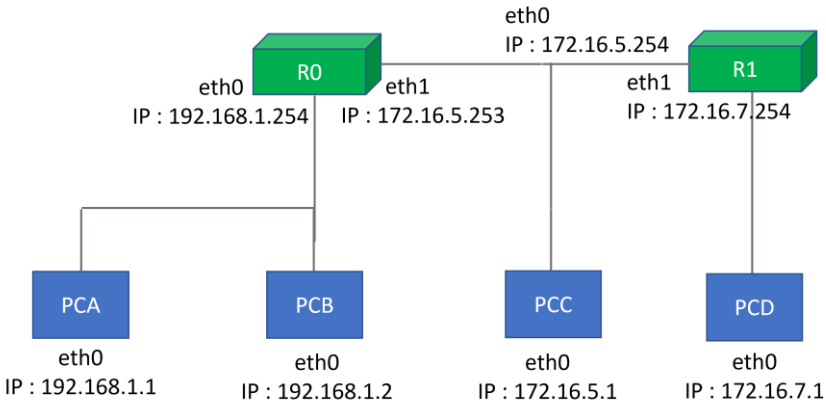
Commande :
Résultat :

7. Maintenant, sur PCA faites un ping vers PCC. Quel est le résultat ? Pouvez-vous l'expliquer en utilisant le cahier de débogage ?

8. Faites en sorte qu'un ping puisse passer sans problème entre toutes les machines de l'infrastructure ci-dessus. Quelles commandes avez-vous dû taper ? Sur quelles machines ?

Exercice II : Une configuration par startup

Nous allons regarder une topologie étendue du lab par rapport à l'exercice précédent. Elle est représentée ci-dessous. Le réseau de PCD est en /24.



1. Pour éteindre Kathará vous pouvez taper dans un premier temps `kathara lstop`. Puis tapez `kathara lclean`.

2. Modifiez le fichier lab.conf pour mettre en place cette topologie.

3. Si on fait démarrer le lab Kathará maintenant, aucune des machines n'aura aucune configuration. Créez, en utilisant nano, des fichiers de startup pour les machines PCA, PCB, PCC et PCD. Ces fichiers devront configurer les adresses IP des 4 machines (seulement les adresses IP).

   Quel est le contenu du fichier startup de la machine PCD ?

4. Faites démarrer le lab Kathará. Quelle est l'instruction utilisée ?

5. Faites un ping de PCA vers PCC. Quel est le résultat ? Pourquoi ?

6. Écrivez des fichiers de startup pour R0 et R1 et faites en sorte que chaque machine utilisateur – PCA, PCB, PCC, PCD – ait un routeur : PCA, PCB et PCD ont le routeur par défaut R0, alors que PCD envoie des messages via R1.

   Quel est le contenu du fichier de startup de la machine PCD maintenant ?

7. Pour redémarrer le lab, il suffit de taper kathara lclean, puis kathara lstart.

8. Faites un ping de PCA vers PCB, puis vers PCC, puis vers PCD. Lesquels des pings fonctionnent-ils ? Pouvez-vous justifier ce résultat ?

9. Modifiez les fichiers de startup pour assurer le succès des pings entre toutes les machines du lab.

Exercice III : 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 ?