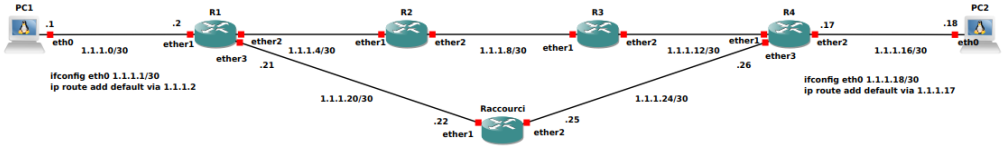
UNIVERSITÉ CAEN NORMANDIE

TP-Ping et traceroute

12.01.2023

Sont dans un bateau, ping tombe à côté... ☺

Auteur : Pascal Fougeray



Source : Moi ☺

---

1 Préambule

— Ce TP peut être fait chez vous, il n'y a aucune difficulté majeure, il ne va pas vous occuper 2h30 !☺
— Ce TP utilise des routeurs, on n'a pas encore vu ce que c'est mais ce n'est pas grave.
— On travaille dans la VM et qu'avec les logiciels GNS3 et Wireshark
— Il y a 2 structures presque identiques. Vous pouvez directement utiliser la seconde en laissant le routeur raccourci éteint !
— **Prenez des notes sur ce que vous comprenez, ces notes vous y aurez le droit de les avoir avec vous au CT !**

2 Introduction

Dans ce TP, je vous propose de **voir** :
— L'utilité du ping
— Les @IP source et destination dans un parcours sont toujours les mêmes.
— L'utilité du traceroute
— Dans le réseau on passe par le chemin le plus court !
— Qui garde les adresses MAC !
— etc...

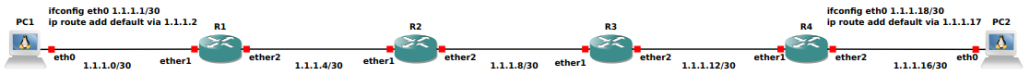
Nous n'avons pas encore étudié le routage et les routeurs, mais ce n'est pas un problème ici.

Je vous rappelle ce que l'on a vu au TP1 intitulé Environnement

Le routage c'est savoir comment aller d'un point A à un point B et par où passer, aussi bien à l'aller qu'au retour ?

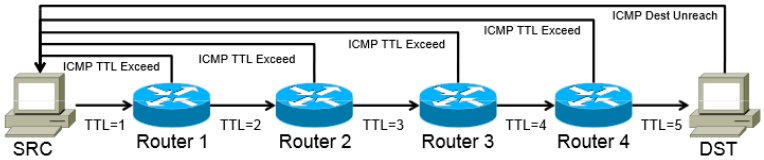
3 L'étude théorique

Soit la première structure suivante, on a supprimé le raccourci en éteignant le routeur raccourci ☺



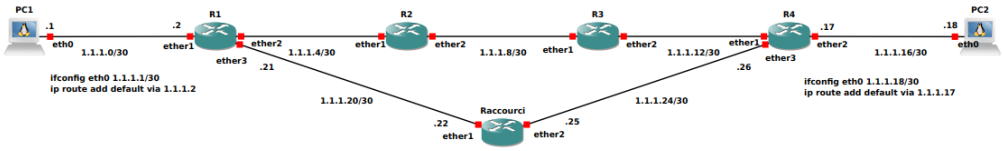
1. **Combien a-t'on de réseaux ?**
2. Combien de fois un paquet IP change de réseau pour aller de PC1 à PC2 ?
3. Combien a-t'on d'@IP dans un /30 ?

4. Quelles sont les @IP possibles de PC1 et PC2 ?
5. Combien d'@IP possède chaque réseau de cette structure et quelles sont ces adresses ?
   Pour la seconde partie de cette question, le faire que pour un réseau.
6. **Rappelez** le fonctionnement de **traceroute**
   Allez je vous aide car ce n'est pas facile ☺



Le principe de fonctionnement de Traceroute consiste à envoyer des paquets UDP, TCP ou bien ICMP avec des paquets **ECHO Request**, avec un **TTL** de plus en plus grand en commençant à 1. Chaque routeur recevant un paquet IP en décrémente le TTL. Lorsque le TTL atteint 0, le routeur émet un paquet ICMP d'erreur (type 11, code 1). Traceroute découvre ainsi les routeurs de proche en proche.

Soit la seconde structure on a allumé le routeur raccourci ☺

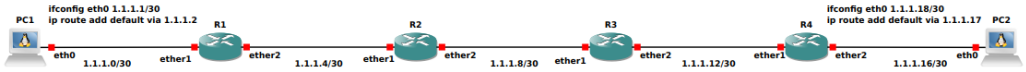


1. Dans cette structure combien a-t'on de réseaux ?
2. Par où un paquet IP passe pour aller de PC1 à PC2 ?
3. Combien de fois un paquet IP change de réseau pour aller de PC1 à PC2 ?

4 L'étude pratique

Pour se loguer sur un routeur, le login est admin et il n'y a pas de MDP donc on valide

4.1 Sans raccourci



1. **Récupérez** sur ecampus le projet nommé **ping sans raccourci**
2. **Lancez** tous les composants en cliquant sur la grosse flèche verte
3. Sur PC1 **lancez** les commandes
   (a) ***ifconfig eth0 1.1.1.1/30***
   (b) ***ip route add default via 1.1.1.2***
   (c) ***ip route ls***
   (d) **Expliquez** ces 3 commandes
4. Sur PC2 **lancez** les commandes
   (a) ***ifconfig eth0 1.1.1.18/30***
   (b) ***ip route add default via 1.1.1.17***
   (c) ***ip route ls***
   (d) **Expliquez** ces 3 commandes
5. **Mettez** une sonde wireshark sur les 5 câbles et **filtrez** avec **arp || icmp**
6. Sur PC1 **lancez** la commande **ping -c2 1.1.1.18**
7. **Relevez** les @IP source et destination sur chaque capture wireshark

8. **Concluez** !
9. Sur PC1et PC2 **lancez** la commande ***arp***, que **constatez** vous ?
10. **Sur les 4 routeurs lancez** les commandes ***ip arp print***, *que* ***constatez*** *vous ?*

Une trame ARP ne traverse pas un routeur ! ! !

11. **Supprimez** toutes les sondes wireshark **sans sauvegarder.**
12. **Mettez** une sonde wireshark entre PC1 et R1et **filtrez** avec **icmp**
13. Sur PC1 **lancez** la commande ***traceroute 1.1.1.18*** et **relevez** le nombre de sauts. Cela est-il conforme à la réponse de l'étude théorique **Combien a-t'on de réseaux ?**
14. Sur wireshark, **relevez** les paquet ICMP et vous devez obtenir cela.

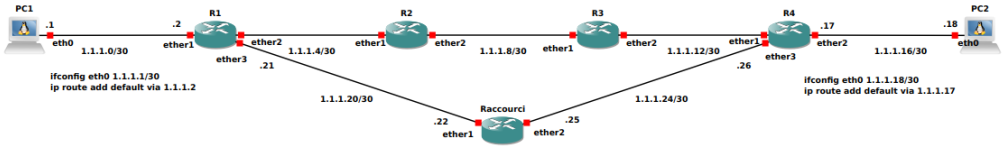
icmp

No.	Time	Source	Destination	Protocol	Length	Info
26	30.082760	1.1.1.2	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
27	30.082852	1.1.1.2	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
28	30.082913	1.1.1.2	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
32	30.089730	1.1.1.6	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
33	30.089849	1.1.1.6	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
34	30.089889	1.1.1.6	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
38	30.095588	1.1.1.10	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
39	30.095706	1.1.1.10	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
40	30.095750	1.1.1.10	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
44	30.102811	1.1.1.14	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
45	30.103159	1.1.1.14	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
46	30.103326	1.1.1.14	1.1.1.1	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
50	30.106919	1.1.1.18	1.1.1.1	ICMP	102	Destination unreachable (Port unreachable)
51	30.107050	1.1.1.18	1.1.1.1	ICMP	102	Destination unreachable (Port unreachable)
52	30.107105	1.1.1.18	1.1.1.1	ICMP	102	Destination unreachable (Port unreachable)
53	30.107151	1.1.1.18	1.1.1.1	ICMP	102	Destination unreachable (Port unreachable)
54	30.107194	1.1.1.18	1.1.1.1	ICMP	102	Destination unreachable (Port unreachable)
55	30.107590	1.1.1.18	1.1.1.1	ICMP	102	Destination unreachable (Port unreachable)

15. Sur PC1 **lancez** la commande ***traceroute 1.1.1.8*** (oui oui 8 et non 18 !)
    (a) **Expliquez** ce qui se passe
    (b) Pourquoi ?
    (c) C'est quelle type d'@IP ?
16. **Faites** de même avec l'@IP 1.1.1.11 !
    (a) **Expliquez** ce qui se passe
    (b) Pourquoi ?
    (c) C'est quelle type d'@IP ?
17. **Concluez** sur traceroute

4.2 Avec raccourci

On va devoir refaire certaines mêmes questions.



1. **Récupérez** sur ecampus le projet nommé **ping avec raccourci**
2. **Lancez** tous les composants en cliquant sur la grosse flèche verte
3. Sur PC1 **lancez** les commandes
   (a) ***ifconfig eth0 1.1.1.1/30***
   (b) ***ip route add default via 1.1.1.2***
4. Sur PC2 **lancez** les commandes
   (a) ***ifconfig eth0 1.1.1.18/30***
   (b) ***ip route add default via 1.1.1.17***
5. **Mettez** une sonde wireshark entre les routeurs R2 et R3 et **filtrez** avec **arp || icmp**
6. Sur PC1 **lancez** la commande **ping -c2 1.1.1.18**

7. Le ping marche ? Si oui, **allez** voir ce qu'il y a sur wireshark ☺
   Pourquoi ? ? ?
8. **Réponse** : Sur PC1 **lancez** la commande ***traceroute 1.1.1.18*** et **relevez** le nombre de sauts. Cela est-il conforme à la réponse de l'étude théorique **Combien a-t'on de réseaux ?**
   On est passé de 5 à 4 c'est bien cela ?
9. **Vérifiez** en mettant une sonde wireshark entre les routeurs R1 et Raccourci et **filtrez** avec **arp || icmp**
10. Sur PC1 **lancez** la commande **ping -c2 1.1.1.18**
11. Il y a quelque chose ? Si oui, ouf ☺
12. **Concluez**

5 Bonus

Si vous avez fini... et qu'il n'est pas l'heure

1. Sur chaque routeur **lancez** la commande ***ip route print***
   Vous devez voir quelque chose comme ça

```
[admin@Raccourci] > ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static,
r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADo  1.1.1.0/30                         1.1.1.21                110
 1 ADo  1.1.1.4/30                         1.1.1.21                110
 2 ADo  1.1.1.8/30                         1.1.1.26                110
                                           1.1.1.21
 3 ADo  1.1.1.12/30                        1.1.1.26                110
 4 ADo  1.1.1.16/30                        1.1.1.26                110
 5 ADC  1.1.1.20/30        1.1.1.22        ether1                    0
 6 ADC  1.1.1.24/30        1.1.1.25        ether2                    0
 7 ADo  11.11.11.11/32                     1.1.1.21                110
 8 ADo  22.22.22.22/32                     1.1.1.21                110
 9 ADo  33.33.33.33/32                     1.1.1.26                110
10 ADo  44.44.44.44/32                     1.1.1.26                110
11 ADC  55.55.55.55/32     55.55.55.55     lo                        0
[admin@Raccourci] >
```

2. C'est quoi ces 12 réseaux ?
3. C'est quoi ADo et ADC ?
4. C'est quoi ces @IP en /32, des loopbacks ?
5. C'est quoi Distance (en mm, en m, en km en année lumière ☺)

Vivement le cours sur le routage ☺

6 Conclusion