# NSI - Terminale

Réseau : routage - Travaux dirigés

qkzk

2020/10/11

**Compétence :** *Analyser un datagramme IP*

## Exercice 1

Nous avons utilisé le logiciel WireShark (analyse de trames) pour capturer les datagrammes échangés sur un réseau local. Nous étudions le datagramme suivant :

```
Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp3s0, id 0
    Interface id: 0 (enp3s0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 11, 2020 13:56:25.823292748 CEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1602417385.823292748 seconds
    [Time delta from previous captured frame: 0.192323401 seconds]
    [Time delta from previous displayed frame: 0.192323401 seconds]
    [Time since reference or first frame: 1.013317818 seconds]
    Frame Number: 12
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Micro-St_5d:b2:f4 (44:8a:5b:5d:b2:f4), Dst: AnovFran_7f:95:56 (a4:3e:51:7f:95:56)
Internet Protocol Version 4, Src: 192.168.1.21, Dst: 192.161.1.26
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x71b3 (29107)
    Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x457d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.21
    Destination: 192.161.1.26
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xd436 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
```

```
Identifier (LE): 256 (0x0100)
Sequence number (BE): 19 (0x0013)
Sequence number (LE): 4864 (0x1300)
[No response seen]
Timestamp from icmp data: Oct 11, 2020 13:56:25.000000000 CEST
[Timestamp from icmp data (relative): 0.823292748 seconds]
Data (48 bytes)
```

1. Quelle est la nature du réseau utilisé ?
2. Extraire l'adresse IP de l'émetteur et celle du destinataire.
3. Quelle est l'application qui a généré ce datagramme ?

---

**Compétence :** *Connaître le fonctionnement du protocole de routage RIP*

## Exercice 2

Un routeur a la table de routage suivante :

| Adresse de destination | Passerelle | Interface | Vecteur de distance |
|---|---|---|---|
| 192.8.13.20 | 192.168.1.254 | 192.168.1.3 | 3 |
| 192.168.1.0 | 192.168.1.254 | 192.168.1.3 | 1 |
| 180.18.0.0 | 180.18.1.254 | 192.168.1.1 | 1 |
| 180.19.0.0 | 180.19.1.254 | 192.168.1.1 | 2 |
| 180.19.3.0 | 180.19.1.254 | 192.168.1.1 | 2 |
| *défaut* | 192.168.1.254 | 192.168.1.13 | 1 |

1. Donner le message RIP émis par ce routeur.

## Exercice 3

Soit le réseau suivant :

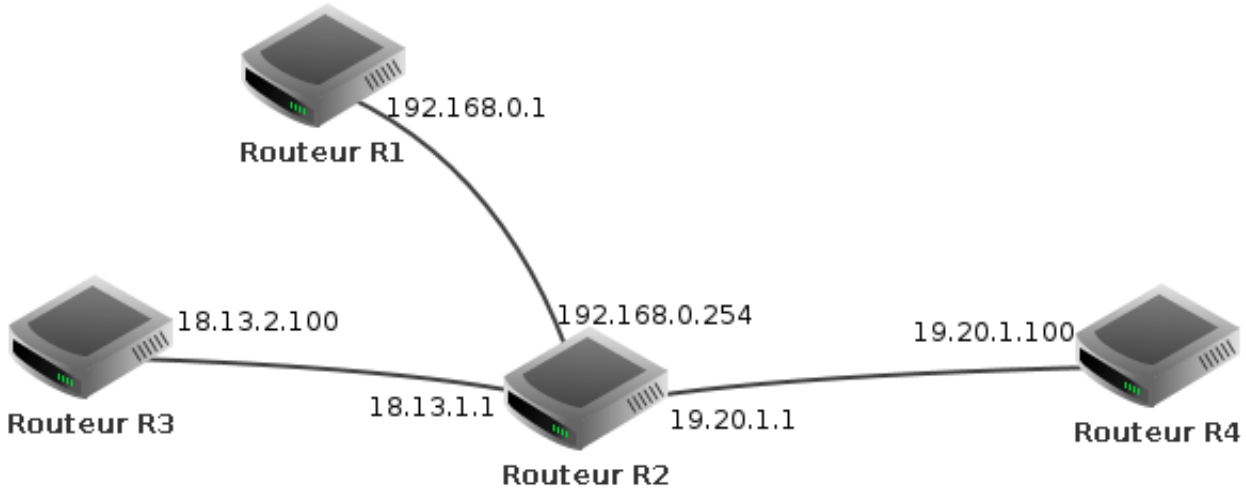


Figure 1: réseau 1

Donner la table de routage RIP du routeur 1

# Exercice 4

Soit le réseau suivant :

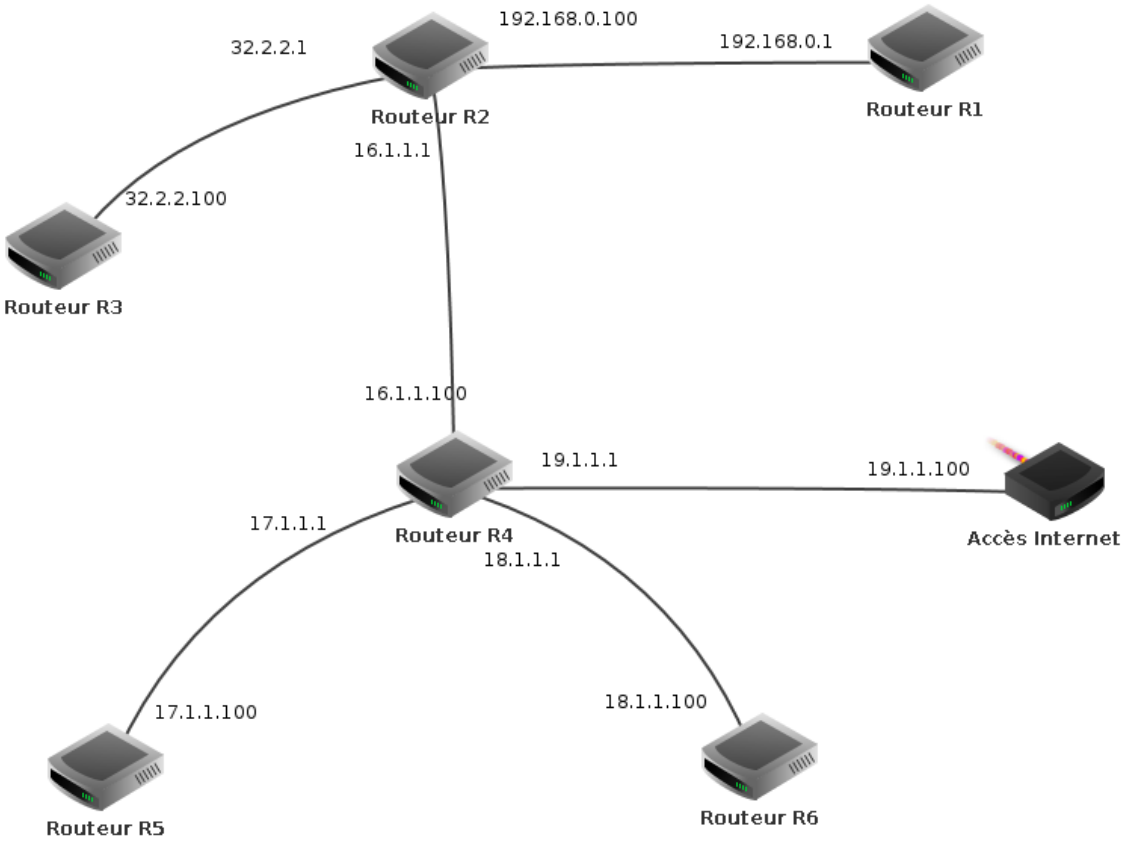


Figure 2: réseau 2

1. Expliquer comment, lorsqu'il reçoit un datagramme sur l'une de ses interfaces le routeur R2 retransmet ce datagramme en fonction de son destinataire.
2. Donner la table de routage RIP du routeur R2.
3. Donner la table de routage RIP du routeur R4.
4. Donner la table de routage RIP du routeur R6.

# Exercice 5

La société IMPORT3000 est spécialisée dans l'import de produits numériques et dans leur revente sur le marché français. Son réseau informatique est structuré en 3 parties :

- Le réseau administratif abritant tous les postes de travail et les serveurs de fichier et de gestion (réseau 192.168.1.0)
- Le réseau commercial (réseau 142.7.0.0)
- la zone démilitarisée (DMZ) hébergeant les serveurs web accessibles par internet (réseau 19.0.0.0)

L'organisation de ce réseau est la suivante :

1. Donner la ligne de la table de routage d'un hôte du réseau administratif nécessaire pour qu'il puisse joindre tout hôte du réseau commercial.
2. Donner la ligne de la table de routage de cet hôte du réseau administratif nécessaire pour qu'il puisse joindre le serveur Web
3. Donner la ligne de la table de routage d'un hôte du réseau commercial nécessaire pour qu'il puisse joindre le serveur Web

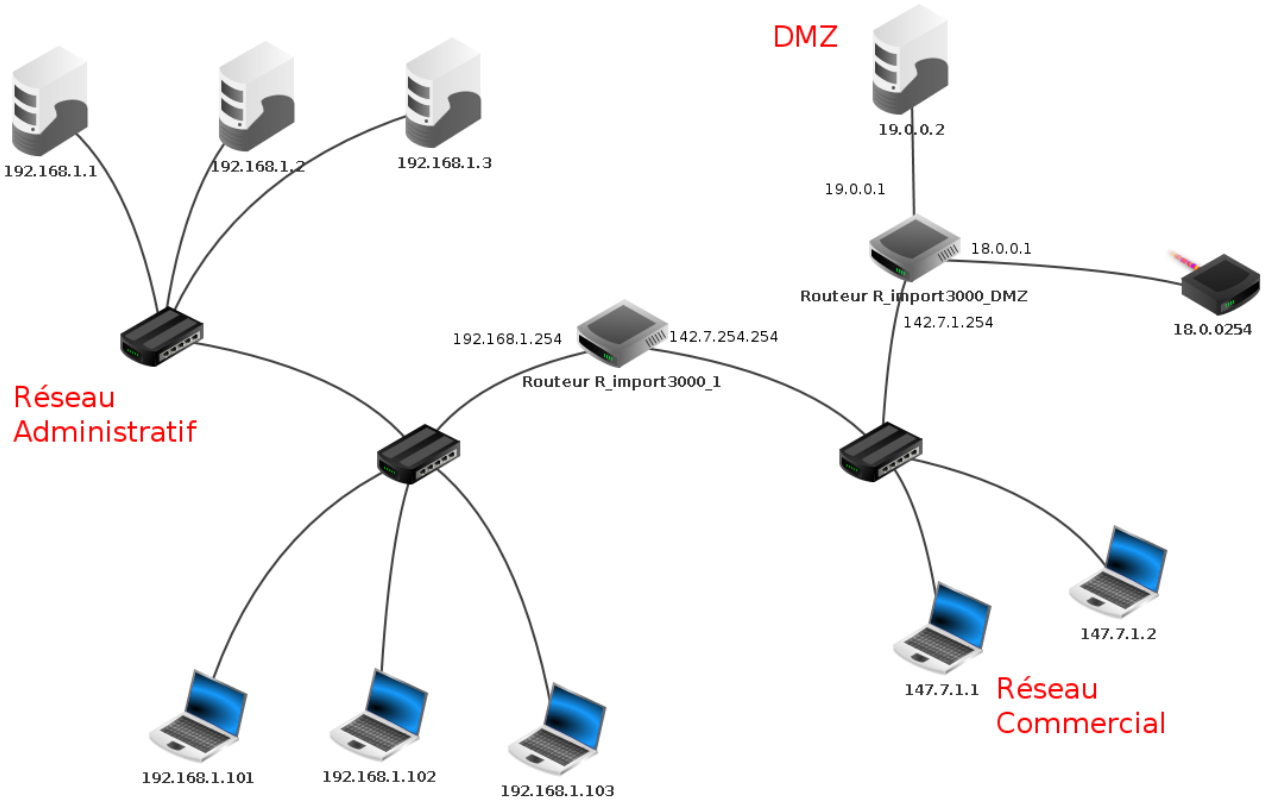


Figure 3: réseau 3

**Compétence :** *Analyse une situation réelle de routage*

## Exercice 6

Sur un serveur Linux, la commande qui permet d'afficher la table de routage est `route`.

Dans cet exercice, nous exécutons `route` sur un serveur en activité, le résultat est le suivant :

```
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
192.169.1.36    0.0.0.0         255.255.255.0   UH    0      0        0 eth0
192.169.1.0     0.0.0.0         255.255.255.0   U     1      0        0 eth0
195.1.1.0       0.0.0.0         255.255.255.0   U     1      0        0 eth1
70.0.1.0        0.0.0.0         255.0.0.0       U     3      0        0 eth1
127.0.0.1       0.0.0.0         255.0.0.0       U     0      0        0 lo
default         0.0.0.0         0.0.0.0         UG    1      0        0 eth0
```

## Exercice 7 - Bilan

HTTP est le protocole de base du Web : c'est lui qui transmet les requêtes de pages Web et assure le transport de ces pages Web entre le serveur et le client, pour que le navigateur de celui-ci puisse les afficher.

Les transferts générés par HTTP ne sont pas sécurisés : il a donc éé nécessaire de lui ajouter des outils assurant la sécurité des transmissions des requêtes et pages.

La sécurité a été ajoutée à HTTP par les protocoles SSL, puis TLS, donnant un complexe qui a pris le nom d'HTTPS.

HTTPS intègre la sécurité aux différents niveaux d'un échange, par l'utilisation des techniques de chiffrement :

- l'échange sécurisé de clés,
- l'authentification du client et du serveur,
- la confidentialité des transmissions (requêtes et pages) par un mécanisme de chiffrement.

1. Sachant que HTTPS assure la confidentialité des données par un chiffrement symétrique, représenter par un schéma la transmission sécurisée de la requête d'une page Web d'un client à destination d'un sereur Web
2. Ajouter à ce schéma la transmission de la page Web du serveur vers le client.
3. Nous avons dit que la clé publique utilisée par le client et le sereur pour cette transmission des pages est générée au départ de l'échange par le serveur, puis transmise au client.

   Quelle est la problématique qui se pose à ce niveau ?
4. Proposer une solution pour sécuriser cette transmission de la clé publique de chiffrement symétrique.
5. Compléter le schéma de 2. en intégrant la diffusion de la clé publique symétrique.