



# TP - Obtention d'informations à l'aide d'une commande standart

Énoncé 7.1 Obtention d'informations à l'aide d'une commande standart

## 1. Énoncé 7.1.1

Durée estimative : 10 minutes

L'objectif de ce premier exercice est d'extraire les informations utiles à partir d'une commande standart. Examinez l'affichage de la commande proposée et répondez aux questions ciaprès :

C:\>XXXXXXXXXX

Configuration IP de Windows 2000

Nom de l'hôte . . . . . : PENELOPE Suffixe DNS principal . . . . . : sofiatel.local Type de nœud. . . . . : Diffuser  
Routage IP activé . . . . . : Oui  
Proxy WINS activé . . . . . : Non  
Liste de recherche de suffixe DNS : sofiatel.local Ethernet carte Interne:  
Suffixe DNS spéc. à la connexion. :  
Description . . . . . : Carte Realtek RTL8139 (A) PCI Fast Ethernet #3  
Adresse physique. . . . . : 00-50-FC-1F-3C-6F  
DHCP activé . . . . . : Non  
Adresse IP. . . . . : 172.25.0.100

Masque de sous-réseau . . . . . : 255.255.0.0 Passerelle  
par défaut . . . . . :  
Serveurs DNS. . . . . : 172.25.0.3  
172.25.0.4

#### Ethernet carte Public:

Suffixe DNS spéc. à la connexion. :  
Description . . . . . : Carte Realtek RTL8139  
(A) PCI Fast Ethernet #2  
Adresse physique. . . . . : 00-50-FC-0B-AF-96  
DHCP activé . . . . . : Non  
Adresse IP. . . . . : 193.121.49.58  
Masque de sous-réseau . . . . . : 255.255.255.248 Passere  
lle par défaut . . . . . : 193.121.49.60 Serveurs DNS. .  
. . . . . : 194.2.0.20  
194.2.0.50

NetBIOS sur Tcpip . . . . . : Désactivé Ethernet cart  
e reseauB:

Suffixe DNS spéc. à la connexion. :  
Description . . . . . : Carte Realtek RTL8139  
(A) PCI Fast Ethernet

Adresse physique. . . . . : 00-50-FC-0B-9A-80  
DHCP activé . . . . . : Non  
Adresse IP. . . . . : 172.16.0.100  
Masque de sous-réseau . . . . . : 255.255.0.0 Passerelle  
par défaut . . . . . :  
Serveurs DNS. . . . . : 172.25.0.3  
172.25.0.4

#### Ethernet carte DMZ:

Suffixe DNS spéc. à la connexion. :  
Description . . . . . : Carte Fast Ethernet PCI  
D-Link DFE-530TX  
Adresse physique. . . . . : 00-80-C8-EC-81-E5  
DHCP activé . . . . . : Non

```
Adresse IP. . . . . : 172.20.0.100
Masque de sous-réseau . . . . . : 255.255.0.0 Passerelle
par défaut . . . . . :
Serveurs DNS. . . . . :
```

1. Quelle commande a été saisie ?
2. Identifiez les réseaux logiques sur lesquels est placé ce serveur.
3. Combien d'interfaces sont configurées pour ce serveur ?
4. Quel type de serveur est-ce ?
5. Définissez les plages d'adresses des sous-réseaux pour chacune des interfaces correspondantes.

## 2. Énoncé 7.1.2

Durée estimative : 10 minutes

```
C:\>XXXXXXXX
```

```
Interface : 172.16.0.100 on Interface 0x2
```

Adresse Internet	Adresse physique	Type
172.16.0.200	00-50-da-b8-22-9d	dynamique
172.16.101.1	00-60-97-37-12-3b	dynamique
172.16.103.1	00-50-da-d6-3e-e8	dynamique
172.16.104.1	00-10-4b-b6-5b-27	dynamique
172.16.205.1	00-50-04-ec-ae-4c	dynamique
172.16.206.254	00-50-da-84-cb-62	dynamique
172.16.208.1	00-50-da-36-33-91	dynamique

Interface : 172.20.0.100 on Interface 0x3

Adresse Internet	Adresse physique	Type
172.20.0.3	00-50-fc-4b-06-9c	dynamique
172.20.0.57	00-60-97-c5-a8-ad	dynamique

Interface : 195.101.229.57 on Interface 0x1000005 Adresse I  
nترنت Adresse physique Type 195.101.229.60 00-20-6f-0d  
-75-c8 dynamique

Interface : 172.17.0.100 on Interface 0x1000006 Adresse Int  
ernet Adresse physique Type

172.17.0.3	00-50-fc-0b-39-f1	dynamique
172.17.0.4	00-50-fc-54-0e-28	dynamique
172.17.64.48	00-50-56-50-00-7f	dynamique
172.17.71.1	00-50-fc-1f-7a-3a	dynamique
172.17.207.89	00-50-fc-20-3a-39	dynamique

1. Quelle commande a été saisie ici ?
2. De combien d'interfaces dispose cet ordinateur ?
3. Parmi les interfaces, quelles sont celles situées sur u  
n réseau privé ?

.....

.....

.....

4. Quels types de cartes réseau sont utilisés sur ce résea  
u ? Quel est le constructeur associé à chaque composant dis  
posant d'adresses IP ?

.....

5. Quelle est la particularité de l'ordinateur dont l'adresse IP est 172.17.64.48 ?

.....

6. Combien de cartes réseau 3Com sont référencées ici ?

.....

7. Est-il possible d'en déduire le masque de sous-réseau de chaque interface ? Le numéro de réseau sans ambiguïté ?

.....

.....

### 3. Énoncé 7.1.3

Durée estimative : 5 minutes

```
[root@linus /root]# XXXXXXXXXXXXXXXXX
XXXXXX XXXXXXXXX (XXXXXXXXXXXXXX): 56 data bytes
64 bytes from 172.16.0.2: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 172.16.20.3: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 172.16.98.102: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 172.16.0.2: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 172.16.1.253: icmp_seq=0 ttl=255 time=98.7 ms
(DUP!)
64 bytes from 172.16.140.5: icmp_seq=0 ttl=255 time=0.1 ms
64 bytes from 172.16.1.253: icmp_seq=1 ttl=255 time=1.0 ms
(DUP!)
--- XXXXXXXXXXXXXXXXX statistics ---
5 packets transmitted, 5 packets received, +2 duplicates,
0% packet loss round-trip min/avg/max = 0.1/6.0/98.7 ms
```

1. Quelle commande a été spécifiée ?
2. Quel est le réseau logique concerné ?
3. Quelle est la durée de vie de la trame émise ?
4. Quelle est la signification de 'DUP' ?
5. Quel est le temps moyen de parcours d'une telle trame ?
6. Quel système d'exploitation est utilisé ?

## 1. Énoncé

### 1. Quelle commande a été saisie ?

La commande saisie est très probablement

`ipconfig /all` sous Windows 2000. Cette commande affiche la configuration IP détaillée de toutes les interfaces réseau de la machine.

### 2. Identifiez les réseaux logiques sur lesquels est placé ce serveur.

Le serveur est connecté à quatre réseaux logiques différents, comme indiqué par les adresses IP des différentes cartes Ethernet :

- Réseau "Interne" avec l'adresse IP 172.25.0.100
- Réseau "Public" avec l'adresse IP 193.121.49.58
- Réseau "reseauB" avec l'adresse IP 172.16.0.100
- Réseau "DMZ" avec l'adresse IP 172.20.0.100

### 3. Combien d'interfaces sont configurées pour ce serveur ?

Il y a quatre interfaces réseau configurées sur ce serveur, chacune correspondant à une carte Ethernet différente.

### 4. Quel type de serveur est-ce ?

Sur la base des informations fournies, il est difficile de déterminer avec précision le rôle spécifique de ce serveur. Cependant, le fait qu'il ait plusieurs interfaces réseau, y compris une interface dans une DMZ (zone démilitarisée), suggère qu'il pourrait être un serveur frontal (par exemple, un serveur web ou un serveur proxy) ou un serveur de sécurité (comme un pare-feu ou un serveur de passerelle). La présence d'une interface dans la DMZ est typique des serveurs

qui doivent être accessibles à la fois depuis des réseaux internes et externes, tout en étant isolés pour des raisons de sécurité.

## 5. Définissez les plages d'adresses des sous-réseaux pour chacune des interfaces correspondantes.

Pour déterminer les plages d'adresses, nous devons examiner l'adresse IP et le masque de sous-réseau de chaque interface :

- **Ethernet carte Interne** (172.25.0.100 avec un masque de sous-réseau 255.255.0.0) : La plage d'adresses va de 172.25.0.1 à 172.25.255.254.
- **Ethernet carte Public** (193.121.49.58 avec un masque de sous-réseau 255.255.255.248) : La plage d'adresses va de 193.121.49.49 à 193.121.49.62.
- **Ethernet carte reseauB** (172.16.0.100 avec un masque de sous-réseau 255.255.0.0) : La plage d'adresses va de 172.16.0.1 à 172.16.255.254.
- **Ethernet carte DMZ** (172.20.0.100 avec un masque de sous-réseau 255.255.0.0) : La plage d'adresses va de 172.20.0.1 à 172.20.255.254.

## 2. Énoncé

### 1. Quelle commande a été saisie ici ?

La commande saisie semble être

`arp -a` . Cette commande affiche la table ARP (Address Resolution Protocol) du système, montrant les correspondances entre les adresses IP et les adresses MAC des appareils sur le réseau.

2.

### De combien d'interfaces dispose cet ordinateur ?

L'ordinateur dispose de quatre interfaces réseau, comme indiqué par les différentes interfaces listées (0x2, 0x3, 0x1000005, 0x1000006).

3.

### Parmi les interfaces, quelles sont celles situées sur un réseau privé ?

Les interfaces situées sur un réseau privé sont celles avec les adresses IP suivantes :

◦

172.16.0.100 (Interface 0x2)

◦  
172.20.0.100 (Interface 0x3)

◦  
172.17.0.100 (Interface 0x1000006)

Les adresses IP commençant par 172.16 à 172.31 sont des adresses privées selon la norme RFC 1918.

4.

**Quels types de cartes réseau sont utilisés sur ce réseau ? Quel est le constructeur associé à chaque composant disposant d'adresses IP ?**

Pour déterminer les fabricants des cartes réseau, on examine les trois premiers octets de l'adresse MAC (identifiant de l'organisation). Par exemple, les adresses MAC commençant par "00-50-da" peuvent correspondre à un fabricant spécifique. Cependant, sans un outil ou une base de données pour rechercher ces identifiants, il n'est pas possible de déterminer précisément le fabricant de chaque carte réseau.

5.

**Quelle est la particularité de l'ordinateur dont l'adresse IP est 172.17.64.48 ?**

Il n'y a pas d'information spécifique dans les données fournies qui indique une particularité de l'ordinateur avec l'adresse IP 172.17.64.48. Cependant, si cette adresse IP est notablement différente des autres adresses IP sur la même interface réseau, cela pourrait indiquer un rôle ou une configuration spécifique.

6.

**Combien de cartes réseau 3Com sont référencées ici ?**

Sans une base de données pour rechercher les identifiants des fabricants dans les adresses MAC, il n'est pas possible de déterminer le nombre de cartes réseau 3Com.

7.

**Est-il possible d'en déduire le masque de sous-réseau de chaque interface ? Le numéro de réseau sans ambiguïté ?**

Non, il n'est pas possible de déduire le masque de sous-réseau ou le numéro de réseau pour chaque interface à partir des informations fournies dans la table ARP. La table ARP montre seulement les correspondances entre les adresses IP



et MAC, mais ne fournit pas d'informations sur la configuration du réseau, comme le masque de sous-réseau ou le numéro de réseau.

**1. Quelle commande a été saisie ici ?**

La commande est toujours

```
arp -a .
```

**2. De combien d'interfaces dispose cet ordinateur ?**

L'ordinateur dispose de quatre interfaces réseau.

**3. Parmi les interfaces, quelles sont celles situées sur un réseau privé ?**

Les interfaces avec les adresses IP suivantes sont sur un réseau privé :

- 172.16.0.100 (Interface 0x2)
- 172.20.0.100 (Interface 0x3)
- 172.17.0.100 (Interface 0x1000006)

**4. Quels types de cartes réseau sont utilisés sur ce réseau ? Quel est le constructeur associé à chaque composant disposant d'adresses IP ?**

- Adresses MAC commençant par "0050da", "006097", et "00104b" sont associées à **3Com Corporation**.
- Adresses MAC commençant par "005004" sont associées à **3Com Corporation**.
- Adresses MAC commençant par "0050fc" sont associées à **Edimax Technology Co., Ltd.**
- Adresses MAC commençant par "00206f" sont associées à **Flowpoint Corporation**.
- Adresses MAC commençant par "005056" sont associées à **VMware, Inc.**

**5. Quelle est la particularité de l'ordinateur dont l'adresse IP est 172.17.64.48 ?**

L'adresse MAC associée à l'adresse IP 172.17.64.48 (005056) indique que cet appareil est un produit de **VMware, Inc.** Cela suggère que l'adresse IP appartient à une machine virtuelle gérée par VMware.

**6. Combien de cartes réseau 3Com sont référencées ici ?**

Les adresses MAC de 3Com se trouvent plusieurs fois dans la liste :

- "0050da" (3 occurrences)
- "006097" (2 occurrences)
- "00104b" (1 occurrence)
- "005004" (1 occurrence)

Cela fait un total de 7 références à des cartes réseau 3Com.

**7. Est-il possible d'en déduire le masque de sous-réseau de chaque interface ? Le numéro de réseau sans ambiguïté ?**

Non, il n'est toujours pas possible de déduire le masque de sous-réseau ou le numéro de réseau pour chaque interface à partir des informations ARP. Ces informations nécessitent l'accès à la configuration réseau de l'ordinateur ou du réseau lui-même.

### 3. Énoncé

**1. Quelle commande a été spécifiée ?**

La commande est

`ping` avec une option pour un ping multiple. **2. Quel est le réseau logique concerné ?**

Il s'agit du réseau 172.16.0.0, un réseau IP privé.

**Quelle est la durée de vie (TTL) de la trame émise ?**

La durée de vie (TTL) est de 255.

**4. Quelle est la signification de 'DUP' ?**

'DUP' indique la réception de réponses en double pour un même paquet.

5.

**Quel est le temps moyen de parcours d'une telle trame ?**

Le temps de parcours moyen des trames est de 6.0 ms.

**6. Quel système d'exploitation est utilisé ?**

Le système d'exploitation est Linux.