Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Plan :

- Quelques commandes réseaux basiques
- Les commandes “NET”’
- Les commandes “NETSH”

Bonus :

- L’outil de surveillance “ARPWATCH”

Jean-François Costecèque
DSI UT3 - Pôle Infrastructure
Équipe Gestion de parc

UNIVERSITÉ TOULOUSE III PAUL SABATIER
Université de Toulouse

Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Quelques commandes réseaux basiques

Jean-François Costecèque
DSI UT3 - Pôle Infrastructure
Équipe Gestion de parc

UNIVERSITÉ TOULOUSE III PAUL SABATIER
Université de Toulouse

Quelques commandes réseaux basiques

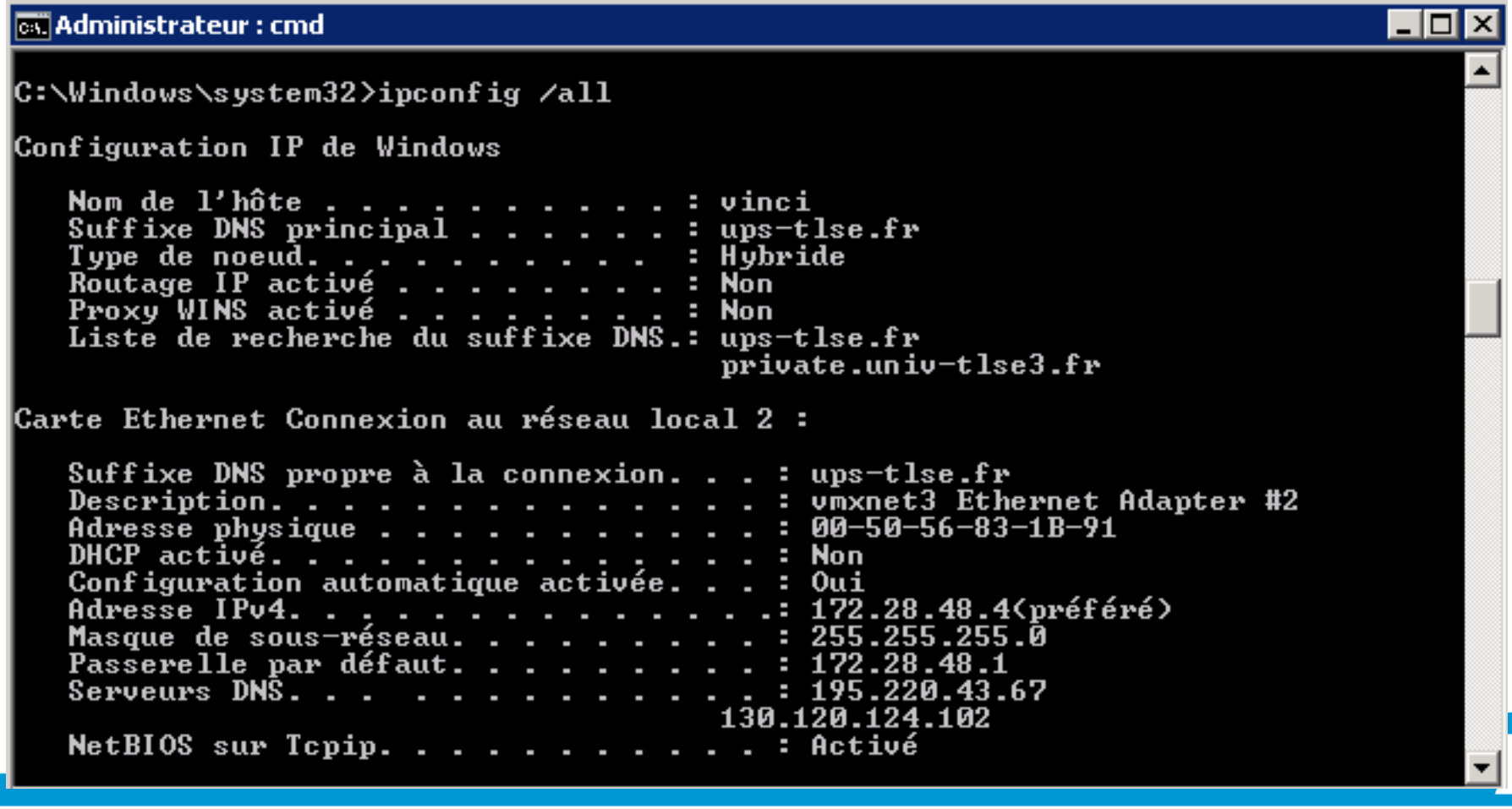
IPCONFIG

- `ipconfig /all`
  - **Affiche toutes les informations sur les interfaces réseaux**
- `ipconfig /release`
  - **Termine le bail DHCP**
- `ipconfig /renew`
  - **Renouvelle le bail DHCP**
- `ipconfig /flushdns`
  - **Vide le cache DNS**
- `ipconfig /displaydns`
  - **Affiche le contenu du cache DNS**

Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Quelques commandes réseaux basiques

IPCONFIG



Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Quelques commandes réseaux basiques

- **PING**
  - **Test connectivité réseau**
- **NSLOOKUP**
  - **Test DNS**
- **NETSTAT**
  - **Statistique réseau, affiche les connexions en cours**
- **ARP**
  - **Affiche et modifie les tables ARP**
- **TRACERT**
  - **Liste les routeurs traversés**
- **ROUTE**
  - **Gère les tables de routage**

Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Quelques commandes réseaux basiques

- **PING**
  - **Test connectivité réseau**

```
C:\>ping google.fr

Envoi d'une requête 'ping' sur google.fr [216.58.211.99] avec 32 octets de donné
es :
Réponse de 216.58.211.99 : octets=32 temps=23 ms TTL=52
Réponse de 216.58.211.99 : octets=32 temps=23 ms TTL=52
Réponse de 216.58.211.99 : octets=32 temps=25 ms TTL=52
Réponse de 216.58.211.99 : octets=32 temps=23 ms TTL=52

Statistiques Ping pour 216.58.211.99:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 23ms, Maximum = 25ms, Moyenne = 23ms
```

Quelques commandes réseaux basiques

- **NSLOOKUP**
  - **Test DNS**

```
C:\>nslookup
Serveur par dÚfaut :   nsr2.cict.fr
Address:  130.120.124.102

> google.fr
Serveur :   nsr2.cict.fr
Address:  130.120.124.102

Réponse ne faisant pas autorité :
Nom :     google.fr
Addresses:  2a00:1450:4006:803::2003
          216.58.210.195
```

Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Quelques commandes réseaux basiques

- **NETSTAT**
  - **Statistique réseau, affiche les connexions en cours**

```
C:\>netstat

Connexions actives

  Proto  Adresse locale         Adresse distante       État
  TCP    127.0.0.1:1079         DPROX13:1080           ESTABLISHED
  TCP    127.0.0.1:1080         DPROX13:1079           ESTABLISHED
  TCP    127.0.0.1:1081         DPROX13:5939           ESTABLISHED
  TCP    127.0.0.1:1087         DPROX13:1088           ESTABLISHED
  TCP    127.0.0.1:1088         DPROX13:1087           ESTABLISHED
  TCP    127.0.0.1:1089         DPROX13:5939           ESTABLISHED
  TCP    127.0.0.1:1146         DPROX13:1147           ESTABLISHED
  TCP    127.0.0.1:1147         DPROX13:1146           ESTABLISHED
  TCP    127.0.0.1:5939         DPROX13:1081           ESTABLISHED
  TCP    127.0.0.1:5939         DPROX13:1089           ESTABLISHED
  TCP    130.120.5.104:1063     server10013:5938       ESTABLISHED
  TCP    130.120.5.104:1117     vinci:microsoft-ds     ESTABLISHED
  TCP    130.120.5.104:1144     dpsrv2:https           CLOSE_WAIT
  TCP    130.120.5.104:1145     dpsrv2:https           ESTABLISHED
  TCP    130.120.5.104:1152     dpsrv2:902             ESTABLISHED
  TCP    130.120.5.104:1546     server10018:5938       ESTABLISHED
  TCP    130.120.5.104:1787     dpsrv2:https           ESTABLISHED
  TCP    130.120.5.104:1790     dpsrv2:https           ESTABLISHED
  TCP    130.120.5.104:1794     dpsrv2:https           ESTABLISHED
  TCP    130.120.5.104:1803     dpsrv2:https           ESTABLISHED
```

Quelques commandes réseaux basiques

- **NETSTAT**
  - **Statistique réseau, affiche les ports ouverts en écoute**

```
C:\>netstat -a -b

Connexions actives

  Proto  Adresse locale         Adresse distante       État
  TCP    0.0.0.0:135            DPROX13:0              LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            DPROX13:0              LISTENING
 Impossible d'obtenir les informations de propriétaire
  TCP    0.0.0.0:1025           DPROX13:0              LISTENING
 [wininit.exe]
  TCP    0.0.0.0:1026           DPROX13:0              LISTENING
  eventlog
 [svchost.exe]
  TCP    0.0.0.0:1027           DPROX13:0              LISTENING
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:1055           DPROX13:0              LISTENING
 [services.exe]
  TCP    0.0.0.0:1058           DPROX13:0              LISTENING
 [lsass.exe]
  TCP    0.0.0.0:1062           DPROX13:0              LISTENING
  PolicyAgent
```

Quelques commandes réseaux basiques

- **ARP**
  - **Affiche et modifie les tables ARP**

```
C:\Users\Kane>arp -a

Interface : 192.168.1.10 --- 0xe
  Adresse Internet      Adresse physique      Type
  192.168.1.22          00-0d-4b-0d-09-dd     dynamique
  192.168.1.254         6c-2e-85-a5-8e-e0     dynamique
  192.168.1.255         ff-ff-ff-ff-ff-ff     statique
  224.0.0.2             01-00-5e-00-00-02     statique
  224.0.0.22            01-00-5e-00-00-16     statique
  224.0.0.252           01-00-5e-00-00-fc     statique
  239.192.152.143       01-00-5e-40-98-8f     statique
  239.255.67.250        01-00-5e-7f-43-fa     statique
  239.255.255.250       01-00-5e-7f-ff-fa     statique
  255.255.255.255       ff-ff-ff-ff-ff-ff     statique
```

Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Quelques commandes réseaux basiques

- **ROUTE**
  - **Gère les tables de routage**

Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Quel

C:\Windows\system32\cmd.exe

```
c:\Windows\System32>route print
===========================================================================
Liste d'Interfaces
 15...00 ff a3 76 93 ca ......TAP-Windows Adapter V9
 14...d4 3d 7e da 47 8a ......Killer e2200 PCI-E Gigabit Ethernet Controller (ND
IS 6.20)
  1...........................Software Loopback Interface 1
 11...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP
 12...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
 13...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP #2
===========================================================================

IPv4 Table de routage
===========================================================================
Itinéraires actifs :
Destination réseau    Masque réseau  Adr. passerelle   Adr. interface Métrique
          0.0.0.0          0.0.0.0    192.168.1.254     192.168.1.10     10
          0.0.0.0        128.0.0.0       172.17.8.5       172.17.8.6     20
        127.0.0.0        255.0.0.0         On-link          127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link          127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link          127.0.0.1    306
        128.0.0.0        128.0.0.0       172.17.8.5       172.17.8.6     20
       172.17.8.1  255.255.255.255       172.17.8.5       172.17.8.6     20
       172.17.8.4  255.255.255.252         On-link          172.17.8.6    276
       172.17.8.6  255.255.255.255         On-link          172.17.8.6    276
       172.17.8.7  255.255.255.255         On-link          172.17.8.6    276
     192.168.1.0    255.255.255.0         On-link       192.168.1.10     266
    192.168.1.10  255.255.255.255         On-link       192.168.1.10     266
   192.168.1.255  255.255.255.255         On-link       192.168.1.10     266
   195.220.43.32  255.255.255.255     192.168.1.254     192.168.1.10     10
       224.0.0.0        240.0.0.0         On-link          127.0.0.1    306
       224.0.0.0        240.0.0.0         On-link       192.168.1.10     266
       224.0.0.0        240.0.0.0         On-link          172.17.8.6    276
  255.255.255.255  255.255.255.255         On-link          127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link       192.168.1.10     266
  255.255.255.255  255.255.255.255         On-link          172.17.8.6    276
===========================================================================
Itinéraires persistants :
  Aucun
```

Les commandes “NET”

- **Gestion des services :**
  - **NET START, STOP, PAUSE, CONTINUE**
- **Connexion à un partage réseau**
  - **NET USE**
- **Gestion des partages réseau**
  - **NET SHARE, VIEW**
- **Gestion des fichiers et des sessions**
  - **NET FILE, SESSIONS**
- **Manage Network Time**
  - **NET TIME**
- **Sécurité**
  - **NET ACCOUNTS, USER, GROUP, LOCALGROUP**

Les commandes NET

NET START / STOP / PAUSE / CONTINUE

Liste des services en cours d'exécution :

```
C:\Windows\system32>net start
Les services Windows suivants ont été lancés :

   Accès du périphérique d'interface utilisateur
   Agent de stratégie IPsec
   Alimentation
   Appel de procédure distante (RPC)
   Assistance IP
   Assistance NetBIOS sur TCP/IP
   ATLOISAService
   Audio Windows
```

```
C:\Windows\system32>net stop "Audio Windows"
Le service Audio Windows s'arrête.
Le service Audio Windows a été arrêté.
```

Les commandes NET

NET USER / GROUP

Liste des utilisateurs et des groupes :

```
C:\Windows\system32>net group /domain

Groupes de \\VINCI

-------------------------------------------------------------------------------
*Administrateurs de l'entreprise
*Administrateurs du schéma
*Admins du domaine
*Assistance Sociale
*Bureau Europe
*Concours
*Contrôleurs de domaine
*Contrôleurs de domaine d'entreprise en lecture seule
*Contrôleurs de domaine en lecture seule
*Crèche
```

Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Les commandes NET

NET USER / GROUP

Création d'un groupe :

```
C:\Windows\system32>net group grp_test /add /domain /comment:"groupe de test"
La commande s'est terminée correctement.
```

Création d'un utilisateur :

```
C:\Windows\system32>net user test /add /domain /comment:"test" /random
Le mot de passe pour test est : $Aumy0D$
```

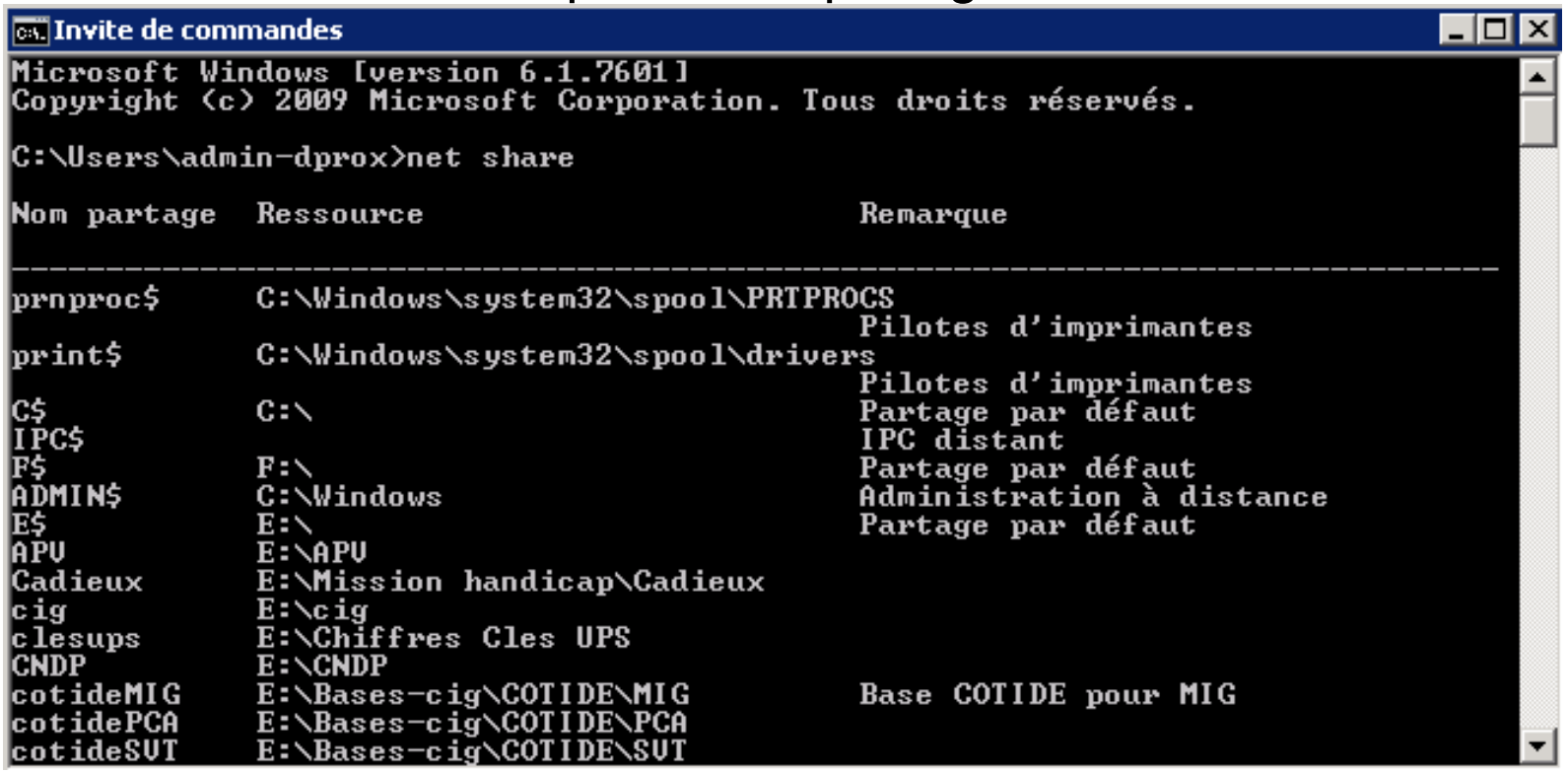
```
C:\Windows\system32>net group grp_test test /add
La commande s'est terminée correctement.


C:\Windows\system32>net group grp_test
Nom de groupe     grp_test
Commentaire       groupe de test

Membres

-------------------------------------------------------------------------------
test
La commande s'est terminée correctement.
```

Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Les commandes NET

NET SHARE

Liste des dossiers et imprimantes partagés :



Les commandes NET

NET SHARE

Création d'un partage réseau coté serveur

```
C:\Windows\system32>net share partage_test=c:\temp  /GRANT:test,READ
partage_test a été partagé.
```

Les commandes NET

NET USE

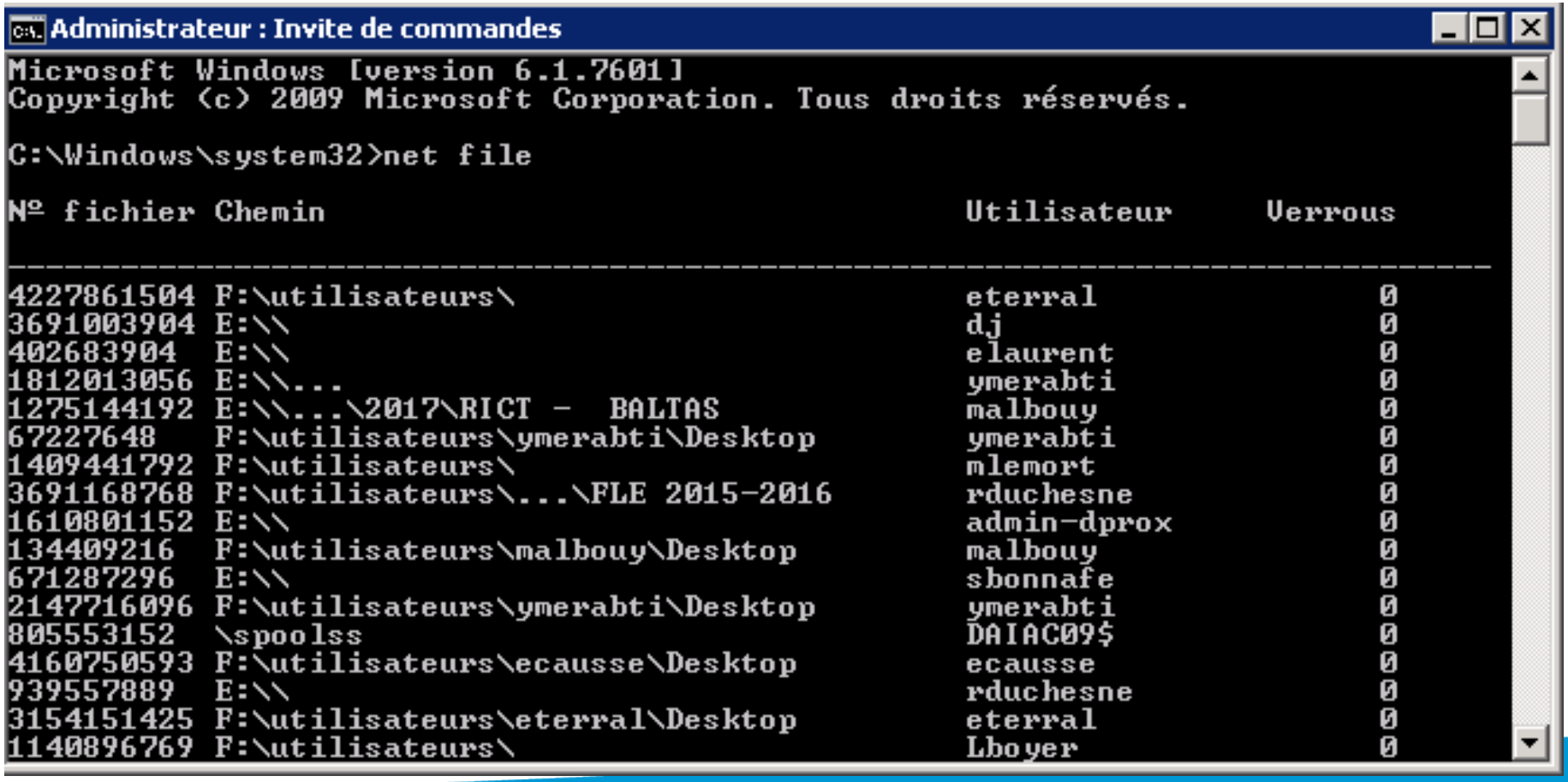
Utilisation d’un partage réseau coté client

```
C:\>net use z: \\vinci\partage_test /user:ups-cig\test $Aumy0D$
La commande s’est terminée correctement.
```

Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Les commandes NET

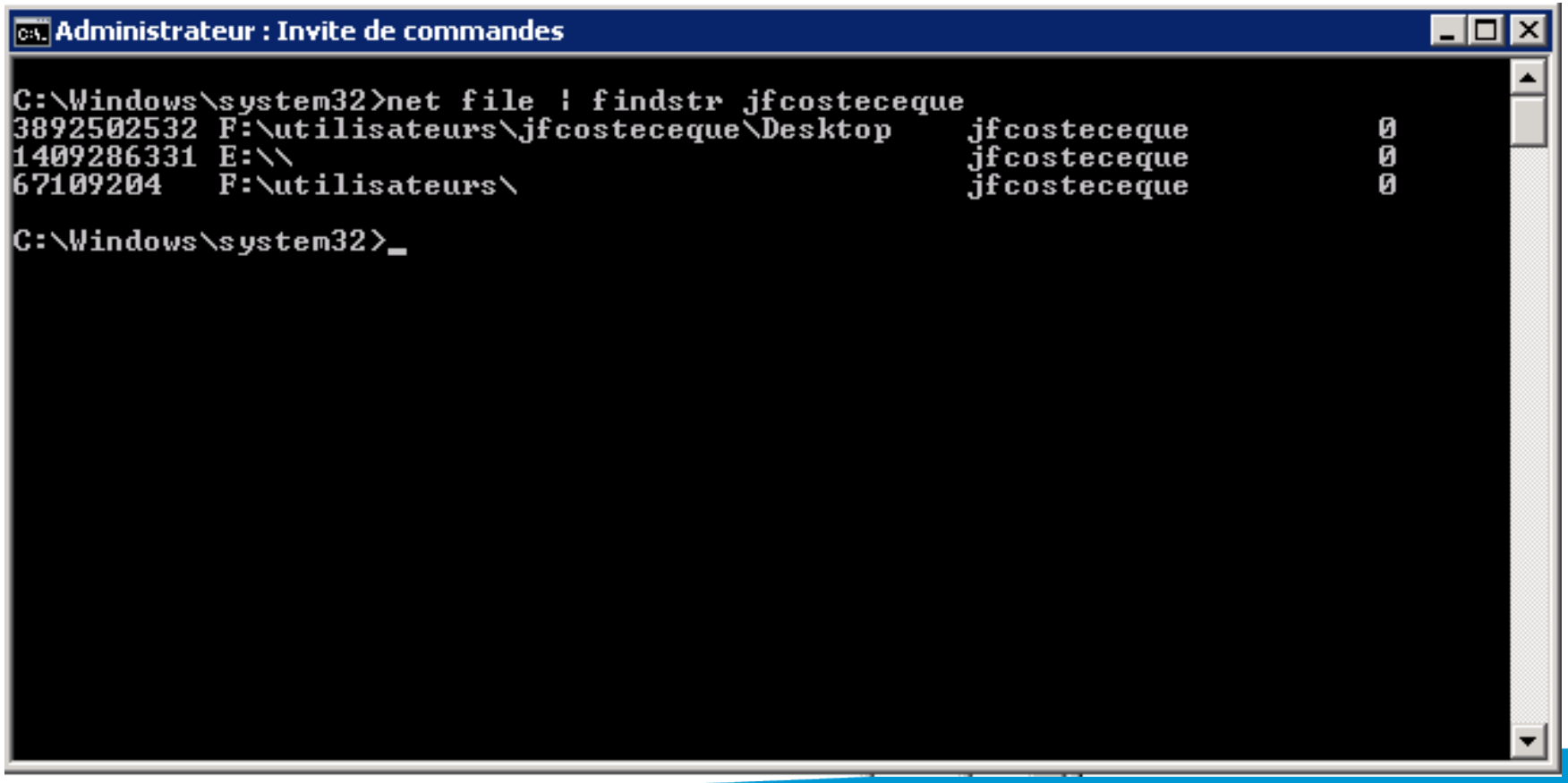
NET FILE



Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Les commandes NET

NET FILE

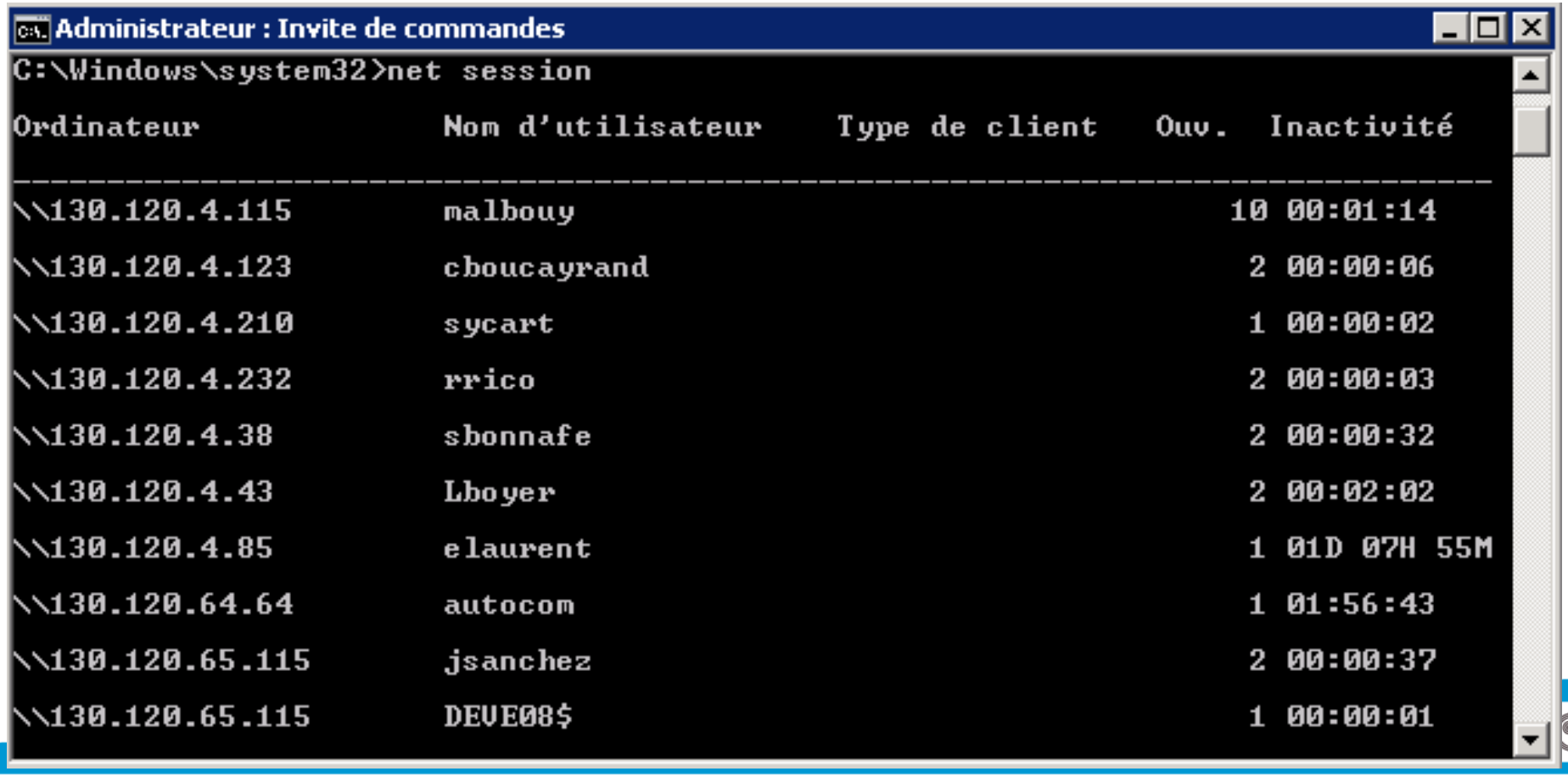


Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

Les commandes NET

NET SESSION

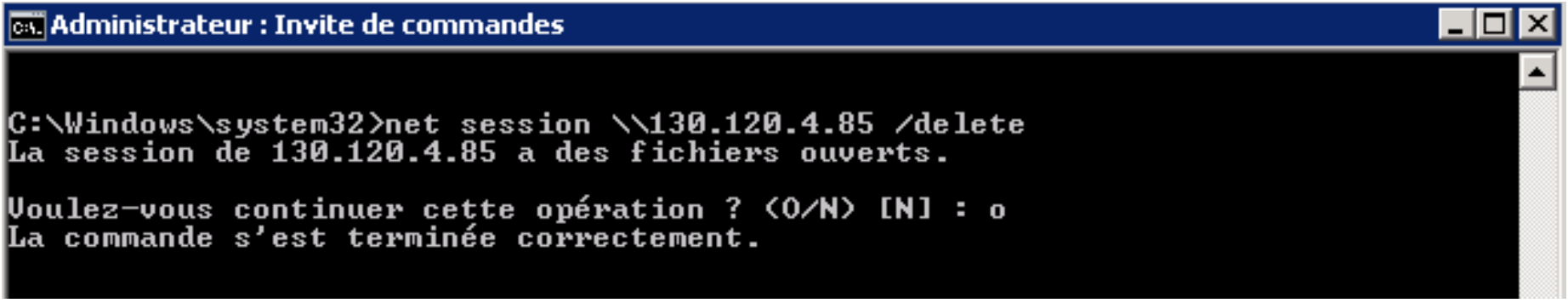
Listing des sessions ouvertes :



Les commandes NET

NET SESSION

Fermeture d’une session



Les commandes “NETSH”

- **Gestion du Firewall :**
  - `netsh advfirewall firewall`
- **Gestion de l’interface réseau :**
  - `netsh interface`

Autres contextes :

```
bridge
dhcpclient
ipsec
winhttp
winsock
...
```

Les commandes NETSH

NETSH INTERFACE

Changement d'une adresse IP fixe

```
C:\>netsh interface ip set address name="Connexion au réseau local" static 192.1
68.1.110 255.255.255.0 192.168.0.254


C:\>ipconfig

Configuration IP de Windows


Carte Ethernet Connexion au réseau local :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::d63:9272:839:4ed2%13
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.110
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.0.254
```

```
C:\>netsh interface ip set address name="Connexion au réseau local" source=dhcp
```

Les commandes NETSH

NETSH ADVFIREWALL

Exemple d'ajout d'une règle

```
netsh advfirewall firewall add rule name="Open
Port 80" dir=in action=allow protocol=TCP
localport=80
```

Les Outils Windows en ligne de commande pour l'administrateur systèmes et réseaux

MERCI

Les sources :

https://**technet**.microsoft.com/

http://ss64.com

Jean-François Costecèque
DSI UT3 - Pôle Infrastructure
Équipe Gestion de parc

UNIVERSITÉ TOULOUSE III PAUL SABATIER
Université de Toulouse

Outil de surveillance ARPWatch

ARPWatch

Jean-François Costecèque
DSI UT3 - Pôle Infrastructure
Équipe Gestion de parc

UNIVERSITÉ TOULOUSE III PAUL SABATIER
Université de Toulouse

Outil de surveillance ARPWatch

Présentation

- **Écoute passive du réseau**
- **Basé sur ARP (table de correspondance IP/MAC)**
- **Envoie d'alertes par mail**
- **Base de donnée facilement exploitable**

Outil de surveillance ARPWatch

Installation

- **Exemple d'Installation Debian**
  - `sudo apt-get install arpwatch`
- **Edition du fichier de conf**
  - `sudo vi/etc/arpwatch.conf`

```
eth0 -n 130.120.64.0/22  -m jean-francois.costeceque@univ-tlse3.fr
```

- **(re)Démarrer le service**
  - `sudo /etc/init.d/arpwatch restart`

Outil de surveillance ARPWatch

Les alertes

- **Nouvelle machine**
  - **Cette adresse MAC n'avait jamais été vue sur le réseau**
- **Nouvelle Activité**
  - **Cette paire IP/MAC n'avait pas été vue depuis 6 mois**
- **Changement d'adresse MAC**
  - **L'adresse IP est liée à une nouvelle MAC**
- **Flip-Flop**
  - **Bascule entre deux adresses MAC**

Outil de surveillance ARPWatch

Exemple d'alerte

```
FLIP-FLOP
hostname: FMR-APPAR-01.ups-tlse.fr
            ip address: 130.120.65.41
             interface: eth0
     ethernet address: b8:ca:3a:bd:9f:03
      ethernet vendor: Dell Inc.
old ethernet address: 00:13:72:77:ad:10
 old ethernet vendor: Dell Inc.
             timestamp: Tuesday, November 3,
2015 12:19:02 +0100
  previous timestamp: Monday, November 2,
2015 15:30:26 +0100
                delta: 20 hours
```

Outil de surveillance ARPWatch

Exemple d'extraction du fichier arp.dat

Recherche par l'adresse IP 130.120.65.41

```
root@testreseau:/# grep 130.120.65.41 /var/lib/arpwatch/arp.dat
b8:ca:3a:bd:9f:03       130.120.65.41   1447159393                  eth0
00:13:72:77:ad:10       130.120.65.41   1446554478                  eth0
root@testreseau:/# _
```

Outil de surveillance ARPWatch

MERCI

Les sources :

Lawrence Berkeley National Laboratory

http://ee.lbl.gov/

Jean-François Costecèque
DSI UT3 - Pôle Infrastructure
Équipe Gestion de parc

UNIVERSITÉ TOULOUSE III PAUL SABATIER
Université de Toulouse