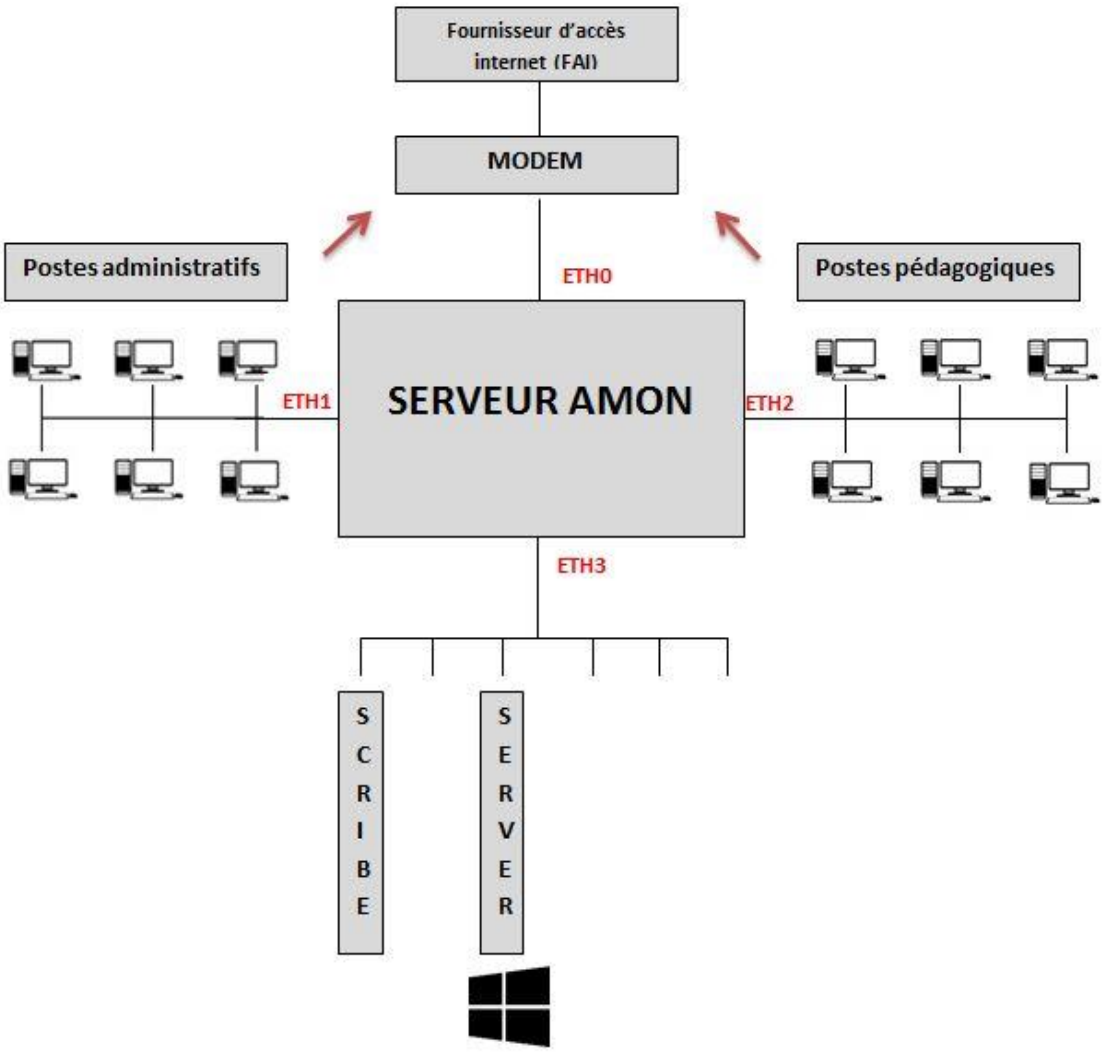
Diagnostique de serveur d'établissement

Au sein de mon service, nous sommes amenés à intervenir sur des connexions de serveur Amon, Horus et Scribe d'établissement.

Ce tutoriel concerne un serveur Amon. Pour des raisons de sécurité certaines données sont modifiée ou cachées.

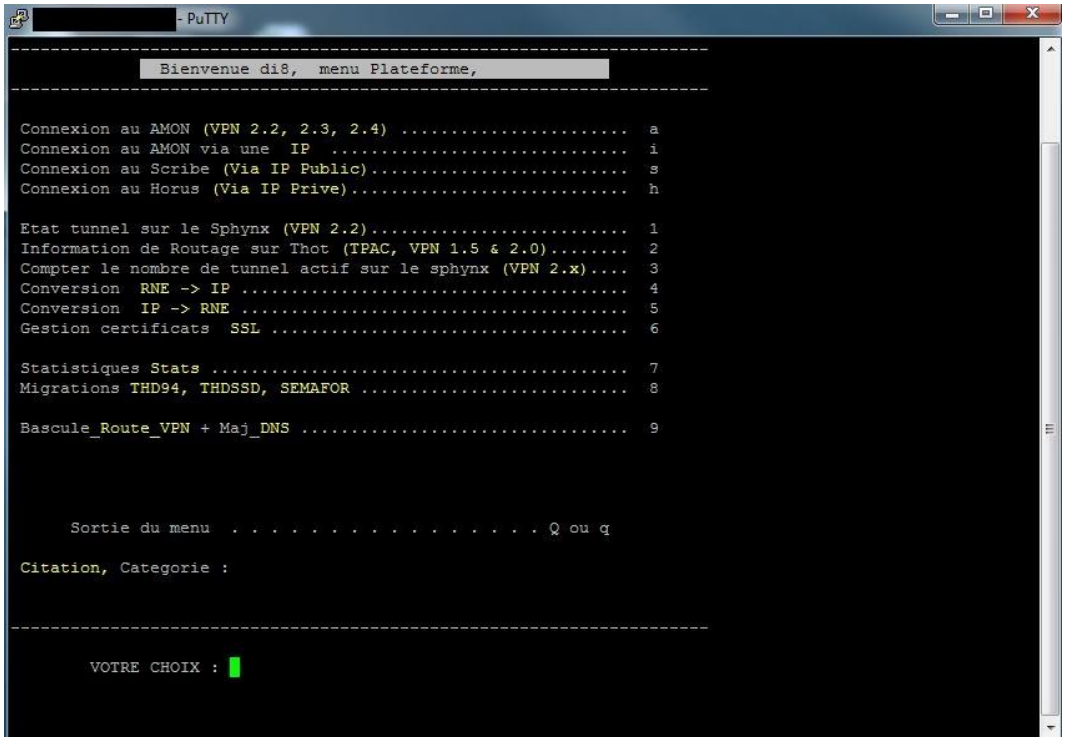
http://aduchateau.fr.ht	**Lycée Professionnel Jacques Prévert BTS SIO**	**Adrien Duchateau**

Le schéma type d'un établissement :

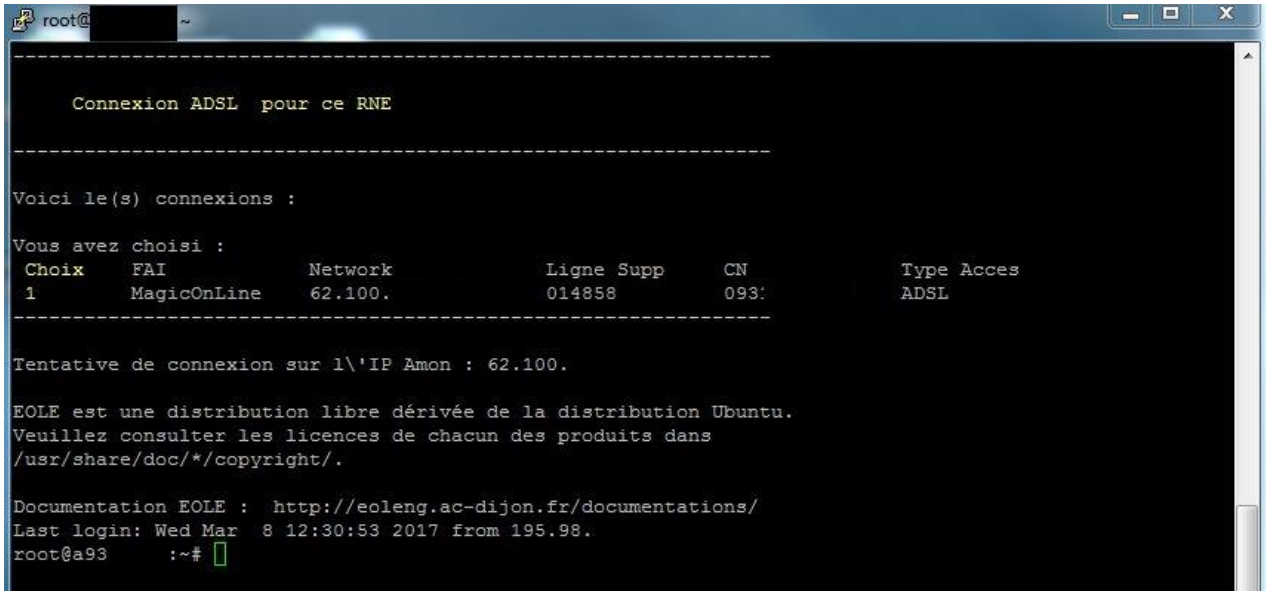


Pour accéder au serveur Amon de l'établissement, nous nous connectons en SSH (protocole de communication sécurisé) via PUTTY sur notre serveur.

Il faut saisir le code « a » pour obtenir la gestion des serveurs Amon.



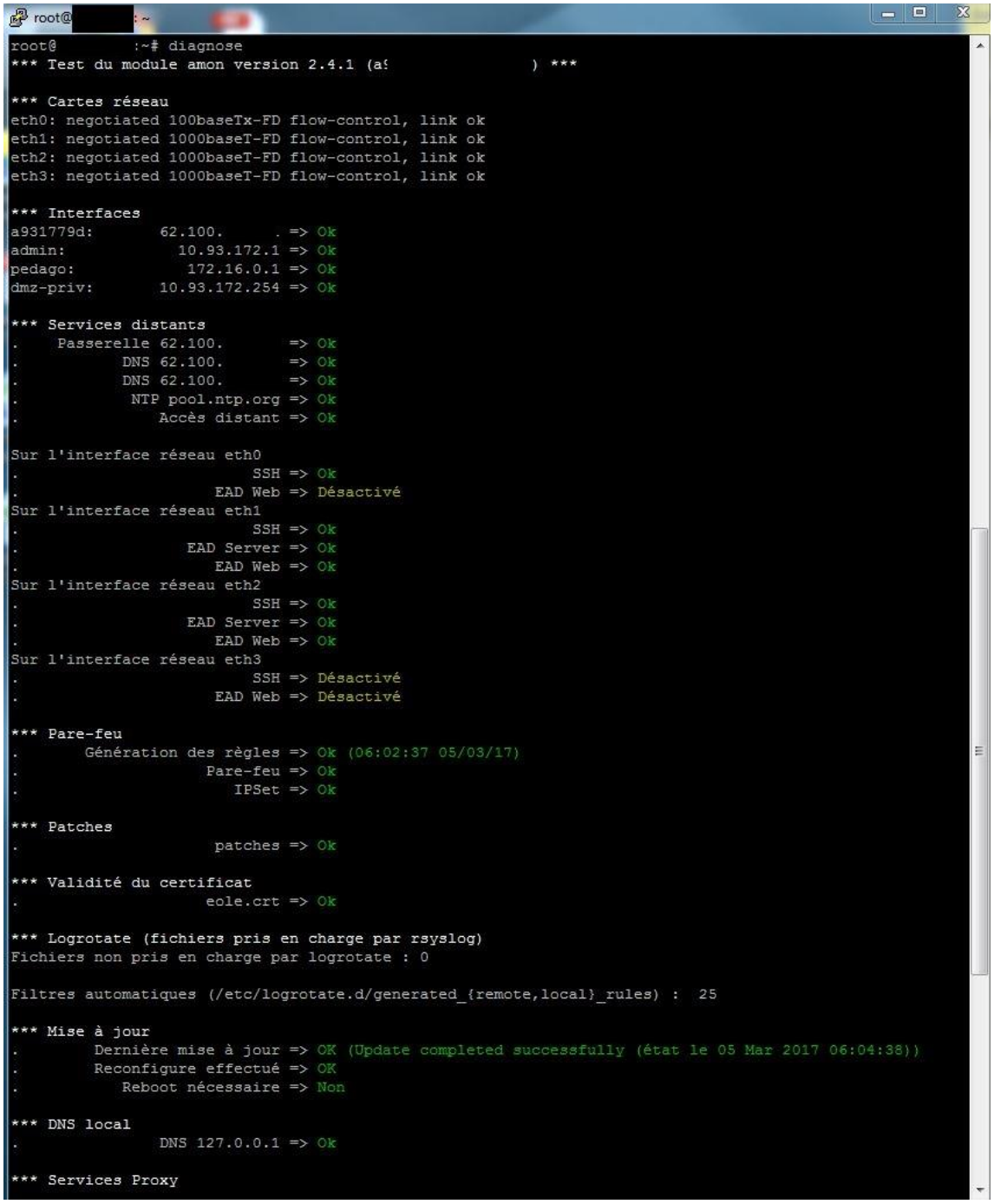
Une fois le code saisit, il est demandé de saisir le code RNE de l'établissement (propre à chaque établissement), nous voici sur le serveur Amon.



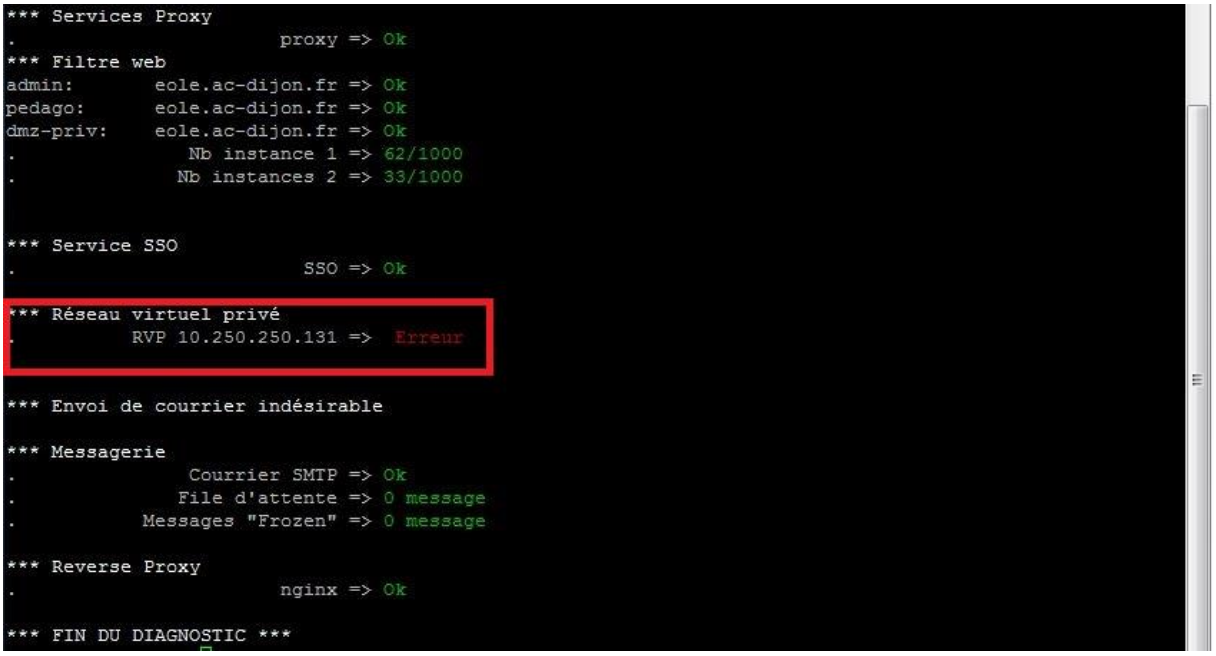
Lors de chaque connexion, pour diagnostiquer le serveur il faut entrer la commande « **diagnose** »

Nous obtenons en résultat :

La présence des cartes réseaux, les interfaces, les serveurs distants, l'état du pare feu et des patches, la validité de certificat, l'état des mises à jour, le DNS, le proxy, l'état des filtres, le service SSO (méthode permettant à un utilisateur d'accéder à plusieurs applications), l'état du réseau virtuel privé et l'état du serveur de messagerie



```
root@        :~# diagnose
*** Test du module amon version 2.4.1 (a                ) ***

*** Cartes réseau
eth0: negotiated 100baseTx-FD flow-control, link ok
eth1: negotiated 1000baseT-FD flow-control, link ok
eth2: negotiated 1000baseT-FD flow-control, link ok
eth3: negotiated 1000baseT-FD flow-control, link ok

*** Interfaces
a931779d:       62.100.      . => Ok
admin:            10.93.172.1 => Ok
pedago:            172.16.0.1 => Ok
dmz-priv:       10.93.172.254 => Ok

*** Services distants
.    Passerelle 62.100.       => Ok
.           DNS 62.100.       => Ok
.           DNS 62.100.       => Ok
.           NTP pool.ntp.org => Ok
.              Accès distant => Ok

Sur l'interface réseau eth0
.                         SSH => Ok
.                    EAD Web => Désactivé
Sur l'interface réseau eth1
.                         SSH => Ok
.                  EAD Server => Ok
.                    EAD Web => Ok
Sur l'interface réseau eth2
.                         SSH => Ok
.                  EAD Server => Ok
.                    EAD Web => Ok
Sur l'interface réseau eth3
.                         SSH => Désactivé
.                    EAD Web => Désactivé

*** Pare-feu
.       Génération des règles => Ok (06:02:37 05/03/17)
.                   Pare-feu => Ok
.                      IPSet => Ok

*** Patches
.                     patches => Ok

*** Validité du certificat
.                    eole.crt => Ok

*** Logrotate (fichiers pris en charge par rsyslog)
Fichiers non pris en charge par logrotate : 0

Filtres automatiques (/etc/logrotate.d/generated_{remote,local}_rules) :  25

*** Mise à jour
.        Dernière mise à jour => OK (Update completed successfully (état le 05 Mar 2017 06:04:38))
.        Reconfigure effectué => OK
.           Reboot nécessaire => Non

*** DNS local
.              DNS 127.0.0.1 => Ok

*** Services Proxy
```

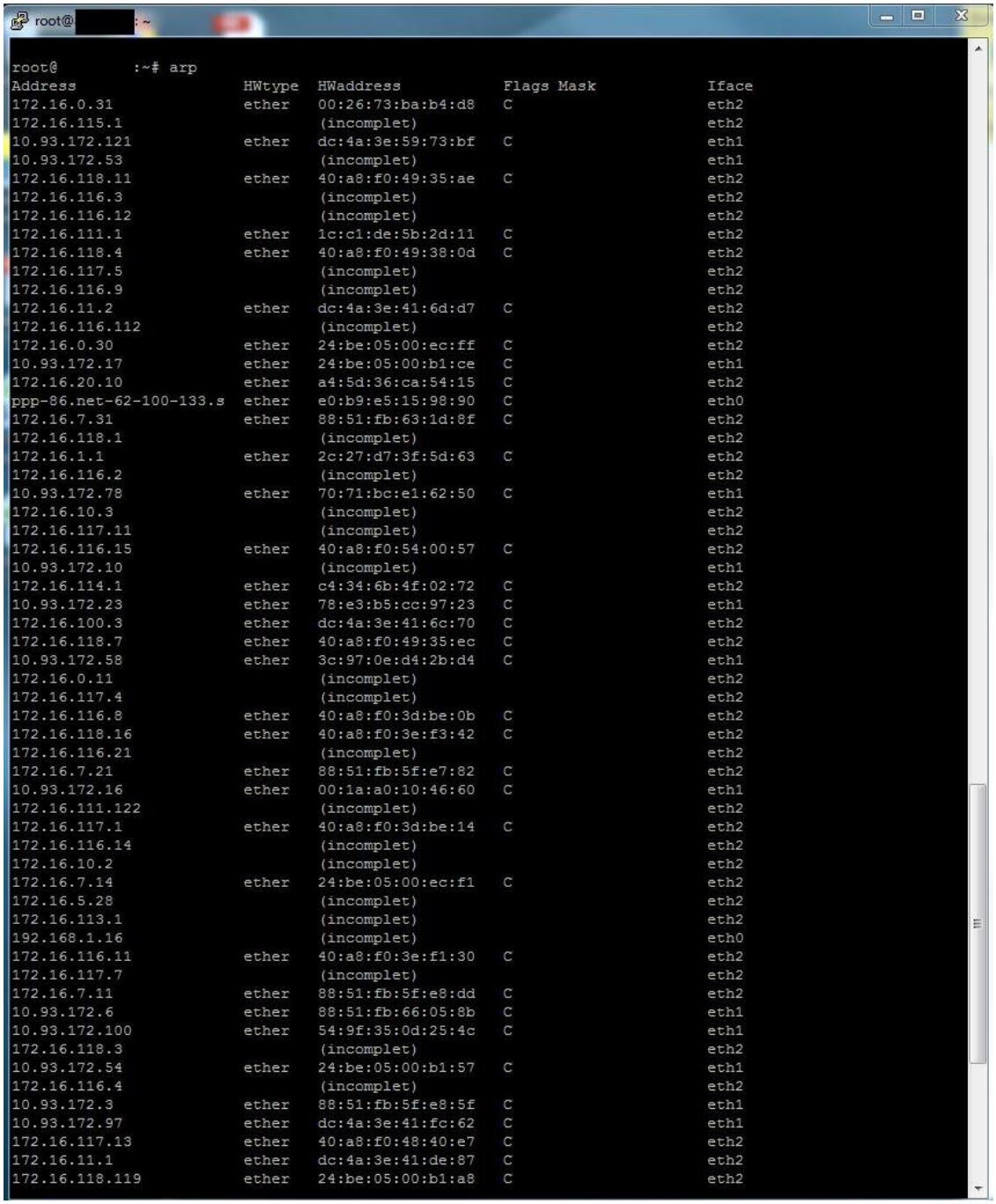


L'accès au réseau intranet du rectorat se fait via un tunnel VPN établi entre le serveur Amon de l'établissement et l'équipement concentrateur au rectorat.

L'état du réseau privé virtuel en « **Erreur** » indique que les utilisateurs ne pourront pas accéder aux applications d'intranet (par exemple http://sconet.in.ac-creteil.fr)

Pour résoudre le problème, la saisie de la commande « **service RVP restart** » peut corriger cela.

Il est possible d'observer les IPs présentes sur le réseau avec la commande « **arp** » (protocole de résolution d'adresse)



```
root@        :~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.0.31              ether   00:26:73:ba:b4:d8   C                     eth2
172.16.115.1                     (incomplet)                               eth2
10.93.172.121            ether   dc:4a:3e:59:73:bf   C                     eth1
10.93.172.53                     (incomplet)                               eth1
172.16.118.11            ether   40:a8:f0:49:35:ae   C                     eth2
172.16.116.3                     (incomplet)                               eth2
172.16.116.12                    (incomplet)                               eth2
172.16.111.1             ether   1c:c1:de:5b:2d:11   C                     eth2
172.16.118.4             ether   40:a8:f0:49:38:0d   C                     eth2
172.16.117.5                     (incomplet)                               eth2
172.16.116.9                     (incomplet)                               eth2
172.16.11.2              ether   dc:4a:3e:41:6d:d7   C                     eth2
172.16.116.112                   (incomplet)                               eth2
172.16.0.30              ether   24:be:05:00:ec:ff   C                     eth2
10.93.172.17             ether   24:be:05:00:b1:ce   C                     eth1
172.16.20.10             ether   a4:5d:36:ca:54:15   C                     eth2
ppp-86.net-62-100-133.s  ether   e0:b9:e5:15:98:90   C                     eth0
172.16.7.31              ether   88:51:fb:63:1d:8f   C                     eth2
172.16.118.1                     (incomplet)                               eth2
172.16.1.1               ether   2c:27:d7:3f:5d:63   C                     eth2
172.16.116.2                     (incomplet)                               eth2
10.93.172.78             ether   70:71:bc:e1:62:50   C                     eth1
172.16.10.3                      (incomplet)                               eth2
172.16.117.11                    (incomplet)                               eth2
172.16.116.15            ether   40:a8:f0:54:00:57   C                     eth2
10.93.172.10                     (incomplet)                               eth1
172.16.114.1             ether   c4:34:6b:4f:02:72   C                     eth2
10.93.172.23             ether   78:e3:b5:cc:97:23   C                     eth1
172.16.100.3             ether   dc:4a:3e:41:6c:70   C                     eth2
172.16.118.7             ether   40:a8:f0:49:35:ec   C                     eth2
10.93.172.58             ether   3c:97:0e:d4:2b:d4   C                     eth1
172.16.0.11                      (incomplet)                               eth2
172.16.117.4                     (incomplet)                               eth2
172.16.116.8             ether   40:a8:f0:3d:be:0b   C                     eth2
172.16.118.16            ether   40:a8:f0:3e:f3:42   C                     eth2
172.16.116.21                    (incomplet)                               eth2
172.16.7.21              ether   88:51:fb:5f:e7:82   C                     eth2
10.93.172.16             ether   00:1a:a0:10:46:60   C                     eth1
172.16.111.122                   (incomplet)                               eth2
172.16.117.1             ether   40:a8:f0:3d:be:14   C                     eth2
172.16.116.14                    (incomplet)                               eth2
172.16.10.2                      (incomplet)                               eth2
172.16.7.14              ether   24:be:05:00:ec:f1   C                     eth2
172.16.5.28                      (incomplet)                               eth2
172.16.113.1                     (incomplet)                               eth2
192.168.1.16                     (incomplet)                               eth0
172.16.116.11            ether   40:a8:f0:3e:f1:30   C                     eth2
172.16.117.7                     (incomplet)                               eth2
172.16.7.11              ether   88:51:fb:5f:e8:dd   C                     eth2
10.93.172.6              ether   88:51:fb:66:05:8b   C                     eth1
10.93.172.100            ether   54:9f:35:0d:25:4c   C                     eth1
172.16.118.3                     (incomplet)                               eth2
10.93.172.54             ether   24:be:05:00:b1:57   C                     eth1
172.16.116.4                     (incomplet)                               eth2
10.93.172.3              ether   88:51:fb:5f:e8:5f   C                     eth1
10.93.172.97             ether   dc:4a:3e:41:fc:62   C                     eth1
172.16.117.13            ether   40:a8:f0:48:40:e7   C                     eth2
172.16.11.1              ether   dc:4a:3e:41:de:87   C                     eth2
172.16.118.119           ether   24:be:05:00:b1:a8   C                     eth2
```

La commande « **arp** » peut être complétée de la mention « **| grep eth1** »

C'est pour permettre de faire la résolution d'adresse d'IPv4 en adresse MAC et cela seulement pour les ordinateurs présents sur le réseau **eth1** qui correspond au personnel administratif.