Connexion à un réseau local

Configuration et dépannage

Philippe Latu
Linux France
philippe.latu@linux-france.org

Connexion à un réseau local: Configuration et dépannage

par Philippe Latu

Découverte des caractéristiques logicielles et matérielles d'une connexion réseau. Dans un contexte de maintenance ce support fournit une méthodologie simple de localisation de défaut tandis que dans le cas d'une formation, il montre comment s'organisent les différents composants de la connexion réseau.

L'interconnexion réseau est abordée à partir des outils Unix classiques : **arp**, **ifconfig** et **route**.

Copyright et Licence

Historique des versions

Version Revision: 1.7 Date: 2000/09/13 19:09:21 Revu par : PL
Edition 2001

Table des matières

1. Configurer et Dépanner Ethernet 1
1.1. Les éléments du réseau 1
1.1.1. Ethernet et le modèle OSI 1
1.1.2. Les normes IEEE 802.3 1
1.1.3. Format de trame 3
1.1.4. Travaux pratiques 4
1.2. Configuration de l'interface 4
1.2.1. Commande **ifconfig** 4
1.2.2. Commande **ping** 5
1.2.3. Commande **arp** 7
1.2.4. Commande **host** 8
1.2.5. Travaux pratiques 8
1.3. Routage 8
1.3.1. Commande **route** 9
1.3.2. Commande **traceroute** 9
1.3.3. Travaux pratiques 9
1.4. Dépannage 10
1.4.1. Trop de bruit 10
1.4.2. Trop de collisions 10
1.4.3. Trop de trames *runt* 10
1.4.4. Collisions tardives 10
1.4.5. Pas de lien 11
1.4.6. Problèmes d'adressage IP 11
2. Analyse réseau 12
2.1. Analyse avec Ethereal 12
2.1.1. Capture d'une série de trame 12
2.1.2. Filtrage d'une série 13
2.2. Travaux pratiques 14
3. Analyse des services 16
3.1. Commande **netstat** 16
3.2. Configuration des services 16

Liste des tableaux

1-1. Caractéristiques des connexions 2

Chapitre 1. Configurer et Dépanner Ethernet

Ethernet illustre parfaitement les caractéristiques des connexions aux réseaux locaux. Pour maintenir un réseau local Ethernet il faut : montrer comment cette technologie s'intègre dans la modélisation, présenter les normes, les différents type de connexions et les formats de trames. Ensuite, il faut introduire les outils de configuration et de maintenance associés aux réseaux locaux.

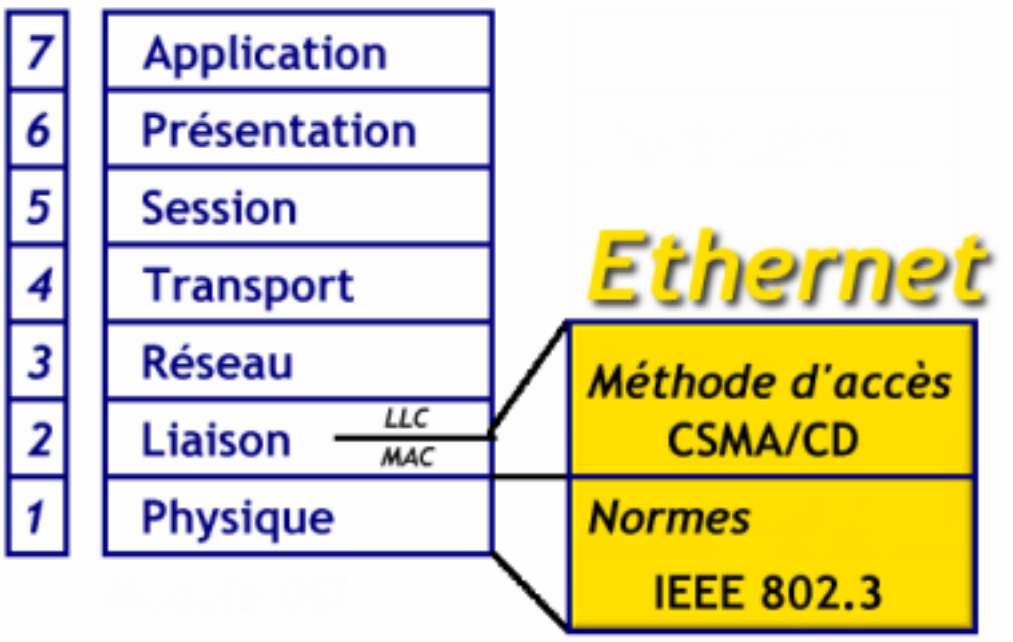
Pour obtenir plus de détails sur la modélisation réseau, l'adressage IP et la technologie Ethernet, consultez les articles de référence sur le site *inetdoc* (../../articles/). Avoir lu ces articles est le seul prérequis pour aborder ce document.

1.1. Les éléments du réseau

1.1.1. Ethernet et le modèle OSI

Ethernet a été développé à l'origine pour combler le vide entre les réseaux longues distances à faibles débits et les connexions spécialisées utilisées pour transporter les données entre ordinateurs dans une même salle. Cette technologie est donc adaptée aux communications locales à hauts débits.

Ethernet recouvre les couches Physique et la sous-couche MAC de la modélisation OSI :



Note : Le Modèle d'Interconnexion des Systèmes Ouverts (OSI) est décrit dans l'article *Modélisations Réseau* (http://www.linux-france.org/prj/inetdoc/articles/model/)

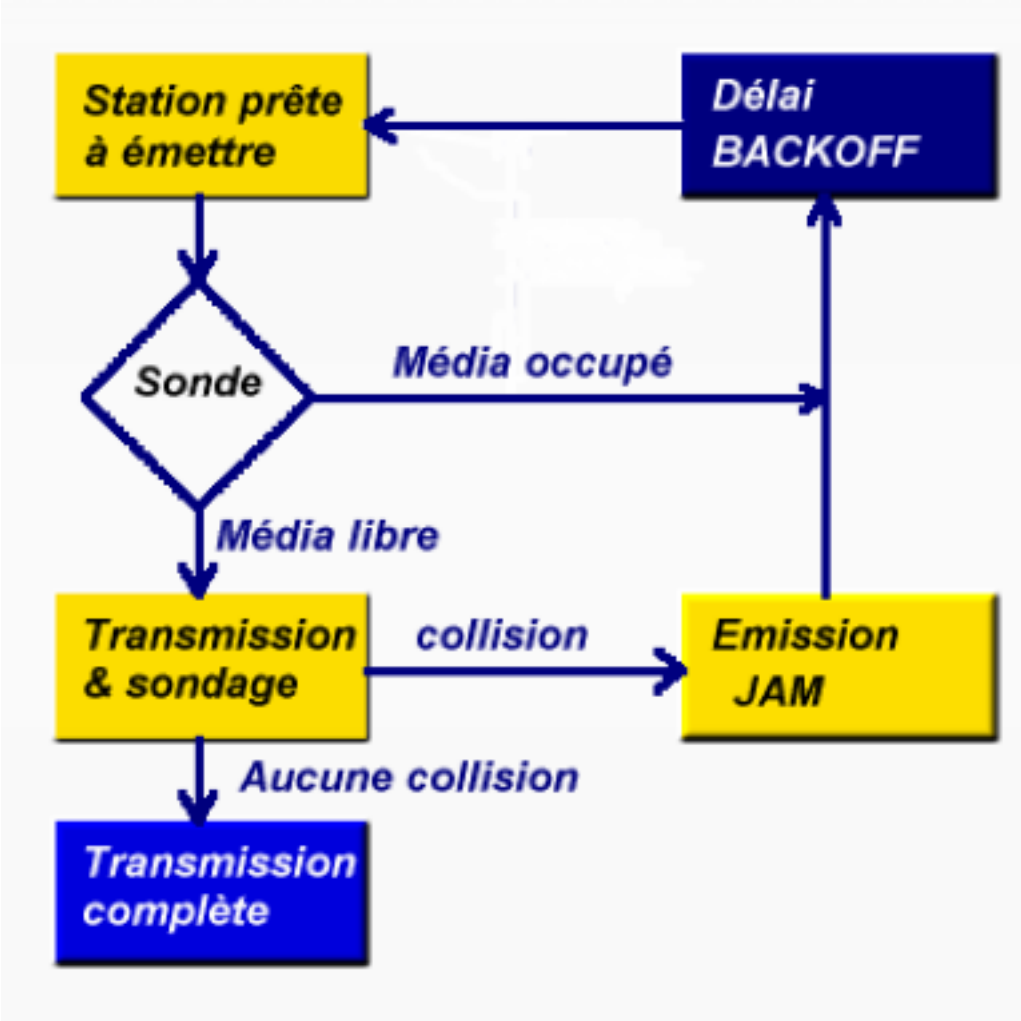
1.1.2. Les normes IEEE 802.3

Les dénominations Ethernet et IEEE 802.3 sont similaires. Elles désignent des réseaux locaux utilisant la méthode d'accès CSMA/CD.

1.1.2.1. La méthode d'accès

La méthode d'accès *Carrier Sense Media Access with Collision Detection* CSMA/CD constitue le principe de base des réseaux Ethernet. Elle définit les conditions d'émission et de réception des données sur le média.

Avant d'émettre, une station « écoute » le réseau. Si le média est « occupé » la station attend, sinon elle émet. Une collision intervient lorsque deux stations émettent simultanément. Dans ce cas, les stations réémettent après un temps d'attente aléatoire appelé BACKOFF.



Méthode d'accès

Les réseaux Ethernet sont des réseaux de *diffusion*. Tous les équipements « voient » toutes les trames indépendamment de leur destination. Chaque équipement doit examiner toutes les trames pour savoir si l'une d'entre elles lui est destinée.

1.1.2.2. Les connexions physiques

Le tableau suivant résume les différents types de connexions Ethernet :

Tableau 1-1. Caractéristiques des connexions

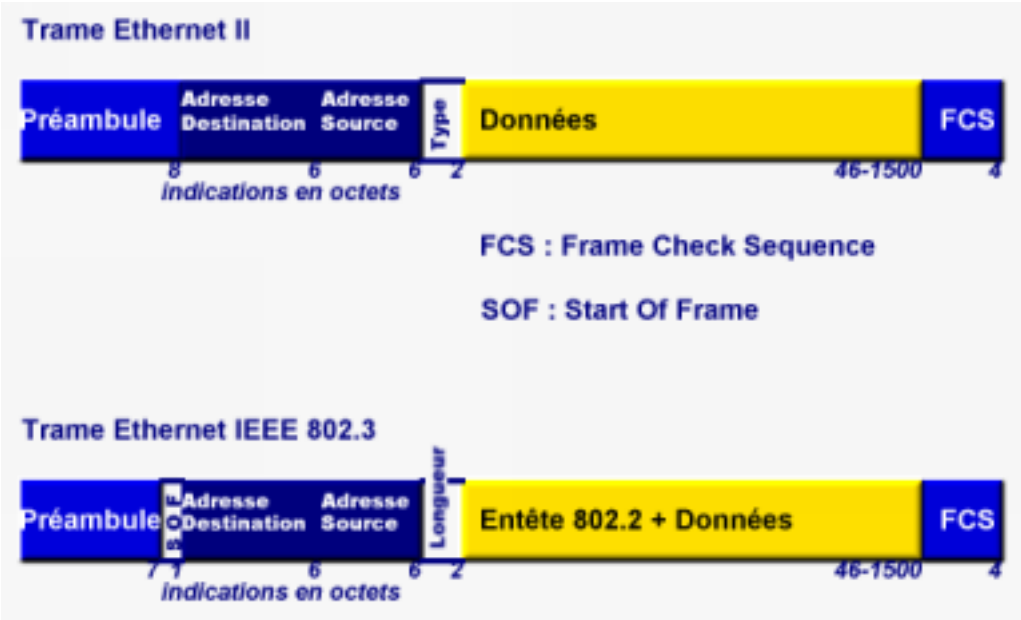
Appelation	Débit	Longueur maximum	Média	Topologie

Appelation	Débit	Longueur maximum	Média	Topologie
Thick Ethernet 10Base5	10Mbps	500m	Coaxial 50 Ohms N-BNC	Bus
Thin Ethernet 10Base2	10Mbps	185m	Coaxial 50 Ohms BNC	Bus
10BaseT	10Mbps	100m	UTP cat. 3	Etoile
10BaseFL	10Mbps	2Km	f.o. multimode	Point à point
100BaseTX	100Mbps	100m	UTP cat. 5	Etoile
100BaseFX	100Mbps	400m	f.o. multimode	Point à point
1000BaseLX	1000Mbps	3Km	f.o. multimode	Point à point
1000BaseCX	1000Mbps	25m	STP 150 Ohms	Etoile
1000BaseTX	1000Mbps	100m	FTP cat. 5	Etoile

- UTP : Unshielded Twisted Pair ; paire torsadée non blindée.
- STP : Shielded Twisted Pair ; paire torsadée blindée.
- cat. : catégorie ; bande passante = 100MHz pour la catégorie 5.
- f.o. : Fibre Optique.

> **Note :** On trouve une description précise et détaillée de l'ensemble des dispositifs de connexion sur le site de *l'Université de Genève* (http://www.unige.ch/seinf/jfl/elem/etherhom.htm)

1.1.3. Format de trame



Les 2 types de trames reconnues

> **Note :** Le détail des définitions des champs des trames Ethernet est fourni dans l'article *Technologie Ethernet* (http://www.linux-france.org/prj/inetdoc/articles/ethernet)

En règle générale, les deux types de trames sont employés sur des réseaux différents :

- Le format IEEE 802.3 est surtout utilisé sur les réseaux IPX.
- Le format Ethernet II est utilisé sur tous les réseaux TCP/IP dont l'Internet.

1.1.4. Travaux pratiques

1. Avec quel type de câble est connecté votre station ?

coaxial, paire torsadée ou fibre optique.

2. Quelle est la topologie utilisée pour le câblage de la salle ?

bus, étoile ou point-à-point.

3. Quel est le débit maximum de la connexion ?

10Mbps, 100Mbps ou 1000Mbps.

4. Ce débit maximum est-il disponible pour chacune des stations ?

oui dans le cas d'un réseau commuté ou non dans le cas d'un réseau partagé. Consulter l'article *La segmentation des réseaux locaux* (../../articles/route-switch/).

5. A quel élément actif votre station est-elle reliée ?

pont, routeur, hub ou commutateur.

6. Quelles sont les couches du modèle OSI traitées par cet élément actif ?

physique, liaison, réseau ,transport et application.

1.2. Configuration de l'interface

Pour configurer une interface réseau, il faut utiliser les commandes de base disponibles sur n'importe quel système Unix. Voici une présentation succinte des commandes classiques de configuration et de test d'une connexion réseau : **ifconfig**, **ping**, **arp** et **host**.

Avant d'aborder les questions de travaux pratiques, il faut tester les différentes options de ces commandes.

1.2.1. Commande ifconfig

ifconfig sert à fixer les paramètres d'une interface ; eth0 dans notre exemple.

1.2.1.1. Etat de l'interface

```
[linuxBox]$ /sbin/ifconfig -a
eth0      Lien encap:Ethernet  HWaddr 00:50:04:4C:28:27 (1)
          inet adr:192.168.1.1  Bcast:192.168.1.255  Masque:255.255.255.0 (2)
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1 (3)
          Paquets Reçus:134 erreurs:0 jetés:0 débordements:0 trames:0   (4)
```

```
          Paquets transmis:17 erreurs:0 jetés:0 débordements:0 carrier:0
          collisions:0 lg file transmission:100
          Interruption:10 Adresse de base:0xe000  (5)

lo        Lien encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          Paquets Reçus:13599 erreurs:0 jetés:0 débordements:0 trames:0
          Paquets transmis:13599 erreurs:0 jetés:0 débordements:0 carrier:0
          collisions:0 lg file transmission:0
```

(1) Informations sur la couche liaison (2) :
- `encap:Ethernet` = format de trame Ethernet II.
- `HWaddr ...` = Adresse MAC de la carte réseau.

(2) Informations sur la couche réseau (3) :
- `inet adr:` = adresse IP de l'interface.
- `Bcast:` = adresse de diffusion du réseau.
- `Masque:` = masque de sous-réseau.

(3) Informations sur l'état de l'interface :
- `UP BROADCAST RUNNING MULTICAST` = interface de diffusion active.
- `MTU:1500` = Maximum Transmission Unit. La taille maximum des trames Ethernet transmises sur Internet est fixée par le document *RFC 1191*.
- `Metric:1` = nombre de sauts autorisés pour obtenir un routage vers n'importe quelle destination.

(4) Statistiques de l'interface. Ces informations sont essentielles pour déterminer la « qualité » du réseau.

(5) Paramètres d'entrées/sorties de l'interface. Ces informations indiquent si la carte réseau est correctement reconnue par le système.

1.2.1.2. Configurer l'interface

Typiquement, on configure une interface Ethernet avec une commande du type :

```
[linuxBox]$ ifconfig eth0 192.168.1.1 netmask 255.255.255.0 up
```

La commande **ifconfig** possède de nombreuses options. Les principales sont :

- `up` : activation de l'interface,
- `down` : désactivation de l'interface,
- `[-]arp` : activation/désactivation du protocole ARP sur l'interface,
- `netmask <addr>` : valeur du masque de réseau,
- `broadcast <addr>` : valeur de l'adresse de diffusion.

Pour obtenir la syntaxe de toutes les options disponibles, il faut utiliser la commande **man ifconfig** ou **kdehelp** : **System man page contents**⟶**Section 8 Administration système**⟶**ifconfig**.

1.2.2. Commande ping

ping sert à tester la communication à travers une interface. Cette commande utilise un protocole particulier : *Internet Control Message Protocol* ou ICMP. Ce protocole est décrit dans le document *RFC792* (http://sunsite.cnlab-switch.ch/ftp/doc/standard/rfc/7xx/792).

Comme le protocole IP n'est pas fiable, l'objectif des messages ICMP est d'obtenir des informations sur les problèmes rencontrés en cours de communication.

1.2.2.1. Etat de la pile TCP/IP

La commande suivante permet de valider le fonctionnement de *l'inter-processus* dans le système.

```
[linuxBox]$ ping -c 2 127.0.0.1
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=0.1 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=255 time=0.1 ms

--- 127.0.0.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms
```

Il s'agit ici de contrôler que les processus pairs à l'intérieur du même système sont capables de dialoguer entre eux.

On teste ensuite le fonctionnement de l'interface seule :

```
[linuxBox]$ ping -c 2 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.1 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.1 ms

--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms
```

Il s'agit ici de contrôler que l'interface réseau est bien configurée et active.

Une fois ces deux étapes franchies, on peut tester les communications avec les autres systèmes.

1.2.2.2. Tests vers l'extérieur

Exemple d'echec :

```
[linuxBox]$ ping -c 5 192.168.1.14
PING 192.168.1.14 (192.168.1.14): 56 data bytes

--- 192.168.1.14 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

Exemple de succès :

```
[linuxBox]$ ping -c 2 192.168.1.13
PING 192.168.1.13 (192.168.1.13): 56 data bytes
64 bytes from 192.168.1.13:(1) icmp_seq=0(2) ttl=255(3) time=1.1 ms
64 bytes from 192.168.1.13: icmp_seq=1 ttl=255 time=0.8 ms

--- 192.168.1.13 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.9/1.1 ms
```

(1) Adresse de réponse du message ICMP : destinataire du test.

(2) Numéro de séquence du message.

(3) La valeur du champ TTL d'un paquet IP correspond au nombre maximum d'interfaces que le paquet doit traverser pour atteindre son destinataire.

Pour obtenir la syntaxe de toutes les options disponibles, il faut utiliser la commande **man ping** ou **kdehelp** : **System man page contents⟶Section 8 Administration système⟶ping**.

1.2.2.3. Tests de la résolution des noms

Cette commande est aussi très utile pour savoir si la résolution des noms de domaines DNS fonctionne correctement.

```
[linuxBox]$ ping -c 5 www.nic.fr (1)
PING rigolo.nic.fr (192.134.4.20)(2): 56 data bytes
64 bytes from 192.134.4.20: icmp_seq=0 ttl=54 time=57.6 ms
64 bytes from 192.134.4.20: icmp_seq=1 ttl=54 time=51.0 ms
64 bytes from 192.134.4.20: icmp_seq=2 ttl=54 time=57.0 ms
64 bytes from 192.134.4.20: icmp_seq=3 ttl=54 time=109.8 ms
64 bytes from 192.134.4.20: icmp_seq=4 ttl=54 time=165.3 ms

--- rigolo.nic.fr ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 51.0/88.1/165.3 ms
```

(1) Utilisation de la commande **ping** avec un nom d'hôte au lieu d'une adresse IP.

(2) Affichage de la correspondance entre le nom de l'hôte et son adresse IP.

En cas d'echec sur la résolution des noms, il faut contrôler la validité des informations dans les deux fichiers suivants :

- `/etc/resolv.conf`

  ```
  search <domaine-fai>.fr(1)
  nameserver <addr dns-fai>(2)
  ```

  (1) Nom du domaine auquel l'interface est connectée.

  (2) Adresse IP du serveur de noms.

- `/etc/host.conf`

  ```
  order hosts, bind(1)
  multi on
  ```

  (1) Ordre de recherche des noms d'hôtes.

1.2.3. Commande arp

La commande **arp** utilise le protocole du même nom : *Address Resolution Protocol* décrit dans le document *RFC826* (http://sunsite.cnlab-switch.ch/ftp/doc/standard/rfc/8xx/826).

Elle sert à localiser un hôte du réseau local en faisant la correspondance entre l'adresse IP et l'adresse MAC de cet hôte.

Dans l'exemple suivant, on visualise la table des adresses MAC connues avec la commande **arp**.

```
[linuxBox]$ arp
Adresse       TypeMap    AdresseMat          Indicateurs    Iface
router        ether      00:60:3E:10:48:20   C              eth0
dns           ether      00:A0:24:A0:A4:11   C              eth0
```

On effectue une « localisation » sur le réseau local avec la commande **ping**.

```
[linuxBox]$ ping -c 2 server
PING server (192.168.10.10) from 192.168.10.34 : 56(84) bytes of data.
64 bytes from server (192.168.10.10): icmp_seq=0 ttl=128 time=0.9 ms
64 bytes from server (192.168.10.10): icmp_seq=1 ttl=128 time=0.4 ms

--- server ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0.4/0.6/0.9 ms
```

Le résultat de la « localisation » apparaît lorsque l'on visualise à nouveau la table des adresses MAC.

```
[linuxBox]$  arp
Adresse       TypeMap    AdresseMat          Indicateurs    Iface
router        ether      00:60:3E:10:48:20   C              eth0
dns           ether      00:A0:24:A0:A4:11   C              eth0
server        ether      00:60:97:91:60:0A   C              eth0
```

1.2.4. Commande host

La commande **host** recherche la correspondance nom - adresse Ip et vice versa :

```
[linuxBox]$ host www.yahoo.fr
www.yahoo.fr is a nickname for homerc.europe.yahoo.com
homerc.europe.yahoo.com has address 194.237.109.73
homerc.europe.yahoo.com has address 194.237.109.72
homerc.europe.yahoo.com mail is handled (pri=10) by nomail.yahoo.com

[linuxBox]$ host 194.237.109.70
70.109.237.194.IN-ADDR.ARPA is a nickname for 70.194-237-109-rev-map.europe.yahoo.com
```

Pour obtenir la syntaxe de toutes les options disponibles, il faut utiliser la commande **man host** ou **kdehelp** : **System man page contents⟶Section 1 Commandes utilisateur⟶host**.

1.2.5. Travaux pratiques

1. Quels sont les paramètres de l'interface Ethernet de la station ?

adresses MAC et IP de l'hôte, masque de réseau et adresse de diffusion.

2. Quels sont les paramètres de l'interface de la passerelle par défaut ?

Déduire, à partir de vos adresses hôte + réseau + masque, l'adresses IP de la passerelle par défaut. Généralement, il s'agit de la première adresse du réseau ou sous-réseau sur lequel l'hôte est connecté.

Cette question sera à nouveau traitée dans la partie routage.

3. Visualiser la table des adresses MAC connues de votre station avec la commande **arp**.

Tester les commandes **ping** et **host** sur une station du réseau local.

Visualiser à nouveau la table des adresses MAC avec **arp**.

Quel est le rôle du protocole ARP sur un réseau local ?

Identifier le mécanisme de résolution des adresses MAC des hôtes du réseau local.

1.3. Routage

Le routage est un sujet à part entière auquel il faut consacrer beaucoup de temps si on veut mener une étude approfondie. L'objectif de ce chapitre est limité à l'observation des routes connues de l'interface de l'hôte et à la détection de pannes.

1.3.1. Commande route

route, tout comme **ifconfig** sert à la fois à connaître l'état de la table de routage de l'hôte et à configurer de nouvelles routes au besoin.

Cette commande n'a rien à voir avec le routage dynamique qui fonctionne sur un routeur. Elle ne sert qu'à poser des routes statiques entre interfaces.

```
#>route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags(1) Metric Ref    Use Iface(2)
127.0.0.1       0.0.0.0         255.255.255.255 UH    0      0        0 lo
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
```

(1) Indicateurs d'état :

- U : Up ; l'interface est active.
- H : Host ; désigne un hôte.
- G : Gateway ; C'est l'interface à partir de laquelle on atteind les autres hôtes/réseaux.

(2) On retrouve les deux interfaces : lo l'interface de boucle locale et eth0 l'interface Ethernet.

Pour obtenir la syntaxe de toutes les options disponibles, il faut utiliser la commande **man route** ou **kdehelp** : **System man page contents**⟶**Section 8 Administration système**⟶**route**.

1.3.2. Commande traceroute

traceroute renvoie les informations sur la route suivie pour atteindre un hôte. Le résultat obtenu donne la liste des routeurs traversés.

```
#>traceroute www.nic.fr
traceroute to rigolo.nic.fr (192.134.4.20), 30 hops max, 38 byte packets
 1  toulouse-50-254-gw.dial.proxad.net (212.27.50.254)  24.806 ms  21.489 ms  21.530 ms
 2  paris11-2-p1.routers.proxad.net (212.27.32.225)  43.597 ms  33.325 ms  33.270 ms
 3  paris11-1-p1.routers.proxad.net (212.27.32.226)  149.188 ms  129.723 ms  147.430 ms
 4  sfinx.routers.proxad.net (212.27.32.167)  126.530 ms  138.881 ms  126.858 ms
 5  ri-renater.gix-paris.ft.net (194.68.129.34)  107.966 ms  132.974 ms  135.544 ms
 6  nio-i.cssi.renater.fr (193.51.206.57)  144.283 ms  122.517 ms  127.308 ms
 7  193.51.206.146 (193.51.206.146)  132.595 ms  145.998 ms  148.399 ms
 8  stlambert1.rerif.ft.net (193.48.53.102)  124.040 ms  260.685 ms  108.853 ms
 9  inria-rocquencourt-atm.rerif.ft.net (193.48.53.226)  38.604 ms  167.956 ms  143.657 ms
10  rocq-gw.inria.fr (192.93.122.2)  151.084 ms  96.052 ms  100.700 ms
11  nic-gw.inria.fr (192.93.1.112)  126.699 ms  153.840 ms *
12  rigolo.nic.fr (192.134.4.20)  155.644 ms  150.290 ms  191.674 ms
```

Dans l'exemple ci-dessus, l'hôte recherché a été trouvé. En cas de défaut, cette commande est très utile pour repérer le routeur sur lequel se situe le problème d'interconnexion.

Pour obtenir la syntaxe de toutes les options disponibles, il faut utiliser la commande **man traceroute** ou **kdehelp** : **System man page contents**⟶**Section 8 Administration système**⟶**traceroute**.

1.3.3. Travaux pratiques

1. Quels sont les paramètres de la passerelle par défaut ?

adresse IP et masque.

2. La passerelle par défaut peut-elle appartenir à un autre réseau que celui de la station ?

oui ou non.

3. Reconstituer le schéma de l'interconnexion réseau à laquelle est reliée votre station.

Identifier la station, la passerelle par défaut et les éventuels routeurs en notant les numéros de réseaux.

1.4. Dépannage

Voici quelques éléments pour dépanner les connexions Ethernet.

1.4.1. Trop de bruit

1. Utiliser la commande **ifconfig** pour obtenir le décompte des erreurs et des collisions. Un nombre d'erreurs élevé et un nombre de collisions faible traduit un niveau de bruit excessif sur les câbles.
2. Vérifier les câbles en cherchant les parties abimées : écrasement, gaine et blindage déchiré, etc.
3. Vérifier les baies de brassage : débrancher toutes les stations sauf celle à partir de laquelle on utilise **ifconfig** et rechercher par élimination le brassage défectueux.
4. Vérifier que la catégorie de câble correspond bien au débit voulu. On ne peut pas utiliser des connexions 100BaseTX sur des câbles de catégorie 3 par exemple.

1.4.2. Trop de collisions

1. Utiliser la commande **ifconfig** pour obtenir le décompte des collisions. Un taux de collision inférieur 0.1% correspond à une bonne qualité de transmission.
2. Dans le cas des câbles coaxiaux, vérifier les branchements des bouchons de terminaison.
3. Rechercher par élimination les éléments actifs (transcievers, repéteurs, etc.) qui provoquent le phénomène de *Jabber* (trames trop longues).

1.4.3. Trop de trames *runt*

1. Si le taux de collision est faible dans un réseau commuté, le problème vient probablement d'un mauvais logiciel ou d'une carte réseau défectueuse.
2. Utiliser un analyseur de réseau pour isoler les sources des trames « courtes » : phénomène de *runt*.

1.4.4. Collisions tardives

1. Généralement, les collisions tardives n'interviennent que sur des réseaux mal conçus pour lesquels les longueurs de câbles dépassent la norme.
2. Vérifier le diamètre du réseau pour s'assurer qu'il respecte bien les spécifications IEEE 802.3.

1.4.5. Pas de lien

1. Un défaut de lien intervient lorsque l'on utilise des câbles en paires torsadées :
   - non-croisés pour connecter une station à un HUB,
   - croisés pour réaliser une cascade entre commutateur/HUB et commutateur/HUB.
2. Vérifier qu'il n'y a pas d'echec d'auto négociation de bande passante entre deux éléments : 10BaseT, 10baseT Full Duplex, 100BaseTX et 100BaseTX Full Duplex.
3. Vérifier le cas *Trop de bruit*.

1.4.6. Problèmes d'adressage IP

1. A l'intérieur d'un réseau, utiliser la commande **ping** en respectant l'ordre indiqué dans la partie *Configuration de l'interface*.
2. Entre réseaux, utiliser la commande **traceroute** pour isoler l'élément d'interconnexion qui ne fonctionne pas correctement.

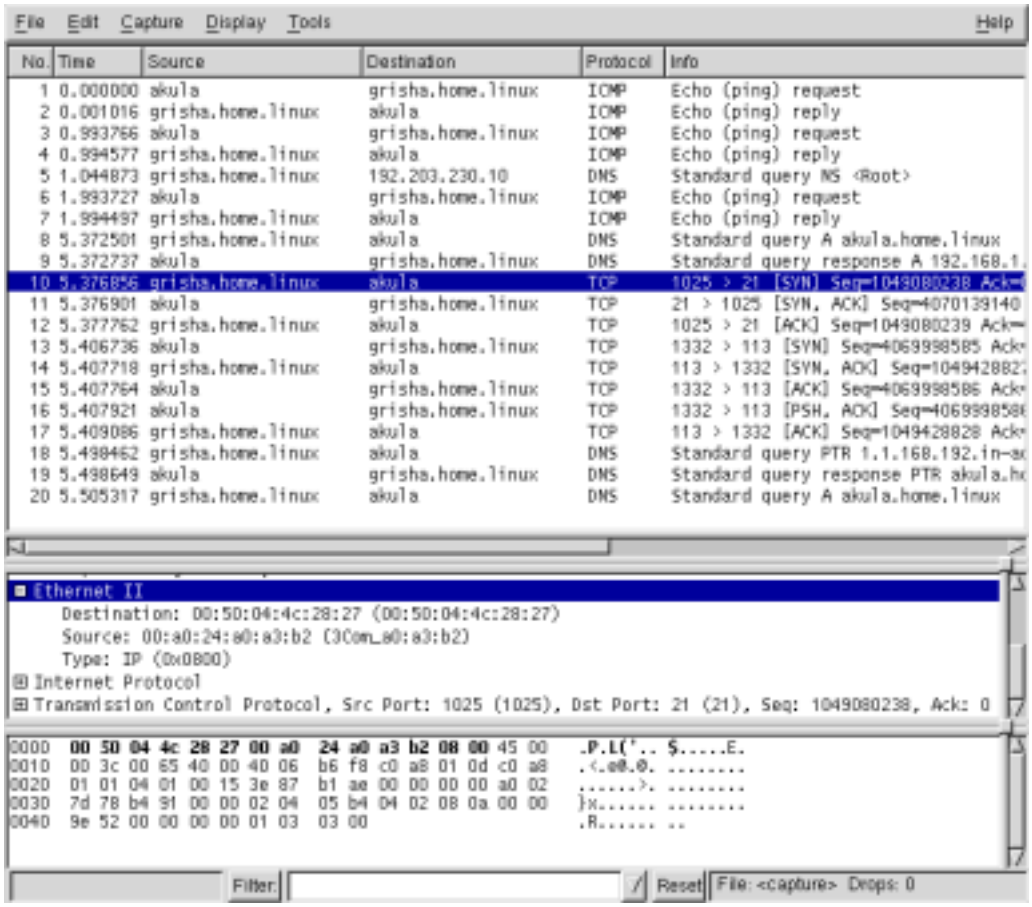
Chapitre 2. Analyse réseau

L'analyse est un thème important dans l'étude des réseaux. Ce chapitre est une introduction à l'analyse des protocoles réseau basée sur un outil issu du Logiciel Libre : *Ethereal* (http://www.ethereal.com/).

Avant d'aborder les questions de travaux pratiques sur l'analyse, il faut introduire succintement le fonctionnement de l'outil.

2.1. Analyse avec Ethereal

Ethereal (http://www.ethereal.com) est un analyseur réseau orienté transmission. Les informations qu'il collecte concernent principalement les couches basses. Voici un mini-guide d'utilisation d'*Ethereal*.



Capture d'écran Ethereal.

2.1.1. Capture d'une série de trame

Après avoir lancé le logiciel *Ethereal*, suivre la séquence suivante pour capturer une série de 60 trames :

1. Sélectionner **Capture** puis **Start**.
2. Entrer le nombre de trames à capturer dans la case count.

3. Clicker OK.

2.1.2. Filtrage d'une série

Une étape importante de l'analyse des flux réseau consiste à isoler un échange au milieu du trafic de l'ensemble du réseau. Cette opération est réalisée par filtrage en appliquant des règles avant ou après la capture.

2.1.2.1. Avant capture

Ethereal reprend la syntaxe de filtrage d'un autre outil très connu : *tcpdump*. La documentation complète sur cette syntaxe s'obtient soit en tapant **man tcpdump** à la console, soit en utilisant **kdehelp** : **System man page contents⟶Section 8 Administration système⟶tcpdump**.

Pour spécifier le type de paquets que l'on veut capturer, il suffit donc de saisir un filtre dans la case Filter: de la fenêtre **Capture**. Par exemple, pour ne capturer que les paquets IP il faut saisir : **ip**.

2.1.2.2. Après capture

Une fois la capture terminée, il est possible d'isoler par filtrage les paquets transmis par une station.

Isoler les paquets émis par un hôte

1. Dans la *fenêtre de capture*, sélectionner un paquet émis ou reçu par la station recherchée avec le bouton gauche de la souris.
2. Dans la *fenêtre de trame*, développer le niveau **Internet Protocol** et pointer l'adresse de la station.
3. Clicker sur le bouton droit de la souris et sélectionner Match selected.

La fenêtre de capture n'affiche plus que les paquets où l'adresse de la station recherchée est présente.

Isoler une connexion TCP

1. Dans la *fenêtre de capture*, sélectionner un message émis ou reçu par la station recherchée avec le bouton droit de la souris.
2. Sélectionner Follow TCP stream

Une nouvelle fenêtre apparaît. Elle contient les données vues de la couche Transport. La fenêtre de capture n'affiche plus que les paquets correspondant à la connexion TCP : établissement, transfert et libération de connexion.

2.2. Travaux pratiques

1. Adressage IP de la station

1.1. Quels sont les paramètres de l'interface Ethernet de la station ?

Il s'agit ici de retrouver les paramètres de sa propre station dans le flot des paquets capturés. On doit donc identifier les adresses MAC et IP de l'hôte sur lequel on effectue l'analyse. Ces informations ont déjà été obtenues à l'aide de la commande **ifconfig**. Il s'agit donc d'une simple vérification.

1.2. Quels sont les paramètres de l'interface de la passerelle par défaut ?

Pour se repérer dans l'interconnexion réseau, il est important de connaître les paramètres de l'interface qui fournit toutes les *routes* au réseau étudié : adresses MAC, IP et nom. Ces informations on déjà été obtenues avec la commande **route**. Avec un analyseur, on repère les interfaces de routage en capturant les échanges qui utilisent des protocoles de routage spécifiques : OSPF par exemple.

2. Encapsulation et adressage

2.1. Relevez une trame Ethernet II et recopiez sur papier son en-tête.

Après avoir choisi une trame Ethernet II dans une série capturée, repérer les en-têtes des niveaux OSI et les différentes adresses utilisées pour chacun de ces niveaux.

2.2. Quel est le type de protocole réseau utilisé ?

Repérer l'en-tête réseau. Relever les formats des adresses source et destination.

2.3. Relevez une requête **arp**. Dans quelles conditions cette requête a-t-elle été émise ?

Relever les différentes adresses source et destination pour déterminer la localisation de l'hôte visé.

3. Protocole TCP

3.1. Quels sont les niveaux OSI et les protocoles correspondant aux éléments A, B, C et D ?

Compléter le schéma ci-dessous

3.2. Relevez la séquence d'établissement d'une connexion TCP.

Il faut lancer une capture juste avant d'initier une connexion à un serveur Web par exemple.

3.3. Recopier sur papier les étapes de l'établissement de connexion.

En s'aidant de la documentation sur la couche Transport, reprendre les différents graphiques (5 étapes) en y ajoutant les paramètres de séquence propre à votre capture.

Chapitre 3. Analyse des services

Il est important de connaître et de contrôler la liste des services actifs sur une interface. Ce chapitre est une introduction à une autre commande classique du système Unix : **netstat** suivie d'une recherche documentaire sur le super-démon **inetd**.

dans cette partie, il faut faire des recherches dans les documentations pour répondre aux questions posées : pages de manuels, pages infos et le site *Linux Documentation Project* (http://www.linuxdoc.org).

3.1. Commande netstat

1. Documentation

1.1. Donner 3 sources de documentation pour la commande **netstat** ?
1.2. Quelle est la fonction de cette commande ?
1.3. Quelle est la différence entre **netstat** et un *scanner* ?

2. Utilisation de netstat

2.1. Quelle est l'option qui donne l'état des interfaces réseau ?
2.2. Quelle est l'option qui donne l'état de la table de routage ?
2.3. Quelle est l'option qui donne la liste des ports/services ouverts ?
2.4. Quelle est l'option qui donne la l'état des connexions TCP en cours ?

3.2. Configuration des services

1. Documentation

1.1. Donner une adresse Internet de documentation présentant les services TCP.
1.2. Qu'appelle-t-on un service ?
1.3. Donner quelques exemples très courants.
1.4. Donner une adresse Internet de documentation présentant le super-démon **inetd**.
1.5. Quel est le rôle de ce super-démon ?
1.6. Donner la liste des services administrables avec **inetd**.
1.7. Donner des exemples de services non administrables avec **inetd**.

2. Outils de configuration

2.1. Quel est le nom du fichier qui donne la liste des services utilisables ?
2.2. Quel est le nom du fichier de configuration du super-démon **inetd** ?
2.3. Quels sont les fichiers utilisés pour le contrôle d'accès aux services ?
2.4. Donner un exemple de configuration autorisant le transfert de fichiers entre 2 hôtes du réseau.