UPMC
PARIS UNIVERSITAS

Préparation LPI

Exam 102

111. Principes réseaux

Sommaire

- Principes TCP/IP
- TCP/IP Configuration et troubleshooting
- Configuration client PPP
- Configuration DNS

1.112.1 Principes TCP/IP

- Adressage IP
  - @ IP sur 4 octets
- Adresse de reseau
  - @ IP = @ reseau + @ hote
- Principe du masquage
  - Sur 4 octets
  - @ IP AND MASK = @ reseau
- 2 notations
  - 192.168.1.1 255.255.255.0
  - 192.168.1.1/24
  - 24 = 24 premiers bits à 1

- Nombre d'hôtes
  - Calculé sur le nombre de bits restant
  - 32-24 = 8 bits pour les hôtes
  - 2^8 - @ reseau - @ broadcast
  - @ reseau = bits restants à 0
  - @ broadcast = bits restants à 1
- Classes d '@
  - A : 1.0.0.0-127.255.255.255
  - B : 128.0.0.0-191.255.255.255
  - C : 192.0.0.0-223.255.255.255
  - D : 224.0.0.0-239.255.255.255 (multicast)
  - E : 240.0.0.0-255.255.255.255 (expérimental)

1.112.1 Principes TCP/IP

- Classes d '@ privées
  - A : 10.0.0.0-10.255.255.255
  - B : 172.16.0.0-172.31.255.255
  - C : 192.168.0.0-192.168.255.255
- Réseaux non routés sur internet
- Peuvent être routés en interne
- Subnetting : division d'un réseau en plusieurs sous-réseaux
- CIDR (Classless subnetting)
- Correspondance notation masque :
  - 255.255.255.192 <=> /24

- Exemple 1
  - 172.20.50.0 : quel type de réseau ?
  - On veut découper en 3 sous-réseaux : quels sont les masques ? Combien d'hôtes possibles ?
- Exemple 2 : @ IP 172.20.50.65 et masque 255.255.255.192. Quelle(s) @ IP n'appartient au même réseau ?
  - 172.20.50.111
  - 172.20.50.63
  - 172.20.50.126
  - 172.20.50.132

Quelques conseils LPI...

- Savoir extraire @ de réseau et @ d'hôte à partir d'une @ IP et d'un masque
- Savoir faire les conversions binaire<->decimal
- Connaître les classes d'@ privées

- Protocoles
  - IP
    - Sans connection
    - Datagrammes IP
    - Schéma d'adressage (@ IP)
    - Routage des datagrammes inter-réseaux
    - IP fournit un service d'acheminement de datagrammes

1.112.1 Principes TCP/IP

- Protocoles...
  - TCP
    - Couche transport
    - Orienté connexion
    - Retransmission des paquets TCP perdus
    - Respect de l'ordre
  - UDP
    - Couche transport
    - Orienté « performance »
    - Pas de contrôle des paquets

- Protocoles...
  - ICMP (Internet Control Message Protocol)
    - Orienté « sans connexion »
    - Utilisé pour le contrôle d'IP, informations sur les erreurs
    - Contrôle de flux
    - Détection des réseaux injoignables
    - Changement de routes
    - Contrôle des hôtes (ping)
  - PPP (Point to Point Protocol)
    - Protocole de connexion internet via une ligne série
    - cf. plus loin

Quelques conseils LPI...

- Savoir à quoi sert ICMP et dans quelles conditions l'utiliser

- Services
  - Identification des service (TCP ou UDP) par un n° de port
  - Codé sur 16 bits (1 à 65535)
  - Liste officielle gérée par l'IANA (Internet Assigned Numbers Authority)
    http://www.iana.org/assignments/port-numbers
  - Association n°port<->protocole(tcp/udp)<->nom dans `/etc/services`
  - Ports 1 à 1023 : privileged ports
  - Ports 1024 à 65535 : unprivileged ports

```
ftp-data        20/tcp
ftp-data        20/udp
# 21 is registered to ftp, but also used by fsp
ftp             21/tcp
ftp             21/udp          fsp fspd
ssh              22/tcp                      # SSH Remote Login Protocol
ssh              22/udp                       # SSH Remote Login Protocol
telnet           23/tcp
telnet           23/udp
# 24 - private mail system
lmtp             24/tcp                      # LMTP Mail Delivery
lmtp             24/udp                       # LMTP Mail Delivery
smtp              25/tcp          mail
smtp              25/udp           mail
time             37/tcp          timserver
time             37/udp           timserver
rlp              39/tcp         resource       # resource location
rlp              39/udp          resource       # resource location
nameserver       42/tcp           name           # IEN 116
nameserver       42/udp           name           # IEN 116
nicname         43/tcp          whois
```

- Fichier /etc/protocols
  - Identification dans un fichier des protocoles avec leur type IP associé

```
ip    0     IP          # internet protocol, pseudo protocol number
#hopopt 0     HOPOPT            # IPv6 Hop-by-Hop Option [RFC1883]
icmp      1     ICMP          # internet control message protocol
igmp      2     IGMP          # Internet Group Management
ggp 3     GGP           # gateway-gateway protocol
ipencap 4     IP-ENCAP    # IP encapsulated in IP (officially ``IP'')
st    5     ST          # ST datagram mode
tcp   6     TCP           # transmission control protocol
egp 8     EGP           # exterior gateway protocol
igp   9     IGP       # any private interior gateway (Cisco)
pup 12    PUP           # PARC universal packet protocol
udp 17    UDP           # user datagram protocol
hmp20     HMP           # host monitoring protocol
```

- Numéros de ports à connaître
  - 20 : ftp-data
  - 21 : ftp
  - 22 : ssh
  - 23 : telnet
  - 25 : smtp
  - 53 : serveur dns
  - 67 : serveur BOOTP/DHCP
  - 68 : client BOOTP/DHCP
  - 80 : http
  - 110 : pop3
  - 111 : portmapper

- Numéros de ports à connaître...
  - 113 : auth/ident
  - 119 : NNTP (network news transfer protocol) news
  - 139 : netbios
  - 143 : IMAP
  - 161 : SNMP
  - 177 : XDMCP
  - 389 : LDAP
  - 443 : Annuaire AD Microsoft (samba)
  - 465 : SMTPS
  - 631 : CUPS
  - 993 : IMAPS

- Numéros de ports à connaître...
  - 995 : POPS

Quelques conseils LPI...

- Connaître les noms et n° de port des services précédants

- Utilitaires TCP/IP
- `host`
  - Interrogation dns
  - host [-l] [-v] [-w] [-r] [-d] [-t types] [-a] machine [serveur]
  - Machine = @IP ou nom FQDN ou nom + domaine local (extrait via hostname) si pas terminé par un point
  - Serveur : nom ou @IP d'un serveur DNS spécifique
  - -v : mode verbeux
  - -r : supprime la recherche récursive
  - -l : liste d'un domaine complet
  - -t : précise un type d'enregistrement (filtre sur recherche sur l'ensemble d'un domaine) -t mx
  -

```
[franck@localhost ~]$ host www.lpi.org
www.lpi.org has address 24.215.7.162

[franck@localhost ~]$ host 195.42.251.40
40.251.42.195.in-addr.arpa domain name pointer www.fnac.com.

[franck@localhost ~]$ host www.ipsl.jussieu.fr
www.ipsl.jussieu.fr is an alias for weberie.ipsl.jussieu.fr.
weberie.ipsl.jussieu.fr has address 192.168.1.56
weberie.ipsl.jussieu.fr mail is handled by 100 shiva.jussieu.fr.
```

```
[franck@localhost ~]$ host -v www.formation.jussieu.fr
Trying "www.formation.jussieu.fr"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63736
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.formation.jussieu.fr.      IN      A

;; ANSWER SECTION:
www.formation.jussieu.fr. 172800 IN     A       134.157.46.132

Received 58 bytes from 192.168.1.1#53 in 34 ms
<snip>
;; ANSWER SECTION:
www.formation.jussieu.fr. 172800 IN     MX      200 soleil.uvsq.fr.
www.formation.jussieu.fr. 172800 IN     MX      100 shiva.jussieu.fr.

Received 92 bytes from 192.168.1.1#53 in 32 ms
```

- `dig`
  - Interrogation dns
  - Idem commande host mais avec plus d'options possibles

```
[franck@localhost ~]$ dig www.lpi.org

; <<>> DiG 9.5.0b1 <<>> www.lpi.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59007
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.lpi.org.                   IN      A

;; ANSWER SECTION:
www.lpi.org.            3600    IN      A       24.215.7.162

;; Query time: 675 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Mar 23 22:34:35 2009
;; MSG SIZE  rcvd: 45

[franck@localhost ~]$ host  www.lpi.org
www.lpi.org has address 24.215.7.162
```

- `ftp`
  - Transfert de fichier
  - ftp [-pinegvd] [hôte]
  - Entre dans un mode interactif
  - Options
    - -i : désactive l'option interactive dans les transferts multiples
    - -n : desactive l'autoconnexion (infos récupérées de .netrc)
    - -v : mode verbeux
    - -d : mode debug

- `ftp`...
  - Commandes
    - ! : shell interactif sur machine locale ou prefixe pour comandes locales
    - ascii : mode de transfert ascii
    - binary : mode de transfert binaire
    - bye (quit) : quitte la session ftp et quitte ftp
    - close : quitte la session ftp et reste dans l'interpréteur de commandes ftp
    - get fichier-distant [fichier-local] : récupération d'un fichier
    - mget fichiers-distants : récupération de fichiers multiples
    - mput fichiers-locaux : soumissions de fichiers multiples

- `ftp`...
  - Commandes ...
    - open : ouverture d'une connexion ftp
    - prompt : (dés)activation du mode interactif
    - put fichier-local [fichier-distant] : soumission d'un fichier
    - pwd : print working directory
    - user : identification utilisateur
    - cd; ls; dir
    - ? : help
- Connexions anonymes
  - Login : anonymous
  - Mot de passe : @ mail (ex : toto@)

- `telnet`
  - Connexion à un hôte distant via le protocole TELNET
  - telnet [-8EFKLacdfrx] [-X authtype] [-b hostalias] [-e escapechar] [-k realm] [-l user] [-n tracefile] [host [port]]
  - Si pas de host dans la commande : mode interactif (prompt telnet>)
- `ping`
  - ping [options] destination
  - -c n: n envois de paquets ECHO_REQUEST
  - -v : mode verbeux
  - -q : affiche démarrage et fin de l'exécution
  - Ctrl + c pour sortir du mode continu

- whois
  - Recherche d'information générales sur un domaine
  - Base de données au format RFC-812
  - Enregistrement des infos auprès d'un serveur whois
  - whois cible[@serveur]
    - Cible : nom de domaine ou @ IP
    - Possibilité de spécifier un serveur whois particulier
    - Sinon détermination automatique
      - whois.internic.net ou un whois.nic.xx (xx = fr par exemple)
      - whois.arin.net pour une @ Ipv4
      - whois.6bone.net pour @ IPv6

```
$ whois jussieu.fr
[Requête en cours whois.nic.fr]
[whois.nic.fr]
%%
<snip>
domain:      jussieu.fr
identified:  O
ref-id:      http://[NOT_YET_KNOWN_URL]?id=19751722000012
holder:      UNIVERSITE PARIS 6 PIERRE ET MARIE CURIE
address:     centre de Calcul Recherche, Tour 55/65,
address:     4, place Jussieu
address:     75252 Paris Cedex 5
country:     FR
<snip>

 registrar:   RENATER
 anniversary: 01/01
 created:     01/01/1995
 last-update: 11/03/2009
 ident-date:  13/06/2005
 status:      ACTIVE
```

Sommaire

1.112.3 Configuration TCP/IP et troubleshooting

- Fichiers de configuration
  - /etc/hosts
  - /etc/nsswitch.conf
  - /etc/host.conf
  - /etc/resolv.conf
  - /etc/networks

1.112.3 Configuration TCP/IP et troubleshooting

- Commandes de configuration
- `host`
  - -l : liste tout un domaine
  - -v : verbose
  - Cf nslookup et dig
- `hostname`
  - Affiche ou définit un nom d'hôte

hostname - affiche ou définit le nom d'hôte du système
domainname - affiche le nom de domaine NIS/YP du système
dnsdomainname - affiche le nom de domaine du système
nisdomainname - affiche ou définit le nom de domaine NIS/YP du système
ypdomainname - affiche ou définit le nom de domaine NIS/YP du système

1.112.3 Configuration TCP/IP et troubleshooting

- Configurer le réseau sur un poste Linux c'est définir :
  - une adresse IP + un masque de réseau + une adresse de diffusion
  - la route par défaut
  - la méthode de résolution de noms (serveur DNS)
  - un nom de machine
- Nommage des cartes réseau sous Linux
  - eth0, eth1, eth2,...
  - Commande `dmesg` renseigne entre autres sur les interfaces présentes et leur alias (ethx)
  - Fichiers de configuration `/etc/sysconfig/network-scripts/ifcfg-eth0`

1.112.3 Configuration TCP/IP et troubleshooting

- /sbin/ifconfig
  - Utilitaire de configuration des interfaces réseau
  - ifconfig -a : affiche l'état de la configuration de toutes les interfaces

```
# ifconfig -a
eth0      Lien encap:Ethernet  HWaddr 00:A0:C9:DD:F2:B3 (1)
          inet adr:134.157.45.218 Bcast:134.157.45.255
Masque:255.255.255.128 (2)
          adr inet6: fe80::2a0:c9ff:fedd:f2b3/64 Scope:Lien
        (3)UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        (4)RX packets:2282 errors:0 dropped:0 overruns:0 frame:0
           TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 lg file transmission:1000
           RX bytes:197746 (193.1 Kb)  TX bytes:6357 (6.2 Kb)
```

1.112.3 Configuration TCP/IP et troubleshooting

- (1) Infos couche liaison
  - `encap:Ethernet :` format des trames
  - `Hwaddr :` adresse matérielle de l'interface
- (2) Infos couche réseau
  - `Inet adr :` adresse IP
  - `Bcast :` adresse de diffusion (broadcast)
  - `Masque :` masque de réseau
- (3) Etat de l'interface
  - `UP.... :` Interface active
- (4) Statistiques sur le traffic de l'interface

1.112.3 Configuration TCP/IP et troubleshooting

- Modifier dynamiquement sa configuration
  - Commande `ifconfig`

```
$ /sbin/ifconfig eth0 192.168.45.1 netmask 255.255.255.0
broadcast 192.168.1.255 up
```

(1) eth0 : nom de l'interface

(2)192.168.45.1 : adresse IP de l'hôte

(3) netmask 255.255.255.0 : masque de réseau

(4) broadcast 192.168.45.255 : adresse de diffusion du réseau

(5) up : active l'interface

1.112.3 Configuration TCP/IP et troubleshooting

- Démarrer manuellement une interface
  - Commande `ifup interface`
- Stopper manuellement une interface
  - Commande `ifdown interface`

1.112.3 Configuration TCP/IP et troubleshooting

- Rendre la configuration permanente
  - 3 fichiers à modifier
    - `/etc/sysconfig/network` : contient le nom de la machine et la passerelle par défaut
    - `/etc/sysconfig/network-scripts/ifcfg-eth0` : contient les paramètres de l'interface eth0. Autant de fichier que d'interfaces actives (eth0, eth1, lo, ppp,...)
    - `/etc/resolv.conf` : contient la liste des serveurs DNS qui seront contactés pour la résolution de nom (correspondance entre un nom de machine FQDN et une adresse IP.
      Le fichier `/etc/hosts` contient des associations statiques utilisables localement
  - Redémarrer le réseau avec les nouveaux paramètres

```
$ /etc/init.d/network restart
```

1.112.3 Configuration TCP/IP et troubleshooting

- /etc/sysconfig/network

```
NETWORKING=yes (1)
HOSTNAME=nom-machine (2)
GATEWAY=192.45.45.254 (3)
```

(1) Activation de l'interface réseau

(2) Nom de la machine

(3) Adresse IP de la passerelle par défaut

1.112.3 Configuration TCP/IP et troubleshooting

- /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0 (1)
BOOTPROTO=static
IPADDR=192.168.45.1 (2)
NETMASK=255.255.255.0 (3)
NETWORK=192.168.45.0 (4)
BROADCAST=192.168.45.255 (5)
ONBOOT=yes (6)
```

(1) Alias de l'interface réseau – eth0 si une seule carte

(2) Adresse IP de la machine

(3) Masque de réseau

(4) Adresse de réseau

(5) Adresse de diffusion

(6)Activation de l'interface réseau au démarrage de la machine

1.112.3 Configuration TCP/IP et troubleshooting

- /etc/resolv.conf

```
search domain.com (1)
nameserver 192.168.45.200 (2)
```

(1) Liste de recherche pour les noms de machine

(2) Adresse IP du serveur de nom (DNS) – Plusieurs possibles

(3) Adresse IP de la passerelle par défaut

- /etc/hosts

```
127.0.0.1 (1) localhost.localdomain (2) localhost (3)
192.168.45.2 web.formation.jussieu.fr web
```

(1) Adresse IP de la machine

(2) Nom FQDN de la machine

(3) Alias – remplaçant court du nom FQDN

1.112.3 Configuration TCP/IP et troubleshooting

- Après avoir modifié les trois fichiers de configuration, il faut réactiver l'interface avec les nouveaux paramètres
  Utiliser le script /etc/init.d/network ou la commande
  `# service network restart`

```
# /etc/init.d/network restart
Arrêt de l'interface eth0 :                                [  OK  ]
Arrêt de l'interface loopback :                            [  OK  ]
Désactivation de la retransmission de paquets IPv4 :       [  OK  ]
Application des paramètres réseau                          [  OK  ]
Démarrage de l'interface loopback :                        [  OK  ]
Activation de l'interface eth0 :                           [  OK  ]
```

1.112.3 Configuration TCP/IP et troubleshooting

- La commande `ping` permet de tester l'interface
- Ping s'appuie sur le protocole ICMP destiné à contrôler les communication au niveau réseau
- Etapes pour valider une configuration correcte de l'interface :
  - Adresse IP de l'interface locale : lo (loopback)
  - Adresse IP de l'interface : eth0, ppp0
  - Adresse IP de la passerelle par défaut
  - Adresse IP extérieure au réseau local
- Paramètre
  - -c 2 : envoi de 2 paquets ICMP
  - Sans paramètre : envoi de paquets en continu. Arrêt par [Ctrl] +[C]

1.112.3 Configuration TCP/IP et troubleshooting

- `netstat`
  - -i : liste des interfaces
  - -n : mode numérique. Affiche les adresses plutôt que des noms
  - -p : affiche les processus réseau (PID, user)
  - -r : affiche les informations de route
  - -v : verbose

1.112.3 Configuration TCP/IP et troubleshooting

- Gestion des routes
  - `route` : affiche, ajoute et supprime les routes de la table de routage locale
  - route add [options] cible
  - route del [options] cible

1.112.3 Configuration TCP/IP et troubleshooting

- La table de routage locale indique le chemin que doit emprunter le trafic hors réseau local
  - L'utilitaire route permet de contrôler et de modifier les routes locales
  - **#route add default gw <@ de la passerelle>**
  - **#route del default**
  - **#route** ou **#netstat -rn** pour afficher les routes définies

```
# netstat -rn
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic   MSS Fenêtre
irtt Iface
134.157.45.128  0.0.0.0         255.255.255.128 U         0 0
 0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0
 0 eth0
0.0.0.0         134.157.45.254  0.0.0.0         UG        0 0
 0 eth0
```

1.112.3 Configuration TCP/IP et troubleshooting

- La commande **traceroute** liste les différents routeurs traversés pour atteindre une machine distante

```
# traceroute www.ipsl.jussieu.fr
traceroute to s8.ipsl.jussieu.fr (134.157.45.217), 30 hops max, 38 byte
packets
 1  d213-103-64-1.cust.tele2.fr (213.103.64.1)  23.348 ms  24.799 ms  24.928
ms
 2  lim1-core.pos9-2.swip.net (130.244.193.201)  23.978 ms  23.824 ms  23.935
ms 3  par2-core.gigabiteth3-0.swip.net (130.244.193.150)  35.826 ms  25.866 ms
 21.936 ms
 4  renater.sfinx.tm.fr (194.68.129.102)  43.572 ms  23.816 ms  24.930 ms
 5  jussieu-pos4-0.cssi.renater.fr (193.51.180.157)  41.428 ms  22.774 ms
23.932 ms
 6  rap-jussieu.cssi.renater.fr (193.51.181.101)  48.303 ms  23.878 ms  26.893
ms
 7  cr-jussieu.rap.prd.fr (195.221.126.77)  31.696 ms  23.830 ms  24.942 ms
 8  jussieu-rap.rap.prd.fr (195.221.127.182)  51.629 ms  25.818 ms  22.919 ms
 9  r-intercon.reseau.jussieu.fr (134.157.254.123)  63.246 ms  23.856 ms
23.925 ms
10  * *
```

Quelques conseils LPI...

- Savoir lire les informations affichée d'une table de routage
- Savoir ajouter une route par défaut
- Savoir détecter dans une table de routage la route qui mamnque

Sommaire

1.112.4 Configuration d'un client PPP

- PPP (Point to Point Protocol) : protocole PtP de connexion réseau entre deux équipements série (modem ou cable null modem)
- Côté client uniquement pour le LPI
- Toutes les distributions supportent normalement PPP. Sinon : recompilation du noyau en incluant « PPP support »
- Côté client ou serveur : le service pppd se charge de l'établissement de la connexion

1.112.4 Configuration d'un client PPP

- Connexion PPP
  1) Établissement d'une connexion avec un serveur PPP
     a) Config paramètres du port série
     b) Config paramètres du modem (controle de flux)
     c) Numérotation
     d)Négociation de la communication
  2) Authentification (login/mdp, PAP, CHAP, MS-CHAP)
  3) Démarrage PPP sur le client
  4) Le serveur fournit une @IP et établit un canal d'échange de données avec le client
  5) Le client configure une interface spécifique avec l'@ IP fournie et la route

1.112.4 Configuration d'un client PPP

- Ports série
  - Nommage
    - Il y longtemps : /dev/cuax
    - Maintenant (kernel 2.0.x) : /dev/ttySx
    - Lien /dev/modem -> /dev/ttyS0
- dmesg : permet de retrouver les ports coms détectés au démarrage par le noyau
- COM1 à COM4 : initialisés par défaut au boot
- setserial : interrogation et configuration des ports série
  - setserial -g /dev/ttySx
  - setserial /dev/ttyS2 port 0x2000 irq 4 uart 16650V2

1.112.4 Configuration d'un client PPP

- setserial ...
  - setserial autoconfig : à lancer après définition du port I/O, permet au noyau de déterminer une bonne valeur d'uart
  - setserial autoirq : déterminer automatiquement l'irq
- Modifications de la configuration par défaut à mettre dans le fichier /etc/rc.serial appelé en fin de séquence de boot par /etc/rc.local

- Configuration “standard » des ports série

The "standard MS-DOS" port associations are given below:

/dev/ttys0 (COM1), port 0x3f8, irq 4
/dev/ttys1 (COM2), port 0x2f8, irq 3
/dev/ttys2 (COM3), port 0x3e8, irq 4
/dev/ttys3 (COM4), port 0x2e8, irq 3

1.112.4 Configuration d'un client PPP

- chat : utilitaire de configuration/dialogue avec le modem sur un principe commande/réponse
- Commandes/réponses peuvent être envoyé au modem par un utilitaire comme minicom (« à la main ») ou via l'utilitaire chat
- Séquence type :
  - Série de réponse attendue suivie par un envoi

1.112.4 Configuration d'un client PPP

- ABORT BUSY ABORT ERROR ABORT NO CARRIER
- ABORT 'NO DAIL TONE' ABORT 'Invalid Login'
- ABORT 'Login incorrect'
- " ATZ
- OK ATDT0144278000
- CONNECT "
- ogin: franck
- ssword: mdp-franck
- TIMEOUT 5
- > pppd

1.112.4 Configuration d'un client PPP

- Autre possibilité : pppd se charge de lancer le script de chat

```
/usr/sbin/pppd /dev/ttyS2 115200 \
lock \
asyncmap 00000000 \
crtscts \
connect "/usr/sbin/chat -f /etc/sysconfig/network-scripts/chat-ppp"
```

- Le fichier /etc/sysconfig/network-scripts/chat-ppp contient les séquences de chat vues plus haut

1.112.4 Configuration d'un client PPP

- pppd
  - pppd device vitesse options
- Options
  - asyncmap map : préserver des bits pour caractères de contrôle
  - call conf-upmc : /etc/ppp/peers/upmc contient des options particulières à la connexion ppp à l'UPMC
  - connect chat-script : appelle le script chat-script qui contient les séquences de connexion
  - crtscts : active le contrôle de flux matériel (CTS/RTS)
  - debug : active le mode debug
  - defaultroute : active la route par défaut (passerelle : @IP du correspondant)

1.112.4 Configuration d'un client PPP

- Options...
  - lock : accès exclusif au périphérique
  - nodetach : exécution en avant-plan
  - persist : reconnexion automatique en cas de problème sur la ligne

1.112.4 Configuration d'un client PPP

- Authentification
  - login/mot de passe en clair
  - PAP (Password Authentication Protocol) : le client envoie un login/mot de passe stocké dans le fichier /etc/ppp/pap-secrets au serveur
  - CHAP (Challenge Handshake Authentication Protocol) : challenge initié par le serveur. Le client répond avec le login/mot de passe stocké dans le fichier /etc/ppp/chap-secrets
  - MSCHAP : CHAP à la mode Microsoft

1.112.4 Configuration d'un client PPP

```
# cat /etc/ppp/pap-secrets
# Secrets for authentication using PAP
# client        server  secret                  IP addresses
######## system-config-network will overwrite this part!!! (begin) ##########
######## system-config-network will overwrite this part!!! (end) ############

# cat /etc/ppp/chap-secrets
# Secrets for authentication using CHAP
# client        server  secret                  IP addresses
######## system-config-network will overwrite this part!!! (begin) ##########
######## system-config-network will overwrite this part!!! (end) ############
```

1.112.4 Configuration d'un client PPP

- Fichiers de conf de ppp
  - /etc/ppp/options : contient les options de pppd plutôt que de les ajouter à la ligne de commande
  - /etc/ppp/ip-up : contient les différentes configurations réseau une fois la connexion établie (routes, serveur DNS, pas de hostname en connexion ppp)
  - /etc/ppp/ip-down : opérations inverses à /etc/ip-up à la déconnexion

1.112.4 Configuration d'un client PPP

- wvdial
  - wvdial remplace chat
  - Configuration plus facile avec l'utilitaire wvdialconf :création du fichier /etc/wvdial.conf
  - /etc/wvdial.conf peut contenir plusieurs configurations ppp différentes isolées dans des sections
  - wvdial upmc

UPMC PARIS UNIVERSITAS

Sommaire

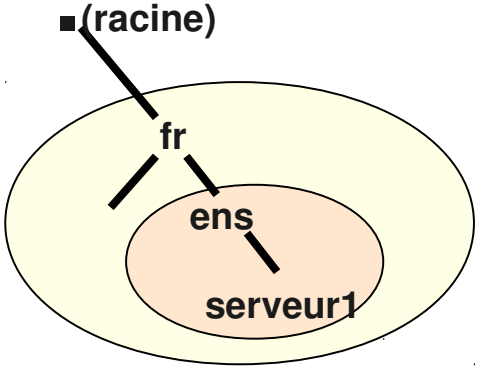
- Principes TCP/IP
- TCP/IP Configuration et troubleshooting
- Configuration client PPP
- Configuration DNS

1.113.5 Configuration DNS

- Petits rappels sur le DNS
- Des noms ?
  - Plus facile à mémoriser par les humains
  - Retrouver des machines qui changent d'adresse IP
- Base de données distribuée
  - Administration partagée
  - Charge répartie
  - Permets des duplications et des caches
  - résolution :
    - des noms en adresses (résolution directe)
    - des adresses en noms (résolution inverse)

1.113.5 Configuration DNS

- Système hiérarchisé
  - Structure d'un arbre
  - Sommet est appelé racine et noté par .
  - Administration en zone
  - Possibilité de déléguer

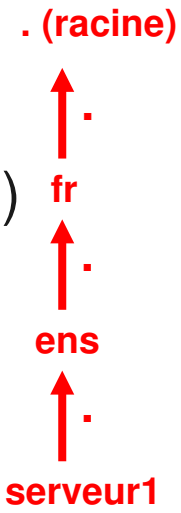


- La racine
  - Ensemble de 13 serveurs dans le monde gérés par l'ICANN
  - page d'information officielle sur les serveurs racines du DNS : http://root-servers.org/

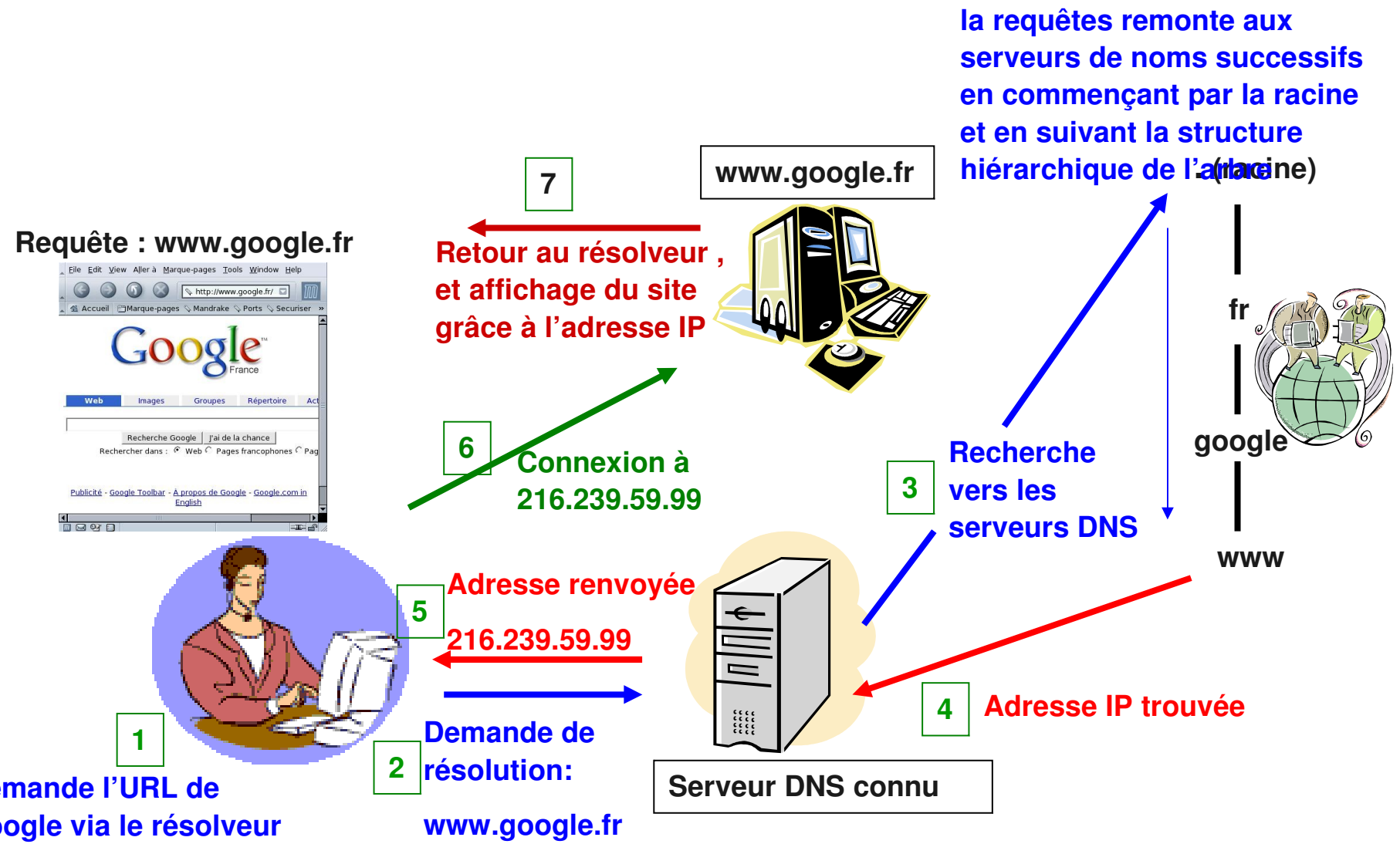
- Les différentes tâches liées au DNS
  - Le résolveur
    - Programme qui formate une requête DNS dans un paquet UDP, puis l'envoie au serveur cache, et récupère le résultat.
  - Le serveur cache
    - Renvoie une réponse déjà existante,
    - Sinon recherche un serveur autoritaire qui possède la réponse, puis met son résultat en cache (itératif)
    - Il peut devoir demander à d'autres serveurs de nom de localiser sa requête (récursif)
      - Enregistrement des serveurs en caches
    - Réduit la charge sur les serveurs de noms très sollicités

- Les différentes tâches liées au DNS
  - Le serveur autoritaire (serveur maître)
    - possède une base d'informations d'une zone dont il a l'autorité administrative
  - Duplication de DNS (serveur esclaves)
    - Les données sont enregistrées sur un serveur autoritaire (maître) et copier vers un (des) serveur(s) autoritaire(s) (esclave(s))
    - Pas de différence visible entre les 2 types de serveurs depuis l'Internet
  - Ces serveurs sont aussi appelés serveurs primaires et secondaires
  - Un serveur peut être primaire pour certaines zones et secondaires pour d'autres

- Syntaxe d'un nom de domaine
  - Une longueur total de 255 caractères
  - Chaque partie est composée de 63 caractères maximum et séparée par un point (.)
  - Concaténation de 127 noms au plus
  - Restriction au niveau des caractères composant le nom du domaine:
    - a-z (commence forcément par une lettre)
    - 0-9
    - - (tirés) autorisés, mais pas les _ (underscores)
    - Pas de distinction minuscule/majuscule
  - Notation complète :
    - serveur1.ens.fr. ⇔ serveur1.ens.fr
    - dite FQDN (Fully Qualified Domain Name)



1.113.5 Configuration DNS



- Processus d'une requête
  - Interrogation :
    - Le client envoie la requête à son serveur de nom
    - Ce serveur de noms transmet la requête au serveur de noms racine
    - Le serveur de noms racine renvoie l' (les) adresse(s) du serveur de noms qui a autorité sur le domaine demandé
    - Le serveur de noms initial interroge alors le(l'un des) serveur(s) de noms renvoyé(s) (dans un ordre aléatoire) etc..
  - Les résultats renvoyés sont appelés enregistrement de ressources (RR = Resource Records)
    - Les RR peuvent être de différents types

- Mise en œuvre d'un DNS
  - BIND (Berkeley Internet Name Domain) est une implémentation du protocole de système de serveur de nom (DNS)
  - Fonctionne en mode Client-Serveur
  - 99% des serveurs DNS utilisent bind
  - Développé par ISC (Internet Systems Consortium)

- Organisation locale
  - Accès aux données de nommage par le résolveur
    - /etc/host.conf : Le fichier signale au résolveur quels services sont disponibles et dans quel ordre il doit les appliquer

```
[root@caruso named]# cat /etc/host.conf
order hosts,bind
```

    - /etc/nsswitch.conf : Ce fichier indique dans quel ordre le système doit chercher un nom d'hôte. Il est apparu avec la dernière librairie C de Linux contenant le code du résolveur en lui même.

```
#hosts:     db files ldap nis dns
hosts:      files dns
```

1.113.5 Configuration DNS

- Organisation locale
  - Résolveur local d'un serveur DNS
    - /etc/hosts : table de correspondance des adresses IP des machines et de leur nom d'hôtes. Ne rien spécifier pour un serveur DNS à part le boucle locale

```
127.0.0.1       localhost       localhost.localdomain
```

    - /etc/resolv.conf : ne doit résoudre que lui-même (127.0.0.1), ne pas configurer d'autres serveurs.

```
[root@caruso etc]# cat resolv.conf
search ens.fr lmdnet adm.lmdnet res.lmdnet
nameserver 127.0.0.1
```

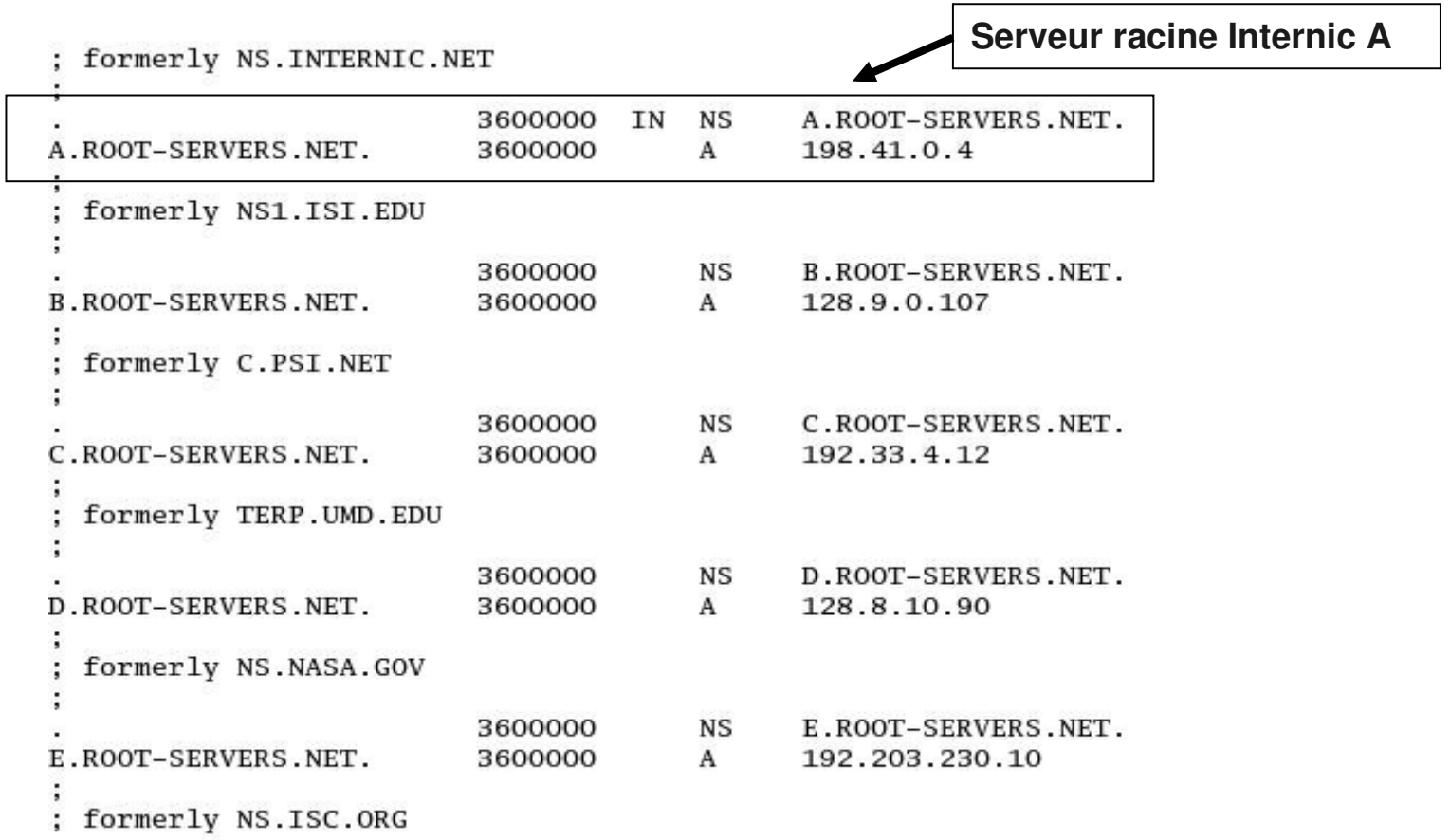
- Organisation locale
  - Fichier de configuration contrôlant le service bind
    - /etc/named.conf
      - Défini le comportement du serveur aux travers de diverses options
      - Défini des restrictions d'accès (ACL)
      - indique au serveur la liste des zones qu'il gère et dans quels fichiers se trouvent leur description.
  - Répertoire des fichiers de zone et de résolution inverse
    - /var/named

- Définition et localisation des serveurs "racine"
  - La déclaration des serveurs "racine"
    - Délivré avec le package bind
    - Fichier appelé named.root, db.cache ou aussi named.ca
    - Doit être régulièrement mise à jour (~ 3 à 6 mois)
      - ftp://ftp.internic.net/domain/named.root (db.cache ou named.cache)
    - Emplacement du fichier /var/named : spécifié dans le fichier named.conf par la variable file
    - Cette déclaration est définie dans la zone "." par un type hint

```
zone "." {
        type hint;
        file "named.root";
};
```

1.113.5 Configuration DNS

- /var/named/named.root : fichier contenant les 13 serveurs racines




```
; formerly NS.INTERNIC.NET
;
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     128.9.0.107
;
; formerly C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
;
; formerly TERP.UMD.EDU
;
.                        3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     128.8.10.90
;
; formerly NS.NASA.GOV
;
.                        3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
;
; formerly NS.ISC.ORG
```

- Informations dans un fichier de zone
  - Les noms de domaines complets sont terminés par un point, sinon ils sont considérés comme relatifs au domaine courant (ajouté implicitement lors des réponses
  - Contient les enregistrements de ressources (RR)
    - SOA (Start Of Authority) : nom du serveur primaire et de son administrateur
    - NS : indique les noms des serveurs de noms pour cette zone
      - SOA et NS : sont utilisés pour les délégations et le fonctionnement du DNS
    - A (Address) : associe les noms aux adresses IP
    - PTR (PoinTeR) : associe les adresses IP aux noms
    - MX (Mail eXchanger) : routage de courrier électronique
    - CNAME (Canonical NAME) : associe des alias au nom réel
    - TXT (TeXT) : information sous forme de texte descriptif

- Structure d'un fichier de zone
  - Options globales
    - $TTL : durée de vie des enregistrements de ressources
  - Enregistrement de ressources SOA
    - Informations administratives et de maintenance de la zone
  - Enregistrement de ressources NS
    - Liste des serveurs de noms pour cette zone
  - Autres enregistrements de ressources (A, PTR etc…)
    - Les données à publier

- Descriptif d'un fichier de zone
  - TTL : Time To Live
    - Indique pendant combien de temps un enregistrement (réponse) peut-être gardée en cache
  - @
    - Désigne l'origine du domaine. Remplace le nom de domaine donné dans le fichier named.conf pour la zone concernée
  - Exemple d'un fichier zone avec ou sans les variables @ et TTL

```
$TTL 1d
@   1h    IN SOA ( ... )
          IN NS ns

www       IN A 192.168.10.2
```

⇔

```
ens.fr.      86400 IN SOA ( ... )
ens.fr.      86400 IN NS ns.ens.fr
www.ens.fr.  86400 IN A 192.168.10.2
```

- Descriptif d'un fichier de zone
  - Descriptif de la SOA
    - serial number : incrémenté par l'administrateur de la zone à chaque modification. Permet la détection d'un changement sur la zone et donc la nécessité de la recharger
    - refresh time : rythme que les serveurs secondaires doivent vérifier le numéro de série sur le primaire
    - retry : à quel rythme les serveurs secondaires doivent essayer de contacter le primaire en cas d'échecs
    - expire : si le secondaire n'a pu contacter le primaire durant la période définie, il supprime les données locales des zones du primaire
    - ttl : pendant combien de temps un cache peut garder une requête non existante

1.113.5 Configuration DNS

- Fichier de zone (ex : db.lmd.polytechnique.fr) :
  - Enregistrement SOA
  - Liste des serveurs de noms (maître et esclaves) de la zone
  - enregistrement des noms du domaine

```
$TTL    3h
; origine de la zone
@               IN SOA  lmdx.lmd.polytechnique.fr.      postmaster.lmd.polytechnique.fr.  (
                                        2004030809      ; serial annee mois jour heure
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                IN NS   lmdx.lmd.polytechnique.fr.
                IN NS   rackham.polytechnique.fr.
                IN NS   milou.polytechnique.fr.
;
; Adresses pour les noms canoniques
localhost               IN A            127.0.0.1
lmdx                    IN A            129.104.13.4
                        IN MX           10 mx-a.polytechnique.fr.
                        IN MX           20 mx-b.polytechnique.fr.
lmd.polytechnique.fr.   IN A            129.104.13.4
lmd.polytechnique.fr.   IN MX           10 mx-a.polytechnique.fr.
lmd.polytechnique.fr.   IN MX           20 mx-b.polytechnique.fr.
;
; Reseau 129.104.13     LMD
;
nemo                    IN A            129.104.13.1
```

Enregistrements NS

Association des MX à un nom

Enregistrements des adresses

Nemo → 129.104.13.1

1.113.5 Configuration DNS

- Fichier named.conf
  - Déclaration des zones sur le serveur autoritaire

Définition de la zone racine :

Type : local (pas d'interrogation depuis l'extérieur)

File : fichier associé

```
zone "." IN {
        type hint;
        file "db.cache";
};
```

```
zone "lmd.polytechnique.fr" IN {
        type master;
        file "db.lmd.polytechnique.fr";
        allow-query { any; };
};
```

Définition de la zone déléguée :

Type : master = autorité sur la zone

File : fichier associé

Allow-query : autorisation d'interroger depuis l'extérieur

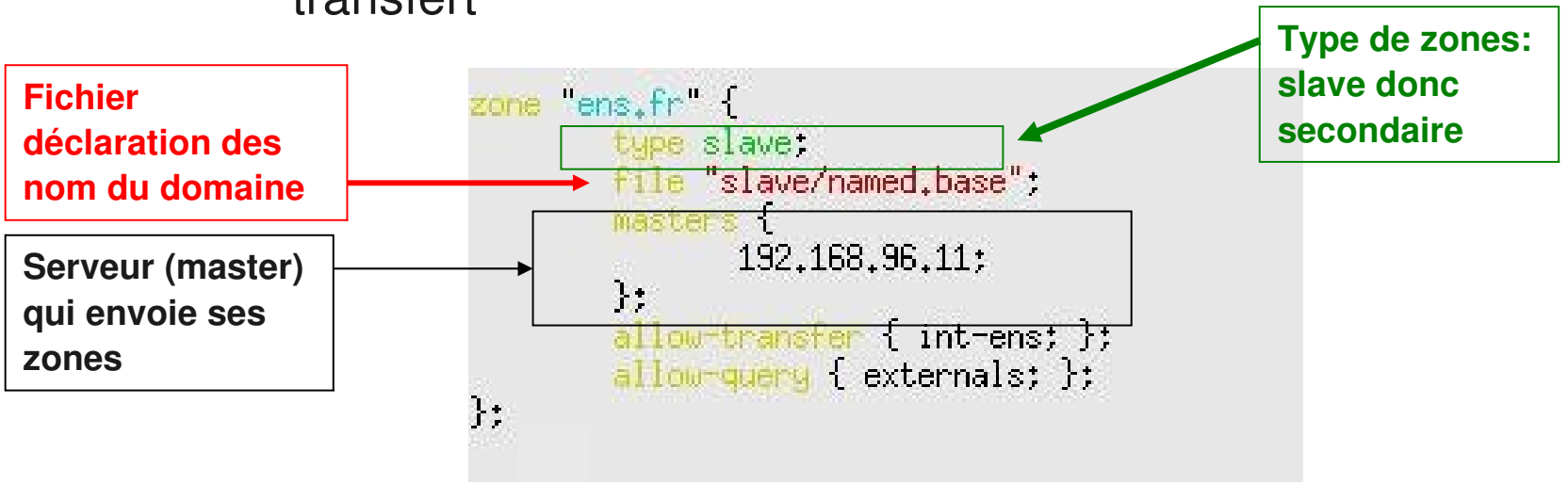
Définition de la Zone reverse

```
zone "13.104.129.in-addr.arpa" IN {
        type master;
        file "db.129.104.13";
        allow-query { any; };
};
```

Définition de la Zone reverse locale

```
zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "db.127.0.0";
        allow-update { none; };
};
```

- Fichier named.conf
  - Déclaration d'une zone d'un serveur secondaire
  - Transfert de zone
    - Le serveur secondaire contacte le serveur primaire après la durée du refresh et demande serial number de la zone
    - Compare le serial number avec celui de sa copie locale
    - Si le numéro a augmenté, le serveur effectue le transfert



1.113.5 Configuration DNS

- Changement des données dans les zones
  - Se rappeler de changer le serial number
  - Vérifications syntaxiques du fichier de zone
    - named-checkzone

```
[root@caruso named]# named-checkzone lmdnet db.lmdnet
zone lmdnet/IN: loaded serial 2006042701
OK
```

  - Vérifications syntaxiques du fichier named.conf
    - named-checkconf : rapporte les erreurs dans ce fichier
  - Redémarrage après un changement de modification :
    - service named restart
    - service named reload
  - Vérifications dans les journaux
    - tail /var/log/messages

1.113.5 Configuration DNS

- Serveur Bind : application client - serveur
  - Requêtes et réponse sont envoyées dans des paquets UDP, port 53
  - Utilise occasionnellement les paquets TCP, port 53
    - Pour les transferts de zones entre primaire et secondaire

```
root@lmdx:/var/named# netstat -na |grep ":53 "
tcp        0      0 129.104.13.4:53         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:53              0.0.0.0:*
udp        0      0 129.104.13.4:53         0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
```

- Maintenance (à distance) : rndc
  - BIND contient un utilitaire appelé rndc qui permet d'administrer, localement ou à distance, le démon named grâce à des déclarations en lignes de commandes.
  - Le programme rndc utilise le fichier /etc/rndc.conf pour ses options de configuration qui seront outrepassées par la priorité des options de lignes de commandes.
  - Afin d'empêcher des utilisateurs non autorisés sur d'autres systèmes de contrôler BIND sur un serveur, on utilise une méthode de clé secrète partagée pour accorder explicitement des privilèges à certains hôtes.
    - Pour que rndc émette des commandes vers n'importe quel named, même sur un ordinateur local, les clés utilisées dans /etc/named.conf et /etc/rndc.conf doivent correspondre.

- Maintenance (à distance) : rndc
  - Ligne de commande rndc
    - status : donne l'état du serveur
    - querylog **:** Déclenche le logging pour toutes les requêtes effectuées par des clients vers le présent serveur de noms.
    - refresh **:** Rafraîchit la base de données du serveur de noms.
    - reload : Dit au serveur de noms de recharger les fichiers de zone mais conserve toutes les réponses précédemment placées en cache. Cela vous permet d'opérer des changements sur les fichiers de zone et de leur faire prendre effet sur vos serveurs maîtres et esclaves sans perdre toutes les résolutions de nom stockées.
    - stats — Evacue les statistiques du named en cours vers le fichier /var/named/named.stats.
    - stop — Arrête le serveur avec égards, en enregistrant toute mise à jour dynamique et donnée IXFR avant l'arrêt complet.
    - **flush — vide le cache**

1.113.5 Configuration DNS

- Test et interrogation de DNS
  - 3 programmes permettent de faire des requêtes DNS et en afficher les résultats
    - dig
      - Le plus complet
      - Permet un débogage des problèmes liés au DNS
    - nslookup
      - *deprecated* ! Moins intuitif pour utiliser les options
    - host
      - Utilitaire le plus simple à utiliser pour obtenir rapidement et clairement la traduction
      - Options intéressantes : -t type, -a tous les types, -d debug, -v verbose.

1.113.5 Configuration DNS

- dig et le degogage

```
fbongat@berlioz ~ $ dig www.lmd.jussieu.fr a

; <<>> DiG 9.3.1 <<>> www.lmd.jussieu.fr a
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9445
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 3

;; QUESTION SECTION:
;www.lmd.jussieu.fr.            IN      A

;; ANSWER SECTION:
www.lmd.jussieu.fr.     70917   IN      CNAME   goudimel.lmd.jussieu.fr.
goudimel.lmd.jussieu.fr. 70917  IN      A       134.157.47.95

;; AUTHORITY SECTION:
lmd.jussieu.fr.         77639   IN      NS      blakey.lmd.jussieu.fr.
lmd.jussieu.fr.         77639   IN      NS      soleil.uvsq.fr.
lmd.jussieu.fr.         77639   IN      NS      cendrillon.lptl.jussieu.fr.
lmd.jussieu.fr.         77639   IN      NS      shiva.jussieu.fr.

;; ADDITIONAL SECTION:
shiva.jussieu.fr.       75823   IN      A       134.157.0.129
blakey.lmd.jussieu.fr.  77639   IN      A       134.157.47.99
soleil.uvsq.fr.         75186   IN      A       193.51.24.1

;; Query time: 1 msec
;; SERVER: 129.199.72.99#53(129.199.72.99)
;; WHEN: Fri May 12 14:55:18 2006
;; MSG SIZE  rcvd: 220
```

Informations complémentaires:

Le temps de réponse

le serveur qui a répondu à la requête

- Interprétation des résultats avec la commande dig
  - status
    - NOERROR : 0 ou plusieurs RR renvoyés
    - NXDOMAIN : domaine non existant
    - SERVFAIL : cache ne peut trouver la réponse
  - flags
    - aa : réponse autoritaire donc pas d'un cache
    - qr : requête ou réponse
    - rd : récursion désirée
    - ra : récursion disponible
    - tc : tronquée
  - ANSWER
    - Nombre de RR dans la réponses
    - Dans la section associée : TTL de chaque RR qui indique combien de temps le cache peut le garder, le type des RR
  - AUTHORITY
    - Les NS autoritaires pour ce domaine
  - ADDITIONNAL
    - les IP des NS autoritaires

1.113.5 Configuration DNS

- NSS : Name Service Switch
- Permet de spécifier quels services d'annuaire seront sollicités et dans quel ordre
- Configuration dans /etc/nsswitch.conf
- Bases habituellement utilisées :
  - passwd
  - shadow
  - group
  - host
  - services

- Les librairies utilisées

```
# ls /lib/libnss_*
/lib/libnss_compat-2.5.so  /lib/libnss_hesiod.so.2
/lib/libnss_compat.so.2    /lib/libnss_ldap-2.5.so
/lib/libnss_db-2.2.so      /lib/libnss_ldap.so.2
/lib/libnss_db.so.2        /lib/libnss_nis-2.5.so
/lib/libnss_dns-2.5.so     /lib/libnss_nisplus-2.5.so
/lib/libnss_dns.so.2       /lib/libnss_nisplus.so.2
/lib/libnss_files-2.5.so   /lib/libnss_nis.so.2
/lib/libnss_files.so.2     /lib/libnss_winbind.so.2
/lib/libnss_hesiod-2.5.so  /lib/libnss_wins.so.2
```

- Fichier /etc/nsswitch.conf

```
passwd:     files ldap
shadow:     files ldap
group:      files ldap

#hosts:     db files nisplus nis dns
hosts:      files dns

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files
```

1.113.5 Configuration DNS

- Avant NSS, ce service de sélection d'annuaire de nom était défini dans le fichier :
  - /etc/host.conf

```
..
order:    hosts,bind
...
```

1.113.5 Configuration DNS

- Différence entre les versions V4 et V8 de BIND
- Format de named.conf vu plus haut
- Sous V4, named.conf se nomme named.boot et diffère dans son formalisme

```
directory               /var/named
cache .                 root.hints
primary exemple.fr      exemple.fr.zone
primary 1.168.192.in-addr.arp   1.168.192.rev
```

- En version V8, cela donne

```
options         {
                directory               "/var/named";
};
zone    "."     {
                type hint;
                file "root.hints;
};
zone    "exemple.fr"    {
                type master;
                file "exemple.fr.zone";
};
zone    "1.168.192.in-addr.arp" {
                type master;
                file "1.168.192.rev";
};
```

1.113.5 Configuration DNS

- Enregistrement de nom de domaine
  - http://www.internic.net/regist.html
- Utiliser named comme serveur cache local
  - /etc/resolv.conf : nameserver 127.0.0.1
- En cas de pb :
  - Journaux dans /var/log/message

Quelques conseils LPI...

- Connaître le fonctionnement global de DNS
- Savoir comment /etc/nsswitch.conf fonctionne
- Connaître l'ancienne version : /etc/hosts.conf
- A quoi sert /etc/hosts
- A quoi sert un serveur cache local
- Configuration différence entre V4 et V8

Quelques conseils LPI...

- Connaître les séquences standard d'un script de chat
- Connaître les options de pppd (persist en particulier)
- Comment débuger une connexion ppp
- Savoir à quoi servent PAP, CHAP et MSCHAP