

[inetdoc.LINUX]

<http://www.linux-france.org/prj/inetdoc>

Administration Système & Réseau

- Domain Name System
 - ▶ Historique & Concepts
 - ▶ Fonctionnalités & Hiérarchie
 - ▶ Requêtes & Base de donnée DNS
- Dynamic Host Configuration Protocol



Philippe Latu

philippe.latu@linux-france.org

IUT 'A' Paul Sabatier - IUP STRI

Domain Name System (DNS)

- Pourquoi un système de résolution des noms ?
 - Identification sur Internet
 - Échanges d'adresses IP
 - Identification «humaine»
 - Échange de noms
- Service DNS
 - Correspondance entre adresses IP et noms d'hôtes
- Domain Name System (DNS)
 - Base de données hiérarchique distribuée
 - Service Internet => couche application
 - RFCs 1034 et 1035 en 1987

Domain Name System (DNS)

- Notion de nom récurrente
 - Fichiers dans un système de fichiers
 - Processus dans un système d'exploitation
 - Pages Web sur l'Internet
 - Imprimantes sur le réseau
- Découplage entre nom et localisation
 - Niveau d'adressage indirect entre
 - ▶ nom d'hôte
 - ▶ localisation géographique
- Conception du système de résolution des noms
 - Espace des noms «à plat» ou hiérarchique
 - Approche centralisée ou distribuée

Domain Name System (DNS)

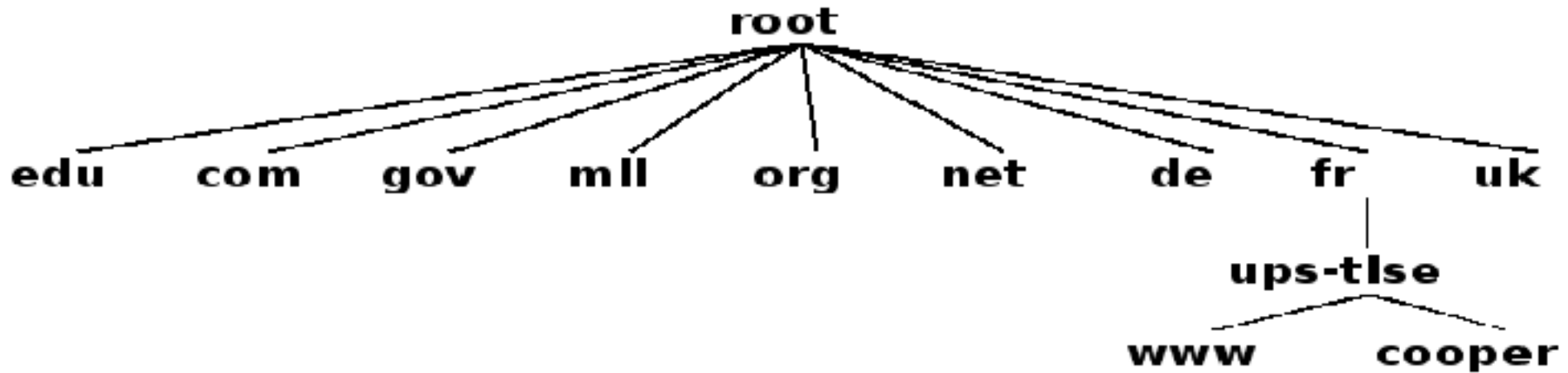
- À l'origine de l'Internet
 - Fichier texte unique HOSTS.TXT
 - Gestion par une structure unique (SRI)
 - Demandes de modification par E-mail
 - Publications périodiques via FTP
- Avec le développement de l'Internet
 - Structure centralisée unique saturée
 - Duplication de certains noms d'hôtes
 - Différentes versions du fichier HOSTS.TXT en circulation
- Besoin d'un nouveau service Internet
 - Évolutif et adaptable avec la croissance de l'Internet
 - Puissance de «calcul» décentralisée
 - Administration décentralisée

Domain Name System (DNS)

- **Fonctionnalités du service DNS**
 - **Espace des noms de domaines = arborescence hiérarchique**
 - ▶ Arborescence indépendante de la topologie réseau et/ou de la géographie
 - **Architecture de stockage distribuée**
 - ▶ Zones affectées à des serveurs de noms dans l'arborescence hiérarchique
 - ▶ Serveurs de sauvegarde pour la redondance et la disponibilité
 - **Administration répartie suivant la hiérarchie des noms**
 - ▶ Rôle le plus simple : client DNS ou 'resolver'
 - **Protocole client/serveur communicant sur le port n° 53**
 - ▶ Protocole UDP utilisé par les clients
 - ▶ Protocole TCP préconisé pour les échanges entre serveurs

Domain Name System (DNS)

- Hiérarchie des noms de domaines



- Arborescence limitée à 128 niveaux
- Un domaine est un sous-ensemble de l'arborescence
- Aucune possibilité de doublon
 - ▶ hôte : cooper, domaine : ups-tlse, gTLD : fr
 - ▶ Fully Qualified Domain Name : cooper.ups-tlse.fr

Domain Name System (DNS)

- Conventions sur les noms de domaines
 - Top Level Domains (TLD)
 - ▶ .com, .net, .org, .edu, .mil, .gov, .int, .biz
 - Geographical Top Level Domains (gTLD)
 - ▶ .de, .fr, .uk, .jp, .au
 - Cas particulier de la zone .ARPA
 - ▶ Adressage inverse
 - ▶ Correspondance entre adresse IP et nom de domaine

Domain Name System (DNS)

- Hiérarchie des serveurs

- Serveurs «distribués» dans l'arborescence hiérarchique

- ▶ Un serveur ne maintient qu'un sous-ensemble de l'arborescence
- ▶ On parle d'autorité sur une zone : **Authoritative Name Server**

- Un serveur détient ses enregistrements

- ▶ Hôtes et services appartenant à «sa» zone
- ▶ Enregistrement : **Resource Record (RR)**

- Un serveur est en relation avec ses homologues

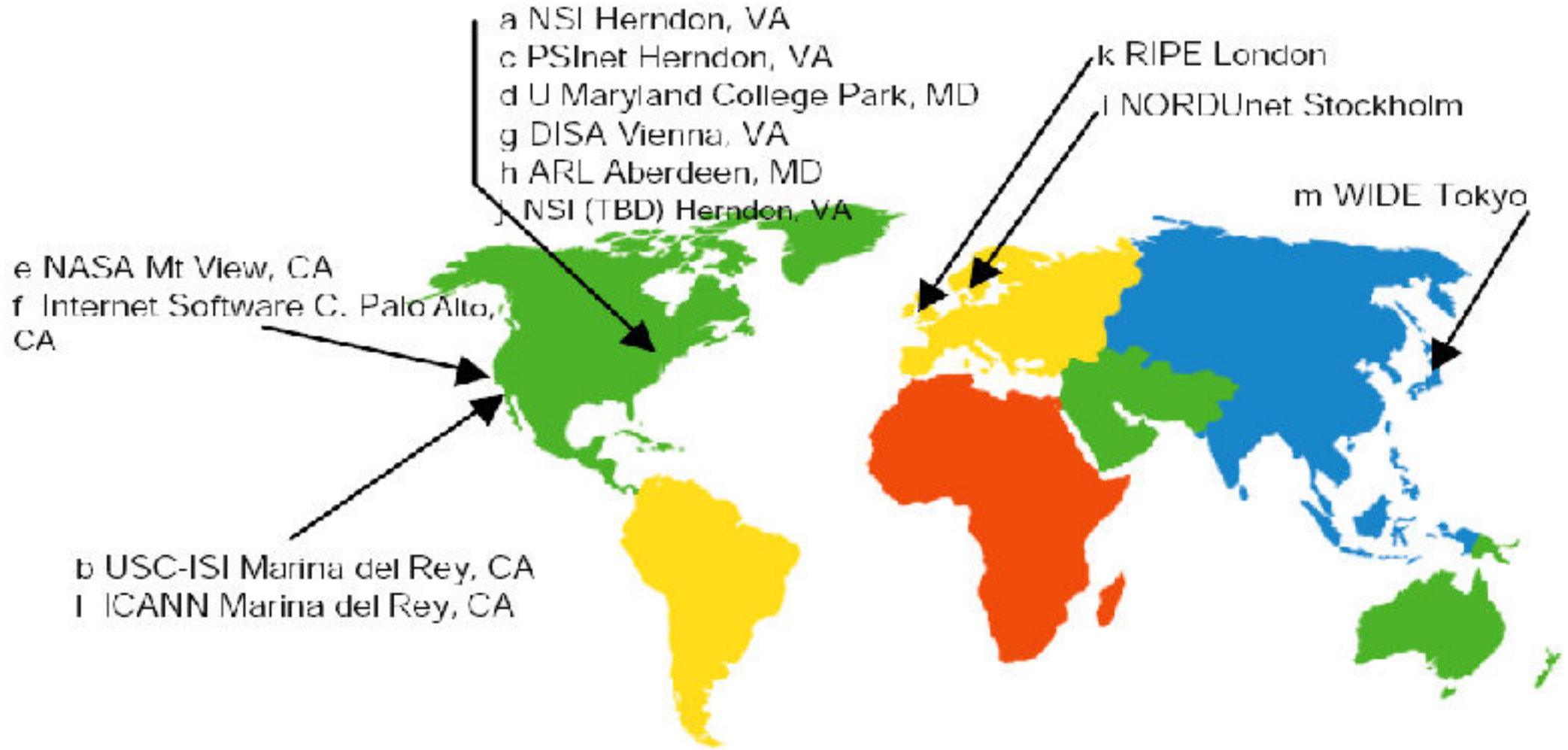
- ▶ Chaque serveur connaît la liste des serveurs racines : **Root Servers**

- Chaque serveur racine

- ▶ Connaît tous les serveurs TLDs et gTLDs
- ▶ Connaît un serveur intermédiaire à contacter pour joindre celui qui a autorité sur une zone

Domain Name System (DNS)

- Serveurs racine : Root Servers



Domain Name System (DNS)

- Gestion de cache

- Stockage des résultats des requêtes en mémoire cache

- ▶ Optimisation de la charge des serveurs des niveaux supérieurs

- Durée de vie des enregistrements (RRs)

- ▶ Champ TTL fixé par configuration pour une zone
- ▶ TTL élevé : moins de trafic et moins de mises à jour
- ▶ TTL petit : plus de trafic et plus de mises à jour

- Même les requêtes non résolues sont conservées en cache

- ▶ RFC 2308 - **Negative Caching of DNS Queries**
- ▶ Optimisation de la charge des serveurs

- Risques de dénis de services importants (M\$!)

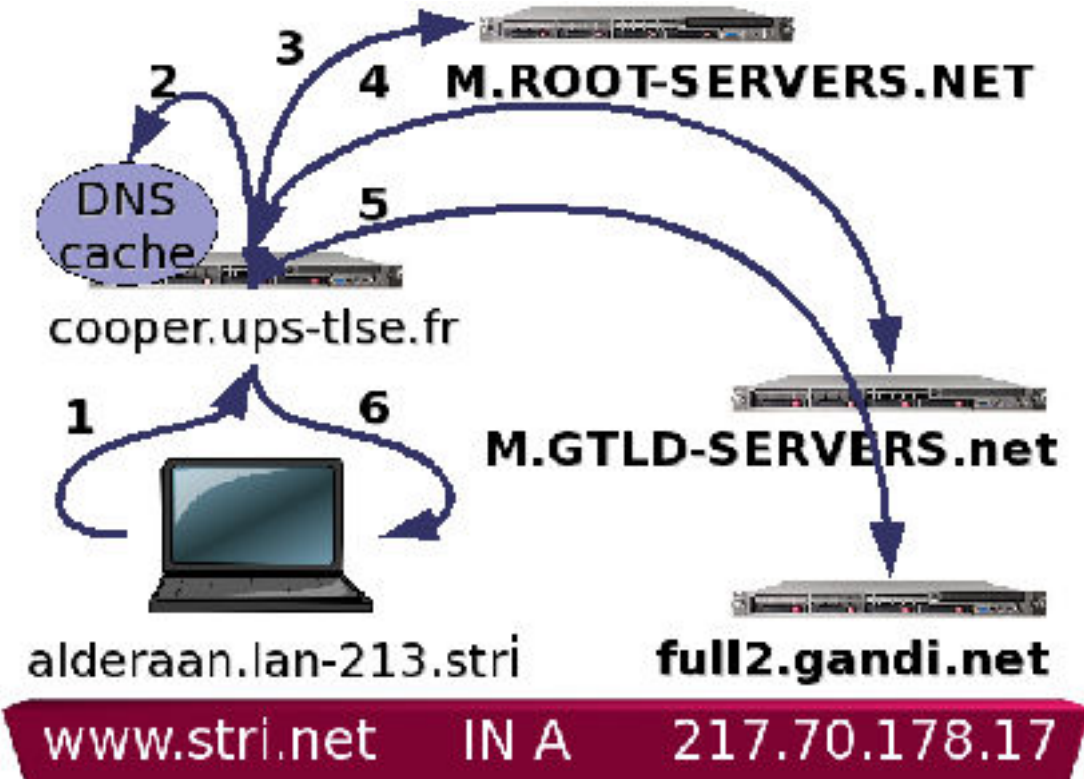
- ▶ Un intrus «fournit» une réponse négative au service DNS local
- ▶ Toute nouvelle requête pour cette zone obtient une réponse négative !
- ▶ Attention au réglage TTL minimum du service

Domain Name System (DNS)

- 2 types de requête DNS
- Requête récursive
 - Le serveur DNS contacté traite la requête et répond
 - Situation normale pour les hôtes du réseau de confiance
 - Situation anormale pour les hôtes du réseau public
 - Utilisation de la notion de «vue»
 - BIND 9 Administrator Reference Manual
 - Section [View Statement Definition and Usage](#)
- Requête itérative
 - Le client contacte les serveurs DNS individuellement
 - Mise au point de la configuration du service DNS
 - Identification du point de «rupture» dans la chaîne de résolution des noms

Domain Name System (DNS)

- Exemple de requête DNS récursive
 - Requête du poste alderaan : Adresse IP du site `www.stri.net` ?

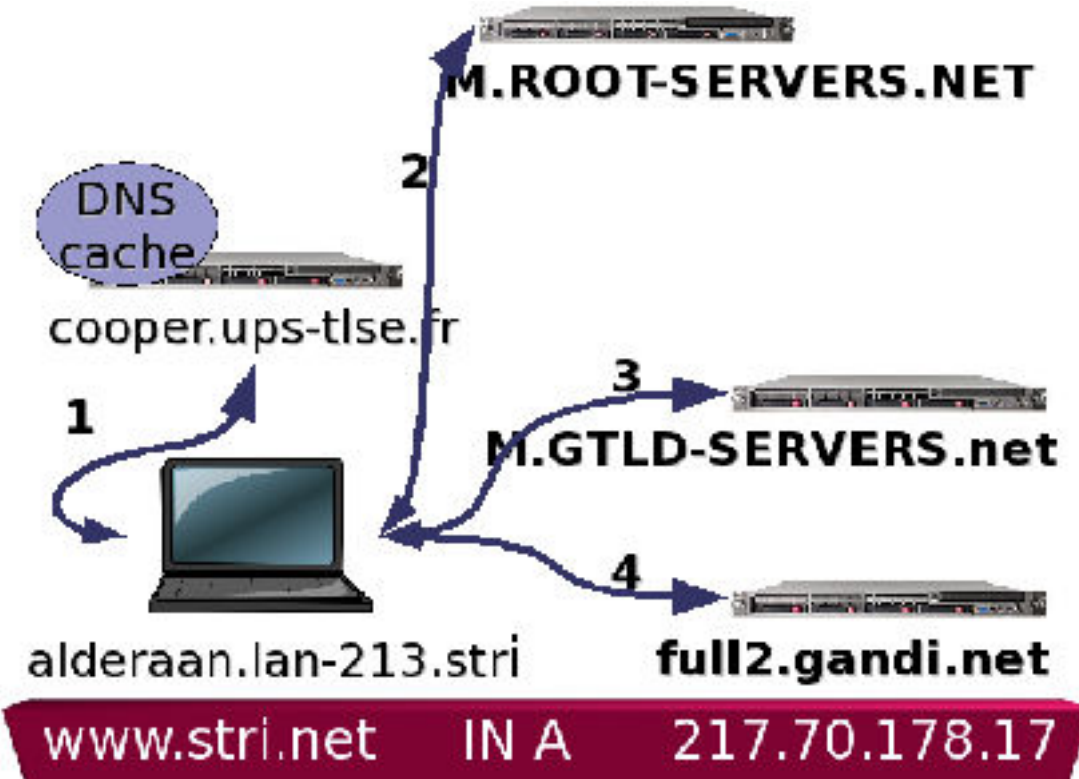


- ▶ (1) alderaan contacte le serveur DNS local `cooper.ups-tlse.fr`
- ▶ (2) cooper consulte son cache
- ▶ (3) cooper contacte un serveur racine `M.ROOT-SERVERS.NET`
- ▶ (4) cooper contacte un serveur du niveau `.net` `M.GTLD-SERVERS.net`
- ▶ (5) cooper contacte le serveur qui a autorité sur la zone `full2.gandi.net`
- ▶ (6) cooper renvoie la réponse

Domain Name System (DNS)

• Exemple de requête DNS itérative

- Requête du poste alderaan : Adresse IP du site `www.stri.net` ?



- ▶ (1) alderaan contacte le serveur DNS local `cooper.ups-tlse.fr`
- ▶ (2) alderaan contacte un serveur racine `M.ROOT-SERVERS.NET`
- ▶ (3) aserix contacte un serveur du niveau `.net` `M.GTLD-SERVERS.net`
- ▶ (4) alderaan contacte le serveur qui a autorité sur la zone `full2.gandi.net`
- ▶ Commande `dig` avec l'option `+trace`

Domain Name System (DNS)

- Base de données
 - 3 champs par Resource Record (RR)
 - ▶ classe, type, valeur
 - 2 classes principales
 - ▶ Internet (IN), Chaosnet (CH)
- Principaux types de la classe Internet
 - A : adresse IPv4
 - A6 ou AAAA : adresse IPv6
 - NS : Name Server
 - ▶ Serveur de noms de domaines
 - CNAME : Canonical Name
 - ▶ Alias d'un d'hôte
 - HINFO|TXT : informations
 - ▶ Chaîne de caractères

Domain Name System (DNS)

- Principaux types de la classe Internet (suite)
 - MX : Mail eXchange
 - ▶ Prise en charge du courrier électronique
 - PTR : Pointer
 - ▶ Adressage inversé
 - ▶ Correspondance adresse IP - nom d'hôte
 - SOA : Start Of Authority
 - ▶ Déclaration de zone
 - ▶ Champ multiple : horodatage, n° de série, TTL
 - ▶ Utiliser un patron de fichier de déclaration de zone
- BIND 9 Administrator Reference Manual
 - Section **Zone File**
 - ▶ Types of Resource Records and When to Use Them

Domain Name System (DNS)

- Types de la classe Chaosnet
 - version.bind
 - Numéro de version du logiciel du serveur DNS
 - authors.bind
 - Liste des auteurs du logiciel de serveur DNS
 - Masquage des valeurs Chaosnet
 - <http://www.cymru.com/Documents/secure-bind-template.html>

Domain Name System (DNS)

- Distribution de la base de données
 - Notion de zone
 - ▶ espace contigu de l'espace des noms de domaines séparé par des points '.'
 - Plusieurs types de serveurs DNS
- Primary Master
 - Serveur primaire
 - Contient les enregistrements (RR) originaux
- Slave Server ou Secondary Server
 - Serveur redondant
 - Contient les copies des enregistrements (RR) originaux
 - Transferts automatisés via la requête AXFR

Domain Name System (DNS)

- Stealth Server ou Hidden Primary
 - Serveur ayant autorité sur une zone
 - Non déclaré dans la liste publique des serveurs de noms
 - Dépôt de référence non exposé sur le réseau public
- Cache Only Server
 - Serveur sans déclaration de zone ; donc sans autorité
 - Optimise le trafic sur l'hôte qui utilise le cache
 - Risque de surcharge des serveurs racine
 - Utilisation de l'option **forwarders** conseillée

Domain Name System (DNS)

- Client DNS ou **resolver**
 - Bibliothèque partagée - GNU C Library
 - ▶ (Enregistrement|Structure) hostent
 - ▶ Sous-programmes : gethostbyname() et gethostbyaddr()

```
$ man gethostbyname
```

- Configuration

- ▶ Un client doit connaître au moins une adresse IP de serveur DNS
- ▶ Configuration manuelle via édition du fichier `/etc/resolv.conf`
- ▶ Configuration automatique via un service : DHCP ou PPP

```
$ cat /etc/resolv.conf
```

```
search linux-land.stri.net
```

```
nameserver 192.168.1.1
```

```
nameserver 192.168.3.1
```

Domain Name System (DNS)

- Configuration du service DNS
 - Logiciel de référence
 - ▶ BIND (Berkeley Internet Name Domain)
 - ▶ Internet Support Consortium
 - ▶ <http://www.isc.org>
 - Paquets Debian GNU/Linux
 - ▶ bind9-host : commande 'host' associée à BIND 9.x
 - ▶ bind9 : logiciel serveur
 - ▶ bind9-doc : **BIND 9 Administrator Reference Manual**
 - ▶ dnsutils : clients fournis avec BIND ; commande **dig**
 - Configuration après installation du paquet bind9
 - ▶ Configuration **Cache Only** par défaut
 - ▶ Répertoire **/etc/bind/** : fichiers de configuration du service
 - ▶ Répertoire **/var/cache/bind/** : fichiers de zones contenant les RRs

Domain Name System (DNS)

- Documentation & patrons de configuration
 - Éviter de se «disperser» dans l'étude des documents
 - ▶ Google n'est pas forcément notre ami !
 - ▶ Rester concentré sur la documentation officielle
 - Pour la syntaxe de configuration du service
 - ▶ BIND 9 Administrator Reference Manual
 - Pour la syntaxe de déclaration de zone et des RRs
 - ▶ DNS-HOWTO
 - ▶ <http://www.tldp.org/HOWTO/DNS-HOWTO.html>
 - Pour une configuration complète plus robuste
 - ▶ Secure BIND Template
 - ▶ <http://www.cymru.com/Documents/secure-bind-template.html>
 - ▶ Particulièrement intéressant pour l'utilisation des vues
- Bon courage pour les travaux pratiques !
 - ▶ <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.dns>

Dynamic Host Configuration Protocol

- Configuration réseau automatisée
 - Adresse IP
 - Adresse de diffusion
 - Masque réseau
 - Passerelle par défaut
 - Domaine DNS
 - Adresse IP du serveur de noms
- Dynamic Host Configuration Protocol (DHCP)
 - Service Internet => couche application
 - RFCs 2131 et 2132 en 1997
 - Ports UDP 67 (client) et 68 (serveur)

Dynamic Host Configuration Protocol

- 3 générations de protocoles
 - Reverse Address Resolution Protocol (RARP)
 - ▶ RFC903 en 1984 puis RFC1931 en 1996
 - ▶ Protocole entre couche liaison et réseau
 - ▶ Objectif simple : obtenir une adresse IP à partir d'une adresse MAC
 - Bootstrap Protocol (BOOTP)
 - ▶ RFC951 en 1985 puis RFC1497 et RFC 1542 en 1993
 - ▶ Protocole de couche application sur UDP
 - ▶ Configuration réseau des hôtes sans dispositif de stockage
 - Dynamic Host Configuration Protocol (DHCP)
 - ▶ Protocole de couche application sur UDP ; comme BOOTP
 - ▶ Format des messages échangés identique à BOOTP
 - ▶ Affectation dynamique des paramètres et gestion centralisée
 - ▶ Bail de «location» des paramètres pour une durée limitée

Dynamic Host Configuration Protocol

- Configuration du service DHCP

- Logiciel de référence

- ▶ Dynamic Host Configuration Protocol (DHCP)
- ▶ Internet Support Consortium
- ▶ <http://www.isc.org>

- Paquets Debian GNU/Linux

- ▶ dhcp3-common, dhcp3-client, dhcp3-server
- ▶ netbase : configuration des interfaces intégrée

- Organisation des fichiers de configuration

- ▶ Répertoire `/var/lib/dhcp3/` : stockage des informations de bail client et serveur
- ▶ Fichier `/etc/network/interfaces` : directives d'utilisation du service DHCP

```
auto eth0
```

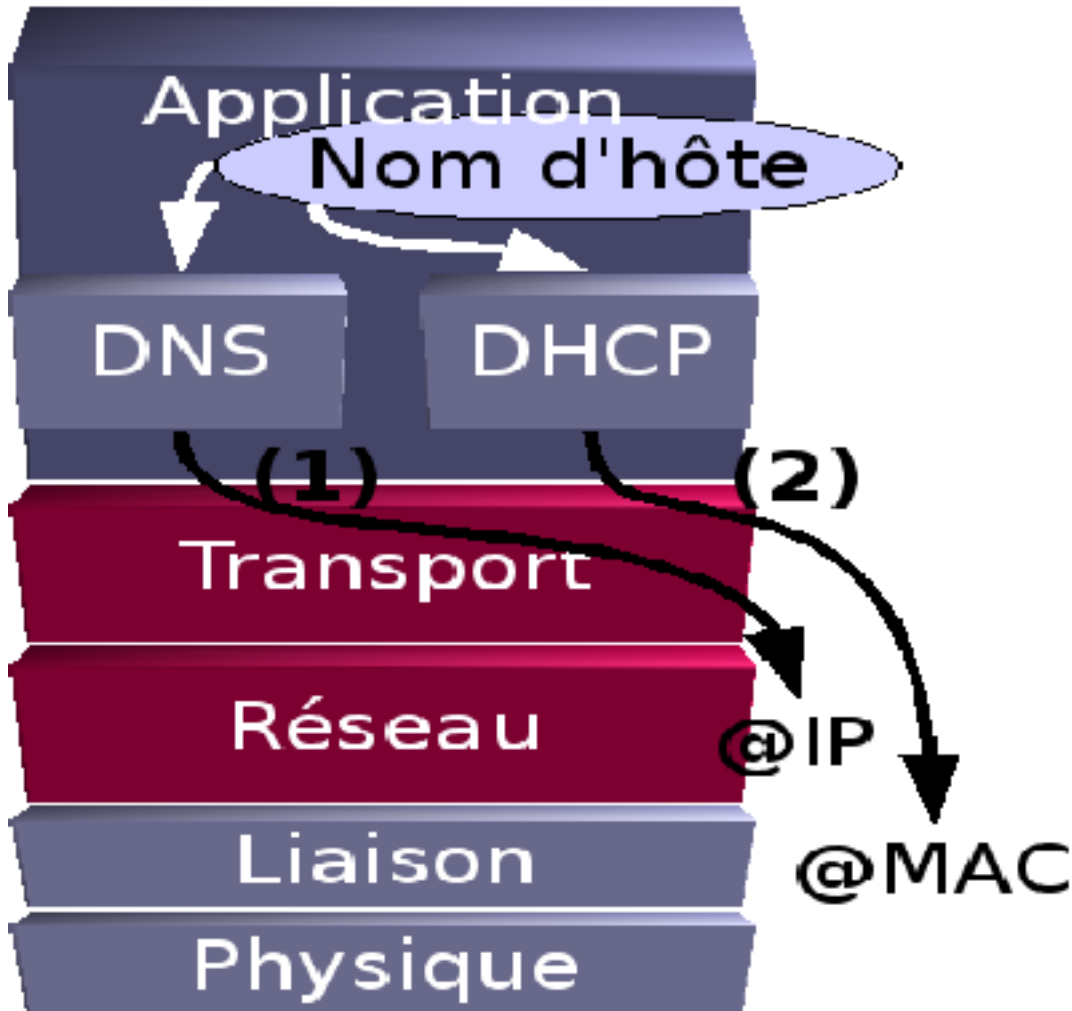
```
iface eth0 inet dhcp
```

- ▶ Fichier `/etc/dhcp3/dhcpd.conf` : configuration du service DHCP

Dynamic Host Configuration Protocol

- Relations DNS & DHCP

- Le nom d'hôte sert de lien entre les 2 services



- ▶ Serveur DNS (1)

```
$ORIGIN lan.stri.  
rubis A 192.168.1.4
```

- ▶ Serveur DHCP (2)

```
option subnet-mask 255.255.255.0;  
option broadcast-address 192.168.1.255;  
option routers 192.168.1.1;  
option domain-name "lan.stri";  
option domain-name-servers 192.168.1.1;
```

```
host rubis {  
  fixed-address rubis.lan.stri;  
  hardware ethernet a8:dc:59:9d:29:c6;  
}
```

Dynamic Host Configuration Protocol

- Documentation & patrons de configuration
 - Éviter de se «disperser» dans l'étude des documents
 - ▶ Rester concentré sur la documentation officielle
 - Syntaxe de configuration du service
 - ▶ Documentation sur la configuration des interfaces réseau

\$ man interfaces

- ▶ Documentation du paquet Debian dhcp3-server

\$ less /usr/share/doc/dhcp3-server/examples/dhcpd.conf

- ▶ Pages de manuels

\$ man dhcpd.conf

- ▶ Format imprimable des pages de manuels

\$ man -t dhcpd.conf | ps2pdfwr - dhcpd.pdf

Synthèse DNS + DHCP

- Domain Name System
 - Configuration dynamique DDNS
 - ▶ Stratégies de gestion des entités mobiles
 - ▶ Paquet dhcp3-server-ldap
 - ▶ Service DHCP sur annuaire LDAP
 - Contrôle des flux et de la congestion
 - ▶ Passer au protocole TCP ...
 - Sécurité
 - ▶ Comment garantir l'intégrité des informations ?
 - ▶ Comment authentifier client et serveur ?
 - ▶ Utiliser DNSSEC ...
 - ▶ Vulnérabilité des 13 serveurs racine
- Dynamic Host Configuration Protocol
 - Sécurité
 - ▶ Comment authentifier client et serveur ?