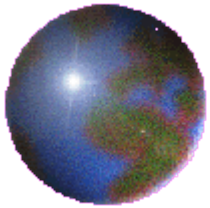
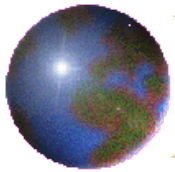


Cours d'administration réseau TCP-IP et sécurité : Quelques applications fondamentales

Denis Pugnère

CNRS / IN2P3 / IPNL

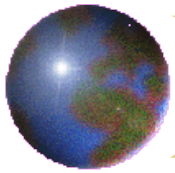
d.pugnere @ ipnl.in2p3.fr



Affectation des ports aux applications

- Référence : http://www.iana.org/assignments/port-numbers
- Sous unix : les services sont référencés dans /etc/services

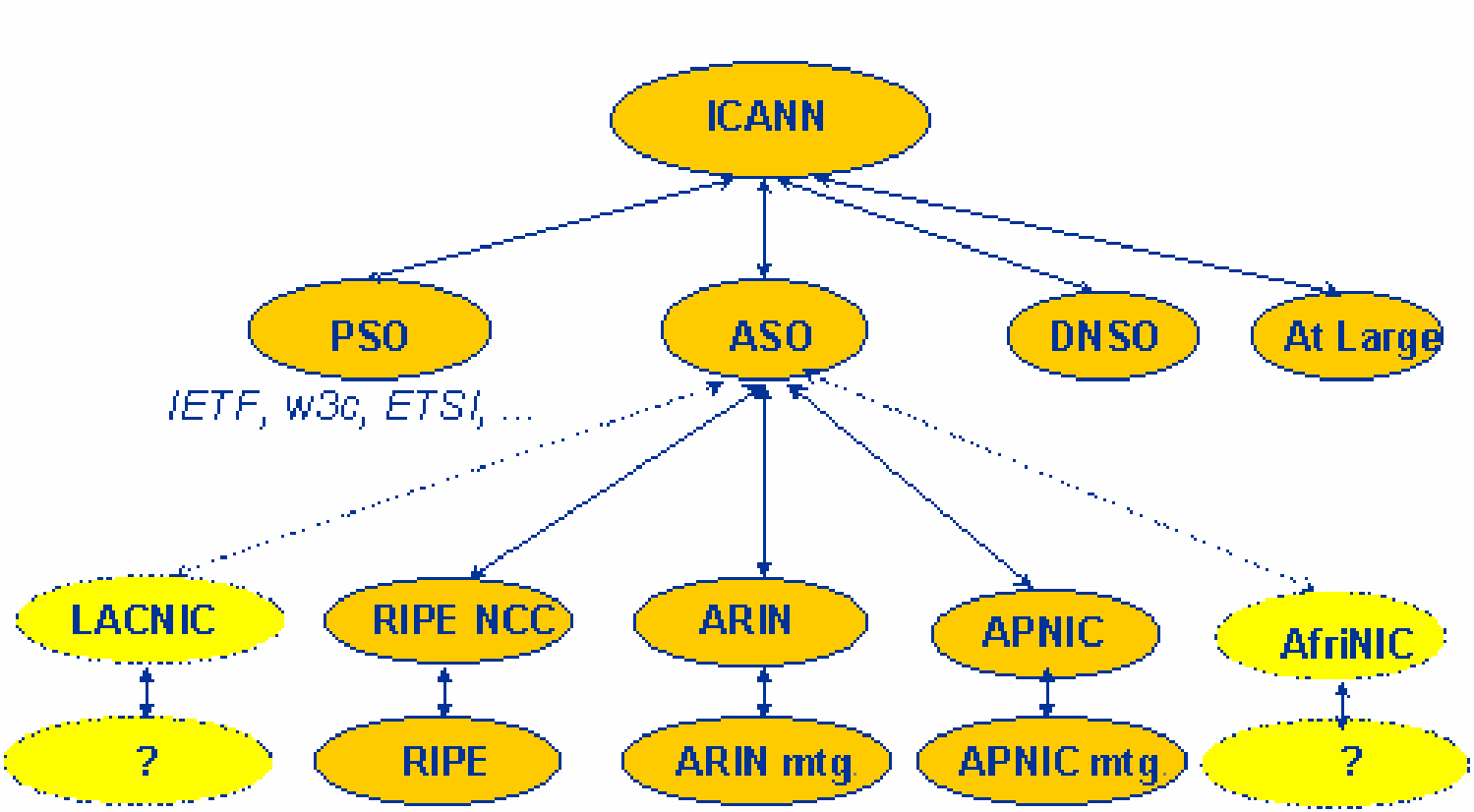
```
ssh             22/udp      # SSH Remote Login Protocol
ssh             22/tcp      # SSH Remote Login Protocol
#                       Tatu Ylonen <ylo@cs.hut.fi>
telnet          23/udp      # Telnet
telnet          23/tcp      # Telnet
#                       Rick Adams <rick@UUNET.UU.NET>
smtp            25/udp      # Simple Mail Transfer
smtp            25/tcp      # Simple Mail Transfer
#                       Susie Armstrong <Armstrong.wbst128@XEROX>
domain          53/udp      # Domain Name Server
domain          53/tcp      # Domain Name Server
#                       Bill Croft <Croft@SUMEX-AIM.STANFORD.EDU>
tftp            69/udp      # Trivial File Transfer
tftp            69/tcp      # Trivial File Transfer
#                       Pierre Arnaud <pierre.arnaud@iname.com>
ntp             123/udp     # Network Time Protocol
ntp             123/tcp     # Network Time Protocol
#                       Marty Schoffstahl <schoff@NISC.NYSER.NET>
snmp            161/udp     # SNMP
snmp            161/tcp     # SNMP
#                       Bill Davidson <billd@equalizer.cray.com>
https           443/udp     # http protocol over TLS/SSL
https           443/tcp     # http protocol over TLS/SSL
```

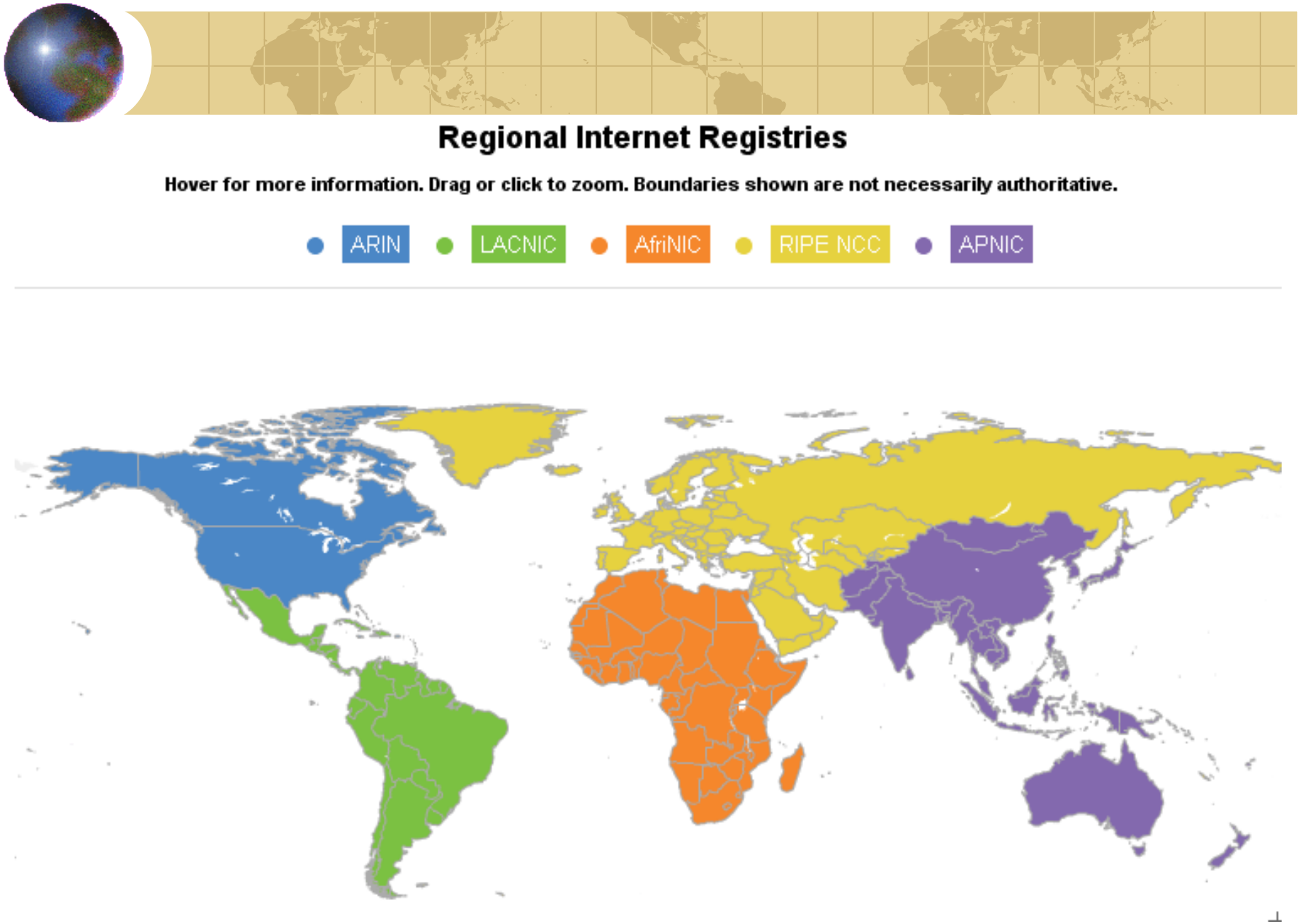


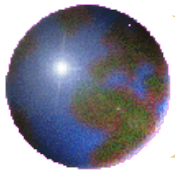
ICANN

- ICANN : Internet Corporation for Assigned Names and Numbers
- gère les adresses IP, l ’organisation de protocoles, les noms de domaines, et les serveurs « root » au niveau mondial.
- La majorité de ces tâches étaient sous la responsabilité du gouvernement des U.S.A
- 3 Supporting Organizations (S0) : Recommendations sur la politique d ’Internet et sa structure :
  - Address Supporting Organization (ASO) : concerné par l ’adressage IP
  - Domain Name Supporting Organization : (DNSO) : concerné par la gestion du système de noms (DNS) : gTLD, ccTLD, registrars
  - Protocol Supporting Organization (PSO) : concerné par l ’affectation des paramètres des protocoles Internet
- Le GIP Renater est actif dans ICANN.
- Le Nic Français (afnic) est actif dans le DNSO de l ’ICANN

Organisation de l'ICANN




Regional Internet Registries
Hover for more information. Drag or click to zoom. Boundaries shown are not necessarily authoritative.
ARIN
LACNIC
AfriNIC
RIPE NCC
APNIC



Les Regional Internet Registeries

RIPE NCC (Réseaux IP Européens Network Coordination Centre) : Europe, Moyen Orient, partie de l'Asie Centrale

ARIN (American Registry for Internet Numbers) : Amérique du Nord, Afrique du Sud

APNIC (Asia Pacific Network Information Centre) : Asie

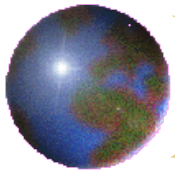
LACNIC (Latin America and Caribbean Network Information Centre) : Amérique du Sud et Amérique Centrale

AfrNIC (Africa Network Information Centre) : Afrique

Le RIPE est l'organisme qui gère les adresses IP au plan européen. Il est un des 5 RIR, son activité (au plan européen) :

- L'allocation des adresses IP
- L'allocation « interdomain routing identifiers » (n° AS BGP)
- L'allocation reverse DNS (in-addr.arpa et ip6.int)
- La gestion base Whois RIPE

Le GIP Renater participe aux travaux de RIPE.



DNS

Domain name system : RFC 1032, 1033, 1034 et 1035

- Système mondial, coopératif, cohérent et hiérarchisé de nommage.
- Gestion décentralisée des informations de la base de données globale :
- Usage général indépendant des types d'applications et du type de machines : du micro au mainframe !
- Les équipements communiquent grâce à leur adresse IP.
- Seules les applications utilisent les noms des équipements :
- A une adresse IP peut correspondre un ou plusieurs noms (alias)
- Un nom doit être unique au monde. Exemple :
  @Ip : 134.158.138.12 = lyomail.in2p3.fr (alias smtp.ipnl.in2p3.fr)
- Case insensitive : lyomail.in2p3.fr <=> LyOmAiL.IN2p3.fR
- Deux mécanismes de résolution de noms :
  - Résolution normale : nom -> adresse(s) ?
  - Résolution inverse : adresse -> nom(s) ?

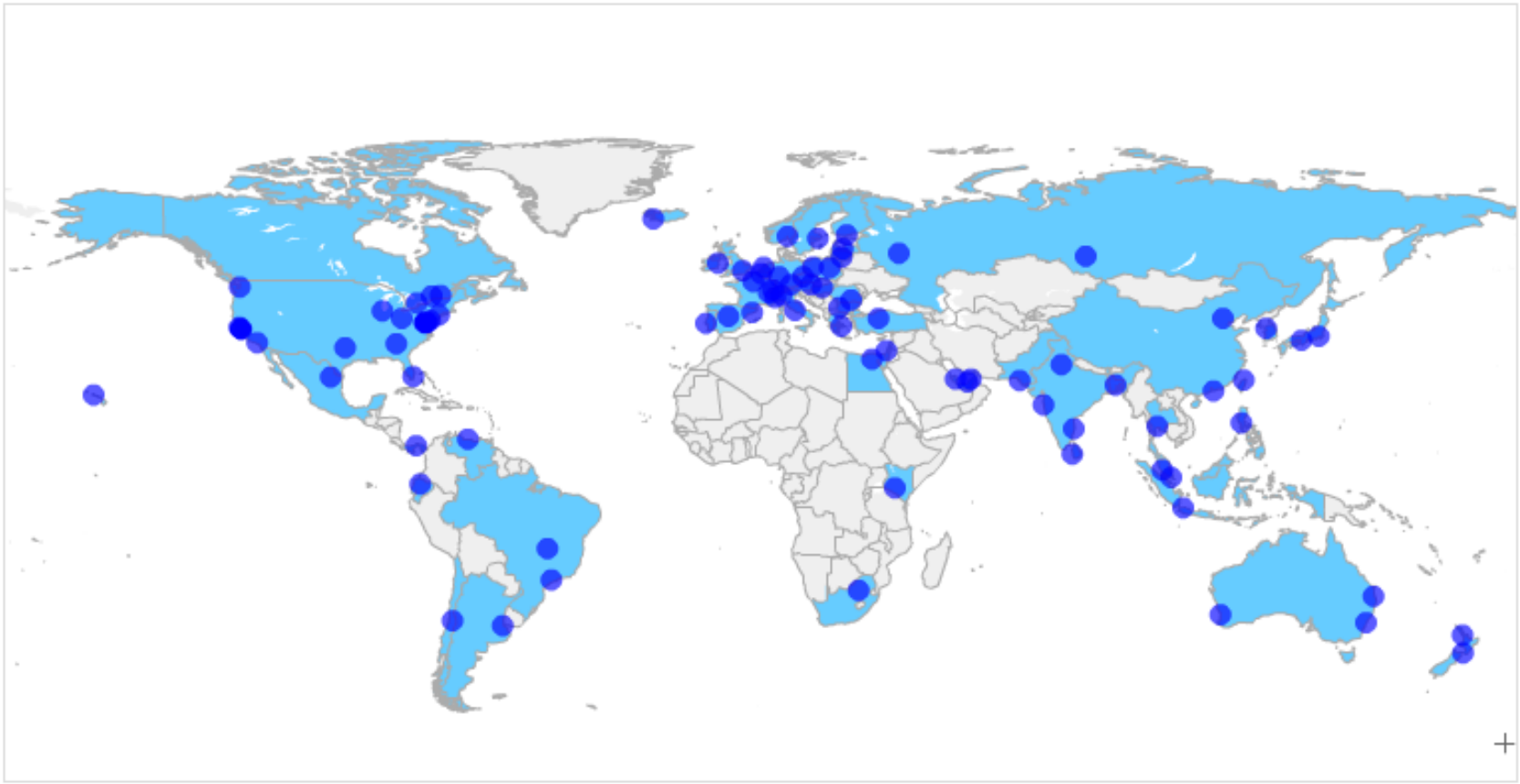
Localisation des serveurs DNS racine

Operator Sites: A, B, C, D, E, F, G, H, I, J, K, L, M

Countries and Distinct Economies Hosting Root-Zone Servers

City Locations of Root-Zone Servers

Source: http://www.root-servers.org



Les Top Level Domains

Les TLD (top level domains : exemple .Com, .Mil, .Net, .Edu, .Uk, .Fr) délèguent la résolution des SLD (sous domaines) à d 'autres (exemple : cnrs.fr)…

ccTLD (country code) : composé de 2 lettres : ISO 3166 : .fr, .us, .uk, .de … (+ de 240)

RTLD (Regional) : .int, .eu, .asia

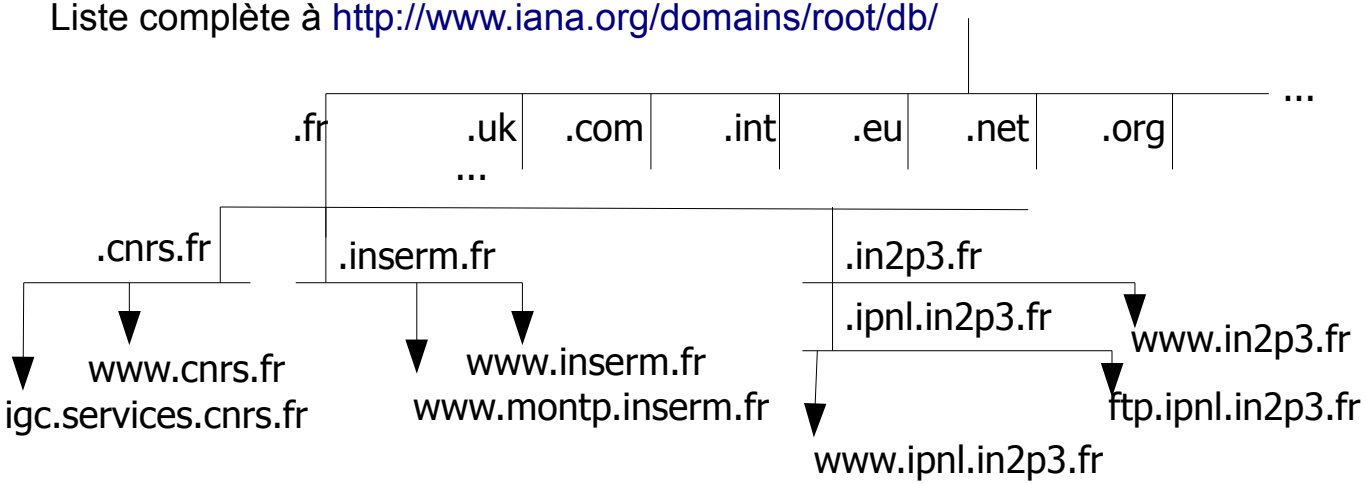
gTLD (generic) :

- en 1980 : .int, .edu, .mil, .gov, .com, .org, .net
- En 2000 : unsponsored (.biz, .info, .name, and .pro), sponsored (.aero, .coop, and .museum)
- En 2004 : .asia, .cat, .jobs, .mobi, .tel, .travel

En 2009 : Internationalized IDN ccTLD : avec alphabet non Latin

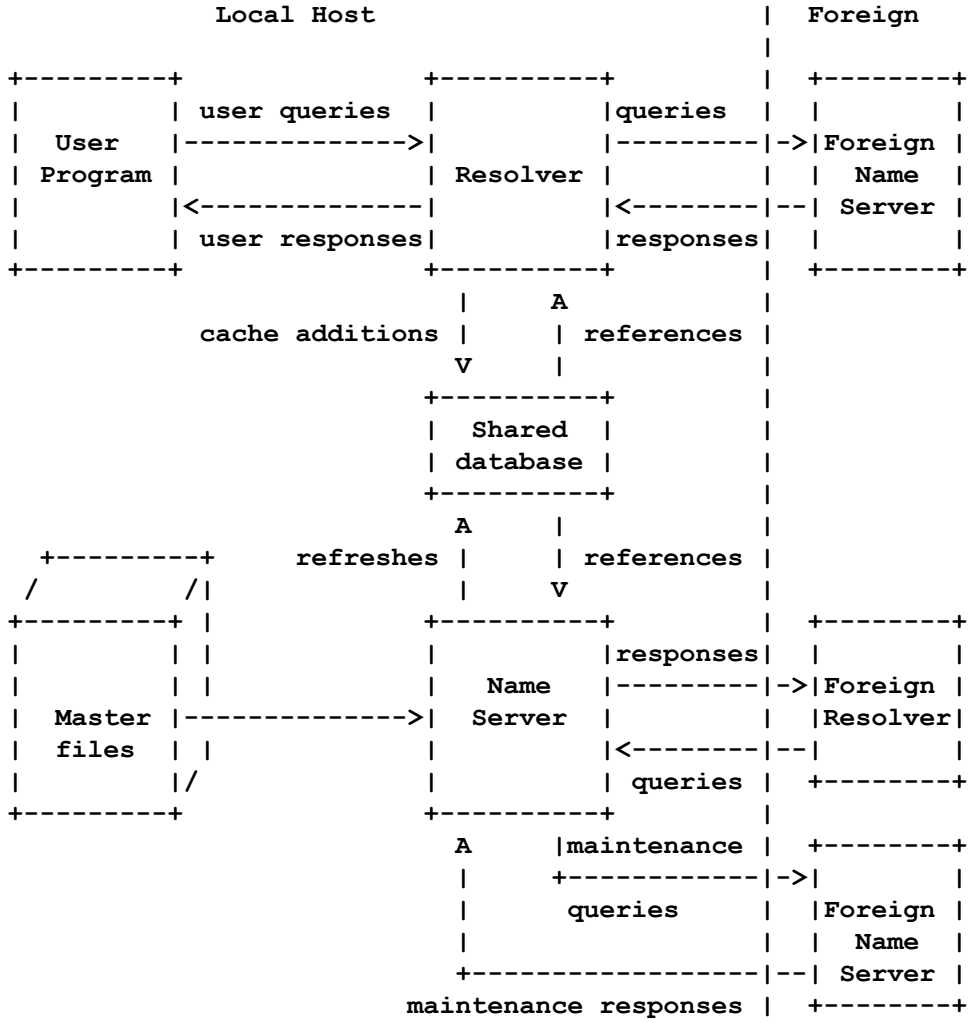
Spécial (raisons techniques) : in-addr.arpa et ip6.arpa (RFC3596), uri.arpa, urn.arpa, e164.arpa...

Liste complète à http://www.iana.org/domains/root/db/



DNS : Les différents intervenants

- RFC1035 : Domain Names – Implementation and specifications



DNS : types de requêtes

Requêtes itératives :

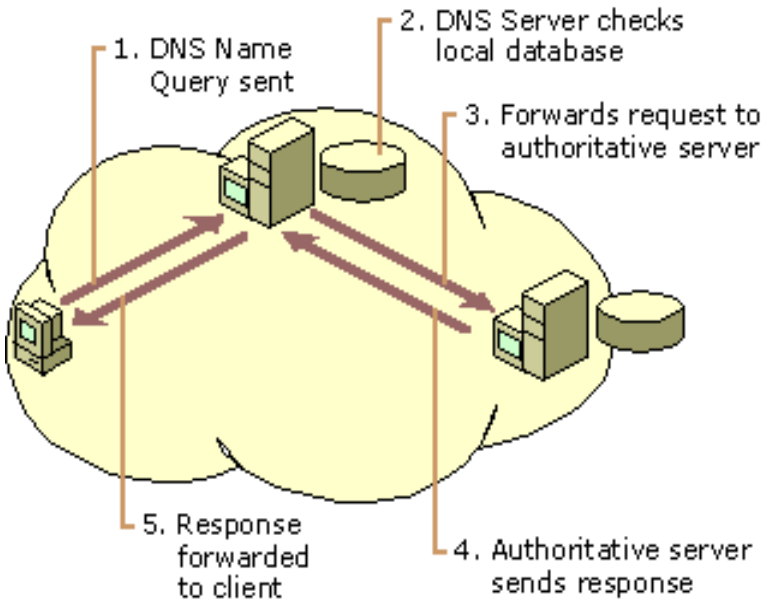
Le serveur retourne soit la bonne réponse soit une référence vers un autre serveur de nom à contacter

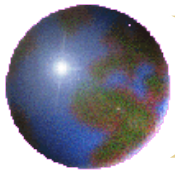
Les serveurs non récursifs répondent seulement aux requêtes pour les zones pour lesquels ils font "autorité". Ils ne conservent pas d'information en cache !

Requêtes récursives :

Les serveurs récursifs ont obligation de donner réponse au client. Ils questionnent à leur tour d'autres serveurs jusqu'à obtention de la réponse (ou erreur)... leur cache se remplit

Fonctionnement d'un serveur DNS récursif





DNS : Les serveurs

Les serveurs primaires détiennent l'origine des informations d'une zone (ensemble de machines) grâce à des fichiers de configuration

/etc/named.conf

/etc/named.data/db.hosts

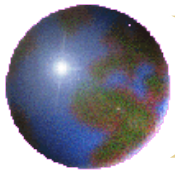
/etc/named.data/named.local

Les serveurs secondaires (esclaves) obtiennent leurs informations (périodiquement ou à la demande) par un échange (tranfer de zone) avec le serveur primaire

Les clients : demandent une résolution de nom (via un "resolver" (gethostbyname, gethostbyaddress))

DNS : les enregistrements

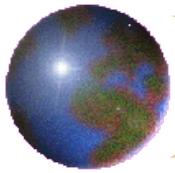
Type	Signification	Valeur
SOA	Start of Authority(acte de naissance)	Paramètres de la zone
A	Adresse IP d'u hote	Entier sur 32 bits
MX	Relais de messagerie	Domaine prenant le courrier
NS	nom de serveur	Nom d'un serveur pour ce domaine
CNAME	Nom de canonique	Nom de domaine
PTR	Pointeur	Alias pour une adresse IP
FO	Description de l'hote	UC et Système d'exploitation en ASCII
TXT	Texte	Texte ASCII non interprété



DNS : configuration (1)

```
; acte de naissance de la zone IPNL.IN2P3.FR
@ IN SOA lyodns.in2p3.fr. root.ipnl.in2p3.fr. (
                2010083102 ; Serial YYYYMMDDnn
                3600       ; refresh   1h
                600        ; retry    10min
                604800     ; expire    7j
                86400      ; minimum   1j
    )
;
; serveurs DNS pour la zone ipnl.in2p3.fr.
 IN NS lyodns.in2p3.fr.
 IN NS ccpnvx.in2p3.fr.
 IN NS ccpntc3.in2p3.fr.
;
; Mail Exchangers pour @ipnl.in2p3.fr
@ IN MX 10 ccpntc20.in2p3.fr.
@ IN MX 10 ccpntc21.in2p3.fr.

; serveur web
www             IN              A               134.158.138.23
;
ntp             IN              A               134.158.136.1
; lyopcs8 (mail)
imap            IN              A               134.158.138.12
smtp            IN              CNAME           lyopcs8.in2p3.fr.
; lyodmz3 (ftp)
ftp             IN              A               134.158.81.231
```



Commandes utiles pour DNS

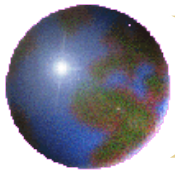
Dig : requêtes normales

```
$ dig +trace fr ns
$ dig +trace cnrs.fr ns
$ dig +trace igh.cnrs.fr ns

$ dig igh.cnrs.fr ns
$ dig ipnl.in2p3.fr mx
$ dig lyoinfo.in2p3.fr a
```

Dig : requêtes inverses

```
$ dig +trace 195.in-addr.arpa ns
$ dig +trace 83.195.in-addr.arpa ns
$ dig +trace 84.83.195.in-addr.arpa ns
```



SMTP (Rfc 821 & Rfc 822)

Définit :

L ’adresse électronique (RFC 822) :

Login@machine.Domaine ou prenom.Nom@domaine

Pas de différence entre minuscules et majuscules

Pas d ’accents, ni de caractères non imprimables.

Les caractères . et - autorisés. Le caractère _ non préconisé

Le format du message (entête et enveloppe)

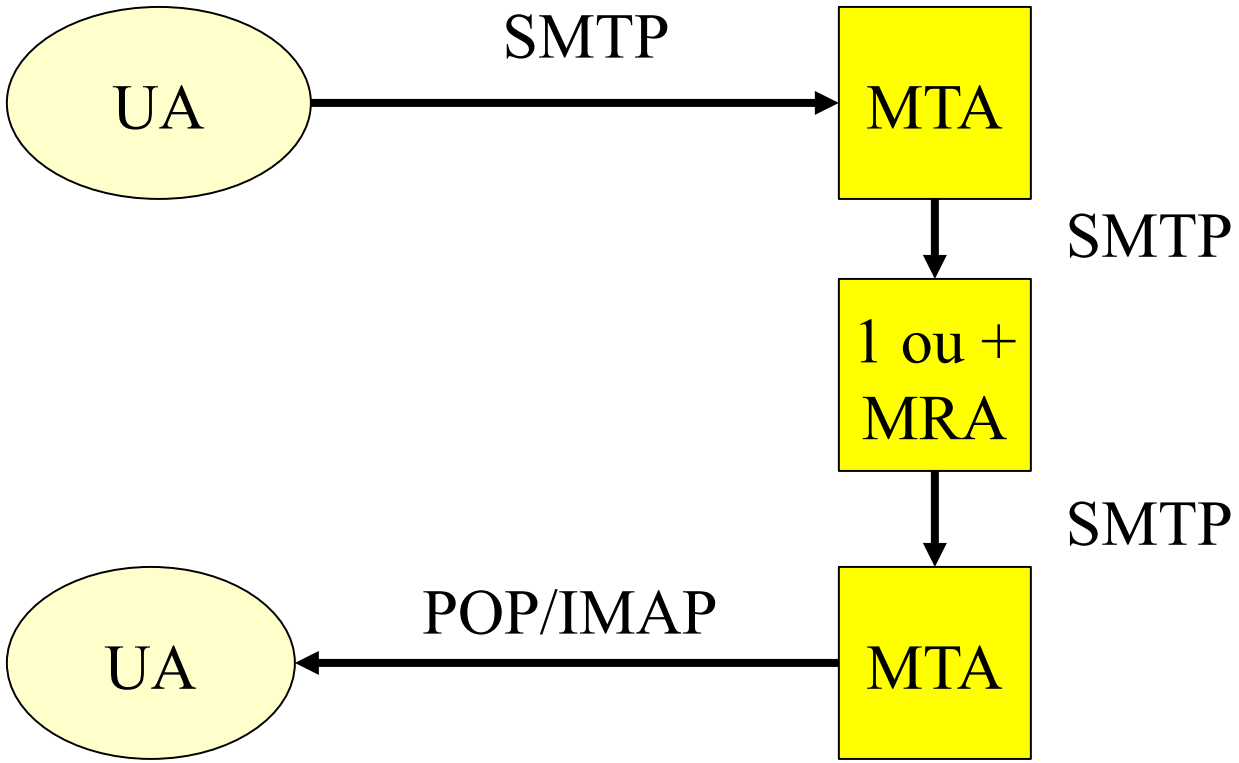
les notions suivantes :

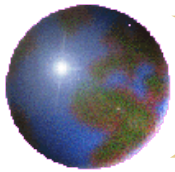
UA (User agent) : votre logiciel de messagerie (Thunderbird, Webmail, pine, mutt...)

MTA (Mail Transport Agent) : Un agent de transport reçoit un message et une direction, et l'achemine à l'endroit indiqué. Ne prends pas de décision sur le routage. Un agent de transport de messages est spécialisé pour un type de transmission particulier (local, UUCP…)

MRA (Mail Routing Agent) : Un agent de routage reçoit un message. En fonction de l'adresse du destinataire, il décide de faire appel à un agent de transport de messages, dont le but est d'acheminer le message dans la direction du destinataire.

Courrier électronique





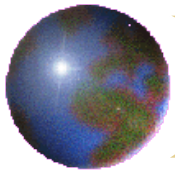
SMTP : Commandes / réponses

Commandes :

- HELO/EHLO (identifie le client)
- MAIL FROM (adresse de l ’expéditeur)
- RCPT TO (adresse du destinataire)
- DATA (introduit le message)

Réponses :

- 2xx accepté
- 3xx attentes de données
- 4xx refusé (erreur temporaire)
- 5xx refusé (erreur permanente)



SMTP : En tête d ’un message (1)

Voir la RFC 2076 : Common Internet Message Headers

From : Identité de l'expéditeur (la personne qui a souhaité que le message soit envoyé), placée par l'UA de l'émetteur.

To : Destinataires principaux du message, spécifiés par l'expéditeur à l'aide de son UA

Cc (carbon copy) : Destinataires auxiliaires du message, spécifiés par l'expéditeur à l'aide de son UA ;

Bcc (blind carbon copy) : Destinataires auxiliaires, spécifiés par l'expéditeur à l'aide de son UA. Ce champ n'est pas transmis aux destinataires spécifiés par To et Cc

Date : Date d'expédition, placée par l'UA de l'expéditeur

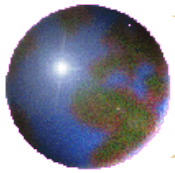
Subject : Sujet du message, spécifié par l'expéditeur à l'aide de son UA ;

Reply-To : Adresse de retour, placée par l'expéditeur, utilisée par le destinataire pour les réponses. Si ce champ n'est pas spécifié, From est pris par défaut ;

Received : Ajouté par chaque agent de routage le long du chemin emprunté par le message pour signer et tracer ce chemin en cas de problème.

Return-Path : Ajouté lors de la remise physique du message, c'est-à-dire lors du dépôt dans la boîte aux lettres finale par le dernier agent de transport, pour identifier le routage vers l'expéditeur

Sender : Identité de l'expéditeur réel : la personne (personne physique ou processus) qui a composé et envoyé le message, et qui reçoit les messages d'erreur liés au routage du message.



SMTP : En tête d ’un message (2)

Message-Id : Identificateur unique du message, placé par le premier agent de routage, servant à référencer le message. In-Reply-To : En cas de réponse, référence au message original placée automatiquement par l'UA de l'expéditeur de la réponse ;

References : Identification de messages précédemment envoyés et cités en référence ;

Comments : Commentaires (aucune utilité pour le routage), spécifiés par l'expéditeur

Encrypted : Indique que le message est chiffré et spécifie la méthode utilisée

X-??? : Les champs commençant par X- ne sont pas définis et sont réservés pour les extensions non encore standardisées ou pour des champs laissés aux utilisateurs.

Resent-??? : messages par un utilisateur si son UA le lui permet.
Exemples (Resent-From, Resent-Reply-To, Resent-To, Resent-Cc…)

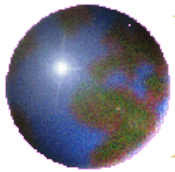
Le standard MIME définit également des champs d'en-tête :
Mime-Version : 1.0

Content-Type : text/plain; charset=« iso-8859-1 »

Return-Receipt-To : Pas ajouté par sendmail, mais par l'expéditeur du message. Lorsque sendmail réalise la remise physique du message et que ce champ est présent, il envoie un message de confirmation de remise (ce qui ne doit pas être confondu avec un accusé de réception) à l'adresse indiquée. Fortement déconseillée pour deux raisons essentielles :
il n'est reconnu que par sendmail, c'est-à-dire par une seule implémentation

il peut générer des boucles de courriers lorsqu'une liste de diffusion est en jeu.

Precedence : Ce champ donne la priorité devant être affectée au traitement du message.



Fiabilité du courrier électronique

Pas fiable :

- Qui l ’a envoyé ? (adresse source)
- Quand est-il arrivé ?
- comment savoir si le correspondant l ’a reçu ?
- comment savoir si le correspondant l ’a lu ?

Erreurs fréquentes :

- « Host unknown » : la partie domaine (APRÈS @) est invalide !
- « User unknown » : la partie utilisateur (AVANT @) est invalide !
- erreur sur le serveur mail qu ’utilise le correspondant (config, disque…)

Transite en clair sur le réseau, stocké en clair sur les serveurs :

- Utiliser le chiffrement pour les messages sensibles / confidenciels
- Utiliser le SSMTP pour chiffrer le transport des messages entre le UA et le MTA ou entre MTA

FTP (RFC959)

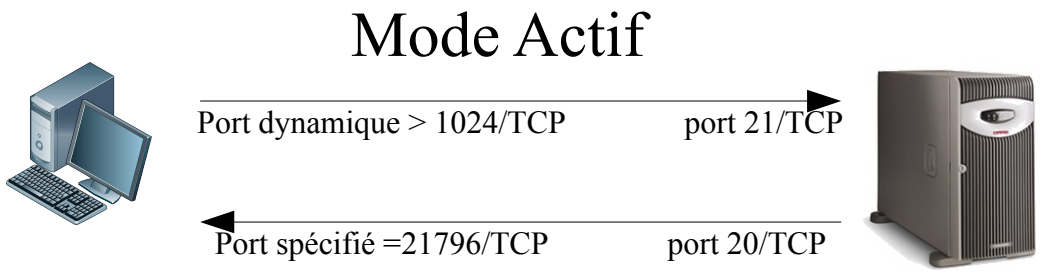
File Tranfer Protocol : Application pour transférer des fichiers

Utilise 2 connexions TCP :

1 canal de contrôle (commandes et réponses) : *port 21*

1 canal de données : cette connexion est ouverte puis fermée à chaque transfert

Modes actif / passif



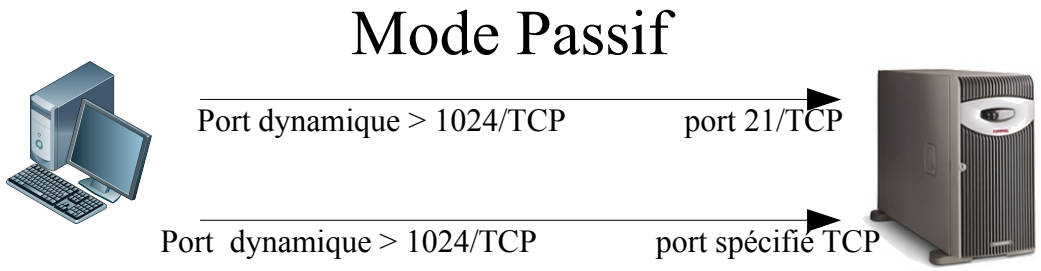
Le client FTP se connecte sur le port des commandes (21).

Le client FTP envoie la commande PORT N au serveur Ftp.

Exemple : PORT 192,168,0,186,85,36

Le serveur FTP initialise une connexion sur le port N (85*256+36=21796) du client pour engager un transfert.

FTP : mode passif



Le client FTP se connecte sur le port des commandes (21).

Le client FTP envoie la commande PASV au serveur.

Le serveur FTP envoie la commande PORT N au client. Exemple :

PASV

```
227 Entering Passive Mode (192.168.0.186,215,205).
```

Le client FTP initialise une connexion sur le port N (215*256+205=55245) du serveur FTP pour engager un transfert. Exemple :

LIST

Connect socket #564 to 192.168.0.186, port 55245...

FTP (3)

La réponse du serveur :

Précédée d'un nombre de 3 caractères :

1er chiffre permet de savoir à quoi se rapporte la réponse

1XX :

la commande commence a être exécutée, il y aura une autre réponse.

Ex :150 Opening data connection for ... (message en début de transfert)

2XX :

La commande a été exécutée avec succès.

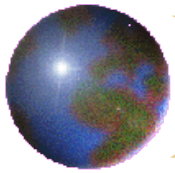
Vous pouvez envoyer une autre commande.

Ex: 226 Transfer complete (message en fin de transfert)

5XX :

Commande non acceptée.

Ex: 550 fichier: No such file or directory en réponse à "get fichier"



FTP (4)

Permet de transférer des fichiers

En mode "stream" ou "block" (Unix toujours en mode stream)

Texte (ASCII sous Unix)

Suite d'octets avec 7 bits significatifs.

Les fins de ligne, de page ... sont détectées et transformées si besoin pour être adaptées à la machine cible.

Il peut y avoir un transcodage: ASCII-EBCDIC

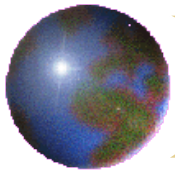
Binaire (Image)

Suite d'octets avec 8 bits significatifs.

Aucune transformation est apportée

Et les Macs ? La fameuse « ressource fork »

Mac Binary, Binhex, AppleDouble...



FTP (5)

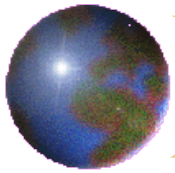
Principales commandes

help ou ?	liste des commandes
status	état des connexions
open	ouvrir une connexion (transparent)
user	entrer un nom d'utilisateur (transparent)
passwd	envoyer le mot de passe (transparent)
ls	fait un ls sur la machine distante
type	indiquer le type de fichier (**ascii** ou **binary**)

bin : Passer du mode binaire : transfert de fichiers non texte

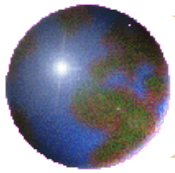
ascii : (transfert de fichiers texte simple -sans mise en page-

cd	changer de répertoire sur la machine distante
get	rapatrier un fichier (ouvre une connexion TCP)
put	envoyer un fichier (ouvre une connexion TCP)
delete	effacer un fichier sur la machine distante
quit	fermer une connexion



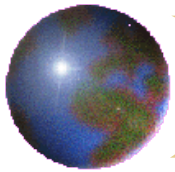
TFTP (RFC 783)

- Utilise UDP
- Sans contrôle d'accès
- Utilisé pour charger le système dans des équipements sans mémoire non-volatile et sans disque
- Utilisé pour charger la configuration des routeurs



Protocole DHCP

- Messages DHCPDISCOVER émis en broadcast par le poste client qui démarre sur le LAN, pour découvrir les serveur DHCP du LAN
- Message DHCPOFFER émis en broadcast aussi par un serveur DHCP, en retour d'un message DHCDISCOVER
- Message DHCPREQUEST du client pour obtenir une adresse IP, ou prolonger son bail
- Message DHCPACK *[ou DHCPNACK]* du serveur pour passer tous les paramètres réseau nécessaires, et confirmer allocation d'adresse
- Message DHCPRELEASE lorsque le client libère son IP



SSH présentation

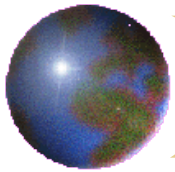
SSH est un protocole, devant sécuriser les communications. SSH chiffre, compresse un tunnel de session qui sécurise les données transmises (permet d'éviter les sniffers réseaux)

SSH est composé d'un ensemble d'outils permettant des connexions sécurisées entre des machines. Ces outils ont pour but de remplacer les utilitaires de connexions classiques n'utilisant pas de chiffrement. Il remplace : rcp, rlogin, rsh, telnet, ftp

La suite d'utilitaires est : ssh, scp, sftp, ssh-add, ssh-agent, ssh-copy-id, ssh-keygen, ssh-keyscan

Chaque **machine** et **utilisateur** créent et possèdent leur propre jeu de clés uniques (une clé privée = secrète, une clé publique = accessible par tous)

Une nouvelle connexion nécessite l'installation de la clé privée sur le client et de la clé publique sur le serveur



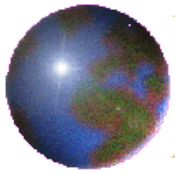
SSH : les composantes

Fonctionnement sur le schéma d'un système client – serveur

Les clients *ssh* demandent une ouverture de connexion au serveur *sshd*

La boîte à outils SSH est généralement composée de :

- Serveur : sshd
- Clients : ssh, scp, sftp(ssh= slogin)
- Des outils de gestion: ssh-add, ssh-agent, ssh-keygen, ssh-copy-id
- Les fichiers de configuration (OpenSSH) sont souvent dans:
  - Pour le serveur : /etc/ssh
  - Pour les clients : /etc/ssh et $HOME/.ssh



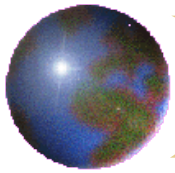
SSH : l'authentification

Lorsqu'un client se connecte par SSH, **le serveur lui envoie sa clef publique**, il y a alors **négociation d'une clef de session**, celle-ci sera chiffrée par la clef publique du serveur pour son transport sur le réseau, seul le serveur possesseur de la clef privée pourra déchiffrer cette clef de session.

Ensuite, toutes les données échangées entre les deux machines seront chiffrées et déchiffrées par l'algorithme avec la clef de session

Une fois que la connexion sécurisée est mise en place entre le client et le serveur, **le client doit s'identifier** sur le serveur afin d'obtenir un droit d'accès :

- **Par mot de passe** : Le client envoie un nom d'utilisateur et un mot de passe au serveur au travers de la communication sécurisé et le serveur vérifie si l'utilisateur concerné a accès à la machine et si le mot de passe fourni est valide
- **Par clés publiques** : Si l'authentification par clé est choisie par le client, le serveur va créer un *challenge* et donner un accès au client si ce dernier parvient à déchiffrer le challenge avec sa clé privée
- **Par hôte de confiance** : système équivalent aux systèmes utilisant rhost ou hosts.equiv



SSH et X11: X11 Forwarding

Relaye simplement toutes applications X11 à travers le canal chiffré

Ne pas configurer de variable *$DISPLAY* dans les scripts de connexion (.cshrc, .profile, .bashrc etc..), ssh doit remplir lui-même cette valeur

Donc c'est plus simple que telnet !

Il est nécessaire d'avoir un serveur X11 sur la machine du client (exemple Xming sous Microsoft Windows) et de le mettre en fonctionnement

Sous OpenSSH, serveurs et clients Unix sont configurés ***par défaut*** pour transmettre des données X11 dans le canal sécurisé

En cas de soucis, un test de fonctionnement peut être effectué en initiant la connexion avec l'option ***-X*** (active l'X11 en cas de non configuration dans le fichier /etc/ssh/ssh_config: voir côté serveur):

ssh –X login@machine

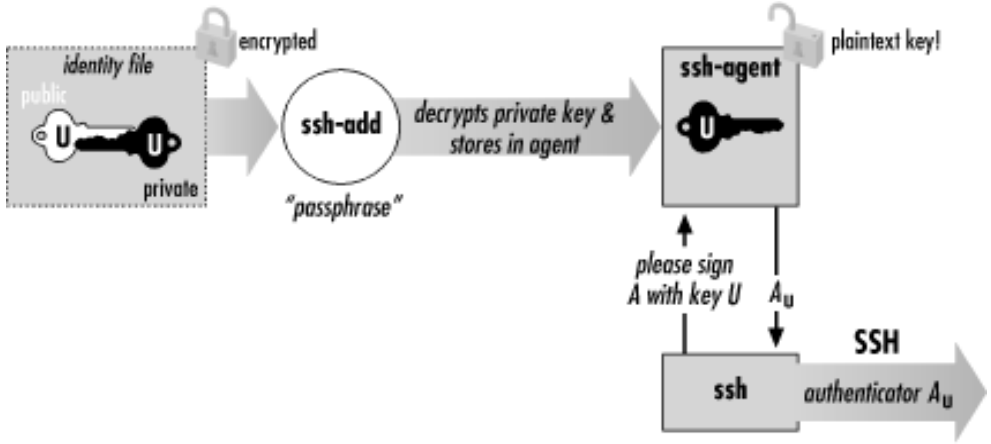
Les autres services : agents, tunnels

Des services additionnels. Décrits dans la suite :

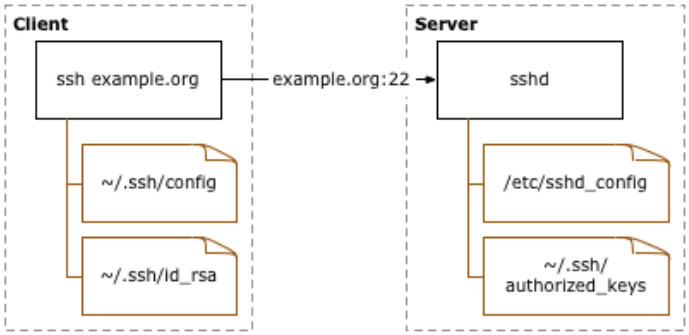
Agent SSH: utilisation en mode authentification forte : Programme qui garde les clés privées en mémoire et qui fournit les services d'authentification aux autres clients SSH.

Agent Forwarding: utilisation en mode authentification forte : Relaye les demandes d'authentification entre les différents clients-serveurs jusqu'au client initial (agent de mandatement)

Tunneling: permet de rediriger tout service TCP à travers un canal chiffré.



SSH : coté serveur



- Deux fichiers de configuration :

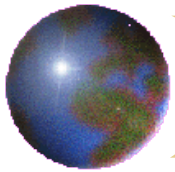
  - sshd_config : paramétrages lors des connexions du serveur local, ce fichier s'applique au démon sshd

  - ssh_config : paramétrages base et général du client ssh, ce fichier s'applique donc pour les commandes ssh, scp, sftp

- Les fichiers des clés privées/publiques du serveur :

  - Clés compatible V1 (sshv1) : ssh_host_key(privée), ssh_host_key.pub(publique)

  - Clés compatibles V2 (sshv2) : ssh_host_dsa_key(privée) , ssh_host_dsa_key.pub (publique) ssh_host_rsa_key(privée) , ssh_host_rsa_key.pub (publique)



SSH coté serveur : sshd_config

PermitRootLogin: autorise le compte *root* à se connecter

StrictModes yes: vérifie les permissions des fichiers et répertoires importants (accès au propriétaire uniquement)

PubkeyAuthentication yes: méthode d'authentification forte (rsa ou dsa) en V2

PasswordAuthentication yes: autorise la connexion par mot de passe

Host *: spécifie les hôtes concernés par la configuration qui suit (adresse ip ou nom DNS, * = toutes)

ForwardAgent yes: indique à l'agent que l'agent d'authentification doit être renvoyé vers la machine distante

X11Forwarding yes: active le transfert X pour sshd

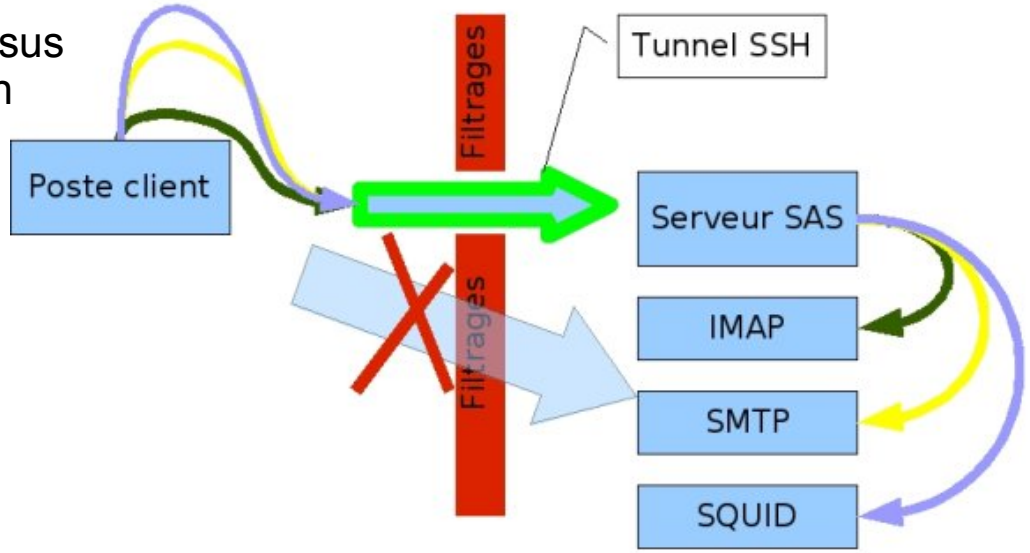
AllowUserslogin: autorise le compte local et seulement ce compte à se connecter via ssh

DenyUserslogin: indique que ce compte ne pourra pas recevoir de connexions ssh

SSH : les Tunnels

Les tunnels créés dans la figure ci-dessus pourraient l'être avec la commande ssh suivante :

```
ssh  -L10443:imap.domaine.fr:443 \
     -L10025:smtp.domaine.fr:25 \
     -L13128:squid.domaine.fr:3128 \
     user@sas.domaine.fr
```



Une fois *user* authentifié et connecté sur la machine *sas*, il peut alors se connecter sur :

- *localhost:10443* pour que sa connexion soit relayée à travers le tunnel à la machine *imap.domaine.fr* située derrière les filtres
- *localhost:10025* pour que sa connexion soit relayée à travers le tunnel à la machine smtp.domaine.fr située derrière les filtres
- *localhost:13128* pour que sa connexion soit relayée à travers le tunnel à la machine *squid.domaine.fr* située derrière les filtres