Administration Système et réseau
[M2 - 2015/2016]

http://www.infop7.org/cursus/M2/AdminSys#exam
http://info.paris7.free.fr/M2/Administration/
http://poireau.informatique.univ-paris-diderot.fr/~jmm/

M2 Info en société, Vue d'artiste

(Aimé, Gros Nico et Kevin)
(j'adore IT Crowd)

[Cours 1 - 06/01/2016]

Processeur

Sparc → pour faire du calcul par Fujitsu
power PC → pour transactionnel ou calcul par IBM
intel 8080A “premier” processeur

2 conneries d’IBM :

- Pas d’interet pour Unix
- Pas de brevet sur le montage du PC (Donc apparition de clones)

Processeur Intel 8080A :

- 1 Mhz
- 64 Ko

Multi-Core :

- multi-core => plusieurs CPU
- Pour 1 CPU on a 2 Thread (File d’execution que le CPU peut traiter)
- Le système d’exploitation voit 1 thread comme un CPU…

LE PC DE YANN COUTE 35 000 DOLLARZ (88 processeurs)

Mémoire

Max Ram actuellement : 32 Go.
Avant c’était limité à 4 Go à cause du 32 bits (2 ^ 32 = 4.294.967.296).
HS: Yann coûte cher !

Un peu de vocabulaire :

- Memoire = RAM
- Memoire secondaire = disque
- Géometrie d’un disque = nombre de têtes et nombre de plateaux
- NAS = serveur de fichier
- SSD (solid state drive) = mémoire flash
  -> plus rien de mécanique, pas d’usure
  -> rapide (pas aussi rapide qu’un processeur
  -> memoire est contigue
  -> durée de vie limité :
  lecture / écriture destructrice car necessite Raz de la mémoire, pour pallier au problème , taille mémoire plus grande qu’en réalité
- DSI = Direction des sytèmes d’informations
  -> gère l’ensemble du réseau dans une boite
-

Disque dur actuel:

- jusqu’à 10 teraoctets
- sujet à usure, car fonctionne “mécaniquement” ,
  -> tête de lecture sur un plateau qui tourne

Memoire primaire : Si on coupe l’electricité, on a plus rien, la mémoire flash résout ce problème.

Le **buffer cache** est un ensemble de structures de données et d'algorithmes qui permettent de minimiser le nombre des accès disque.

Pour optimiser la lecture disque "physique" (Pas SSD) : Le système de fichier tient compte de la géométrie du disque de manière à s'arranger pour écrire des données "proches" (d'un même fichier par exemple) sur un même cylindre de manière à y acceder en une seule fois.

Gestion SSD différente: (pas des géométrie de disque)

A Savoir (TODO):
- LACP
- VLAN ??
- zone de swap

Problèmes quand on a des composants (exemple : SSD, vitesse réseau) trop rapides: ils génèrent pleins d'interruptions ce qui peut ralentir le systeme

c'est quoi un "chipset" ? Une puce, un element d'electronique, c'est assez generique

LAMP / MAMP / WAMP
-> apache (se prononce apatchi) mysql PHP

machine (processeur basse fréquence) VS machine (processeur haute fréquence)
-> basse fréquence
- bien pour le WEB , peut gerer en simultané beaucoup de requêtes qui ne consomment pas beaucoup de CPU

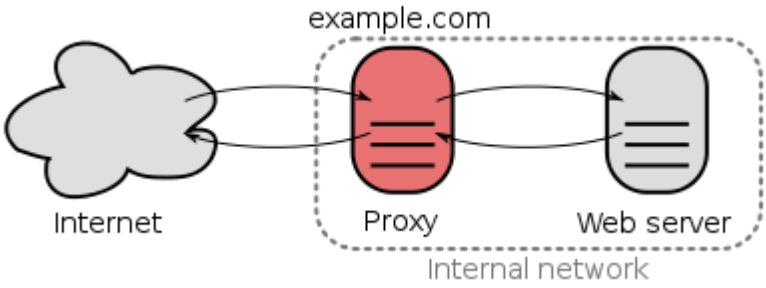
-> haute fréquence
- utile pour faire du calcule
- consomme plus d'electricité

[Cours 2 - 13/01/2016]

proxy (relais) :
- dispositif intermediaire entre un serveur et un client
- on s'en sert les ¾ du temps pour faire du WEB

avec un cache : 30% d'efficacité à cause d'un nombre important de pages dynamiques.

-> on se connecte depuis l'exterieur (par exemple pour acceder à magma, on passe par porrum depuis l'exterieur. Dans l'url on a "porrum" alors qu'on accede en fait au serveur magma)
Un proxy inverse (reverse proxy) est un type de serveur, habituellement placé en frontal de serveurs web. Contrairement au serveur proxy qui permet à un utilisateur d'accéder au réseau Internet, le proxy inverse permet à un utilisateur d'Internet d'accéder à des serveurs internes.

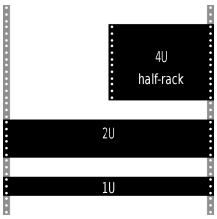


taille de baie (serveur) :

→ serveur raquable opposé au serveur tour (ne necessite pas de clim)

→ baie 42U : Le “U” etant une unité de mesure. Dans une baie 42U on peut mettre 42 equipement de taille 1U (hauteur).

 ⇒ serveur rackable qu’on insére dans des baies 



⇒ 1u (racket unit)

Une souris optique sur un support un peu rougeatre ça marche pas très bien. (JMM - 2016 - salle 2003)

Hot swap = Enfichable à chaud

-> si une alimentation tombe en marche , on change l’alim à chaud sans couper le serveur (2 plug de branchement dispo sur le serveur)

-> en gros un composant est enfichable a chaud si on peut le changer sans couper le serveur et endommager le système

les serveurs possèdent également un mecanisme de surchauffe:

-> ventilo/clim qui tombe en marche implique coupures des serveurs

Les disques durs sur un serveur sont enfichable à chaud, ce qui veut dire que physiquement, cela ne pose pas de problème d’enlever ou de brancher un disque “à chaud” mais il faut aussi que le système supporte ce genre de modification.

Si il y a une coupure de courant, les serveurs restent operationnel grâce aux onduleurs qui permettent aussi de rendre le courant electrique plus “constant”. Mais si au bout de 5 minutes l’electricité n’est pas revenue, les serveurs se coupent à cause du manque de climatisation (Risque imminent de surchauffe)

port serie : RS-232 est une norme standardisant un bus de communication de type série sur trois fils minimum (électrique, mécanique et protocole). Disponible sur presque tous les PC depuis 1981 jusqu'au milieu des années 2000, il est communément appelé le « port série ».

KVM: Keyboard Video Mouse

→ En informatique, un commutateur écran-clavier-souris ou commutateur KVM (switch KVM ou keyboard-video-mouse switch en anglais) est un commutateur qui permet de partager clavier, écran et souris entre plusieurs ordinateurs.

BMC : BaseBoard Management Controller

(Controleur de gestion de la carte mère) -> se situe dans le serveur, permet d'allumer, d'eteindre la machine sans y acceder. D'avoir des capteurs pour monitorer les ventilateurs par exemple.
Permet d'avoir une console virtuelles representant la console de la machine.
Permet d'avoir un media virtuelle qui permet de la configurer à distance.

Une fois que la BMC est configuré (une fois qu'elle a une adresse) on peut "gerer" le serveur à distance.

RFC1918

→ adresse internet privée

-> genre celle que notre pc utilise pour ce connecter a notre box

→ adresse non routable (Utile pour des soucis de securité)

#blague du prof
C'est Marcel un copain du lycée - JMM - 2016
OUARHAHAHARARARAR - JMM - 2016

Quand une machine ventile à fond, c'est qu'il y a un problème

→ en gros les ventilo ne sont pas asservie par le BIOS

⇒ du coup c'est synonyme que le serveur a crasher

→ machine trop demandée

Système de RAID

→ Les disques sont toujours de meme taille. Les données ne sont pas répartie de maniere unique sur les disques et donc les données sont reconstitutable à un certains degrès.

Disques :
- RAID0 -> entrelacement (permet d'utiliser plusieurs disques physiques pour stocker des données sans s'occuper de "ou est quoi").
- RAID1 -> miroir (les données sont stocker sur 2 disques à l'identique (Un genre de sauvegarde)

SNMP = protocole de gestion IP

→ permet de recevoir des informations

comment tafé? ça te regarde pas
c'est utile pour les schema en algo répartie ..
.c'est pour l'interet générale

blade (lame):

→ un ou plusieurs processeurs, pas mal de mémoire, et un peu de disque (juste le necessaire) et on met ça dans un chassis ayant un minimum d'intelligence et on voit ça comme un espace pour utiliser plusieurs machines virtuelles
interet: possibilité de clonage qui permet de rédémarrer plus facilement la machine
au niveau sécurité ça ne change rien par rapport à un DD physique

SAN VS NAS
→ ensemble de disques qui se différence par la façon de y accéder
SAN : ensemble de disque vu comme un seul element, cela permet de presenter un espace disque.
NAS : La gestion des disques est fait par le système NAS lui même. Il gêre le disque tout seul.
Un NAS est cher car on garanti qu'on ne eut pas perdre de données?
→ parcequ'il a un disque dure "Spaire" qui prend le relais si 'lun tombe en rade
→ car en cas de panne, le constructeur est prévenu et fourrnit la piece de rechange

df
→ display free disk space

mount
→ mount file systems

[Cours 3 - 20/01/2016]

Virtualisation (1970 par IBM)

Premier système de virtualisation : VM370 (Par IBM donc), ce sont des machines à écrire.Permet à chaque utilisateur d'avoir sa machine virtuelle sans empiéter l'un sur l'autre.
90% des attaques sur les systemes sont faites par injection de code (sur de l'intel car il faut connaitre l'architecture du système). Exemple en javascript, la fonction 'eval' est potentiellement dangereuse car elle peut évaluer du code d'un utilisateur.

Grâce aux machines ayant beaucoup de memoire, on peut maintenant lancer pas
mal de machines virtuelles sur une seule machine physique. Intel et AMD fournissent des outils specifiques pour ce genre de tâche.

KVM (keyboard video mouse): deja vu au cours précédent

Simulateur vs Virtualisation:
→ Simulateur: c'est à l'ancienne , pour simuler les vieilles machines, on simule réelement le processeur (simulateur mips)
→ Virtualisation : On utilise une machine virtuelle sur la meme architecture que la machine hote. La machine virtuelle va executer directement le processeur.
but: avoir des environnements disjoints qui ne communiquent pas entre eux.

FTP anonyme (file transport protocol): utilise le port 20 et 21 en TCP
-> utlisé dans le WEB

chroot (commande UNIX) emprisonne un programme dans une nouvelle arborescence de fichier:

sudo chroot ls new_root/ => affiche les fichiers à la racine de new_root/

le programme lancé de cette façon ne peut pas accéder aux fichiers à la vraie racine de l'arborescence.

Logiciel de virtualisation : VirtualBox (gratuit et marche sur toute une serie de système, c'est pas le meilleur…), xen, qemu.
Dans les payants on a VMware (*"Le moindre merdier, c'est 10 000 euros, c'est pas pour les pauvres"* - JMM - 20 janvier 2016 - Université Paris Diderot - salle 2003)

Mise au point sur les OS :

- Linux s'inspire de System V. Il a totalement été réécrit mais les commandes sont les mêmes (à quelques exceptions près) que sous les UNIX.
- Dans un BSD les commandes d'origines sont celles d'Unix, ce qui va poser un problème au niveau utilisateur, les flags de la commande "ls" different par rapport a Linux par exemple.
- De plus entre Linux et BSD, le file system est différent. On a d'un coté un file system journalisé sur Linux : *ext2, 3, 4* et un file system *ZFS* du coté de BSD

→ ZFS: un filestyme qui inclut un LVM à l'interieur, gère le cryptage, et le "REd logiciel" ???, taille de la partition sans limites

swapping : complémentaire à la mémoire virtuelle, utilisation de la mémoire disque ROM pour étendre la mémoire vive RAM.

<u>mécanisme de boot : (bootstrap)</u>

- En premier on execute les "post"
- Ensuite le moniteur BIOS ou OpenBoot, OpenProm (totalement hardware)
- Ensuite execution du Kernel qui regarde la configuration de la machine puis execute le programme.

tables de processsus :
table ou on a l'ensemble des processus (utilisateur , PID)
table des description,
contient l'ensemble des fichier ouvert avec le descripteurs associée

buffer cache :
→ permet de garder les info en memoire sans forcement les écrires directements

processus en mode noyau:
→ lancé directement par le noyau, accéde au info, ressource du noyau à contrario du processus user;

root :
→ est un user avec des droits priviligiés, il a pas accès au noyau

processus en mode user :

→ lancé directement par le user
→ pas d'acces aux tables sauf avec des apples systèmes

processus swapper :
→ Sauvegarder une partie de la mémoire centrale sur un périphérique de stockage pour la libérer pour utilisation par un programme qui en a besoin.

mémoire virtuelle (pas mal d'info ici site de barbus):
→ pagination controler par "page deamon" (en général, une page pèse 4096 octets)
→ un MMU (Memory Management Unit) est indispensable: fait la correspondance (mécanisme de conversion) entre adresse physique et virtuelle. La taille physique d'un binaire est plus importante que que sa taille virtuelle.
→ défaut de page: Un défaut de page correspond à une série d'événements se déroulant lorsqu'un programme essaie d'accéder à des données (ou à un code) qui se trouvent dans son espace d'adressage mais ne sont pas actuellement placées dans la mémoire vive (ou RAM) du système. Le système d'exploitation doit traiter les défauts de pages en permettant, d'une manière ou d'une autre, l'accès à la mémoire des données recherchées afin que le programme puisse continuer ses opérations, comme si le défaut de page ne s'était jamais produit.

2 types de pages
→ pages de texte :
- correspond au code, programme, pas dans la zone de swapp,
- dans le buffer cache
→ page de données,
- dans la zone de swap on veut sauvegarder les données

adress MAc : adress de niveau 2

une bague d'or ? backdoor nan ? ok allons posée et se gratter le machin !

[Cours 4 - 3/02/2016]

Le Cloud (l'informatique dans les nuages):
→ le cloud utilise des clients légers
- on se connecte sur le client léger pour acceder à des donnees qui ne sont pas stockées en local
→ problème: on devient dépendant du réseau
- pas de réseau, pas d'acces aux données ,pas de taff
- données sur le réseau implique faille de sécurité

Client léger :

→ évolution du terminal X : (gestion du graphisme avec supplément (type gestion de périphique que le simple terminal X ne peut pas faire))
Pas de disque -> Peu de chance que ça tombe en panne, possible d'interchanger les machines sans problème car rien n'est stocké dessus.
Parfait pour le Cloud : Le client leger se connecte au cloud et ne fait que recuperer les données du serveur.

protocole X11:
→ ça gère un display (c'est le serverX qui le gère en communicant avec des Clients (exemple XTerm) et en utilisant des prototoles comme TCP avec des ports à partir de 6000)
→ ce display correspond à l'ecran/clavier/souris

Terminal X :
→ Une machine sur laquelle on avait le strict minimum : un serveur graphique qui permettait de gerer l'ecran et le clavier.

Un entreprise qui à pleins de terminaux (clients légers, PC, …) chacun se connectant au réseau de l'entreprise pour fonctionner. Tous dépendent du réseau donc si le réseau tomber plus personne ne peut travailler.

RSS = Résidante Set Size
tmp = c'est un memory file system (activable sur linux)
→ memoire virtuelle stocker la dedans

RTFM !
→ ride ze friendly/fucking manual
#blague du prof
"En shell ou en seychelle - JMM- 2016"

Shell
→ interpréteur de commande

ksh : Korn Shell. Un shell puissant assez présent sur les Unix propriétaires, mais aussi disponible en version libre, compatible avec bash.

sh : Bourne Shell. L'ancêtre de tous les shells.
bash : Bourne Again Shell. Une amélioration du Bourne Shell, disponible par défaut sous Linux et Mac OS X.

Cshell = dispo sou BSD
TCSH =
screen : permet d'ouvrir une session ssh et éventuellement de la suivre après

tee : redirige qqch vers un fichier et l'affiche

“RRRRRRRRRIIIIINNNN-RRRRRRRRRRRIIIIINNNNNN - JMM”

[Cours 5 - 10/02/2016]

Salut le cours 5 ! Comment ça va ? On va bien rigoler. Promis !
En fait
En fait
En fait en fait en fait … en fait

- Parametrage de la machine virtuelle
- “C’est quoi les bails.”
- Une adresse (IP) est attribuée pour un certain bail donnée (un temps) ensuite elle doit être renouvellée.

C’est quoi un NAT monsieur ?
chown : commande changement d’user

le catalogue master2 est monté sur un NAS , et permet de récupérer un fichier effacer grace au snapshot. $.snapshot/
le snapshot est sur un NAS.

rm sur un fichier
→ c’est la suppression des liens sur le fichier

zone de swapp
→ ça sert a mettre les pages des processus dans la zone d’échange

fg
→ reprendre un job qu’on a suspendu (on suspend un job avec Control Z)

halt -p
→ pour arreter la bécane

“NAT, c’est comme les couettes HAAHAHAHAhAHA - JMM - 2016”

[Cours 6 - 17/02/2016]

Bonne Lecture.

Authentication d'utilisateur.

Système crypté

2 types d'auth :

- par un fichier local. : /etc/password
- soit repartis :
(Protocol Yp : Yellow Pages)

Protocol LDAP : mis en place avec Microsoft : protocole **d'annuaire** pr avoir des infos (sous windows c'est acitive directory) pas vraiment pour authentifier.

LDAP : c'est du Tcp. : client qui ouvre une **session** sur un serveur ldap. : **très lourd** si nb clients qui tentent de s'y connecter.
On s'en sert (Mac Os)

LDAP (light directory access protocol) :
→ mis au point par microsoft
→ Protocole d'annuaire pour obtenir des infos (pas pour authentifier)
→ sur windows, active directory permet de tout référencer

LDP : basé sur RPC, (XSR ?!) c'est du UDP, ca marche avec un serveur qui contient toutes les données.

NFU : N For Unix : Services Unix qui étaient offerts de ddl, abandonnée à partir de Win Seven.
Sur tous les unix a l'exception de OpenBSD, il y a un fichier /etc/nsswitch.conf où l'on précise pour les users (les password ?)

passwd	File	nis	ldap (precise l'aiguillage pour dire quel … utiliser)
…	File	dns	

sur OpenBSD ce n'est pas comme çà. #c'estAnnectodic

login → par convention c'est 8 caracteres
chaine cr**y**pté: avec algo DES (13 charactères) (Ubuntu SHA12)
la constante 0 va ê codé avec la constante 0, c'est le cryptage de cette constante qui est stocké, on compare ensuite, EN FAITE, on vérifie que les 2 chaines cryptés coincides.
Pb : 2 users mdp identiques.
-> on rajoute un **piment :** la **salt key** : on la rajoute au mdp crypté, on rajoute en faite **la date.**

uid → a priori plus de limite (pour les users il connait le UID)
gid → identification du groupe
fingername (ou champs GCOS) →
(commande finger …)
catalogue de travail (**working directory:**) → celui sur lequel on se connecte

Sous Unix pas de system de verrou intern (ils sont externes..)
-> Pour gérer les mecanismes de verrou de etc/password : il y a le fichier de travail : /etc/ptmp : qui permet de vérifier : garanti que la chaine crypté n'est pas visible : garanti : 2 personnes pas le meme mot de passe.

#blague c’est mon cousin Germain, un pote du lycée

-> Si perte du mdp de root :
Solution : boot -s (sur OpenBSD) : permet de booter en single user , donc en principe les démons n’ont pas été lancés (les démons de minuit) .

Certains systemes : demande d’entrer le mdp de root avant de rentrer de mode single user.
-> solution : booter a partir d’un system d’installation, monter la partition à la main , puis modifier le fichier /etc/passwd à la main (JACKPOT).

Certains font des versions hachés du mdp (compliqué…).

Cas de Solaris : qd boot single user : avant de booter demande le mdp root (cas cité juste en haut).
#DoncC’estUnEnferEnFaite.

En faite, DES ne serait pas crackable.
Par, contre, avec l’attaque en force brute ? possible à decracker .?
un fichier etc/passwd et un dictionnaire.

#BrooklynHacker !!!

le 

commande naive : gmake
commande amélioré : gmake -j (nb de processeur) (bcp + rapide)

idée : appliquer gmake -j au fichier /etc/passwd
-> utiliser au max les CPU cores, et les repartir.

Ainsi, on ne veut pas que ces chaines (fichier /etc/passwd) soit visibles de l’extérieur.
L’user se connecte en mode root, pas de pb de droits.

ls -l /bin/passwd

7 uid bit ?
set uid bit ?
cet uid bit ?

-> si kk1 au café, on prend une copy de /bin/sh , on le copi sy chez soit, puis … cette copie appratient au mec, apres on met 7 uid bit sur sa copie, du coup on aura une sessiosn en son nom ! Lancement d'un shell sous son nom.
-> donc 7 uid bit :très dangereux.
Bla bla chocolat en californie.

7 gid bit ?

- -

/etc/passwd : permet liaison uid pid.

le LDAP : permet de crypté la chaine crypté qui ne sera pas visible.

Dans etc/passwd : info necessaire.
le mdp va etre dans le fichier etc/shadow

cat etc/password pour afficher le truc du dessous:

jmm:x:1000:1000,,,:/homedirectory:/bin/bash
login : mdp : uid : gid

sudo cat etc/shadow

jmm:$SALT KEY$(très longue chaine qui decri lalgo utilisé, SHA- 512 ici)...

Système à base de clé : bcp moins sensible à la casse.

du shadowing ?
du passwordadjing ?

definiir des param de calucités.
appliquer des contraintes (majuscules, minuscule, …) : changer le mdp au bout de 3 mois par xemple, on peut empecher un changement aussi (sécurité)
EN faite, en faite, en faite, en faite …

On peut forcer la consultation sur dictionnaire.
MDP très très simple : au bout de 2 jours on se fait carroter, annecdocte :
login carine, mdp : carine : elle s'est fait connécté depuis l'afrique du sud et la géorgie.
Donc, 1 journée pour le piratage.
EN faite, en faite, en faite, en faite …

cat /etc/nsswitch.conf

Samba : implémentation de CIFS sur Unix (serveur mail de mAIYcrosoft): permet d'acceder à du CUFS .? donc utilisable par des clients ouindoswe.
kismet : c'est un utilitaire pour scanner le wifi (commande)

#Pause. 14h26.
#C'est la fin de la récré les enfants.

On va regarder des logs: pour voir eventuellement les tentatives de piratages.
On attends. On arrete d'attendre.

Log de routeur d'accès à l'ufr : IPV4 , IPV6.
Le rooteur :

- ca root
- capable de définir des accès.

Différence avec FireWall :
Un rooteur fait du **stateless.** : on ne memorise pas le faite que l'action ait eu lieux, laisse passer en port 20 et 21
Firewall : **statefull** : capable de prendre des decisions: pouvoir bloquer. types actions de déni de services (#attaqueDDOS #Safir #Camille)

Routeur CISCO.
Rooteur :JUNIPER (a la fac) : config + simple et intuitive en droits d'accès.
Politique : on (la fac) bloque tous en faite et on interdit uniquement.
c'est des routers en GigaBit.

commande tail : fin de fichier
tail -f : fin du fichier en continu.
commande head: debut du fichier.

Juniper : 4 interfaces.

- management
- sortie
- entree

Actions:
A : autorized
D : Denied.

machine a Riflet : 194.254.199.51 voilà, elle est mal configuré.

Nivose n'est pa A à sortir sur le port 25.
->il y a 1 relais qui contact 1 relais de l'université :

- On essai de configurer au max , port 25 , securise.

MacOS espionne + encore que Windows.

port 23 : service TELNET : on n'utilise pas: une session de terminale.
Surement une faille de sécu, qui a été publiée.
(Rlogin : rien n'est crypté, session de login aussi)
-> tentative de piratage
Spoofing d'adresses : kk1 qui change son adresse IP.
Spoofing d'adresses mac facile à faire aussi.
-> avec VirtualBOx notamment on peut changer son adresse MAC.
Pb de Windows: a chaque sortie on passe par un Proxy.
Mais il y a des services qui ne passe pas par des Proxy.
Par exemple le Windows Update : proxy de systeme.

Si, ya quelque chose qui repond alors on passe à une attaque de types diifférentes.

--
Dans fichier le log de connexion de nivose :

qq1 a essayer de se login avec le "cisco" parce que mot de passe et utilisateur par defaut prédéfini.

JMM à du BlackLister : une centaines d'adresses en chine: car il y a un grand nombre d'adresse disponible en autres.

Interêt : de pirater
- l'ufr : Aucun.
- un poste du voisin : c'est de rebondir.(la police viendra chez lui).
- depot de Warez.

Explications: un robot qui lance sur les adresses ip qu'il trouve.
nmap: donne les ports ouverts.

OpenBSD : sure.
Choisir une architecture pas connu (pas Linux en l'occurrence), et une architecture pas connu, i386, amd64 sont connus !

Utiliser un OpenBSD sur Spark : rend les choses difficiles: mais comme il y a un trou de sécurité sur PHP pourra …
"SYNDROME de l'ukrainienne à poils ou à la poile ?" - JMM 2016

La loi : politique qui dit de les conservés 1 an !

" On fait autre choses que du Camel ici " - HRmmmm- Blague

Tentative de piratage dans un sens et dans l'autre.

-> qq1 sur le port 22 vas faire un essai sur toutes les adresses: sur une machine acces : … : sur nivose pleins de mdp recuperer ?!

Le CERT : Notification de pb de sécurité sur les logiciels.
-> qq jours après il y a des tentatives de connexions sur ces protocoles !

machine mal configuré : machine qui parle bcp : Proxy mal configuré.
-> qui essaient d'envoyer du mail : mal configuré : essai d'envoyer du mail sur le port 25 mais qui n'as pas le droit/

EN somme : on a pas configuré les machines avec protocoles sil on le droit ou pas sur certains port .

Les logs sont gardés pour ?...

changement de taille de police en 10.

Questions sur les logs examens !

Dans les logs :

on a la session, pas le contenu, il n'ont pas le droit de regarder les fichiers, et nous pas ceux des autres.
GMail -> spam sur un certain message -> interdit.
En faite, en faite

machines systèmes de Vlan..

Toutes ces consignes sont possibles car ils y a des protocoles de consignations.
(log = consignation) // les anglais sont des sales types.

SYSLOG : protocol sur le port 13.
→ standard de l'internet : RFC

grep syslog /etc/setr
grep syslog /etc/services

Syslog d : demon implémente le prot, message en UDP, dans /etc/syslog.conf il y a des entitiés (mail, hotes, kernel, lpr(impression)): le msg est associé à telle entité.

more /usr/include/sys/syslog.h

entité LOCAL 0 à LOCAL 7 sont à la dispo de l'utilisateur.

pour evité d'afficher constatment des msg dans le ter, on envoi les msg avk Syslog.

un message va être estampillé…

le fichier syslog.conf va permettre de faire un choix.

commande write : write pseudoNivose
envoie message.

openlock ? openlog ?
closeLock ? closelog ?
syslog

Fin Du cours, pour aujourd'hui, Gros.
a faire chez nous → faire tourner wireshark pour voir qui tente d'attaquer chez nous.

[Cours 7 - 24/02/2016]

HotSwapping

VMWare
Virtualbox pas possilbe

Comment partitionner un disk, un filesystem, nous verrons celà.

disk dur : sas, vdi (vhd sur vmware)
ajouter un controleur sas

SAS ; standard SCSI : standard pour les serveur:
→ Alan Sugartch -> protocole SASI

il a fondé Seagate.

stantard SASI : transfert en parallèle.

SASI 3 : norme , standard en couche donc rapelle IP et le modèle OSI.
on prend un protocole et on le fait passer au dessu de IP et de l'Internet.
→ On à créer le ISCSI : standard au dessu de l'internet. → permet de connecter des SAN. pose des problèmes de longueurs.

""l'idée qui" est eu derière…" - JMM 2016
"il fallai l'OSI le dire" - JMM 2016

SATA : (Serial Advanced Technology Attachment)
en série bit a bit comme l'ubs (pas en parallèle)

Système Fiber Channel : pas de l'ethernet pas de l'IP.
→ connectique réseau qui n'est pas de l'éternet
On peut faire passer çà a travers un switch et la router.

SCSI

SCSI, *Small Computer System Interface* en anglais, est un standard définissant un bus informatique reliant un ordinateur à des périphériques ou à un autre ordinateur. (wiki)

SAS:

→ plus de transfert en paralléle mais en serie (bite à bit)
-> HBA : host bus adapter
→ fait la jonction entre (la machine ?) et le SCSI
→ debit de l'ordre de 6 gigabits jusqu'a 25 GBits
difference entre SAS et SATA
→ SAS plus chere (c'est du SCSI)
→ + rapide en 10 et 15 K tours par moins = disque rapide.
→ 146 Go à 1,6 Téra : disk rapide et chère.
→ 1.6 Téra SSD : 16 000 € : Méga Chère : Peu Utile
-> mieux vaut plusieurs disque peu chères.

Différence : Pb de coûts !!

SATA:

→ moins chère
→ 5,4 K tours minutes pour les portables / pc
→ pour Serveur : 7200 Tours/min
→ capacité jusqu'a 8-9-10 Téra.

Le RAID est un ensemble de techniques de virtualisation du stockage permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit les performances, soit la sécurité ou la tolérance aux pannes de l'ensemble du ou des systèmes.

Redundant Array of Independent Disks, ce qui signifie « regroupement redondant de disques indépendants ». Le coût au mégaoctet des disques durs ayant diminué d'un facteur de 1 300 000 en 29 ans, aujourd'hui le RAID est choisi pour d'autres raisons que le coût de l'espace de stockage

Controleur RAID Hardware ??

il va proposer les volumes deja …

Un ensemble RAID
En gros : serveur rapadité need :prendre SAS
si pas need de rapidité : prendre SATA.

SAS ET SATA : supporte le hot swap.
un disque sata est considéré comme un disque SCSI.
label GRUB défini : les … quon peut avoir.

commande: disklabel

tmpfs : filesystem en mémoire.
dans **Run** : soit des PID , soit des PID démons, ou fichiers temporarire, pas de programmes.

fichier c : fichier bufferisé, sinon ils sont pas bufferisé. (historiquement caractere)

/dev/zero → équivalent de dev/null mais ????

le num majeur: defini le type de peripheriques
    s'il change celà signifie des ph différents.
    num majeur= 5 pour /dev/ttyp*

le num mineur : Saphir ?? yo no sé
    Un ID pour differencier les peripheriques de ce numero de majeur ?

commande:
ls -l /dev/wd0*
brw-r----- 1 root operator   0,   0 Feb 10 14:25 /dev/wd0a
brw-r----- 1 root operator   0,   1 Feb 10 14:25 /dev/wd0b
brw-r----- 1 root operator   0,   2 Feb 10 14:25 /dev/wd0c
brw-r----- 1 root operator   0,   3 Feb 10 14:25 /dev/wd0d

b: pour bufferisé
Ecriture asynchrone, bufferisé.

putin Jean Neymar , yaura rien de tous çà à l'examen sa mére.
oui

commande: **df -kh**

Installation de bash.
pour BSD : 1 seul source de package.
Ubuntu on peut ajouter une/des source
Systeme de packages : permet de faires des upgrade de tous ce qui à été installé.

su : faire une sessoin au nom de KK1 d'aautres.

su - : meme condition que le login
su - // root
su -jmm // exactemetn pareil que session de login

vi /etc/pkg.conf

ed /etc/pkg.conf

sed et ed : très puissant.

ctrl h pour revenir en arrière.

‘Comme j’suis un peu fumié, je vous l’ai pas dit.” - JMM 2016

pkg_add bash

/etc/profile : où on met toutes les commandes qu’on veut exporter.

après faire

. /etc/profiler

nslookup 194.254.200.25 : machine de la dsi

```
cat /etc/resolv.conf
# Generated by em0 dhclient
search univ-paris-diderot.fr
nameserver 194.254.200.25
nameserver 194.254.200.26
lookup file bind
```

Dans le fichier resolve.conf ajouter une adresse :

ps -auxw

les processus en backgrounds n’ont pas de terminal de rattachement.

/sbin/init : controlle les passages en user ou multi usier
le role de init c’est de controle le passage en multi-utilisateur

ls /etc/rc.d
→ contient un ensembler de scripts d'initialisation pour chaque niveau.

---

pour activer un service:

svcadm -v disable ntp
svcadm -v enable ntp

ls /var/

cd system/contract/all
ls
…….

a retenir

sur les bsd :
sur les linux : histoires d''etats

ls /etc/rc0.d/

il peut avoir un idle par processeur.

ps -auxwk

…

ps -eaf
ps aux

ps -auxwH
-H : threads
le thread soi s'execute, soit ne s'execute pas.

codé threadé ou pas :

taille virtuelle , taille physique

[Cours 8 - 02/03/2016]

FileSystem, Reseaux, DNS
machine : un controlleur sas …

Sémantique de FileSysteme:
Pb de formatage de clé usb par exemple: on veut que ca fonctionne partout.
Tentative de Piratage port SSH

Vazy Momo sert a qq chose nan ? ecrit nan ?
Ah ouaiiiiiiss !!

Scsi : parallele : on n'en fait plutôt plus.
dernieres monture du sas 12 Go bit.

commande :**sysctl**

tout les commandes … du noyau.
On peut configurer des choses concernant le noyau.

Partioner un disk :
→ But : Securiser certaines partitions.

FreeBSD : par défaut une seule partition:

Si configuration Serveur : il ne faut pas les differents catalogues remplisses les disques.

par defaut OpenBSD :
	/usr/obj : objet

Partitionner → pour essayer de faire des choses un peu détaché.

Pb dual boot: redemarrer machine.
Virtualisation: mieux en gros, à

Filesystem : structure : System de gestion de fichiers.
partition :

on va partition sd0

commande : disklabel sd0

→ Nb d'octets par secteur
	octet : bytes de 8 bits.
→ Nb de secteurs par pistes
→ Nb de pistes par cylindre
→ temps accès fait partie de la géométrie

Régles tous systèmes Unix :
	→ la 1ére partition : c'est toujours la racine : /
	→ la 2 eme : c'est la zone de Swap
	→ la 3 eme : (s' appelle c ou 2) contient le disque entier.

Sous BSD : 16 partitions autorisé.
Linux : 8 partitions Max

16 partitions meme disque : Grandes pertes de performances de temps d'accès !
	→ à cause des positionnements des données.

disklabel sur Linux = Gparted

variable d'environnement EDITOR
	EDITOR = nano ou emacs
	exporter la variable d'environnement.

fsize : fragments size
bsize: blok size

on à le droit de mettre du swap sur plusieurs disques.

SWAP : sert a sauvegarder un processu par exemple
→ permet au système de minimiser les temps d'accès.

commande : newfs

ext3 et ext4 : sont journalisé et peuvent des volumes de 16 Téra …. que ne permert pas ext2.

commande mount
mount : prendre une arboresccence et la raccorcher a une arborescence de systéme.

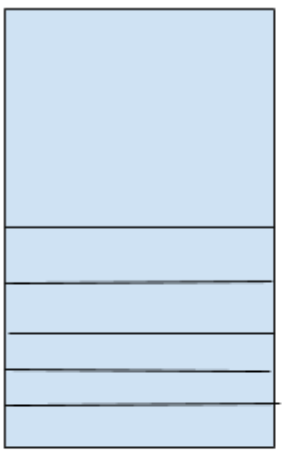
création et montage d'un filesysteme pose probleme :

montage: il faut que le kernel puissent comprendre le ntfs (windows) ou autres.
ntfs : syst très fragmentés : pb de fragmentation different de celui d'unix : oblige à modifier le noyau

FUSE : File Systeme User Space

→ permet d'acceder à des filesystemes sans modifier le noyau.
→ relativement intéressant, c'est lente : acceder ou ecrire des données de facons ponctuelle.
FileSystème de MacOS: HFS+ :" saloperie antique " - JMM - 2016

mode charactère : écriture direct sur disque.



-inode
-UID
-GID
-taille
-dates
(derniere modif)
-derniere consultation
- type catalogue : 'd'
→ permet lien fichier et lien d'inode
- type c : charctère
- type b : buferrise
- lien symbolique
→ fichier : contenu c'est le fichier sur lequel il pointe
- socket domain unix (commence par 's')
- tube nommé
- regular files
- mode (read, write …)

——— Adresse zone de données

---

commande :
find
netsat : commande à tout faire pour le réseaux

voir man stat : pour descriptions des types de fichier disponible.

fragmentation : on va continuer à garder des blocks de 16K, ie on creer un charactere: on nous allou 16 K

J'ai en marre sa race, c'est pas intéressant.
Hey mec, ça saoule.

rien à voir avec la fragmentation de windows.

Sticky Bit : permet de garder éventuellement en zone de swap

Pose pb de temporaire: /var/tmp droit 777 et donc qq dautres peut effacer sans quon puisse rien faire

→ sticky bit permet de supprimer ssi on est le proprietaire du fichier.

---

clri
commande clear inode: dispo que pour root : c'est mortifaire

cnri : d'un catalogue ; perte d'acces de tous les fichiers qui il y en dessous.

rm :
retire dans le catalogue :enlever la ligne
et supprimer le nombre de liens en dur , pour qu'il soit supprimé au faut 0 liens dessu et il faut aucun descripteur actif dessus: sinon les bloks de données continu a exister.

le nom de fichier : info dans le catalogue.

PAUSE

RSS : taille reel occupé sur la barette
SIZE : taille virtuelle

-- prog gonflette qui alloue un grand tableau

vitualisation permet de depasser la taille memoire

on peut pas faire un processus + gros que free mem
taille virtuelle 8go.
taille reel : 800k

commande : od pour faire des dump dans tous les formats.
od -c : pour avoir en characteres.

od -c c

catalogue ; fichier un numero d'inode et un fichier et taille de l'entrée.
taille du nom de fichier.

RSYNC, LFTP : commande pour copier

vazy ecrivez le cours nan ?!
ah ouais

NFS : utilise les RPC et les XDR

→ il y a primitive d'acces au catalgoue : READDIR

être incensible à la case : min et maj c'est pareil.

interet du swap: acces rapide : pas de structure

journalisation :

journal : partie du disk non structuré.

démon : update SYNC : syn

extended 3 est journalisé.

zfs list :
Problématique de FileSystème.

[Cours 9 - 10/03/2016]

LTO: En Gros pas de questions dessus à l'exam !

LTO 3 : Ultrium : Bande.
intéret
⇒ **Archivage !**
→ on peut mettre dans la poche lolilol
→ compression gérer au niveau du Lecteur.

LTO1 à LTO7.
entre chaque version : on multiplie la capacité * 2.

LTO3 = capacité 400Go.
LTO10 = 30 Téra en natif , 65-70 Tera en compressé.

LTO (n) capable de lire/écrire du LTO (n - 1)
LTO (n) capable de lire du LTO (n - 2)

"Les schtrofs " - JMM 2016 - Les stores

LTO6 - max 6 Téra par bande ~~ 9 000 €

Il y a des softs gratuits:
- [AMANDA
- BACULA (BackupDracula)]
- TAR

Sauvegarde incrémentale : niveau 0 puis ce qui à été modifié.

---
la personne esaie de scanner toute la plage d'adresses.
Elle est en train de scanner tous les ports.

1 / Scan
2/ tentative de crackage password.
→ avec des mots de pass par défauts , qu'on peut trouver sur l'internet.
→ puis des mots de pass pour des users cible.

Action A: il à réussi : retour positif.

Pirates
“et une bouteille de rhum … Oh Oh Oh …”

---

auth.log : connexion failled et réussi.

#On va causer de réseau
Ethernet en 1990.

Réseau Local :
Topologie : Bus : Pacquet passe dans les deux sens.
IBM : technologie jeton (token ring) → pas si bien → Le poste qui a le jeton peut emettre → l’anneau s’est ouvert.
LateCollision : collision retardé.

1er Bus : gros Coaxiale (ba parce qu’il est gros !)
→ nécessité de transmetteur.

petit ethernet : ethernet fin
→ 10 mbits , pb si on rajoute une machine: on doit couper le réseau.
10bases2 - 200m
10bases5

milieu 90 : Cable en cuivre
cablage cuivre.
structure de bus point to point, entre le point et l’equipements.

concentrateur HUB : envoi d’un porc puis repeté sur tous les porcs
concentrateur SWITCH
→ SNMP.
→ pas répeté sur tous les porcs.
→ port 48 gigas : 1500 €
per torsadé : vitèsse 10 gigabits

“Ah jpeux tout niquer là !” - JMM 10/03/2016 14h03
“UTP - Union des Travailleurs Portoricains - Ah Yaya ein gro β e rigolad !” - JMM 10/03/2016 14h08

Cat5 100m/bits
Cat5e 16 b/s
Cat6 1Gb
Cat6a = + rapide 10 Gbs

Cables

UTP : cable très souple
STP:-
FTP:--SFTP:---

Half duplex: on sait juste envoyer dans un sens
full duplex : envoyer et recevoir en mm temps

Fibre monomode
→ cable sous-marin

Fibre multimode
→ usage : grande distance.
→ - chere : peut rebondir sur les parois

Fibre métro : chemin de fer…

10 gbits : necessite Switch qui coute chere10 gbits : Chère.

IEEE 802.3 (802.3a, 802.3b, 802.3c, … Les lettres sont des additifs, la même chose pour le wifi 802.11a, b, c, ...)
→ ça concerne ethernet
802.1x
→ c’est ce qu’on utilise qu’on on se connect au wifi avec un mdp

TCP/IP (abus de langage): ARP/ICMP/IP/UDP/TCP/IGMP (mais c’est long, comme ma bip !)

PAUSE gros !

Tcpdump : interfaces en mode proximité : permet de voir tous les packets.
Commande: tcpdump icmp host 192.254…..

ICMP :

→ permet de gerer le flux;
→ ping est dans ICMP (envoie ECHO REQUEST, reçoit ECHO REPLY). Pong par contre ...

ARP : arp -a
→ machines sur le réseau physique
→ ne fait pas partie de la suite IP et à sa propre RFC

netstat : commande à tous faire
netstat -f = print routage table
→ donne les routes et statisqtiques.
→ resolution adresse logique et adresse matérielle.

IGMP
→ envoi de message à une machine qui gère un groupe
→ permet de s'associer à un groupe, se désassocier.
→ a n t i c o n s t i t u t i o n n e l l e m e n t
dans la jungle paisible jingle le lyon est mort est soir , et tarzan trankill s'endord le lion est mort ce soir

Adressage IPv4:
→ classe A, B, C, … n'existent plus
→ classe A étaient pour les grandes institutions, classe B pour les institutions moyennes, classe C pour les toute petites institutions (moins de 256 postes).
→ on commence à manquer d'adresse en IPv4 donc on a sorti l'IPv6
→ 192.254.199.0/24 : les 24 premiers sont pour le réseau, le reste (0) sont pour la machine.
→ Une adresse IPv6 est longue de 128 bits, soit 16 octets, contre 32 bits pour IPv4

L'Internet c'est grand ! Grillé qu'il a dit. adresse 10 …

Cidr …?

/24 : privilégié : on peut définir 255 machines .

Un alias : donner à une interface , une adresse IP.
nom de l'interface : donne le chipset utilisé.

more /etc/services : fichier ens des ports

ifconfig -a

notion de VLAN ? :
 → comme si on fesait un second (ethernet)réseau, (bus) , virtuelle.
→ mais physiquement ils utilisent le même réseau
→ lorem ipsum
→ de façon virtuel un réseau local

→ lorem ipsum

Peut être gérer au niveau du switch

show vlans porrs 32 de
VLAN) resua phizik

LACP :
→ plusieurs liens groupé ensembe (on reste o nivo 2 lethernet)
C'est quoi lorem ipsum ? c'est comme Git et svn
c'est du latin.du latin africain

Correction Examen 2015

moralité : Vlan et LLDP : à l'examen

Exo1

On se retrouve avec une adresse ipv6 routable
C'est ladress du routeur

Questions ipv6

On a une adresse ipv6 routabe

Adresse 78:19:f7 appartient au routeur qui a répondu.

Exo2
Surtout ce qui ne cest pas produit.
3 sollicitation : personnes qui répond.-> pas de routeur derriere
Pas d'adresse routble. -> czr pad de prefixe ipv6

MOmo veut pas ecrire.
Gaston " ya le telefon qui son et person qui repodn"

Ex3
On adresse qu'on a forcé, a cause des ::.
a causes des 2point 2 points.

.pas obtenue paR un routeur

exo4

l'interface vlan929
→ elle est sur le réseau des salles de tp : le reseau vlan929

car (192.168.70.97)

L'adresse IP correspond au reseau d'une salle de TP (192.168….)
Interface Vlan-iser car le nom commence par Vlan…

exo5

(hme0 est connecté sur le port 6 de l'interface v1)

ce port est associé a 2 VLANs
Un vlan tagé et pas l'autre.

Pourquoi c'est cohérent ?
⇒ Oui , cohérent.
→ VLAN 929 est une interface taggé.

→ on suppose l'interface hme0 pas taggé

taggé = interface associé au vlan.

sur une interface taggé : si on recoit des messages de tagg differents , on ne les traites pas.

port 581 : non tagged.

exo6

proc intel
architecture 64 bits (amd 64)
24 cpu
48 Go de RAM
mp = version multiprocesseur

Tagger : veut dire que l'interface est directement associée au vlan

Config : 48 Go de ram, 24 CPU, a quoi ça peut servir ?
→ Serveur de virtualisation, faire de l'apache, LAMP etc… Peut être des bases de données si on a de la memoire disque. Peut être du web (LAMP). Le probleme est qu'on a pas d'info sur la memoire disque.

Question 7

A priori c'est un serveur PHP/MYsql. Donc un serveur LAMP,
Correspond à la config ci dessus, si on rajoute du disque.

EXAM 2011

Exo 1
Cat : date de derniere access
Chmod: De de modif de linode
Ls-l >> totor : les 3 dates modifiés.

Momo veut pas écrire.
Safir veut pas écrire.
Casotoah
Le derniere acces couvre les 3 propositions
Mais pas vraiment de réponse

Ex2

Memconf dit quell processeur on a.

Utilisation :

- CPu pas tres rapide.
- Grossomodo faire du WEB ‘(php,)
- Pas de la vituraliasation car pas assez de RAMM
- Pas de SQL car pas assez de disque

EX3

Nivose est une spark 7, 64 bites , 20 go dique
Processeur de calcul en raison de sa fréquence 2,4 Ghz et 8coeurs.
Machine de calcul plutot malgré bcp de ram.

EX4
A priopi add de la ram , de facon a ce ke tous soit equivalent
En GROS 2 gb ram / Coeur CPU.
Il faut parité

Exo5

7 % de batteries les filles c’est tendax.
Pb : files etc/hots : pas de adreese ipv6 , il essai de faire la resolution il faudrait dans ect/host: mettre ladres ipv6
Sinon modifuer le fichier …

Exo6

. Ladresse ipv6 ne devrai pas etre celle la
Parce que passerelle de courier.

Exo 7
Il est en train d'ecouter en ipv6 ou ipv4
Il ecoute sur 53 udp, tcp, en ipv4 , ipv6,

A priori c'ese serveur de nom qui est entrain d'écouter

EXO8
Yaura pas car

Ex9
Pas les mm interfaces.
Nom bizare donc c la mm machine, visiblement ce sont des interfaces dusr 2 vlan differents.
La machine à un alias, avec 2 adresse et lautre une seule adresse

[Cours 10 - 16/03/2016]
examen

Adresse IPv6:
→ Fin novembre 1995 : 1ère RFC IPv6 `
→ problèmes avec IPv4:
→ nb d'adresse limité (plus que IPv6 en tout cas). IPv4 en 32 bits ça fait environ 4 milliards d'addresses.
→ IPV6 devait remplacer IPV4 assez rapidement, alors qu'en realité son utilisation est anecdotique
→ s'exprime en hexadecimal en non en décimal contrairement a IPV4

PDU electrique
→ prise connecté directement sur le reseau
→ a une adresse ipv6
→ contrôle sur le réseau (ex: éteindre une machine)

NAT est apparu : translation d'adresse IP.

NAT ←→ RFC 1918
= limiter le nb d'adresse possible : réduire.

IP et IPV6
→ protocole de meme famille
→ IPV6 : protocole différent : il faut investir dans le personnel formé à IPV4 : donc chère.

IPV6 :

- Pas de montage NFS.

Connexion d'abord en IPV6, puis en IPV4.

Commande df :
Affiche le catalogue des disques de montages.

Différence entre ipv4 et ipv6
→ IPV6 :128bits (4 * plus que IPV4)
→ IPV4: 32 bits/
→ ethernet : 48 bits
→ type d'adressage
→ uniscast / anycast / multicast
→ pas d'autoconfiguration en ipv4 (utilisation d'un protocole externe DHCP)

Anycast : envoyé a une série de **porcs(c'est pas halal tout ça)**, une seule qui recoit et répond à la requete et les autres ignore.

Adresse Lien-local :
Plan d'adressage aggrégé : adresse Routage.
Mtu : atm : max 64 octets.

On va configurer une interface en ipv6.

Icmp6 : protocole decouverte des voisins de niveau 3
Joue le role de ...

2001::onsaitpas::3301:8070:47/64
Année, bla, 33 indicatid, 01 paris,

Tcpdump -i hme1 icmp6

DAD : Duplication Adress Detection.
→ pour detecter/déterminier si on a une duplication d'adresse en demandant aux voisins leur adresses IP.

Sur une meme interface : 2 adresse IPV6.: 1 seule utilisé

J'ai pas compris le but de ce cours.

Sur la carte mère: ya le chipset ethernet : adresse IPv6 change.

"J'ai tout niqué !" - 16/03/16 14h10 - Terre
"J'ai fais counerie".
"Y'a plus qu'à voir et on voit tout"

Tcpdump
Ipv6 who has , adv*

Ndp : voisiin…

Ndp -an

Étude DNS.

DNS
→ resolution d'un nom en adresse

TTL : 1 journée

Les serveurs de noms doivent être déclarés.

FQDM

Reverse DNS
→ resolution par DNS mais à l'envers
DNS : serveur droit et inverse.

Nslookup
Dig : plus complexe.
On peut intéroger un autre serveur de nom.
Par priorité demande ipv6 en 1er.

Cat /etc/resolv.conf

SOA: Start Of Authority
→ defini le nom du serveur de nom, de la personne à contacter.
Pb de choérence des informations : lors de modification.
Port : 53 en udp et tcp.

Dig -x : resolution inverse
Dig -short -x ip
Hostname
Si pas . on concatene le domain pour le soa
On va interroger en priorité forwarders, et koralev
Bd.cache : les serveurs de la racine.