

Cours SAR

Chapitre 1 : Rappel et notions de base.

Architecture Client Serveur :

Architecture N-tiers VS Architecture Client Serveur :

Pour développer une application Web, on suit l'Architecture N-tiers.

Architecture N-tiers : on a **N-entités**

Application Web

Serveur Web

Serveur d'application

base de données

cette hiérarchie
(3 entités)

Pour les services Web, on suit l'architecture client serveur.

Standard de communication

Application

Application

Assurer la communication entre Client & Serveur \Rightarrow les protocoles

- de la couche application

- Pour interagir entre un web browser et un serveur Web

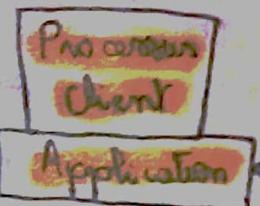
⇒ Requests HTTP
ou HTTPS

Serveur: C'est une machine configurée par une @IP fixe \rightarrow le serveur DNS va mettre en correspondance celle @IP avec un nom de domaine.
 \Rightarrow Configuration statique fixe.

Client: On utilise toujours une configuration dynamique.

Pour les services en générale, on se base sur l'architecture client serveur.

Résumé :

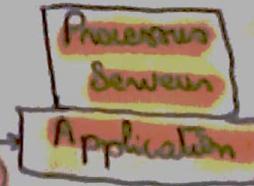


Architecture Client Serveur.

répose sur

Communication d'égal à égal.

réalisée par dialogue entre processus (2 à 2)



Les processus ne sont pas identiques \rightarrow forment un système coopératif (un échange de données).

Client	Service	Serveur
Initiation d'échange: Envoyer une requête de service au serveur.	C'est le traitement effectué par le serveur.	d' l'ordre d'une requête clienté éventuelle.
Réception du résultat final délivré par le serveur.		Envoyer une réponse à la requête de client Service demandé par le client

NB: Protocoles de la couche application : http (service web), SMTP (service de messagerie) ...

\Rightarrow Couche application permet d'accéder aux différents types de services.

Couches du modèle OSI & couches du modèle TCP / IP;

Modèle OSI

1 Application	Accès aux données
4 Présentation	Gestion de la syntaxe des données
5 Session	Contrôle du dialogue entre les applications
4 Transport	Qualité de transmission (de bout en bout)
3 Réseau	Sélection de chemin (routing) et cheminement logique
2 Liaison de données	Adressage physique (@MAC)
1 Physique	Transmission sur support physique

Modèle TCP/IP

4 Application	Application
3 Transport	TCP/Internet Protocol
2 Internet IP	
1 Accès réseau	Protocole d'accès au réseau
	Protocole physique

Modèle en 7 couches.

Comparaison du TCP/IP avec le modèle OSI :

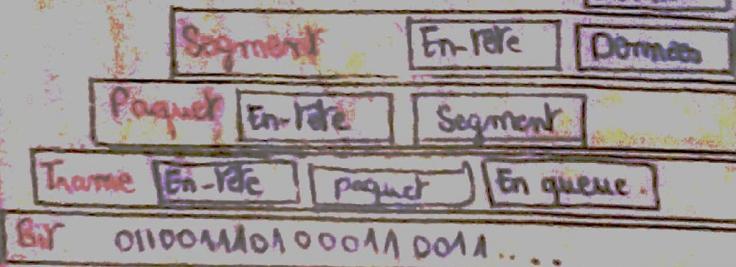
- Differences :
 - Modèle OSI → un modèle de référence
 - Pré protocole TCP/IP → plus couramment utilisé.
} ⇒ On va se concentrer donc sur le modèle TCP/IP.

- Points communs :
 - Modèle en couches
 - Couche application similaire mais avec des services différents.

des PDUs:

Application
Présentation
Session
Transport
Réseau
Liaison de données
Physique

Encapsulation



Données
Données
Données

Application
Présentation
Session
Transport
Réseau
Liaison de données
Physique

Machine 1

Décapacitation.

Machine 2.

- Envoyer des informations → Encapsulation → on descend de la couche application au niveau physique ⇒ Pour chaque protocole de la couche application, il utilise un protocole de la couche transport
 - Protocole UDP
 - Protocole TCP
} ⇒ Protocole de transmission

Il faut spécifier ici la méthode de transmission

Porte fixe
Porte rapide

Notions des ports

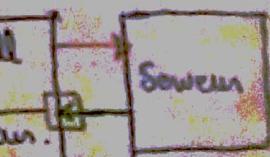
Requête (Ex: demande une page).

Réponse (Ex: Envoyer la page)

port en sortie → doit être ouvert

Identifiant du traffic

doit être ouvert



port en sortie doit être ouvert.

Port de sortie doit être ouvert

Le pare-feu (Firewall) → soit un traffic à autoriser, soit un traffic à bloquer.

Sur le niveau du gateway, on a configuré des règles de filtrages (ACL).

L'unité de communication est créée grâce à une socket (TCP + num port)

Port → num codes sur 16 bits

1^{re} plage : 0 - 1023 → ports connus
 2^{de} plage : 1024 - 49151 → ports enregistrés
 3^{de} plage : 49152 - 65535 → ports dynamiques réservés

Connexion TP 1 : Enregistrement SAR-WEB [29.30 - 54.00]

Récapitulatif sur les services de la couche applicative

langage de dialogue machine
moyens d'échange
d'information

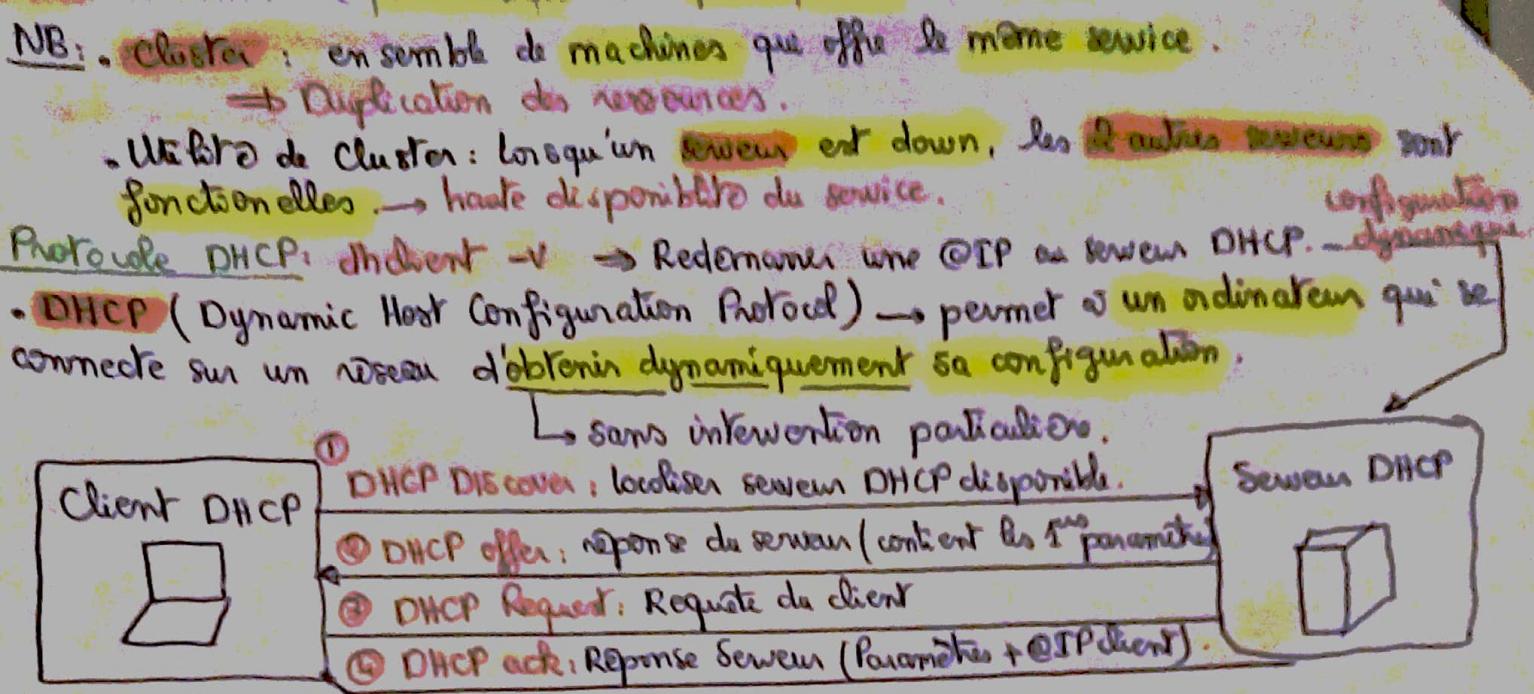
Permet de faire la différence entre
2 services utilisant la même IP.
utilisé côté serveur.

Couche Transport

Service	Protocole port	Clien	Serveur	Couche
Web	HTTP 80	Firefox, Opera, Chrome	Apache, IIS, Lighttpd	TCP
	HTTPS 443			
Transfer de fichiers	FTP 20 21 22	FileZilla, FlashFXP, CuteFTP	VSFTpd, Role PFTP, Filezilla server	TCP
	FTPS 99			UDP
Messagerie	SMTP 25	Outlook, Thunderbird	Postfix, dovecot	TCP
	POP 110	Evolution	Exchange, Lotus Domino	TCP
	IMAP 143			
Administration à distance	DNS 53	Resolver	BIND Role DNS	TCP et UDP
	SSH 22			
Configuration IP	Telnet 23	Cmd	telnetd	TCP
	OpenSSH 22	Shell linux, putty	openSSH	UDP et TCP
Vérification de signature	DAP 129	OS client	RoleDHCP dhcpd	UDP
Contrôle de sécurité	DAP 129	Messagerie, OS client	openDAP	TCP
Contrôle de sécurité	SNMP 161	Nagios, Cacti, Zabbix	Agent SNMP	UDP
	SNMP 162			
E-mail	IRC 194	ICchatIRC, Chatzilla	UnrealIRCd	TCP
Streaming	RTSP 554	VLC media player, MPlayer	Ampache, LIVESS3 Media server	UDP/TCP

RTSP : Real Time Streaming Protocol

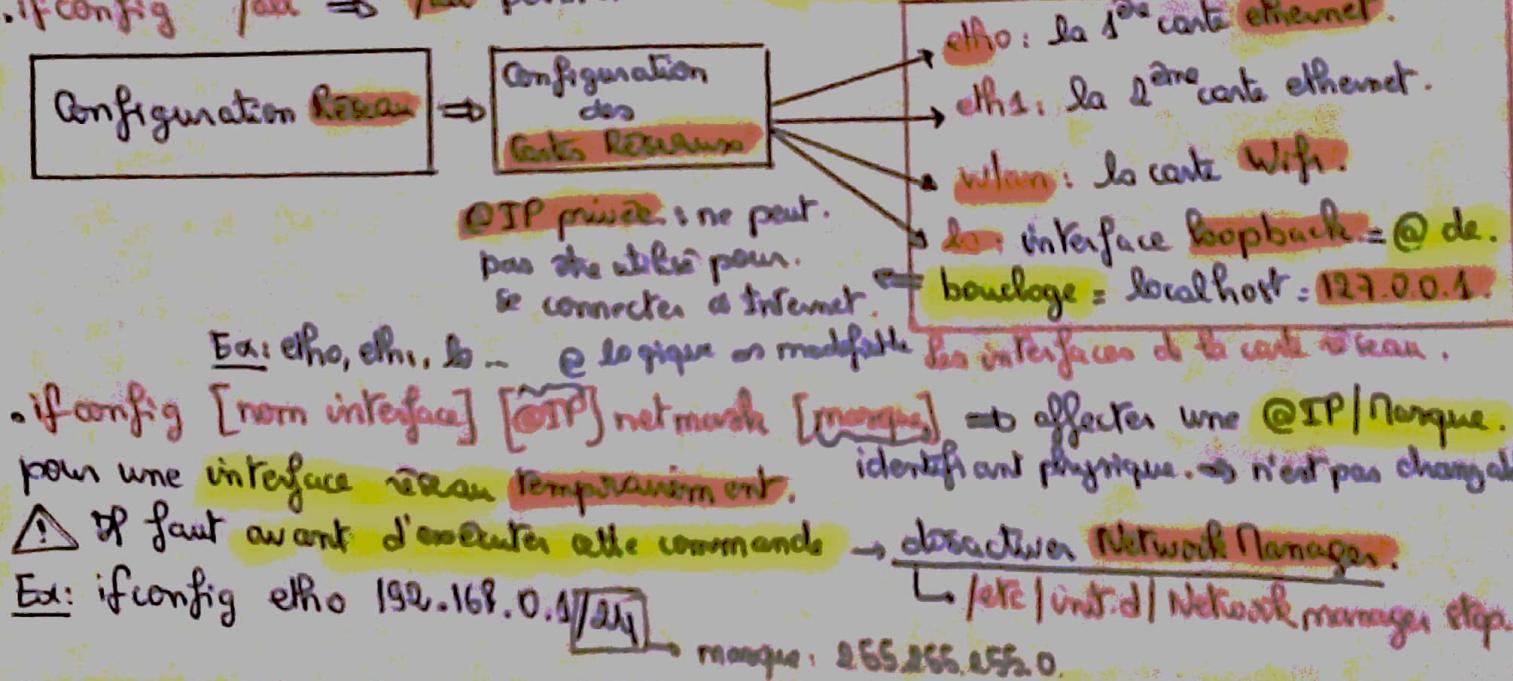
- Pour le protocole de utiliser dans la couche transport :
 - Si on a besoin de la fiabilité → TCP
 - Si on a besoin de la rapidité → UDP
- c/s : communication entre client et serveur. (Requête DNS)
- s/s : communication entre serveur et serveur. (Nécessaire entre 2 serveurs DNS).
- port → identifiant du traffic → chaque port fait un rapport spécifique.
(Ex: http → port 80 | FTP → port 21 | POP3 → port 110).



Ses commandes utiles:

ifconfig: La commande affiche l'état de vos cartes réseau ⇒ tracé la configuration réseau de la machine.

ifconfig /all ⇒ /all permet d'avoir toute la configuration.



ifconfig [nom interface] [@IP] netmask [masque] ⇒ affecter une @IP / Masque pour une interface réseau temporairement. identifiant physique. ⇒ n'est pas changeable

⚠ Il faut avant d'exécuter cette commande → désactiver Network Manager.

Ex: ifconfig eth0 192.168.0.1/24 masque: 255.255.255.0 ↗ /etc/init.d/NetworkManager stop.

Création d'interface alias: Pour chaque interface réseau → créer des alias (logique).

¶ Pour une même réseau → on peut lui affecter 254@IP +.

ifconfig [nom interface] [num alias] [@IP] netmask [masque]

Ex: ifconfig eth0:1 192.168.1.1 netmask 255.255.255.0
 ifconfig eth0:2 192.168.2.1 netmask 255.255.255.0 } eth0 192.168.1.1
 192.168.2.1

Activation carte réseau: ifconfig [nom interface] up / ifup [nom interface].

Désactivation carte réseau: ifconfig [nom interface] down / ifdown [nom interface].

ping: Rôle: . vérifier l'existence de machine sur le réseau.
 . détecter problèmes configuration IP.

[@IP] → Ex: ping localhost
 ping 192.168.24.3

! Envoi seulement 5 requêtes:
 ping [@IP] -t 5

! Augmenter taille paquet de 128 K:
 ping -s 128 [@IP]

nouveau: Affecter @IP passerelle (Gateway) → une interface
 - route add default gw [IP de la passerelle]

! Afficher table de routage:
 route -n

Syntaxe générale:

route [-n]
 route add [-host] [-net] [<@IP destination>] netmask [masque]
 (del) gw [passerelle] [metric N] → optionnelle

Ex: route add -net 192.168.1.0 netmask 255.255.255.0 gw 10.0.8.1.

traceroute: permet d'identifier à quel niveau on a une panne.

Voir les routes intermédiaires.

traceroute [panneau du problème]

⚠ l'option -n du traceroute → demande l'affichage de l'@IP du serveur.

Fichier de configuration des paramètres réseau

- S'assurer de la configuration réseau → Sauvegarder et éditer le fichier de configuration.

l'interface réseau: /etc/sysconfig/network-scripts/ifcfg-[nom interface]

- Pour la passerelle : /etc | sysconfig | network
 - { GATEWAY = @IP passerelle }.

Configuration nom machine

nom machine est utile

pour tag interface

configuration DNS

serveur messagerie

host name → afficher nom de la machine.

fichier /etc | hostnames → changer nom de la machine.

Configuration adresses DNS

- Configurer @IP DNS : fichier /etc | resolv.conf

- Syntaxe fichier : nom serveur 193.95.66.11.

nom serveur 8.8.8.8 } liste de serveurs de noms.

@IP DNS Google

⚠️ Serveur DHCP → serveur qui permet d'avoir une configuration dynamique.

Serveur DNS : serveur d'attribution de la configuration dynamique

← Pour avoir cette configuration

@serveur → Pour contacter ce serveur => il faut avoir @IP de ce serveur.

@IP DNS → nslookup [@IP DNS] ⇒ Client DNS : Résolveur.

/etc | resolv.conf : fichier /etc | resolv.conf → indiquer comment doit se faire @solution la ligne hosts

se connecter à Internet

bouclage = localhost = 127.0.0.1.

DEVICE = nom interface réseau

BOOTPROTO = dhcp | static

ONBOOT = Yes | No

IPADDR = @Ip

NETMASK = masque SR

NETWORK =

Adress interface réseau

Ed. hosts, fileo dns njs.

① fichier locaux (pm | etc | hosts)

② serveur dns :

③ serveur njs.

Cours SAR:

Chapitre 2: Services Web

Introduction:

- Service Web → Service le plus banique et le plus répandu Simple
rapide lors de l'exécution
- On va utiliser Apache comme serveur web.

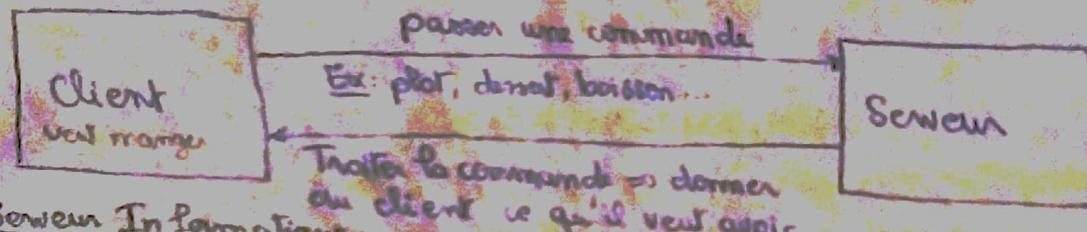
↳ Installer Apache : `yum install httpd`.

Architecture du service Web:

L'architecture du service Web se base sur Architecture Client Serveur.

Architecture Client Serveur:

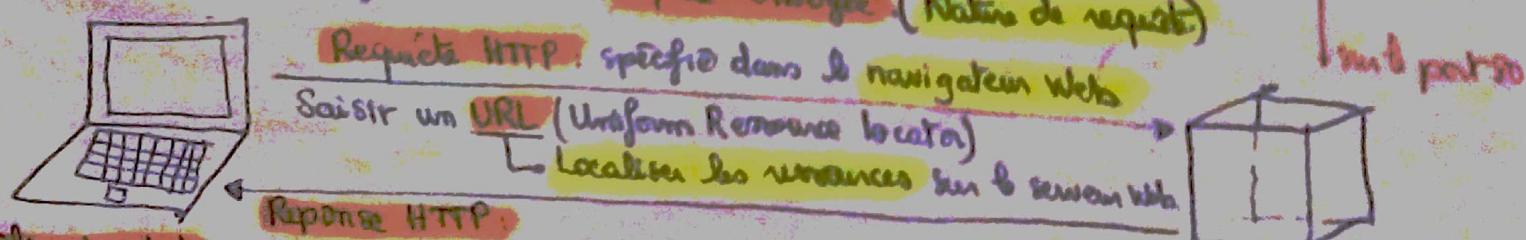
Serveur hardware
physiquement une machine équipée de ressources physiques (RAM, Processeur)
avec une carte réseau (interface eth0) pour avoir une @IP Fixe / unespondance va logiquement : partie logiciel = une application qui nous permet d'avoir un standard dans l'environnement
Rôle: Exemple de Restaurant. software service bien déterminé :



Serveur Informatico:

Un serveur informatique → joue le même rôle → va fournir des services aux autres (Ex: service de navigation sur des pages web, service de messagerie électronique, une BD qui stock des informations, serveur d'application ...)

- Le serveur est toujours en écoute et son rôle est d'offrir un service.
- Service dépend toujours de la requête envoyée (Nature de requête)



Client Web → Application : Web Browser.
atteindre le serveur => (Navigation).

→ on utilise toujours des @IP fixes.
des numéros fixes

Serveur Web

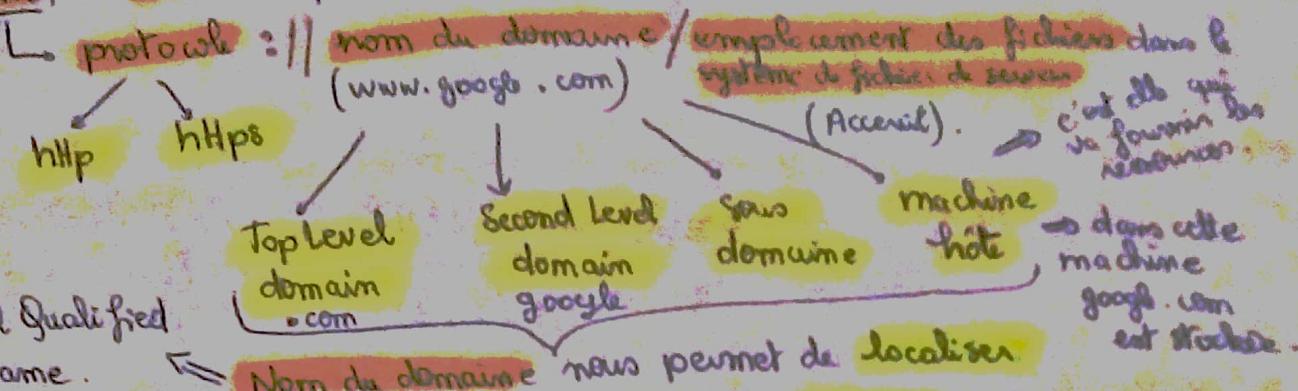
Stocker un ensemble de ressources (Image, front-end, back-end...)

Protocoles HTTP / HTTPS

protocole HTTP → standard de communication : permet d'avoir une communication entre le navigateur Web et le serveur Web.

- Pour les requêtes, HTTP, le serveur est en écoute sur le port 80.
- HTTPS (HyperText Transfer Protocol) : Protocole de transmission sécurisé.

Dans l'URL, le client va préférer le nom du domaine (google.com).



FQDN : Full Qualified

Domain Name.

Nom du domaine nous permet de localiser les ressources au niveau du serveur.

On peut rajouter un numéro de port à notre URL:

protocol : // nom du domaine : num port / emplacement des fichiers.

Ex: https://www.facebook.com:443/mail.R.ajmi.9.

443

protocol http → utilisé par 80

· port 8080 → Virtualisation par port.

protocol https → utilisé par 443

· port 8000 → Interface de l'administration

proxy → un outil qui va être en éveil avant le serveur web.

· intercepte la communication entre client et serveur.

· se trouve dans le côté client ⇒ écouter le traffic avant de passer le traffic au serveur web. (port)

Le client va avoir le proxy avant d'avoir le contenu du site web.

· Le proxy est utilisé pour filtrer des truffes

{ pour changer le @IP → côté client.

Ex: pour un site qui filtre les adresses (@ n'a pas d'accès).

Le client va avoir le msg ⇒ service non disponible dans votre pays) ⇒ une solution de filtrage (firewall) et il est en train d'appliquer des rules de filtrages.

Ex: les utilisateurs ayant un @ qui commence par 41 n'ont pas accès à ce site.

⇒ l'importance des proxy pour la falsification des @ ou on utilise les VPN.

Types de Requêtes: par de

de demande.

- GET → permet de récupérer des ressources, échanger des informations du serveur.
- HEAD → demande des informations concernant la ressource.
- POST → envoie de données (formulaire vers le serveur) et demande la ressource.
- PUT → changer des données au niveau serveur (UPLOAD).
 - enregistrement du corps de la requête de l'URL indiquée
- DELETE → suppression de la ressource désignée par l'URL, après le serveur.

Types de Réponses:

- La réponse sera en relation avec la méthode demandée \Rightarrow en somme de contenu.
- Au niveau du réponse, il y a un code envoyé de 3 chiffres.
Le permet de vérifier l'état de la réponse.
- 1xx \rightarrow Information 2xx \rightarrow Succès 3xx \rightarrow Redirection
- 4xx \rightarrow Erreur côté client Web (Ex: 404 Not Found). 5xx \rightarrow Erreur côté serveur.

Ex: Avant la révolution, lorsqu'on veut accéder au YouTube \rightarrow on aura 404 Not Found
 \Rightarrow le problème ici n'est pas relatif au serveur YouTube mais c'est relatif au client (le problème est au niveau Gateway (Interface de sortie) \Rightarrow gérée par l'ATI.
 ↳ Ex: Routeur.

- La réponse 4xx \Rightarrow problème de sécurité, d'authentification.

Exemple problème côté serveur 5xx: S'affiche lors de l'accès au site d'Esprit pour la délibération des notes. \Rightarrow Internal Error: problème côté serveur.

\Rightarrow Ex: le service Web d'Esprit gère 1000 session / seconde, s'il reçoit en même temps 5000 session (5000 étudiants veulent se connecter) \Rightarrow Service va atteindre les ressources maximales \Rightarrow Saturation \Rightarrow Service Down.

- 5xx: Problème de disponibilité du service,
 - Service en saturation
 - Service en cours de configuration / migration

- 3xx: Redirection \Rightarrow ma requête en tant que client va être gérée par un autre serveur.

Tехниque Virtual Host:

- Généralement, chaque serveur ne peut héberger qu'un seul site Web.
- Virtual Host \rightarrow permet d'héberger plusieurs sites Web sur un ^{même} solution Apache.

Ex: Serveur Esprit \rightarrow esprit.tn (au public) + pfe.esprit.tn (étudiants en PFE).

Méthode de Virtualisation:

Il existe 3 méthodes:

✓ Virtualisation par Nom: Héberger plusieurs sites avec des noms différents, mais en utilisant la même machine physique et la même @IP.

Ex: On va créer un Virtual Host qui s'appelle Site A, la machine est en écoutant sur la port 80 et on va créer au niveau du fichier httpd.conf (fichier de configuration du serveur web), un autre virtual host b.com qui pointe sur la même @IP de la machine et sur la même num de port.

⚠ Il faut avoir des ressources qui supporte les requêtes de 2 sites.

✓ Virtualisation par IP: Chaque site est hébergé sur une interface
Sur nos machines → une seul carte réseau → une seule carte Ethernet (carte eth0) → 2 interfaces

▷ Interface loopback loopback ne peut pas être utilisée pour héberger des sites

- On va utiliser la virtualisation des interfaces (création des alias) → nous permet de créer des cartes réseau de façon virtuelle.
- On peut créer jusqu'à 254 @IP virtuelle sur la même carte eth0
- Deux méthodes de configuration → on peut configurer eth0:1
 - nom de l'alias

Créer un fichier de configuration

soit /etc/systemd/network script

↳ créer un fichier ifcfg eth0:1

- ✓ Suite à la création de ce fichier, on garde cette configuration de façon statique permanente.

Une carte virtuelle sur la carte eth0.

X lors de redémarrage, on perd le seuil.

⇒ Nous d'alias pouvons créer pour chaque site, on va utiliser une @IP différente.

Ex: eth0 → site A | eth0:0 → site B | eth0:1 → site C

soit en donnant le port 80, et distinguer et pointer des @IP.

✓ Virtualisation par port: En utilisant la même machine, la même @IP, le même serveur web, je vais héberger plusieurs sites tous sous num de port différents.

→ On va changer les numéros de port, on général on utilise le port 80.

⇒ au niveau de fichier de configuration: listen 80

mon serveur est l'ip en deux num.
le port 80.

→ lorsque on veut créer un autre site, il va utiliser le port 8080. → ajouter dans le fichier de configuration: listen 8080.

⚠ Le choix de num de port ne s'effectue pas d'une manière aléatoire.

- 3 plages:
 - ✓ Ports utilisés côté serveur: 0 → 1024.

Ex: On ne peut pas associer le port 53 pour un site Web.

consultation
TP web

- ✓ Ports utilisés côté client:
 - 1025 → 49 000 (Ports enregistrés)
 - Administrateur port choice

Cours N°8

Chapitre 3 : Service de messagerie.

Introduction au service de messagerie.

Service de messagerie

- Service de messagerie le plus répandu par la simplicité d'exploitation
- bâti sur une architecture, différents agents (NUA, NDA, NTA) et des protocoles.
- permet d'envoyer un msg ou consulter une boîte à lettre grâce à une application installée sur client.

Architecture du système de messagerie.

Présentation de l'architecture :



- Service de messagerie est basé sur l'architecture Client-Serveur.
- Serveur → traite plusieurs requêtes de plusieurs clients

Pour envoyer un msg :

- une machine sur ISP
- savoir l'adresse de messagerie de récepteur (xx@xx.com)
- ID de service de messagerie

Terminologie :

NUA (Not User Agent)
navigateur ou application de messagerie (Outlook).

Client de messagerie

adresse de messagerie
(Ex : malak@frstf.fr)

nom destinataire destinataires nom du domaine
détails des champs dans domaine

récepteur de messagerie.

NB : on a pu écrire nom du domaine (ex : fr)

Le un serveur de messagerie (@frstf.fr)

Itinéraire d'un message électronique :

1) Lancer l'application de messagerie (NUA : Not User Agent)

2) Composer : email de récepteur, objet, corps du msg.

3) Envoyer msg → le client va émettre l'mission du msg.

4) Application de messagerie (NUA) va contacter le serveur de messagerie responsable de notre domaine grâce au protocole SMTP.

NB : Rôle SMTP : Envoyer des emails.

5) NTA va vérifier la validité de l'adresse msg de destination :

SMTP : Simple Mail Transfer Protocol

POP3 : Post Office Protocol

IMAP : Internet Message Access Protocol

1) équipement

2) fonctionnalité

Envoyé de mail

Reception de mail

serveur de messagerie.

un agent

charge l'équipement

agent responsable

de l'envoi

NTA (Not Transfer Agent)

agent responsable

de réception

NDA (Not Deliver Agent)

un logiciel pour

serveur de messagerie

agent

logiciel de

distribution de messages électroniques.

Prot : 25

SMTP

?

Procédure

Client

- Si adresse mail non valide (champ enroulé) : utilisateur inexistant, pas de @, domaine inexistant) → Notifier l'utilisateur (via un mail de notification).
- Si adresse mail valide → vérifier si le destinataire fait partie de ses clients :
 - (lie @mail destinataire et comparer domaine du destinataire)
 - Fait partie de ses clients → placer le mail dans la boîte de lettre du destinataire

NB: • un serveur de messagerie peut gérer seulement les utilisateurs de même domaine
 ⇒ 1 nom de domaine → 1 serveur de messagerie. Le récepteur va utiliser son NDA pour vérifier s'il y a des nouveaux mails.
 • NDA → serveur de stockage (BD). L'espace mémoire pour chaque utilisateur est domaine.

→ placer l'avis dans NDA → protocole SMTP.
 ⇒ SMTP a fini son rôle
 NDA va contacter NVA grâce protocole de réception POP3 / IMAP → vérifier s'il y a des nouveaux mails (vérifier les e-mails stockés dans l'espace mémoire de l'utilisateur) → envoyer msg à l'application NVA.

→ ne fait pas partie de ses clients → destinataire a un nom du domaine différent (Edu émetteur (expt.tn), récepteur (yahoc.fr)) :

- Envoyer le mail vers le NTA responsable du domaine de destinataire (acheminement du mail vers le nom du domaine du récepteur) → protocole SMTP.
- NTA va vérifier la validité et si l'utilisateur fait partie de la liste des utilisateurs du domaine ⇒ Si fait partie → placer l'avis dans la boîte de lettre de l'utilisateur en utilisant le protocole SMTP et l'utilisateur va consulter boîte de lettre → protocole POP3 / IMAP.

Protocoles de messagerie :

Protocole d'envoi de messages:

SMTP → toujours en écoute sur le port 25, au niveau de la couche transport → protocole TCP (fiabilité).

Rôle : Transférer les mails vers les serveurs de messageries afin que les utilisateurs puissent consulter leurs mails.

Protocoles de réception de message:

- En tant que client récepteur de msg, je peux choisir entre POP3 et IMAP.

POP3 : Post Office Protocol.
 Port : 110

IMAP : Internet Message Access Protocol.
 Port : 113

Utilisation	utilisé seulement avec les applications de messagerie.	utilisé avec navigateur et configuré automatiquement avec tous les applications de messagerie.
Connexion	lien Connexion	Une connexion constante au serveur de messagerie.
Stockage	<ul style="list-style-type: none"> Supprimer les msg de boîte de messagerie → <u>Télécharger boîte de messagerie (NDA)</u> → sur la machine physique Utilisation minimale des ressources du serveur. 	<ul style="list-style-type: none"> Créer des copies des msg stockées dans la NDA → <u>Renvoyer les copies</u>. L'application de messagerie. → Stocker les courriels dans le serveur. Gérer l'espace disque de serveur.
Accès	Gérer : {un seul accès unique à une boîte (une seule boîte de lettres)}	Gérer : {plusieurs accès simultanés plusieurs boîtes aux lettres}
Gestion	<ul style="list-style-type: none"> Permet une gestion des msg en local après téléchargement → Recherche et tri plus rapide. 	Permet une gestion simplifiée de la messagerie en cas de mobilité de l'utilisateur.

choix du protocole dépend de la situation et de l'utilisation.

NB: C'est vrai que l'IMAP nous permet de consulter nos mails n'importe où (PC, smartphone, autre PC...) mais il stocke les mails dans le NRA et quand NRA sera rempli, il va supprimer des mails aléatoirement.

- des serveurs de stockage → plus vulnérable que les clients

→ possèdent des failles de sécurité : @IP statique → l'attaquant peut identifier la machine.
⇒ Préférance de confidentialité de données (ne pas échanger des informations via Mail).
(mdp, emplacement...)

des différents applications de messagerie:

Il existe deux façons d'envoyer et de recevoir des mails:

- de Web Mail (Navigateur) : navigateur est un client de service web → protocole HTTP

⇒ on n'est pas en train d'utiliser l'architecture de messagerie

⇒ de service web va jouer le rôle d'un client de messagerie → Service Web Mail.

- Le client de messagerie (Outlook, Thunderbird...) : protocole SMTP, POP3, IMAP.

des différents clients de messagerie:

	Web Mail	IMAP	Client de messagerie	POP3
Avantages	<ul style="list-style-type: none">+ Consultation des mails depuis n'importe quel équipement connecté à Internet.+ Configuration simple : définir l'adresse mail.		<ul style="list-style-type: none">+ L'envoi et la réception sont instantanés : sans passer par un serveur web.+ plus de rapidité.	
Inconvénients	<ul style="list-style-type: none">- Nécessite une connexion permanente pour consulter boîte de messagerie.- Limiter les capacités de stockage		<ul style="list-style-type: none">- Installation et configuration de logiciel de messagerie (clients lourds).- Consultation assurée depuis seul machine	

TP: Création d'un serveur de messagerie:

1) Installation des outils : yum install postfix, yum install dovecot, yum install Thunderbird, yum install telnet (telnet : protocole → accès à distance à la machine (comme ssh) → accéder au serveur à distance) → Configuration dynamique.

2) Crédit des utilisateurs : # useradd -m user1 # passwd user1.
Pour tester ⇒ Chaque utilisateur a son @mail → Echange des mails entre utilisateurs

3) Configuration d'iptables : c'est le firewall du cent OS

gedit /etc/sysconfig/iptables

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT  
-A INPUT -m state --state NEW -m tcp -p tcp --dport 110 -j ACCEPT  
-A INPUT -m state --state NEW -m tcp -p tcp --dport 143 -j ACCEPT
```

3 règles qui autorisent l'accès sur le port 25 (SMTP), 110 (POP3), 143 (IMAP).

• Redémarrer service iptables : Service iptables restart.

4) Configuration Postfix: # gedit /etc/postfix/main.cf

• Définir le hostnam du serveur : myhostname = (ex: espirit.com)

• Définir le domaine : mydomain = (ex: espirit.com)

• Changer inet-interface (les interfaces réseau sur lesquelles Postfix peut recevoir du courrier) : inet_interfaces = all

• Définir les @ réseau IP (@Réseau de votre interface) → plage d'autorisation (Postfix (serveur de messagerie) exécute les requêtes des clients de cette plage d'@):

Exemple works = (exp 192.168.1.0/24, 129.0.0.0/8)

5) Rédemander les services Postfix : # service postfix restart.
chfeconfig postfix on (lancer Postfix en tant que serveur).

6) Tester Postfix en utilisant telnet:

Vérifier si le MTA est fonctionnel ou non → connecter au serveur MTA avec telnet
Via SMTP : #telnet localhost smtp. (langage compréhensible par le serveur) :

- echo local host : hello from localhost (je suis connecté depuis la machine local).
- mail from : <user1@esprit.com>
- rcpt to : <user1@esprit.com>
- data [corps du mail] → écrire data → tapez entrée → écrire corps.

NB: Il faut ajouter . au corps pour indiquer fin de message

- quit → pour quitter.

Vérifier si l'email est bien envoyé ou non :

• Vérifier si l'email est bien envoyé ou non :
Naviguer vers le dossier Maildir qui se trouve dans le répertoire personnelle de

User1 : # cd \$home/user1

Maildir | new

contient

des nouveaux mails reçus

les messages.

de messagerie

• Lister les messages : # ls → on va trouver fichier de msg.

• lire le message : # cat [nom du fichier du msg].

data manifbe.
•

NB: cat permet d'afficher le message dans le terminal.

Received from: localhost \Rightarrow on a envoyé depuis le serveur local.

domaine

7) Configuration de l'NDA (Dovecot):

- Ouvrir fichier de configuration : #gedit /etc/dovecot/dovecot.conf
- Enlever commentaire sur : protocols = imap pop3 lmtp.
- Ouvrir fichier de configuration : #gedit /etc/dovecot/conf.d/10-mail.conf.
- Enlever commentaire sur : mail_location = maildir:~/Maildir
- Ouvrir fichier configuration d'authentification : #gedit /etc/dovecot/conf.d/10-auth.conf.
- disable-plain-text-auth = no : authentification est basée sur l'NDA. (enlever commentaire)
- Précesser le mécanisme d'authentification : auth-mechanisms = plain login
des mots non chiffrés.
- #gedit /etc/dovecot/conf.d/10-mail.conf.

```
unix_listener auth-unsafe {  
    user = postfix  
    group = postfix}
```

- Redémarrer service dovecot : #service dovecot restart
#dkiconfig dovecot on

8) Tester dovecot en utilisant telnet : # telnet localhost pop3.

- Authentification : user user1 pass user1
- Lister les messages : list \Rightarrow on trouve 1 msg \Rightarrow synchronisation entre NTA et NDA
- Voir le premier message : retr1 \Rightarrow on trouve n msg.
- quit \Rightarrow quitter.

Chapitre 3 : La résolution de nom

10.10.10

Introduction

- PC Exchange : Service de messagerie Windows (MTA + MDaemon)
- DNS : Domain Name System → permet de faire la correspondance entre les @IP et les noms de domaines → une entrée qui contient pour chaque nom du domaine un @IP correspondant.

Pourquoi utiliser un nom de domaine ?

- la plupart des utilisateurs préfèrent un nom convivial (Ex: expert.tn) au lieu de l'utilisation d'un @IP qui accorde à un administrateur ↗ service de messagerie ↗ service web.

Résolution de nom: Résolveur : client DNS → middleware → Configuration : file hosts.confRésolution locale: Résolution comme sur la machine locale → Utilisation du fichier de résolution locale (hosts.txt) : modifier les correspondances déliquemment et manuellement.
→ Toute modification dans ce fichier doit être fait sur toutes les machines.Résolution à travers un serveur DNS: Si la résolution ne se trouve pas en local (file hosts), le résolveur va contacter le serveur DNS autoritaire pour la zone (bulletin RNSL).Présentation

NB: le DNS du serveur de google est 8.8.8.8

- . Quelques mots à propos DNS velozi, chaque site web a son @IP qui est statique (Ex: ns1)
- le serveur authoritative (DNS de machine) est un serveur cache qui contient d'autre serveur DNS (Ex 8.8.8.8 de google) pour avoir l'@IP.

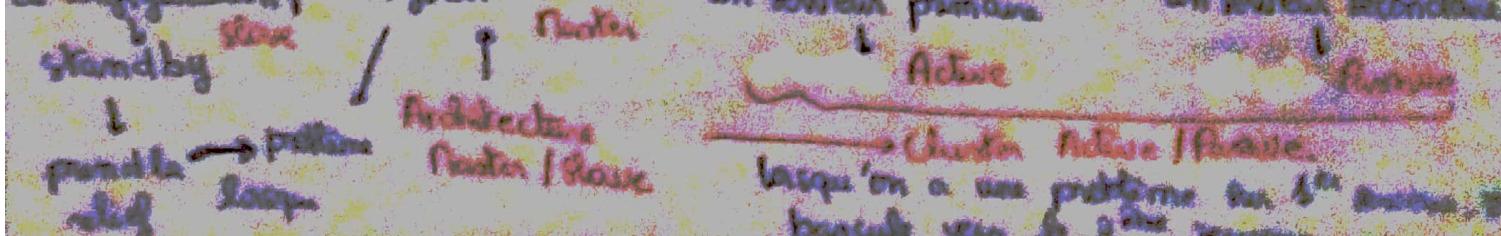
- . La résolution à travers le processus de résolution de nom en utilisant le protocole DNS (Domain Name System = Système des noms de domaines) → un système multi-chargeur qui établit correspondance entre nom de domaine et @IP.
 - travail sur des couches application (part. 53)
 - utilise sur la couche transport le protocole UDP et TCP

- DNS offre deux types de résolutions :

Résolution directe: renvoie une @IP à partir d'un nom de domaine (Ex: www.expert.tn → 192.168.1.100)Résolution inverse: renvoie un nom de domaine à partir d'une @IP (Ex 192.168.1.100 → www.expert.tn)Les DNS n'ont pas biseau:

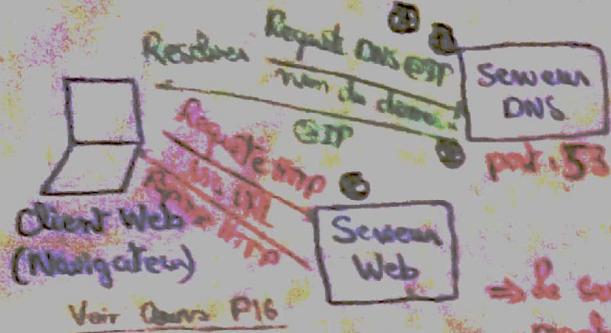
NB: même les applications de messageries sont entourées d'un biseau service DNS afin de trouver @IP du serveur de messagerie (Ex: mail.expert.tn → 192.168.1.100)

- . Un service DNS nécessite la haute disponibilité (service fourni par deux machines)
- Service DNS doit être implementé sur un ensemble de machines



Quand il y a un problème sur l'un des serveurs, on bascule vers le deuxième.

- Une révolution de nom / savoir qui connait la toute disponibilité (répartition) et consommation de ressources
- La réponse de requête de résolution de noms (Resolveur) → @IP du serveur primaire
- NB: on peut aussi utiliser les chaines Active | Active
- ⇒ Assurer l'équilibre → Rôle des deux machines (temps de réponse)
- Architecture du serveur DNS:
- Service de résolution de noms → basé sur l'architecture Client-Serveur → comme tout autre service



• Navigateur va contacter Resolveur pour trouver la correspondance entre nom du domaine et @IP.

• Resolveur va contacter serveur DNS → @IP du serveur DNS stocké dans un fichier /etc/hosts

⇒ Le serveur DNS permet au navigateur d'identifier la machine qui héberge un site via son @IP.

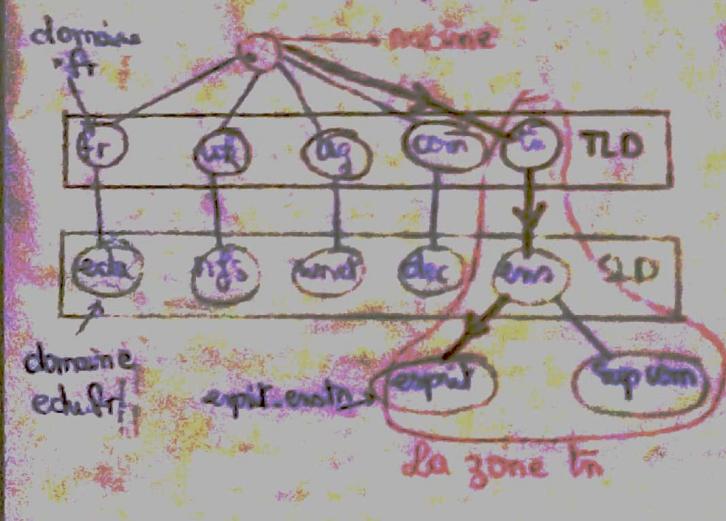
l'infrastructure DNS

Définition: DNS (Domain Name System) assure un système de résolution

FQDN: Full Qualified Domain Name

FQDN: • Lecture URL → est en tant que utilisateur: gauche → droite (Ex: www.ezpi.ezpi.it) système

localise la machine qui héberge et → pour faire la résolution



Racine: un point de départ pour la résolution DNS, ajouté par le système DNS à l'URL (à la fin) de façon automatique.

→ FQDN = nom du domaine + Racine

nom complet utilisé pour trouver la résolution NB: Dans un système hiérarchique, on commence toujours par un point de départ.

• niveau → définit un domaine.
niveau → suite de noms séparés par des points.
• 12 caractères
• correspond à une ressource (peut être vide).

TLD (Top Level Domain): des niveaux primaires / supérieurs → organisés au niveau géographique et/ou thématiques

→ TLD National: .tn (Tunisie), .fr (France), .uk (UK)

→ TLD Thématique: .com (géré par une entreprise)

• .org (géré par une organisation).

NB: On assure la communication entre les TLD à travers la racine :

Ex: .tn → racine → .fr (Enseignement, info, news, ...)

Le point commun entre les TLD

SLD (Second Level Domain): domaine du deuxième niveau → un sous-domaine du TLD (Ex: .edu - domaine de .fr) → .ens (enseignement → regroupe les universités de la tunisie)

ezpi: un sous-domaine du domaine .ezpi (des entreprises)

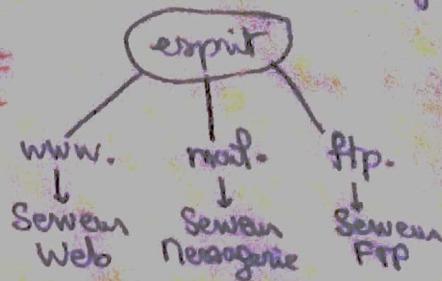
NB: • Chaque entreprise a des machines (machine hébergeant serveur web, machine hébergeant serveur de messagerie →)

⇒ Pour faire la résolution DNS, suiv une résolution hiérarchique (racine → TLD → SLD → sous-domaine → hôte qui héberge le site www.)

NB: • Dans le monde, on a seulement 13 racines (serveurs).

• Deux nœuds frères, ne peuvent pas avoir le m^{ême} nom.

(on peut pas avoir deux sous-domaine esprit ou .fr ...)

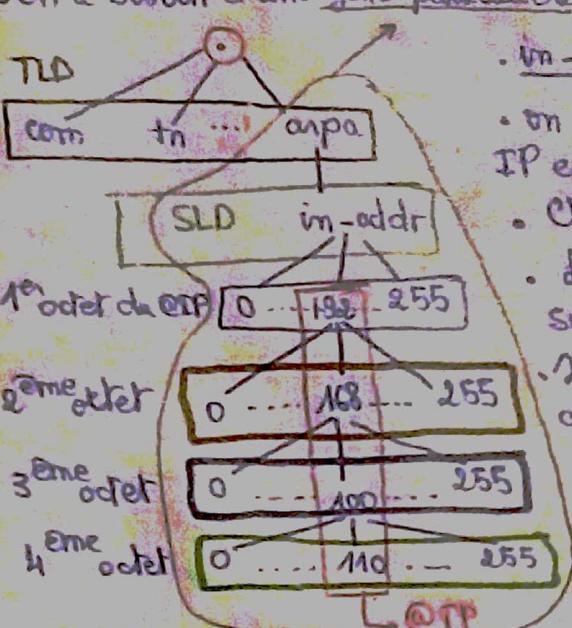


Zone: organisation logique (administrative) des domaines (Ex: ATI : Agence Tunisienne d'Internet)
Rôle: simplifier l'administration des domaines (dépassement de domaine en plusieurs zones)

de la résolution inverse:

Principe: Le processus doit fournir, pour une @IP, le nom correspondant : L'utilisateur va entrer l'@IP et le serveur DNS retourne le nom du domaine.

Fonctionnement:

- On a besoin d'une zone particulière, [in-addr.arpa], qui permet la résolution inverse d'@IP.
 - in-addr : input-address → c'est quoi l'@IP dans l'input?
 - on commence la résolution du 1^{er} octet au 4^{eme} octet (l'IP est codé sur 4 octets)
 - Chaque octet varie entre 0 et 255.
 - Le serveur DNS pointe sur les 4 octets d'un niveau au suivant : 1^{er} octet → 2^{ème} octet → 3^{ème} octet → 4^{ème} octet.
 - Jusqu'à arriver au 4^{ème} octet → la machine / l'hôte qui héberge le site.

relookup 192.168.100.110 → www.esprit.tn

- Au niveau système DNS
 - TLD: Résolution directe
 - Zone particulière (arpa): Résolution inverse

Le Resolver/Serveur:

- Client: Resolver → Serveur

NB: Les serveurs autoritaires vont délivrer les mises à jour / les nouveaux serveurs autoritaires dans le serveur primaire.

Le Resolver:

Définition: Le résolveur de noms (Resolver) est un programme qui extrait l'information des serveurs de noms en réponse d'une requête client ⇒ l'interrogation.

Fonctionnement: Contacter un serveur de nom (DNS) → Interpréter réponse → Retourner l'information au logiciel appelant → Gérer le cache (dépend de la mise en œuvre).

Le Serveur: primaire

Le serveur ~~autorisé~~ (Serveur maître): possède sur la zone qu'il a l'autorité administrative une base d'informations.

Le serveur secondaire/esclave (Duplication du DNS): une copie du serveur primaire.

NB: Un serveur peut être primaire pour certains zones et secondaire pour d'autres.



www.english-test.net

Key Vocabulary

- | | |
|------------------------------------------|-----------------------------------------------------------------------------|
| 4) pour la demande
de l'application | 4) faire faire à
un(e) (réaliser un com-
munication qui a l'effet de) |
| 5) faire la demande
d'un papier écrit | 5) une telle chose |
| 6) faire demander quelque chose | faire |

La section Information
gère une base de données
pour la propagation des
informations.

THE BIRDS

Outline of Configuration

REND (Robotic Internet Name Decoding) Software - Implementation

Technische Universität Darmstadt, Institut für Mechanik

to you with coding questions (Source Code)

Confidential to all but the members of your Board.

Explanation of Test Test Explanation Test Explanation

It is best to take the first GDP dynamics - GDP values recorded

APRIL 1998

friction de configuration de tension de masse : $f_{\text{tension}} = \frac{1}{2} \rho V^2 C_D A$

卷之三

120. Ireland 2000

10 *lotion - en pat 53 [medicament] 10-10*

On Exercise 8 we saw that $\text{GPP} = \text{NPP} + \text{RPP}$. This is true for all plants, but it is not true for all animals.

Conditon den jaren (Agosto til April) & Lop de jaren
1900-1901 1901-1902 1902-1903 1903-1904

• "espaço de" (o que é o espaço da gente) → espaço de pessoas e comunidades (sociedade portuguesa) ||

confundit abebo 103) infelici qui vident hinc bec contemplacionem
de pene dorsi

2 °C.P.H. von - abhängig | OMP - RADS = C.R.A

Cost of materials - \$10.00 - 0.10 per sq. ft.

get a refundable credit for CHP as the "equity".

3) Vérification du système. Normal fonctionnement fait fonctionner
→ Si c'est bon, rien ne sera affiché sur le terminal.

III. Sintaxis de las ideas de los participios (se presentan)

Worship

For what you have learned I do not thank

ABRIBA - EDITORIO; FONI, voci da domani

Q3N **is equal to** $\text{M}_2 \cdot \text{Three Scores} \rightarrow \text{Growth DNA segments A, B, C}$

Com a confiança da direção da Vila, o Dr. Th. A. Góes, Dr. Adelmo e Dr. D. P.A.

En la actualidad se considera que el **gabinete** es el organismo que más se acerca a la administración directa.

1. In a group of 20 students, 12 are boys and 8 are girls. If one student is selected at random, what is the probability that the student selected will be a girl?

Chapitre 5: Service SupervisionIntroduction:

- Supervision → Surveillance → Monitoring → vérification et administration d'un parc informatique
- Services destinés pour les entreprises : Supervision, Annuaire
 - des entreprises n'ont pas qu'une simple machine → ils ont des serveurs
 - ils ont besoin de vérifier l'état s'assurer du bon fonctionnement de toute l'infrastructure
- Cette administration et surveillance doit être automatique → pour éviter que l'administrateur se déplace et vérifie équipement par équipement → N'est pas faisable.
- ⇒ assurer la fiabilité et la continuité du service via le service Supervision.
- Rôle Service Supervision: détecter les pannes, prévenir les problèmes et notifier l'administrateur en cas de problème.

- qui va appliquer les solutions et assurer le redressement du service.
- downtime: temps d'arrêt d'un serveur qui peut avoir une grande perte sur les entreprises.
(Ex: Pour un service critique (Serveur Web Amazon) qui doit être toujours disponible, fiable et continue → 1 seconde de downtime du site Amazon est une perte de 1084 \$)
- ⇒ Non disponibilité des services peut causer des problèmes pour les entreprises.

Definition du Network Management

- Network Management → système qui va surveiller et superviser
 - état des serveurs
 - état de l'infrastructure
 - afin d'assurer l'efficacité et la continuité de toute l'infrastructure
- Network Management → un service qui nous permet de
 - perte au niveau d'un seul équipement qui est défaillant
 - verifier / superviser en temps réel.
 - communiquer l'état global des équipements.
 - Créer les événements
 - Analyser la configuration de façon centralisée.
 - bande passante
 - critères de performances

Modèle du Network Management

(Selon ISO)

5 différents fonctions qui constituent le concept de supervision :Fault Management:Fault Management (Gestion des fautes/pannes/ anomalies)

C'est le processus de localisation des problèmes ou des pannes sur le réseau de données.

Fault Management implique les étapes suivantes :

- Détecter / localiser des problèmes, pannes, anomalies (passager / persistant)
- Identifier les problèmes.

- Essayer de corriger les problèmes de façon automatique

→ Dès le départ, l'administrateur va créer des scénarios

Si Serveur Web est down → Fault Management va détecter qu'il est down et exécuter des commandes et des scripts de façon automatique.

NB: on attend toujours l'intervention physique de l'administrateur.

Configuration Management

- Configuration Management → Gestion des configurations → Contrôler les fichiers de configuration

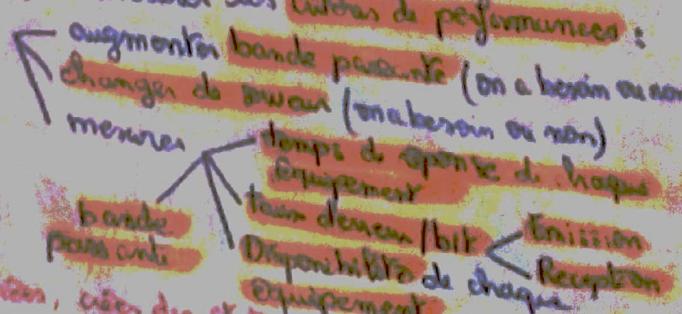
- NB:
- Fault Management (Gestion des fautes) → Vérification de l'état (sauve fonctionnel)
 - Configuration Management → Vérifier les fichiers de configuration.
- ⇒ La gestion de configuration est la première de recherche et de configuration des périphériques réseau :
- 1) Collecter toutes les fichiers de configuration (httpd.conf, named.conf, db... com, db.conf)
 - 2) Centraliser les fichiers de configuration → Configuration Management.
 - 3) Vérifier et contrôler l'état → Si on a un changement de configuration, on va sauvegarder la nouvelle configuration et l'historique dans la configuration Management.
- ⇒ Centraliser tous les fichiers de configuration et permettre à l'administrateur de vérifier l'historique et l'état de chaque fichier de configuration.

Accounting Management:

- Accounting Management (Gestion de comptabilité) → Système de facturation → connecte les changes des objets, changes des utilisateurs, changes des clients, change des serveurs et leur coût de communication.
- ⇒ Suivi de l'utilisation et du regroupement des ressources réseau pour assurer que les utilisateurs disposent des ressources suffisantes.
- (Exemple: Portail captif de l'Esprit qui permet de se connecter au réseau d'Esprit → dans le but est de contrôler l'accès) rende la connexion disponible que d'accès à l'Esprit.
- Detecter les utilisateurs créer des statut. chaque utilisateur peut se connecter à 1 ou plusieurs qui consomme + de charge.
- Ex: limite / coût d'utilisation → Chaque utilisateur peut utiliser jusqu'à 3/4 Giga/jour.
- ⇒ Si dépassement → introduire un système de facturation.
- ⇒ Cette gestion vise à limiter ou la suppression de l'autorisation d'accès au réseau.

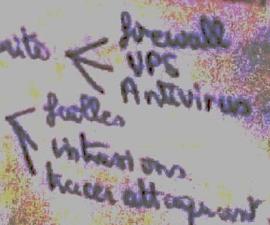
Performance Management:

- Performance Management (Gestion des performances) → mesurer les critères de performances : paramètres qui nous permet d'évaluer un réseau
- ⇒ Ce système permet de collecter les données à partir des équipements, liaison (câbles).
- Utilez un câble → bande passante ↘ → Utiliser fibre optique.
- ⇒ Gestion des performances : collecter des données, créer des stratégies statiques et établir un tableau de bord → obtenir des informations ⇒ planifier des évolutions de réseau.



Security Management:

- Security Management (Gestion de sécurité) → Gestion de solution de sécurité
- Centraliser toutes les données qui concerne la sécurité → Pour détecter
- Realiser des missions d'audit afin de trouver les vulnérabilités.
- Collecter, stocker et examiner les journaux d'audit de sécurité.
- Gérer et distribuer et stocker les clés de chiffrement.
- Maintenir et distribuer les normes d'utilisateurs et les mots de passe.
- Analyser les configurations du routeur, commutateur (switch) et serveur pour les comparer avec les politiques et procédures de sécurité.



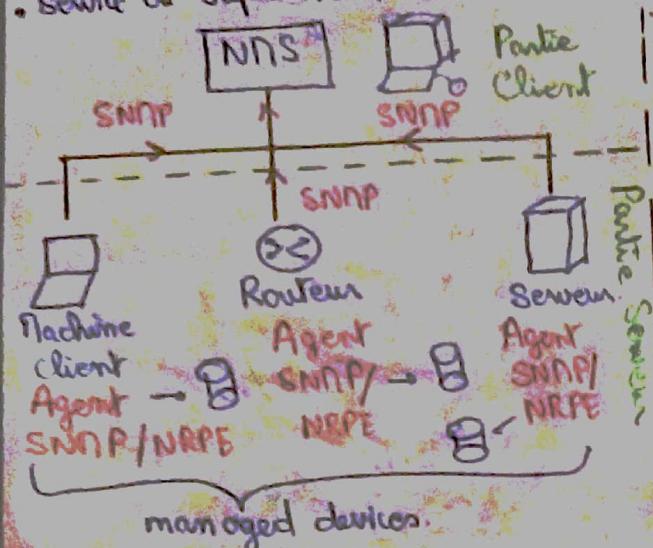
Architecture du service supervision (Network Management)

Composants:

- Un système de gestion de réseau (NMS : Network Management System) est une console dédiée pour l'administrateur qui exécute des applications pour afficher les données de gestion, surveiller / superviser en temps réel l'état de tous les équipements supervisés et communiquer avec les agents.
- Un périphérique géré (a managed device) est un nœud de réseau qui collecte et stocke les informations de gestion supervision.
- Un agent est un logiciel de supervision qui réside dans un périphérique supervisé.

Architecture:

- Service de supervision est basé sur l'architecture client-serveur.



- NMS : Network Management Station où dans laquelle le Network Management System est installé.
- Agent va collecter les données → Envoyer les données au NMS.
- NMS va afficher seulement les données → Traitement est assuré par l'agent.
- L'architecture est un peu inversée : la partie NMS utilisée par l'administrateur va être le client (sauf que à l'affichage) et l'agent installé chez le client va jouer le rôle de serveur (collecte données).
- Agent va préparer une BD dans laquelle il va stocker les données du modèle (5管理体制). → remonter en temps réel les informations au NMS.

⇒ Base de données de gestion (NDB)

NDB-object DB

- Agent est en écoute sur le port 161 → attend les requêtes envoyées par client (NMS).
- En cas de problème va notifier l'administrateur (client)

Simple Network Management Protocol (SNMP)

Définition : Protocole de gestion de réseau qui autorise

C'est le protocole de gestion et l'échange des informations entre le Network Management Station et les équipements à superviser

- Un protocole de communication qui permet à un administrateur de :
 - gérer les équipements réseau au niveau de l'infrastructure
 - diagnostiquer les problèmes à distance.
 - évaluer / Gérer les performances du réseau.
 - Trouver et résoudre les problèmes de réseau.
 - Planifier la croissance du réseau.

Composants de base:

• Network Management Station (Gestionnaire) : Station de travail PC

Collecte et stocke les informations de gestion et met ces informations disponibles à NMS (Network Management System) en utilisant SNMP.

• exécute des applications qui surveillent et contrôlent les périphériques gérés.

• Agent: Procédure en cours d'exécution sur chaque équipement qui collecte des

informations sur le périphérique sur lequel il s'exécute.

- Gestion des informations (NIB): Utilisé par le gestionnaire et l'agent pour échanger des informations de gestion.

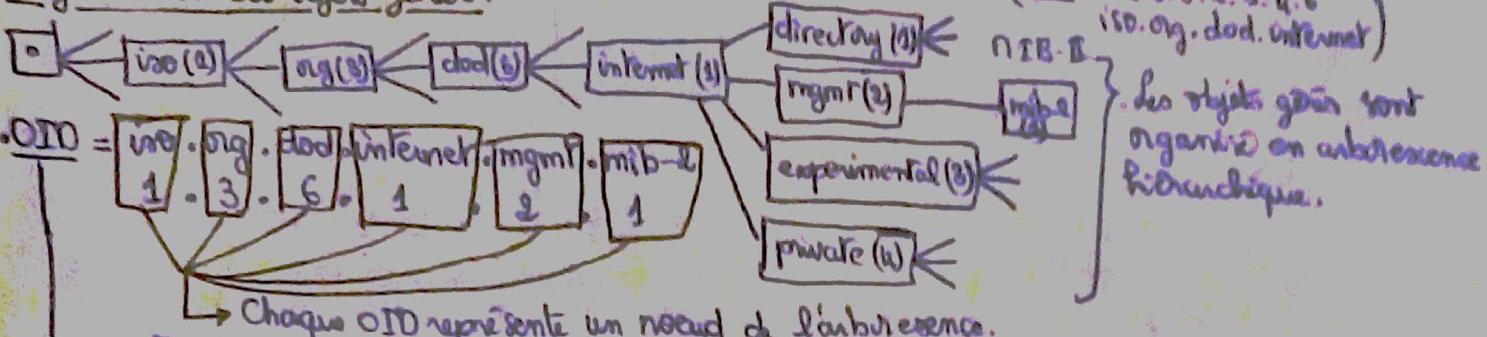
→ propriétés des ressources gérées, données pris en charge par les agents (objets gérés).

↳ Chaque objet géré → identificateur obligé (OID) → spécifié dans un fichier NIB

NB: lorsque un gestionnaire SNMP envoie une requête d'un sujet, il envoie l'OID à l'agent SNMP.

→ représenté comme une séquence d'entiers séparés par des points décimaux / par trait de trait (ex: 1.3.6.3.2.1.4.6.1.0.org.etc.internet)

Organisation des objets gérés:



NB: des fabricants d'équipements réseau peuvent ajouter des objets spécifiques au produit à la hiérarchie.

Ports et UDP:

SNMP utilise le protocole UDP pour des raisons de rapidité (puisque il transporte les messages SNMP).

NB: on ne peut pas utiliser le TCP (TCP utilise l'accès exclusif et consomme beaucoup de ressources) si notre but est la supervision en temps réel; on va envoyer plusieurs requêtes SNMP → on crée du trafic sur la ligne d'infrastructure avec les requêtes SNMP.

on utilise l'UDP avec

- Port 161 → SNMP Message (protocole)
- Port 162 → SNMP Trap Message (protocole).

Clients Pull & Server Push:

Il existe deux approches pour le système de gestion pour obtenir des informations de SNMP:

= Client Pull (SNMP Message): NMS (client) extrait les données de l'agent (serveur).

= Server Push (SNMP Trap Message): l'agent (serveur) envoie un message d'interruption (Trap Message) au NMS (client) → dans le cas du problème de défaillance.

Ex: problème de routeur: système est fonctionnel mais on a un problème à l'entrée du routeur.

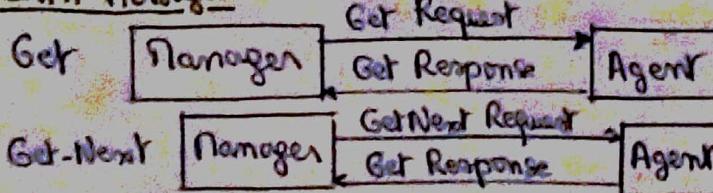
→ on attend l'émission de requête de NMS et on va retourner l'état (agent) sans pas critique.

⇒ SNMP Pulling (Client Pull): Port 161 (évenement d'interruption).

• problème critique au niveau du routeur qui cause l'in disponibilité du service (coupure de tension, défaillance générale au niveau du routeur) → agent va envoier des notifications spontanément au NMS (client) → protocole SNMP Trap (Port 162).

→ l'intervention de l'administrateur est nécessaire ⇒ Server Push.

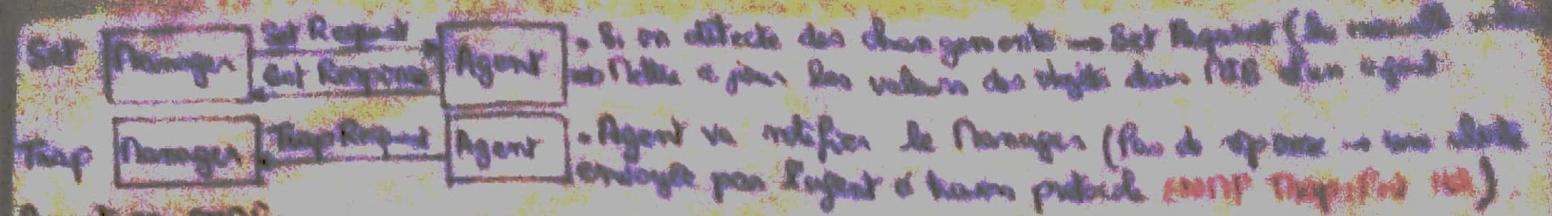
SNMP Message:



• On va collecter les données
→ Recuperer les valeurs des objets dans NIB de l'agent

• Vérifier en temps réel:
= paramètres et données stockées en mémoire.
= paramètres stockés au niveau agent.

→ Recuperer les valeurs des objets suivants
dans NIB d'un agent.



Architecture SNP

- Conception et mise en place simple : les utilisateurs peuvent facilement programmer les variables qu'ils souhaitent surveiller.
- Rapportabilité : le protocole peut être mis en place pour répondre aux besoins futurs.

Intégration SNP :

- Protocole de sécurité : les utilisateurs accèdent aux informations transmises sur le réseau.
- Pas un protocole pour l'audit officiel : les bandes passantes sont gérées avec des déformations énormes.

TP : Service de supervision

Installer et configurer Nginx :

Où va installer dashboard (dien) → Nginx

yum -y install epel -y install nginx nginx-plugins-{php,auth,users,proxy,fastcgi,fcgi}

Nginx est la version qui donne à l'administration pour vérifier les informations. Etat ...
 . Agent (installé sur la même machine) : supervise la mémoire, le charge de processeur, les utilisateurs connectés, supervise et vérifie l'état des serveurs.
 - Il faut vérifier que la configuration réseau est stable (commande `ifconfig`).

b) Configuration Nginx

1) Nodifier fichier de configuration Nginx : `http://192.168.1.1/nginx.conf`.

Order deny, allow] Nodification du paramètre d'autorisation d'accès.

Allow from 129.0.0.1 **10000/10.0.0.0** → Choisir la banane, je dois définir une IP dans cette plage.

2) Ajouter un utilisateur nginx admin : `http://192.168.1.1/nginx/pwdadmin nginx-admin`.

3) Démarrer service Nginx : `http://192.168.1.1/nginx start`

Et le service Nginx tourne.

4) Redémarrer service httpd : `http://192.168.1.1/nginx restart` Si le service httpd redémarre.

5) Exécuter la nouvelle configuration : `http://192.168.1.1/nginx reload`.

6) Activer le service Nginx : `http://192.168.1.1/nginx ifconfig`

7) Accéder via navigateur au `http://192.168.1.1/nginx` et poster deux clients sur le même port pour le serveur Nginx et s'authentifier avec l'identification "nginx-admin".

NB: Si on sélectionne "Not running" dans le conseil de Nginx (Problème de permission sur Nginx ne peut pas collecter des informations concernant les files) :

• Arrêter la solution de sécurité : `http://192.168.1.1/nginx stop`

• Arrêter elogin (solution de sécurité dans le menu de Nginx) : `http://192.168.1.1/nginx stop`

→ on a besoin d'avoir des informations sur les utilisateurs connectés, méthode elogin, méthode ... → des informations concernant OS → on a besoin d'avoir des permissions sur les fichiers d'écriture de la configuration.

Il faut supprimer les bannières, on accede à l'ordre "service".

- Dens A. Cofundat de rugine, în următoarele decenii "lăsat" să se dezvolte.
- În prezent, raza 61 (Dens) este la sfârșit perioada industrială.
- Apărării sunt obiecte de importanță, cum sunt comunalele "Piatra" și "Piatra" | 100% proprietatea sa.
- Industria comună este în desfășurare și în dezvoltare | Dens și Agro-61.
- Creștere de doar 10% în urmă cu cinci ani.
- Dens este 100% proprietatea sa.
- Apărării sunt proprietatea sa | 100% proprietatea sa.
- Creștere foarte de configurație și raza, și peste 100% proprietatea sa.

**1) Creștere
de configurație
și raza**
- Creștere
de configurație
și raza
- Creștere
de configurație
și raza
- Creștere
de configurație
și raza
- Creștere
de configurație
și raza

**2) Creștere
de configurație
și raza**
- Creștere
de configurație
și raza
- Creștere
de configurație
și raza
- Creștere
de configurație
și raza
- Creștere
de configurație
și raza

- Pădurile sunt o resursă și jumătate din teritoriul românesc.

Chapitre 4 : Annuaire

Définition et concept

Définition :

- un conteneur d'informations organisées en système de stockage de données
- Un annuaire permet d'organiser les informations concernant le monde de l'entreprise
- organisation d'une manière hiérarchique
- Donnée des BD relatives aux utilisateurs

NB : Ressources de l'entreprise (Système d'informations d'une entreprise)

- Ex: S) Esprit, authentification, Sessions → Fonctionnalités offertes (Ex: pour enseignant, étudiant, enseignant, administrateur...)
- Belle cohérence, change emploi de temps...)
- Ressources de l'entreprise :
 - physique : machines, serveurs, réseaux, BD
 - logique : applications, liste utilisateurs, listes groupes...
 - Un annuaire est une base de données
 - Une base de données n'est pas un annuaire

Annuaire = Stockage de données + Gestion de permissions
Rôle du BD (utilisateur)

Exemples d'annuaires :

- Annuaire téléphonique (du rouge jaune) : contient des données organisées alphabétiquement → BD, adresses et numéro de l'opérateur des abonnés dans service téléphonique.
- Annuaire de serveur de messagerie : lorsque on tape commence à taper l'e-mail de destinataire, on constate qu'il suggère la liste des utilisateurs de les serveurs d'qui commencent par la lettre tapée.
- DNS : un annuaire pour les applications qui se stockent des données → liste de noms de domaines et leur correspondance est dans le TP

Annuaire Electronique

les données sont stockées dans réseau

hierarchiques (Ex: DNS : racine → TLD → SUD-IDF)

→ Structure hiérarchique peut plus rapidement

rechercher que les structures relationnelles.

• Un annuaire électronique est conçu pour être consulté, authentifier →翅膀 de données, vérifier des permissions, lire des données,

NB : à travers l'annuaire, on peut modifier ou supprimer ou ajouter.

• Pour interroger un annuaire, on utilise le protocole LDAP (serveur réseau) : plus rapide, plus sécurisé, plus centralisé.

NB : l'interoperabilité dans l'annuaire, l'ajout d'utilisateurs (champs dans AD) est facile à utiliser.

→ Pas de reconstruction de base.

l'annuaire LDAP.

Définition :

LDAP (Lightweight Directory Access Protocol) est un protocole qui opère au niveau de la couche application → un protocole light weight = un protocole très facile, très efficace.

→ LDAP utilise port 389 entre serveur et client à protocole TCP (Transmission Control Protocol).

Base de données

- des bases de données sont dites relationnelles, elles sont basées sur les enregistrements de façon tabulaire.
- Structure relationnelle sont plus rapides, on utilise que des requêtes relationnelles.
- Dans les BD, on a une complète dans la forme → les BD sont utilisées plus en lecture que de l'ajout.
- Pour interroger une BD, on utilise des requêtes SQL → problème de syntaxe, compliquée en syntaxe, on a besoin de savoir plusieurs paramètres.