**ENVIRONNEMENT INTERNET**

**INTRO**

Internet : 1960 débuts -> viens des USA, volonté de réunir les facs américaines er développer les communications entre elles

Gouvernement américain qui a mandaté des chercheurs (ARPA) => réseau Arpanet

Pour permettre la gestion des paquets

1980 : le gouvernement (la défense) demande de l’aide a d’autres organismes comme HP (intérêt business)

1983 : internet = protocole TCP/IP (encore utilisé ajd)

**I – LES RESEAUX**

*Type :*

* LAN (physique) = connexion physique (L=local maison entreprises)

VLAN (logique) = LAN configurable (V=virtuel)

* MAN (LAN niveau zone : campus par exemple) = LAN mais plus grand
* WAN (internet) = wordwilde / dans le monde

*Typologie réseau :*

Chaque point représente un nœud (ordi, imprimante, objet connecté …)

* Anneau :

Un cercle avec des nœuds autour et sur lesquelles l’info circule

Chaque nœud régénère un jeton (token) pour l’envoyer à celui d’après

* Bus : (ex : dans l’industrie)

Un fil sur lequel se connectent les différentes device

Si 2 envoient une info en même temps il y a un arbitre dans le réseau, cela évite les conflits de paquets

* Etoile : (livebox)

Nœud central = centre de toutes les comm

Sur ce nœud on a un switch qui est connecté à dautres nœud

Le switch retransmet l’info à tout le monde

Si le nœud central/concentrateur tombe en panne alors plus rien fonctionne

*Réseau filaire :*

Câble RJ45

Carte ethernet : support pour brancher le câble

Commutateur / Concentrateur : appareil informatique qui permet de se connecter au réseau et d’accéder au serveur, ça donne l’adresse IP

Serveur :

*Réseau sans fil :*

Carte wifi

Commutateur / concentrateur

Serveur

*Switch = Commutateur*

Petit appareil qui permet de transférer les paquets (info) vers une adresse MAC de destination

Manière d’envoi : unicast (1personne) ou broadcast (plusieurs personnes)

Adresse MAC : identifiant unique pour identifier un appareil (constructeur, model, année de fabrication…)

Très utilisé

*Hub :*

Concentrateur / répartiteur

Propage sur tous les ports, pas d’intelligence

On ne l’utilise plus

*Protocoles :*

(s) = sécurisé

HTTP(S) : obtenir des infos d’un site web, très recommandé

(s) FTP : pour transférer des fichiers

SMTP : serveur de messagerie sortant (IMAP : serveur entrant)

TCP/IP : transporte l’information

*Modèle OSI :*

PRENDRE IMAGE SUR PPT PROF

Couche matérielle (basse) : gérer par le nœud

Couche hautes :

7 couches

*Octet :*

1 octet = 8 bits

2^8 = 255 possibilités

1 octet = 1 byte

1 byte = 8 bits

Algèbre de bool

Exo papier

*IPv4 : (4octets)*

Internet protocole version 4

Nécessaire pour se connecter à un réseau

2^32 possibilités = 4.3 milliards

ARCEP a donné derniers IP en 2019

X.X.X.X où 0 < X < 255 (X=1 octet)

Soit 4 octets

Ecrit sur 1 octet donc en **décimal**

*IPv6 : (16octets)*

Internet protocol version 6

Pour pallier à la pénurie

Adresse de 128 bits

2^128 possibilités = 340 milliards de milliards de milliards (sextillions)

Ecriture en hexa : 2001:db8:0:85a3::ac1f:8001

***Hexadécimal****:*

Base 16

Chiffre de 0 à 9

Lettre A à F

2 hexa = 1 octet

On peut le précéder de 0x

Ex : couleur RVB => FF0A12

TABLEAU PPT PROF

*Masque sous réseau :*

Netmask

Le réseau commun aux appareils

& logique bit à bit

??? PPT PROF

*&logique :*

0&0=0

0&1=0

1&0=0

1&1=1

Le résultat vaut 1 seulement si les 2 bits valent 1

*CIDR : classless inter-domain routing*

*Nouvelle notation pour les masques de sous réseaux*

/ suivi du nombre de bit à 1

La masque max est /32

X.X.X.X.255 => broadcast

*Commande ping :*

Permet de tester la réponse à une requête et donne des infos comme :

* Temps de réponse
* Perte des paquets

*Commande ipconfig :*

Permet de connaître les interfaces et des infos comme :

* IP de notre carte réseau
* Mac (adresse physique de la carte réseau)
* Wifi / Ethernet

*Commande nslookup :*

Permet de connaître des informations DNS (mémoriser les infos plus simplement, une IP=nom de domaine) :

* IP
* Nom

*DNS : domain name serveur*

Permet de retenir le nom de domaine (ex Google.com) au lieu de l’adresse IP

Nom / IP / Simple à retenir

Sous-domaine.domaine.tld

*TLD : top level domain*

Extension de domaine (.com , .fr , …)

Pays (fr, be, it)

Générique (com, org, mil …)

* 2012 : 1200 extension supplémentaires (paris, sport, leclerc ..)

*Registrar : bureau d’enregistrement*

Permet d’acheter un nom de domaine

On va sur OVH ou un autre site (gandy)

Entre 15 et 100€ par an

Un nom de domaine on l’achète pour 3 ans max, il faut penser à le racheter sinon on tombe dans le domaine public

*URL : (les éléments qui peuvent la composer)*

Protocole

Sous domaine (facultatif)

Domaine

Port

Tld

Chemin (path)

Paramètres

Ancre

*Protocole :*

* Explicite http://
* Implicite // ne précise pas le protocole mais reprend celui sur lequel est la page html donc http

URL absolue : on met l’url en entier

URL relative : on ne met qu’une partie

*Client-serveur : la personne qui initie la demande – vers quoi il veut aller*

App web : client = navigateur serveur = wordpress

= front (client) / back (serveur)

**III – LES USAGES**

*http : hypertext transfer protocol*

Permet de faire transiter une info vers un serveur / pour faire des requêtes / protocole de comm

Port 80 (http) / 443 (https) = faculté du nom de domaine a communiqué avec des serveurs

1996 : http/1.0

1997 : http/1.1

2012 : http/2.0

**Protocole sans état : envoie une requête et qd elle est terminée il ne mémorise pas**

Méthodes : GET, POST, PUT, OPTION, CONNECT

Entêtes :

* Referer : indique la page d’où l’on vient avant
* Host : domaine sur lequel on est
* User agent : combinaison entre OS, serveur et connexion
* Date
* Content type : texte, image …
* Content length : détermine la taille de la ressource que l’on demande
* …

*http/2 : évolutions*

Initié par le SPDY de google

Ce qui a été amélioré :

* Compression des header
* Push serveur (les données arrivent sans qu’on les demande)
* Multiplexage (1 requête pour plusieurs ressources)
* Envoi partiel (header)

*FTP : file transfer protocol*

ftp://

pour envoyer des fichiers

filezilla : logiciel pour faire ça

version sécurisée

Filezilla (arborescence de fichiers + pour les transférer)

*Moteurs de recherche :*

Google

Bing

Baidu (chine)

Yahoo

Duckduckgo

Qwant …

*Fonctionnement des moteurs de recherche :*

Google = 90%

On ne connaît pas son algorithme alors on fait des tests pour voir comment être bien référencé …

Les différentes versions des algorithmes :

Panda : 2011

Permet d’identifier les contenus dupliqués, plagiés ou de faible qualité et les bourrages de mots-clés

Pingouin : 2012

Permet d’identifier les spams au travers des liens frauduleux SEO

Colibri : 2013

MAJ importante portant sur l’intention de la recherche plutôt que sur les mots clés (IA)

Pigeon : 2014

Prise en compte de la localisation de l’internaute

Rank Brain :

Machine Learning (apprentissage automatique) pour mieux connaitre le sens des demandes

Fred :

Identification des sites centrés sur la monétisation uniquement

Medic : 2018

Respect des normes liés à un domaine (santé, politique, droits …)

Bert : 2019

La suite de RankBrain avec une analyse de liaison entre mots grâce à l’IA

Core update : décembre 2020

Amélioration indexation des pages

Core web vitals :

UX et performances du site

**SEO.fr => un référenceur donne une conférence par mois sur le référencement**

**PAGE SPEED INSIGHTS**

*Requêtes google complexes :*

Recherche avancée

Exemple : pour chercher un mot exact on le met entre « »

Pour chercher dans le site : site :cciformation.fr

0..45 : pour chercher dans une tranche

Filtype :pdf : pour chercher un type de fichier

….

*Sécurité :*

OWASP : organisation qui met en avant le top 10 des vulnérabilités des sites internet tous les ans

Exemple : injection SQL (faculté d’un attaquant à détourner l’usage d’un formulaire pour extraire les infos de la base de données)

Comment s’en protéger : utiliser des modules déjà faits & regarder que le code utilise des requêtes préparées

Attaques XSS : vérifier l’échappement des caractères dans du javascript

CSRF : pour éviter le vol d’identité

Disclosure information : fuite d’infos (enlever le « propulsé par … »)

Importance de protéger son site, bon plugin WP, captcha sur formulaire, bonne conscience

*Chiffrement :*

<https://chiffrer.info>

! CRYPTER = ça n’existe pas on dit CHIFFRER

*Chiffrement symétrique :*

On génère 1 clé unique qui permet de chiffrer et déchiffrer

Comment transmettre la clé de manière sécurisée ?? attention au facteur humain

*Chiffrement asymétrique :*

1 clé pour chiffrement

1 clé de déchiffrement

Clé publique (on donne au destinataire) / clé privée (on la garde pour soi) => paire de clés générée en même temps qui peuvent chiffrer et déchiffrer

Il faut faire attention à ne pas partager la clé publique et à la manière dont on la partage (man in the middle = attaquant est sur le chemin entre celui qui envoie et celui qui reçoit)

Certificat mis en place par des tiers de confiance : ex :OpenPGP (permet de générer des clés)

Utilisation : clé PGP (chiffrement de mails) et connexion SSH

*Infos cert :*

Voir diapo prof

*Algo chiffrement symétrique :*

ROT 13 / AES / DES / Blowfish : algorithmes les + utilisés

*Algo chiffrement asymétrique :*

RSA / DSA

*Encodage : ne pas utiliser pour chiffrer des données*

Différent du chiffrement : permet de générer un H (empreinte) sur une chaîne

A partir de l’empreinte on trouve le contenu

Il permet de transformer la chaîne

Base64 : le + connu

*SSL : secure socket layer*

Couche transport basé sur un chiffrement asymétrique

SSL 3.0 (faille sécurité) A PROSCRIRE : il est donc moins utilisé maintenant et il est remplacé par TLS 1.3 (futur)

**IV – Les technologies**

*OS : operating system*

Système d’exploitation

3 familles : Mac, Windows & Linux (unix sous ensemble)

3 firmes : Apple, X, Microsoft

Payant vs Gratuit

(voir PPT)

*OS server :*

Avec ou sans UI

Sans interface graphique UI = pas de ralentissement

Accès SSH

Support entreprise

Fonctionnalités adaptées

*Serveur http :*

Apache / Nginx / IIS

Est le lien entre le client et l’application

Il peut être décline en 2 autres modes :

* En mode reverse proxy : config le serveur pour que l’appli ai différentes boîtes
* Load balancer : répartiteur de charges de requêtes, pour absorber la charge

*Hébergement :*

Wordpress.com

O2switch

AWS / Azure / Heroku / Scaleway