Université Nice Sophia Antipolis

Parcours des écoles d'ingénieurs Polytech (PeiP1)

Configuration des Clickers

Pour dynamiser et rendre interactif le cours en amphi

Configuration du Boitier de Vote

- Réglage du canal de communication :
  - Appuyer sur Channel
  - Composer le numéro de canal
  - Appuyer sur Channel
  - La LED du boitier devient verte
- Votre boitier est-il prêt ?

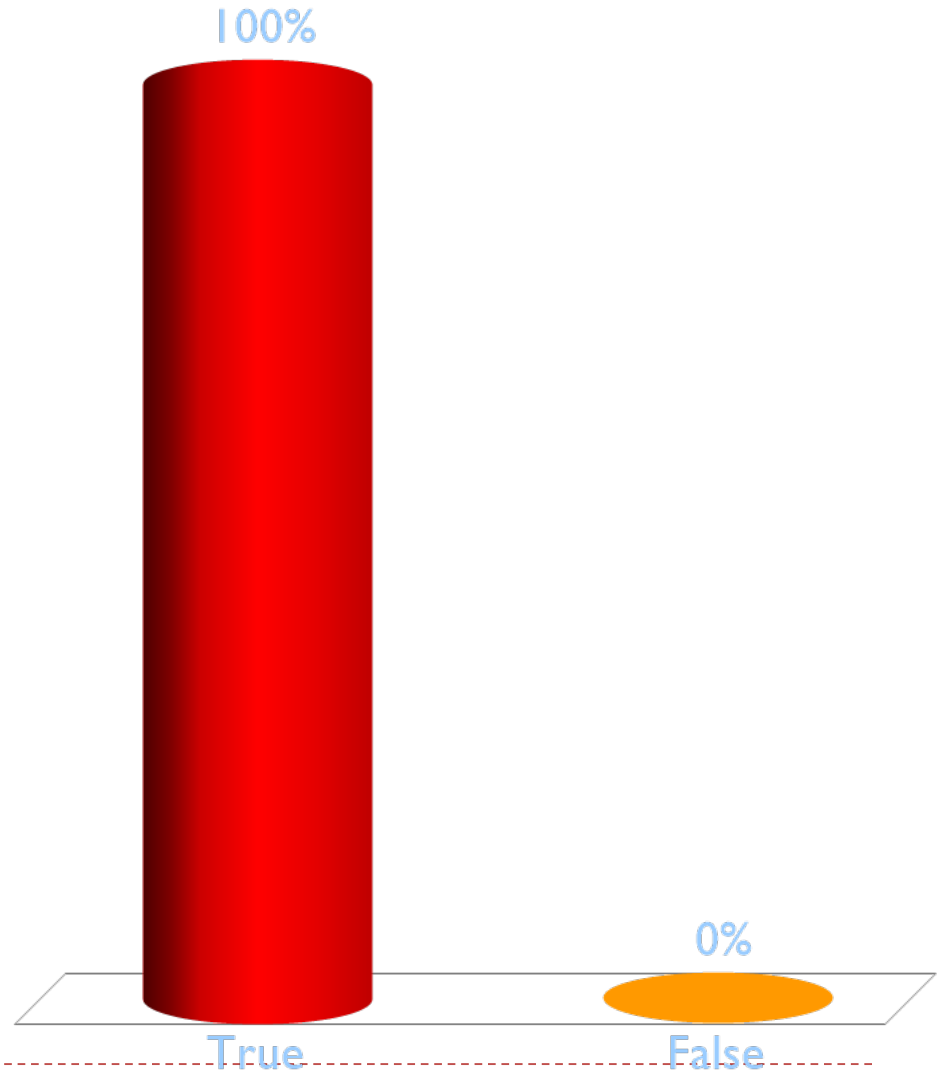
Est-ce que vous êtes prêts ?

- Etes-vous prêts ?

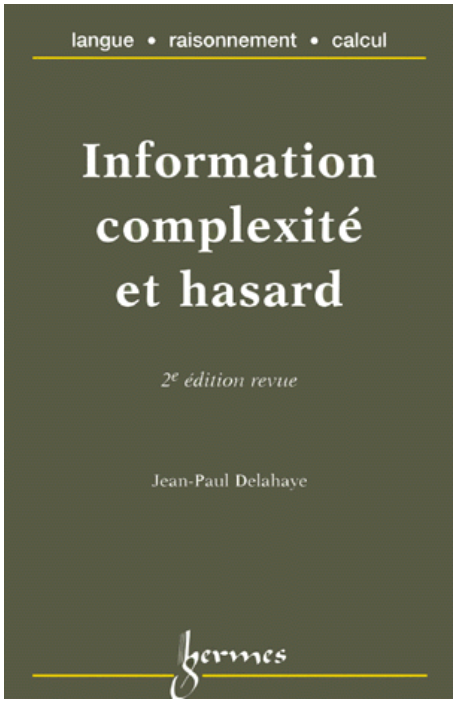
1. True
2. False

- Combien de votants ?

1



Université Nice Sophia Antipolis



Codage et Théorie de l'Information

« Information, complexité et hasard » de **Jean-Paul Delahaye**, revu par **Pierre Bernhard**

Exemples et textes proposés par **Gilles Dowek, Jean-Pierre Archimbault, Emmanuel Baccelli, Thierry Viéville et Benjamin Wack**

Vous avez dit information ?

- Dans la suite :
  - 00000 00000 00000 00000 00000 00000 00000 00000
- il y a sûrement moins d'information que dans la suite :
  - 14159 26535 89793 23846 26433 83279 50288 41971 69399
- qui est plus complexe mais… Pourquoi ?

- Serait-ce que la 2ème suite
  - a une complexité aléatoire :
    - aléatoire, sans ordre, sans régularité, chaotique ?
  - ou une complexité organisée :
    - organisé, fortement structuré, riche en information ?

Vous avez dit information ?

- Distinguons donc bien :
  - Un contenu **brut** en information qui ne dépend pas du sens
  - La **valeur** d'une information dépend du but fixé

- Avec deux grandes théories (selon le but) :
  - **Théorie probabiliste de l'information** (Shannon)
  - **Théorie algorithmique de l'information** (Kolmogorov / Bennett)

- En lien avec :
  - l'informatique théorique, les neurosciences computationnelles etc..

Contenu Brut en Information

1. Le contenu brut en information d'un booléen
   - (1/0 vrai/faux oui/non yin/yang)
   - C'est l' « atome » d'information: le « bit »
2. Le contenu en information d'une valeur v {1,N}
   - (digits (N = 10), lettre de l'alphabet (N = 26), ..) est **log2(N)**.
   - **C'est le nombre de bits pour "coder" la valeur**
3. Le contenu brut en information de n éléments « indépendants » est la somme des contenus bruts.
   - mais inférieure s'il y a de la redondance (compression)
   - mais sans valeur si il n'y a aucun lien entre les éléments !

⇨ **C'est le nombre minimal de questions oui/non à poser pour trouver la valeur donnée !**

Nombre minimum de questions oui/non à poser pour trouver la bonne personne ?

Exemple de Codage

- Exemple du jeu « Qui est-ce ? »™
  - Quelles sont les question à poser ?

	Genre	Cheveux	Lunettes	
Robert	Homme	Brun	Non	100
Anita	Femme	Blond	Non	010
Charles	Homme	Blond	Non	110
Marie	Femme	Brun	Non	000
Anne	Femme	Brun	Oui	001
Tom	Homme	Brun	Oui	101
Claire	Femme	Blond	Oui	011
Joe	Homme	Blond	Oui	111

$\log_2(8) = 3$

Exemples de Codages

- Combien de questions poser pour deviner:
  - l'âge d'un élève du secondaire entre 11 et 14 ans

11	12	13	14
00	01	10	11

  - coder les couleurs de l'arc en ciel

violet	Indigo	bleu	vert	jaune	orange	rouge
000	001	010	011	100	101	110

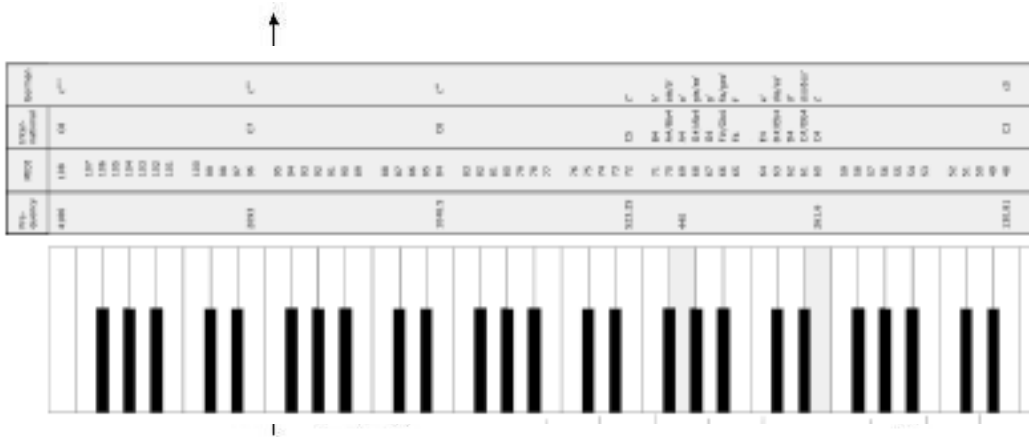
- Mesure physique:
  - la quantité brute d'information se mesure en bits
  - Comme la température en degré, la tension électrique en volt…

Symboles pour Coder l'Information

- Combien de symboles pour tout coder ?
  - 1? Avec un seul on ne fait pas grand-chose
    - Au moins deux !
  - Plus de deux symboles ? Pourquoi pas…
    - 10 chiffres arabes,
    - 22 lettres de l'alphabet phénicien,
    - 24 lettres de l'alphabet grec,
    - 26 lettres de l'alphabet latin,
    - …
- Tout coder avec deux symboles uniquement ?
  - Oui car:
    - Choix indépendant de la nature des informations décrites
    - Plus simple à mettre en œuvre dans une machine (ouvert/fermé)
    - Plus robuste: si états intermédiaires, il y aurait plus d'erreurs

Les Objets Numériques

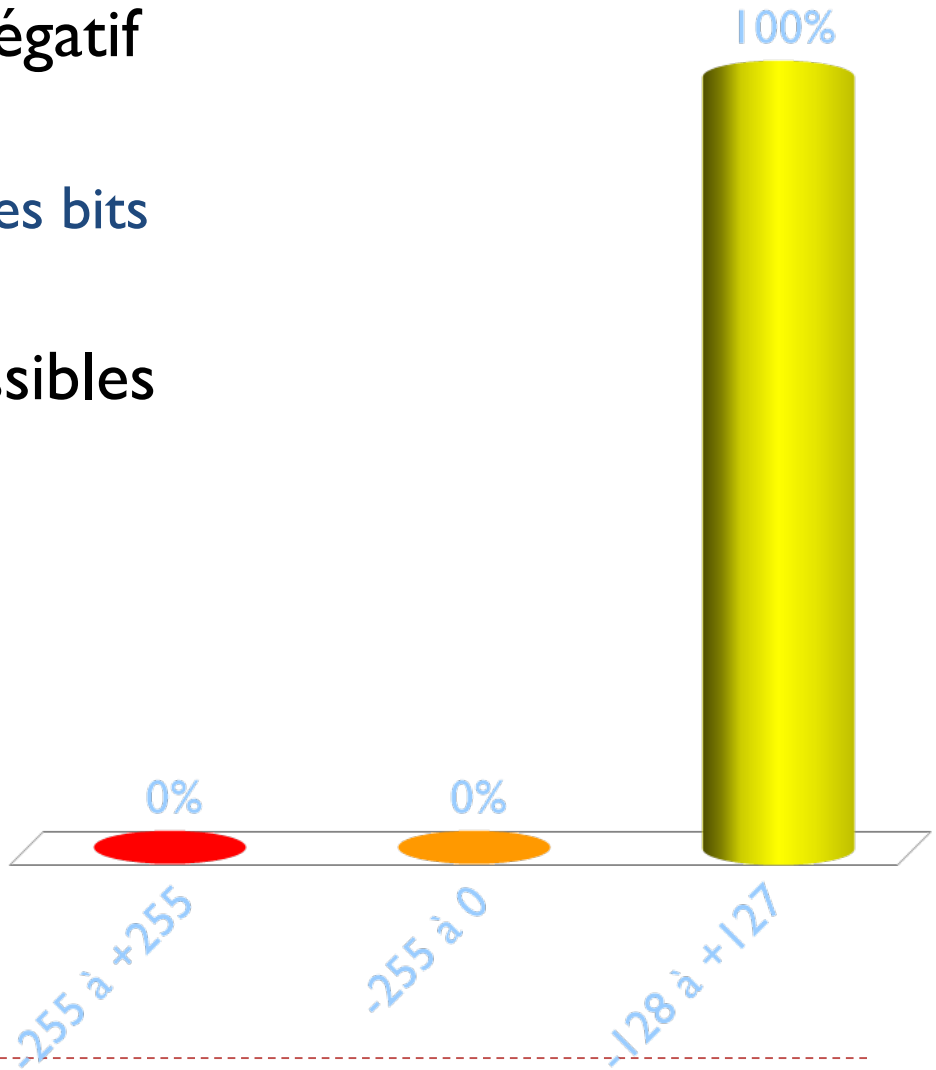
- Décrire numériquement des objets:
  - Un texte: code ASCII ou UTF-8 pour chaque caractère
    - Nombre maximum de caractères à coder
  - Un nombre: codage des nombres entiers et décimaux
0 à 1	0 à 3	0 à 7	0 à 15	0 à 255	0 à 1023	0 à 4 millions	0 à plus de 1.8×10^{20}
1 bit	2 bits	3 bits	4 bits	8 bits	10 bits	32 bits	64 bits
  - Une image: codage de l'information de couleur
    - Nombre maximum de couleurs à coder
  - Une mesure physique:
    - Un son
    - Une musique (MIDI)
    - Un film



Codage de nombres négatifs

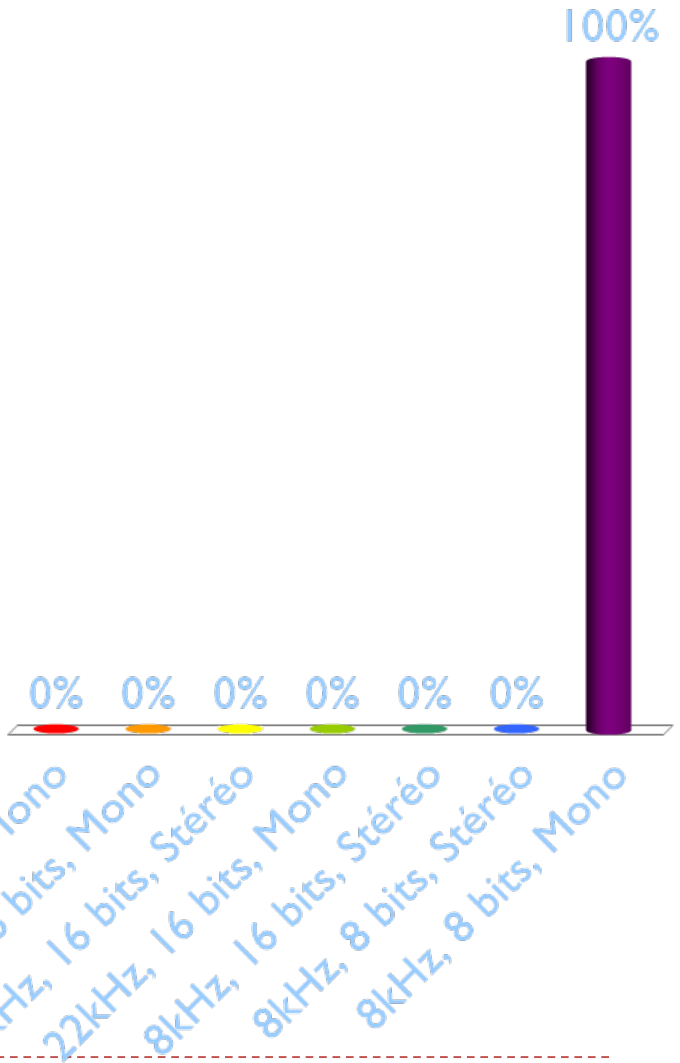
- Et le codage d'un nombre négatif est-ce possible ?
  - Bien sûr ! On va utiliser un des bits pour coder le signe
- Quelles sont les valeurs possibles pour des entiers (positifs et négatifs) sur 1 octet ?

1. -255 à +255
2. -255 à 0
3. -128 à +127



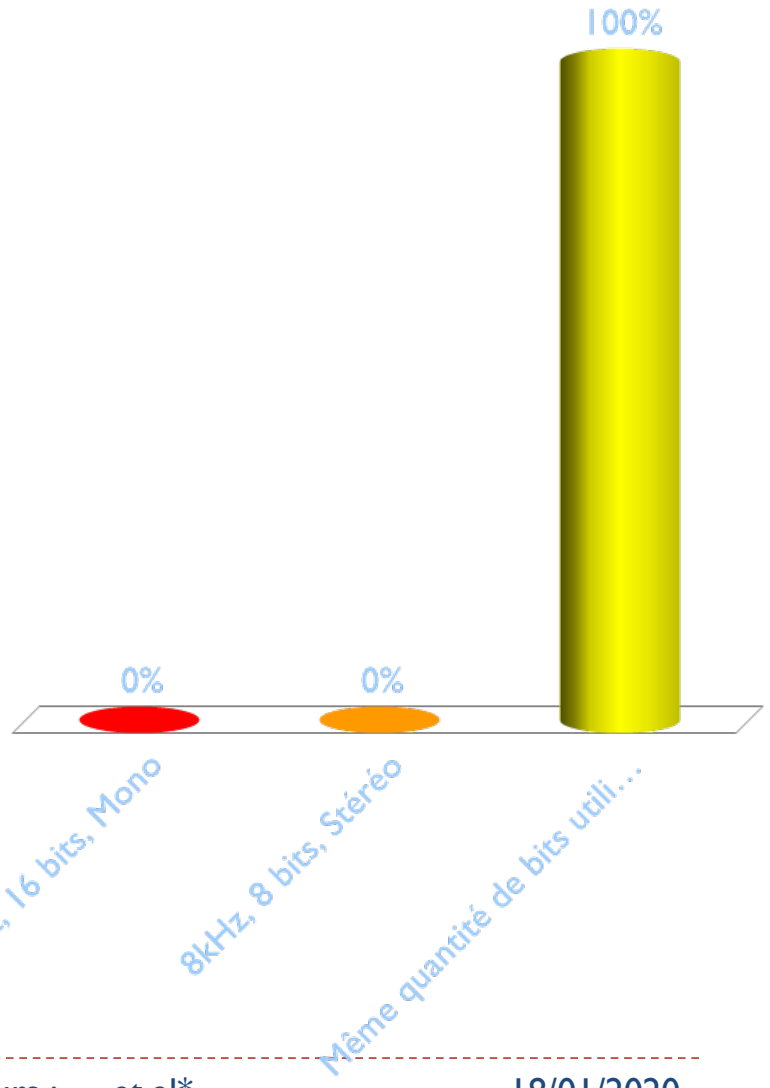
Quel est le format le plus adapté à la téléphonie ?

1. 44kHz, 8 bits, Mono
2. 44kHz, 16 bits, Mono
3. 44kHz, 16 bits, Stéréo
4. 22kHz, 16 bits, Mono
5. 8kHz, 16 bits, Stéréo
6. 8kHz, 8 bits, Stéréo
7. 8kHz, 8 bits, Mono



Quel format nécessite le plus d'informations: 8kHz, 16bits, Mono ou 8kHz, 8bits, Stéréo ?

1. 8 kHz, 16 bits, Mono
2. 8kHz, 8 bits, Stéréo
3. Même quantité de bits utilisée



Contenu Probabiliste en Information

- Pour le contenu probabiliste en information qui :
  1. N'est fonction que de la probabilité des évènements
  2. Est additif pour deux sources indépendantes
  3. Croît linéairement avec le nombre de réponses équiprobables
- On parle d'entropie au sens de Shannon et obtient une définition :

$$H(p:\{1..n\}\rightarrow[0,1]) = -\sum_{n} p(n)\log_2(p(n))$$

contenu <u>moyen</u> en information d'une distribution de probabilité.

Contenu Probabiliste en Information

- Pour une distribution binaire $p : \{0, 1\} \rightarrow [0, 1]$
  - H = 1 si p(0) = p(1) = 1/2 : hasard complet, non-redondance
  - H = 0 si p(0) = 1, p(1) = 0 : valeur fixe, rien à découvrir

- Pour une distribution uniforme $p : \{0,N\{ \rightarrow [0, 1]$, p(i)=1/N .
  - H est maximale
  - H = log2(N) : nb de bits pour coder la valeur

- Au delà :
  - H est une valeur positive, bornée.
  - Elle se définit dans le cas continu à une résolution donnée.

Applications de l'Information Probabiliste

- Codage de l'information
  - On a vu cela sur la partie codage de l'information
- Compression de données (exemple 1)
  - Vous l'utilisez quand vous compressez un fichier texte (zip)
- Cryptographie
  - Quand vous avez le petit cadenas dans votre navigateur
- Correction d'erreurs (exemple 2)
  - Quand on transmet une information dont une partie peut avoir été perdue pendant le transport ou la lecture
  - Attention à ne pas confondre avec la vérification

La compression d'un texte est plus efficace avec un algorithme avec perte d'information ?

1. Cela n'a pas de sens
2. Oui
3. Non

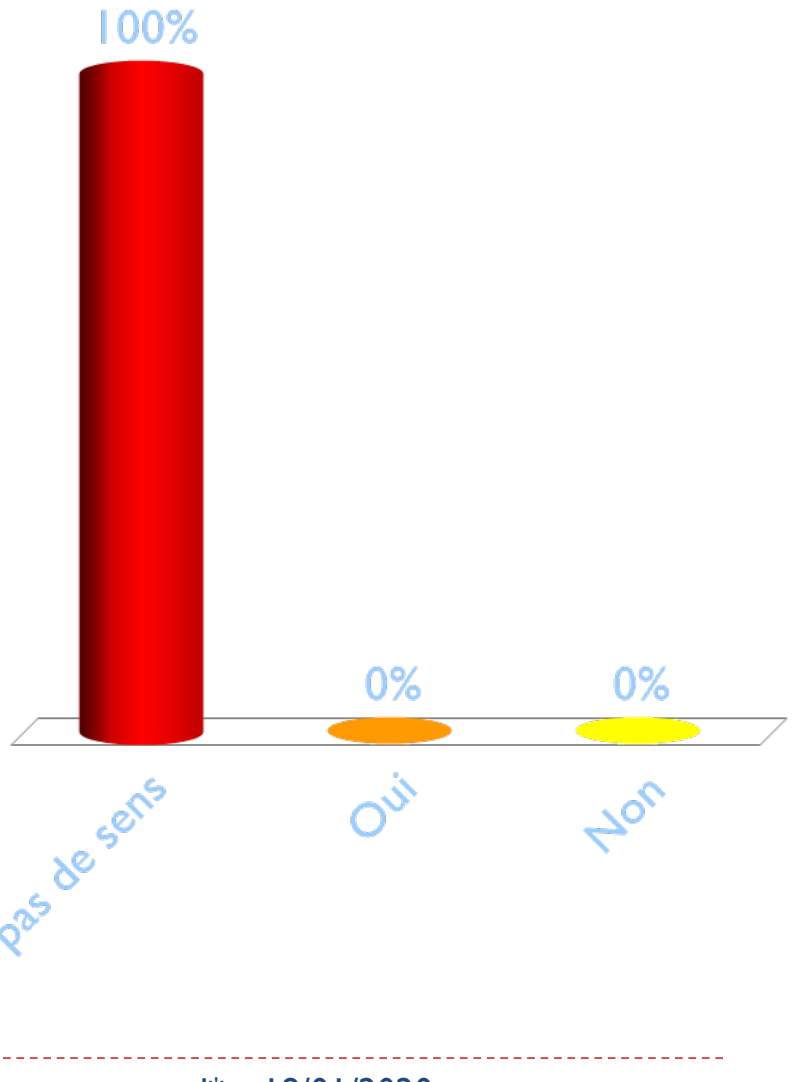
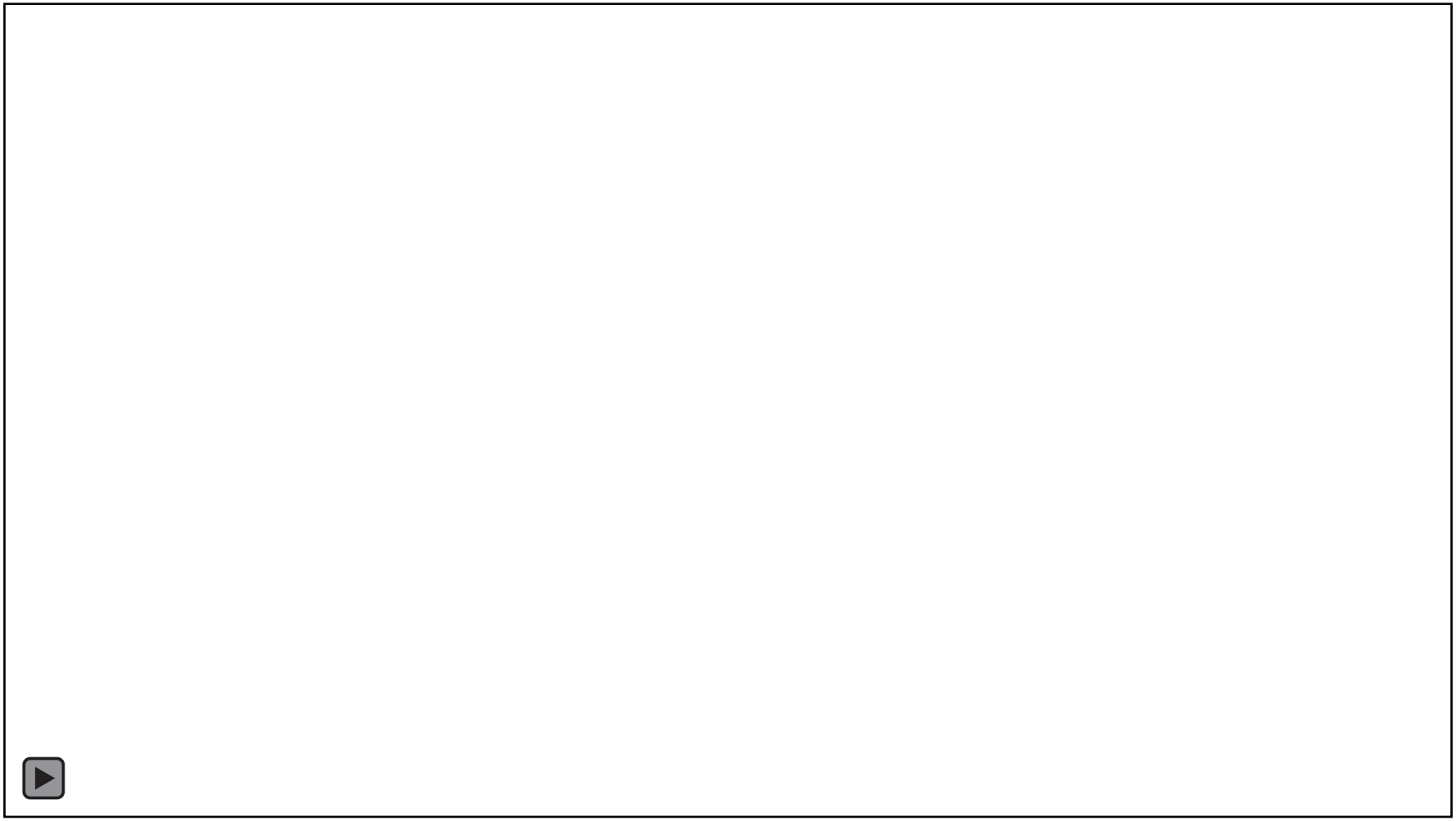


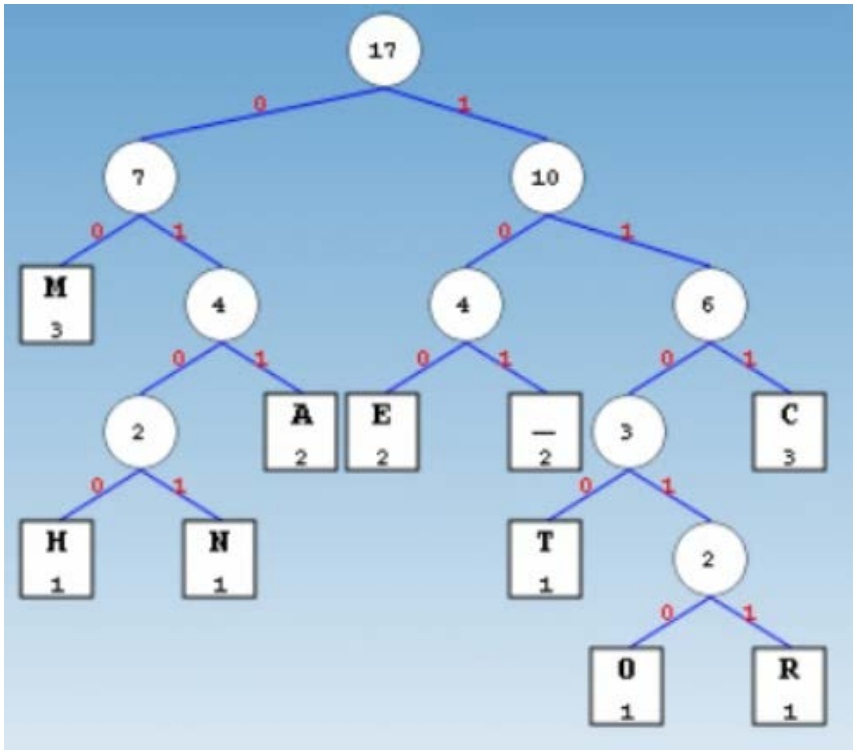
Illustration de la compression sans perte

- Le codage de Huffman
  - est un algorithme de compression de données sans perte
  - basé sur l'information probabiliste/statistique
  - Utilise un codage de longueur variable, préfixé
- Soit la phrase « *comment_ca_marche* »
- On commence par calculer la fréquence de chaque lettre
  - C=3, O=1, M=3, E=2, N=1, T=1, _=2, A=2, R=1, H=1
- Ce qui en les ordonnant donne:
  - H=1, N=1, O=1, R=1, T=1, A=2, E=2, _=2, C=3, M=3
- Puis on construit un arbre à l'aide de ces données
  - la suite en images…

Construction de l'arbre de Huffman



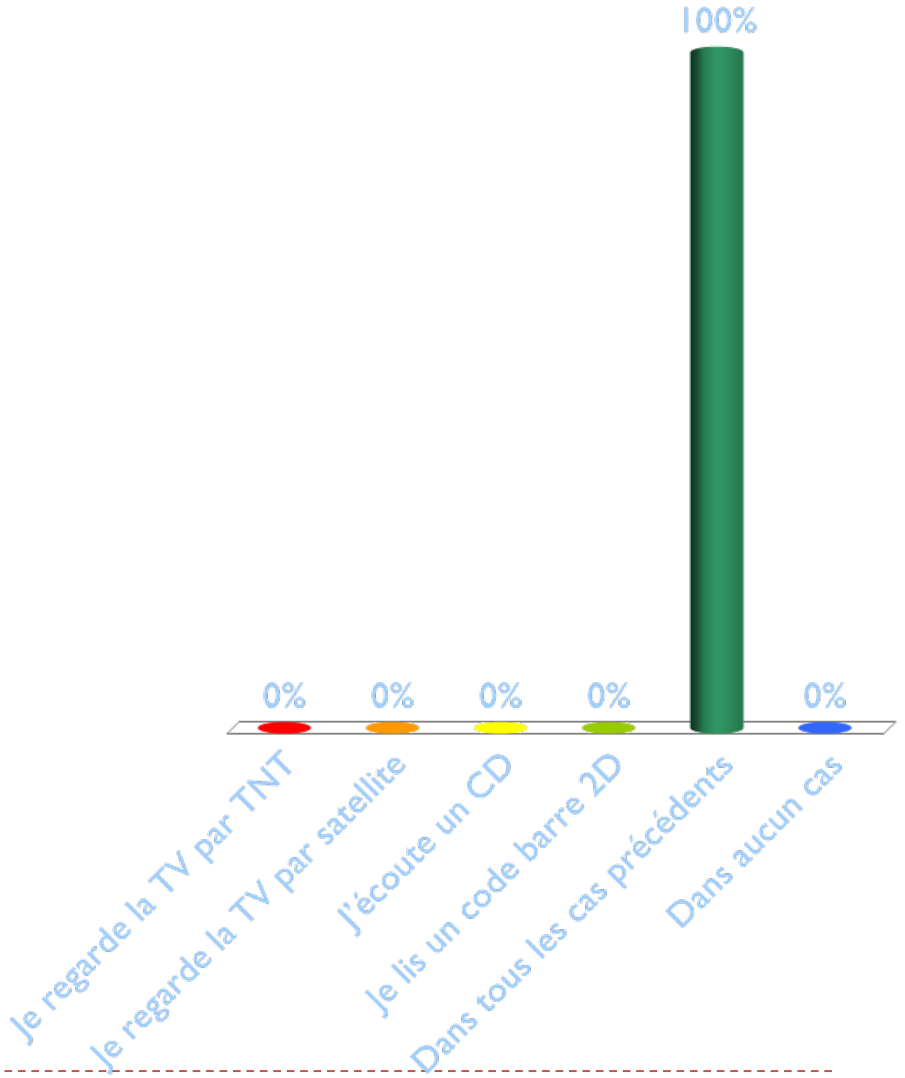
Résultat du Codage de Huffman



- M = 00
- H = 0100
- N = 0101
- A = 011
- E = 100
- _ = 101
- T = 1100
- O = 11010
- R = 11011
- C = 111
- On passe de 136 bits à 55 bits (gain de 60%)

Dans quel(s) cas est-ce que j'utilise la correction d'erreur sans le savoir ?

1. Je regarde la TV par TNT
2. Je regarde la TV par satellite
3. J'écoute un CD
4. Je lis un code barre 2D
5. Dans tous les cas précédents
6. Dans aucun cas



Introduction du Code Reed-Solomon

- Code très utilisé:
  - permet de corriger des erreurs dues à la transition imparfaite d'un message
  - De nombreuses application:
    - Stockage de données (CD, DVD)
      - Corrige les problèmes de rayures
    - Transmission d'information numériques: DVB-S, DVB-T, ADSL*
      - Corrige les problèmes d'interférences (bruit impulsif)
- Principe basé sur :
  - Les corps de Galois (base de la théorie de l'information)
  - Construire un polynôme formel à partir des symboles à transmettre et le sur-échantillonner
  - La redondance permet au récepteur de reconstruire le polynôme même s'il y a des erreurs pendant la transmission

Description Intuitive du Code Reed-Solomon

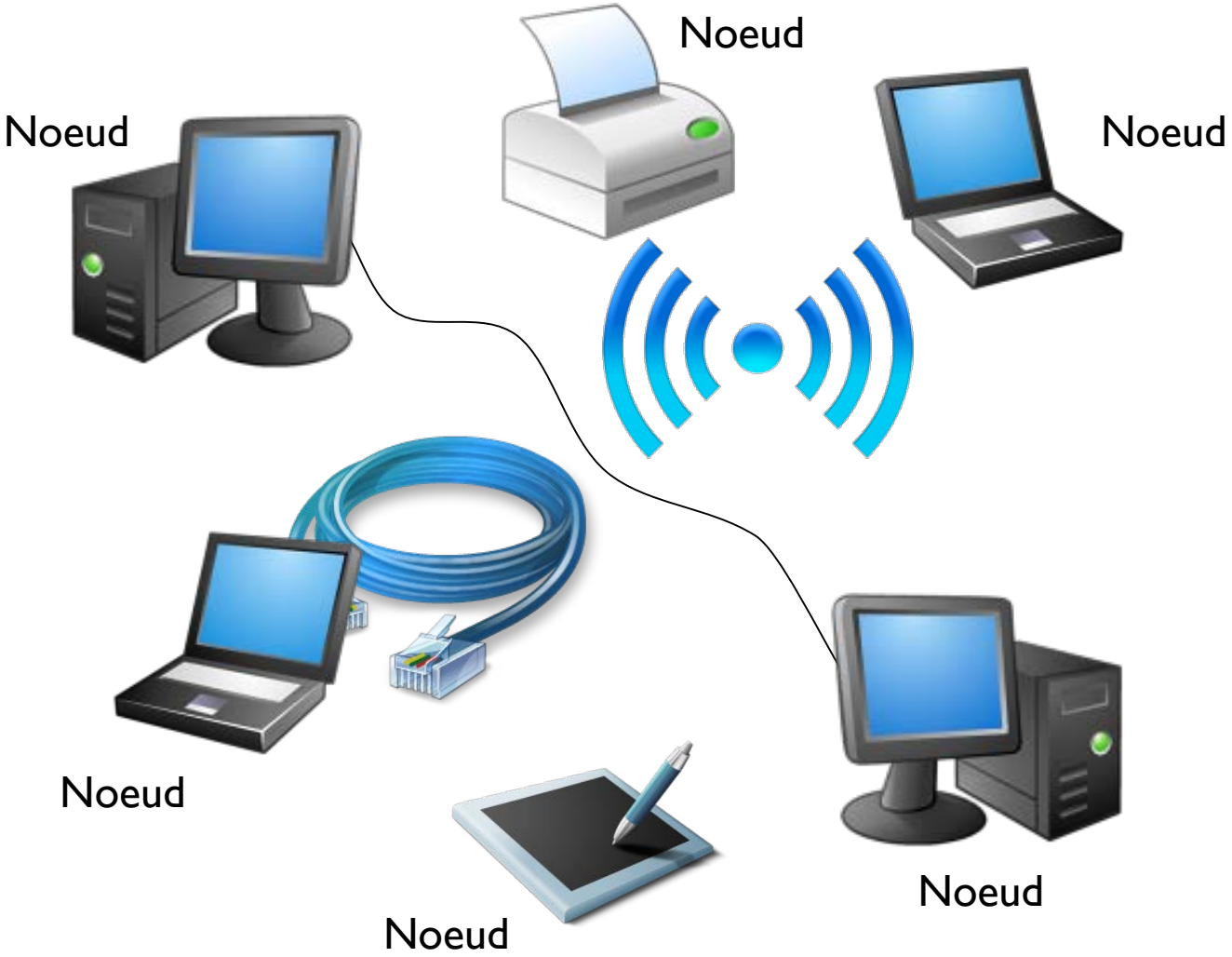
- On souhaite transmettre un bloc de 3 nombres
  - 02 09 12
- On ajoute deux nombres de redondance :
  - La somme des 3 nombres: 02 + 09 + 12 = 23
  - La somme pondérées par le rang: 02 * 1 + 09 * 2 + 12 * 3 = 56
- Donc l'information transmise est : 02 09 12 23 56
- Si l'information reçue est : 02 13 12 23 56
  - La somme est : 02 + 13 + 12 = 27
  - La somme pondérée est : 02 * 1 + 13 * 2 + 12 * 3 = 64
- Recherche de l'erreur:
  - Sur la somme simple: 27 – 23 = 4
  - Sur la somme pondérée: (64 – 56) / 4 = 2
- Il faut donc retirer 4 à la donnée de rang 2 !

Université
Nice
Sophia Antipolis

Réseaux informatiques

Environnement Informatique 1

Réseau informatique

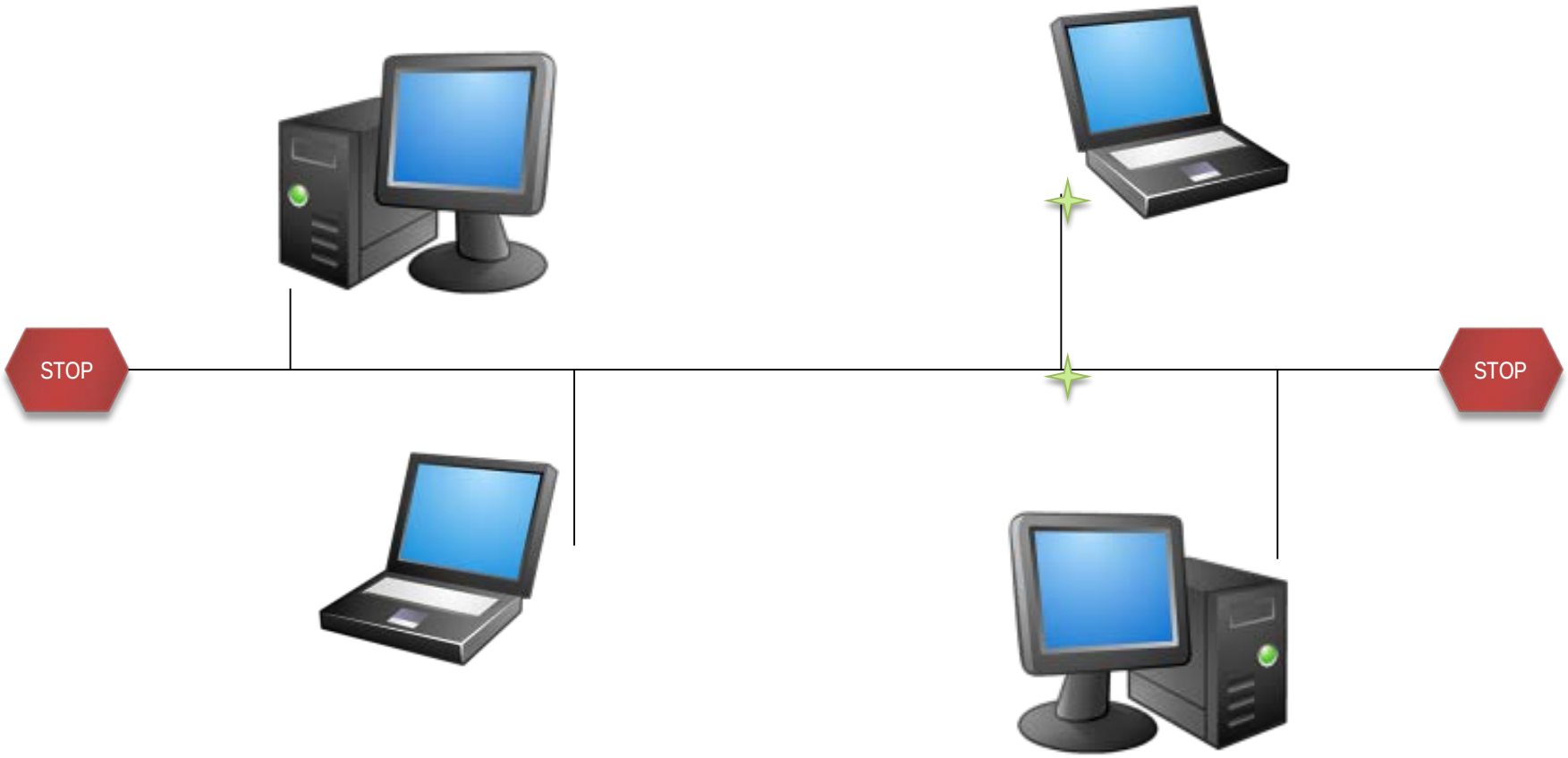


Topologie Physique vs Logique

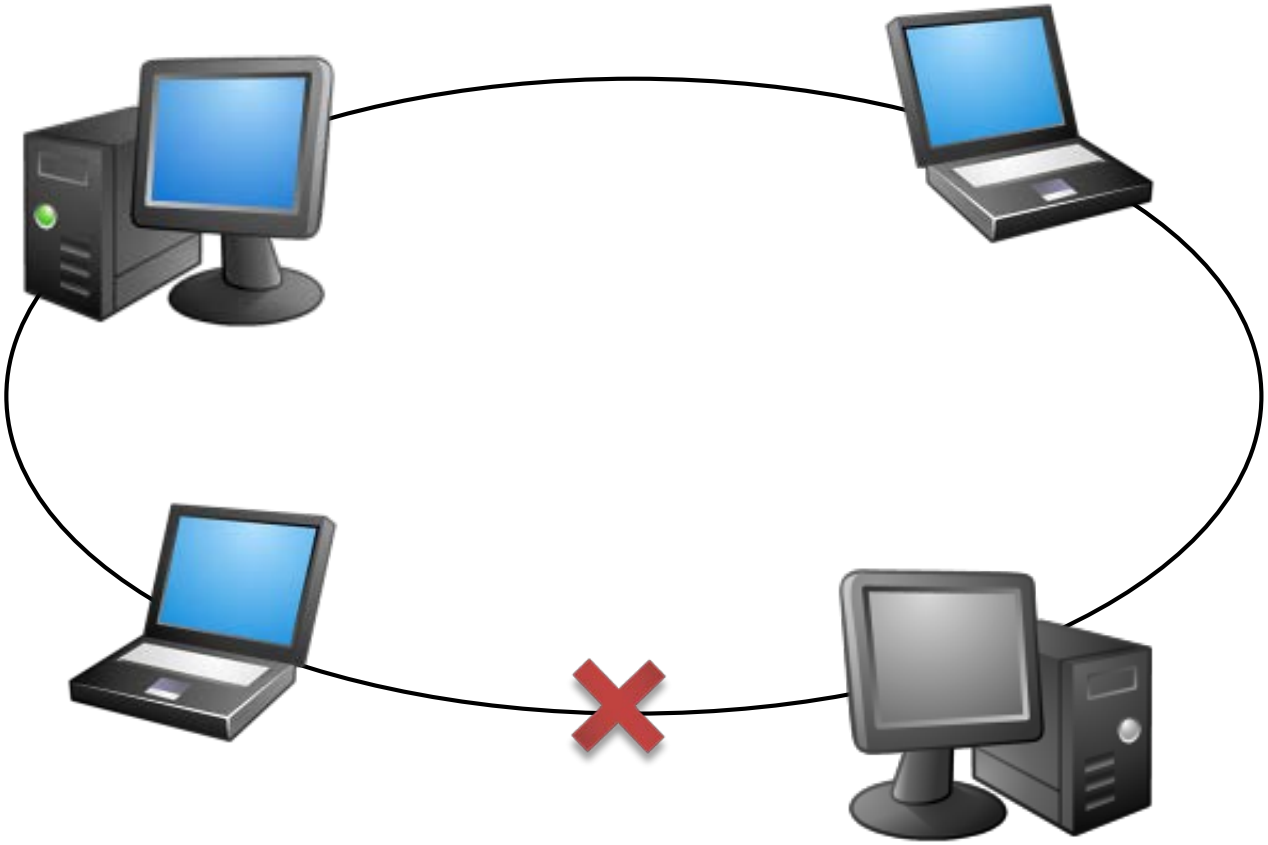
- Physique
  - Le schéma d'implantation physique d'un réseau
    - Les nœuds du réseau
    - Les connexions entre les nœuds du réseau
- Logique
  - Comment les données sont véhiculées à travers le réseau
- Les 5 principales topologies physiques
  - Topologie Point à Point (dans la diapositive précédente)
  - Topologie Etoile
  - Topologie Bus
  - Topologie Anneau
  - Topologie Maillée

Topologie en Etoile

Topologie en Bus

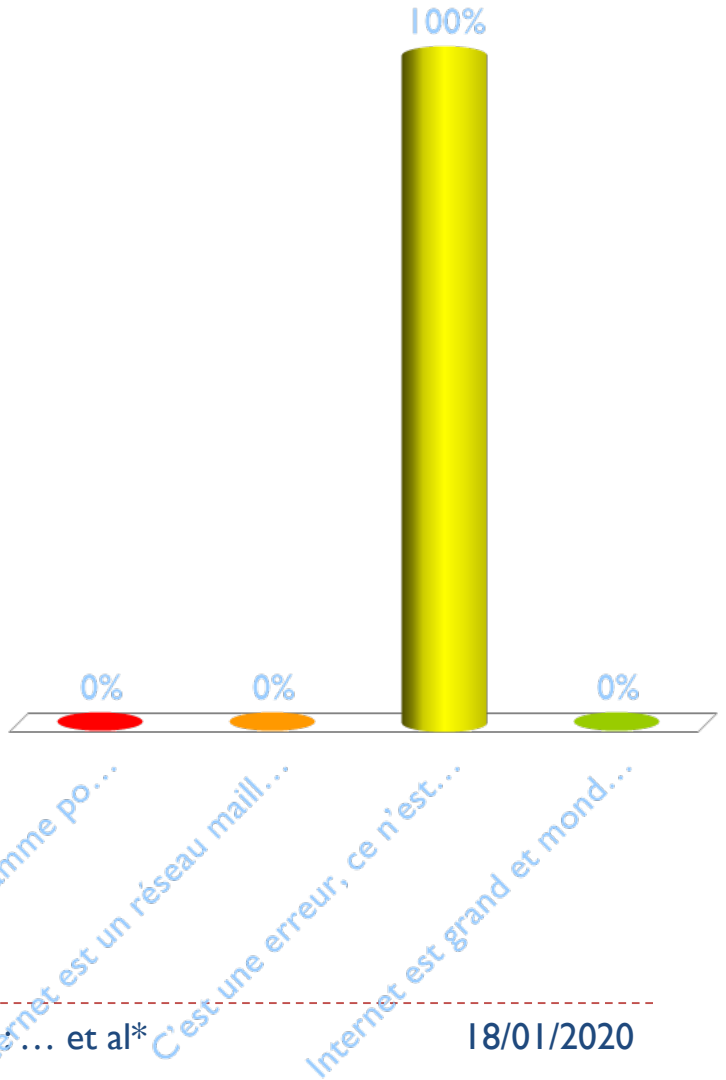


Topologie en Anneau



Quand on parle d'Internet, on dit souvent le Web, car…

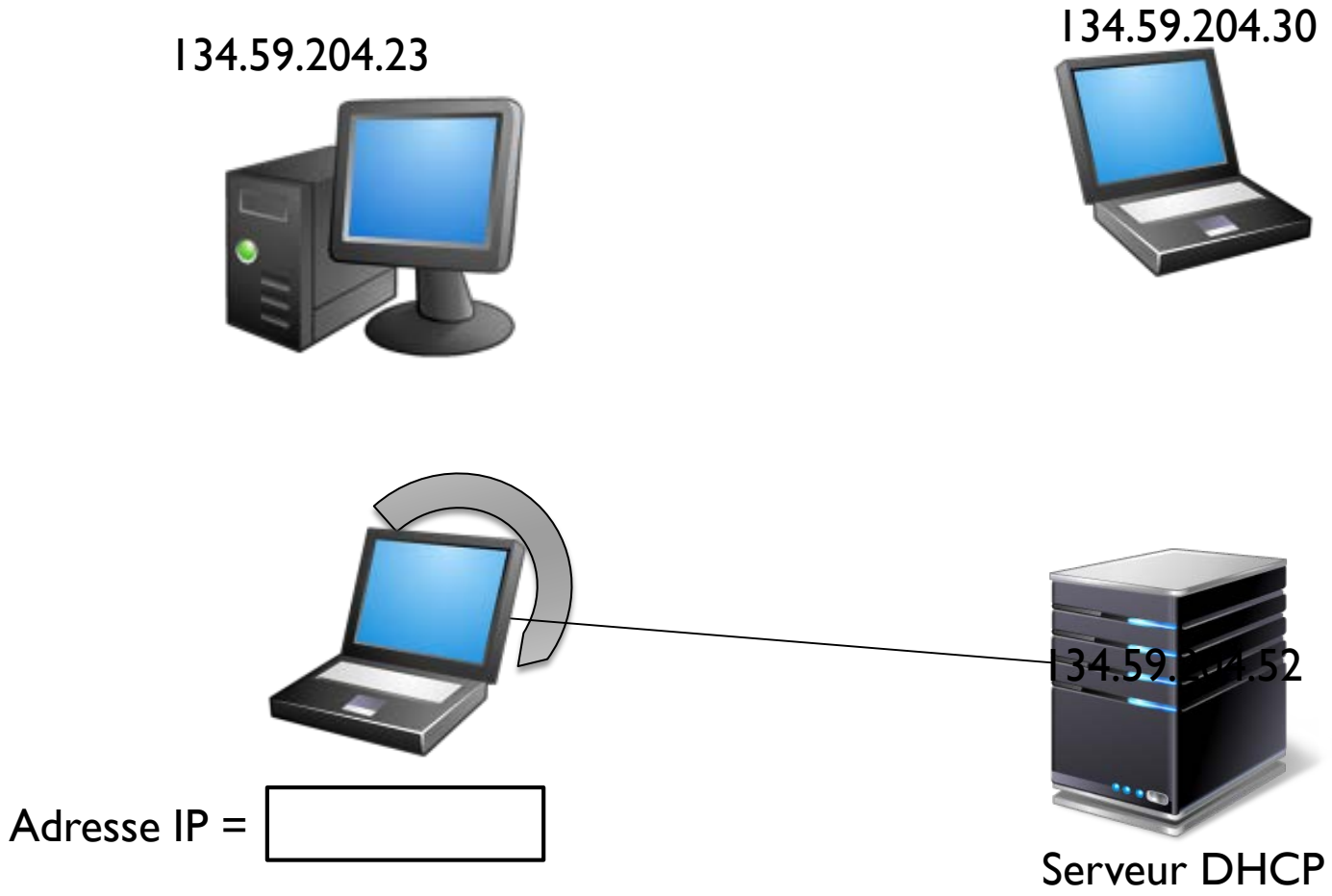
1. Le premier programme pour rechercher les pages sur Internet s'appelait spider
2. Internet est un réseau maillé comme une toile d'araignée
3. C'est une erreur, ce n'est pas la même chose
4. Internet est grand et mondial (World Wide Web)



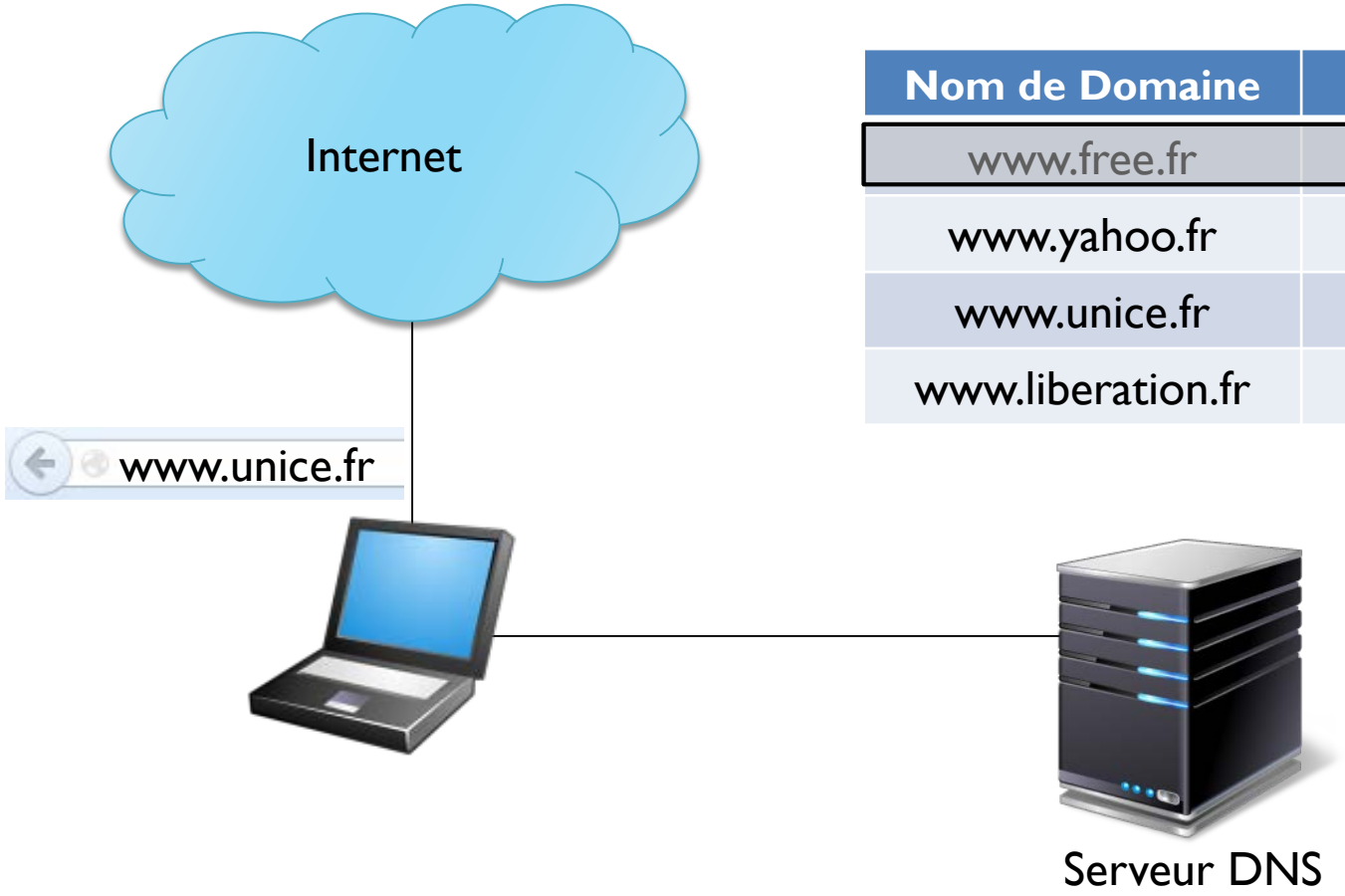
Construire un réseau c'est bien, le faire marcher c'est mieux !

- Points essentiels pour que les machines puissent communiquer (exemple d'un réseau IP) :
  - Besoin de les identifier
    - IP dynamique: DHCP
    - Nommage: DNS
  - Sortir d'un sous-réseau (calcul du sous-réseau)
    - Passerelle
- Mais bien d'autres choses encore:
  - Besoin de désigner une ressources sur un ordinateur distant
  - Besoin de protocoles
  - Besoin de sécurité, confidentialité, authenticité
  - Mais aussi besoin d'anonymat (car tout est « surveillable »)

Obtenir une adresse IP: Serveur DHCP

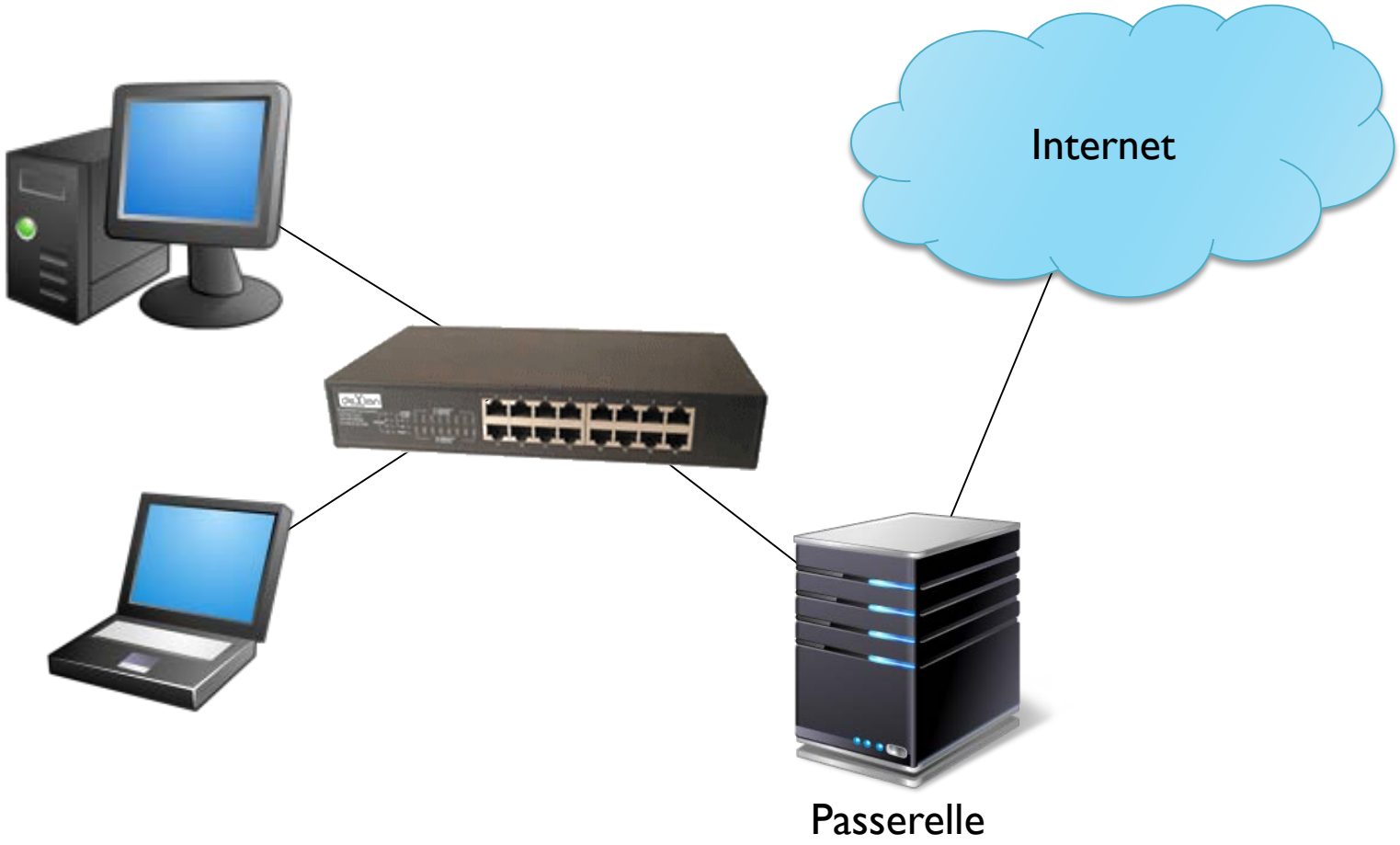


Oui, mais moi je manipule des noms



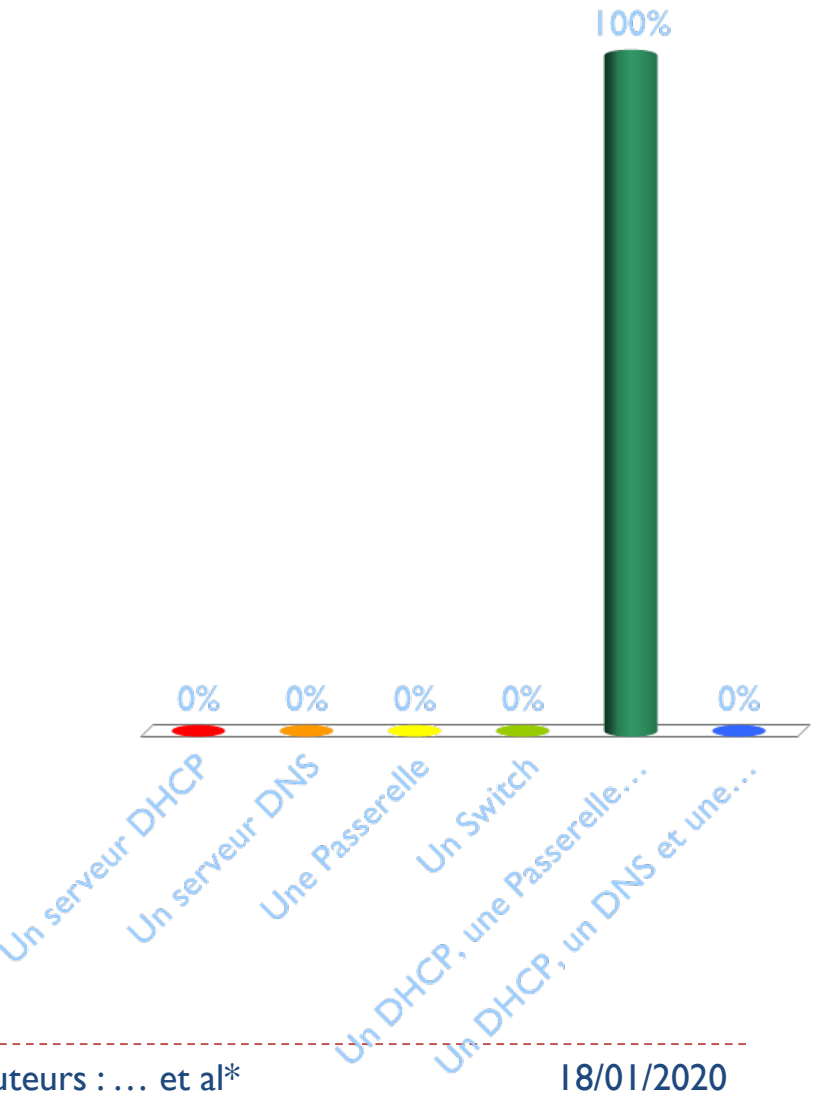
Nom de Domaine	Adresse IP
www.free.fr	212.27.48.10
www.yahoo.fr	77.238.178.122
www.unice.fr	**134.59.204.1**
www.liberation.fr	151.249.94.20

Une passerelle pour faire sortir le trafic du sous-réseau

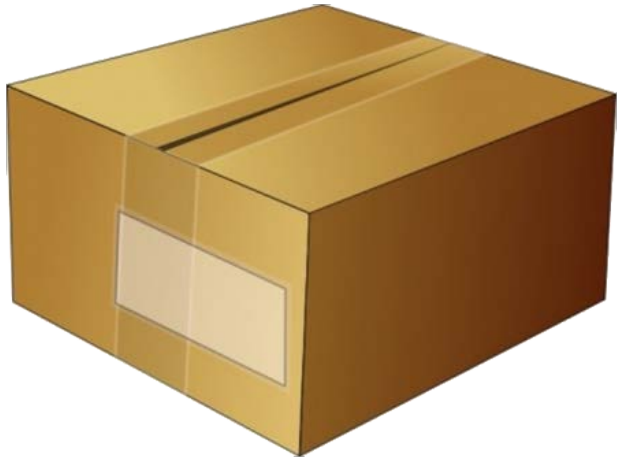


Qu'y a-t-il dans votre box à la maison?

1. Un serveur DHCP
2. Un serveur DNS
3. Une Passerelle
4. Un Switch
5. Un DHCP, une Passerelle et un Switch
6. Un DHCP, un DNS et une Passerelle



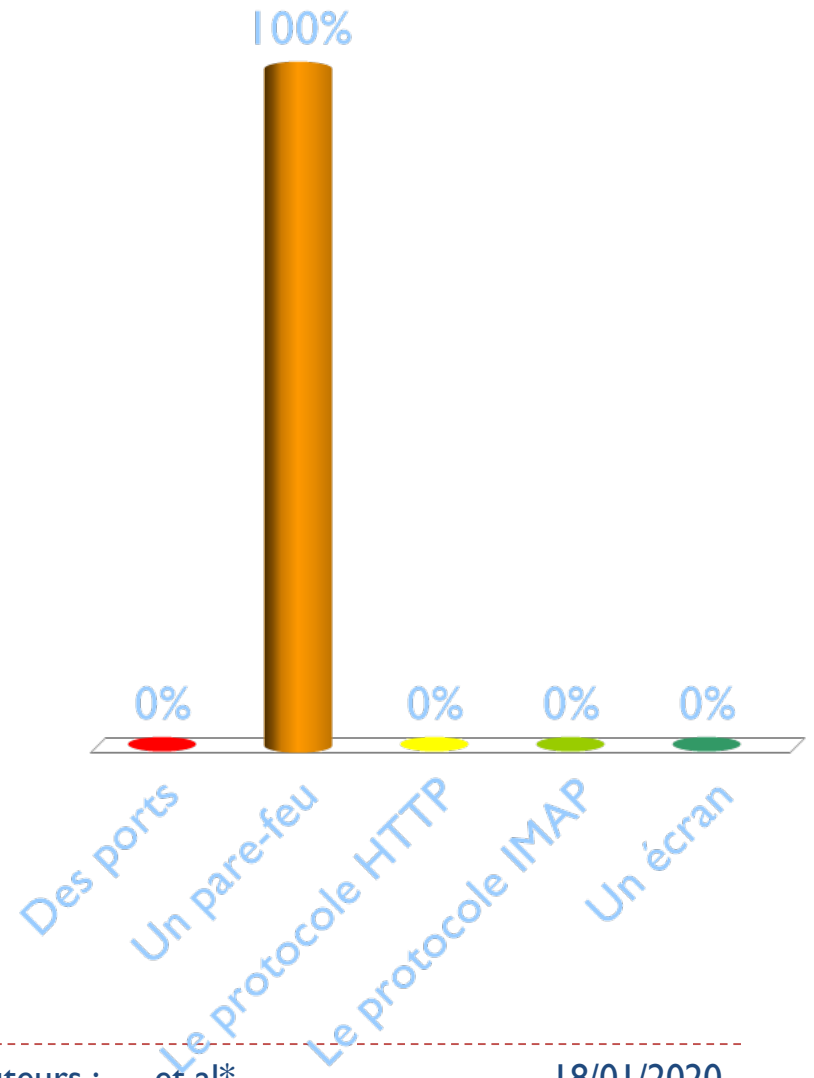
Dans votre box…



Serveur DHCP Serveur DNS Passerelle Switch

Quel élément essentiel pour la sécurité est aussi dans votre box ?

1. Des ports
2. Un pare-feu
3. Le protocole HTTP
4. Le protocole IMAP
5. Un écran



Dans votre box, quelle qu'elle soit…

- Il y a…

Serveur DHCP

Pare-feu

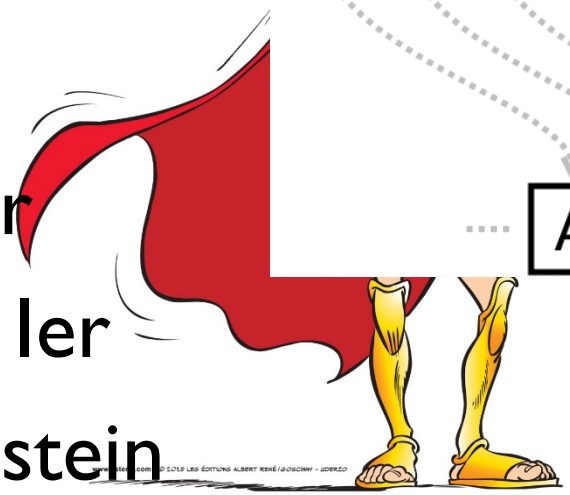
Passerelle

Switch

A propos de la sécurité…

Qui est connu pour avoir utilisé le 1er un système de cryptage basé sur une substitution mono-alphabétique ?

1. L'homme de Neandertal
2. Ramsès II
3. Jules César
4. Napoléon Ier
5. Albert Einstein
6. Alan Turing



Cryptage **symétrique**

Cryptage **asymétrique**

Protocole SSH (Secure SHell)

- Protocole pour la connexion à distance
  - Utilisation des deux mécanismes de chiffrement
    - Clés asymétriques
    - Clé symétrique
- Permet de se connecter à distance à une machine
  - Pour travailler (en ligne de commandes, bien sûr!!!)
  - Pour récupérer ou y déposer des documents
  - Pour éditer ses documents à distance
- La solution pour travailler depuis la maison sur ses documents restés à Polytech !

Université
Nice
Sophia Antipolis

Merci pour votre participation