Réseau informatique du collège
Synthèse

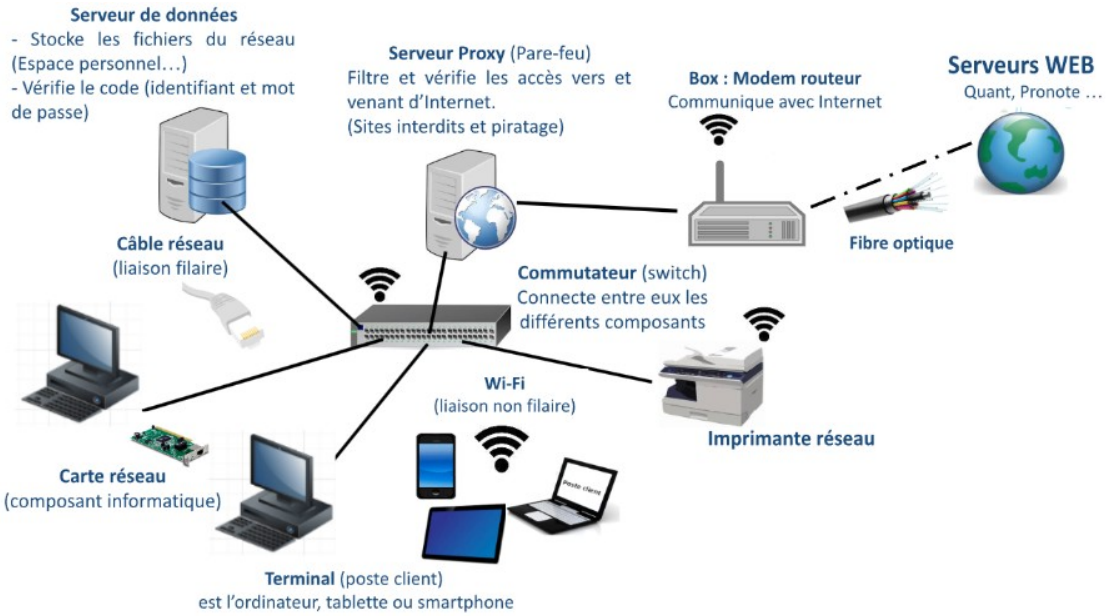
Le rôle d'un terminal, d'une carte réseau, des liaisons, d'un commutateur, d'un routeur, d'un serveur

Lorsqu'on se connecte au collège et qu'on surfe sur Internet, on utilise le réseau informatique.
Il existe deux types de réseaux informatiques :

- Réseau local (LAN) : C'est l'ensemble de composants connectés entre eux, dans un même lieu comme le collège ou la maison.
  Pour y accéder, il faut être présent dans ce lieu et avec un code d'accès.
- Réseau mondial (Internet) : C'est un immense réseau à travers le monde qui relie des milliards de réseaux locaux.

Un réseau informatique local est constitué de composants connectés entre eux dans un même lieu, comme le collège ou la maison.
Le réseau mondial (Internet) est un immense réseau qui relie des milliards de réseaux locaux.
Les réseaux informatiques permettent d'accéder à des informations, communiquer, partager …

On peut représenter le réseau informatique du collège avec un schéma simplifié comme celui-ci :

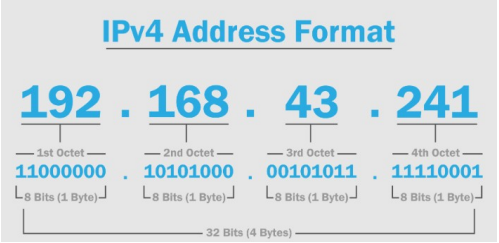


Un réseau informatique est constitué de différents composants : terminaux, cartes réseaux, commutateurs, serveurs, modem routeur. Il sont interconnectés avec le commutateur (Switch) pour partager des informations (fichiers) et des périphériques (imprimantes, …)
Ils sont reliés entre eux par des câbles (liaisons filaires) ou par des ondes Wi-Fi (liaisons non filaires).

Le rôle et la structure d'une adresse IP

Lorsque deux ordinateurs communiquent sur internet, c'est rendu possible car chacun a une adresse internet.

Pour envoyer et recevoir des informations, chaque appareil a besoin d'une adresse unique : c'est l'adresse IP.



Une adresse IP est le Numéro d'identification unique attribué à chaque appareil connecté à un réseau utilisant le protocole Internet (IP). Ce numéro est composé de quatre séries de chiffres compris entre 0 et 255, séparés par des points (IPv4).

- Une adresse IP privée est attribuée à un appareil au sein d'un réseau (LAN). Elle permet aux appareils de communiquer entre eux et d'accéder aux ressources du réseau, comme les imprimantes et les serveurs de fichiers.
- Une adresse IP publique est attribuée à un modem routeur (Box) par un fournisseur d'accès Internet (FAI). Elle permet aux appareils connectés au réseau local d'accéder à Internet et de communiquer avec d'autres appareils sur le Web.

L'adresse IP est l'identifiant unique d'un ordinateur qui lui permet de communiquer dans les réseaux informatiques. L'adresse IP publique d'un ordinateur lui permet de communiquer sur Internet. C'est le Fournisseur d'Accès Internet qui l'attribue à son client. L'adresse IP privée d'un ordinateur permet de l'identifier dans un réseau local.

Cyberviolence : usurpation d'identité, usage détourné

Lorsque l'on utilise Internet et les réseaux sociaux, on peut être confronté à la cyberviolence. Il est important de savoir ce qu'est la cyberviolence et comment s'en protéger.
La cyberviolence peut prendre plusieurs formes :

- Cyberviolence : Actes malveillants commis par le biais des technologies numériques, tels que les insultes, les menaces, le harcèlement ou la diffusion de photos ou vidéos privées.
- Usurpation d'identité : Utilisation de l'identité d'une autre personne sans son consentement pour commettre des actes malveillants.
- Usage détourné : Utilisation d'une image ou d'une information à des fins malveillantes, sans l'autorisation de la personne concernée.

Afin de mieux se protéger des cyberviolences, on peut :
- Ne pas répondre aux cyberviolences : ignorer les messages et les commentaires haineux.
- Conserver les preuves : sauvegarder les messages, les commentaires et les captures d'écran des cyberviolences.
- En parler à un adulte de confiance : parents, professeurs, éducateurs ou responsables associatifs.
- Signaler les cyberviolences : aux plateformes sur Internet et aux autorités.

La cyberviolence se manifeste par des actes malveillants tels que le harcèlement, la diffusion de contenus privés ou l'usurpation d'identité. Pour s'en protéger, il est important de ne pas répondre aux agressions, de conserver les preuves et d'en parler à un adulte de confiance. Il est également possible de signaler les cyberviolences aux plateformes concernées et aux autorités.

Cybersécurité : protection des données personnelles, traces numériques (témoins de connexion, géolocalisation), identification, authentification, respect de la propriété intellectuelle

Lorsque l'on navigue sur Internet, on laisse des traces numériques : une adresse IP, un historique de navigation des sites visités ou les recherches effectuées. Ces informations peuvent être utilisées pour tracer l'utilisateur, l'identifier, lui voler ses données personnelles…

La cybersécurité vise à se protéger contre ces dangers et à garantir la sécurité de nos données.

Il faut connaître les informations qui peuvent être ciblées par malveillance :

- Données personnelles : toutes les informations concernant l'utilisateur, comme le nom, l'adresse, le numéro de téléphone ou des photos privées.
- Traces numériques : informations laissées sur Internet, comme l'historique de navigation, les cookies ou les messages sur les réseaux sociaux.
- Géolocalisation : position géographique déterminée grâce aux GPS des smartphones ou aux adresses IP des ordinateurs.
- Identification : processus qui permet de déterminer l'identité d'une personne.
- Authentification : processus qui permet d'autoriser des accès à des ressources informatiques.
- Propriété intellectuelle : ensemble des droits qui protègent les créations intellectuelles, comme les inventions, les œuvres littéraires et artistiques ou les logiciels.

Pour se protéger des dangers et garantir la sécurité des informations, il convient de :

1. Protéger les données personnelles : Ne jamais donner d'informations personnelles à des inconnus, utiliser des mots de passe forts et uniques pour chaque compte, et activer l'authentification à deux facteurs.
2. Gérer les traces numériques : Supprimer régulièrement les cookies, utiliser un navigateur web privé pour les recherches et configurer les paramètres de confidentialité sur les réseaux sociaux.
3. Respecter la propriété intellectuelle : Ne pas copier ou télécharger illégalement du contenu protégé par des droits d'auteur, et toujours citer les sources que l'on utilise.

La cybersécurité est la pratique consistant à protéger les systèmes, les réseaux et les programmes contre les attaques numériques. Ces cyberattaques visent généralement à accéder à des informations sensibles, à les modifier ou à les détruire, à extorquer de l'argent aux utilisateurs. Il existe des moyens simples de se protéger, comme utiliser des mots de passe forts, gérer ses traces numériques et respecter la propriété intellectuelle.