**Le subnetting (division en sous-réseaux) (Brahim)**

**1. Qu’est-ce que le subnetting ?**

Le **subnetting**, ou sous-réseautage, est une technique permettant de diviser un réseau IP en sous-réseaux plus petits pour mieux gérer les adresses IP et optimiser les performances réseau.

* Chaque sous-réseau peut être configuré avec ses propres paramètres pour faciliter la gestion et améliorer la sécurité.
* Par exemple, les entreprises utilisent cette technique pour séparer les départements ou services (RH, comptabilité, etc.) et limiter les interactions non nécessaires.

**Avantages :**

* **Optimisation des adresses IP** :
  + Réduit le gaspillage en attribuant des plages adaptées aux besoins spécifiques.
  + Utile dans un contexte d’épuisement des adresses IPv4.
* **Segmentation des réseaux** :
  + Améliore la sécurité en isolant les sous-réseaux pour limiter les attaques et les pannes.
  + Réduit les collisions et le trafic inutile (broadcast).
* **Performance et administration** :
  + Optimise la bande passante et simplifie la gestion des ressources en divisant les réseaux complexes.

**2. Notation CIDR (Classless Inter-Domain Routing)**

Le CIDR est une méthode flexible pour représenter les plages d’adresses IP, utilisée à la place des anciennes classes d’adresses (A, B, C).

* **Structure** : Une adresse CIDR se compose de deux parties :
  1. Adresse réseau (ex. : 192.168.1.0).
  2. Masque de sous-réseau indiqué après une barre oblique (/24 pour 24 bits).

**Exemple : 192.168.1.0/24**

* **192.168.1.0** : Adresse réseau.
* **/24** : Masque de sous-réseau indiquant que les 24 premiers bits sont réservés pour le réseau.
* **Adresses disponibles** : 256 adresses totales, dont 254 utilisables pour les hôtes (192.168.1.1 à 192.168.1.254).

**3. Calculs de base**

**Calcul du masque de sous-réseau**

* Le masque de sous-réseau détermine les parties réseau et hôtes de l'adresse IP.
* **Exemple** :
  + Pour /24 :
    - Masque binaire : 11111111.11111111.11111111.00000000.
    - Masque décimal : 255.255.255.0.

**Déterminer les plages d’adresses disponibles**

* Pour une adresse 192.168.1.0/26 :
  + **Masque** : /26 (26 bits pour le réseau, 6 pour les hôtes).
  + **Nombre total d’adresses** : 26=642^6 = 6426=64.
  + **Plage disponible** :
    - Adresses assignables : 192.168.1.1 à 192.168.1.62.
    - Adresse réseau : 192.168.1.0.
    - Adresse de broadcast : 192.168.1.63.

**V. Les enjeux de l’adressage IP aujourd’hui (Brahim)**

**1. Pénurie d’IPv4 et solutions temporaires**

**NAT (Network Address Translation)**

* **Fonctionnement** : Permet à plusieurs appareils d’un réseau local de partager une seule adresse IP publique.
* **Avantages** :
  + Économise les adresses IPv4.
  + Améliore la sécurité en masquant les adresses privées.

**Utilisation accrue d’adresses privées**

* **Rôle** : Réduit la dépendance aux adresses publiques en utilisant des plages privées (192.168.x.x, 10.x.x.x).
* **Limite** : Les appareils privés nécessitent le NAT pour accéder à Internet.

**2. Sécurité liée aux adresses IP**

**Menaces :**

* **Usurpation d’adresse (IP Spoofing)** : Les attaquants falsifient des adresses IP pour contourner les restrictions ou lancer des attaques (DDoS).
* **Piratage** : Exploitation des vulnérabilités pour infiltrer des réseaux ou systèmes.

**Solutions :**

* **VPN** : Crée un tunnel sécurisé en chiffrant les données transmises.
* **Pare-feu** : Filtre le trafic et bloque les connexions suspectes.
* **Chiffrement** : Protège les données sensibles (ex. : HTTPS, IPsec).

**3. Transition vers IPv6**

### Freins :Le subnetting (division en sous-réseaux) (Brahim)

**1. Qu’est-ce que le subnetting ?**

Le **subnetting**, ou sous-réseautage, est une technique permettant de diviser un réseau IP en sous-réseaux plus petits pour mieux gérer les adresses IP et optimiser les performances réseau.

* Chaque sous-réseau peut être configuré avec ses propres paramètres pour faciliter la gestion et améliorer la sécurité.
* Par exemple, les entreprises utilisent cette technique pour séparer les départements ou services (RH, comptabilité, etc.) et limiter les interactions non nécessaires.

**Avantages :**

* **Optimisation des adresses IP** :
  + Réduit le gaspillage en attribuant des plages adaptées aux besoins spécifiques.
  + Utile dans un contexte d’épuisement des adresses IPv4.
* **Segmentation des réseaux** :
  + Améliore la sécurité en isolant les sous-réseaux pour limiter les attaques et les pannes.
  + Réduit les collisions et le trafic inutile (broadcast).
* **Performance et administration** :
  + Optimise la bande passante et simplifie la gestion des ressources en divisant les réseaux complexes.

**2. Notation CIDR (Classless Inter-Domain Routing)**

Le CIDR est une méthode flexible pour représenter les plages d’adresses IP, utilisée à la place des anciennes classes d’adresses (A, B, C).

* **Structure** : Une adresse CIDR se compose de deux parties :
  1. Adresse réseau (ex. : 192.168.1.0).
  2. Masque de sous-réseau indiqué après une barre oblique (/24 pour 24 bits).

**Exemple : 192.168.1.0/24**

* **192.168.1.0** : Adresse réseau.
* **/24** : Masque de sous-réseau indiquant que les 24 premiers bits sont réservés pour le réseau.
* **Adresses disponibles** : 256 adresses totales, dont 254 utilisables pour les hôtes (192.168.1.1 à 192.168.1.254).

**3. Calculs de base**

**Calcul du masque de sous-réseau**

* Le masque de sous-réseau détermine les parties réseau et hôtes de l'adresse IP.
* **Exemple** :
  + Pour /24 :
    - Masque binaire : 11111111.11111111.11111111.00000000.
    - Masque décimal : 255.255.255.0.

**Déterminer les plages d’adresses disponibles**

* Pour une adresse 192.168.1.0/26 :
  + **Masque** : /26 (26 bits pour le réseau, 6 pour les hôtes).
  + **Nombre total d’adresses** : 26=642^6 = 6426=64.
  + **Plage disponible** :
    - Adresses assignables : 192.168.1.1 à 192.168.1.62.
    - Adresse réseau : 192.168.1.0.
    - Adresse de broadcast : 192.168.1.63.

**V. Les enjeux de l’adressage IP aujourd’hui (Brahim)**

**1. Pénurie d’IPv4 et solutions temporaires**

**NAT (Network Address Translation)**

* **Fonctionnement** : Permet à plusieurs appareils d’un réseau local de partager une seule adresse IP publique.
* **Avantages** :
  + Économise les adresses IPv4.
  + Améliore la sécurité en masquant les adresses privées.

**Utilisation accrue d’adresses privées**

* **Rôle** : Réduit la dépendance aux adresses publiques en utilisant des plages privées (192.168.x.x, 10.x.x.x).
* **Limite** : Les appareils privés nécessitent le NAT pour accéder à Internet.

**2. Sécurité liée aux adresses IP**

**Menaces :**

* **Usurpation d’adresse (IP Spoofing)** : Les attaquants falsifient des adresses IP pour contourner les restrictions ou lancer des attaques (DDoS).
* **Piratage** : Exploitation des vulnérabilités pour infiltrer des réseaux ou systèmes.

**Solutions :**

* **VPN** : Crée un tunnel sécurisé en chiffrant les données transmises.
* **Pare-feu** : Filtre le trafic et bloque les connexions suspectes.
* **Chiffrement** : Protège les données sensibles (ex. : HTTPS, IPsec).

**3. Transition vers IPv6**

**Freins :**

* **Compatibilité** : Les appareils et logiciels existants nécessitent des mises à jour coûteuses.
* **Coûts** : L’adoption d’IPv6 implique des investissements en matériel et formation.

**Opportunités :**

* **IoT (Internet des Objets)** : IPv6 offre un espace suffisant pour connecter des milliards d’appareils.
* **Croissance des appareils connectés** : Permet à chaque appareil d’avoir une adresse publique unique, simplifiant les communications.
* **Sécurité renforcée** : Intègre IPsec pour une meilleure protection native.
* **Compatibilité** : Les appareils et logiciels existants nécessitent des mises à jour coûteuses.
* **Coûts** : L’adoption d’IPv6 implique des investissements en matériel et formation.

**Opportunités :**

* **IoT (Internet des Objets)** : IPv6 offre un espace suffisant pour connecter des milliards d’appareils.
* **Croissance des appareils connectés** : Permet à chaque appareil d’avoir une adresse publique unique, simplifiant les communications.
* **Sécurité renforcée** : Intègre IPsec pour une meilleure protection native.