Notions de réseau de base (ip v4).

Les classes

En IPv4, les adresses IP sont divisées en cinq classes : A, B, C, D et E. Chaque classe est définie par un certain nombre de bits dans l'adresse IP qui sont réservés pour l'identification du réseau (ou du sous-réseau) et du hôte.

Voici les différentes classes d'adresses IP en IPv4 :

- **Classe A** : Les adresses IP de classe A ont un premier octet compris entre 1 et 126. Le premier octet est réservé pour l'identification du réseau, et les trois derniers octets sont réservés pour l'identification du hôte. Le masque de sous-réseau par défaut est 255.0.0.0 (ou /8). Exemple : 10.0.0.1
- **Classe B** : Les adresses IP de classe B ont un premier octet compris entre 128 et 191. Les deux premiers octets sont réservés pour l'identification du réseau, et les deux derniers octets sont réservés pour l'identification du hôte. Le masque de sous-réseau par défaut est 255.255.0.0 (ou /16). Exemple : 172.16.0.1
- **Classe C** : Les adresses IP de classe C ont un premier octet compris entre 192 et 223. Les trois premiers octets sont réservés pour l'identification du réseau, et le dernier octet est réservé pour l'identification du hôte. Le masque de sous-réseau par défaut est 255.255.255.0 (ou /24). Exemple : 192.168.1.1
- **Classe D** : Les adresses IP de classe D sont réservées pour la multicasting. Elles ont un premier octet compris entre 224 et 239. Exemple : 224.0.0.1
- **Classe E** : Les adresses IP de classe E sont réservées pour une utilisation future. Elles ont un premier octet compris entre 240 et 254. Exemple : 240.0.0.1

Il est important de noter que ces classes d'adresses IP sont de moins en moins utilisées avec l'avènement de la technologie CIDR (Classless Inter-Domain Routing), qui permet de diviser les adresses IP en sous-réseaux de tailles variables.

Les pools d’adresses privées.

Les pools d'adresses réservées aux réseaux privés sont définis par la RFC 1918 (Request for Comments 1918) et sont les suivants :

- **10.0.0.0/8** : Cette plage d'adresses IP est réservée pour les réseaux privés et peut être utilisée pour les réseaux internes d'une entreprise ou d'une organisation.
- **172.16.0.0/12** : Cette plage d'adresses IP est également réservée pour les réseaux privés et peut être utilisée pour les réseaux internes d'une entreprise ou d'une organisation.
- **192.168.0.0/16** : Cette plage d'adresses IP est réservée pour les réseaux privés et est souvent utilisée pour les réseaux domestiques et les réseaux locaux.

Ces plages d'adresses IP sont considérées comme "privées" car elles ne sont pas routables sur Internet et ne peuvent pas être utilisées pour communiquer avec des hôtes situés en dehors du réseau privé. Elles sont généralement utilisées pour les réseaux internes d'une entreprise ou d'une organisation, et les adresses IP publiques sont utilisées pour communiquer avec Internet.

Il est important de noter que ces plages d'adresses IP ne sont pas attribuées par l'IANA (Internet Assigned Numbers Authority) et peuvent être utilisées librement par tout le monde. Cependant, il est recommandé de suivre les bonnes pratiques de configuration des réseaux privés pour éviter les conflits d'adresses IP.

Les adresses spécifiques

Les adresses spécifiques pour les différentes classes d'adresses IP :

- **Classe A** :
- Adresse de réseau : x.0.0.0 (où x est l'adresse de réseau)
- Adresse de broadcast : x.255.255.255
- Adresses de hôtes : x.y.z.w (où y, z et w sont les adresses de hôtes)

- **Classe B** :
- Adresse de réseau : x.y.0.0 (où x et y sont les adresses de réseau)
- Adresse de broadcast : x.y.255.255
- Adresses de hôtes : x.y.z.w (où z et w sont les adresses de hôtes)

- **Classe C** :
- Adresse de réseau : x.y.z.0 (où x, y et z sont les adresses de réseau)
- Adresse de broadcast : x.y.z.255
- Adresses de hôtes : x.y.z.w (où w est l'adresse de hôte)

En général, les adresses spécifiques suivantes ont des significations particulières dans un réseau :

- **Adresse de réseau** (ou adresse de sous-réseau) : c'est la première adresse du réseau, qui est utilisée pour identifier le réseau lui-même.
- **Adresse de broadcast** : c'est la dernière adresse du réseau, qui est utilisée pour envoyer des paquets de données à tous les hôtes du réseau.
- **Adresses de hôtes** : ce sont les adresses IP attribuées aux hôtes du réseau, qui sont utilisées pour communiquer avec les autres hôtes du réseau.

Il est important de noter que les adresses de réseau et de broadcast ne peuvent pas être attribuées à des hôtes spécifiques, car elles ont des significations particulières dans le réseau.

Exemples :

- Classe A : 10.0.0.0/8
- Adresse de réseau : 10.0.0.0
- Adresse de broadcast : 10.255.255.255
- Adresses de hôtes : 10.1.2.3, 10.4.5.6, etc.

- Classe B : 172.16.0.0/16
- Adresse de réseau : 172.16.0.0
- Adresse de broadcast : 172.16.255.255
- Adresses de hôtes : 172.16.1.2, 172.16.3.4, etc.

- Classe C : 192.168.1.0/24
- Adresse de réseau : 192.168.1.0
- Adresse de broadcast : 192.168.1.255
- Adresses de hôtes : 192.168.1.1, 192.168.1.2, etc.

Le broadcast

Une adresse de broadcast est une adresse IP spéciale qui est utilisée pour envoyer des paquets de données à tous les hôtes d'un réseau. Lorsqu'un hôte envoie un paquet à l'adresse de broadcast, il est reçu par tous les hôtes du réseau.

L'adresse de broadcast est généralement la dernière adresse du réseau, et elle est calculée en fonction du masque de sous-réseau. Par exemple, si le réseau est 192.168.1.0/24, l'adresse de broadcast est 192.168.1.255.

Lorsqu'un hôte envoie un paquet à l'adresse de broadcast, le paquet est diffusé à tous les hôtes du réseau, et chaque hôte reçoit une copie du paquet. Cela permet de réaliser des opérations telles que :

- La découverte de réseau : les hôtes peuvent envoyer des paquets de broadcast pour découvrir les autres hôtes du réseau.
- La mise à jour des tables de routage : les routeurs peuvent envoyer des paquets de broadcast pour mettre à jour les tables de routage des hôtes du réseau.
- La diffusion de données : les hôtes peuvent envoyer des paquets de broadcast pour diffuser des données à tous les hôtes du réseau.

Il est important de noter que les paquets de broadcast ne sont pas routés au-delà du réseau local, ce qui signifie qu'ils ne sont pas transmis à d'autres réseaux. Cela permet de limiter la diffusion des paquets de broadcast et de réduire la charge sur les réseaux.

Voici quelques exemples d'adresses de broadcast :

- 192.168.1.255 (pour le réseau 192.168.1.0/24)
- 10.0.0.255 (pour le réseau 10.0.0.0/8)
- 172.16.255.255 (pour le réseau 172.16.0.0/16)

Le multicast

Le multicast est une technique de transmission de données dans un réseau qui permet d'envoyer des paquets de données à un groupe de destinataires spécifiques, plutôt qu'à un seul destinataire ou à tous les hôtes du réseau.

Le multicast est souvent utilisé pour les applications qui nécessitent la transmission de données à plusieurs destinataires, tels que :

- La diffusion de vidéos ou d'audio en ligne
- La conférence en ligne
- La transmission de données de sécurité
- La mise à jour de logiciels

Le multicast fonctionne en utilisant des adresses IP spéciales, appelées adresses de multicast, qui sont réservées pour les transmissions de multicast. Ces adresses sont comprises entre 224.0.0.0 et 239.255.255.255.

Lorsqu'un hôte envoie un paquet de multicast, il est reçu par tous les hôtes du groupe de multicast qui ont souscrit à cette adresse de multicast. Les hôtes qui ne sont pas membres du groupe de multicast ne reçoivent pas le paquet.

Le multicast présente plusieurs avantages par rapport à la transmission de données unicast (c'est-à-dire la transmission de données à un seul destinataire) ou broadcast (c'est-à-dire la transmission de données à tous les hôtes du réseau) :

- Réduction de la charge sur le réseau : le multicast permet de réduire la charge sur le réseau en évitant de transmettre des paquets de données à des hôtes qui ne les demandent pas.
- Amélioration de la sécurité : le multicast permet de contrôler qui peut recevoir les paquets de données, ce qui améliore la sécurité du réseau.
- Flexibilité : le multicast permet de transmettre des paquets de données à un groupe de destinataires spécifiques, ce qui est utile pour les applications qui nécessitent la transmission de données à plusieurs destinataires.

Cependant, le multicast peut également présenter des défis, tels que :

- La configuration du réseau : le multicast nécessite une configuration spécifique du réseau pour fonctionner correctement.
- La gestion des adresses de multicast : les adresses de multicast doivent être gérées de manière à éviter les conflits et les erreurs de transmission.

Deux protocoles pour communiquer

TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) sont deux protocoles de communication utilisés pour transmettre des données sur Internet. Ils sont tous deux utilisés pour établir des connexions entre des hôtes, mais ils ont des différences fondamentales dans leur fonctionnement et leurs caractéristiques.

TCP (Transmission Control Protocol)

TCP est un protocole de communication orienté connexion, ce qui signifie qu'une connexion est établie entre les hôtes avant de transmettre des données. Voici quelques caractéristiques clés de TCP :

- Orienté connexion : une connexion est établie avant de transmettre des données.
- Garantie de livraison : TCP garantit que les données sont livrées dans l'ordre correct et sans erreurs.
- Contrôle de flux : TCP contrôle le flux de données pour éviter la saturation du réseau.
- Rétablissement de connexion : si la connexion est interrompue, TCP peut rétablir la connexion.
- Ordre des paquets : TCP garantit que les paquets sont livrés dans l'ordre correct.

TCP est utilisé pour les applications qui nécessitent une communication fiable et sécurisée, telles que :

- Les transferts de fichiers
- Les communications en ligne (par exemple, les messageries instantanées)
- Les transactions bancaires en ligne

UDP (User Datagram Protocol)

UDP est un protocole de communication sans connexion, ce qui signifie qu'aucune connexion n'est établie avant de transmettre des données. Voici quelques caractéristiques clés de UDP :

- Sans connexion : aucune connexion n'est établie avant de transmettre des données.
- Pas de garantie de livraison : UDP ne garantit pas que les données sont livrées dans l'ordre correct ou sans erreurs.
- Pas de contrôle de flux : UDP ne contrôle pas le flux de données.
- Pas de rétablissement de connexion : si la connexion est interrompue, UDP ne peut pas rétablir la connexion.
- Ordre des paquets : UDP ne garantit pas que les paquets sont livrés dans l'ordre correct.

UDP est utilisé pour les applications qui nécessitent une communication rapide et efficace, telles que :

- Les jeux en ligne
- Les vidéos en streaming
- Les communications en temps réel (par exemple, les appels téléphoniques en ligne)

Les ports de communication

Les ports de communication sont des numéros utilisés pour identifier les processus ou les applications qui communiquent sur un réseau. Ils sont utilisés pour diriger les paquets de données vers la bonne application ou le bon processus sur un hôte.

– Qu'est-ce qu'un port de communication ?

Un port de communication est un numéro compris entre 0 et 65535 qui est attribué à une application ou un processus sur un hôte. Lorsqu'un paquet de données est envoyé à un hôte, le port de communication est utilisé pour identifier la destination finale du paquet.

– Types de ports de communication

Il existe trois types de ports de communication :

- Ports bien connus (0-1023) : ces ports sont attribués à des applications ou des processus standard, tels que le serveur Web (port 80), le serveur FTP (port 21), etc.
- Ports registres (1024-49151) : ces ports sont attribués à des applications ou des processus qui nécessitent une connexion réseau, mais qui ne sont pas des applications standard.
- Ports dynamiques (49152-65535) : ces ports sont attribués dynamiquement à des applications ou des processus qui nécessitent une connexion réseau, mais qui ne sont pas des applications standard.

– Exemples de ports de communication

Voici quelques exemples de ports de communication couramment utilisés :

- Port 80 : serveur Web (HTTP)
- Port 21 : serveur FTP
- Port 22 : serveur SSH
- Port 25 : serveur SMTP (courrier électronique)
- Port 53 : serveur DNS
- Port 110 : serveur POP3 (courrier électronique)
- Port 143 : serveur IMAP (courrier électronique)

Comment les ports de communication fonctionnent-ils ?

Lorsqu'un paquet de données est envoyé à un hôte, le port de communication est utilisé pour identifier la destination finale du paquet. Voici les étapes suivies :

1. Le paquet de données est envoyé à l'adresse IP du hôte.
2. Le paquet de données est reçu par le hôte et est dirigé vers le port de communication spécifié.
3. Le processus ou l'application qui utilise le port de communication spécifié reçoit le paquet de données et le traite.