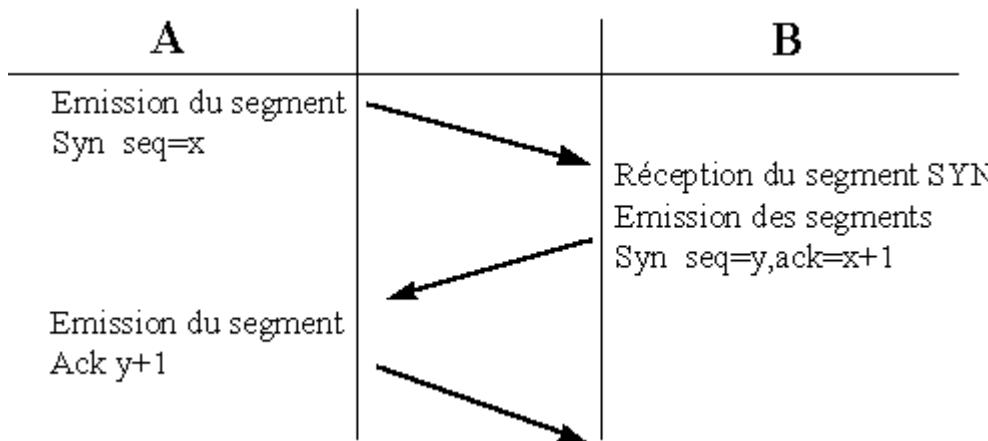


Notions de Base de TCP/IP v4

Etablissement de la connexion TCP



L'établissement de la connexion TCP entre deux stations A et B se fait en trois temps.

1. A émet une demande de connexion avec un message TCP dont le bit SYN est positionné, et dans lequel est fourni son numéro de séquence initial (x).
2. B retourne un message avec les bits SYN et ACK, en acquittant le numéro de séquence de A (x+1) et en fournissant son numéro de séquence initial(y).
3. A retourne un acquittement du numéro de séquence de B (y+1).

En-tête TCP

L'en-tête TCP est codée sur 4 octets soit 32 bits :

| 1er octet | 2ème octet | 3ème octet | 4 ème octet |
|-----------------------|------------|------------------|-------------|
| Port source | | Port destination | |
| Numéro de séquence | | | |
| Numéro d'acquittement | | | |
| Offset | Flags | | Fenêtre |
| Checksum | | Pointeur Urgent | |
| Options | | Padding | |
| Données | | | |

Vous noterez que les numéros de ports sont codés sur 16 bits. Cette information nous permet de calculer le nombres de ports maximum en IPv4, soit 2^{16} ports ou 65 535.

L'**Offset** contient la taille de l'en-tête.

Les **Flags** sont :

- URG - Si la valeur est 1 le pointeur urgent est utilisé. Le numéro de séquence et le pointeur urgent indique un octet spécifique.
- ACK - Si la valeur est 1, le paquet est un accusé de réception
- PSH - Si la valeur est 1, les données sont immédiatement présentées à l'application
- RST - Si la valeur est 1, la communication comporte un problème et la connexion est réinitialisée
- SYN - Si la valeur est 1, le paquet est un paquet de synchronisation
- FIN - Si la valeur est 1, le paquet indique la fin de la connexion

La **Fenêtre** est codée sur 16 bits. La Fenêtre est une donnée liée au fonctionnement d'expédition de données appelé le **sliding window** ou la **fenêtre glissante**. Puisque il serait impossible, pour des raisons de performance, d'attendre l'accusé de réception de chaque paquet envoyé, l'expéditeur envoie des paquets par groupe. La taille de cette groupe s'appelle la Fenêtre. Dans le cas d'un problème de réception d'une partie de la Fenêtre, toute la Fenêtre est ré-expédiée.

Le **Checksum** est une façon de calculer si le paquet est complet.

Le **Padding** est un champ pouvant être rempli de valeurs nulles de façon à ce que la taille de l'en-tête soit un multiple de 32

En-tête UDP

L'en-tête UDP est codée sur 4 octets soit 32 bits :

| 1er octet | 2ème octet | 3ème octet | 4 ème octet |
|-------------|------------|------------------|-------------|
| Port source | | Port destination | |
| longueur | | Checksum | |
| Données | | | |

L'en-tête UDP a une longueur de 8 octets.

Fragmentation et Ré-encapsulation

La taille limite d'un paquet TCP, l'en-tête comprise, ne peut pas dépasser **65 535 octets**. Cependant chaque réseau est qualifié par son MTU (Maximum Tranfer Unit). Cette valeur est la taille maximum d'un paquet autorisée. L'unité est en **octets**. Pour un réseau Ethernet sa valeur est de 1 500. Quand un paquet doit être expédié sur un réseau ayant un MTU inférieur à sa propre taille, le paquet doit être **fractionné**. A la sortie du réseau, le paquet est reconstitué. Cette reconstitution s'appelle **ré-encapsulation**.

Adressage

L'adressage IP requière que chaque périphérique sur le réseau possède une adresse IP unique de 4 octets, soit 32 bits au format XXX.XXX.XXX.XXX De cette façon le nombre total d'adresses est de $2^{32} = 4.3$ Milliards.

Les adresses IP sont divisées en 5 classes, de A à E. Les 4 octets des classes A à C sont divisés en deux, une partie qui s'appelle le **Net ID** qui identifie le réseau et une partie qui s'appelle le **Host ID** qui identifie le hôte :

| | 1er octet | 2ème octet | 3ème octet | 4 ème octet |
|---|-----------|------------|------------|-------------|
| A | Net ID | | Host ID | |
| B | Net ID | | Host ID | |

| | 1er octet | 2ème octet | 3ème octet | 4 ème octet |
|---|------------------|-------------------|-------------------|--------------------|
| C | | Net ID | | Host ID |
| D | | Multicast | | |
| E | | Réservé | | |

L'attribution d'une classe dépend du nombre de hôtes à connecter. Chaque classe est identifiée par un **Class ID** composé de 1 à 3 bits :

| Classe | Bits ID Classe | Valeur ID Classe | Bits ID Réseau | Nb. de Réseaux | Bits ID hôtes | Nb. d'adresses | Octet de Départ |
|---------------|-----------------------|-------------------------|-----------------------|-----------------------|----------------------|-----------------------|------------------------|
| A | 1 | 0 | 7 | $2^7=128$ | 24 | $2^{24}=16\ 777\ 216$ | 1 - 126 |
| B | 2 | 10 | 14 | $2^{14}=16\ 834$ | 16 | $2^{16}=65\ 535$ | 128 - 191 |
| C | 3 | 110 | 21 | $2^{21}=2\ 097\ 152$ | 8 | $2^8=256$ | 192 - 223 |

Dans chaque classe, certaines adresses sont réservées pour un usage privé :

| Classe | IP de Départ | IP de Fin |
|---------------|---------------------|------------------|
| A | 10.0.0.0 | 10.255.255.255 |
| B | 172.16.0.0 | 172.31.255.255 |
| C | 192.168.0.0 | 192.168.255.255 |

Il existe des adresses particulières ne pouvant pas être utilisées pour identifier un hôte :

| Adresse Particulière | Description |
|-------------------------------|--|
| 169.254.0.0 à 169.254.255.255 | Automatic Private IP Addressing de Microsoft |
| Hôte du réseau courant | Tous les bits du Net ID sont à 0 |
| Adresse de réseau | Tous les bits du Host ID sont à 0 |
| Adresse de diffusion | Tous les bits du Host ID sont à 1 |

L'adresse de réseau identifie le **segment** du réseau entier tandis que l'adresse de diffusion identifie tous les hôtes sur le segment de réseau.

Afin de mieux comprendre l'adresse de réseau et l'adresse de diffusion, prenons le cas de l'adresse 192.168.10.1 en classe C :

| | 1er octet | 2ème octet | 3ème octet | 4 ème octet |
|--|------------------|-------------------|-------------------|--------------------|
| | Net ID | | Host ID | |
| | | | | |

| | 1er octet | 2ème octet | 3ème octet | 4 ème octet |
|----------------------------------|------------------|-------------------|-------------------|--------------------|
| | Net ID | | | Host ID |
| Adresse IP | 192 | 168 | 10 | 1 |
| Binaire | 11000000 | 10101000 | 000001010 | 00000001 |
| Calcul de l'adresse de réseau | | | | |
| Binaire | 11000000 | 10101000 | 000001010 | 00000000 |
| Adresse réseau | 192 | 168 | 10 | 0 |
| Calcul de l'adresse de diffusion | | | | |
| Binaire | 11000000 | 10101000 | 000001010 | 11111111 |
| Adresse de diffusion | 192 | 168 | 10 | 255 |

Masques de sous-réseaux

Tout comme l'adresse IP, le masque de sous-réseau compte 4 octets ou 32 bits. Les masques de sous-réseaux permettent d'identifier le Net ID et le Host ID :

| Classe | Masque | Notation CIDR |
|---------------|---------------|----------------------|
| A | 255.0.0.0 | /8 |
| B | 255.255.0.0 | /16 |
| C | 255.255.255.0 | /24 |

Le terme **CIDR** veut dire **Classless InterDomain Routing**. Le terme Notation CIDR correspond au nombre de bits d'une valeur de 1 dans le masque de sous-réseau.

Quand un hôte souhaite émettre il procède d'abord à l'identification de sa propre adresse réseau par un calcul AND (ET) appliqué à sa propre adresse et son masque de sous-réseau qui stipule :

- $1 + 1 = 1$
- $0 + 1 = 0$
- $1 + 0 = 0$
- $0 + 0 = 0$

Prenons le cas de l'adresse IP 192.168.10.1 ayant un masque de 255.255.255.0 :

| | 1er octet | 2ème octet | 3ème octet | 4 ème octet |
|-----------------------|------------------|-------------------|-------------------|--------------------|
| Adresse IP | 192 | 168 | 10 | 1 |
| Binaire | 110000000 | 10101000 | 00001010 | 00000001 |
| Masque de sous-réseau | | | | |
| Binaire | 11111111 | 11111111 | 11111111 | 00000000 |
| Calcul AND | 110000000 | 10101000 | 00001010 | 00000000 |
| Adresse réseau | 192 | 168 | 10 | 0 |

Cet hôte essaie de communiquer avec un hôte ayant une adresse IP de 192.168.10.10. Il procède donc au même calcul en appliquant **son propre masque de sous-réseau** à l'adresse IP de l'hôte destinataire :

| | 1er octet | 2ème octet | 3ème octet | 4 ème octet |
|-----------------------|------------------|-------------------|-------------------|--------------------|
| Adresse IP | 192 | 168 | 10 | 10 |
| Binaire | 110000000 | 10101000 | 00001010 | 00001010 |
| Masque de sous-réseau | | | | |
| Binaire | 11111111 | 11111111 | 11111111 | 00000000 |
| Calcul AND | 110000000 | 10101000 | 00001010 | 00000000 |
| Adresse réseau | 192 | 168 | 10 | 0 |

Puisque l'adresse réseau est identique dans les deux cas, l'hôte émetteur présume que l'hôte de destination se trouve sur son réseau et envoie les paquets directement sur le réseau sans s'adresser à sa passerelle par défaut.

L'hôte émetteur essaie maintenant de communiquer avec avec un hôte ayant une adresse IP de 192.168.2.1. Il procède donc au même calcul en appliquant **son propre masque de sous-réseau** à l'adresse IP de l'hôte destinataire :

| | 1er octet | 2ème octet | 3ème octet | 4 ème octet |
|-----------------------|------------------|-------------------|-------------------|--------------------|
| Adresse IP | 192 | 168 | 2 | 1 |
| Binaire | 110000000 | 10101000 | 00000010 | 00000001 |
| Masque de sous-réseau | | | | |
| Binaire | 11111111 | 11111111 | 11111111 | 00000000 |
| Calcul AND | 110000000 | 10101000 | 00000010 | 00000000 |

| | 1er octet | 2ème octet | 3ème octet | 4 ème octet |
|----------------|------------------|-------------------|-------------------|--------------------|
| Adresse réseau | 192 | 168 | 2 | 0 |

Dans ce cas, l'hôte émetteur constate que le réseau de destination 192.168.2.0 n'est pas identique à son propre réseau 192.168.10.0. Il adresse donc les paquets à la passerelle par défaut.

VLSM

Puisque le stock de réseaux disponibles sous IPv4 est presque épuisé, une solution a du être trouvée pour créer des sous-réseaux en attendant l'introduction de l'IPv6. Cette solution s'appelle le VLSM ou Variable Length Subnet Masks. Le VLSM exprime les masques de sous-réseaux au format CIDR.

Son principe est simple. Afin de créer des réseaux différents à partir d'une adresse réseau d'une classe donnée, il convient de réduire le nombre d'hôtes. De cette façon les bits 'libérés' du Host ID peuvent être utilisés pour identifier les sous-réseaux.

Pour illustrer ceci, prenons l'exemple d'un réseau 192.168.1.0. Sur ce réseau, nous pouvons mettre $2^8 - 2$ soit 254 hôtes entre 192.168.1.1 au 192.168.1.254.

Supposons que nous souhaiterions diviser notre réseau en 2 sous-réseaux. Pour coder 2 sous-réseaux, il faut que l'on libère 2 bits du Host ID. Les deux bits libérés auront les valeurs binaires suivantes :

- 00
- 01
- 10
- 11

Les valeurs binaires du quatrième octet de nos adresses de sous-réseaux seront donc :

- 192.168.1.00XXXXXX
- 192.168.1.01XXXXXX
- 192.168.1.10XXXXXX
- 192.168.1.11XXXXXX

où les XXXXXX représentent les bits que nous réservons pour décrire les hôtes dans chacun des sous-réseaux.

Nous ne pouvons pas utiliser les deux sous-réseaux suivants :

- 192.168.1.00XXXXXX
- 192.168.1.11XXXXXX

car ceux-ci correspondent aux débuts de l'adresse réseau 192.168.1.0 et de l'adresse de diffusion 192.168.1.255.

Nous pouvons utiliser les deux sous-réseaux suivants :

- 192.168.1.01XXXXXX
- 192.168.1.10XXXXXX

Pour le premier sous-réseau l'adresse réseau et l'adresse de diffusion sont :

| | | | | |
|----------------------------------|----------|----------|----------|------------------|
| Sous-réseau #1 | 192 | 168 | 1 | 01XXXXXX |
| Calcul de l'adresse de réseau | | | | |
| Binaire | 11000000 | 10101000 | 00000001 | 01 000000 |
| Adresse réseau | 192 | 168 | 1 | 64 |
| Calcul de l'adresse de diffusion | | | | |
| Binaire | 11000000 | 10101000 | 00000001 | 01 111111 |
| Adresse de diffusion | 192 | 168 | 1 | 127 |

- L'adresse CIDR du réseau est donc 192.168.1.64/26 car le Net ID est codé sur 24+2 bits.
- Le masque de sous-réseau est donc le 11111111.11111111.11111111.11000000 ou le 255.255.255.192
- Nous pouvons avoir 2^6 -2 soit 62 hôtes.
- La plage valide d'adresses IP est de 192.168.1.65 à 192.168.1.126

Pour le deuxième sous-réseau l'adresse réseau et l'adresse de diffusion sont :

| | | | | |
|-------------------------------|-----|-----|---|----------|
| Sous-réseau #2 | 192 | 168 | 1 | 10XXXXXX |
| Calcul de l'adresse de réseau | | | | |

| | | | | |
|----------------------------------|----------|----------|----------|-----------------|
| Binaire | 11000000 | 10101000 | 00000001 | 10000000 |
| Adresse réseau | 192 | 168 | 1 | 128 |
| Calcul de l'adresse de diffusion | | | | |
| Binaire | 11000000 | 10101000 | 00000001 | 10111111 |
| Adresse de diffusion | 192 | 168 | 1 | 191 |

- L'adresse CIDR du réseau est donc 192.168.1.128/26 car le Net ID est codé sur 24+2 bits.
- Le masque de sous-réseau est donc le 11111111.11111111.11111111.11000000 ou le 255.255.255.192
- Nous pouvons avoir $2^6 - 2$ soit 62 hôtes.
- La plage valide d'adresses IP est de 192.168.1.129 à 192.168.1.190

La valeur qui sépare les sous-réseaux est 64. Cette valeur comporte le nom **incrément**.

Ports et sockets

Afin que les données arrivent aux applications qui les attendent, TCP utilise des numéros de ports sur la couche transport. Le numéros de ports sont divisés en trois groupes :

- **Well Known Ports**
 - De 1 à 1023
- **Registered Ports**
 - De 1024 à 49151
- **Dynamic et/ou Private Ports**
 - De 49152 à 65535

Le couple **numéro IP:numéro de port** s'appelle un **socket**.

est mise à disposition selon les termes de la Licence Creative Commons Attribution - Pas d'Utilisation Commerciale - Pas de Modification 3.0 France. </center> </html>

From:

<https://www.ittraining.team/> - **www.ittraining.team**

Permanent link:

<https://www.ittraining.team/doku.php?id=elearning:workbooks:cisco:01:intro:c102>

Last update: **2020/01/30 03:28**

