# Fiches de révision
# Examen : 100-101 ICND1
# Certification : Cisco CCENT



Par Cyril
Certifié CCIE et auteur du site reussirsonccna.fr

# A lire – Avertissement

Ce guide ne peut être utilisé que pour un usage privé uniquement.

Vous n'avez pas le droit de l'offrir ni de le revendre sans accord des auteurs. Toutes reproductions, partielles ou totales, sous quelque forme et procédé que ce soit sont interdites conformément à l'article L.122-4 du Code de la Propriété Intellectuelle.

Toute personne procédant à une utilisation du contenu de ce guide, sans une autorisation expresse et écrite de l'auteur, encourt une peine relative au délit de contrefaçon détaillée à partir de l'article L 335-2 du même Code.

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans autorisation de l'Éditeur ou du Centre Français d'Exploitation du Droit de copie, 20, rue des Grands-Augustins, 75006 Paris.

# A lire – Notice légale

L'auteur s'est efforcé d'être aussi précis et complet que possible lors de la création de cet ouvrage, et malgré ceci, il ne peut en aucun cas garantir ou représenter le contenu de cet ouvrage dû à l'évolution et la mutation rapide et constante de la technologie.

Bien que tout ait été fait afin de vérifier les informations contenues dans cet ouvrage, l'auteur n'assume aucune responsabilité concernant des erreurs, des omissions, une interprétation ou une compréhension contraire du sujet développé.

# Sommaire


| | |
|---|---|
| Introduction | 4 |
| Qui suis-je ? | 4 |
| Tout savoir sur le CCENT et CCNA | 5 |
| Qu'est-ce que le CCENT et le CCNA? | 6 |
| Comment se passe l'examen le jour J ? | 7 |
| **Inscription et déroulement de l'examen** | 7 |
| Quels sont les types de questions ? | 7 |
| Quel score atteindre pour être certifié(e) ? | 8 |
| **Détail de l'examen ICND1** | 8 |
| Quels sont les prérequis pour la certification ? | 8 |
| Mes 9 conseils avant et pendant l'examen | 9 |
| **Avant le jour J** | 9 |
| **Le jour J** | 11 |
| Fiches résumé | 12 |
| Introduction | 13 |
| Théorie de la commutation | 17 |
| Théorie du routage IPv4 | 33 |
| Implémentation du routage IPv4 | 51 |
| Théorie du routage IPv6 | 63 |
| Implémentation du routage IPv6 | 68 |
| Filtrage et NAT | 78 |
| Comment optimiser sa mémoire? | 90 |
| **Flashcard** | 90 |
| **Projet MNEMOSYNE** | 90 |

# Introduction



## Qui suis-je ?

Bonjour je m'appelle Cyril.

Travaillant depuis des années dans le domaine de **l'architecture, l'expertise réseau et la formation**, je souhaite aider et accompagner les personnes vers l'obtention des certifications Cisco. J'ai créé ce guide car beaucoup de personnes ont demandé mon aide afin de comprendre les certifications Cisco CCENT et Cisco CCNA.

Il faut savoir qu'une simple formation Cisco de 5 jours coûte **entre 2000 et 3500€ hors taxe !** Quand votre entreprise vous refuse cette formation, peu de personnes peuvent se permettre de la financer sur ses propres deniers.

En partant de cet état de fait et étant certifié CCIE et CCSI (instructeur officiel Cisco), mon but à très court terme est que vous puissiez poser la première pierre de l'édifice, c'est-à-dire le CCENT puis le CCNA.

Pour plus d'informations sur la pyramide des certifications, je vous invite à faire un tour sur le site de Cisco en cliquant ici.

Je vous souhaite une excellente lecture et n'hésitez pas à vous rendre sur le site http://reussirsonccna.fr ou à me contacter directement sur cyril@reussirsonccna.fr.
Votre réussite est mon objectif !

# Tout savoir sur le CCENT et CCNA

Si vous ne l'avez pas déjà téléchargé, je propose un guide totalement gratuit sur tout ce qu'il faut savoir sur le CCENT et le CCNA. Ce guide est téléchargeable sur le site http://reussirsonccna.fr

Vous y découvrirez les points suivants :

## Comment choisir son cursus ?

- Est-ce que le CCENT ou CCNA est suffisant?
- Quelle est la différence entre le CCNA académique vs CCNA Professionnel ?
- Comment s'inscrire à l'examen ?
- Comment se passe l'examen le jour J ? (inclus dans ce présent document)
- Quels sont les types de questions ? (inclus dans ce présent document)
- Comment optimiser sa mémoire? (inclus dans ce présent document)
- Comment pratiquer les labs ?
- Comment monter son propre lab Cisco ?
- Quel score atteindre pour être certifié(e) ? (inclus dans ce présent document)
- Quels sont les prérequis pour la certification ? (inclus dans ce présent document)
- Où puis-je trouver des livres de révision ? (inclus dans ce présent document)
- Mes 9 conseils avant et pendant l'examen (inclus dans ce présent document)
- Retour d'expérience de Fréderic
- Retour d'expérience de Remi
- Syllabus ICND 1 – 100-101 (inclus dans ce présent document)
- Syllabus ICND2 – 200-101
- Syllabus CCNA (ICND1 + ICND2) – 200-120
- Les blogs Cisco

# Qu'est-ce que le CCENT et le CCNA?

La certification CCNA – Cisco Certified Network Associate est à ce jour la plus connue et **la plus demandée** dans le monde des réseaux informatiques.

La certification CCENT – Cisco Certified Entry Networking Technician est moins connue car plus récente, elle se situe en amont du CCNA.

Selon le site Cisco, ces deux certifications permettent de valider la capacité à installer, opérer et dépanner un réseau informatique pour TPE et PME.

A mon sens, elles permettent surtout de certifier une base de connaissances relativement large, passant de la couche physique (câble cuivre, fibre optique…), aux protocoles niveau 2 (arp, vtp, stp…), aux protocoles de routage (rip, eigrp, ospf…), pour finir sur les protocoles applicatifs (http, ftp, smtp…).

Dans ma carrière de formateur, j'ai été très surpris sur le nombre de personnes qui ont échoué à ces examens pensant qu'ils maitrisaient leur sujet malgré plus de 20 ans d'expérience. Surpris aussi de la mauvaise compréhension des protocoles parce que souvent c'est plug and play, "on branche et ça fonctionne", oui mais pourquoi?

**Alors, pourquoi autant d'échecs au CCNA?**

Parce que la quantité d'information à connaitre est gigantesque. En effet, rien que les livres officiels qui traitent de la théorie font plus de 1000 pages et il y en a deux ! L'un est dédié à la théorie ICND1 et l'un autre à la théorie ICND2. Et il faut connaitre les deux (ICND1 + ICND2) afin  lors de l'examen CCNA.

Certains diront qu'il suffit juste de réviser des examens blancs pour réussir le jour J. Oui c'est possible, mais dans certains cas ce n'est pas suffisant. Cependant, est-ce vraiment ce que vous voulez? Etre certifié CCNA pour ensuite être décrédibilisé en entretien technique? La certification est certes un plus sur son CV mais l'entretien technique reste l'unique façon de vérifier que vous êtes à la hauteur.

C'est pour cela que Cisco a créé un examen intermédiaire, le CCENT, qui permet d'être certifié juste en passant la première théorie ICND1. Une fois cet examen réussi, vous serez certifié Cisco CCENT.
Une fois le CCENT réussi, il ne reste plus qu'à réviser et à passer la théorie ICND2 pour être certifié CCNA. C'est tout de même plus simple que de passer les théories ICND1+ICND2 lors d'un même et unique examen, non ?

Ce livre est destiné à vous donner toutes les billes en main pour réussir votre CCENT pour ensuite continuer avec le CCNA.



## Inscription et déroulement de l'examen

La certification est **valide pour une durée de 3 ans**. Une fois ce délai passé, il faut repasser l'examen afin de prolonger la certification . Mais la plupart des personnes ne s'arrêtent pas au CCNA, ils continuent sur les certifications suivantes. L'avantage est que toute réussite à un examen supérieur revalide le CCNA pour 3 ans supplémentaires. Sympa !

L'examen CCNA dure **2h pour 45 à 55 questions** sous forme de QCM et de simulation de lab (configurer un switch par exemple). Si vous n'êtes pas anglophone, vous aurez droit à **30 minutes supplémentaires** car ce n'est pas votre langue natale.

Les QCM peuvent se présenter sous les formes suivantes:

- choix unique
- choix multiple (dans ce cas, on vous précise le nombre de réponses souhaitées, 2, 3 ou 4)
- drag & drop (ou glisser-déposer). Permet de faire le lien entre 2 tableaux par exemple
- remise des éléments dans l'ordre
- ...

Les labs sont généralement un accès en console à un ou plusieurs équipements avec un choix limité de commandes (n'oublions pas que c'est un simulateur logiciel et non de vrais équipements). Ne vous étonnez pas si en tapant une commande, vous avez un message d'erreur vous signifiant que la commande est inconnue. Elle existe bien mais vous n'en avez pas besoin pour résoudre l'exercice. Les commandes de complétion (via la touche Tabulation) et d'aide (via la touche ?) ne sont pas disponibles lors des labs, c'est voulu. Cisco souhaite que les gens connaissent par cœur les commandes principales.

L'examen est mélangé de questions de type QCM et de labs donc tout est possible: commencer directement avec un lab de configuration ou avec une question QCM.

**Remarque importante:** vous n'avez pas le droit d'amener des notes, votre téléphone ou votre ordinateur portable. On vous fournit un stylo et un papier plastifié que vous remettrez à la fin de l'examen.

## Quels sont les types de questions ?

On est jamais mieux servi que par soi-même et Cisco l'a bien compris : Cisco propose une simulation pour vous montrer visuellement comment se passe l'examen et le style de question sur lesquelles vous pouvez tomber. Je le trouve très bien fait, alors autant en profiter. Pour voir cette animation, **cliquez ICI !**

Si le lien ne fonctionne pas, tapez ces mots clés dans Google pour récupérer le lien a jour : **cisco CCNA tutorial swf**

## Quel score atteindre pour être certifié(e) ?

La question qui revient souvent via les blogs, forum et discussion lors des formations est la suivante:

**Quel score faut-il pour être certifié(e) CCENT ou CCNA ?**

C'est une excellente question et le plus amusant (ou stressant) est qu'il n'y a **pas de score précis** à avoir lors des examens Cisco car cela dépend essentiellement des questions proposées lors de l'examen.

Cisco a une base de données **gigantesque** de questions et pioche dedans pour l'examen. En fonction des questions piochées et de leur **pondération**, le score final requis est **différent**. C'est aussi pour cela que votre voisin d'examen n'aura pas du tout les mêmes questions.

Si on regarde sur le site officiel de Cisco, les informations suivantes sont mentionnées (traduites de l'anglais):

### Détail de l'examen ICND1

- **Nombre de questions:** 40-50
- **Types de question:** choix multiple avec une seule ou plusieurs bonnes réponses, glisser/déposer, simulateur de lab contenant de la configuration (configure terminal) ou de la vérification de configuration (à base de commande show), des valeurs à entrer (par exemple donner une adresse IP)
- **Score à obtenir:** varie selon les questions proposées lors de l'examen mais c'est entre 800 et 850 sur 1000
- **Durée:** 90 minutes + 30 minutes pour les non-anglophones

### Détail de l'examen ICND2

- **Nombre de questions:** 50-60
- **Types de question:** choix multiple avec une seule ou plusieurs bonnes réponses, glisser/déposer, simulateur de lab contenant de la configuration (configure terminal), de la vérification (à base de commande show), des valeurs à entrer (par exemple donner une adresse IP)
- **Score à obtenir:** varie selon les questions proposées lors de l'examen mais c'est entre 800 et 850 sur 1000
- **Durée:** 75 minutes + 30 minutes pour les non-anglophones

**Quels sont les prérequis pour la certification ?**

Il n'y a pas de prérequis pour passer le CCENT ou le CCNA, que ce soit bien clair.

Ah si ! Il y en a un et de taille : savoir utiliser un ordinateur...

## Mes 9 conseils avant et pendant l'examen

Une demande revient **régulièrement** par email sur les conseils à savoir pendant les révisions et lors du jour « J » afin de limiter la casse et optimiser au mieux le rendement de ses capacités intellectuelles.

Alors je vous arrête tout de suite, je ne vais pas vous recommander tel ou tel médicament plus ou moins douteux que l'on trouve sur Internet et curieusement non autorisé en France et d'autres pays. Voici une petite **liste** non exhaustive de conseils sur votre préparation à l'examen.

### Avant le jour J

Avant le jour de l'examen, on se dit toujours qu'on pensera au jour « J » plus tard. Ce qui en soit est une bonne idée pour ne pas **rajouter du stress** pendant les révisions surtout si vous êtes dans un chapitre assez compliqué, comme le résumé de route par exemple.

Cependant, voici quelques conseils sur la préparation avant le jour J de l'examen qui sont importants à mes yeux:



**1.** **Pas la peine de réviser 12h par jour**, cela ne sert à rien sur le long terme. Ce mode de révision intense sert uniquement pour la dernière ligne droite. Par exemple la dernière semaine, c'est là où vous pouvez stimuler votre cerveau pour rafraîchir des chapitres vu il y a bien longtemps. Donc **révisez de manière modérée**, sans acharnement mais dans la continuité et la durée (pas la peine de me demander si 10 minutes par jour sont suffisantes… il vous faudra des années pour tout assimiler et le CCNA aura déjà changé plusieurs fois de version).

**2.** **Dormez… et dormez bien**. Conseil banal mais oh! combien important. Ne faites pas du Yo-Yo avec votre sommeil, c'est à dire un jour vous vous couchez à 21h et un autre jour à 3h du matin, surtout lors de la dernière semaine. Un sommeil long et constant est surement une des clés du succès  Si vous ne me croyez pas, **faites le test suivant**: après une nuit courte, chronométrez-vous sur 10 questions en calcul binaire. Faites le même test après une nuit normale… vous constaterez la différence sur le temps que votre cerveau a mis et sur le taux de bonnes réponses.

**3.** **Rafraîchissez votre mémoire pendant vos révisions**, pas à la fin. Il est impératif que **régulièrement** vous consacriez du temps à revoir **les fiches résumés de ce livre**.

**4.** **sortez !** oui sortez, voyez vos amis, aller au bar, au ciné, faites du sport… faites une activité régulière qui permet à votre cerveau de **décompresser**! Le sport est une très bonne activité pour "décrocher" mentalement et physiquement.

Voyons maintenant un peu les conseils pour le jour J...



**Voici quelques conseils pour que vous soyez dans les meilleures conditions le jour de l'examen:**

5. Il faut arriver bien **en avance** au centre de certification. Arriver pile à l'heure ou en retard est une source de stress des plus horribles et vous mettrez facilement **20 minutes** à faire redescendre la pression. Profitez-en aussi pour aller aux toilettes (oui Papa j'y vais !)

6. Prenez **2 pièces d'identités** avec vous (carte d'identité, passeport, permis de conduire...). Certains centres demandent 2 pièces d'identité et ils ne plaisantent pas.

7. Asseyez-vous devant l'écran de l'ordinateur et mettez-vous dans la tête que **votre objectif** n'est pas d'avoir le CCNA mais de l'avoir avec le meilleure score ! **Échouer n'est pas une option !**

8. La première fois qu'on passe un examen Cisco, on ne fait pas attention mais les **10 premières minutes** sont dédiées à un **tutoriel** qui explique le déroulement de l'examen. Prenez votre temps pour bien comprendre car ce temps **n'est pas décompté** de l'examen. Les indications sont très importantes surtout pour les TP car les écrans d'énoncé, d'accès à la console CLI et de réponse ne sont pas forcément au même endroit !

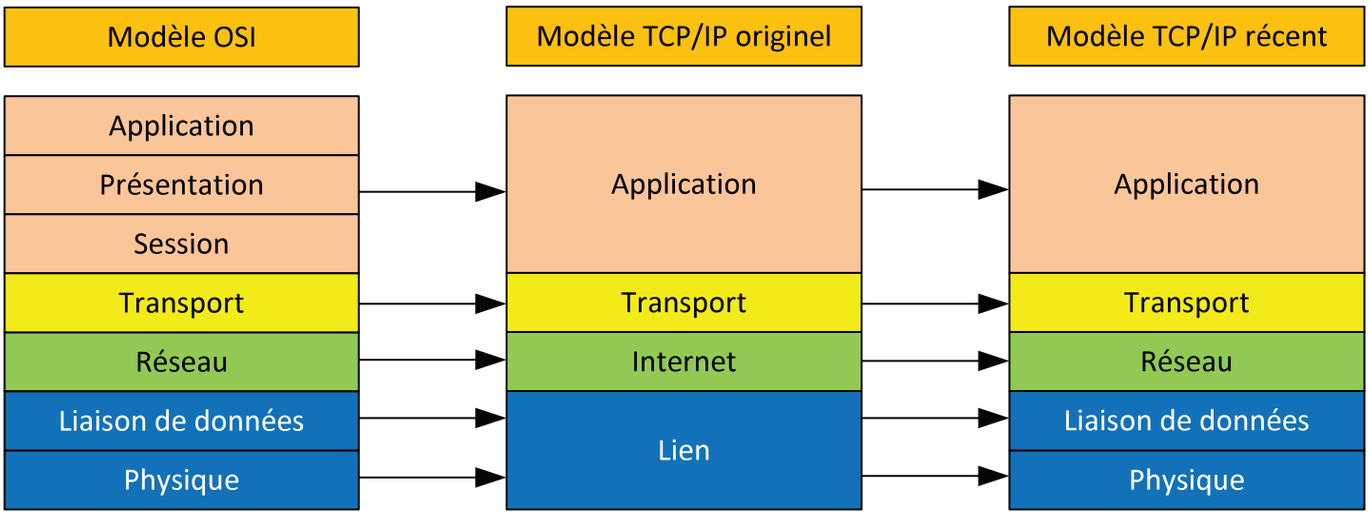
9. Dernière chose: une fois la question validée, **vous ne pouvez plus revenir en arrière**, contrairement à d'autres examens. Donc avant de cliquer sur SUIVANT, relisez rapidement une dernière fois votre réponse.

Les fiches résumés sont découpés 5 grands domaines: la commutation, le routage IPv4 , le routage IPv6 et le filtrage.

| 5 domaines | Sous-domaine |
|---|---|
| La communication | théorie de la communication |
| | Implémentation de la communication |
| Le routage IPv4 | Théorie du routage IPv4 |
| | Implémentation du routage IPv4 |
| Le routage IPv6 | Théorie du routage IPv6 |
| | Implémentation du routage IPv6 |
| Le filtrage | Filtrage et NAT |

# INTRODUCTION

# Modèles OSI et TCP/IP




## Les fondamentaux

- Un réseau est l'ensemble des composants utilisés pour faire communiquer deux ou plusieurs ordinateurs.
- Le média de communication est utilisé pour transmettre les données de A vers B et inversement.
- Les premiers réseaux étaient propriétaires et utilisaient des protocoles propriétaires comme SNA d'IBM ou DECnet.
- À la fin des années 1990, la plupart des réseaux utilisaient le modèle TCP/IP pour communiquer, qui est une suite de protocoles libres et standards.

Le modèle Open Systems Interconnection (OSI) a été défini dans les années 90 comme la première suite de protocoles de communication réseau. Il était développé par l'International Organization for Standardization (ISO). Le département USA de la défense a créé son propre modèle, aujourd'hui appelé TCP/IP. Très similaire au modèle OSI, il consolide les 3 couches hautes en une seule couche appelée "Application". Les deux modèles restent identiques pour les 4 couches basses. Une version originelle de TCP/IP agrégeait les 2 couches basses en une seule. Bien que la plupart des équipements aujourd'hui n'utilisent pas le modèle OSI, celui-ci reste la référence

| Couche TCP/IP | Exemple de protocoles |
|---|---|
| Application | HTTP, HTTPS, POP3, SNMP |
| Transport | TCP/UDP |
| Internet | IP, RIP, OSPF, EIGRP, BGP |
| Liaison de données | Ethernet, PPP, HDLC, Wireless |
| Physique | 802.3, 802.11, E1, STM1 |

| Ports connus | |
|---|---|
| HTTP | 80 |
| HTTPS | 443 |
| SSH | 22 |
| FTP | 21 |
| Telnet | 23 |

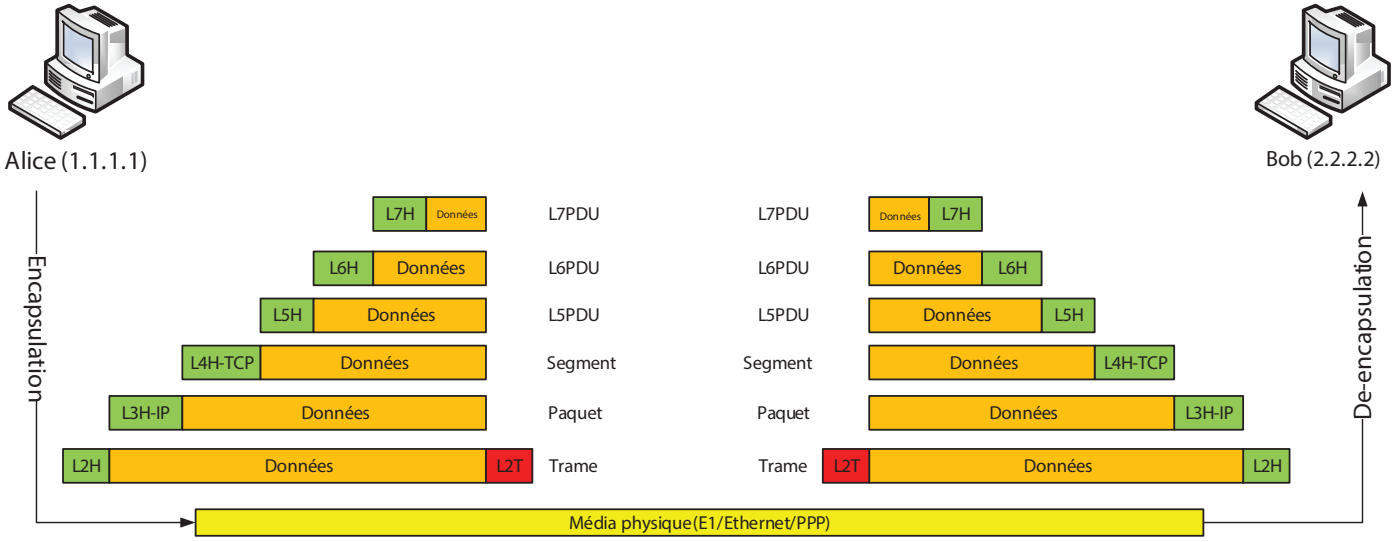
## Points importants à retenir :

- Interaction couche similaire : Deux équipements utilisent les mêmes règles pour échanger des données. Exemple : les routeurs utilisent des protocoles de couche 3 pour échanger leur table de routage.
- Interaction couche adjacente : Au sein d'un équipement, le protocole d'une couche récupère la donnée de la couche supérieure (ou inférieure) puis ajoute (ou supprime) l'entête définissant ses propriétés de protocole.
- Se souvenir des 5 étapes pour envoyer des données sur un réseau TCP/IP : 1/données - 2/entête TCP - 3/entête IP - 4/entête Ethernet - 5/envoi des bits.
- Le modelage d'un réseau par couche a les avantages suivants: Moins complexe, interface standard, facile à comprendre, facile à développer, interopérabilité et ingénierie modulaire.
- Connaitre les bases du routage IP et les modèles OSI et TCP/IP

# L'encapsulation TCP/IP

Alice Veut envoyer à Bob une requête HTTP GET.
Quand Bob reçoit la requête HTTP GET, il répond avec un HTTP OK.

Cet exemple illustre comment la donnée est encapsulée, transmis puis décapsulée




## Encapsulation de la donnée

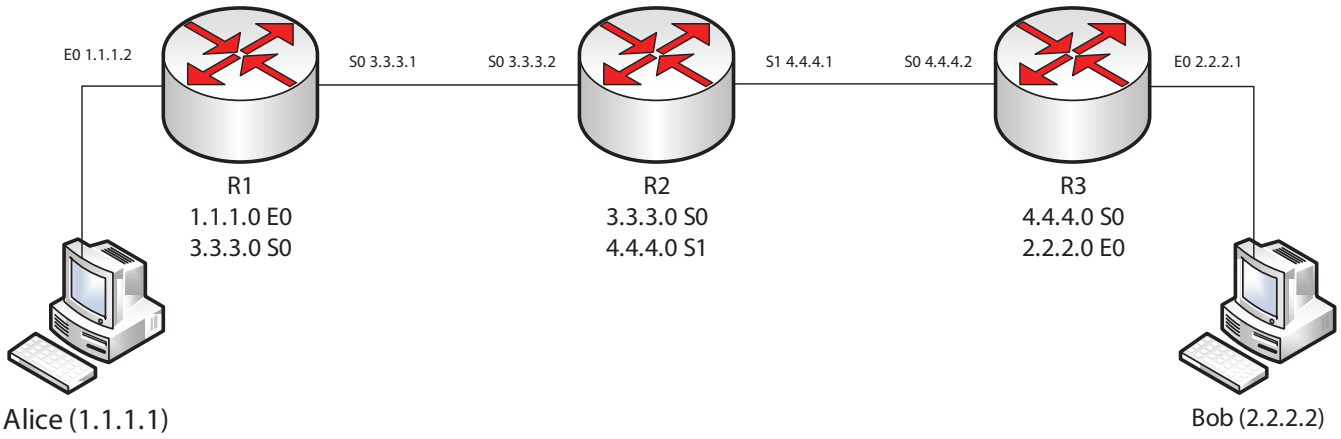
Vu que l'application source ne peut pas communiquer directement avec l application destination, la pile de protocole permet à la donnée d être transmis de la source à la destination. Chaque donnée et entête est appelé Protocol Data Unit ou PDU. Le PDU passe chaque couche en ajoutant l entête de la couche traversée et ainsi de suite...

Point important :

- Le PDU de la couche 4 est appelé Segment
- Le PDU de la couche 3 est appelé Paquet (Packet en anglais)
- Le PDU de la couche 2 est appelé Trame (Frame en anglais)

## Points importants : Étapes de l encapsulation

1. Crée et encapsule la donnée de l application avec l entête de la couche application.
2. Encapsule l ensemble reçu avec l entête de la couche Transport.
3. Encapsule l ensemble reçu avec l entête de la couche Réseau (IP). Cela crée un paquet IP.
4. Encapsule l ensemble reçu avec l entête de la couche Liaison de données. Cela crée une trame.
5. Envoi la trame (succession de bits 0 et 1) sur le média physique.




**Transmission d une donnée sur un réseau TCP/IP**

Dans cet exemple, Alice construit le segment puis le paquet IP pour finir avec la trame. Celle-ci contient l adresse de destination qui a comme valeur l adresse du router R1. La trame est envoyée vers le routeur.

Le routeur R1 reçoit la trame et y extrait le paquet IP pour connaitre quelle est la destination souhaitée (Bob). R1 retransmet le paquet IP dans une nouvelle trame à destination du routeur R2.

R2 effectue la même opération et transmet la trame à R3.

R3 reçoit la trame et y extrait le paquet IP. Il transmet alors le paquet IP dans une trame à destination de Bob. Pour cela il utilise l adresse Ethernet de Bob comme adresse destination.

**Point important à connaitre :**

Le routage IPLe fonctionnement d un réseau avec deux routeurs.

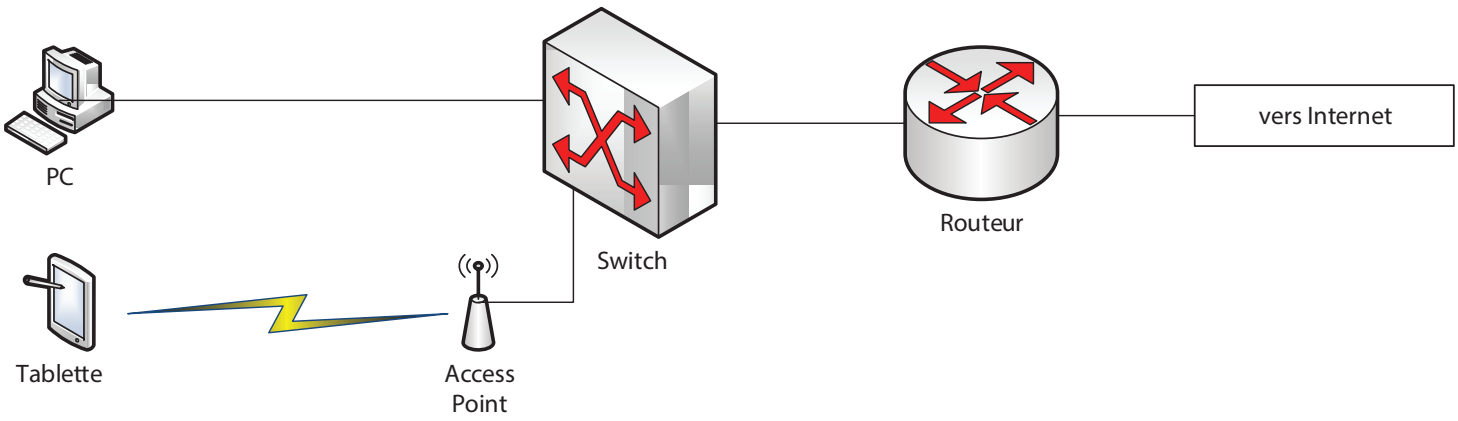
L adressage IP et son utilisation par les routeurs pour déterminer vers quelle direction acheminer le paquet.

Chaque lien entre routeur est appelé une “route”

Dans le cas de la version 4 d IP, une adresse est formée de 4 nombres séparés par un point. Par exemple, l adresse IP de Bob est 2.2.2.2

# THÉORIE DE LA COMMUTATION

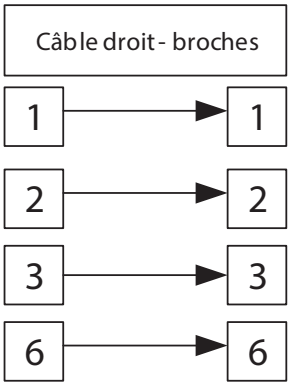
# Les fondamentaux des LANs Ethernet

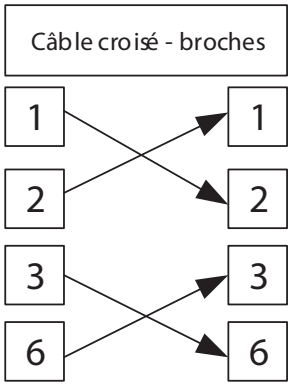



| Exemples et types d'Ethernet | | | | |
|---|---|---|---|---|
| Vitesse<br>Speed | Nom commun | Nom IEEE<br>informel | Nom IEEE<br>formel | Type de câble,<br>longueur max |
| 10 Mbps | Ethernet | 10BASE-T | 802.3 | Cuivre, 100 m |
| 100 Mbps | Fast Ethernet | 100BASE-T | 802.3u | Cuivre, 100 m |
| 1000 Mbps | Gigabit Ethernet | 1000BASE-LX | 802.3z | Fibre, 5000 m |
| 1000 Mbps | Gigabit Ethernet | 1000BASE-T | 802.3ab | Cuivre, 100 m |
| 10 Gbps | 10 Gig Ethernet | 10GBASE-T | 802.3an | Cuivre, 100 m |

Points importants à retenir :

- Connaitre les différents types de LANs Ethernet.
- Designer un réseau Ethernet filaire et sans-fil.
- Connaitre la composition des paires cuivres pour un câble droit et croisé.
- Savoir quand utiliser un câble droit et croisé.
- Savoir comment est forgée une adresse Ethernet unicast, sa longueur. Savoir à quoi ressemble une adresse de broadcast et multicast.
- Connaitre les différences entre un hub et un switch.
- Savoir expliquer le half-duplex, full-duplex et le CSMA/CD.




## Rappel sur l'utilisation des câbles:

| | |
|---|---|
| PC et switch | câble droit |
| Switch et routeur | câble droit |
| PC et PC | câble droit |
| Switch et Switch | câble croisé |
| Routeur et routeur | câble croisé |

# Les fondamentaux des LANs Ethernet

## Trame Ethernet type

| Preamble 7 | SFD 1 | Destination 6 | Source 6 | Type 2 | Données 46 - 1500 | FCS 4 |
|---|---|---|---|---|---|---|

La trame Ethernet est identique quelque soit le support physique. La plupart des équipement peuvent supporter une trame d une taille de 1518 octets

L adresse Media Access Control (MAC) est utilisée dans les réseau Ethernet (niveau 2). Elle est utilisée pour identifier une carte réseau (NIC – Network Interface Card)

## Entête Ethernet et champs:

Preamble – 7 octets (bytes) – Synchronisation

Start of Frame Delimiter (SFD) – 1 octet – Signifie que le prochain octet est l adresse MAC de destination

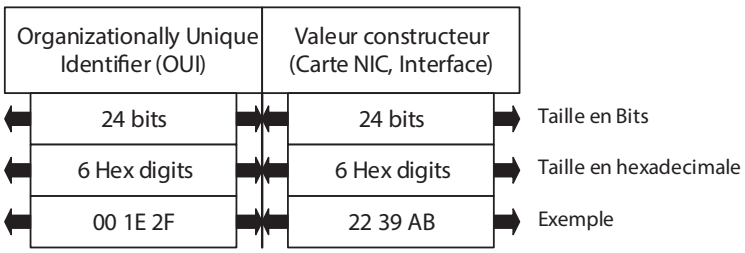
Destination MAC Address – 6 octets – Le destinataire de la trame

Source MAC Address – 6 octets – L émetteur de la trame

Type – 2 octets – Défini le type de protocole transporte au dessus (par ex IPv4 ou IPv6)

Données – Valeur entre 46 et 1500 octets – Données des couches supérieures dont IP, TCP...

Frame Check Sequence – 4 octets – Utilise pour déterminer s il y a eu une erreur de transmission



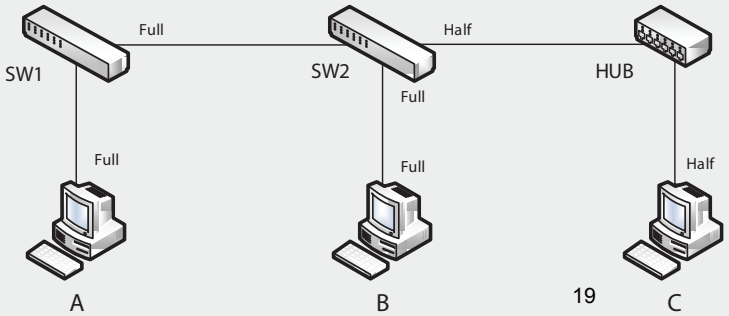

ABLes codes OUI sont assignés par l IEEE. Cet assignement permet l unicité des adresses MAC au niveau mondial.

**Exemple d adresses MAC:**
Adresse Unicast: 00:1E:2F:22:39:AB (spécifique à une interface sur un LAN)Adresse Broadcast: FF:FF:FF:FF:FF:FF (toutes les interfaces sur un LAN)Adresse Multicast: 01:00:5E:23:30:CD (un groupe d interfaces sur un LAN)

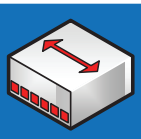
**Half-duplex :** envoi la donnée lorsqu il n en reçoit pas. Ne peut pas envoyer et recevoir en même temps

**Full-duplex :** peut envoyer et recevoir des données en même temps

Les Hub ne sont qu en half-duplex alors que les switch peuvent être half ou full-duplex en fonction du voisin connecté.



# Etablissement d un LAN Ethernet avec les switches



Hub / Répéteur

Le Hub était le premier équipement réseau qui permettait de connecter des PC dans un réseau Ethernet. Quand un Hub reçoit un signal sur un port, il le transmet sur tous les autres ports. Des collisions peuvent exister si 2 PC envoient un signal en même temps. Tous les PC connectés au Hub sont dans le même domaine de collision.



Switch / Commutateur

Le Switch est un Bridge plus intelligent. La trame reçue est uniquement transmise sur le ou les ports nécessaires.

Le switch a aussi la capacité d apprendre les adresses MAC des équipements du réseau. Il réduit les domaines de collision au niveau de chaque port. Un port = un domaine de collision différent.

Chaque port d un switch peut négocier sa vitesse (10/100/1000...) et son duplex (half/-full) avec l équipement connecté.a

Enfin le switch évite les boucles de niveau 2 en utilisant le protocole Spanning-tree (STP).



Bridge / Pont

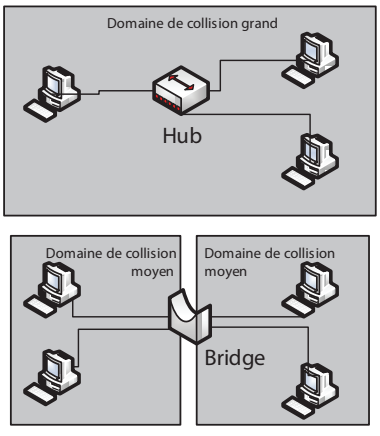
Comme la performance se dégradait proportionnellement au nombre de Hub dans un réseau, le Bridge est apparu.

Le Bridge reçoit une trame sur un port et la transmet sur un second port que si la destination se trouve derrière ce second port. Cela permet de segmenter le réseau et d avoir 2 domaines de collision plus petit, un pour chaque port.

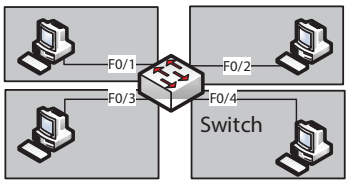
Domaine de collision versus domaine de broadcast.

Un domaine de collision est le nombre d interface Ethernet pour lesquelles l envoi d une trame par une de ces interfaces peut causer une collision avec une trame envoyées par une autre de ses interfaces en même temps.

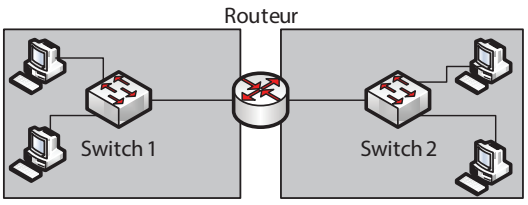
Un domaine de broadcast est le nombre d interface Ethernet pour lesquelles l envoi d une trame de broadcast niveau 2 est vu par toutes ces interfaces.



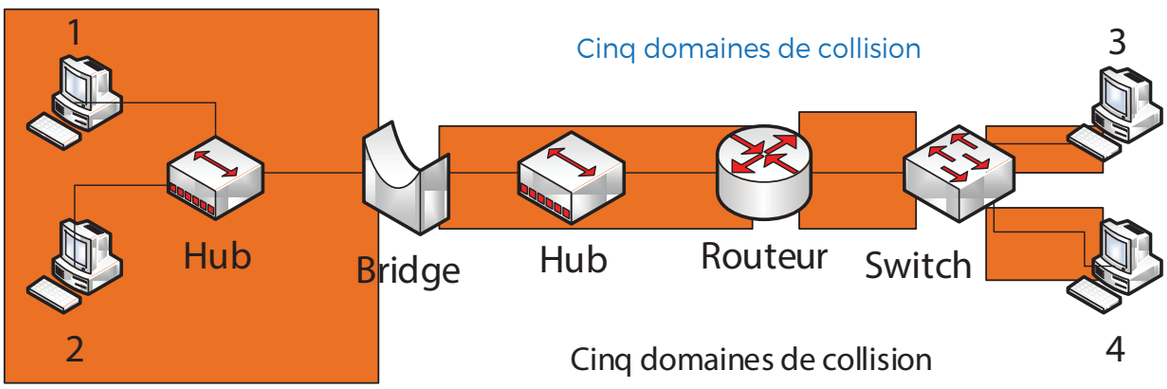

Le Bridge crée deux domaines de collision

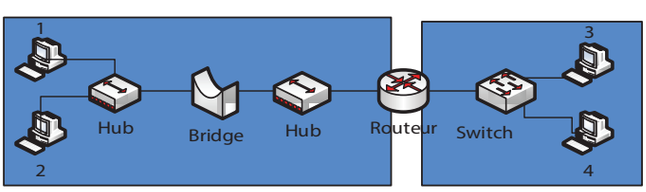



Le Switch crée quatre domaines de collision. Un par port

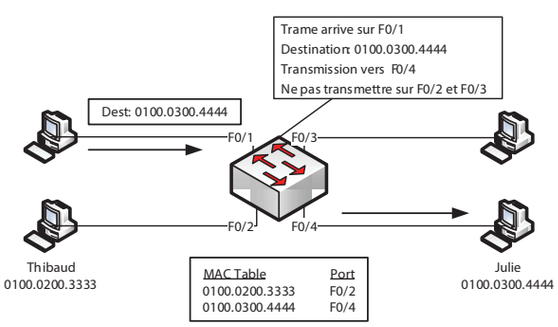



Ici, le routeur sépare les réseaux en deux domaines de broadcast (et pas de collision attention).
Généralement le routeur sépare les LANs en plusieurs domaines de broadcast.




Deux domaines de broadcast




## Logique de commutation :

**Étape 1 :** le switch transmet les trames en fonction des adresses MAC destination si l'adresse de destination est un broadcast, multicast ou adresse inconnue alors le switch inonde la trame sur tous les ports. si l adresse de destination est connue alors le switch transmet la trame vers le port de sortie adéquat. si le port de sortie est le même que le port qui a reçue la trame, celle-ci est supprimée.

**Étape 2 :** le switch apprend les adresses MAC et les stock Pour chaque trame reçue, le switch récupère l'adresse source et note l'interface sur laquelle est reçue cette trame. Si l'adresse MAC n est pas dans sa table de connaissance, il l'ajoute, ainsi que le port source. Si l'adresse MAC est dans la table, il remet les compteurs d inactivité à zéro.

**Étape 3 :** Le switch utilise le protocole STP pour éviter les boucles niveau 2 Apres calcul, certains ports sont bloqués par le STP et ne peuvent plus émettre ou recevoir des trames afin d éviter les boucles niveau 2.

### Résumé de la commutation LAN

Le port d un switch connecté en direct à un équipement lui fournit la vitesse (bande passante) et duplex dédiés.
Le switch permet la communication simultanée sans collision de plusieurs équipements.

Le switch gère facilement et simultanément différentes vitesses et duplex en fonction des équipements connectes, contrairement au Hub.

**Méthode de traitement de commutation :**

Store-and-forward : le switch reçoit la trame Ethernet en entier et la stock. Puis il vérifie les erreurs FCS avant de transmettre la trame vers le port de sortie.

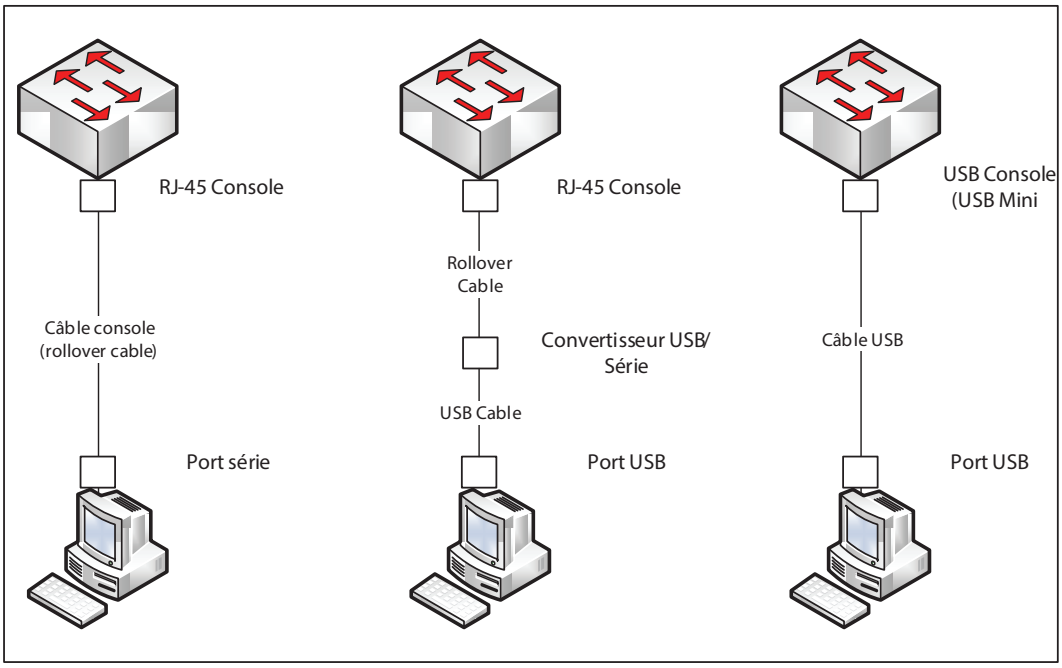
Cut-Trough : Le switch transmet la trame aussi vite que possible. Il n effectue pas de vérification d erreurs FCS.

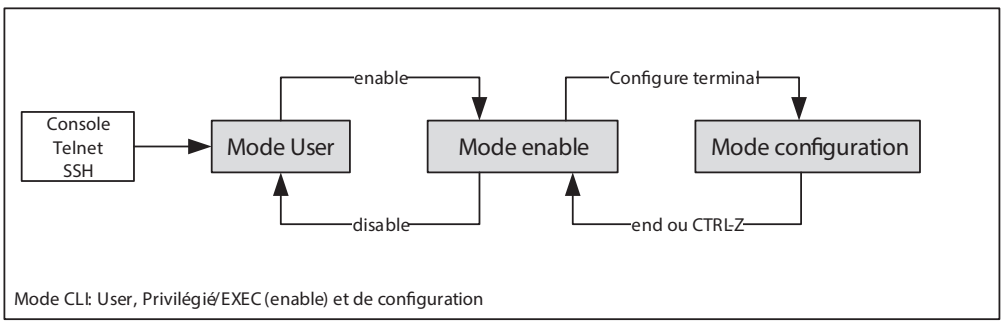
Fragment-free : Le switch reçoit la trame et commence à la transmettre vers le port de sortie lorsque les 64 premiers octets de cette dernière sont reçus.

# IMPLÉMENTATION DE LA COMMUTATION

## SérieMéthodes pour accéder à la CLI Cisco (Command Line Interface)

- **Port série du PC :** utilise un câble avec connecteur DB-9 d un coté (PC) et RJ-45 de l autre (Switch).
- **Convertisseur USB/Série :** dans le cas ou le PC n a pas de port DB-9, on utilise en plus un câble USB entre le PC et le connecteur DB-9.
- **Port console USB :** dans ce cas, le PC et le switch utilise chacun un port USB. Le PC a un port USB standard et le switch a un port mini-USB.

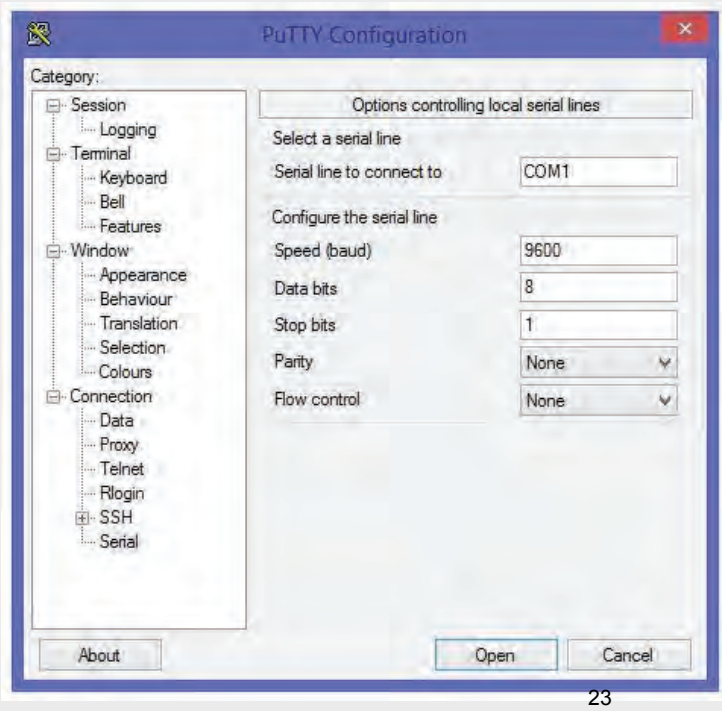



## Paramètres de console Cisco :

Vitesse/speed : 9000 bps
8 ASCII bits
Pas de parite
1 bit d arret (stop bit0
Pas de control de flux (flow control)

un exemple avec le logiciel PuttyMode

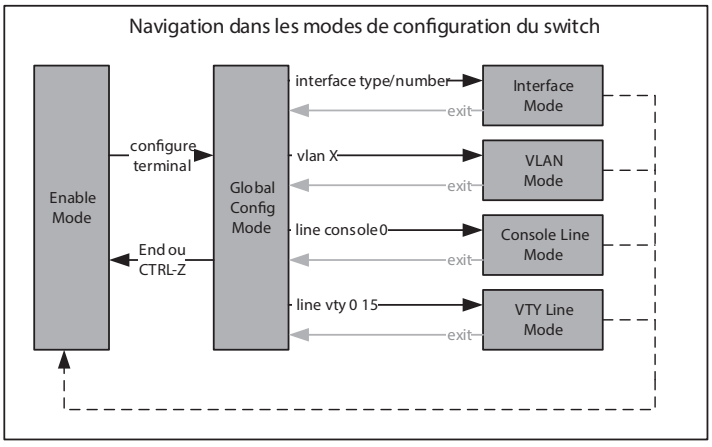


**Les deux modes utilisateur sont User et Enable**

- User (switch>) est le mode par défaut
- Enable (switch#) est le mode qui permet de changer la configuration du switch

Le prompt change en fonction du niveau de configuration dans lequel on se trouve :

| Prompt | Nom du mode |
|---|---|
| Hostname(config)# | Global |
| Hostname(config-line)# | Line |
| Hostname(config-if)# | Interface |
| Hostname(vlan)# | VLAN |




## Types de mémoire du switch Cisco

| RAM | Flash | ROM | NVRAM |
|---|---|---|---|
| Mémoire vive<br><br>Running-configuration | Système d'exploitation Cisco IOS | Programme de démarrage (Bootstrap Program) | Startup-configuration |

Types de mémoire du switch Cisco:

**RAM (DRAM) :** est utilisé comme mémoire vive, la running-config est stockée ici. Toute modification de configuration est effectuée sur cette running-config. Attention toute la RAM est effacée à chaque reboot du switch.

**Flash :** mémoire ou est stockée principalement le système d'exploitation Cisco IOS. Cette mémoire n est pas effacé lors du reboot. Peux stocker d'autres fichiers.

**ROM :** stock le mini-programme de démarrage du switch (Bootstrap) qui permet de décompresser et charger l'IOS dans la RAM.

**NVRAM :** la NonVolatile RAM stock la startup-config. Cette configuration est utilisée par défaut au demarrage du switch ou lors d'un reboot.

CiscoFichiers principaux de l IOS

**Startup-config:** Contient la configuration sauvegardée du switch et est utilisé à chaque démarrage du switch. Ce fichier est stocké dans le NVRAM.

**Running-config:** Contient la configuration en cours d utilisation par le switch. Ce fichier est modifié à la volée par l'administrateur. Il est stocké dans la RAM et doit donc être sauvegardé dans la startup-config pour éviter d'être perdu au prochain reboot

### Points clés dans la sécurisation du switch

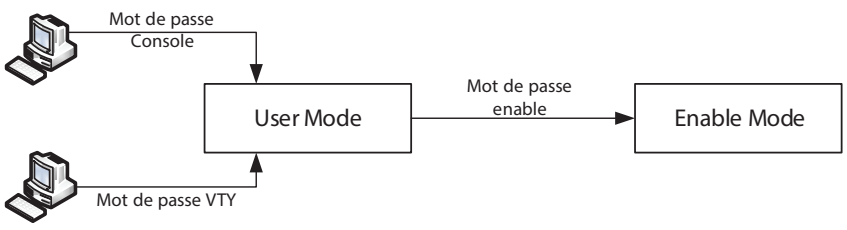
Les lignes console et VTY peuvent être sécurisées par un mot de passe.La commande enable secret doit être mise en place pour protéger l'accès à la configuration du switch.

Les utilisateurs et leur mot de passe sont configurés dans le mode de configuration global (username...). La commande login local est ensuite utilisée dans les lignes console et/ou VTY pour activer l'authentification utilisateur.

### Protection de la commande enable

Les commandes enable password (obsolète) et enable secret peuvent être utilisées pour protéger l accès à la configuration du switch. A retenir:Si les deux commandes sont utilisées en même temps: la commande enable secret a la priorité.

Si aucune des deux commandes n est configurée: en tapant enable , aucun mot de passe est demandé et l utilisateur a accès à la configuration du switch.




Configuration de mot de passe et du hostname

```
Switch> enable
Switch# configure terminal
Switch(config)# enable secret cisco
Switch(config)# hostname Emma
Emma(config)# line console 0
Emma(config-line)# password toto
Emma(config-line)# login
Emma(config-line)# exit
Emma(config)# line vty 0 15
Emma(config-line)# password tata
Emma(config-line)# login
Emma(config-line)# end
Emma#
```

### Buffer historique

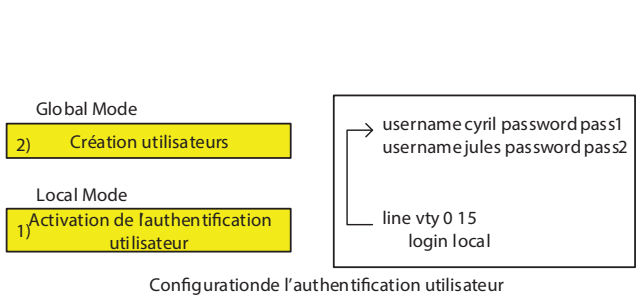
Le buffer historique conserve les commandes tapées par l utilisateur.

**show history:** Affiche les commandes contenu dans le buffer

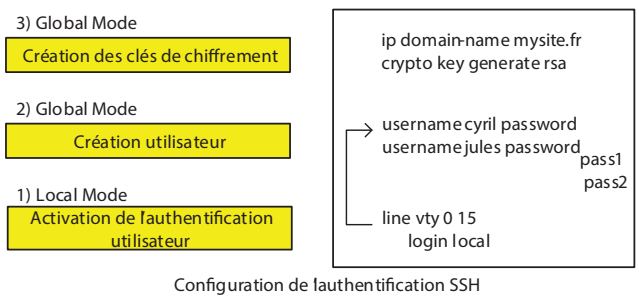
**history size x:** Paramètre la taille du buffer. X étant le nombre de commande à enregistrer

### Étapes de configuration pour sécuriser le switch avec SSH

1. Activer l authentification utilisateur sur les lignes VTY
2. Ajouter les comptes utilisateurs
3. Générer des clés de chiffrement SSH
4. Activer SSH v2 (v1 vulnérable à des attaques connues)




Configurationde l'authentification utilisateur




Configuration de l'authentification SSH

# Configuration du switch

## Configuration d IPv4 sur un Switch

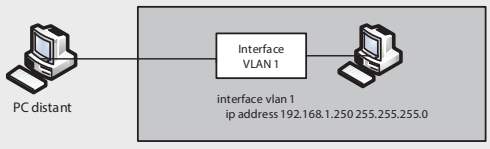
**Étape 1** : Entrer dans le mode de configuration du VLAN 1 avec la commande interface vlan 1

**Étape 2 :** Assigner une adresse IP avec la commande ip address ip-address mask

**Étape 3 :** Activer l interface avec la commande no shutdown

**Étape 4 (optionnel) :** sortir de la configuration de l interface avec exit puis configurer la passerelle par défaut avec la commande ip default-gateway ip-address Étape 5 (optionnel) : configurer le serveur DNS avec la commande ip name-server ip-address

Pour activer le DHCP pour le VLAN 1, utiliser ip address dhcp en etape 2.




Concept de l'interface virtuelle (SVI - Switched Virtual Interface) vers laquelle un PC distant peut y accéder pour configurer le switch

Configuration de l'adressage IPv4 du switch

```
Emma# configure terminal
Emma(config)# interface vlan 1
Emma(config-if)# ip address 192.168.1.250 255.255.255.0
Emma(config-if)# no shutdown
Emma(config-if)# exit
Emma(config)# ip default-gateway 192.168.1.1
```

## Port-Security

Dans un but de réduire les attaques provenant de PC pirates connectés sur le switch, la fonction Port-security définit la ou les adresses MAC sources légitimes qui peuvent transiter sur un port du switch.

Fonctionnalités du Port-security :

- Définition d'un nombre maximum d'adresses MAC source autorisées sur un port en particulier.
- Inspection pour chaque trame reçue sur le port de l'adresse MAC source vue.
- Lorsqu'une adresse MAC n'est pas reconnue, le port peut être désactivé (shutdown) et/ou une alerte peut être envoyée.

Action lorsqu il y a violation du Port-security

Les actions suivantes sont exécutées en fonction de l option configurée:

| Option | Protect | Restrict | Shutdown |
|---|---|---|---|
| Supprime les trames reçues | Yes | Yes | Yes |
| Envoi un log et message SNMP | No | Yes | Yes |
| Désactive l interface | No | No | Yes |

Sécurisation des interfaces du switch non utilisées

Les paramètres par défaut du switch permet à un pirate d accéder au réseau. Pour prévenir cet accès, configurer les commandes suivantes :

Désactiver l interface non utilisée avec la commande shutdown
- Interdire le trunk sur l interface en configurant le mode accesss
- Assigner l interface dans un VLAN non utilisé
- Configurer le native VLAN avec un VLAN non utilisé (par défaut VLAN 1)

## Configuration du Port-security

**Étape 1 :** configurer l interface en mode access (switchport mode access) ou trunk (switchport mode trunk)

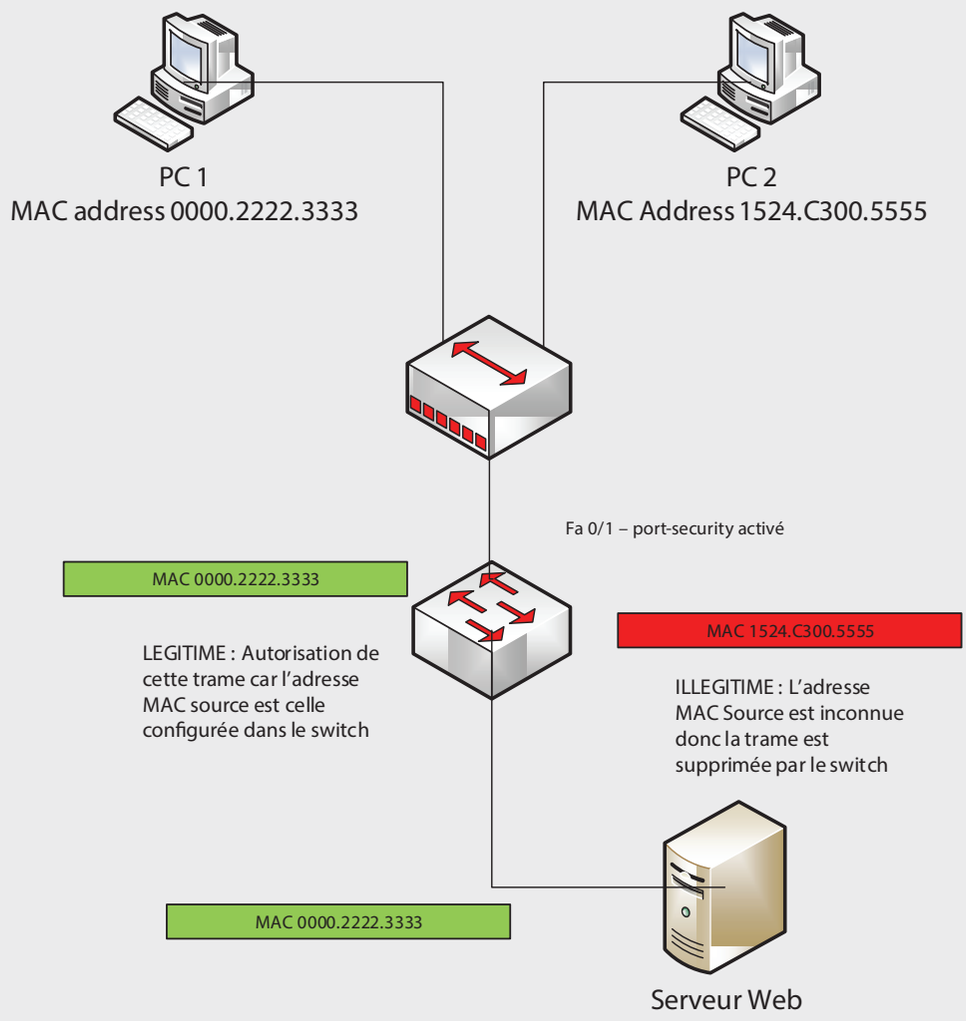
**Étape 2 :** activer la fonction avec la commande switchport port-security

**Étape 3 (optionnel) :** définir le nombre maximum d adresses MAC sources légitimes sur cette interface (switchport port-security maximum number)

**Étape 4 (optionnel) :** changer l action par défaut (shutdown) s il y a violation avec la commande switchport port-security violation {protect | restrict | shutdown}

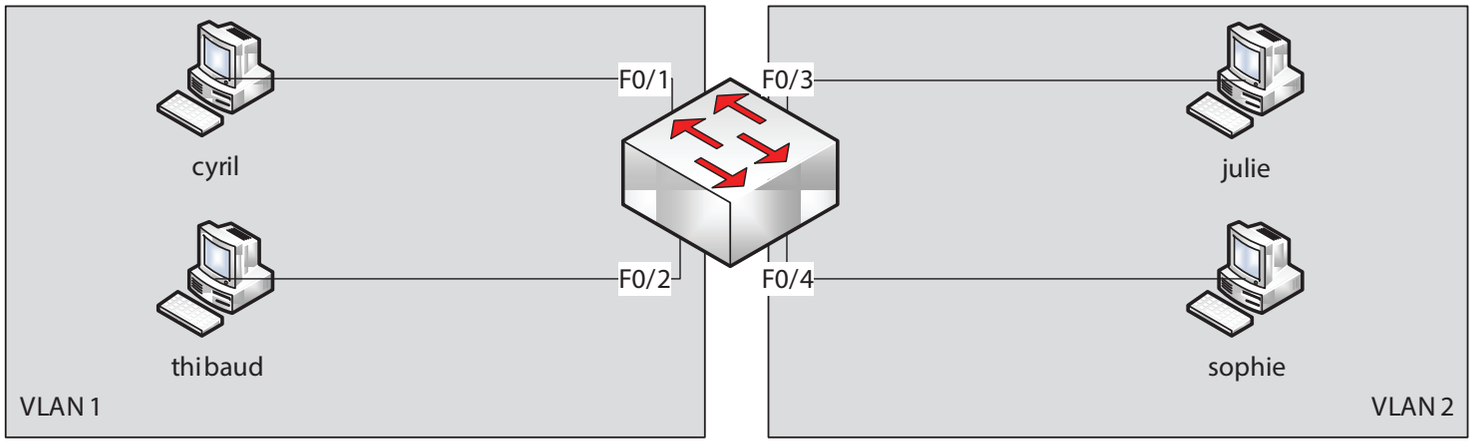
**Étape 5 (optionnel) :** définir les adresses MAC sources légitimes avec la commande switchport port-security mac-address mac-address

**Étape 6 (optionnel) :** au lieu de définir manuellement les adresses MAC sources (étape précédente), configurer l option sticky pour que le switch les apprenne par lui-même. Les premières adresses MAC sont considérées comme légitimes




Configuration du port-security sur une interface du switch
Emma# **configure terminal**
Emma(config)# **interface FastEthernet 0/1**
Emma(config-if)# **switchport mode access**
Emma(config-if)# **switchport port-security**
Emma(config-if)# **switchport port-security mac-address 0000.2222.3333**
Emma(config-if)# **exitPC**

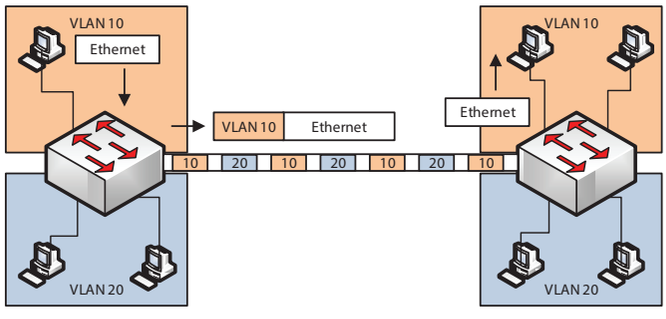
# Implémentation des Virtual LAN Ethernet



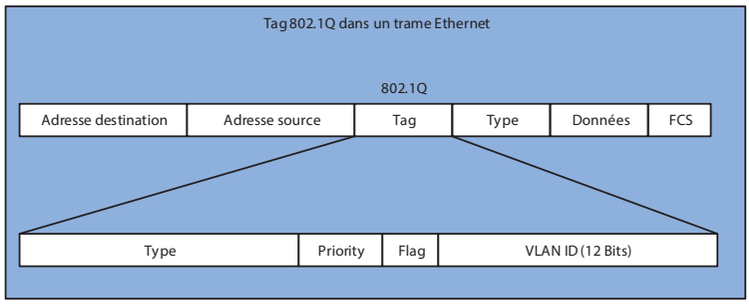

Création de deux domaines de broadcast sur un seul switch grâce à deux VLANs

**Pourquoi utiliser les VLANs**

- Diminue l utilisation CPU de chaque équipement connecté au switch en réduisant le nombre de trames de broadcast reçues
- Diminue le nombre de trames reçues par chaque équipement
- Augmente la sécurité en interdisant la communication entre certains équipements
- Permet de créer un design basé sur des groupes, des départements ou autre besoin métier
- Réduit le temps pour identifier un problème car les domaines de broadcast/VLAN sont indépendants
- Réduit le calcul du Spanning-tree en limitant un VLAN a un switch en particulier




VLAN Trunking entre deux switchs

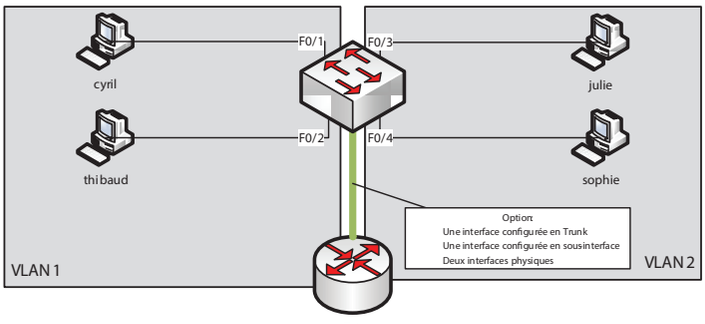



**Notes importantes sur les VLANs :**

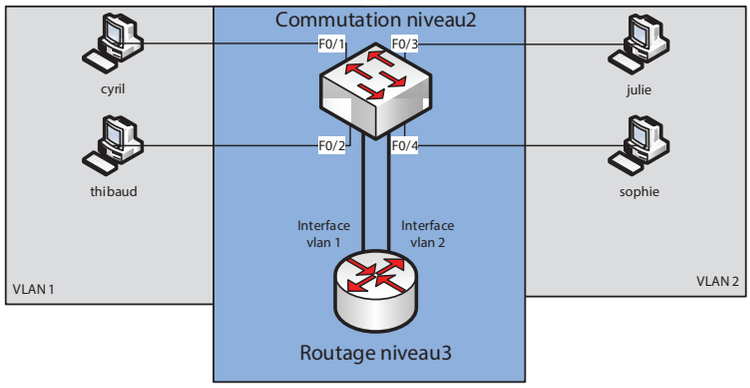
Le switch Cisco utilise les VLANs de 1 à 4094. Cette plage est divisée en deux parties : les VLANs 1 à 1005 sont présents sur tous les switchs. La plage 1006 a 4094 n est présente que sur les switchs récents.

VLAN natif : Ce VLAN aussi appelé VLAN non-tagué (untagged) permet d'envoyer une trame non 802.1Q sur un lien Trunk. Si l'équipement en face ne comprend pas le 802.1Q alors il récupèrera cette trame et la mettra dans le VLAN souhaité.Modifier le VLAN natif peut être utilisé sur un port connecté à un téléphone IP par exemple : le téléphone tague les trames voix et ne tague pas les trames données provenant du PC connecté derrière le téléphone.

# Implémentation des Virtual LAN Ethernet




Routage entre deux VLANs via un routeur




Routage entre deux VLANs sur un switch niveau3
(Le carre bleu décompose le switch niveau3)

**Recommandation: 1 VLAN = 1 sous-réseau IP**

## Création de VLANs et assignation d interfaces

Étape 1 : utiliser la commande vlan vlan-id pour créer un VLAN. Utiliser la commande name name pour lui donner un nom explicite

Étape 2 : Pour chaque interface à mettre dans ce VLAN, utiliser la commande switchport access vlan vlan-id et mettre le port en mode access avec la commande switchport mode access

```
IPSwitch# configure terminal
Switch(config)# vlan 2
Switch(config-vlan)# name COMMERCIAL
Switch(config-vlan)# exit
Switch(config)# interface FastEthernet 0/3
Switch(config-if)# switchport access vlan 2
Switch(config-if)# switchport mode access
Switch(config-if)# exit
Switch(config)# exit
Switch# show vlan
```

| VLAN Name | Status | Ports |
|---|---|---|
| 1 COMMERCIAL | active | Fa0/3 |

Switch#

Note : Au lieu d utiliser un switch pour la commutation et un routeur pour le routage inter-VLAN, les nouveaux switchs Niveau 3 permettent d effectuer les deux fonctions en un seul équipement.

Options de configuration du Trunk

| Commande | Description |
|---|---|
| Access | Active le mode access sur le port (trunk désactivé) |
| Trunk | Active le mode Trunk sur le port |
| Dynamic Desirable | Envoi un message pour monter le port en trunk |
| Dynamic Auto | Attend un message pour monter le port en trunk |

### Vérification des VLANs passant sur un lien Trunk

Il existe plusieurs raisons pour lequel le trafic pour un VLAN en particulier ne transite pas au travers d un lien Trunk, par exemple:

- Le VLAN a été enlevé de la liste autorise sur le lien Trunk
- Le VLAN n existe pas sur le switch en question
- Le VLAN existe mais a été désactivé
- Le VLAN a été pruné par le protocole VTP
- Le protocole Spanning-tree a mis le lien Trunk en blocking mode pour ce VLAN en particulier

| Mode configuré | Access | Dynamic Auto | Trunk | Dynamic Desirable |
|---|---|---|---|---|
| Access | Access | Access | A EVITER ! | Access |
| Dynamic Auto | Access | Access | Trunk | Trunk |
| Trunk | A EVITER ! | Trunk | Trunk | Trunk |
| Dynamic Desirable | Access | Trunk | Trunk | Trunk |

Si dans un lien inter-switch, un port est configuré en Trunk et l autre port en Access, la fonctionnalité Trunk ne fonctionnera pas. Il faut éviter à tout prix cette configuration !

## Procédure de troubleshooting basique:

**Étape 1 :** Analyser et prédire le fonctionnement normal du réseau. Comprendre ce qui est normal de ce qui ne l est pas

**Étape 2 :** Isoler le problème. Localiser le problème et effectuer des tests avec les commandes PING et DEBUG

**Étape 3 :** Analyse de la root cause (la cause du pb). Identifier la cause et trouver une solution pour la résoudre

| Line Status | Protocol Status | Interface Status | Description |
|---|---|---|---|
| Administratively Down | Down | Disabled | Interface désactivée par l'admin (shutdown) |
| Down | Down | notconnect | Pas de câble, câble défectueux, mauvais duplex ou vitesse, voisin éteint |
| Up | Down | notconnect | Résultat impossible |
| Down | Down (err-disabled) | Err-disabled | Le Port-security a désactivé l'interface |
| Up | Up | connected | Interface fonctionne correctement |

### Cisco Discovery Protocol (CDP)

Le CDP est un protocole propriétaire Cisco qui permet de partager des informations entre équipement voisin. Les informations échangées sont :

- Device identifier : Le hostname de l équipement
- Address list : Les adresses réseau (niveau 3) et liaison de données (niveau 2)
- Port Identifier : L interface du voisin qui a émis ce message CDP
- Capabilities list : Information sur l équipement (routeur, switch, IP-phone...)
- Platform : Le modèle et la version IOS utilise par le voisinshow

| Commandes | Description |
|---|---|
| show cdp neighbors | Liste résumé des voisins CDP |
| show cdp neighbors detail | Liste détaillée des voisins CDP |
| show cdp entry name | Liste détaillée pour un voisin CDP particulier |

Détails de la transmission d'une trame au travers du switch :

**Étape 1 :** le switch traite la trame sur l'interface d entrée. Si l'interface est UP/UP, le switch effectue :

**a)** si le Port-security est ON, alors on effectue la vérification
**b)** si le port est en ACCESS, identifier le VLAN associe au port
**c)** si le port est en TRUNK, identifier le VLAN natif

**Étape 2 :** le switch effectue la transmission de la trame grâce à l'adresse MAC destination et à sa table de connaissance :

**a)** si l'adresse (unicast) est dans la table alors le switch transmet la trame vers le port de destination (qui est renseigné dans la table)

**b)** si l'adresse n est pas dans la table, le switch inonde la trame sur tous ses ports excepté le port de réception

**c)** si l'adresse est un broadcast, le switch inonde la trame sur tous ses ports excepté le port de réception

Procédure d'auto-négociation

| Vitesse / Speed | Négocie en: |
|---|---|
| inconnu | 10 Mbps, half-duplex |
| 10 Mbps | 10 Mbps, half-duplex |
| 100 Mbps | 100 Mbps, half-duplex |
| 1 Gbps ou supérieur | 1 Gbps ou sup, full-duplex |

## Status de l interface Ethernet

Avec la commande show interface, on peut visualiser la vitesse, le duplex, les erreurs CRC, les collisions .

Affichage de la commande **show interface**

```
Switch# show interfaces fa0/12
FastEthernet0/12 is up, linae protocol is up (connected)
Hardware is Fast Ethernet, address is 0019.e86a.6f8d (bia 0019.e86a.6f8d)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mbps, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:05, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
85022 packets input, 10008976 bytes, 0 no buffer
Received 284 broadcasts (0 multicast)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 281 multicast, 0 pause input
0 input packets with dribble condition detected
95226 packets output, 10849674 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
Switch#
```

Commandes pour les ports en ACCESS et VLAN

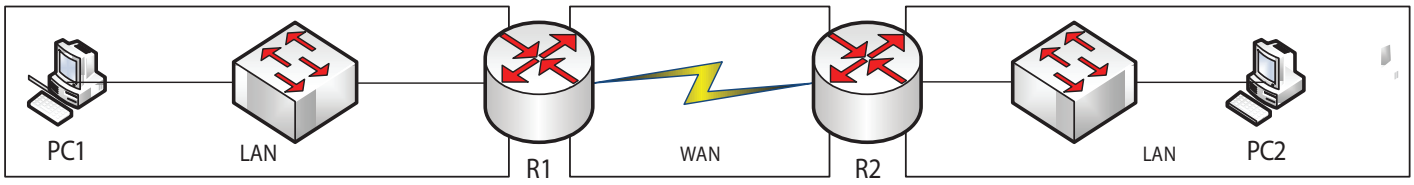
| Commande | Description |
|---|---|
| Show vlan brief<br>Show vlan | Liste les VLAN et les interfaces associées (les Trunks ne sont pas affichées) |
| Show vlan idnum | Liste Les interfaces ACCESS et TRUNK dans le VLAN en question |
| Show interfacestype number switchport | Affiche les informations sur l'interface en question, le mode, le VLAN associé... |
| Show mac address-table | Liste la table des adresses MAC et les VLAN associés |

```
Switch# show vlan brief

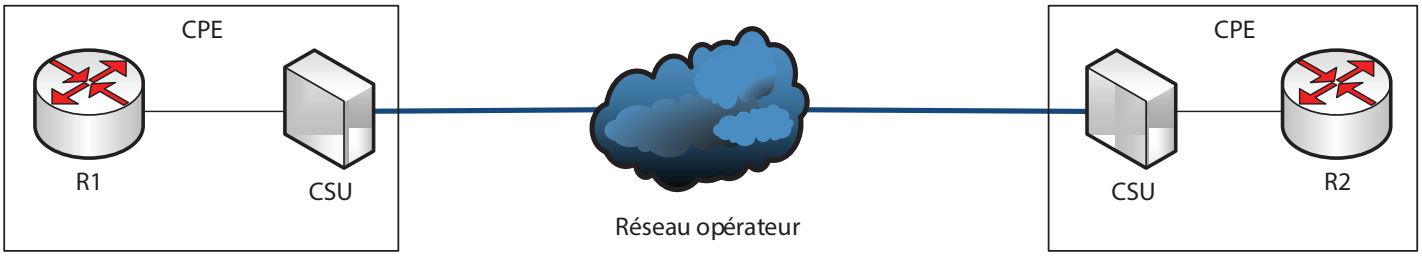
VLAN  Name                             Status    Ports
1     default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8,
                                                 Fa0/9, Fa0/10, Fa0/11
10    VLAN0010                         active    Fa0/12
```

Switch#

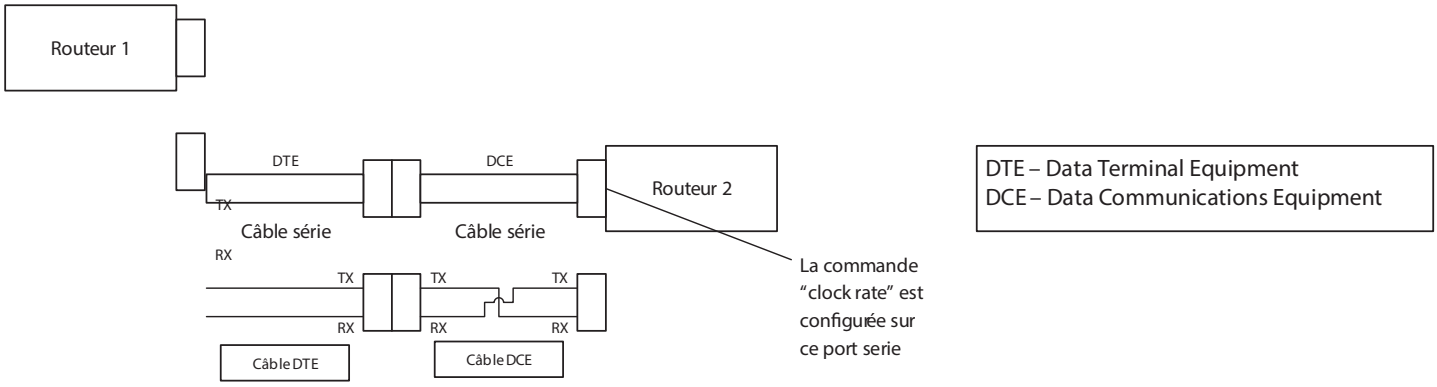
# THÉORIE DU ROUTAGE IPV4

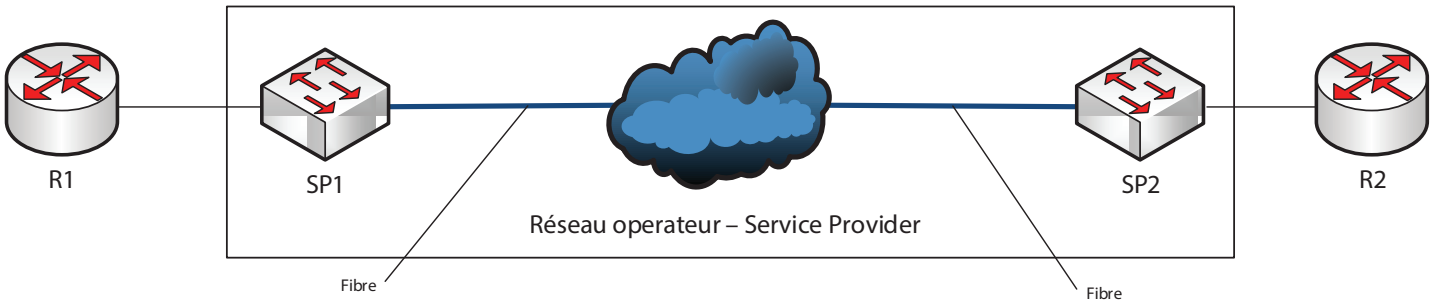



**Design logique :** PC1 et PC2 sont géographiquement séparés. Chaque PC est connecté à un LAN local (switch) puis à un routeur.Entre les routeurs se trouvent un lien géré par le fournisseurs d accès (opérateur). Ce lien WAN est appelé ligne louée et peut prendre différentes formes comme le E1, E3, STM1...



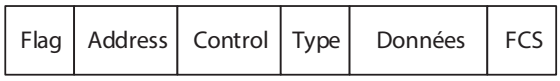

**Configuration physique :** entre les routeurs se trouvent un équipement CSU/DSU qui converti le signal du routeur en un signal utilisé par le réseau de l opérateur. Dans la plupart des cas, le CSU/DSU est intégré directement dans le routeur et ressemble à une interface série. Les deux routeurs utilisent un protocole de couche diffèrent d Ethernet, comme par exemple HDLC (High-Level Data Link Control).



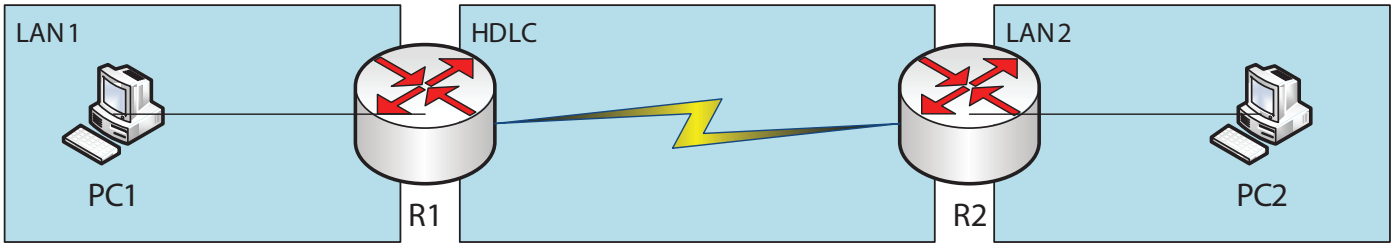



Ethernet comme un WAN : Au lieu d utiliser une ligne louée ou un circuit, le protocole Ethernet est utilise entre R1 et R2. Certains réseaux operateurs émulent le protocole Ethernet en utilisant des protocoles comme MPLS (Multi-protocol Layer Switching) et donc remplacent les anciens protocoles comme HDLC, PPP...

High-Level Data Link Control (HDLC) – Utilisé entre les routeurs avec des interfaces série.
Cisco utilise une version propriétaire de HDLC, comme la destination est implicite (car il n y a qu un seul voisin possible), il ne reste que le champ adresse source




Format Cisco HDLC







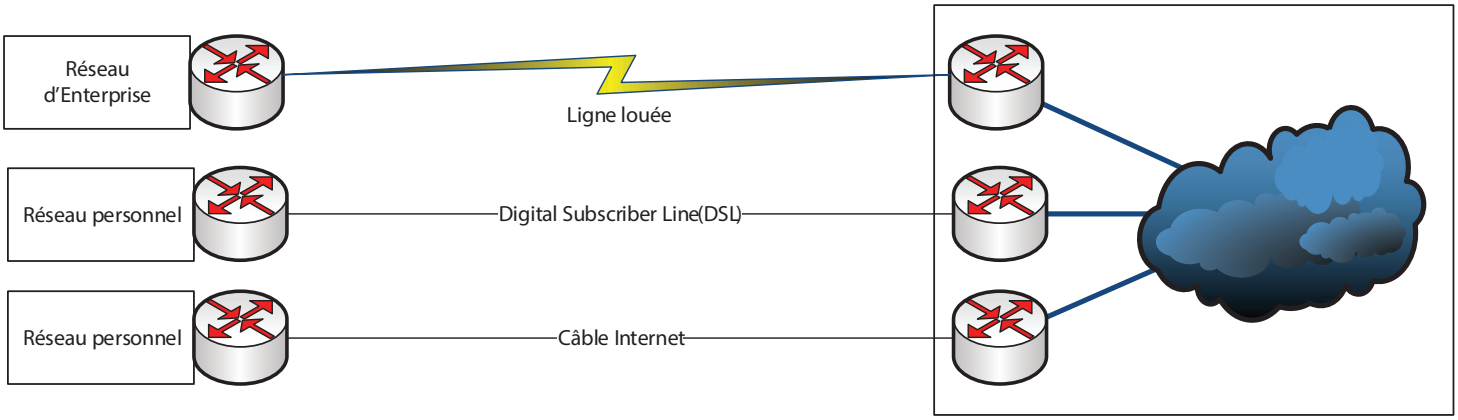
**Encapsulation** et **décapsulation** d un paquet IP au travers d un lien WAN (HDLC):

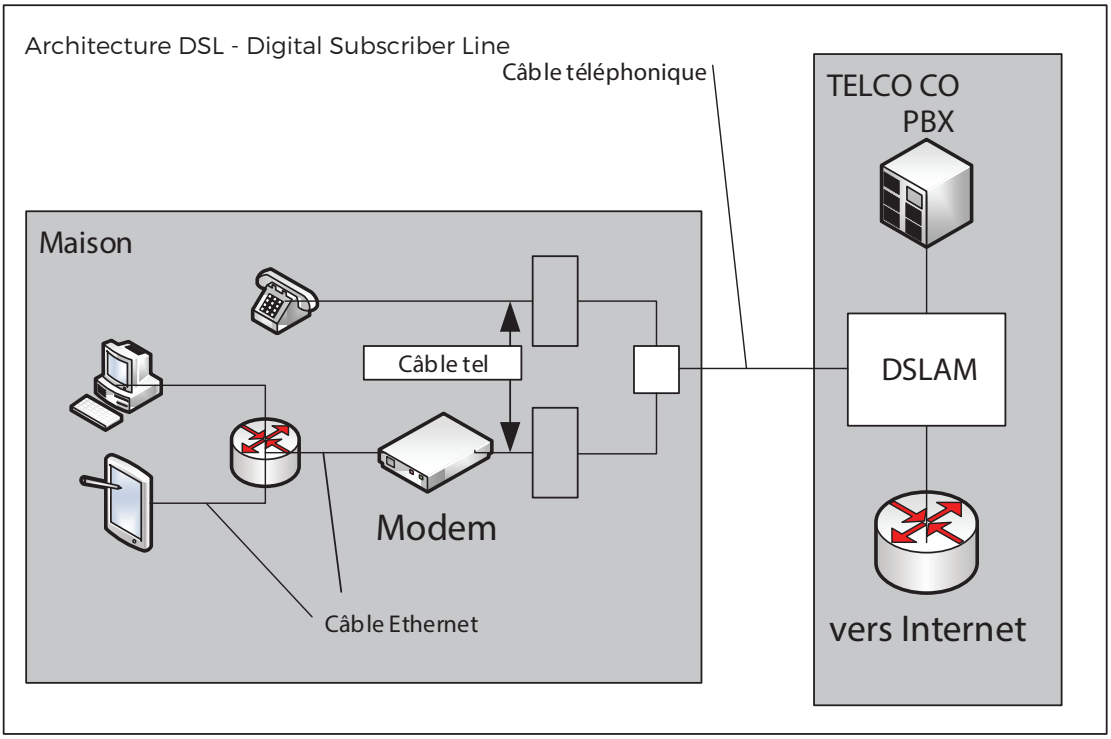
**Étape 1 :** PC 1 génère une donnée, la place dans un paquet IP puis dans une trame Ethernet et l envoi au routeur.

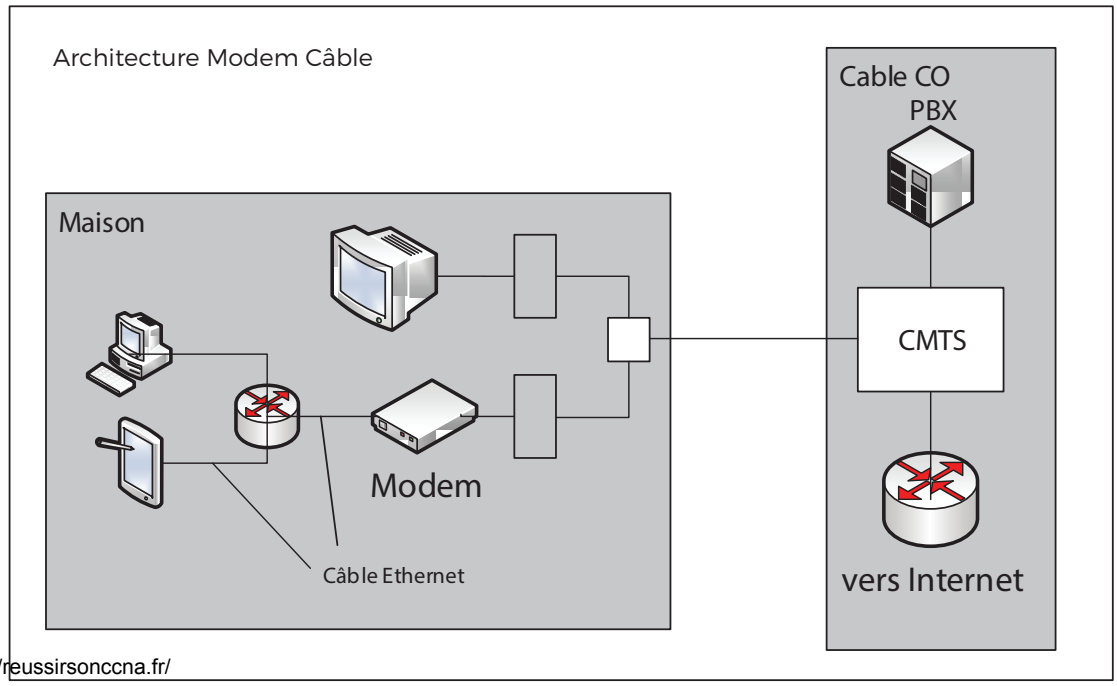
**Étape 2 :** R1 reçoit la trame Ethernet, y extrait le paquet IP, le place dans une trame HDLC et l envoi au routeur R2.

**Étape 3 :** R2 reçoit la trame HDLC, y extrait le paquet IP, le place dans une trame Ethernet et l envoi au PC2

## Technologies d accès à Internet



# Fondamentaux de l'adressage et du routage IPv4

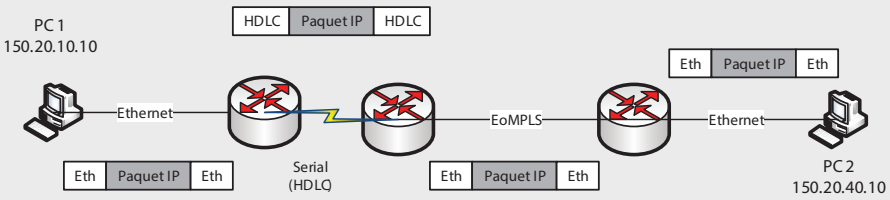
Points clés:

Toutes les adresses IP d un même groupe ne doivent pas être séparées par un routeur.Les adresses IP de groupes différents doivent être séparés par un routeur.

L'adresse IPv4 est formée de 4 octets (4 bytes), séparée par des points, on appelle cette notation décimale ou DDN (Dotted Decimal Notation).
Par exemple: 10.34.21.99

Les classes d'adresses IP sont déterminées par le premier octet de l'adresse.

Classe A: 1 à 126
Classe B: 128 à 191
Classe C: 192 à 223
Classe D: 224 à 239 (réservé pour le multicast)
Classe E: 240 à 255 (utilisation expérimentale)Les réseaux 0 Et 127 sont réservés pour des utilisations spécifiques

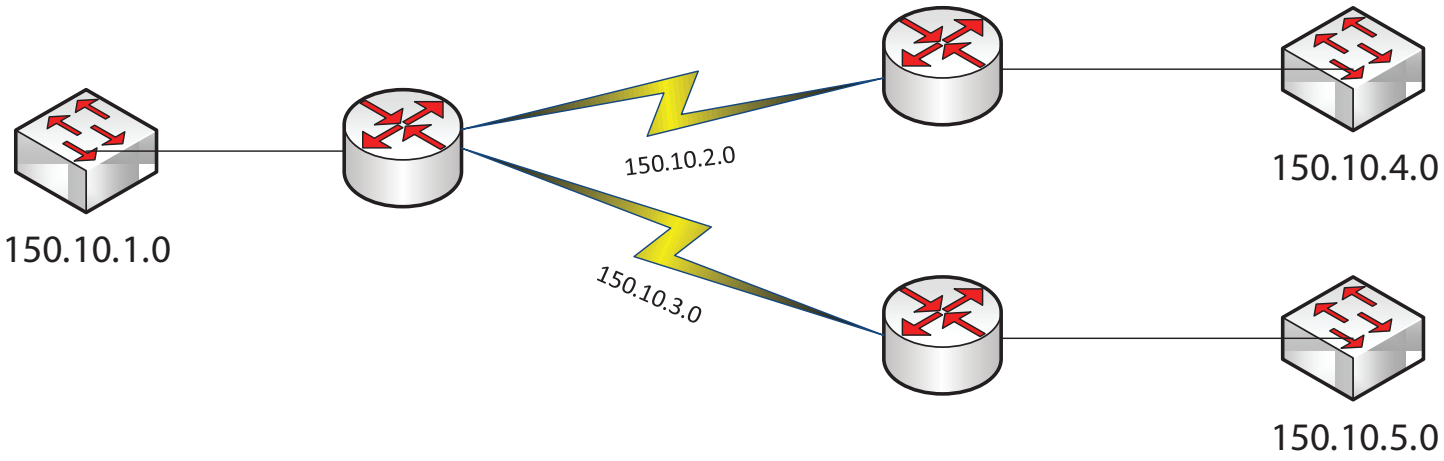



Le paquet traverse des réseaux par divers routeurs. L entête niveau 2 change à chaque traversée de routeur mais le paquet IP reste identique

| | | | Hôtes (Host) par réseau |
|---|---|---|---|
| 0 | Réservée | | |
| 1-126 | Classe A | Unicast | 16,777,214 |
| 127 | Réservée | | |
| 128-191 | Classe B | Unicast | 65,534 |
| 192-223 | Classe C | Unicast | 254 |
| 224-239 | Classe D | Multicast | |
| 240-255 | Réservée | Expérimentale | |

Valeurs possibles pour des réseaux

| Classe | 1er octet | Réseaux valides |
|---|---|---|
| A | 1-126 | 1.0.0.0 à 126.0.0.0 |
| B | 128-191 | 128.0.0.0 à 191.255.0.0 |
| C | 192-223 | 192.0.0.0 à 223.225.255.0 |




Le sous-réseau IP est un processus pour s assurer que les adresses IP sont bien utilisées.

Par exemple, au lieu d utiliser une plage de 254 adresses possible, on va créer un sous-réseau ne contenant que deux adresses IP, pas plus, pour les liens série.

Dans cet exemple, nous découpons le réseau 150.10.0.0 en sous-réseaux plus petits.

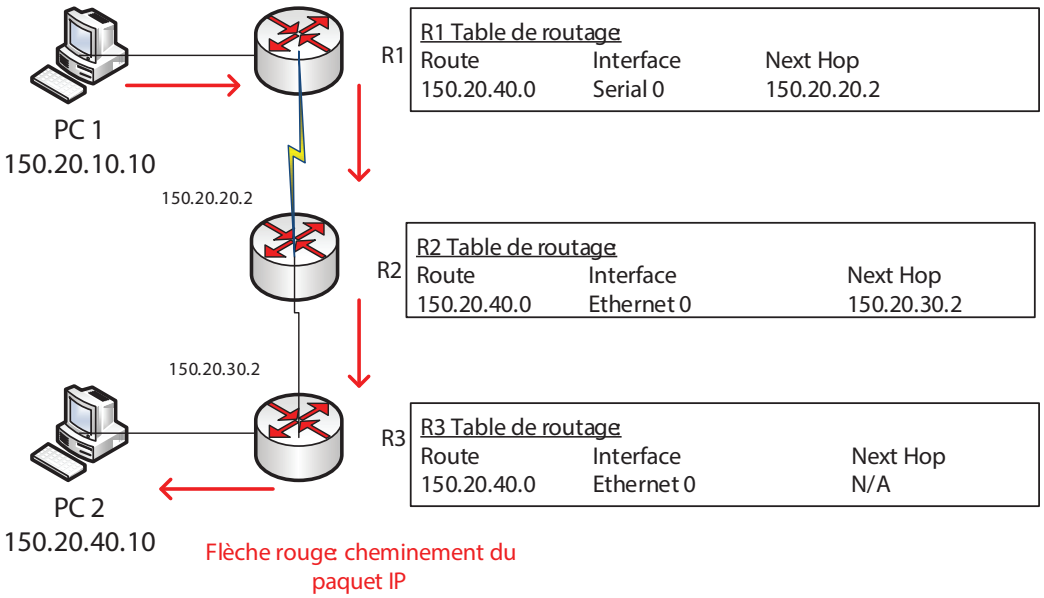
Logique de transmission d un paquet par un routeur:

1. utilise le champ FCS de la trame reçue pour vérifier les eventuelles erreurs de transmission. Supprime la trame si c est le cas.

2. extrait le paquet IP et supprime l entête Ethernet.

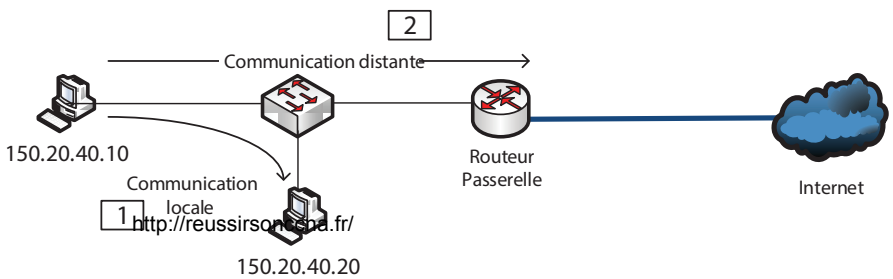
3. Compare le champ adresse IP destination du paquet IP avec les valeurs contenues dans sa table de routage et identifie le prochain routeur voisin.

4. Place le paquet IP dans une nouvelle trame et transmet cette trame sur l interface de sortie.




**Chaque protocole de routage doit avoir les fonctions suivantes:**

- Apprentissage dynamique des routes et alimentation de sa table de routage.
- Si plusieurs routes sont disponibles pour un même réseau alors ajouter dans la table de routage de la meilleure route.
- Avertir lorsqu une route n est plus disponible et l enlever de la table de routage.
- Si une route est supprimée mais qu une autre route, pour le même réseau est disponible, ajouter cette nouvelle route dans la table de routage.
- Agir rapidement dans l ajout et la suppression de routes dans la table de routage.
- Prévenir des boucles de routage




Règle de routage IPv4:

1 1. si le destinataire et mon PC sont dans le même sous-réseau alors je lui envoi le paquet directement

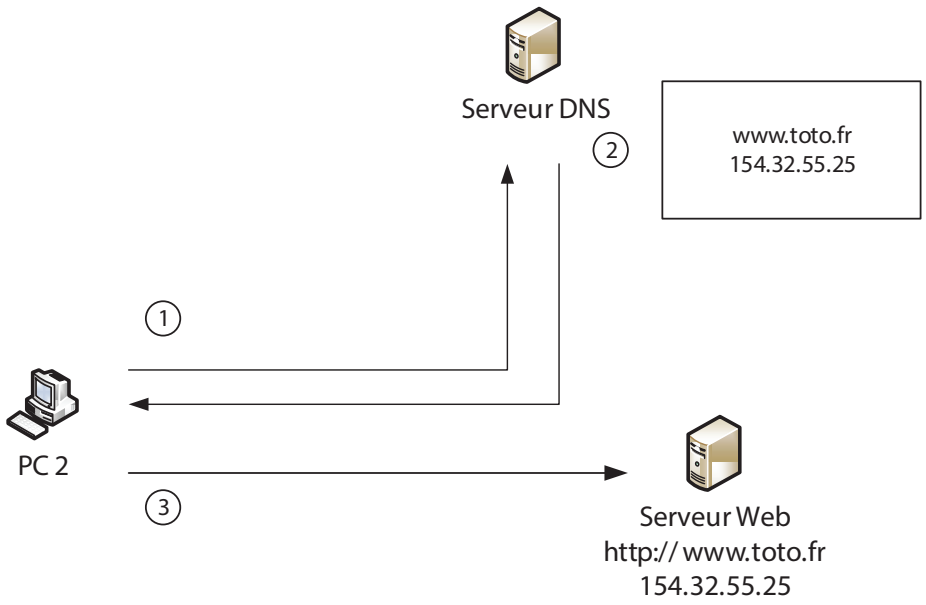
2 2. sinon, j'envoi le paquet à mon routeur (passerelle) pour traitement

http://reussirsonccna.fr/

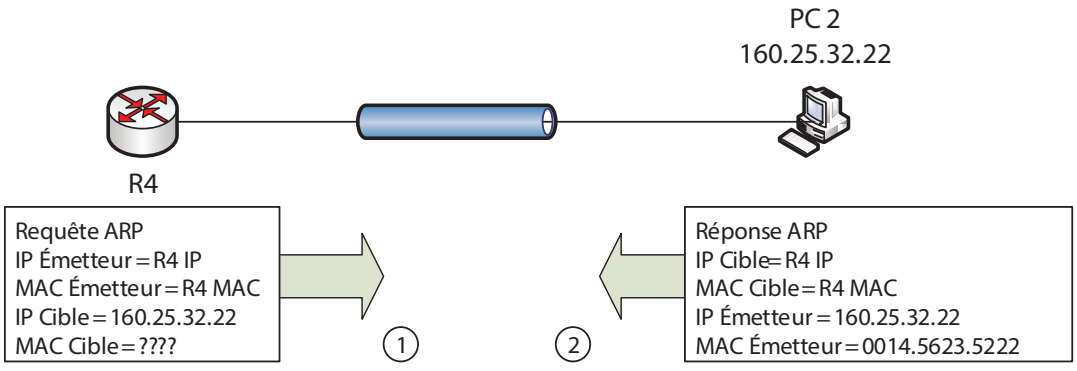
Domain Name System (DNS) : Résout les noms en adresse IP.

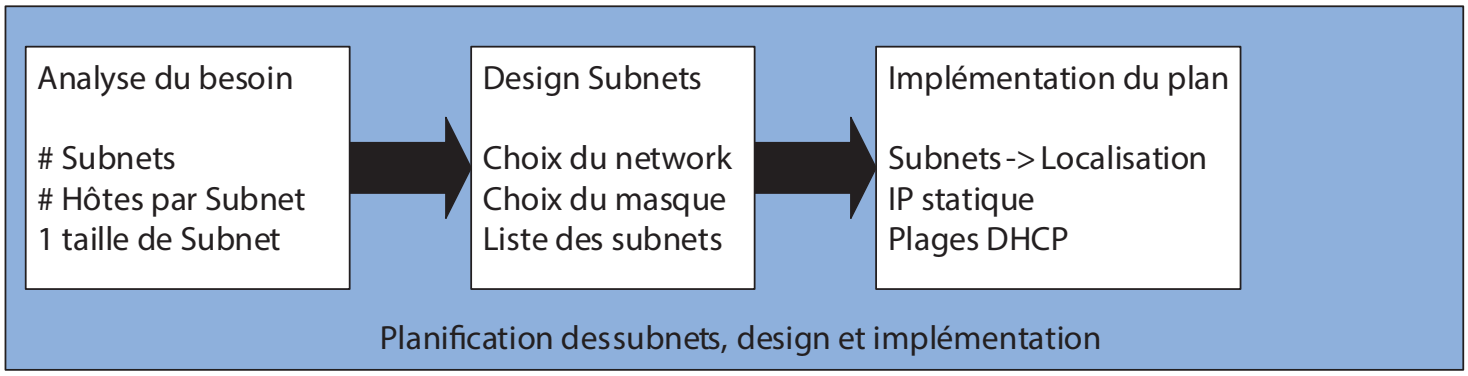
Un hôte configuré pour utiliser le DNS a des informations dans ses paramètres réseaux identifiant les serveurs DNS à solliciter.
Un serveur DNS a une base de données de correspondance entre les noms et les adresses IP associées.

1 – L hôte envoi une requête au serveur DNS concernant un nom de domaine (par exemple : toto.fr).
2 – le serveur DNS réponds avec l adresse IP correspondante au serveur toto.fr.
3 – l hôte initie une communication avec le serveur toto.fr car il connait désormais son adresse IP.




**Address Resolution Protocol** (ARP) : Ce protocole effectue la correspondance entre une adresse niveau 3 (IP) et une adresse niveau 2 (Ethernet).Il est utilisé pour transmettre des paquets IP localement à un destinataire dont on ne connait que l adresse IP et pas l adresse MAC.

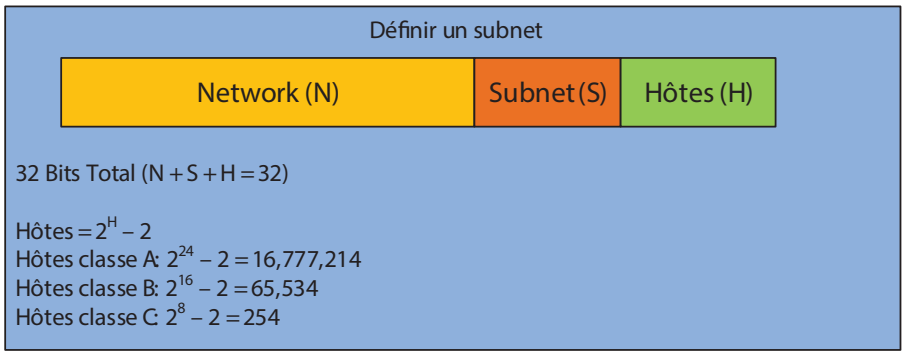


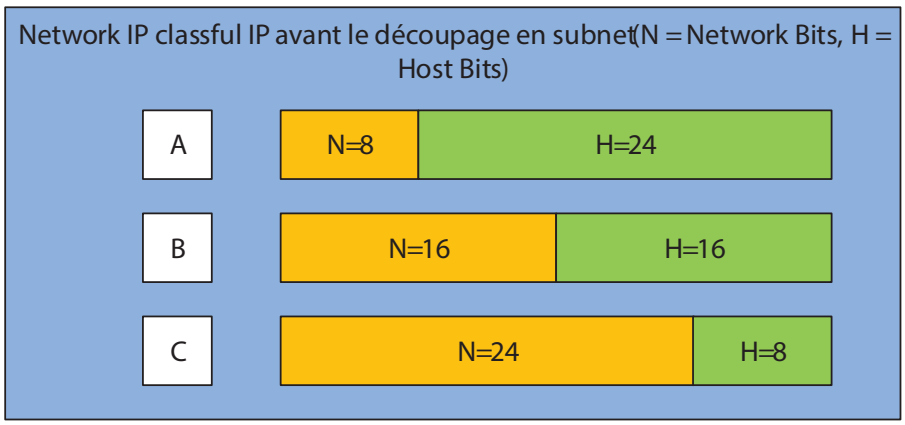



Règles primordiales !Les adresses dans le même subnet ne doivent pas être séparées par un routeurLes adresses dans le subnet diffèrent doivent être séparées par au moins un routeur

Détermination du nombre de subnets

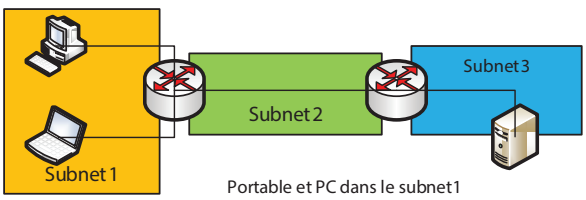
| Type de Network | Nombre d hôtes |
|---|---|
| VLAN | 6+ |
| Lien série point-to-point | 2 |
| Lien WAN émulation Ethernet | 2 |
| PVC Frame Relay | 2 |



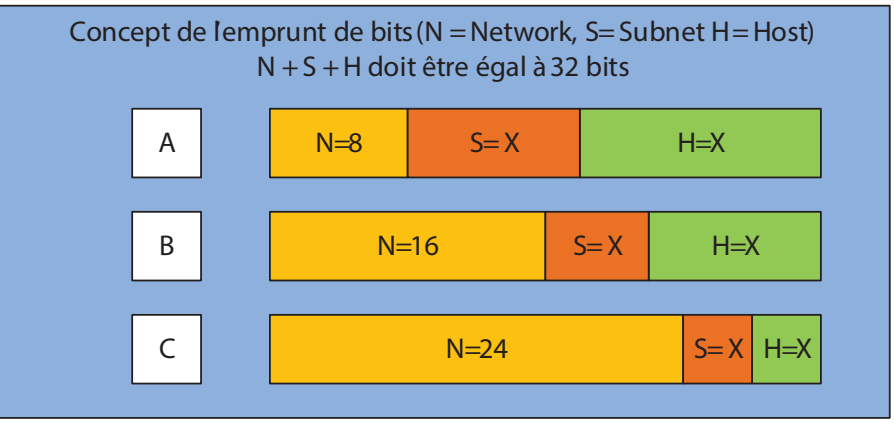




RFC 1918 – plage des adresses IP privées

| Classe | Networks | Nombre de Networks |
|---|---|---|
| A | 10.0.0.0 | 1 |
| B | 172.16.0.0 À 172.31.0.0 | 16 |
| C | 192.168.0.0 À 192.168.255.0 | 256 |



# Les sous-réseaux (subnets) IPv4




Puissance de 2 utile pour définir les masques

| Nombre de bits | $2^X$ | $2^X$-2 |
|---|---|---|
| 1 | 2 | 0 |
| 2 | 4 | 2 |
| 3 | 8 | 6 |
| 4 | 16 | 14 |
| 5 | 32 | 30 |
| 6 | 64 | 62 |
| 7 | 128 | 126 |
| 8 | 256 | 254 |
| 9 | 512 | 510 |
| 10 | 1024 | 1022 |
| 11 | 2048 | 2046 |
| 12 | 4096 | 4094 |

Construction de la liste des subnets

Ci-dessous les objets importants pour la création de subnets

**Subnet number** – Aussi appelé subnet ID, Ce nombre identifie le subnet en lui-même. C est le plus petit nombre du subnet et ne peut pas être utilisé par un hôte

**Subnet broadcast** – Ce nombre identifie l adresse de broadcast de ce subnet. C est le nombre le plus élevé du subnet et ne peut pas être utilisé par un hôte

**IP Addresses** – Ce sont les adresses des hôtes situées entre le subnet number et le broadcast number .

Exemple de subnet : On nous donne le network 195.16.12.0/22 que l on doit le découper en deux subnet contenant au moins 500 adresses IP pour les hôtes. Définir les Subnet ID, Broadcast et la plage IP pour ces subnets.

Chaque subnet contient au moins 500 hôtes. Nous avons besoin de 9 Host bits pour chaque subnet et nous en avons à disposition 10. Cela signifie que nous allons avoir 16 bits pour le network, 7 bits pour les subnets et 9 bits pour les Hosts, soit un total de 32 bits.
Le masque ne sera plus de /22 mais de /23 car nous empruntons 1 bit en plus pour la partie subnet.

Subnet 1 : On prend le premier subnet ID qui est 195.16.12.0/23 (et pas /22). L adresse de broadcast pour ce subnet est 195.16.12.1.255 et la plage des hôtes est comprise de 195.16.12.1 à 195.16.13.254.

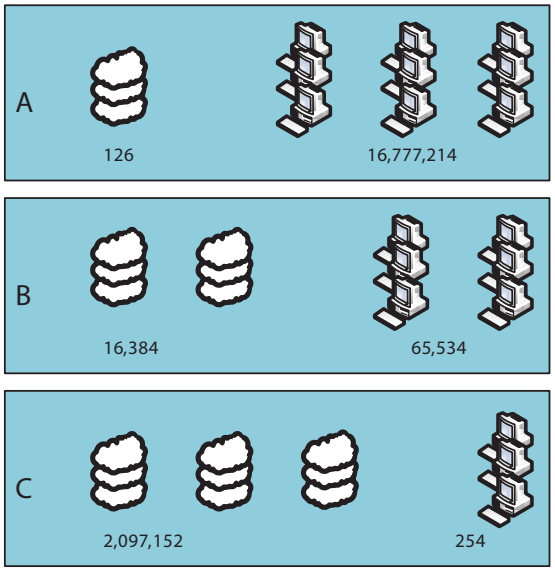
Subnet 2 : On prend le subnet ID suivant qui est 192.16.14.0/23. L adresse de broadcast pour ce subnet est 192.16.15.255 et la plage des hôtes est comprise de 195.16.14.1 à 195.16.15.254

# Analyse des Networks IPv4 classful

Classes des adresses IPv4 En fonction de la valeur du premier octet

| Classe | Valeur 1er octet | Usage |
|---|---|---|
| A | 1-126 | Unicast (larges réseaux) |
| B | 128-191 | Unicast (réseaux tailles moyennes) |
| C | 192-223 | Unicast (petits réseaux) |
| D | 224-239 | Multicast |
| E | 240-255 | Expérimental |

Note importante:Les adresses dans le même Network ont tous la même valeur pour le Network ID et des valeurs différentes pour le Host ID




Nombre de Networks et de Hôtes par classe

| Key Facts | Classe A | Classe B | Classe C |
|---|---|---|---|
| Plage du premier octet | 1-126 | 128-191 | 192-223 |
| Networks valides | 1.0.0.0 – 126.0.0.0 | 128.0.0.0 – 191.255.0.0 | 192.0.0.0 – 223.255.255.0 |
| Nombre total de Networks | $2^7 - 2 = 126$ | $2^{14} = 16,384$ | $2^{21} = 2,097,152$ |
| Hosts/Hôtes par Network | $2^{24} - 2$ | $2^{16} - 2$ | $2^8 - 2$ |
| Octets (bits) côté network | 1 (8) | 2 (16) | 3 (24) |
| Octets (bits) côté hôtes | 3 (24) | 2 (16) | 1 (8) |
| Masque par défaut | 255.0.0.0 | 255.255.0.0 | 255.255.255.0 |

# Analyse des Networks IPv4 classful

Déterminer le Network ID, le broadcast ID et les adresses Hosts

**Étape 1 :** déterminer la classe du Network (A, B, C) par le premier octet

**Étape 2 :** diviser mentalement les octets Network et les octets Host en fonction de la classe

**Étape 3 :** trouver le Network ID en changeant tous les bits de la partie Host à zéro

**Étape 4 :** trouver l adresse du premier Host en ajoutant 1 au dernier octet de la partie Host

**Étape 5 :** trouver l adresse de broadcast en changeant tous les bits de la partie Host à 1

**Étape 6 :** trouver la dernière adresse Host en enlevant 1 à l adresse de broadcast

Masque de subnet de classe A par défaut

| | | | | |
|---|---|---|---|---|
| Décimal | 255 . | 0 . | 0 . | 0 |
| Binaire: | 1111 1111 | 0000 0000 | 0000 0000 | 0000 0000 |
| Concept | Network (8) | Host (24) | | |

Masque de subnet de classe B par défaut

| | | | | |
|---|---|---|---|---|
| Décimal | 255 . | 255 . | 0 . | 0 |
| Binaire: | 1111 1111 | 1111 1111 | 0000 0000 | 0000 0000 |
| Concept | Network (16) | | Host (16) | |

Masque de subnet de classe C par défaut

| | | | | |
|---|---|---|---|---|
| Décimal | 255 . | 255 . | 255 . | 0 |
| Binaire: | 1111 1111 | 1111 1111 | 1111 1111 | 0000 0000 |
| Concept | Network (24) | | | Host (8) |

Exemple: trouver le network ID, la plage des Hosts et l'adresse de broadcast pour 175.17.22.3

1. Grâce au premier octet, nous avons un Network de classe B donc le masque est 255.255.0.0

| | Network | Host |
|---|---|---|
| 2 Diviser en Network et Host | 175.17 | 22.3 |
| 3 Appliquer Host=0 | 175.17 | 0.0 |
| 4 Ajouter 1 | | +1 |
| Premier Host IP | 175.17 | 0.1 |
| 5 Appliquer Host=255 | 175.17 | 255.255 |
| 6 Soustraire 1 | | -1 |
| Dernier Host IP | 175.17 | 255.254 |

Conclusion l'adresse IP 175.17.22.3/16 appartient au subnet

| | |
|---|---|
| Network ID: | 175.17.0.0 |
| Premier Host IP: | 175.17.0.1 |
| Dernier Host IP: | 175.17.255.254 |
| Adresse de Broadcast | 175.17.255.255 |

# Analyse des masques de sous-réseaux

Les 3 formats d'un masque de sous-réseaux

Exemple avec 255.255.255.0 affiche sous 3 formats:
Binaire: 11111111 11111111 11111111 00000000
Décimal: 255.255.255.0 (conversion binaire vers décimal)
Préfix: /24 (Comptage du nombre de 1 binaire)

En notation binaire, tous les 1 doivent se situer à gauche et tous les 0 à droite. Il est interdit d'intervertir un 1 et un 0 !

0010 0010 1011 1111 0011 0001 1100 1111 – Interdit !
1111 1111 1111 1111 1100 0000 0000 0000 - Correct

Valeurs d'un octet et ses équivalents en décimal

| Nombre binaire | Nombre décimal | Nombre de 1 |
|---|---|---|
| 0000 0000 | 0 | 0 |
| 1000 0000 | 128 | 1 |
| 1100 0000 | 192 | 2 |
| 1110 0000 | 224 | 3 |
| 1111 0000 | 240 | 4 |
| 1111 1000 | 248 | 5 |
| 1111 1100 | 252 | 6 |
| 1111 1110 | 254 | 7 |
| 1111 1111 | 255 | 8 |

Conversion binaire vers préfix : compter le nombre de 1 dans le masque et écrire la somme précédé d un slash (/)

Conversion préfix vers binaire : écrire le nombre de 1 en partant de la gauche et remplir ensuite de zéro pour atteindre 32 valeurs (32 bits)

Conversion masque binaire vers notation préfix

| Masque binaire | logique | Préfix |
|---|---|---|
| 11111111 11110000 00000000 00000000 | Compter 8 + 4 + 0 + 0 = 12 x "1" | /12 |
| 11111111 11111111 10000000 00000000 | Compter 8 + 8 + 1 + 0 = 17 x "1" | /17 |
| 11111111 11111111 11111110 00000000 | Compter 8 + 8 + 7 + 0 = 23 x "1" | /23 |

Conversion notation préfix vers masque binaire

| Préfix | Logique | Masque binaire |
|---|---|---|
| /12 | Écrire 12 fois "1" et 20 fois "0" soit 32 | 11111111 11110000 00000000 00000000 |
| /17 | Écrire 17 fois "1" et 15 fois "0" soit 32 | 11111111 11111111 10000000 00000000 |
| /23 | Écrire 23 fois "1" et 9 fois "0" soit 32 | 11111111 11111111 11111110 00000000 |

**décimalAdressage classful :** l'adresse IPv4 est composé de deux parties: Network (réseau) et Host (hôtes). Le sous-réseau est prédéfini par l'appartenance du Network aux classes A, B ou C

**Adressage Classless :** l'adresse IPv4 est composé de trois parties: Network (réseau), Subnet (sous-réseau) et Host (hôtes). Le sous-réseau est défini par l'administrateur et ne suit plus les règles des classes A, B et C

# Analyse des masques de sous-réseaux

Comment identifier avec une adresse IP :

- les bits Network, les bits Subnet, les bits Hosts
- le nombre de Hosts par Subnet et le nombre de Subnet

Étape 1 : convertir le masque en format préfix (/P)
Étape 2 : déterminer le nombre de bits Network base sur la classe par défaut
Étape 3 : calculer S = P – N
Étape 4 : calculer H = 32 – P
Étape 5 : calculer hosts par subnet: 2H – 2
Étape 6 : calculer le nombre de subnets: 2S

Exemple : 185.240.32.0 avec un masque 255.255.192.0

**Étape 1 :** le masque 255.255.192.0 est composé en 1 de 8 + 8 + 2 + 0 donc la notation préfix est /18

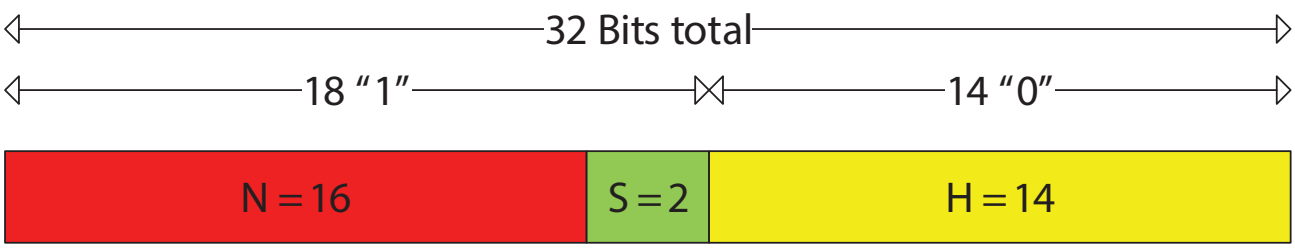
**Étape 2 :** le premier octet est 185 qui est compris entre 126 et 191. Nous sommes dans une classe B, le masque par défaut est donc /16

**Étape 3 :** le Subnet S est calcule en soustrayant: S = 18 – 16 = 2. Nous avons 2 bits pour la partie des sous-réseaux

**Étape 4 :** on identifie les bits H pour la partie Hosts: H = 32 – 18 = 14. Nous avons 14 bits pour la partie Hosts

**Étape 5 :** on calcule alors le nombre de Hosts par Subnet: 214 – 2 = 16384 – 2 = 16382. Il y a 16382 adresses IP dans chaque Subnet !

**Étape 6 :** on calcule aussi le nombre de Subnet: 22 = 4. Il y a 4 SubnetsN

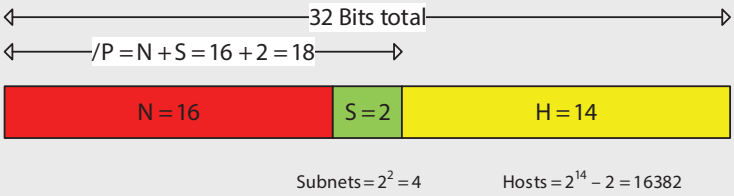



Subnet 185.240.32.0, Masque 255.255.192.0, N = 16, S = 2, H = 14

# Analyse des masques de sous-réseaux

## Définir un sous-réseaux (Subnet)

- Un Subnet détient 2H valeurs où H est le nombre de bits pour les Hosts défini par le masque
- Deux valeurs spéciales ne peuvent pas être utilisées comme adresse IP :
  - La première valeur (la plus basse) identifie le sous-réseau lui-même
  - La seconde valeur (la plus haute) identifie l adresse de broadcast
- Les valeurs restantes se situent entre ces deux valeurs spéciales et peuvent être utilisées comme adresse IP




Subnet 185.240.32.0, Masque 255.255.192.0,
N = 16, S = 2, H = 14

Identifier l ID d un Subnet:

Étape 1 : convertir le masque en prefix (/P) et la longueur de la partie Host (32 - P)
Étape 2 : convertir l adresse IP en son equivalent binaire
Étape 3 : copier les bits de prefix de l adresse IP
Étape 4 : écrire des 0 pour la partie Hosts
Étape 5 : convertir le restant de bits en decimal, par sequence de 8 bits

| Point clé sur le Subnet ID | |
|---|---|
| Définition | Valeur qui identifie le sous-réseau |
| Valeur numérique | Premier nombre du sous-réseau |
| Synonyme | Subnet, prefix, subnet address |
| Synonyme utilisé | Network, network ID, network number |
| Visualisable dans | Tables de routage, documentation |

| Point clé sur le broadcast | |
|---|---|
| Définition | Valeur qui représente l'adresse de broadcast qui permetà un routeur d'envoyer un paquetà tous les Hosts du sous-réseau |
| Valeur numérique | Dernière nombre du sous-réseau |
| Synonyme | Directed broadcast address |
| Synonyme utilisé | Network broadcast |
| Visualisable dans | Le calcul des adresses de sous-réseau |

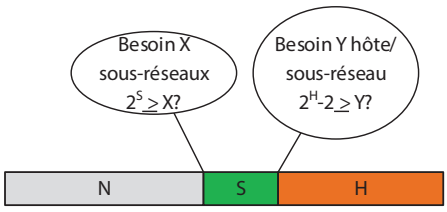
Trouver le Subnet ID avec des masques compliqués

Étape 1 : si l octet du masque = 255, alors copier le décimal de l adresse IP
Étape 2 : si l octet du masque = 0, alors écrire que des 0
Étape 3 : sinon, calculer le magic number (256 – masque). Mettre la valeur du Subnet en le multipliant avec le magic number le plus proche de l adresse IP

Trouver le Broadcast ID avec des masques compliqués

Étape 1 : si l octet du masque = 255, alors copier le Subnet ID
Étape 2 : si l octet du masque = 0, alors écrire que des 0
Étape 3 : sinon, calculer le magic number (256 – masque). Prendre la valeur du Subnet ID, ajouter le magic number et soustraire 1 (ID + magic -1)

# Analyse des masques de sous-réseaux




| Nombre de bits | $2^x$ | Nombre de bits | $2^x$ | Nombre de bits | $2^x$ | Nombre de bits | $2^x$ |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 5 | 32 | 9 | 512 | 13 | 8192 |
| 2 | 4 | 6 | 64 | 10 | 1024 | 14 | 16384 |
| 3 | 8 | 7 | 128 | 11 | 2048 | 15 | 32768 |
| 4 | 16 | 8 | 256 | 12 | 4096 | 16 | 65536 |

réseauTrouver tous les masques : La méthode mathématique

Étape 1 : Calculer le préfixe de la valeur minimale de sous-réseau où P = N + S
Étape 2 : Calculer le préfixe long sur la base de la valeur minimale de H où P = 32 – H
Étape 3 : La gamme de masques valides inclut toutes les valeurs P / découvertes avec les étapes 1 et 2.

Choisir le meilleur masque :
Maximiser le nombre d'hôtes par sous-réseau en utilisant le masque au préfixe le plus court possible. Maximiser le nombre de sous-réseaux en utilisant un masque au préfixe plus long.

Pour maximiser les hôtes et les sous-réseaux, choisir une valeur de préfixe intermédiaire (entre le plus court et le plus long).

Méthode formelle de sélection de masques de sous-réseaux :

**Étape 1 :** Déterminer le nombre de bits de réseau (N) par régles de classe.

**Étape 2 :** Calculer Le nombre minimal de bits de sous-réseau (S) Afin que 2S => Le nombre de sous-reseaux requis.

**Étape 3 :** CalculeR le nombre minimal de bits de hôte (H) afin que 2H – 2 => le nombre requis de hôtes pas sous-reseau.

**Étape 4 :** Si N + S + H > 32, aucun masque ne fonctionnera.

**Étape 5 :** Si N + S + H = 32, un masque fonctionne. Calculer le préfixe /P avec P = N + S.

**Étape 6 :** Si N + S + H < 32, plusieurs masques rencontrent l exigence. Poursuivre avec une des étapes suivantes

- Calculer le masque /P basé sur le nombre minimal de S qui maximize le nombre de hôtes par sous-réseau
- Calculer le masque /P basé sur le nombre minimal de H où P = 32 -H afin de maximiser le nombre de sous-réseaux
- Observer que la gamme complète de masques inclus tous les préfixes entre les deux calculs précédents

Trouvez toutes possibilités de masques de sous-réseau pour le réseau 150.20.0.0, où le besoin est de 125 sous-réseaux et de 250 hôtes par sous-réseau.

Étape 1 : 150.20 est de classe B, alors H = 16 bits.

Étape 2 : Le nombre minimal de bits de sous-réseau (S) est 7 parce que 125 est moins que 27 = 128

Étape 3 : Le nombre minimal de bits hôtes (H) est 8 parce que 250 est moins que 28 = 256

Étape 4 : 16 + 7 + 8 = 31 il y a alors plusieurs masques rencontrant la demande.

Le masque de sous-réseau minimal est /23 et le masque de sous-réseau maximal est /24.

Pour /23, le sous-réseau est 150.20.0.0/23.

Pour /24, Les sous-réseaux sont 150.20.0.0/24 et 150.20.1.0/24.

# Configuration de sous-réseau

Voici le procédé formel pour trouver toutes les identités de sous-réseaux dans un réseau et un sous-réseau simple.

Étape 1 : Inscrire le masque de sous-réseau en nombre décimale à la première rangée du tableau.

Étape 2 : Trouver l'octet ayant une valeur autre que 255 ou zero.

Étape 3 : Calculer le chiffre magique en soustrayant l'octet de 256.

Étape 4 : Inscrire le réseau par classe qui est le sous-réseau zero.

Étape 5 : Pour déterminer tous les réseaux successifs, ajouter le chiffre magique à l'octet et copier les trois autres nombres.

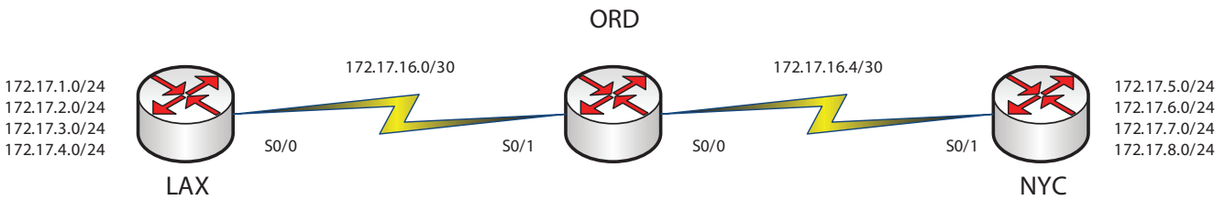
Étape 6 : Arrêter lorsque l'octet arrive à 255..

| Octet | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| Masque | 255 | 255 | 192 | 0 |
| Chiffre magique | 0 | 0 | 64 | 0 |
| Nombre de réseaux/ Zero Sous-réseau | 180 | 32 | 0 | 0 |
| Sous-réseau suivant | 180 | 32 | 64 | 0 |
| Sous-réseau suivant | 180 | 32 | 128 | 0 |
| Diffusion du sous-réseau | 180 | 32 | 192 | 0 |

Utilisez le tableau ci-dessous pour trouver toutes les identités de sous-réseaux pour 180.32.0.0 masque 255.255.192.0

# Masques de sous-réseau à longueurs variables (VLSM)

24Réseau 172.17.0.0/16 divisé parmi plusieurs routeursProtocole




Voici comment ajouter un nouveau sous-réseau à une configuration VLSM existante

Étape 1 : Choisir le masque de sous-réseau (ou la longueur du préfixe) désiré pour le nouveau sous-réseau, basé sur le nombre de hôtes pour ce sous-réseau.

Étape 2 : Calculer le nombre de tous les sous-réseaux possibles du réseau de classe en employant le masque de l étape précédente et l adresse IP de diffusion du sous-réseau.

Étape 3 : Énumérer les adresses de diffusion IP des sous-réseaux existants et les identités de ces sous-réseaux.

Étape 4 : Éliminer le chevauchechement entre sous-réseaux en comparant avec étapes 2 et 3.

Étape 5 : ChoIsir l identité du nouveau sous-réseau parmi les sous-réseaux restants, selon la question du plus bas ou du plus haut sous-réseau.

Dans l exemple ci-après, nous voulons ajouter un autre /23 à R3. Une fois le chevauchement de sous-réseau résolu, nous pourrons utiliser 172.17.136/23 comme nouveau sous-réseau.

| Protocole de routage | Es-ce sans classe? | Masques envoyés dans mises à jour? | Soutien VLSM? | Soutien Pour agrégation de route de façon manuelle? |
|---|---|---|---|---|
| RIP-1 | Non | Non | Non | Non |
| IGRP | Non | Non | Non | Non |
| RIP-2 | Oui | Oui | Oui | Oui |
| EIGRP | Oui | Oui | Oui | Oui |
| OSPF | Oui | Oui | Oui | Oui |

## Configuration de VLSM Avec chevauchement possible

S'il y a chevauchement entre sous-réseaux, les hôtes et les périphériques pourraient êtres incapables de s'identifier (ping) ou de diffuser entre eux.

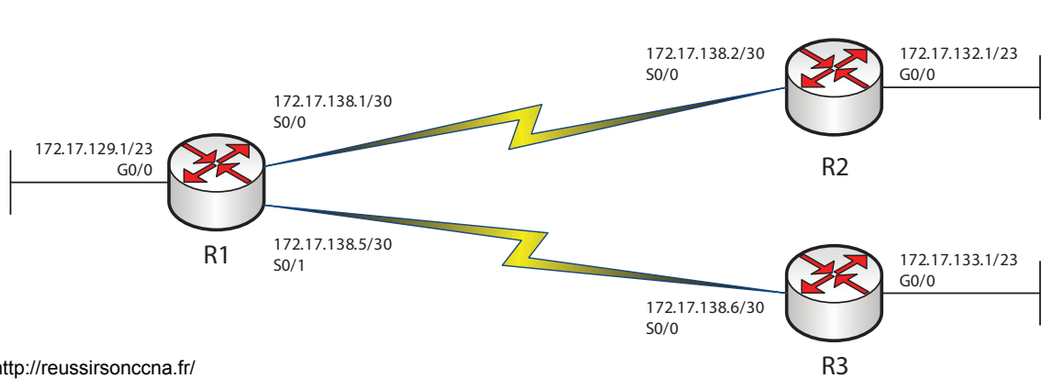
Afin de vérifier s'il y a chevauchement, suivez ce protocole :

Étape 1 : Calculez l identité du sous-réseau et de l adresse IP de diffussion pour chaque sous-réseau.

Étape 2 : Énumérez les identités des sous-réseaux et les adresses de diffusion IP en ordre numérique.

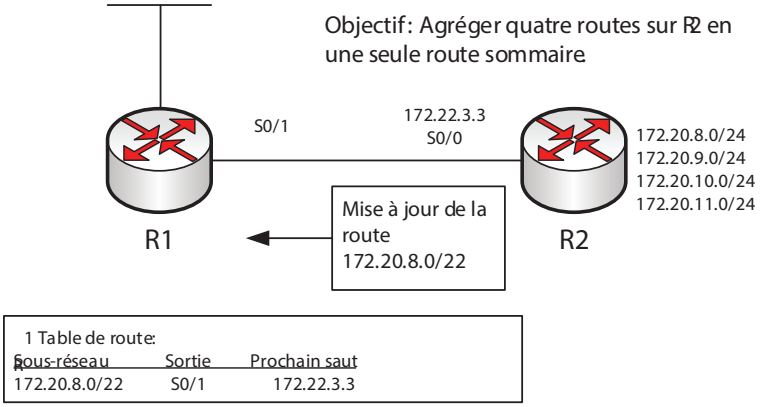
Étape 3 : Vérifiez la liste pour chevauchements possibles.

Dans l'exemple à droite, les IP des sous-réseaux R2 LAN et R3 LAN se chevauchent.



# Agrégation des routes

L agrégation des routes est l'agrégation de plusieurs routes contiguës en une seule mise à jour. L'agrégation réduit les demandes sur d'autres routeurs et permet à l'ingénieur de réseau d'agréger des réseaux ensemble. Certains protocoles de routageeffectuent l agrégation des routes de façon automatique. Attention à certaines situations ou cette agrégation n'est pas recommandée. L'agrégation manuelle fonctionne bien lorsque les routes traversent les puisances binaires de 2 (tel que 4, 5, 6, 7).




Choisir la meilleure agrégation

Élément important : La meilleure agrégation de routes contient la plus petite gamme d adresses qui incluent tous les sous-réseaux à agréger dans une seule route.

Comment trouver la meilleure agrégation de routes :

**Étape 1 :** énumérez toutes les routes subordonnées à agréger, de la plus basse à la plus élevée.

**Étape 2 :** noter la basse et la haute route des sous-réseaux subordonnés en examinant l'identité du sous-réseau le plus bas et l'adresse de diffusion la plus élevée.

**Étape 3 :** sélectionnez le point de départ de la longueur du préfixe (/P) pour la prochaine étape, en choisissant le masque de préfixe le plus court parmi tous les sousréseaux subordonnés, et soustraire 1.

**Étape 4 :** calculer un préfixe sommaire potentiel et un masque basé sur l'identité du sous-réseau la plus inférieure de la liste et sur la longueur du préfixe.

Si la gamme entière est incluse dans le sommaire de la route, arrêtez ici
Si non, soustraire 1 de la longueur du préfixe et répéter l étape 4.

Exemple : Agréger les routes suivantes – 172.20.8.0/24, 172.20.9.0/24, 172.20.10.0/24, et 172.20.11.0/24.

**Étape 1 :** l'identité du sous-réseau le plus bas est 172.20.8.0 et l IP de diffusioon le plus haut est 172.20.11.255.

**Étape 2 :** puisque nous amalgamons quatre /24 routes, Nous pouvons soustraire 2 du préfixe et le préfixe résultant est /22.

La route agrégée est 172.20.8.0/22. L'identité du sous-réseau est 172.20.8.0 et l IP de diffusion est 172.20.11.255.

# IMPLÉMENTATION DU ROUTAGE IPV4

## Installation d un routeur :

Étape 1 : Connecter les câbles LAN aux ports LAN du routeur

Étape 2 : si on utilise un CSU/DSU externe, brancher l interface série au CSU/DSU et connecter le CSU/DSU à la ligne operateur

Étape 3 : si on utilise un CSU/DSU interne, brancher directement la ligne operateur sur l interface série du routeur

Étape 4 : Connecter le port console du routeur au PC avec un câble console. Cela permet de configurer le routeur depuis son PC

Étape 5: Connecter le câble d alimentation sur le routeur

Étape 6 : allumer le routeur

## Similitudes entre la CLI d un switch et d un routeur

- Les modes User et Enable (privilégié)
- Entrer et sortir d un mode de configuration avec les commandes end , exit et/ou la combinaison Ctrl+Z
- Configuration de la console, telnet and le mot de passe secret
- Configuration des clés de chiffrement SSH et de la base d utilisateurs
- Configuration du hostname et description des interface
- Configuration des interfaces Ethernet, speed, duplex, shut/no shut
- Aide en ligne, édition des commandes et rappel d une commande tapée
- Utilisation de la commande debug
- Le mode SETUP
- La startup-config, la running-config, les serveurs externes FTP, la commande copy

...

La CLI du routeur et du switch diffère sur deux aspects :

- La configuration des adresses IP peut être différente selon les cas
- Le routeur à un port auxiliaire (AUX) qui permet de connecter un modem ou une ligne
- téléphonique pour un accès a distance.

Code de status dune interface

| Nom | Localisation | Description |
|---|---|---|
| Line status | Premier code | État de la couche physique |
| Protocol Status | Deuxième code | État de la couche Liaison de données |

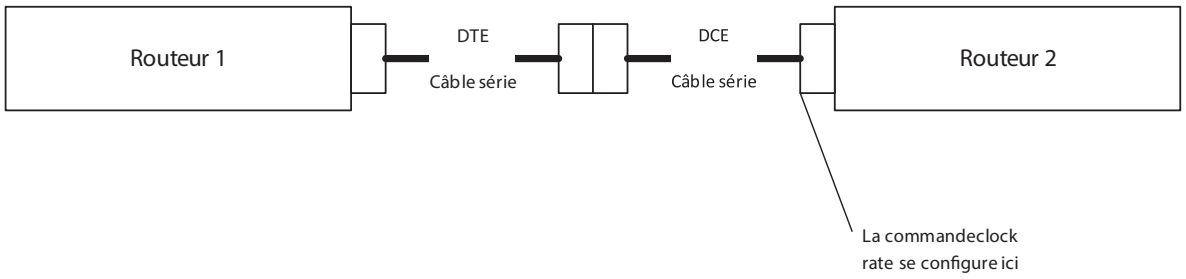
Combinaison des codes de status dune interface

| Line Status | Protocol Status | Raison |
|---|---|---|
| Administratively Down | Down | L'interface est désactivée (Shutdown) |
| Down | Down | L'interface est activée (no shutdown) mais la couche physique ne fonctionne pas pb de câble, équipement voisin éteint.. |
| Up | Down | Pb relatif à la liaison de données Généralement vu avec du HDLC ou PPP |
| Up | Up | Les couches physique et liaison de données fonctionnent! |

Configuration de l int GigabitEthernet 0/0 avec l adresse IP 10.1.1.1/24 et de l interface Serie 0/0/0 avec l adresse IP 10.255.255.1/30

```
R1(config)# interface Gi0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface S0/0/0
R1(config-if)# ip address 10.255.255.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
R1# show protocols
```

GigabitEthernet0/0 is up, Line protocol is up Internet address is 10.1.1.1/24Serial0/0/0 is up, Line protocol is up Internet address is 10.255.255.1/30




Configuration du Clock Rate sur R2 avec une valeur à 1.544 Mbps.

```
R2(config)# interface Serial0/0
R2(config-if)# clock rate 1544000
R2(config-if)# exit
R2(config)#
```

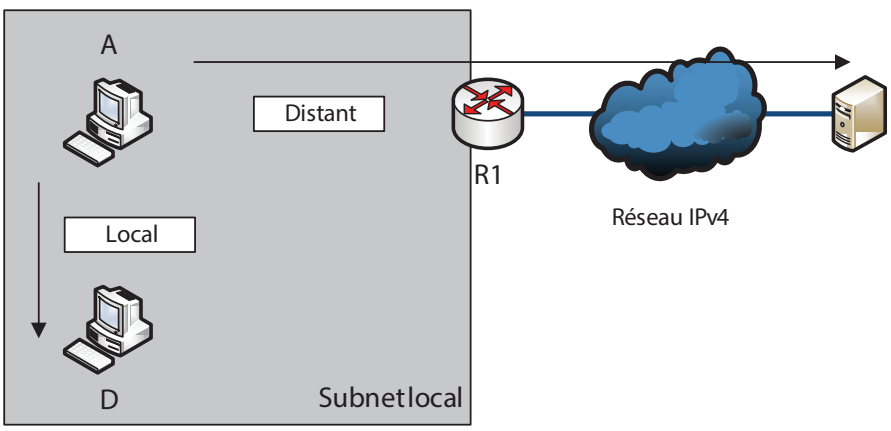
Règle d'un PC pour la transmission d un paquet:

Étape 1 : si la destination est dans le réseau local, l envoi est direct:

- Identifie l adresse MAC du destinataire. Pour cela utilise le cache ARP ou le protocole ARP pour récupérer l adresse MAC.
- Encapsule le paquet dans un nouvel entête niveau 2 avec l adresse MAC de destination.

Étape 2 : si la destination est distante, l envoi se fait vers la passerelle:

- Identifie l adresse MAC de la passerelle. Pour cela utilise le cache ARP ou le protocole ARP pour récupérer l adresse MAC.
- Encapsule le paquet dans un nouvel entête niveau 2 avec l adresse MAC de la passerelle comme destination.

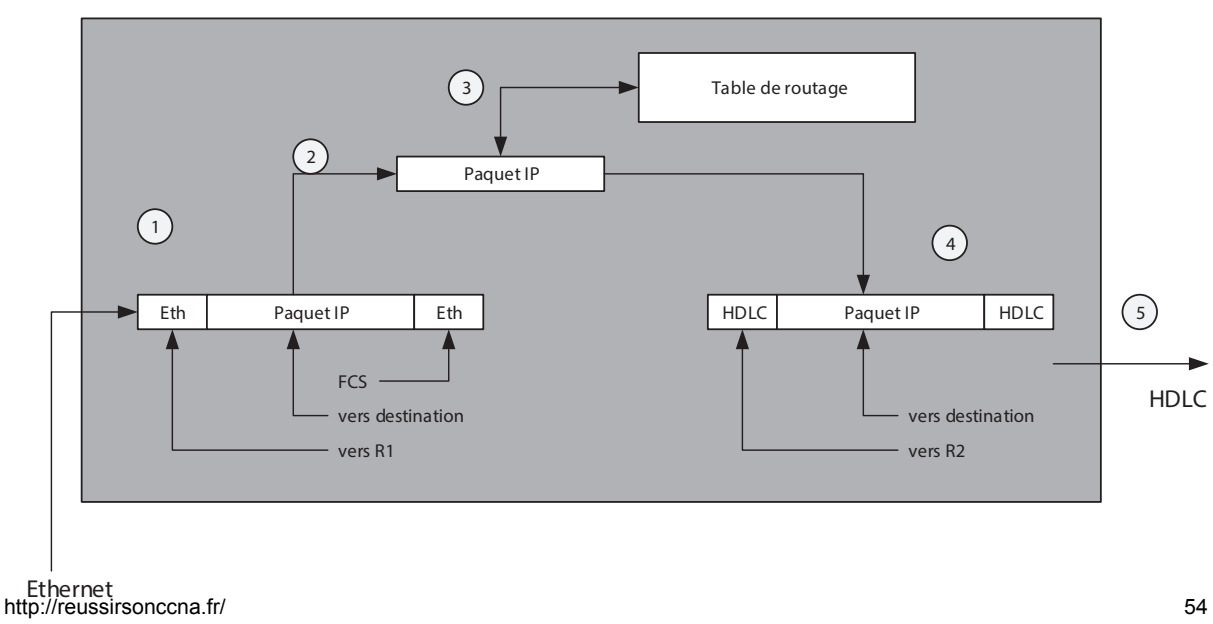



Règle d un routeur pour la transmission d un paquet:

Étape 1 : pour chaque trame niveau 2 reçue, la traiter uniquement si :

- La trame ne contient pas d erreur (vérification du FCS)
- L adresse MAC de destination de la trame correspond à celle de l interface du routeur (peut aussi être une adresse multicast ou broadcast)

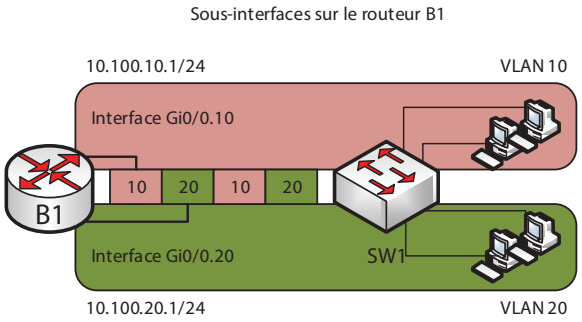
Étape 2 : si OK alors extraire le paquet IP de cette trame.
Étape 3 : en fonction de l adresse IP de destination, trouver la meilleure route pour le réseau de destination et l envoyer vers l interface de sortie du routeur pour encapsulation
Étape 4 : Encapsulation dans un entête niveau 2. Même principe que pour un PC



# Configuration adressage IPv4 et routes

| Fonction d'amélioration du routage | Process Switching | Fast Switching | CEF |
|---|---|---|---|
| Optimisation des entêtes niveau2 pour l'encapsulation | Non | Oui | Oui |
| Utilisation d'une table plus rapide que la table de routage | Non | Oui | Oui |
| Organisation des tables en utilisant une structure hiérarchique pour réduire le temps de recherche de destination | Non | Oui | Oui |

Cisco Express Forwarding(CEF)




Type de route :

**Connected:** la route est automatiquement ajoutée car l adresse IP d une interface du routeur appartient à ce réseau.Static : route ajoutée manuellement par l'administrateur avec la commande ip route.
**Routing protocols:** route apprise dynamiquement car annoncée par un routeur voisin.

Routage entre VLANsIl existe 3 possibilités pour avoir du routage inter-VLANs :

- Utiliser un routeur avec des interfaces Ethernet et chaque interface sur un VLAN particulier
- Utiliser un routeur avec une configuration Trunk entre le routeur (sous-interface) et le switch
- Utiliser un switch niveau 3

Configuration d'une sous-interface :
Interface du routeur ayant l'adresse IP 10.10.1.1/24 dans le VLAN 20

```
Interface Eth0.20
  encapsulation dot1q 20
  ip address 10.10.1.1 255.255.255.0
```

Points clés sur la configuration du VLAN natif sur un routeur

Méthode 1 : configurer l adresse IP sur l interface physique mais sans préciser l encapsulation le routeur considère que l interface physique appartient au VLAN natif.

Méthode 2 : configurer l adresse IP sur une sous-interface en précisant la commande encapsulation...native.

Rappel : le VLAN natif est le VLAN ou les trames ne sont pas taggées. Par exemple, supposons que le VLAN natif est le 100

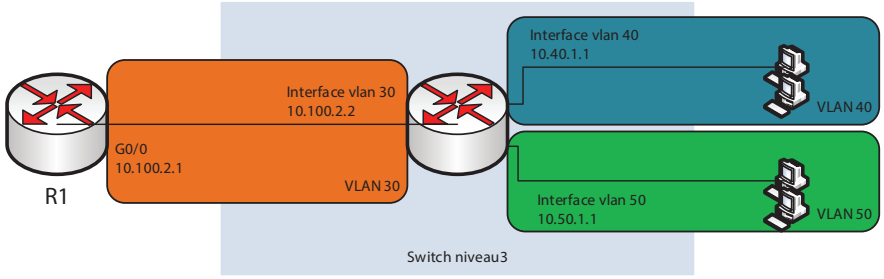
**Méthode 1 :**

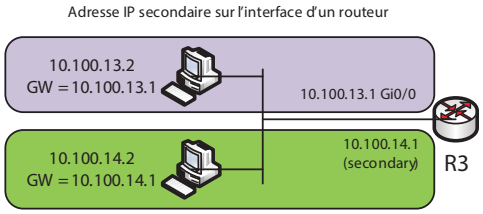
```
Interface gi0/0
ip address 10.100.1.1 255.255.255.0
!
Interface gi0/0.200
encapsulation dot1q 20
ip address 10.200.1.1 255.255.255.0 (Ici on precise un autre VLAN, 20 par exemple)
```

**Méthode 2 :**

```
Interface gi0/0.10
encapsulation dot1q 10 native
ip address 10.100.1.1 255.255.255.0"
```

# Configuration adressage IPv4 et routes

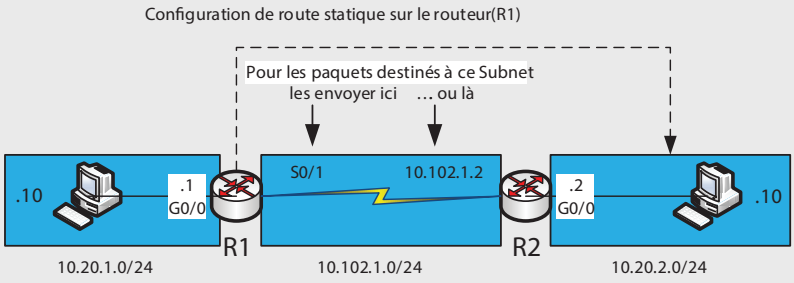



Activation du routage sur un switch Cisco
Étape 1 : activer le support du routage avec la command sdm prefer lanbase-routing et faire un reload.
Étape 2 : une fois redémarré, activer le routage avec ip routing.
Étape 3 : créer des interface VLAN pour chaque VLAN avec la commande interface VLAN...
Étape 4 : configurer une adresse IP pour chaque interface VLAN avec la commande ip address
Étape 5 : activer les interfaces VLAN avec la commande no shutdown.
Exemple de configuration (apres un reload) ip routing

```
!
interface vlan 30
ip address 10.100.2.2 255.255.255.0
no shutdown
!
interface vlan 40
ip address 10.40.1.1 255.255.255.0
no shutdown
!
interface vlan 50
ip address 10.50.1.1 255.255.255.0
no shutdown
!
```

"Configuration de route statique sur le routeur (R1)
**ip route 10.20.2.0 255.255.255.0 10.102.1.2 (ou)**
**ip route 10.20.2.0 255.255.255.0 S0/1"**




Une **route statique** est utilisée lorsque l architecture n est pas supposée changer ou pour une destination en particulier.
Cisco autorise la configuration d une route statique en déclarant l adresse IP du routeur voisin ou l interface locale de sortie (ex Serial 0/1).
La route statique a une **Distance Administrative** à 1 et sera toujours prioritaire aux routes reçues par les protocoles de routage

Fonctions d un protocole de routage

- Apprentissage par les routeurs voisins des Subnet IP joignables
- Annonce aux routeurs voisins des Subnet IP joignables
- S il existe plus d une route pour un Subnet particulier, choisir la meilleure route. Ce choix est basé sur une ou plusieurs métriques (metrics).
- Si la topologie change (un lien tombe par ex.), prévenir les routeurs voisins et trouver une route alternative

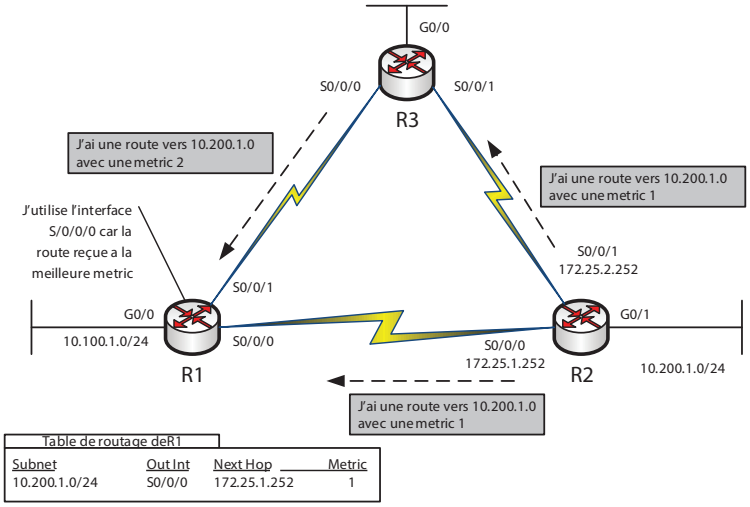
Protocoles de routage interne et externe

Interior Gateway Protocol (IGP) : protocole utilisé au sein d un Autonomous System (AS)
Exterior Gateway Protocol (EGP) : protocole utilisé entre différents Autonomous System (ex: BGP pour Internet)

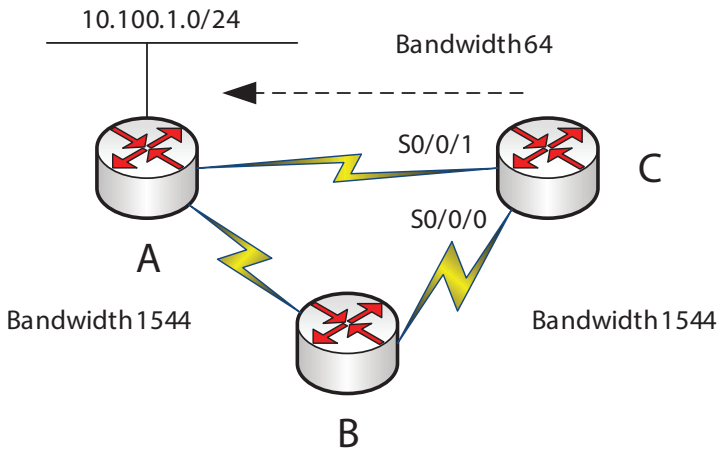
Il existe 3 algorithmes dans les protocoles IGP:

- Distance Vector (ex : RIPv2, IGRP)
- Advanced Distance Vector (ex: EIGRP)
- Link-state (ex: OSPFv2, IS-IS)

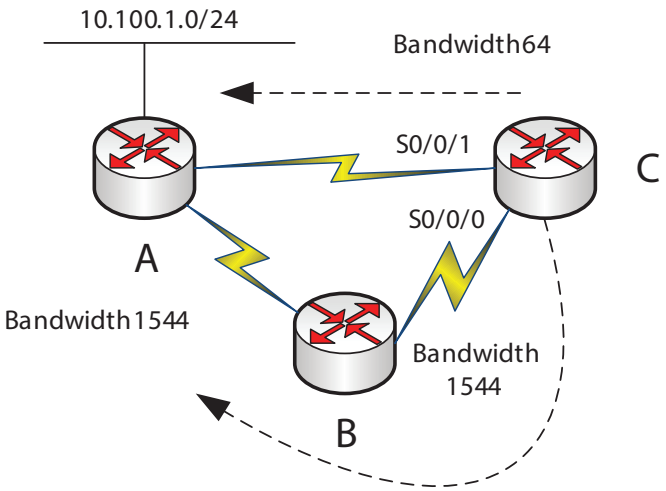
| IGP Metrics IGP | | |
|---|---|---|
| IGP | Metric | Description |
| RIPv2 | Hop Count | Nombre de Hops (de routeurs) entre le Subnet distant et le routeur |
| OSPF | Cost | Somme du Cost (coût) de toutes les interfaces traversées pour atteindre un Subnet Le Cost est par basé sur la Bandwidth de l'interface |
| EIGRP | Composé de la bande passante et du délai | Calcul basé sur le lien le plus lent et sur le délai cumulé de toutes les interfaces traversées pour atteindre un Subnet |



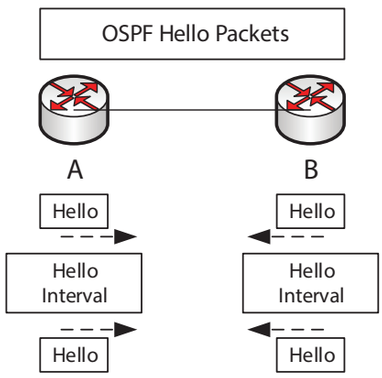

RIP – Hop Count




EIGRP - Composé



| Comparaison de protocoles de routage de type IGP | | | | | |
|---|---|---|---|---|---|
| Fonctionnalités | RIP-1 | RIP-2 | EIGRP | OSPF | IS-IS |
| Classless / Envoi le masques dans les update/ supporte le VLSM | non | oui | oui | oui | oui |
| Algorithme(DV, Advanced DV, LS) | DV | DV | Adv. DV | LS | LS |
| Supporte le résumé de route manuel | non | oui | oui | oui | oui |
| Propriétaire Cisco | non | non | oui | non | non |
| Envoi des updates en multicast | non | oui | oui | oui | N/A |
| Convergence | lent | lent | rapide | rapide | rapide |




| Administrative Distances– Valeurs par défaut | |
|---|---|
| Type de route | Administrative Distance |
| Connected | 0 |
| Static | 1 |
| BGP (external routes) | 20 |
| EIGRP (internal routes) | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| EIGRP (external routes) | 170 |
| BGP (internal routes) | 200 |
| Unusuable | 255 |

## Configuration OSPF

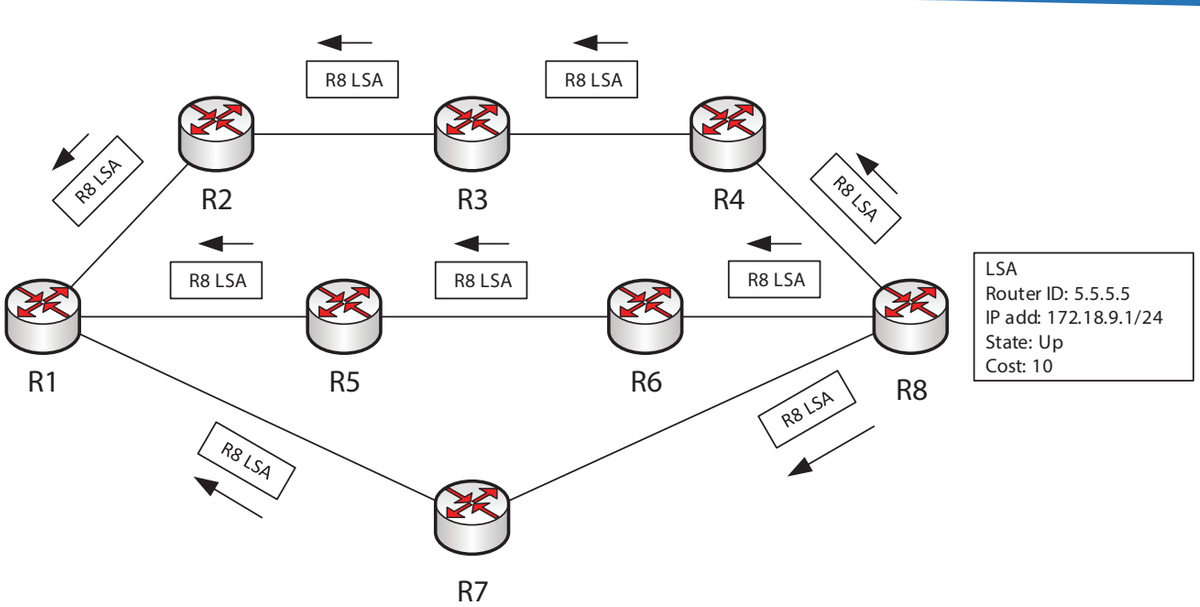
Étape 1 : entrer dans le mode de configuration OSPF en définissant un numéro de processus avec la commande router ospf PROCESS_ID

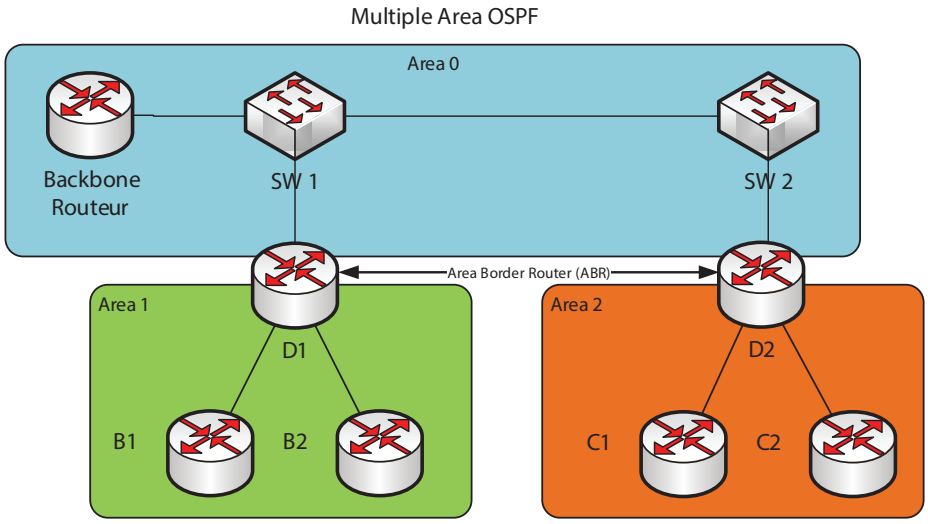
Étape 2 : optionnel – Définir un identifiant du routeur avec la commande router-id VALEUR

Étape 3 : configurer une ou plusieurs entrée pour déclarer des Subnet avec la commande network IP- ADDRESS WILDCARD-MASK area AREA_ID

## Configuration OSPF du routeur B (single area)

```
B(config)# router ospf 1
B(config-router)# router-id 1.2.3.4
B(config-router)# network 10.100.2.0 0.0.0.255 area 2
B(config-router)# exit
```






## Valeur du router-id pour OSPF

**1)** Si la commande router-id VALUE est déclarée alors elle
est utilisée.
**2)** sinon OSPF utilise l adresse IP de la loopback comme router-id. Si plusieurs loopback présents alors c est l adresse IP la plus élevée qui est choisie (199.x.x.x sera choisie par rapport a 12.y.y.y)
**3)** sinon OSPF choisit l adresse IP la plus élevée parmi toutes les autres interfaces physiques qui sont dans un état opérationnel (UP/UP)

### Configuration du router-id

```
C1(config)# router ospf 1
C1(config-router)# router-id 10.255.0.1

ou
C2(config)# interface Loopback1
C2(config-if) ip address 10.254.0.1
255.255.255.255
```

| Valeurs classiques du Wildcard en OSPF | |
|---|---|
| Wildcard Mask | Signification |
| 0.0.0.0 | les 4 octets doivent correspondre |
| 0.0.0.255 | les 3 premiers octets doivent correspondre |
| 0.0.255.255 | les 2 premiers octets doivent correspondre |
| 0.255.255.255 | le premier octet doit correspondre |
| 255.255.255.255 | N'importe quelle valeur |

| Exemples de la commande network et signification | |
|---|---|
| Commande | Signification de la commande |
| Network 10.1.0.0 0.0.255.255 | Si l'IP de l'interface du routeur commence par 10.1 alors OSPF annonce le Subnet associé |
| Network 10.0.0.0 0.255.255.255 | Si l'IP de l'interface du routeur commence par 10. alors OSPF annonce le Subnet associé |
| Network 0.0.0.0 255.255.255.255 | OSPF annonce le Subnet de toutes les interfaces |
| Network 10.1.12.0 0.0.255.255 | Si l'IP de l'interface du routeur commence par 10.1.12. alors OSPF annonce le Subnet associé |
| Network 10.1.12.1 255.255.255.255 | Si l'IP de l'interface du routeur est 10.1.12.1 alors OSPF annonce le Subnet associé |

### Passive Interface OSPF

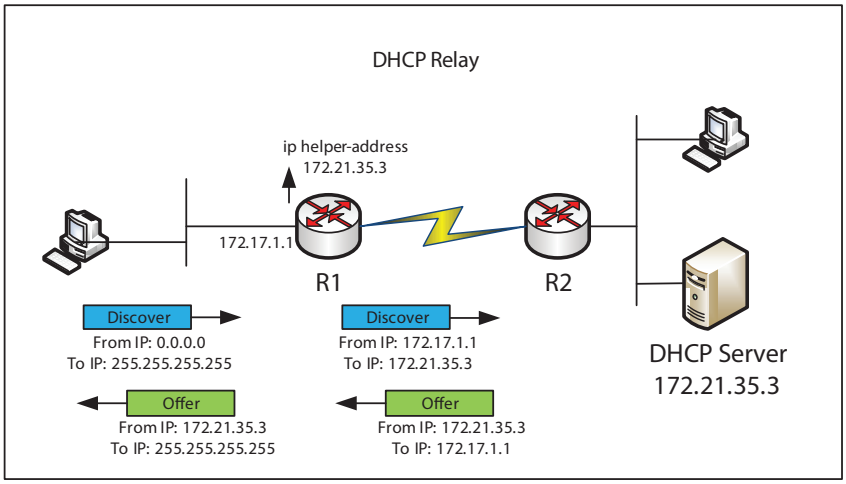
La passive interface est utilisée pour stopper la relation OSPF entre 2 routeurs. La configuration de la passive interface provoque:

- L'arrêt de l envoi des Hellos OSPF sur cette interface
- Ignore les Hellos OSPF reçu sur cette interface
- Interdit toute adjacence OSPF sur cette interface

**Exemple de configuration :**

```
router ospf 1
  passive-interface gigabitethernet0/0.10
  passive-interface gigabitethernet0/0.20
```

| Messages du protocoleDHCP | |
|---|---|
| **Message DHCP** | **Description** |
| Discover | Envoyé par le client DHCP pour trouver un serveur DHCP |
| Offer | Envoyé par le serveur DHCP afin doffrir une adresse IP ainsi que d'autres paramètres (bail, passerelle) |
| Request | Envoyé par le client DHCP pourconfirmer l'offre d'adresse IP du serveur DHCP |
| Acknowledgement | Envoyé par le serveur DHCP pour réserver cette adresse IP pour ce client en particulier |
| Adresses DHCP spéciales<br>0.0.0.0 est utilisée comme adresse IP source par les clients qui n'ont pas encore d'adresse IP attribuée.<br>255.255.255.255 est l'adresse IP de broadcast | |




Configuration du DHCP sur un routeur Cisco

Étape 1 : Exclure de la plage les adresses IP non souhaitées avec la commande **ip dhcpexcluded-address** PREMIERE_IP DERNIERE_IP

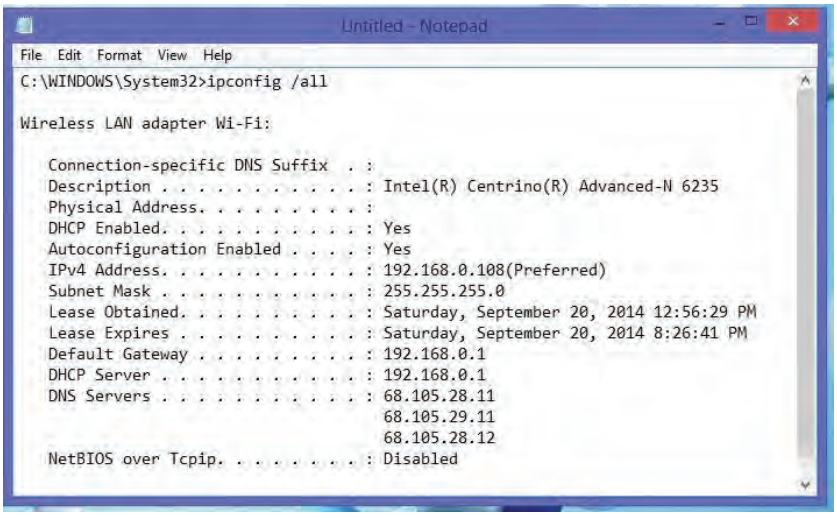
Étape 2: Créer une plage DHCP (scope) avec la commande ip dhcp pool NAME

Étape 3:

Définir le Subnet avec la commande network subnet-ID mask or network subnet-ID prefix
Définir la passerelle avec la commande default-router ADDRESS
Définir le(s) serveur(s) DNS avec la commande dns-server ADDRESS_1 ADDRESS_2
Définir la durée du bail (lease) pour ces informations avec la commande lease DAYS HOURS MINUTES
Définir le nom de domaine DNS avec la commande domain-name NAME

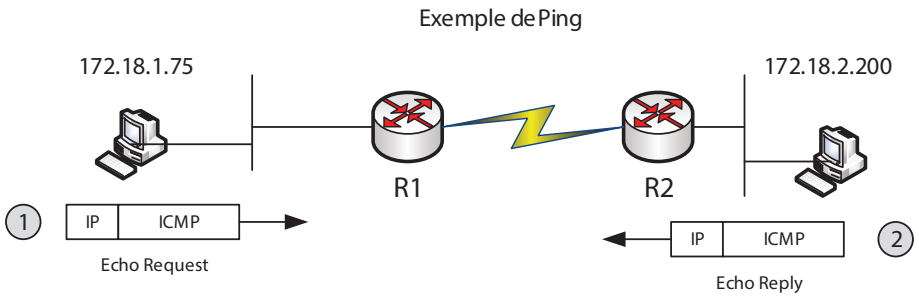
Exemple de configuration:

```
ip dhcp excluded-address 172.18.1.1
172.18.1.40
!
Ip dhcp pool subnet1
network 172.18.1.0 255.255.255.0
dns-server 172.17.16.34
default-router 172.18.1.1
lease 1 0 0
domain-name myexample.com
```




Quand la commande ip helper-address SERVER_IP est configurée, le routeur effectue les actions suivantes:

1) Vérifie que le paquet DHCP reçu a bien la valeur 255.255.255.255 comme adresse IP destination IP
2) Change l adresse IP source par celle de l interface du routeur
qui a reçu le paquet DHCP
3) Change l adresse IP de destination par l adresse du serveur DHCP définie par la commande ip helper-address
4) Transmet le paquet au serveur DHCP



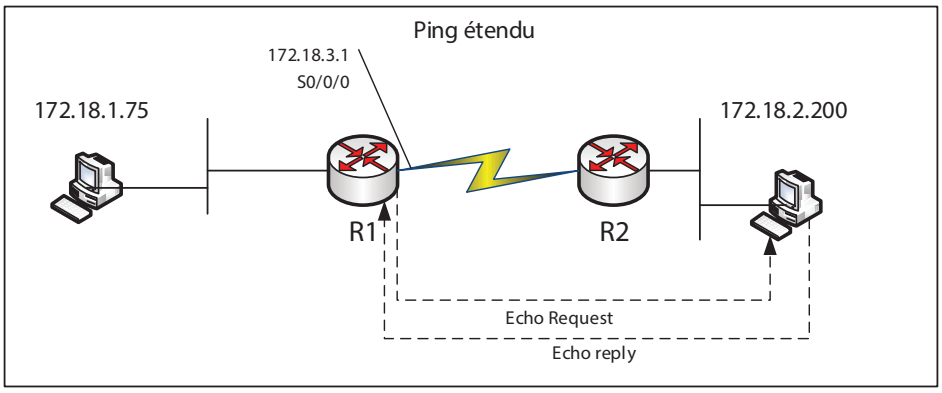

Information sur le routage

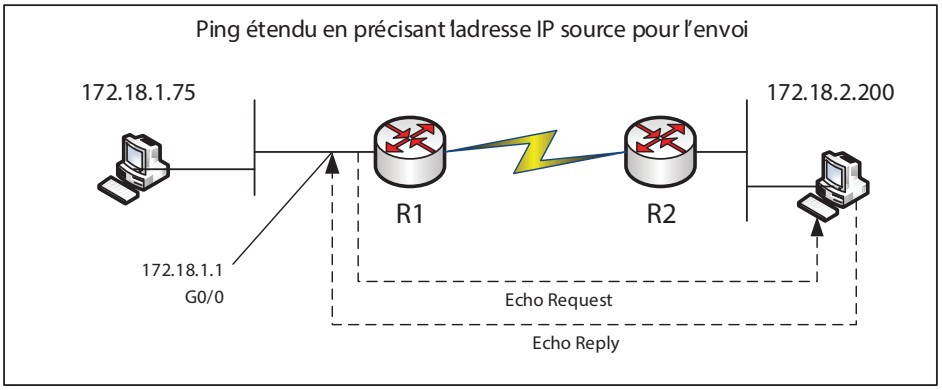
- Le PC (host) et sa passerelle par défaut (routeur) doivent être dans le même LAN
- L adresse IP du PC et celle de la passerelle doivent être dans le même Subnet
- La valeur de la passerelle configurée sur le PC doit être identique à celle configurée sur l interface du routeur

## Ping et Ping étendu

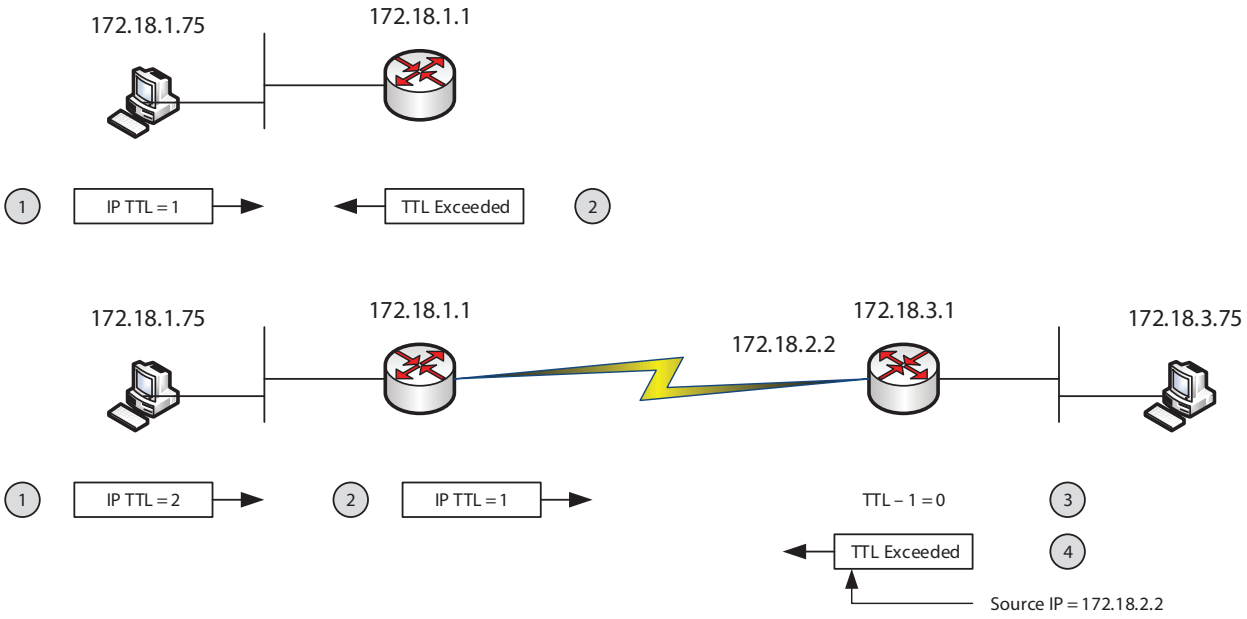
Un Ping régulier d un routeur envoi 5 paquets ICMP echo vers la destination. Si la destination est présente alors elle renverra 5 paquets echo-reply. Il se peut que les premiers paquets envoyés ne reçoivent pas de réponses due au temps de résolution ARP.

Un Ping étendu peut prendre plusieurs paramètres : l adresse IP source, le nombre de paquet à envoyer, la taille



Traceroute se base sur les messages TTL (Time To Live) afin de cartographier le chemin réseau traverse. C est un outil de résolution de problème



# THÉORIE DU ROUTAGE IPV6

## MIGRATION DES PROTOCOLES IPV4 VERS IPV6

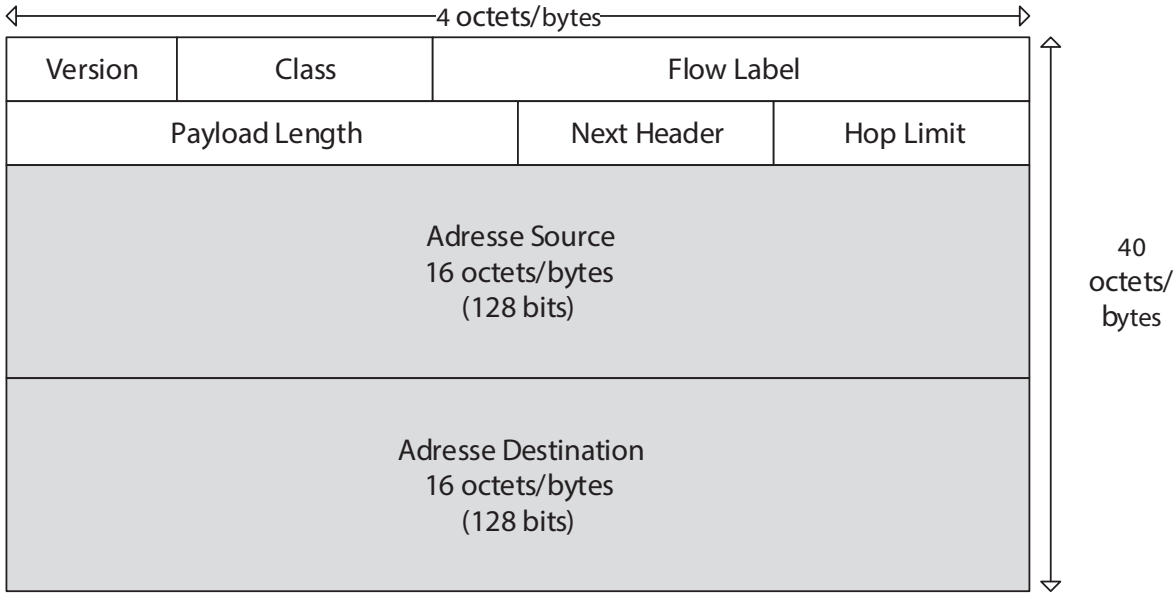
| Protocole IPv4 | Protocole IPv6 | Notes |
|---|---|---|
| OSPFv2 | OSPFv3 | OSPFv3 supporte IPv6 |
| ping | ping6 | Ping6 supporte IPv6 |
| ARP | Neighbor Discovery Protocol (NDP) | NDP remplace ARP dans IPv6. NDP joue aussi un rôle dans l'assignement d'adresse IPv6 |
| RIPv2 | RIPng | RIPng support IPv6. "ng" signifie "Next Generation" |
| BGP 4 | MP BGP 4 | MP-BGP supporte IPv6 avec ses extensions multi-protocole |

## Points clés d IPv6 :

- Une adresse IPv6 doit être configurée sur une interface afin que celui-ci puisse recevoir ou envoyer des paquet IPv6.
- Un Host doit connaître l adresse IPv6 de sa passerelle/gateway s'il souhaite envoyer des paquets hors de son Subnet.
- Un routeur IPv6 désencapsule puis réencapsule chaque paquet IPv6 comme pour IPv4.
- Un routeur IPv6 effectue sa décision de routage en fonction de l adresse IPv6 de destination. C'est le même fonctionnement qu en IPv4

Généralement, IPv6 et IPv4 sont similaires à quelques exceptions près

Entête IPv6 (40 octets/bytes) avec une adresse IPv6 de 128-bit de long)



Comment écrire une adresse IPv6?

Comme la taille de 128 bits à écrire est long, on utilise la notation hexadécimal où A=10, B=11, C=12  F=15. Cela permet d écrire l adresse par portion de 4 chiffres hexadécimaux séparés par deux points (:).
Ce regroupement de 4 chiffres hexa est appelé quatuor. Une adresse IPv6 est composé de huit quatuors.

Règle à connaitre sur l abréviation d une adresse IPv6 :

**Règle 1 :** à l intérieur d un quatuor, on peut supprimer le ou les zéros de la gauche. S il y a 4 zéros successifs alors on écrit un seul zéro à la place
**Règle 2 :** on peut abréger deux ou plusieurs quatuors qui comportent 4 zéros chacun par un double deux-point (::). Attention, cette règle ne peut être utilisée qu une seule fois dans l écriture de l adresse IPv6.

**Exemple :** FE80:0000:0000:0000:ABCD:BFFF:CDEF:1234 peut être abrégé en FE80::ABCD:BFFF:CDEF:1234

**Exemple :** 2100:0000:0020:0200:1000:CAFD:0202:2020 peut être abrégé en 2100:0:20:200:1000:CAFD:202:2020

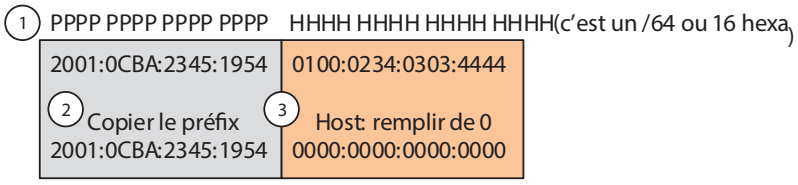
Table de conversion Binaire —— Hexa

| Hexa | Binaire | Hexa | Binaire |
|---|---|---|---|
| 0 | 0000 | 8 | 1000 |
| 1 | 0001 | 9 | 1001 |
| 2 | 0010 | A | 1010 |
| 3 | 0011 | B | 1011 |
| 4 | 0100 | C | 1100 |
| 5 | 0101 | D | 1101 |
| 6 | 0110 | E | 1110 |
| 7 | 0111 | F | 1111 |

Calcul du préfix IPv6 (Subnet ID)

Si le préfix est noté /P, alors noter les premiers P bits et changer le reste par
des zéros pour atteindre 128 bits.

Si la longueur du préfix est un multiple de 4, effectuer le calcul suivant : Diviser la longueur du préfix par 4, copier le résultat en hexadécimal puis compléter par des zéros.



# Adressage IPv6 et sous-réseau (Subnet)

Adresses IPv6 publiques et privées

Comme pour IPv4, IPv6 différencie les adresses publiques et privées :

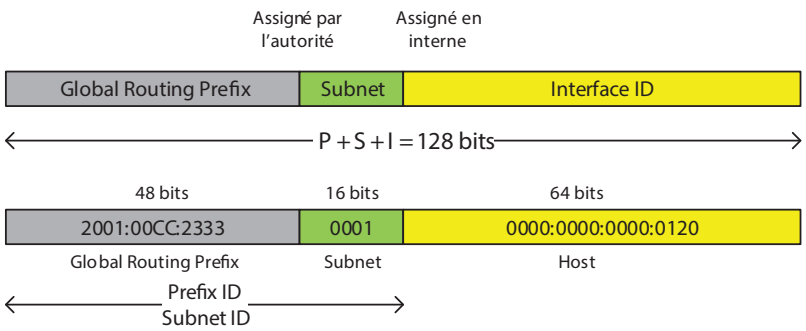
**Global unicast :** ce sont les adresses IPv6 enregistrées par une autorité de nommage sur Internet. Cet assignement est appelé Préfix et est attribué à une organisation (entreprise).

**Unique Local :** ce sont les adresses IPv6 privées car elles sont à l intérieur d une organisation. Ces adresses peuvent être utilisées par plusieurs organisations car elles restent en interne et ne sont pas routable sur Internet.

Type d adresse IPv6 et premiers nombres Hexa de l'adresse

| Type d'adresse | Premiers chiffres Hexa |
|---|---|
| Global Unicast | 2 ou 3 |
| Unique Local | FD |
| Multicast | FF |
| Link-Local | FE80 |

Structure d'une adresse IPv6 dans un Subnet




Lister les Subnet IPv6

Contrairement à IPv4 et les classes A, B et C, les Subnet IPv6 sont plus simples à identifier.
Premièrement, il faut connaître le Global Routing Prefix qui a été assigné à l organisation par l autorité de nommage.
Il faut aussi connaître les règles suivantes concernant le Subnet IPv6 :

- Tous les Subnet ID commencent par le Global Routing Prefix
- Le champ Subnet permet d identifier chaque Subnet par des valeurs différentes
- Tous les Subnet ID ont des zéros dans le champ Interface ID

Exemple : Listez les 4 premiers Subnet du Network 2002:0E88:2222::/48

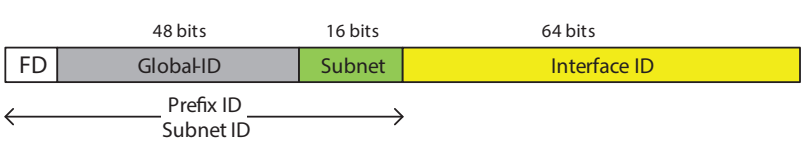
Premièrement, on sait que le Global Routing Prefix est 2002:0E88:2222
Donc nous avons 16 bits pour le champ Subnet (un quatuor) et que des zéros pour le champ Interface ID (Host)

Au final, les 4 premiers Subnet sont :
2002:0E88:2222:0000::
2002:0E88:2222:0001::
2002:0E88:2222:0002::
2002:0E88:2222:0003::

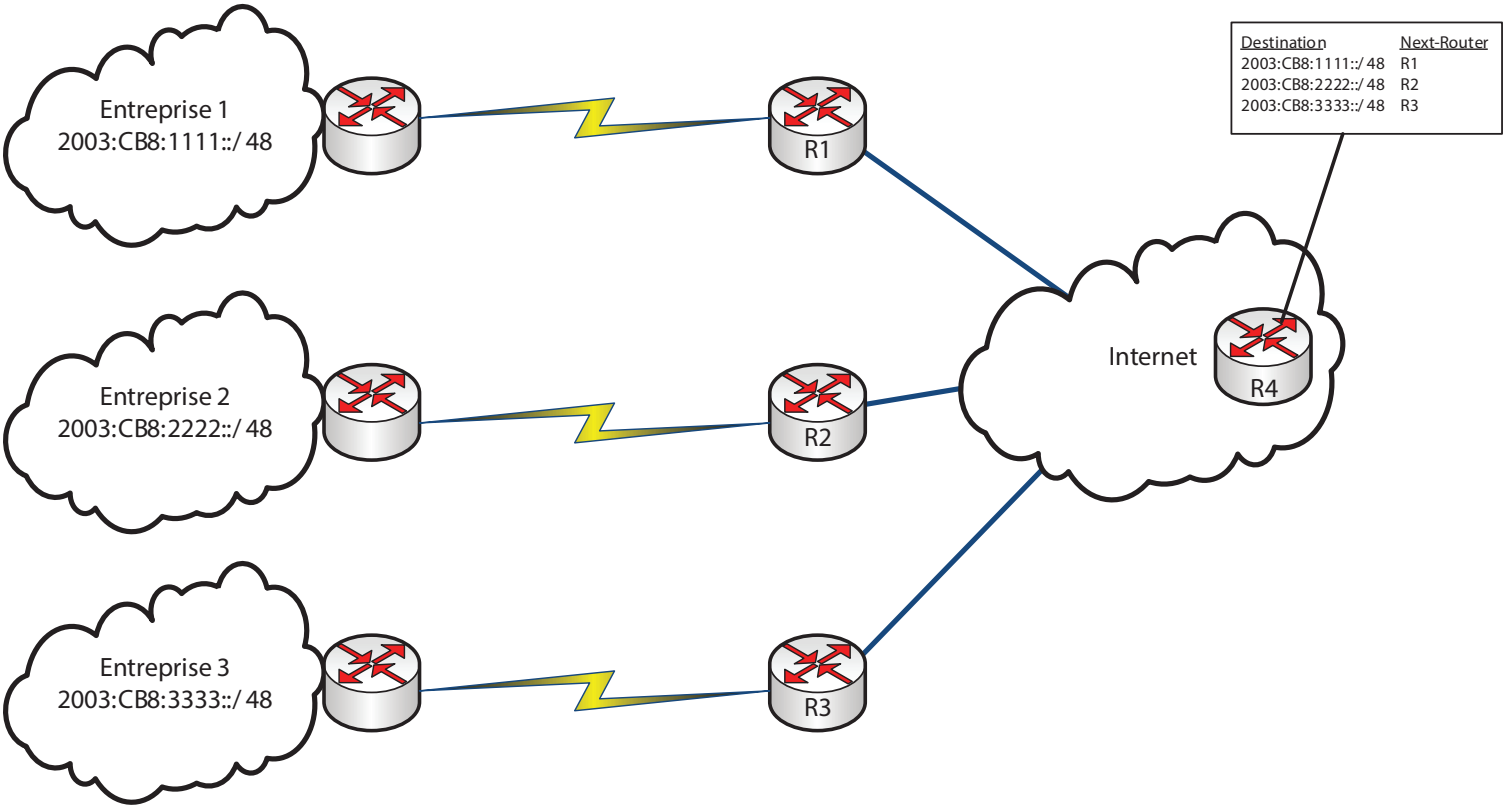
Le champ Subnet peut aller de 0000 à FFFF ce qui fait 65,536 subnets!

Adresse IPv6 de type Unique Local Unicast

- Utiliser le FD pour les deux premiers hexadécimal
- Choisir un Global-ID unique sur 40 bits
- Fusionner le FD avec le Global-ID pour en faire un Préfix de 48 bits
- Utiliser les 16 bits suivants pour le champ Subnet ID
- Les 64 bits restants sont utilisés pour le champ Host (ou Interface ID)




Structure d'adresse IPv6 de type Unique Local




Trois Global Routing Préfix (Subnets) avec une route par Préfix

# IMPLÉMENTATION DU ROUTAGE IPV6

# Configuration de l'adressage IPv6 sur un routeur

Les 2 étapes clés pour configurer IPv6 sur une interface d un routeur :

1 – Activer le routage IPv6 avec la commande ipv6 unicast-routing
2 – Assigner l adresse IPv6 et son masque au format CIDR avec la commande ipv6 address <address>/64

**Exemple :**
R1(config)# ipv6 unicast-routing
R1(config)# interface Gi0/0
R1(config-if)# ipv6 address 2001:ab00:1111:1::2/64

Vérifier que la configuration est bonne avec la commande show ipv6 interface

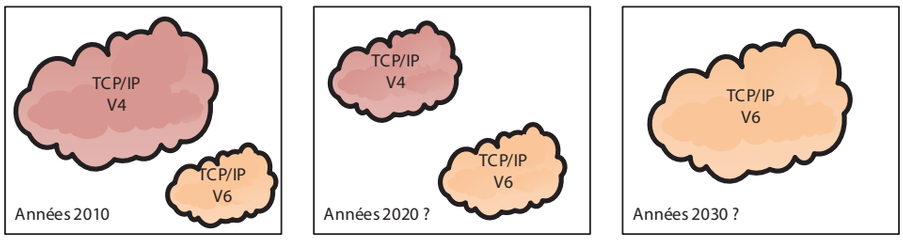
R1# show ipv6 interface Gi0/0
GigabitEthernet0/0 is up, line protocol is up
<lignes omises>
  Global unicast addresses:
    2001:ab00:1111:1::2/64, subnet is 2001:ab00:1111:1::/64

## Génération d un unique Device ID via EUI-64

L adresse d une interface peut être déclarée par la commande ipv6 address ou on peut utiliser une fonction pour générer un EUI-64 (Extended Unique Identifier de 64 bits).
L adresse IPv6 est séparée en deux partie de 64 bits chacune: 64 bits pour la partie Network et Subnet puis 64 bits pour la partie Host.
La génération du EUI-64 s effectue de la manière suivante:

1 – On coupe l adresse MAC en deux morceaux. Cela donne deux morceaux de 6 Hexa chacun
2 – On insère le nombre Hexa FFFE entre les 2 morceaux pour pouvoir atteindre La taille de 16 octets/bytes
3 – On inverse le 7eme bit de l Interface ID (Host)

**Evolution de la double pile IPv4/IPv6 vers le tout-IPv6 sur Internet**







Format de l adresse IPv6 avec l Interface ID et la configuration via EUI-64

Exemple : en utilisant la règle du EUI-64, dériver la partie interface ID de l adresse IPv6 qui a une adresse MAC égale à 00:14:EB:C2:15:24

1 – On coupe l adresse MAC en deux morceaux. Cela donne deux morceaux de 6 Hexa chacun : 00:14:EB d une part et C2:15:24 d autre part

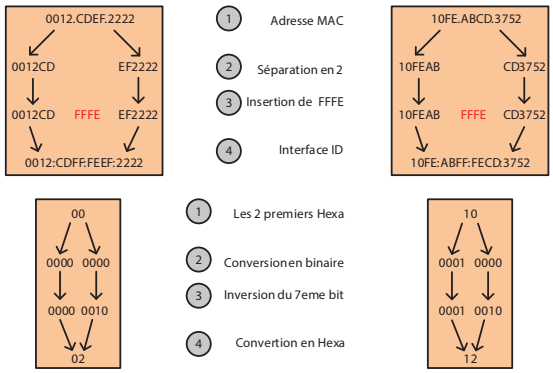
2 – On insère le nombre Hexa FFFE entre les 2 morceaux pour pouvoir atteindre la taille de 16 octets/bytes
00:14:EB:  FF:FE:  C2:15:24  ce qui donne 0014:EBFF:FEC2:1524

3 – Pour inverser le 7eme bits de l interface ID on prend les deux premiers Hexa (00), on les convertit en binaire (0000 0000) puis on inverse le 7eme bit (0000 0010). Et on remet en hexadécimale, ce qui donne **02**

L adresse IPv6 via la méthode EUI-64 est donc : 0214:EBFF:FEC2:1524

# Configuration de l'adressage IPv6 sur un routeur

Deux exemple de configuration d adresse IPv6 avec la règle EUI-64




Adresse IPv6 Multicast de type Local-Scope

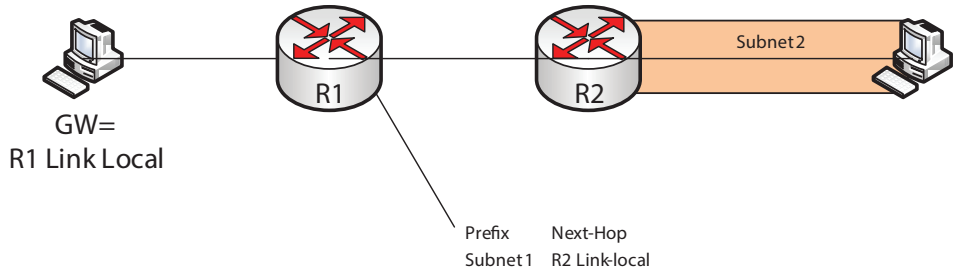
| Nom | Adresse Multicast | Description | Equivalent en IPv4 |
|---|---|---|---|
| All-nodes | FF02:: 1 | Tous les nodes IPv6 sur le lien (link) | Broadcast |
| All-routers | FF02:: 2 | Tous les routeurs IPv6 sur le link | aucun |
| All-OSPF, All-OSPF-DR | FF02:: 5, FF02:: 6 | Tous les routeurs OSPF et OSPF-DR | 224.0.0.5, 224.0.0.6 |
| EIGRPv6 Routers | FF02:: A | Tous les routeurs EIGRP | 224.0.0.10 |

| FF02: 0000: 0000: 0000: 0000: 0001: FF | __ : ____ |
|---|---|

Format d'adresse Solicited Node Multicast abrégé en FF02:: 1:FF __ : ____

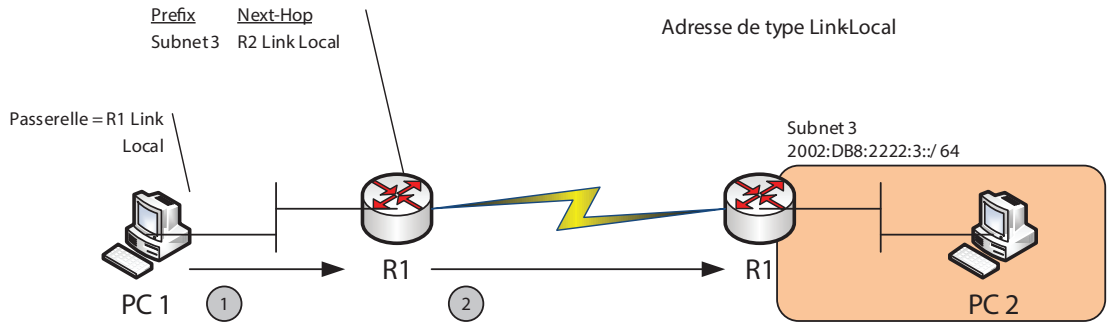
Lorsqu'on attribue une adresse IPv6 à un routeur, Il faut retenir que :

- le routage des paquets IPv6 s active sur cette interface en IN et OUT
- le Prefix (Subnet) de cette interface est ajoutée dans la table de routage IPv6
- Si c est une adresse Link-Local alors tous les paquets envoyés par cette interface ne sortiront pas du Prefix (Subnet) car les routeurs ne routent pas les paquets avec une adresse Link-Local. Elle est utilisée uniquement pour une communication locale, à l intérieur du Prefix (Subnet)




**Solicited-Node Multicast Addresses:**

Cette adresse Multicast fournit une adresse de destination pour tous les Hosts qui partagent les 6 derniers nombre hexadécimaux. Chacun de ces Hosts traitera le même paquet Multicast.




Points clés sur l'adresse de type Link-Local (qui commence toujours par FE80)

**Unicast (not multicast)** : Elle représente un unique Host et les paquets envoyés à la Link-Local ne sont traités que par ce Host.

**Routage de la Link-Local** : les paquets envoyés à la Link-Local ne quittent jamais le Prefix (Subnet) local car les routeurs ne routent pas les paquets dont l'adresse de destination est une Link-Local

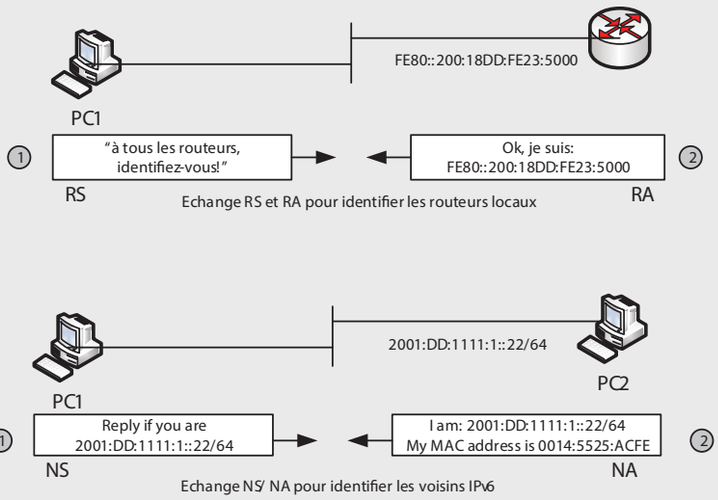
**Génération automatique** : chaque interface d'un Host IPv6 ou routeur IPv6 peuvent s'auto-générer une adresse Link-Local. Cela permet d éviter les problèmes de communication initiale en attendant de recevoir automatiquement leur adresse Global Unicast.

**Utilisation générale** : cette adresse est utilisée principalement pour tous les protocoles qui restent en local du Prefix.




Format d'une adresse Link Local

Rappel sur des adresses IPv6 particulières:
Adresse IPv6 Inconnue - :: (ou que des zéros)
Adresse IPv6 de loopback - ::1 ou 127 zéros et 1 un




Le protocole **NDP** (Neighbor Discovery Protocol) a les fonctionnalités suivantes :

**Stateless Address Autoconfiguration (SLAAC) :** le Host utilise les messages NDP pour identifier la première partie des adresses IPv6 et le Prefix (Subnet).

**Router Discovery :** le Host apprend la liste des routeurs IPv6 qui sont dans le même Prefix via les messages NDP.

**Duplicate Address Detection :** cette fonction de NDP permet d identifier si une adresse est dupliquée sur le réseau local. Si ce n est pas le cas alors le Host utilise la méthode **Neighbor MAC Discovery :** une fois terminée, le Host apprend les adresses MAC de ses voisins. Contrairement à ARP en IPv4, les messages MDP sont utilisés pour matcher les adresses IPv6 et MAC.

**Router Discovery :** Le Host découvre les routeurs par deux messages MDP, le RS et le RA.

**Router Advertisement (RA) :** Message envoyé à toutes les adresses IPv6 connues. Ce message sollicite tous les routeurs locaux afin qu ils fournissent leur RA (Router Advertisement) permettant d identifier les routeurs présents et leurs fonctions.

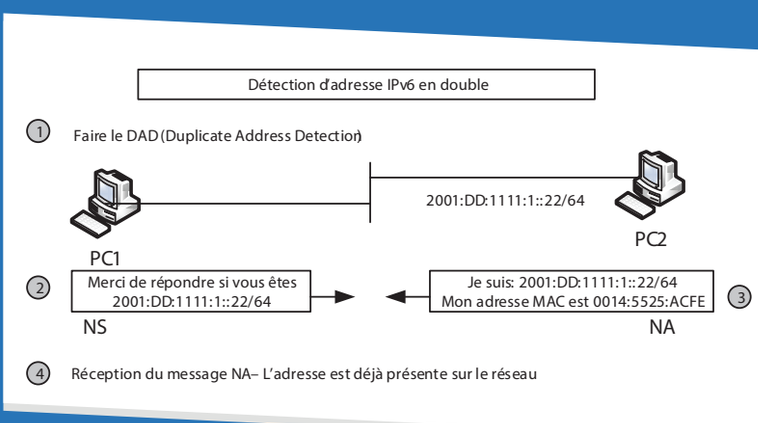
Router Solicitation (RS): Ce message est envoyé en unicast au Host qui a envoyé en amont un RS.

## Découverte des voisins IPv6 avec NDP

Similaire au protocole ARP pour IPv4, NDP utilise deux messages pour effectuer la résolution d adresse Network (**IPv6**) et Liaison de données (**MAC**).

**Neighbor Solicitation (NS):** Requête vers Host avec une adresse IPv6 particulière son adresse MAC correspondante. Ce NS utilise une adresse Multicast

**Neighbor Advertisement (NA):** Réponse du Host avec ce message unicast. Il peut aussi envoyer la réponse à tous le monde en utilisant l adresse FF02:1 (Adresse pour joindre tous les Hosts locaux)



## Protocole NDP et ses fonctionnalités

| Fonction | Message | Qui envoi le message | Qui répond au message | Information de la réponse |
|---|---|---|---|---|
| Router Discovery | RS et RA | Tout Host IPv6 | Tout routeur IPv6 | Adresse Link-local du routeur |
| Prefix discovery | RS et RA | Tout Host IPv6 | Tout routeur IPv6 | Prefix(s) et longueur du Prefix(s) |
| Neighbor Discovery | NS et NA | Tout Host IPv6 | Tout Host IPv6 | Adresse de la couche liaison de données (adresse MAC) |
| Duplicate Address Dedection | NS et NA | Tout Host IPv6 | Tout Host IPv6 | Confirmation si l'adresse est déjà présente localement |

Construction d une adresse IPv6 en utilisant SLAAC :

1) Apprentissage du Prefix IPv6 du Link, en utilisant les messages NDP RS/RA
2) Choix d une adresse IPv6 en utilisant le Prefix et l Interface ID
3) Avant l activation de cette adresse, vérification qu elle n existe pas déjà localement




Construction de l adresse IPv6 avec SLAAC

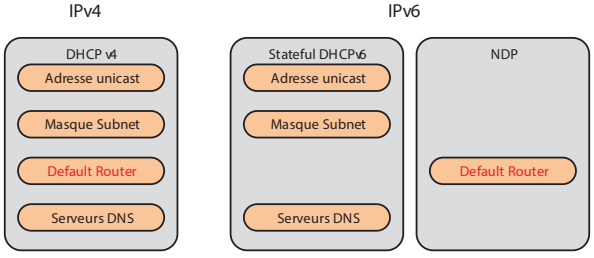
| Fonctionnalités | Stateful DHCP | Stateless DHCP |
|---|---|---|
| Conserve les informations sur les adresses IPv6 des clients (état, bail...) | oui | non |
| Bail envoyé au client | oui | non |
| Fournit la liste des serveurs DNS | oui | oui |
| Utilisé généralement avec SLAAC | non | oui |

Comparaison entre les services Stateless et Stateful DHCPv6

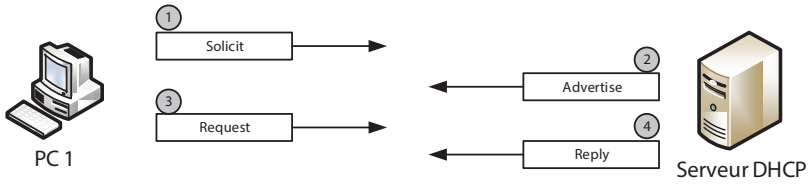
DHCP IPv6

DHCPv6 fonctionne comme le DHCPv4:

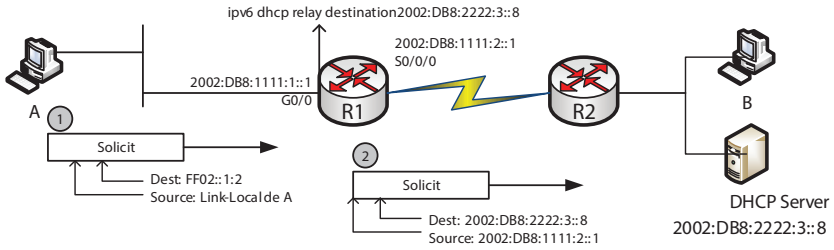
- Le client DHCP envoi sur le LAN un message pour identifier un serveur DHCP
- Si le client et le serveur DHCP sont sur le même LAN alors ils s échangent les messages directement entre eux
- Si le serveur DHCP est sur un LAN diffèrent, un routeur doit transmettre les messages entre le client et le serveur DHCP
- Le routeur doit alors être configuré pour relayer les messages DHCP, il a besoin pour cela de connaitre l adresse IPv6 du serveur DHCP
- Le serveur DHCP a une plage d adresse IPv6 qu il peut distribuer à ses clients avec un bail associé
- Le serveur conserve les informations de chaque client (adresse IP associée, adresse MAC, bail...)

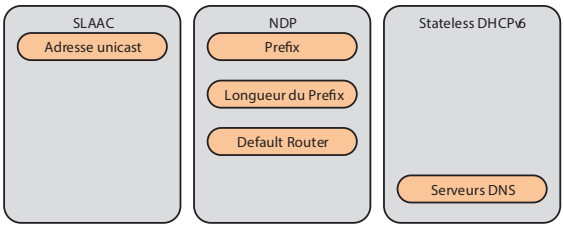


# Configuration d'IPv6 sur les Hosts




Messages DHCPv6 Stateful entre un client et un serveur DHCP




Configuration de l'agent relai DHCPv6 sur le routeur

```
R1(router)# interface GigabitEthernet0/0
R1(router-if)# ipv6 dhcp relay destination 2002:DB8:2222:3::8
```

Exemple de la commande PINGv6:

PC1$ **pingv6 2002:DB8:2222:3::8**
PING **2002:DB8:2222:3::8** (2002:DB8:2222:3::8) 56 data bytes
64 bytes from 2002:DB8:2222:3::8: icmp_seq=1 ttl=64 time=1.31ms
64 bytes from 2002:DB8:2222:3::8: icmp_seq=1 ttl=64 time=1.31ms

Exemple de la commande PINGv6 avancée:

R1# **ping**
**Protocol [ip]: ipv6**
**Target IPv6 address: 2002:DB8:2222:3::8**
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]: yes
Source address or interface: GigabitEthernet0/0
UDP Protocol? [no]: Verbose? [no]: Precedence [0]:
DSCP [0]:
Include hop by hop option [no]: Include destination option [no]: Sweep range of sizes? [no]:
Type escape sequence to abort
Sending 5 100-byte ICMP Echos to 2002:DB8:2222:3::8, timeout is 2
seconds
Packet sent with a source address of 2002:DB8:1111:1::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/4 ms
R1# **traceroute 2002:DB8:2222:3::8**
Type escape sequence to abort
Tracing the route to 2002:DB8:2222:3::8
1 2002:DB8:1111:2::2 2 msec 0 msec 0 msec
2 2002:DB8:2222:3::8 3 msec 1 msec 1 msec

Routes IPv6 Local et Connected

Un routeur ajoute les routes IPv6 en fonction de :
- La configuration des adresses IPv6 de ses interfaces.
- La configuration des routes statiques (par l administrateur).
- La configuration d un protocole de routage dynamique comme OSPFv3.

Règles concernant les routes Local et Connected :

1) le routeur crée la route IPv6 en fonction de chaque adresse IPv6 unicast sur une interface.
   a) le routeur crée la route Connected pour ce Subnet
   b) le routeur crée la route du Host (/128) de l adresse IPv6 de l'interface (équivalent à la route en /32 pour IPv4)

2) le routeur ne crée pas la route pour les adresses de type Link-Local de ses interfaces.

3) le routeur supprime les routes Connected ou Local pour les interfaces qui ne sont plus UP/UP.

Exemple de configuration de route statique IPv6 et vérification :
Configurer la route ipv6 2001:DB8:2222:3::/64 sortant vers l interface serial (série) 0/0/0

```
R1(config)# ipv6 route 2001:DB8:2222:3::/64 Serial0/0/0
R1(config)# exit
R1# show ipv6 route
! ...
...
S  2001:DB8:2222:3::/64 [1/0] via Serial0/0/0, directly connected
C  2001:DB8:1111:1::/64 [0/0] via GigabitEthernet0/0, directly connected
C  2001:DB8:1111:4::/64 [0/0] via Serial0/0/0, directly connected
```

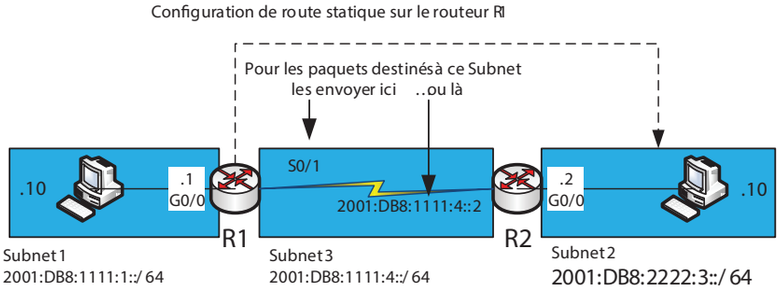
Protocoles de routage et versions

| | RIP | OSPF | EIGRP |
|---|---|---|---|
| Dernière version supportant les routes IPv4 | RIP version 2 (RIPv2) | OSPF Version 2 (OSPFv2) | EIGRP |
| Dernière version supportant les routes IPv6 | RIP Next Generation (RIPng) | OSPF Version 3 (OSPFv3) | EIGRP for IPv6 (EIGRPv6) |

Comparaison entre OSPFv2 et OSPFv3

- Ce sont des protocoles de type Link-State (état de liens)
- Ils utilisent les mêmes concepts de design et terminologie
- Ils imposent que le protocole soit actif sur l interface
- Une fois active sur l interface, une relation d adjacence est initiée
- Ils effectuent des vérifications avant d établir la relation de voisinage
- Une fois que deux routeurs deviennent Neighbor OSPF, ils s échangent leur base de données avec les paquets LSA (Link State Advertisement)
- Une fois les LSA échangés, ils utilisent l algorithme Shortest Path pour générer leur table de routage
- Ils utilisent la même metric
- Ils utilisent les LSA pour décrire la topologie

Configuration de route statique sur le routeur R1



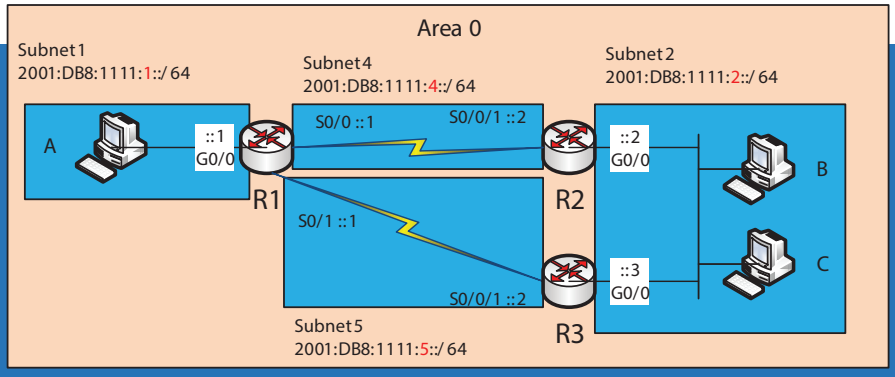
Configuration d OSPFv3 avec une Single Area

Premièrement il faut configurer le router ID :

1) si la commande router-id rid est configurée, OSPF utilise cette valeur
2) sinon, OSPF vérifie les interfaces de Loopback et sélectionne celle qui a l'adresse IP la plus élevée
3) sinon, OSPF vérifie les interfaces physiques UP/UP et sélectionne celle qui a l'adresse IP la plus élevée

Note: La valeur du routeur ID OSPFv3 est une adresse IPv4 !! Ensuite, la configuration de OSPFv3 en Single Area:

1) créer un numéro de process OSPFv3 avec la commande ipv6 router ospf
2) Activer OSPFv3 sur chaque interface qui participe au routage avec la commande ipv6 ospf process-id area area-number




Configuration sur le routeur R1 de OSPFv3 Single Area

```
R1# configure terminal
R1(config)# ipv6 router ospf 1
<output omitted – configure router id first>
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# interface Serial0/0
R1(config-if)# ipv6 ospf area 0
R1(config-if)# interface Serial 0/1
R1(config-if)# ipv6 ospf area 0
R1(config-if)# interface GigabitEthernet0/0
R1(config-if)# ipv6 ospf area 0
R1(config-if)# end
R1#"
```

Configuration OSPFv3 sur un routeur

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 router ospf 1
R1(config-rtr)# router-id 192.168.2.100
R1(config-rtr)# int s0/0/0
R1(config-if)# ipv6 ospf 1 area 0
R1(config-if)# exit
```

OSPFv3 Passive Interfaces

Comme pour OSPFv2, OSPFv3 supporte la fonctionnalités Passive Interface. Activer cette fonction sur une interface provoque :

- L arrêt de l envoi de paquet Hello OSPFv3 sur cette interface
- Ignore les paquets Hello OSPFv3 reçus sur cette interface
- Ne monte pas de relation de voisinage sur cette interface
- Mais continue d annoncer les autres Subnet qui sont connectés à cette interface

Commandeshow OSPFv2 et OSPFv3

| Pour afficher des détails sur | OSPFv2 | OSPFv3 |
|---|---|---|
| Process de routage OSPF | show ip ospf | show ipv6 ospf |
| Les sources | show ip protocols | show ipv6 protocols |
| Détail sur les interfaces OSPF | show ip ospf interface | show ipv6 ospf interface |
| Résumé sur les interfaces OSPF | show ip ospf interface brief | show ipv6 ospf interface brief |
| Liste des voisins | show ip ospf neighbor | show ipv6 ospf neighbor |
| Résumé de la base de données | show ip ospf database | show ipv6 ospf database |
| Routes apprises par OSPF | show ip route ospf | show ipv6 route ospf |

# FILTRAGE ET NAT

Points clés :

TCP est un protocole de la couche 4 et a les fonctionnalités suivantes :

• **Multiplexage en utilisant les ports :** permet à plusieurs applications de choisir quels ports utiliser pour la réception des données.

• **Correction d erreur :** numérotation des segments TCP et demande de retransmissions si un segment est perdu ou corrompu.

• **Contrôle de flux par fenêtrage :** utilise une fenêtre d envoi/ réception pour éviter que le récepteur soit inondé par l émetteur.

• **Etablissement de connexion :** utilise le port pour établir une connexion virtuelle entre émetteur et récepteur.

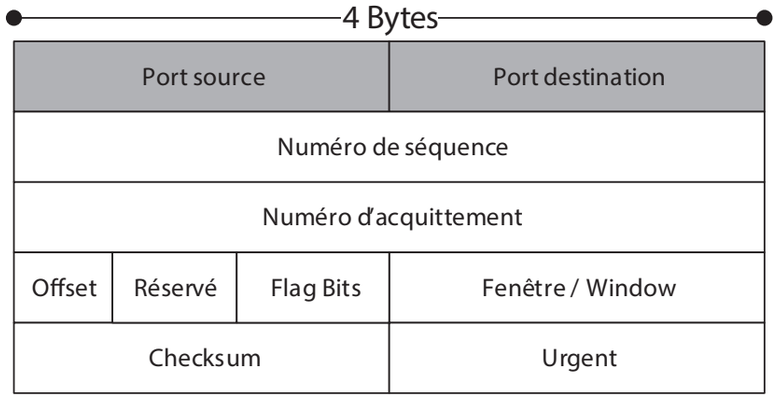
• **Transfert séquence de données et segmentation :** segmente la donnée des couches supérieures et livraison vers le destinataire avec un ordre de séquencement permettant de reconstituer la donnée.

• **Protocole connecté :** un échange préalable entre émetteur et récepteur est établi avant de s échanger des données pures.

Applications populaires et port associés :

| Numéro port | Protocole | Application |
|---|---|---|
| 20 | TCP | FTP Données |
| 21 | TCP | FTP Contrôle |
| 22 | TCP | SSH |
| 23 | TCP | Telnet |
| 25 | TCP | SMTP |
| 53 | TCP, UDP | DNS |
| 67, 68 | UDP | DHCP |
| 69 | UDP | TFTP |
| 80 | TCP | HTTP (WWW) |
| 110 | TCP | POP3 |
| 161 | UDP | SNMP |
| 443 | TCP | SSL (HTTPS) |

Entête TCP (20 Octets/Bytes)




## Champs de l entête TCP

**Port source :** Port utilisé par l émetteur

**Port destination :** Port utilisé par le récepteur Numéro de séquence : Numéro de séquence de la session d échange en cours

**Numéro d acquittement:** Numéro attendu du prochain segment

**Offset :** Taille de l entête TCP

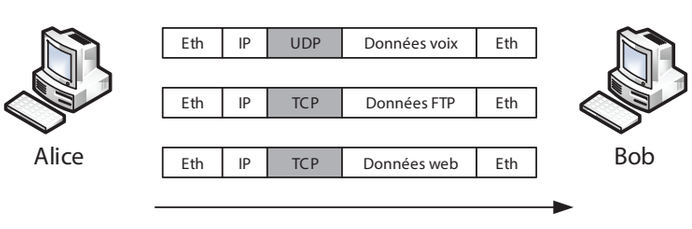
**Réservé :** Non utilisé

**Flag Bits :** bits utilisés pour le contrôle

**Fenêtre / Window :** Nombre de segments que le récepteur peur recevoir en une seule fois

**Checksum :** Vérification des erreurs dans l entête et la données transportée

**Urgent :** Indique l urgence du segment

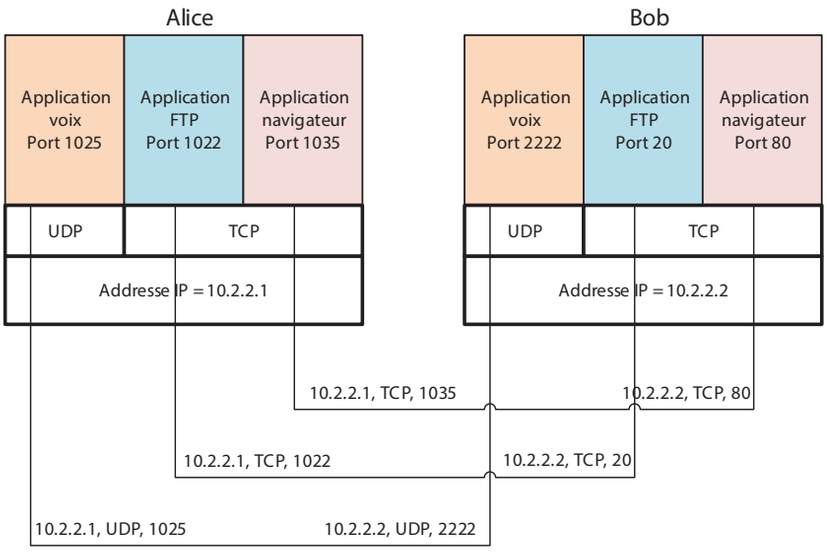



Multiplexage TCP

Bob reçoit 3 paquets d Alice. Bob regarde le port de destination dans l entête UDP ou TCP pour déterminer à quelle application est destiné le paquet

Dans cet exemple, Bob reçoit un paquet voix, un paquet FTP et un paquet Web. Bob identifie les applications adéquates:
Port 2222 : données voix
Port 21 : données FTP
Port 80 : données web

Connexions TCP et UDP avec les sockets




UDP (User Datagram Protocol) n utilise pas d acquittement ACK et a un entête plus petit que TCP. UDP est utilisé lorsqu il n y a pas besoin d acquittement.
Exemple de flux UDP: vidéo, voix, DNS, SNMP...

UDP est sans connexion (connection-less), ce qui signifie qu il envoi les données directement sans étape préalable de communication entre émetteur et récepteur, à contrario de TCP.

TCP - protocole orienté connexion (connection-oriented protocol)

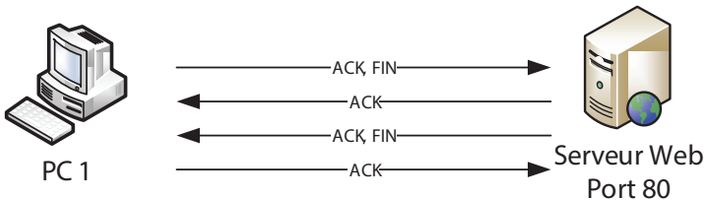
UDP - protocole sans connexion (connectionless protocol)

Paramètres de qualité de service (QoS)
**Bande passante / Bandwidth:** Volume de bits par seconde requis pour une application.
**Délai:** Temps requis par un paquet pour joindre la destination.
**Gigue / Jitter:** Variation du délai.
**Perte / Loss:** Pourcentage de paquets supprimés par le réseau avant d atteindre la destination.

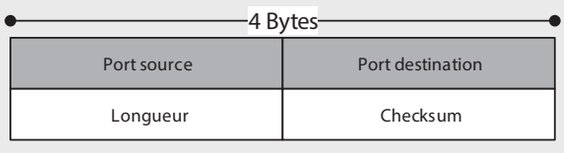
Etablissement de connexion TCP(3-way handshake)




Fermeture de connexionTCP (3-way handshake)



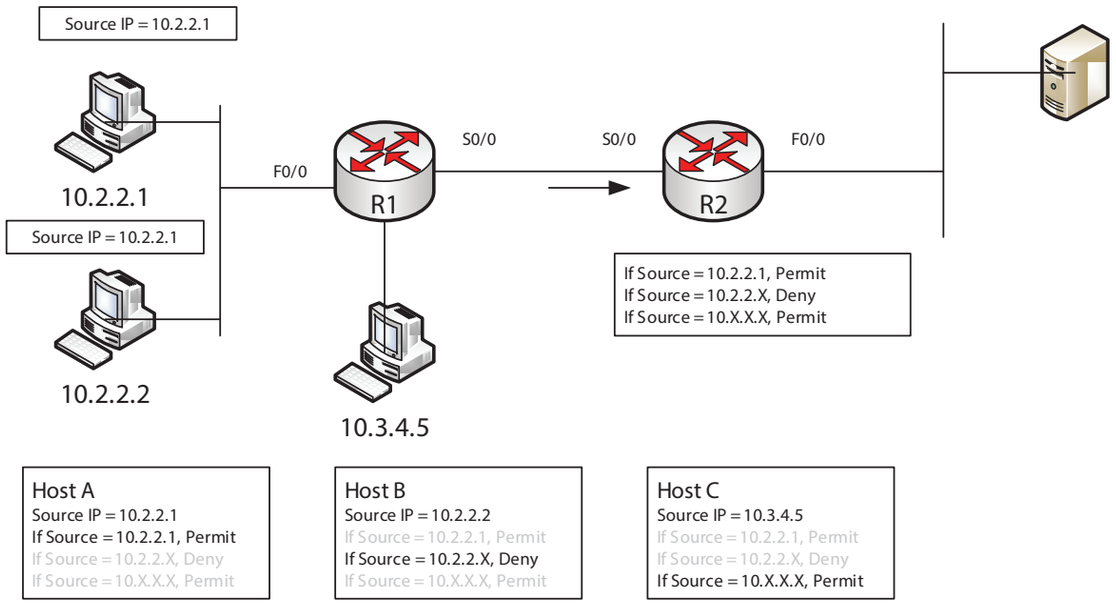

Entête UDP




**Port source:** port de l émetteur.
**Port destination:** port du récepteur.
**Longueur:** longueur de l entête UDP et de la donnée.
**Checksum:** vérification des erreurs dans l entête UDP et dans la donnée.

# Access Control Lists (ACLs) standard IPv4

Une Access-Control List (ACL) est utilisée lorsque le filtrage de paquet IP est nécessaire. Ce filtrage s'opère sur l'interface du routeur et doit être appliqué dans la même direction que le chemin emprunté par le paquet.




## Commande d une ACL

Pour matcher une adresse IP spécifique: permit
10.2.2.2 or permit host 10.2.2.2

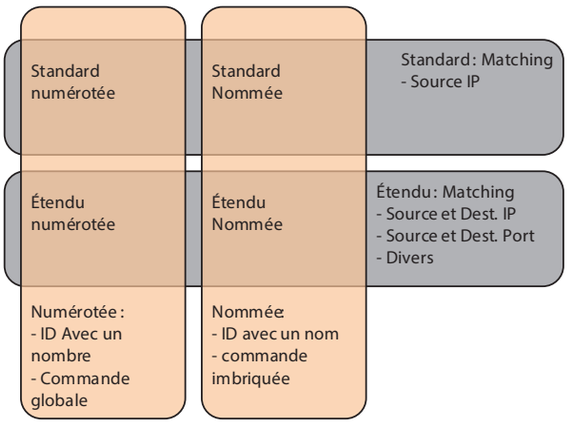
Pour matcher un Subnet /24: permit 10.2.2.0 0.0.0.255 (attention au Wildcard)

Dans un masque Wildcard:
- 0 signifie la valeur doit être identique
- 255 signifie peu importe la valeur

## Exemple d ACL sur le routeur R2

```
access-list 1 permit 10.2.2.1
access-list 1 deny 10.2.2.0 0.0.0.255
access-list 1 permit 10.0.0.0 0.255.255.255

interface S0/0
  ip access-group 1 in
```




Comparaison entre différents types dACL

## Types d ACL:

- ACL standard numérotée (1 – 99)
- ACL étendue chiffrée (100 – 199)
- Valeurs additionnelles sur les nouveaux IOS (standard 1300 – 1399, étendue 2000 – 2699)
- ACL nommée: amélioration de l'édition avec des séquences de commande insérable

## Points clés sur les ACL:

L'ACL est en top-down processing : si un paquet match une entrée de l ACL alors l ACL applique l action associée (permit, deny, log) puis s arrête de lire les autres entrées pour ce paquet.
Donc l ordre de séquencement des entrées dans l ACL sont primordial !

Attention, à la fin de chaque ACL se trouve une règle cachée implicite qui est " deny ip any any "

# Access Control Lists (ACLs) standard IPv4

Pour trouver le bon Wildcard mask pour un Subnet, il faut utiliser le Subnet ID et soustraire cette valeur à 255.255.255.255 - on a alors le Wildcard masque.

Exemple : trouver le Wildcard masque du Subnet 255.255.255.0

255.255.255.255
- 255.255.255.0
0. 0. 0.255

Le Wildcard masque est donc 0.0.0.255

Étapes pour implémenter une ACL standard

Étape 1 : localisation de l ACL
• L ACL standard doit être placé la plus proche de la destination afin que les paquets légitimes soient autorisés.

Étape 2 : configuration de l ACL
• L'ordre des entrées (ACE) d'une ACL est important! La premiere ACE est traité puis la seconde ACE etc....
• Il existe une règle cachée implicite à la fin de l'ACL qui supprime tous les paquets (deny ip any any)

Étape 3: activation de l ACL
• Choisir l interface du routeur et activer l ACL en choisissant le sens d application: in pour les paquets entrant sur l interface ou out pour les paquets sortant de l interface.
• ip access-group number {in | out}

Commande pour implémenter l ACL sur le routeur R2

```
R2(config)# access-list 1 permit 10.2.2.1
R2(config)# access-list 1 deny 10.2.2.0 0.0.0.255
R2(config)# access-list 1 permit 10.0.0.0 0.255.255.255

R2(config)# interface S0/0
R2(config-if)# ip access-group 1 in
```

"Notes sur la configuration de l ACL:

Pour matcher une adresse spécifique, utiliser le mot clé " host ".

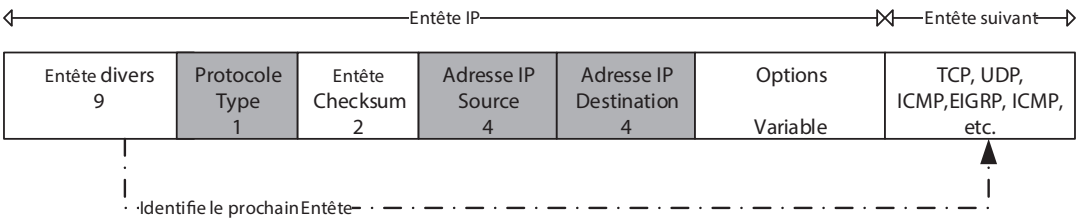
Pour matcher toutes les adresses, utiliser le mot clé " any ".

Pour matcher le 1er octet, les deux premiers octets ou les trois premiers octets, utiliser respectivement les Wildcard masque 0.255.255.255, 0.0.255.255 et 0.0.0.255.

Pour matcher un Subnet particulier, utiliser le Subnet ID puis le soustraire à la valeur 255.255.255.255, Pour obtenir le Wildcard masque associé.

Quand un routeur applique une ACL pour filtrer les paquets sortant (outbound) d'une interface, ce filtrage ne s applique pas pour les paquets initiés par le routeur lui-même.
Par exemple, les paquets OSPF, telnet, ping ne seront pas filtrés par
cette ACL.

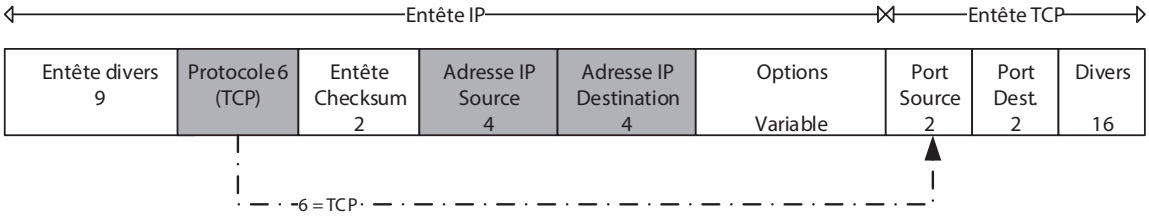
# ACL étendue IPv4 et Sécurité de l'équipement



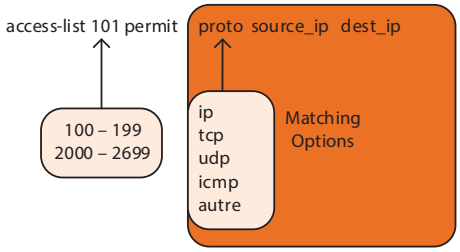

Entête IP avec un focus sur les champs pertinents pour l'ACL étendue

Commandes de l'ACL étendue

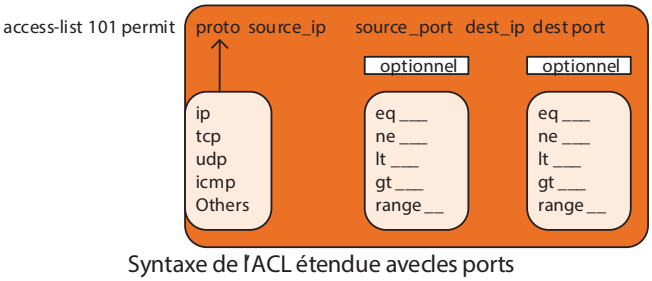
| Entrée d'ACL | Ce que ça match? |
|---|---|
| access-list 101 deny tcp any any | Tous les paquets IP avec un entête TCP |
| access-list 101 deny udp any any | Tous les paquets IP avec un entête UDP |
| access-list 101 deny icmp any any | Tous les paquets IP avec un entête ICMP |
| access-list 101 deny ip host 1.1.1.1 host 2.2.2.2 | Tous les paquets IP provenant de l'hôte 1.1.1.1 allant vers le hôte 2.2.2.2 et ce quelque soit l'entête suivant |
| access-list 101 deny udp 1.1.1.0 0.0.0.255 any | Tous les paquets IP avec un entête UDP provenant du Subnet 1.1.1.0/24 et ce quelque soit la destination (any) |




Entête IP avec un entête TCP et les champs Ports



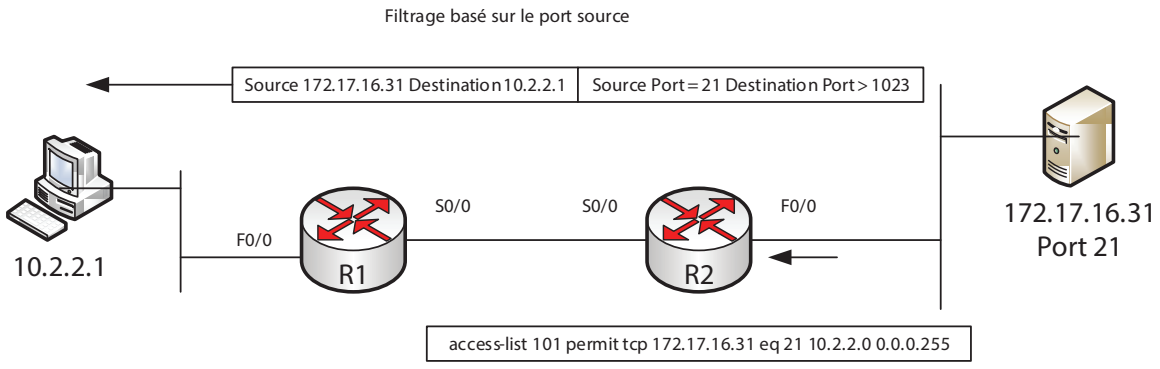

Syntaxe de l'ACL étendue avec les champs obligatoires




Syntaxe de l'ACL étendue avec les ports

Notes sur la localisation de l ACL étendue:

- Placer l ACL étendue le plus proche de l émetteur du paquet à filtrer. Filtrer en amont permet d économiser de la bande passante.
- Tous les paramètres d une entrée d ACL étendue doivent obligatoirement matcher le paquet pour que l action soit effectuée (deny,permit,log)
- Il n y a pas de différence entre la plage 100-199 et la plage 2000-2699.




Commandes de l'ACL étendue

| Entrée de l'ACL | Ce que ça match? |
|---|---|
| access-list 101 deny tcp any gt1023 host 10.1.1.1 eq 23 | Paquet avec un entête TCP, de n'importe quelle adresse IP source dont le port source est supérieur à 1023 et à destination du hôte 10.1.1.1 avec le port de destination égale à 23 (telnet) |
| access-list 101 deny tcp any host 10.1.1.1 eq 23 | Idem que l'ACL précédente mais on ne tient pas compte de la valeur du port source |
| access-list 101 deny tcp any host 10.1.1.1 eq telnet | Idem que l'ACL précédente mais on utilise le mot clé "telnet" au lieu de sa valeur (23) |
| access-list 101 deny udp 1.0.0.0 0.255.255.255 lt 1023 any | Paquet provenant du Subnet 1.0.0.0/8 dont le port source est inferieur À 1023 et à destination de n'importe quelle adresse |

ACL nommée

On peut utiliser un nom à la place d un numéro pour déclarer une ACL, cela rend plus simple la compréhension de la raison de l ACL.

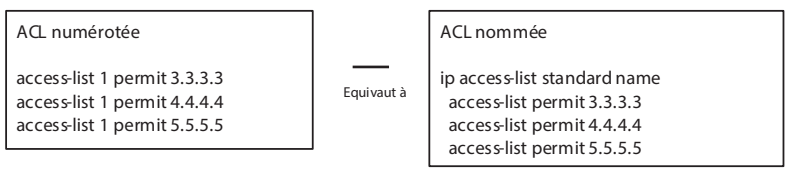
L utilisation de sous-commande de l ACL permet d ajouter/enlever/modifier chaque entrée de l ACL sans avoir à reconfigurer l ACL en entier.

Considérations sur les ACLs:

- Placer l ACL étendue le plus proche de la source pour supprimer le plus tôt les paquets inutiles.
- Placer l ACL standard le plus proche de la destination.
- Déclarer les entrées de l ACL les plus détaillées en premier.
- Avant toute modification d une ACL, désactivez-la d'abord sur l interface puis faites la modification"

Édition des ACLs avec les numéros de séquence:

- L ACL numérotée a désormais le même fonctionnement d'édition que l ACL nommée avec un numéro de séquence unique par entrée.
- Supprimer un numéro de séquence permet de supprimer uniquement l entrée correspondante.
- Insérer une nouvelle entrée est possible en précisant le numéro de séquence.
- Si on ne précise pas le numéro de séquence alors l'entrée sera ajoutée à la fin de l ACL et un numéro de séquence lui sera automatiquement attribué.




Édition d une ACL en utilisant les numéros de séquence

```
R1(config)# ip access-list standard 25
R1(config-std-nacl)# permit 10.1.1.0 0.0.0.255
R1(config-std-nacl)# permit 10.2.2.0 0.0.0.255
R1(config-std-nacl)# do show access-list 25

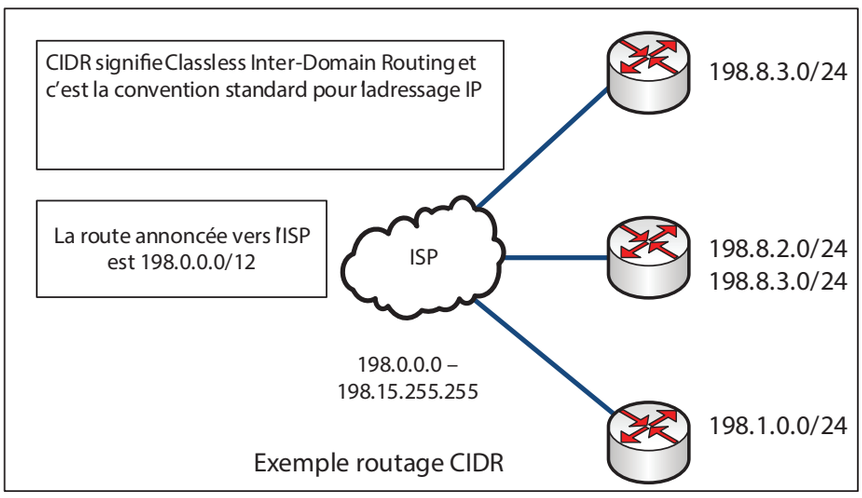
        10 permit 10.1.1.0 0.0.0.255
        20 permit 10.2.2.0 0.0.0.255

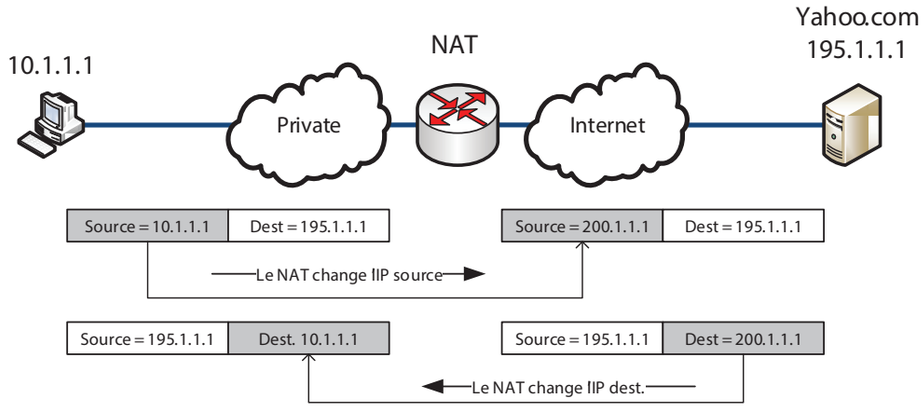
R1(config-std-nacl)# no 20 (ici on enlève la seconde entrée de l ACL)
R1(config-std-nacl)# do show access-list 25

        10 permit 10.1.1.0 0.0.0.255

R1(config-std-nacl)# 5 deny 10.1.1.1 (ici on ajoute une entrée en amont)
R1(config-std-nacl)# do show access-list 25

        5 deny 10.1.1.1
        10 permit 10.1.1.0 0.0.0.255
```




Le NAT permet l'utilisation de l'adressage privéà communiquer sur Internet

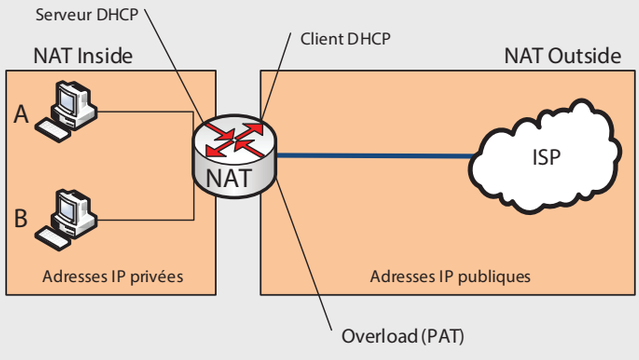
RFC 1918 – adressage IP prive

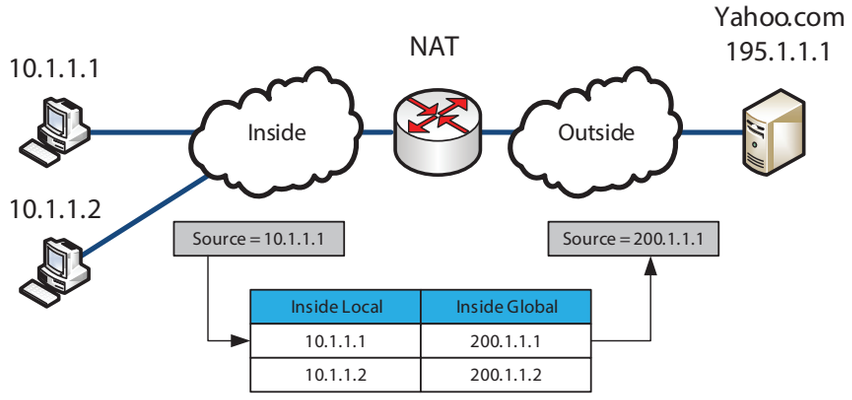
| Plage d'adresses IP | Classe | Networks |
|---|---|---|
| 10.0.0.0 – 10.255.255.255 | A | 1 |
| 172.16.0.0 – 172.31.255.255 | B | 16 |
| 192.168.0.0 – 192.168.255.255 | C | 256 |

Terminologie NAT

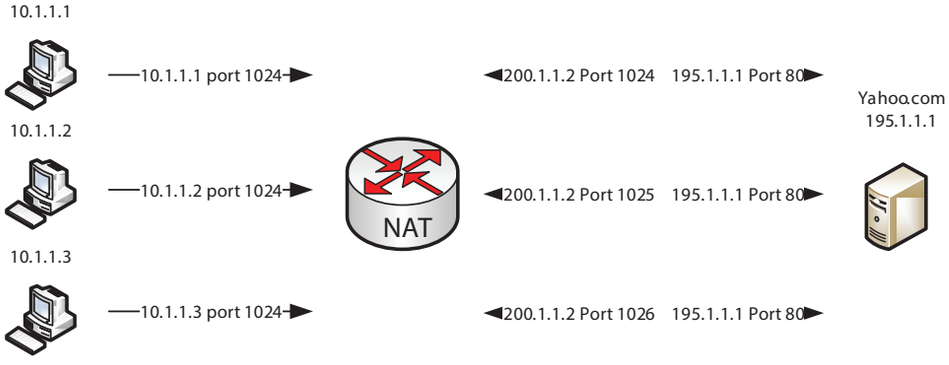
| Terme | Signification |
|---|---|
| Inside local | Inside signifie le réseau interneà l'entreprise. Ce sont doncles adresses IP attribuées aux Hosts, qui sont des adresses IP privées. |
| Inside Global | Cette adresse IP est la nouvelle adresse IP NATée du Host pour aller sur Internet. Le routeur change l'adresse Inside Local par cette adresse Inside Global. C'est généralement une adresse IP publique |
| Outside Global | Cette adresse réside dans la partie extérieur du réseau. Elle représente donc l'adresse IP de destination que le Host interne souhaite joindre |
| Outside Local | Cette adresse est l'adresse externe du Host de destination. Généralement, elle est identique a l'adresse Outside Global |

Localisation des roles DHCP et NAT





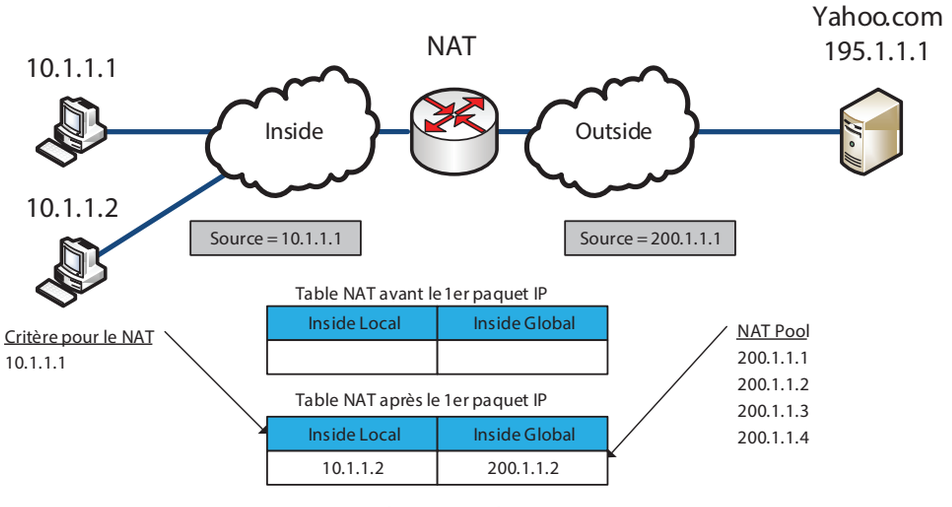

Terminologie NAT statique




| Inside Local | Inside Global |
|---|---|
| 10.1.1.1: 1024 | 200.1.1.2: 1024 |
| 10.1.1.2: 1024 | 200.1.1.2: 1025 |
| 10.1.1.3: 1024 | 200.1.1.2: 1026 |

Table de NAT dynamique avec Overloading

NAT Overload (PAT)




Terminologie NAT dynamique

Exemple de translation de NAT statique

```
NAT# show ip nat translations
Pro   Inside global        Inside Local       Outside Local      Outside Gl obal
---   200.1.1.1            10  .1.1.1         ---                ---
---   200.1.1.2            10  .1.1.2         ---                ---
```

Exemple de translation de NATOverload (ou PAT)

```
NAT# show ip nat translations
Pro   Inside global        Inside Local       Outside Local      Outside Gl obal
---   200.1.1.2:1024       10 .1.1.1:1024     195 .1.1.1:80      195 .1.1.1:80
---   200.1.1.2:1025       10 .1.1.2:1024     195 .1.1.1:80      195 .1.1.1:80
---   200.1.1.2:1026       10 .1.1.3:1024     195 .1.1.1:80      195 .1.1.1:80
```

Configuration NAT dynamique

Étape 1 : configurer l interface pour qu elle fasse partie du réseau interne avec la commande ip nat inside.

Étape 2 : configurer l autre interface pour qu elle fasse partie du réseau externe avec la commande ip nat outside.

Étape 3 : configurer une ACL qui match les paquets entrant sur l interface interne.

Étape 4 : configurer une plage (pool) d adresses IP publiques avec la commande ip nat pool name first-address last-address netmask subnet-mask.

Étape 5 : Activer le NAT en précisant l ACL et le pool avec la commande ip nat inside source acl-number pool pool-name.

Exemple:
Configurer le routeur avec un NAT dynamique ou le Host A (10.1.1.1) et le Host B (10.1.1.2) soient NATtés avec la plage d adresses IP 200.1.1.1 à 200.1.1.2.
Utiliser l interface G0/0 comme interface interne et l interface
S0/0/0 comme interface externe.

NAT(config)# interface G0/0 NAT(config-if)# ip nat inside NAT(config-if)# interface S0/0/0
NAT(config-if)# ip nat outside NAT(config-if)# exit
NAT(config)# access-list 1 permit 10.1.1.1
NAT(config)# access-list 1 permit 10.1.1.2
NAT(config)# ip nat pool TOTO 200.1.1.1 200.1.1.2 netmask
255.255.255.252
NAT(config)# ip nat inside source list 1 pool TOTO

Configuration du NAT overload (PAT)

Étape 1 : configurer l interface pour qu elle fasse partie du réseau interne avec la commande ip nat inside.
Étape 2 : configurer l autre interface pour qu elle fasse partie du réseau externe avec la commande ip nat outside.
Étape 3 : configurer une ACL qui match les paquets entrant sur l interface interne.
Étape 4 : configurer L Overload en précisant l adresse IP de l interface externe ou son identifiant avec la commande ip nat source list acl-number interface type/number overload

**Exemple :**

Configurer le routeur avec un NAT Overload ou le Host A (10.1.1.1) et le Host B (10.1.1.2) soient NATtés avec l adresse IP de l interface externe.
Utiliser l interface G0/0 comme interface interne et l interface
S0/0/0 comme l interface externe

NAT(config)# interface G0/0 NAT(config-if)# ip nat inside NAT(config-if)# interface S0/0/0
NAT(config-if)# ip nat outside NAT(config-if)# exit
NAT(config)# access-list 1 permit 10.1.1.1
NAT(config)# access-list 1 permit 10.1.1.2
NAT(config)# ip nat inside source list 1 interface Serial0/0/0
overload"

Configuration du NAT statique

Étape 1 : configurer l interface pour qu elle fasse partie du réseau interne avec la commande ip nat inside.
Étape 2 : configurer l autre interface pour qu elle fasse partie du réseau externe avec la commande ip nat outside.
Étape 3 : configurer la relation statique avec la commande ip nat inside source static inside-local inside-global command.

**Exemple :**

Configurer le routeur avec un NAT statique où :
- le Host A (10.1.1.1) est NATté en 200.1.1.1
- le Host B (10.1.1.2) est NATté en 200.1.1.2 Utiliser l interface G0/0 comme interface interne et l interface S0/0/0 comme l interface externe.

NAT(config)# interface G0/0 NAT(config-if)# ip nat inside NAT(config-if)# interface S0/0/0 NAT(config-if)# ip nat outside NAT(config-if)# exit
NAT(config)# ip nat inside source static 10.1.1.1
200.1.1.1
NAT(config)# ip nat inside source static 10.1.1.2
200.1.1.2

**Troubleshooting avec du NAT**

• S'assurer que les commandes ip nat inside et ip nat outside sont configurées sur les bonnes interfaces. Les variables inside et outside sont importantes.

• Pour du NAT statique, vérifier que l ACL est bien déclarée avec les Inside Local Address en 1er puis les Inside Global Address en second.

• Pour le NAT dynamique, vérifier que l ACL match le paquet envoyé par le Host interne avant le changement de son adresse IP par le NAT. Par exemple, il faut que l ACL match le paquet provenant du Host A en 10.1.1.1 et non en 200.1.1.1

• Pour le NAT dynamique sans Overload (PAT), s assurer que la plage IP réservée contient assez d adresses IP par rapport au réseau source. S il n y a plus d adresse disponible dans la plage alors tous les nouveaux Host ne pourront pas être NATté et ne sortiront pas sur Internet.

• Pour le PAT, on oublie souvent la variable overload à la fin de la commande.

• Si le NAT est bien configuré, vérifiez qu une ACL de filtrage n est pas en place sur l interface et qu elle supprime le paquet que vous souhaitez NATter.

# FIN DES FICHES RÉSUMÉ

## Comment optimiser sa mémoire?

Comment faire pour assimiler toute la théorie réseau afin de réussir avec succès l'examen et obtenir la certification CCNA?

Cette question, beaucoup de personnes me l'ont posée. Et j'avoue que moi-même, j'étais dans le désarroi lorsque j'ai récupéré mes supports de cours ICND1 et ICND2 qui compose toute la théorie pour l'examen. **Plus de 1000 pages à apprendre par cœur !**

En plus, libre à  de me croire ou non mais je fais partie des personnes qui ont des soucis avec leur cerveau. Je ne retiens quasiment rien. Le pire étant les **prénoms que j'oublie** en 30 secondes, **les films** dont j'oublie le titre le surlendemain, **les histoires et blagues de la veille**... alors dans ma vie professionnelle, je m'appuie sur l'agenda Outlook et Google. Merci à eux car ils m'ont sauvé plus d'une fois.

Alors comment faire pour réussir un examen où il y a une tonne d'informations à conserver dans sa mémoire?

A chacun sa formule mais en voici deux qui ont fonctionné à merveille pour moi:

Pour vous aider dans la mémorisation, il existe un site web qui propose de tester vos connaissances avec l'utilisation de cartes de révision. Ce site, c'est FlashCardExchange.

Sur le site, faites une recherche de carte en tapant "**CCENT**" ou "**CCNA**" et vous allez trouver une quantité hallucinante de cartes de révision, et le tout gratuitement !

Faites tout de même attention, certaines cartes ne sont pas forcément à jour par rapport au contenu de l'examen.

Pour ceux qui veulent **créer leur propre carte mentale** pour pouvoir réviser directement sur leur ordinateur sans Internet, je vous conseille vivement le logiciel **Mnemosyne** qui est totalement gratuit. Je vous le présente ci-dessous.



### Projet MNEMOSYNE

Ce projet n'est en fait qu'un **logiciel libre et gratuit**.

C'est celui que j'ai utilisé pour mes révisions, non pas pour le CCNA que j'avais déjà, mais **pour le CCIE**! Et oui, imaginez-moi avec mes problèmes de mémoire, à engloutir des centaines de pages de configuration, de design, de conseils pour à la fin les ressortir le jour de l'écrit et le jour du Lab de 8h. Sans cette aide "extérieure", je n'aurai jamais réussi mon examen, j'en suis certain.

## Syllabus ICND 1 – 100-101




ICND1 – Interconnecting Cisco Networking Devices Part 1 – est la première partie de la certification CCNA.

Regardons en détail le contenu de l'examen ICND1 100-101. Une fois réussi vous devenez certifié CCENT – Cisco Certified Entry Network Technician. C'est la certification juste avant le CCNA, plus connu.

**Remarque**

Il peut y avoir des questions lors de l'examen qui ne sont pas inclues dans cette liste... pas fou Cisco

## Syllabus

### Exploitation des réseaux de données IP

- Comprendre les différents composants réseau tel que les routeurs, commutateurs, ponts et concentrateurs
- Choisir correctement les composants pour un réseau donné
- Identifier les applications les plus courantes et leur impact sur le réseau
- Décrire le but et le fonctionnement des protocoles dans les modèles OSI et TCP/IP
- Prédire le cheminement de données dans le réseau entre deux hôtes
- Identifier les médias, les câbles, les ports et connecteurs pour connecter des périphériques de réseau à d'autres périphériques réseau sur un réseau local LAN

### Technologies de commutation LAN

- Déterminer la technologie et la méthode de contrôle d'accès pour les réseaux Ethernet
- Identifier les concepts de commutation et le fonctionnement des commutateurs Cisco.
- Domaine de collision
- Domaine de broadcast
- Type de commutation
- Table CAM
- Vérifier la configuration initiale du commutateur, y compris la gestion de l'accès à distance.
- Vérifier l'état du réseau et le fonctionnement du commutateur en utilisant les outils de base tels que ping, telnet et ssh.
- Expliquer comment les VLANs séparent logiquement le réseau et la nécessité du routage entre eux.
- Configurer et vérifier les VLANs
- Configurer et vérifier le Trunking sur les commutateurs Cisco
- DTP
- Auto negotiation

## Adressage IPv4 et IPv6

- Décrire le fonctionnement et la nécessité d'utiliser des adresses IP privées et publiques pour l'adressage IPv4
- Identifier un plan d'adressage IPv6 approprié pour satisfaire aux exigences d'un environnement LAN / WAN.
- Identifier un plan d'adressage IPv4 approprié en utilisant la méthode VLSM et le résumé afin de satisfaire aux exigences d'un environnement LAN / WAN.
- Décrire les exigences technologiques pour utiliser IPv4 et IPv6 en même temps, comme la double pile TCP/IP
- Décrire les adresses IPv6

    - Global unicast
    - Multicast
    - Link local
    - Unique local
    - eui 64
    - autoconfiguration

## Technologies de routage IP

- Décrire de façon basique les concepts de routage

    - CEF
    - transmission de paquet
    - Processus de routage

- Configurer et vérifier en utilisant la CLI la configuration de base des routeurs
- Configurer et vérifier l'état de fonctionnement d'une interface Ethernet
- Vérifier la configuration du routeur et la connectivité réseau
- Configurer et vérifier la configuration de routage statique et de la route par défaut
- Différencier les méthodes de routage et les protocoles de routage

    - Statique versus dynamique
    - Etat de lien versus vecteur de distance
    - Prochain saut
    - Table de routage IP
    - Interface passive

- Configurer et vérifier OSPF (aire simple)

    - Bénéfices d'une aire simple
    - Configurer OSPFv2
    - Configurer OSPFv3
    - Router ID
    - Interface passive

- Configurer et vérifier le routage inter-VLAN (appelé Router On The Stick)

    - sous interface
    - routage en amont
    - encapsulation

- Configurer les interfaces SVI – Switch Virtual Interface

## Services IP

- Configurer et vérifier le DHCP sur un routeur
    - Configurer les interfaces du routeur pour activer le DHCP
    - Les options DHCP
    - Les adresses exclues
    - Le bail
- Décrire les types, les fonctionnalités et comment utiliser les ACLs
    - ACL standard
        - Numéro de séquence
        - Edition
    - ACL étendue
    - ACL nommées
    - ACL chiffrées
- Journalisation
- Configurer et vérifier les ACL dans un réseau
- Opération basique du NAT
    - L'objectif du NAT
    - Plage
    - Statique
    - 1 pour 1
    - Surcharge
    - Adressage par la source
    - NAT unidirectionnel
- Configurer et vérifier le NAT dans un réseau
- Configurer et vérifier le NTP en mode client

## Sécurité des équipements réseau

- Configurer et vérifier les fonctionnalités de sécurité pour les équipements réseau
- Sécurité des mot de passe
- Enable secret versus enable password
- Transport
- Désactiver le protocole telnet
- SSH
- VTYs
- Sécurité physique
- Fonctionnalité service password
- Décrire les méthodes d'authentification externes
- Configurer et vérifier la fonctionnalité Port-security
- Sticky MAC
- Limitation du nombre d'adresses MAC
- Statique versus dynamique
- Mode de violation
- err disable
- shutdown
- protect / restrict
- Désactivation des ports non utilisés
- Recouvrement suite à un err disable
- Assigner les ports non utilisés à un VLAN non utile
- Paramétrer le VLAN natif sur un autre numéro que le VLAN 1
- Configurer et vérifier les ACLs pour limiter l'accès telnet et SSH vers un routeur

## Résolution de problème – Troubleshooting

- Identifier et résoudre les problèmes associés à l'adressage IP et configuration des hôtes
- Identifier et résoudre les problèmes relatifs aux VLANs
    - Identification des VLANs configurés
    - Corriger l'appartenance des ports aux VLANS associés
    - Corriger l'adressage IP
- Identifier et résoudre les problèmes de Trunk sur les commutateurs
    - Corriger l'état des Trunk
    - Corriger la configuration de l'encapsulation
    - Corriger les VLAN autorisés dans le Trunk
- Identifier et résoudre les problèmes relatifs aux ACLs
    - Statistiques
    - Réseaux autorisés
    - Direction par interface
- Identifier et résoudre les problèmes de la couche physique
    - Frame
    - CRC
    - Runts
    - Giants
    - Paquets supprimés
    - Late collision
    - Erreur en Input et Output




**Je vous donne rendez-vous sur http://reussirsonccna.fr pour découvrir tout ce qu'il faut savoir sur les certifications et les nouveautés Cisco CCENT et CCNA !**