

REUSSIRSONCCNA.FR

TOUT SAVOIR POUR ÊTRE CERTIFIÉ

EXAMEN

100-105 ICND1

CERTIFICATION

CISCO CCENT

PAR
CYRIL

CERTIFIÉ CCIE ET AUTEUR DU SITE
[REUSSIRSONCCNA.FR](https://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 LEGALE

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	004
QUI SUIS-JE ?	004
TOUT SAVOIR SUR LE CCENT ET CCNA	005
QU'EST-CE QUE LE CCENT ET LE CCNA?	006
QUELS SONT LES PRÉREQUIS POUR LA CERTIFICATION ?	008
MES 9 CONSEILS AVANT ET PENDANT L'EXAMEN	009
AVANT LE JOUR J	009
LE JOUR J	010
FICHES RÉSUMÉ	012
THÉORIE DE LA COMMUTATION	013
IMPLEMENTATION DE LA COMMUTATION	028
GESTION DES ÉQUIPEMENTS CISCO	051
THÉORIE DU ROUTAGE IPV4	067
FILTRAGE ET NAT	129
ROUTAGE IPV6 THEORIE	146
IMPLEMENTATION DU ROUTAGE IPV6	154
ET APRÈS ?	173

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>

TÉLÉCHARGER LE GUIDE

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'?
- ✓ Quels sont les types de questions ?
- ✓ Comment optimiser sa mémoire?
- ✓ Comment pratiquer les labs ?
- ✓ Comment monter son propre lab Cisco ?
- ✓ Quel score atteindre pour être certifié(e) ?
- ✓ 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 Frédéric
- ✓ Retour d'expérience de Remi
- ✓ Syllabus ICND 1 – 100-105
- ✓ Syllabus ICND2 – 200-105
- ✓ Syllabus CCNA (ICND1 + ICND2) – 200-125
- ✓ 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 maîtrisaient 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 connaître 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 connaître 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? Être 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 ?

Ces fiches résumé sont destinées à vous donner toutes les billes en main pour réussir votre CCENT pour ensuite continuer avec le CCNA.



QUELS SONT LES PRÉREQUIS POUR LA CERTIFICATION ?

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

Ah si ! Il y en a un et de taille : être motivé(e) !





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 **réviser 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 sûrement 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...

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 !)

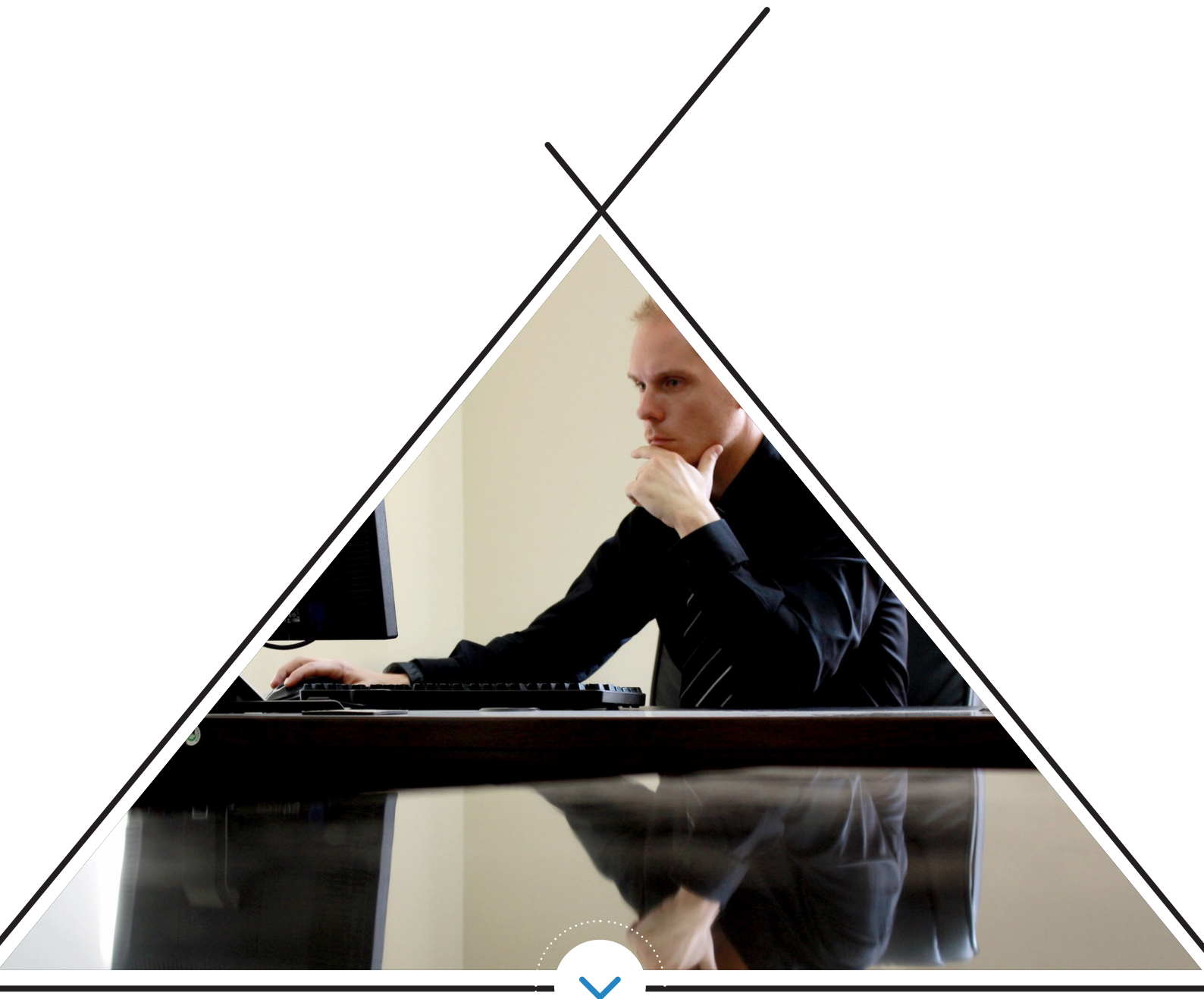
6 Prenez **2 pièces d'identités** avec vous (carte d'identité, passeport, permis de conduire...). Certains centres demandent 2 pièces d'identité et ils ne plaisantent pas.

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.





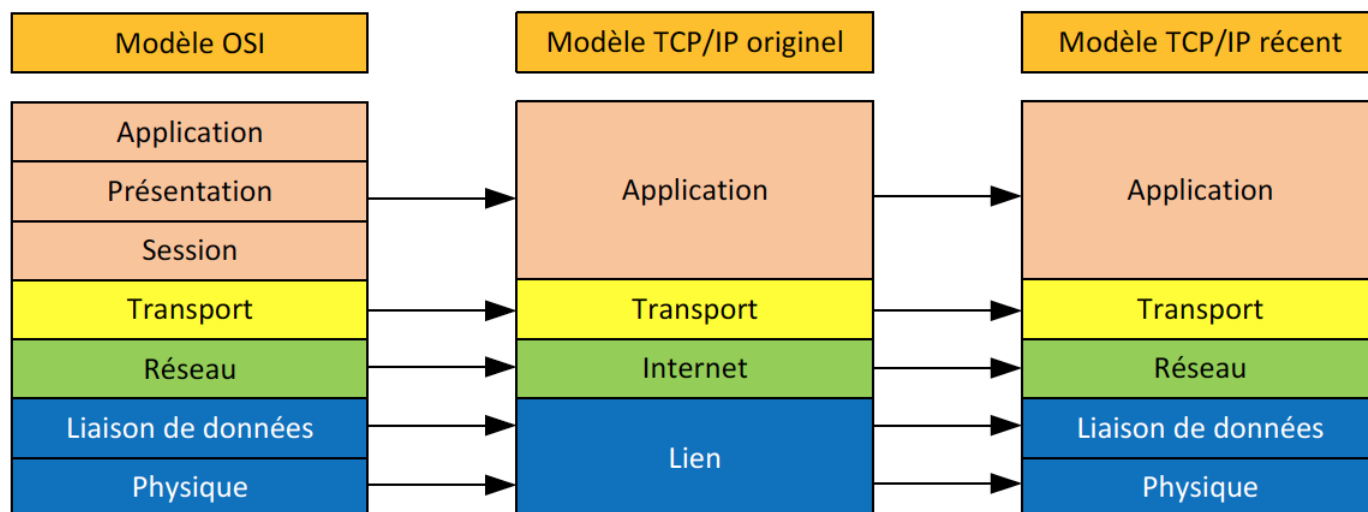
FICHES RÉSUMÉ

Les fiches résumés sont découpés 5 grands domaines: la commutation, la gestion des équipements Cisco, le routage IPv4 , le filtrage/NAT et le routage IPv6.

5 DOMAINES	SOUS-DOMAINES
La commutation	Théorie de la commutation
	Implémentation de la commutation
Gestion des équipements Cisco	Gestion des fichiers et licences Cisco
Le routage IPv4	Théorie du routage IPv4
	Implémentation du routage IPv4
Le filtrage	Filtrage et NAT
Le routage IPv6	Théorie du routage IPv6
	Implémentation du routage IPv6

THÉORIE DE LA COMMUTATION





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.

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.

La modélisation 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

Le modèle **Open Systems Interconnection (OSI)** a été défini dans les années 90 comme la première suite de protocoles de communication réseau. Il a été développé par l'**International Organization for Standardization (ISO)**. Attention à ne pas mélanger OSI et ISO...

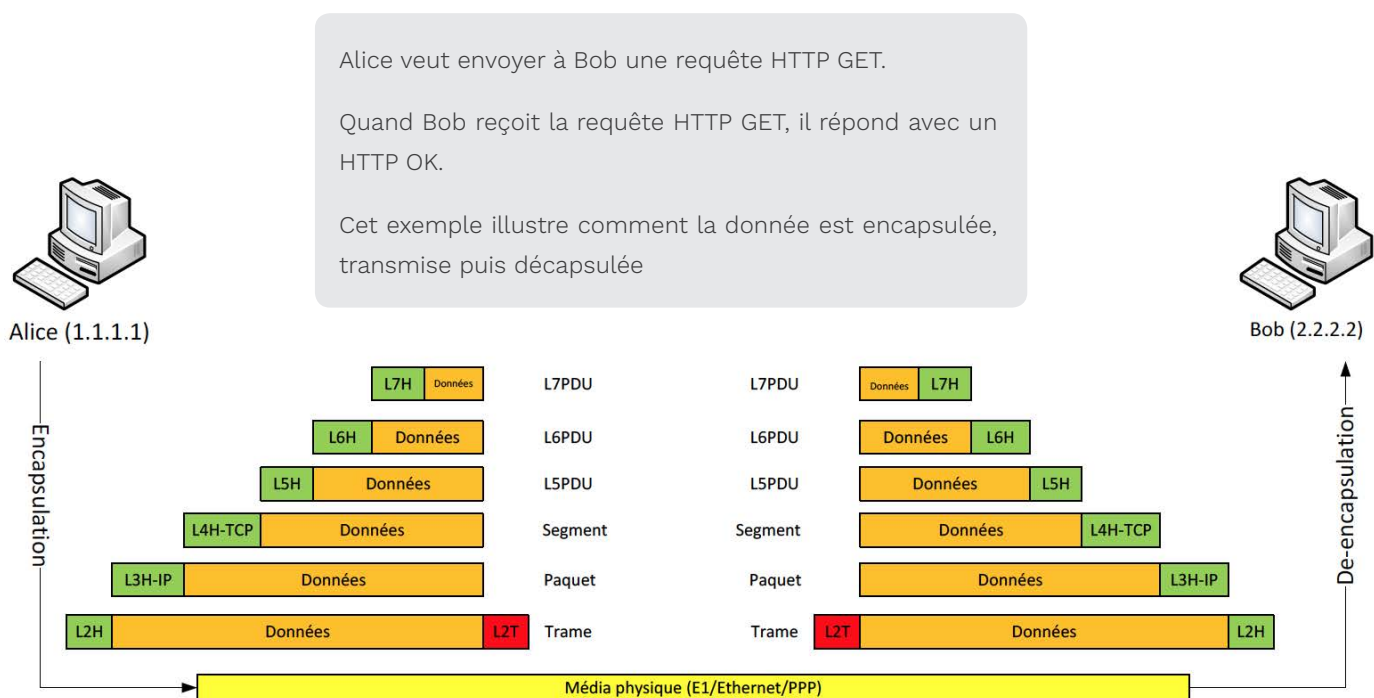
Le département USA de la défense a créé son propre modèle, aujourd'hui appelé **TCP/IP**. Très similaire au modèle OSI, il consolide les 3 couches hautes en une seule couche appelée **"Application"**. Les deux modèles restent identiques pour les 4 couches basses. Une version originelle de TCP/IP agrégeait les 2 couches basses en une seule.

Bien que les équipements d'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

L'ENCAPSULATION TCP/IP



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 transmise de la source à la destination. Chaque donnée et entête est appelée **Protocol Data Unit** ou **PDU**. Le PDU passe chaque couche en ajoutant l'entête de la couche traversée et ainsi de suite...

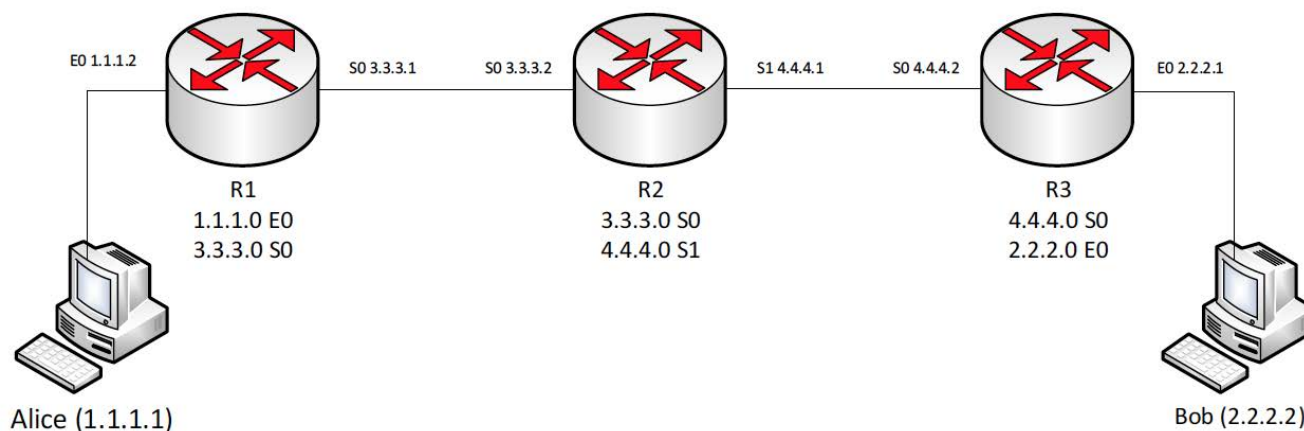
POINT IMPORTANT :

- 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

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

LES BASES DU ROUTAGE



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 (MAC) 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 connaître quelle est la destination souhaitée (IP de Bob). R1 retransmet le paquet IP **dans une nouvelle trame** à destination du routeur R2.

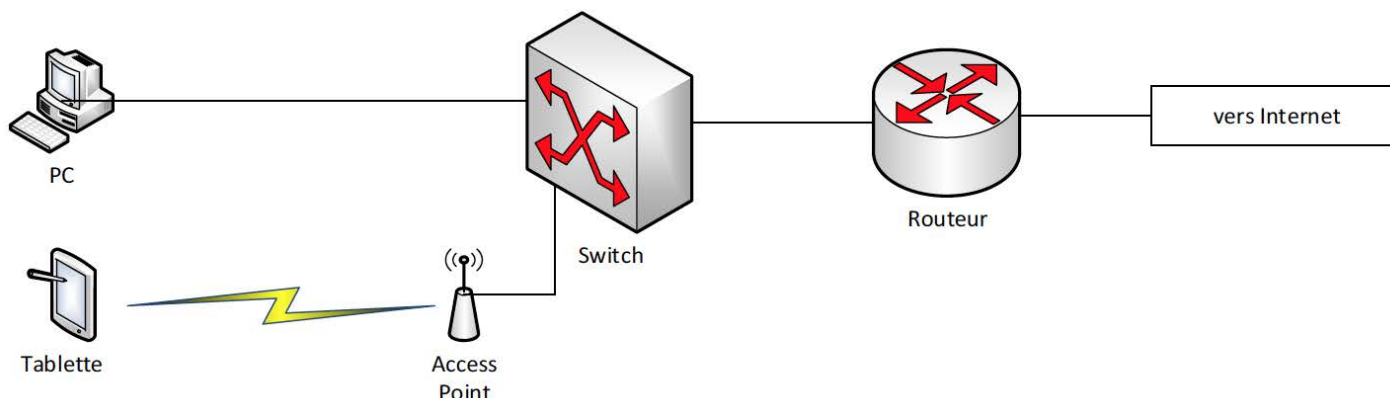
R2 effectue la même opération et transmet la trame à R3.

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 (MAC) de Bob comme adresse destination.

POINT IMPORTANT À CONNAITRE

- Le routage IP
- Le 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

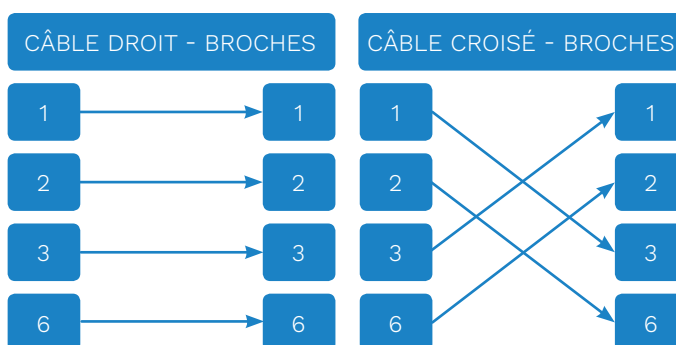
LES FONDAMENTAUX DES LANS ETHERNET



VITESSE (SPEED)	NOM COMMUN	NOM IEEE INFORMEL	NOM IEEE FORMEL	TYPE DE CÂBLE, 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

- Connaître les différents types de LANs Ethernet.
- Designer un réseau Ethernet filaire et sans-fil.
- Connaître 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**.
- Connaître 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 croisé
- Switch et Switch > câble croisé
- Routeur et routeur > câble croisé

LES FONDAMENTAUX DES LANS ETHERNET

La trame Ethernet est **identique** quel que soit le support physique. La plupart des équipements peuvent supporter une trame d'une taille de **1518 octets**

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

COMPOSITION D'UNE TRAME ETHERNET TYPE

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

ENTÊTE ETHERNET ET CHAMPS:

Preamble – octets (bytes)

Synchronisation

Start of Frame Delimiter (SFD) – 1 octet

Signifie que le prochain octet est l'adresse MAC de destination

Destination – octets

Le destinataire de la trame (adresse MAC)

Source – octets

L'émetteur de la trame (adresse MAC)

Type – 2 octets

Définit le type de protocole transporté au dessus (par ex IPv4 ou IPv6)

Données – Valeur entre 46 et 1500 octets

Données des couches supérieures dont IP, TCP...

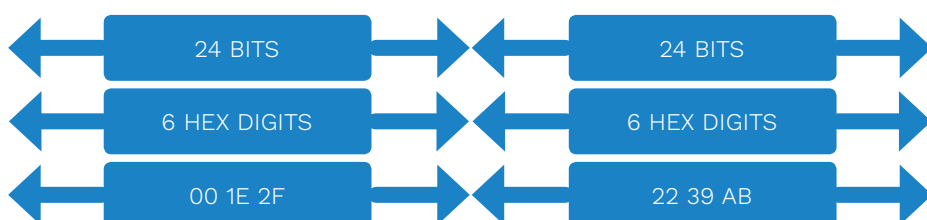
Frame Check Sequence – octets

Utilisé pour déterminer s'il y a eu une erreur de transmission

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

ORGANIZATIONALLY UNIQUE
IDENTIFIER (OUI)

VALEUR CONSTRUCTEUR
(CARTE NIC, INTERFACE)



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)

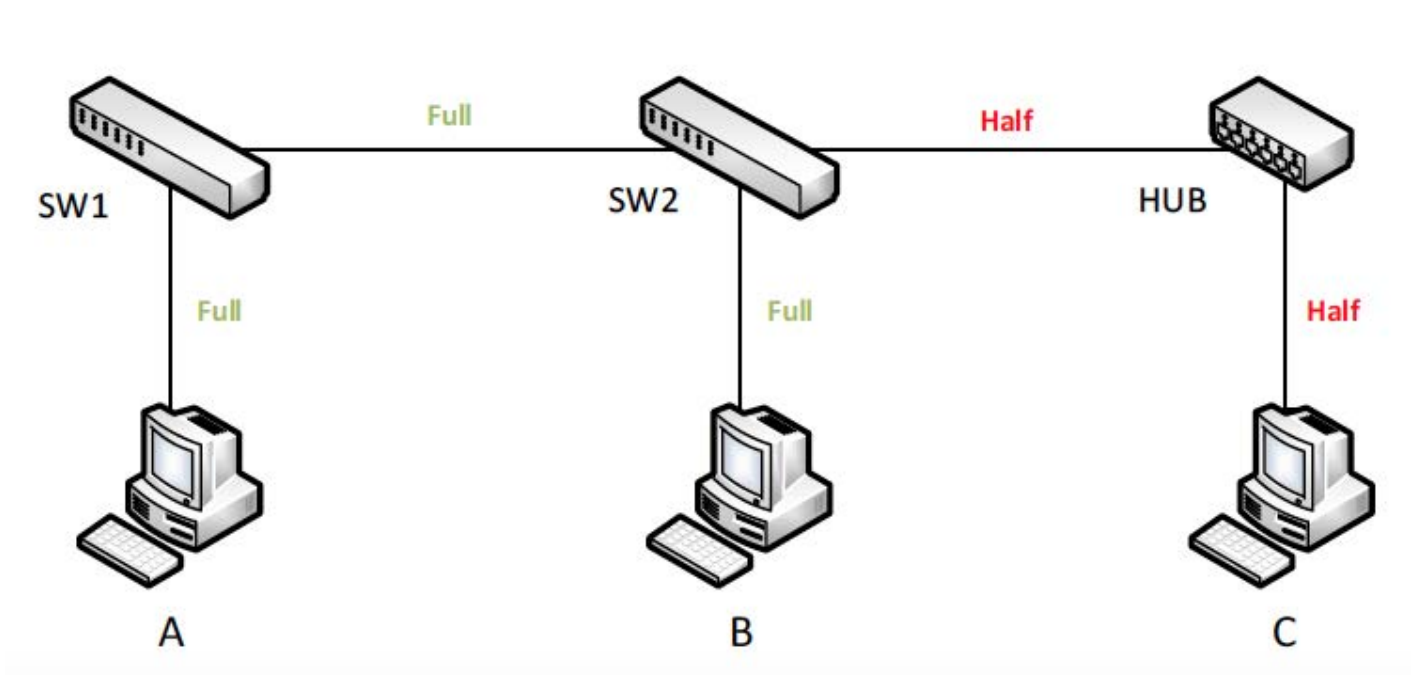
HALF-DUPLEX :

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 fonctionnent qu'en half-duplex alors que les switch peuvent être half ou full-duplex en fonction des possibilités du voisin connecté.



ANALYSE DE LA COMMUTATION LAN ETHERNET

Les fonctions de base d'un commutateur Ethernet sont les suivantes:

- 1 Transférer ou non la trame en fonction de l'adresse MAC de destination
- 2 Apprendre les adresses MAC reçues sur chaque port afin que le commutateur puisse prendre les bonnes décisions de transfert
- 3 Utiliser le protocole Spanning Tree (STP) pour garantir une topologie de couche 2 (layer-2) sans boucle et s'assurer que le port de destination ne reçoit qu'une seule copie de la trame.

EXEMPLE D'UNE TRAME ETHERNET 802.3

Préambule 7	SFD 1	Destination MAC 6	Source MAC 6	Type 2	Data / Pad 46 -1500	FCS 4
----------------	----------	----------------------	-----------------	-----------	------------------------	----------

Header

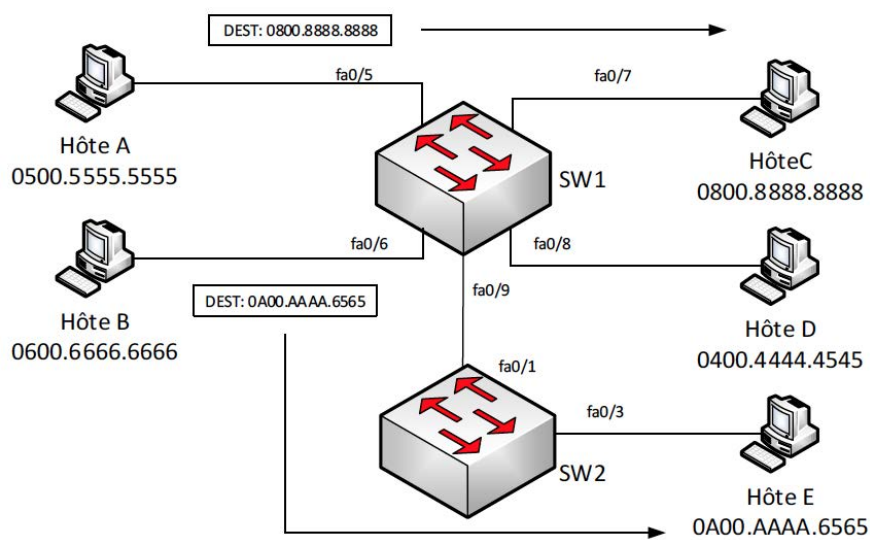
Trailer

REMARQUE

Si une adresse MAC est inconnue, la trame est envoyée à tous les ports du commutateur sauf pour le port d'origine de la trame. Ce processus est appelé **"inondation"** (flooding).

Une fois qu'un hôte répond, le commutateur placera cette adresse MAC de destination dans la table CAM avec le port signalé.

UNICAST FORWARDING - COMMUTATEUR SIMPLE ET DEUX COMMUTATEURS



Switch# **show mac-address table dynamic**

MAC Address Table - SW1

Address	Port
-----	-----
0500.5555.5555	fa0/5
0600.6666.6666	fa0/6
0800.8888.8888	fa0/7
0400.4444.4545	fa0/8
0A00.AAAA.6565	fa0/9 (via SW2)

FONCTIONNEMENT DU COMMUTATEUR - EXEMPLE 1

- la trame arrive sur fa0/5 avec comme MAC destination 0800.8888.8888.
- le switch envoie la trame sur le port de sortie fa0/7 et ne l'envoie pas sur les trames fa0/6 et fa0/8 (filtrage).

FONCTIONNEMENT DU COMMUTATEUR - EXEMPLE 2

- la trame arrive sur le port fa0/6 avec comme MAC destination 0A00.AAAA.6565
- Le switch envoie la trame uniquement sur fa0/9 vers le switch SW2 et ne l'envoie pas sur les ports fa0/5, fa0/7 et fa0/8 (filtrage)
- Le Switch SW2 reçoit la trame destinée à 0A00.AAAA.6565 sur son port fa0/1
- il envoie la trame sur le port fa0 / 3



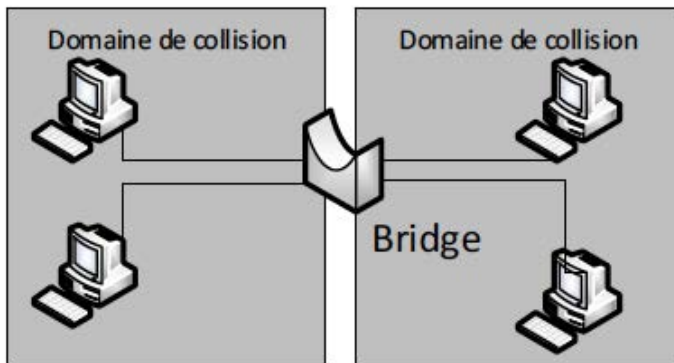
PROTOCOLE SPANNING TREE

Le Spanning Tree Protocol est utilisé pour empêcher les boucles dans un réseau de couche 2 (layer 2). Si des boucles sont présentes sur un réseau de couche 2, la trame sera transmise plusieurs fois à mesure que la trame passe d'un commutateur à l'autre.

RÉSUMÉ DE LA COMMUTATION LAN

En fonction de l'adresse MAC de destination, le switch procède de la manière suivante:

- 1 Pour chaque trame entrante, le commutateur enregistre l'adresse MAC source associée à chaque port de commutateur dans la table d'adresses MAC
- 2 Si la MAC de destination est une adresse unicast, multicast ou broadcast inconnue par le switch (aucune entrée dans la table MAC), la trame est envoyée à tous les ports de commutation, à l'exception du port entrant.
- 3 Si la MAC de destination est une adresse de monodiffusion connue (unicast), le switch recherche dans la table MAC (quel port associé) et envoie la trame vers le port de destination, à moins que l'adresse de destination se trouve sur le même port que la trame entrante. Si tel est le cas, la trame est rejetée.
- 4 Le protocole Spanning Tree est utilisé pour bloquer les ports et arrêter les boucles de commutation.



Le Pont (bridge) crée deux domaines de collision

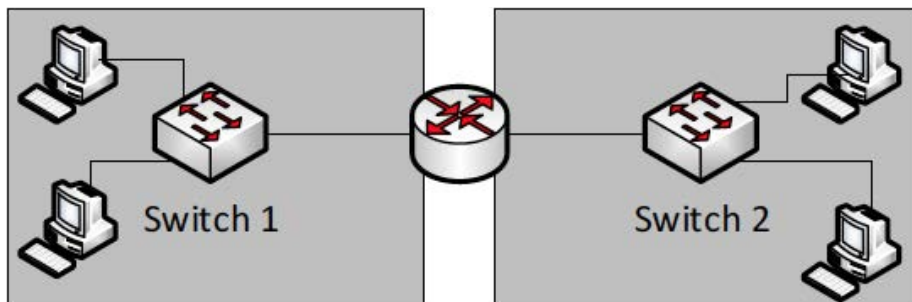
DOMAINES DE COLLISION VERSUS DOMAINES DE DIFFUSION

Un domaine de collision est un ensemble d'interfaces réseau pour lesquelles une trame envoyée par un équipement peut provoquer une collision avec une trame envoyée par tout autre équipement du réseau.

Un domaine de diffusion est un ensemble d'interfaces réseau pour lequel une trame de diffusion (broadcast) envoyée par un équipement est vue par tous les autres équipements sur le même domaine.

- Le concentrateur LAN (Hub) placent toutes les interfaces dans le même domaine de Collision.
- Le pont et le commutateurs LAN (switch) ont un domaine de collision par port.
- Le routeur place chaque interface LAN dans un domaine de collision (les liens WAN n'ont pas de domaines de collision).
- Un réseau local virtuel (VLAN) est un domaine de diffusion configuré par l'administrateur.

ROUTEUR



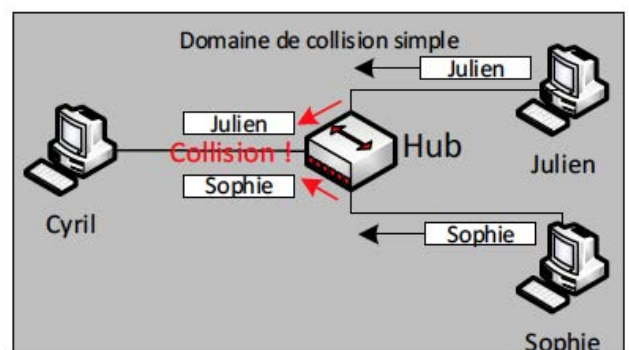
Ici le routeur a séparé le réseau en deux domaines de diffusion. Les routeurs séparent les réseaux locaux en plusieurs domaines de diffusion.

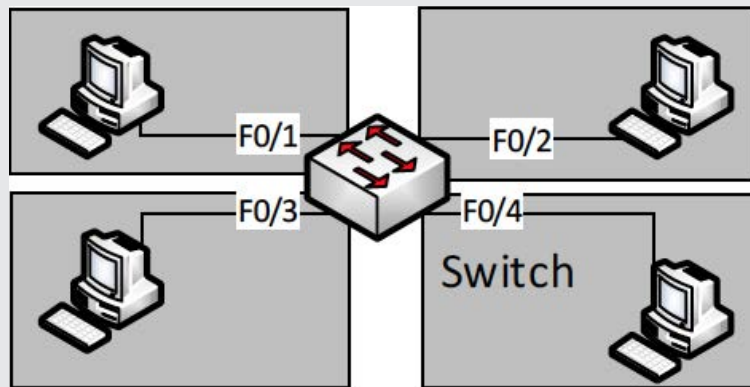
Le concentrateur (Hub) agit comme un répéteur avec plusieurs ports. Le concentrateur prend des trames de chaque port et les dupliquent sur le reste des ports.

Lorsque deux ou plusieurs PC transmettent en même temps, chaque trame est corrompue.

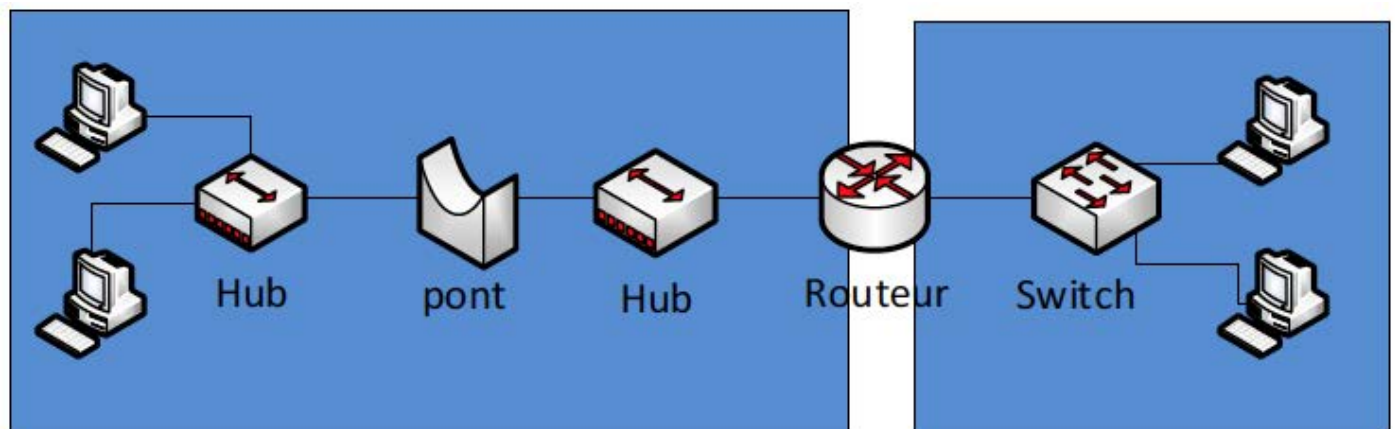
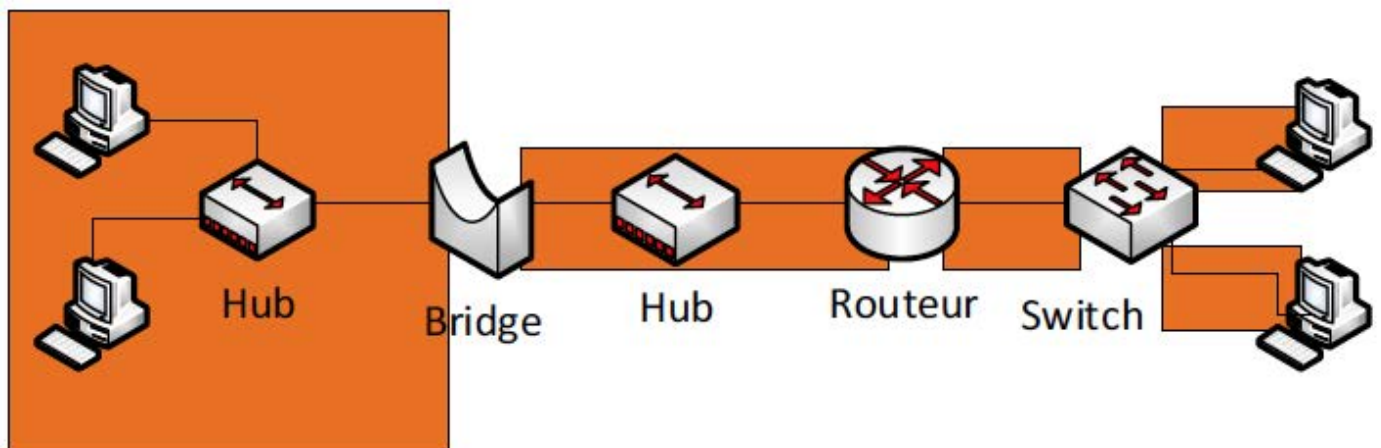
L'accès multiple de détection de porteuse avec détection de collision (CSMA / CD) est utilisé pour atténuer les collisions.

La topologie créée par le hub ressemble à une étoile.

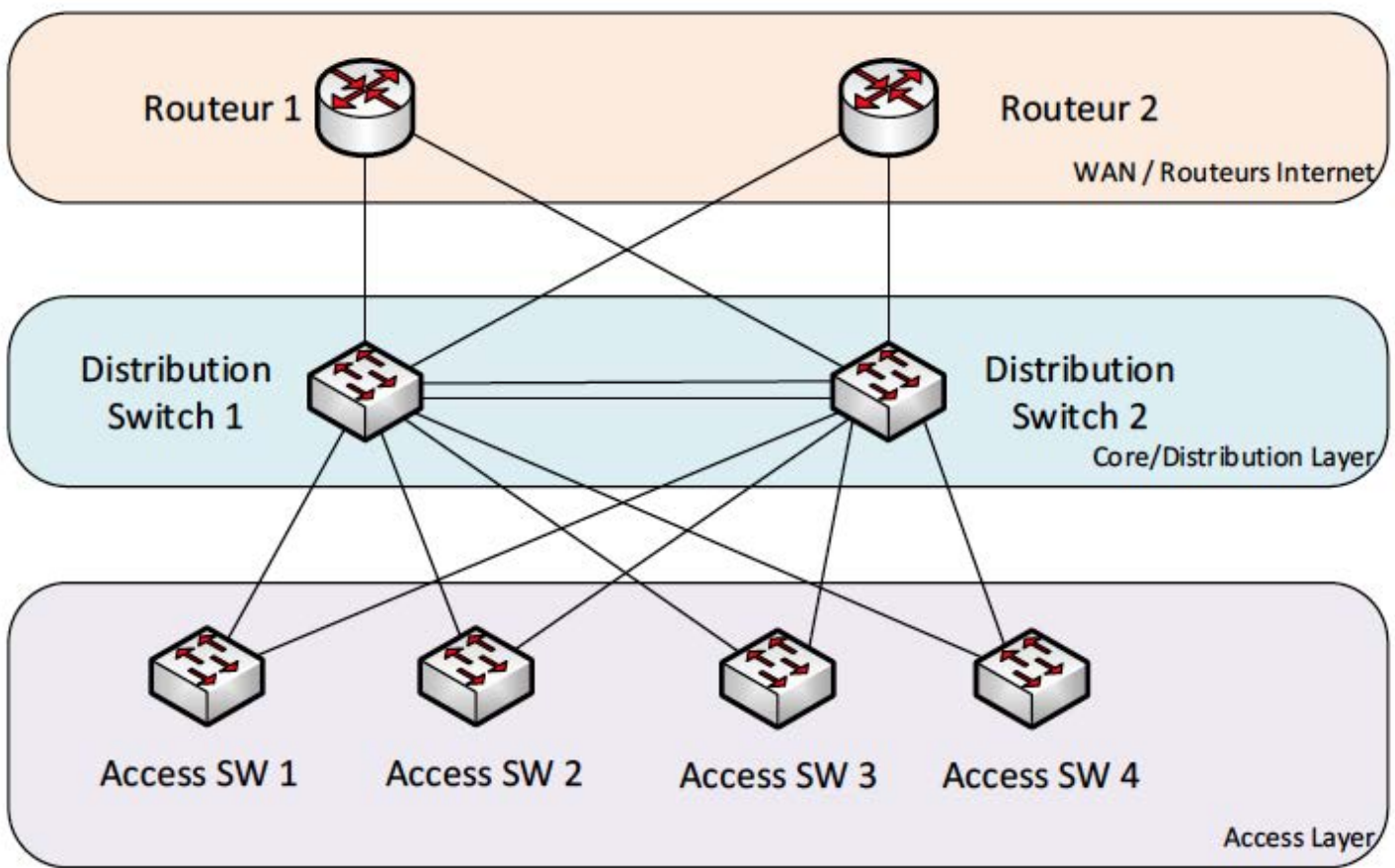




Le Switch crée un domaine de collision par interface Ethernet (ici 4 domaine de collision)



DEUX DOMAINES DE DIFFUSION



Terminologie de campus LAN avec indications de couche – Niveau 2

NIVEAU 3

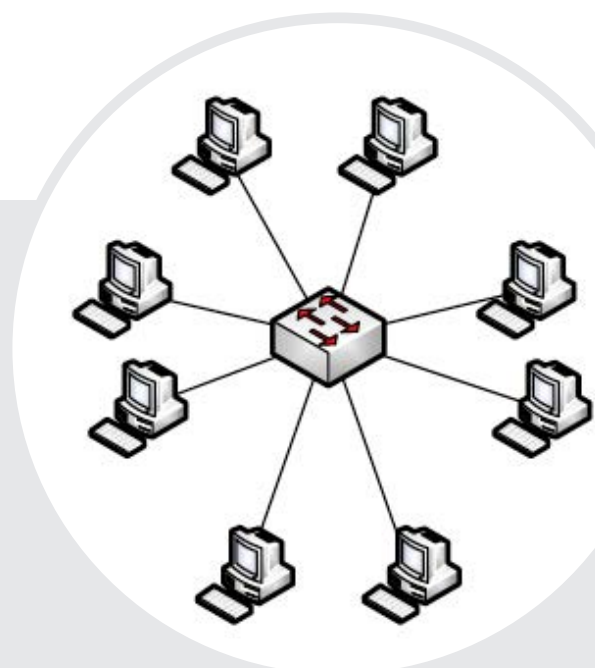
- Couche d'accès
- Couche de distribution
- Couche centrale or coeur

NIVEAU 2 (COLLAPSED CORE)

- Couche d'accès
- Couche distribution et coeur fusionné

DÉFINITIONS DE TOPOLOGIE

- Etoile (Star): un seul équipement est au centre des noeuds. Le schématiser engendre un résultat du schéma en forme d'étoile
- Maillage complet (Full Mesh): chaque noeud dispose d'une connexion vers l'autre noeud dans le réseau.
- Maillage partiel (Partial Mesh) – certains noeuds ont un lien avec d'autres mais pas tous.
- Hybride – une combinaison de différentes topologies



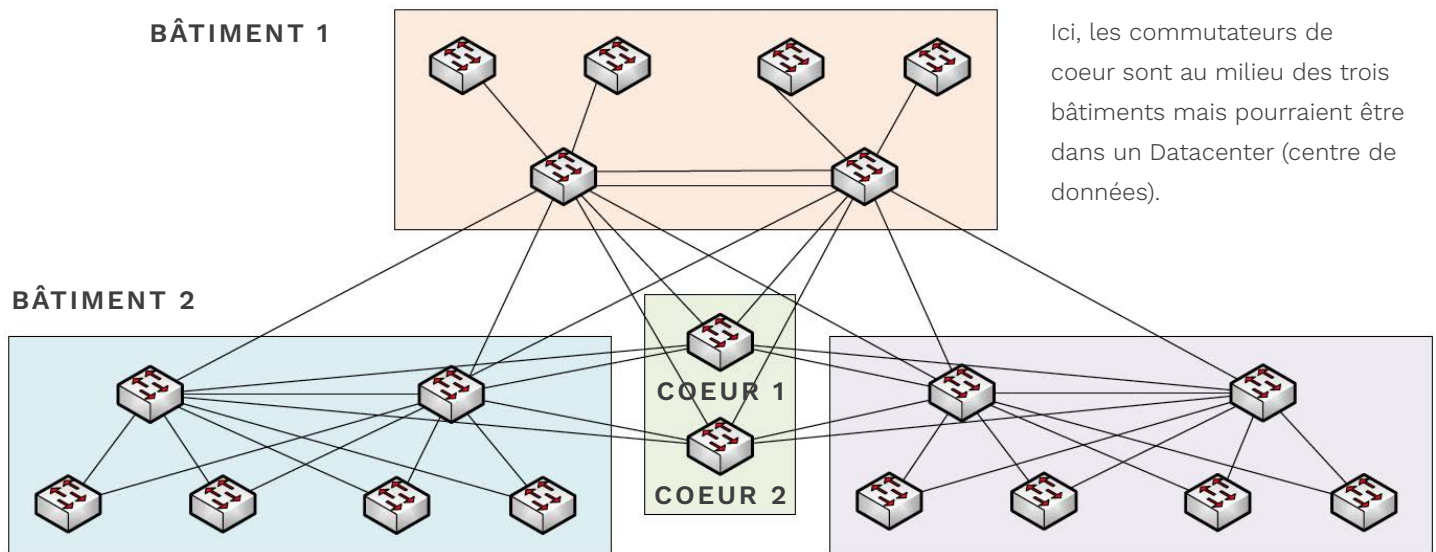
NORMES ETHERNET

L'IEEE a défini plusieurs normes pour la transmission Ethernet. Ces normes sont conçues en tenant compte de la distance, des médias et de la vitesse.

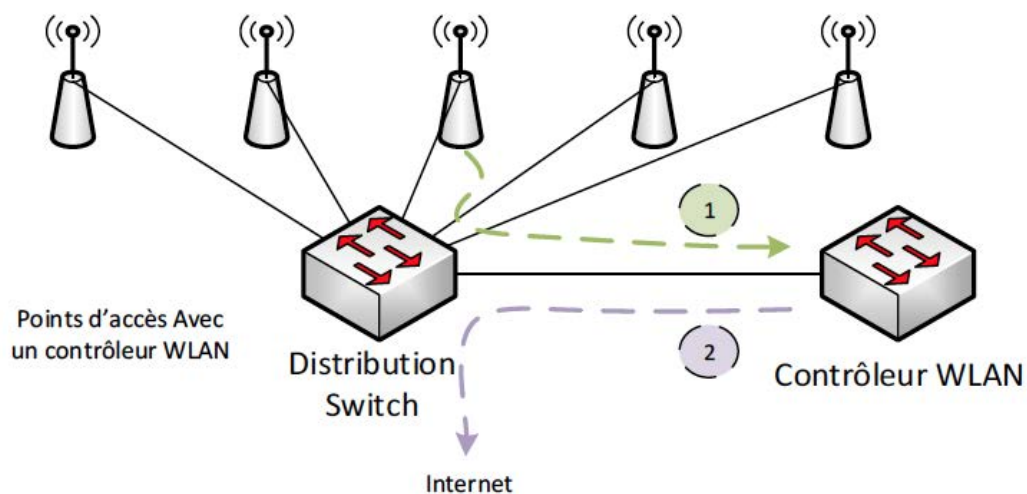
Chaque norme a le même format de trame pour que le trafic utilisant une norme puisse être traduit à une autre norme dans la logique de commutation. Les formats sont les mêmes (sauf pour la longueur dans certains cas).



ANALYSE DES MODÈLES LAN ETHERNET



Campus LAN Avec 3 lieux (ex: Bâtiments) distincts – Niveau 3



Le contrôleur WLAN (WLC) contrôle toutes les fonctions WLAN, y compris l'itinérance, l'authentification et d'autres fonctions.



Les AP (Access-Point) transfèrent le trafic des utilisateurs Wi-Fi au WLC



Ensuite le WLC envoie le trafic à Internet

En utilisant cette configuration, un grand réseau sans fil (WLAN) peut être construit au lieu de multiples réseaux disjoints.

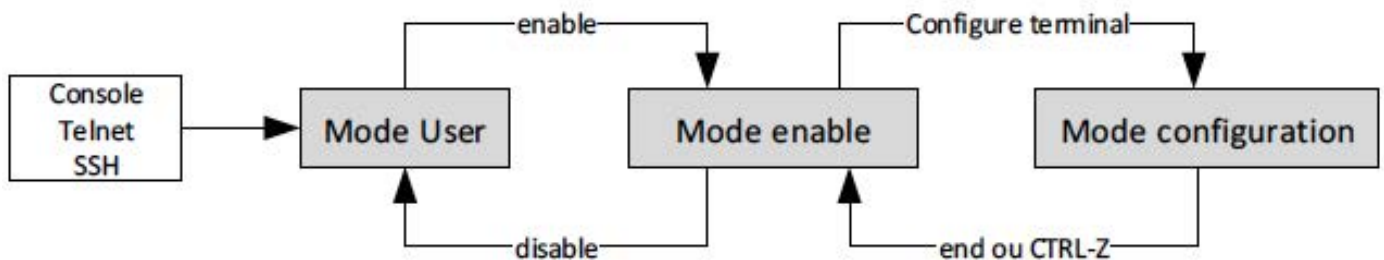
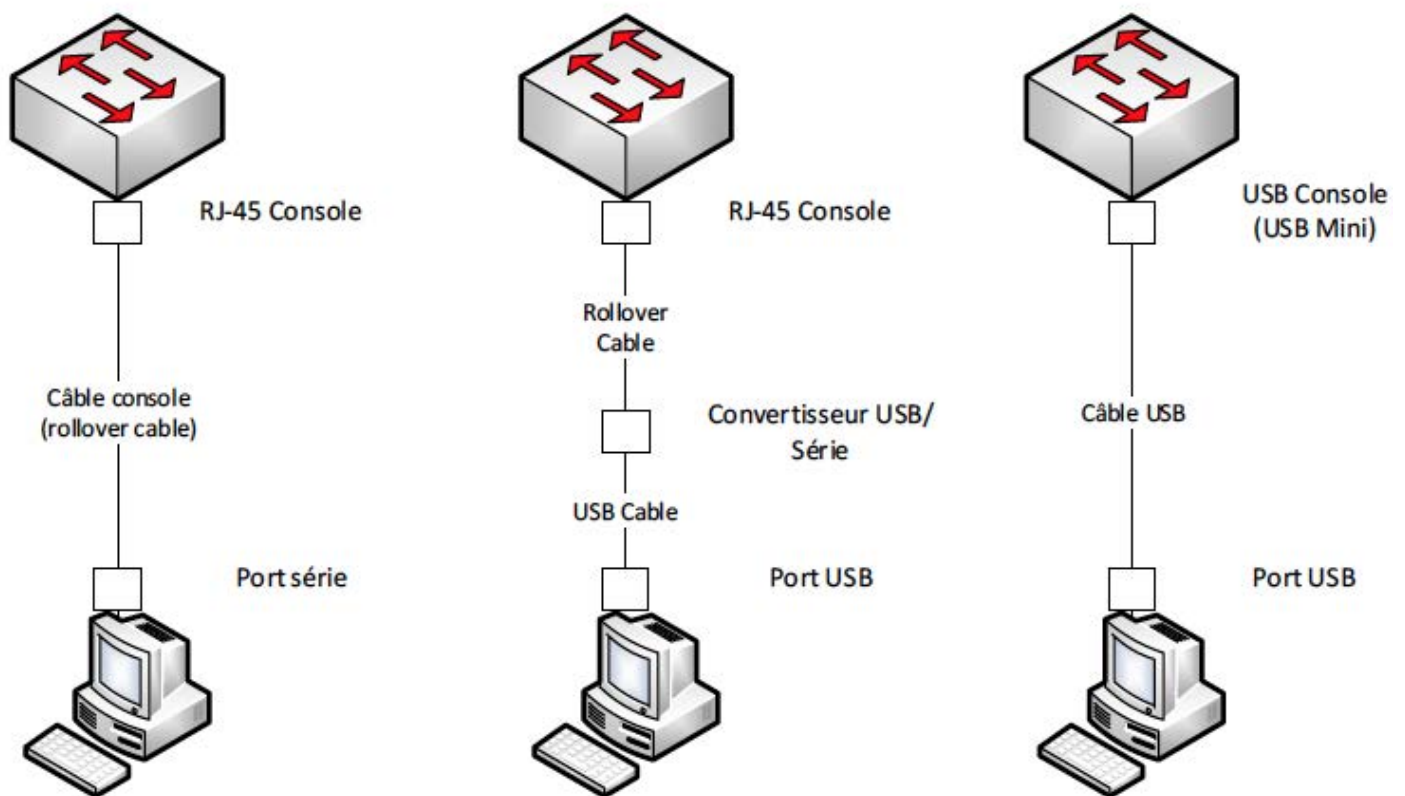
IMPLÉMENTATION DE LA COMMUTATION



INSTALLER ET CONFIGURER UN SWITCH CISCO

Méthodes pour accéder à la CLI Cisco (Command Line Interface) :

- **Port série** du PC : utilise un câble avec connecteur DB-9 d'un côté (PC) et RJ-45 de l'autre (Switch).
- **Convertisseur USB/Série** : dans le cas où 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 utilisent chacun un port USB. Le PC a un port USB standard et le switch a un port mini-USB.

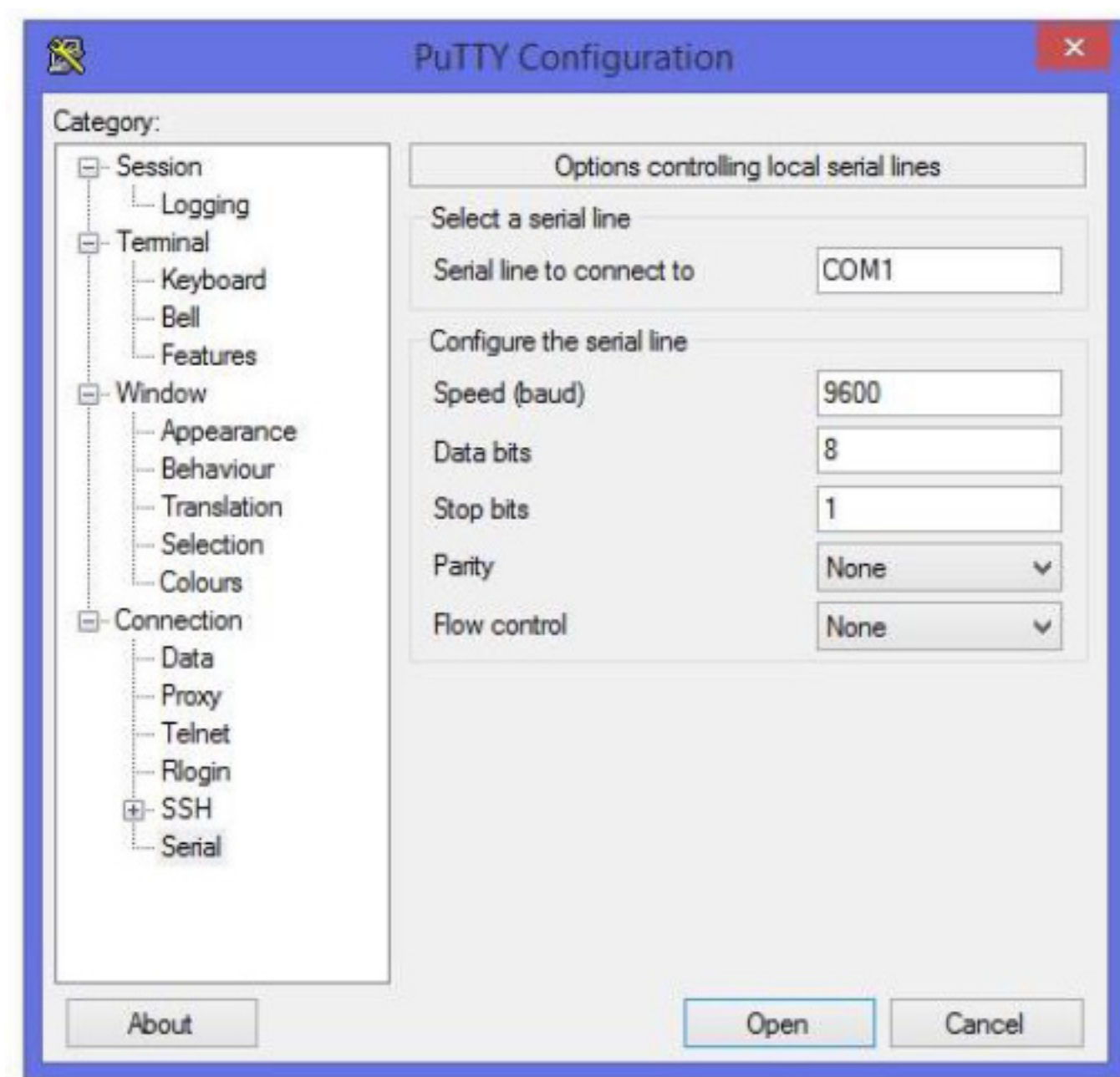


MODE CLI: USER, PRIVILÉGIÉ/EXEC (ENABLE) ET DE CONFIGURATION

PARAMÈTRES DE CONSOLE CISCO

- Vitesse/speed : 9600 bps
- 8 ASCII bits
- Pas de parité
- 1 bit d'arrêt (stop bit)
- Pas de contrôle de flux (flow control)

Ci dessous un exemple avec le logiciel Putty



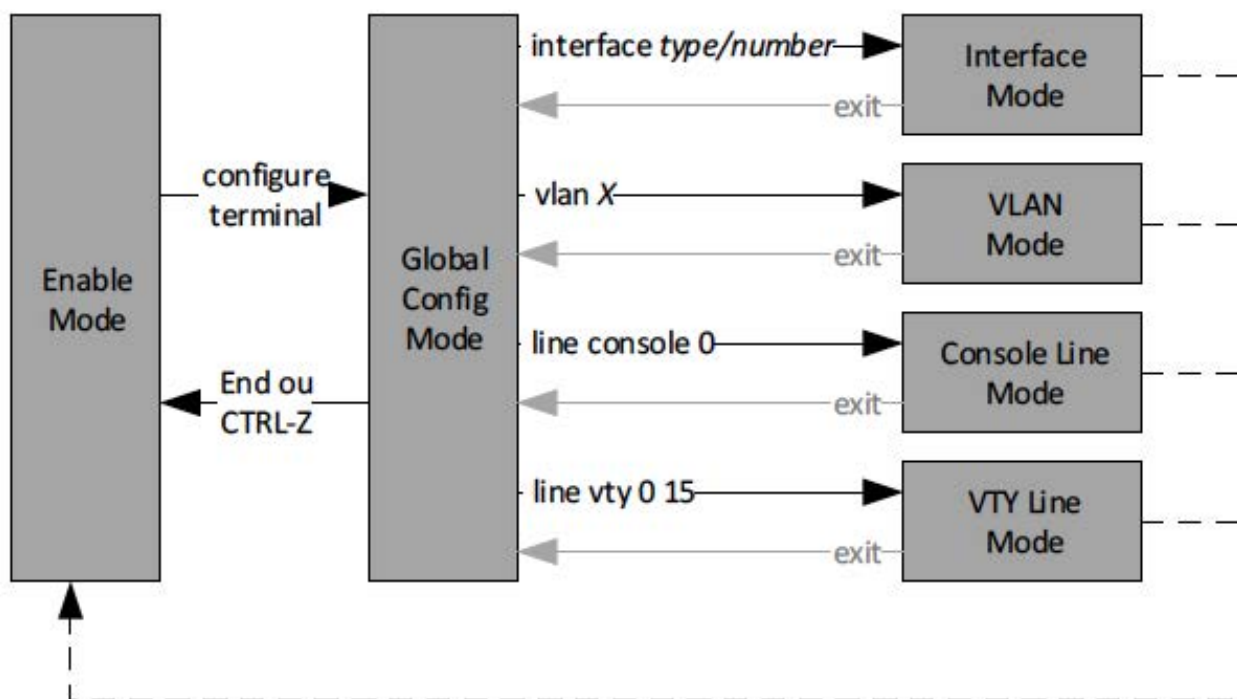
INSTALLER ET CONFIGURER UN SWITCH CISCO

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

Mémoire vive
Running-configuration

FLASH

Système d'exploitation
Cisco IOS

ROM

Programme de
démarrage (Bootstrap
Program)

NVRAM

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 où est stockée principalement le système d'exploitation Cisco IOS.

Cette mémoire n'est pas effacée lors du reboot. Peut 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 démarrage du switch ou lors d'un reboot.

FICHIERS PRINCIPAUX DE L'IOS

Startup-config: Contient la configuration sauvegardée du switch et est utilisée 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

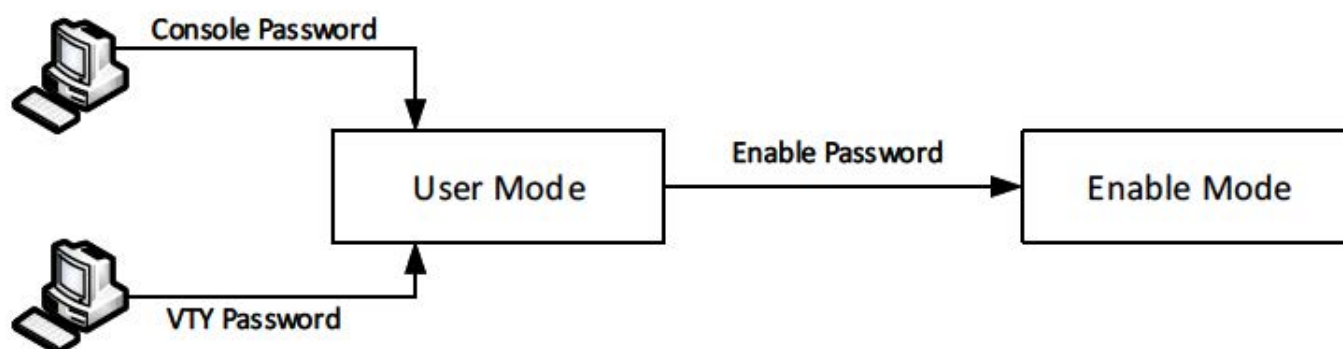
CONFIGURATION DE LA GESTION DE BASE DES COMMUTATEURS

POINTS CLÉS POUR SÉCURISER LE ROUTEUR

Les lignes **console** et **vty** peuvent être configurées pour utiliser des mots de passe simples.

Le mot de passe secret doit être défini car ce mot de passe contrôle l'accès à la configuration.

Les noms d'utilisateur et les mots de passe entrés en **mode global** peuvent également être utilisés pour sécuriser le routeur. La sous-commande **login local** est utilisée sur la console et les lignes **vty** lorsque les noms d'utilisateur et les mots de passe sont définis.



CONFIGURATION DES MOTS DE PASSE ET DU NOM D'HÔTE

```
Commutateur> enable
Switch # configure terminal
Commutateur (config) # enable secret CISCO
Switch (config) # hostname Cyril-Switch
Cyril-Switch (config) # line console 0
Cyril-Switch (config-line) # Password TOTO
Cyril-Switch (config-line) # login
Cyril-Switch (config-line) # exit
Cyril-Switch (config) # ligne vty 0 15
Cyril-Switch (config-line) # password TATA
Cyril-Switch (config-line) # login
Cyril-Switch (config-line) # end
Cyril-Switch #
```

2) Mode global

Créer des utilisateur et des mots de passe

1) Mode local

Activer l'utilisation des utilisateurs locaux

```
username cyril password deokfrgrg
username julien password shfsodfh

line vty 0 15
login local
```

CONFIGURATION POUR L'AUTHENTIFICATION DE CONNEXION NOM D'UTILISATEUR LOCAL

PROTECTION DU MOT DE PASSE ENABLE

La commande **enable password** et la commande **enable secret** peuvent être utilisées pour protéger le mode de configuration du routeur. Voici les règles d'accès au mode de configuration dans le routeur:

- les deux commandes sont configurées: Utiliser le mot de passe de la commande **enable secret** (car precedence).
- une commande est configurée: Utiliser le mot de passe dans cette commande.
- Aucune commande n'est configurée: les utilisateurs de la console peuvent accéder au mode de configuration sans mot de passe.

ÉTAPES DE CONFIGURATION POUR SÉCURISER LE ROUTEUR AVEC SSH

- 1 Configurez les lignes **vty** pour utiliser les noms d'utilisateurs
- 2 Ajoutez une ou plusieurs paires utilisateur / mot de passe dans la configuration globale
- 3 Générer les clés
- 4 Activez SSH v2.

2) Mode global

Créer des utilisateur et des mots de passe

1) Mode local

Activer l'utilisation des utilisateurs locaux

```
username cyril password deokfrgrg  
username julien password shfsodfh
```

```
line vty 0 15  
login local
```

CONFIGURATION POUR UNE CONNEXION SSH ENTRANTE

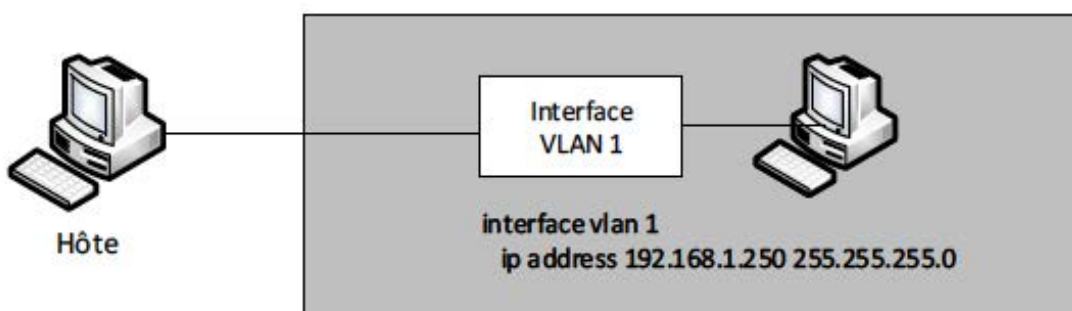
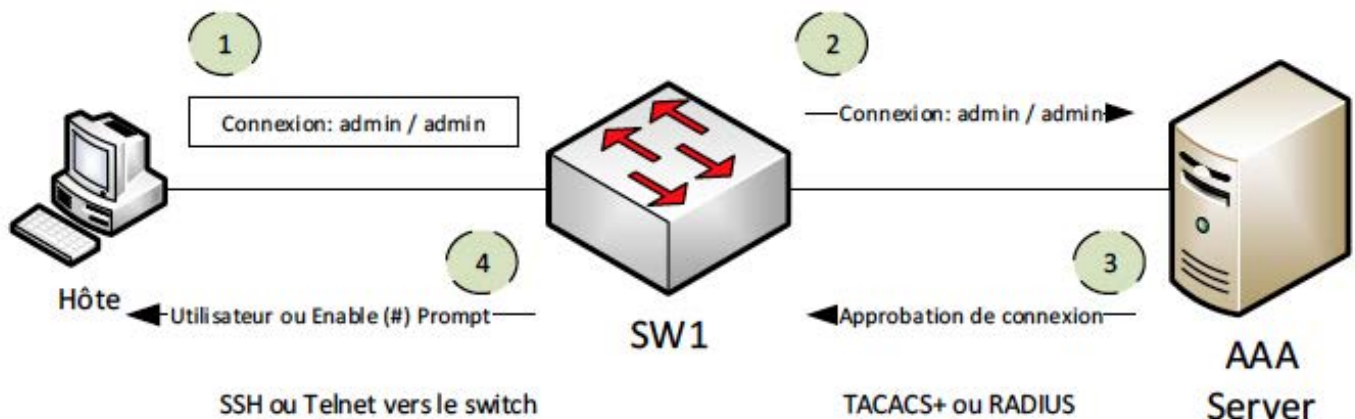
CONFIGURATION DE LA GESTION DE BASE DES COMMUTATEURS

UTILISATION DE SERVEURS EXTERNES POUR SÉCURISER L'ACCÈS AUX COMMUTATEURS

Lorsqu'il y a beaucoup de commutateurs à gérer, la configuration de l'utilisateur et du mot de passe pour chaque commutateur peut être fastidieuse. Par conséquent, les serveurs externes peuvent être utilisés pour authentifier les utilisateurs pour de nombreux commutateurs. Cisco appelle ces serveurs AAA. AAA signifie Authentication, Authorization and Accounting (comptabilité).

Il existe deux types de serveurs AAA: RADIUS et TACACS +

AUTHENTIFICATION AVEC UN SERVEUR D'AUTHENTIFICATION EXTERNE TACACS + OU RADIUS



Concept d'une interface virtuelle commutée (SVI) où un hôte distant peut accéder au commutateur à distance.

CONFIGURER LA VITESSE, LE DUPLEX ET LA DESCRIPTION D'UNE INTERFACE D'UN SWITCH

Switch # configure terminal

Switch (config) # interface FastEthernet 0/3

Switch (config-if) # duplex full

Switch (config-if) # speed 100

Switch (config-if) # description serveur SYNOLOGY

Switch (config-if) # exit

CONFIGURER UNE PLAGES DE PORTS

Switch # configure terminal

Switch (config) # interface range FastEthernet 0/3 - 11

Switch (configuration-if-range) # spanning-tree portfast

Switch (config-if-range) # exit

ARRÊT D'UNE INTERFACE AVEC LA COMMANDE SHUTDOWN

Switch # configure terminal

Switch (config) # interface FastEthernet 0/4

Switch (config-if) # shutdown

Switch (config-if) # exit

REACTIVATION DU PORT APRÈS L'ARRÊT

Switch # configure terminal

Switch (config) # interface FastEthernet 0/4

Switch (config-if) # no shutdown

Switch (config-if) # exit

CONFIGURATION DES INTERFACES DE COMMUTATION

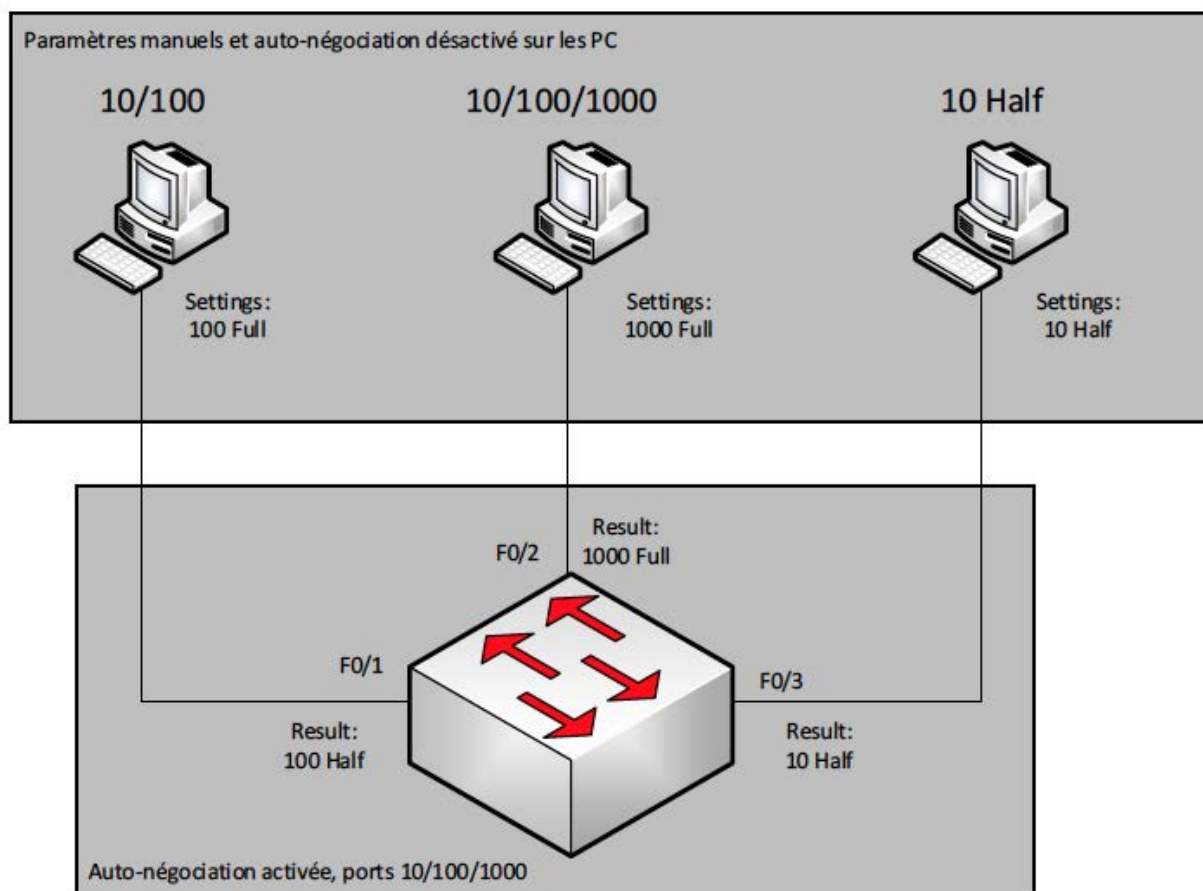
Vitesse et duplex: les commutateurs Cisco négocient automatiquement la vitesse du lien et si l'activité bidirectionnelle (duplex) peut avoir lieu. Ce processus de négociation automatique a lieu en envoyant une impulsion sur le fil et en attendant une réponse. Les valeurs par défaut sont les suivantes:

- **Vitesse:** négociation automatique de la vitesse jusqu'à l'échec. Sinon, utilisation de la vitesse la plus lente (10 Mbps)
- **Duplex:** Si la vitesse est 10 Mbps ou 100 Mbps alors ce sera en half-duplex, sinon ce sera en full-duplex.

Pour toutes les versions / variantes de la sécurité des ports (commande portsecurity),

voici les éléments en commun:

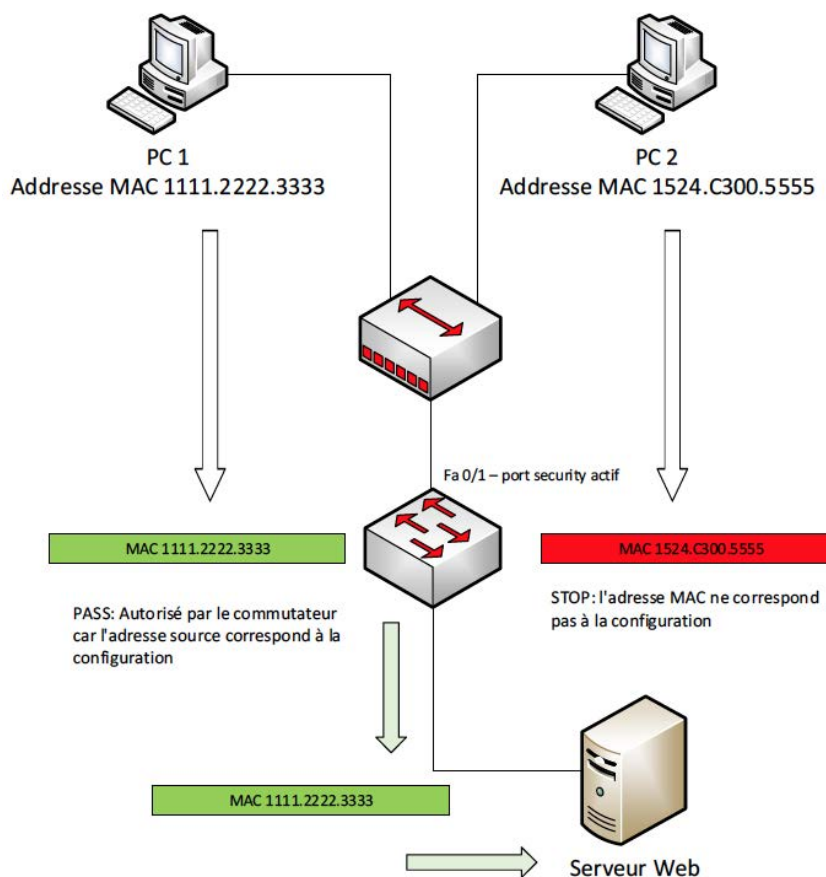
- Définissez une valeur sur l'interface pour définir le nombre maximum d'adresses MAC autorisées arrivant sur l'interface
- Le switch comptabilise les différentes adresses MAC entrantes sur une interface et déclenche la sécurité du port si le nombre maximal d'adresses MAC arrivant sur l'interface a augmenté au-delà du nombre défini



OPTIONS DE COMMANDE DE VIOLATION DU PORT-SECURITY	PROTECT	RESTRICT	SHUTDOWN
Infraction au trafic rejeté	oui	oui	oui
Envoyer une trap SNMP et un log	non	oui	oui
Compteur de violations augmente pour chaque trame de violation	non	oui	oui
Mettre l'interface en état err-disabled et jetez tout le trafic	non	non	oui

CONFIGURATION DE LA SÉCURITÉ DES PORTS

- **ÉTAPE 1:** Configurez l'interface comme un port d'accès (**switchport mode access**) ou Trunk (**switchport mode trunk**).
- **ÉTAPE 2:** Activer la sécurité du port via la commande **switchport port-security**
- **ÉTAPE 3:** (facultatif) Définissez le nombre d'adresses MAC autorisées à l'aide de la commande **switchport port-security maximum number**
- **ÉTAPE 4:** (facultatif) Remplace l'action par défaut (shutdown) en cas de violation de sécurité: **switchport {protect | restrict | shutdown}**
- **ÉTAPE 5:** (facultatif) Définissez les adresses MAC source via la commande **switchport-security mac-address mac-address**
- **ÉTAPE 6:** (facultatif) Configurez le commutateur à apprendre automatiquement les adresses MAC entrantes via la commande **port-security mac-address sticky**



CONFIGURATION D'ADRESSES MAC STATIQUES

Switch # **configure terminal**

Switch(config) # **interface FastEthernet 0/1**

Switch(Config-if) # **switchport mode access**

Switch(Config-if) # **switchport port-security**

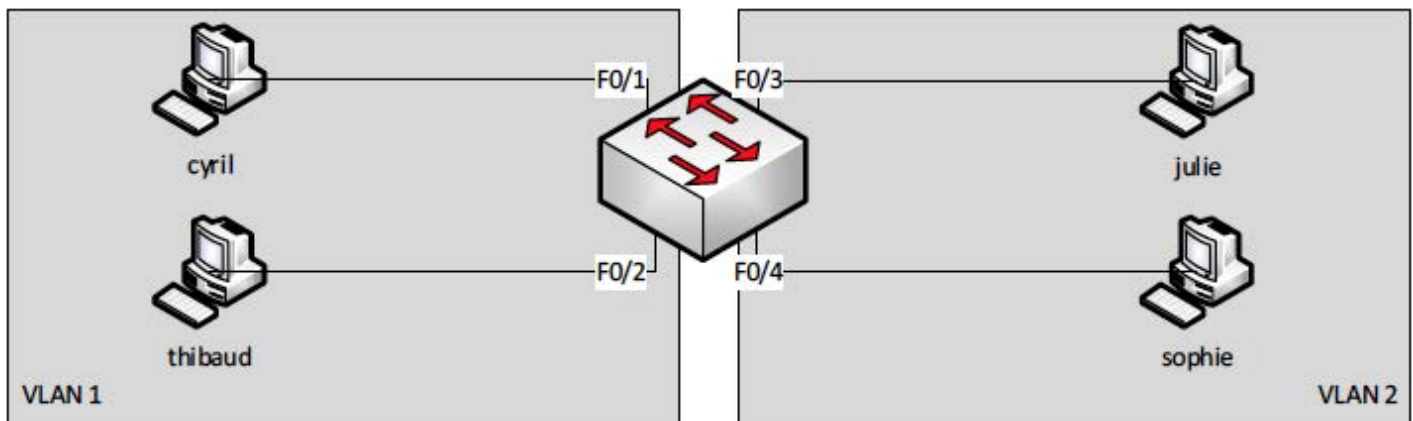
Switch(Config-if) # **switchport port-security mac-address 1111.2222.3333**

Switch(Config-if) # **switchport port-security mac-address 4444.5555.6666**

Switch(Config-if) # **exit**



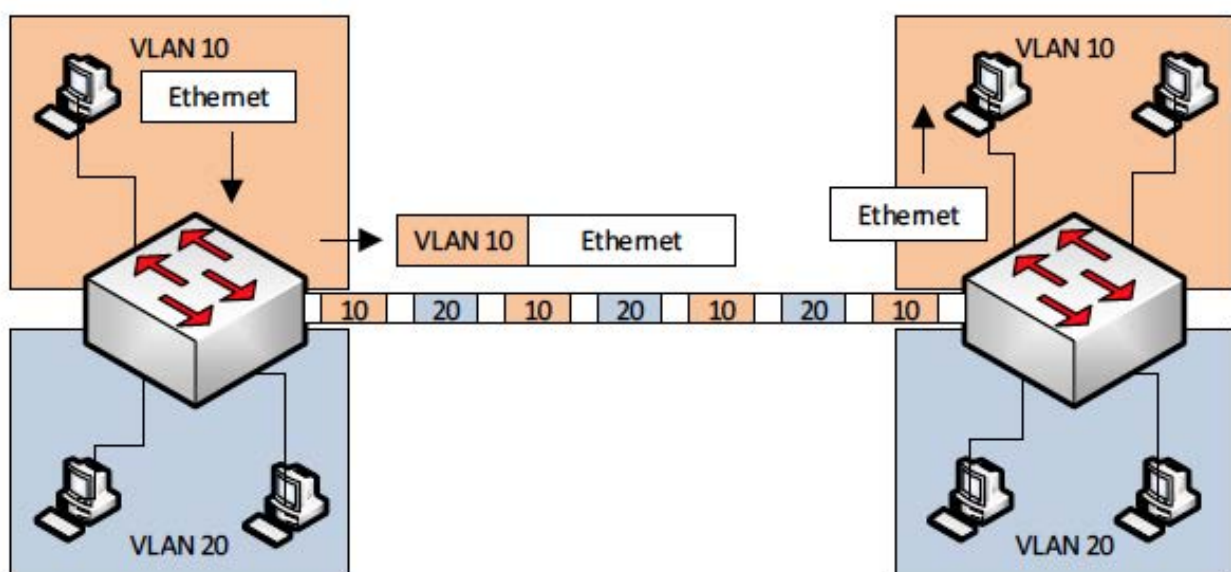
IMPLÉMENTATION DES VIRTUAL LAN ETHERNET



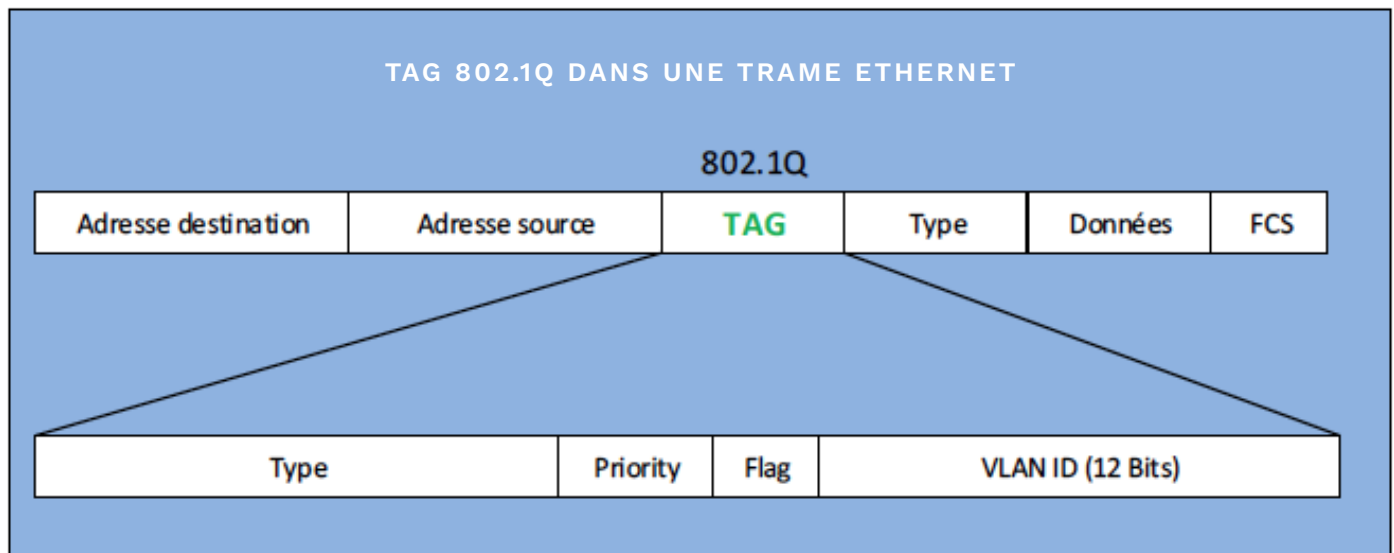
Création de deux domaines de broadcast sur un seul switch grâce à deux VLANs

POURQUOI UTILISER LES VLANS ?

- **Diminue le nombre de trames reçues** par chaque équipement.
- **Diminue l'utilisation CPU** de chaque équipement connecté au switch en réduisant le nombre de trames de broadcast reçues.
- **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 à un switch en particulier.



TRUNK ENTRE DEUX SWITCHS



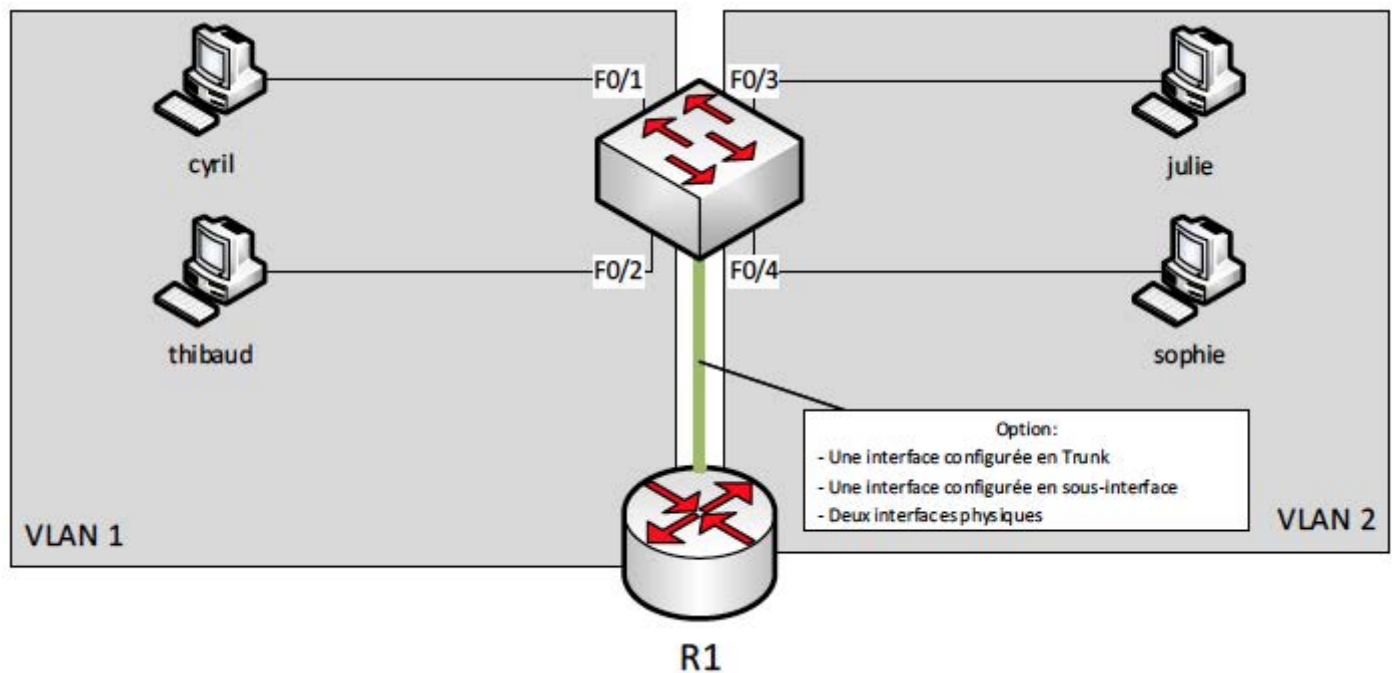
**NOTES IMPORTANTES
SUR LES VLANS**

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 à 4094 n'est présente que sur les switchs récents.

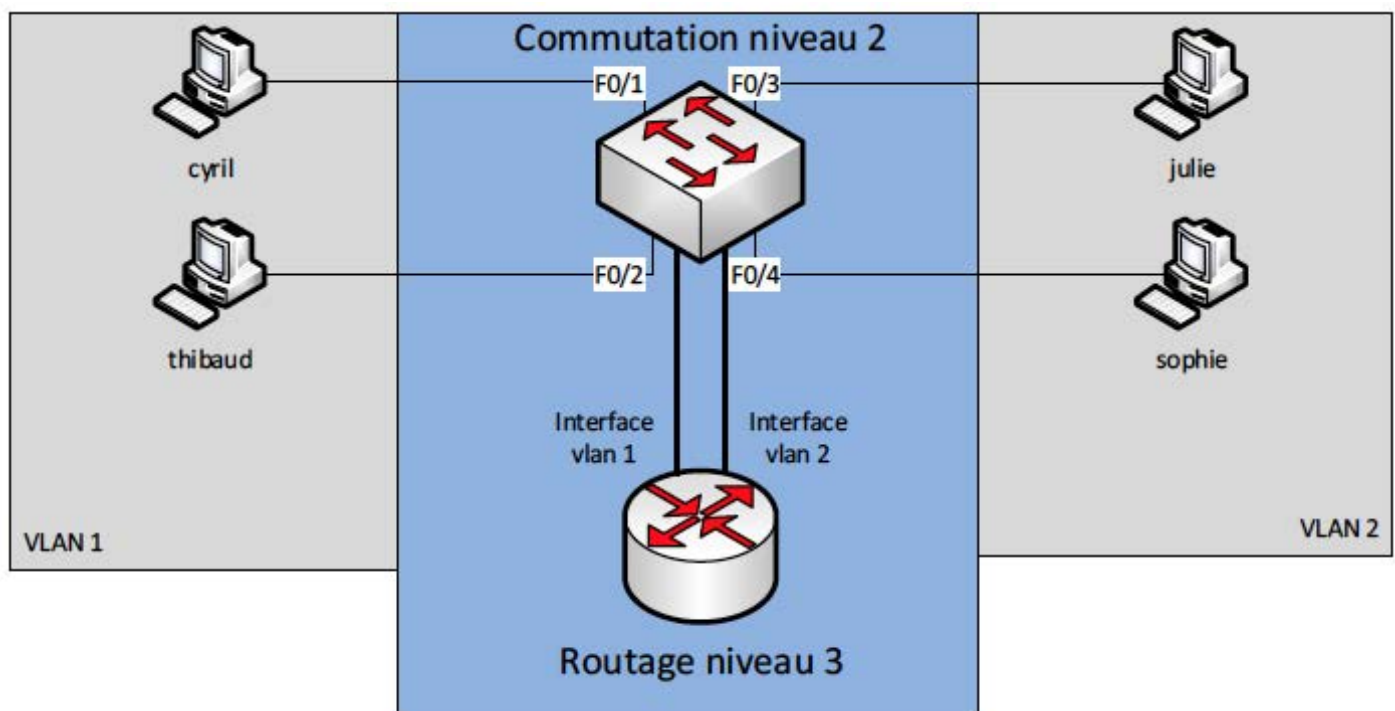
VLAN NATIF : Ce VLAN, aussi appelé VLAN non-tagué (**untagged**), permet d'envoyer une trame non 802.1Q sur un lien Trunk. Si l'équipement en face ne comprend pas le 802.1Q alors le switch récupérera cette trame et la mettra dans le VLAN souhaité.

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 NIVEAU 3

(Le carré bleu décompose le switch niveau 3)

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" 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**"

CONFIGURATION VLAN ET ASSIGNATION

```
Switch# 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



REMARQUE

En plus d'utiliser un routeur physique et de basculer entre les VLAN, certains commutateurs intègrent les fonctionnalités de niveau 3. Ces commutateurs sont appelés commutateurs multicouches et permettent à l'administrateur réseau d'avoir la commutation Layer-2 et le routage Layer-3 dans la même boîte physique. L'administrateur réseau a juste à configurer les VLAN et les ports, branchez les périphériques, et le switch fait la commutation et le routage.

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 autorisée 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

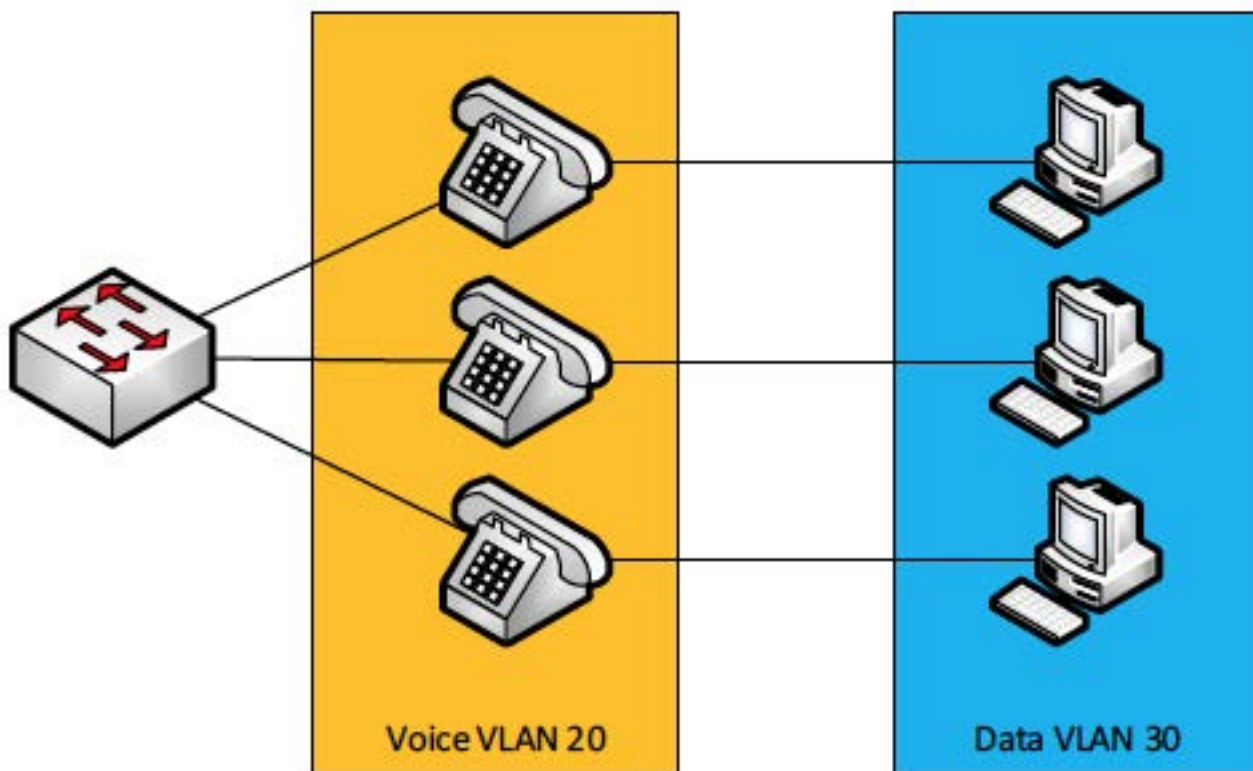
OPTIONS DE CONFIGURATION DU TRUNK

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 !

UTILISATION DU TÉLÉPHONE ET DU PC SUR LE MÊME PORT CONNECTÉ AU SWITCH

Les commutateurs Cisco peuvent marquer différemment le trafic voix et le trafic de données sur le même port de commutateur physique. Le VLAN de données est configuré comme un port d'accès. Le VLAN voix a un tag différent de celle du VLAN de données. De plus le trafic pour le VLAN de données ne sera pas tagué entre le téléphone et le PC.



CONFIGURATION DE LA VOIX ET DES DONNÉES VLANS

```
SW1# configure terminal
```

```
SW1 (config)# interface FastEthernet 0/1
```

```
SW1 (config-if)# switchport mode access
```

```
SW1 (config-if)# switchport access vlan 30
```

```
SW1 (config-if)# switchport voice vlan 20
```

```
SW1 (config-if)# exit
```

Tout d'abord, configurez l'interface en tant que port d'accès puis définissez le VLAN de données. Enfin, définissez le VLAN voix. Notez que Le trunk est implicite et n'est pas directement configuré sur l'interface.

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

SHOW INTERFACE STATUS

PORT	NOM	STATUS	VLAN	DUPLEX	SPEED	TYPE
Fa0/1		notconnect	1	auto	auto	10/100BaseTX
Fa0/2		notconnect	1	auto	auto	10/100BaseTX
Fa0/3		connected	1	half	100	10/100BaseTX
Fa0/4		connected	1	a-full	a-100	10/100BaseTX
Fa0/5		connected	1	a-full	a-100	10/100BaseTX
Fa0/6		notconnect	1	auto	auto	10/100BaseTX

On voit que sur l'Interface FastEthernet 0/3, il s'agit d'une mauvaise négociation où la vitesse est de 100 Mbps/s mais le duplex est en half.

ANALYSE DE VLAN ET TRUNK

1. S'assurer que tous les ports d'accès sont affectés à leur VLAN respectifs. Reconfigurer au besoin.
2. S'assurer que les VLAN sont actifs sur chaque commutateur. Configurer les VLAN au besoin.
3. Vérifier la liste des VLAN autorisés. Configurer si nécessaire.
4. Vérifiez les interfaces Trunk dans le cas où l'interface agit comme un Trunk mais que l'interface sur l'autre switch n'est pas configuré comme un Trunk. Reconfigurer au besoin.

CODE D'ÉTAT D'UNE INTERFACE LAN ETHERNET

LINE STATUS	PROTOCOL STATUS	INTERFACE STATUS	DESCRIPTION
Administratively Down	Down	Disabled	Interface désactivée par l'admin (shutdown)
Down	Down	notconnected	Pas de câble, câble défectueux, mauvais duplex ou vitesse, voisin éteint
Up	Down	notconnected	Résultat impossible
Down	Down (err-disabled)	Err-disabled	Le Port-security a désactivé l'interface
Up	Up	connected	Interface fonctionne correctement

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 les opérations suivantes:

- a si le Port-security est actif, alors le switch effectue la vérification
- b si le port est en ACCESS, le switch identifie le VLAN associé au port
- c si le port est en TRUNK, Le switch identifie 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 (Table MAC ou CAM) :

- 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 DE VITESSE/DUPLEX SANS AUTO-NÉGOCIATION

SI VITESSE / SPEED	ALORS 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

COMMANDES POUR LES PORTS EN ACCESS ET VLAN

COMMANDE	DESCRIPTION
show vlan brief show vlan	Liste les VLAN et les interfaces associées (les Trunks ne sont pas affichés)
show vlan id num	Liste les interfaces ACCESS et TRUNK dans le VLAN en question
show interfaces type 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

AFFICHAGE DE LA COMMANDE SHOW INTERFACE

Switch# **show interfaces fa0/12**

FastEthernet0/12 is up, line 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 runs, 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#

STATUS DE L'INTERFACE ETHERNET

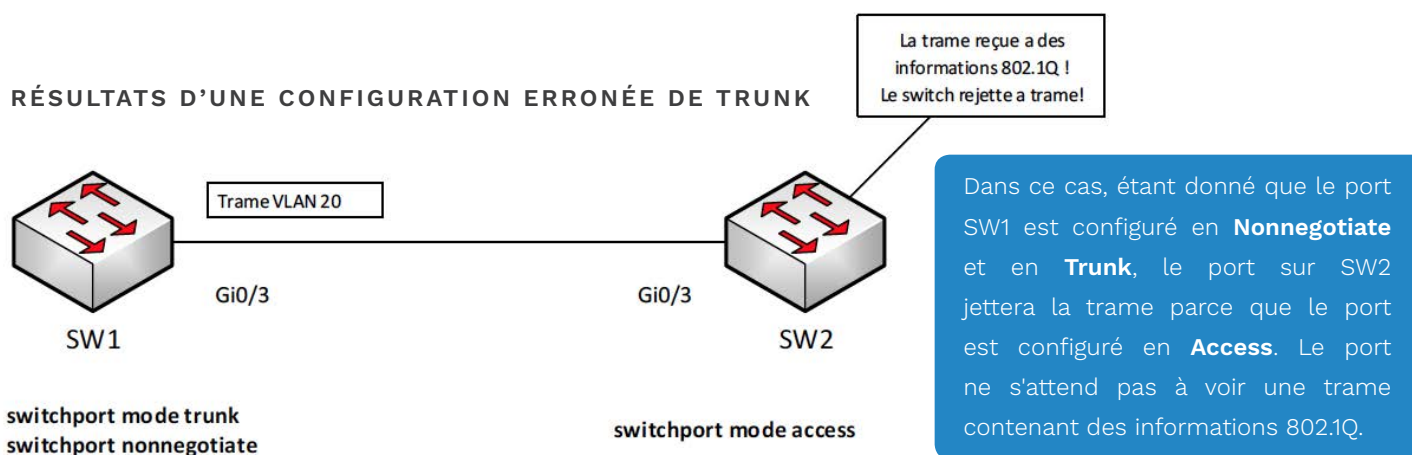
Avec la commande **show interface**, on peut visualiser la vitesse, le duplex, les erreurs CRC, les collisions...

COMPTEURS D'INTERFACE

- **Runts:** Trame courte de moins de 64 octets indiquant une collision
- **Giants:** Trame longue supérieure à 1518 octets
- **Input errors:** Total de toutes trames entrantes erronées
- **CRC:** échec de la vérification FCS
- **Frame:** Trame mal formatée pouvant être causée par une collision
- **Packets Output:** Nombre de paquets envoyés par l'interface
- **Output errors:** Nombre total de paquets qui auraient dû être envoyés mais qui ne l'ont pas été suite à une erreur
- **Collisions:** Un compteur de toutes les trames ayant subi une collision
- **Late Collisions** (Collisions tardives): Il s'agit de collisions qui ont eu lieu après la transmission de 64 octets. Les collisions tardives peuvent indiquer un décalage en duplex

FONCTIONNEMENT DE LA FONCTION PORT-SECURITY SUR L'INTERFACE

1. Utilisez les commandes **show running-config** ou **show port-security** pour déterminer les interfaces configurées avec la fonction Port-security.
2. Vérifiez si une violation de sécurité se produit en fonction de la configuration du Portsecurity:
 - a **Shutdown** - le port est dans l'état **err-disabled**
 - b **Restrict** - l'interface est opérationnelle (UP), connectée, fait passer le trafic uniquement légitime et la commande **show port-security Interface** affiche un compteur qui s'incrémente.
 - c **Protect** - l'interface est opérationnelle (UP), fait passer le trafic uniquement légitime mais la commande **show port-security Interface** n'affiche pas un compteur qui s'incrémente.
3. Dans tous les cas, comparez les adresses MAC source vue et les adresses MAC configurées via la commande **show port-security interface**.



GESTION DES ÉQUIPEMENTS CISCO



JOURNALISATION (LOGGING)

Le routeur ou le commutateur (switch) enregistrera des événements tels que les états haut (up) et bas (down) de l'interface, les requêtes multicast et les avertissements environnementaux (température,...) sur la console. Par défaut, les événements sont envoyés à la console. Mais pour les utilisateurs connectés à distance (telnet, ssh), la commande **terminal monitor** doit être utilisée sur chaque session de connexion.

Pour un examen ultérieur, le routeur peut faire l'une des deux choses:

- Tout d'abord, le routeur peut mettre en mémoire tampon les entrées du journal à l'aide de la commande **logging buffered**.
- Ensuite, la commande **show logging** peut être utilisée par un utilisateur pour examiner les journaux. Les journaux peuvent aussi être envoyés à un serveur syslog avec la commande **logging X.X.X.X** où X.X.X.X est l'adresse du serveur syslog.

<u>Mots clés</u>	<u>Nombre</u>	<u>Description</u>	
Emergency	0	Mesures immédiates à prendre	Sévère
Alert	1	Système inutilisable	
Critical	2	Événement critique (Maximum de 3)	Impactant
Error	3	Événement d'erreur (au milieu de 3)	
Warning	4	Événement d'avertissement (le plus bas de 3)	
Notice	5	Normal, plus important	Normal
Informational	6	Normal, moins important	
Debug	7	Action immédiate requise	Déboguer

Niveaux de gravité des messages Syslog

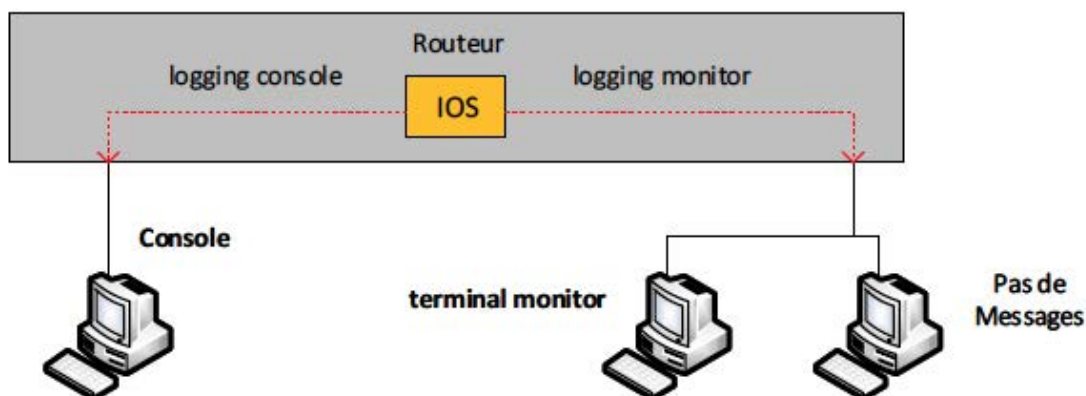
CONFIGURATION DES MESSAGES ENREGISTRÉS POUR CHAQUE SERVICE D'ENREGISTREMENT

SERVICE	POUR ACTIVER LA JOURNALISATION	POUR DÉFINIR DES NIVEAUX DE MESSAGE
Console	logging console	logging console level-name level-number
Moniteur (telnet, ssh)	logging monitor	logging monitor level-name level-number
Buffer	logging buffered	logging buffered level-name level-number
Syslog	logging host X.X.X.X	logging trap level-name level-number

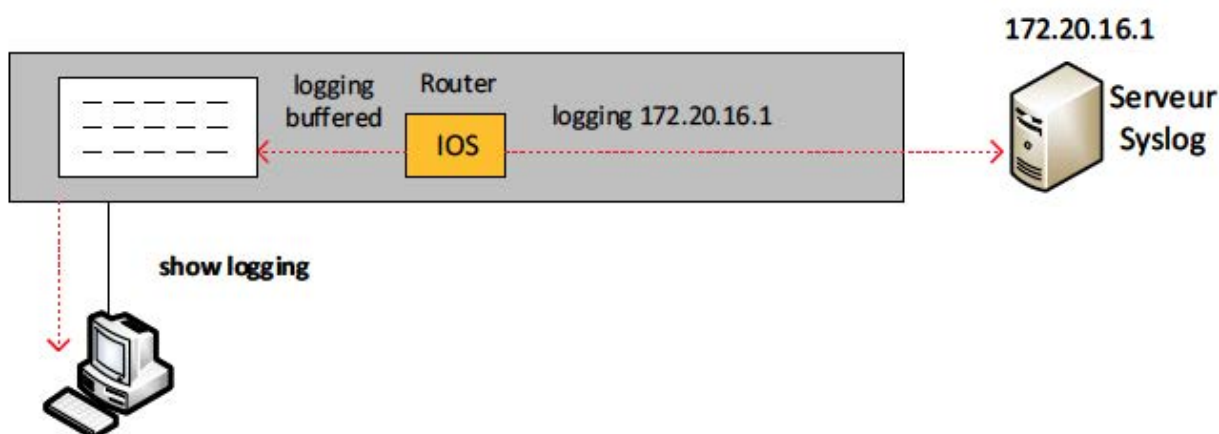
UTILISATION D'UNE LOOPBACK POUR LES INFORMATIONS NTP AU LIEU D'UNE INTERFACE PHYSIQUE:

Si un client demande des informations NTP à partir d'une interface physique qui est en panne, le client ne sera pas en mesure de mettre à jour son horloge. Toutefois, en utilisant une interface Loopback (interface de bouclage) cela assure que le client recevra des informations NTP. L'interface Loopback configurée est toujours disponible tant que le routeur est sous tension.

Enregistreur
d'évènement



Enregistrement
des événements
pour examen
ultérieur



CONFIGURATION NTP:

Network Time Protocol est utilisé pour synchroniser le temps entre plusieurs périphériques.

Cela est particulièrement utile lorsque la journalisation est activée sur plusieurs périphériques et qu'un problème doit être résolu.

CONFIGURATION:

```
ntp server X.X.X.X
```

DIFFÉRENCES ENTRE LES CLIENTS NTP ET LES SERVEURS:

- Les clients NTP ajustent leur temps en fonction de ce qu'ils reçoivent d'un serveur NTP
- Les serveurs NTP envoient de l'information sur le temps mais n'ajustent pas leurs horloges internes
- Les clients et les serveurs NTP synchronisent leur temps et transmettent des informations temporelles à d'autres périphériques.

CISCO DISCOVERY PROTOCOL (CDP):

CDP est utilisé par les routeurs et switch pour communiquer des informations entre les périphériques directement connectés. CDP peut servir de dispositif de dépannage et de cartographie de la topologie du réseau.

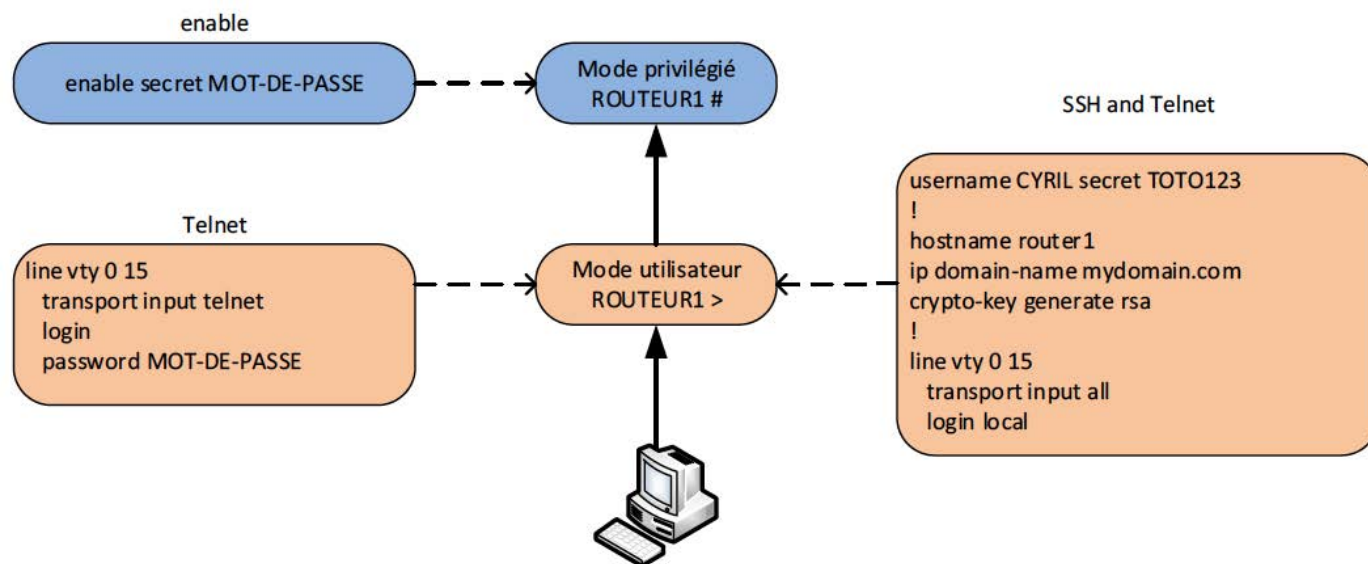
Informations communiquées par CDP :

- **Device identifiant** – généralement le nom d'hôte
- **Address list** – adresse réseau et adresse liaison de données
- **Port Identifier** – l'interface distante qui a envoyée l'annonce CDP
- **Capacities List** – ce que le périphérique distant peut faire, comme un routeur, un switch, un telephone, une borne Wi-Fi...
- **Plateform** – modèle de périphérique et la version de l'IOS

COMMANDE CDP

COMMANDE	DESCRIPTION
show cdp neighbors type <i>number</i>	Liste un résumé sur chaque voisin. Si une interface a été spécifiée, seul le périphérique connecté à cette interface sera affiché
show cdp neighbors detail	Énumère un ensemble d'information, une pour chaque voisin
show cdp entry <i>name</i>	Énumère les mêmes informations que la commande show cdp neighbors detail , mais uniquement pour le nom de voisin (note: le nom est sensible à la casse)

CONFIGURATION D'UNE CONNEXION SÉCURISÉE



MOTS DE PASSE SUR LES ANCIENS APPAREILS IOS:

Voici les commandes utilisées pour définir des mots de passe pour sécuriser la commande enable du routeur et les port VTY:

password *password* (console ou vty line)

username *name* **password** *password* (global)

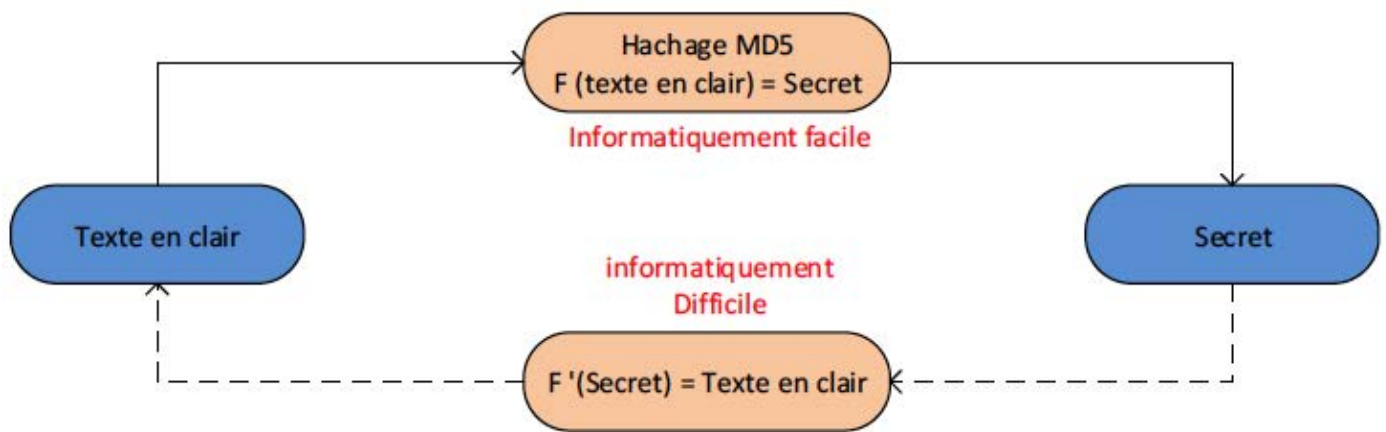
enable *name* **password** *password* (global)

ACTIVEZ LE MOT DE PASSE ENABLE:

Initialement, la commande **enable password** a été utilisée pour sécuriser le routeur. Avec les nouvelles versions d'IOS, la commande **enable password** a été remplacée par la commande **enable secret**. Voici les règles entre ces deux commandes:

- Si les deux commandes sont configurées, **enable secret** est utilisé et **enable password** est ignoré.
- Si seulement une seule commande est configurée, utilisez le mot de passe associé à cette commande.
- Si aucune des deux n'est configurée, les utilisateurs de la console passeront directement au mode privilégié mais l'accès Telnet et ssh est désactivé jusqu'à ce qu'un mot de passe **enable** ou un mot de passe sur la ligne VTY soit configurée.

CONFIGURATION D'UNE CONNEXION SÉCURISÉE



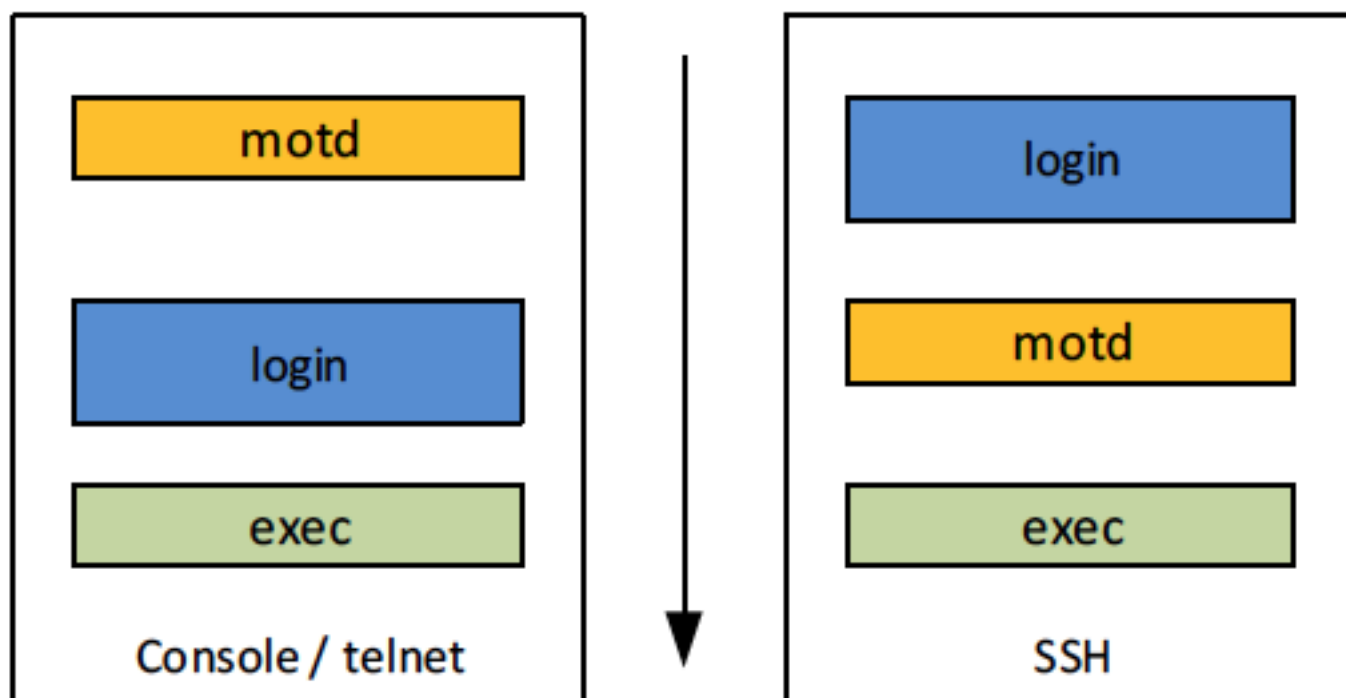
Comment le routeur utilise le hachage MD5 du mot de passe **enable secret** pour l'authentification?

- 1 Lorsque la commande **enable secret** est exécutée, le routeur crée un hachage MD5 du mot de passe en texte brut et stocke le hachage dans la configuration.
- 2 Lorsqu'un utilisateur ouvre une session et tape **enable**, le mot de passe est demandé. Le routeur exécute alors un hachage MD5 sur le mot de passe entré.
- 3 Le routeur compare le hachage stocké et le hachage entré. Si les deux hachages correspondent, le mot de passe saisi est considéré correct et l'utilisateur bascule en mode privilégié (routeur1#)

DIFFÉRENTS TYPES DE BANNIÈRES PRIS EN CHARGE PAR CISCO DEVICES

TYPE DE BANNIÈRE	USAGE
Message de la journée (motd)	Utilisé pour des avis temporaires qui changent régulièrement, telles que les notifications de maintenance pour les temps d'arrêt.
login	Il s'agit du premier message illustré lors de la connexion, donc il s'afficherait des messages comme « Accès non autorisé interdit »
exec	Cette bannière s'affiche après la connexion. Cette bannière pourrait afficher des informations sur le périphérique, telles que l'emplacement exact ou autres paramètres.

DIFFÉRENCES DANS L'ORDRE DE BANNIÈRE BASÉE SUR LA MÉTHODE D'ACCÈS



QUATRE TYPES DE MÉMOIRE DU ROUTEUR:

RAM

Mémoire de travail et
running-config

FLASH

Logiciel Cisco IOS

ROM

Programme
d'amorçage (Bootstrap)
et ROMMON

NVRAM

startup-config

SÉQUENCE D'AMORÇAGE DU ROUTEUR:

Quand un routeur est sous tension, les choses suivantes ont lieu:

- 1 L'auto-test d'alimentation (POST) est exécuté pour connaître tous les composants matériels et vérifier leur fonctionnement
- 2 Le routeur charge le programme bootstrap de la ROM dans la RAM et l'exécute.
- 3 Le bootstrap décide de la version IOS à exécuter et démarre l'IOS à partir de Flash.
- 4 Le logiciel IOS charge la **startup-config** depuis la NVRAM et la copie dans le fichier **running-config** de la RAM.

REMARQUE:

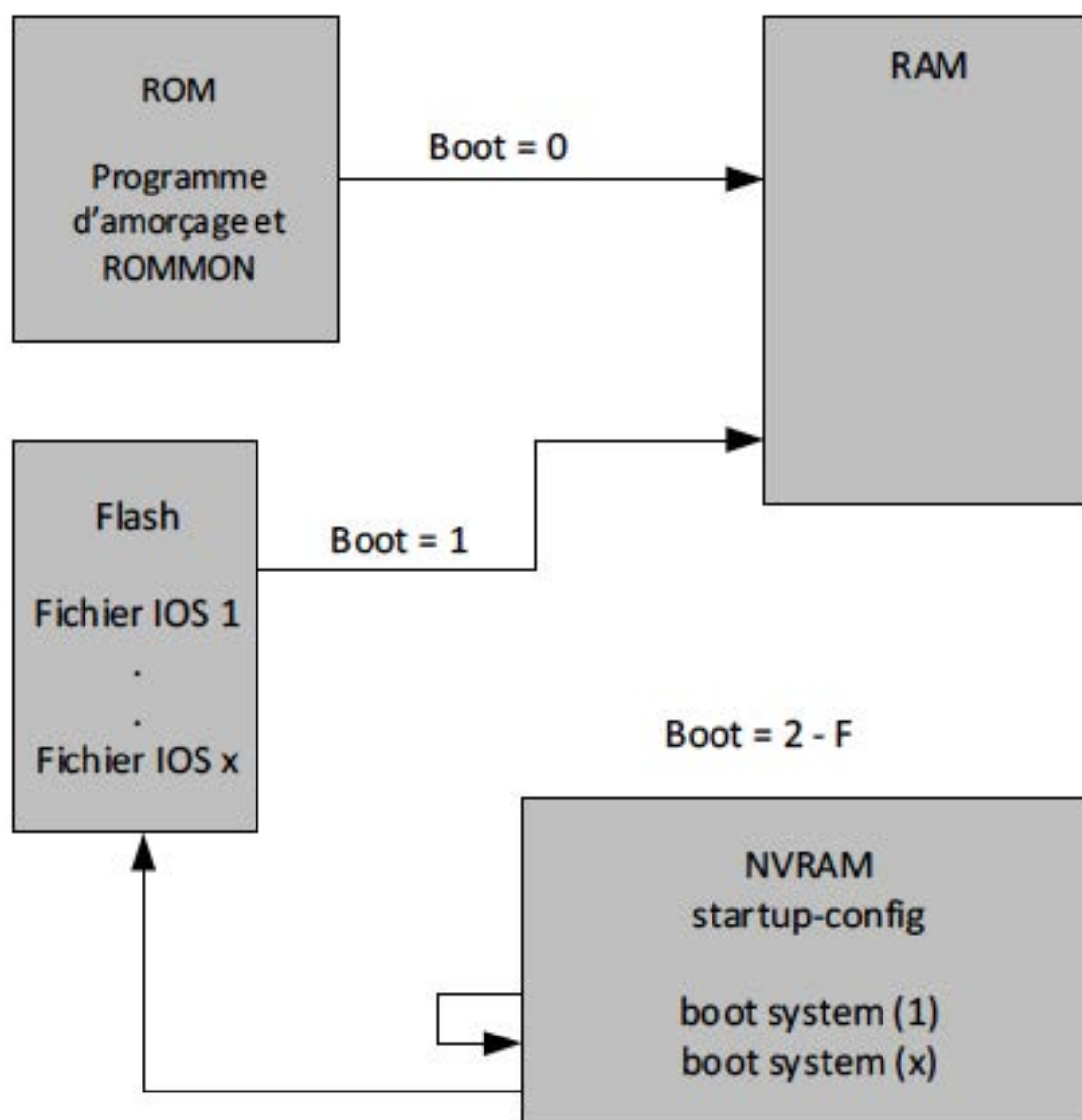
Si les étapes 1 ou 2 échouent, Cisco TAC devra être appelé pour réparer le routeur.

CHOIX DE L'IOS À CHARGER:

Le registre de configuration (**config-register**) contrôle un grand nombre d'éléments, y compris l'ordre d'amorçage et la vitesse de transmission initiale du port console. Par défaut, le registre de configuration est 0x2102, définit le port de la console à 9600 bps et charge une image IOS. Le dernier chiffre du registre de configuration détermine l'ordre d'amorçage.

- Si le dernier chiffre est 0, charge la ROMMON
- Si le dernier chiffre est 1, charge le premier fichier IOS trouvé dans le flash
- Si le dernier chiffre est compris entre 2 et F, essaye chaque commande du système d'amorçage dans le fichier de configuration de démarrage dans l'ordre. Si cela échoue, charge le premier fichier ISO trouvé dans flash

CHOIX POUR DÉMARRAGE BASÉ SUR LE CONFIG-REGISTER:



NOMS, FONCTIONS ET EMPLACEMENTS DES FICHIERS DE CONFIGURATION

NOM DE FICHIER DE CONFIGURATION	FONCTION	STOCKAGE EMPLACEMENT
startup-config	La configuration initiale chargée par le routeur lors d'une redémarrage	NVRAM
running-config	Stocke les commandes de configuration et les mises à jour actuelles lorsque de nouvelles commandes sont entrées dans le routeur	RAM

COMMANDE SHOW VERSION:

La commande **show version** affiche beaucoup de choses importantes dans le routeur:

- Version IOS
- Temps de fonctionnement de l'appareil (uptime)
- Raison de la dernière recharge
- Temps de rechargement d'IOS
- Source IOS actuelle (flash, TFTP)
- Quantité de RAM
- Nombre et types d'interfaces
- Quantité de mémoire flash
- Paramètres actuels et futurs du **config-register**

RouterA# **show version**

Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), **Version 15.2(4)M1**,
RELEASE

SOFTWARE (fc1)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Thu 26-Jul-12 20:54 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

R2 uptime is 44 minutes

System returned to ROM by reload at 19:44:01 UTC Tue Feb 12 2013

System restarted at 19:45:53 UTC Tue Feb 12 2013

System image file is "flash:c2900-universalk9-mz.SPA.152-4.M1.bin"

Last reload type: Normal Reload

Last reload reason: Reload Command

<snip>

Cisco CISCO2901/K9 (revision 1.0) with **483328K/40960K bytes of memory.**

Processor board ID FTX1628837T

2 Gigabit Ethernet interfaces

4 Serial(sync/async) interfaces

1 terminal line

DRAM configuration is 64 bits wide with parity enabled.

255K bytes of non-volatile configuration memory.

3425968K bytes of USB Flash usbflash1 (Read/Write)

250880K bytes of ATA System CompactFlash 0 (Read/Write)

<snip>

Configuration register is 0x2102

COMMANDES DU SYSTÈME DE DÉMARRAGE (BOOT SYSTEM):

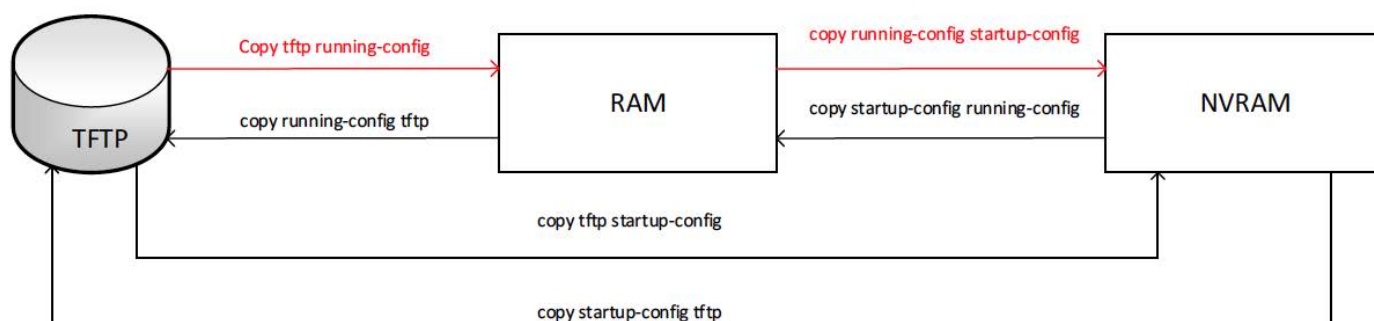
COMMANDE BOOT SYSTEM	RÉSULTAT
boot system flash	La configuration initiale chargée par le routeur lors d'un redémarrage
boot system flash NOM	Stocke les commandes de configuration et les mises à jour actuelles lorsque de nouvelles commandes sont entrées dans le routeur
boot system tftp 10.1.1.2 NOM	Le routeur charge l'IOS spécifié depuis le serveur tftp 10.1.1.2

RÉCUPÉRATION DE MOT DE PASSE DE BASE:

Bien que le processus de récupération de mot de passe varie selon les équipements Cisco, le processus de base reste le même:

- 1 Éteindre le routeur
- 2 Retirez la carte Compact Flash du routeur
- 3 Allumer le routeur
- 4 Attendez que rommon 1> s'affiche
- 5 Insérez soigneusement la carte Compact Flash dans le routeur
- 6 Réglez le registre de configuration sur **0x2142** avec la commande **confreg 0x2142**
- 7 Lancez la commande **reset** à l'invite rommon pour réinitialiser le routeur
- 8 Attendez que IOS passe en mode de configuration. Entrez no à l'invite.
- 9 Connectez-vous au routeur sans mot de passe et entrez enable pour obtenir un accès administrateur
- 10 Chargez la configuration de démarrage dans la RAM avec la commande **copy startup-configuration running-configuration**
- 11 Réinitialiser le mot de passe
- 12 Enregistrez la nouvelle configuration en lançant la commande **copy running-configuration startup-configuration**

COMMANDE COPY:



COPIE DE FICHIERS VIA SCP (SECURE COPY):

SCP permet de copier des fichiers entre des hôtes utilisant SSH comme protocole sous-jacent.

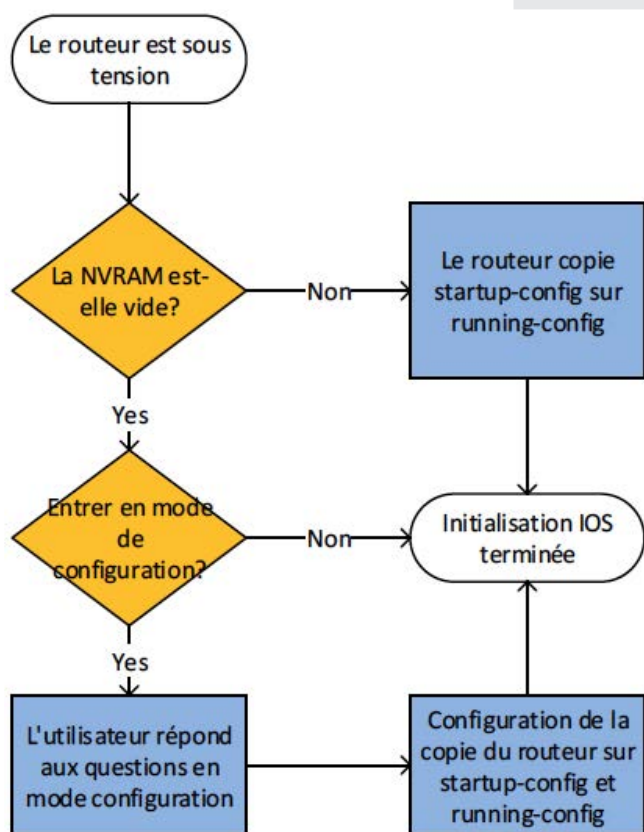
L'activation de SCP sur un routeur Cisco nécessite les deux étapes suivantes.

- 1 Autoriser l'accès direct au compte SSH pour activer le mode avec la commande **username cyril privilege 15 password TOTO**
- 2 Activez le serveur SCP avec la commande **ip scp server enable**

AVEC LES VERSIONS RECENTES D'IOS, LA COMMANDE ARCHIVE EST UNE COMMANDE DE COPIE AMÉLIORÉE:

La commande **archive** peut créer des configurations de sauvegarde en fonction de l'heure ou de la mise à jour de la configuration

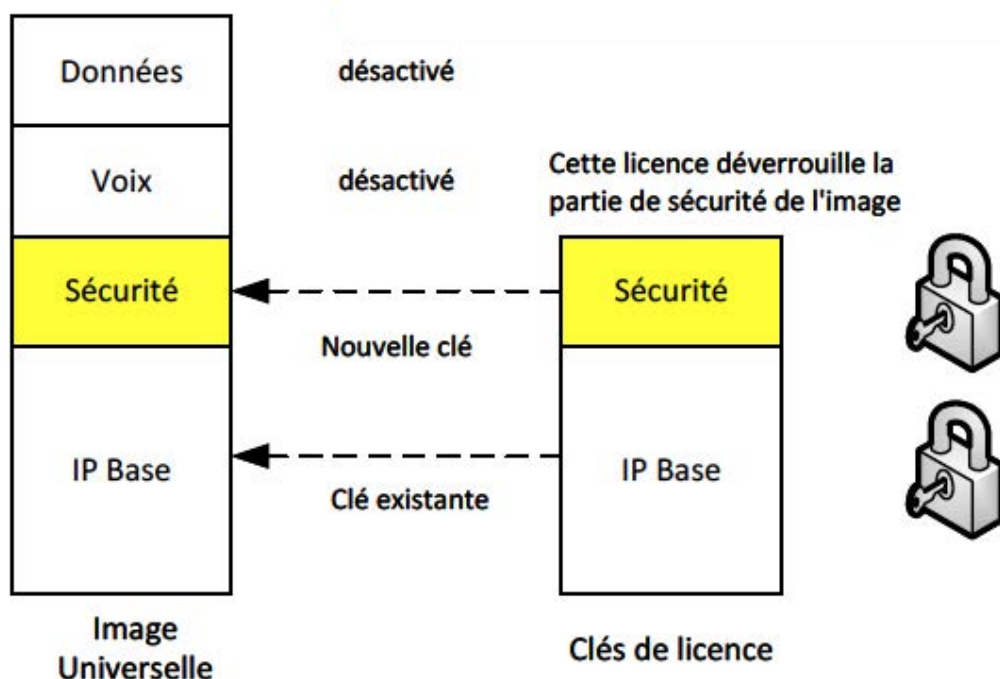
La commande **configure replace** permet de restaurer une configuration archivée sans forcer un reload.



MODÈLE ORIGINAL DE LICENSING CISCO:

Sous le modèle original de licensing Cisco, il y avait différentes versions de l'IOS basé sur l'ensemble des fonctionnalités. La version de base est la **IP Base** avec en option les fonctions **voix, données et sécurité**. Chacune de ces combinaisons est un fichier IOS distinct. Sous le nouveau modèle de licensing, un seul fichier IOS est placé dans le routeur. C'est ce qu'on appelle l'**image universelle** et les fonctions de l'image universelle sont déverrouillés avec des fichiers de licence fournis par Cisco.

COMMENT LES CLÉS DE LICENCE DÉVERROUILLEMENT LES FONCTIONNALITÉS D'IOS



LICENSE	CARACTÉRISTIQUES
IP Base	Fonctions d'IOS d'entrée de gamme
Application experience	Performances de routage (PfR), NBAR2, WAAS
Unified Communications	VoIP, téléphonie sur IP
Security	IOS Firewall, IPSec, VPN, DMVPN

TABLEAU DE QUELQUES LICENCES DISPONIBLES

Utilisez la commande show license udi pour afficher les licences installées sur le routeur.

RouteurA# **show license udi**

Device#	PID	SN	UDI

*0	CISCO2901/K9	FTX165113H0	CISCO2901/K9:FTX165113H0

Utilisez show license pour voir les licences IOS activées dans le routeur:

R1# **show license**

Index 1 Feature: ipbasek9

Period left: Life time

License Type: Permanent

License State: Active, In Use

License Count: Non-Counted

License Priority: Medium

Index 2 Feature: securityk9

Period left: Not Activated

Period Used: 0 minute 0 second

License Type: EvalRightToUse

License State: Not in Use, EULA not accepted

License Count: Non-CountedLicense Priority: None

Index 3 Feature: uck9

Period left: Not Activated

Period Used: 0 minute 0 second

License Type: EvalRightToUse

License State: Not in Use, EULA not accepted

License Count: Non-Counted

License Priority: None

Index 4 Feature: datak9

Period left: Not Activated

Period Used: 0 minute 0 second

License Type: Permanent

License State: Active, Not in Use

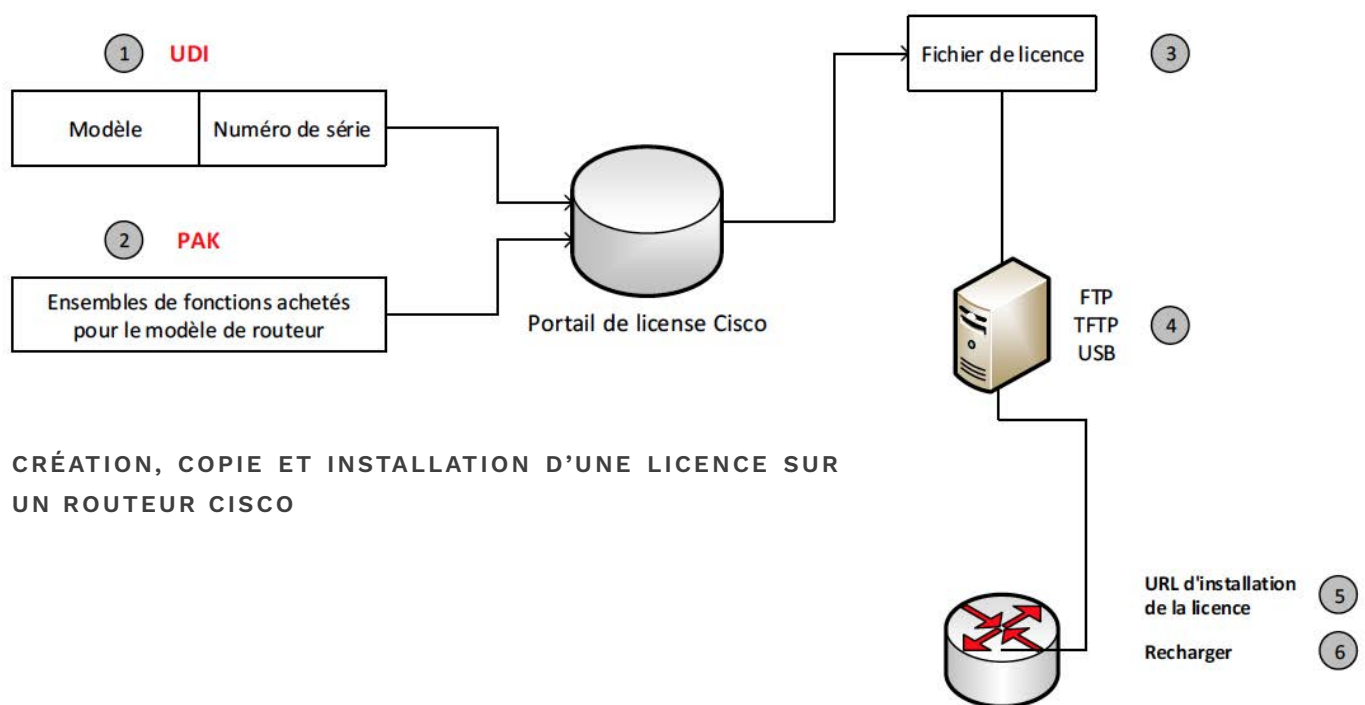
License Count: Non-Counted

License Priority: Medium

! Lines omitted for brevity; 8 more feature licenses available

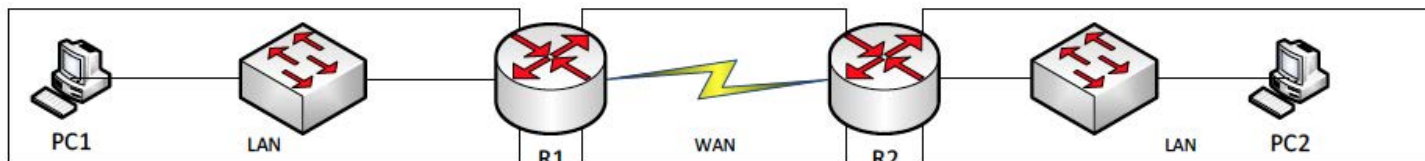
ÉTAPES POUR METTRE À JOUR OU AJOUTER DES LICENCES CISCO:

- 1 Sur le portail de licences Cisco, entrez l'UDI du routeur en utilisant les informations de la commande **show license**.
- 2 Tapez la PAK (Product Access Key) que vous avez reçue de Cisco ou de votre revendeur
- 3 Copiez le fichier de licence lorsque le portail l'affiche
- 4 Téléverser le fichier de licence vers un serveur FTP/TFTP ou clé USB
- 5 Installez la licence avec la commande install URL (url pointe vers le fichier de licence)
- 6 Redémarrez le routeur pour mettre à jour les fonctionnalités concédées



THÉORIE DU ROUTAGE IPV4

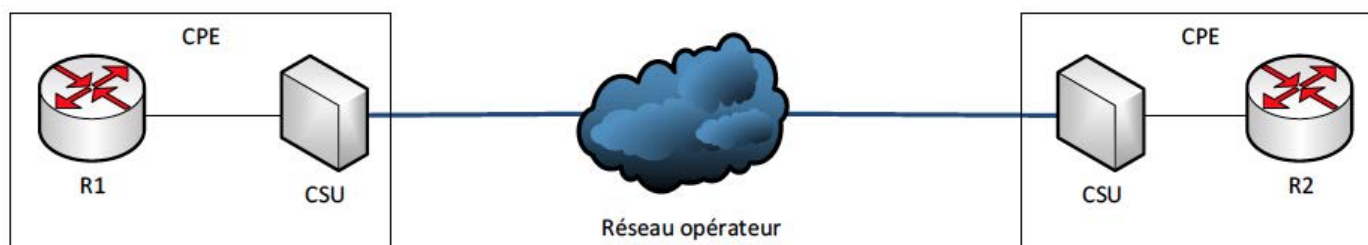




DESIGN LOGIQUE :

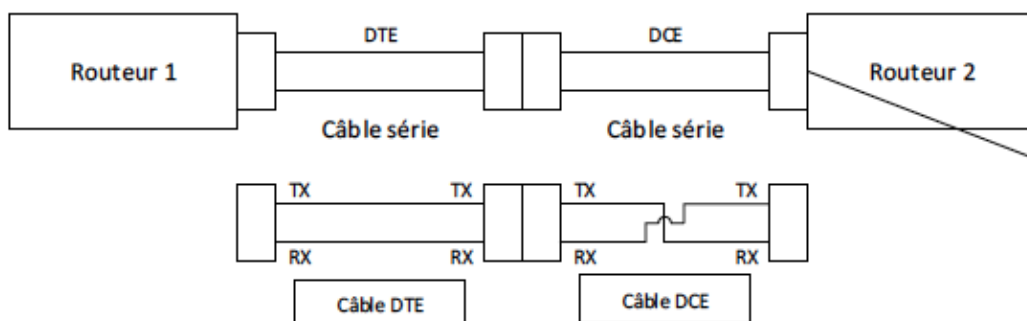
PC1 et PC2 sont géographiquement séparés. Chaque PC est connecté à un LAN local (switch) puis à un routeur.

Entre les routeurs se trouvent un lien géré par le fournisseurs d'accès (opérateur ou ISP en anglais). Ce lien WAN est appelé **ligne louée** et peut prendre différentes formes comme le E1, E3, STM1...



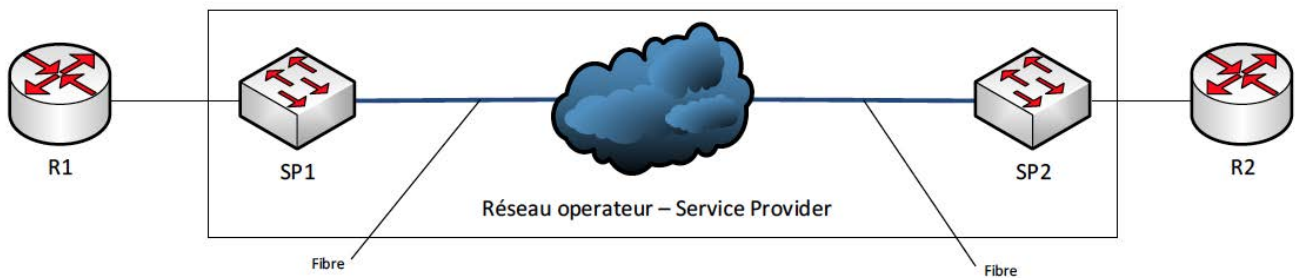
CONFIGURATION PHYSIQUE :

Entre les routeurs se trouvent un équipement **CSU/DSU** qui convertit 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 différent d'Ethernet, comme par exemple **HDLC** (High-Level Data Link Control).



La commande
"clock rate" est
configurée sur ce
port serie

DTE – Data Terminal Equipment
DCE – Data Communications Equipment

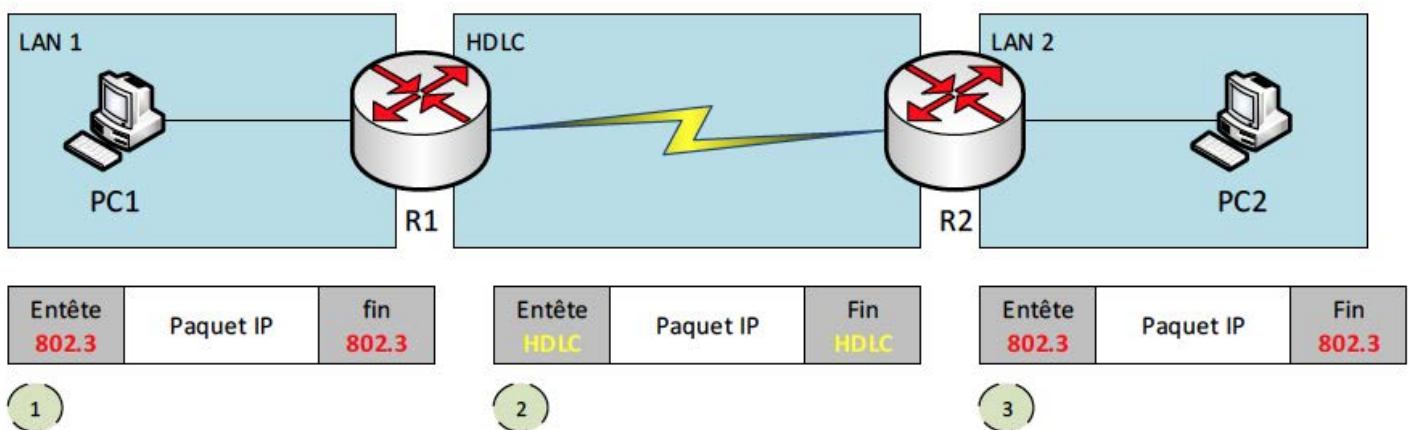


Ethernet comme un WAN : Au lieu d'utiliser une ligne louée ou un circuit, le protocole **Ethernet** est utilisé entre R1 et R2. Certains réseaux opérateurs émulent le protocole Ethernet en utilisant des protocoles comme **MPLS** (Multi-protocol Layer Switching) et donc remplacent les anciens protocoles 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), la trame Cisco HDLC ne précise que le champ adresse source

Flag	Address	Control	Type	Données	FCS
------	---------	---------	------	---------	-----

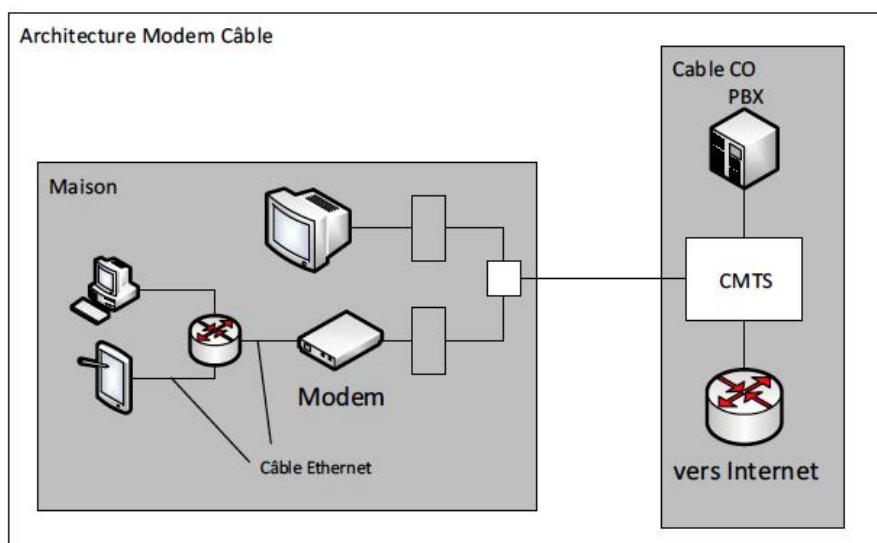
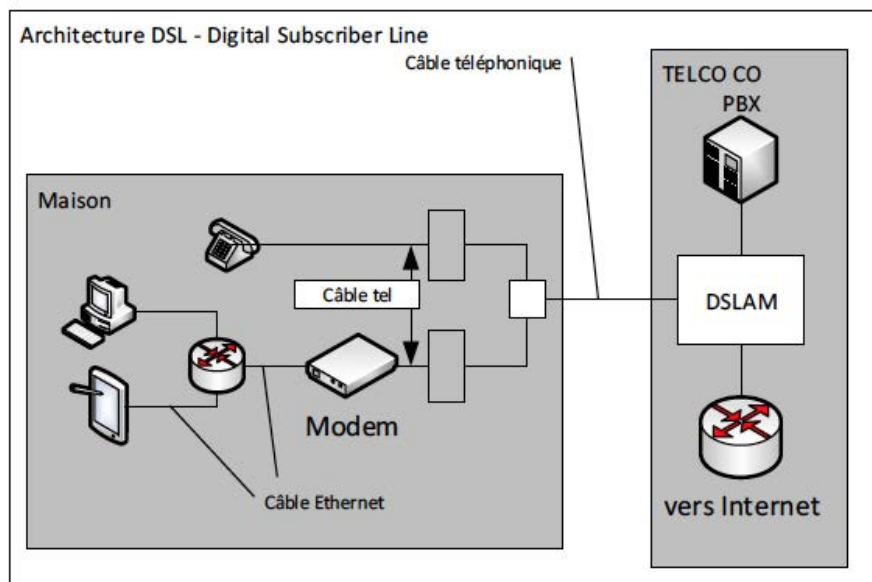
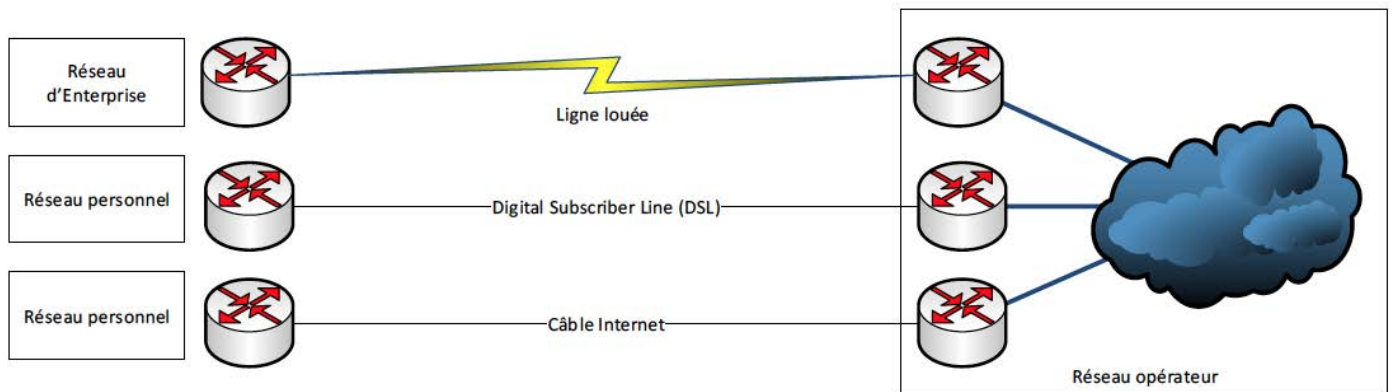


Encapsulation et décapsulation d'un paquet IP au travers d'un lien WAN (HDLC):

ÉTAPE 1 : PC 1 génère une donnée, la place dans un paquet IP puis l'insère dans une trame Ethernet 802.3 et l'envoi au routeur.

ÉTAPE 2 : R1 reçoit la trame Ethernet, y extrait le paquet IP, l'insère dans une trame HDLC et l'envoi au routeur R2.

ÉTAPE 3 : R2 reçoit la trame HDLC, y extrait le paquet IP, l'insère dans une trame Ethernet 802.3 et l'envoi au PC2



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)

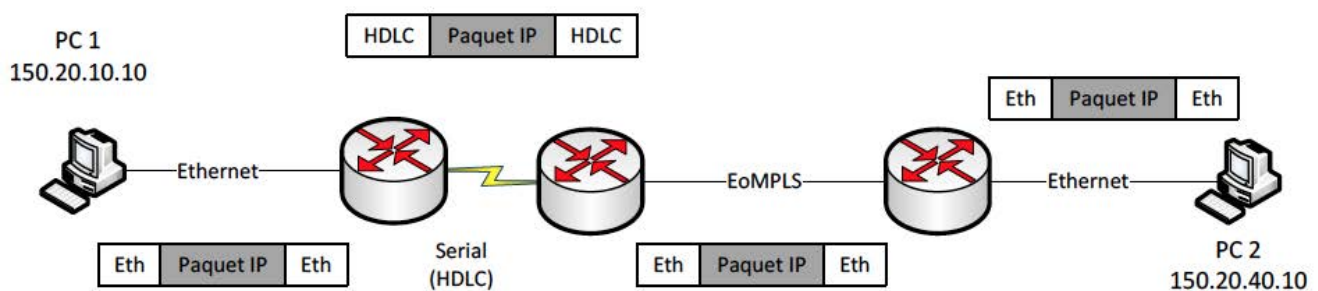
Classe E: 240 à 255 (utilisation expérimentale)

Les réseaux 0 Et 127 sont réservés pour des utilisations spécifiques.

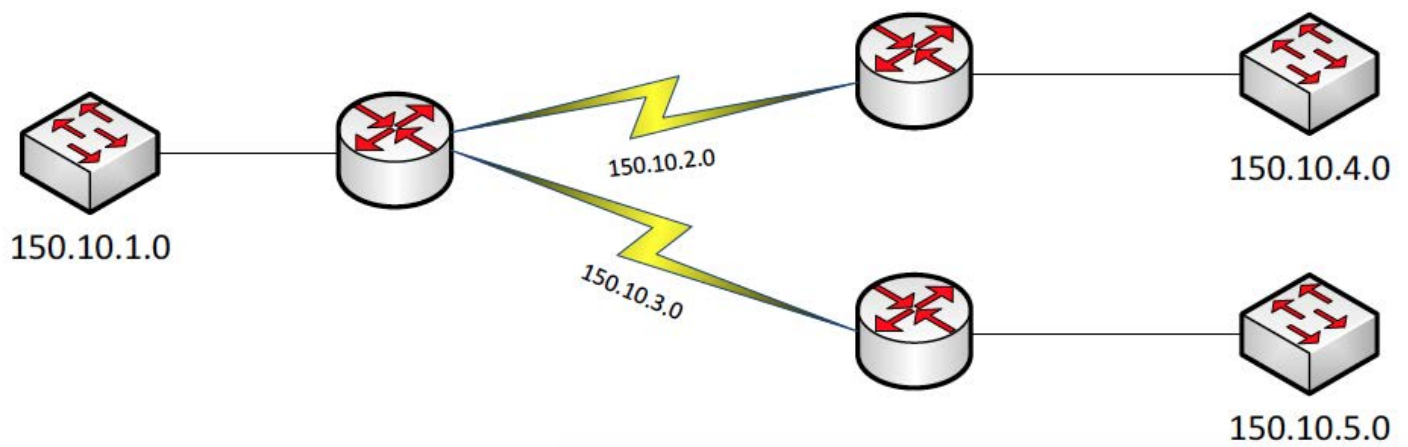
0	Réservée		Hôtes (Host) par réseau
1-126	Classe A	Unicast	16,777,214
127	Réservée		
128-191	Classe B	Unicast	65,534
192-223	Classe C	Unicast	254
224-239	Classe D	Multicast	
240-255	Réservée	Expérimentale	

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



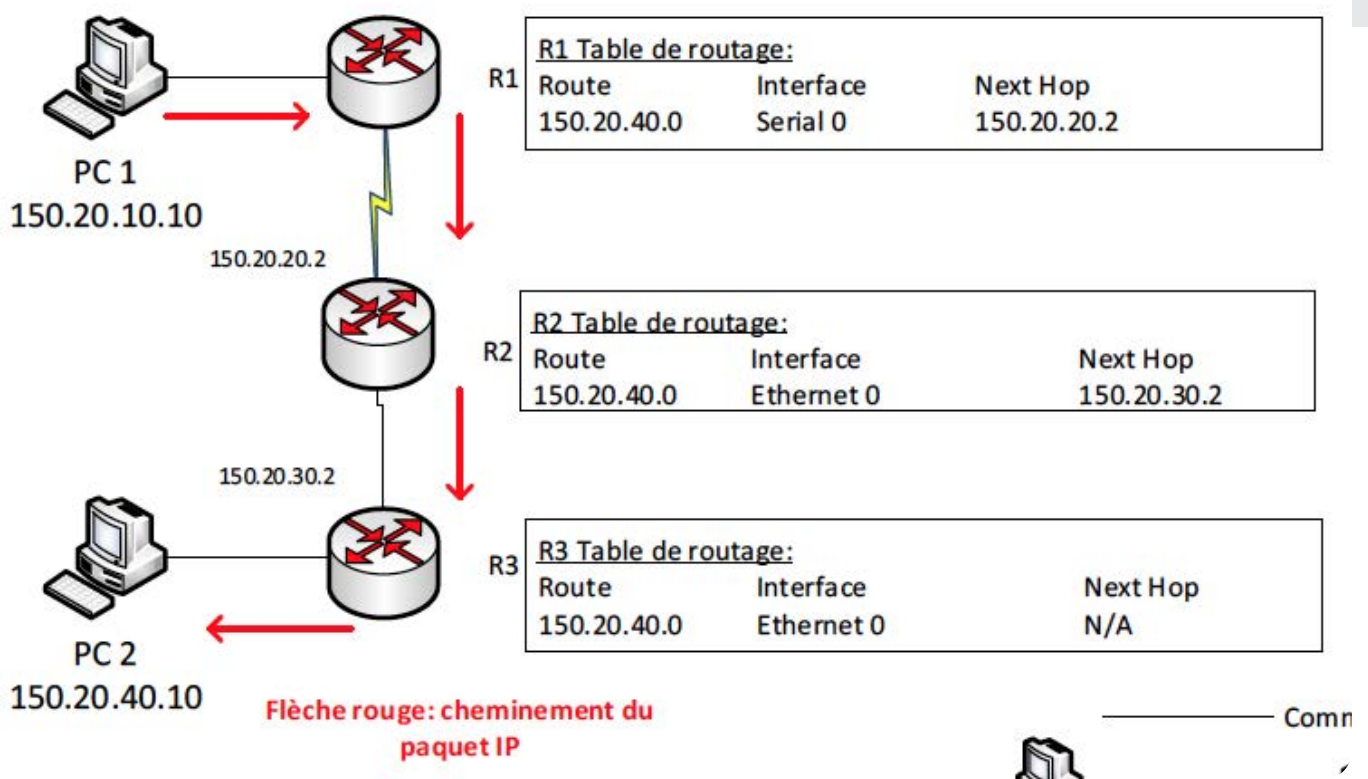
Le sous-réseau IP est un processus pour s'assurer que les adresses IP sont bien utilisées.

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 Le routeur utilise le champ FCS de la trame reçue pour vérifier les éventuelles erreurs de transmission et supprime la trame si c'est le cas.
- 2 Le routeur **extraie** le paquet IP et **supprime** l'entête Ethernet.
- 3 Le routeur **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 Le routeur place le paquet IP dans une **nouvelle trame** et transmet cette trame sur l'interface de sortie.

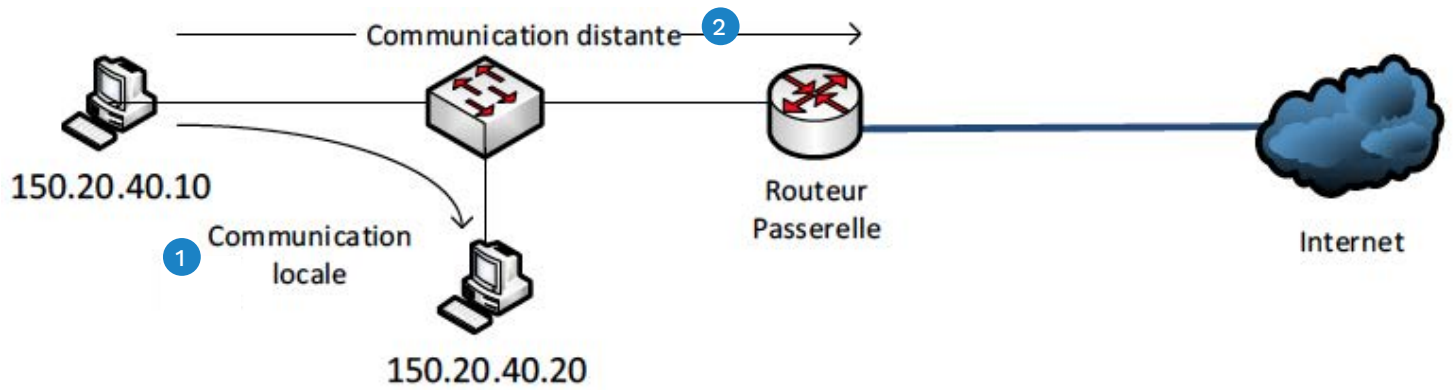


CHAQUE PROTOCOLE DE ROUTAGE DOIT AVOIR LES FONCTIONS SUIVANTES

- **Apprentissage dynamique** des routes et alimentation de sa table de routage.
- Si plusieurs routes sont disponibles pour un même réseau alors ajout dans la table de routage de **la meilleure route**.
- **Avertit** 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, **ajoute** cette nouvelle route dans la table de routage.
- Agit rapidement dans l'ajout et la suppression de routes dans la table de routage.
- **Prévient des boucles de routage**

RÈGLE DE ROUTAGE IPV4:

- 1 Si le destinataire et mon PC sont dans le **même sous-réseau** alors je lui envoie le paquet **directement**
- 2 Sinon, j'envoie le paquet à mon routeur (passerelle) pour traitement



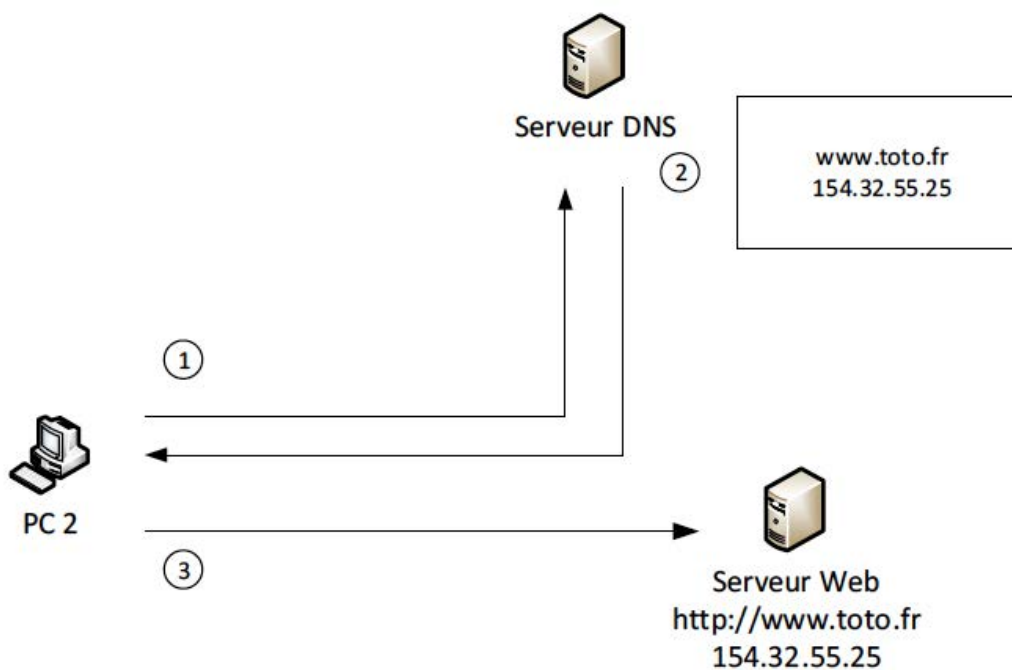
DOMAIN NAME SYSTEM (DNS) : Résout les noms en adresse IP.

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 (www.toto.fr) et les adresses IP associées (124.23.165.43).

FONCTIONNEMENT:

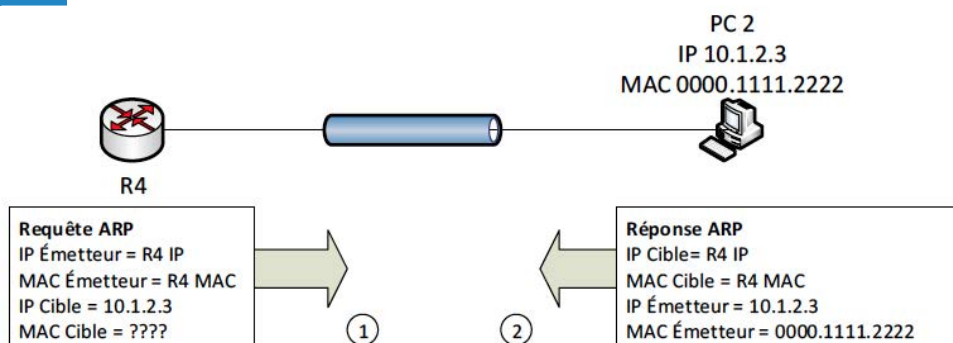
- 1 L'hôte envoie une requête au serveur DNS concernant un **nom de domaine** (par exemple : toto.fr).
- 2 Le serveur DNS répond avec **l'adresse IP correspondante** au serveur toto.fr.
- 3 L'hôte initie une communication avec le serveur toto.fr car il connaît désormais son adresse IP.



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 connaît que l'adresse IP et pas l'adresse MAC.



POINTS CLÉS

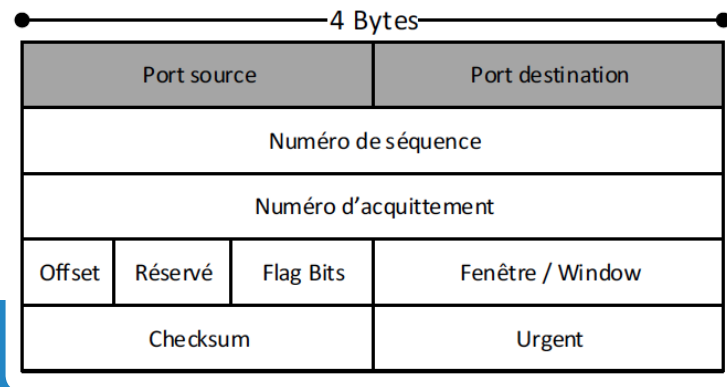
TCP est un **protocole de la couche 4** et possède les fonctionnalités suivantes :

- **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 séquençement 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

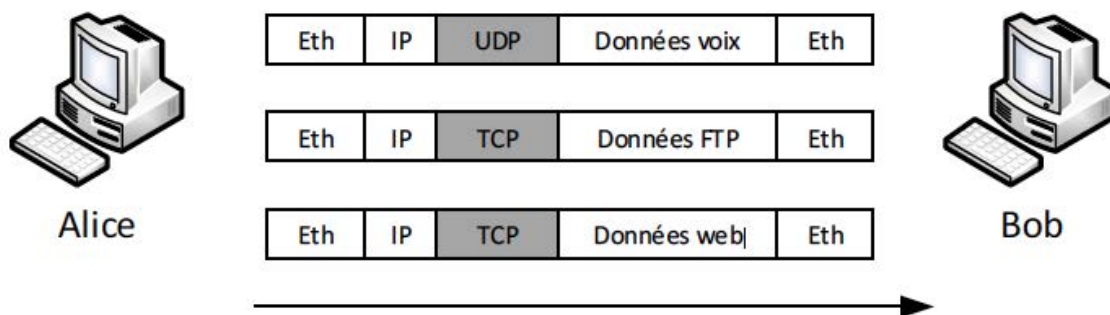
Réservé : Non utilisé

Flag Bits : bits utilisés pour le contrôle

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

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

Urgent : Indique l'urgence du segment



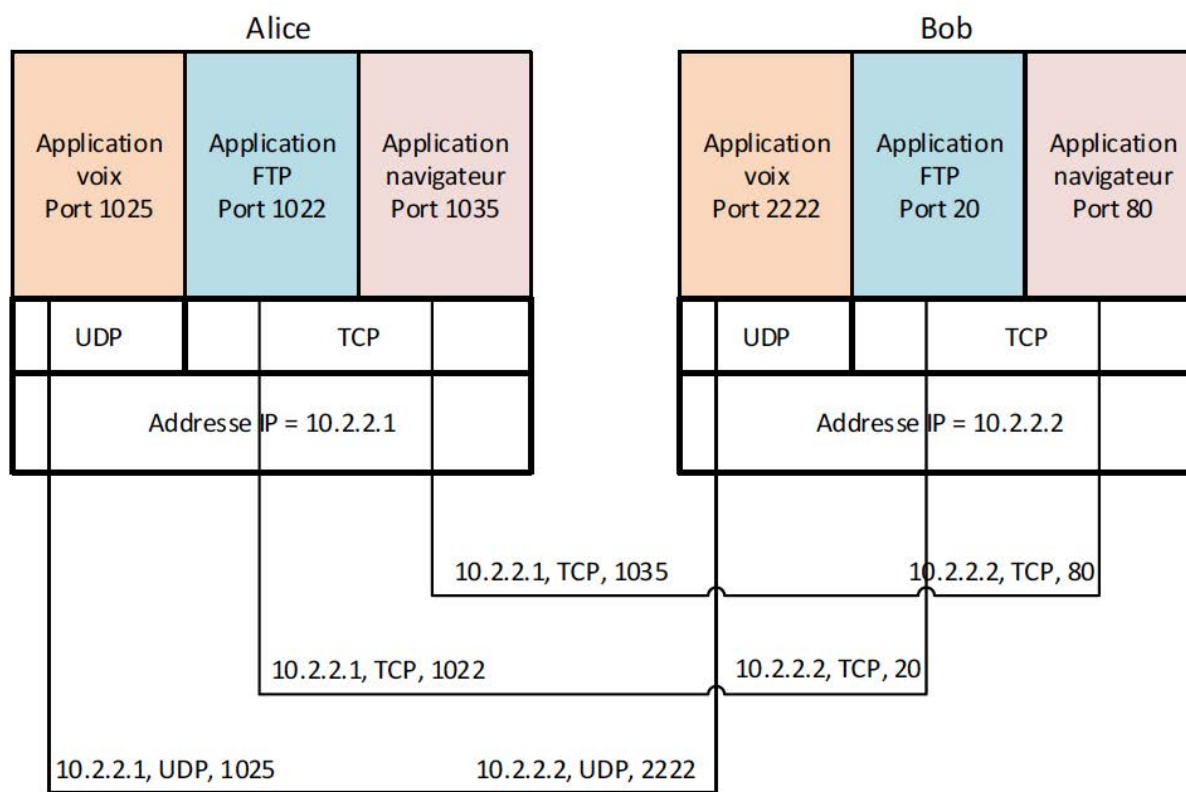
MULTIPLEXAGE TCP

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 envoie 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.

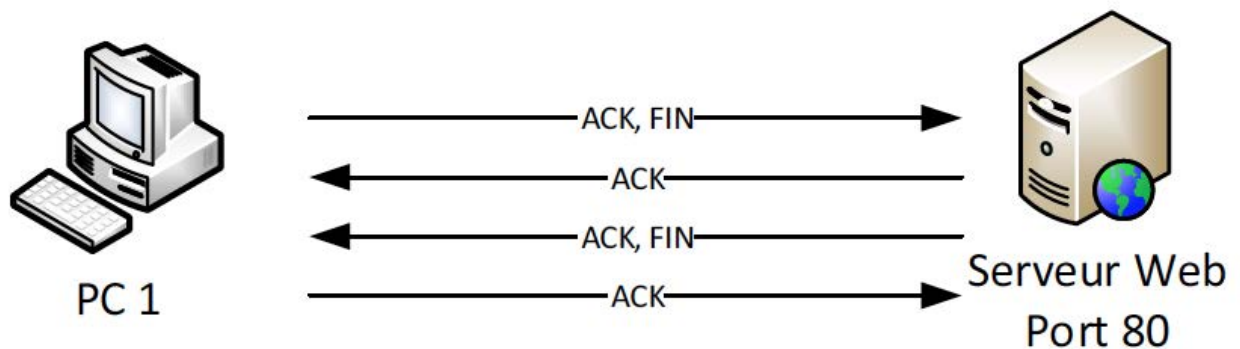
Gigue / Jitter: Variation du délai.

Perte / Loss: Pourcentage de paquets supprimés par le réseau avant d'atteindre la destination.

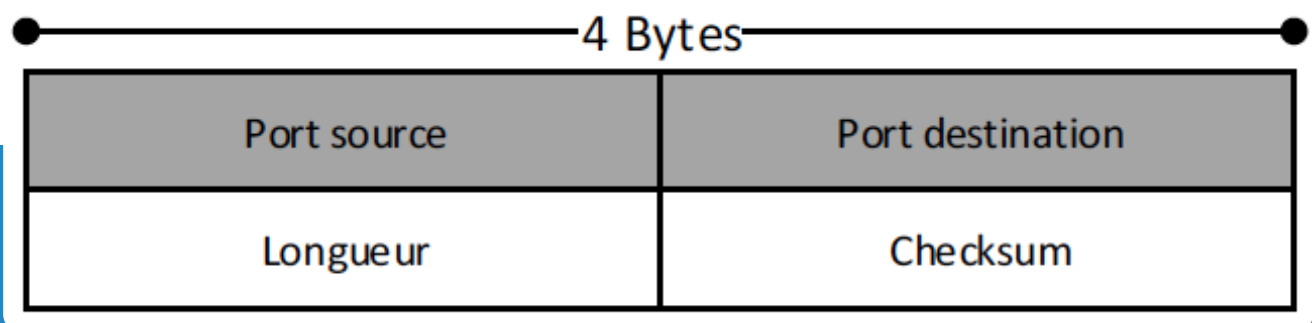
ETABLISSEMENT DE CONNEXION TCP (3-WAY HANDSHAKE)



FERMETURE DE CONNEXION TCP (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.

PERSPECTIVES SUR LES SOUS-RÉSEAU IPv4

Analyse du besoin

Subnets
Hôtes par Subnet
1 taille de Subnet

Design Subnets

Choix du network
Choix du masque
Liste des subnets

Implémentation du plan

Subnets -> Localisation
IP statique
Plages DHCP

Planification des subnets, design et implémentation

RÈGLES PRIMORDIALES !

- Les adresses dans le même subnet ne doivent pas être séparées par un routeur.
- Les adresses dans des subnets différents 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

Définir un subnet

Network (N)

Subnet (S)

Hôtes (H)

32 Bits Total (N + S + H = 32)

Hôtes = $2^H - 2$

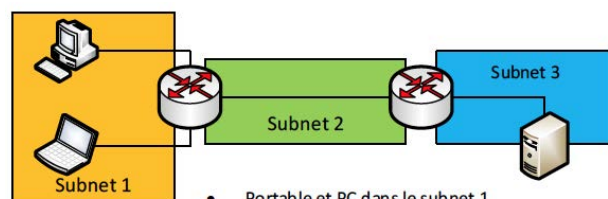
Hôtes classe A: $2^{24} - 2 = 16,777,214$

Hôtes classe B: $2^{16} - 2 = 65,534$

Hôtes classe C: $2^8 - 2 = 254$

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



- Portable et PC dans le subnet 1
- Routeurs dans les subnets 1, 2 et 3
- Serveur in subnet 3

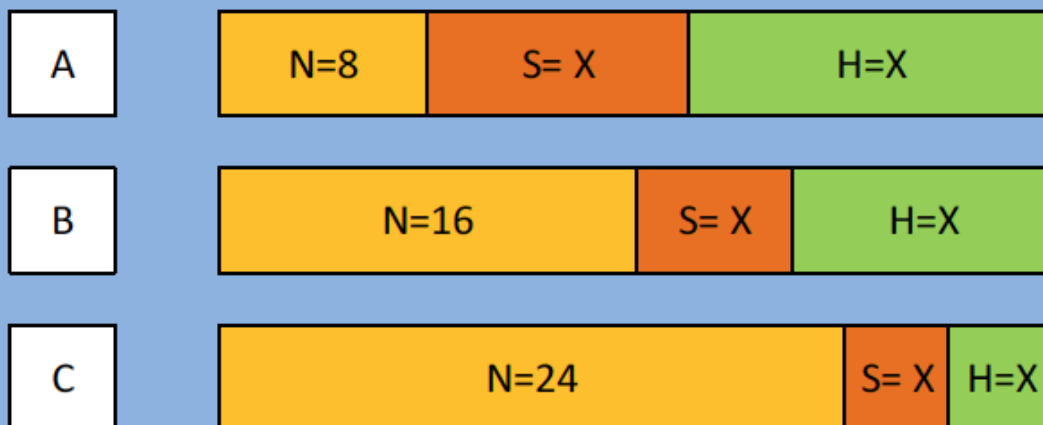
Network IP classful IP avant le découpage en subnet

(N = Network Bits, H = Host Bits)

A	N=8	H=24
B	N=16	H=16
C	N=24	H=8

Concept de l'emprunt de bits (N = Network, S= Subnet H = Host)

N + S + H doit être égal à 32 bits



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 il 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 il 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 découper en deux subnets contenant au moins 500 adresses IP pour les hôtes.

QUESTION

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.

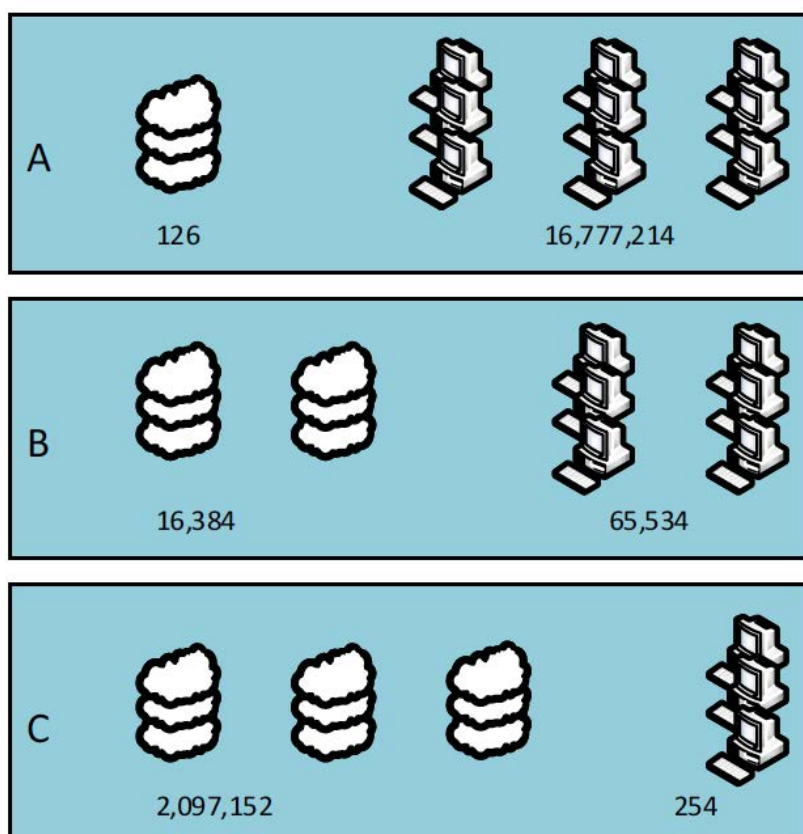
Le masque ne sera plus de /22 mais de /23 car nous empruntons 1 bit en plus pour la partie subnet.

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 195.16.12.255 et la plage des hôtes est comprise de 195.16.12.1 à 195.16.12.254.

Subnet 2 : On prend le subnet ID suivant qui est 195.16.13.0/23. L'adresse de broadcast pour ce subnet est 195.16.13.255 et la plage des hôtes est comprise de 195.16.13.1 à 195.16.13.254

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



NOMBRE DE NETWORKS ET DE HÔTES PAR CLASSE

FACTEUR CLÉS	CLASSE A	CLASS B	CLASS 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 - 233.255.255.0
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

**NOTE
IMPORTANTE:**

Les adresses dans le même Network ont toutes la même valeur pour le **Network ID** et des valeurs différentes pour le **Host ID**

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)
--------------	----------

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

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 Premier Host IP	175.17	+1 0.1
⑤	Appliquer Host = 255	175.17	255.255
⑥	Soustraire 1 Dernier Host IP	175.17	-1 255.254

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

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

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)

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 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

ADRESSAGE CLASSFUL :

l'adresse IPv4 est composée 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?

Solution:

ÉTAPE 1 : convertir le masque en format préfix (/P)

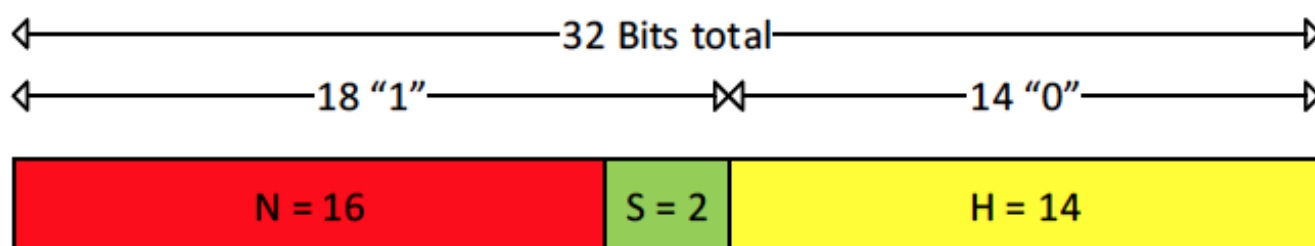
ÉTAPE 2 : déterminer le nombre de bits Network base sur la classe par défaut

ÉTAPE 3 : calculer $s' = P - N$

ÉTAPE 4 : calculer $H = 32 - P$

ÉTAPE 5 : calculer hosts par subnet: $2^H - 2$

ÉTAPE 6 : calculer le nombre de subnets: 2^s



SUBNET 185.240.32.0, MASQUE 255.255.192.0, N' = 16, S' = 2, H = 14

Exemple : 185.240.32.0 avec un masque 255.255.192.0

ÉTAPE 1 : le masque 255.255.192.0 est composé "1" en 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 calculé 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

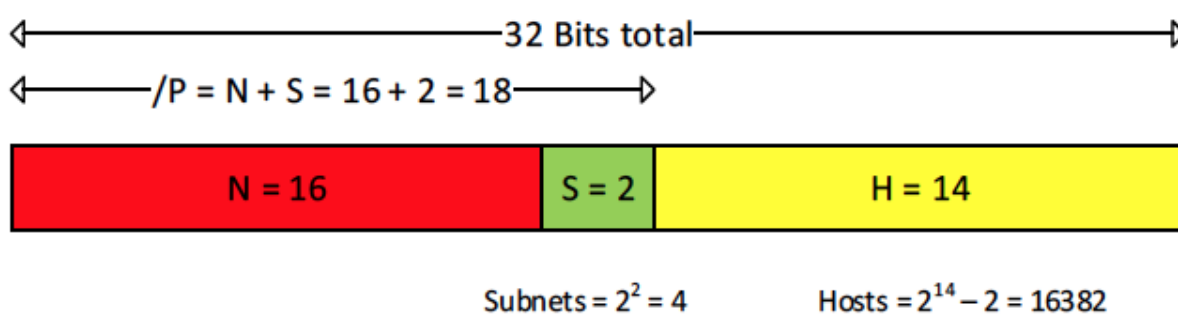
ÉTAPE 5 : on calcule alors le nombre de Hosts par Subnet: $2^{14} - 2 = 16384 - 2 = 16382$. Il y a 16382 adresses IP dans chaque Subnet !

ÉTAPE 6 : on calcule aussi le nombre de Subnet: $2^2 = 4$. Il y a 4 Subnets

ANALYSE DES MASQUES DE SOUS-RÉSEAUX

DÉFINIR UN SOUS-RÉSEAU (SUBNET)

- Le Subnet contient un ensemble de nombres consécutifs
- Un Subnet détient 2^H 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 IPN



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 équivalent binaire

ÉTAPE 3 : copier les bits de prefix de l'adresse IP

ÉTAPE 4 : écrire des pour la partie Hosts

ÉTAPE 5 : convertir le restant de bits en décimal, par séquence 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 permet à un routeur d'envoyer un paquet à tous les Hosts du sous-réseau
Valeur numérique	Dernier 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 la décimale de l'adresse IP

Étape 2 : si l'octet du masque = 0, alors écrire que des "0"

Étape 3 : sinon, calculer le magic number ($256 - \text{masque}$). 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 ($256 - \text{masque}$). Prendre la valeur du Subnet ID, ajouter le magic number et soustraire 1 ($\text{ID} + \text{magic} - 1$)

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 opérateur

ÉTAPE 3 : si on utilise un CSU/DSU interne, brancher directement la ligne opérateur 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** (privilegié)
- Entrer et sortir d'un mode de configuration avec les commandes "**end**" "**exit**" et/ou la combinaison **Ctrl+Z**
- Configuration de la console, telnet et activer le mot de passe "**secret**"
- Configuration des clés de chiffrement SSH et de la base d'utilisateurs
- Configuration du **hostname** et **description** des interfaces
- Configuration des interfaces Ethernet, speed, duplex, shut/no shut
- Configurer une interface pour être administrativement désactivée (shutdown) et activée (no shutdown)
- Navigation dans différents contextes de mode de configuration à l'aide de commandes telles que **line console 0** et **interface**
- Aide en ligne, édition des commandes et rappel d'une commande tapée
- L'utilisation de nombreuses options de la commande debug pour créer des messages de log sur certains événements, afin que n'importe quel utilisateur peut surveiller ces messages à l'aide de la commande **monitor terminal**
- La signification et le contenu des fichiers **startup-config** (en NVRAM), **running-config** (en RAM) et des serveurs externes (comme TFTP), ainsi que la façon d'utiliser la commande copy pour copier les fichiers de configuration et les images IOS
- La CLI du routeur et du switch diffère sur deux aspects :
- La **configuration des adresses IP** peut être différente selon les cas
- Le routeur a un **port auxiliaire** (AUX) qui permet de connecter un modem ou une ligne téléphonique pour un accès à distance.

CODE DE STATUS D'UNE INTERFACE

NOM	DESCRIPTION
Line status	État de la couche physique
Protocol Status	État de la couche Liaison de données

COMBINAISON DES CODES DE STATUS D'UNE 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'interface 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 10.1.1.1/24
Serial0/0/0 is up, Line protocol is up
Internet address is 10.255.255.1/30
```

STATUS D'INTERFACE COMMANDES

COMMANDE	LIGNES DE SORTIE PAR INTERFACE	CONFIGURATION IP	ETAT DE L'INTERFACE AFFICHÉ
sh ip interface brief	1	Adresse	oui
show protocols [type/number]	1 or 2	Adresse et masque	oui
show interface [type/number]	multiple	Adresse et masque	oui

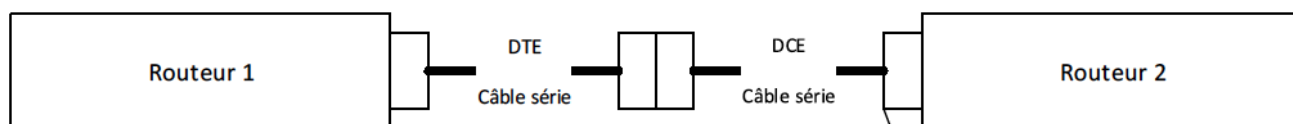


ROUTEUR CISCO 7206

Port de console - utilisé pour configurer initialement le routeur

Le port AUX était utilisé pour la connexion directe à un modem pour l'accès à distance

Port Gigabit Ethernet
(trafic réseau)



La commande clock rate se configure ici

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)#
```

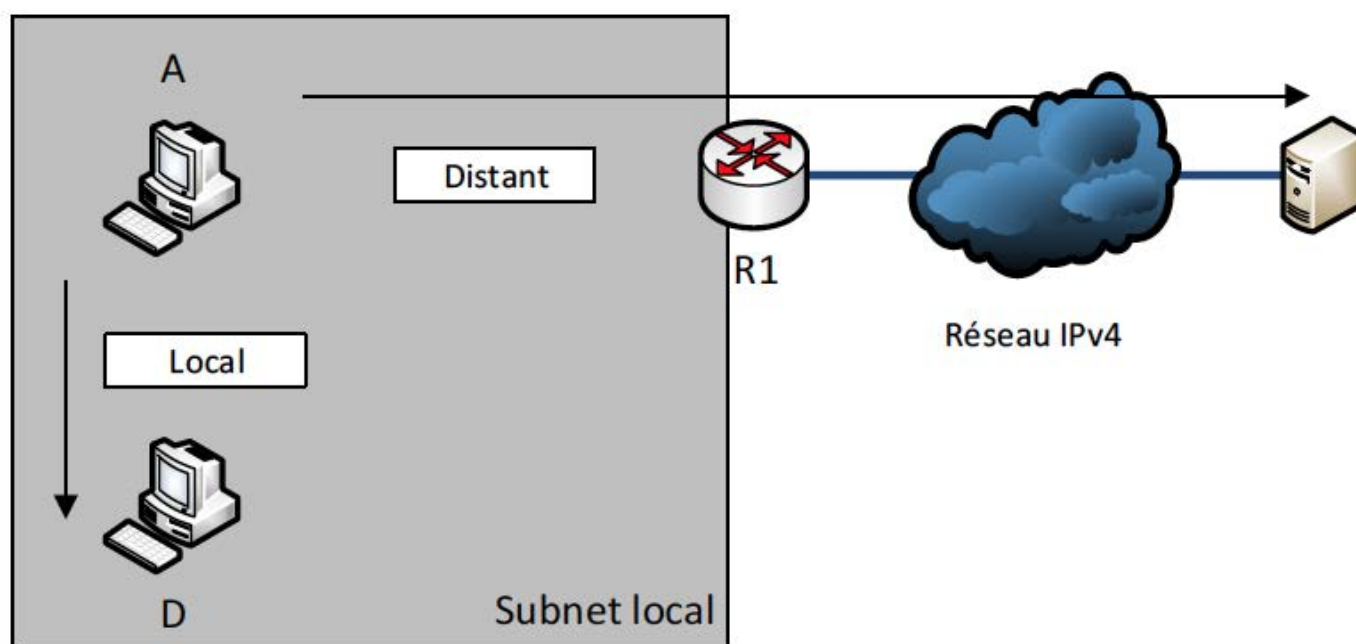
RÈGLE D'UN PC POUR LA TRANSMISSION D'UN PAQUET

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

- Le PC identifie l'adresse MAC **du destinataire**. Pour cela le PC utilise le cache ARP ou le protocole ARP pour récupérer l'adresse MAC.
- Ensuite il encapsule le paquet dans un nouvel entête niveau 2 avec l'adresse MAC de destination.

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

- Le PC identifie l'adresse MAC **de la passerelle**. Pour cela le PC utilise le cache ARP ou le protocole ARP pour récupérer l'adresse MAC.
- Ensuite il 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

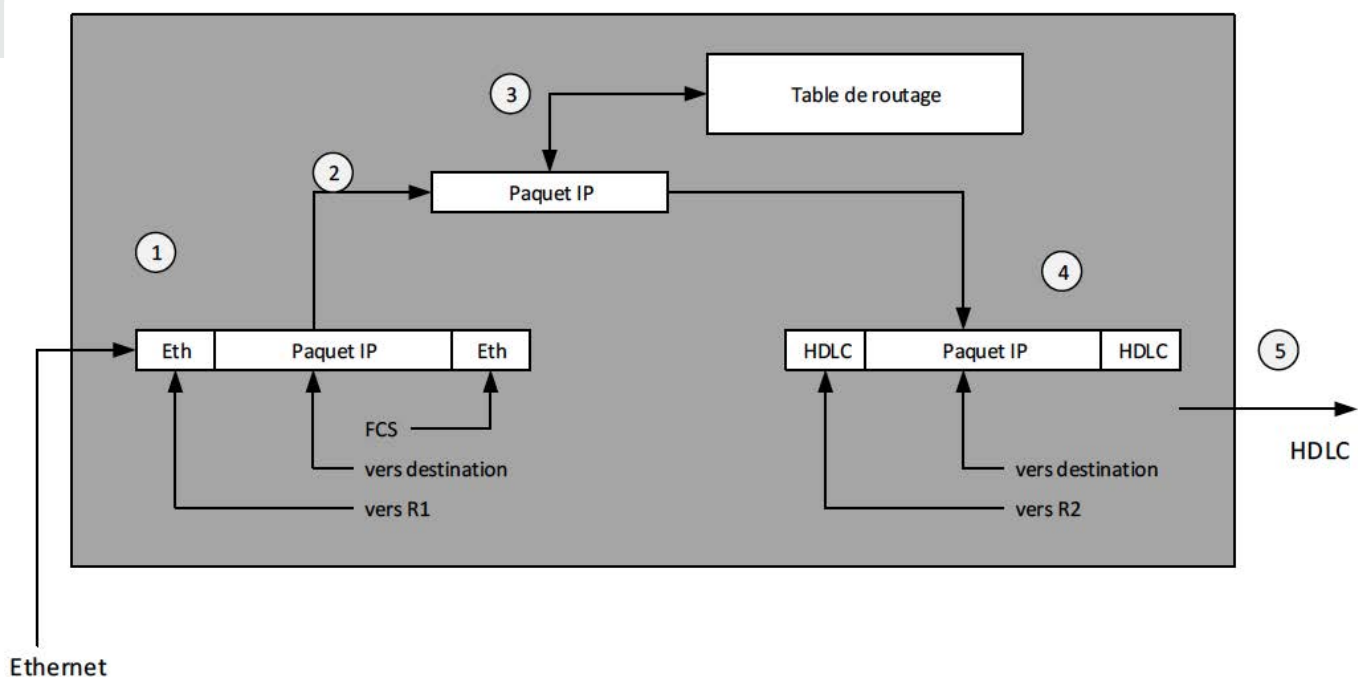
ÉTAPE 1 : pour chaque trame niveau 2 reçue, la traiter uniquement si :

- 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



AMÉLIORATION DU ROUTAGE	PROCESS SWITCHING	FAST SWITCHING	CEF
Réduction de l'entête niveau 2 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)

Comparaison entre le process switching, fast switching et Cisco Express Forwarding (CEF)

TYPE DE ROUTE

- **Connected** : la route est automatiquement ajoutée car l'adresse IP d'une interface du routeur appartient déjà 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 VLANS

Il existe 3 possibilités pour avoir du routage inter-VLANs :

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

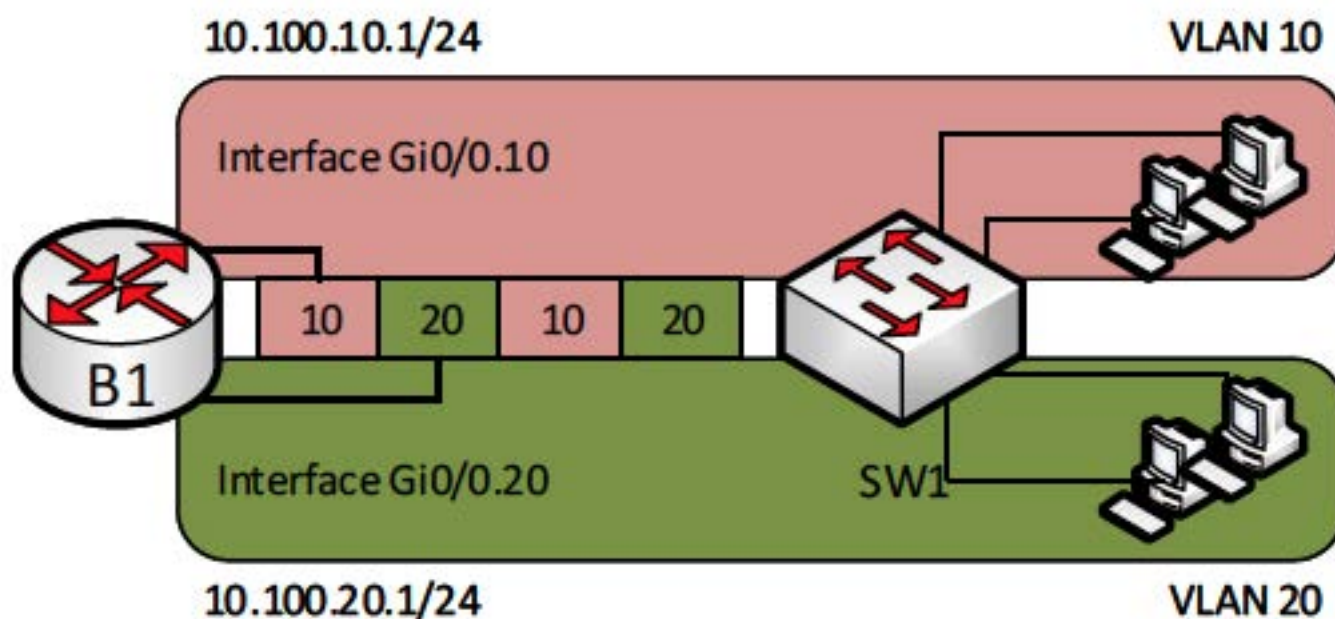
CONFIGURATION D'UNE SOUS-INTERFACE

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

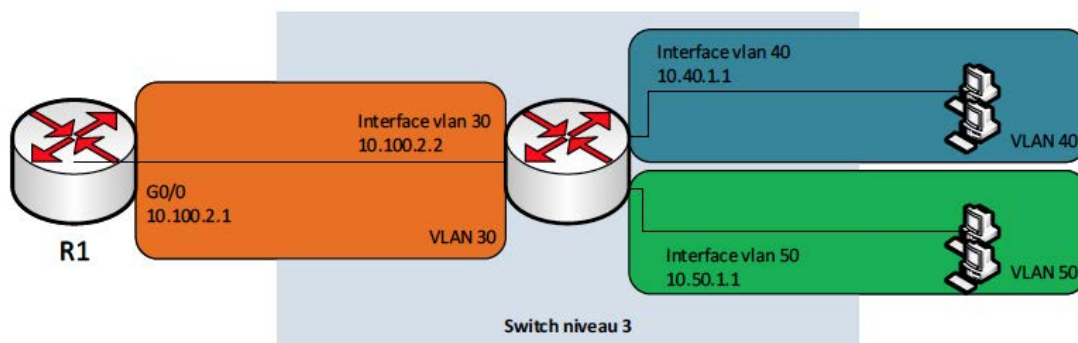
Le VLAN natif est le VLAN où les trames ne sont pas taguées. Par exemple, supposons que le VLAN natif est le 10

Méthode 1 :

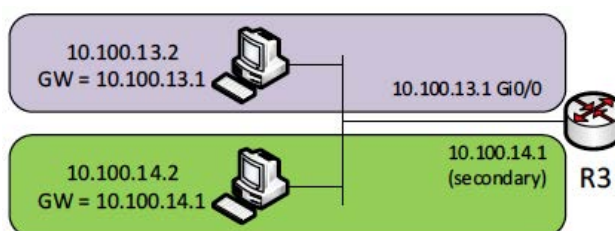
```
interface gi0/0
  ip address 10.100.1.1 255.255.255.0
!
interface gi0/0.200
  encapsulation dot1q 20
  ip address 10.200.1.1 255.255.255.0 (ici on précise un autre VLAN, 20 par exemple)
```

Méthode 2 :

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



ADRESSE IP SECONDAIRE SUR L'INTERFACE D'UN ROUTEUR



POINTS CLÉS SUR LA CONFIGURATION DU VLAN NATIF SUR UN ROUTEUR

ÉTAPE 1 : activer la fonctionnalité routage avec la commande `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...`

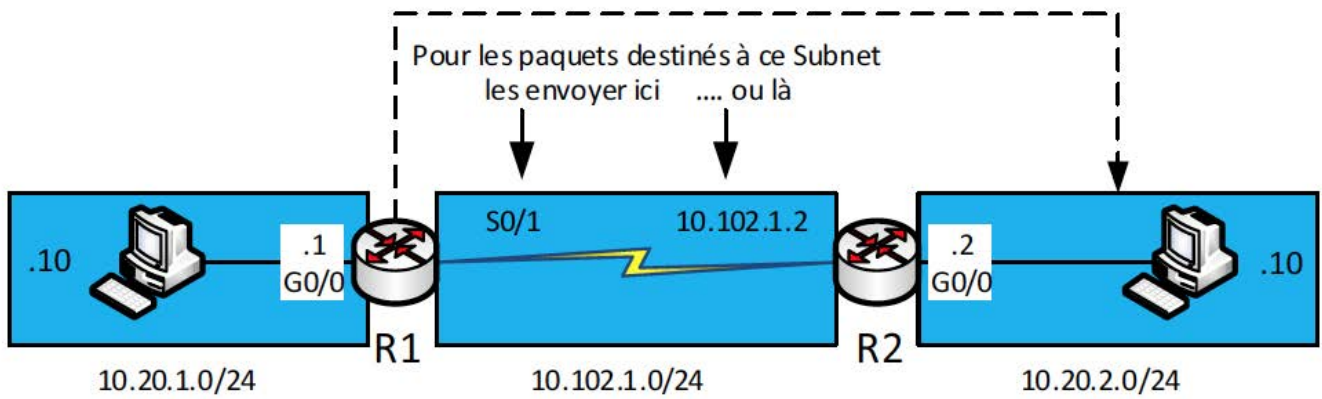
ÉTAPE 4 : configurer une adresse IP pour chaque interface VLAN avec la commande `ip address`

ÉTAPE 5 : activer les interfaces VLAN avec la commande **no shutdown**.

Exemple de configuration (après 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)



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.

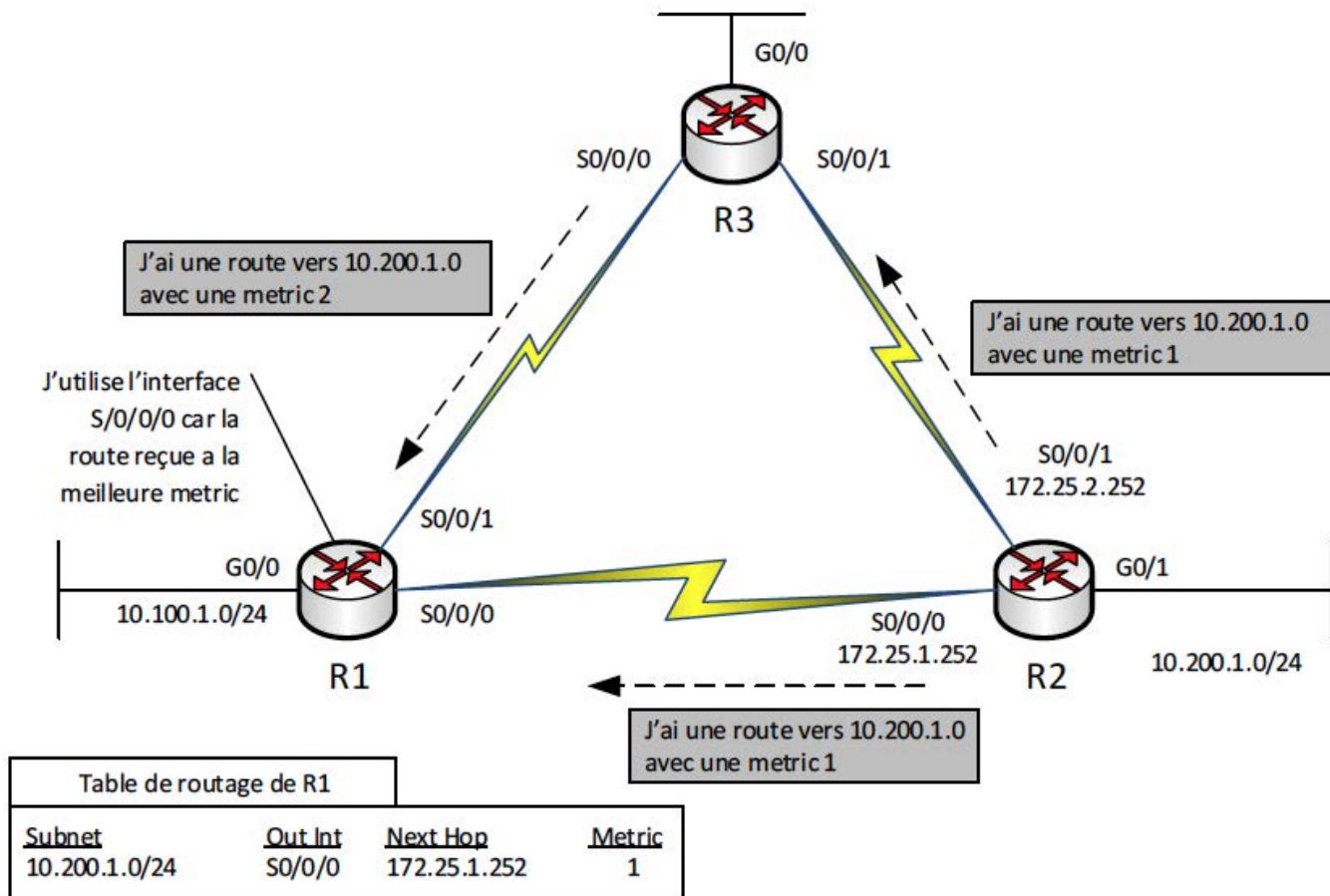
FONCTIONS D'UN PROTOCOLE DE ROUTAGE

- **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.

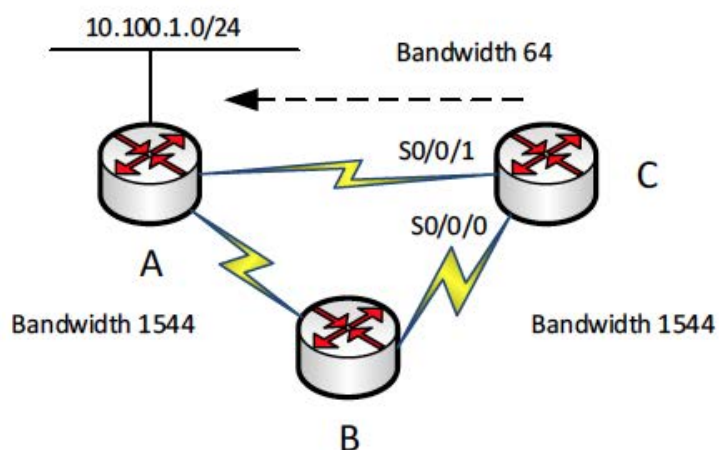
COMPARAISON DES PROTOCOLES DE ROUTAGE

- L'algorithme sous-jacent est-il un vecteur de distance (distance vector) ou état de liens (link state)?
- L'utilité de la métrique - La métrique est utilisée pour déterminer l'itinéraire, donc la sélection d'itinéraire est basée sur la métrique.
- Vitesse de convergence - Combien de temps faut-il pour que tous les routeurs se synchronisent? Ce temps est appelé temps de convergence
- Norme ou propriétaire - Le protocole est-il publique, couvert par les RFC? RIP et OSPF sont couverts par RFCs. EIGRP était un protocole propriétaire de Cisco jusqu'à 2013 quand EIGRP a été libéré au public.

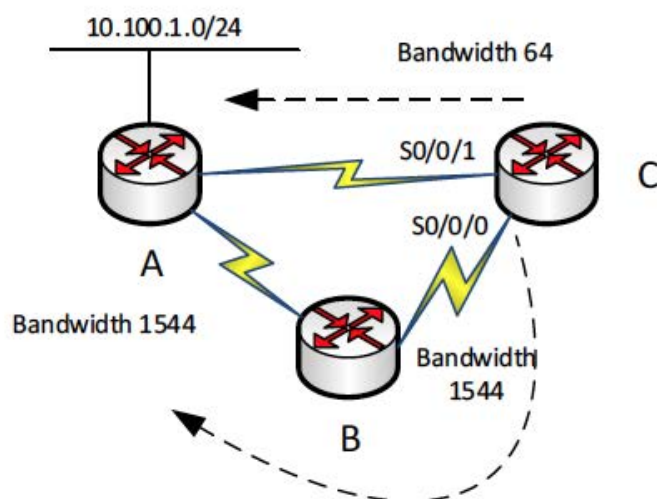
IGP	METRIQUE (METRIC)	DESCRIPTION
RIPv2	Hop Count	Nombre de Hops (de routeurs) entre le Subnet distant et le routeur
OSPF	Cost	Somme du coût (Cost) de toutes les interfaces traversées pour atteindre un Subnet. Le Cost est basé sur la bande passante (bandwidth) de l'interface
EIGRP	Composé de la bande 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 / non 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
Connecté	0
Statique	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
Inutilisable	255

ADMINISTRATIVE DISTANCES – VALEURS PAR DÉFAUT

FONCTIONNALITÉ	RIPV1	RIPV2
Métrique de nombre de sauts	Oui	Oui
La plus grande métrique est 15	Oui	Oui
Mises à jour complètes de routage?	Oui	Oui
Split horizon?	Oui	Oui
Itinéraire empoisonnement / 16 est métrique infinie ?	Non	Oui
Envoie le masque, soutenant VLSM ?	Non	Oui
Support manuel de synthèse des itinéraires	Non	Oui
Mises à jour via l'adresse multicast 224.0.0.9	Non	Oui
Authentification des supports	Non	Oui

CONFIGURATION RIP

Accédez au mode de configuration RIP avec la commande **router rip** en mode configuration globale.

Utilisez la commande **version 2** en mode de configuration RIP pour indiquer au routeur de prendre en charge VLSM

Annoncez un ou plusieurs réseaux avec la commande **network X.X.X.X**

CONFIGURATION RIP

Lorsque RIP est activé sur une interface, le protocole de routage effectue les opérations suivantes:

- Envoi des mises à jour d'itinéraire via l'interface
- Reçoit et traite les mises à jour des itinéraires entrants sur chaque interface
- Annonce le sous-réseau associé à chaque interface

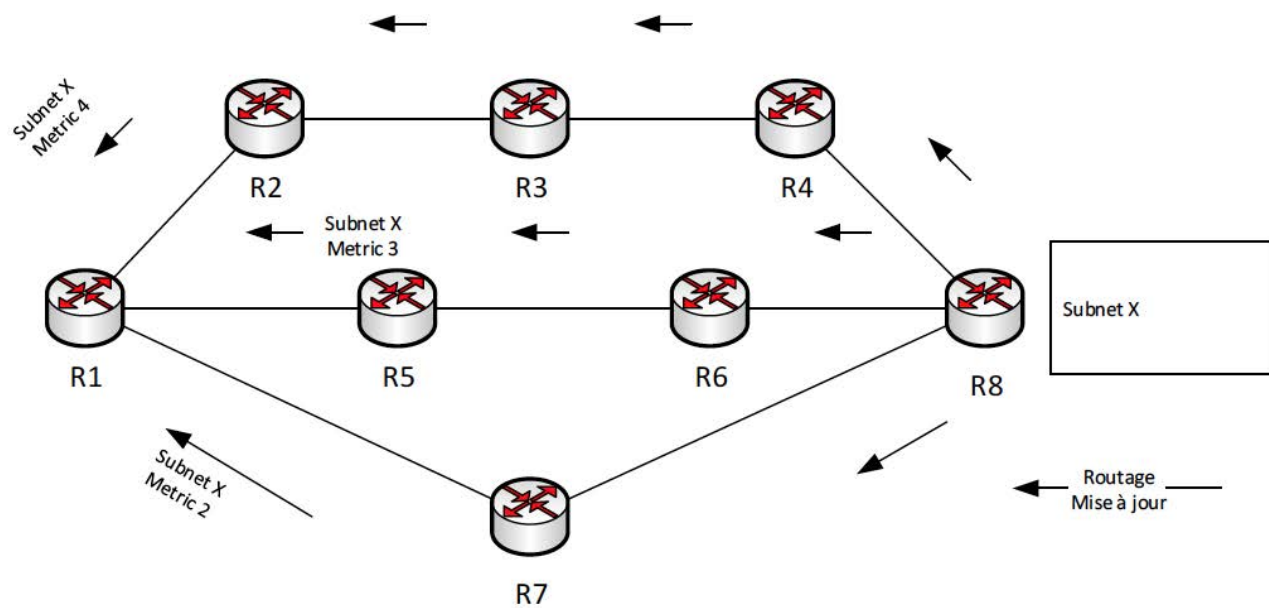
CONFIGURATION RIP

```
B (config) # router rip
B (config-routeur) # version 2
B (config-routeur) # network 172.18.0.0
B (config-routeur) # network 172.20.0.0
```

CONFIGURATION DE L'INTERFACE

```
interface Fa0 / 1
  ip address IP 172.18.0.1 255.255.0.0
interface Fa0 / 2
  ip address 172.20.0.1 255.255.255.0
interface Fa0 / 3
  ip address 172.20.1.1 255.255.255.0
```

INONDATION DES ANNONCES D'ÉTAT DE LIAISON À L'AIDE D'UN
PROTOCOLE DE ROUTAGE D'ÉTAT DE LIAISON



EXEMPLE D'INTERFACE PASSIVE

```
router rip
network 172.25.0.0
passive interface Gi0/1 (les mises à jour ne quittent pas cette interface)
```

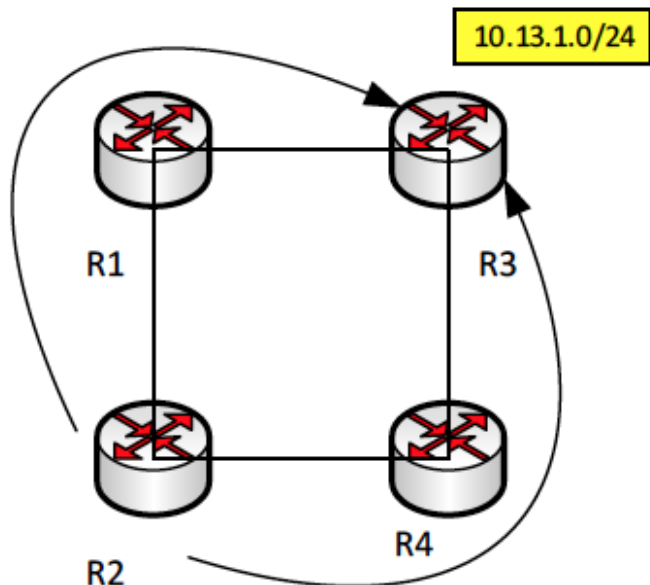
CONFIGURATION RIP

```
router rip
version 2
network 172.19.0.0
network 192.168.100.0

interface fa0 / 0
ip address 172.19.1.0 (annonces RIP sur cette interface)
interface fa0 / 1
ip address 192.168.1.0 (pas d'annonces RIP)
interface fa0 / 2
ip address 192.168.100.0 (annonces RIP sur cette interface)
```

COMMANDES RIP

COMMANDE	UTILISATION
show ip route [rip]	Répertorie les itinéraires enregistrés par RIP. La Commande show ip route affiche tous les itinéraires
show ip protocols	Affiche la configuration RIP, réseaux annoncés, et les adresses IP où les routes ont été apprises
show ip rip database	Montre les meilleures routes connues, y compris les routes RIP voisine et les routes connectées



Ici, R2 peut envoyer du trafic vers 10.13.1.0/24 via R1 ou R4. Il s'agit d'un exemple d'équilibrage de charge à coût égal.

L'utilisation de la commande **maximum paths** contrôlera ce comportement. La valeur par défaut est 4 chemins maximum, mais peut être configuré différemment en fonction du modèle de routeur et de la version IOS

SOUS-RÉSEAUX CLASSFULL NON CONTIGUS

Par défaut, le routeur résume les itinéraires. Dans le cas de réseaux non contigus, ceci peut provoquer un fonctionnement indésirable, y compris l'envoi de paquets au mauvais routeur. Utilisez la commande **no auto-summary** lorsque des réseaux discontigus existent.

```
router rip
  version 2
  no auto-summary
```

ANNONCE D'UNE ROUTE PAR DÉFAUT

Le routeur a la route par défaut vers Internet et cette route doit être annoncée via le protocole RIP. Utilisez la sous-commande RIP **default-information-originate** pour propager l'itinéraire par défaut

```
R1 (config) # ip route 0.0.0.0 0.0.0.0 10.0.0.1
R1 (config) # router rip
R1 (config-router) # default-information-originate
```

show ip route

R 192.168.2.0/24 [120/1] via 192.168.5.2, 00:00:21, Serial0/0/0

R 192.168.3.0/24 [120/1] via 192.168.4.3, 00:00:05, Serial0/0/1

Signification de la première ligne:

192.168.2.0/24 → Numéro du réseau et masque de sous-réseau

[120/1] → Comptage métrique et de sauts

192.168.5.2 → Via le routeur voisin

00:00:21 → Depuis le dernier parcours

Serial 0/0/0 → Interface où la route a été apprise

COMMENT DÉPANNER LE ROUTAGE RIP

1 Vérifier la configuration de routage RIP

- a. Si une déclaration de réseau (commande **network**) est manquante, le routeur n'annoncera pas le sous-réseau
- b. Les mises à jour ne seront pas traitées sur l'interface

2 N'utilisez pas la commande **passive-interface** pour les interfaces connectées à d'autres routeurs.

3 Fonctionnalités affectant le routage RIP

- a. Les interfaces doivent être activées pour que les mises à jour passent entre les routeurs
- b. Les routeurs doivent avoir les adresses IP dans le même sous-réseau pour passer des itinéraires
- c. Recherchez les ACL qui filtrent les mises à jour RIP sur les interfaces. Ces ACL peuvent empêcher RIP de fonctionner correctement

MESSAGES DU PROTOCOLE DHCP

MESSAGE DHCP	DESCRIPTION
Discover	Envoyé par le client DHCP pour trouver un serveur DHCP
Offer	Envoyé par le serveur DHCP afin d'offrir une adresse IP ainsi que d'autres paramètres (bail, passerelle)
Request	Envoyé par le client DHCP pour confirmer 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:

- 0.0.0.0 est utilisée comme IP source par les clients qui n'ont pas encore d'IP attribuée.
- 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 dhcp excluded-address** PREMIERE_IP DERNIERE_IP

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

ÉTAPE 3 :

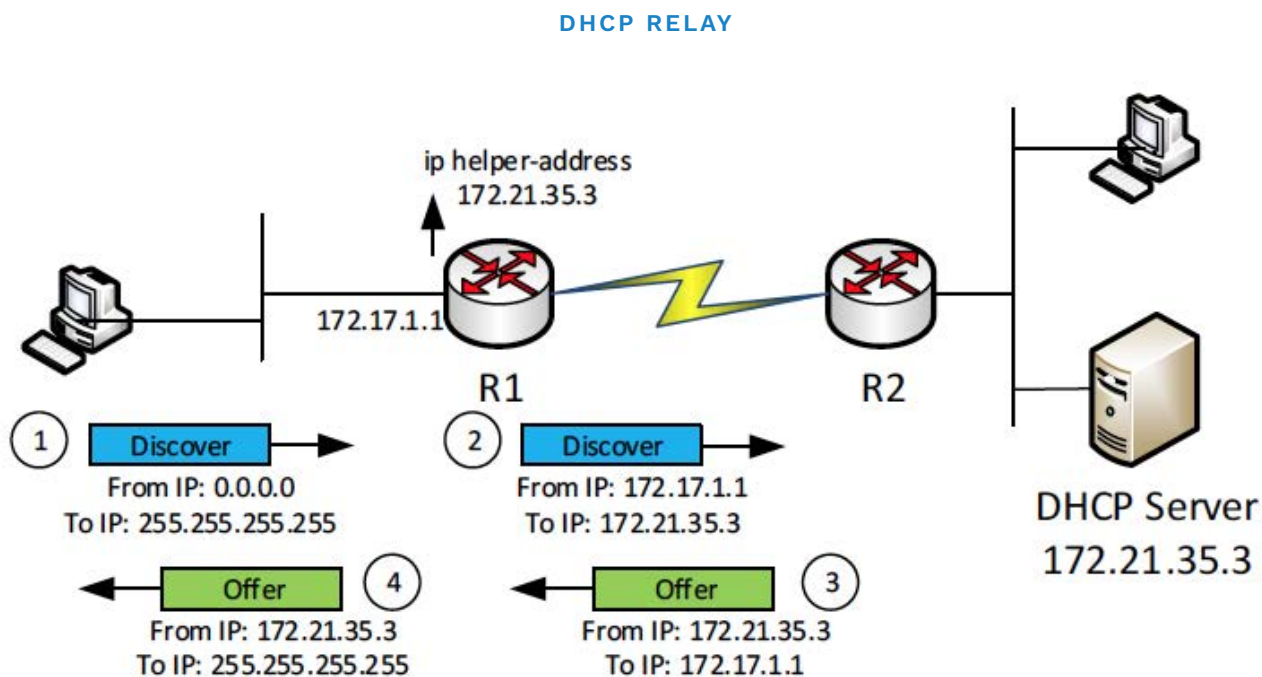
- Définir le Subnet avec la commande **network** subnet-ID mask or **network** subnet-ID prefix
- Définir la passerelle avec la commande **default-router** ADDRESS
- Définir le(s) serveur(s) DNS avec la commande **dns-server** ADDRESS_1 ADDRESS_2
- Définir la durée du bail (lease) pour ces informations 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 reussirsonccna.fr
```

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

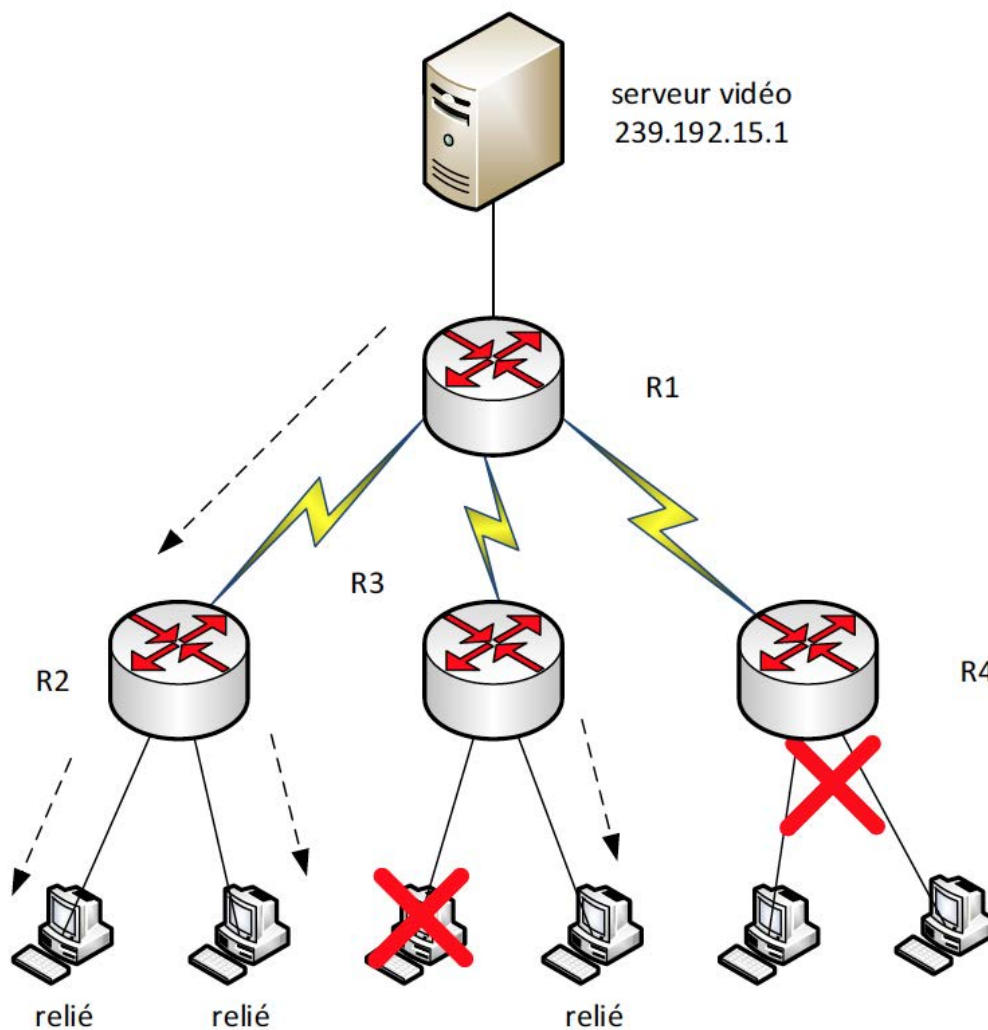


```
Untitled - Notepad
File Edit Format View Help
C:\WINDOWS\System32>ipconfig /all

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Intel(R) Centrino(R) Advanced-N 6235
    Physical Address. . . . . : 
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.0.108(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Saturday, September 20, 2014 12:56:29 PM
    Lease Expires . . . . . : Saturday, September 20, 2014 8:26:41 PM
    Default Gateway . . . . . : 192.168.0.1
    DHCP Server . . . . . : 192.168.0.1
    DNS Servers . . . . . : 68.105.28.11
                           68.105.29.11
                           68.105.28.12
    NetBIOS over Tcpip. . . . . : Disabled
```

Exemple de multidiffusion (Multicast) pour plusieurs hôtes enregistrés:



Seuls les ordinateurs connectés reçoivent le flux multicast

VÉRIFICATION DU SERVEUR DHCP

show ip dhcp bindings - affiche les adresses MAC et les adresses IP associées aux clients

show ip dhcp pool [nom] - Affiche la plage d'adresses IP

show ip dhcp server statistics - Affiche les statistiques du serveur DHCP

DÉPANNAGE DHCP

- 1 Avec DHCP centralisé, au moins un routeur doit avoir l'adresse IP helper configurée
- 2 Assurez-vous que la plage d'adresses des pools DHCP correspond à l'interface d'un routeur
- 3 Dépannage de la connectivité IP entre l'hôte et le serveur DHCP
- 4 Résoudre tous les problèmes LAN entre le client et le relai DHCP

POINTS CLÉS SUR LE ROUTEUR PAR DÉFAUT

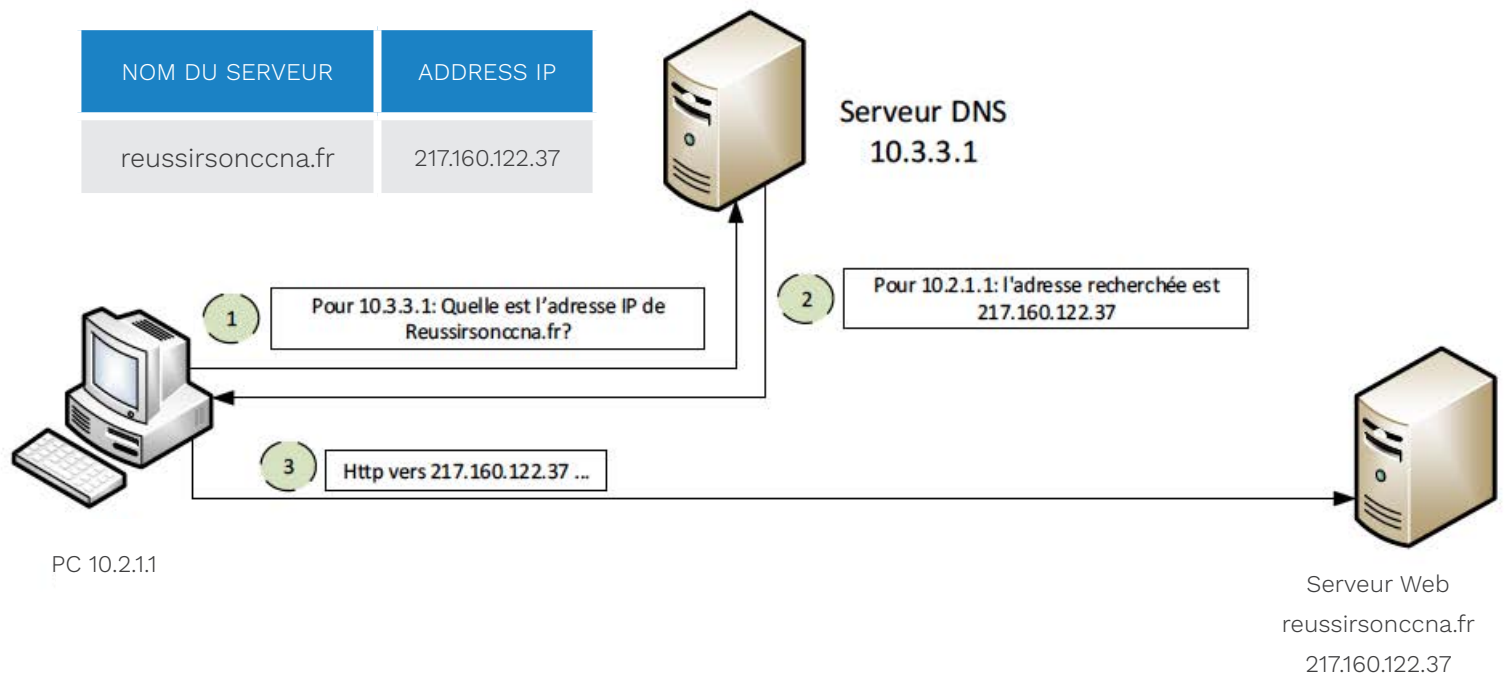
- L'hôte et le routeur par défaut doivent être dans le même VLAN
- Les adresses IP de l'hôte et du routeur par défaut doivent être dans le même sous-réseau
- La configuration du routeur par défaut sur l'hôte doit faire référence à la même adresse IP configurée sur le routeur (si l'hôte indique que le routeur par défaut est 10.100.1.1, l'interface du routeur ne devrait pas être 10.100.1.2)
- Les commutateurs LAN ne doivent pas écarter la trame en raison de la configuration de la sécurité d'un port (port-security)

ADRESSES DE DIFFUSION IP

0.0.0.0 est réservé aux hôtes qui n'ont pas encore d'adresse IP.

255.255.255.255 est l'adresse de diffusion locale. Le routeur ne transmet pas l'adresse de diffusion.

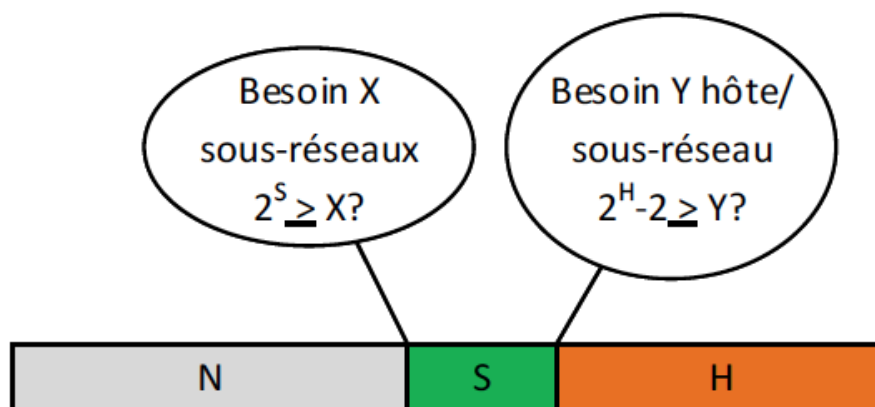
DHCP ET RÉSEAU IP SUR LES HÔTES



Le système de noms de domaine (DNS) est un système de serveurs qui ont un seul but: **résoudre les noms en adresses IP**.

Dans cet exemple, le PC à 10.2.1.1 souhaite contacter Reussirsonccna.fr.

- 1 Le PC contacte d'abord le serveur DNS à 10.3.3.1 pour résoudre l'adresse Reussirsonccna.fr.
- 2 Le serveur DNS résout le site Web avec l'adresse IP 217.160.122.37.
- 3 Une fois que le PC a l'adresse IP de Reussirsonccna.fr, le PC lancera une requête HTTP au serveur à 217.160.122.37.



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

TROUVER 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 $P \geq 32 - H$

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 règles de classe.

ÉTAPE 2 : Calculer Le nombre minimal de bits de sous-réseau (S) Afin que $2^S \Rightarrow$ Le nombre de sous-réseaux requis.

ÉTAPE 3 : Calculer le nombre minimal de bits de hôte (H) afin que $2^H - 2 \Rightarrow$ le nombre requis de hôtes par sous-réseau.

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 maximise 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 inclut 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 $2^7 = 128$

Étape 3 : Le nombre minimal de bits hôtes (H) est 8 parce que 250 est moins que $2^8 = 256$

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.

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 décimal à la première rangée du tableau.

ÉTAPE 2 : Trouver l'octet ayant une valeur autre que 255 ou zéro.

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

ÉTAPE 4 : Inscrire le réseau par classe qui est le sous-réseau zéro.

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

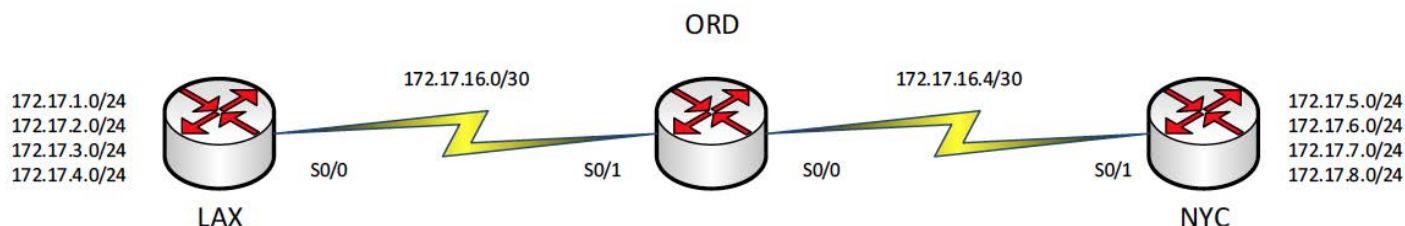
ÉTAPE 6 : Arrêter lorsque l'octet arrive à 255..

**TABLEAU UTILE POUR TROUVER TOUTES LES IDENTITÉS DE SOUS-RÉSEAUX POUR
180.32.0.0 MASQUE 255.255.192.0**

OCTET	1	2	3	4
Masque	255	255	192	0
Chiffre magique	0	0	64	0
Nombre de réseaux / Zero Sousréseau	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

MASQUES DE SOUS-RÉSEAU À LONGUEURS VARIABLES (VLSM)

RÉSEAU 172.17.0.0/16 DIVISÉ PARMI PLUSIEURS ROUTEURS



LES PROTOCOLES DE ROUTAGE IP SANS CLASSE (CLASSLESS) ET PAR CLASSE (CLASSFUL)

PROTOCOLE DE ROUTAGE	EST-CE SANS CLASSE?	MASQUE ENVOYÉ DANS LE MISES À JOUR?	SUPPORT VLSM	SUPPORT DE L'AGRÉATION DE ROUTE 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

MÉTHODE POUR 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 chevauchement 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 pourrions utiliser 172.17.136/23 comme nouveau sous-réseau.

CONFIGURATION DE VLSM AVEC CHEVAUCHEMENT (OVERLAP) POSSIBLE

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

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

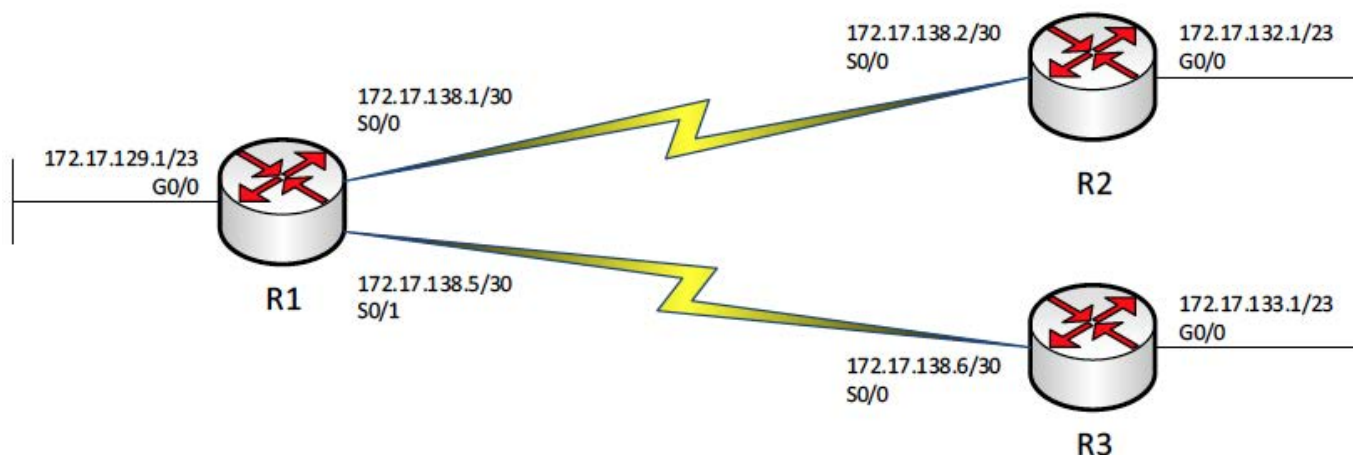
ÉTAPE 1 : Calculez l'identité du sous-réseau et de l'adresse IP de diffusion pour chaque sous-réseau.

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.

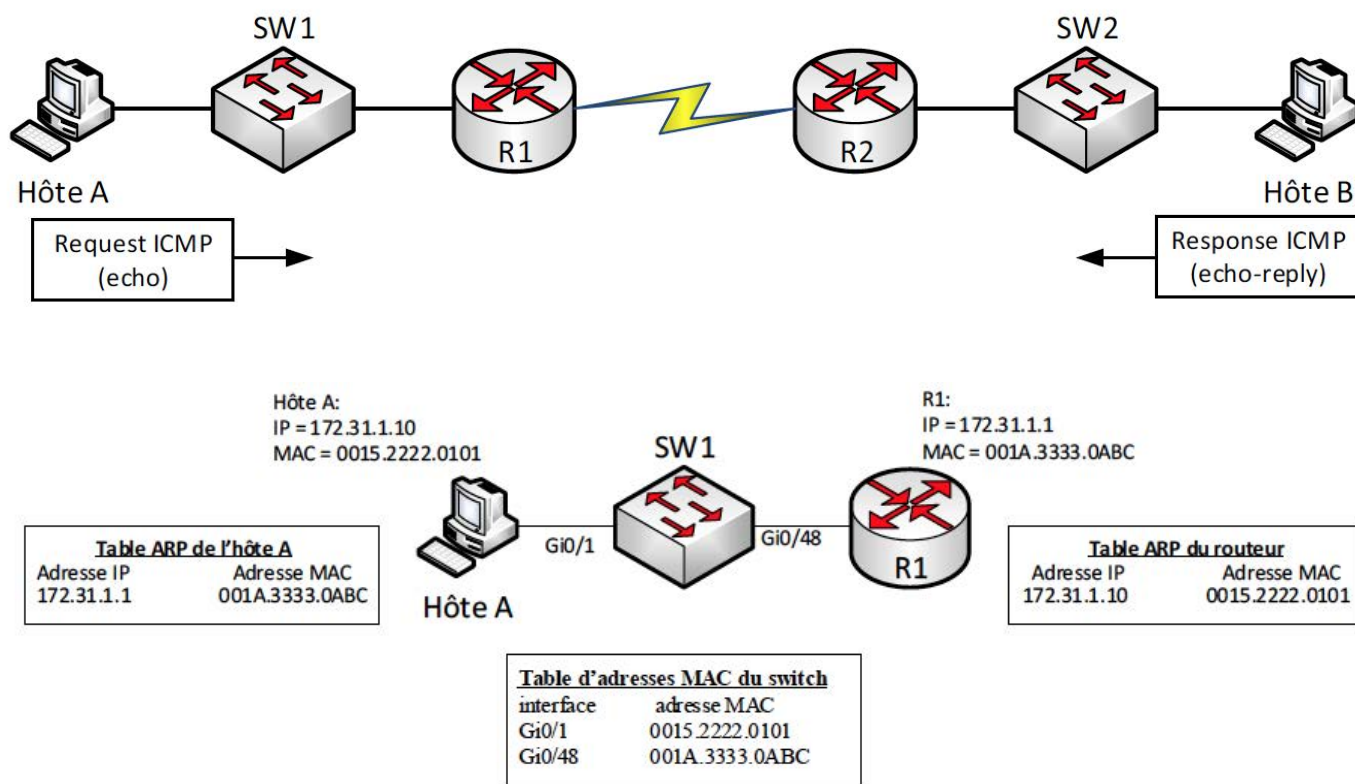
Dans l'exemple ci-après, nous voulons ajouter un autre /23 à R3. Une fois le chevauchement de sous-réseau résolu, nous pourrions utiliser 172.17.136/23 comme nouveau sous-réseau.

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



OUTILS DE DÉPANNAGE IPV4

Le Ping est un outil de base utilisé pour tester la connectivité entre deux hôtes sur un réseau. Lorsque l'hôte A ping l'hôte B, l'hôte A envoie une requête d'écho ICMP à l'hôte B. Lorsque l'hôte B reçoit la requête d'écho, une réponse d'écho est envoyée de l'hôte B à l'hôte A. Si le ping réussit, alors le réseau fonctionne correctement.

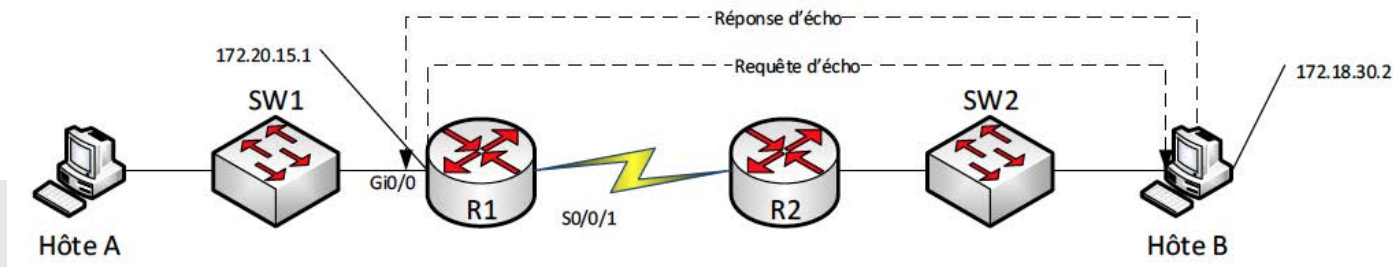


À la suite de la commande ping, nous savons également que les requêtes ARP ont été envoyées et reçues. Nous savons également que les tables ARP du routeur et du PC sont remplies.

Le ping étendu est utilisé pour tester la connectivité à partir de n'importe quelle interface d'un routeur vers un hôte en spécifiant une adresse IP d'interface comme source. Ce test déterminera si l'hôte a une route de retour à la source, également appelée la route inverse.

Problèmes de réseau qui ne peuvent pas être détectés par le ping ou les commandes ping étendu:

- Une ACL bloque les paquets de l'adresse IP d'un hôte, mais pas l'adresse IP du routeur
- Problèmes de sécurité du switch du port LAN de commutation et blocage des trames basées sur l'adresse MAC de l'hôte A (fonction port-security)
- R1 a un problème avec sa route par défaut
- D'autres routeurs ayant un itinéraire différent de 172.20.15.1 par rapport à R1



R1# **ping**

Protocol [ip]:

Target IP address: **172.18.30.2**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: **y**

Source address or interface: **172.20.15.1**

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.18.30.2, timeout is

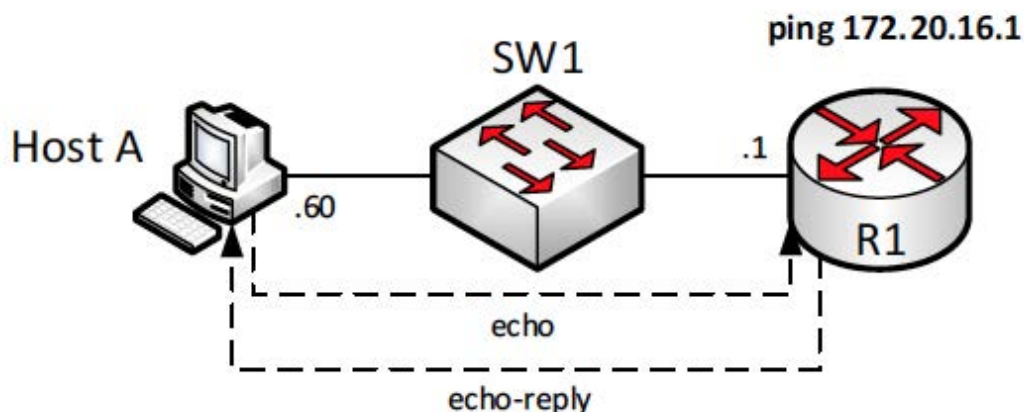
2 seconds:

Packet sent with a source address of 172.20.15.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max

= 1/2/4 ms



PINGS SUR LE SOUS-RÉSEAU LOCAL

Si le ping régulier échoue sur le sous-réseau local, cela peut être causé par:

- **Problème d'adressage IP:** L'hôte A peut avoir une mauvaise adresse IP configurée
- **Problèmes DHCP:** L'hôte A n'a pas reçu l'adresse IP 172.20.16.60, la configuration DHCP pourrait être incorrecte, le routeur n'a pas relayé la requête DHCP donc l'hôte A n'a pas son adresse IP
- **Problème VLAN Trunking:** Le port du commutateur est configuré en trunk et l'hôte ne l'est pas (ou vice versa)

COMPARAISON ENTRE LES COMMANDES PING ET TRACEROUTE

- Les deux commandes envoient des messages dans le réseau pour tester la connectivité
- Les deux s'appuient sur d'autres hôtes pour envoyer une réponse
- Les deux commandes sont largement prises en charge sur différents systèmes d'exploitation (Windows, Linux, MAC)
- Les deux commandes peuvent utiliser des adresses IP ou des noms d'hôtes pour identifier l'hôte de destination
- les routeurs ont une version étendue de chaque commande où l'itinéraire inverse peut être testé.

QUE FAIT LA COMMANDE TRACEROUTE?

- La commande **tracert** génère des paquets avec une valeur TTL (time to live) très faible.
- Les routeurs renverront ces paquets au routeur d'origine avec une réponse TTL-dépassée (TTL timeout).
- La commande **tracert** examine ensuite chaque réponse TTL dépassée reçue avec l'adresse IP source et commence à construire le chemin.
- Ensuite, la commande augmente la valeur TTL par un et répète le processus jusqu'à ce que l'hôte final soit atteint.

ISOLEMENT DE PROBLÈME À L'AIDE DE TRACEROUTE POUR ISOLER DEUX ROUTEURS

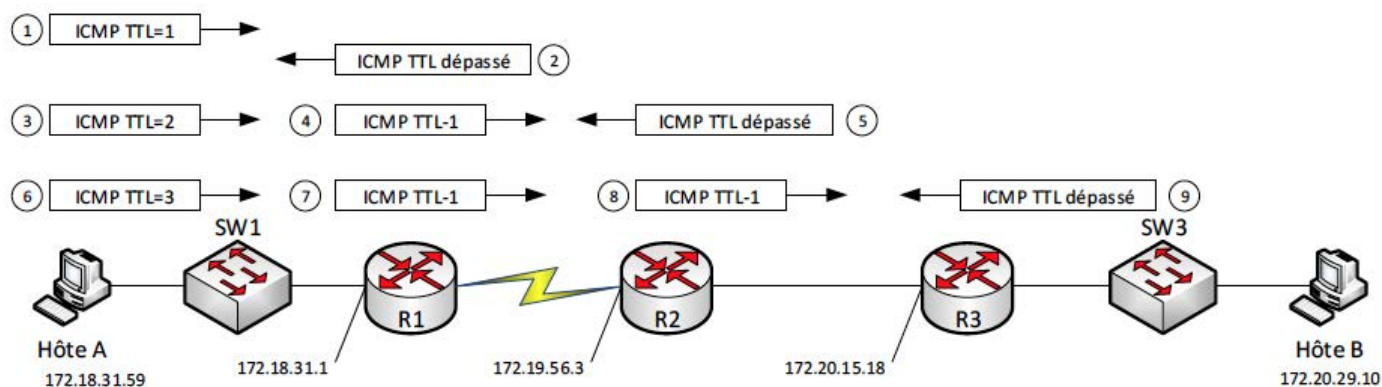
- Trouvez le dernier routeur qui répond à la commande traceroute et le routeur de destination.
- Connectez-vous à la CLI sur chaque routeur et vérifiez si l'itinéraire existe depuis le dernier routeur et le routeur de destination.
- Vérifiez également le dernier routeur pour voir s'il existe des problèmes de couches physiques ou de couche de liaison de données.

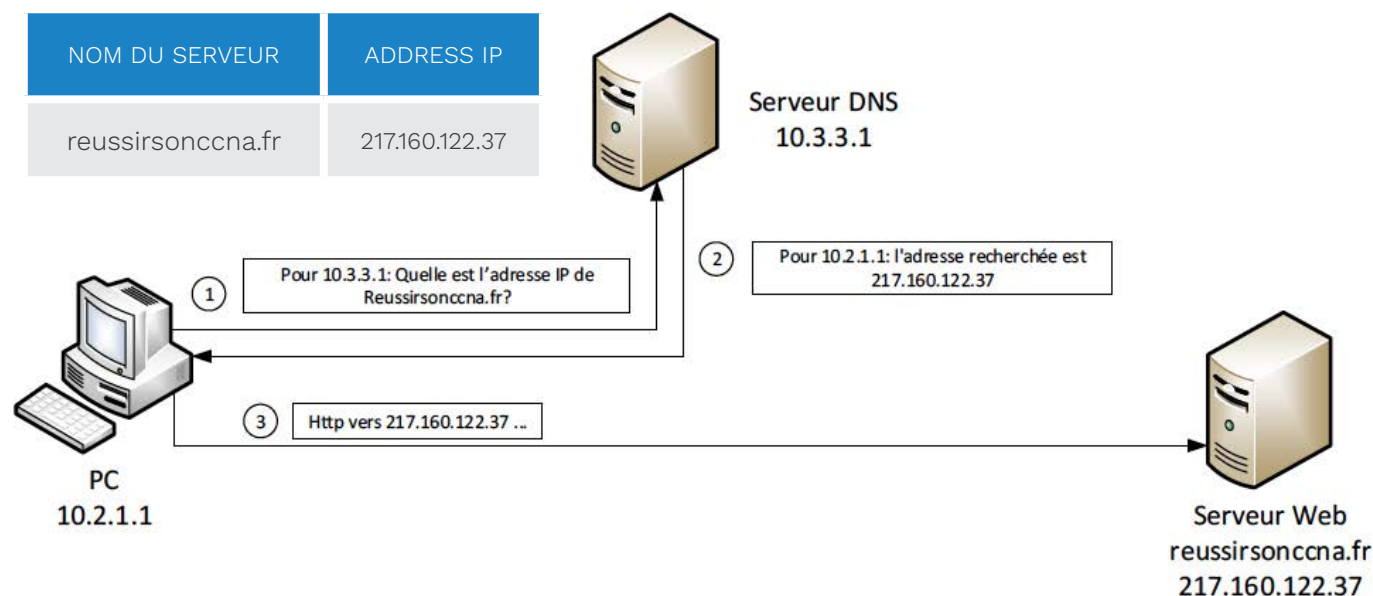
EXEMPLE DE TRACEROUTE DE L'HÔTE A À L'HÔTE B

HostA# **traceroute 172.20.29.10**

traceroute to 172.20.29.10, maximum 64 hops, packets 50 bytes each

1	172.18.31.1	0.1 ms	0.2 ms	0.5 ms
2	172.19.56.3	2 ms	3 ms	4.5 ms
3	172.20.15.18	4 ms	5 ms	5.5 ms
4	172.20.29.10	6 ms	6.5 ms	8 ms





Lors de la vérification des problèmes de connectivité hôte, vérifiez les points suivants:

- 1 Vérifiez la liste d'adresses DNS du serveur par rapport aux adresses IP réelles des serveurs DNS
- 2 Vérifiez le paramètre de la passerelle par défaut de l'hôte par rapport à l'adresse IP du routeur LAN
- 3 Vérifiez le masque de sous-réseau utilisé par le routeur et l'hôte pour voir s'ils correspondent
- 4 L'hôte et le routeur doivent être dans le même sous-réseau. Pour vérifier, regardez le masque de sous-réseau et les adresses IP sur le routeur et l'hôte. Déterminez l'ID de sous-réseau et l'adresse IP de diffusion. Si les adresses IP de l'hôte et du routeur se situent entre l'ID de sous-réseau et l'IP de diffusion, l'hôte et le routeur se trouvent dans le même sous-réseau.

CAUSES PRINCIPALES DES PROBLÈMES DNS

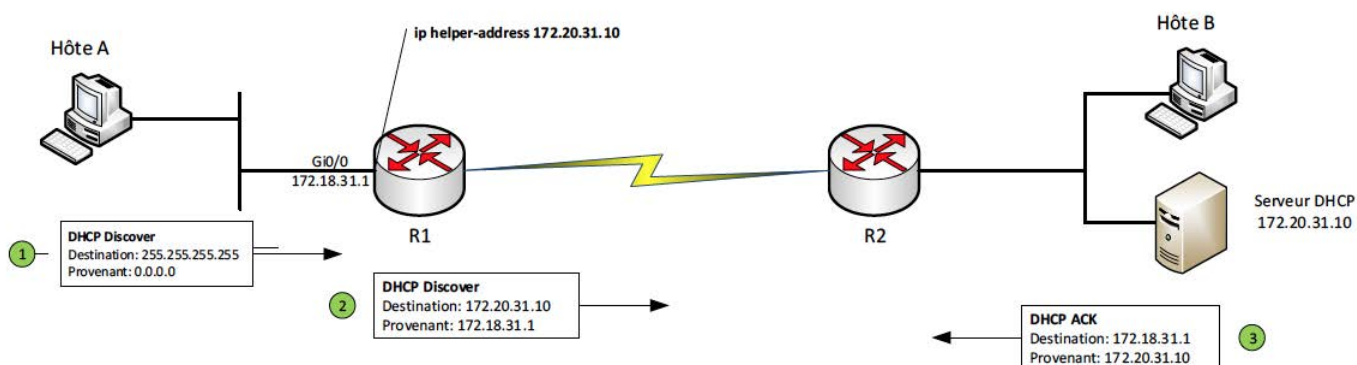
- 1 Les adresses DNS ne pointent pas vers les serveurs DNS corrects
- 2 le routeur n'a pas la connectivité aux bons serveurs de DNS

RAISONS POUR LESQUELLES LES INTERFACES D'UN ROUTEUR NE SONT PAS UP/UP

RAISON	DESCRIPTION	ÉTAT DE L'INTERFACE
Vitesse incompatible	Le routeur et le switch sont réglés manuellement à des vitesses différentes	down/down
Shutdown sur le routeur	L'interface du routeur est arrêtée manuellement à l'aide de la commande shutdown	Admin down/down
Shutdown sur le switch	L'interface du switch est arrêtée manuellement à l'aide de la commande shutdown , mais l'interface du routeur n'est pas arrêtée.	down/down
Port du switch est dans l'état errdisabled	L'interface du switch utilise le portsecurity et une violation s'est produite. Le port switch a été automatiquement désactivé	down/down
Pas de câble ou mauvais câble	Le routeur n'a pas de câble installé, le brochage pourrait être incorrect, ou il y a un fil cassé dans le câble	down/down

```
1 10.0.0.0/8 Est variablement subdivisée, 13 sous-réseaux, 5 masques
2 C 10.1.3.0/26 Est directement connecté, GigabitEthernet0/1
3 L 10.1.3.3/32 Est directement connecté, GigabitEthernet0/1
4 O 10.1.4.64/26 [110/65] via 10.2.2.10, 14:31:52, En série0/1/0
O 10.2.2.0/30 [110/128] via 10.2.2.5, 14:31:52, En série0/0/1
5
6
7
8
9
10
11
```

NUM	CONCEPT	VALEUR DE LA FIGURE	DESCRIPTION
1	Classful Network	10.0.0.0/8	Table de routage organisée par le réseau classful. Dans ce cas, c'est un réseau de classe A avec le masque de sous-réseau par défaut de 8
2	Nombre de sous-réseaux	13 sous-réseaux	Nombre de toutes les routes pour ce réseau classful provenant de n'importe quelles sources, y compris des routes locales - le /32 correspond à chaque interface locale
3	Nombre de masques	5 masques	Nombre de différents masques connus pour ce réseau classful
4	Legende	C, L, O	Lettre indiquant l'origine de la route. C'est relié (connected), O est OSPF, l'est local
5	ID de sousréseau	10.2.2.0	Numéro de sous-réseau de cet itinéraire
6	Prefixe ID	/30	Préfixe (masque de sous-réseau) de cet itinéraire
7	Administrative Distance	110	Le routeur utilisera l'itinéraire avec la distance administrative la plus basse basée sur toutes les routes de toutes les sources.
8	Métrique	128	Métrique de la route
9	Routeur de saut suivant	10.2.2.5	Les paquets correspondant à cet itinéraire sont transférés vers cette destination
10	Heures	14:31:52	Temps depuis que cette route a été signalée par OSPF et EIGRP
11	Interface de sortie	Serial0/0/1	Les paquets correspondant à ce parcours sont transmises par cette interface



La commande **ip helper-address** sur R1 agit comme un agent de relai:

- 1 l'hôte A envoie une requête DHCP DISCOVER à l'adresse de diffusion à tous les hôtes 255.255.255.255
- 2 R1 convertit le DHCP DISCOVER diffusion à une diffusion unique avec une destination de 172.20.31.10
- 3 Le serveur DHCP renvoie la demande à 172.18.31.1

DÉPANNAGE DES PROBLÈMES DHCP

- 1 Si le serveur DHCP est centralisé, au moins un routeur sur chaque sous-réseau doit transmettre les transmissions de requêtes DHCP au serveur DHCP via la commande **ip helper-address**. Ce routeur est l'agent de relais DHCP.
- 2 Vérifiez la connectivité entre l'agent de relais DHCP et le serveur DHCP centralisé.
- 3 Résoudre tous les problèmes de réseau local.
- 4 Dépanner une configuration de serveur incorrecte.

FILTRAGE ET NAT

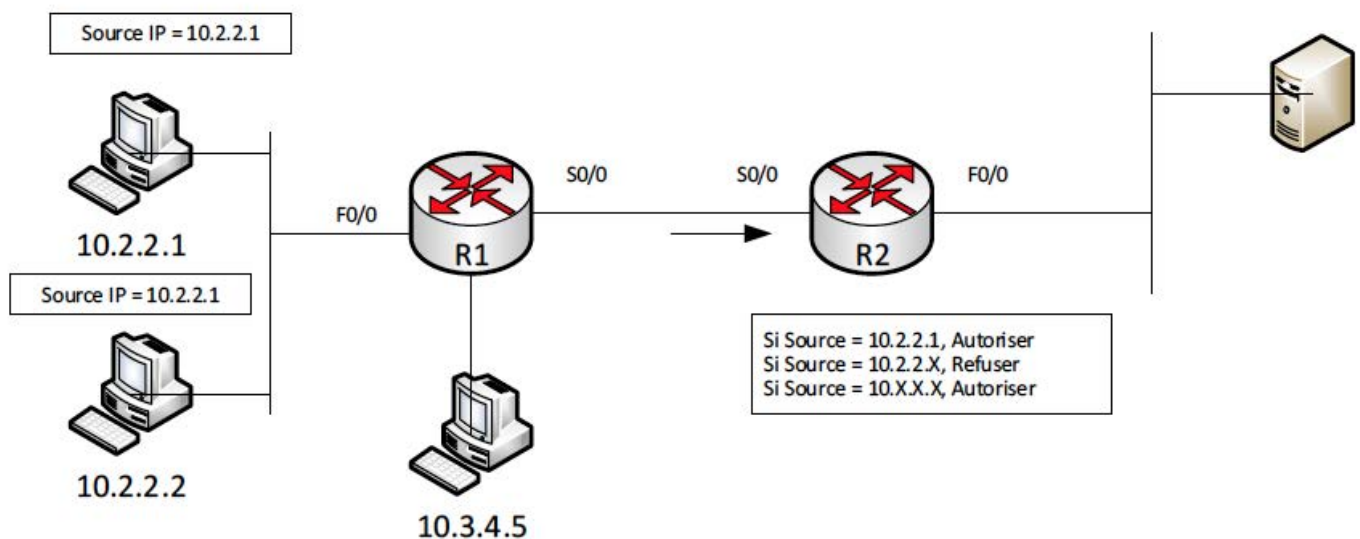


ACCESS CONTROL LISTS (ACLs) STANDARD IPV4

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 initial.

DÉPANNAGE DES PROBLÈMES DHCP

- Decimal 0: Doit correspondre à cet octet
- Decimal 255: Ignorer cet octet



Hôte AIP source = 10.2.2.1

Si Source = 10.2.2.1, Autoriser
Si Source = 10.2.2.X, Refuser
Si Source = 10.X.X.X, Autoriser

Hôte B

Source IP = 10.2.2.2
Si Source = 10.2.2.1, Autoriser
Si Source = 10.2.2.X, Refuser
Si Source = 10.X.X.X, Autoriser

Hôte C

IP source = 10.3.4.5
Si Source = 10.2.2.1, Autoriser
Si Source = 10.2.2.X, Refuser
Si Source = 10.X.X.X, Autoriser

Standard numérotée	Standard Nommée	Standard - Identifie: - IP source
Étendu numérotée	Étendu Nommée	Étendu - Identifie: - Source et Dest. IP - Source et Dest. Port - Divers
Numérotée : - ID Avec un nombre - Commande globale	Nommée: - ID avec un nom - commande imbriquée	

COMPARAISON ENTRE DIFFÉRENTS TYPES D'ACL

TYPES D'ACL

- ACL **standard numérotée** (1 – 99)
- ACL **étendue chiffrée** (100 – 199)
- Valeurs additionnelles sur les nouveaux IOS (standard 1300 – 1399, étendue 2000 – 2999)
- ACL **nommée**: amélioration de l'édition avec des séquences de commande insérable

COMMANDES DE LA LISTE D'ACCÈS

Correspondance d'adresse IP exacte: **permit 10.2.2.2 ou permit host 10.2.2.2**

Correspond d'un sous-réseau en /24: **permit 10.2.2.0 0.0.0.255** (notez bien le masque inversé, wildcard mask)

Dans le masque inversé, un 0 signifie "ne se souci pas" et 255 signifie "il faut que ca corresponde exactement".

COMMANDES POUR METTRE EN OEUVRE L'ACL SUR 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
```

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 séquençement des entrées dans l'ACL est 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

$$\begin{array}{r} 255.255.255.255 \\ - 255.255.255.0 \\ \hline 0. 0. 0.255 \end{array}$$

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 première ACE est traitée 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”** .

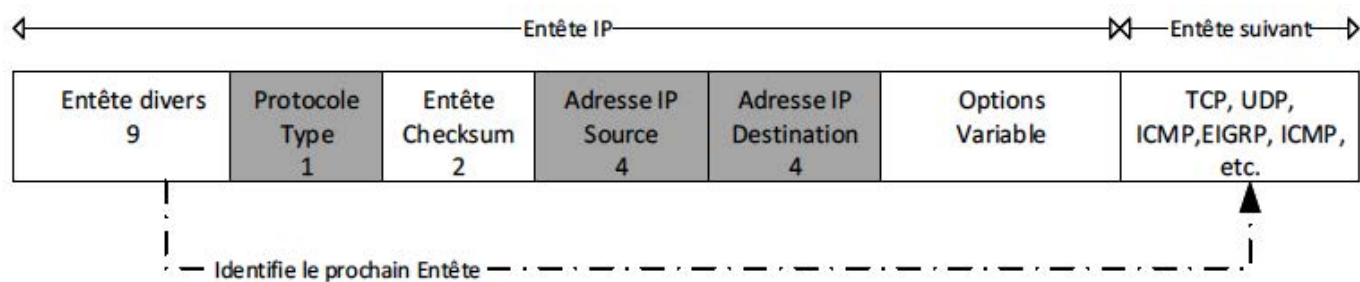
Pour matcher toutes les adresses, utiliser le mot clé **“any”** .

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.

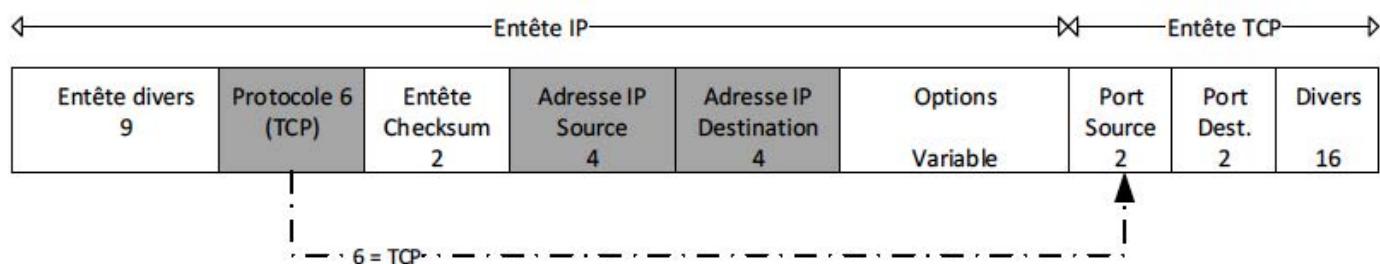
Par exemple, les paquets OSPF, telnet, ping ne seront pas filtrés par cette ACL.



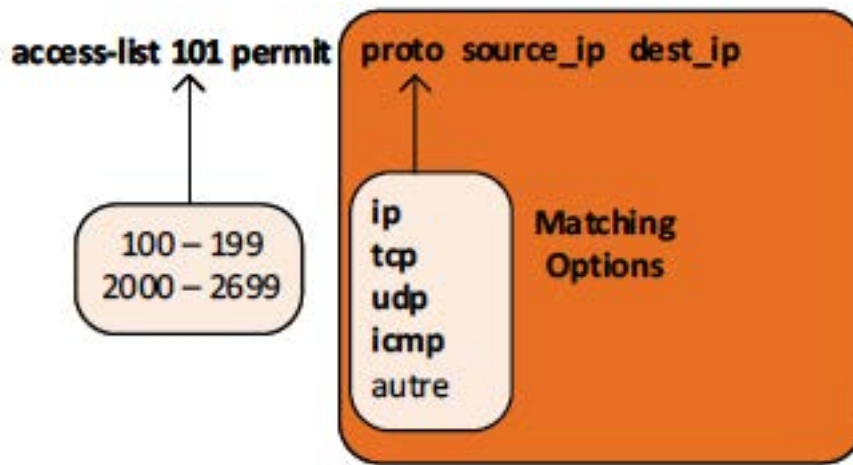
ENTÊTE IP AVEC UN FOCUS SUR LES CHAMPS PERTINENTS POUR L'ACL ÉTENDUE

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)

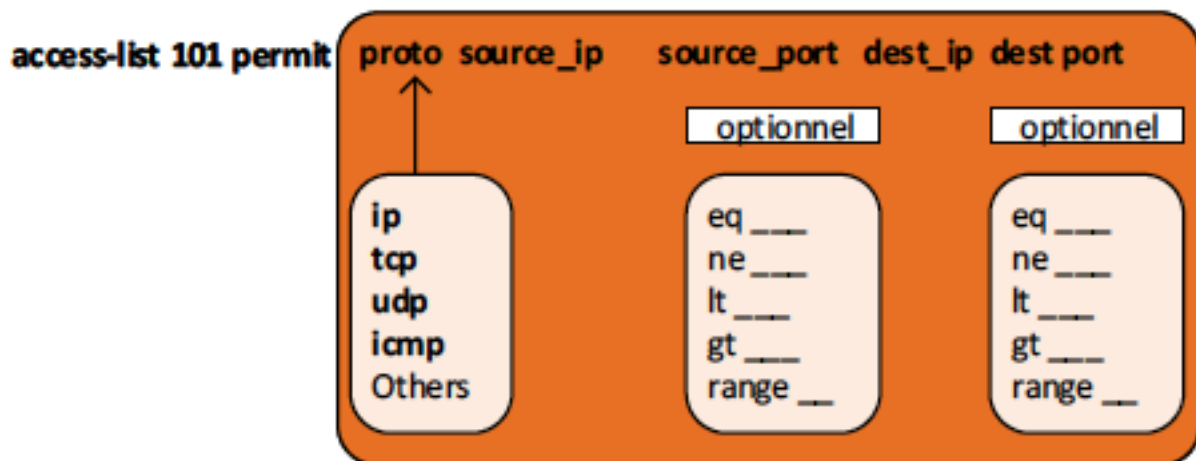
Dans une ACL étendue, tous les paramètres de la commande doivent correspondre au paquet afin de traiter le paquet



ENTÊTE IP AVEC UN ENTÊTE TCP ET LES CHAMPS PORTS



SYNTAXE DE L'ACL ÉTENDUE AVEC LES CHAMPS OBLIGATOIRES

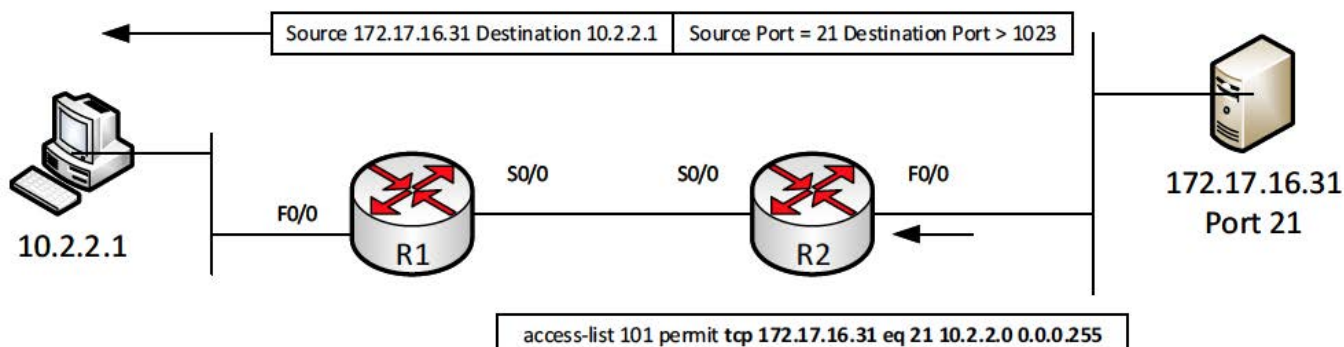


SYNTAXE DE L'ACL ÉTENDUE AVEC LES PORTS

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.

FILTRAGE BASÉ SUR LE PORT SOURCE



ENTRÉE D'ACL	CE QUE ÇA MATCH?
access-list 101 deny tcp any gt 1023 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 inférieur 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.

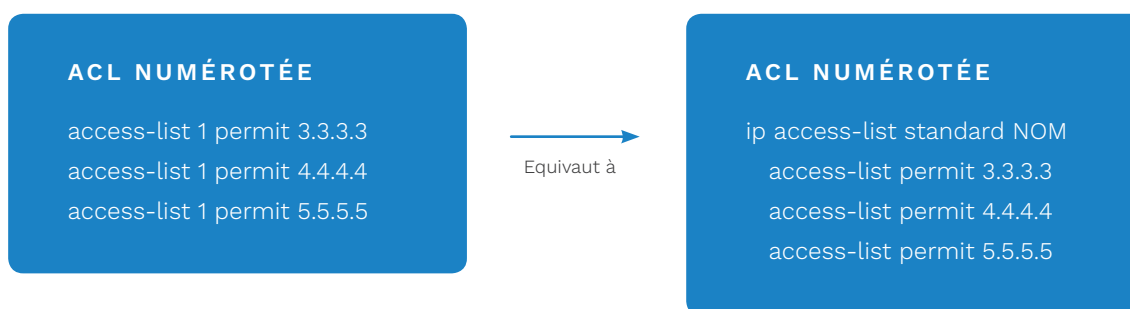
L'utilisation de sous-commande de l'ACL permet d'**ajouter/enlever/modifier** chaque entrée de l'ACL sans avoir à reconfigurer l'ACL en entier.

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, puis réactivez-la sur l'interface

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)
```

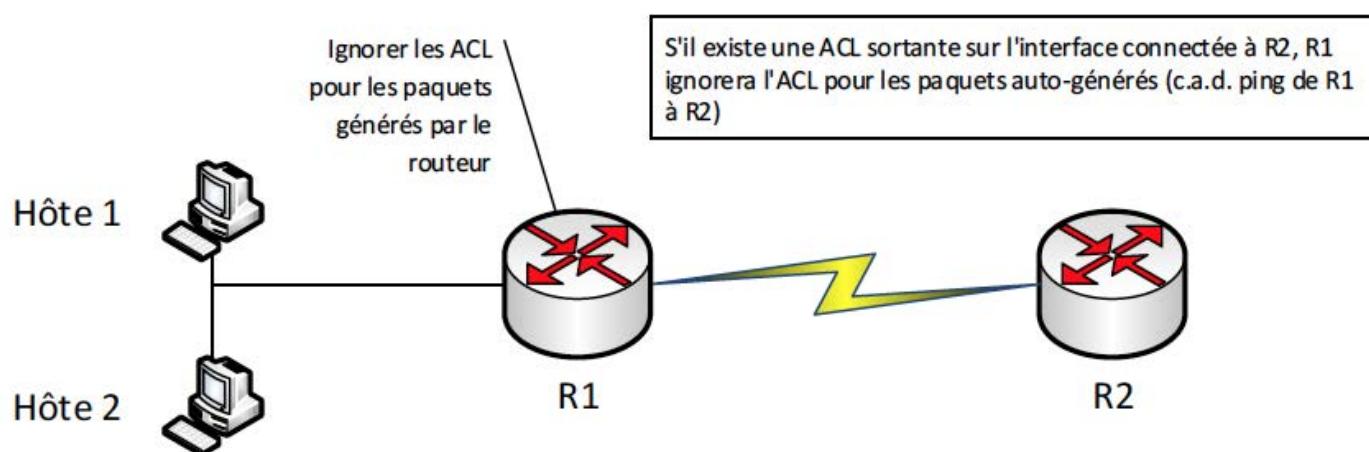
```
R1(config-std-nacl)# do show access-list 25
```

```
5 deny 10.1.1.1
```

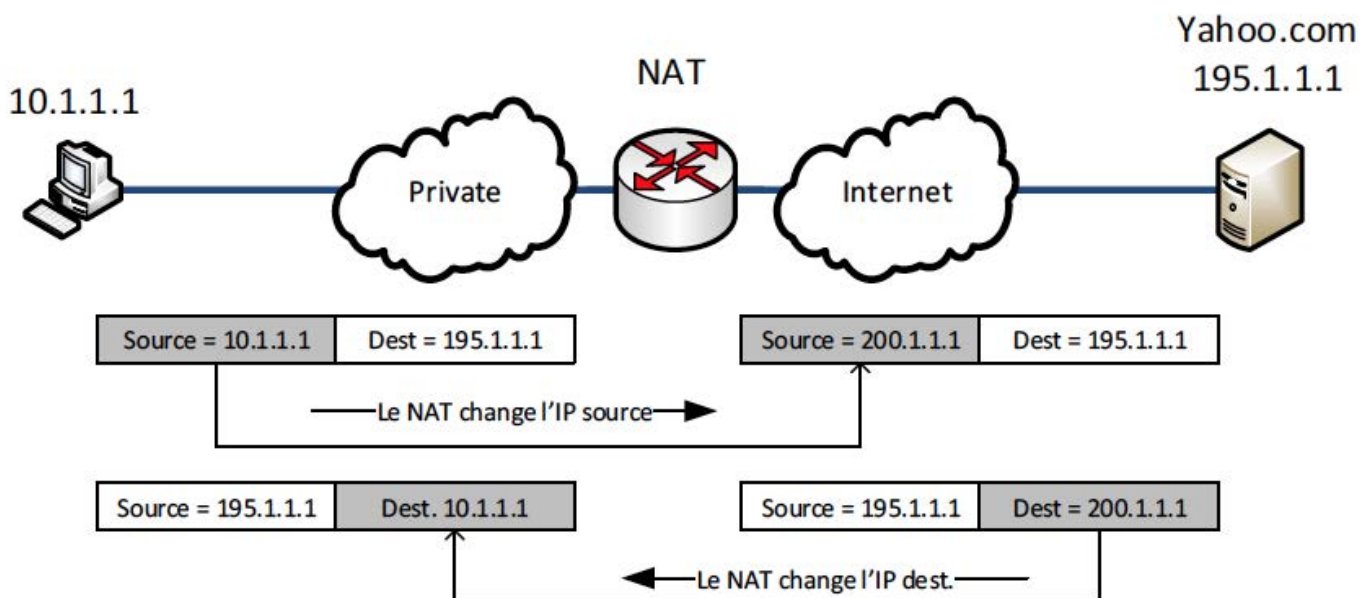
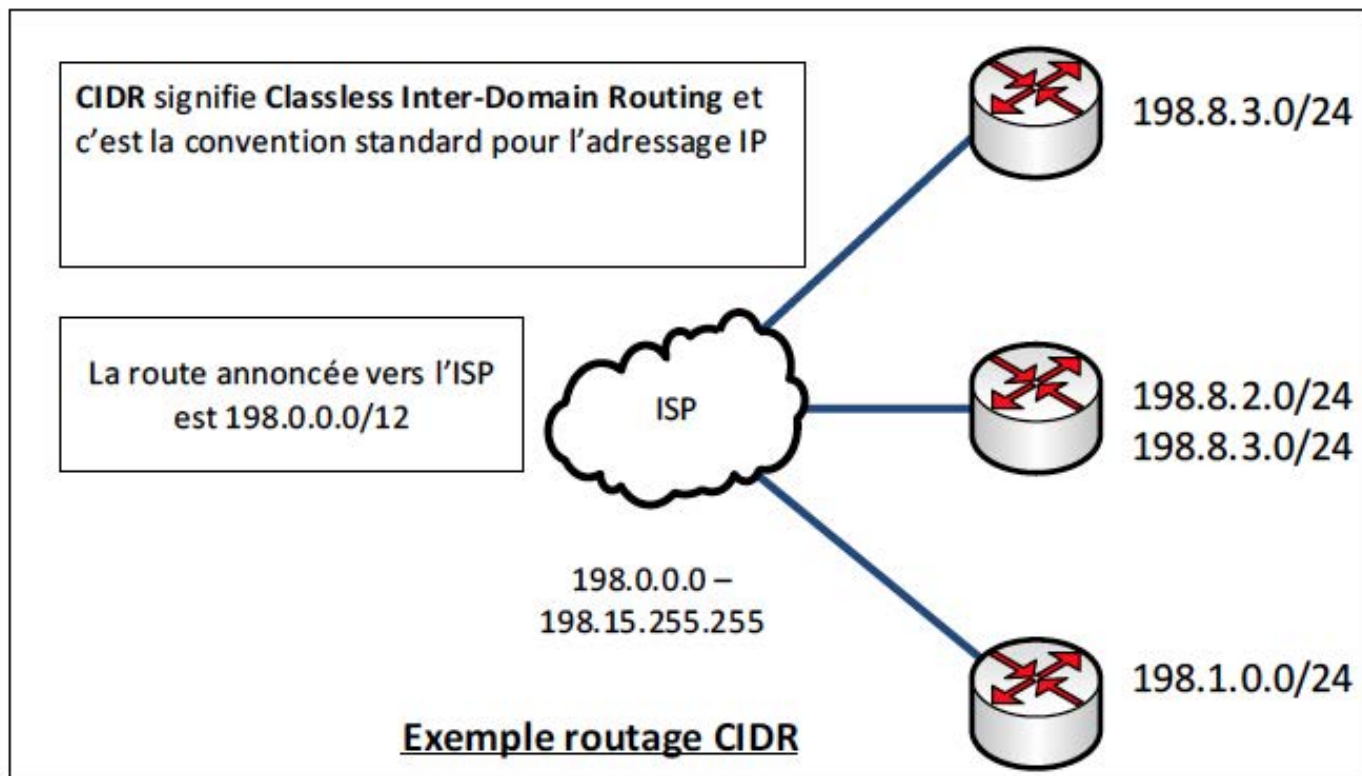
```
10 permit 10.1.1.0 0.0.0.255
```

DÉPANNAGE DES LISTES DE CONTRÔLE D'ACCÈS

- 1 Déterminer les ACL activées sur chaque interface (**show running-config** ou **show ip interfaces**)
- 2 Trouver la configuration de chaque ACL (**show access-list**, **show ip access-list**, **show running-config**)
- 3 Analyser les ACL par les paramètres suivants:
 - a. Vérifiez si les lignes sont désordonnées
 - b. Adresse IP source / destination inversée
 - c. Ports source / destination inversés
 - d. Syntaxe - assurez-vous que les mots-clés **tcp** et **udp** sont utilisés correctement
 - e. Syntaxe (ICMP) - rappelez-vous que pings utilisé **ICMP**, et non TCP ou UDP
 - f. Explicite **deny all** - était-il inclus dans le haut de l'ACL?
 - g. Emplacement standard de l'ACL - l'ACL se trouve-t-elle au bon endroit? S'il est près de la destination, il pourrait y avoir des problèmes



NETWORK ADDRESS TRANSLATION (NAT)



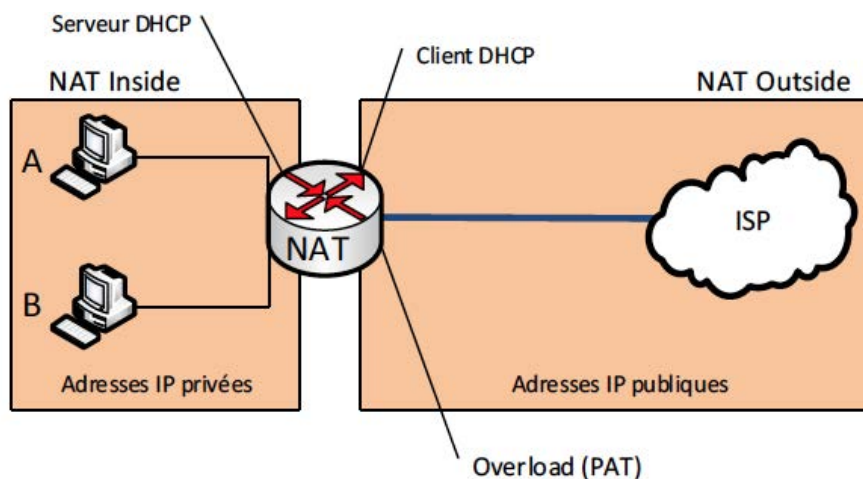
LE NAT PERMET L'UTILISATION DE L'ADRESSAGE PRIVÉE POUR COMMUNIQUER SUR INTERNET

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

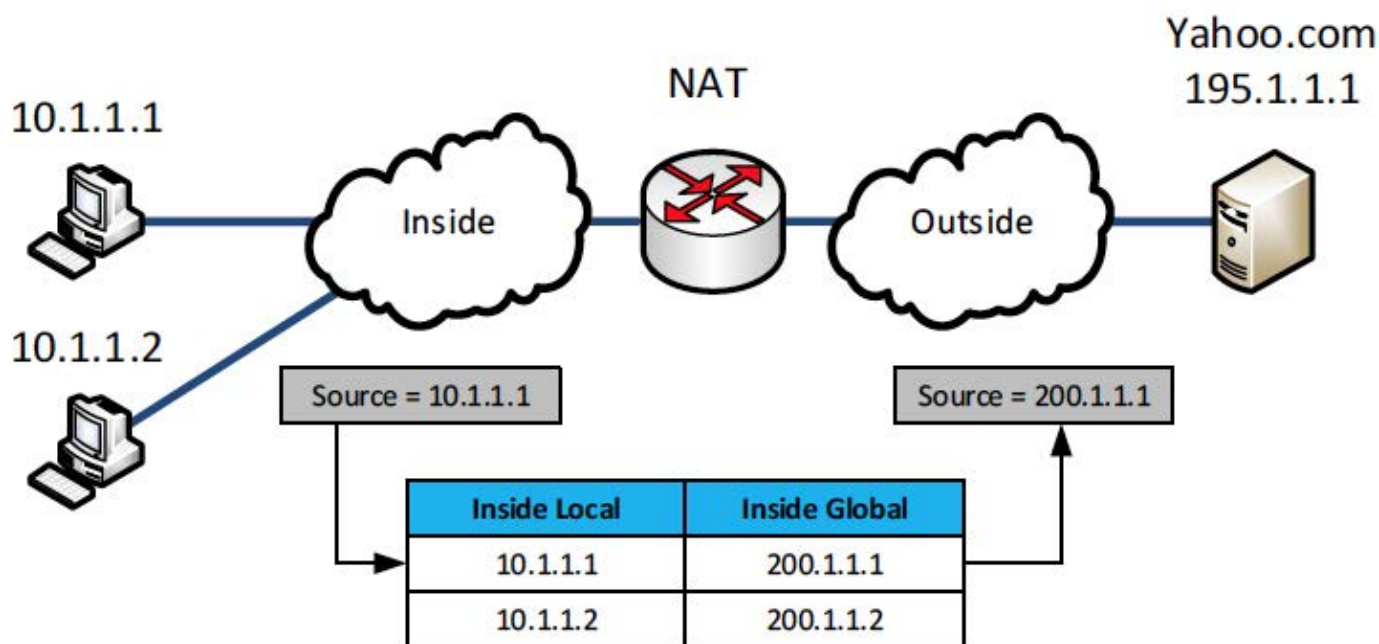
TERMINOLOGIE NAT

TERME	SIGNIFICATION
Inside local	Inside signifie le réseau interne à l'entreprise. Ce sont donc les 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.

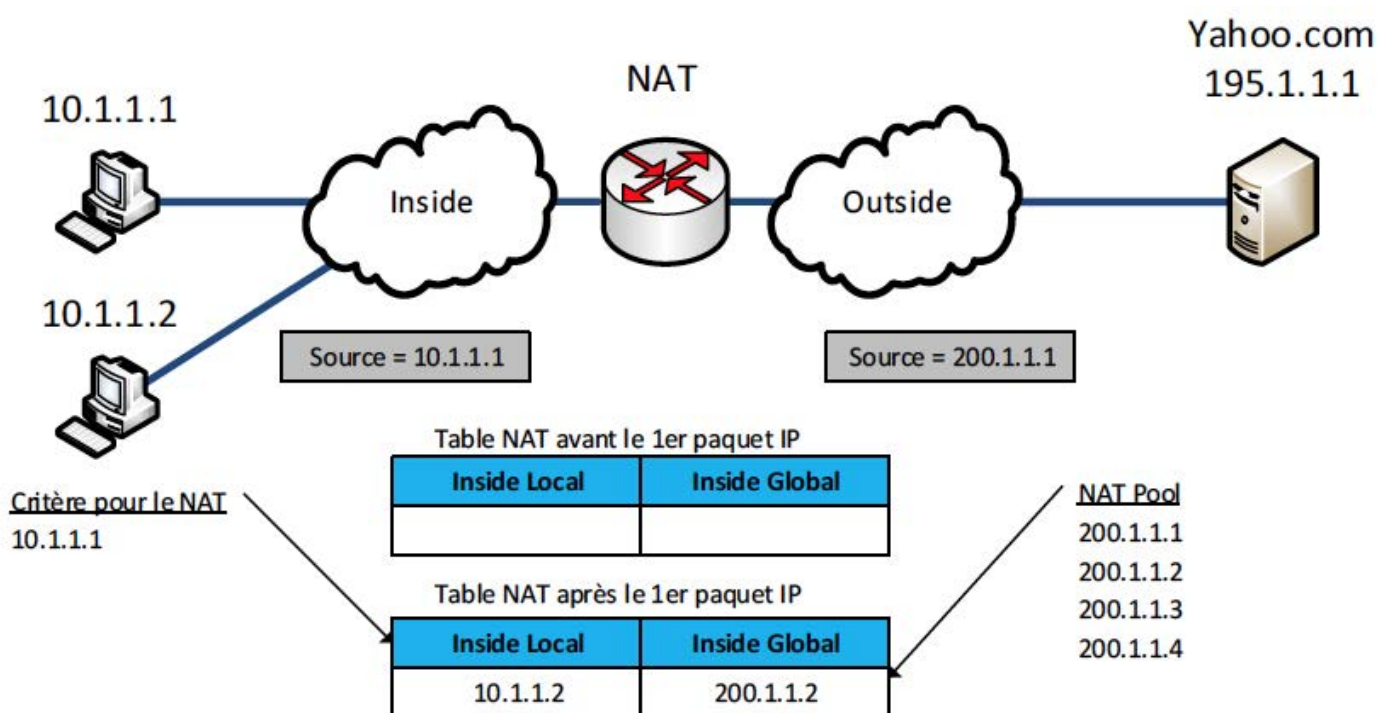
LOCALISATION DES ROLES DHCP ET NAT



NETWORK ADDRESS TRANSLATION (NAT)



TERMINOLOGIE NAT STATIQUE



TERMINOLOGIE NAT DYNAMIQUE

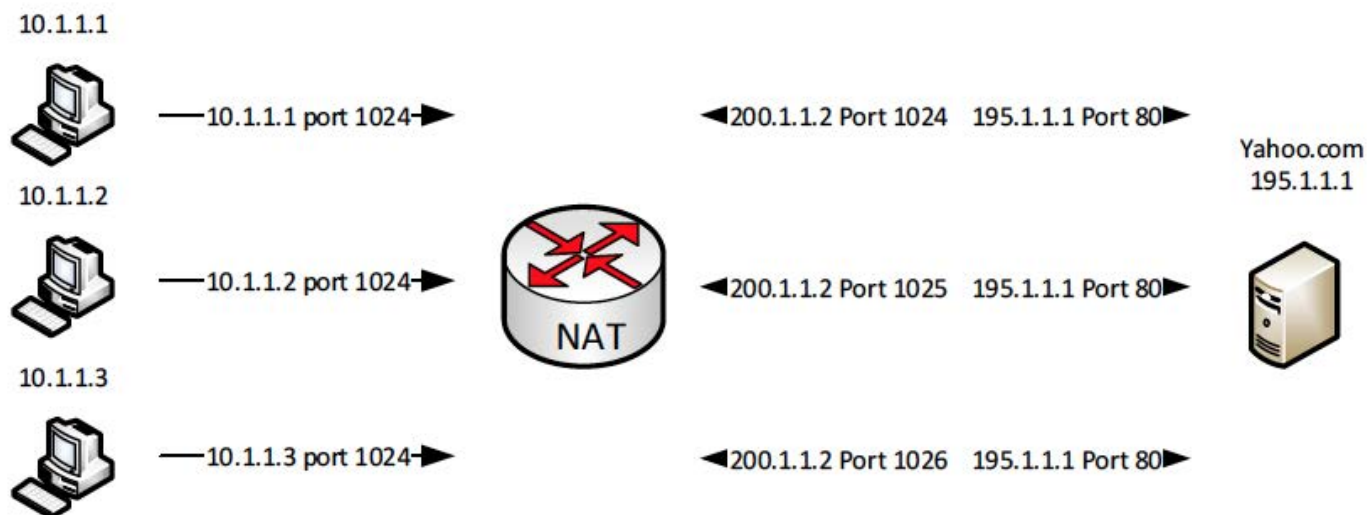


TABLE DE NAT DYNAMIQUE AVEC OVERLOADING
NAT OVERLOAD (PAT)

INSIDE LOCAL	CLASSE
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

EXEMPLE DE TRANSLATION DE NAT STATIQUE

NAT# **show ip nat translations**

Pro	Inside global	Inside Local	Outside Local	Outside Global
---	200.1.1.1	10.1.1.1	---	---
---	200.1.1.2	10.1.1.2	---	---

EXEMPLE DE TRANSLATION DE NAT OVERLOAD (OU PAT)

NAT# **show ip nat translations**

Pro	Inside global	Inside Local	Outside Local	Outside Global
---	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:

EXEMPLE DE TRANSLATION DE 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 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 où 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)# 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
```

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, si l'adresse Inside Local 10.1.1.1 doit être converti en 200.1.1.1, 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. Sans cela, NAT fonctionne, mais PAT ne le fait pas, ce qui se traduit souvent par des paquets d'utilisateurs qui ne sont pas NATté et des hôtes ne pouvant pas accéder à Internet.
- 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. Notez que IOS traite les ACL avant NAT pour les paquets entrant dans une interface et après avoir traduit les adresses des paquets sortant d'une interface.
- Assurez-vous que le trafic utilisateur entre dans le routeur NAT sur une interface interne, déclenchant NAT pour effectuer une traduction. NAT réagit aux paquets qui entrent dans une interface, puis correspond à la logique référencée dans la configuration NAT. La configuration NAT peut être parfaite, mais si aucun trafic entrant ne correspond à la configuration NAT, NAT ne fait rien.

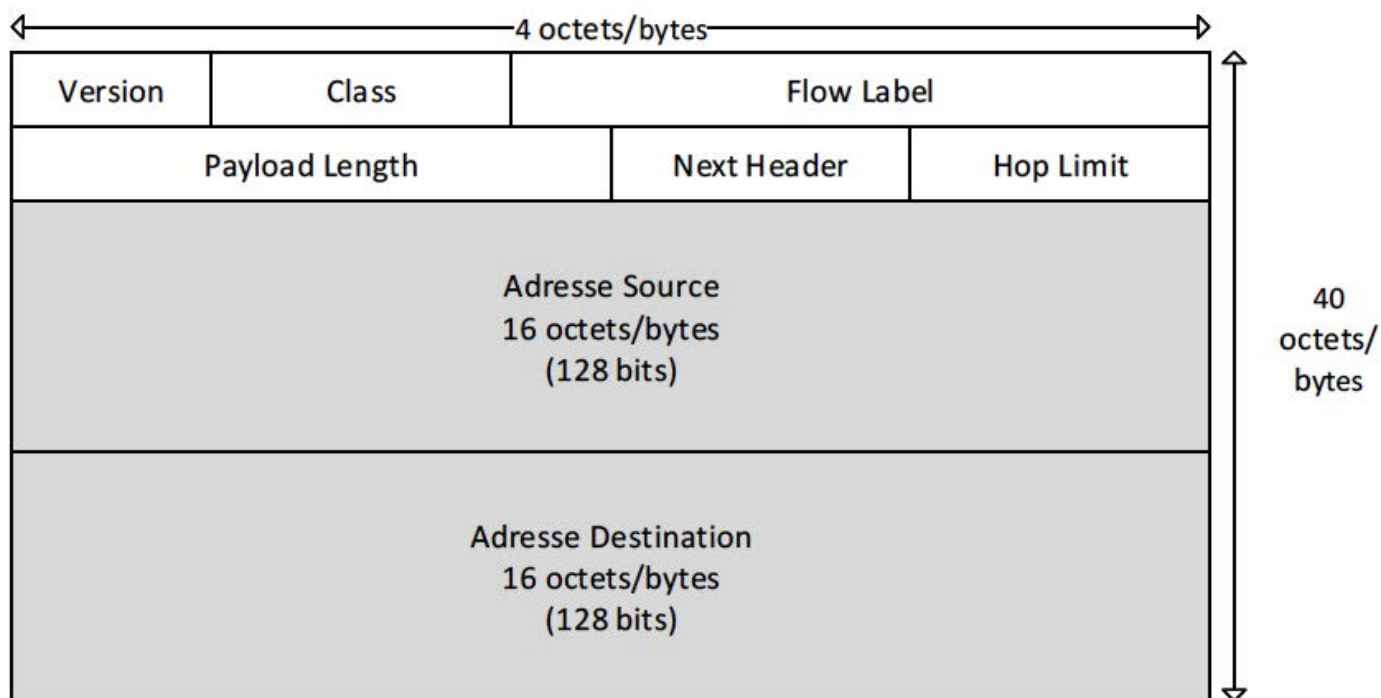
ROUTAGE IPV6 THEORIE



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 supporte IPv6. "ng" signifie "Next Generation"
BGP 4	MP BGP 4	MP-BGP supporte IPv6 avec ses extensions multi-protocole

ENTÊTE IPV6 (40 OCTETS/BYTES) AVEC UNE ADRESSE IPV6 DE 128-BIT DE LONG)



POINTS CLÉS D'IPv6

- Une adresse IPv6 doit être configurée sur une interface afin que celle-ci puisse recevoir ou envoyer des paquets 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

COMMENT ÉCRIRE UNE ADRESSE IPV6?

Comme la taille de 128 bits à écrire est longue, on utilise la **notation hexadécimale** 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 abrégé 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

EXPANSION DES ADRESSES IPV6 ABRÉGÉES:

RÈGLE 1 : Dans chaque quartet, ajoutez les zéros avant jusqu'à quatre chiffres hexadécimaux.

RÈGLE 2 : Pour le double cône :: compter le nombre de quatuors. Ajouter quatuor quad-zéro jusqu'à ce que le numéro 8 est atteint pour l'adresse.

EXEMPLE

2220 :: peut être étendu à 2220: 0000: 0000: 0000: 0000: 0000: 0000: 0000

EXEMPLE

21CA: C: C: D: 20 peut être étendu à 21CA: 000C: 000C: 000D: 0000: 0000: 0000: 0020 (notez le double cône et les zéros de tête).

EXPANSION DES ADRESSES IPV6 ABRÉGÉES:

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.

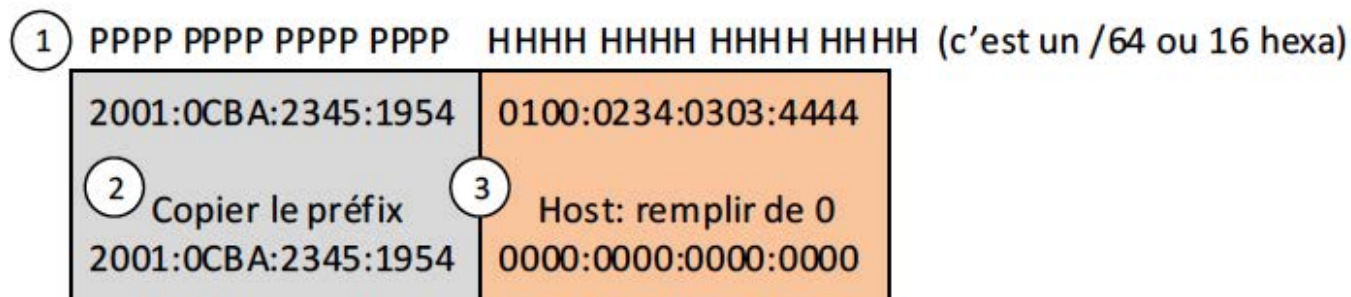


TABLE DE CONVERSION BINAIRE ↔ HEXA

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

ADRESSAGE IPV6 ET SOUS-RÉSEAU (SUBNET)

ADRESSES IPV6 PUBLIQUES ET PRIVÉES:

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

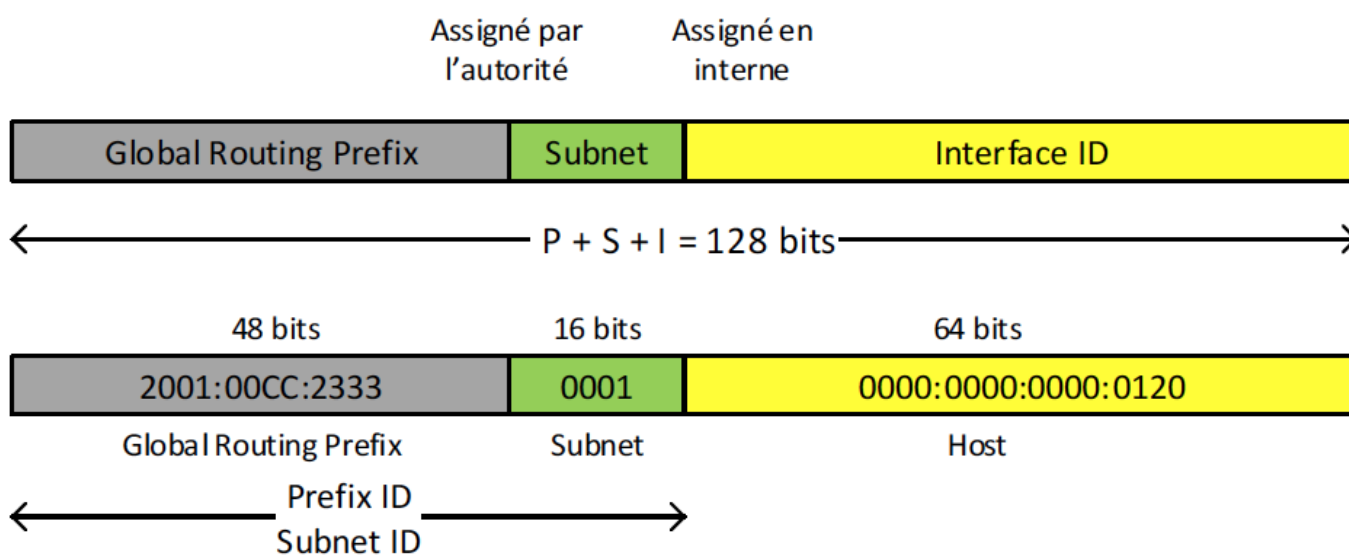
GLOBAL UNICAST : ce sont les adresses IPv6 enregistrées par une autorité de nommage sur Internet. Cet assignement est appelé **Préfix** et est attribué à une organisation (entreprise).

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::

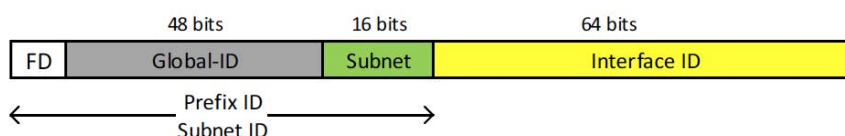
2002:0E88:2222:0002::

2002:0E88:2222:0003::

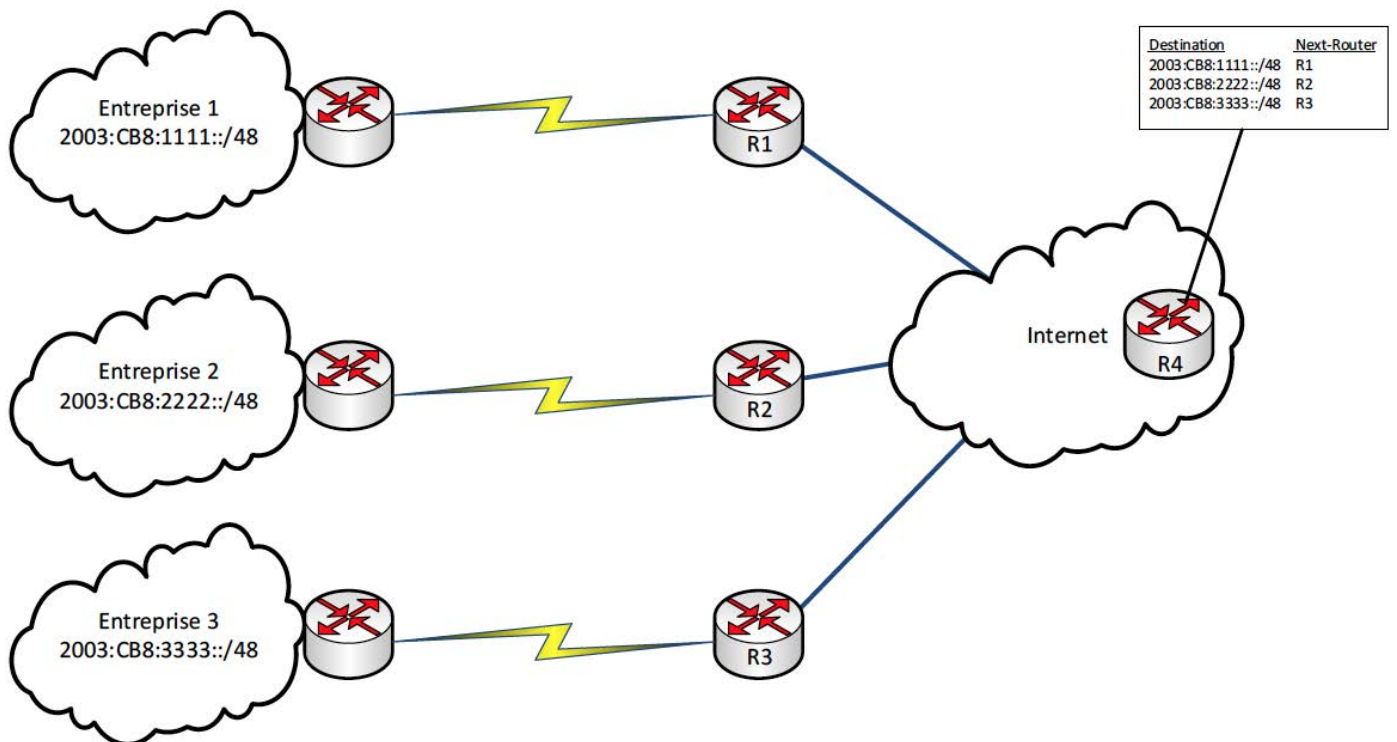
Le champ Subnet peut aller de 0000 à FFFF ce qui fait 65,536 subnets!

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

IMPLEMENTATION 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>

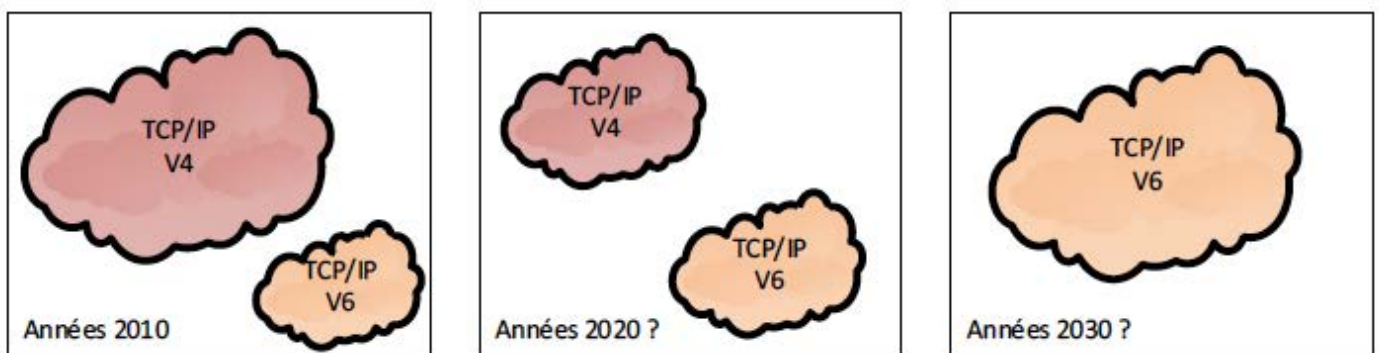
Global unicast addresses:

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` où on peut utiliser une fonction pour générer un **EUI-64** (Extended Unique Identifier de 64 bits).
- L'adresse IPv6 est séparée en deux parties 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 7ème bit** de l'Interface ID (Host)



EVOLUTION DE LA DOUBLE PILE IPV4/IPV6 VERS LE TOUT-IPV6 SUR INTERNET

Subnet Prefix	1 st MAC Half	FFFE	2 nd MAC half
---------------	--------------------------	------	--------------------------

FORMAT DE L'ADRESSE IPV6 AVEC L'INTERFACE ID ET LA CONFIGURATION VIA EUI-64

EXEMPLE

En utilisant les règles EUI-64, dérivez la partie d'adresse hôte de l'adresse IPv6 sur la base d'une adresse MAC de 00:14:EB:C2:15:24

ÉTAPE 1: Divisez l'adresse MAC en deux et insérez FFFE entre les deux moitiés. Modifiez le résultat en un nombre de 64 bits.

Résultats: 0014:EBFF:FEC2:1524

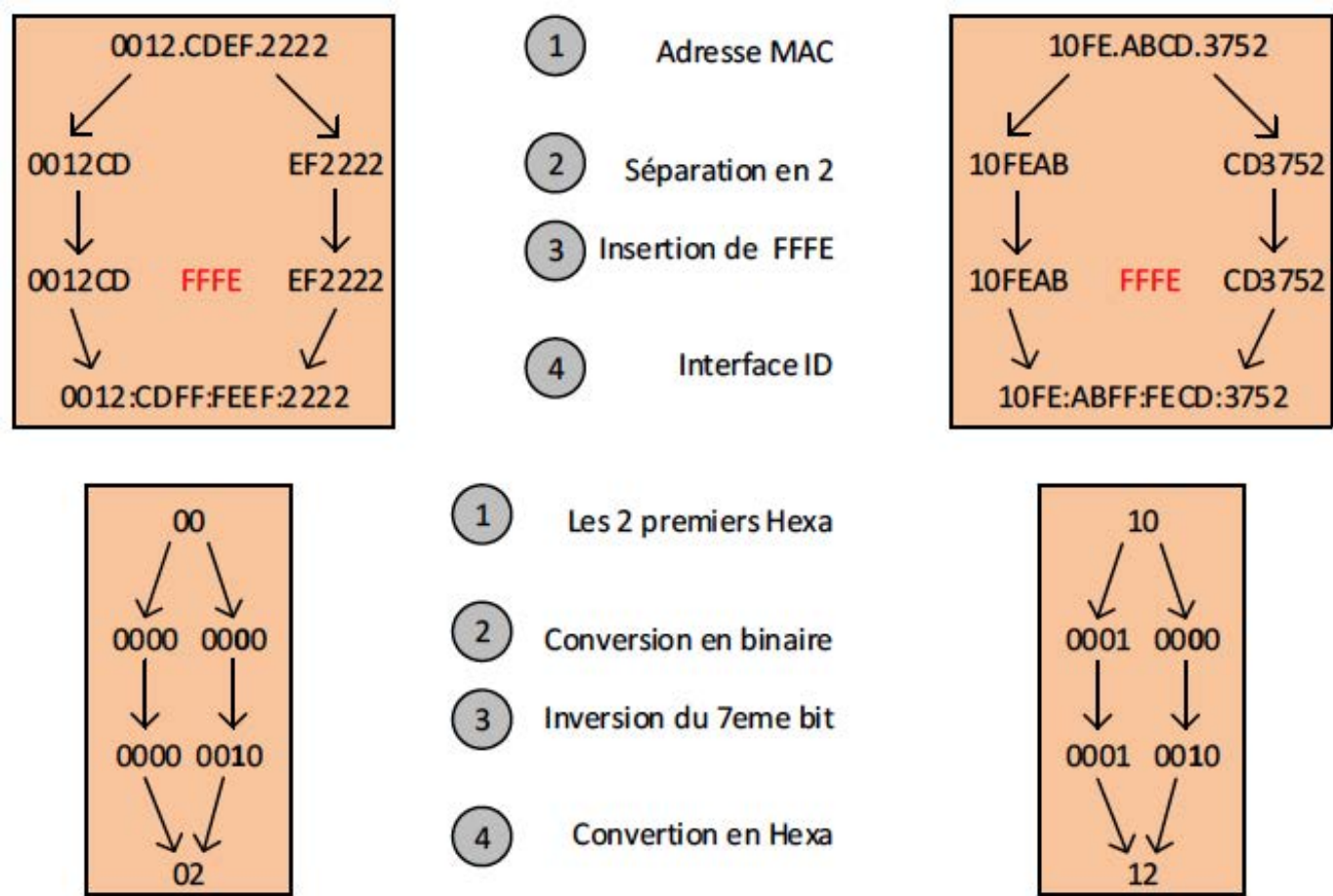
ÉTAPE 2: Prenez les deux premiers chiffres hexadécimaux, convertissez-les en binaire, inversez le septième bit, et convertissez à hex.

Les deux premiers chiffres sont 00, donc l'inversion du septième bit donne 0000 0010 ou 02.

L'adresse d'hôte EUI-64 résultante est 0214:EBFF:FEC2:1524Subnet

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:

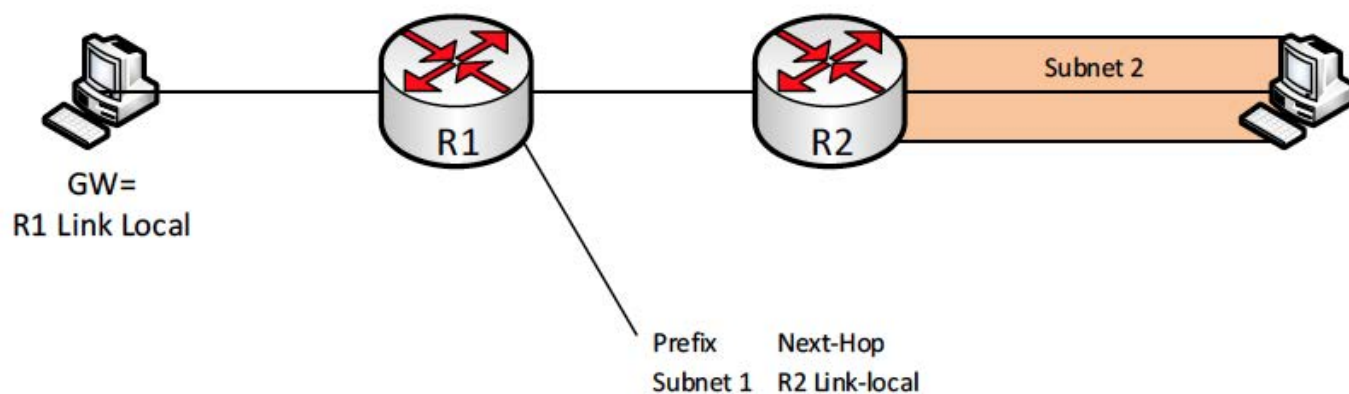
NOM	ADRESSE MULTICAST	DESCRIPTION	EQUIVALENT EN IPV4
All-nodes	FF02::1	Tous les nodes IPv6 sur le lien (link)	Broadcast
All-routers	FF02::2	Tous les routeurs IPv6 sur le link	aucun
All-OSPF, All-OSPF-DR	FF02::5, FF02::6	Tous les routeurs OSPF et OSPF-DR	224.0.0.5, 224.0.0.6
EIGRPv6 Routers	FF02::A	Tous 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 :

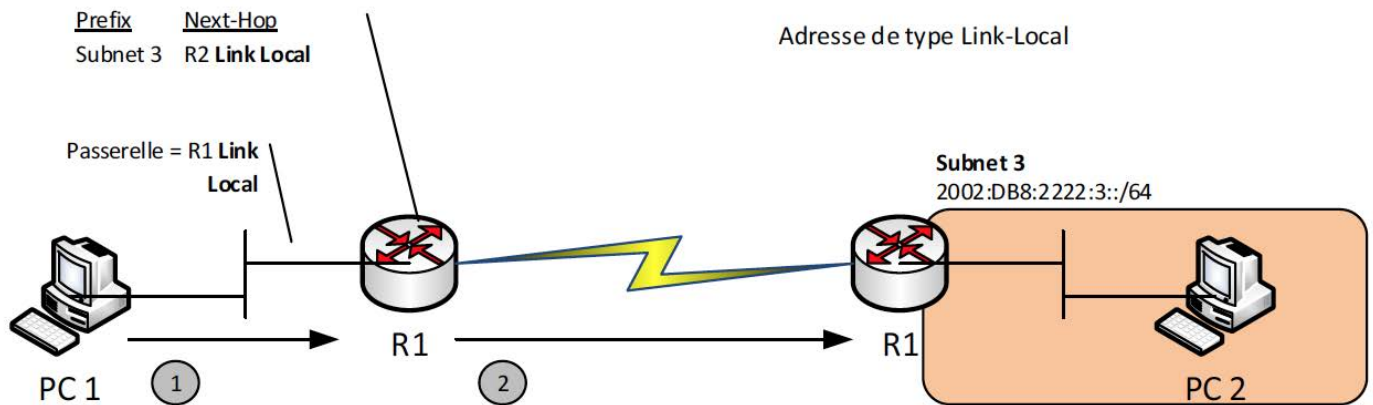
- le routage des paquets IPv6 s'active sur cette interface en **IN et OUT**
- le **Prefix (Subnet)** de cette interface est ajouté dans la table de routage IPv6
- Si c'est une adresse **Link-Local** alors tous les paquets envoyés par cette interface ne sortiront pas du **Prefix (Subnet)** car les routeurs 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.

CONFIGURATION DE L'ADRESSAGE IPV6 SUR UN ROUTEUR



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'autogénérer** 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

LES ADRESSES IPV6 CRÉÉ PAR COMMANDE:

TYPE	PRÉFIXE / NOTES D'ADRESSE	ACTIVITÉ PAR SOUS-COMMANDE D'INTERFACE
Global Unicast	Plusieurs préfixes	Adresse ipv6 adresse / longueur préfixe Ipv6 adresse adresse / préfixe longueur eui- 64
Autre type	FD00::/8	Adresse ipv6 adresse / longueur préfixe
Link Local	FE80::/10	Ipv6 adresse adresse link-local Généré automatiquement par toutes les commandes ipv6 address et ipv6 enable
Tous les hôtes multicast	FF02::1	Généré automatiquement par toutes les commandes d'adresses ipv6
Protocole de routage multicast	Divers	Ajouté à l'interface lorsque le protocole de routage est activé sur cette interface
Solicited mode multicast	FF02::1:FF/104	Généré automatiquement par toutes les commandes d'adresses ipv6
Anycast	N'importe quelle adresse de monodiffusion	Ipv6 adresse adresse / longueur de préfixe anycast

RAPPEL SUR DES ADRESSES IPV6 PARTICULIÈRES:

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

CONFIGURATION D'IPv6 SUR LES HOSTS

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 NDP sont utilisés pour matcher les adresses IPv6 et MAC.

ROUTER DISCOVERY : Le Host découvre les routeurs par deux messages NDP, 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.

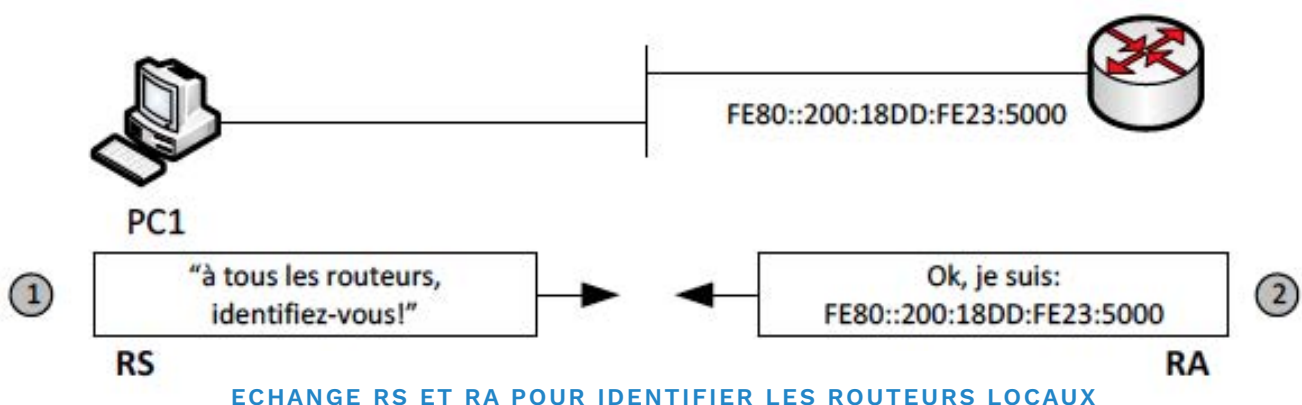
ROUTER SOLICITATION (RS): Ce message est envoyé en unicast au Host qui a envoyé en amont un RS.

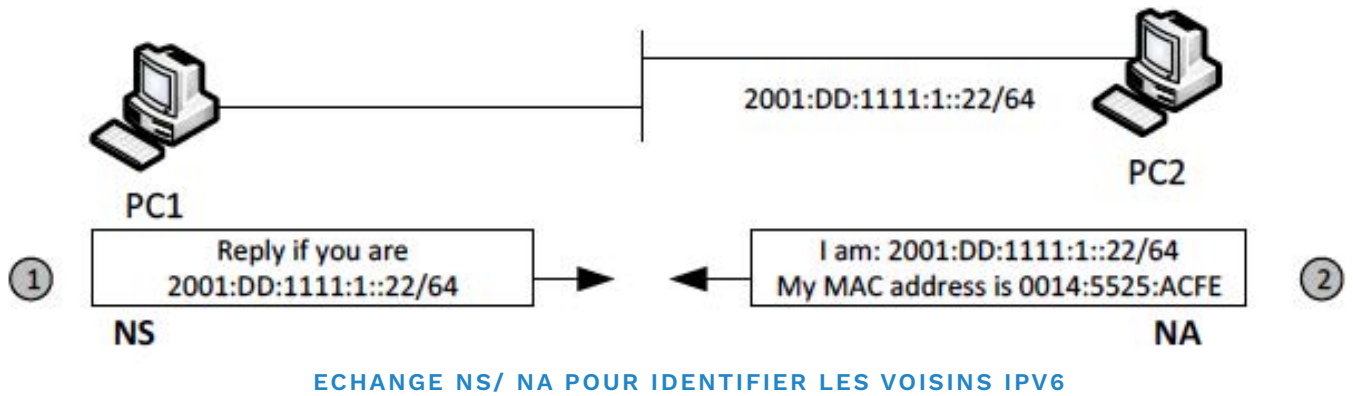
DÉCOUVERTE DES VOISINS IPV6 AVEC NDP:

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

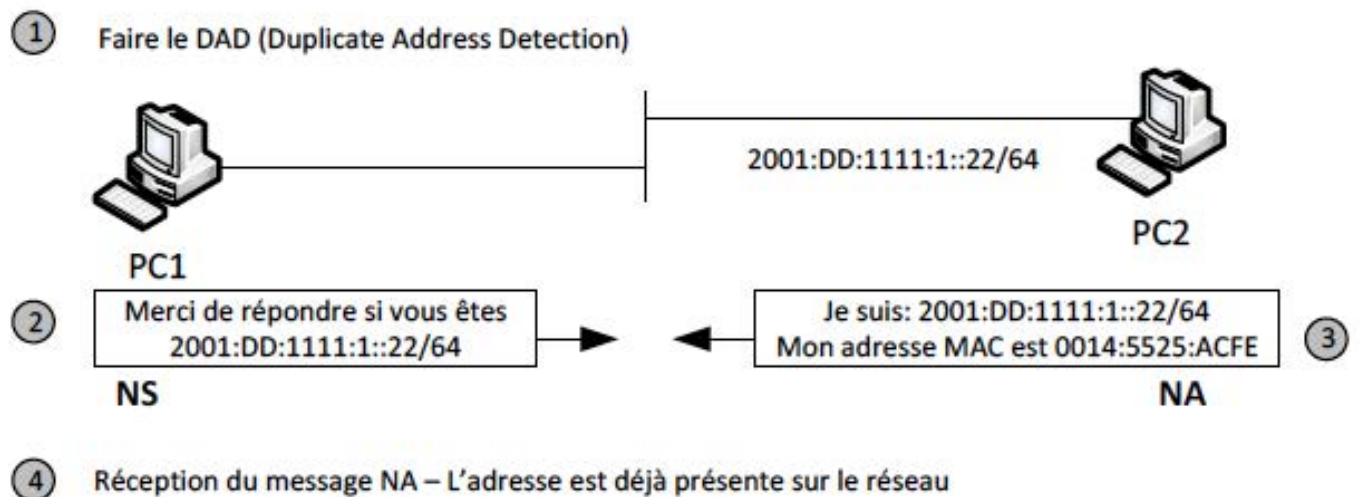
NEIGHBOR SOLICITATION (NS): Requête vers Host avec une adresse IPv6 particulière son adresse MAC correspondante. Ce NS utilise une adresse Multicast

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





DÉTECTION D'ADRESSE IPV6 EN DOUBLE



CONFIGURATION D'IPv6 SUR LES HOSTS

PROTOCOLE NDP ET SES FONCTIONNALITÉS:

FONCTION	MESSAGE	QUI ENVOI LE MESSAGE	QUI REPOND 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	RS et RA	Tout Host IPv6	Tout Host IPv6	Adresse de la couche liaison de données (adresse MAC)
Duplicate Address Dedection	RS et RA	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

Prefix (précisé par le routeur)	Interface ID (choisi par le Host)
--	--

CONSTRUCTION DE L'ADRESSE IPV6 AVEC SLAAC

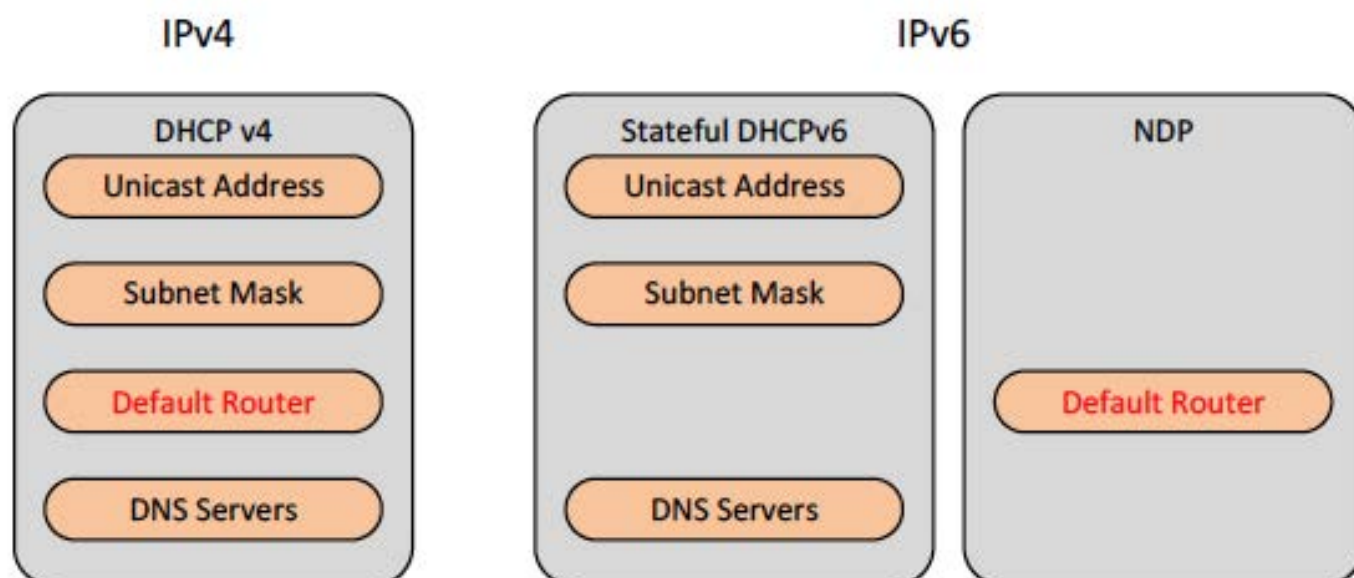
FONCTIONNALITÉS	STATEFUL DHCP	STATELESS DHCP
Conserve les informations sur les adresses IPv6 des clients (état, bail...)	oui	non
Bail envoyé au client	oui	non
Fournit la liste des serveurs DNS	oui	oui
Utilisé généralement avec SLAAC	non	oui

COMPARAISON ENTRE LES SERVICES STATELESS ET STATEFUL DHCPV6

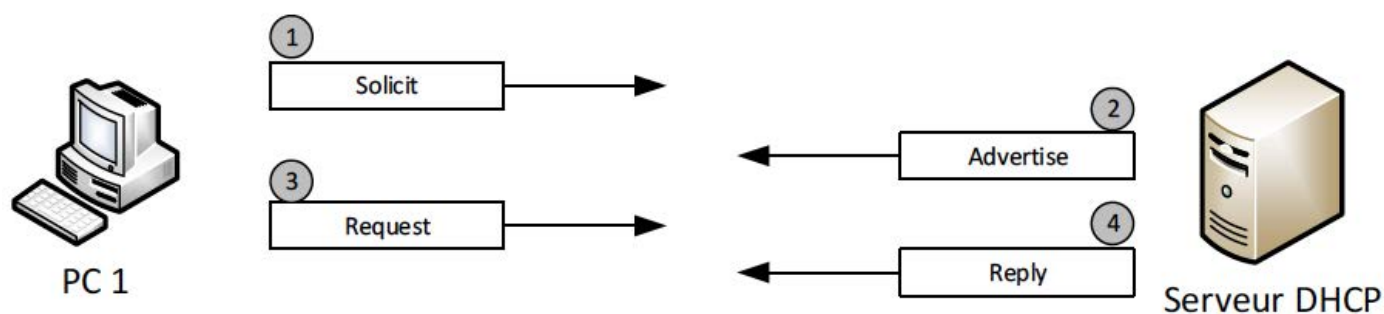
IPv6 DHCP À L'AIDE DE DHCP STATEFUL ET NDP

DHCPv6 fonctionne comme DHCPv4 de ces façons :

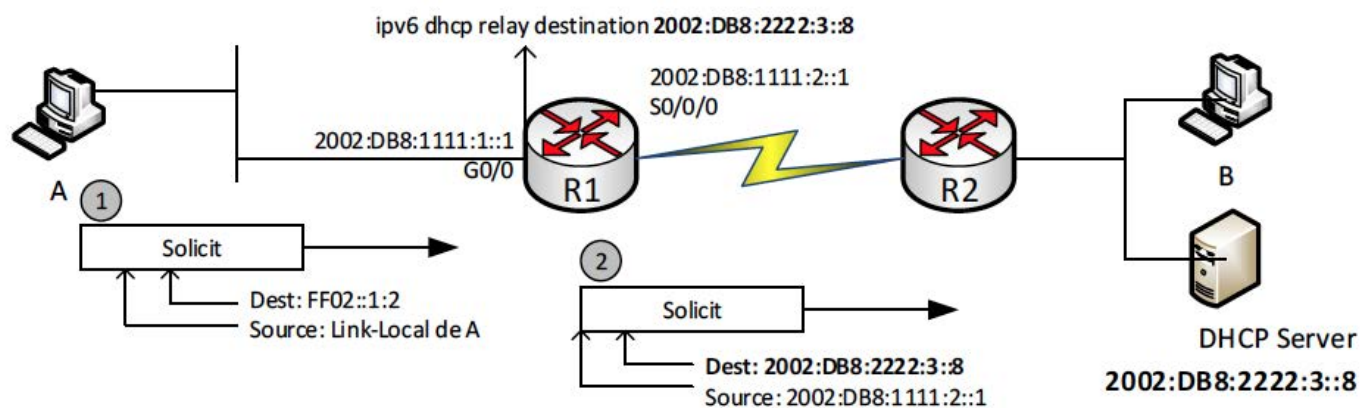
- Le client DHCP envoie sur le LAN un message pour identifier un serveur DHCP
- Si le client et le serveur DHCP sont sur le même LAN alors ils s'échangent les messages directement entre eux
- Si le serveur DHCP est sur un LAN différent, un routeur doit transmettre les messages entre le client et le serveur DHCP
- Le routeur doit alors être configuré pour **relayer** les messages DHCP, il a besoin pour cela de connaître l'adresse IPv6 du serveur DHCP
- Les serveurs ont une configuration qui répertorie les adresses pools pour chaque sous-réseau
- Le serveur DHCP a une plage d'adresse pool 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



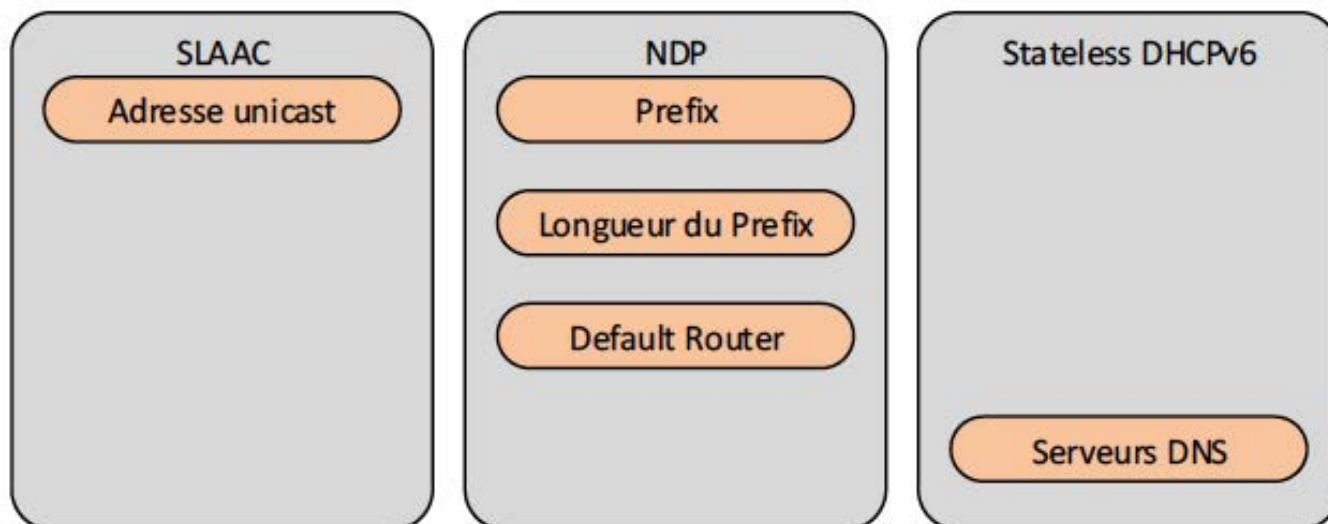
MESSAGES DHCPV6 STATEFUL ENTRE UN CLIENT ET UN SERVEUR DHCP



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
```

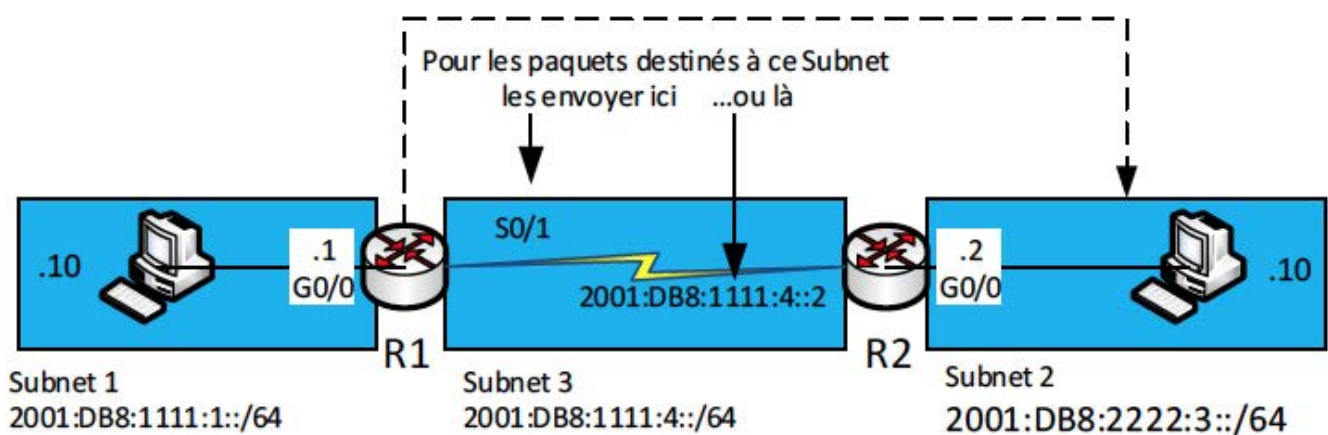
PROTOCOLES DE ROUTAGE ET VERSIONS

	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 actif 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 Neighbors OSPF (voisins), 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'IPv6 SUR LES HOSTS

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

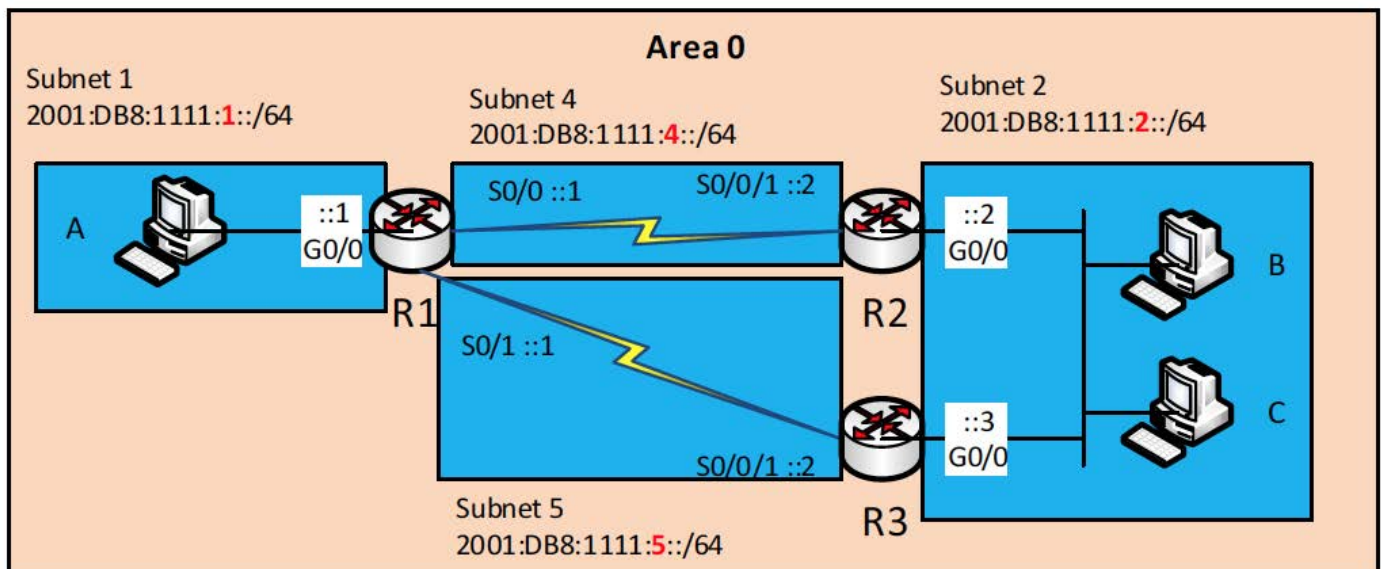
NOTE:

La valeur du router 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 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
```

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#
```



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

COMMANDE SHOW 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
Routes apprises par OSPF	show ip ospf neighbor	show ipv6 ospf neighbor
Résumé de la base de données	show ip ospf database	show ipv6 ospf database

FIN DES FICHES RÉSUMÉ



Et après ?

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 !

REUSSIRSONCCNA.FR