



# Chapitres 6 & 8: La couche réseau

## Adressage IP



## Initiation aux réseaux

Cisco | Networking Academy®  
Mind Wide Open™



# Chapitre 6 : Les objectifs

Les étudiants seront capables de :

- Expliquer comment les protocoles et services de couche réseau prennent en charge les communications sur les réseaux de données
- Expliquer en quoi les routeurs permettent une connectivité de bout en bout dans un réseau de PME
- Déterminer le périphérique approprié pour acheminer le trafic dans un réseau de PME
- Effectuer la configuration de base d'un routeur



# Chapitre 8: Les objectifs

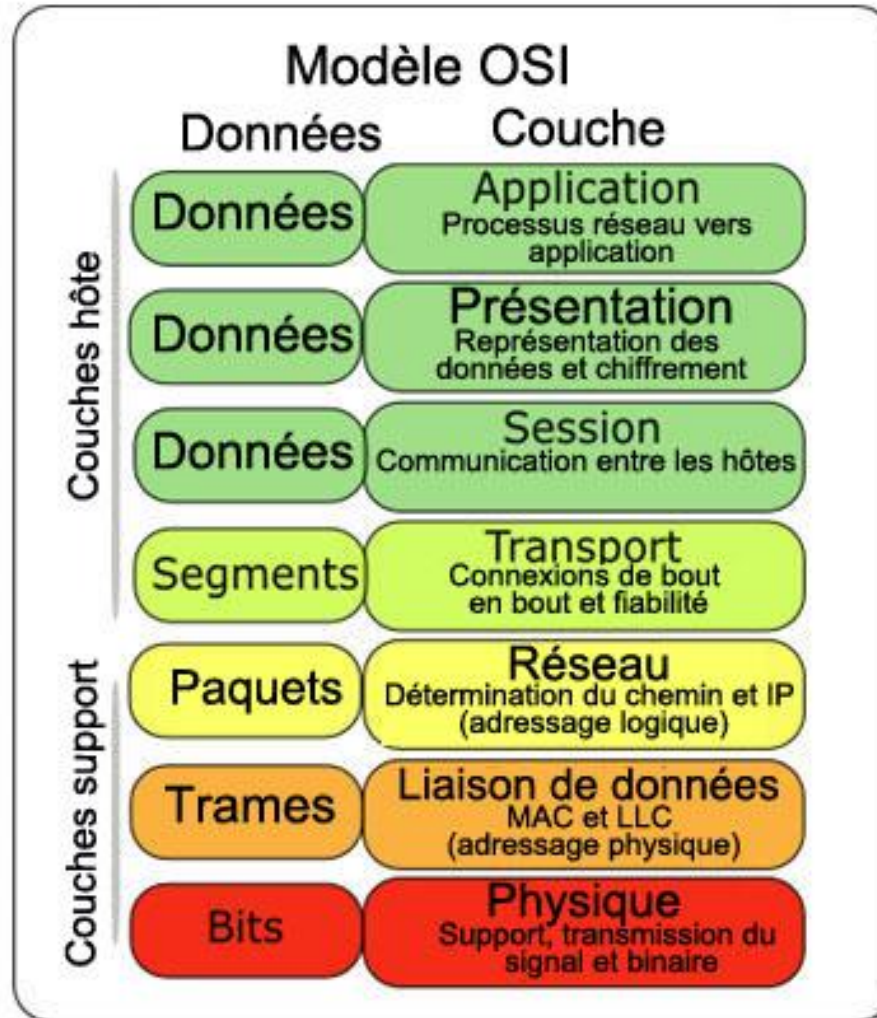
Dans ce chapitre, vous allez apprendre à :

- Décrire la structure d'une adresse IPv4
- Décrire le rôle du masque de sous-réseau
- Comparer les caractéristiques et les utilisations des adresses de monodiffusion (unicast), de diffusion (broadcast) et de multidiffusion (multicast) IPv4
- Expliquer la nécessité de l'adressage IPv6
- Décrire la représentation d'une adresse IPv6
- Décrire les types d'adresses réseau IPv6
- Configurer les adresses de monodiffusion globale
- Décrire les adresses de multidiffusion
- Décrire le rôle du protocole ICMP dans un réseau IP (IPv4 et IPv6)
- Utiliser les utilitaires ping et traceroute pour tester la connectivité réseau



## La couche réseau

# Couche réseau

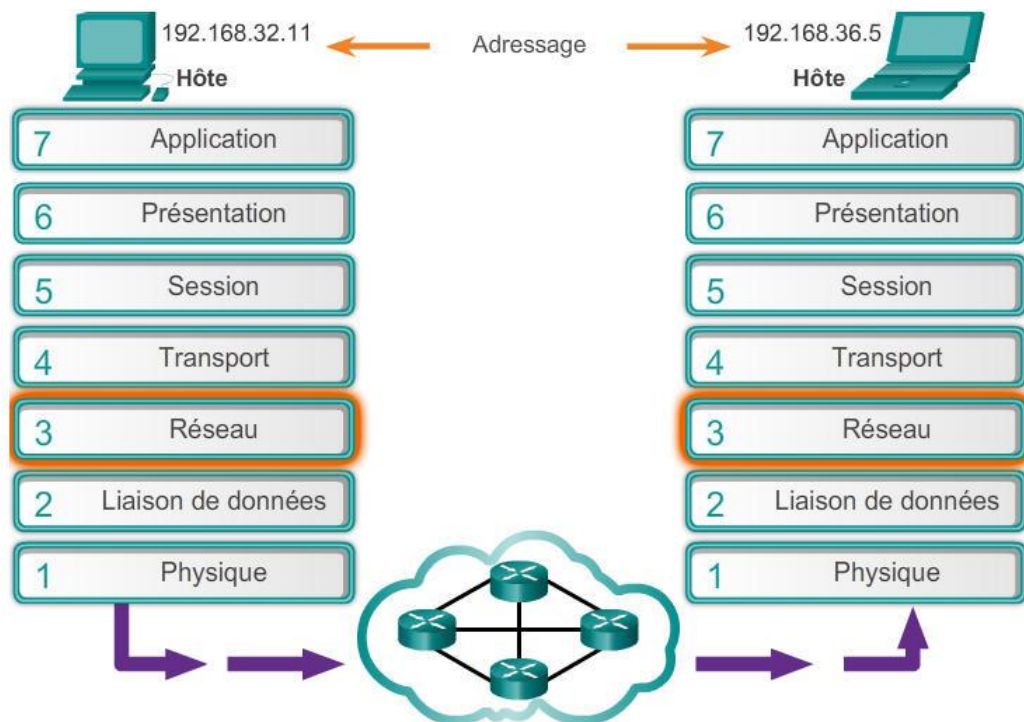


## Les protocoles de couche réseau

# Couche réseau de la communication

Pour effectuer le transport de paquets d'un hôte source à un hôte destination:

- Adressage des périphériques finaux
- Encapsulation
- Routage
- Désencapsulation



Les protocoles de couche réseau transfèrent les unités de données de protocole de la couche transport entre les hôtes.



Couche réseau de la communication

# Les protocoles de couche réseau

Les protocoles de couche réseau courants

- **Le protocole IP version 4 (IPv4)**
- **Le protocole IP version 6 (IPv6)**

Les anciens protocoles de couche réseau

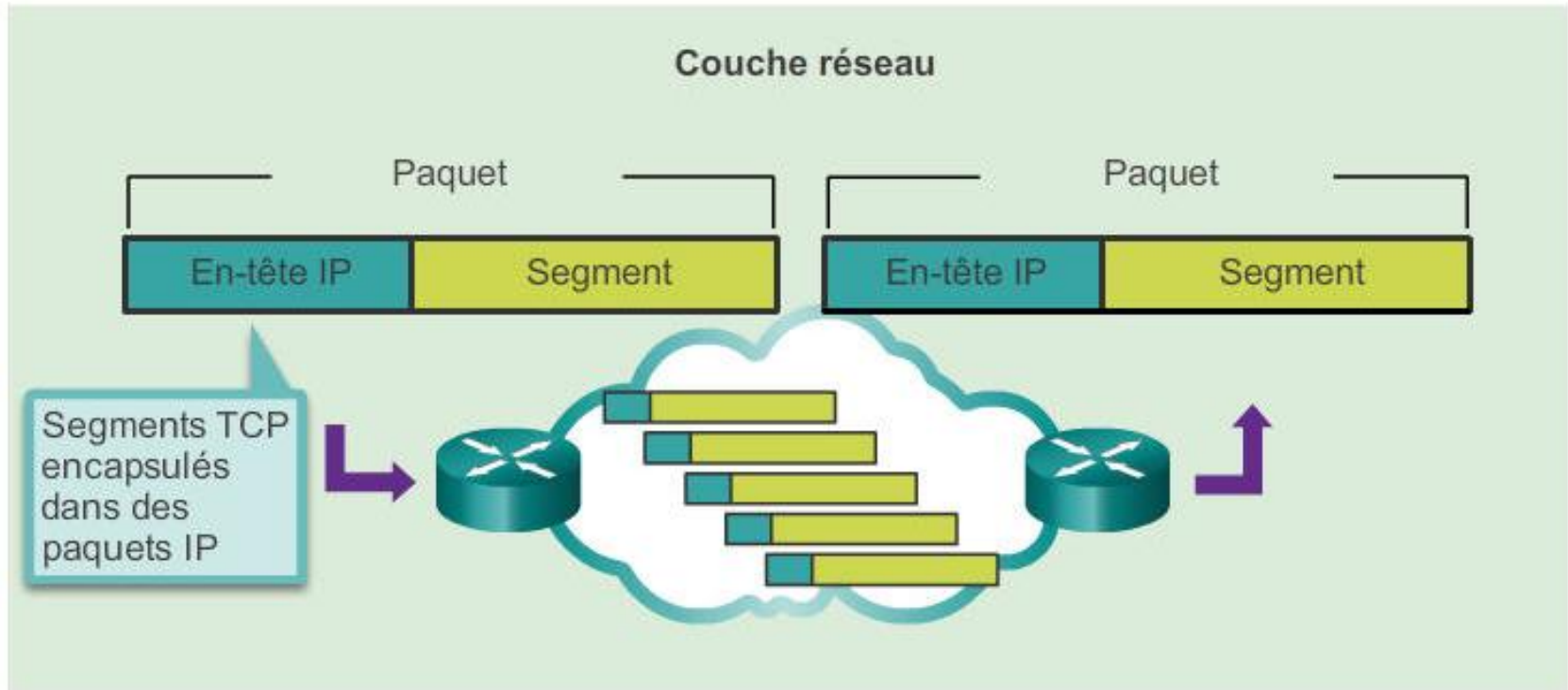
- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)



## Caractéristiques du protocole IP

# Caractéristiques du protocole IP

TCP/IP



Les paquets IP circulent dans l'interréseau.





## Caractéristiques du protocole IP

# IP – Sans connexion

### Communication sans connexion



Une lettre est envoyée.

#### L'expéditeur ne sait pas :

- si le destinataire est présent ;
- si la lettre est arrivée ;
- si le destinataire peut lire la lettre.

#### Le destinataire ne sait pas :

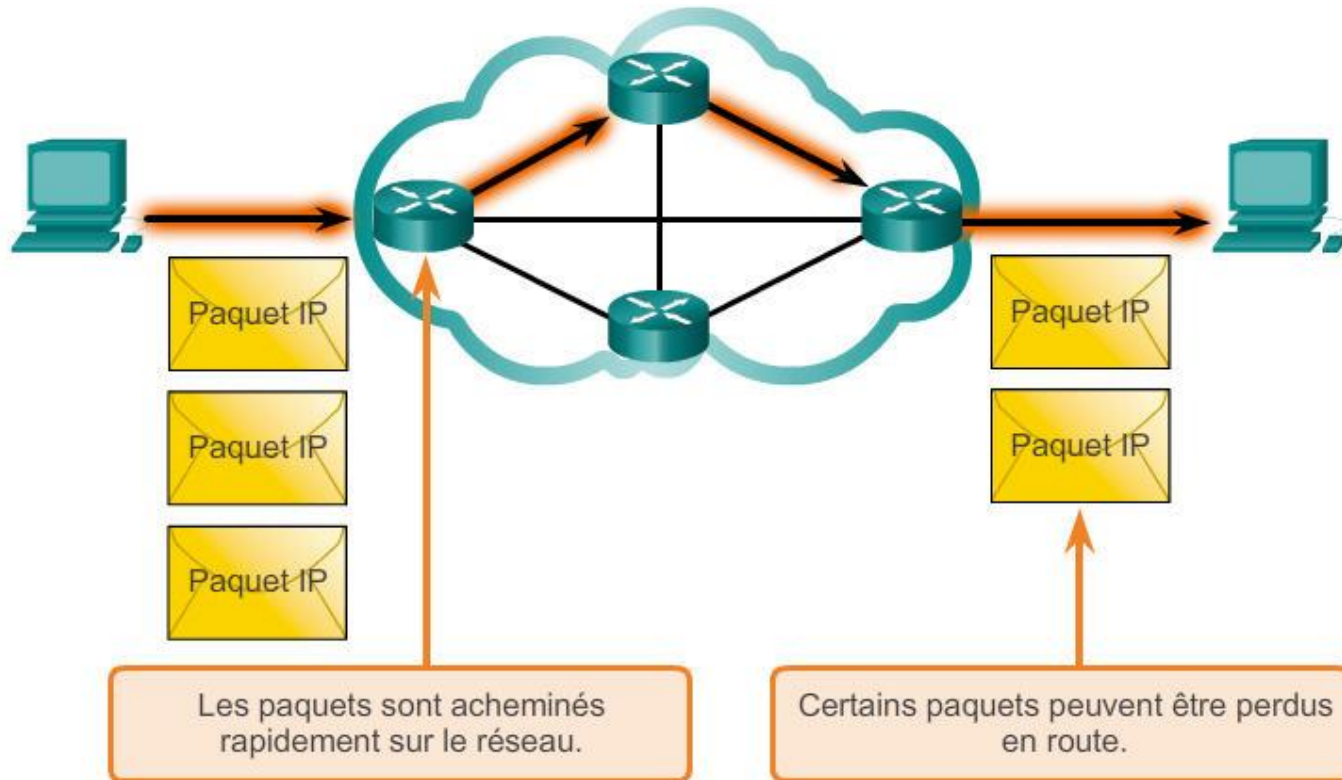
- quand la communication va arriver.





## Caractéristiques du protocole IP

# IP – Acheminement au mieux

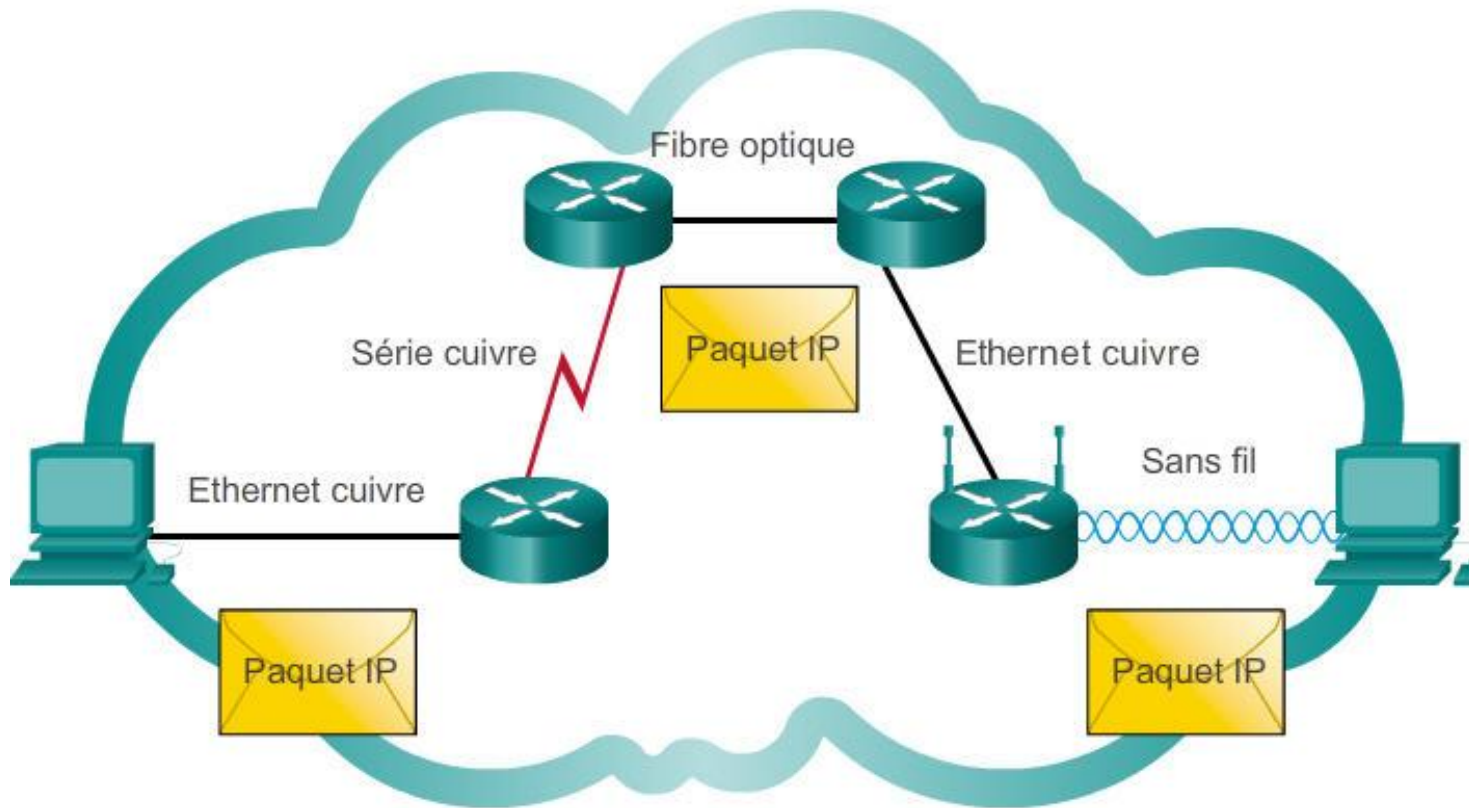


En tant que protocole de couche réseau peu fiable, le protocole IP ne garantit pas que tous les paquets envoyés seront reçus. D'autres protocoles gèrent le processus de suivi des paquets et garantissent leur livraison.



## Caractéristiques du protocole IP

# Indépendance vis-à-vis des supports





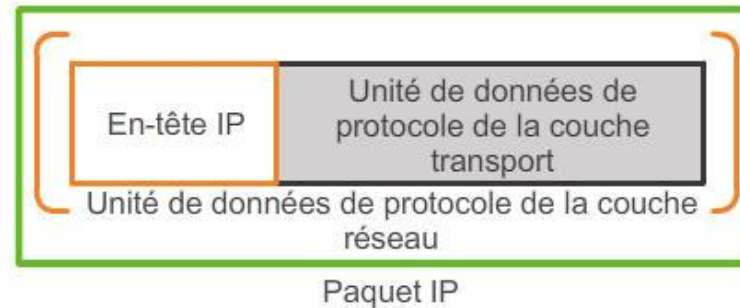
# Paquet IPv4

## Encapsulation IP

Encapsulation de couche transport



Encapsulation de couche réseau

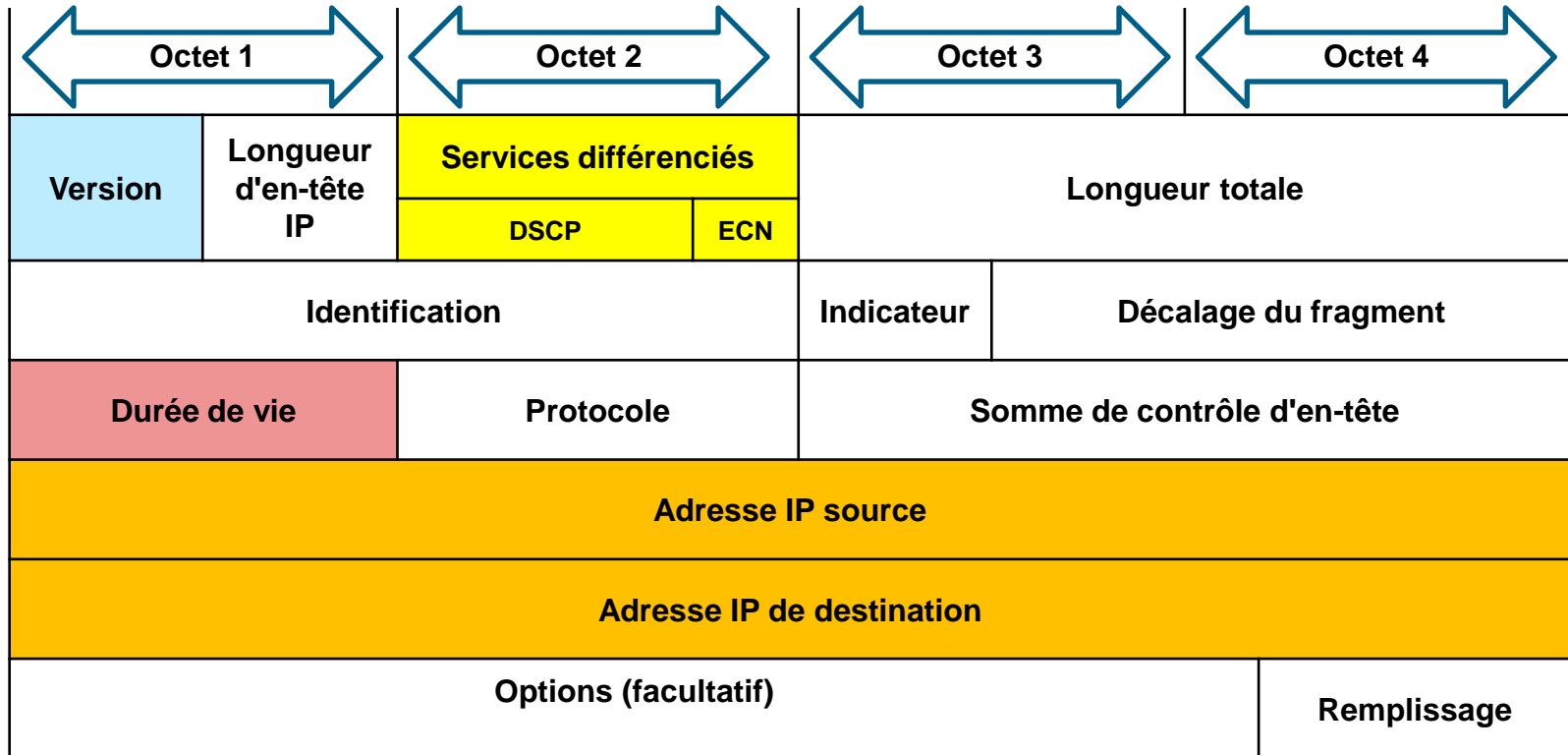


La couche réseau ajoute un en-tête de sorte que les paquets puissent être acheminés via des réseaux complexes et atteindre leur destination. Dans les réseaux TCP/IP, l'unité de données de protocole de couche réseau est le paquet IP.



## Paquet IPv4

# En-tête de paquet IPv4





## Paquet IPv4

# Champs d'en-tête IPv4

- **VERS** : numéro de version de protocole IP, actuellement version 4,
- **HLEN** : longueur de l'en-tête en mots de 32 bits, généralement égal à 5 (pas d'option),
- **Services différenciés** – ancien type de service codé sur 8 bits. Les 6 premiers bits définissent la valeur DCSP (Differentiated Services Code Point) et les 2 derniers bits identifient la valeur de notification explicite de congestion.
- **Longueur totale** : longueur totale du datagramme en octets (en-tête + données)
- **Identification** – ce champ de 16 bits identifie de manière unique le fragment d'un paquet IP d'origine.
- **Indicateurs** – ce champ de 3 bits donne une information sur la fragmentation.
- **Décalage du fragment** – ce champ de 13 bits indique la position du fragment dans le paquet d'origine.



## Paquet IPv4

# Champs d'en-tête IPv4

- **Durée de vie** : codé sur 8 bits. Il est utilisé pour limiter la durée de vie d'un paquet. Les passerelles qui traitent le datagramme doivent décrémenter cette valeur de 1. Lorsque cette valeur atteint 0 (expire) le datagramme est détruit et un message d'erreur est renvoyé à l'émetteur.
- **Protocole**: Ce champ identifie le protocole de niveau supérieur véhiculé dans le champ données du datagramme : TCP:6, UDP:17, ICMP:1
- **Somme de contrôle de l'en-tête** : champ de 16 bits utilisé pour le contrôle des erreurs sur l'en-tête IP.
- **Adresse IP source** – contient une valeur binaire de 32 bits qui représente l'adresse IP source du paquet.
- **Adresse IP de destination** – contient une valeur binaire de 32 bits qui représente l'adresse IP de destination du paquet.



# Paquet IPv4

## Exemples d'en-tête IPv4

Microsoft: \Device\NPF\_{7BB3C130-30C5-4419-B79E-C0868085ABED} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
16	3.64050300	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128
17	3.64506800	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64
18	3.68215500	192.168.1.109	38.112.107.53	TCP	54	55502 > https [ACK] Seq=1 Ack=134 Win=16661 Len=0
19	4.19945400	fe80::15ff:98d8:d28ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
20	4.60748800	fe80::15ff:98d8:d28ff02::c		SSDP	453	HTTP/1.1 200 OK
21	4.64229900	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128
22	4.64509200	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64
23	4.73605200	192.168.1.109	255.255.255.255	DB-LSP	154	Droobox LAN svnc Discoverv Protocol

Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: IntelCor\_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li\_a0:d1:be (00:18:39:a0:d1:be)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1)

Version: 4  
Header length: 20 bytes  
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))  
Total Length: 60  
Identification: 0x3704 (14084)  
Flags: 0x00  
Fragment offset: 0  
Time to live: 128  
Protocol: ICMP (1)  
Header checksum: 0x7ffe [correct]  
Source: 192.168.1.109 (192.168.1.109)  
Destination: 192.168.1.1 (192.168.1.1)  
[Source GeoIP: Unknown]  
[Destination GeoIP: Unknown]

Internet Control Message Protocol

```

0000  00 18 39 a0 d1 be 24 77 03 45 5d c4 08 00 45 00  ..9...$w .E]...E.
0010  00 3c 37 04 00 00 80 01 7f fe c0 a8 01 6d c0 a8  .<7.....m..
0020  01 01 08 00 4d 56 00 01 00 05 61 62 63 64 65 66  ...MV.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
  
```

Internet Protocol Version 4 (ip), 20 bytes    Packets: 35 Displayed: 35 Marked: 0 Dropped: 0    Profile: Default





## Structure d'une adresse IPv4

### Formats décimal/ binaire d'une adresse IPv4

- Une adresse IPv4 est codée sur 32 bits
- Elle est représentée en format décimal: 4 octets séparés de « . » : 192.168.10.10

192	.	168	.	10	.	10
11000000		10101000		00001010		00001010

192.168.10.10 est une adresse IP attribuée à un ordinateur.

Base	2	2	2	2	2	2	2	2
Exposant	7	6	5	4	3	2	1	0
Valeurs des bits de l'octet	128	64	32	16	8	4	2	1
Adresse binaire	1	1	0	0	0	0	0	0
Valeurs binaires des bits	128	64	0	0	0	0	0	0

Ajouter les valeurs binaires des bits

$$128 + 64 = 192$$



## Structure d'une adresse IPv4

# Conversion d'une adresse décimale en adresse binaire

Convertissez les nombres décimaux en nombres binaires

192.168.10.10

11000000

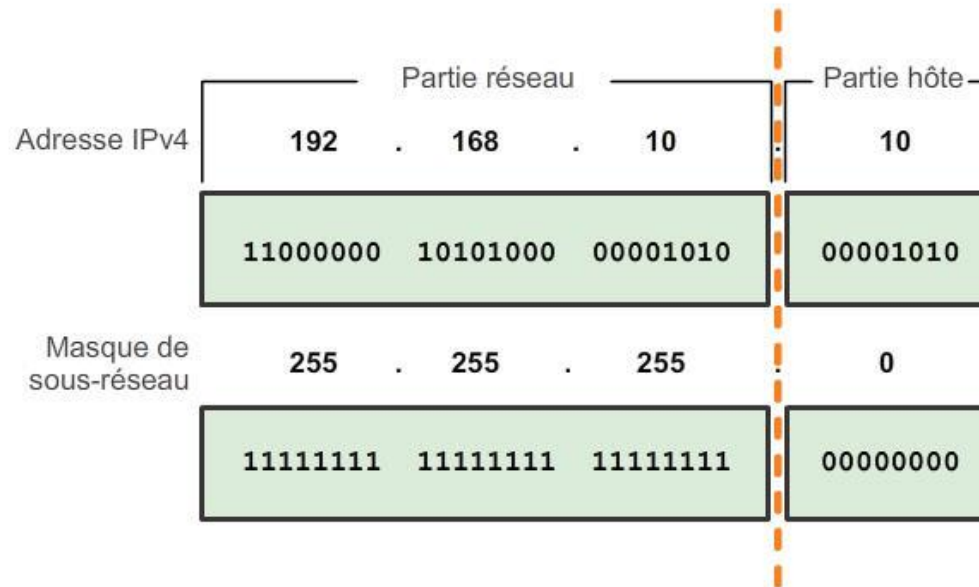
10101000

	128	64	32	16	8	4	2	1
168 > 128, placez un 1 à la position 128.	1							
-128 moins 128								
40 < 64, placez un 0 à la position 64.	1	0						
Ne pas soustraire								
40 > 32, placez un 1 à la position 32.	1	0	1					
-32 moins 32								
8 < 16, placez un 0 à la position 16.	1	0	1	0				
Ne pas soustraire								
8 = 8, placez un 1 à la position 8.	1	0	1	0	1			
Soustraire 8								
0 placez un 0 dans toutes les positions restantes.								
Terminé. Résultats	1	0	1	0	1	0	0	0



## Le masque de sous-réseau IPv4

### La partie réseau et la partie hôte d'une adresse IPv4



- Pour définir les parties réseau et hôte d'une adresse, les périphériques utilisent un modèle 32 bits distinct appelé masque de sous-réseau
- Le masque de sous-réseau ne contient pas réellement le réseau ou la partie hôte d'une adresse IPv4 ; il indique simplement où rechercher ces parties dans une adresse IPv4 donnée



# Les types d'adresses IPv4

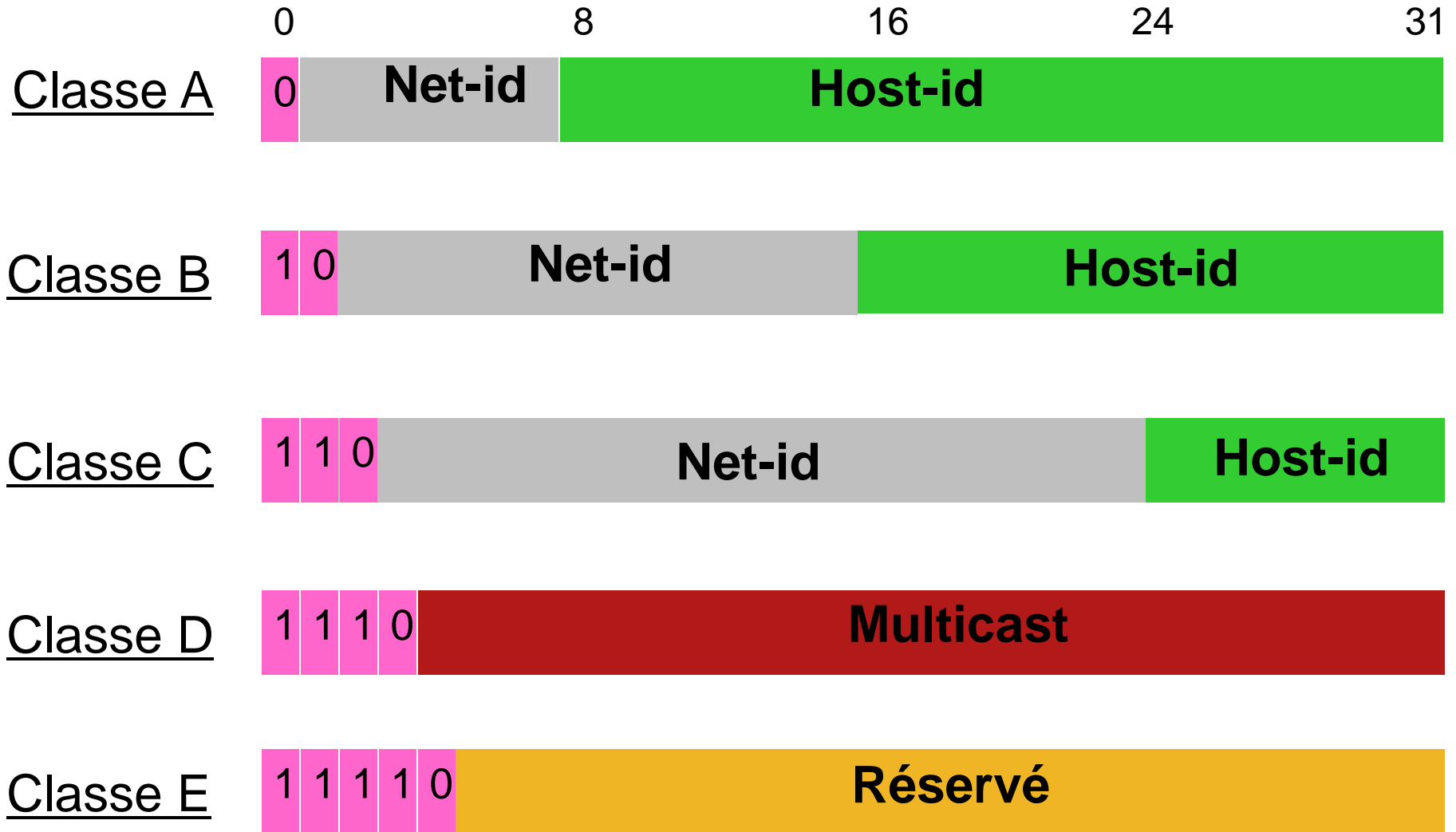
- Adresse réseau : bits de la partie hôte mis à 0 (192.168.10.0)
- Adresse machine: bits de la partie hôte non tous à 0, non tous à 1 (192.168.10.1 à 192.168.10.254)
- Adresse diffusion: correspond à tous les hôtes du réseau. bits de la partie hôte tous à 1 (192.168.10.255)

Adresse IPv4	192	.	168	.	10	.	10
	11000000		10101000		00001010		00001010
Masque de sous-réseau	255	.	255	.	255	.	0
	11111111		11111111		11111111		00000000
Adresse réseau	192	.	168	.	10	.	0
	11000000		10101000		00001010		00000000



# Les types d'adresses IPv4

## Adressage par classe





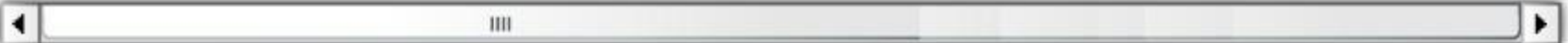
# Les types d'adresses IPv4

## Adressage par classe

### Les classes d'adresses IP

Classe de l'adresse	Plage du premier octet (décimal)	Bits du premier octet (les bits en vert ne changent pas)	Parties réseau (N) et hôte (H) de l'adresse	Masque de sous-réseau par défaut (décimal et binaire)	Nombre de réseaux et d'hôtes possibles par réseau
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128réseaux ( $2^7$ ) 16777214hôtes par réseau ( $2^{24}-2$ )
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16384réseaux ( $2^{14}$ ) 65534hôtes par réseau ( $2^{16}-2$ )
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2097150réseaux ( $2^{21}$ ) 254hôtes par réseau ( $2^8-2$ )
D	224-239	11100000-11101111	ND (multidiffusion)		
E	240-255	11110000-1111 1111	ND (expérimental)		

**Remarque:** les adresses contenant uniquement des zéros (0) et des uns (1) ne sont pas des adresses d'hôte valides.





## Le masque de sous-réseau IPv4

# Longueur du préfixe

- La longueur de préfixe est une autre façon d'exprimer le masque de sous-réseau.
- La longueur de préfixe correspond au nombre de bits définis sur 1 dans le masque de sous-réseau
- Par exemple, si le masque de sous-réseau est 255.255.255.0, la longueur du préfixe est donc de 24 bits, soit /24

## Adressage sans classe

- Un nouvel ensemble de normes a été créé pour permettre aux fournisseurs de services d'allouer les adresses IPv4 sur n'importe quelle limite binaire (longueur de préfixe) plutôt que seulement avec une adresse de classe A, B ou C.
- Le nom officiel est Routage interdomaine sans classe (CIDR, Classless Inter-Domain Routing)





## Le masque de sous-réseau IPv4

# Examen de la longueur du préfixe

Décimale à point		Bits significatifs affichés en binaire
<b>Adresse réseau</b>	<b>10.1.1.0/24</b>	<b>10.1.1.00000000</b>
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.254	10.1.1.11111110
Adresse de diffusion	10.1.1.255	10.1.1.11111111
Nombre d'hôtes: $2^8 - 2 = 254$ hôtes		

<b>Adresse réseau</b>	<b>10.1.1.0/25</b>	<b>10.1.1.00000000</b>
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.126	10.1.1.01111110
Adresse de diffusion	10.1.1.127	10.1.1.01111111
Nombre d'hôtes: $2^7 - 2 = 126$ hôtes		

<b>Adresse réseau</b>	<b>10.1.1.0/26</b>	<b>10.1.1.00000000</b>
Première adresse d'hôte	10.1.1.1	10.1.1.00000001
Dernière adresse d'hôte	10.1.1.62	10.1.1.00111110
Adresse de diffusion	10.1.1.63	10.1.1.00111111
Nombre d'hôtes: $2^6 - 2 = 62$ hôtes		

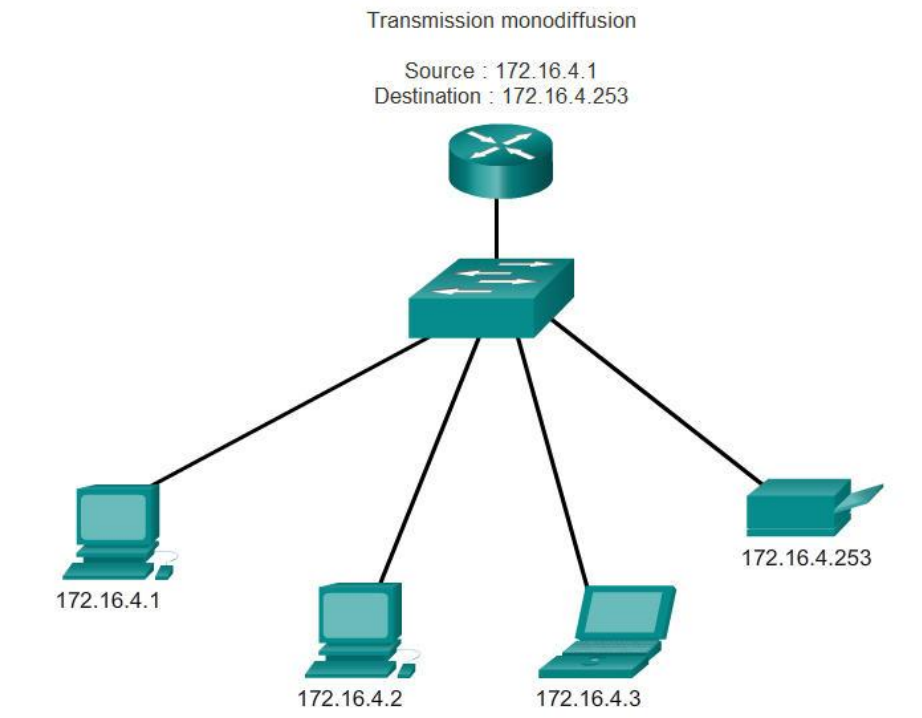


Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

## Transmission en monodiffusion

Dans un réseau IPv4, les hôtes peuvent communiquer de trois façons :

1. **Monodiffusion (unicast)** : consiste à envoyer un paquet d'un hôte à un autre



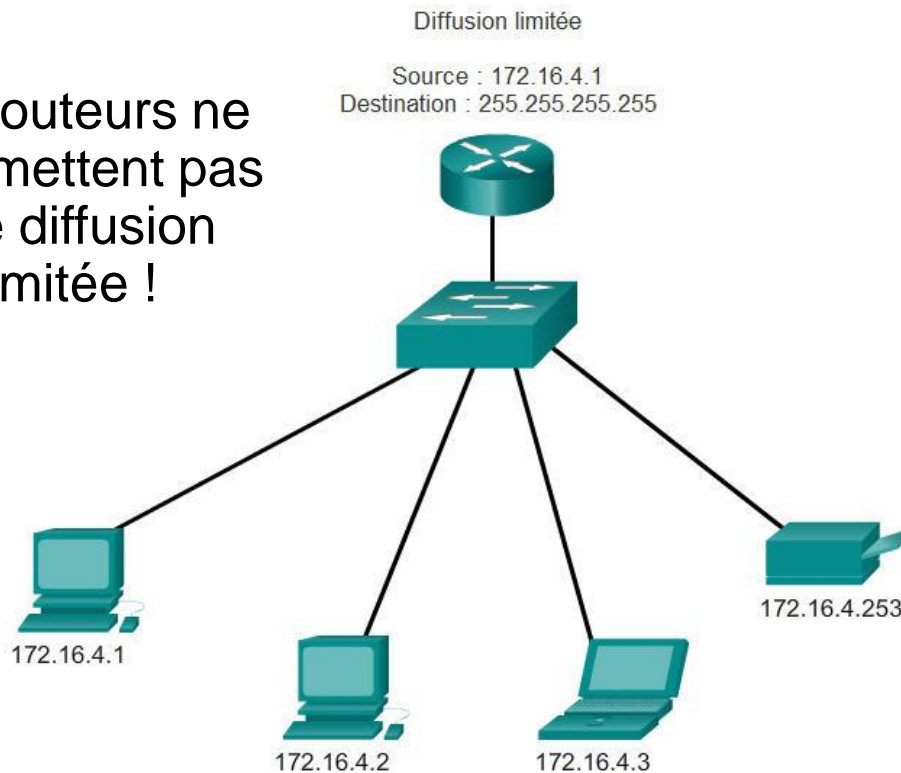


Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

# Transmission en diffusion

**2. Diffusion (broadcast) :** consiste à envoyer un paquet d'un hôte à tous les hôtes du réseau

Les routeurs ne transmettent pas une diffusion limitée !



Diffusion dirigée

- Destination 172.16.4.255
- Hôtes situés dans le réseau 172.16.4.0/24



Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

# Transmission en multidiffusion

- **Multidiffusion (multicast)** : consiste à envoyer un paquet d'un hôte à un groupe d'hôtes en particulier, même situés dans des réseaux différents
- Réduit le trafic
- Réservé à l'adressage à des groupes de multidiffusion - de 224.0.0.0 à 239.255.255.255
- link-local : de 224.0.0.0 à 224.0.0.255 (exemple : informations de routage échangées par les protocoles de routage)
- Adresses d'une étendue globale : de 224.0.1.0 à 238.255.255.255 (exemple : 224.0.1.1 a été réservée au protocole NTP)



## Les types d'adresses IPv4

# Les adresses IPv4 réservées

- **Adresses réseau et de diffusion** : dans chaque réseau, les première et dernière adresses ne peuvent pas être attribuées à des hôtes
- **Adresse de bouclage** : 127.0.0.1 est une adresse spéciale utilisée par les hôtes pour diriger le trafic vers eux-mêmes (les adresses de 127.0.0.0 à 127.255.255.255 sont réservées)
- **Adresse link-local** : les adresses de 169.254.0.0 à 169.254.255.255 (169.254.0.0/16) peuvent être automatiquement attribuées à l'hôte local
- **Adresses TEST-NET** : les adresses de 192.0.2.0 à 192.0.2.255 (192.0.2.0/24) sont réservées à des fins pédagogiques et utilisées dans la documentation et dans des exemples de réseau
- **Adresses expérimentales** : les adresses de 240.0.0.0 à 255.255.255.254 sont indiquées comme étant réservées



## Les types d'adresses IPv4

# Les adresses IPv4 publiques et privées

## Blocs d'adresses privées :

- 10.0.0.0 à 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 à 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 à 192.168.255.255 (192.168.0.0/16)
- Les hôtes ayant des adresses privées ne peuvent accéder à Internet que si leurs adresses soient translatées en adresse publique (NAT)

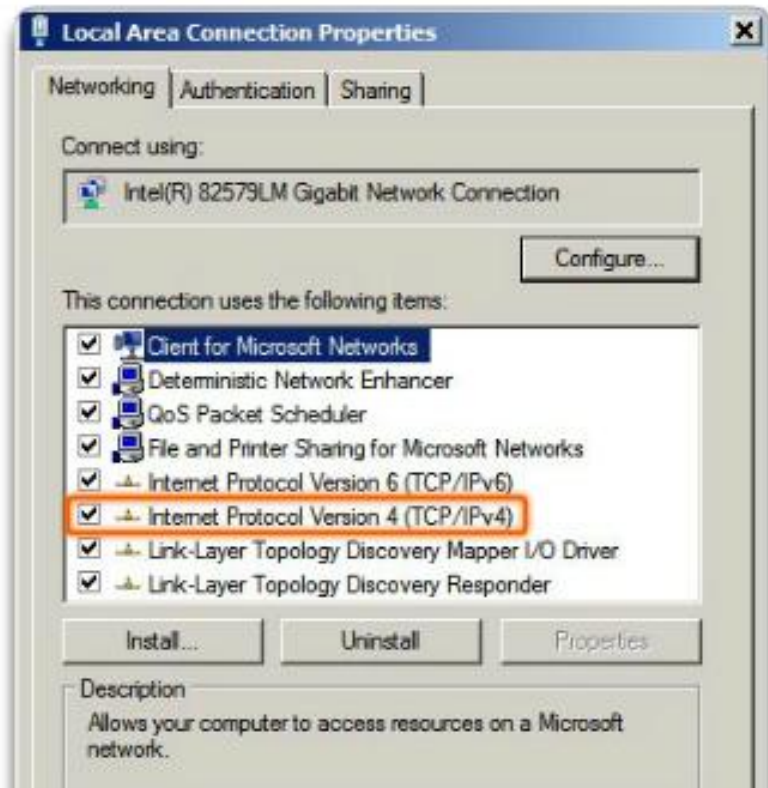




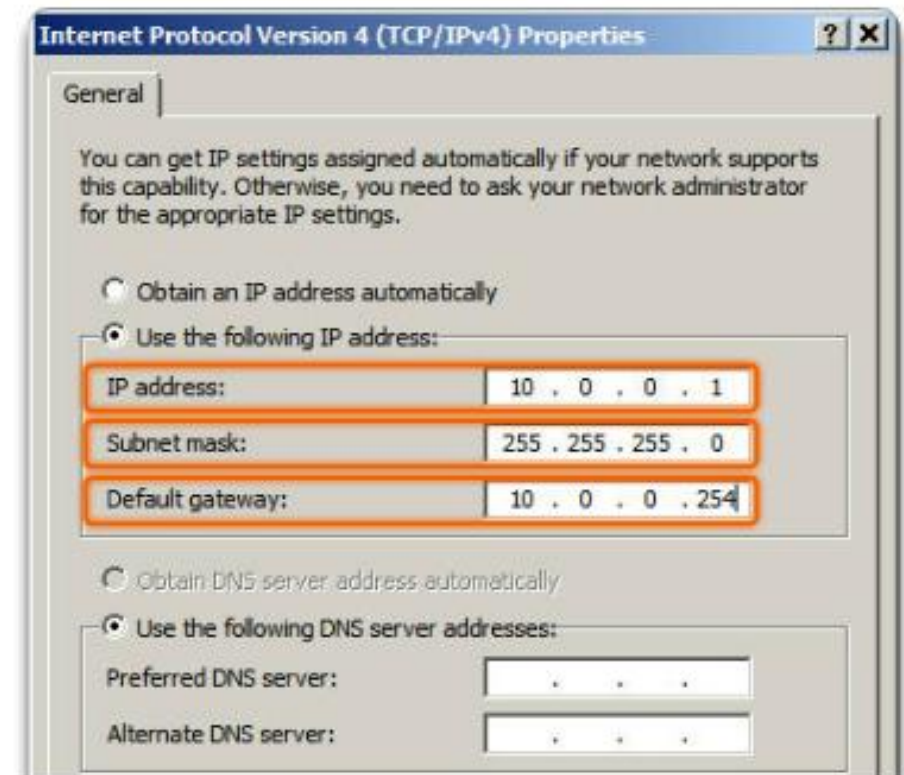
# Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

## Attribution d'une adresse IPv4 statique à un hôte

### Propriétés d'interface LAN



### Configuration d'une adresse IPv4 statique

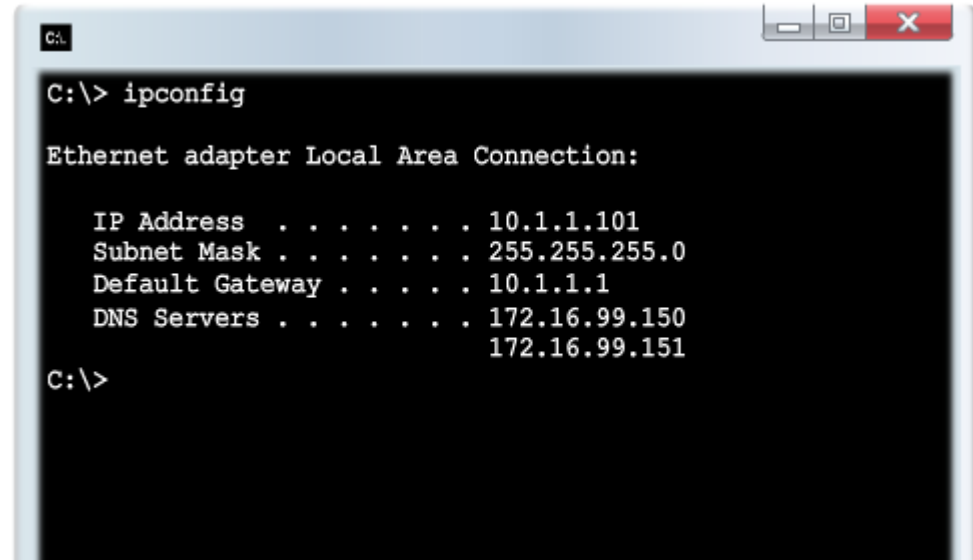
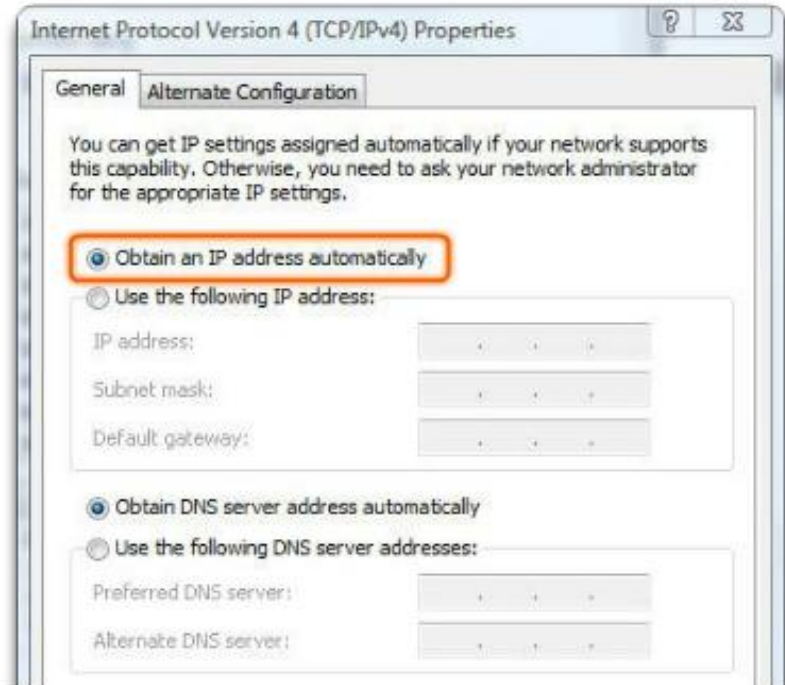






# Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

## Attribution d'une adresse IPv4 dynamique à un hôte



## Vérification

DHCP : méthode privilégiée d'attribution des adresses IPv4 aux hôtes sur les grands réseaux, car elle réduit la charge de travail de l'assistance technique et élimine presque toutes les erreurs d'entrée



Les types d'adresses IPv4

# L'attribution des adresses IP

Les organismes d'enregistrement Internet locaux:





## Couche réseau de la communication

# Limitations de l'IPv4

- Manque d'adresses IP
- Croissance de la table de routage Internet
- Absence de connectivité de bout en bout (NAT)





## Les problèmes liés au protocole IPv4

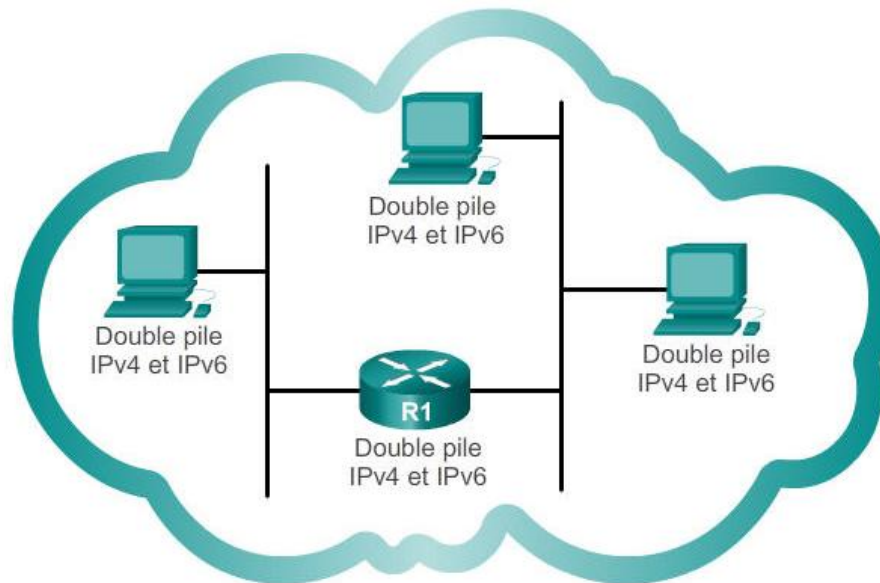
# La nécessité du protocole IPv6

- IPv6 est conçu pour être le successeur d'IPv4
- L'épuisement de l'espace d'adressage IPv4 a motivé la migration vers IPv6 (les cinq organismes d'enregistrement Internet locaux manqueront d'adresses IPv4 entre 2015 et 2020)
- Avec l'utilisation croissante d'Internet, un espace limité d'adresses IPv4, les problèmes liés à la fonction NAT et les objets connectés, le moment est venu d'entamer la transition vers IPv6 !
- L'espace d'adressage IPv6 est de 128 bits, il fournit 340 undécillions d'adresses ( $3,4 \times 10^{38}$ )
- IPv6 élimine les problèmes de limitation d'IPv4 et apporte d'autres améliorations (simplification d'entête, support de la sécurité, auto-configuration, ICMPv6, etc.)

## Les problèmes liés au protocole IPv4

# La coexistence des protocoles IPv4 et IPv6

Les techniques de migration peuvent être classées en trois catégories :



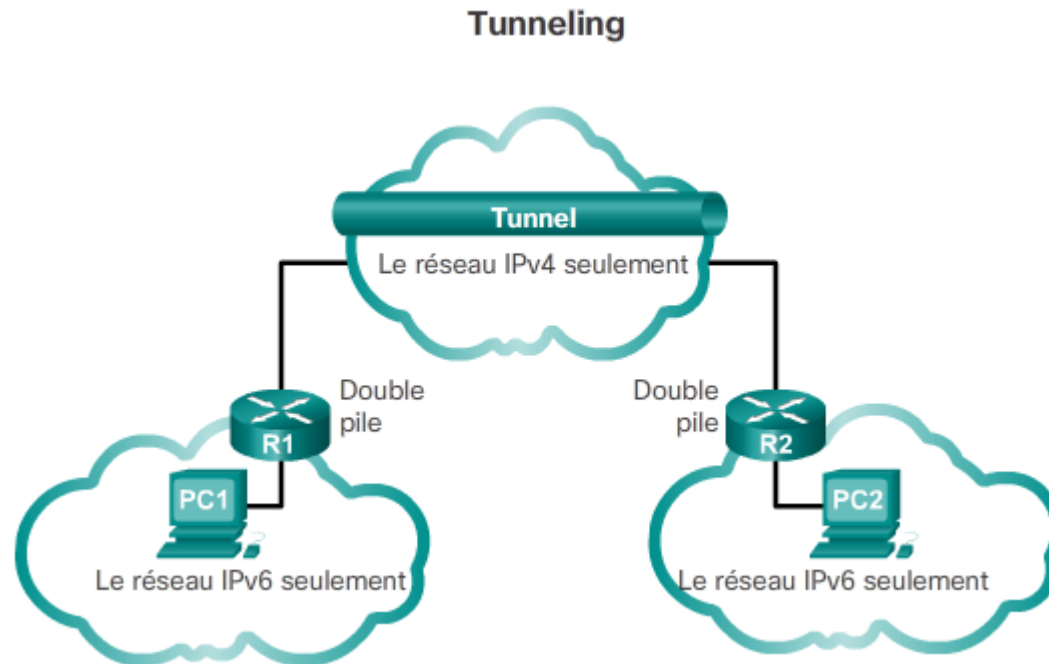
**1. Dual-stack** : permet la coexistence IPv4/IPv6 sur le même réseau. Les périphériques utilisent les deux piles de protocoles, IPv4 et IPv6, en même temps.



Les problèmes liés au protocole IPv4

# La coexistence des protocoles IPv4 et IPv6

Les techniques de migration peuvent être classées en trois catégories :



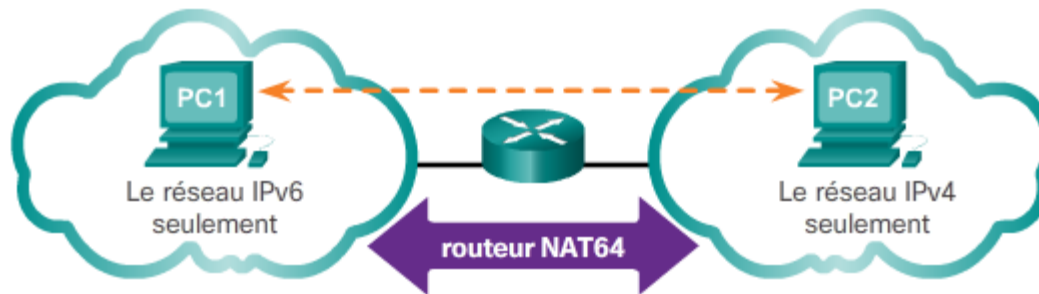
**2. Tunneling** : méthode qui consiste à transporter un paquet IPv6 sur un réseau IPv4 en l'encapsulant dans un paquet IPv4.



Les problèmes liés au protocole IPv4

# La coexistence des protocoles IPv4 et IPv6

Les techniques de migration peuvent être classées en trois catégories :



**3. Traduction :** le NAT64 (Network Address Translation 64) permet aux périphériques IPv6 de communiquer avec des périphériques IPv4 à l'aide d'une technique de traduction analogue au NAT pour IPv4. Un paquet IPv6 est converti en paquet IPv4, et inversement.





# Paquet IPv6

## Encapsulation IPv6

En-tête IPv4

Version	IHL	Type de service	Longueur totale	
Identification			Indicateurs	Décalage du fragment
Time To Live (durée de vie)	Protocole		Somme de contrôle d'en-tête	
Adresse source				
Adresse de destination				
Options				Remplissage

### Légende

- Noms des champs conservés de IPv4 à IPv6
- Nom et position modifiés dans IPv6
- Champs non conservés dans IPv6

En-tête IPv6

Version	Classe de trafic	Étiquetage de flux		
Longueur des données utiles		En-tête suivant	Limite de nombre de sauts	
Adresse IP source				
Adresse IP de destination				

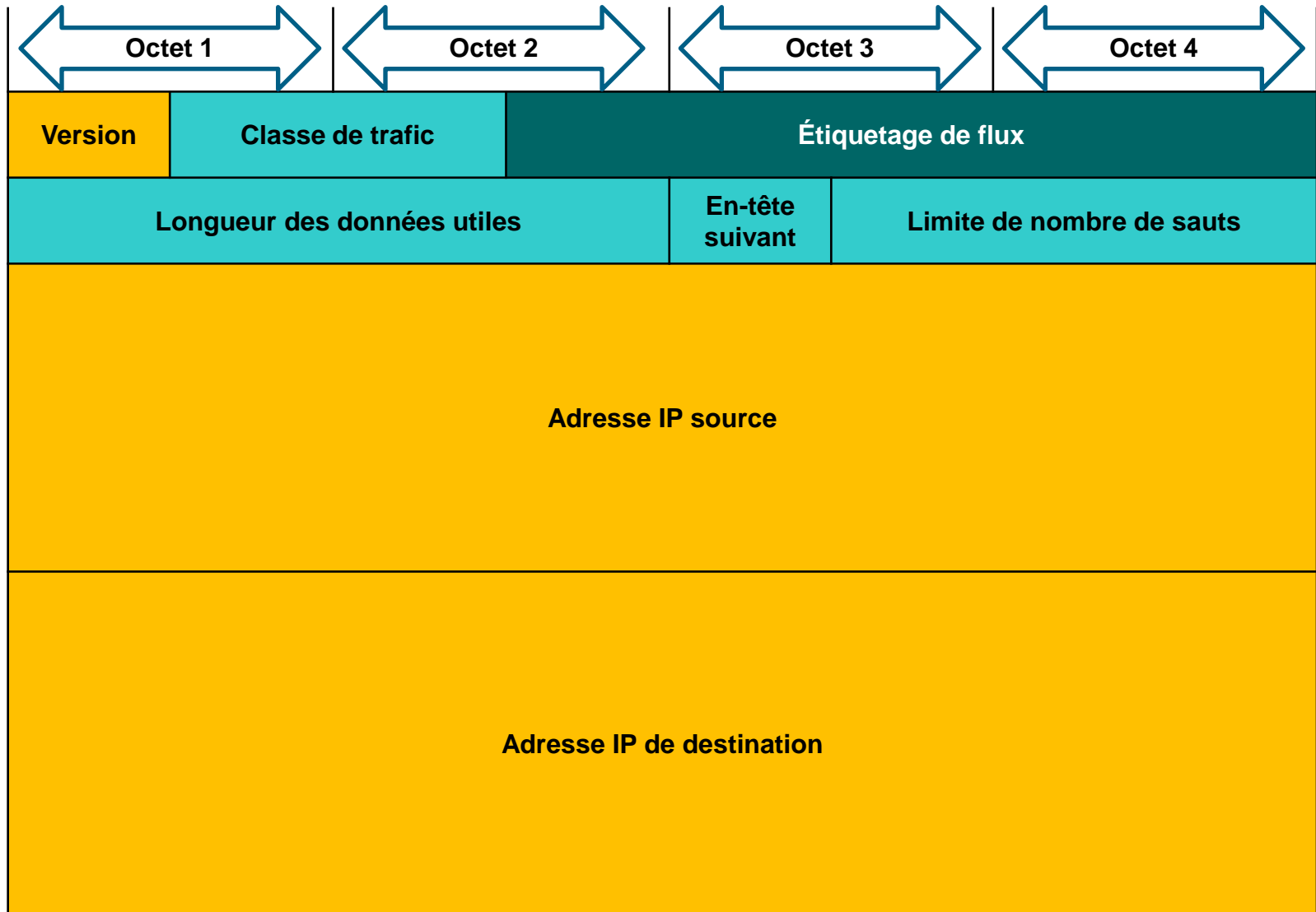
### Légende

- Noms des champs conservés de IPv4 à IPv6
- Nom et position modifiés dans IPv6
- Nouveau champ dans IPv6



## Paquet IPv6

# En-tête de paquet IPv6





## Paquet IPv6

# En-tête de paquet IPv6

- Version: numéro de version sur 4 bits dont la valeur est 6
- Classe de trafic: équivalent au champ TOS ou DiffServ (IPV4), 6 bits utilisés pour classer le paquet (DSCP) et deux bits de notification de congestion
- Etiquette de flux : champ de 20 bits permettant d'identifier divers flux
- Taille datagramme: entier sur 16 bits donnant la longueur en octets du paquet suivant l'en-tête (données utiles)
- Entête Suiv : indicateur sur 8 bits qui identifie le type d'en-tête suivant immédiatement l'en-tête IPv6 (mêmes valeurs que dans IPV4)
- Nbre sauts: entier sur 8 bits qui est décrémenté de 1 à chaque passage dans un routeur. Le paquet est supprimé lorsque sa valeur atteint 0
- Adresse source : adresse sur 128 bits identifiant l'hôte source du paquet
- Adresse destination : adresse sur 128 bits identifiant le destinataire du paquet.



# Paquet IPv6

## Exemple d'en-tête IPv6

Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8) interface showing a packet capture of an IPv6 HTTP GET request.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
47	325.030878	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:9ff:fee3:e8de	TCP	82	59201 > 59201 [SYN, ACK] Seq=0 Ack=1 win=6
48	325.031166	2001:6f8:102d:0:2d0:9ff:fee3:e8de	2001:6f8:900:7c0::2	TCP	74	59201 > 59201 [ACK] Seq=1 Ack=1 win=5760
49	325.040411	2001:6f8:102d:0:2d0:9ff:fee3:e8de	2001:6f8:900:7c0::2	HTTP	314	GET / HTTP/1.0
50	325.045496	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:9ff:fee3:e8de	TCP	1506	[TCP segment of a reassembled PDU]
51	325.045525	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:9ff:fee3:e8de	HTTP	901	HTTP/1.1 200 OK (text/html)
52	325.045627	2001:6f8:900:7c0::2	2001:6f8:102d:0:2d0:9ff:fee3:e8de	TCP	74	59201 > 59201 [FIN, ACK] Seq=2260 Ack=241

**Packet Details (Frame 49):**

- Frame 49: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
- Ethernet II, Src: HsingTec\_e3:e8:de (00:d0:09:e3:e8:de), Dst: Ibm\_82:95:b5 (00:11:25:82:95:b5)
- Internet Protocol Version 6, Src: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de), Dst: 2001:6f8:900:7c0::2 (2001:6f8:900:7c0::2)
  - 0110 .... = Version: 6
  - .... 0000 0000 .... = Traffic class: 0x00000000
  - .... 0000 0000 0000 0000 = Flowlabel: 0x00000000
  - Payload length: 260
  - Next header: TCP (6)
  - Hop limit: 64
  - Source: 2001:6f8:102d:0:2d0:9ff:fee3:e8de (2001:6f8:102d:0:2d0:9ff:fee3:e8de)
  - [Source SA MAC: HsingTec\_e3:e8:de (00:d0:09:e3:e8:de)]
  - Destination: 2001:6f8:900:7c0::2 (2001:6f8:900:7c0::2)
  - [Source GeoIP: Unknown]
  - [Destination GeoIP: Unknown]
- Transmission Control Protocol, Src Port: 59201 (59201), Dst Port: http (80), Seq: 1, Ack: 1, Len: 240
- Hypertext Transfer Protocol

**Packet Bytes:**

Offset	Hex	ASCII
0000	00 11 25 82 95 b5 00 d0 09 e3 e8 de 86 dd 60 00	..%.....
0010	00 00 01 04 06 40 20 01 06 f8 10 2d 00 00 02 d0	.....@.....
0020	09 ff fe e3 e8 de 20 01 06 f8 09 00 07 c0 00 00	.....A.P...a.J
0030	00 00 00 00 00 02 e7 41 00 50 ab dc d6 61 01 4a	S.P....H..GET /
0040	73 9f 50 18 16 80 f4 48 00 00 47 45 54 20 2f 20	HTTP/1.0 ..Host:
0050	48 54 54 50 2f 31 2e 30 0d 0a 48 6f 73 74 3a 20	cl-1985. ham-01.d
0060	63 6c 2d 31 39 38 35 2e 68 61 6d 2d 30 31 2e 64	e.sixxs. net...Acc
0070	65 2e 73 69 78 78 73 2e 6e 65 74 0d 0a 41 63 63	



## L'adressage IPv6

# La représentation des adresses IPv6

- Comportent 128 bits, sous la forme d'une chaîne de valeurs hexadécimales
- Une adresse IPv6 est représentée en 8 mots de 16 bits séparés par « : »
- Dans l'adressage IPv6, 4 bits représentent un seul chiffre hexadécimal, 32 valeurs hexadécimales = adresse IPv6
 

**2001 : 0DB8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200**

**FE80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF**
- Un hextet fait référence à un segment de 16 bits ou quatre hexadécimales
- Peuvent être écrites en minuscules ou en majuscules



## L'adressage IPv6

# Règle n° 1 - Omettre les zéros en début de segment

- Première règle pour réduire les adresses IPv6 : les zéros (0) du début d'une section de 16 bits (ou hextet) peuvent être omis
- 01AB est équivalent à 1AB
- 09F0 est équivalent à 9F0
- 0A00 est équivalent à A00
- 00AB est équivalent à AB

Recommandé	2001:0DB8:000A:1000:0000:0000:0000:0100
Sans zéros en début de segment	2001: DB8: A:1000: 0: 0: 0: 100



## L'adressage IPv6

# Règle n° 2 - Omettre toutes les séquences de zéros

- Une suite de deux deux-points (::) peut remplacer toute chaîne unique et continue d'un ou plusieurs segments de 16 bits (hextets) comprenant uniquement des zéros.
- Cette suite (::) ne peut être utilisée qu'une seule fois dans une adresse, sinon celle-ci devient ambiguë.
- C'est ce qu'on appelle le *format compressé*
- *Exemple: 2001:0DB8:0000:ABCD:0000:0000:0000:1234*
  - Adresse incorrecte – ~~2001:DB8::ABCD::1234~~
  - Adresse correcte – 2001:DB8:0:ABCD::1234





Les types d'adresses IPv6

# Types d'adresses IPv6

Il existe trois types d'adresses IPv6 :

- **Monodiffusion**
- **Multidiffusion**
- **Anycast**

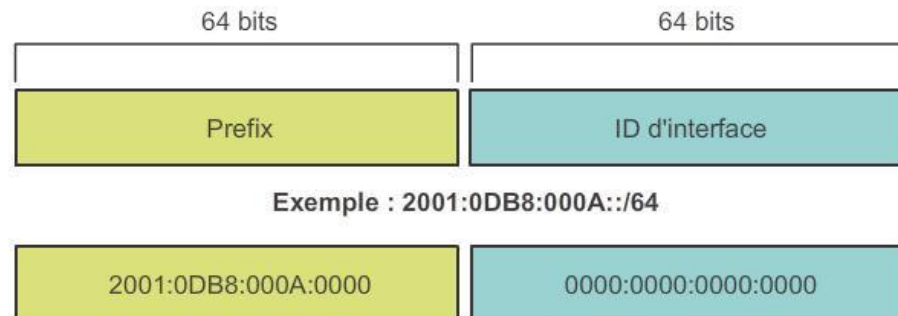
Remarque : IPv6 n'a pas d'adresses de diffusion.



## Les types d'adresses IPv6

# La longueur du préfixe IPv6

- IPv6 n'utilise pas la notation décimale à point du masque de sous-réseau.
- La longueur de préfixe indique la partie réseau d'une adresse IPv6 au format suivant :
  - Adresse IPv6/longueur de préfixe
  - La longueur de préfixe peut aller de 0 à 128
  - La longueur de préfixe est généralement /64



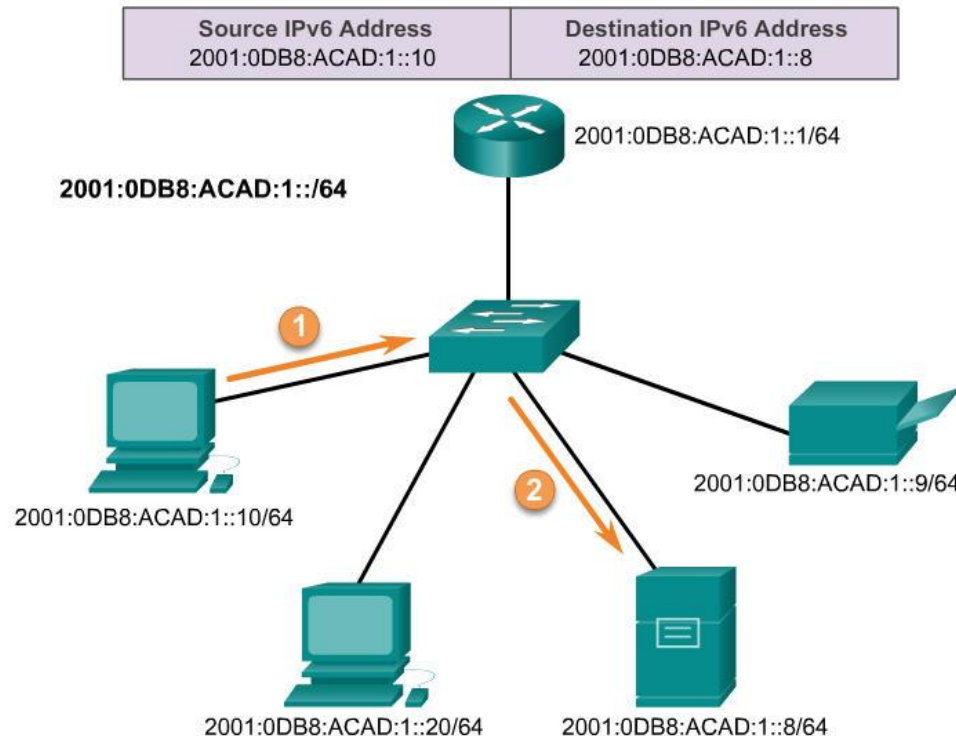


## Les types d'adresses IPv6

# Les adresses IPv6 de monodiffusion

### ■ Monodiffusion

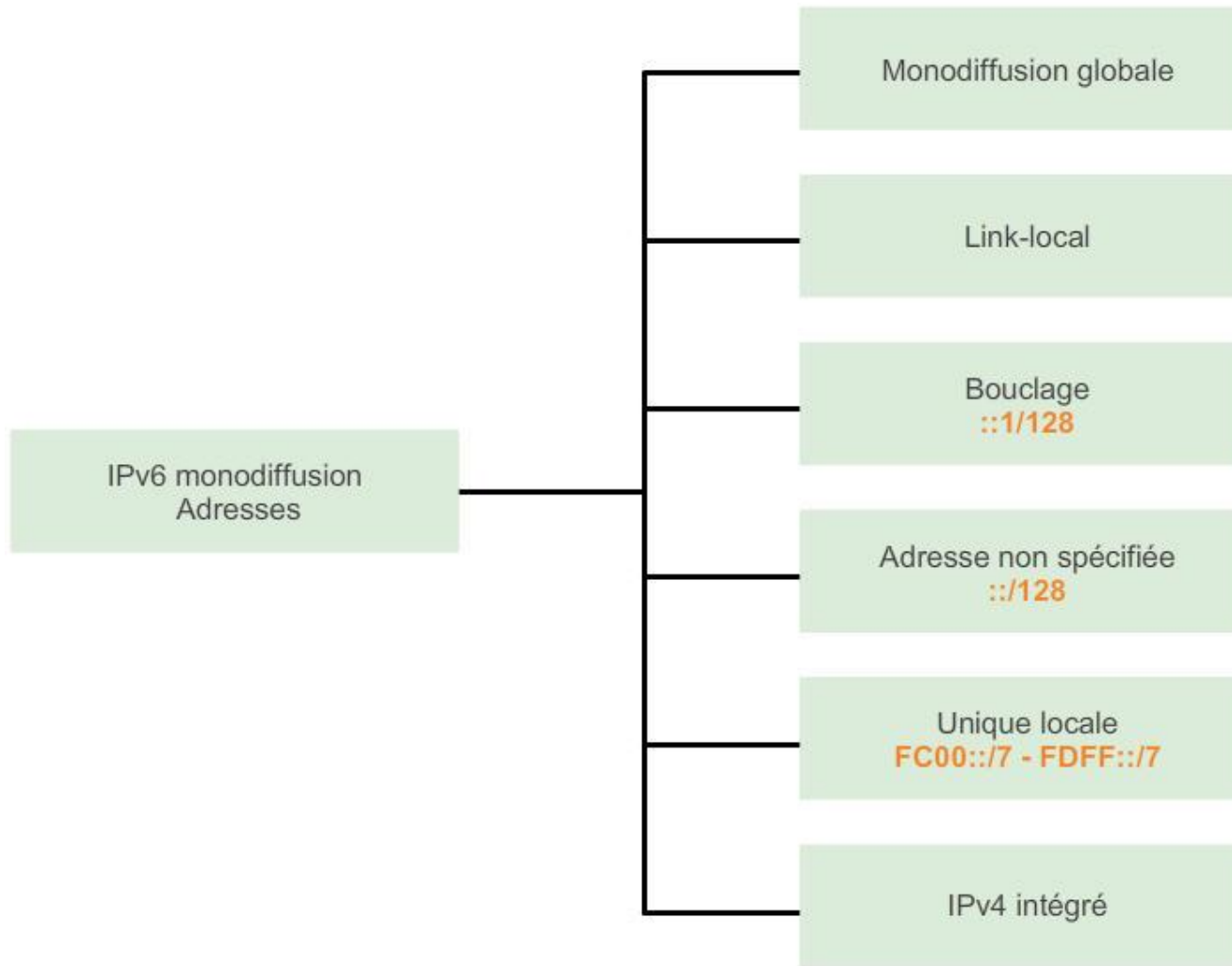
- Identifie de façon unique une interface sur un périphérique IPv6
- Un paquet envoyé à une adresse de monodiffusion est reçu par l'interface correspondant à cette adresse.





## Les types d'adresses IPv6

# Les adresses IPv6 de monodiffusion





## Les types d'adresses IPv6

# Les adresses IPv6 de monodiffusion

### ■ Monodiffusion globale

- Similaire à une adresse IPv4 publique
- Globalement unique
- Adresses routables sur Internet
- Peuvent être configurées statiquement ou dynamiquement

### ■ Link-local

- Pour communiquer avec les autres périphériques sur la même liaison locale (segment Ethernet, liaison PPP)
- Restriction à une seule liaison - non routables au-delà de la liaison



## Les types d'adresses IPv6

# Les adresses IPv6 de monodiffusion

### ■ Envoi en boucle

- Permet à un hôte de s'envoyer un paquet à lui-même ; pas d'attribution à une interface physique
- Envoyez une requête ping à l'adresse de bouclage pour tester la configuration TCP/IP de l'hôte local
- Seulement des 0, sauf pour le dernier bit – adresses avec la syntaxe `::1/128` ou juste `::1`

### ■ Adresse non spécifiée

- Adresse contenant uniquement des 0 – Représentée sous la forme `::/128` ou juste `::`
- Ne peut pas être attribuée à une interface et est utilisée uniquement comme adresse source
- Une adresse non spécifiée est utilisée comme adresse source lorsque le périphérique n'a pas encore d'adresse IPv6 permanente ou lorsque la source du paquet est inappropriée pour la destination



## Les types d'adresses IPv6

# Les adresses IPv6 de monodiffusion

### ■ Adresse locale unique

- Similaire aux adresses privées pour IPv4
- Adresse utilisée pour l'adressage local à l'intérieur d'un site ou entre un nombre limité de sites
- Comprise entre FC00::/7 et FDFF::/7

### ■ IPv4 intégré (non traité dans ce cours)

- Permet de faciliter la transition d'IPv4 vers IPv6

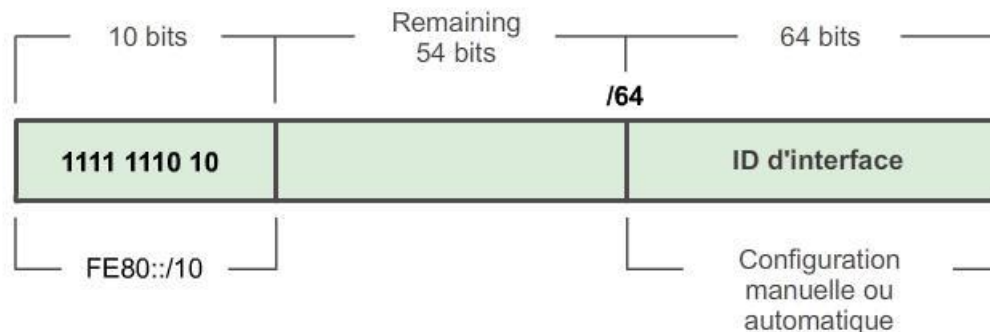




## Les types d'adresses IPv6

# Les adresses de monodiffusion link-local IPv6

- Chaque interface réseau IPv6 DOIT avoir une adresse link-local
- Associée automatiquement à une interface
- Permet à un périphérique de communiquer avec les autres périphériques IPv6 sur la même liaison et seulement sur celle-ci (le sous-réseau)
- Plage FE80::/10, les 10 premiers bits étant 1111 1110 10xx xxxx
- 1111 1110 10**00 0000** (FE80) - 1111 1110 10**11 1111** (FEBF)



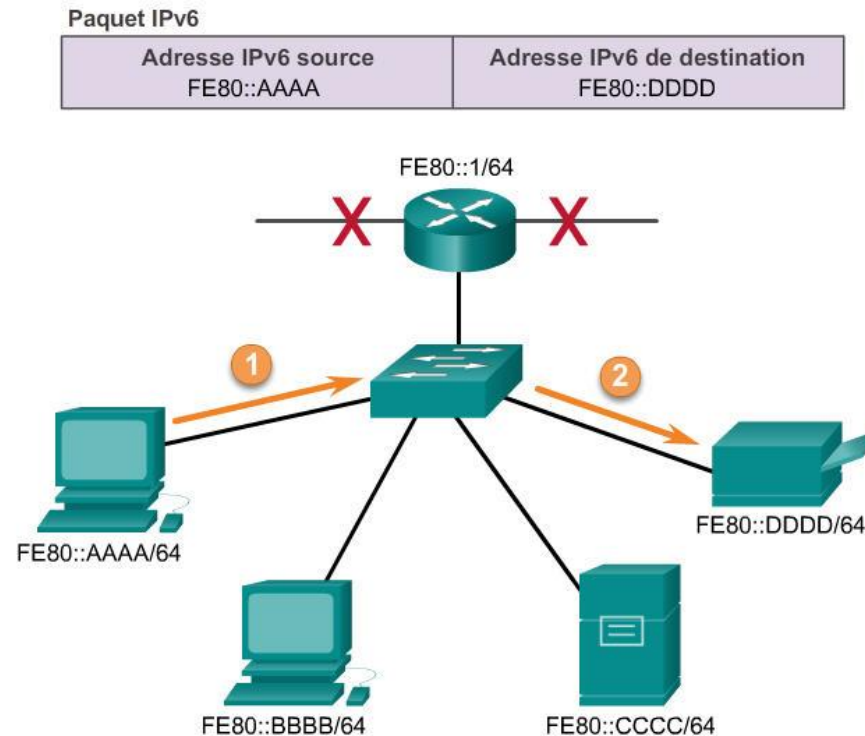


## Les types d'adresses IPv6

# Les adresses de monodiffusion link-local IPv6

- Les paquets associés à une adresse link-local source ou de destination ne peuvent pas être acheminés au-delà de leur liaison d'origine.

Communications link-local IPv6





## Les adresses de monodiffusion IPv6

# Structure d'une adresse de monodiffusion globale IPv6

- Les adresses de monodiffusion (unicast) globale IPv6 sont globalement uniques et routables sur le réseau Internet IPv6
- L'équivalent des adresses IPv4 publiques
- ICANN attribue les blocs d'adresses IPv6 aux cinq organismes d'enregistrement Internet locaux (RIR)
- Actuellement, seules des adresses de monodiffusion globale dont les premiers bits sont 001 ou 2000::



## Les adresses de monodiffusion IPv6

# Structure d'une adresse de monodiffusion globale IPv6

- Actuellement, seules des adresses de monodiffusion globale dont les premiers bits sont 001 ou 2000::/3 sont attribuées

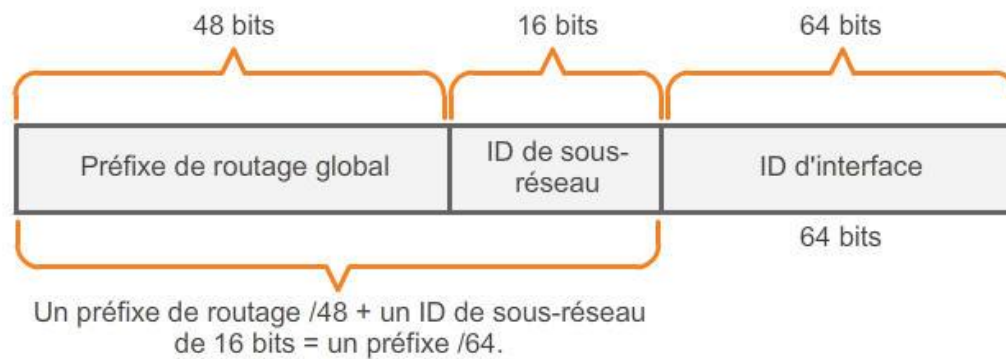




## Les adresses de monodiffusion IPv6

# Structure d'une adresse de monodiffusion globale IPv6

- Une adresse de monodiffusion globale se compose de trois parties :



- **Préfixe de routage global** : préfixe ou partie réseau de l'adresse attribué(e) par le fournisseur (par exemple un FAI) à un client ou à un site. Actuellement, les organismes d'enregistrement Internet locaux attribuent le préfixe /48 aux clients.
- 2001:0DB8:ACAD::/48 a un préfixe qui indique que les 48 premiers bits (2001:0DB8:ACAD) constituent le préfixe ou la partie réseau.



## Les adresses de monodiffusion IPv6

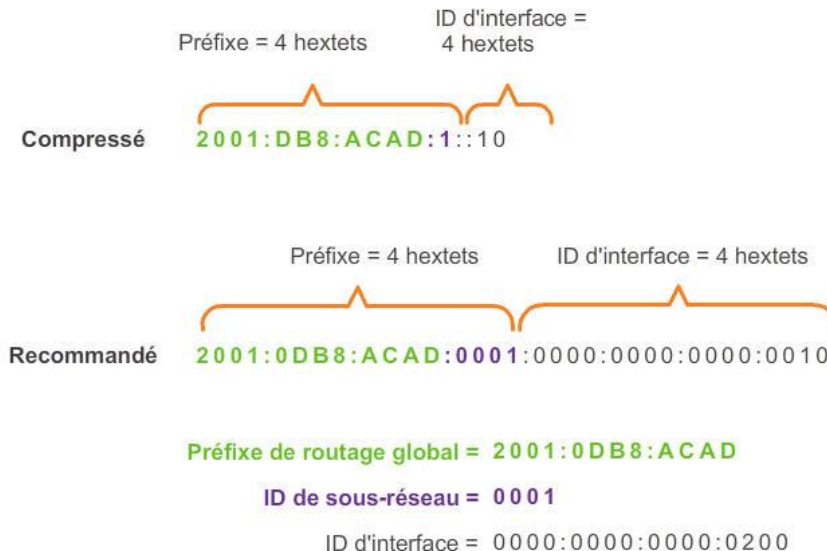
# Structure d'une adresse de monodiffusion globale IPv6

### ■ ID de sous-réseau

- Utilisé par une organisation pour identifier les sous-réseaux de son site

### ■ ID d'interface

- Équivaut à la partie hôte d'une adresse IPv4
- Elle est utilisée parce que le même hôte peut avoir plusieurs interfaces, chacune ayant une ou plusieurs adresses IPv6





## Les adresses de monodiffusion IPv6

# La configuration d'une adresse de monodiffusion globale

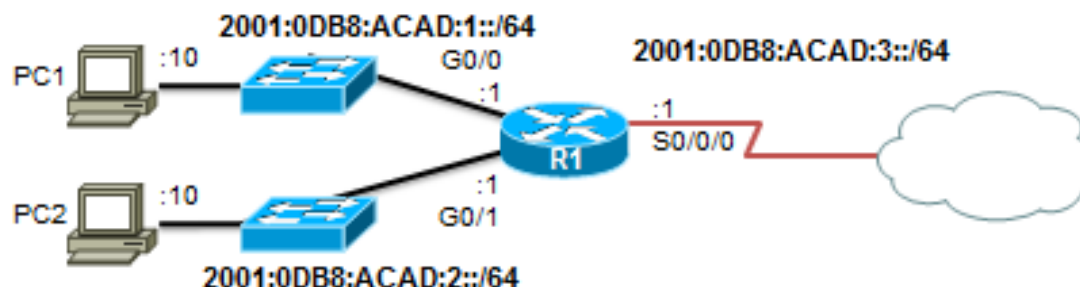
- Configuration manuelle
  
- Configuration automatique (SLAAC, DHCPv6)
  
- Dans le cas de configuration automatique sans état (SLAAC), le client doit générer son identifiant d'interface
  - à partir de l'adresse MAC en l'étendant à une adresse EUI-64
  - par un algorithme pseudo aléatoire





## Les adresses de monodiffusion IPv6

# La configuration statique d'une adresse de monodiffusion globale



```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
```



## Les adresses de monodiffusion IPv6

# La configuration statique d'une adresse de monodiffusion globale IPv6

**Internet Protocol Version 6 (TCP/IPv6) Properties** [?] [X]

**General**

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

☐ Obtain an IPv6 address automatically

☒ Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit



## Les adresses de monodiffusion IPv6

# Configuration dynamique d'une adresse de monodiffusion globale avec la méthode SLAAC

## Configuration automatique des adresses sans état (SLAAC)

- Méthode permettant à un périphérique d'obtenir son préfixe, sa longueur de préfixe et sa passerelle par défaut auprès d'un **routeur IPv6**
- Aucun serveur DHCPv6 n'est nécessaire
- Repose sur les messages ICMPv6 d'annonce de routeur
- Les routeurs envoient des messages d'annonce ICMPv6 en utilisant l'adresse link-local comme adresse IPv6 source



# Configuration dynamique d'une adresse de monodiffusion globale avec la méthode SLAAC

- Le routage IPv6 n'est pas activé par défaut (les routeurs Cisco sont tous configurés pour l'IPv4 par défaut).
- La commande **IPv6 unicast routing** active le routage IPv6

## Routeurs IPv6

- Transfèrent les paquets IPv6 entre les réseaux
- Peuvent être configurés avec des routes statiques ou un protocole de routage IPv6 dynamique
- Envoyent des messages d'annonce de routeur ICMPv6 (auto-configuration des hôtes)



## Les adresses de monodiffusion IPv6

# Configuration dynamique d'une adresse de monodiffusion globale avec la méthode SLAAC

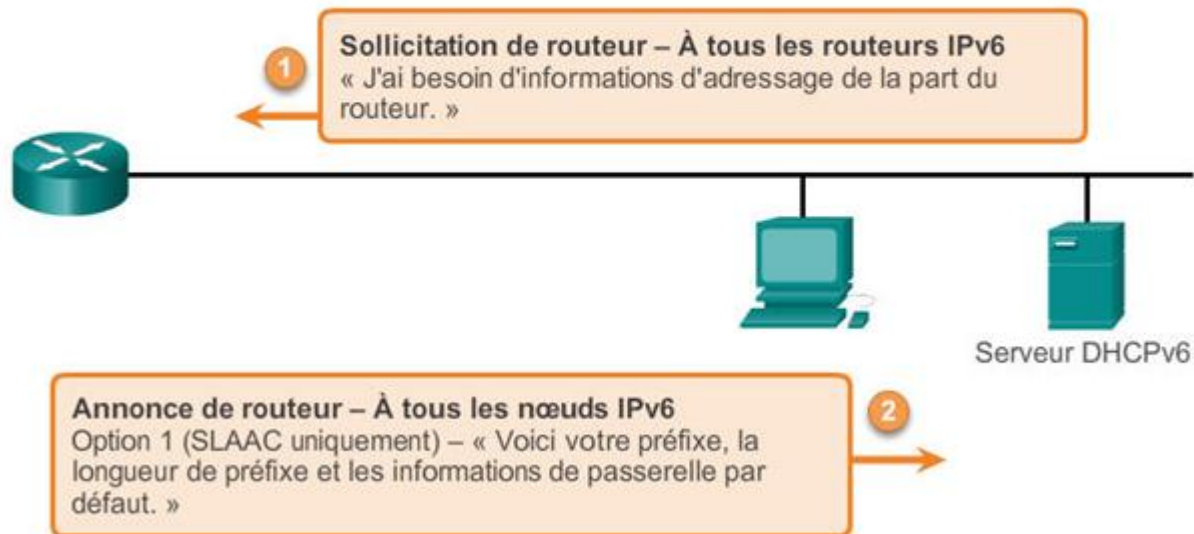
- Le message d'annonce de routeur ICMPv6 contient le préfixe, la longueur du préfixe et d'autres informations destinées au périphérique IPv6.
- Le message d'annonce de routeur indique également au périphérique IPv6 comment obtenir ses informations d'adressage.
- Les messages d'annonce de routeur peuvent contenir une des trois options suivantes :
  - SLAAC uniquement : pour utiliser les informations contenues dans le message d'annonce de routeur
  - SLAAC et DHCPv6 (DHCPv6 sans état) : pour utiliser les informations contenues dans le message d'annonce de routeur et obtenir d'autres informations par le serveur DHCPv6 (exemple : DNS)
  - DHCPv6 uniquement ((DHCPv6 avec état): le périphérique ne doit pas utiliser les informations de l'annonce de routeur. Toutes les informations sont récupérées du serveur DHCPv6



# Les adresses de monodiffusion IPv6

## Configuration dynamique d'une adresse de monodiffusion globale avec la méthode SLAAC

### Messages de sollicitation et d'annonce de routeur





## Les adresses de monodiffusion IPv6

# Configuration dynamique d'une adresse de monodiffusion globale avec la méthode DHCPv6

### Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

- Similaire à IPv4
- Réception automatique des informations d'adressage comprenant une adresse de monodiffusion globale, la longueur du préfixe, l'adresse de la passerelle par défaut et les adresses des serveurs DNS via les services d'un serveur DHCPv6
- Le périphérique peut recevoir une partie ou la totalité des informations d'adressage IPv6 en provenance d'un serveur DHCPv6 selon que l'option 2 (SLAAC et DHCPv6) ou l'option 3 (DHCPv6 uniquement) est spécifiée dans le message d'annonce de routeur ICMPv6
- L'hôte peut décider d'ignorer le contenu du message d'annonce de routeur et obtenir son adresse IPv6 et les autres informations directement auprès d'un serveur DHCPv6

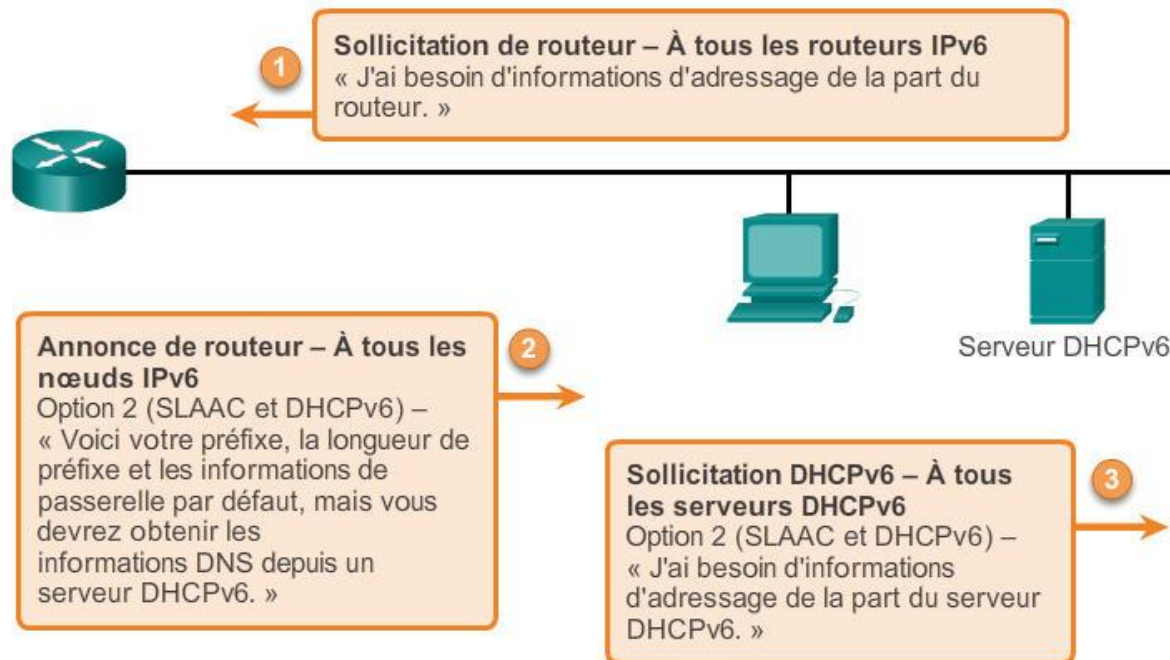




# Les adresses de monodiffusion IPv6

## Configuration dynamique d'une adresse de monodiffusion globale avec la méthode DHCPv6

### Messages de sollicitation et d'annonce de routeur



**Remarque :** une annonce de routeur avec l'option 3 (DHCPv6 uniquement) nécessite que le client obtienne toutes les informations à partir du serveur DHCPv6.



## Les adresses de monodiffusion IPv6

# Génération de l'identificateur d'interface

### Processus EUI-64

- Ce processus utilise l'adresse MAC Ethernet 48 bits d'un client et insère 16 autres bits au milieu de l'adresse MAC 46 bits pour créer un ID d'interface sur 64 bits
- L'avantage est que l'adresse MAC Ethernet peut être utilisée pour déterminer l'interface – traçage plus facile

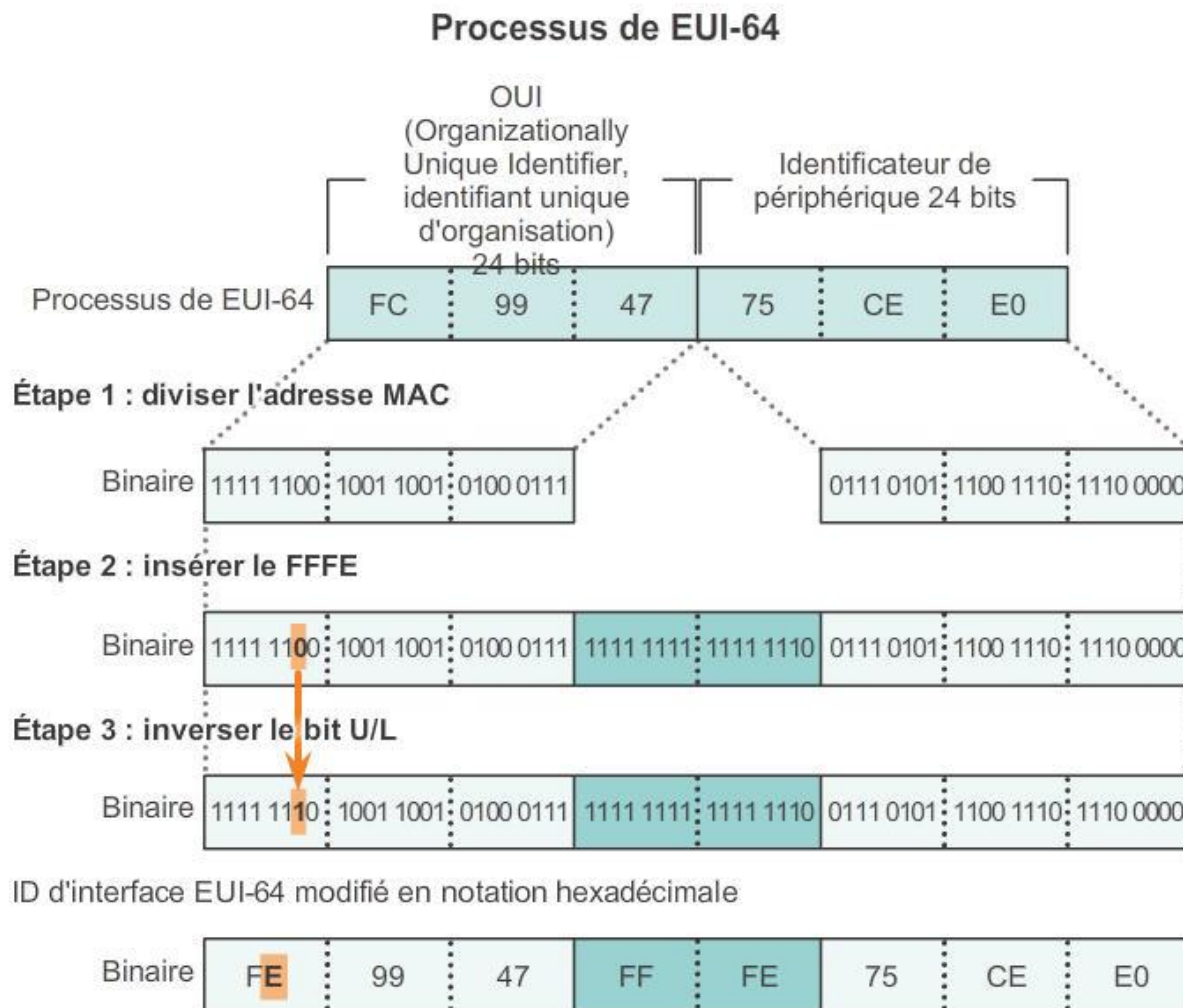
L'ID d'interface EUI-64 est représenté au format binaire et comprend trois parties :

- Le code OUI sur 24 bits, provenant de l'adresse MAC du client, mais dont le septième bit (universellement/localement) est inversé (le 0 devient un 1)
- Valeur FFFE 16 bits insérée
- ID de périphérique sur 24 bits déterminé d'après l'adresse MAC du client



# Les adresses de monodiffusion IPv6

## Génération de l'identificateur d'interface





## Les adresses de monodiffusion IPv6

# Génération de l'identificateur d'interface

```
R1#show interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
<Output Omitted>

R1#show ipv6 interface brief
GigabitEthernet0/0 [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:1::1
GigabitEthernet0/1 [up/up]
  FE80::FE99:47FF:FE75:C3E1
  2001:DB8:ACAD:2::1
Serial0/0/0 [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:3::1
Serial0/0/1 [administratively down/down]
  unassigned
R1#
```

Adresses link-local utilisant le format EUI-64



## Les adresses de monodiffusion IPv6

# Génération de l'identificateur d'interface

## ID d'interface générés aléatoirement

- Selon le système d'exploitation, un périphérique peut utiliser un ID d'interface généré aléatoirement plutôt que l'adresse MAC et le processus EUI-64
- À partir de Windows Vista, Windows utilise un ID d'interface généré aléatoirement au lieu d'un ID créé avec EUI-64
- Windows XP et les systèmes d'exploitation précédents utilisaient EUI-64



## Les adresses de monodiffusion IPv6

# Adresses lien-local

- Une adresse link-local peut être établie dynamiquement ou configurée manuellement comme adresse link-local statique.
- Une adresse de lien-local :
  - Permet à un appareil de communiquer avec les autres périphériques IPv6 situés sur le même sous-réseau
  - Un hôte utilise l'adresse lien-local du routeur local comme adresse IPv6 de passerelle par défaut
  - Les routeurs échangent des messages du protocole de routage dynamique via des adresses lien-local
  - Les tables de routage des routeurs utilisent l'adresse lien-local pour identifier le routeur du tronçon suivant lors du transfert des paquets IPv6



## Les adresses de monodiffusion IPv6

# Adresses link-local dynamiques

- Une fois qu'une adresse de monodiffusion globale est attribuée à une interface, le périphérique IPv6 génère automatiquement son adresse link-local

## Attribution dynamique

- L'adresse link-local est créée dynamiquement à l'aide du préfixe FE80::/10 et de l'ID d'interface



- Sur une interface série, le routeur utilise l'adresse MAC de l'interface Ethernet pour générer son ID





## Les adresses de monodiffusion IPv6

# Adresses link-local statiques

## La configuration des adresses link-local

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
    link-local    Use link-local address

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#
```



## Les adresses de monodiffusion IPv6

# Adresses link-local statiques

## La configuration des adresses link-local

```
R1#show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::1
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::1
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
R1#
```

Adresses link-local  
configurées  
de manière statique

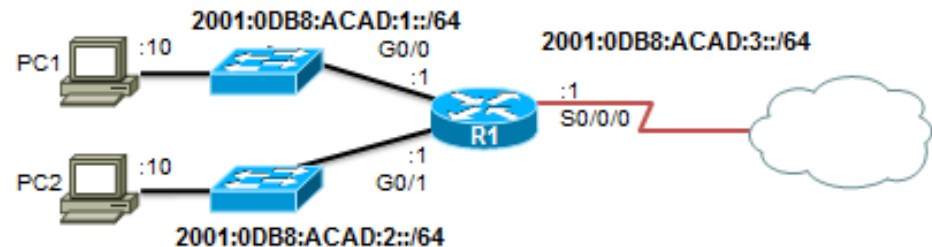


## Les adresses de monodiffusion globale IPv6

# Vérifier la configuration des adresses IPv6

Chaque interface possède au moins deux adresses IPv6 -

1. l'adresse de monodiffusion globale qui a été configurée
2. une adresse de monodiffusion link-local commençant par FE80 est automatiquement ajoutée



```
R1#show ipv6 interface brief
GigabitEthernet0/0    [up/up]
FE80::FE99:47FF:FE75:C3E0
2001:DB8:ACAD:1::1
GigabitEthernet0/1    [up/up]
FE80::FE99:47FF:FE75:C3E1
2001:DB8:ACAD:2::1
Serial0/0/0           [up/up]
FE80::FE99:47FF:FE75:C3E0
2001:DB8:ACAD:3::1
Serial0/0/1           [administratively down/down]
unassigned
R1#
```



Les adresses de multidiffusion IPv6

# Les adresses de multidiffusion IPv6 attribuées

- Les adresses de multidiffusion IPv6 ont le préfixe FFxx::/8
- Il existe deux types d'adresses de multidiffusion IPv6 :
  - Les adresses de multidiffusion attribuées
  - Les adresses de multidiffusion de nœud sollicité



## Les adresses de multidiffusion IPv6

# Les adresses de multidiffusion IPv6 attribuées

Les deux groupes suivants de multidiffusion IPv6 attribuée sont les plus courants :

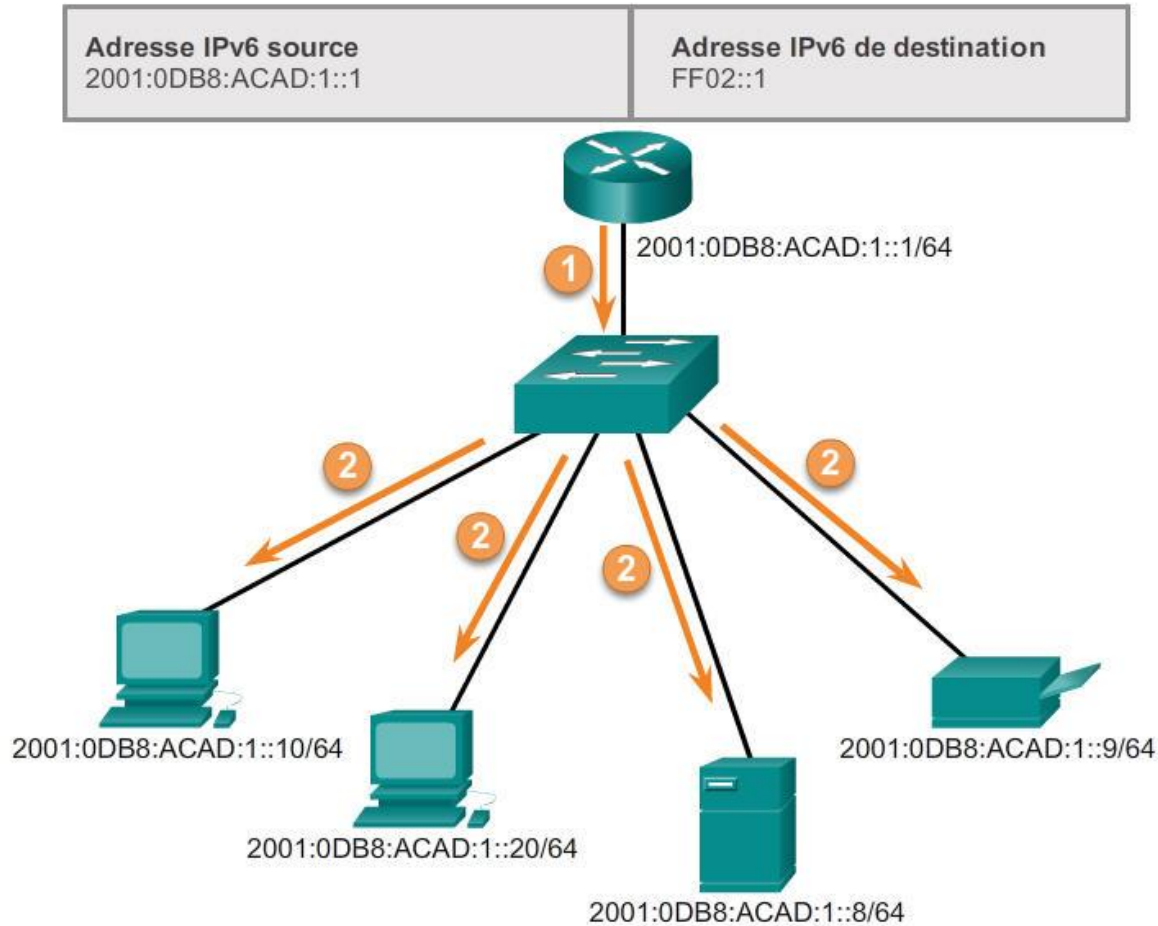
- **FF02::1 Groupe de multidiffusion avec tous les nœuds –**
  - Tous les périphériques IPv6 sont inclus
  - Même effet qu'une adresse de diffusion IPv4
- **FF02::2 Groupe de multidiffusion avec tous les routeurs –**
  - Tous les routeurs IPv6 sont inclus
  - Un routeur devient un membre de ce groupe lorsqu'il est activé en tant que routeur IPv6 (**ipv6 unicast-routing**)
  - Un paquet envoyé à ce groupe est reçu et traité par tous les routeurs IPv6 situés sur la liaison ou le réseau
- **FF02:: 1:0 Groupe de multidiffusion avec tous les serveurs DHCP**



## Les adresses de multidiffusion IPv6

# Les adresses de multidiffusion IPv6 attribuées

Transmissions multidiffusion à tous les nœuds IPv6

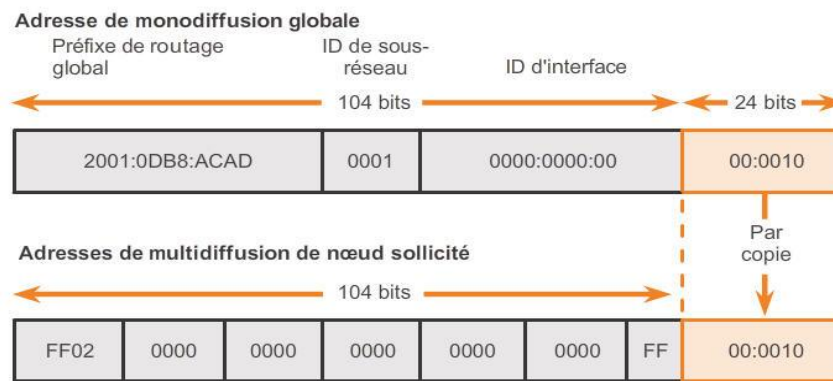




## Les adresses de multidiffusion IPv6

# Les adresses de multidiffusion IPv6 de nœud sollicité

- Sont similaires à l'adresse de multidiffusion sur tous les nœuds ; concordance uniquement avec les 24 derniers bits de l'adresse de monodiffusion globale IPv6 d'un périphérique
- Sont créées automatiquement lorsque la monodiffusion globale ou les adresses de monodiffusion link-local sont attribuées
- Sont créées en combinant un préfixe FF02:0:0:0:0:FF00::/104 spécial avec les 24 derniers bits de son adresse de monodiffusion
- Utilisées dans la résolution d'adresse physique



Adresse de monodiffusion globale IPv6 :  
2001:0DB8:ACAD:0001:0000:0000:0000:0010

Adresse de multidiffusion de nœud sollicité IPv6 :  
FF02::0:FF00:0010





## Le protocole ICMP

# Les messages ICMPv4 et ICMPv6

- ICMP permet d'envoyer des messages si certaines erreurs se produisent
- Les messages ICMP ne sont pas obligatoires et sont souvent interdits au sein des réseaux pour des raisons de sécurité.
- Les messages ICMP communs à ICMPv4 et à ICMPv6 sont notamment les suivants :
  - Host confirmation (Confirmation de l'hôte)
  - Destination or Service Unreachable (destination ou service inaccessible)
  - Time exceeded (Délai dépassé)
  - Route redirection (Redirection de la route)
- ICMPv6 est utilisée dans la configuration automatique des équipements (découverte des routeurs, découverte des voisins)
- ICMP v6 reprend les fonctions de ARP utilisé dans IPv4
- Gestion de groupe multicast : MLD(Multicast Listener Discovery)



## Le protocole ICMP

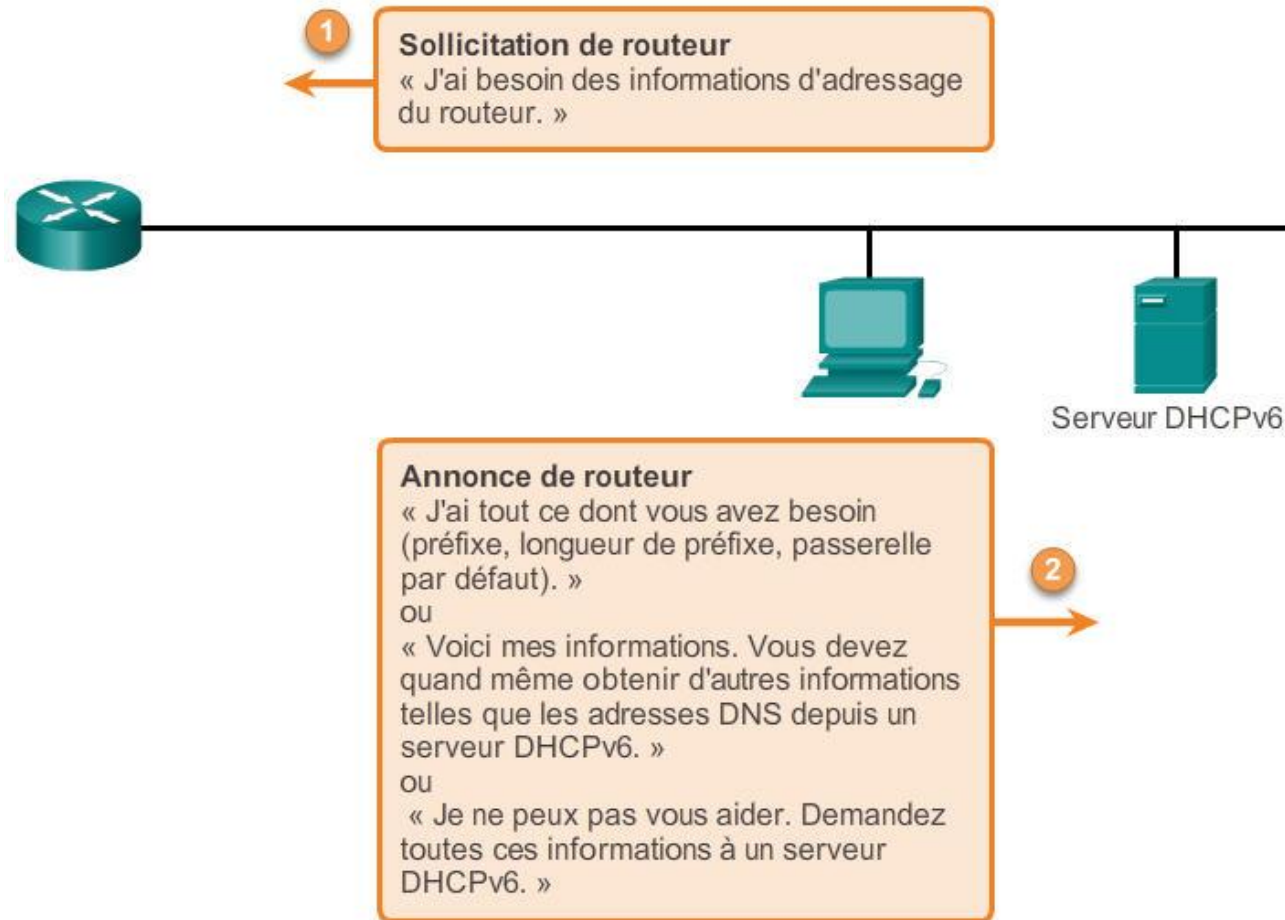
# Les messages de sollicitation et d'annonce de routeur ICMPv6

- ICMPv6 inclut quatre nouveaux protocoles dans le cadre du protocole Neighbor Discovery Protocol (ND ou NDP) :
  - Message de sollicitation de routeur
  - Message d'annonce de routeur
  - Message de sollicitation de voisin
  - Message d'annonce de voisin
- **Messages de sollicitation et d'annonce de routeur** : échangés entre les hôtes et les routeurs
- **Messages de sollicitation de routeur** : envoyés sous forme de message de multidiffusion « tous les routeurs » IPv6
- **Messages d'annonce de routeur** : envoyés par les routeurs pour fournir les informations d'adressage



## Le protocole ICMP

# Les messages de sollicitation et d'annonce de routeur ICMPv6





## Le protocole ICMP

# Les messages de sollicitation et d'annonce de voisin ICMPv6

Deux types de message supplémentaires

- Sollicitation de voisin
- Messages d'annonce de voisin

Utilisés pour :

- La résolution d'adresse
  - Utilisés lorsqu'un périphérique du réseau local (LAN) connaît l'adresse de monodiffusion IPv6 d'une destination, mais pas son adresse MAC Ethernet
- La détection d'adresses en double (DAD)
  - Sur l'adresse pour s'assurer qu'elle est unique
  - Le périphérique envoie un message NS avec sa propre adresse IPv6 comme destination



## Le protocole ICMP

# Les messages de sollicitation et d'annonce de voisin ICMPv6

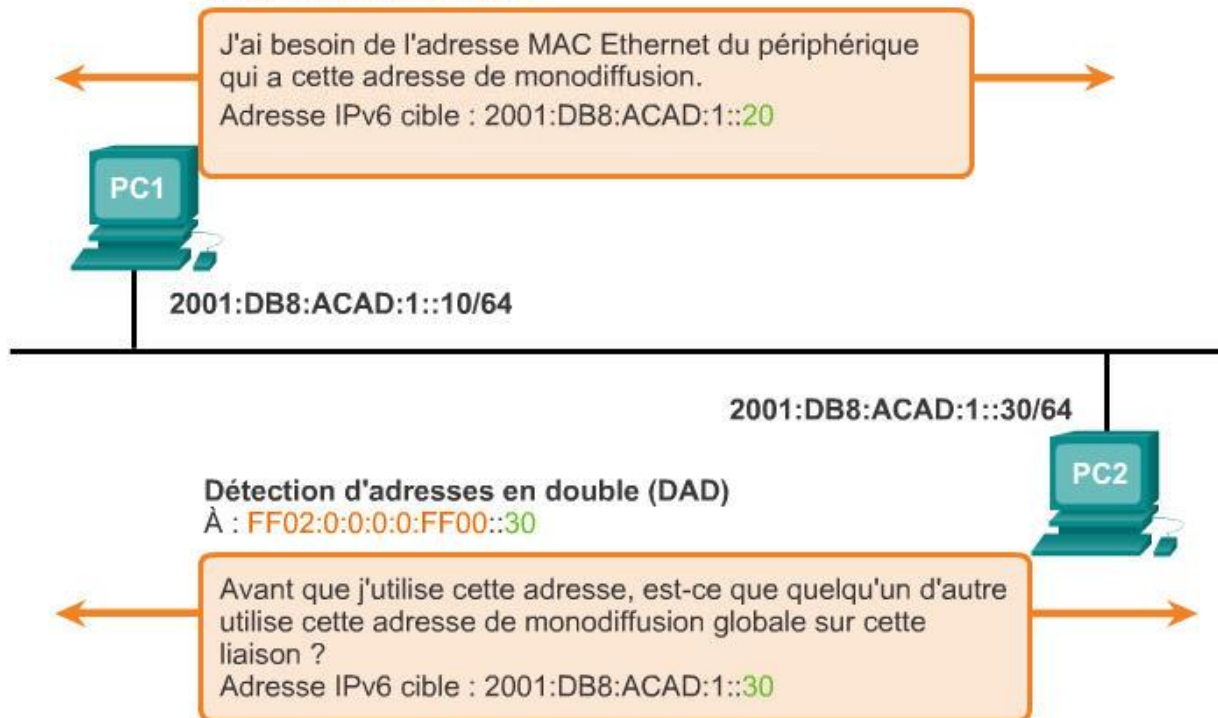
### Protocole Neighbor Discovery Protocol ICMPv6

#### Résolution d'adresse

À : FF02:0:0:0:FF00::20

J'ai besoin de l'adresse MAC Ethernet du périphérique qui a cette adresse de monodiffusion.

Adresse IPv6 cible : 2001:DB8:ACAD:1::20



#### Détection d'adresses en double (DAD)

À : FF02:0:0:0:FF00::30

Avant que j'utilise cette adresse, est-ce que quelqu'un d'autre utilise cette adresse de monodiffusion globale sur cette liaison ?

Adresse IPv6 cible : 2001:DB8:ACAD:1::30



# Routage

- Le rôle de la couche réseau est de diriger les paquets entre les hôtes (routage)
- Un hôte peut envoyer un paquet à lui-même, à un hôte local ou à un hôte distant
- Le fait que l'hôte destination est local ou distant est déterminé par la comparaison de l'adresse réseau destination avec celle source.
- Si l'hôte destination est distant (un autre réseau distinct de la source) alors l'aide du routeur et du routage est nécessaire.

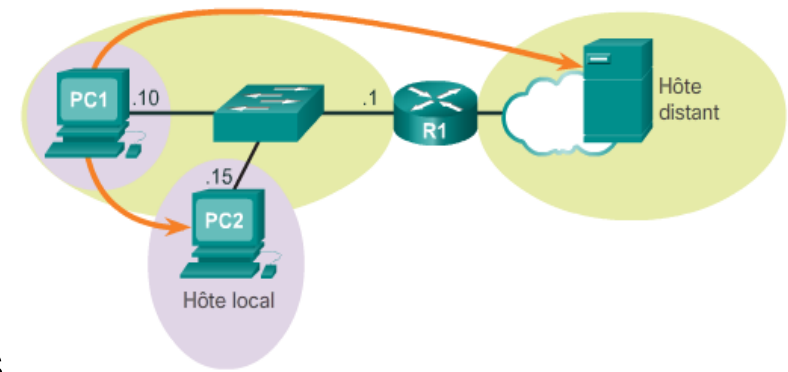
■ Le routage consiste à déterminer

le meilleur chemin vers la destination.

- Les meilleurs chemins sont enregistrées dans une table appelée table de routage

- Le routeur connecté au segment d'un réseau

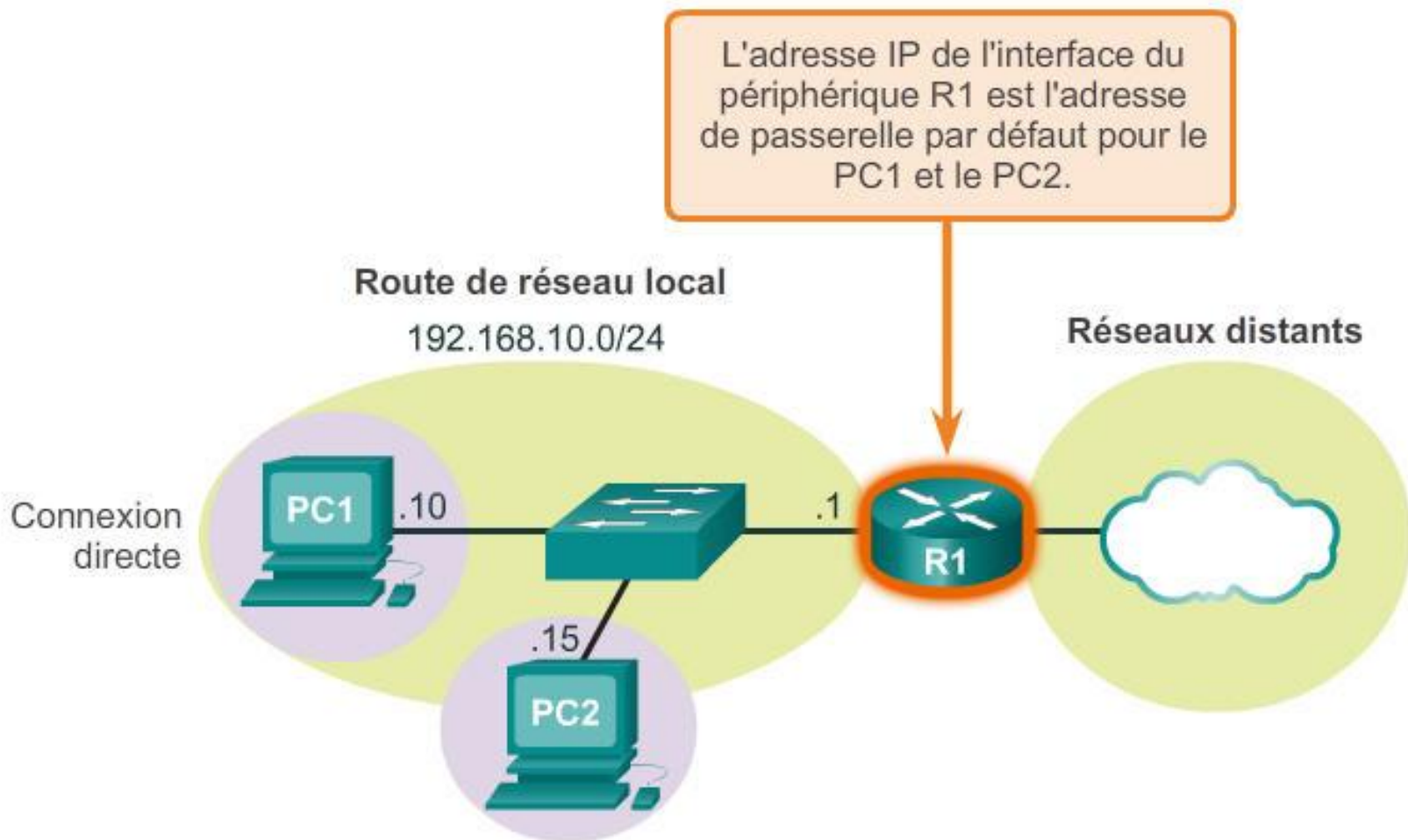
LAN est dit passerelle par défaut





Tables de routage des hôtes

# Décisions relatives à la transmission des paquets







## Tables de routage des hôtes

# La passerelle par défaut

- Les hôtes ont également besoin d'une table de routage locale pour diriger correctement les paquets vers le réseau de destination correspondant.
- La table locale de l'hôte contient généralement :
  - Connexion directe (route vers l'interface de bouclage)
  - Route de réseau local
  - Route par défaut locale (utile pour router les paquets destinés aux réseaux distants)



## Tables de routage des hôtes

# Table de routage d'hôte IPv4



```
C:\Users\PC1>netstat -r
```

<Output omitted>

### IPv4 Route Table

#### Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0		0.0.0.0	192.168.10.1	192.168.10.10	25
127.0.0.0		255.0.0.0	On-link	127.0.0.1	306
127.0.0.1		255.255.255.255	On-link	127.0.0.1	306
127.255.255.255		255.255.255.255	On-link	127.0.0.1	306
192.168.10.0		255.255.255.0	On-link	192.168.10.10	281
192.168.10.10		255.255.255.255	On-link	192.168.10.10	281
192.168.10.255		255.255.255.255	On-link	192.168.10.10	281
224.0.0.0		240.0.0.0	On-link	127.0.0.1	306
224.0.0.0		240.0.0.0	On-link	192.168.10.10	281
255.255.255.255		255.255.255.255	On-link	127.0.0.1	306
255.255.255.255		255.255.255.255	On-link	192.168.10.10	281

<Output omitted>



## Tables de routage des hôtes

# Exemple de table de routage d'hôte IPv4



```
C:\Users\PC1> netstat -r
```

```
<Output omitted>
```

```
IPv4 Route Table
```

```
=====
```

```
Active Routes:
```

Network	Destination	Netmask	Gateway	Interface	Metric
	<b>0.0.0.0</b>	<b>0.0.0.0</b>	<b>192.168.10.1</b>	<b>192.168.10.10</b>	<b>25</b>
127.0.0.0		255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255		On-link	127.0.0.1	306
127.255.255.255	255.255.255.255		On-link	127.0.0.1	306
192.168.10.0	255.255.255.0		On-link	192.168.10.10	281
192.168.10.10	255.255.255.255		On-link	192.168.10.10	281
192.168.10.255	255.255.255.255		On-link	192.168.10.10	281
224.0.0.0	240.0.0.0		On-link	127.0.0.1	306
224.0.0.0	240.0.0.0		On-link	192.168.10.10	281
255.255.255.255	255.255.255.255		On-link	127.0.0.1	306
255.255.255.255	255.255.255.255		On-link	192.168.10.10	281

```
<Output omitted>
```



## Tables de routage des hôtes

# Exemple de table de routage d'hôte IPv6

fe80::2c30:3071:e718:a926/128  
2001:db8:9d38:953c:2c30:3071:e718:a926/128



C:\Users\PC1> **netstat -r**

<Output omitted>

IPv6 Route Table

=====

Active Routes:

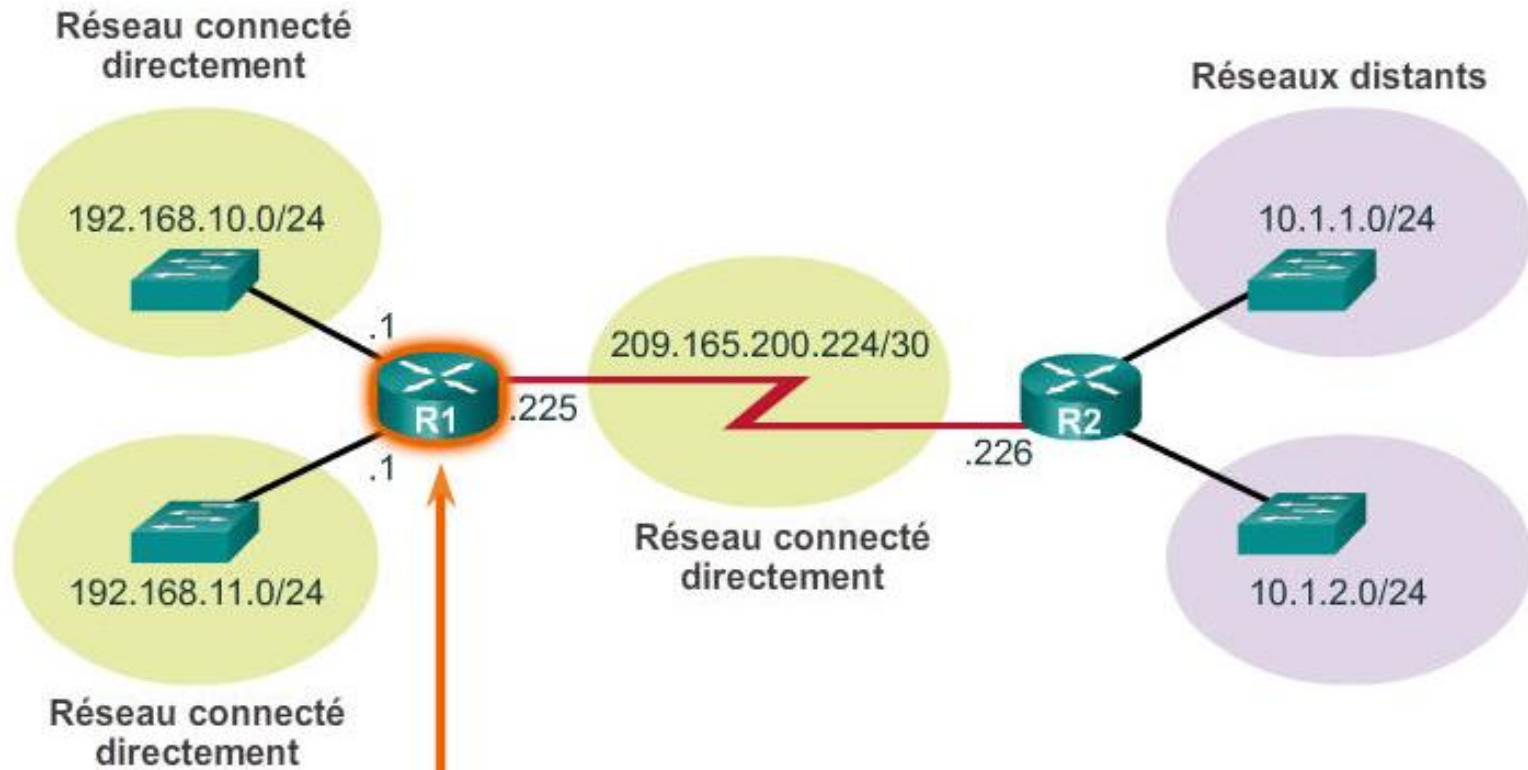
If	Metric	Network	Destination	Gateway
16	58	::/0		On-link
1	306	::1/128		On-link
16	58	2001::/32		On-link
16	306	2001:0:9d38:953c:2c30:3071:e718:a926/128		On-link
15	281	fe80::/64		On-link
16	306	fe80::/64		On-link
16	306	fe80::2c30:3071:e718:a926/128		On-link
15	281	fe80::b1ee:c4ae:a117:271f/128		On-link
1	306	ff00::/8		On-link
16	306	ff00::/8		On-link
15	281	ff00::/8		On-link

<Output omitted>



## Tables de routage du routeur

# Décisions relatives à la transmission des paquets du routeur

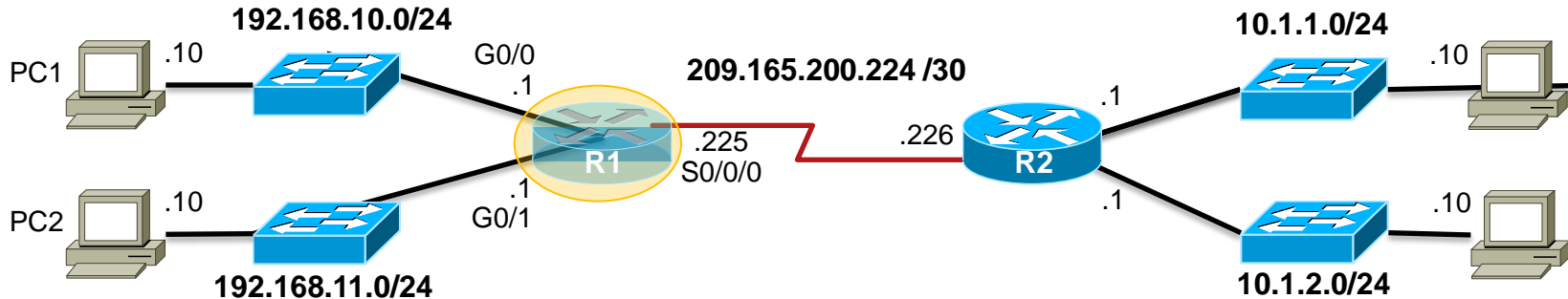


Le routeur R1 est relié à trois réseaux connectés directement : 192.168.10.0/24, 192.168.11.0/24, et 209.165.200.224/30. Le routeur R1 est également relié à deux réseaux distants auxquels il peut accéder via R2 : 10.1.1.0/24 et 10.1.2.0/24.



## Tables de routage du routeur

# Table de routage d'un routeur IPv4



R1#**show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
 \* - candidate default, U - per-user static route, o - ODR  
 P - periodic downloaded static route

Gateway of last resort is not set

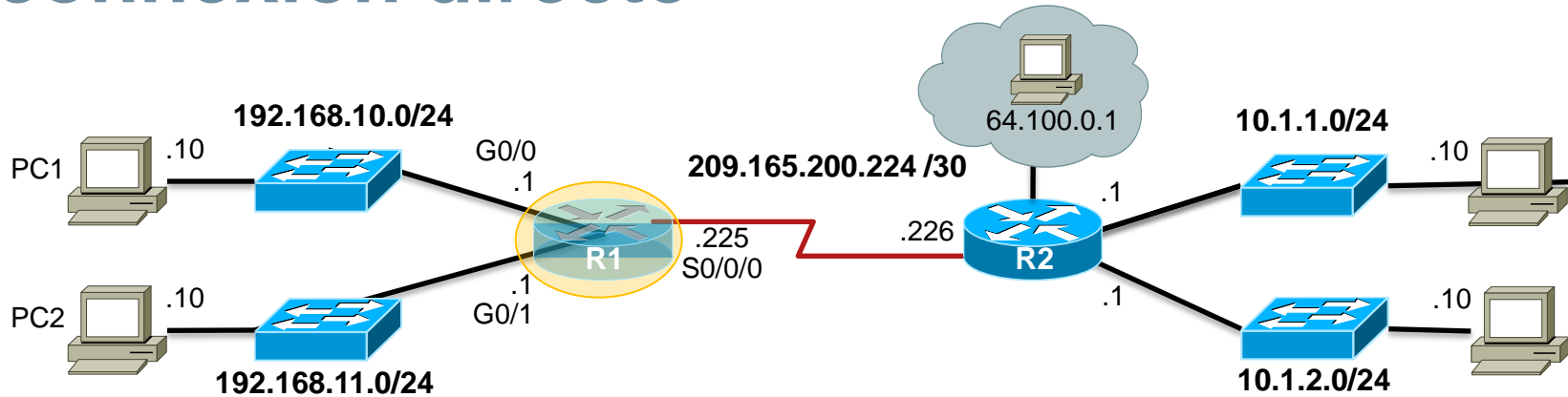
```

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
D    10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0
192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C    192.168.11.0/24 is directly connected, GigabitEthernet0/1
L    192.168.11.1/32 is directly connected, GigabitEthernet0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C    209.165.200.224/30 is directly connected, Serial0/0/0
L    209.165.200.225/32 is directly connected, Serial0/0/0
R1#
  
```



## Tables de routage du routeur

# Entrées d'une table de routage pour une connexion directe



**A**

**B**

**C**

<b>C</b>	<b>192.168.10.0/24 is directly connected,</b>	<b>GigabitEthernet0/0</b>
<b>L</b>	<b>192.168.10.1/32 is directly connected,</b>	<b>GigabitEthernet0/0</b>

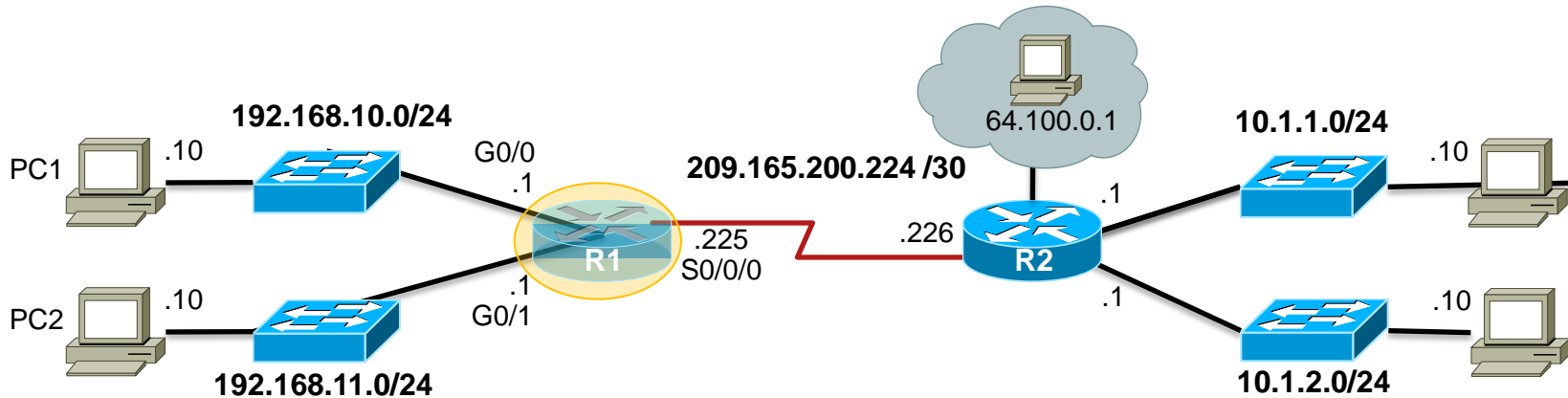
<b>A</b>	
<b>B</b>	Identifie le réseau de destination et la manière dont celui-ci est connecté.
<b>C</b>	Identifie l'interface du routeur qui est connectée au réseau de destination.





## Tables de routage du routeur

# Entrées d'une table de routage d'un réseau distant

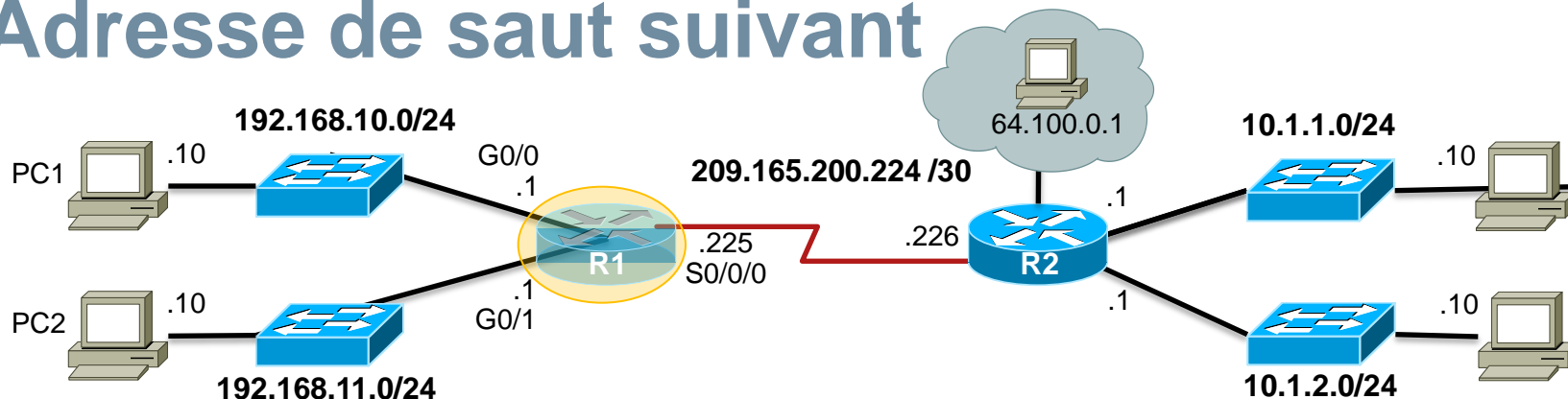


<b>D</b>	10.1.1.0/24	[90/2170112]	via	209.165.200.226,	00:00:05,	Serial0/0/0
----------	-------------	--------------	-----	------------------	-----------	-------------

<b>A</b>	Indique la façon dont le réseau a été « appris » par le routeur.
<b>B</b>	Identifie le réseau de destination.
<b>C</b>	Identifie la distance administrative (fiabilité) de la route source.
<b>D</b>	Identifie la métrique pour atteindre le réseau distant.
<b>E</b>	Identifie l'adresse IP du saut suivant pour atteindre le réseau distant.
<b>F</b>	Identifie le temps écoulé depuis que le réseau a été découvert.
<b>G</b>	Identifie l'interface de sortie du routeur utilisée pour atteindre le réseau de destination.

# Tables de routage du routeur

## Adresse de saut suivant



```
R1#show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

```
D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
```

```
D 10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
```

```
192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
```

```
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0
```

```
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0
```

```
192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
```

```
C 192.168.11.0/24 is directly connected, GigabitEthernet0/1
```

```
L 192.168.11.1/32 is directly connected, GigabitEthernet0/1
```

```
209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
```

```
C 209.165.200.224/30 is directly connected, Serial0/0/0
```

```
L 209.165.200.225/32 is directly connected, Serial0/0/0
```

```
R1#
```



## Test et vérification

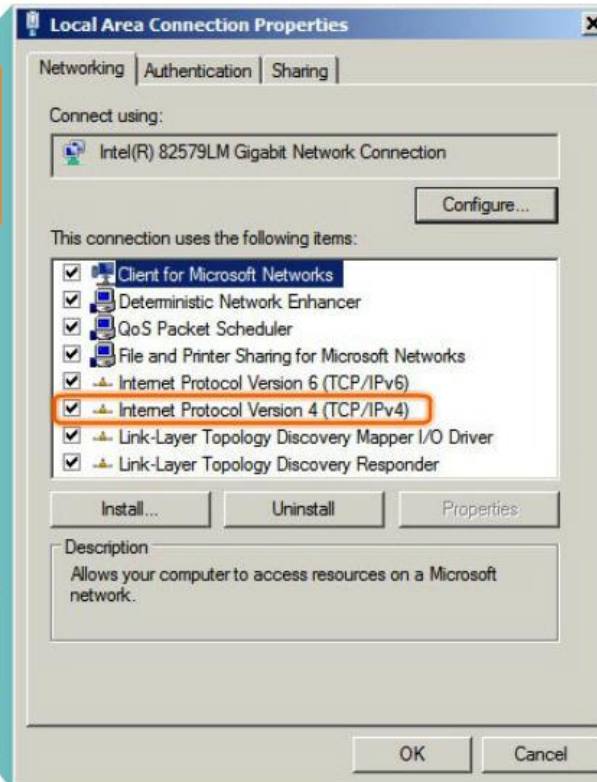
# Ping - Tester la pile locale

### Test de la pile TCP/IP locale

L'exécution de la commande ping sur l'hôte local confirme que la suite de protocoles TCP/IP est installée et fonctionne sur l'hôte local.

C:\>ping 127.0.0.1

Si vous envoyez une requête ping 127.0.0.1, le périphérique se teste lui-même.

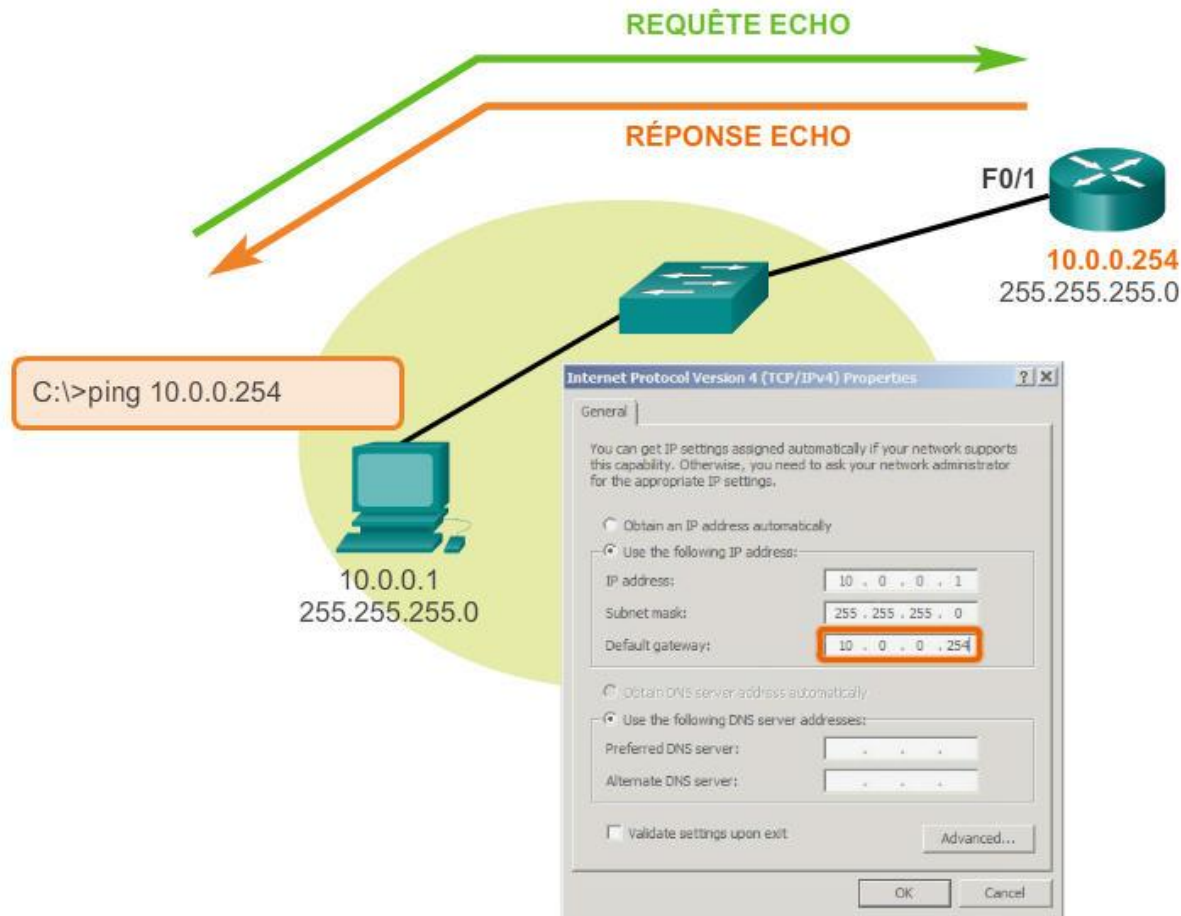




## Test et vérification

# Ping – Tester la connectivité au réseau local

### Test de la connectivité IPv4 au réseau local

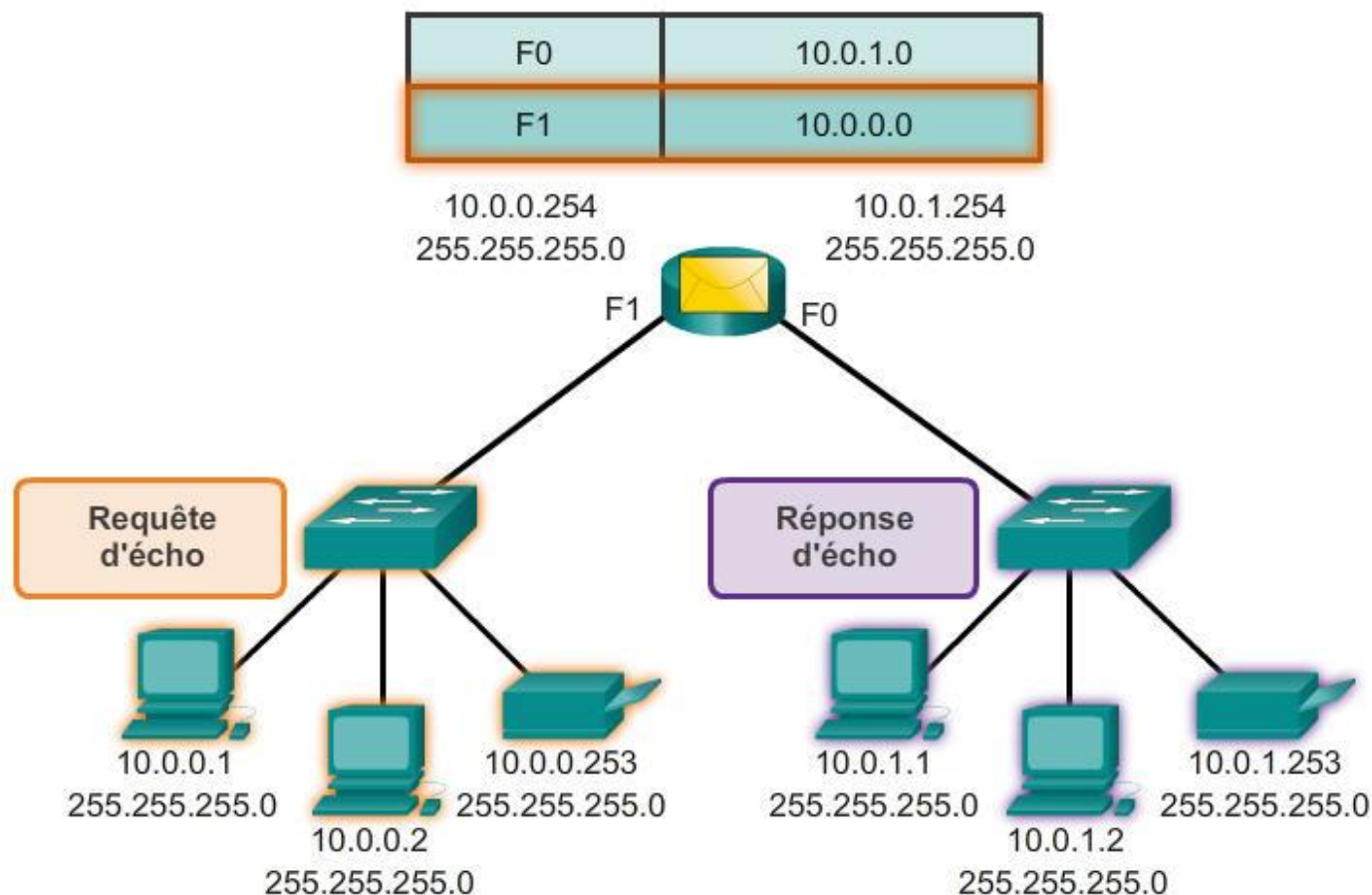




## Test et vérification

# Ping – Tester la connectivité à distance

Test de la connectivité au réseau local distant  
Requête ping à un hôte distant





## Test et vérification

# Traceroute – Tester le chemin

### Traceroute (tracert)

- Génère une liste de sauts déjà atteints le long du chemin
- Fournit des informations de contrôle et de dépannage
- Si les données parviennent à destination, la commande affiche tous les routeurs situés entre les hôtes
- Si les données restent bloquées au niveau d'un saut, l'adresse du dernier routeur ayant répondu à la commande peut fournir une indication sur l'endroit où se situe le problème ou sur d'éventuelles restrictions de sécurité
- Fournit la durée de transmission sur chacun des sauts rencontrés et indique si l'un d'eux ne répond pas





## Les routeurs

# Composants d'un routeur







## Composants d'un routeur

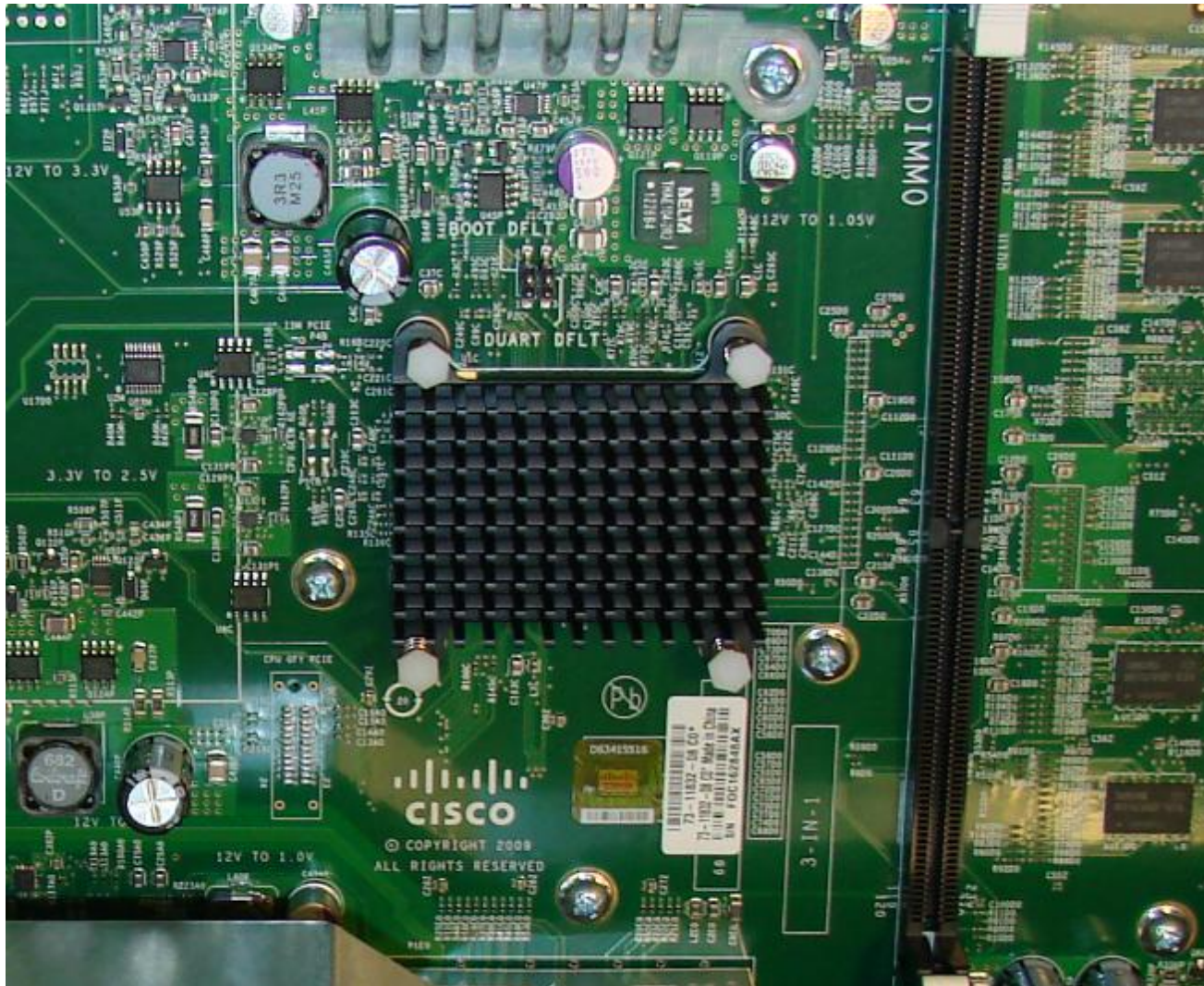
# Un routeur est un ordinateur





## Composants d'un routeur

# Processeur et système d'exploitation d'un routeur





## Composants d'un routeur

# Mémoire du routeur

Mémoire	Volatile / Non volatile	Données stockées
<b>Mémoire vive (RAM)</b>	Volatile	<ul style="list-style-type: none"> <li>• IOS en cours d'exécution</li> <li>• Fichier de configuration en cours</li> <li>• Tables ARP et de routage IP</li> <li>• Mémoire tampon de paquets</li> </ul>
<b>ROM</b>	Non volatile	<ul style="list-style-type: none"> <li>• Instructions de démarrage</li> <li>• Logiciel de diagnostic de base</li> <li>• IOS limité</li> </ul>
<b>NVRAM</b>	Non volatile	<ul style="list-style-type: none"> <li>• Fichier de configuration initiale</li> </ul>
<b>Flash</b>	Non volatile	<ul style="list-style-type: none"> <li>• IOS</li> <li>• Autres fichiers système</li> </ul>





## Composants d'un routeur

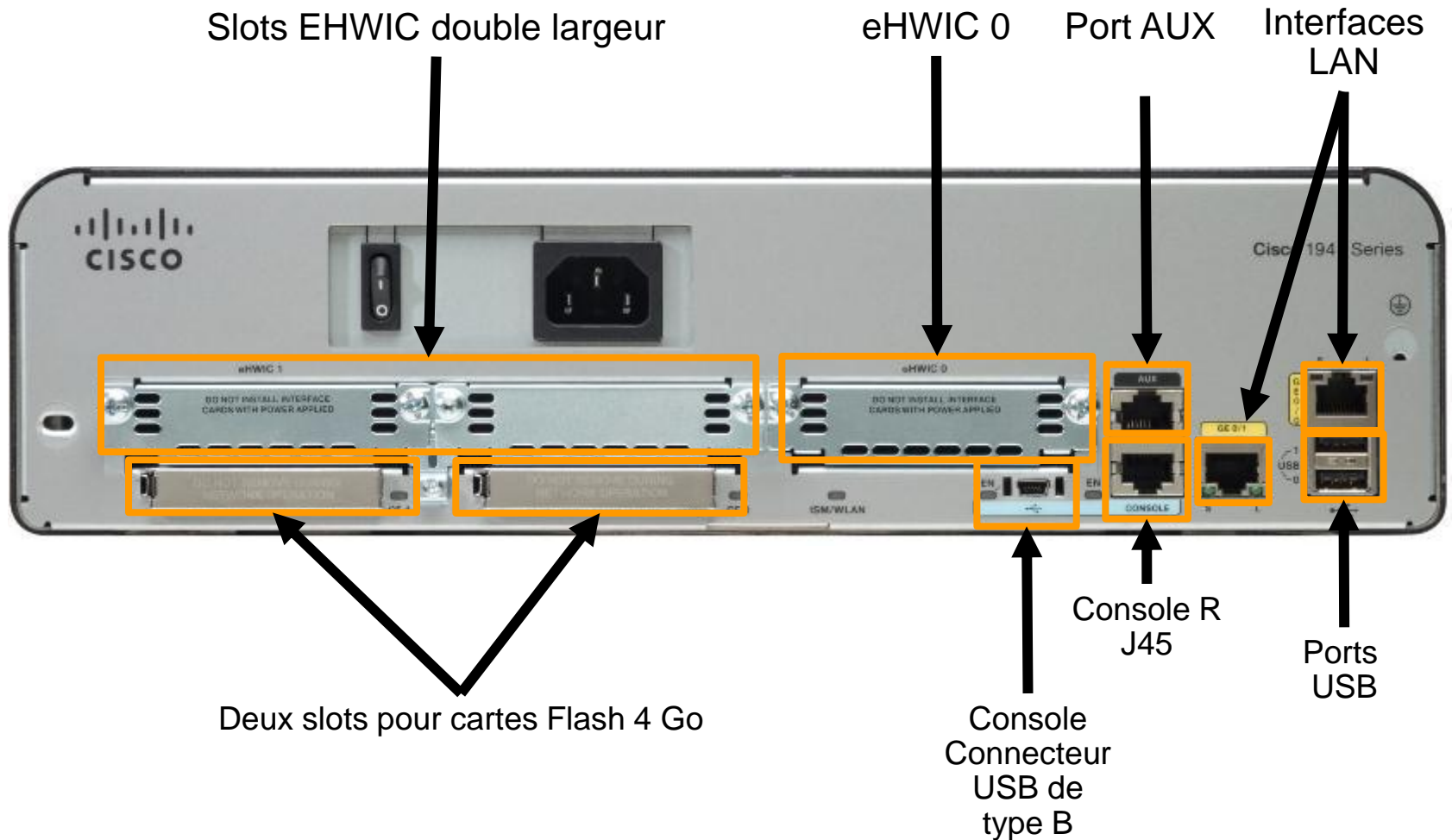
# À l'intérieur d'un routeur





## Composants d'un routeur

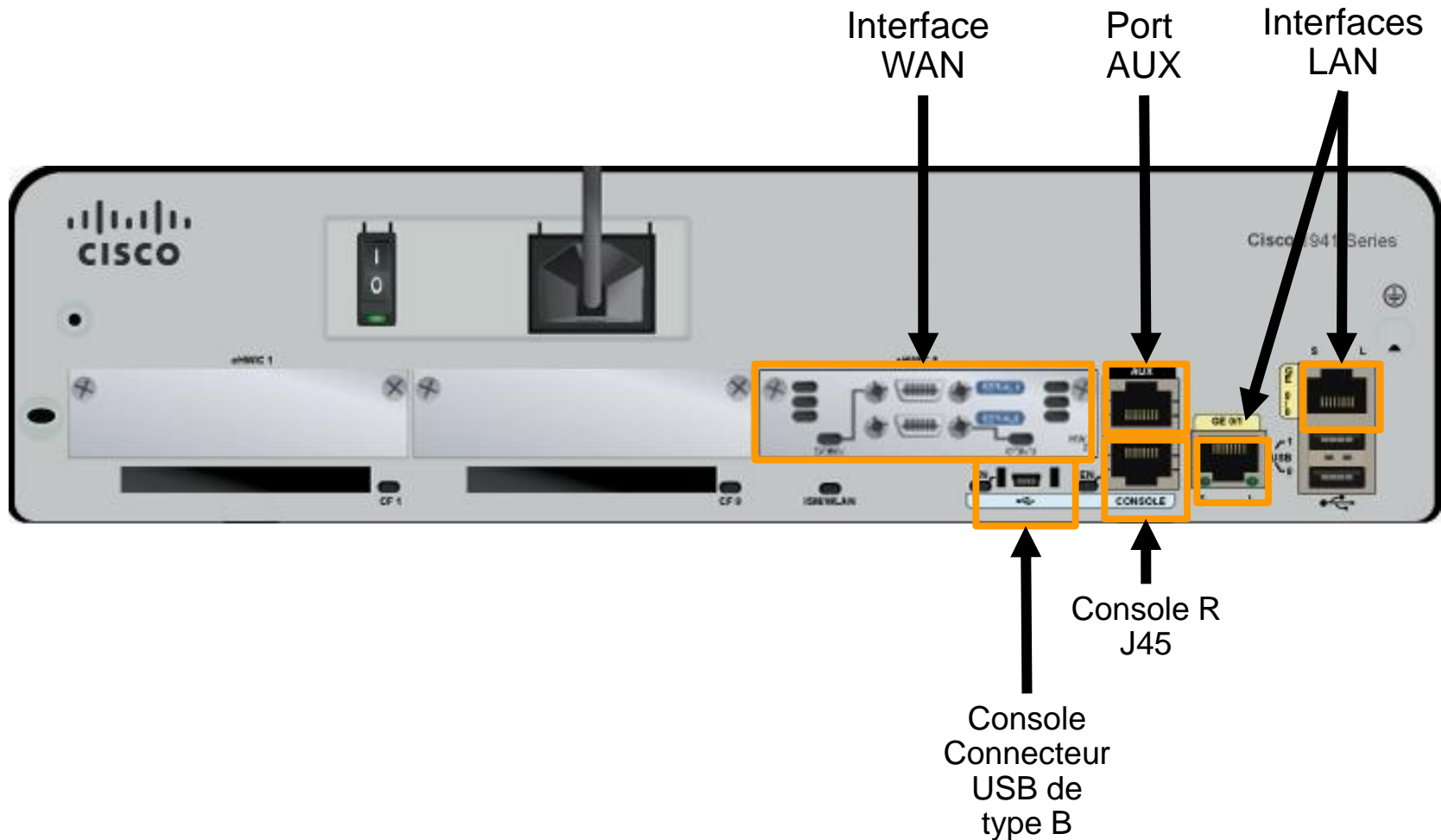
# Fond de panier du routeur





## Composants d'un routeur

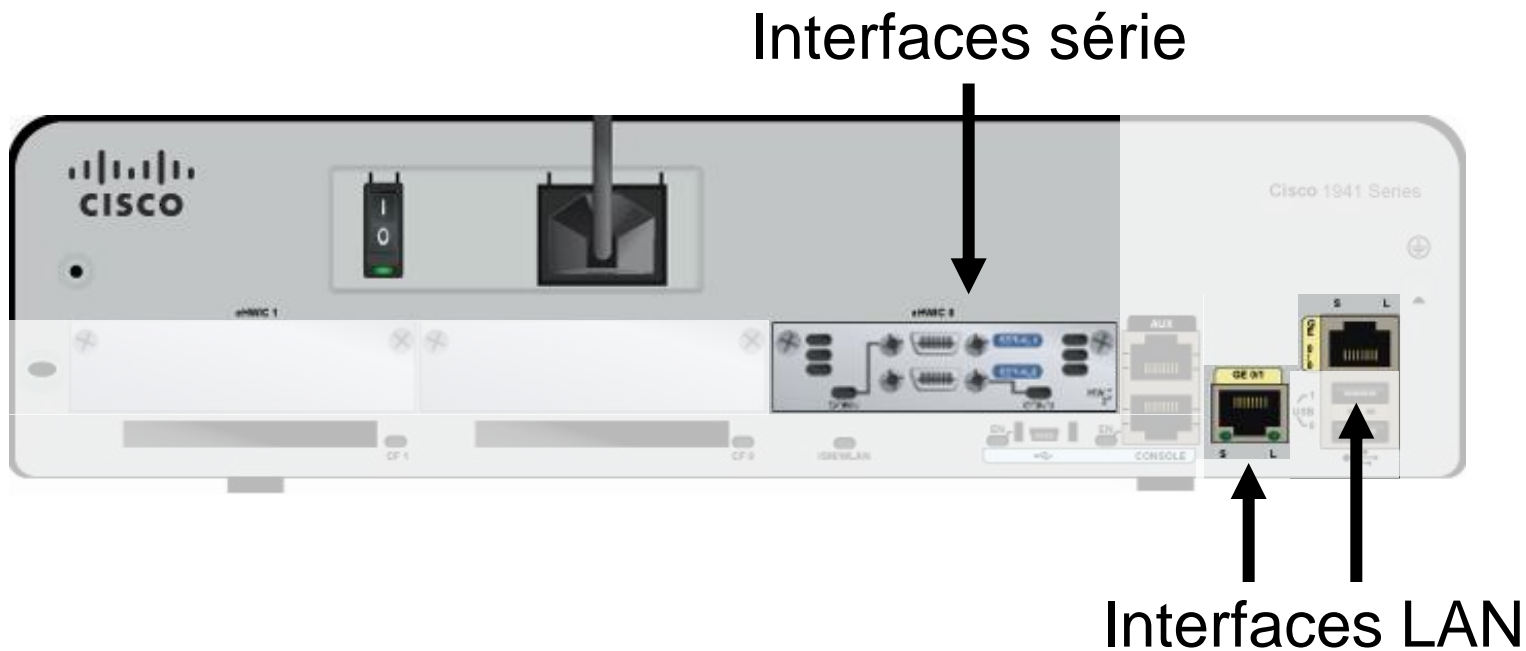
# Connexion à un routeur





## Composants d'un routeur

# Interfaces LAN et WAN







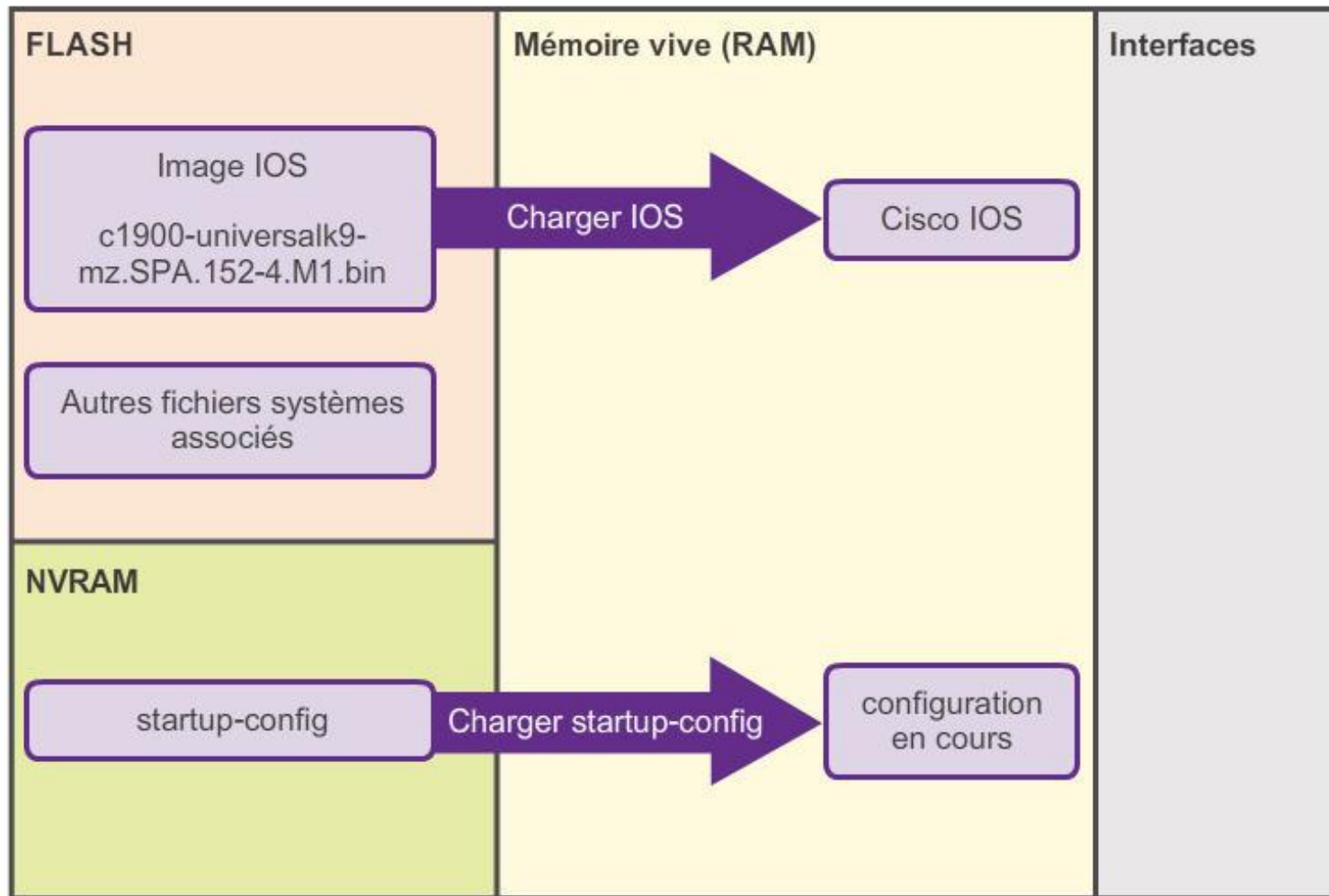
# Démarrage du routeur Cisco IOS





## Démarrage du routeur

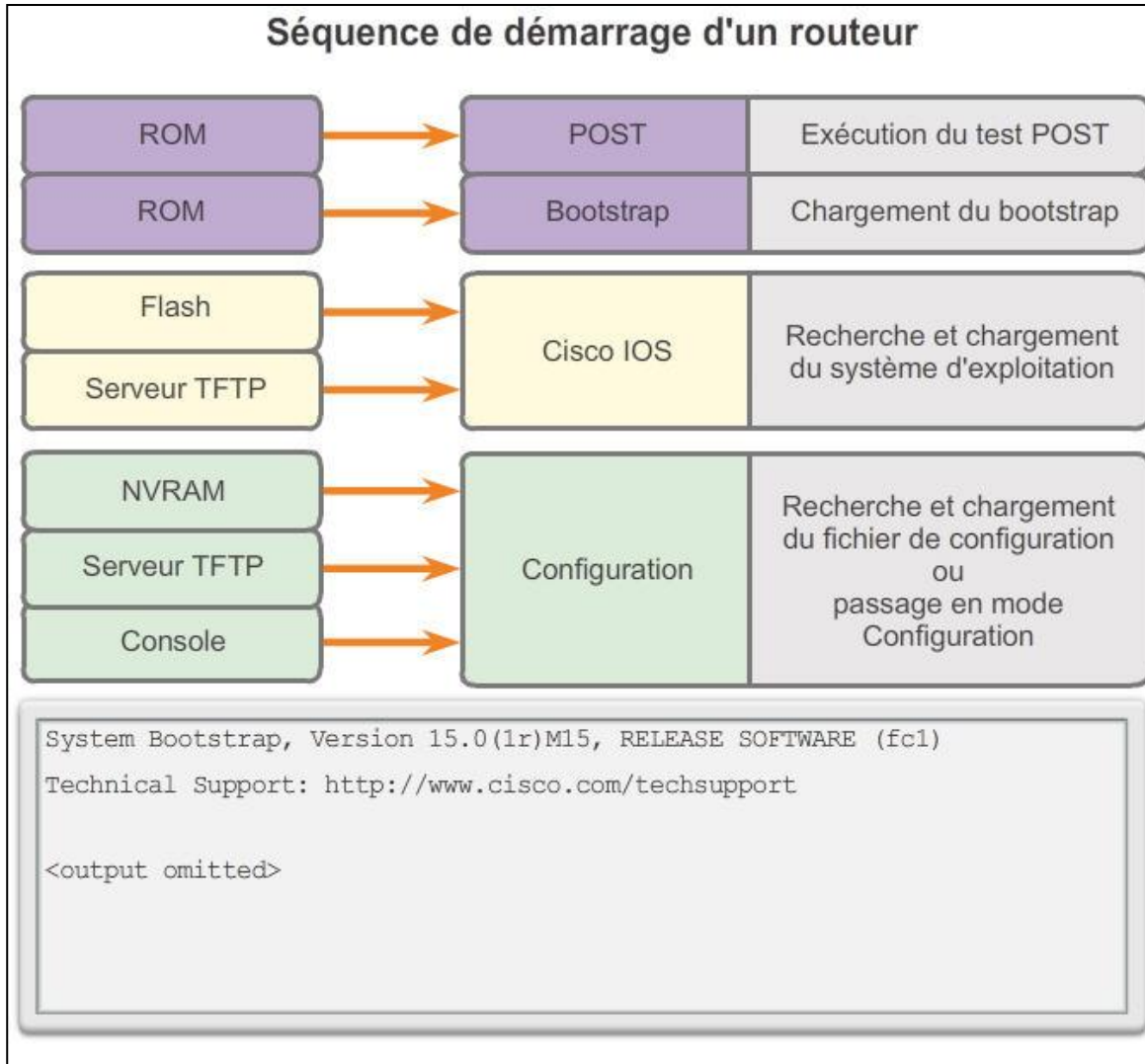
# Fichiers de démarrage prédéfinis





## Démarrage du routeur

# Processus de démarrage d'un routeur



1. Exécution du test POST et chargement du bootstrap

2. Recherche et chargement du logiciel Cisco IOS

3. Recherche et chargement du fichier de configuration initiale ou passage en mode Configuration



## Démarrage du routeur

# Résultat de la commande show version

```
Router# show version
Cisco IOS Software, C1900 Software (C1900-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 19:34 by prod_rel_team

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

Router uptime is 10 hours, 9 minutes
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.152-4.M1.bin"
Last reload type: Normal Reload
Last reload reason: power-on

<Résultat omis>

Cisco CISC01941/K9 (revision 1.0) with 446464K/77824K bytes of memory.
Processor board ID FTX1636848Z
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)

<Résultat omis>

Technology Package License Information for Module:'c1900'

-----
Technology      Technology-package      Technology-package
                Current       Type                Next reboot
-----
ipbase          ipbasek9               Permanent          ipbasek9
security        None                   None               None
data            None                   None               None

Configuration register is 0x2142 (will be 0x2102 at next reload)

Router#
```



La couche réseau

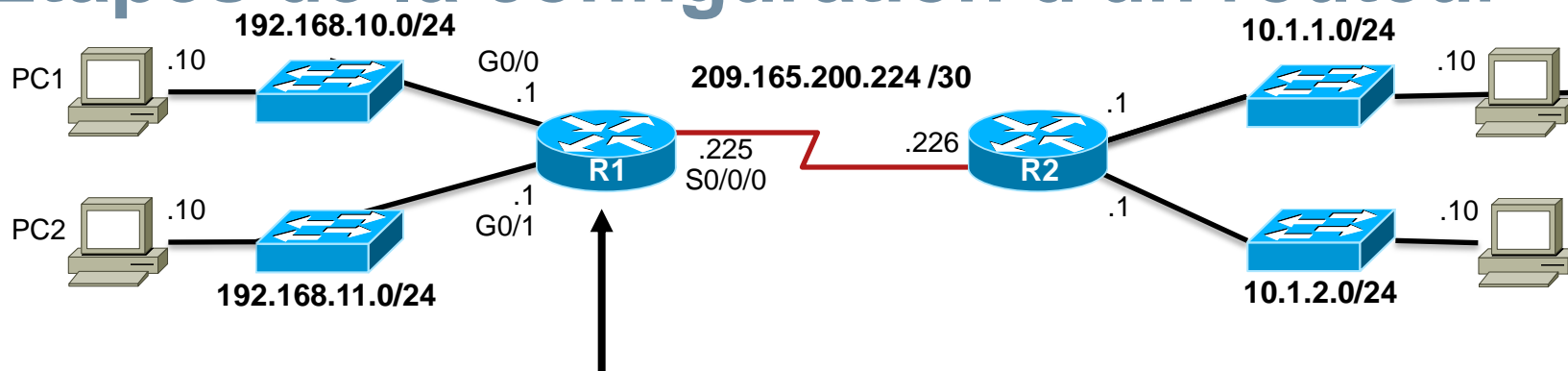
# Configuration d'un routeur Cisco





## Configuration des paramètres initiaux

# Étapes de la configuration d'un routeur



```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.
Terminez par CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

OU

```
Router> en
Router# conf t
Enter configuration commands, one per line.
Terminez par CNTL/Z.
Router(config)# ho R1
R2(config)#
```

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

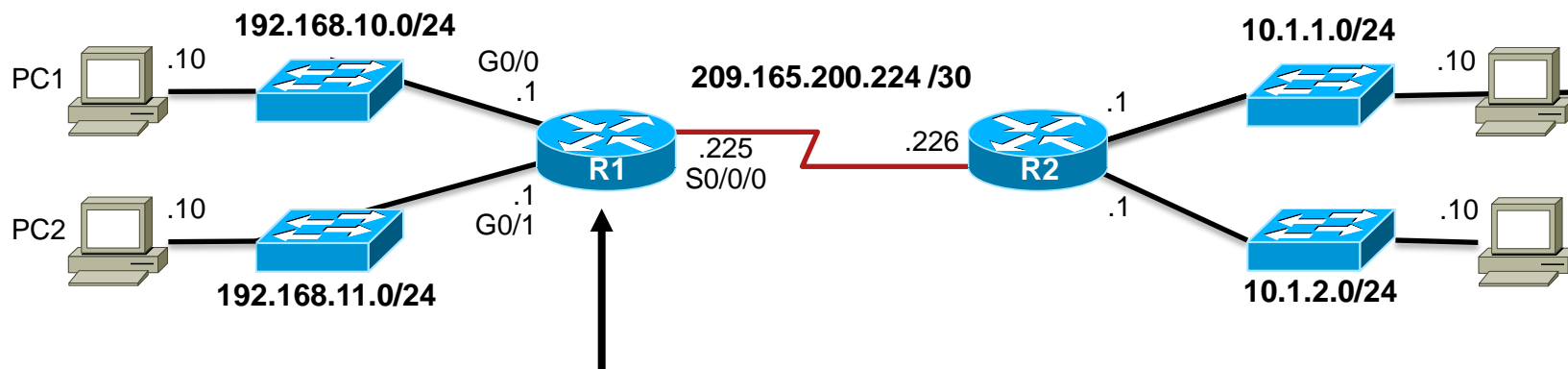
```
R1(config)# banner motd #
Entrez le TEXTE du message. End with the character
'#'.
*****
WARNING: Unauthorized access is prohibited!
*****
N°
R1(config)#
```

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```



## Configuration des interfaces

# Configuration des interfaces LAN



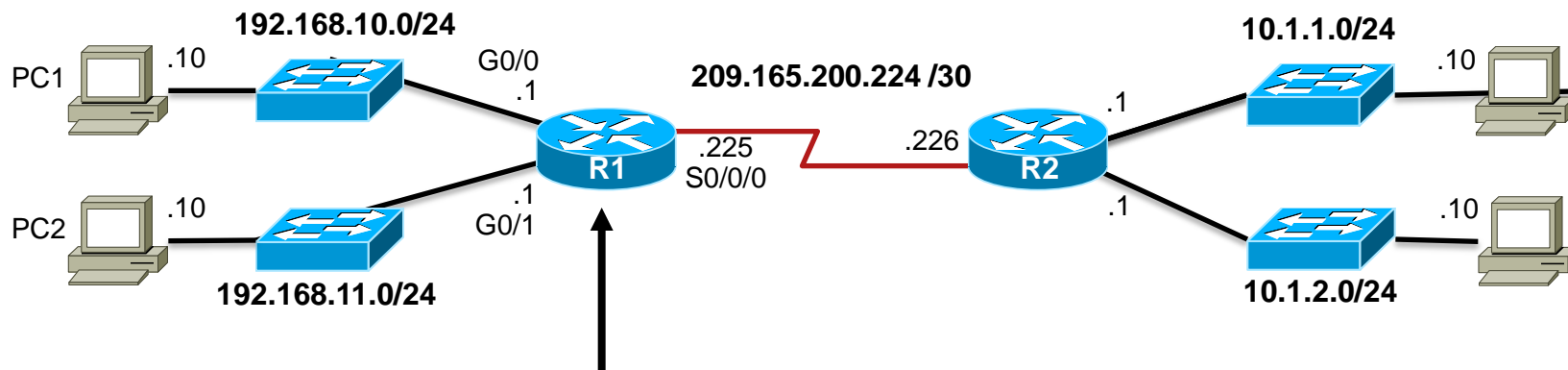
```
R1# conf t
Enter configuration commands, one per line.  Terminez par CNTL/Z.
R1(config)#
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# description Link to LAN-10
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
R1(config-if)# exit
R1(config)#
R1(config)# int g0/1
R1(config-if)# ip add 192.168.11.1 255.255.255.0
R1(config-if)# des Link to LAN-11
R1(config-if)# no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
R1(config-if)# exit
R1(config)#
```





# Configuration des interfaces

## Vérification de la configuration des interfaces



```
R1# show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0       192.168.10.1    YES manual  up          up
GigabitEthernet0/1       192.168.11.1    YES manual  up          up
Serial0/0/0               209.165.200.225 YES manual  up          up
Serial0/0/1               unassigned      YES NVRAM   administratively down down
Vlan1                     unassigned      YES NVRAM   administratively down down
R1#
R1# ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209 165 200 226, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
R1#
```



## Configuration d'un routeur Cisco

# Configuration de la passerelle par défaut

**Microsoft TCP/IP Properties** [?] [X]

IP Address | DNS | WINS Address | DHCP Relay | Routing

An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter:

☐ Obtain an IP address from a DHCP server  
☒ Specify an IP address

IP Address:   
 Subnet Mask:   
 Default Gateway:

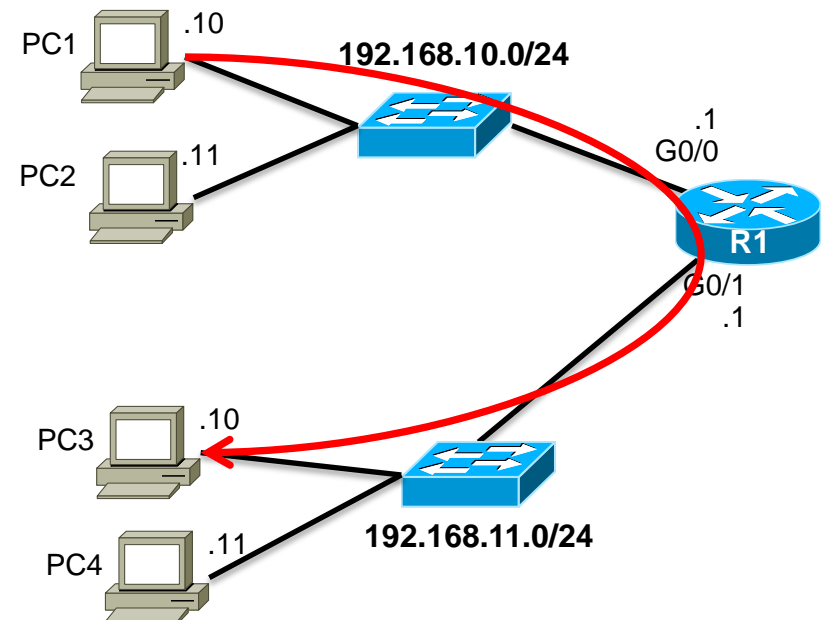
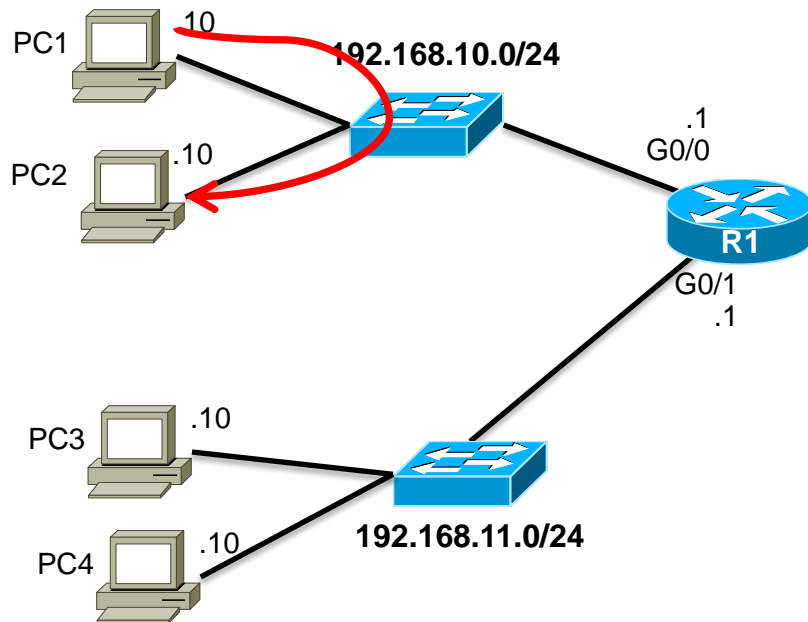
Advanced...

OK Cancel Apply



## Configuration de la passerelle par défaut

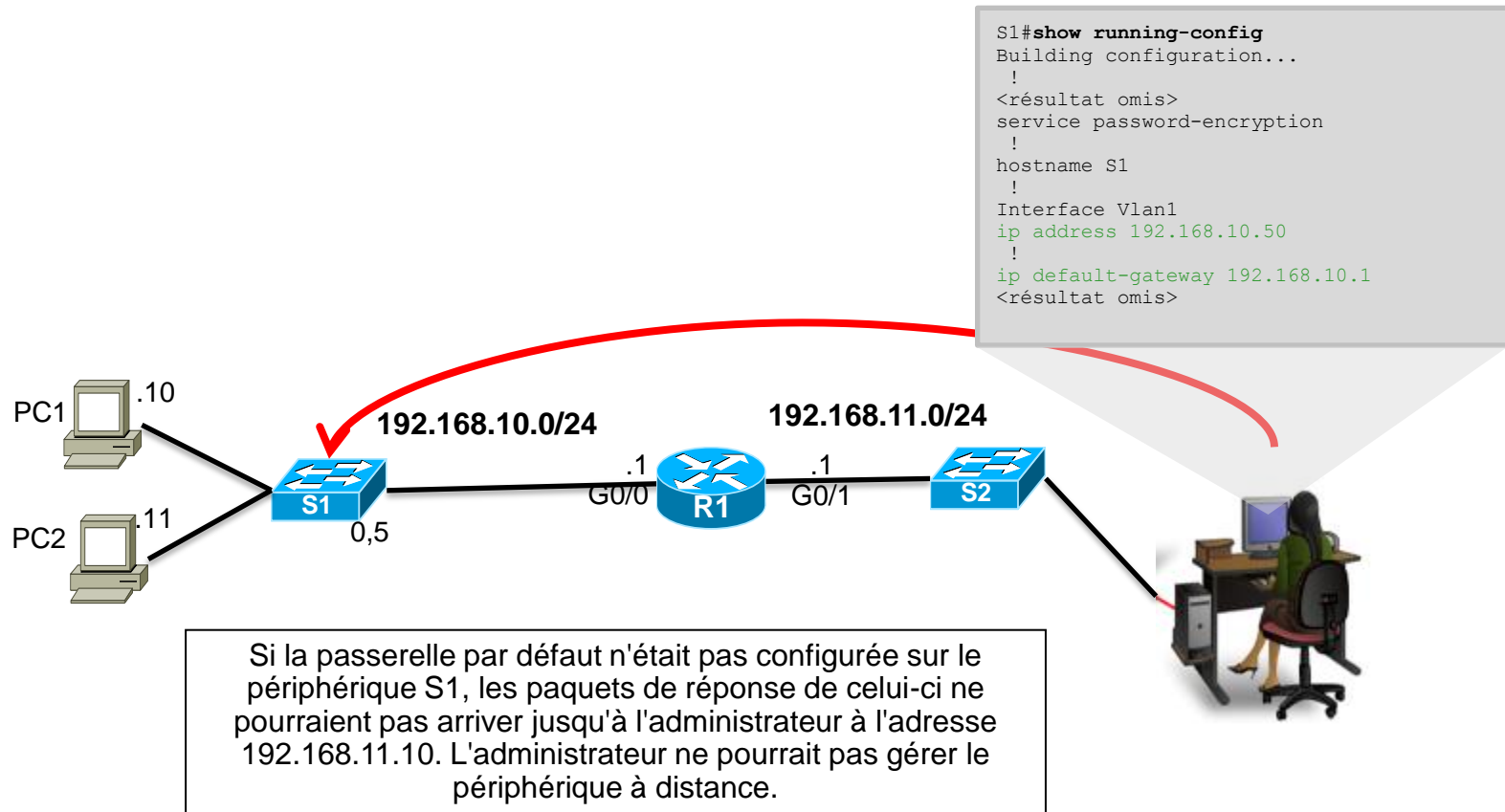
# Passerelle par défaut sur un hôte





## Configuration de la passerelle par défaut

# Passerelle par défaut sur un commutateur





## La couche réseau

# Résumé

Dans ce chapitre, vous avez appris les notions suivantes :

- La couche réseau, ou couche 3 du modèle OSI, fournit des services permettant aux périphériques finaux d'échanger des données sur le réseau.
- La couche réseau utilise quatre fonctions de base : l'adressage IP, l'encapsulation, le routage et la désencapsulation.
- Internet repose essentiellement sur l'IPv4, qui est toujours le protocole de couche réseau le plus répandu.
- Un paquet IPv4 contient l'en-tête IP et les données utiles.
- Une nouvelle version de IP (IPv6) est définie pour faire face aux limitations de IPv4
- L'en-tête simplifié IPv6 offre plusieurs avantages par rapport à l'IPv4, y compris une meilleure efficacité du routage, des en-têtes d'extension simplifiés et le traitement par flux.



## La couche réseau

# Résumé

Dans ce chapitre, vous avez appris les notions suivantes :

- La couche réseau est également responsable du routage.
- Les hôtes ont besoin d'une table de routage locale pour s'assurer que les paquets sont dirigés vers le réseau de destination correct.
- La route locale par défaut est la route à la passerelle par défaut.
- La passerelle par défaut est l'adresse IP d'une interface de routeur connectée au réseau local.
- Lorsqu'un routeur, tel que la passerelle par défaut, reçoit un paquet, il examine l'adresse IP de destination pour déterminer le réseau de destination.



## La couche réseau

# Résumé

Dans ce chapitre, vous avez appris les notions suivantes :

- La table de routage d'un routeur stocke des informations sur les routes connectées directement et les routes distantes vers les réseaux IP.
- Si le routeur possède une entrée dans sa table de routage correspondant au réseau de destination, le routeur transfère le paquet. Sinon le routeur peut transférer le paquet vers sa propre route par défaut, si elle est configurée, ou il abandonne le paquet.
- Les entrées de la table de routage peuvent être configurées manuellement (routage statique), ou les routeurs peuvent se transmettre les informations concernant les routes de manière dynamique à l'aide d'un protocole de routage.
- Pour que les routeurs soient accessibles, l'interface de routeur doit être configurée.





## L'adressage IP

# Résumé

- Les adresses IP sont hiérarchiques et comportent des parties réseau, sous-réseau et hôte.
- Une adresse IP peut représenter tout un réseau, un hôte particulier ou l'adresse de diffusion du réseau.
- Le préfixe ou masque de sous-réseau sert à déterminer la partie réseau d'une adresse IP.
- Le protocole DHCP permet l'attribution automatique des informations d'adressage (adresse IP, masque de sous-réseau, passerelle par défaut, et d'autres paramètres).
- Les hôtes IPv4 peuvent communiquer de trois façons : monodiffusion, diffusion et multidiffusion.
- Les blocs d'adresses IPv4 privées sont les suivants : 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16.



## L'adressage IP

# Résumé

- Le manque d'espace d'adressage IPv4 motive la migration vers IPv6.
- Une adresse IPv6 se compose de 128 bits alors que les adresses IPv4 en comportent 32.
- La longueur de préfixe sert à indiquer la partie réseau d'une adresse IPv6. Le format suivant est utilisé : adresse IPv6/longueur de préfixe.
- Il existe trois types d'adresses IPv6 : monodiffusion, multidiffusion et anycast (un parmi un groupe).
- Une adresse link-local IPv6 permet à un périphérique de communiquer uniquement avec d'autres périphériques IPv6 qui se trouvent sur cette liaison (sous-réseau)

