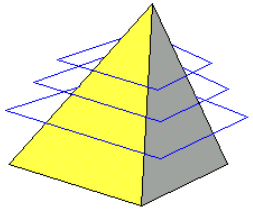


Open SI.NERGIE

KALYST
INGENIERIE INFORMATIQUE

Cours Réseaux

Open SI.nergie / Kalyst

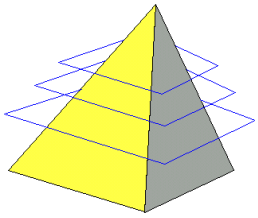
COURS RÉSEAUX

Patrick Girard
patrick.girard@ip-training.fr / patrick.girard@kalyst.fr

Instructeur Certifié depuis Octobre 2001 – Glasgow LTS - **CCAI** (CCNA: CSCO10362533) – Copenhague 2001
CCNP 1 (**BSCI**) 7/2004; CCNP2 (**ISCWN**) 10/2009; CCNP 3 (**BCMSN**) 8/2005;
CCNP4 (TSHOOT) 12/2010 – Birmingham UCE
Network Security I (**NS1**) 2/2006 – Birmingham UCE
Network Security II (**NS2**) 7/2006 - Glasgow LTS
Cisco Airespace Wireless (**CAIAM**) 3/2006 – Nice/Maidenhead/Amsterdam – Daclem
ACSE OmniSwitch R6 – 11/2006 - Brest Alcatel University

KALYST
INGENIERIE INFORMATIQUE

Contenu de la formation



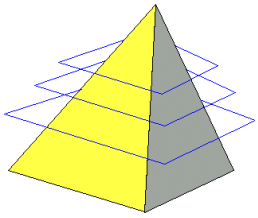
- **Concepts à la base d'Internet Protocol**
  - Comprendre pourquoi IP est devenu le standard de fait de toutes les communications
- **Architecture de réseaux IP**
  - Distinguer les différents réseaux IP d'un LAN
  - Architecture physique versus Architecture logique
- **Pile de protocoles et de services**
  - Sous les acronymes, les services à l'utilisateur

CISCO
Networking Academy

Objectifs de la formation

- Pratiquer (un peu) pour comprendre
- Savoir distinguer les équipements réseaux
- Savoir diagnostiquer de simples pannes
- Pouvoir être plus précis en cas d'appel à une hot-line (interne ☺)
- Devenir un utilisateur éclairé

Histoire

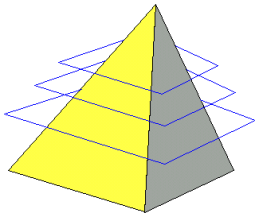


- 1971 : **Louis Pouzin** propose un concept novateur : la **commutation de paquets**

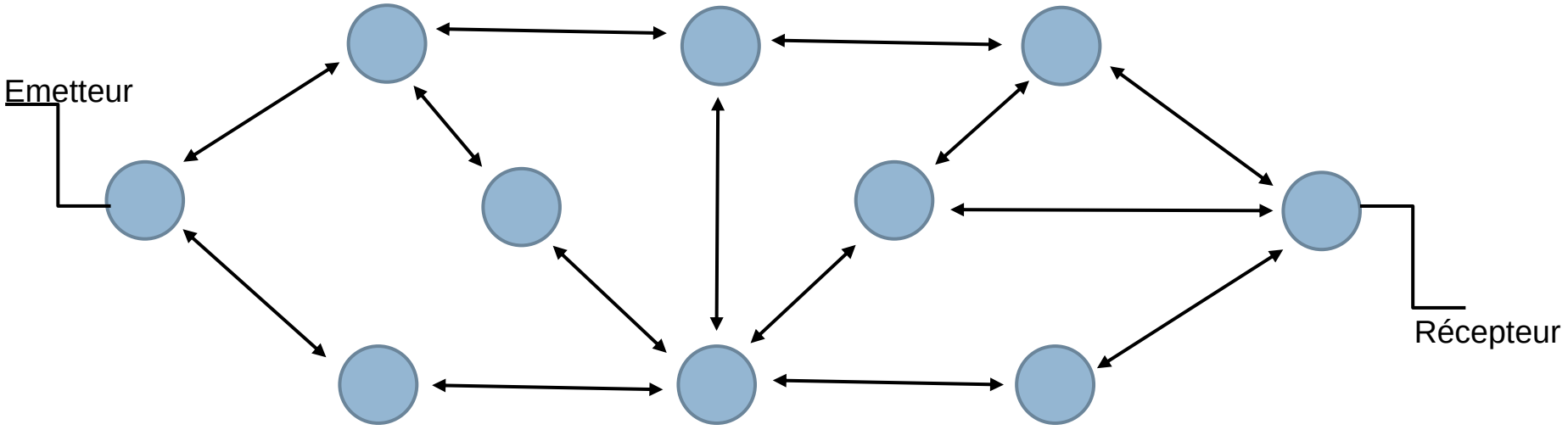
« Louis Pouzin, polytechnicien et chercheur de très grand talent, (est à l'époque) venu proposer un projet de réseau maillé d'ordinateurs basé sur quelque chose de totalement nouveau : la commutation de paquets. »
Maurice Allègre

- 1974 : Vinton Cerf and Bod Kahn publient un article via l'IEEE : A Protocol for **Packet Network Inter**communication
- 1984 : Le Transmission Control Program est divisé en deux parties (couches) qui s'intègrent au modèle OSI : **Transmission Control Protocol** et **Internet Protocol**

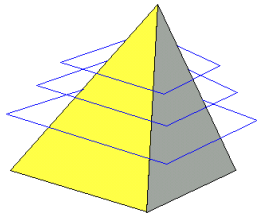
Orienté connexion



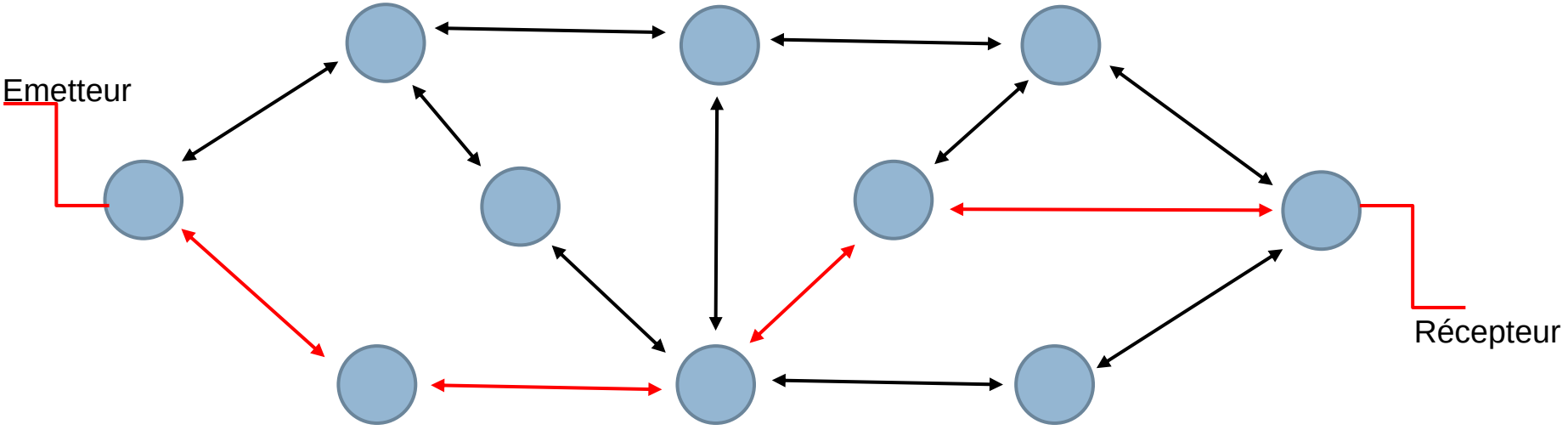
- Le circuit est établi au préalable
- Les données empruntent toutes le même chemin prédéfini



Orienté connexion

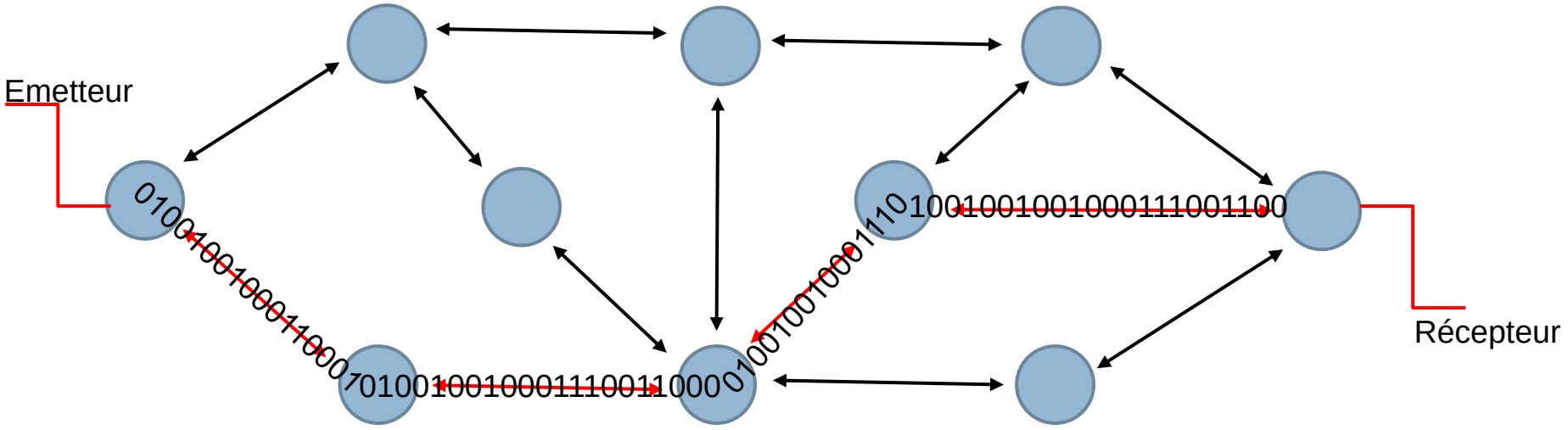


- **Le circuit est établi au préalable**
- Les données empruntent toutes le même chemin prédéfini

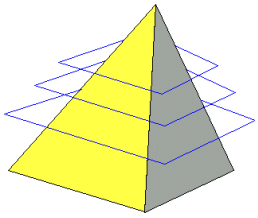


Orienté connexion

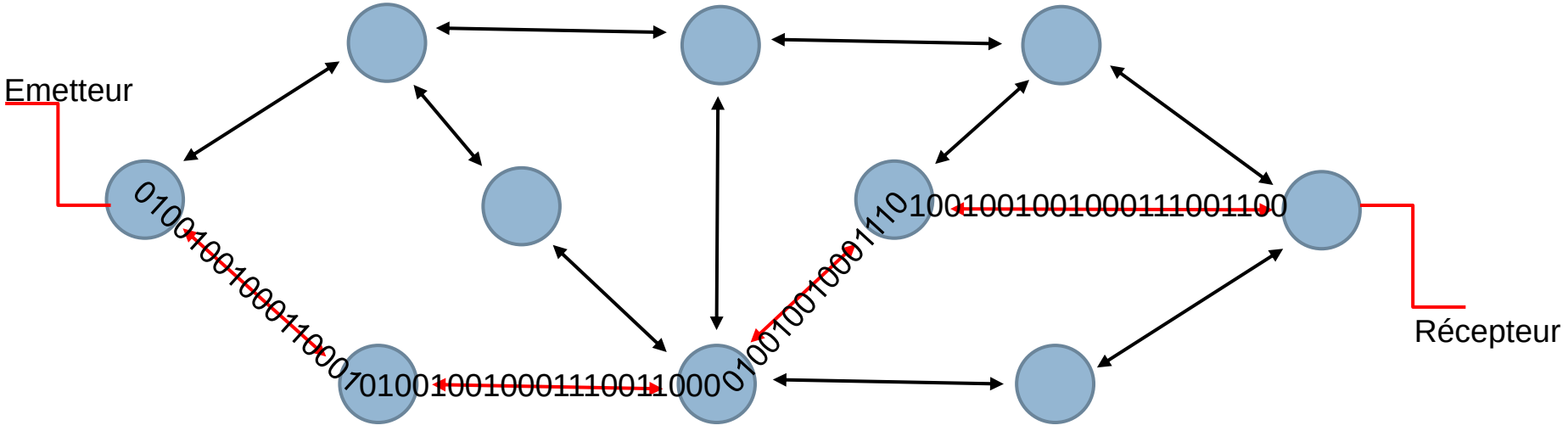
- Le circuit est établi au préalable
- **Les données empruntent toutes le même chemin prédéfini**



Orienté connexion



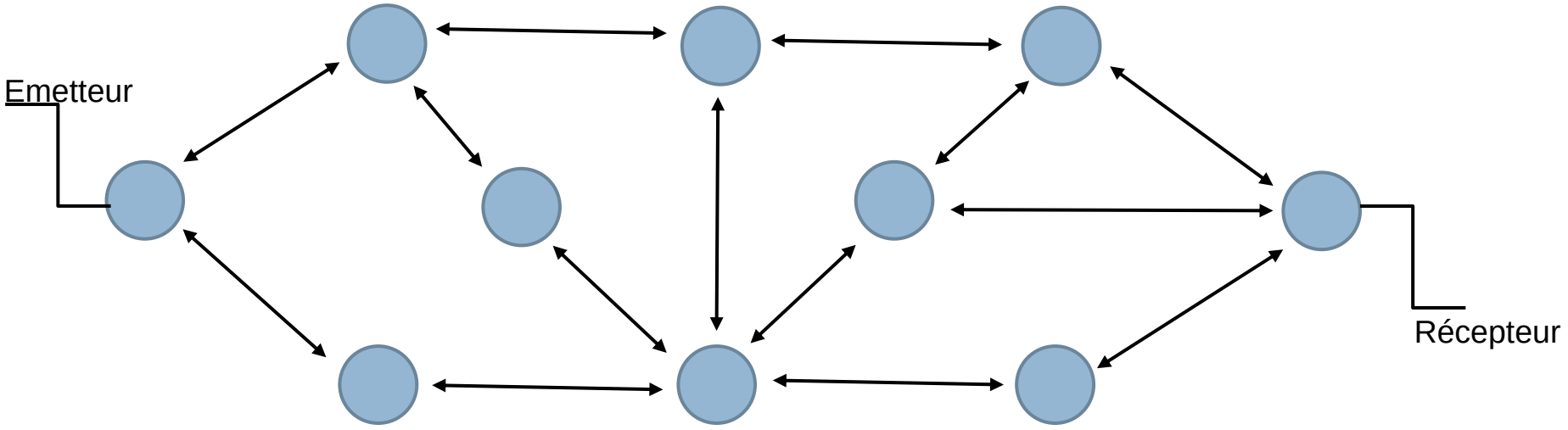
- Le circuit est établi au préalable
- **Les données empruntent toutes le même chemin prédéfini**



Commutation de circuits

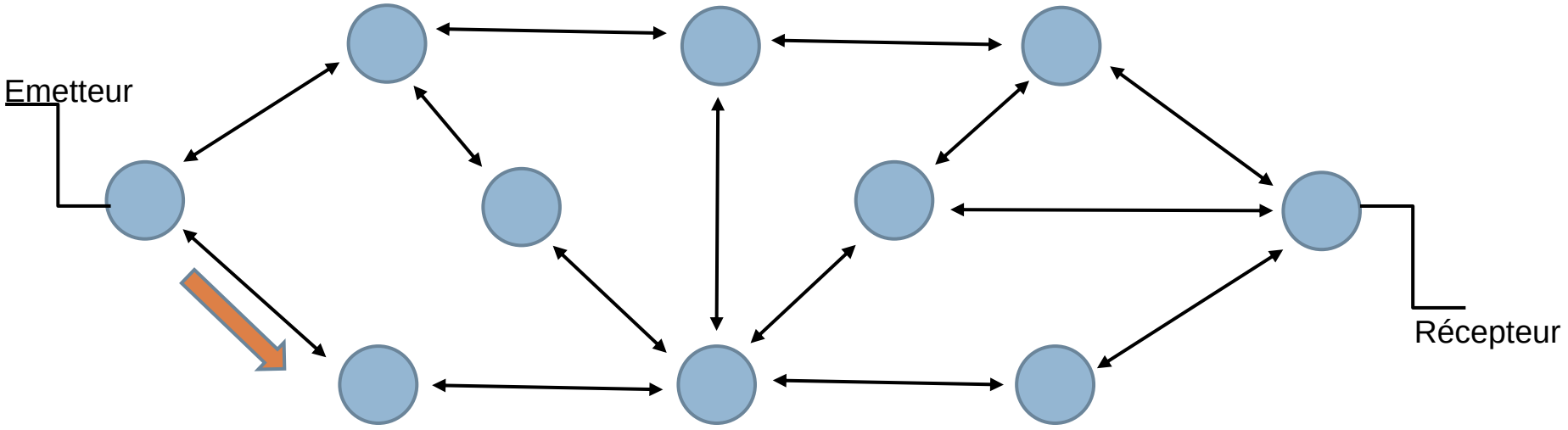
Déconnecté

- **Aucun circuit prédéfini**
- Chaque « paquet » de données connait son adresse de destination

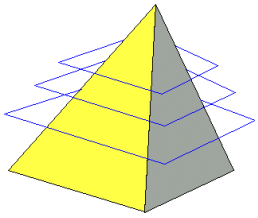


Déconnecté

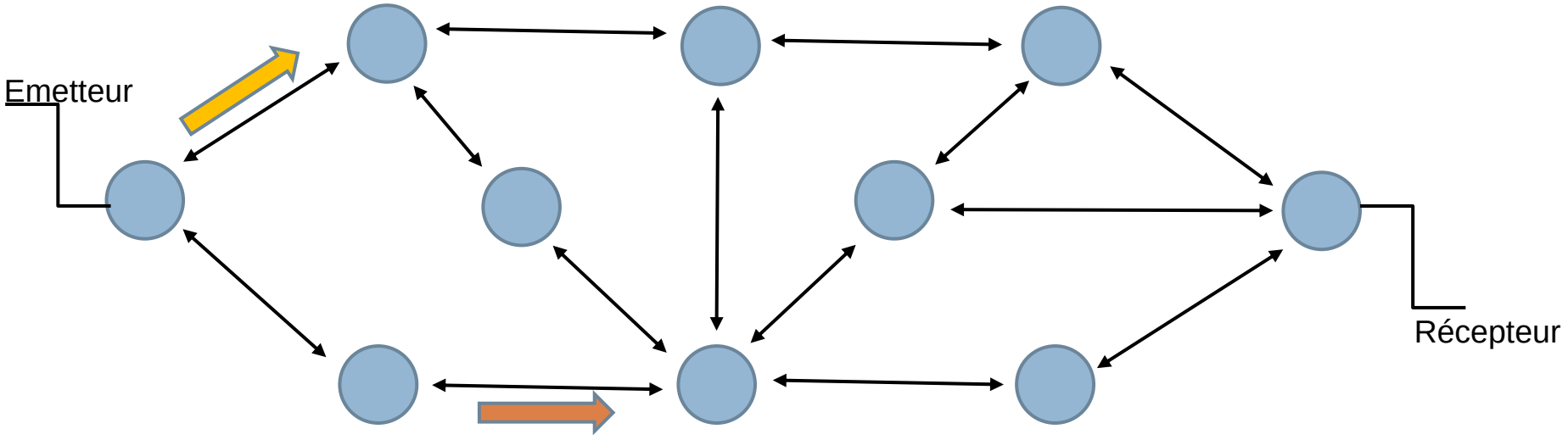
- Aucun circuit prédéfini
- **Chaque « paquet » de données connait son adresse de destination**



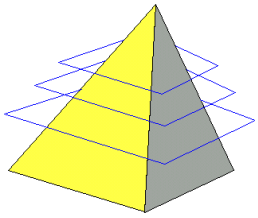
Déconnecté



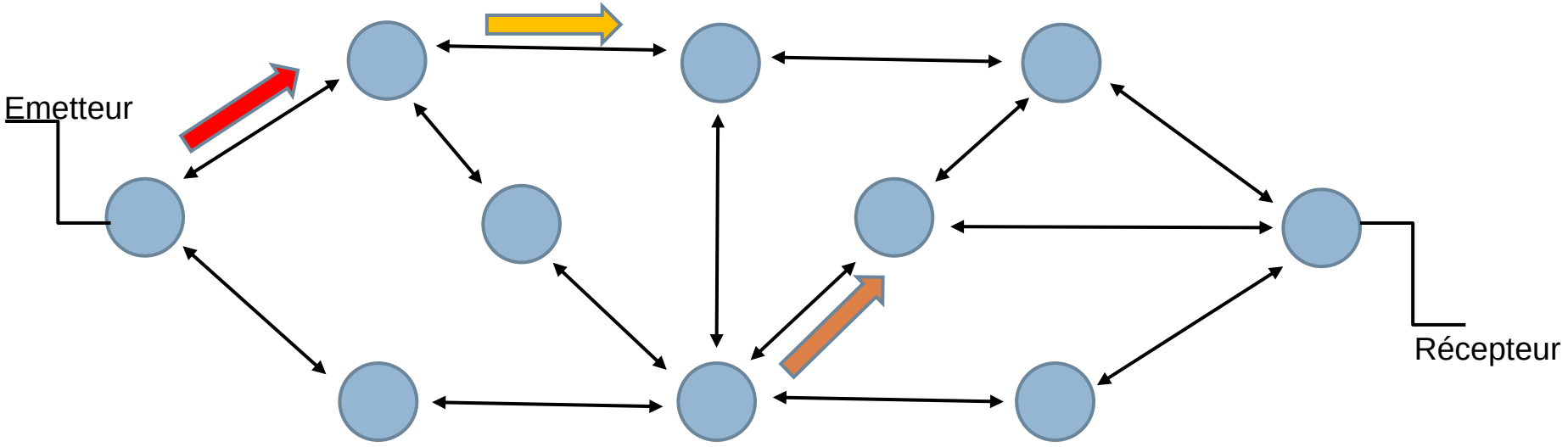
- Aucun circuit prédéfini
- **Chaque « paquet » de données connait son adresse de destination**



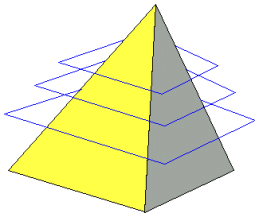
Déconnecté



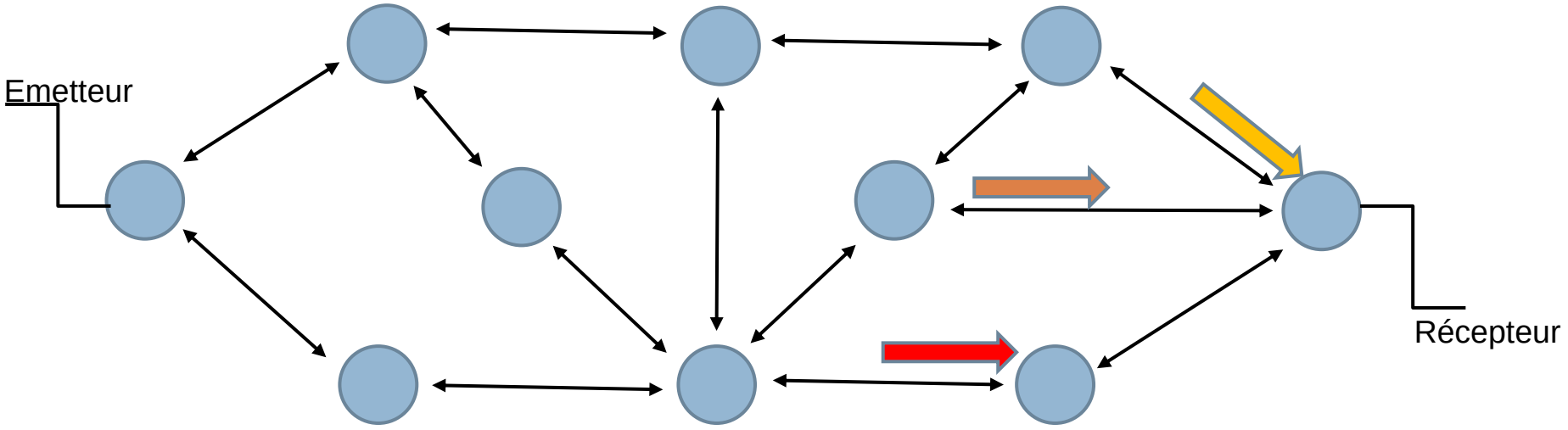
- Aucun circuit prédéfini
- **Chaque « paquet » de données connait son adresse de destination**



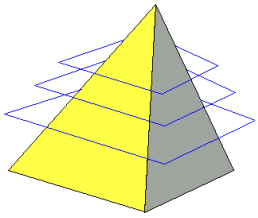
Déconnecté



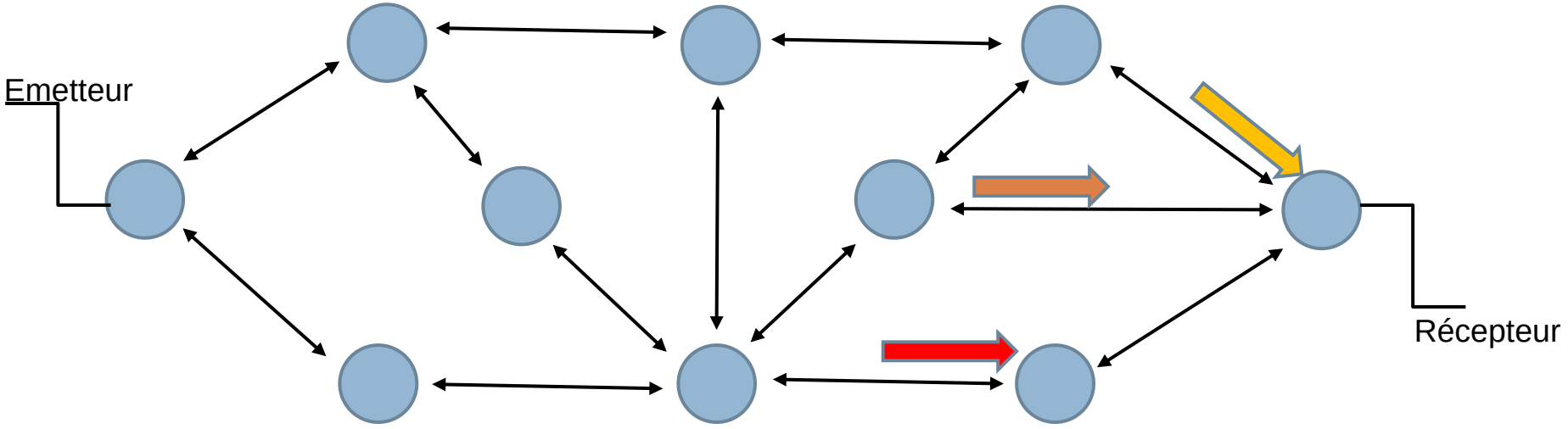
- Aucun circuit prédéfini
- **Chaque « paquet » de données connait son adresse de destination**



Déconnecté



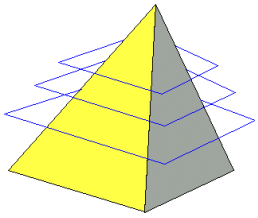
- Aucun circuit prédéfini
- **Chaque « paquet » de données connait son adresse de destination**



Commutation de paquets

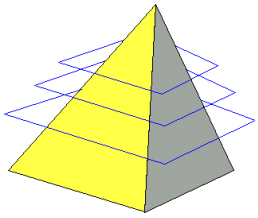
KALYST
INGENIERIE INFORMATIQUE

Commutation de paquet



- Le réseau à commutation de paquets nécessite des nœuds d'aiguillage
- Ces ordinateurs (TCProgram) deviennent des **routeurs** (TCProtocol) spécialisés (Cisco Systems)
- Chaque paquet est entièrement chargé en mémoire avant d'être retransmis
- Certains paquets sont rejetés en cas de congestion ou de destination inaccessible : **Best Effort Delivery**
- **Alors pourquoi c'est mieux ?**

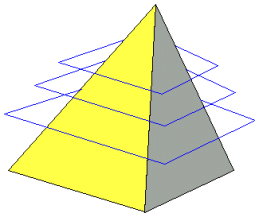
Pourquoi c'est mieux ?



Parce que

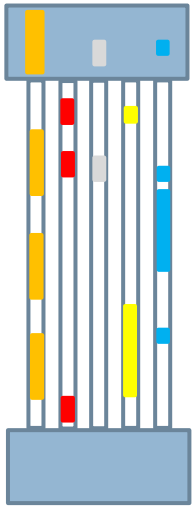
- …la nature du trafic « informatique » est différente
  - Des rafales suivies de silences…
  - Des données non urgentes
  - Des données qui peuvent être perdues quitte à être renvoyées si nécessaire
- …les données peuvent être **découpées** en morceaux
- …les nœuds peuvent organiser des files d'attente pour **remplir** les tuyaux de façon optimale

Se libérer du circuit

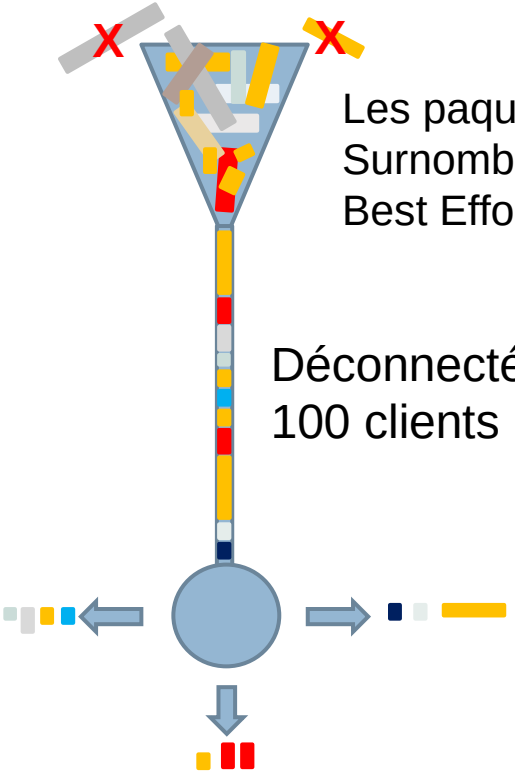


- **Optimisation des tuyaux qui peuvent être partagés**

Orienté Connexion
10 clients



Certains liens réservés sont quasiment vides



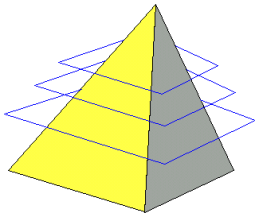
Les paquets en Surnombre sont rejetés : Best Effort Delivery

Déconnecté
100 clients

Les liens réservés sont utilisés à 100%

KALYST
INGENIERIE INFORMATIQUE

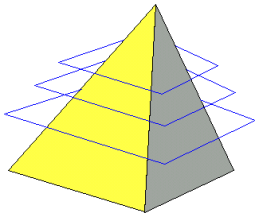
Se libérer du circuit



- Le fait de ne pas avoir à établir un circuit de bout en bout apporte une souplesse cruciale
  - Possibilité de ralentir certains flux au profit d'autres flux urgents : Qualité de Service
  - Insensibilité (relative) à la perte d'un nœud
  - **Optimisation des tuyaux qui peuvent être partagés**
- Le « Best Effort Delivery » force les applications à être insensibles à la perte de paquets
- => Modèle en couche

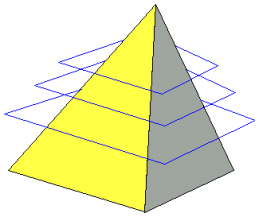
CISCO
Networking Academy

Sociologie



- Au-delà de la nouveauté de la vision « datagramme », la méthode a beaucoup influencé le développement d'Internet
  - Technologies « Open » vs « Propriétaires »
  - Formes associatives vs Entreprises privées
  - Culture différente : Informatique vs Télécomms
- Ces mêmes leviers d'entrainement ont :
  - Amené la victoire par KO d'Ethernet contre Token Ring
  - Installé IP comme protocole de communication universel

RFC, bureau IEEE… (digression)



- Une Request For Comment démarre le processus de standardisation de fait
- Le bureau concerné accepte ou non la RFC et désigne éventuellement un sous-bureau
- Les gens bossent…
- Et cela aboutit, parfois, à une nouvelle « standard »

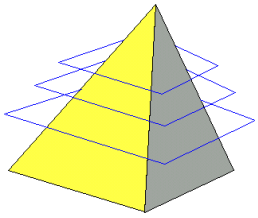
Exemple de Hiérarchie des protocoles

IEEE 802

IEEE 802.11 – Wireless Lan
802.11b
802.11g
IEEE 802.15 - Bluetooth
IEEE 802.2 - LLC
IEEE 802.3 – Ethernet
802.3 u - Fast Ethernet
802.3 x - Full Duplex
IEEE 802.4 - Token Bus
IEEE 802.5 - Token Ring
…

KALYST
INGENIERIE INFORMATIQUE

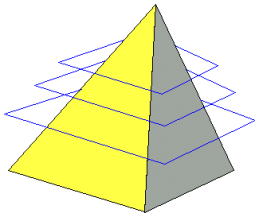
Dynamique industrielle



- Du très grand nombre d'idées farfelues émergent des standards de fait (Ethernet, RIP)
- … ou des protocoles largement discutés via les Request for Comment (RFC)
- Dans tous les cas, un protocole ouvert s'impose inévitablement au plus grand nombre d'utilisateurs
- Le grand nombre d'utilisateurs fait baisser les prix (donc plus d'utilisateurs encore) et fait progresser les technologies (donc plus d'utilisateurs encore)
- **CQFD !**

KALYST
INGENIERIE INFORMATIQUE

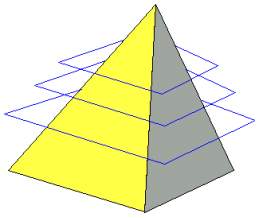
Dynamique industrielle



- Du très grand nombre d'idées farfelues émergent des standards de fait (Ethernet, RIP)
- … ou des protocoles largement discutés via les Request for Comment (RFC)
- Dans tous les cas, un protocole ouvert s'impose inévitablement au plus grand nombre d'utilisateurs
- Le grand nombre d'utilisateurs fait baisser les prix (donc plus d'utilisateurs encore) et fait progresser les technologies (donc plus d'utilisateurs encore)
- **CQFD !**

En 1984 la création tout azimut est normalisée via le Modèle OSI

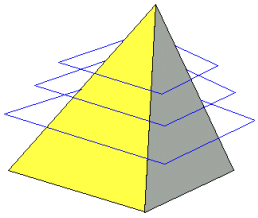
Modèle en couche : Modèle OSI



Open System Interconnection reference model

- Conçu par l'ISO en 1984
- Objet : créer un cadre conceptuel à la problématique d'interconnexion des réseaux
- But : favoriser l'évolution technologique en assurant l'interopérabilité sans nuire à la vitalité des acteurs
- Le moyen :
  - Différencier 7 couches indépendantes
  - Normaliser pour chaque couche l'interface avec la couche supérieure et la couche inférieure
  - Normaliser chaque couche en terme de service pour la couche supérieure

Modèle OSI

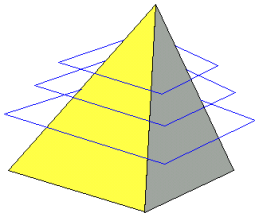


Open System Interconnection reference model

- Il permet de sérier les problématiques de communication sur le réseau en éléments plus petits et plus simples;
- Il uniformise les éléments du réseau afin de faciliter le développement et le soutien multi constructeur;
- Il permet à différents types de matériel et de logiciel réseau de communiquer entre eux;
- Il empêche les changements apportés à une couche d'affecter les autres couches, ce qui assure un développement plus rapide.

KALYST
INGENIERIE INFORMATIQUE

Modèle OSI

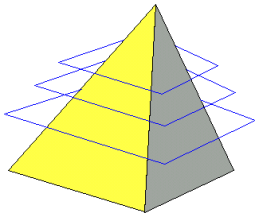


7	Application	Accès au service	Telnet, SMTP, NFS, TFTP, HTTP, FTP…	
6	Présentation	Conversion de format	ASCII, EBCDIC, jpeg, aiff, mpeg, mp3…	
5	Session	Gestion sessions	X-Window System, RPC, NFS, SQL…	
4	Transport Clients, Serveurs	Orienté connexion, contrôle de flux & fiabilité	Segments Ports	TCP
3	Réseau Routeurs	Adressage, Routage, Commutation, Best Effort Del.	Paquets Adresses logiques	IP
2	Liaison NIC, Pont, Switch	Gest. transmission, fiabilité, contrôle de flux, topologie rés	Trames Adresses physiques	LLC, MAC, CSMA/CD
1	Physique Répéteurs, Hubs, …	Transmission bit à bit, spécification physique du lien	01101011011101	Standards EIA/TIA…

CISCO
Networking Academy

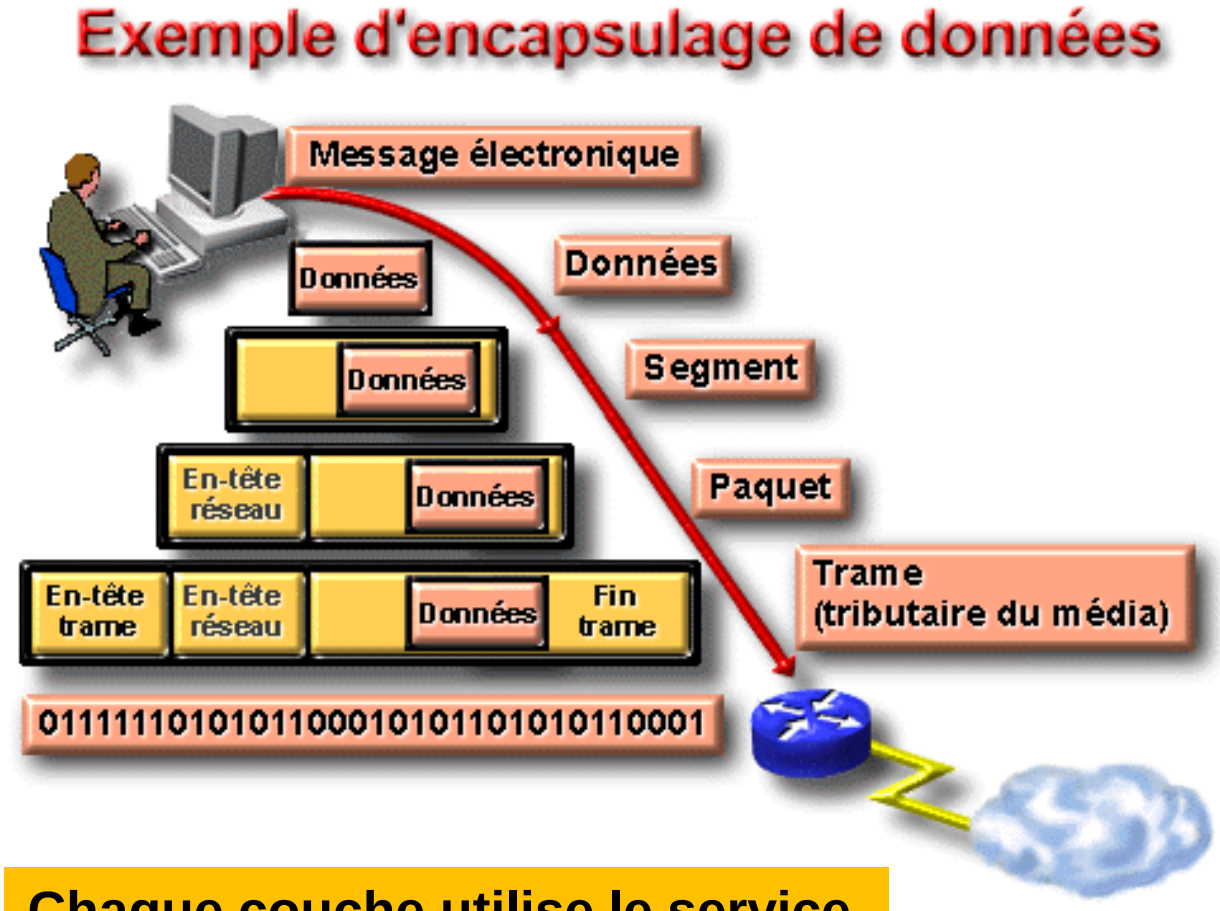
KALYST
INGENIERIE INFORMATIQUE

Internet



- Le modèle en couche libère l'innovation sans remettre en cause toute la chaine
- Les applications sont indépendantes des problématiques de transport
- Les circuits sont virtuels (TCP) ou inexistants (UDP)
- Les nœuds se spécialisent dans des tâches qu'ils réalisent de plus en plus vite
- Le modèle associatif perdure et fait d'Internet un objet bizarre que personne ne contrôle réellement

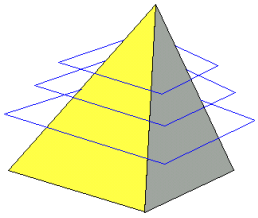
Encapsulation / Désencapsulation



Chaque couche utilise le service offert par la couche inférieure

KALYST
INGENIERIE INFORMATIQUE

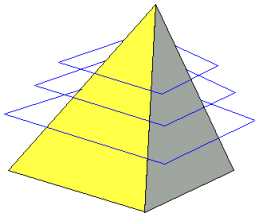
Peer to Peer



7	Application	⟷	7	Application
6	Présentation	⟷	6	Présentation
5	Session	⟷	5	Session
4	Transport	⟷	4	Transport
3	Réseau	⟷	3	Réseau
2	Liaison	⟷	2	Liaison
1	Physique	⟷	1	Physique

CISCO
Networking Academy

Modèle TCP / IP



Intègre OSI 5, 6 & 7

Propose en plus un transport de service non fiable UDP

Intègre OSI 1 & 2

Application	⟷	7 - Application
		6 - Présentation
		5 - Session
Transport	⟷	4 - Transport
Réseau	⟷	3 - Réseau
Accès	⟷	2 - Liaison
		1 - Physique

Service Postal vs IP

- Responsabilité de l'opérateur dans un service postal ?

Service Postal vs IP

- Responsabilité de l'opérateur dans un service postal ?

- Boite aux lettres personnalisée

Service Postal
Foyer

187.25.12.129 / 26

187.25.12.128
.1

Service Postal vs IP

- Responsabilité de l'opérateur dans un service postal ?

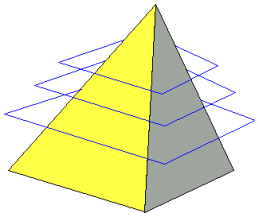
- Boite aux lettres commune à l'immeuble

Service Postal
Distribution interne

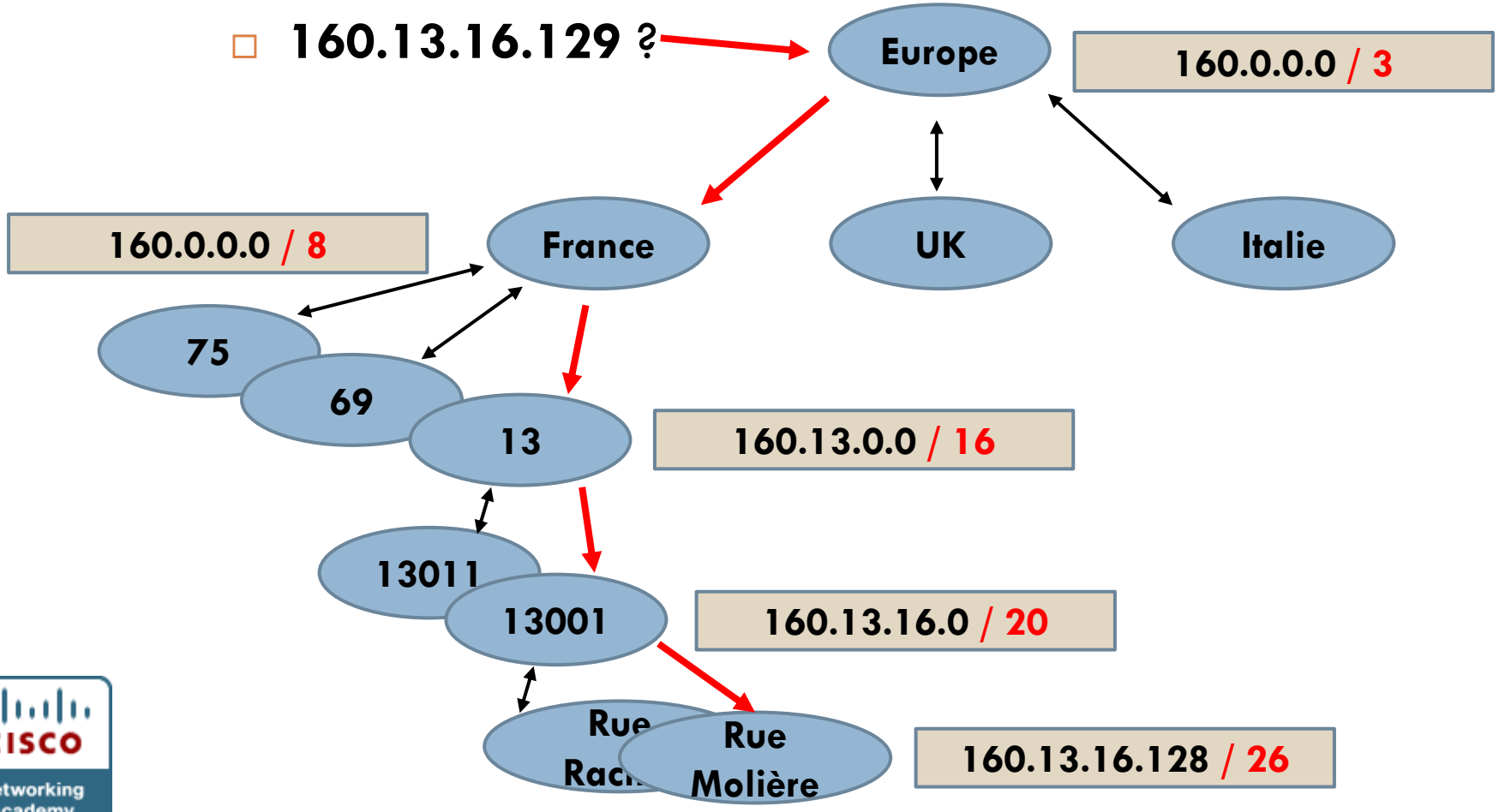
187.25.12.129 / 24

187.25.12.0
.129

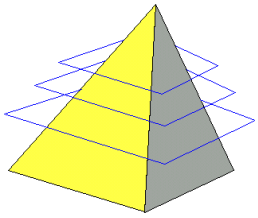
Service Postal vs (idéal) IP

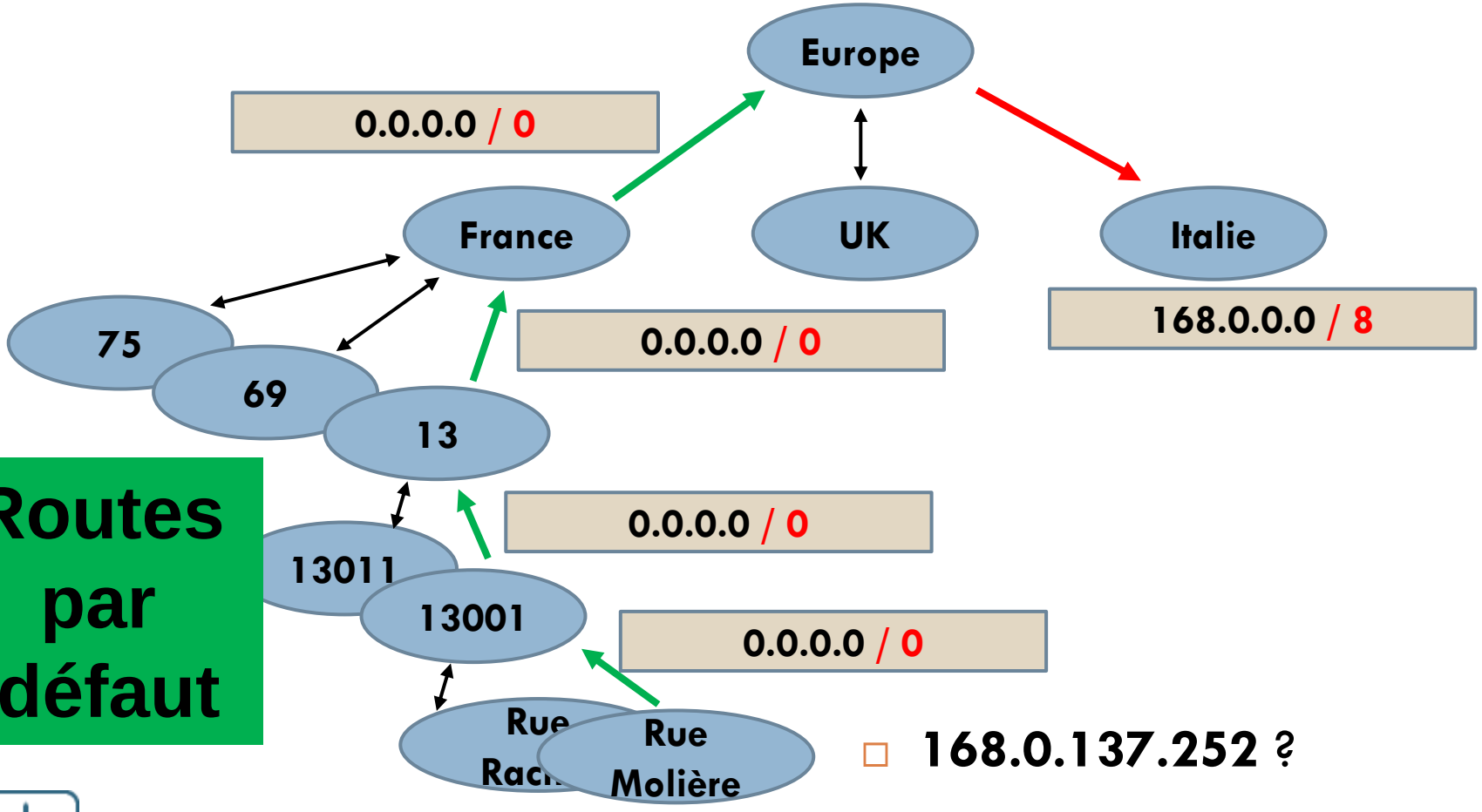


- Routage hiérarchique ?



Service Postal vs (idéal) IP

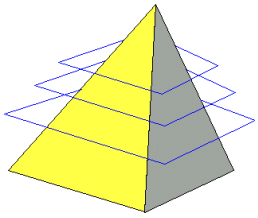




Routes par défaut

- 168.0.137.252 ?

Réalité



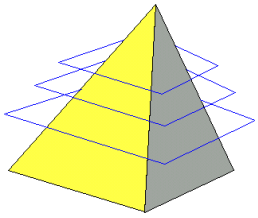
- La commutation de paquets est gérée par les routeurs
  - Quand un routeur reçoit un paquet sur une interface, il cherche à déterminer via quelle interface de sortie il doit transmettre le paquet
  - Pour cela il ne s'intéresse qu'aux routes qu'il connait : la partie « host » des adresses IP n'est pas pris en compte
- Malheureusement les adresses de réseaux ne correspondent que rarement à une localisation géographique =>
  - Les chemins ne sont pas toujours optimaux
  - Les routeurs doivent connaître des milliers de routes

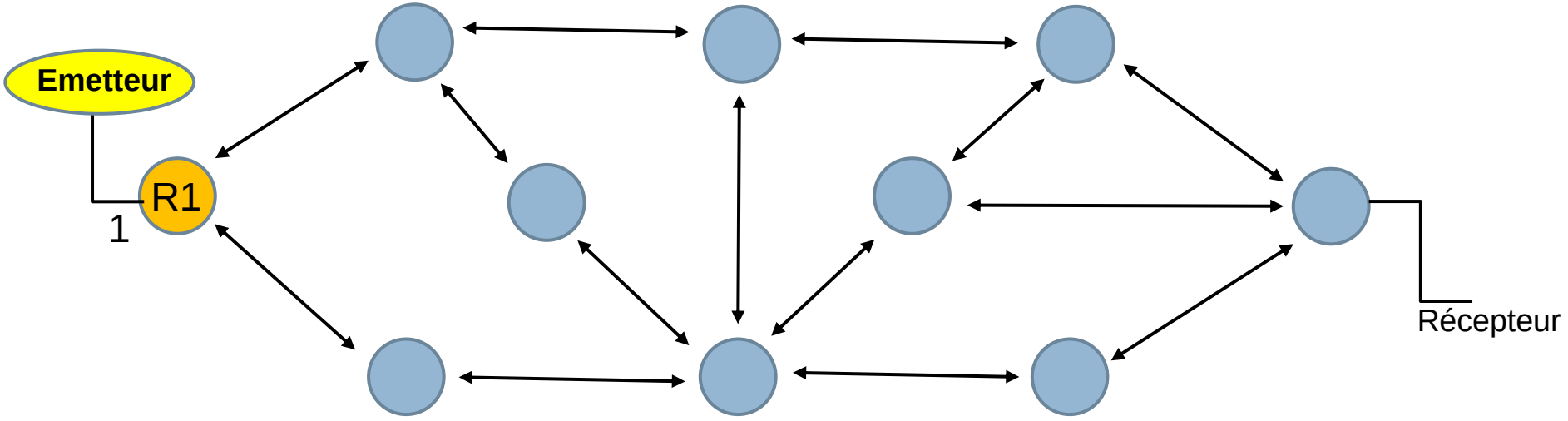
Routeur

- Un routeur est un « ordinateur » spécialisé pour cette tâche, ou une machine standard configurée pour cela.

- Il assure deux tâches essentielles :
  - La **commutation de paquets** : choisir la meilleure interface de sortie en fonction de la destination d'un paquet et des informations de la **table de routage**
  - La gestion des **protocoles de routage** : échanger des informations avec d'autres routeurs pour maintenir et faire évoluer sa **table de routage**.

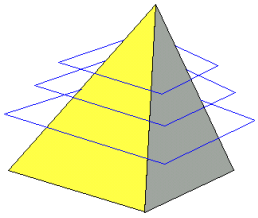
Routeur

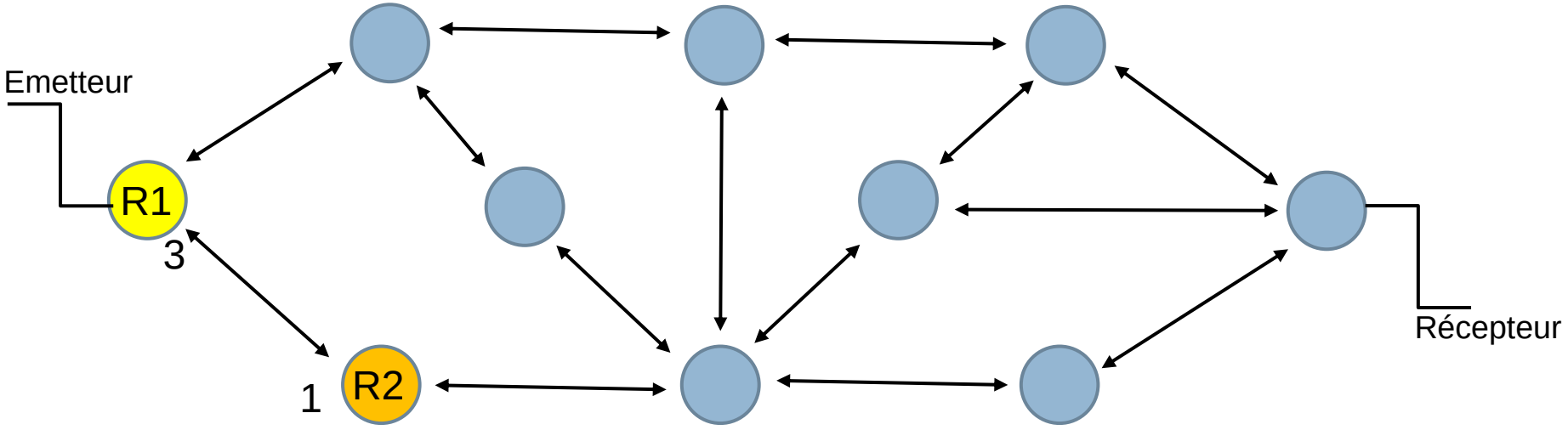




Payload
85.32.14.201 193.32.126.2
MAC Emetteur MAC 51:1 - Passerelle

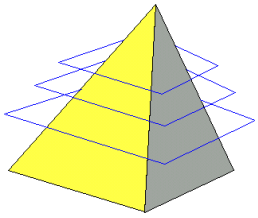
Routeur

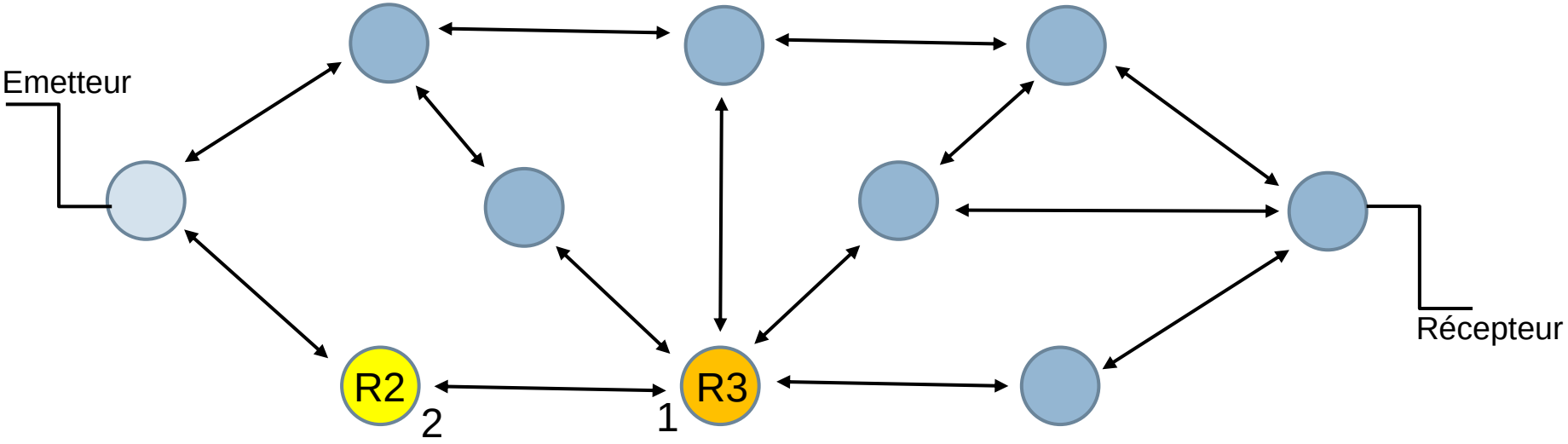




Payload
85.32.14.201 193.32.126.2
MAC R1:3 MAC R2:1

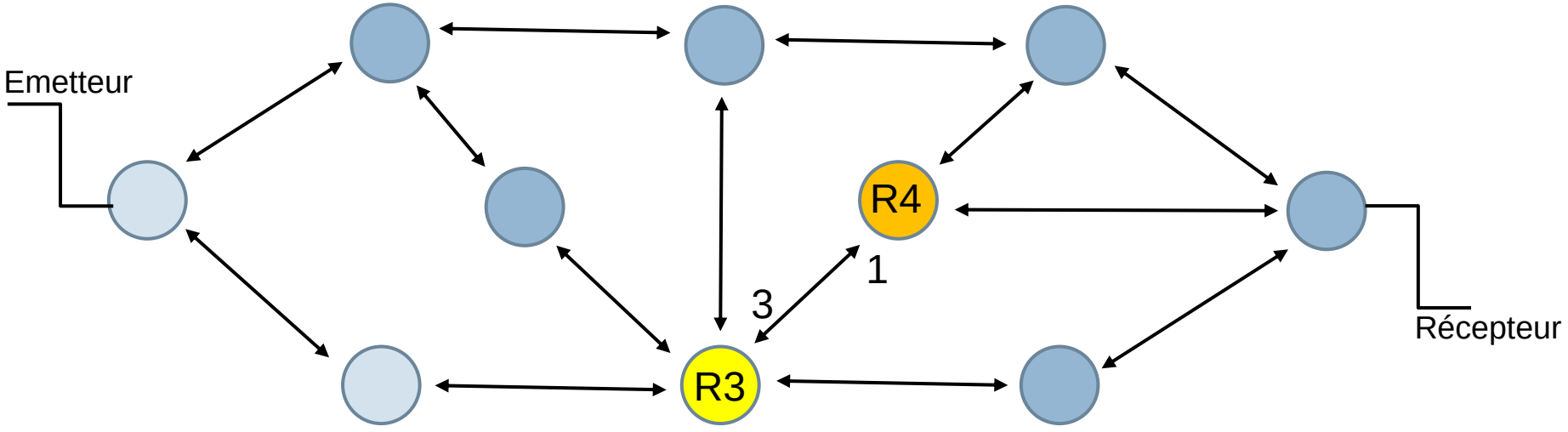
Routeur





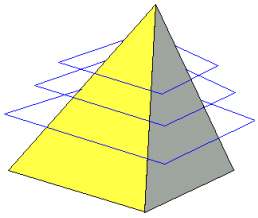
Payload
85.32.14.201 **193.32.126.2**
MAC R2:2 **MAC R3:1**

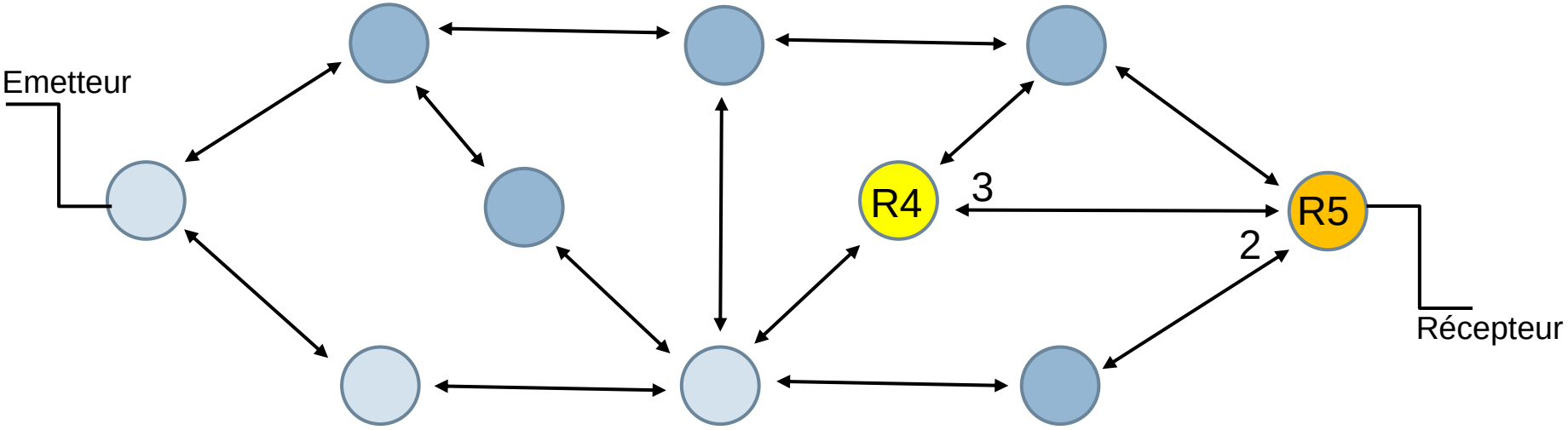
Routeur



Payload
85.32.14.201 193.32.126.2
MAC R3:3 MAC R4:1

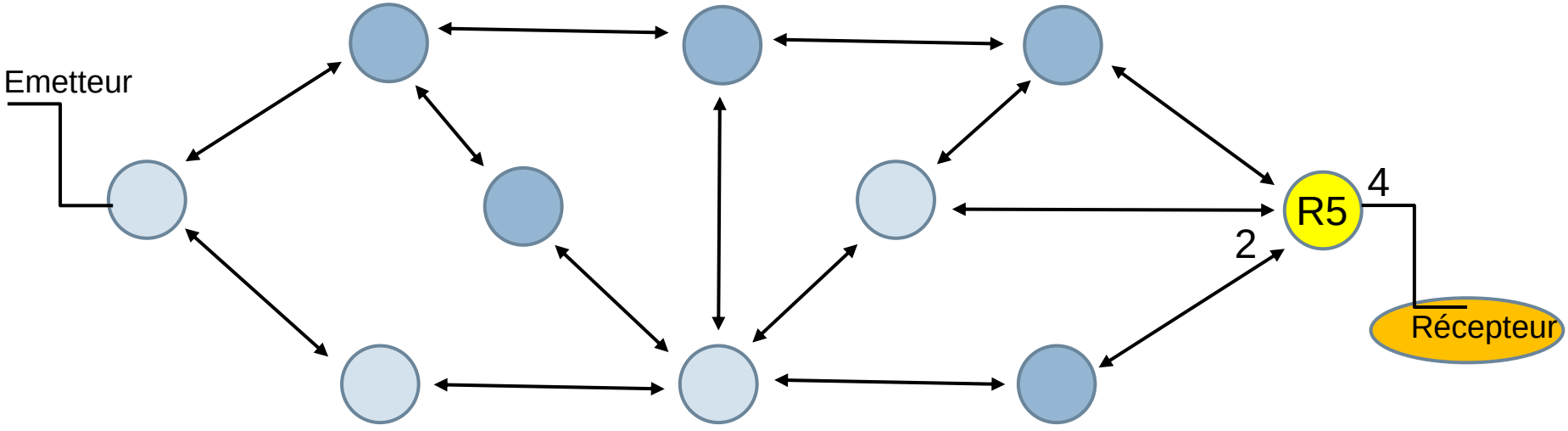
Routeur





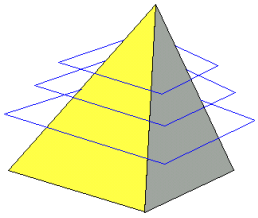
Payload
85.32.14.201 193.32.126.2
MAC R4:3 MAC R5:2

Routeur



Payload
85.32.14.201 **193.32.126.2**
MAC R5:4 - Passerelle **MAC Récepteur**

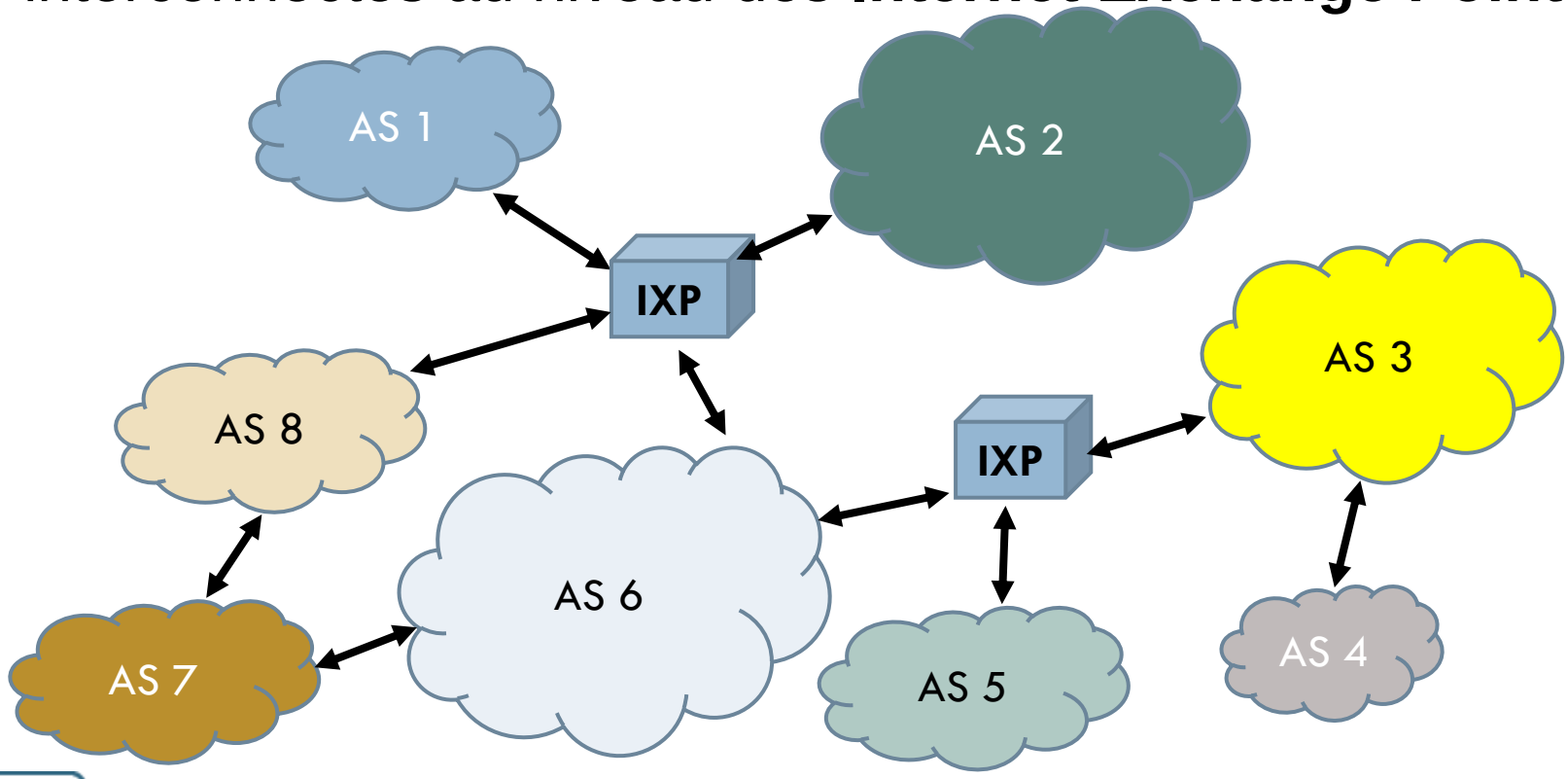
Organisation d'Internet



- Est-ce que un routeur connaît toutes les routes du réseau mondial ?
  - S'il s'agit d'un routeur « **intérieur** » il n'a besoin de connaître que les routes de son propre domaine
  - S'il s'agit d'un routeur « **de bordure** » il n'a besoin de connaître que les super-réseaux des autres grands domaines
- Commutation de paquets
  - Routeur intérieur : si la destination est dans le même domaine : **routage intérieur**
  - Routeur intérieur : si la destination est dans un autre domaine : **route par défaut** vers le **routeur de bordure** le plus proche
  - **Routeur de bordure** : transmet le paquet via l'interface qui ouvre le chemin vers le domaine cible

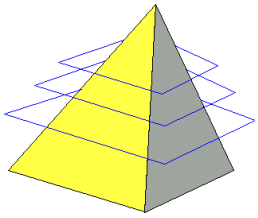
Organisation d'Internet 1/3

Une collection de **systèmes autonomes**, reliés entre eux ou interconnectés au niveau des **Internet Exchange Points**



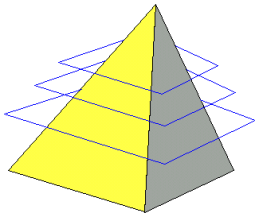
KALYST
INGENIERIE INFORMATIQUE

Internet Exchange Points



KALYST
INGENIERIE INFORMATIQUE

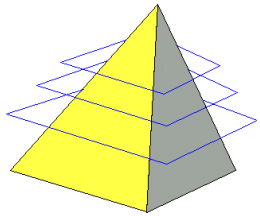
IXP Europe

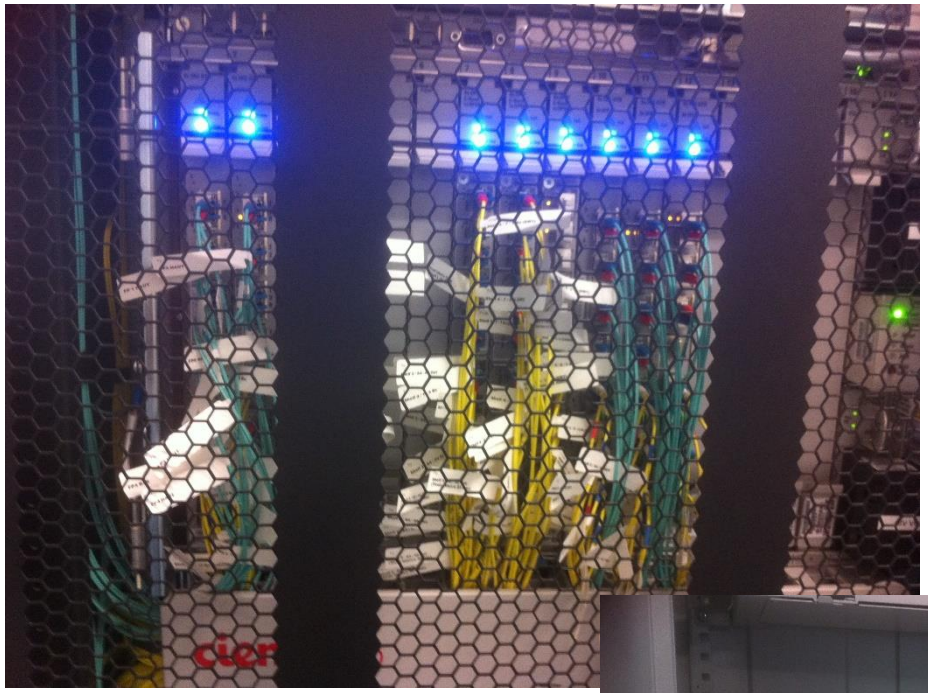


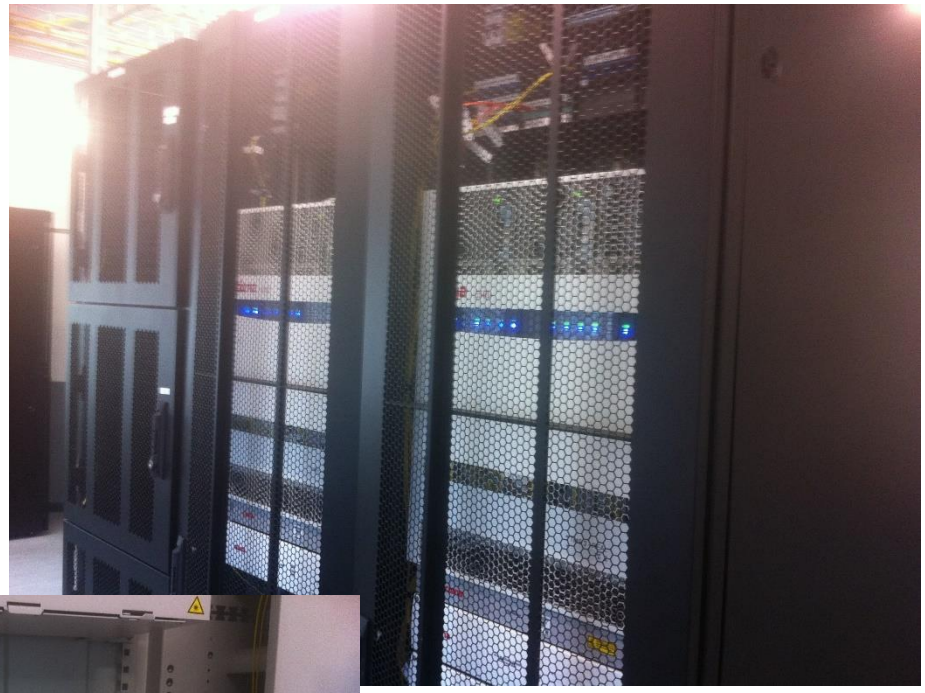
CISCO
Networking Academy

KALYST
INGENIERIE INFORMATIQUE

IXP Interxion – Meet me Room



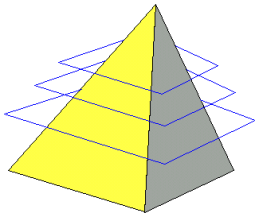


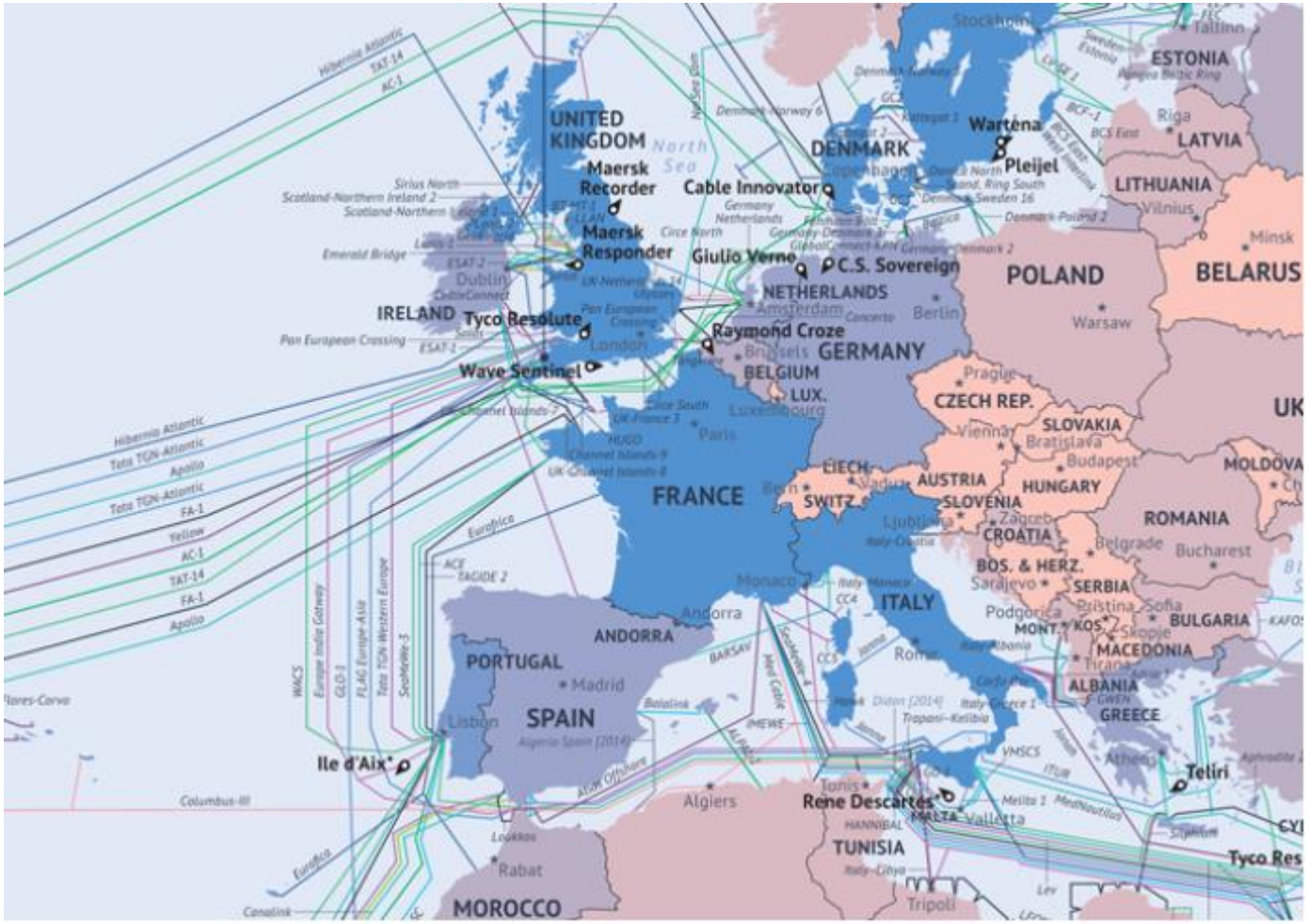


CISCO
Networking Academy

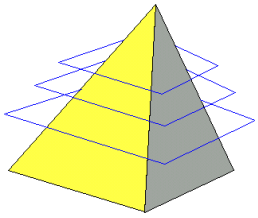
KALYST
INGENIERIE INFORMATIQUE

Câbles sous-marins

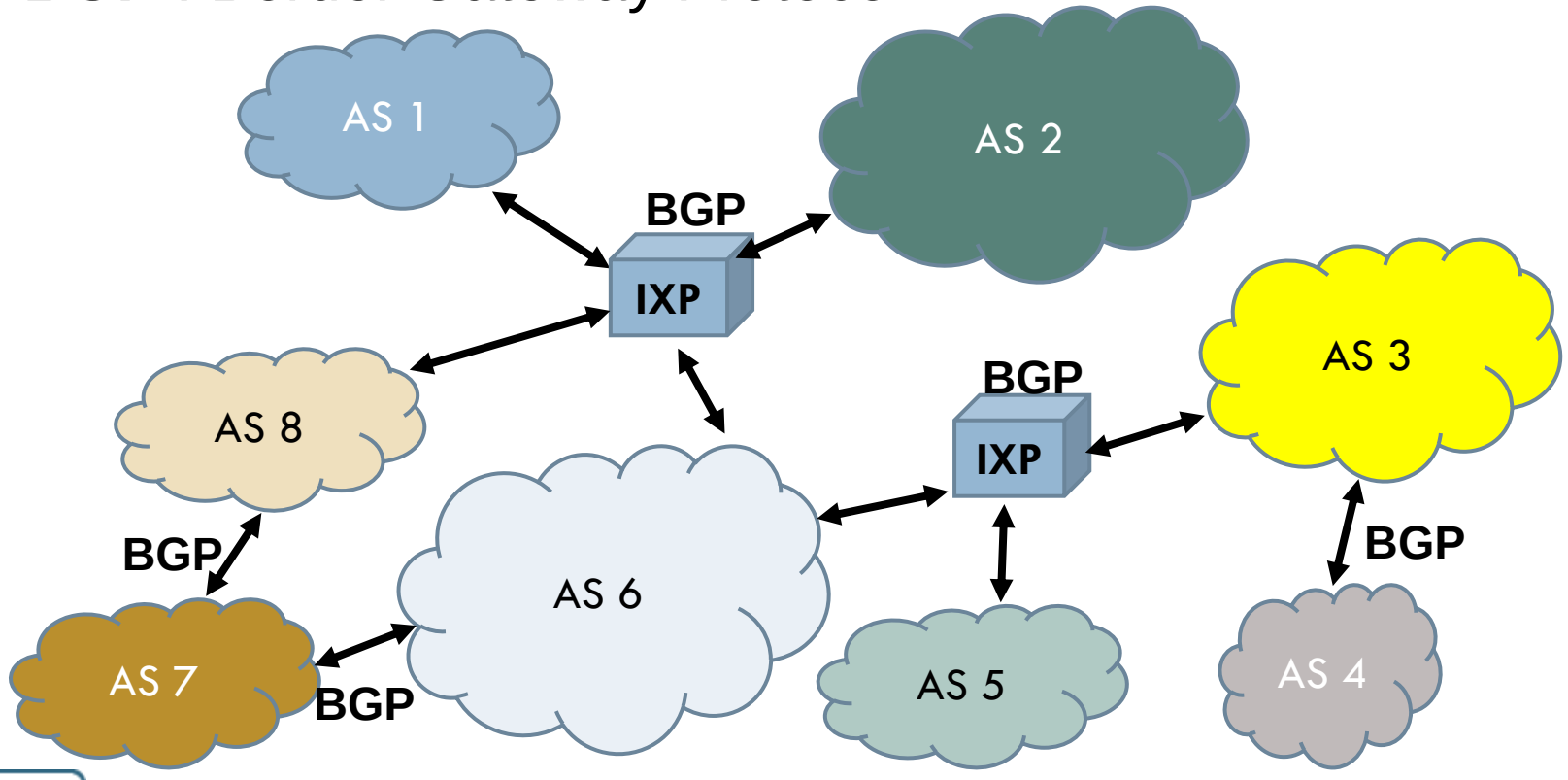




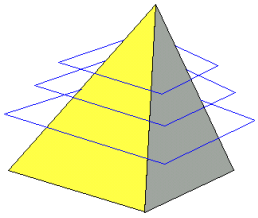
Organisation d'Internet 2/3



L'interconnexion entre **systèmes autonomes** est gérée via **BGP** : Border Gateway Protocol

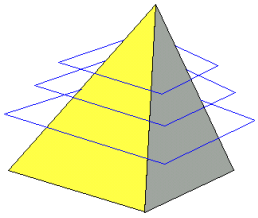


AS – Autonomous System



- Ensemble de routeurs administrés par la même entité (même politique d'administration)
  - Typiquement : un FAI (ISP)
  - Ou plus généralement : un opérateur
- Les numéros de AS : ASN
  - Sont distribués, à l'instar des adresses IP par l'IANA ou ses représentants locaux (en Europe : RIPE-NCC)
  - Sont définis par un nombre de 2 ou 4 octets (2007)
    - x sur deux octets (0 à 65525) ou x.y
  - La plage 64512 à 65535 est privée (voir IP privées)

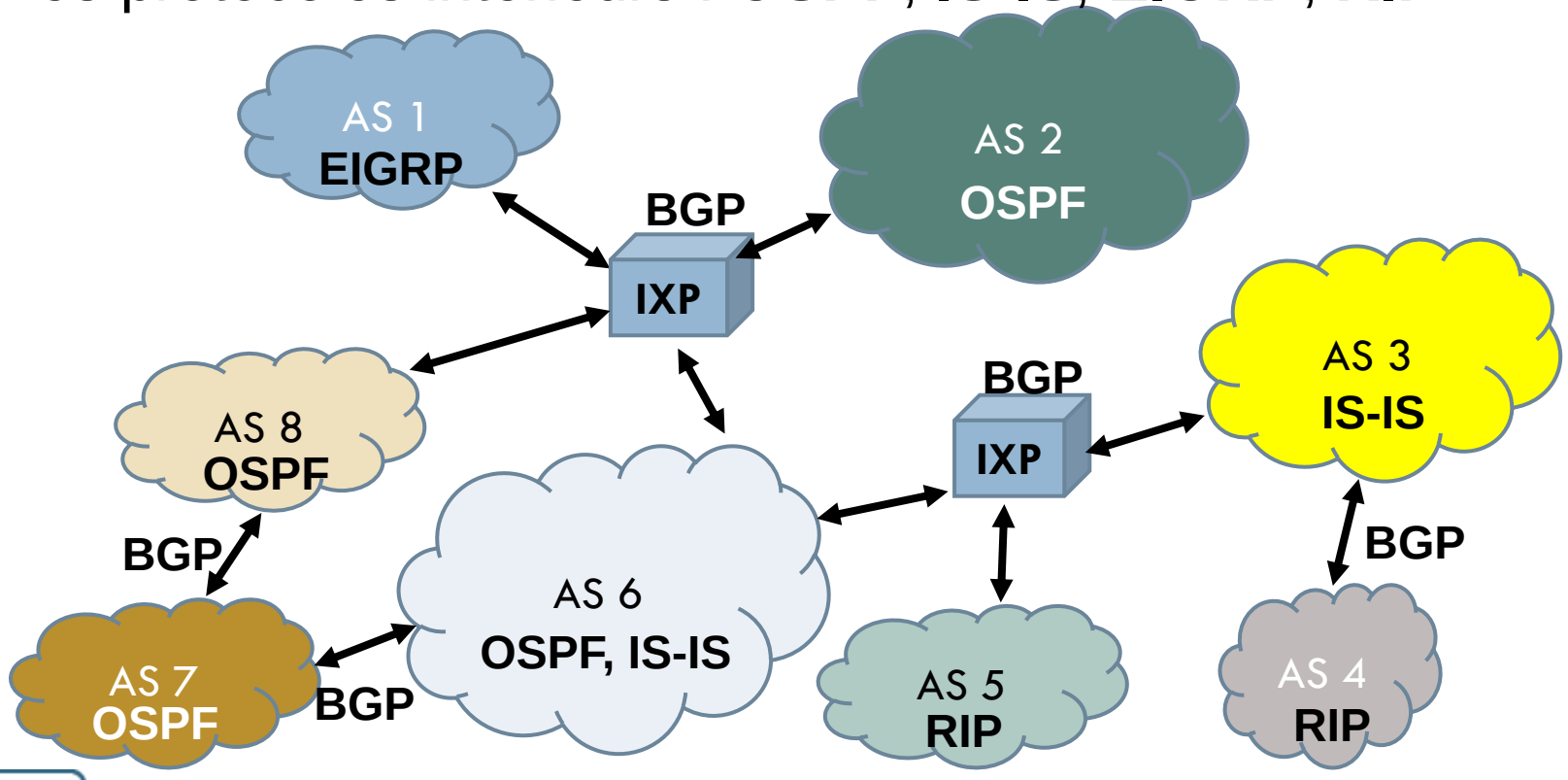
Border Gateway Protocol



- Echange de routes entre AS
  - Protocole de type : vecteur de chemin
  - Les informations sont échangées entre des routeurs de Bordure : ASBR (Autonomous System Border Routeurs)
  - Pas de métrique, mais des règles définies par les administrateurs des AS sur les ASBR
  - Deux cas : un paquet arrivant sur un ASBR est destiné
    - … à une route interne de l'AS : il est pris en charge par le routage intérieur de l'AS
    - … à une route externe à l'AS : dans ce cas l'AS est traversé par le paquet qui utilise ses ressources.
    - C'est pourquoi on parle de « règles » qui autorisent ou pas un paquet à traverser un AS.
- Protocole très complexe

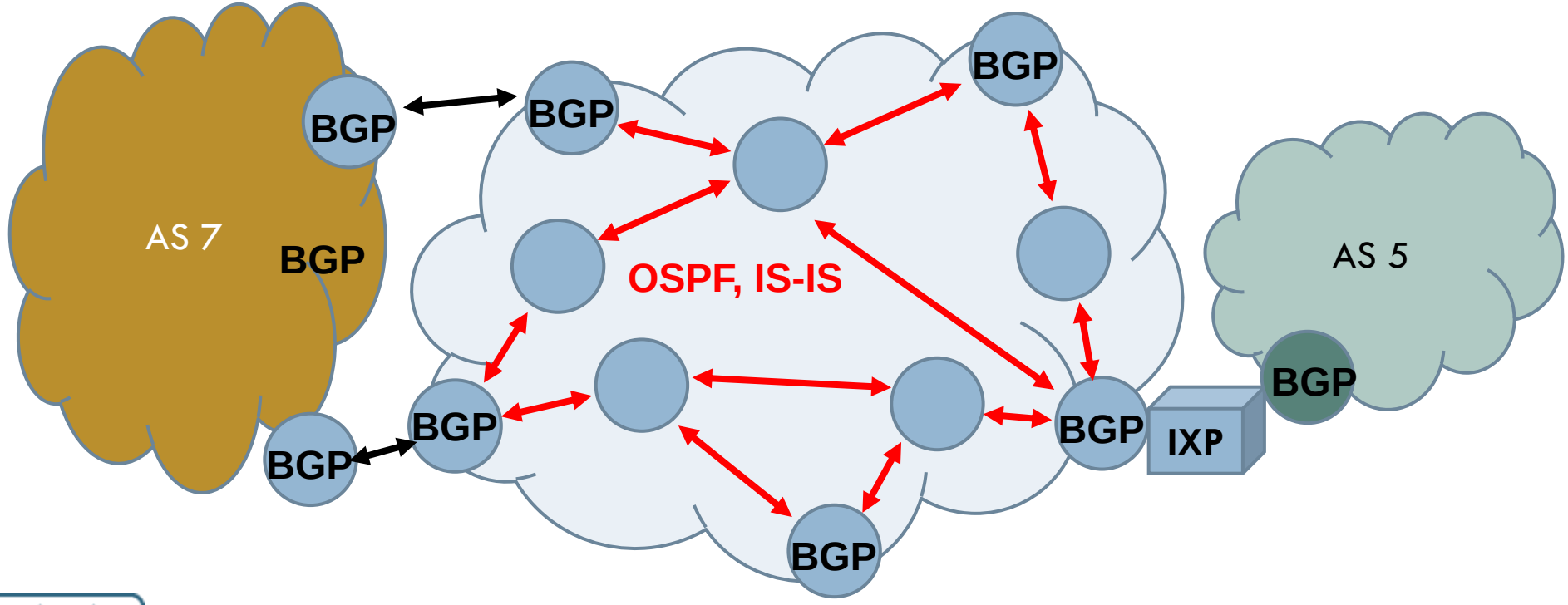
Organisation d'Internet 3/3

Le routage interne aux **systèmes autonomes** est gérée via les protocoles intérieurs : **OSPF**, **IS-IS**, **EIGRP**, **RIP**

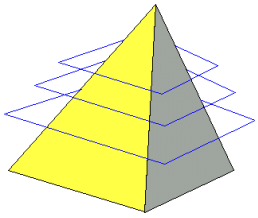


Organisation d'Internet 3/3

Routeurs internes : **OSPF, IS-IS, EIGRP, RIP**
Routeurs de Bordure : **routage interne**

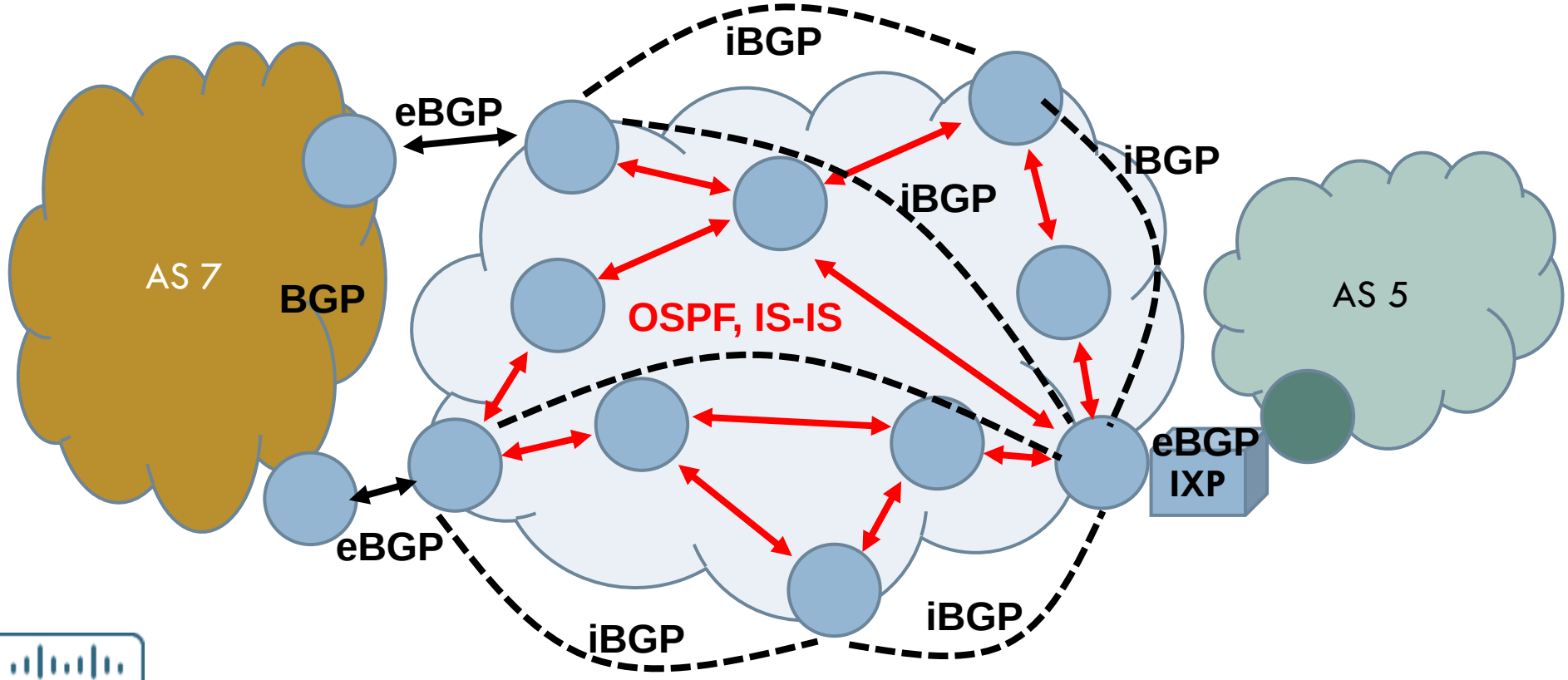


Organisation d'Internet 3/3

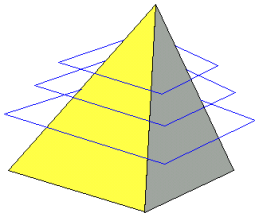


Routeurs internes : OSPF, IS-IS, EIGRP, RIP

Routeurs de Bordure : routage interne **+ eBGP + iBGP**

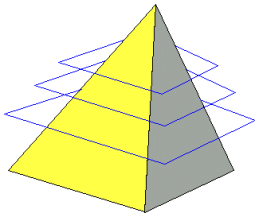


Border Gateway Protocol



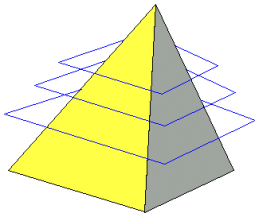
- eBGP : BGP extérieur
  - Routage entre AS
  - Cela revient à « dézoomer » pour ne voir l'ensemble des routeurs d'un opérateur que comme un nœud unique
  - Les connexions (en générale directes) entre AS s'établissent dans des sites d'interconnexion (IXP) entre opérateurs (ou FAI)
- iBGP : BGP intérieur
  - Permet de propager les routes BGP à l'intérieur d'un AS
  - Les connexions (en générales indirectes) s'établissent entre les ASBR de l'AS
- MP-BGP : BGP multi-protocoles
  - Prend en charge des protocoles non-IPv4, comme MPLS ou IPV6

Conclusion (provisoire) Couche Réseau



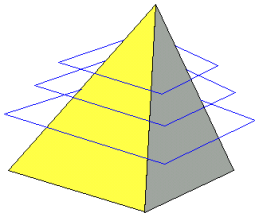
- Gérée par les routeurs
- Les routeurs sont configurés manuellement (routeurs d'extrémité) ou apprennent dynamiquement les chemins via les protocoles de routage
- Dans un AS la plupart des routeur possède une route par défaut qu'il utilise quand il ne connaît pas le chemin vers la destination
- Les routeurs de la **DFZ** (Default-free Zone) n'ont pas de routes par défaut. Ils forment une communauté BGP : dorsale de l'AS et gèrent jusqu'à **600 000 routes** !
- L'interconnexion mondiale est assurée par les IXP. Il n'y a plus de Backbone Internet.

Travaux Pratiques



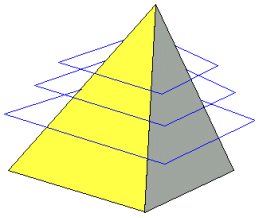
- **TP1 : introduction à Packet Tracer**
  - Adresses IP
  - Commutateurs
  - Protocole ICMP
  - Protocole ARP
  - Protocole DHCP
  - Routage entre deux réseaux d'un LAN
  - Connexion à distance sur un routeur via Telnet

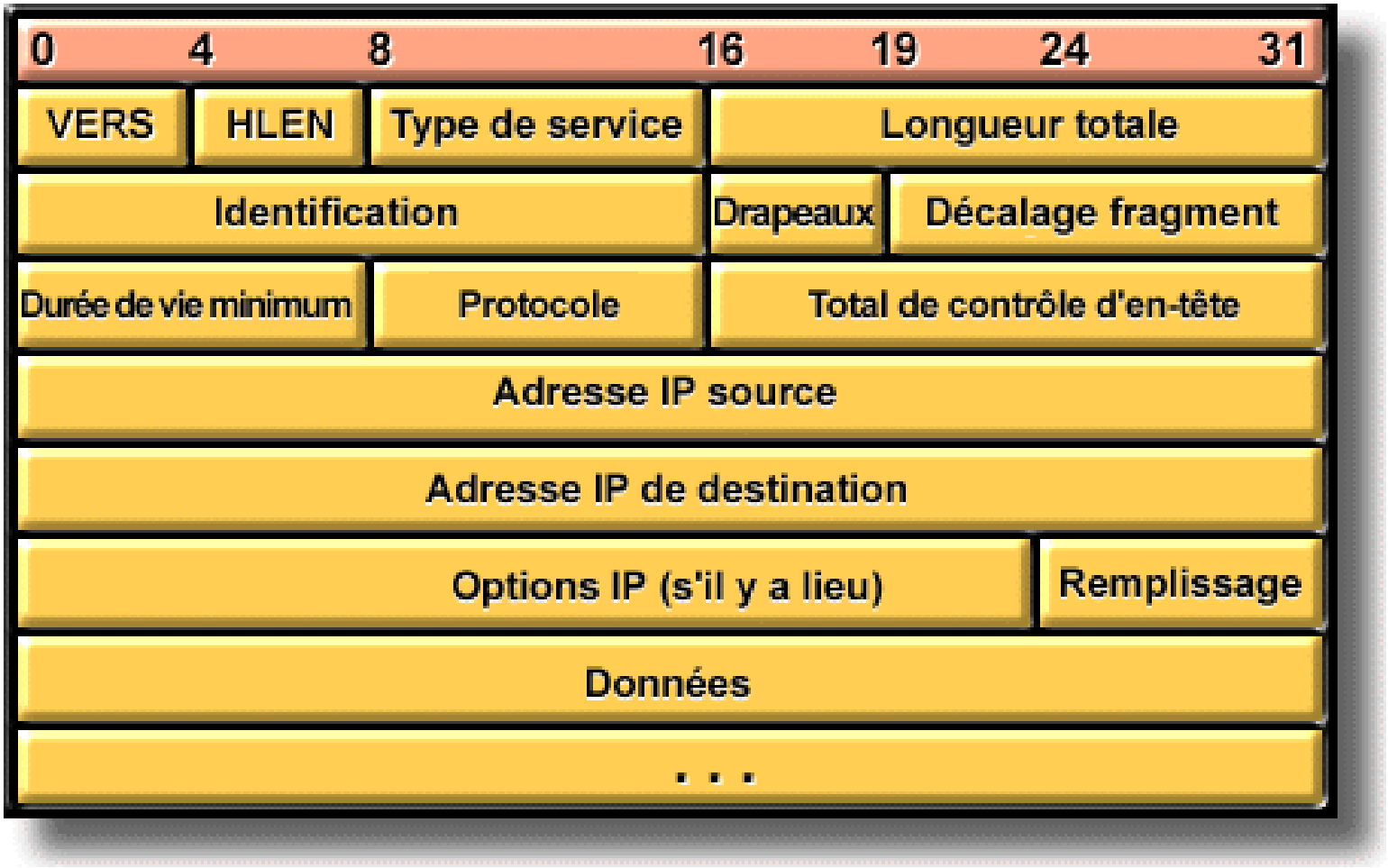
COUCHE 3 : Réseau



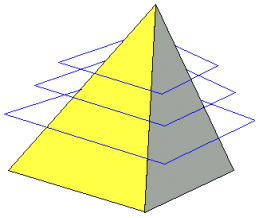
- Paquet
- Adresse de couche 3 : adresse IP
- Adresses publiques / adresses privées
- Réseaux et sous-réseaux

Paquet IP




0
4
8
16
19
24
31
VERS
HLEN
Type de service
Longueur totale
Identification
Drapeaux
Décalage fragment
Durée de vie minimum
Protocole
Total de contrôle d'en-tête
Adresse IP source
Adresse IP de destination
Options IP (s'il y a lieu)
Remplissage
Données
. . .

Adresse IP : <network,host>



- Une Adresse IP est composée de deux parties :
  - <network>, gérée par le service postal : 128 rue Pierre, 13012 Arles
  - <host>, gérée localement : Jean-Louis Azerty
- Le masque sert à distinguer ces deux parties
  - C'est une frontière : la partie network s'étend sur n bits
  - Puis, la partie host se prolonge sur h bits, jusqu'au dernier bit
  - n + h = 32 bits
- Le masque se note sur 4 octets comme l'adresse IP…
  - Les bits du masque sont à 1 sur la partie network
  - Puis, passent à 0 jusqu'au dernier bit
- … ou en format CIDR : /n (n bits d'adresse réseau)

Masque

- Le résultat d'un « et logique » entre une adresse IP et son masque est l'adresse du réseau correspondant
- Exemple : 174.18.14.139 / 16

Adresse IP en format binaire

1	0	1	0	1	1	1	0	.	0	0	0	1	0	0	1	0	.	0	0	0	0	1	1	1	0	.	1	0	0	0	1	0	1	1

Masque en format binaire

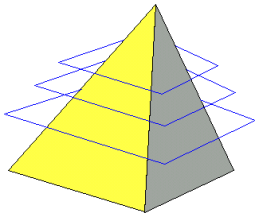
1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	0	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	0

ET logique =

1	0	1	0	1	1	1	0	.	0	0	0	1	0	0	1	0	.	0	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	0

Donc, l'adresse du réseau auquel appartient ce host est : 174.18.0.0

Digression : calcul binaire



- Valeur des bits dans un octet

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

- Conversion : binaire vers décimal

1	0	0	0	1	0	1	1

= 1x128 + 0x64 + 0x32 + 0x16 + 1x8 + 0x4+ 1x2 + 1x1
= 128 + 8 + 2 + 1 = 139

- Conversion : décimal vers binaire

67 = 0x128 + 1x64 + 0x32 + 0x16 + 0x8 + 0x4+ 1x2 + 1x1 =

0	1	0	0	0	0	1	1

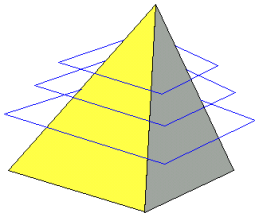
- Trucs & astuces
  - 127 c'est 128-1, donc :

0	1	1	1	1	1	1	1

  - 128 c'est :

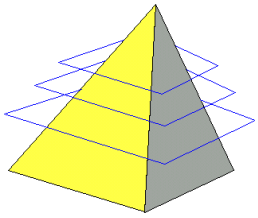
1	0	0	0	0	0	0	0

Classes d'adresses



- Taille des réseaux « en classe » (classful)
  - A : 0…127 – Masque : 8 bits – Host : 2^{24}-2 (16 777 214)
  - B : 128…191 – Masque : 16 bits – Host : 2^{16}-2 (65 534)
  - C : 192…223 – Masque : 24 bits – Host : 2^{8}-2 (254)

Adresses privées

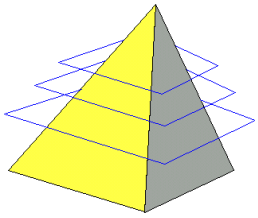


Adresses privées – RFC 1918

- Class A 10.0.0.0 … 10.255.255.255
- Class B 172.16.0.0 … 172.31.255.255
- Class C 192.168.0.0 … 192.168.255.255

- Adresses internes à un réseau qui peuvent etre gérées par un Network Address Translation

Classes d'adresses

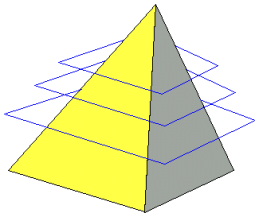


Adresse de broadcast ou adresse de diffusion

- L'adresse de broadcast d'un réseau permet de s'adresser à tous les hosts de ce réseau
- Elle est obtenue en donnant à tous les bits de la partie host de l'adresse IP du réseau la valeur 1
- Exemple :
  - Réseau : 141.12.0.0
  - Masque : 255.255.0.0
  - Broadcast : 141.12.255.255

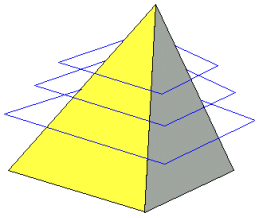
Ni l'adresse du réseau, ni l'adresse de diffusion ne doivent être attribuées à un host !

Classes d'adresses



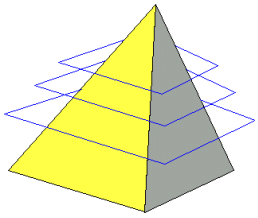
- Les sauts d'une classe à l'autre sont trop grands
  - Car le passage d'une classe à l'autre se fait aux frontières des octets
  - => Nécessité d'affiner le découpage en plaçant la frontière à l'intérieur des octets.

Sous réseaux - Subnets



- Créer un sous-réseau consiste à prolonger la partie réseau de l'adresse en « empruntant » des bits dans sa partie host
- L'idée sous-jacente est de prolonger la responsabilité du service postal « un cran plus loin », comme par exemple :
  - <network> : Société Corp, BP 1308, 128 rue Pierre, 13012 Arles
  - <host>, gérée localement : Directeur des Ressources Humaines
- <network> : le courrier n'est plus distribué globalement à l'adresse 128 rue Pierre, mais affiné entre les différentes entreprises présentes à cette adresse.
- <host> : le responsable courrier de la société Corp (la passerelle du LAN) émettra un broadcast ARP pour savoir qui est le DRH.

Subnets : découpage régulier

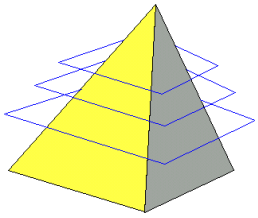


- Un découpage régulier consiste à créer des sous-réseaux en leur appliquant le même masque étendu
- A partir d'une adresse de réseau : <n><h>, j'emprunte « s » bits de la partie host pour étendre l'adresse de réseau en <n+s><h-s>, de façon à créer « S » sous-réseaux.
- Le nombre « s » de bits à emprunter est tel que : $2^s \geq S$
- Exemple : Créer 4 subnets à partir de l'adresse 174.18.14.0 / 24
  - Pour obtenir 4 subnets il faut emprunter deux bits ($2^2=4$)
  - Le masque devient / 26
  - Les bits empruntés sont les deux premiers bits du dernier octet
  - Les réseaux ainsi créés sont :

174.18.14.0 / 26, 174.18.14.64 / 26, 174.18.14.128 / 26, 174.18.14.192 / 26

  - Voir cela en détail dans la page suivante…

Subnets : découpage régulier



- Créer 4 subnets à partir de l'adresse 174.18.14.0 / 24
  - Deux bits empruntés (voir page précédente), qui vont donc pouvoir prendre les valeurs 0 ou 1, alors que ces bits étaient précédemment bloqués à 0 (partie host).
  - Nouveau masque : 255.255.255.192

1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	0	0	0	0	0	0

  - Adresse du premier réseau : 174.18.14.0 / 26

1	0	1	0	1	1	1	0	.	0	0	0	1	0	0	1	0	.	0	0	0	0	1	1	1	0	.	0	0	0	0	0	0	0	0

  - Adresse du deuxième réseau : 174.18.14.64 / 26

1	0	1	0	1	1	1	0	.	0	0	0	1	0	0	1	0	.	0	0	0	0	1	1	1	0	.	0	1	0	0	0	0	0	0

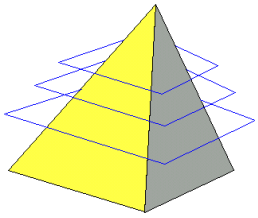
  - Adresse du troisième réseau : 174.18.14.128 / 26

1	0	1	0	1	1	1	0	.	0	0	0	1	0	0	1	0	.	0	0	0	0	1	1	1	0	.	1	0	0	0	0	0	0	0

  - Adresse du quatrième réseau : 174.18.14.192 / 26

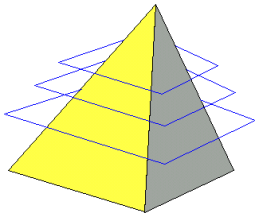
1	0	1	0	1	1	1	0	.	0	0	0	1	0	0	1	0	.	0	0	0	0	1	1	1	0	.	1	1	0	0	0	0	0	0

Subnets VLSM



- **Variable Length Subnet Masking** permet d'opérer un découpage en sous-réseaux dotés de masques de différentes longueurs
- Exemple
  - Découper 174.18.14.0 / 24 en :
    - Un subnet de 100 hosts,
    - Un subnet de 40 hosts
    - Deux subnets de 20 hosts

Subnets VLSM



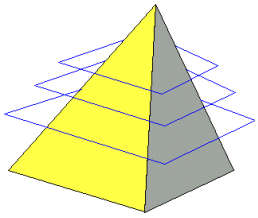
- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts,
  - Un subnet de 40 hosts
  - Deux subnets de 20 hosts

Première étape : définir les masques correspondants aux consignes

Le dernier bit du masque correspond au « pas », c'est-à-dire le nombre d'adresses pour passer au réseau suivant, donc le nombre d'adresses disponibles dans le réseau concerné (moins 2 !).

Masque,	Pas
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Subnets VLSM



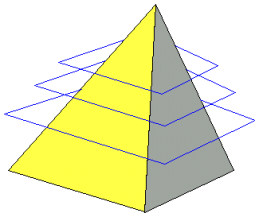
- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, **? 64 (/26), pas assez**
  - Un subnet de 40 hosts
  - Deux subnets de 20 hosts

Première étape : définir les masques correspondants aux consignes

Le dernier bit du masque correspond au « pas », c'est-à-dire le nombre d'adresses pour passer au réseau suivant, donc le nombre d'adresses disponibles dans le réseau concerné (moins 2 !).

Masque, Pas	
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Subnets VLSM



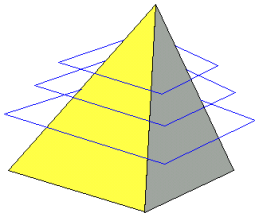
- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, **? 128 (/25), OK => / 25**
  - Un subnet de 40 hosts
  - Deux subnets de 20 hosts

Première étape : définir les masques correspondants aux consignes

Le dernier bit du masque correspond au « pas », c'est-à-dire le nombre d'adresses pour passer au réseau suivant, donc le nombre d'adresses disponibles dans le réseau concerné (moins 2 !).

Masque,	Pas
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Subnets VLSM



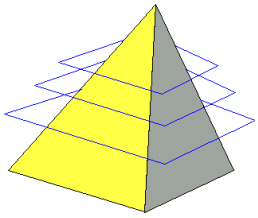
- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, / 25
  - Un subnet de 40 hosts, **? 32 (/27), pas assez**
  - Deux subnets de 20 hosts

Première étape : définir les masques correspondants aux consignes

Le dernier bit du masque correspond au « pas », c'est-à-dire le nombre d'adresses pour passer au réseau suivant, donc le nombre d'adresses disponibles dans le réseau concerné (moins 2 !).

Masque	Pas
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Subnets VLSM



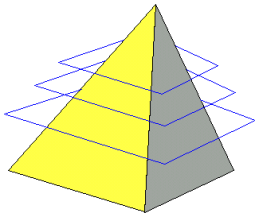
- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, / 25
  - Un subnet de 40 hosts, **? 64 (/26), OK => / 26**
  - Deux subnets de 20 hosts

Première étape : définir les masques correspondants aux consignes

Le dernier bit du masque correspond au « pas », c'est-à-dire le nombre d'adresses pour passer au réseau suivant, donc le nombre d'adresses disponibles dans le réseau concerné (moins 2 !).

Masque,	Pas
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Subnets VLSM



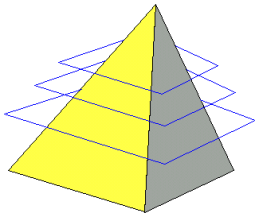
- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, / 25
  - Un subnet de 40 hosts, / 26
  - Deux subnets de 20 hosts, **? 16 (/28), pas assez**

Première étape : définir les masques correspondants aux consignes

Le dernier bit du masque correspond au « pas », c'est-à-dire le nombre d'adresses pour passer au réseau suivant, donc le nombre d'adresses disponibles dans le réseau concerné (moins 2 !).

Masque, Pas	
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Subnets VLSM



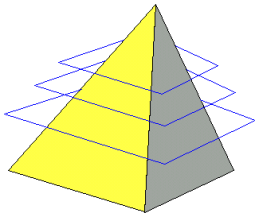
- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, / 25
  - Un subnet de 40 hosts, / 26
  - Deux subnets de 20 hosts, **? 32 (/27), OK => /27**

Première étape : définir les masques correspondants aux consignes

Le dernier bit du masque correspond au « pas », c'est-à-dire le nombre d'adresses pour passer au réseau suivant, donc le nombre d'adresses disponibles dans le réseau concerné (moins 2 !).

Masque,	Pas
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

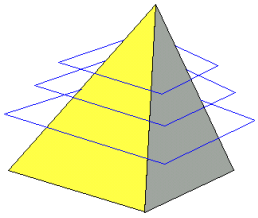
Subnets VLSM



- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, / 25
  - Un subnet de 40 hosts, / 26
  - Deux subnets de 20 hosts, / 27

Masque,	Pas
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

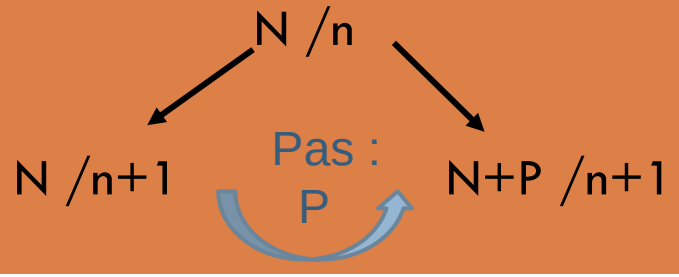
Subnets VLSM



- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, / 25
  - Un subnet de 40 hosts, / 26
  - Deux subnets de 20 hosts, / 27

Deuxième étape : construire l'arbre de découpage

Chaque bit emprunté découpe le réseau supérieur en 2. L'adresse de la branche de gauche est identique au réseau supérieur (le bit reste à 0). L'adresse de la branche de droite est égale à l'adresse du réseau supérieur, plus le « pas ».

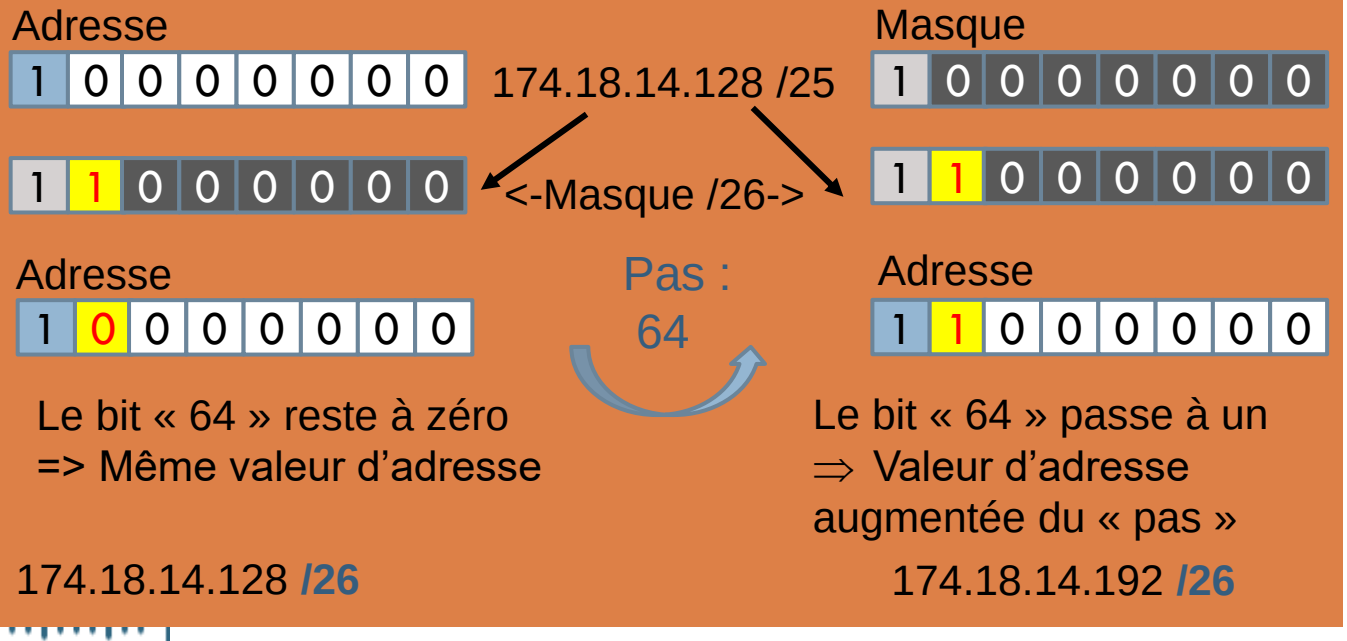


Masque, Pas	
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Arbre VLSM et valeur du pas

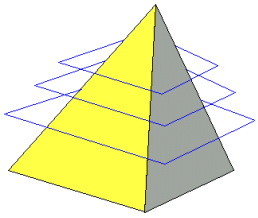
Deuxième étape : Exemple 174.18.14.128 / 25

Chaque bit emprunté découpe le réseau supérieur en 2. L'adresse de la branche de gauche est identique au réseau supérieur (le bit reste à 0). L'adresse de la branche de droite est égale à l'adresse du réseau supérieur, plus le « pas ».



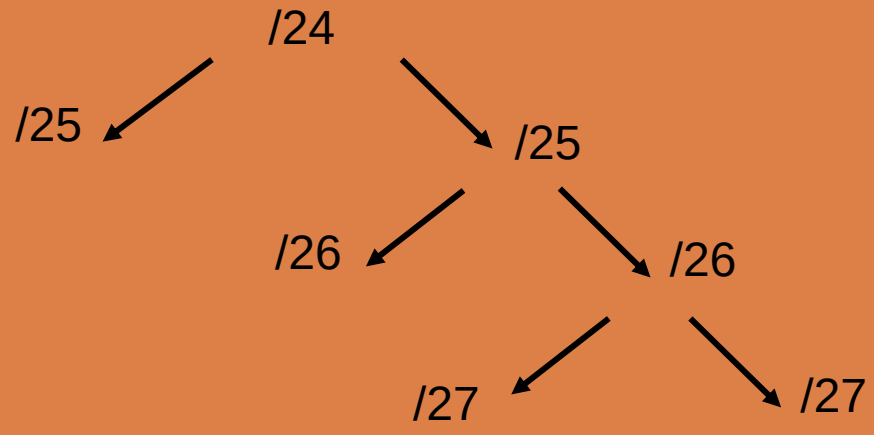
Masque, Pas	
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Subnets VLSM



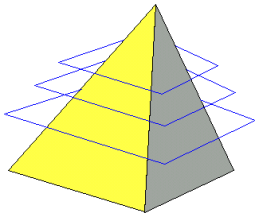
- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, / 25
  - Un subnet de 40 hosts, / 26
  - Deux subnets de 20 hosts, / 27

Deuxième étape : construire l'arbre de découpage



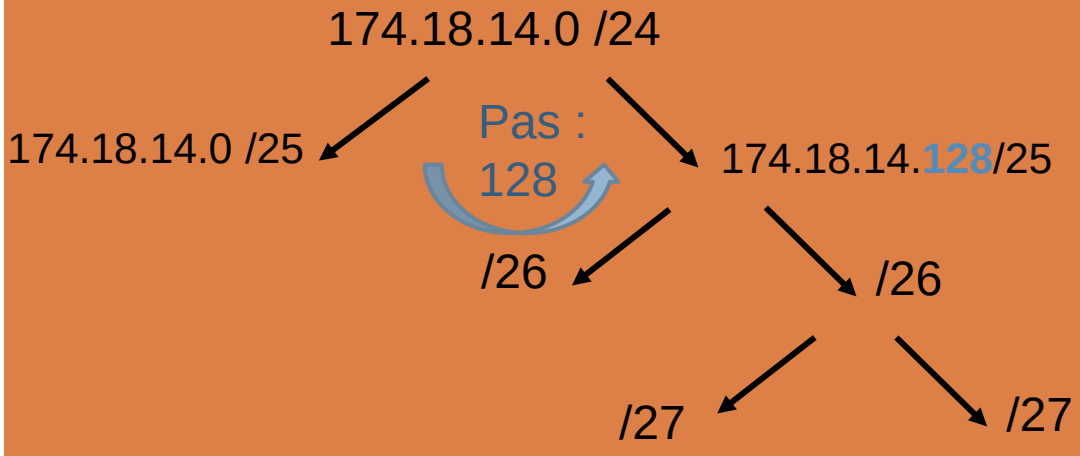
Masque, Pas	
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Subnets VLSM



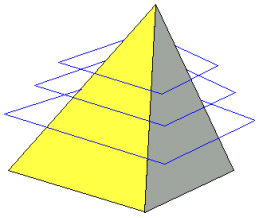
- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, / 25
  - Un subnet de 40 hosts, / 26
  - Deux subnets de 20 hosts, / 27

Troisième étape : calculer les adresses des réseaux



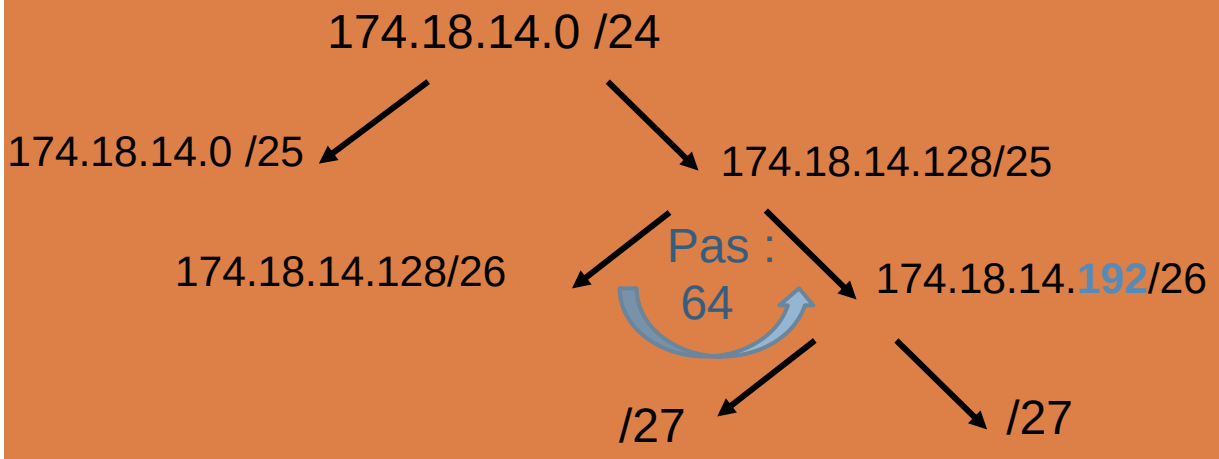
Masque,	Pas
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Subnets VLSM



- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, / 25
  - Un subnet de 40 hosts, / 26
  - Deux subnets de 20 hosts, / 27

Troisième étape : calculer les adresses des réseaux



Masque,	Pas
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

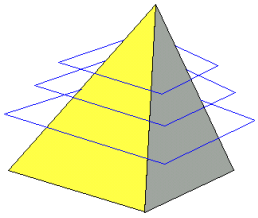
Subnets VLSM

- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts, / 25
  - Un subnet de 40 hosts, / 26
  - Deux subnets de 20 hosts, / 27

Troisième étape : calculer les adresses des réseaux

Masque,	Pas
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Subnets VLSM



- Découper 174.18.14.0 / 24 en :
  - Un subnet de 100 hosts : 174.18.14.0 / 25
  - Un subnet de 40 hosts : 174.18.14.128 / 26
  - Deux subnets de 20 hosts :
    - 174.18.14.192 / 27
    - 174.18.14.224 / 27

Masque, Pas	
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

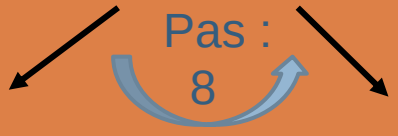
Subnets VLSM - 3°octet

- Utiliser la valeur des bits dans le 3°octet

Plus simple que d'ajouter 2048 à 0, tout en restant inférieur à 255 !

Pas dans le troisième octet

174.18.32.0 /20

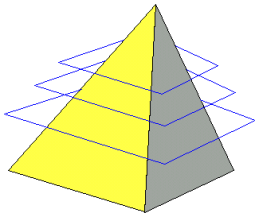


174.18 **32**.0 /21 174.18 **40**.0 /21

Masque	Pas
/17	128
/18	64
/19	32
/20	16
/21	8
/22	4
/23	2
/24	1

Masque	Pas	
/18	16384	3° octet
/19	8192	
/20	4096	
/21	2048	
/22	1024	
/23	512	
/24	256	
/25	128	4° octet
/26	64	
/27	32	
/28	16	
/29	8	
/30	4	
/31	2	
/32	1	

Subnets VLSM



- Découper (dans l'ordre) 174.18.64.0 / 21 en :
  - N1-200 hosts,
  - N2 -100 hosts,
  - N3 - 60 hosts,
  - N4 - 35 hosts,
  - N5 -260 hosts,
  - N6 -400 hosts,
  - N7 -110 hosts,
  - N8 - 30 hosts,
  - N9 – 40 hosts,
  - N10 -200 hosts.

Subnets VLSM

- Découper (dans l'ordre) 174.18.64.0 / 21 en :
  - N1-200 hosts,
  - N2 -100 hosts,
  - N3 - 60 hosts,
  - N4 - 35 hosts,
  - N5 -260 hosts,
  - N6 -400 hosts,
  - N7 -110 hosts,
  - N8 - 30 hosts,
  - N9 – 40 hosts,
  - N10 -200 hosts.

Première étape : définir les masques correspondants aux consignes.

Masque,	Pas
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

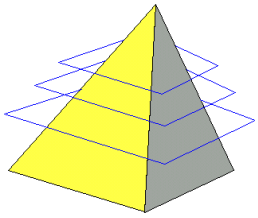
Subnets VLSM

- Découper (dans l'ordre) 174.18.64.0 / 21 en :
  - N1-200 hosts /24
  - N2 -100 hosts /25
  - N3 - 60 hosts /26
  - N4 - 35 hosts /26
  - N5 -260 hosts /23
  - N6 -400 hosts /23
  - N7 -110 hosts /25
  - N8 - 30 hosts /26
  - N9 – 40 hosts /26
  - N10 -200 hosts /24

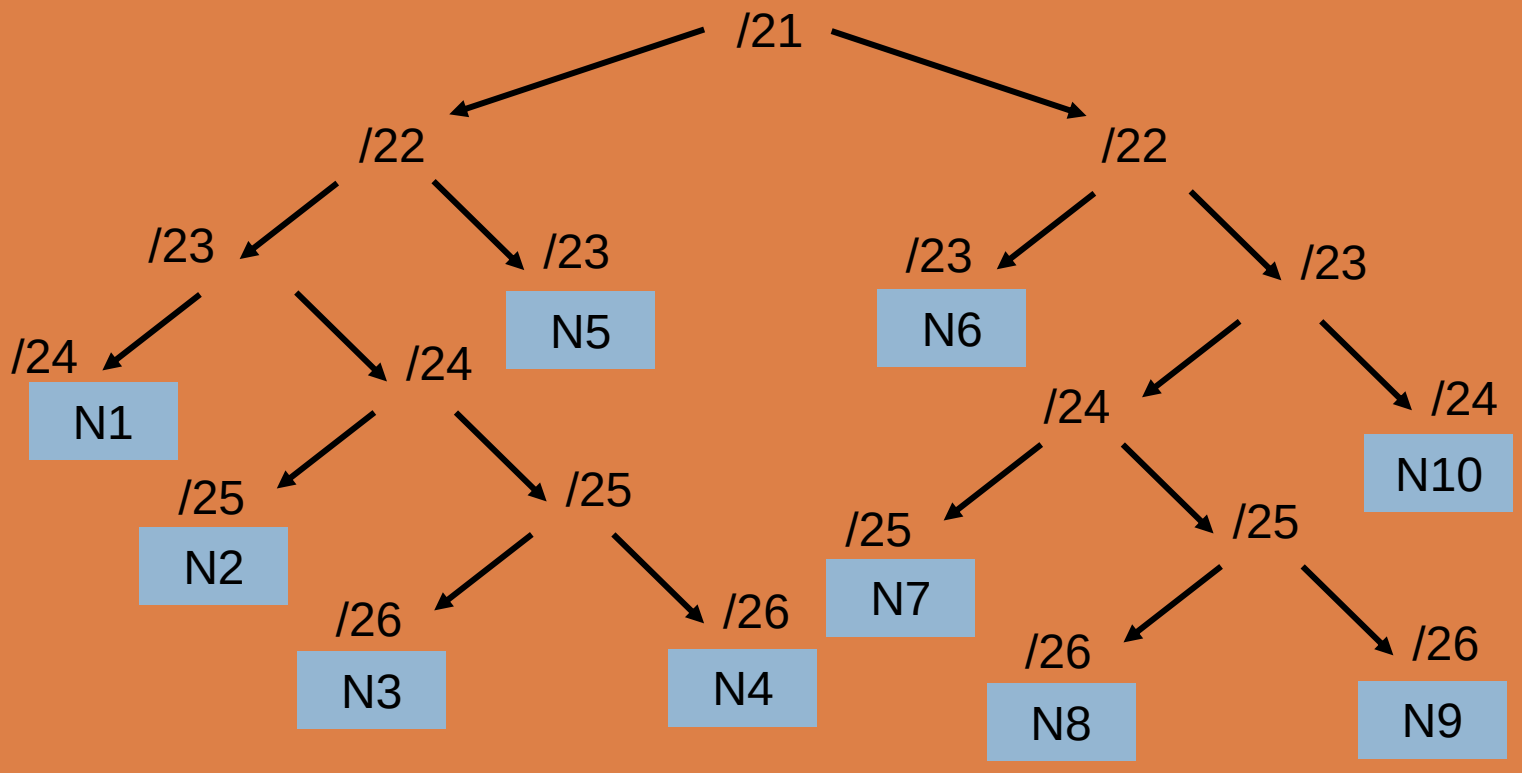
Première étape : définir les masques correspondants aux consignes.

Masque, Pas	
/18	16384
/19	8192
/20	4096
/21	2048
/22	1024
/23	512
/24	256
/25	128
/26	64
/27	32
/28	16
/29	8
/30	4

Subnets VLSM

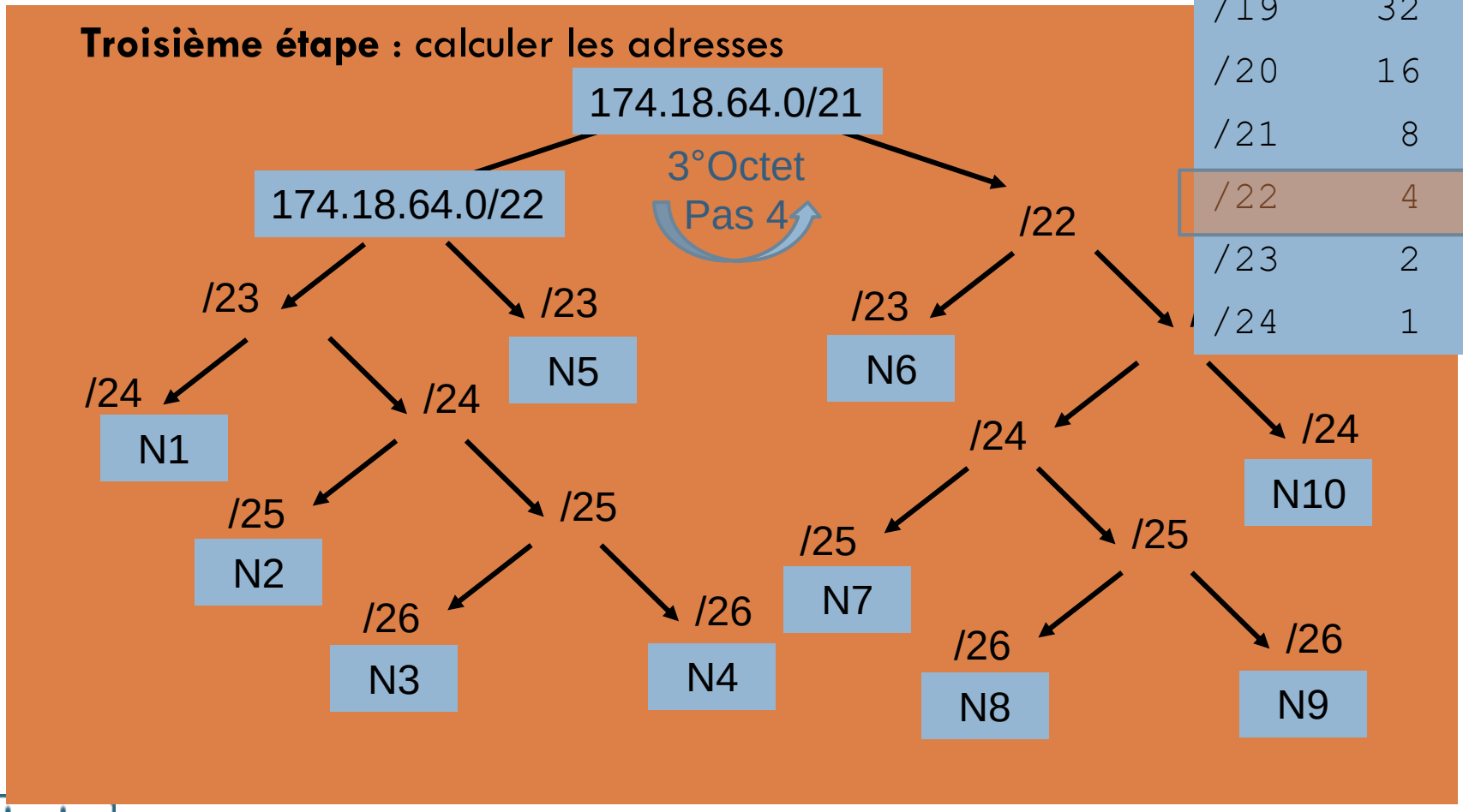


Deuxième étape : construire l'arbre de découpage



Subnets VLSM

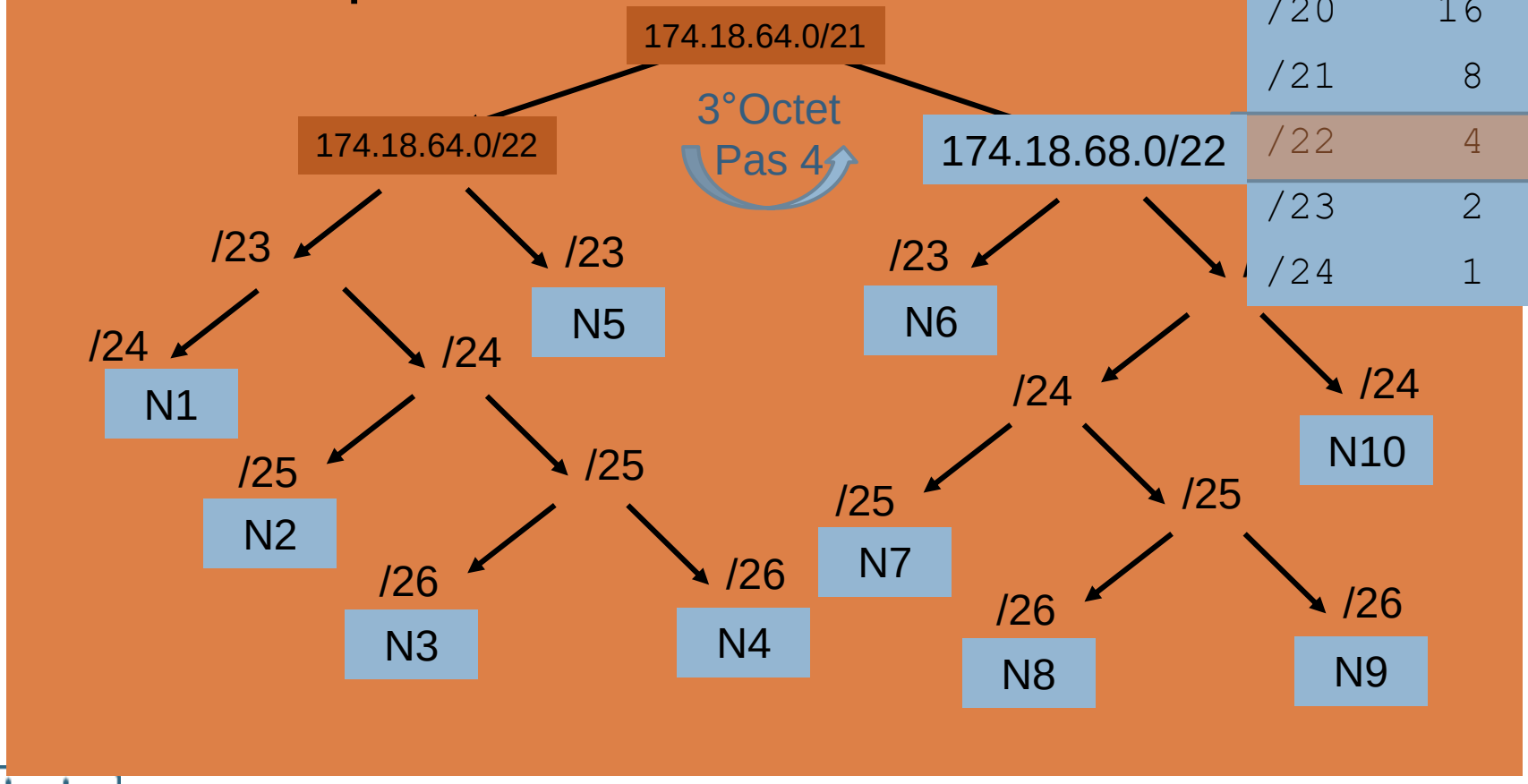
Troisième étape : calculer les adresses



3°Octet	
/17	128
/18	64
/19	32
/20	16
/21	8
/22	4
/23	2
/24	1

Subnets VLSM

Troisième étape : calculer les adresses

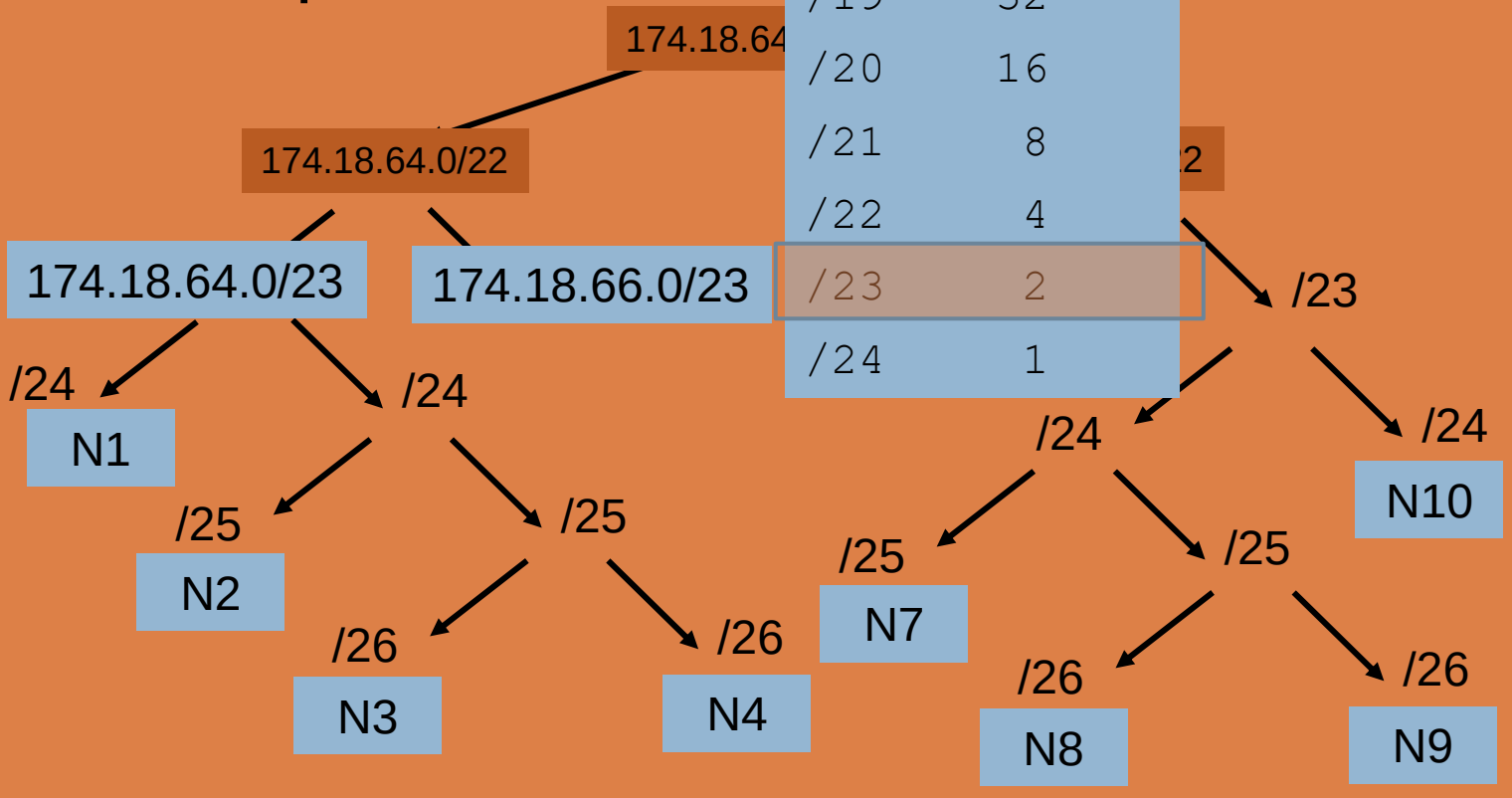


3°Octet	
/17	128
/18	64
/19	32
/20	16
/21	8
/22	4
/23	2
/24	1

Subnets VLSM

Troisième étape : calculer les adresse

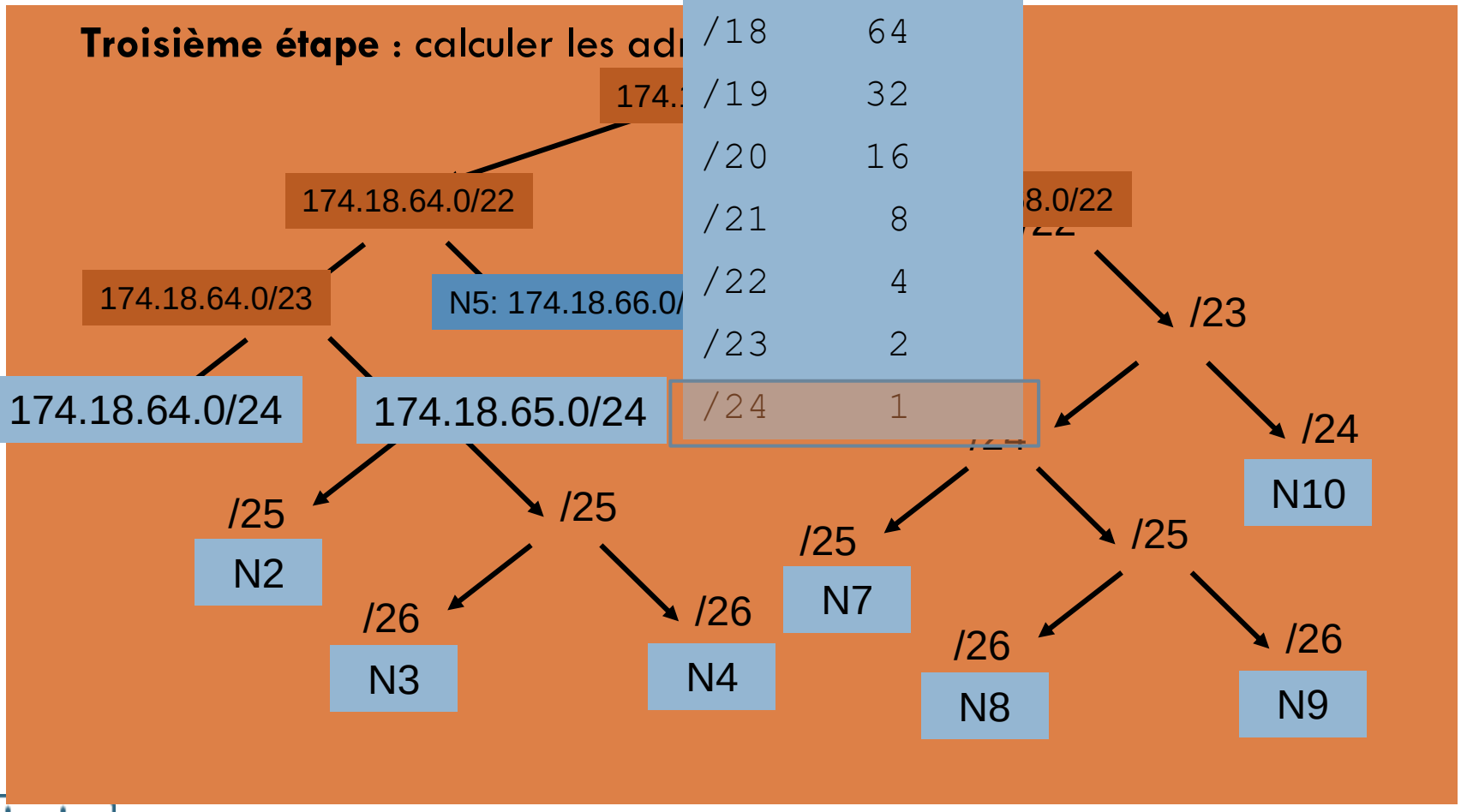
3°Octet	
/17	128
/18	64
/19	32
/20	16
/21	8
/22	4
/23	2
/24	1



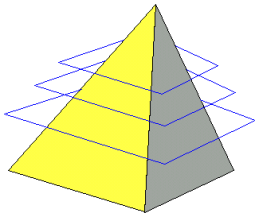
Subnets VLSM

Troisième étape : calculer les adr

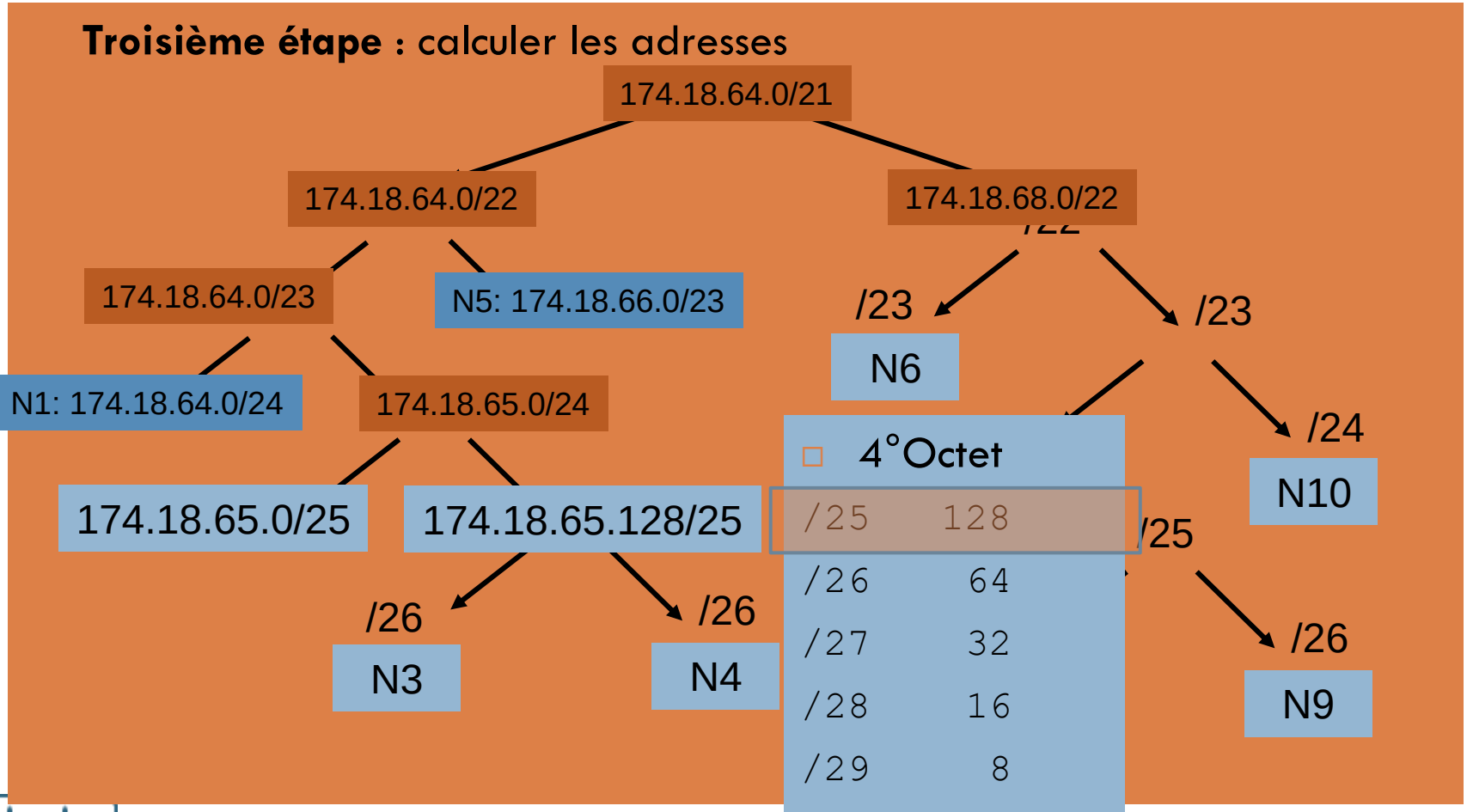
3°Octet	
/17	128
/18	64
/19	32
/20	16
/21	8
/22	4
/23	2
/24	1



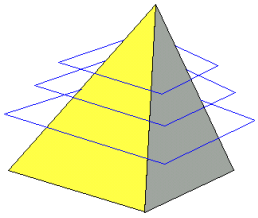
Subnets VLSM



Troisième étape : calculer les adresses

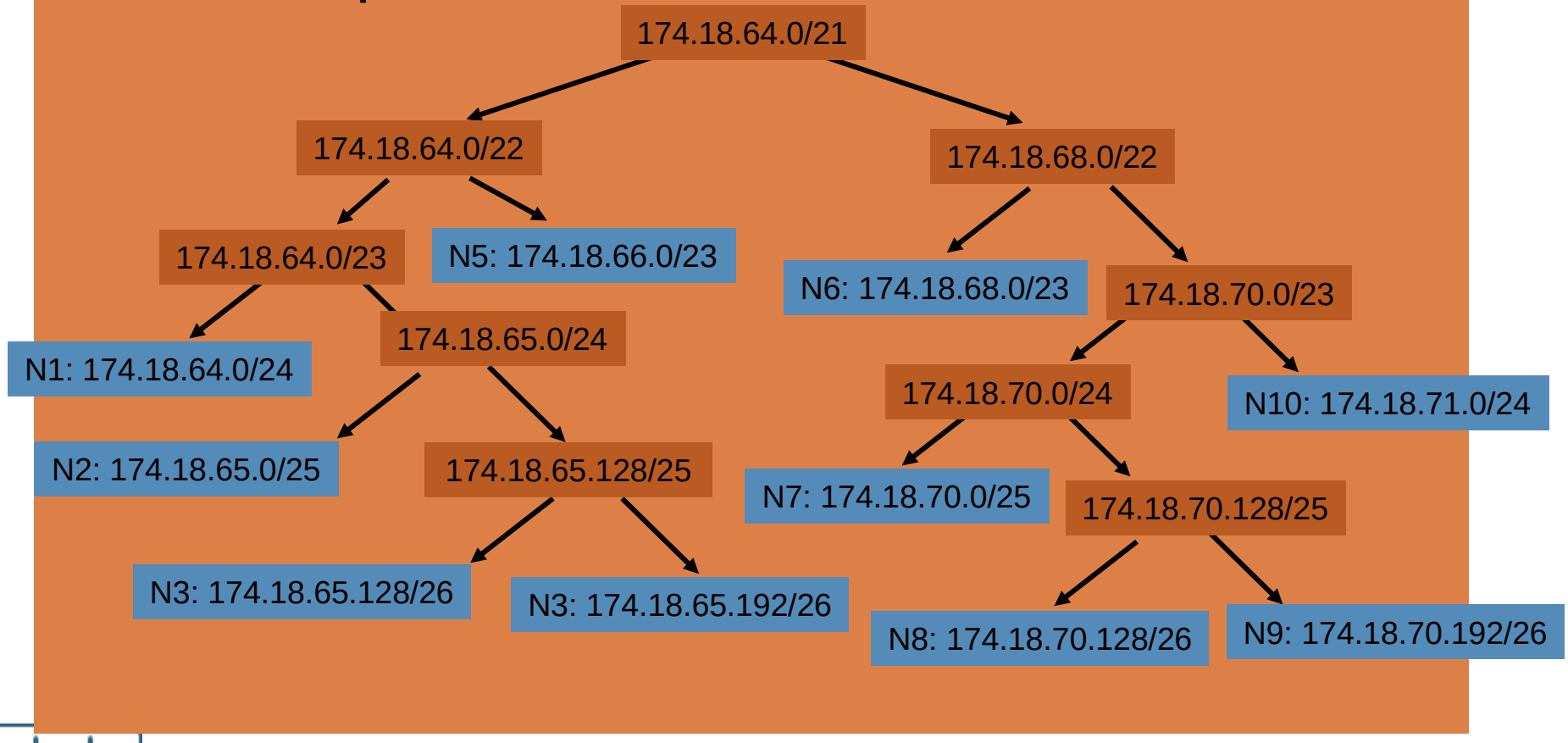


Subnets VLSM

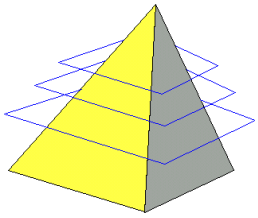


Approfondissement

Troisième étape : calculer les adresses



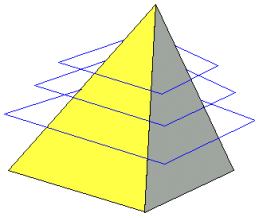
Subnets VLSM



- Découper (dans l'ordre) 174.18.64.0 / 21 en :
  - N1-200 hosts 174.18.64.0/24
  - N2 -100 hosts 174.18.65.0/25
  - N3 - 60 hosts 174.18.65.128/26
  - N4 - 35 hosts 174.18.65.192/26
  - N5 -260 hosts 174.18.66.0/23
  - N6 -400 hosts 174.18.68.0/23
  - N7 -110 hosts 174.18.70.0/25
  - N8 - 30 hosts 174.18.70.128/26
  - N9 – 40 hosts 174.18.70.192/26
  - N10 -200 hosts 174.18.71.0/24

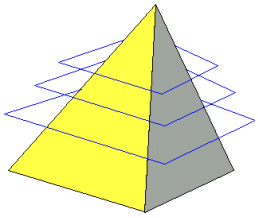
KALYST
INGENIERIE INFORMATIQUE

Subnets (autres exercices)



- Parmi les adresses suivantes, lesquelles sont valides :
  - 174.18.65.0/23
  - 23.81.260.4/28
  - 17.14.254.127/24
  - 17.14.254.127/25
  - 197.237.1.223/26
  - 197.237.1.223/27
  - 197.237.1.223/28
  - 197.237.1.223/25
  - 23.57.146.247.39/28
  - 23.57.146.247.39/29
  - 174.18.65.255/23
  - 174.18.64.255/23
  - 189.224.12.72/30
  - 189.224.12.72/29
  - 189.224.12.72/27
  - 45.45.45.45/7
  - 45.45.45.45/32
  - 45.45.45.45/31
  - 16.0.60.0/23
  - 16.0.60.0/22

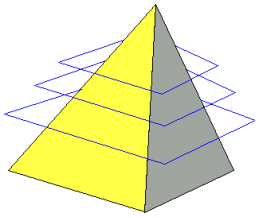
Subnets (autres exercices)



- Parmi les adresses suivantes, lesquelles sont valides :
  - **174.18.65.0/23**
  - **23.81.260.4/28**
  - **17.14.254.127/24**
  - 17.14.254.127/25
  - **197.237.1.223/26**
  - 197.237.1.223/27
  - 197.237.1.223/28
  - **197.237.1.223/25**
  - **23.57.146.247.39/28**
  - 23.57.146.247.39/29
  - 174.18.65.255/23
  - **174.18.64.255/23**
  - 189.224.12.72/30
  - 189.224.12.72/29
  - **189.224.12.72/28**
  - **45.45.45.45/7**
  - **45.45.45.45/32**
  - **45.45.45.45/31 – Si configuration ad-hoc**
  - 16.0.60.0/23
  - **16.0.60.0/22**

KALYST
INGENIERIE INFORMATIQUE

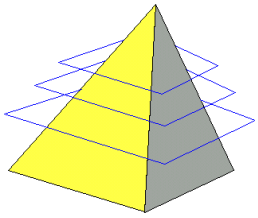
Routage intérieur



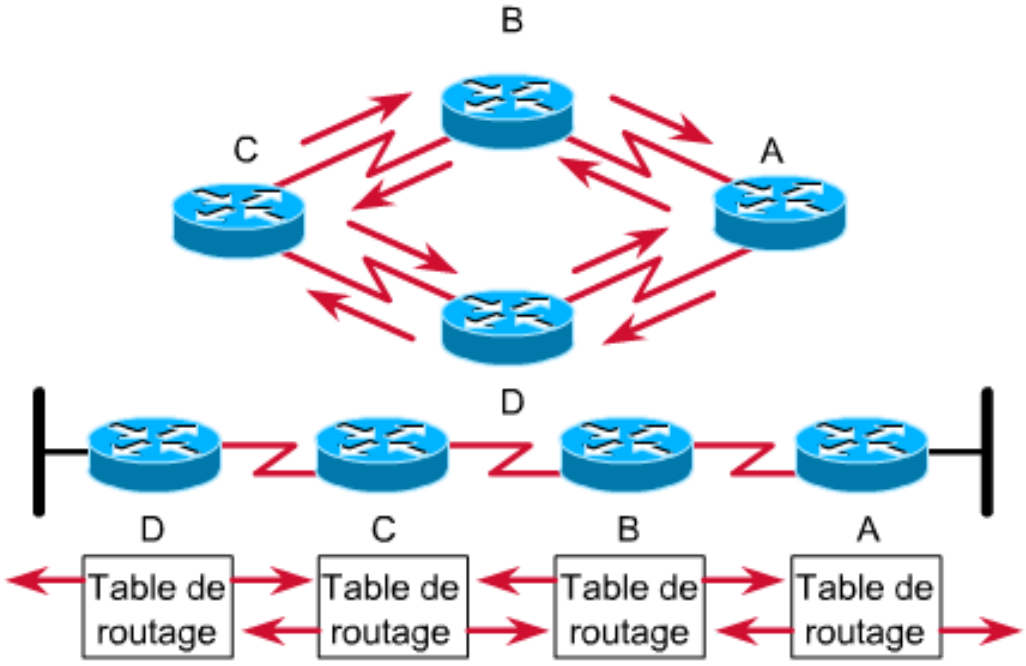
- RIP
- OSPF

CISCO
Networking Academy

RIP (Routing Interior Protocol)

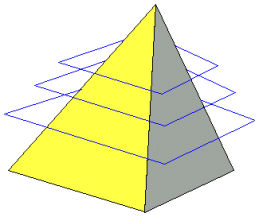


Routage à vecteur de distance



- Envoi périodique de copies de la table de routage aux routeurs voisins et addition des vecteurs de distance.

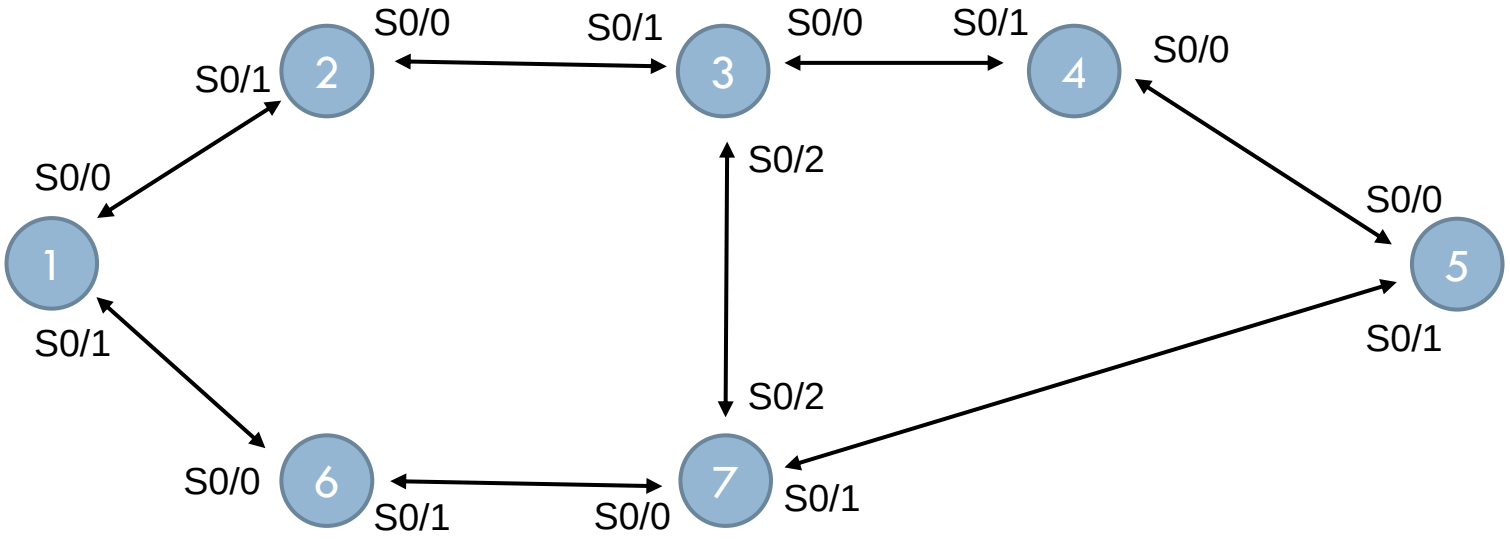
RIP – Fiche technique



- Métrique : nombre de sauts
- Mise à jour : périodique (30 secondes)
- Vision : limitée aux « voisins »
- Taille : limitée à 15 sauts (16 hops = inaccessible)
- Historique : classful (version 1), puis classless (v 2)
- Configuration : influencée (y compris en version 2) par son origine
- Convergence : lente

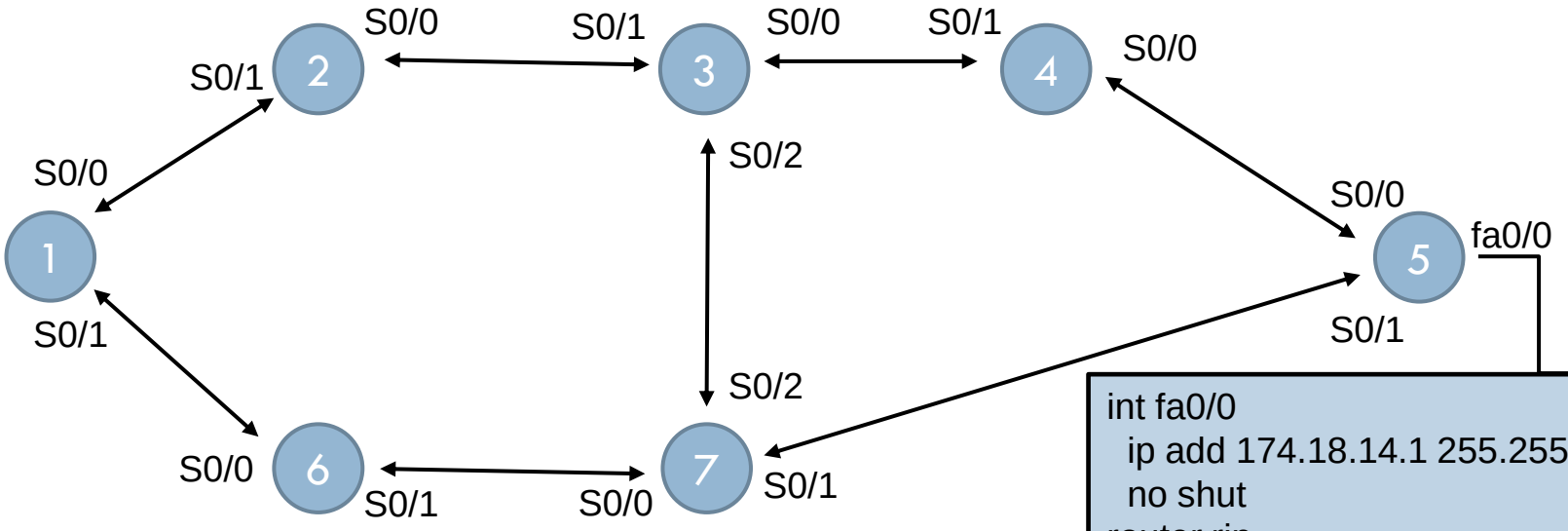
RIP - Convergence

Soit le réseau suivant dans lequel tous les routeurs opèrent RIP sur toutes leurs interfaces.



RIP - Convergence

Un administrateur réseau entre un nouveau réseau sur le routeur 5 et l'intègre dans RIP. Le réseau est marqué « RIP » et entre dans la table de routage du routeur 5. Il va donc être « annoncer » via RIP aux autres routeurs.

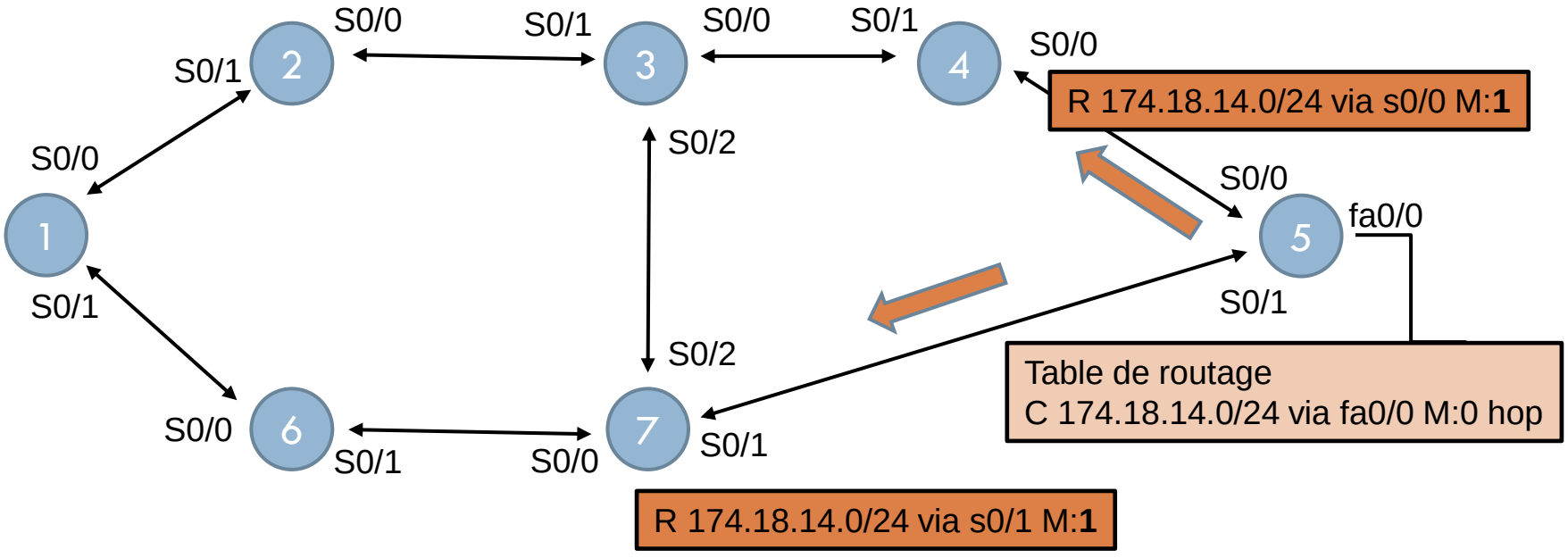



```
int fa0/0
  ip add 174.18.14.1 255.255.255.0
  no shut
router rip
  network 174.18.0.0
```

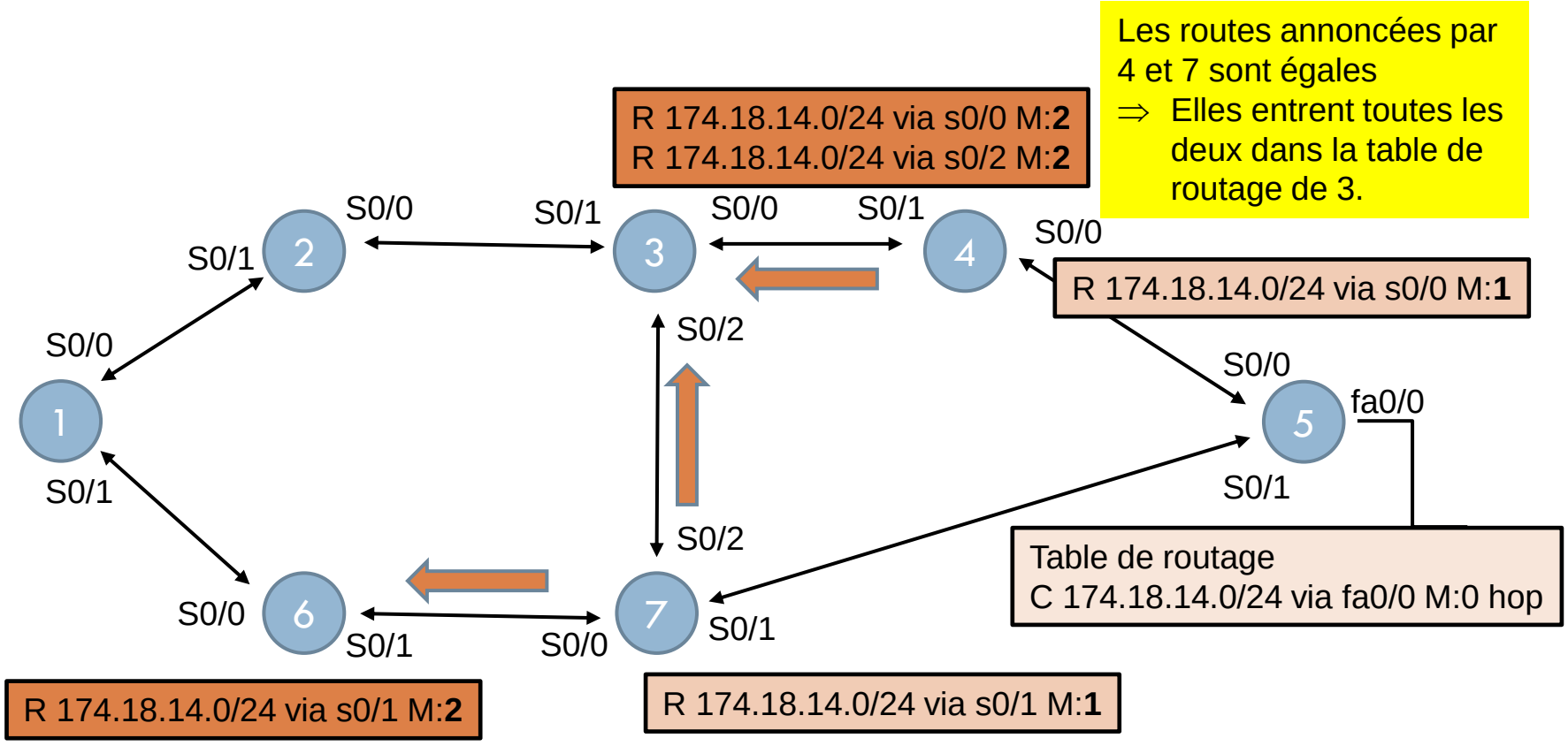
```
Table de routage
  C 174.18.14.0/24 via fa0/0
```

RIP - Convergence

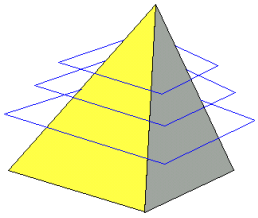
Un administrateur réseau entre un nouveau réseau sur le routeur 5 et l'intègre dans RIP. Le réseau est marqué « RIP » et entre dans la table de routage du routeur 5. Il va donc être « annoncer » via RIP aux autres routeurs.

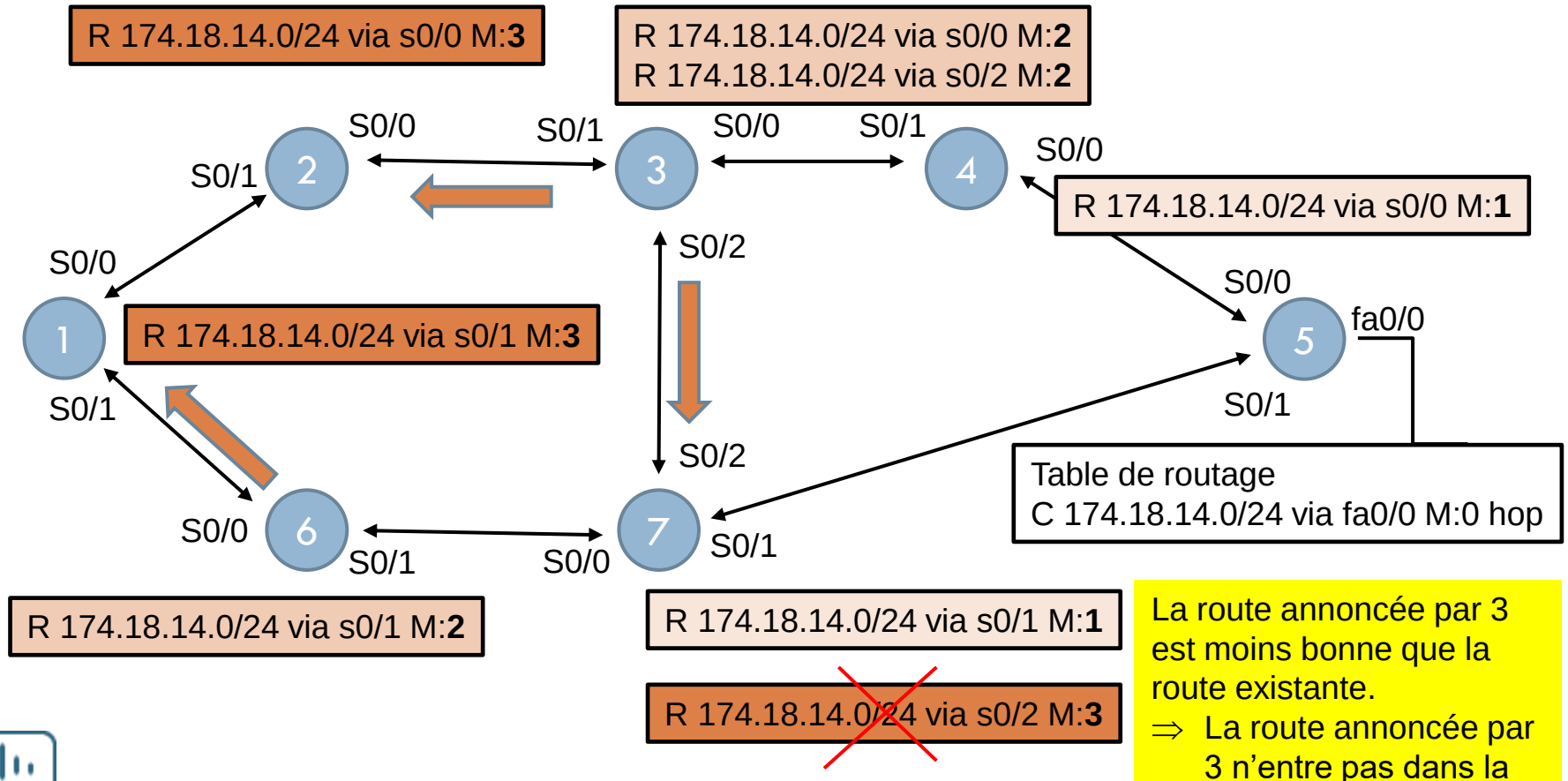


RIP - Convergence



RIP - Convergence

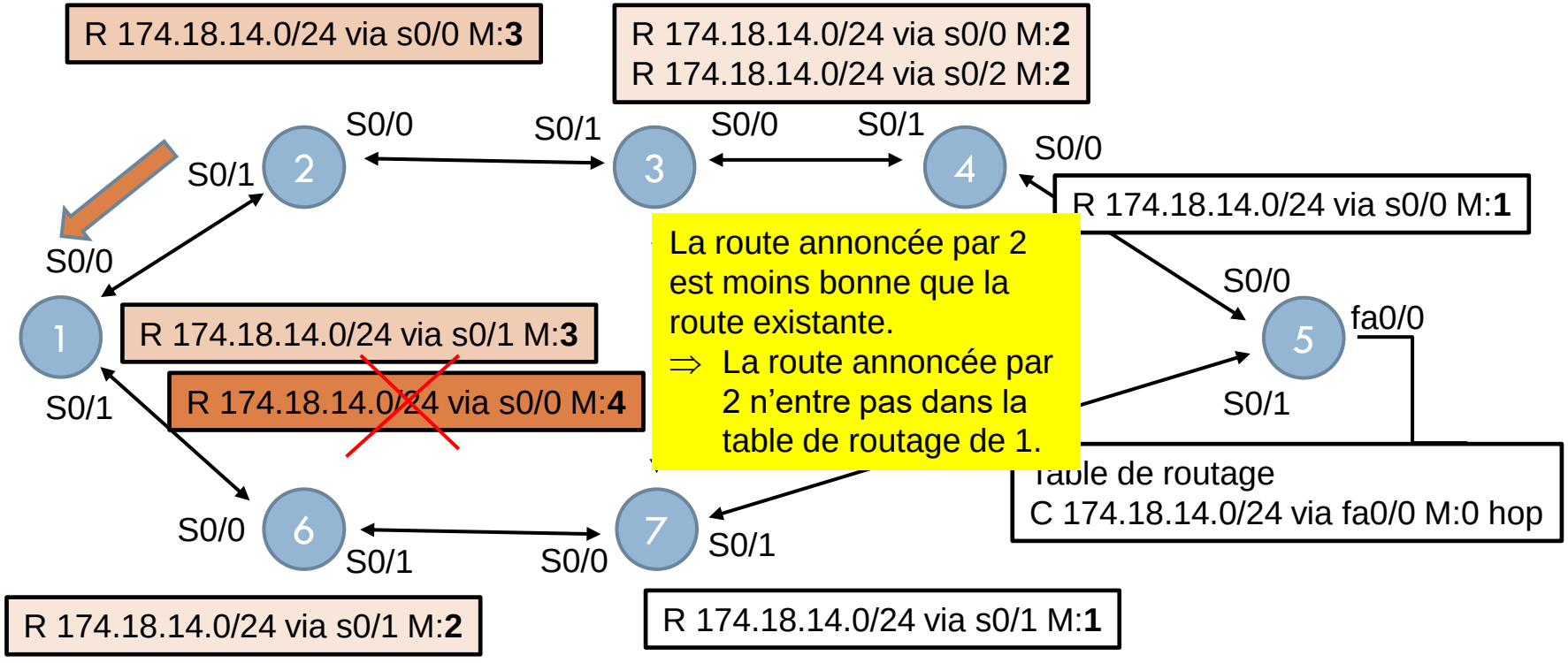




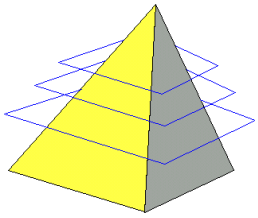
La route annoncée par 3 est moins bonne que la route existante.

⇒ La route annoncée par 3 n'entre pas dans la table de routage de 7.

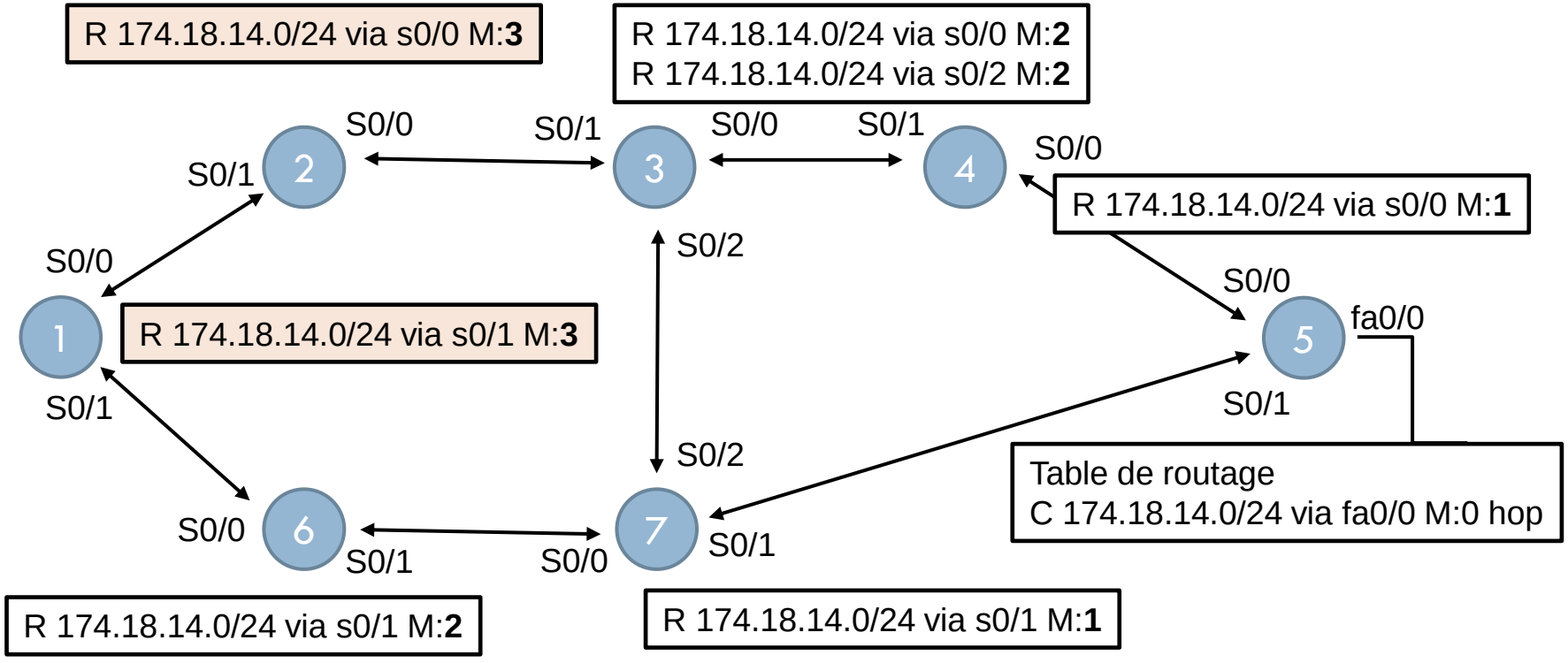
RIP - Convergence



RIP - Fonctionnement

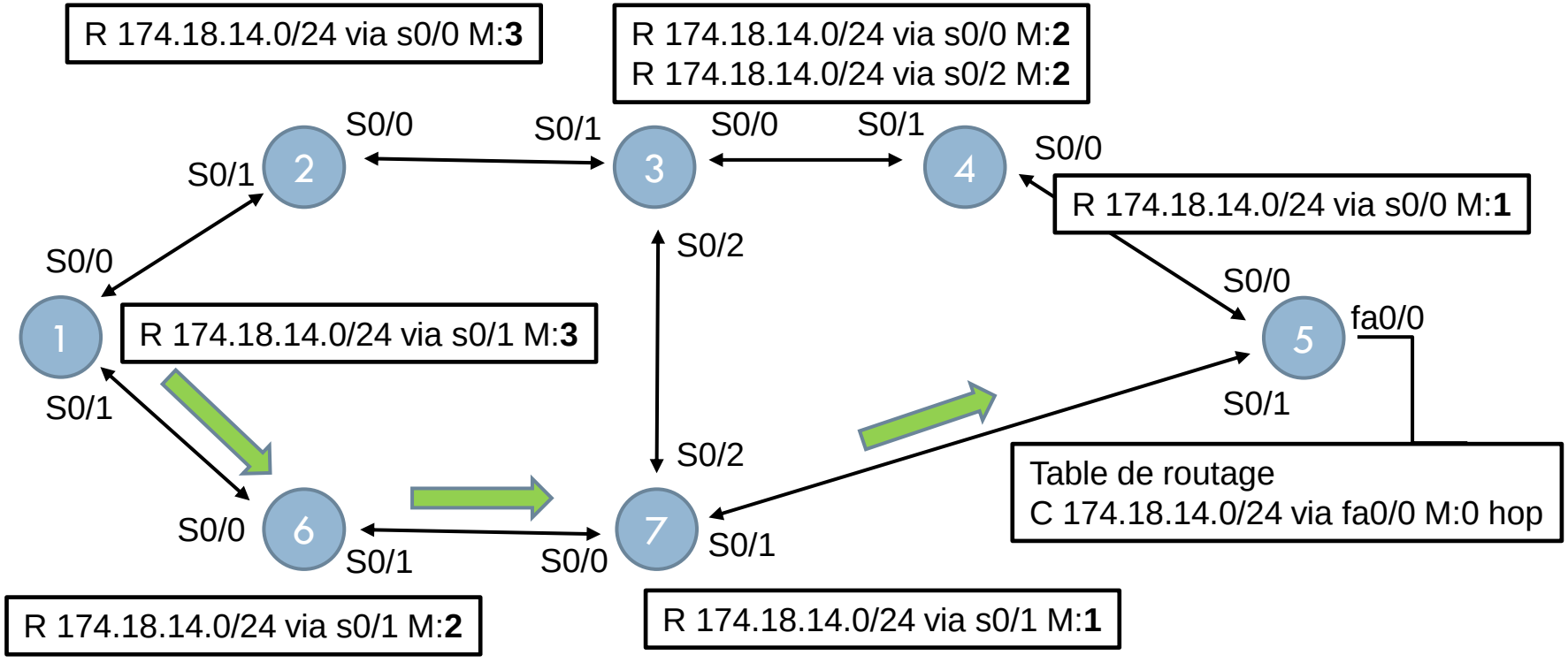


La nouvelle route a été diffusée dans tout le réseau RIP : le réseau a convergé !



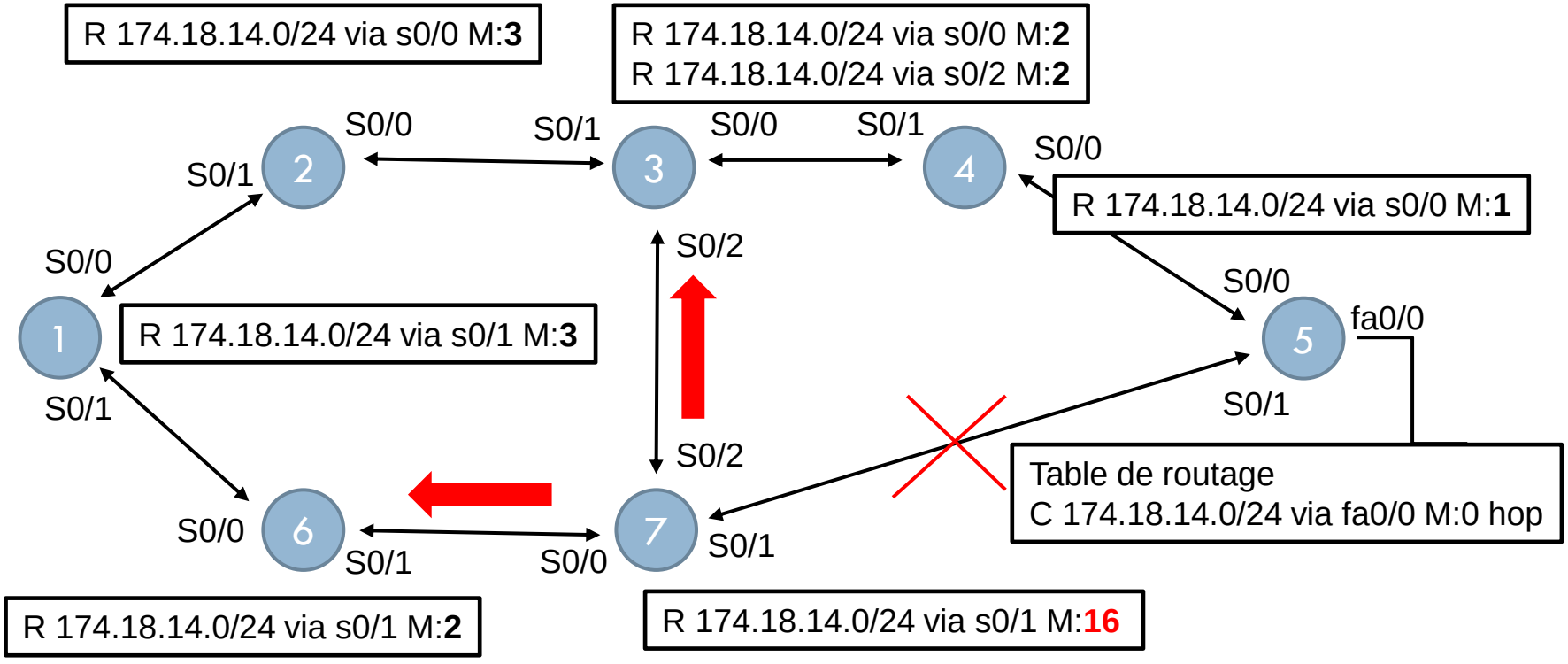
RIP - Fonctionnement

Un paquet arrivant sur le routeur 1 à destination du réseau 174.18.14.0 sera commuté sur s0/1



RIP – Fonctionnement

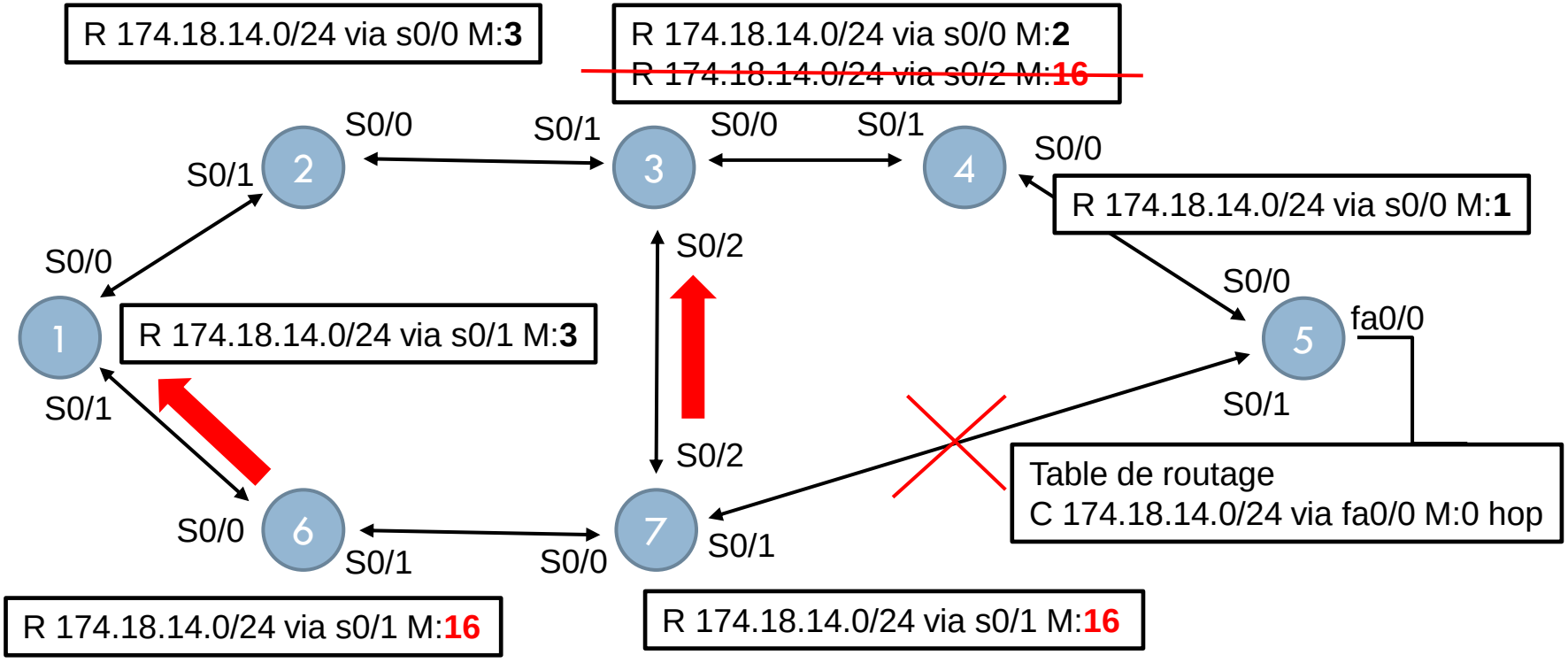
Le réseau 174.18.14.0 devient inaccessible via s0/1 sur le routeur 7



Le routeur 7 émet des mises à jour déclenchées vers ses voisins

RIP - Fonctionnement

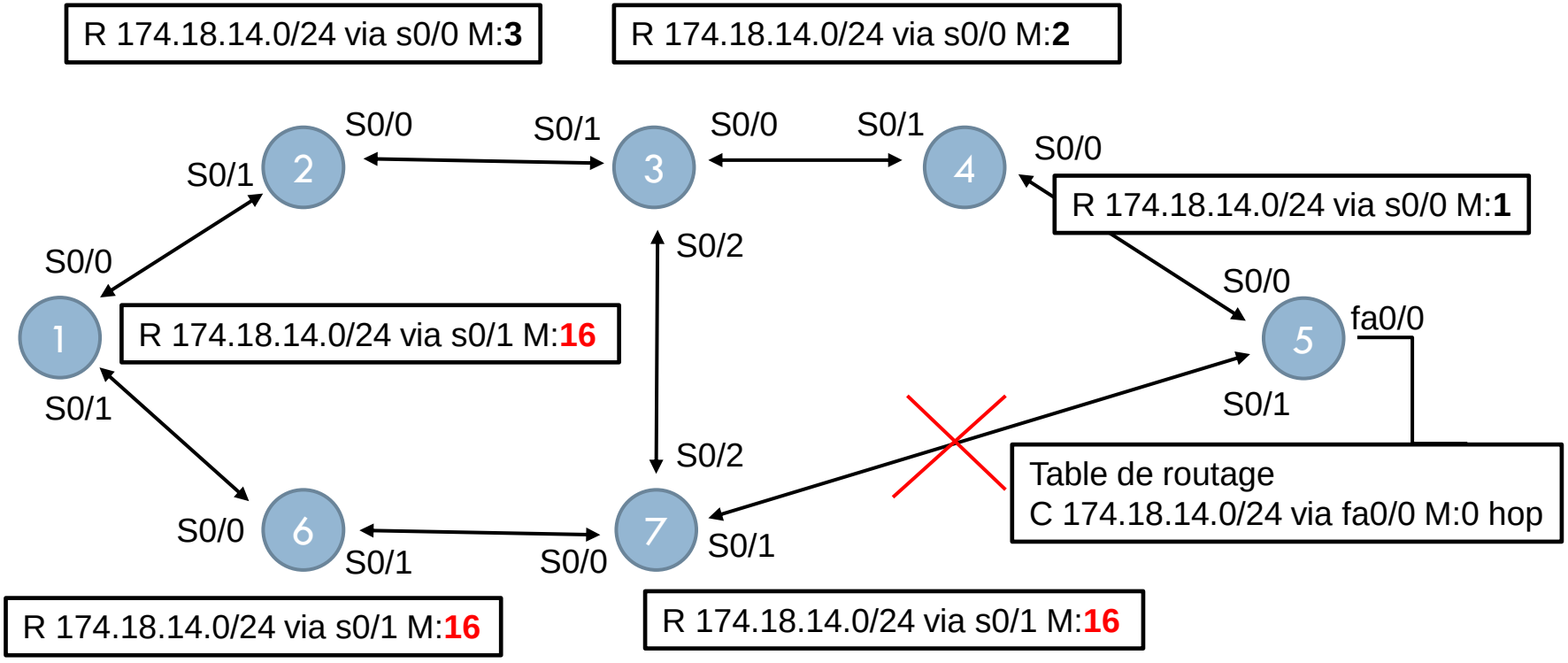
Le routeur 3 possède une route alternative : il supprime la route via s0/2 de sa table de routage



Le routeur 6 émet une mise à jour déclenchée vers le routeur 1

RIP - Fonctionnement

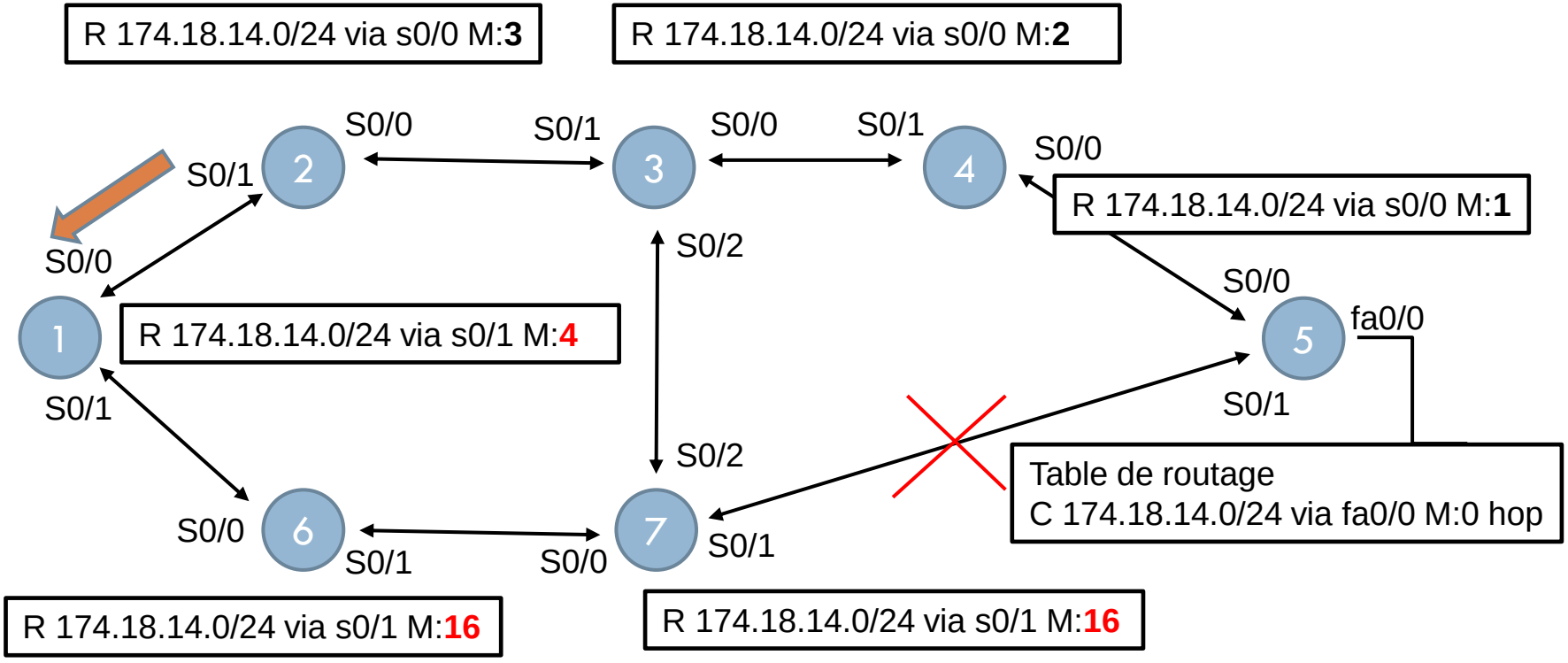
Le routeur 2 ne reçoit aucune mise à jour déclenchée (pour lui, rien de changé)



Le routeur 1 prend en compte la route devenue inaccessible

RIP - Fonctionnement

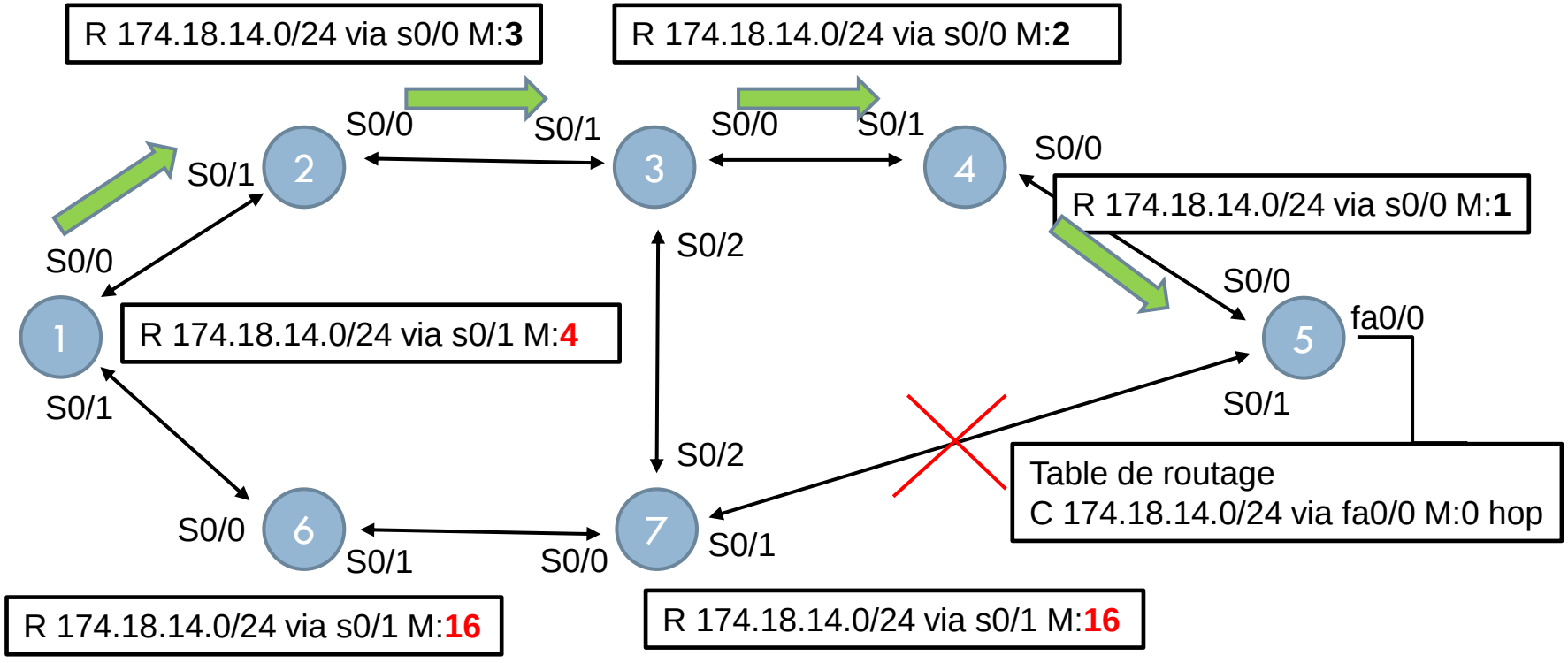
Le routeur 1 reçoit une meilleure route du routeur 2 (mise à jour régulière)



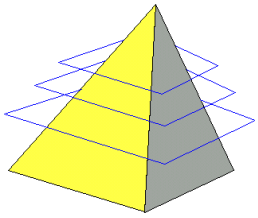
Le routeur 1 prend en compte cette nouvelle route

RIP - Fonctionnement

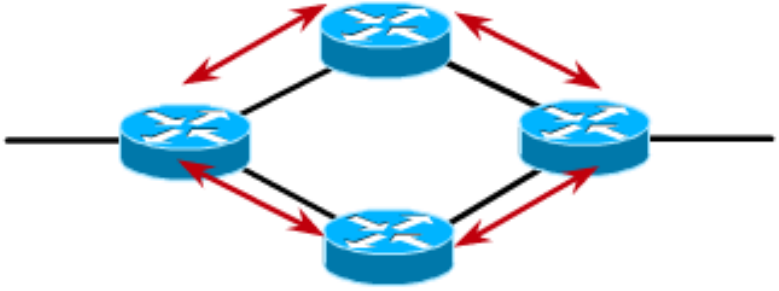
Le routeur 1 dirige les paquets pour le réseau 174.18.14.0 via s0/0



Protocoles de Routage

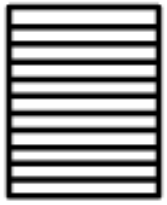


Notion d'état de la liaison



Paquets de mise à jour à état de liaison

Base de données topologiques



Algorithme SPF

Arbre du plus court chemin d'abord

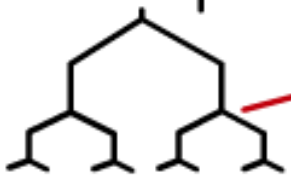
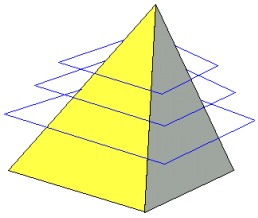


Table de routage

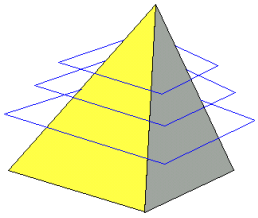
- Après le flot initial, envoi de petites mises à jour déclenchées par événement à tous les autres routeurs.

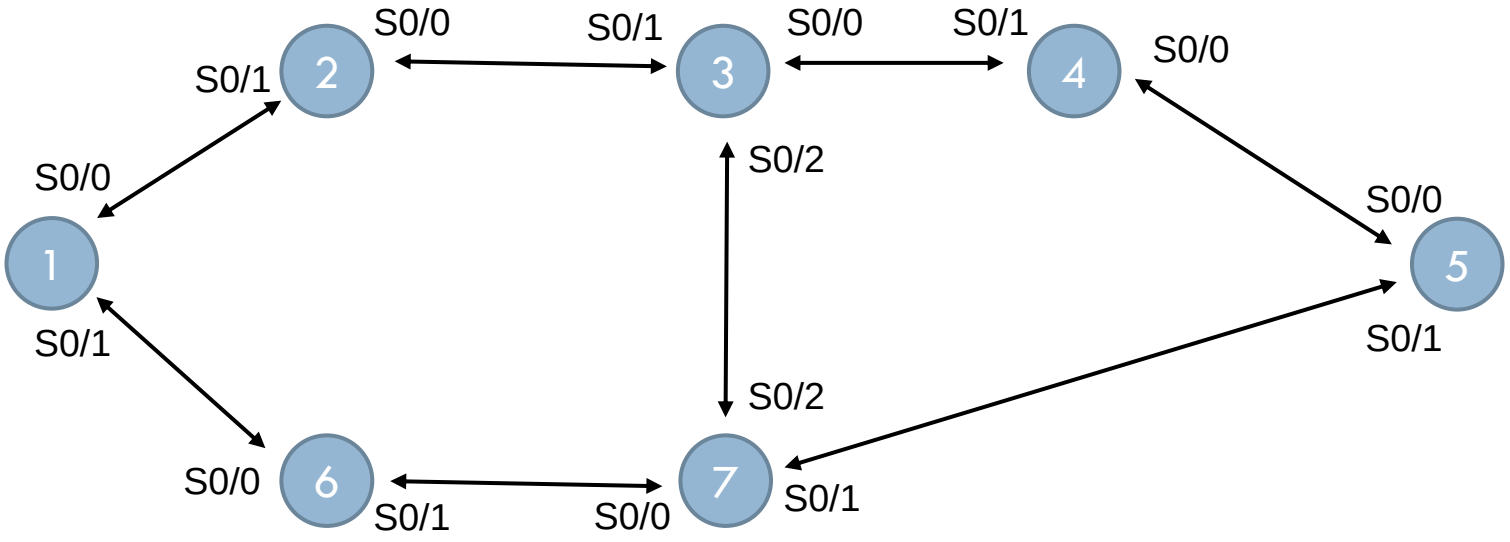
OSPF – Fiche technique



- Métrique : somme des coûts des liens
- Mise à jour : par événement et périodique (30 minutes)
- Vision : ensemble du domaine OSPF
- Taille : non limitée (en pratique pas plus de 50 routeurs)
- Historique : classless /CIDR
- Configuration : relativement complexe (multi-areas)
- Convergence : rapide

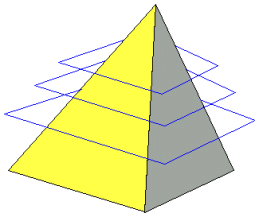
OSPF - Fonctionnement



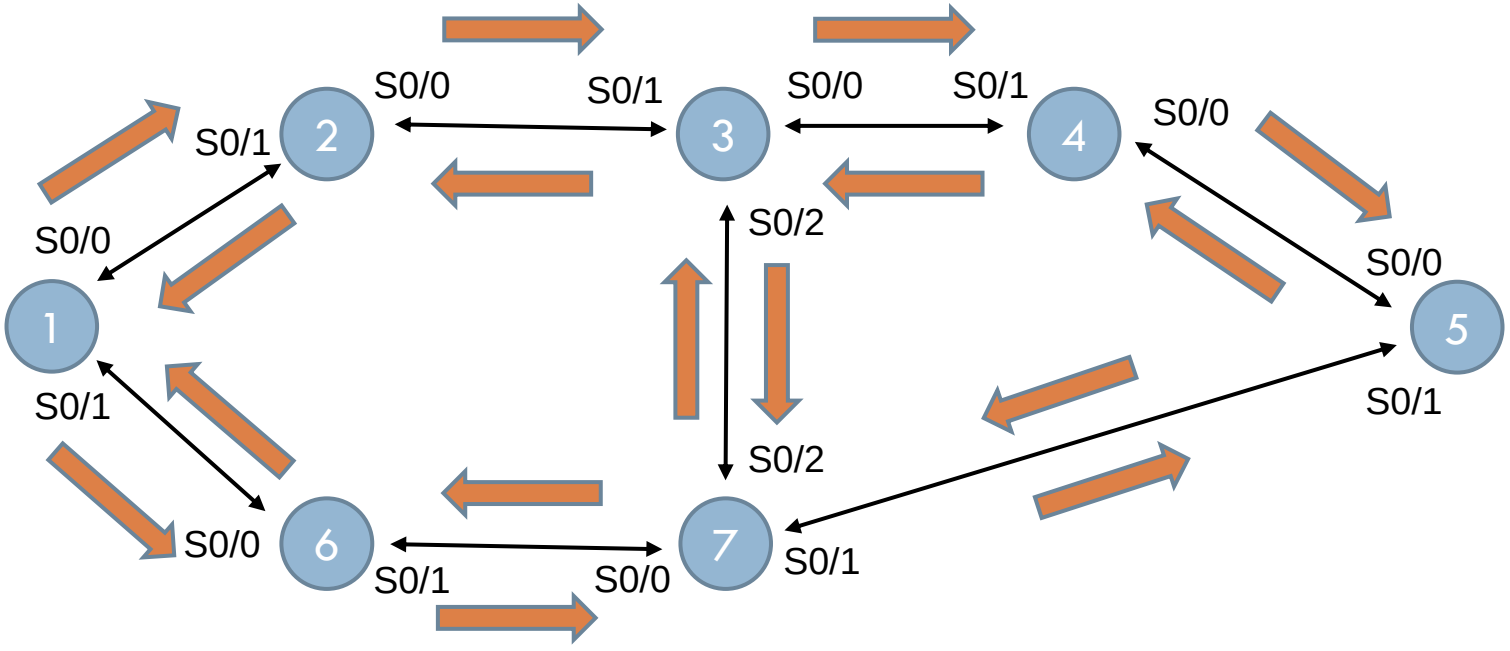


Supposons que tous les routeurs redémarrent et voyons ce qu'il se passe.

OSPF - Fonctionnement

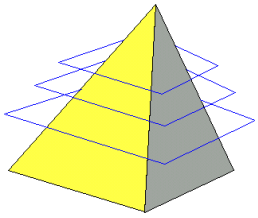


Première phase : les routeurs échangent des paquets HELLO

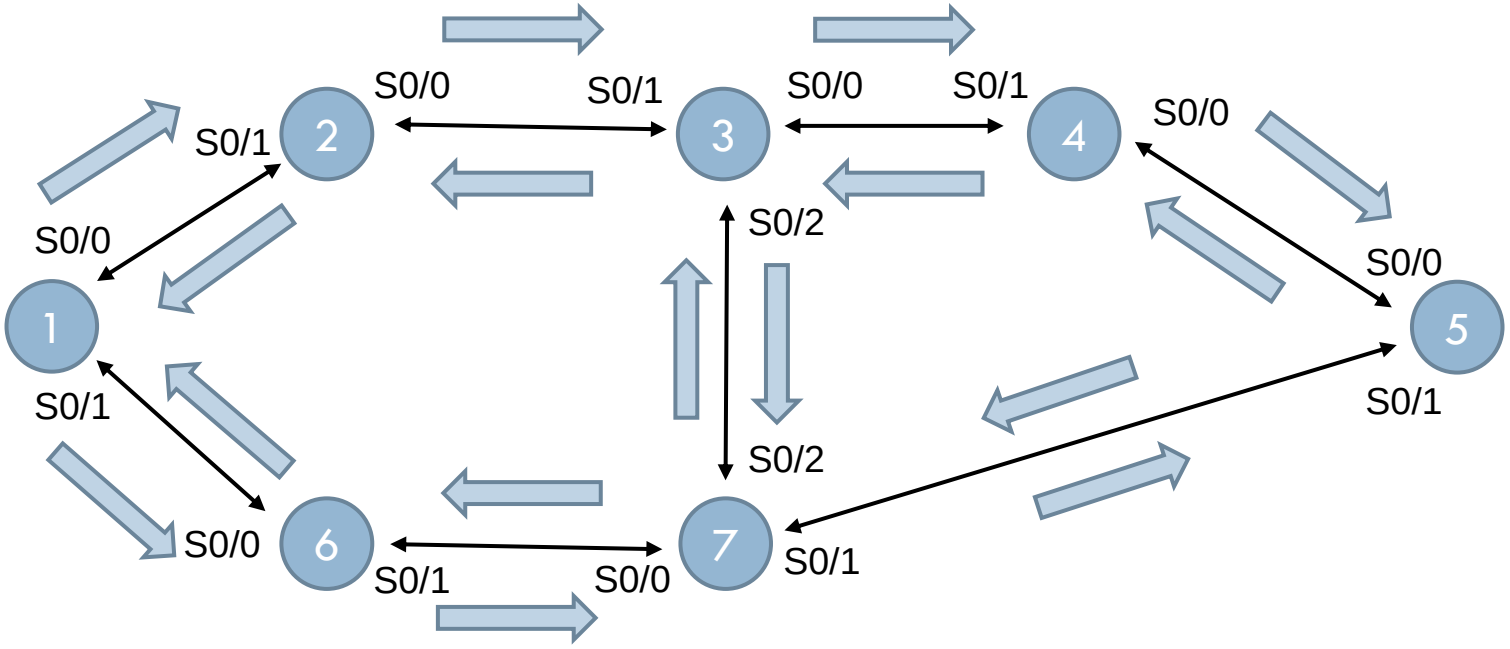


Etat : ExStart.

OSPF - Fonctionnement

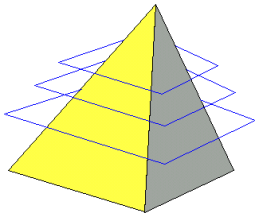


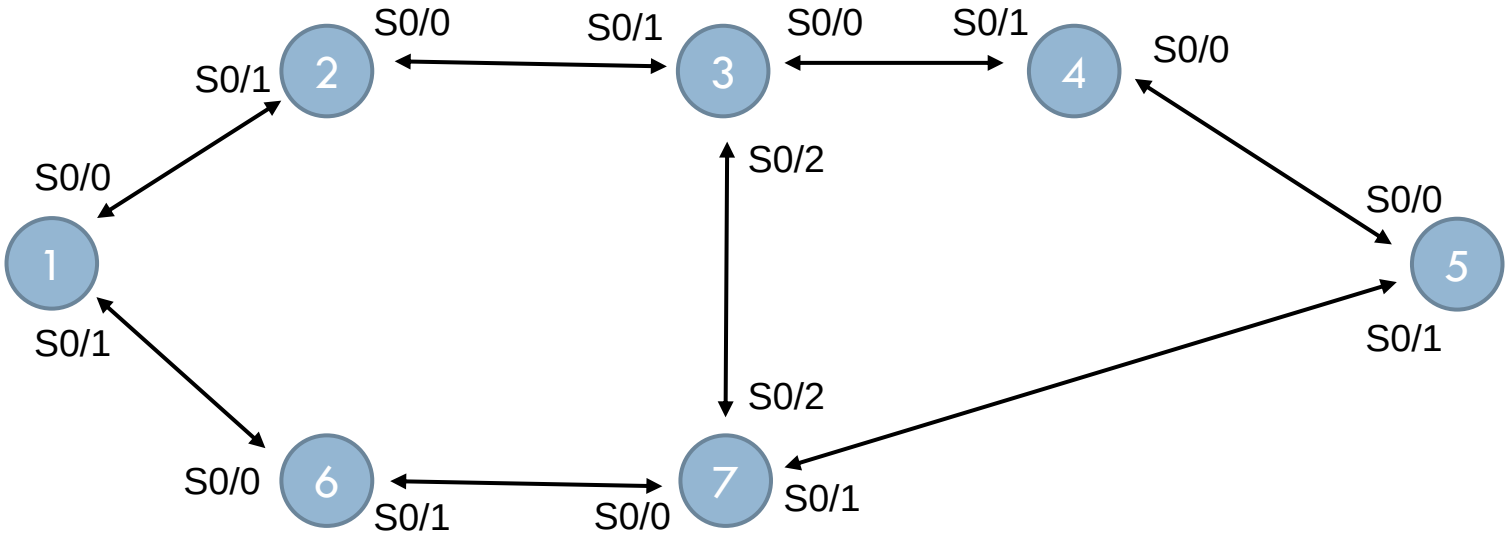
Deuxième phase : les routeurs échangent des informations topologiques



Etat : Loading.

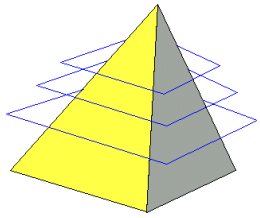
OSPF - Fonctionnement

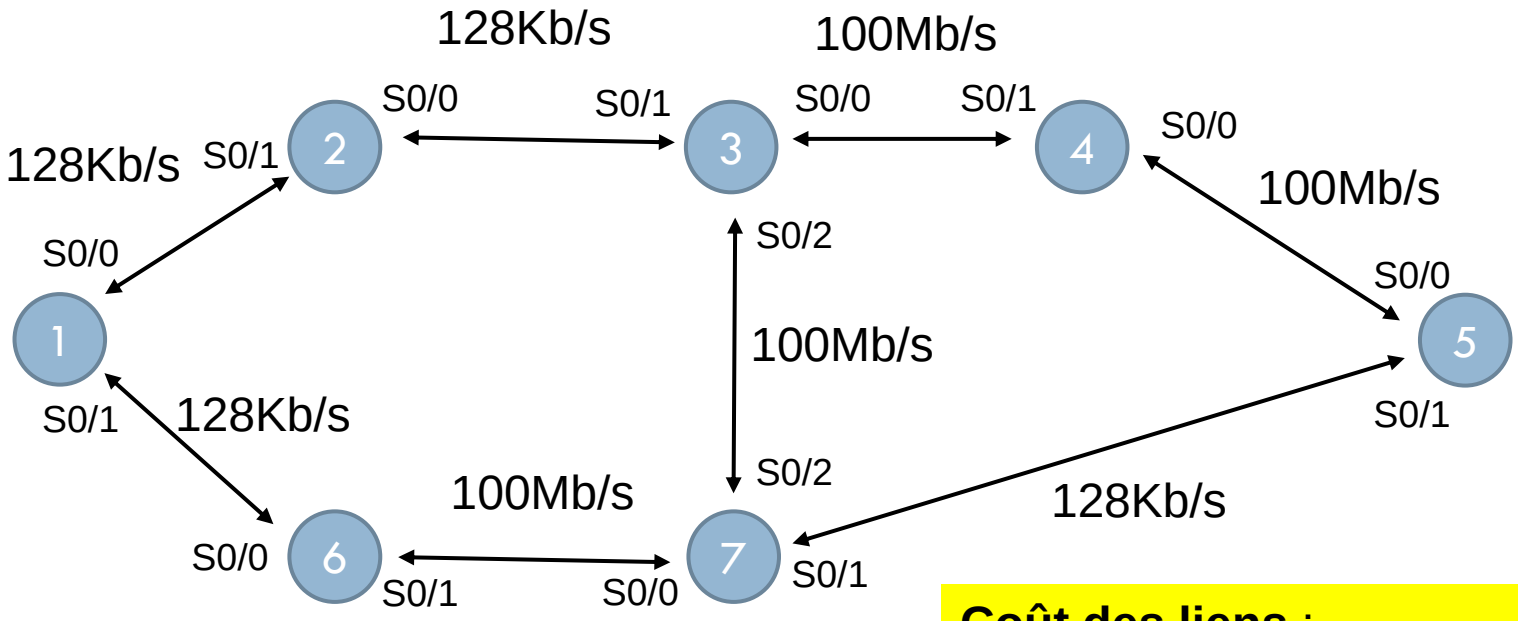




Etat : Full.

OSPF - Fonctionnement

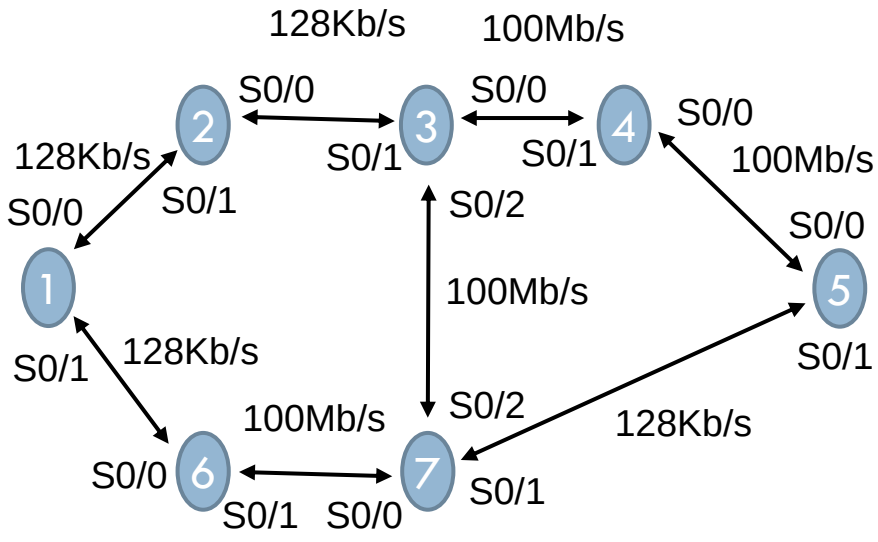




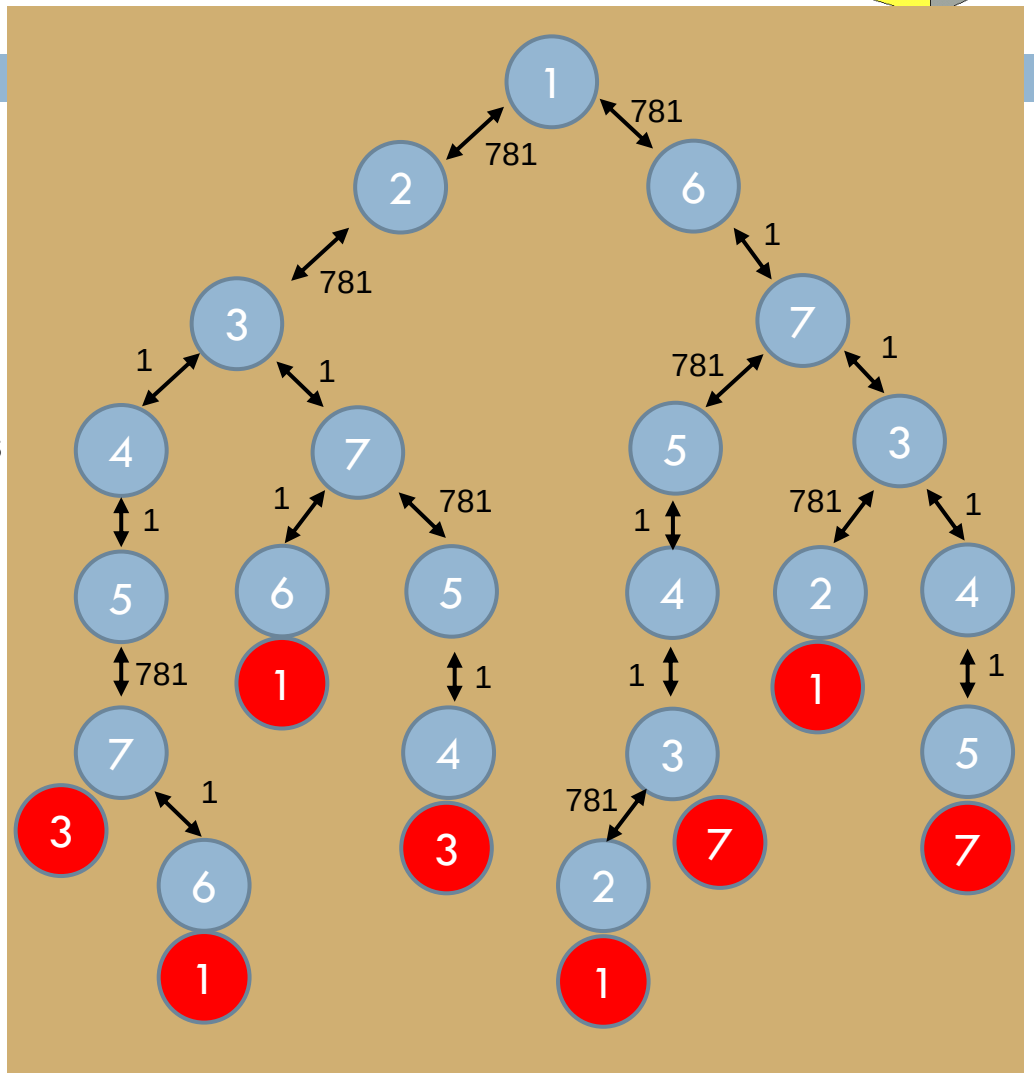
Coût des liens :
100Mb/s : 1
128Kb/s : 781

OSPF - Fonctionnement

Arbre du point de vue du routeur 1

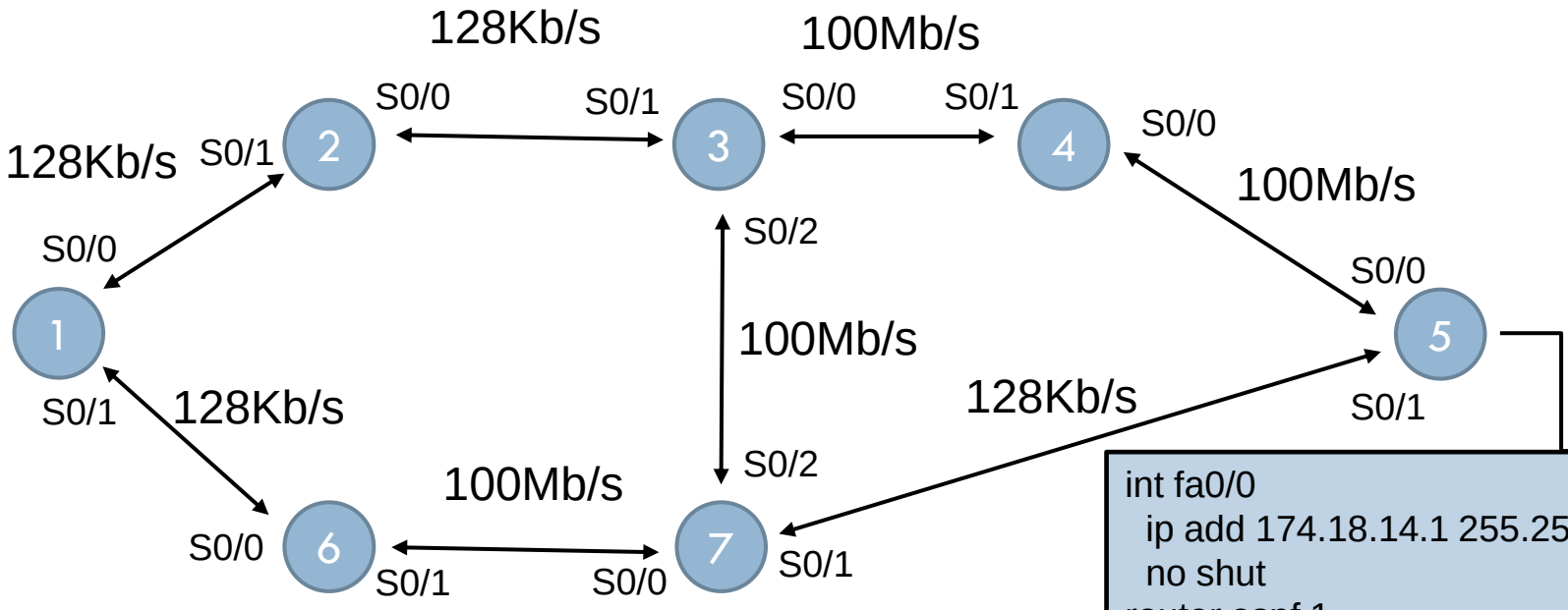


Coût des liens :
100Mb/s : 1
128Kb/s : 781



OSPF - Fonctionnement

Si un administrateur réseau entre les commandes suivantes sur le routeur 5…



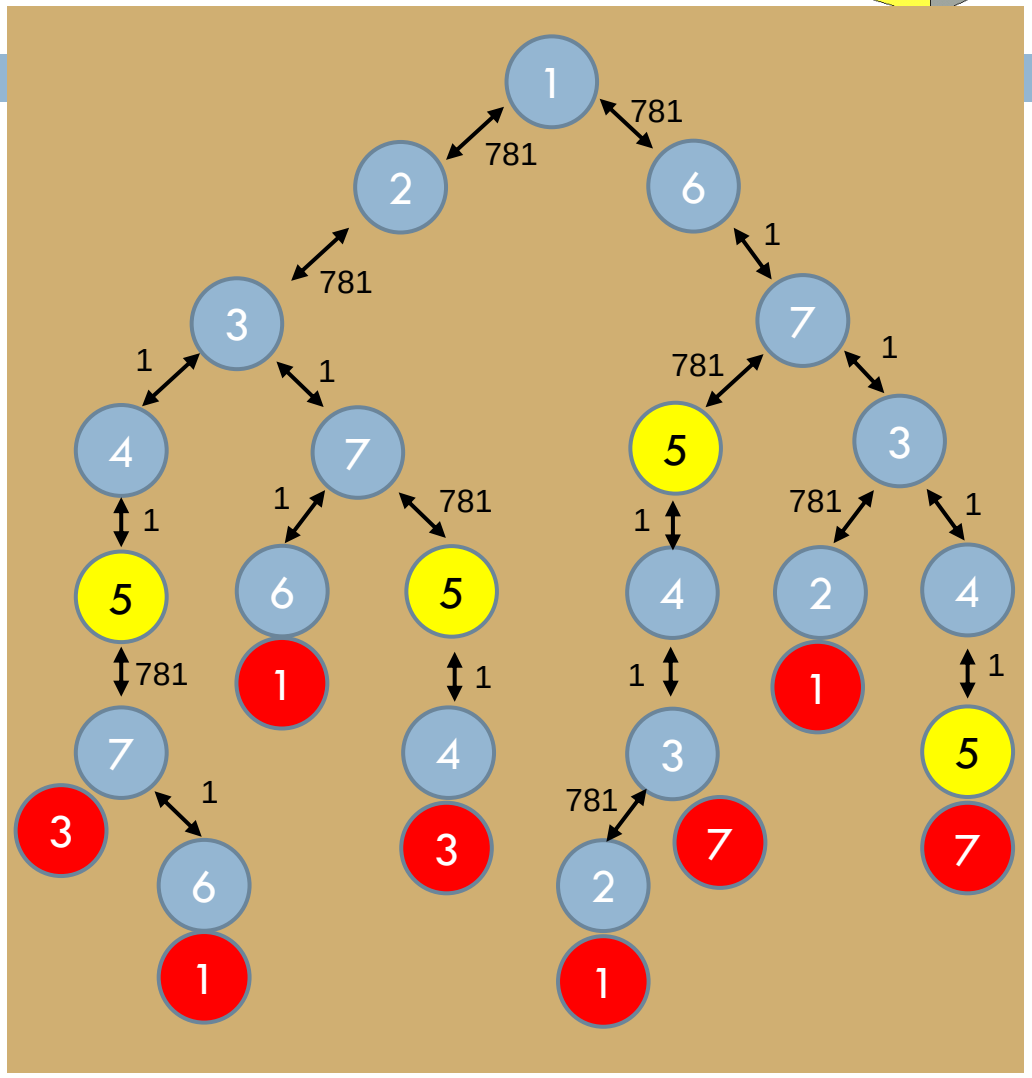

```
int fa0/0
  ip add 174.18.14.1 255.255.255.0
  no shut
router ospf 1
  network 174.18.14.1 0.0.0.0 area 0
```

… la nouvelle route va être propagée (mise à jour événementielle) à travers le domaine OSPF, jusqu'à R1

OSPF - Fonctionnement

1) R1 reçoit la mise à jour,
2) Puis actionne l'algorithme SPF pour calculer le chemin de moindre coût vers cette destination.

La route via 2, 3 et 4 coûte :
781+781+1+1= 1564
La route via 2, 3 et 7 coûte :
781+781+1+781= 2344
La route via 6, 7 et 5 coûte :
781+1+781= 1563
Enfin, la route via 6, 7,3, 4 coûte :
781+1+1+1+1=**785**

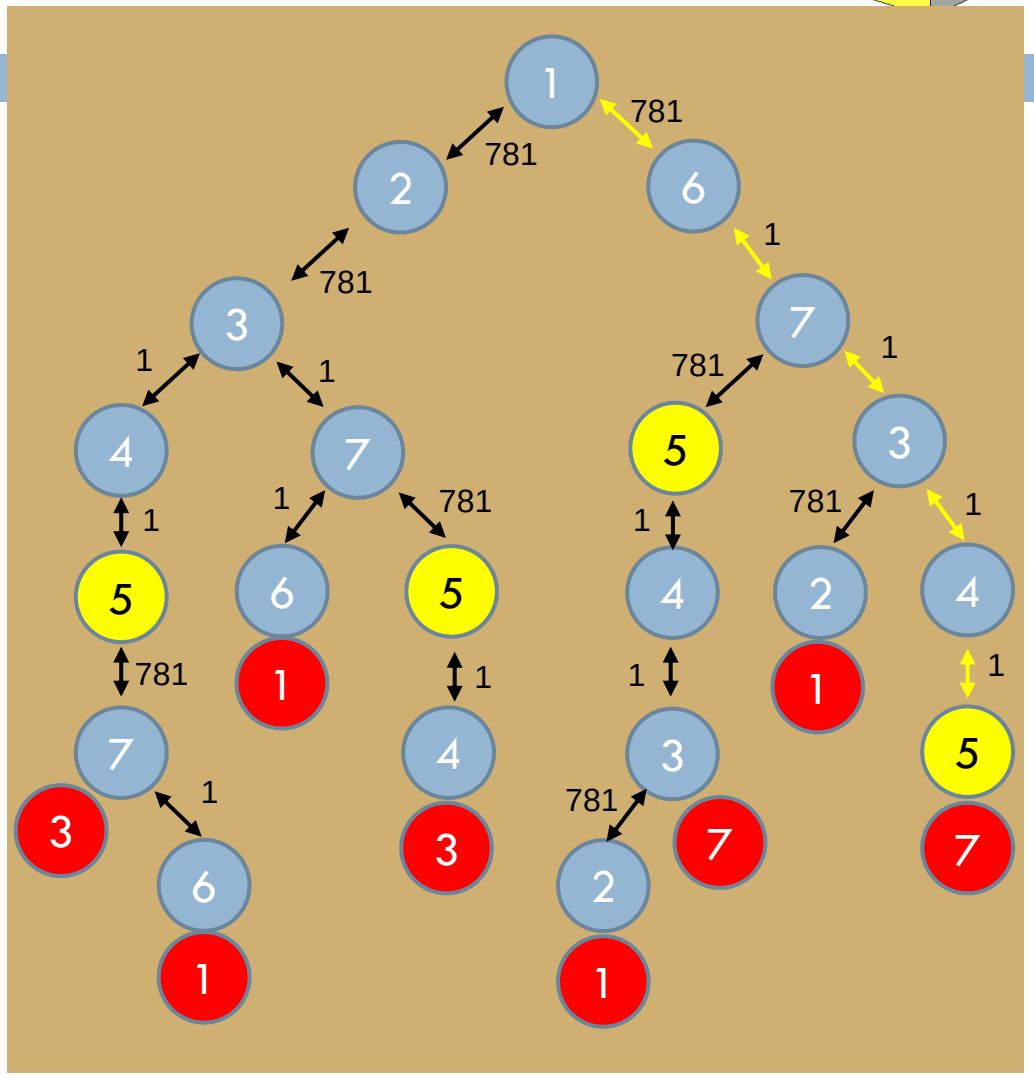


OSPF - Fonctionnement

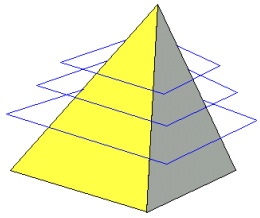
1) R1 reçoit la mise à jour,
2) Puis actionne l'algorithme SPF pour calculer le chemin de moindre coût vers cette destination.

La route via 2, 3 et 4 coûte :
781+781+1+1= 1564
La route via 2, 3 et 7 coûte :
781+781+1+781= 2344
La route via 6, 7 et 5 coûte :
781+1+781= 1563
Enfin, la route via 6, 7,3, 4 coûte :
781+1+1+1+1=**785**

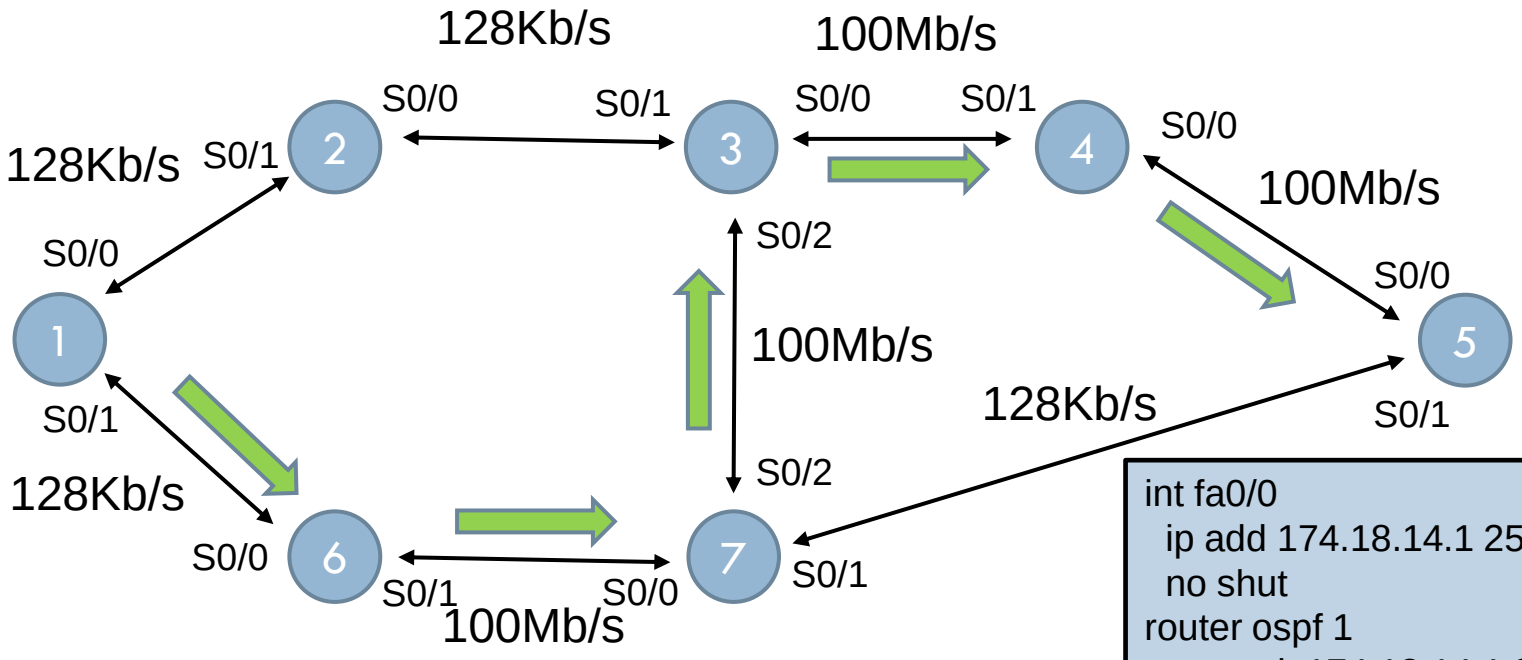
R1 installe la meilleure route, via R6 dans sa table de routage.



OSPF - Fonctionnement



Route de R1 vers net 174.18.14.0 : R6, R7, R3, R4, R5



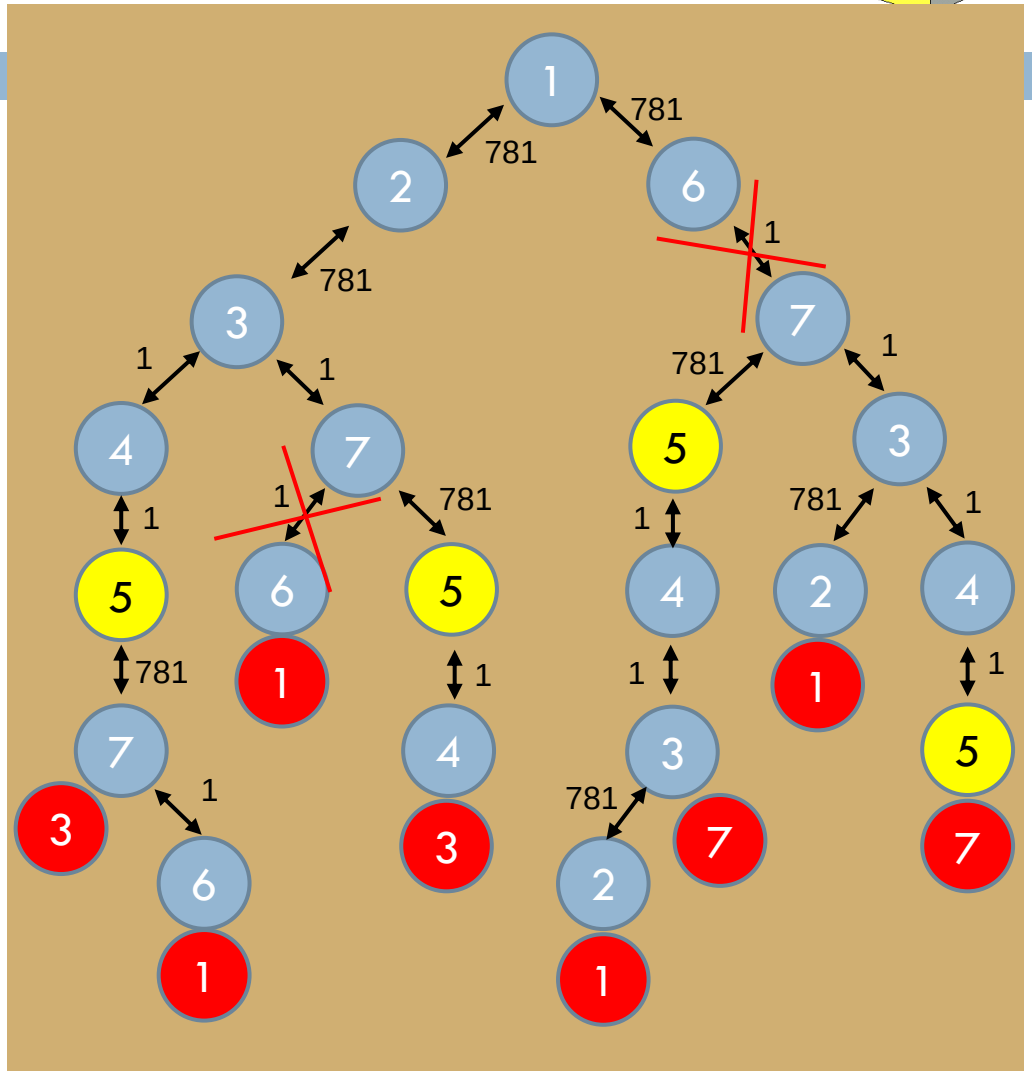

```
int fa0/0
  ip add 174.18.14.1 255.255.255.0
  no shut
router ospf 1
  network 174.18.14.1 0.0.0.0 area 0
```

OSPF - Fonctionnement

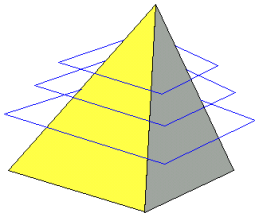
Si le lien entre R6 et R7 est rompu, R1 reçoit une mise à jour, modifie son arbre et relance SPF.

La route via 2, 3 et 4 coûte :
781+781+1+1= **1564**
La route via 2, 3 et 7 coûte :
781+781+1+781= 2344

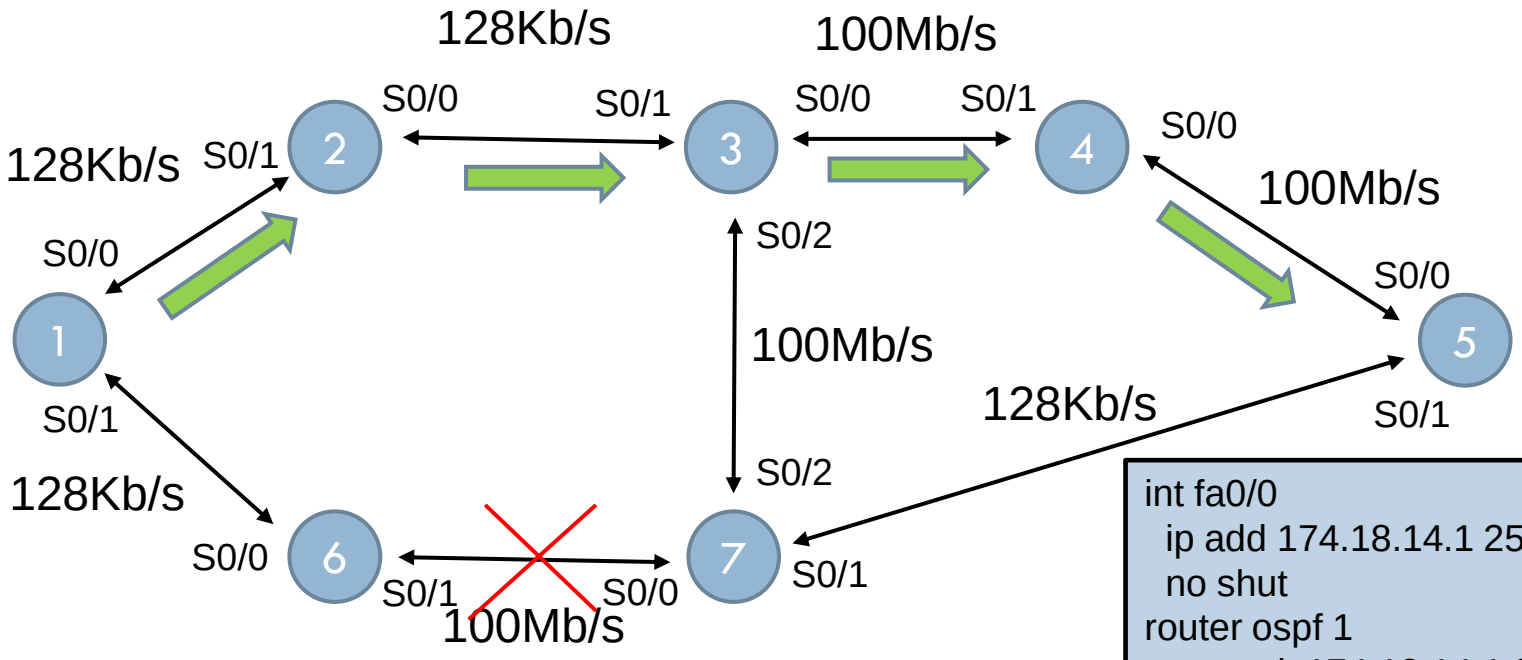
La nouvelle route installée passe maintenant par R2.



OSPF - Fonctionnement

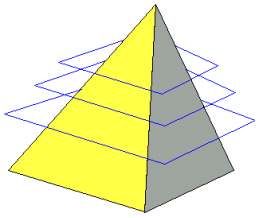


Route de R1 vers net 174.18.14.0 : R2, R3, R4, R5




```
int fa0/0
  ip add 174.18.14.1 255.255.255.0
  no shut
router ospf 1
  network 174.18.14.1 0.0.0.0 area 0
```

Subnets : VLSM - CIDR



- En 1996, les routeurs explosent sous le nombre de routes à traiter (180 000 routes)
- La solution est de **résumer** (ou synthétiser) plusieurs routes en une seule, qui devient ainsi un **super-réseau**
- VLSM est alors associé à CIDR (Classless Inter Domain Routing) pour modifier la façon dont un routeur commute les paquets
  - Les super-réseaux ont des masques parfois plus petits que leur classe
  - D'où le dénominatif : classless (sans classe)
  - CIDR permet d'accepter des exceptions en favorisant la route la plus précise

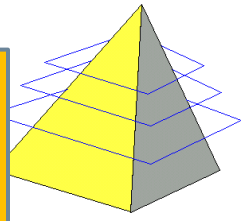


Table de routage

- Fa0/0 : 174.18.64.0/24
- Fa0/0 : 174.18.65.0/25
- Fa0/0 : 174.18.65.128/26
- Fa0/0 : 174.18.66.0/23
- Fa0/0 : 174.18.65.192/26
- … 10 routes !

Fa0/0 174.18.64.0/21 Fa0/1

174.18.64.0/22

174.18.64.0/23

N5: 174.18.66.0/23

N1: 174.18.64.0/24

174.18.65.0/24

N2: 174.18.65.0/25

174.18.65.128/25

N3: 174.18.65.128/26

N3: 174.18.65.192/26

174.18.68.0/22

N6: 174.18.68.0/23

174.18.70.0/23

174.18.70.0/24

N10: 174.18.71.0/24

N7: 174.18.70.0/25

174.18.70.128/25

N8: 174.18.70.128/26

N9: 174.18.70.192/26

VLSM

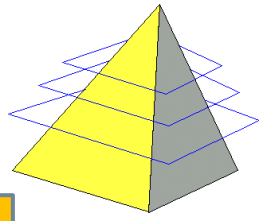
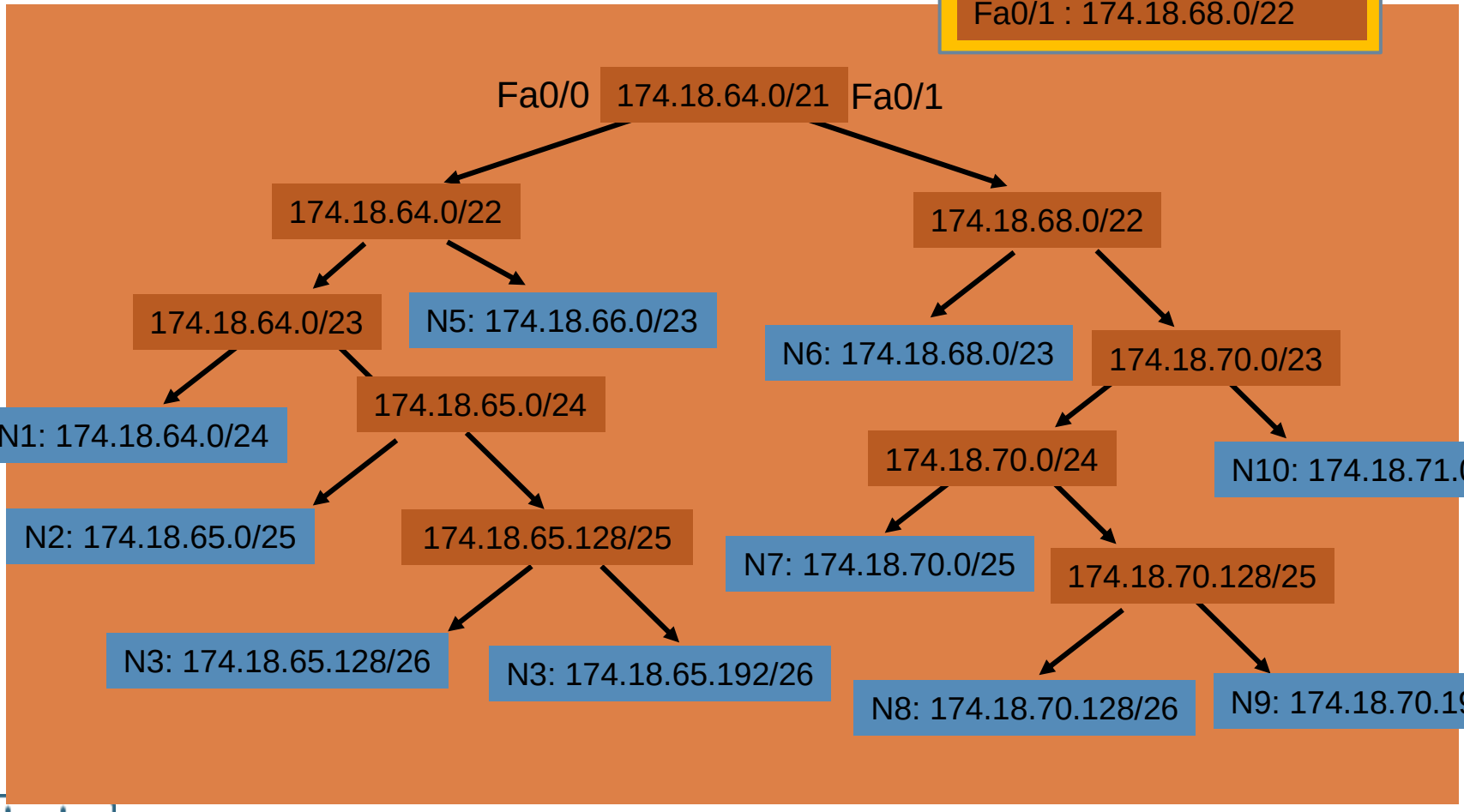


Table de routage

Fa0/0 : 174.18.64.0/22
Fa0/1 : 174.18.68.0/22



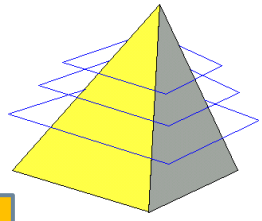
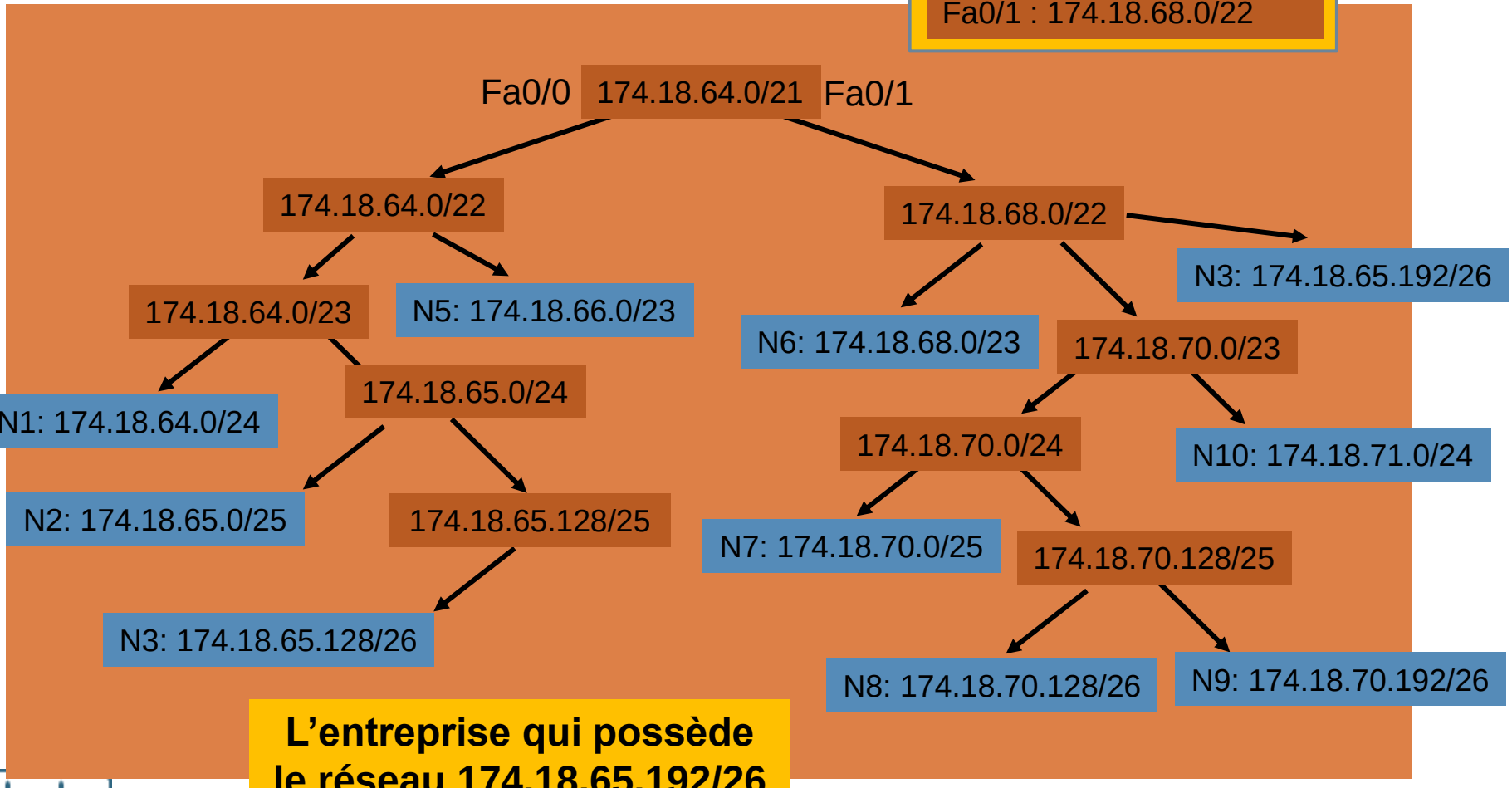


Table de routage

Fa0/0 : 174.18.64.0/22
Fa0/1 : 174.18.68.0/22



L'entreprise qui possède le réseau 174.18.65.192/26 déménage

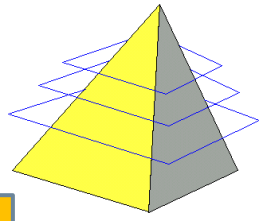
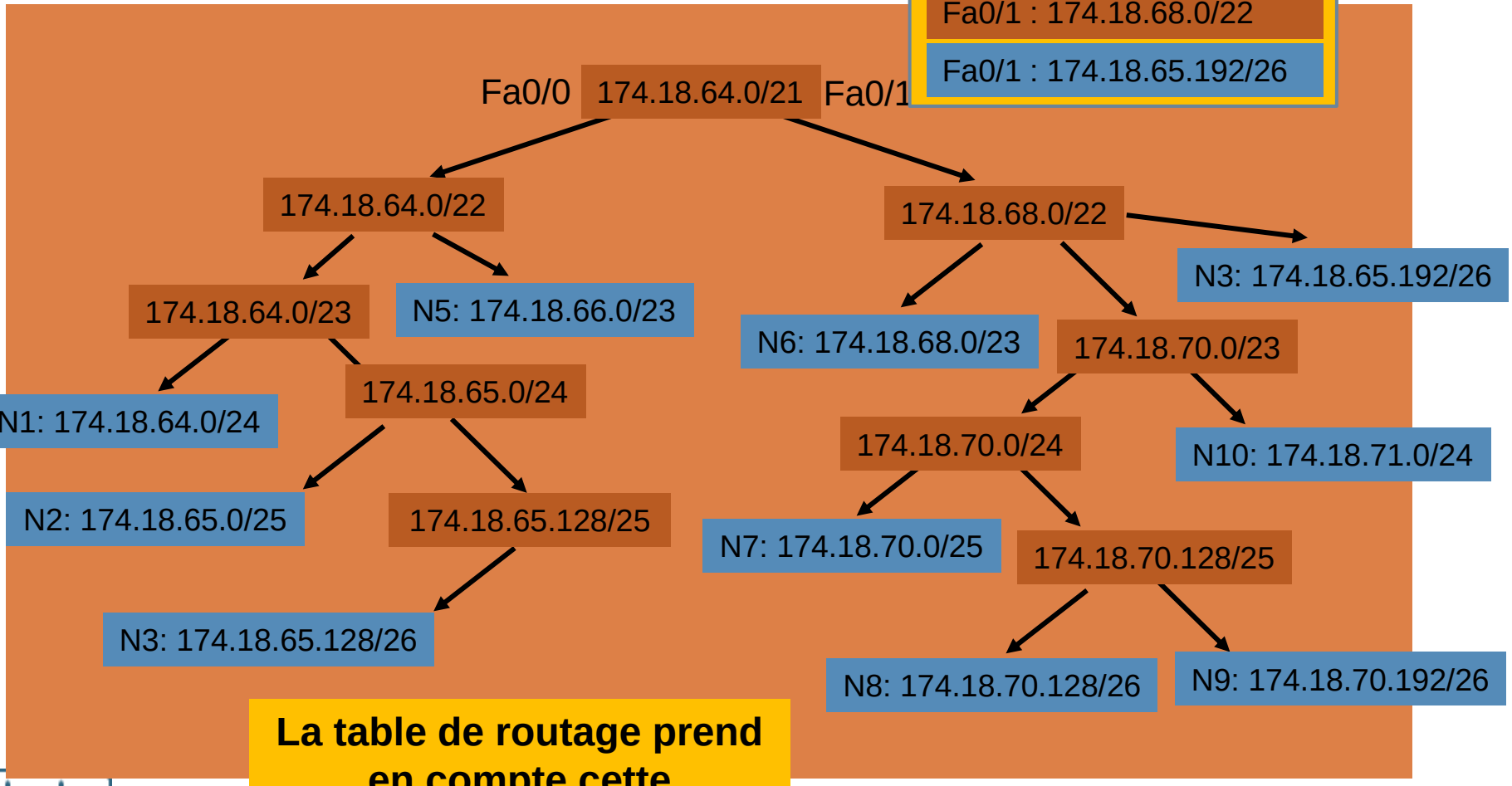


Table de routage

- Fa0/0 : 174.18.64.0/22
- Fa0/1 : 174.18.68.0/22
- Fa0/1 : 174.18.65.192/26



La table de routage prend en compte cette modification

VLSM & CIDR

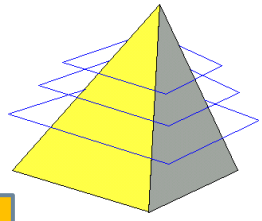
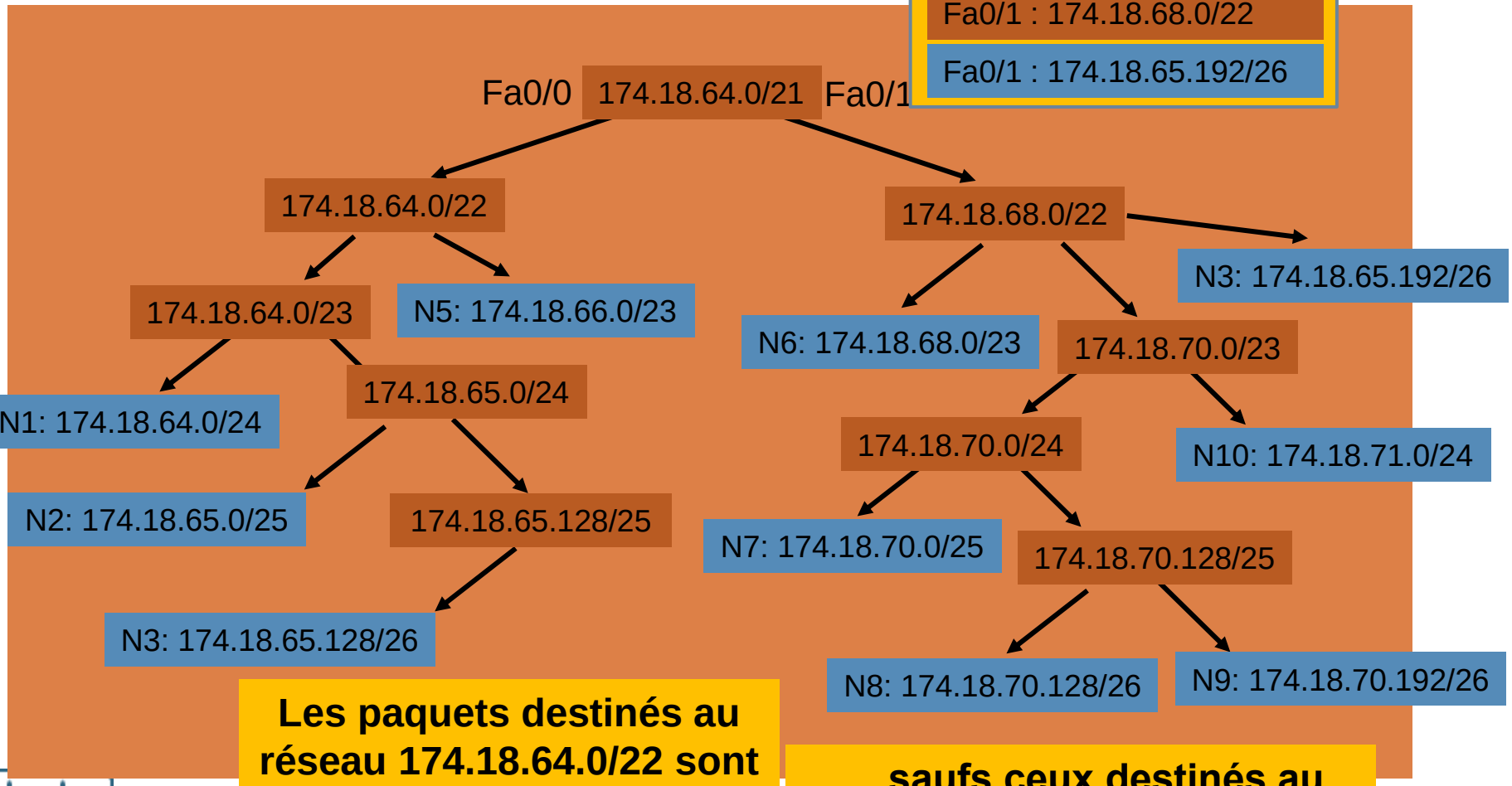


Table de routage

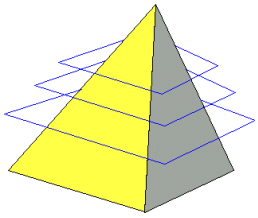
- Fa0/0 : 174.18.64.0/22
- Fa0/1 : 174.18.68.0/22
- Fa0/1 : 174.18.65.192/26



Les paquets destinés au réseau 174.18.64.0/22 sont commutés via la Fa0/0…

… saufs ceux destinés au réseau 174.18.65.192/26 qui sont commutés via la Fa0/1

Subnets : VLSM - CIDR



- En 1996, les routeurs explosent sous le nombre de routes à traiter (180 000 routes)
- La solution est de **résumer** (ou synthétiser) plusieurs routes en une seule, qui devient ainsi un **super-réseau** (=>90 000 routes)
- VLSM est associé à CIDR (Classless Inter Domain Routing) pour modifier la façon dont un routeur commute les paquets
  - Avant CIDR, la première route concordante était utilisée pour commuter le paquet
    - Exemple : 192.168.14.0/24 via s0/0/0 – Paquet arrivant destiné à 192.168.14.139 => **s0/0/0**
  - Avec CIDR, la table de routage est entièrement parcourue et c'est la route la plus précise qui est choisie
    - Exemple : Table de routage

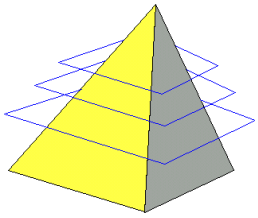
      192.168.14.0/24 via s0/0/0

      192.168.14.128/25 via s0/1/0

      192.168.14.128/28 via s0/1/1

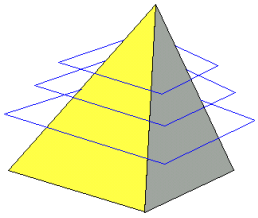
Paquet arrivant destiné à 192.168.14.139 => s0/1/1
Paquet arrivant destiné à 192.168.14.159 => s0/1/0
Paquet arrivant destiné à 192.168.14.19 => s0/0/0

COUCHE 4 : connexion



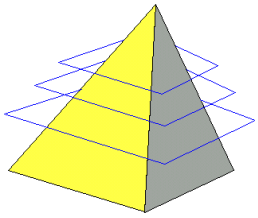
- Est-il raisonnable d'échanger avec quelqu'un sans savoir s'il existe ? (ou écoute)
  - Oui, s'il s'agit d'une diffusion
  - Oui, si la réponse attendue tient en une seule phrase
  - Non, dans les autres cas
- Dans ce troisième cas, TCP construit un lien virtuel entre deux paires
  - TCP installe une relation orientée connexion au dessus d'un transport déconnecté

COUCHE 4 : Transport

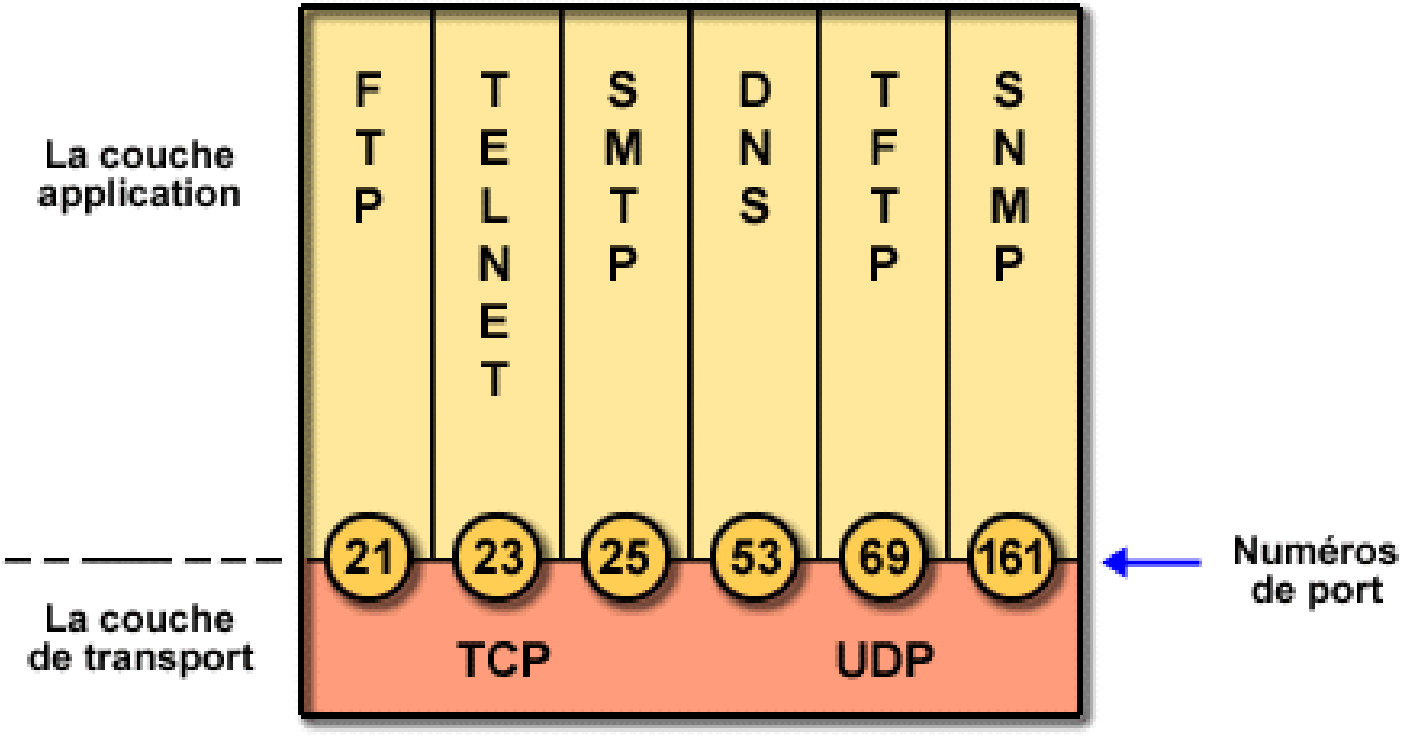


- Segment
- Adresses de couche 4 : ports
- Structure d'un segment TCP
- Structure d'un segment UDP

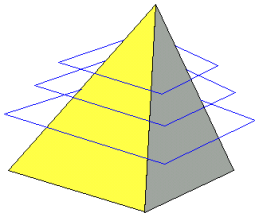
Adressage de couche 4



Numéros de port



Segment TCP



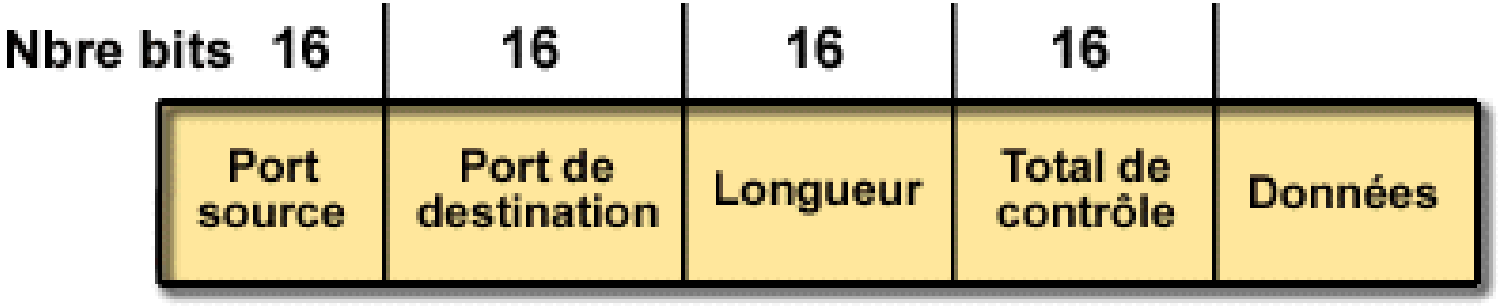
Structure de segment TCP

Nbre bits	16	16	32	32	4	6	6
	Port source	Dest. Port	Numéro de séquence	Numéro d'accusé de réception	HLEN	Réservé	Bits code

16	16	16	0 ou 32	
Fenêtre	Total de contr.	Pointeur d'urgence	Option	Données…

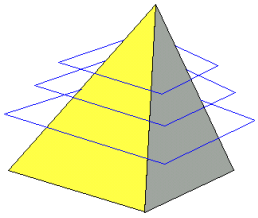
Segment UDP

Structure de segment UDP



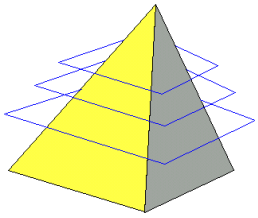
- Pas de champs de séquence ou d'accusé de réception

UDP : sans connexion



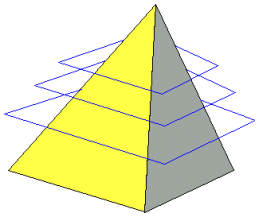
- UDP = ni fenêtrage, ni accusés de réception.
- => les protocoles de couche application doivent assurer la fiabilité.
- UDP est conçu pour les applications qui n'ont pas à assembler des séquences de segments.
- Voici quelques protocoles qui utilisent UDP :
  - TFTP, SNMP, DHCP, DNS
- Applications qui utilisent UDP
  - VoIP, Visioconférence, Streaming,… pour le transport des données temps réel

TCP : orienté connexion

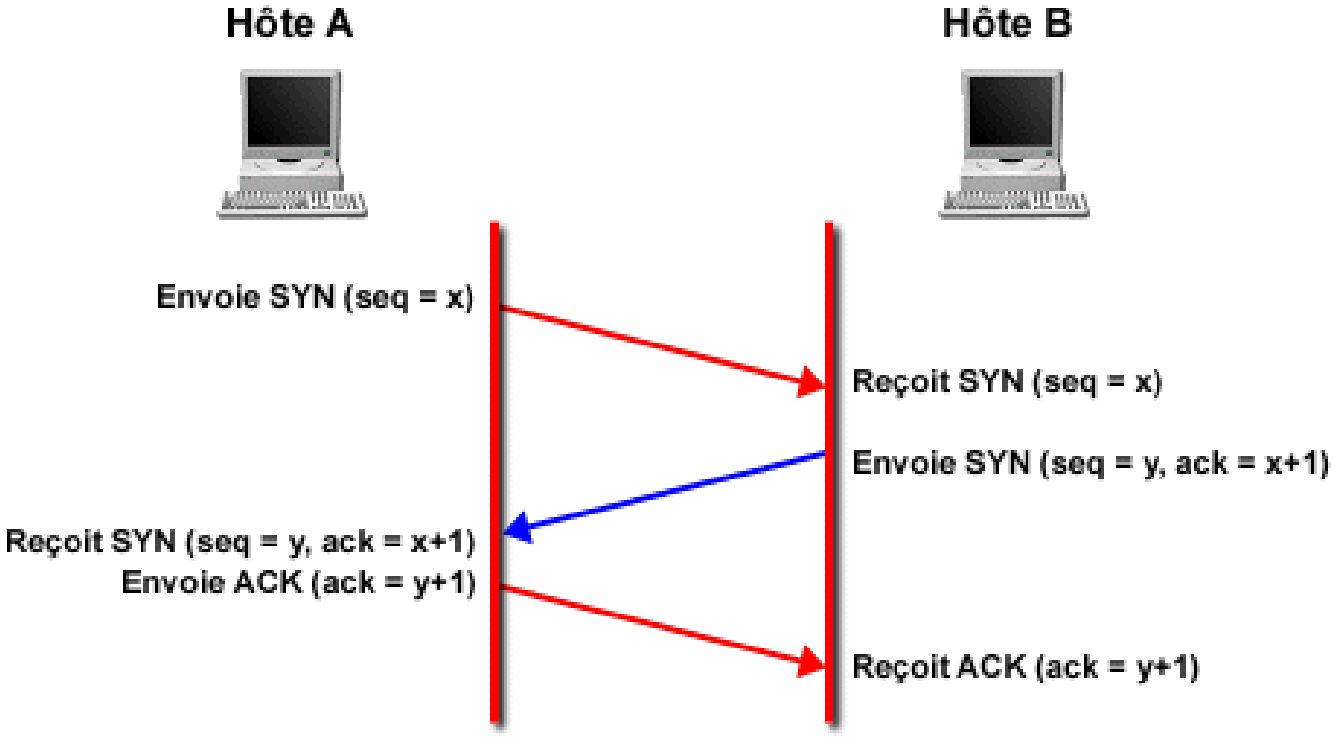


- Three way handshake
- Numérotation des segments
- Accusés de réception
- Fenêtre TCP

Three Way Handshake

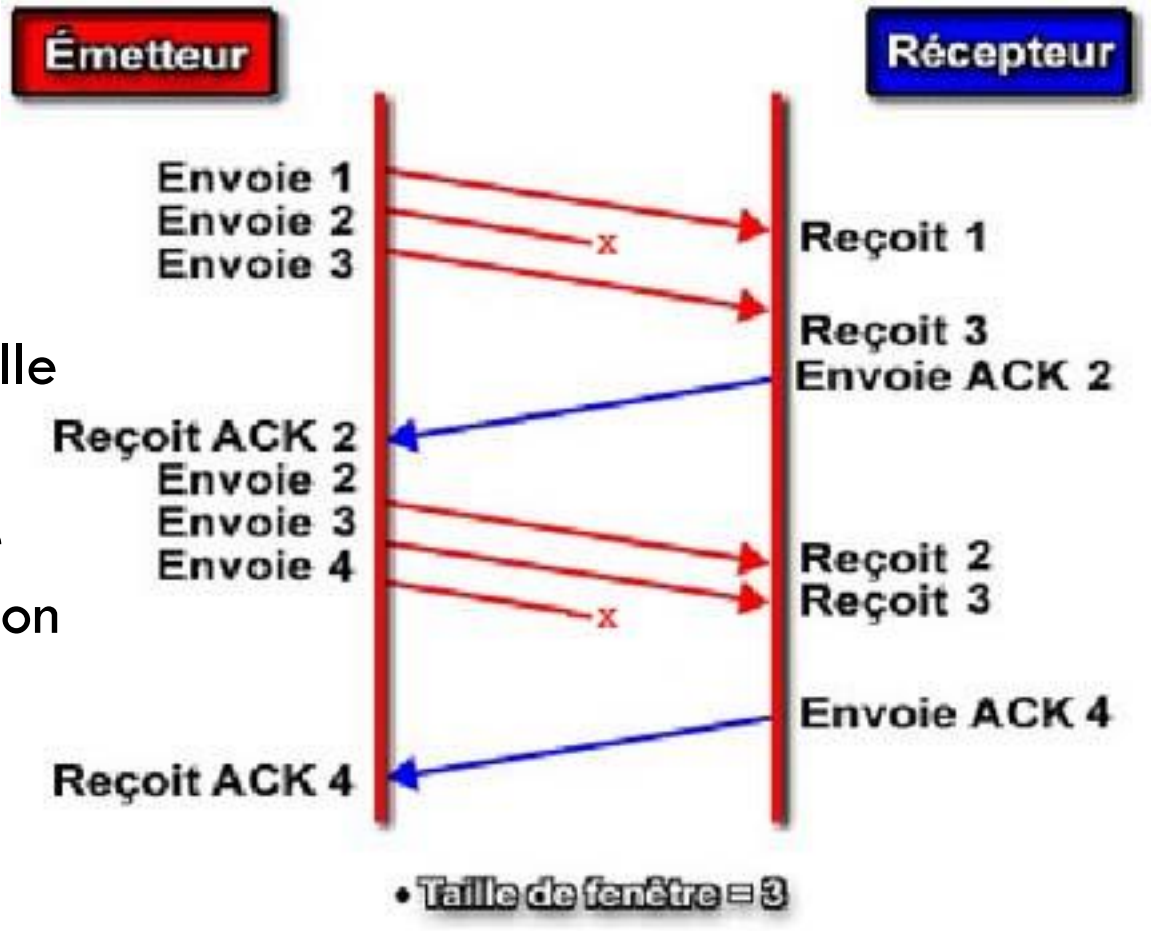


Établir une connexion/échange en 3 étapes TCP



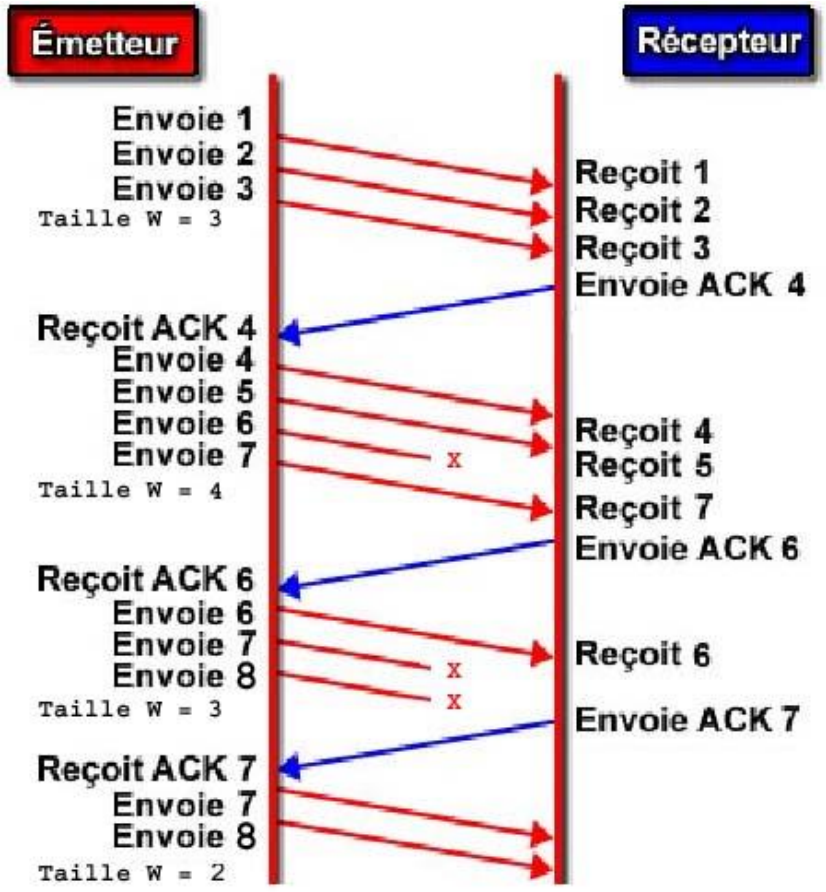
Mécanisme d'accusé réception

- L'émetteur envoie plusieurs segments numérotés.
- Leur nombre est déterminé par la taille de la fenêtre TCP.
- Le récepteur renvoie un accusé de réception avec le numéro du prochain segment attendu.

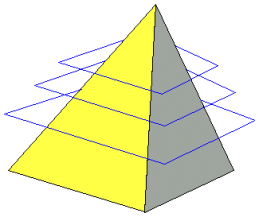


Fenêtre glissante

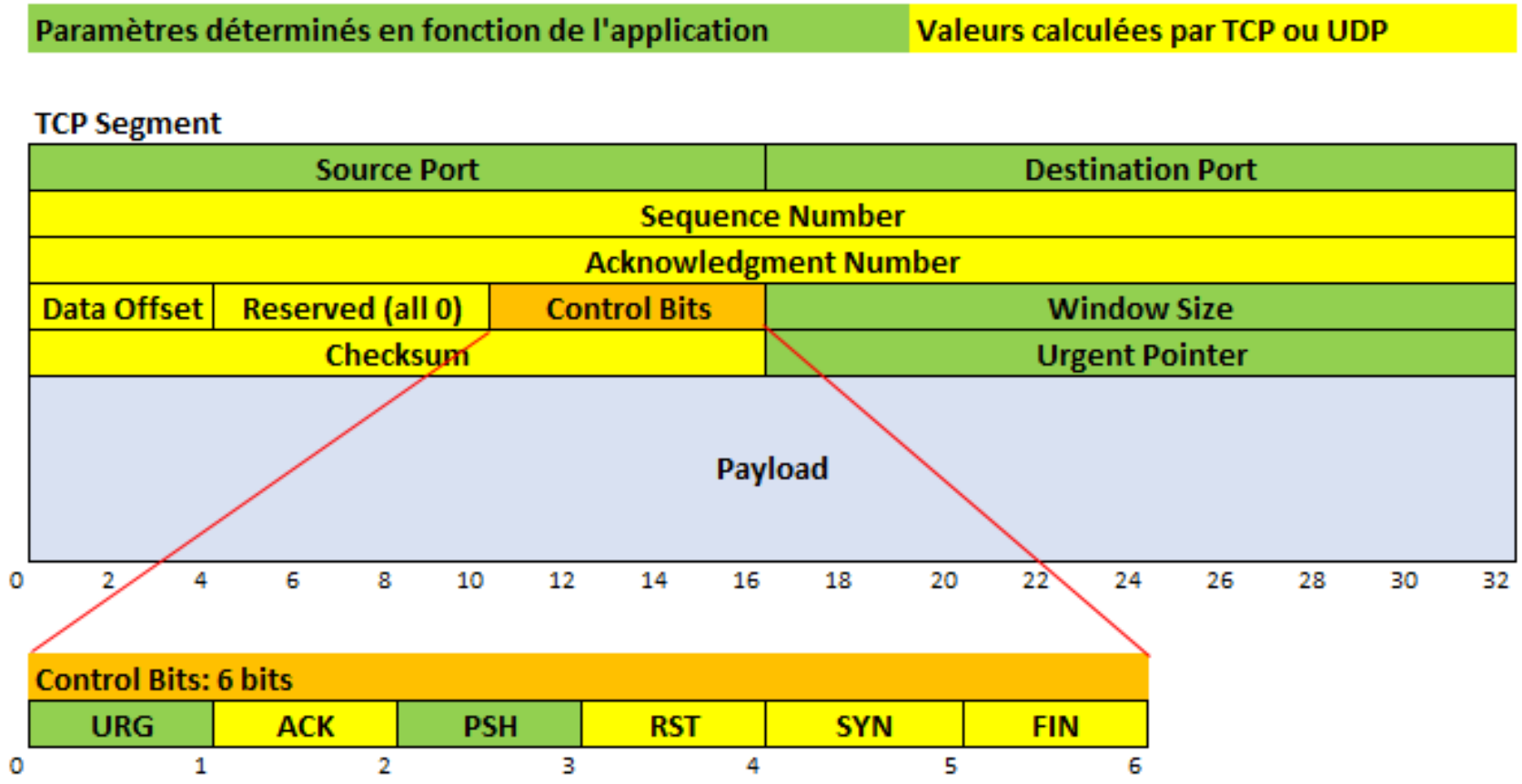
- Les hôtes commencent l'échange avec une taille de fenêtre par défaut.
- Ils cherchent ensuite à augmenter cette taille si la disponibilité du réseau est suffisante.
- Si les communications sont peu fiables ils diminueront la taille de la fenêtre glissante.



TCP Flags

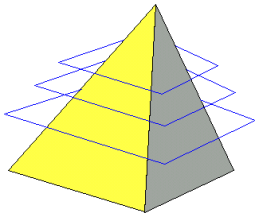


- URGENT, PUSH



KALYST
INGENIERIE INFORMATIQUE

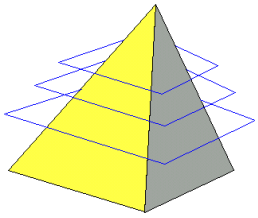
Algorithme d'émission



- Couple <IP/Port> = socket
- Ports parfaitement définis (Well known ports) :
  - plage 0 à 1023
- Ports déposés (Registered ports) :
  - plage1024 à 49151
- Ports Dynamiques et/ou Privés (Dynamic ports) :
  - plage 49152 à 65535
- L'émetteur tire aléatoirement un numéro de port dynamique et lance un processus système d'attente de la réponse => plusieurs conversations **simultanées**

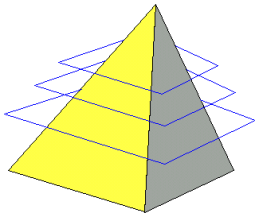
KALYST
INGENIERIE INFORMATIQUE

Conclusion Couche Transport



- Désignation du service demandé
- Temps réel ou très faible quantité de données : UDP
- Fiabilité, gestion de flux, données volumineuses : TCP

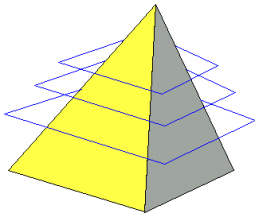
Architectures de Réseaux



- Site unique (TP Box)
  - Un réseau interne, connecté à un opérateur
  - Cas de votre Box
- Plusieurs sites (TP OSPF-BGP-VLAN)
  - Plusieurs sites connectés à un ou plusieurs opérateurs (Multihoming)
  - Le réseau Internet partagé par tout le monde va permettre d'établir des liaisons entre les sites, comme s'ils étaient proches = VPN (Virtual Private Network)

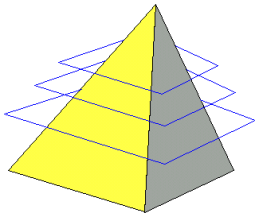
KALYST
INGENIERIE INFORMATIQUE

Topologies de réseaux

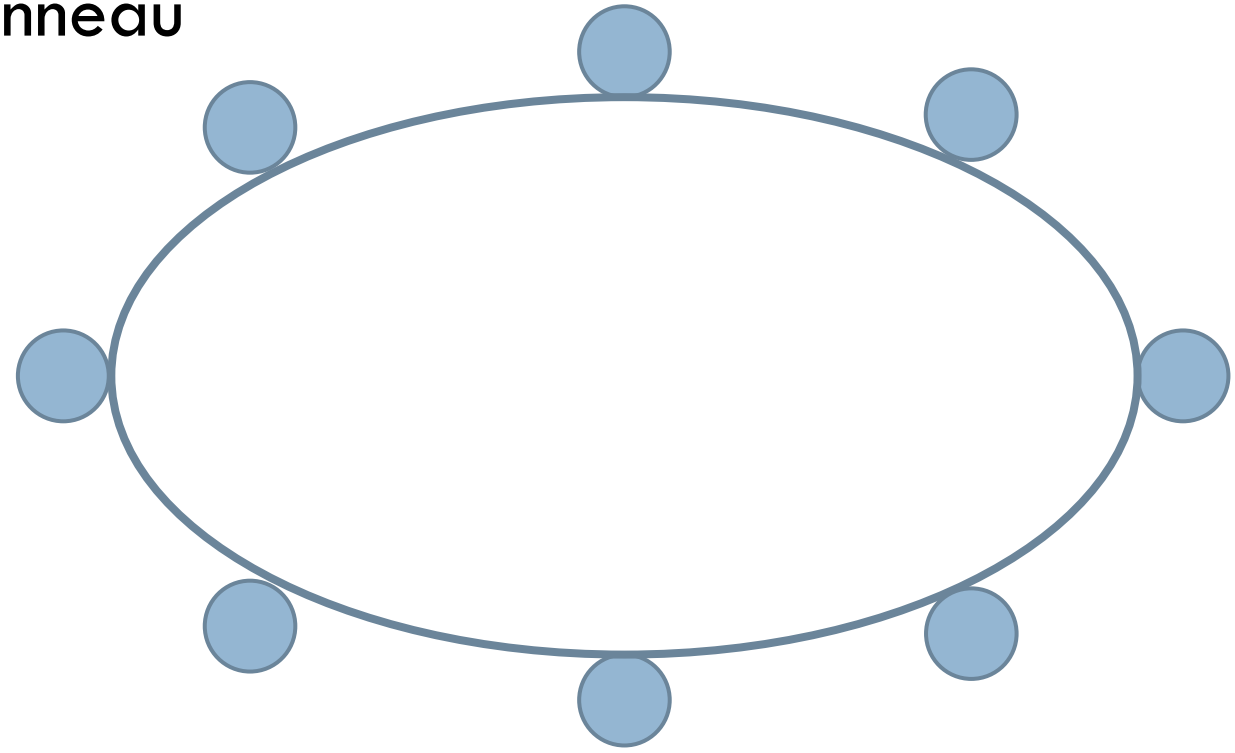


- Anneau
- Etoile
- Etoile étendue
- Réseau maillé
  - Mesh (partial mesh)
  - Full Mesh
  - Hub&Spoke

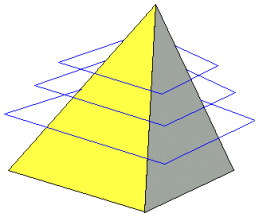
Topologies de réseaux



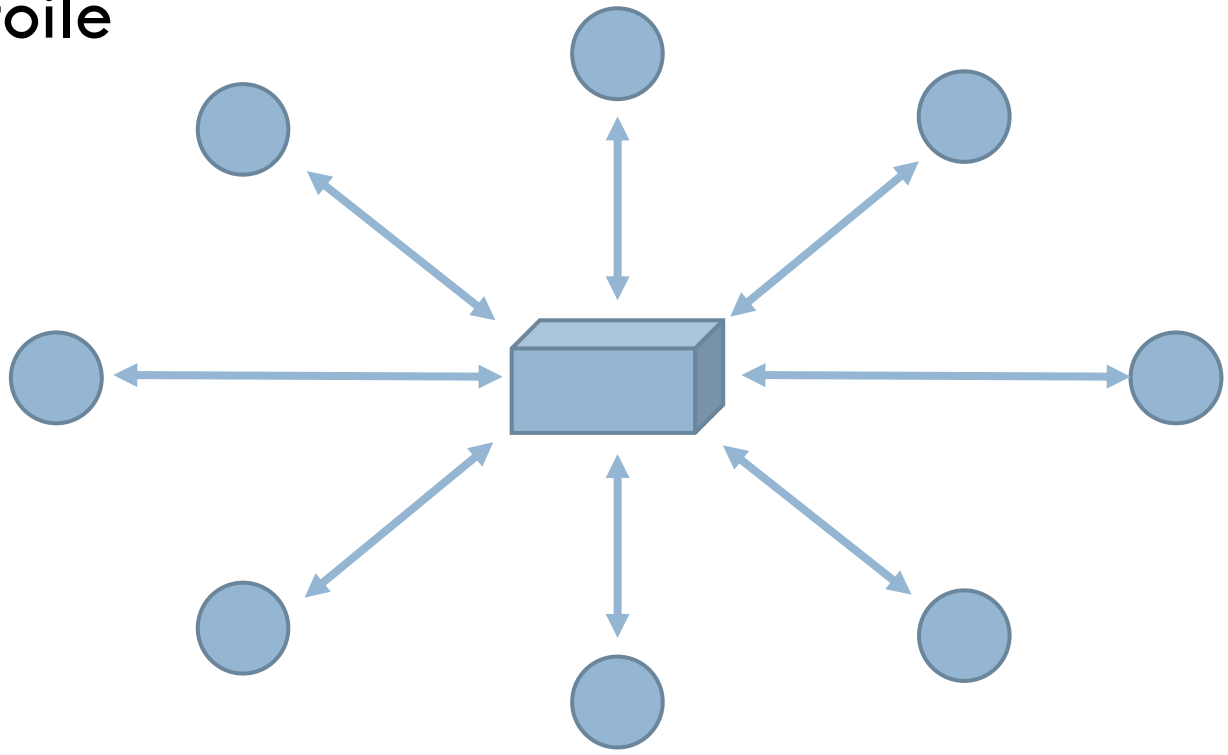
- Anneau



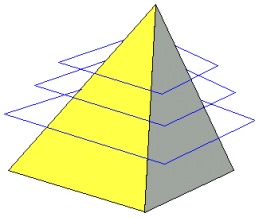
Topologies de réseaux



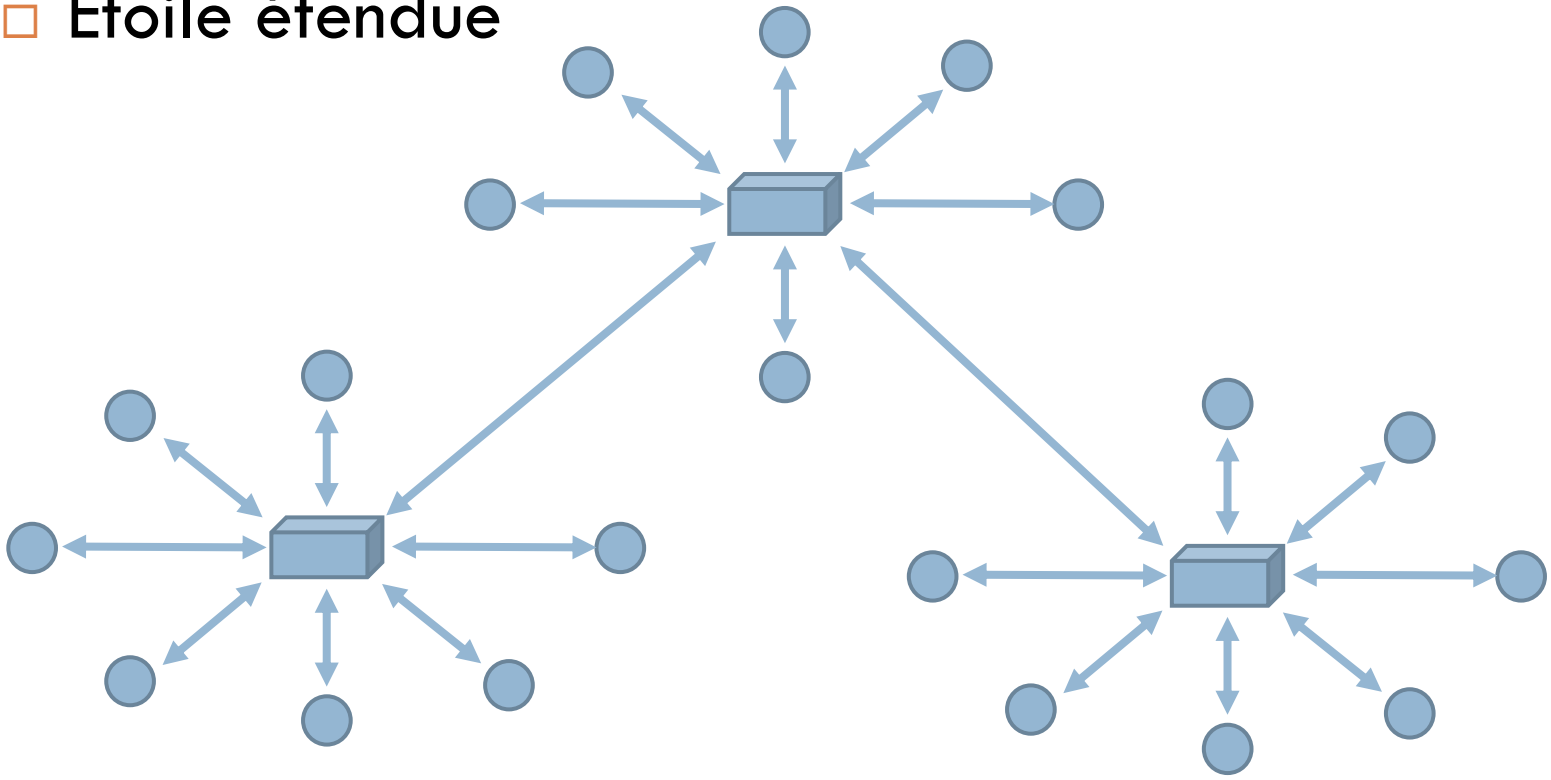
- Etoile



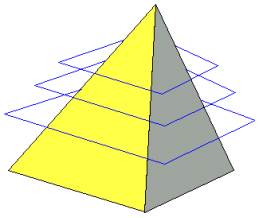
Topologies de réseaux



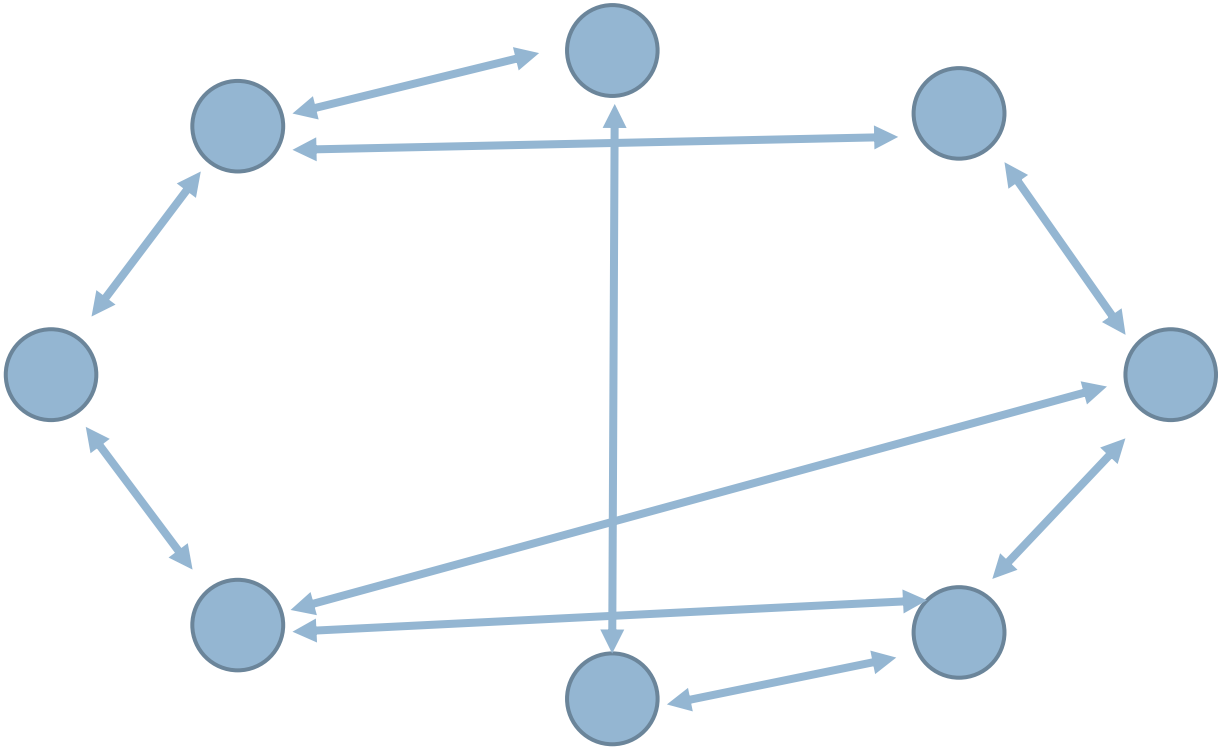
- Etoile étendue



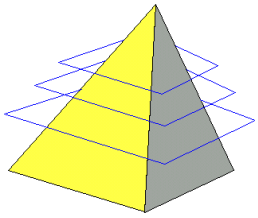
Topologies de réseaux



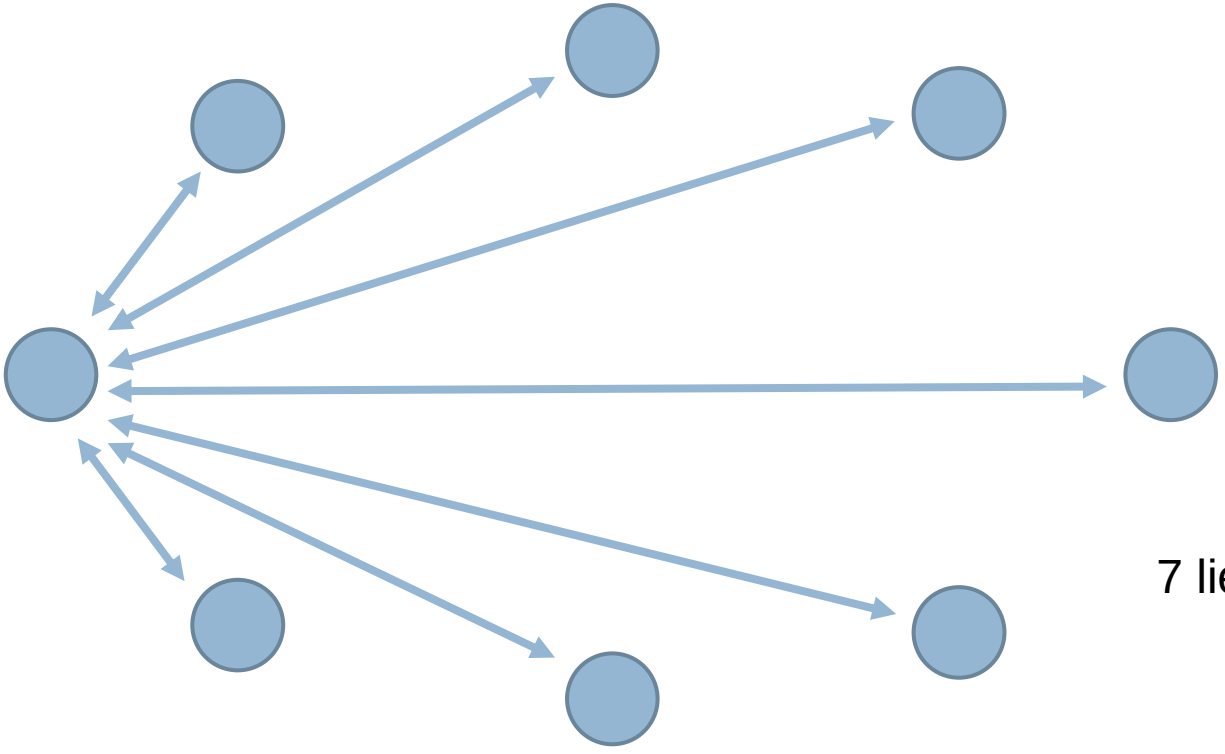
- Maillé (Partial Mesh)



Topologies de réseaux

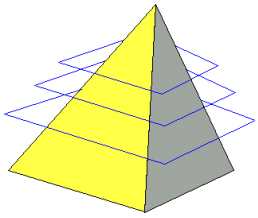


- Totalement Maillé (Full Mesh) = n (n-1) / 2

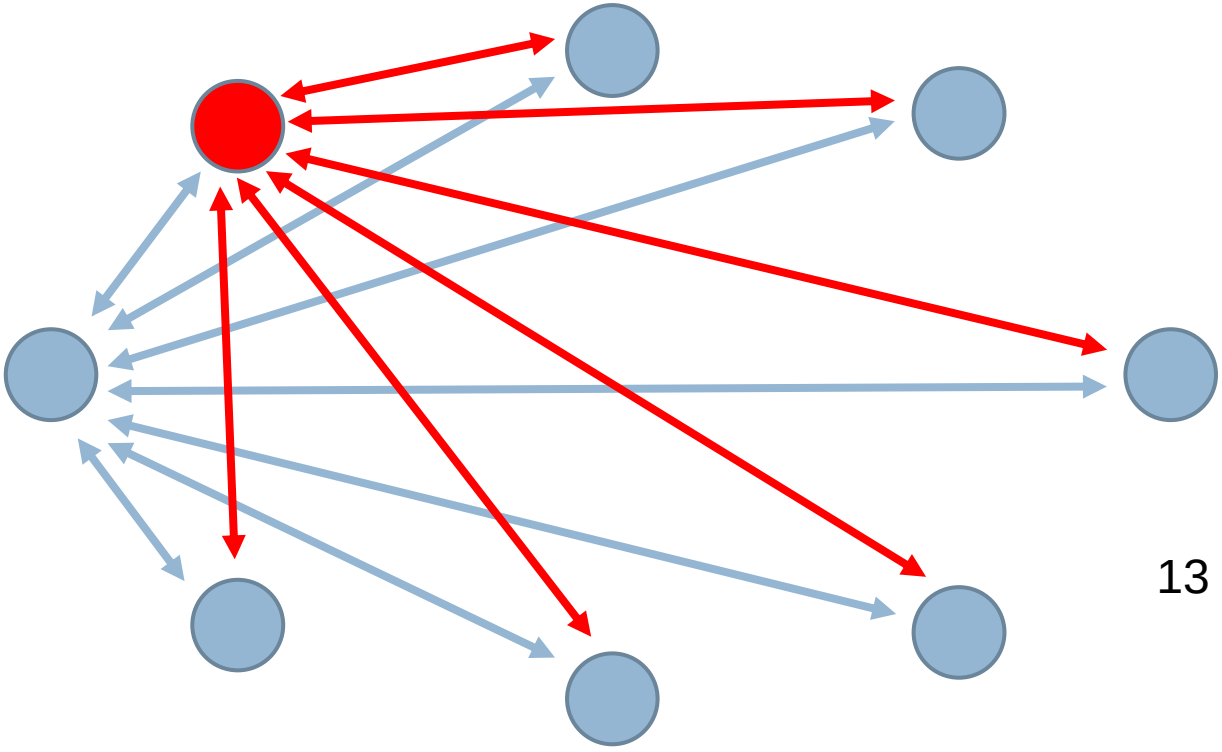


7 liens

Topologies de réseaux

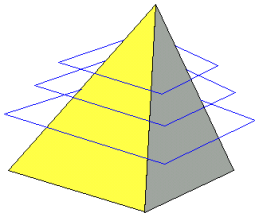


- Totalement Maillé (Full Mesh) = n (n-1) / 2

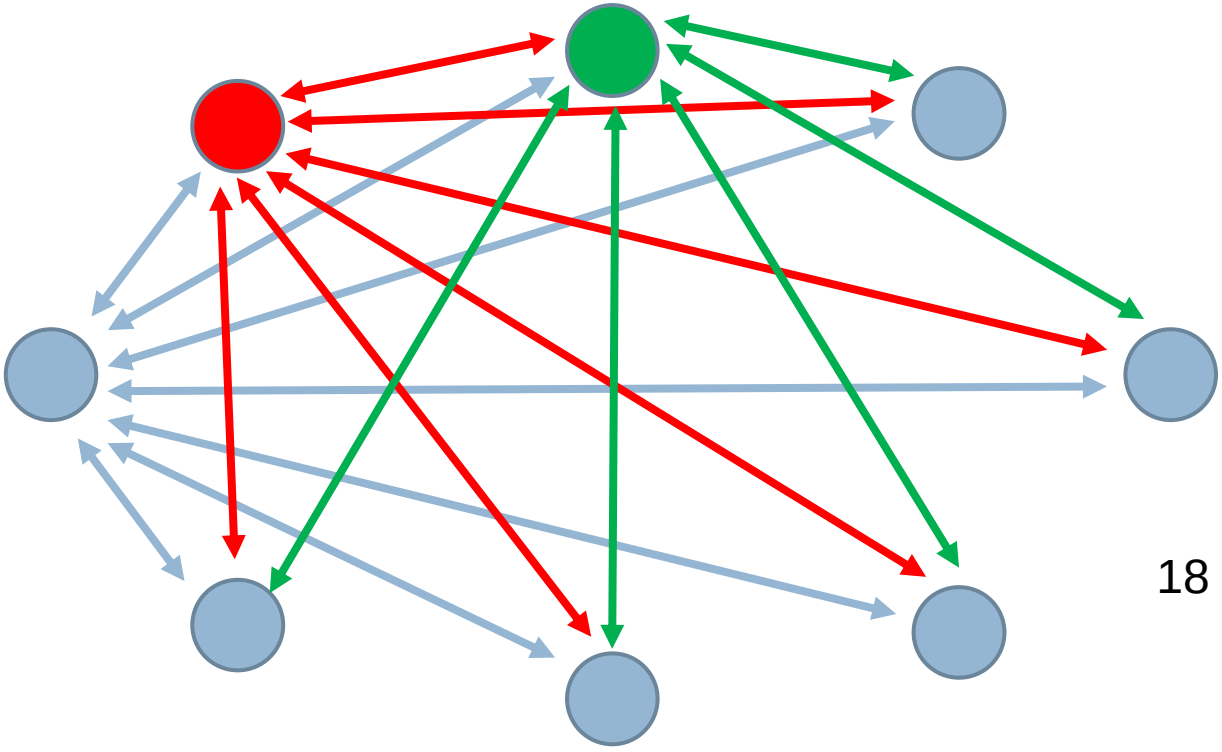


13 liens

Topologies de réseaux

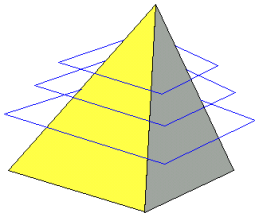


- Totalement Maillé (Full Mesh) = n (n-1) / 2

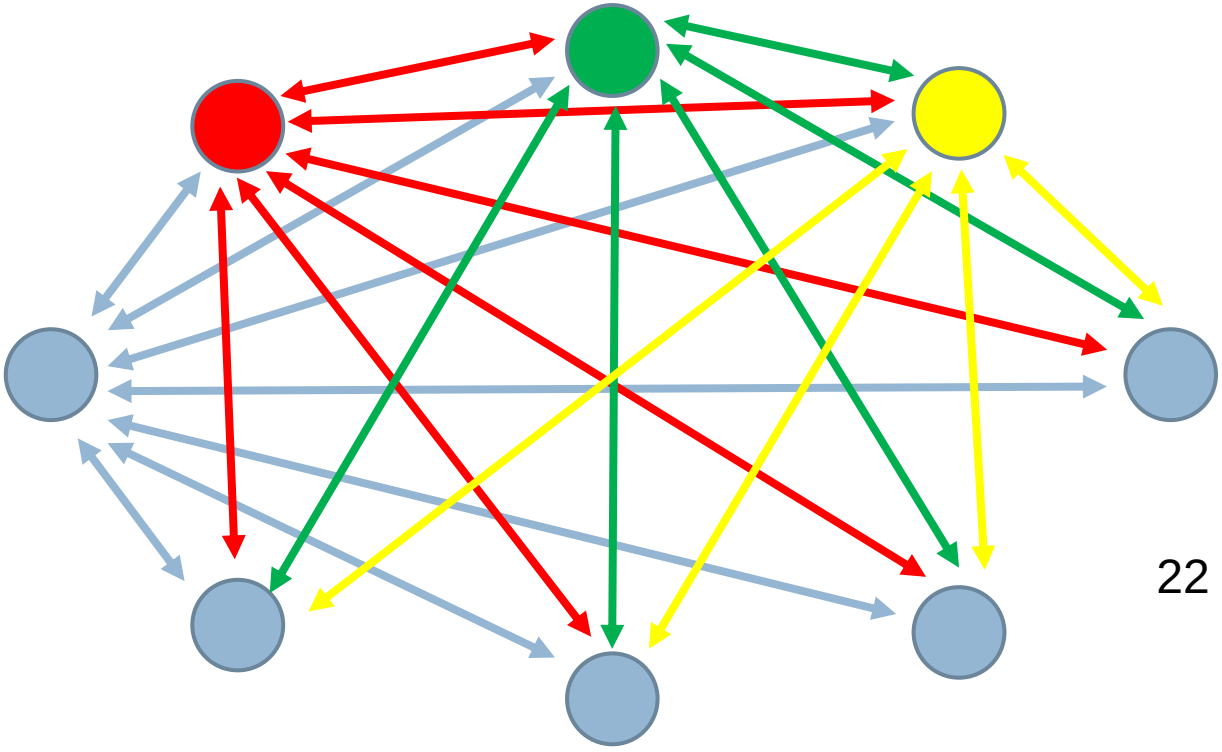


18 liens

Topologies de réseaux

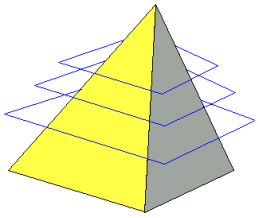


- Totalement Maillé (Full Mesh) = n (n-1) / 2

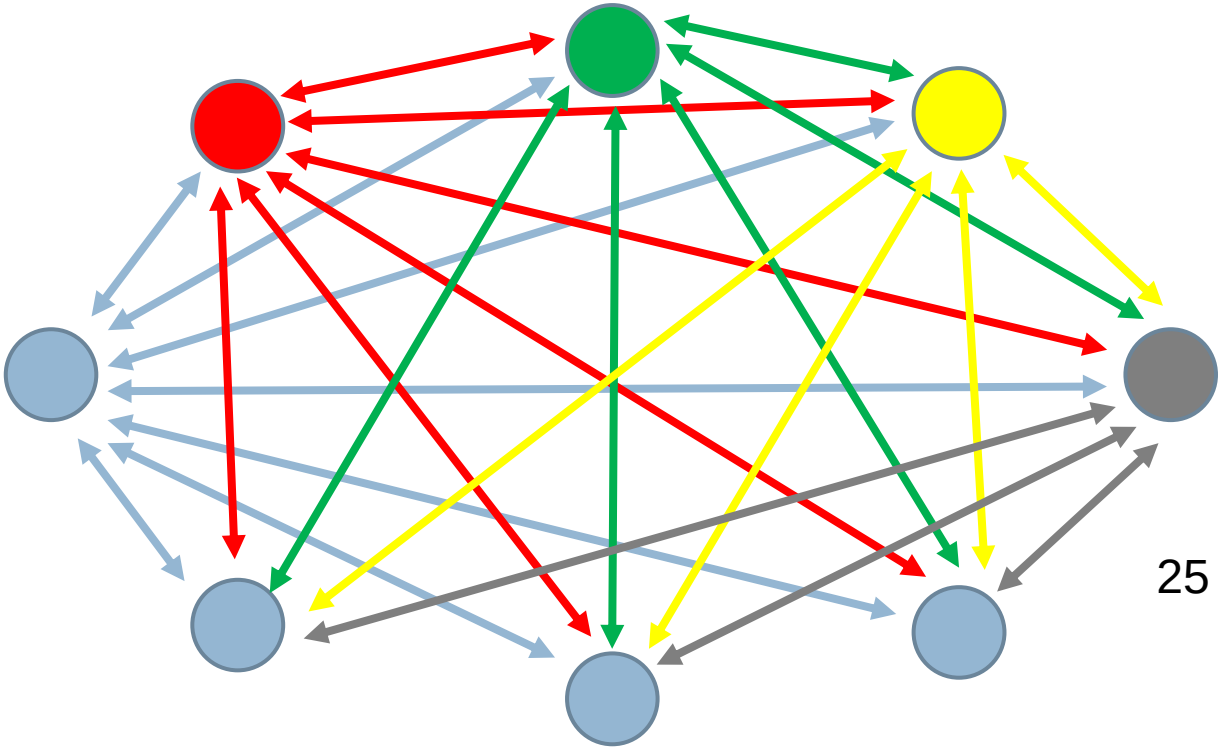


22 liens

Topologies de réseaux

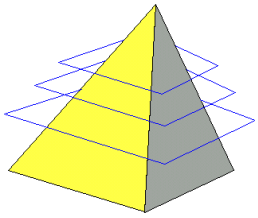


- Totalement Maillé (Full Mesh) = n (n-1) / 2

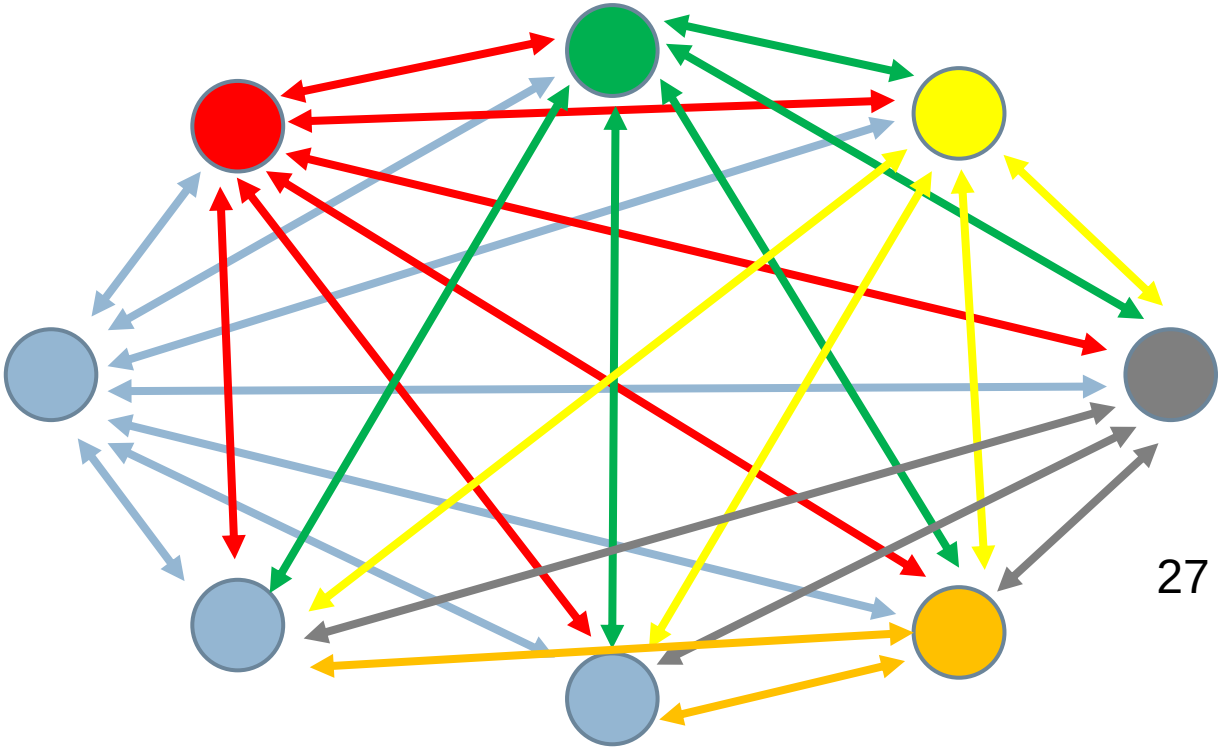


25 liens

Topologies de réseaux

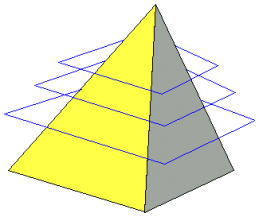


- Totalement Maillé (Full Mesh) = n (n-1) / 2

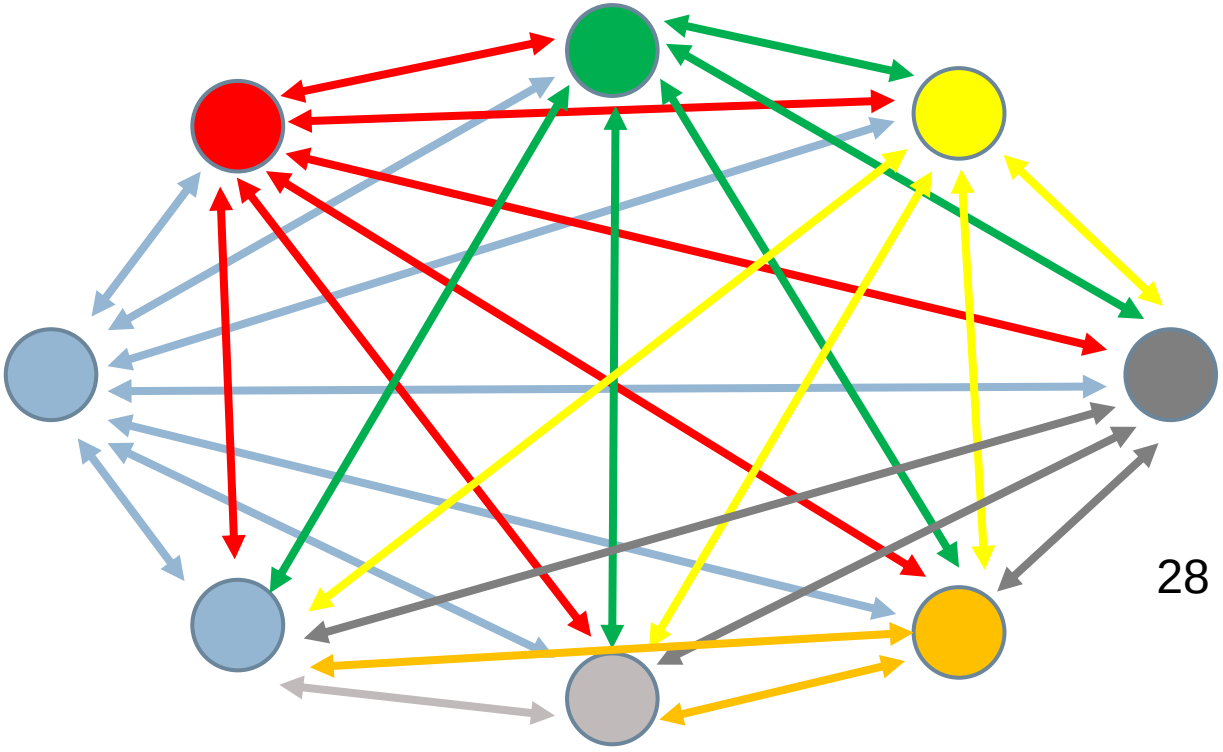


27 liens

Topologies de réseaux

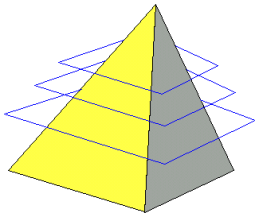


- Totalement Maillé (Full Mesh) = n (n-1) / 2

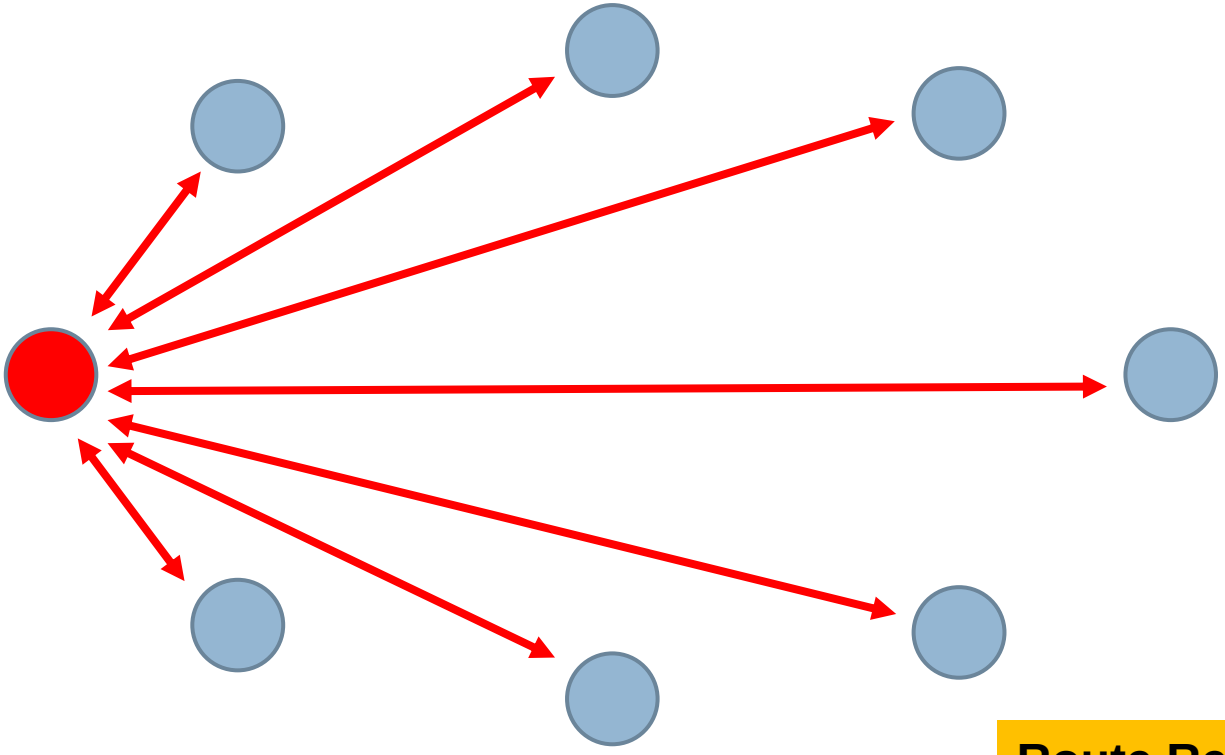


28 liens

Topologies de réseaux



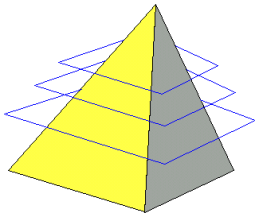
- Hub & Spoke = n-1 liens



Route Reflector (BGP)

KALYST
INGENIERIE INFORMATIQUE

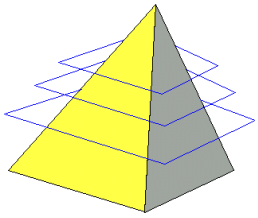
Documentation



- Topologie physique
- Topologie logique
- Architecture globale

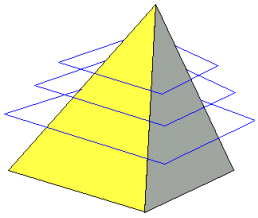
CISCO
Networking Academy

Topologie physique



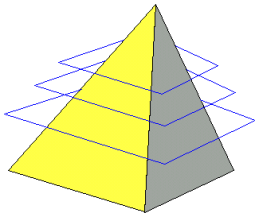
- C'est un plan détaillé du réseau
  - Les équipements (nature, type, marque…)
  - Les connexions entre les équipements (types de liens)
  - Les endroits où ils sont disposés (plan des pièces)
  - Les plans des baies
  - Les groupes de machines
  - Les serveurs
  - …

Topologie logique



- C'est un schéma du réseau en terme d'IP et de services
  - Les adresses de réseaux
  - Les routeurs et les interconnexions
  - Les VLANs
  - Les tunnels (VPN, GRE, IPSEC, MPLS)
  - Les services (DHCP, DNS, AAA, …)
  - Les équipements de sécurité
  - …

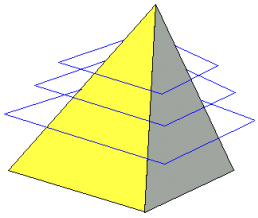
Architecture globale



- Ce sont des schémas de principe qui décrivent le réseau d'un certain point de vue ou pour un objectif particulier
- Ils regroupent essentiellement des données de la topologie logique et quelques données physiques
- Ils synthétisent souvent certaines parties de faço imagée
  - Un anneau représente un réseau commuté (MPLS)
  - Un groupe de routeurs exprime une redondance…

KALYST
INGENIERIE INFORMATIQUE

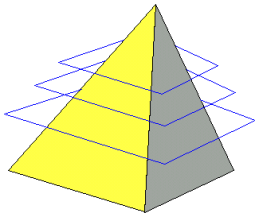
Topologies LAN



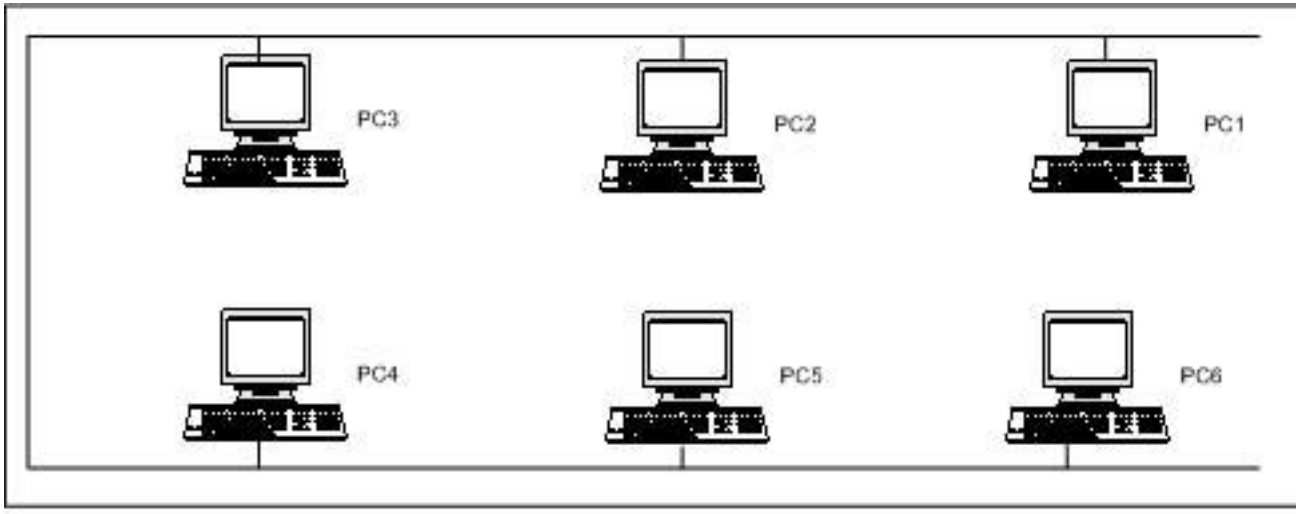
- Anneau
- Etoile
- Etoile étendue

CISCO
Networking Academy

Topologie en anneau

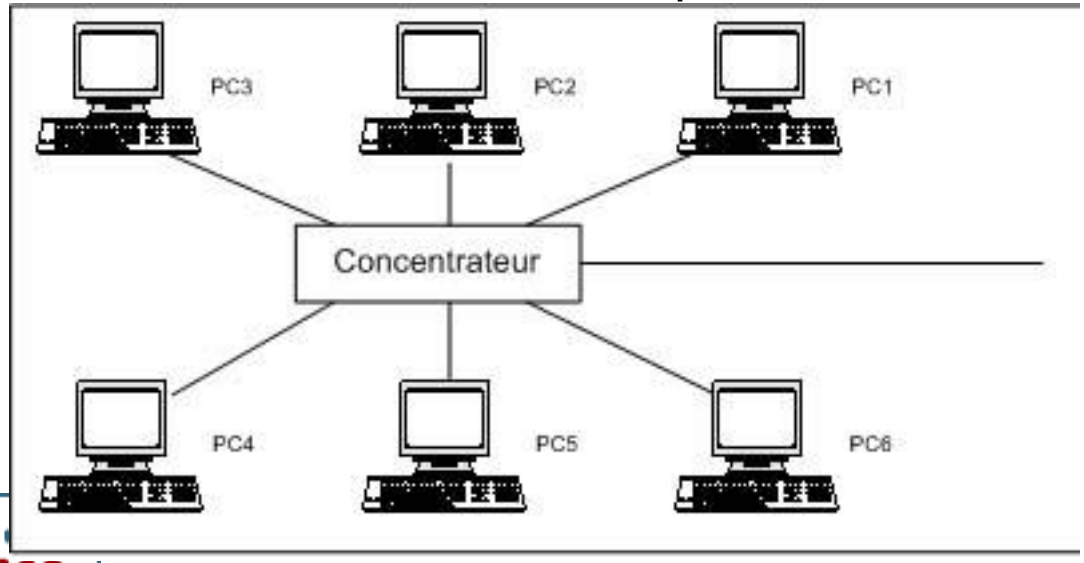


- Le signal parcoure le câble partagé en passant par PC1, PC2, … jusqu'à PC6 avant de retourner vers le reste du réseau.
- Chaque host est connecté au câble par un connecteur en T qui assure l'accès du host au média ET la continuité des signaux qui traversent le câble.
- Point de défaillance unique : câble coupé ou connecteur en T.

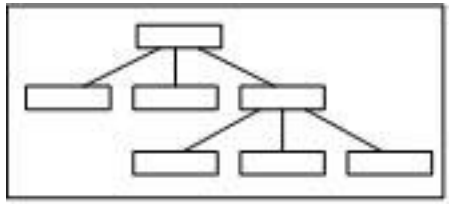


Topologie en étoile

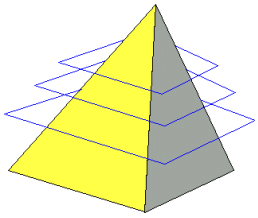
- Chaque host est connecté à un appareil qui concentre la connectivité du réseau.
- Ce concentrateur permet aux hosts de partager le média.
- Une coupure de lien ou une défaillance d'un connecteur n'affecte plus qu'un seul host.
- Point de défaillance unique : le concentrateur !



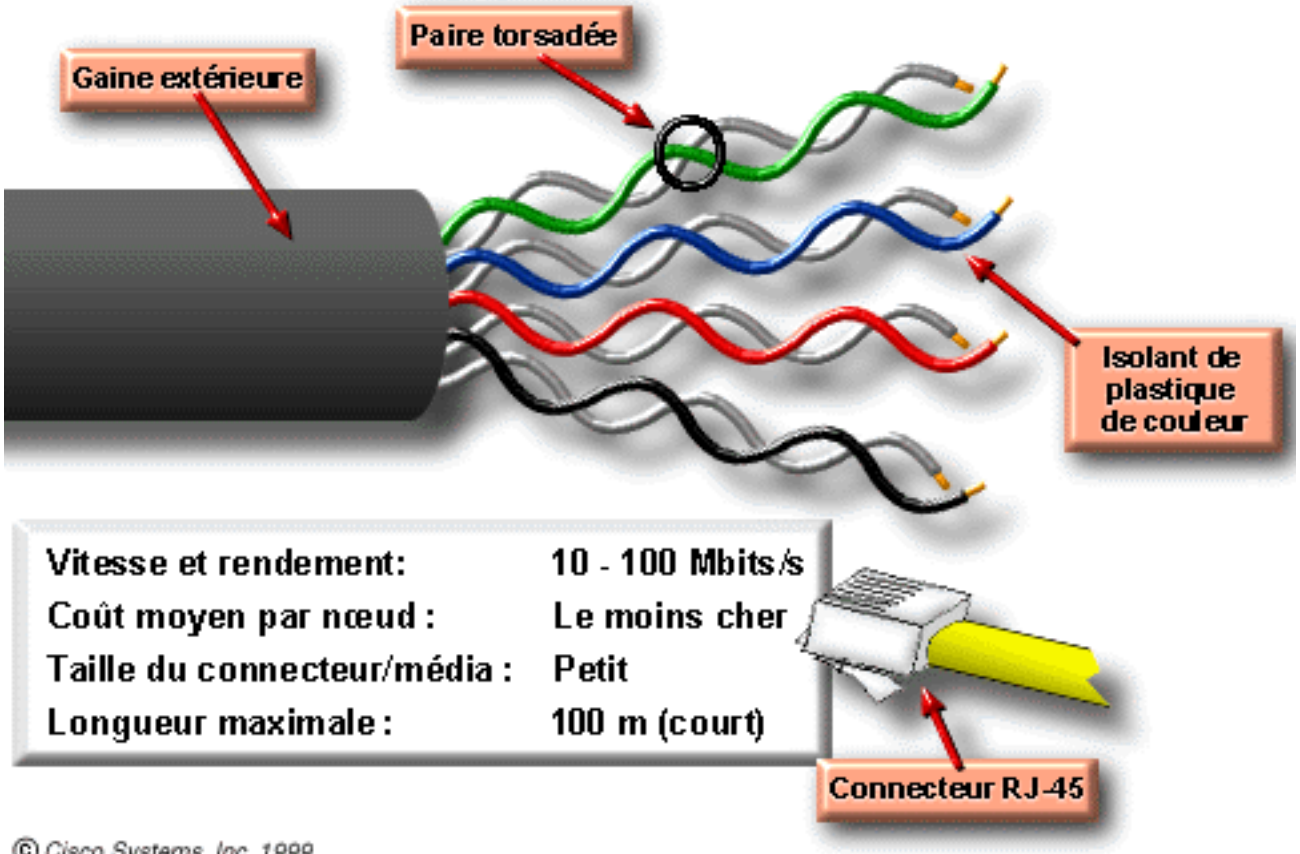
Une topologie en étoile étendue est composée d'étoiles reliées entre elles.



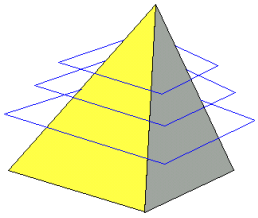
Les types de média - 1/3



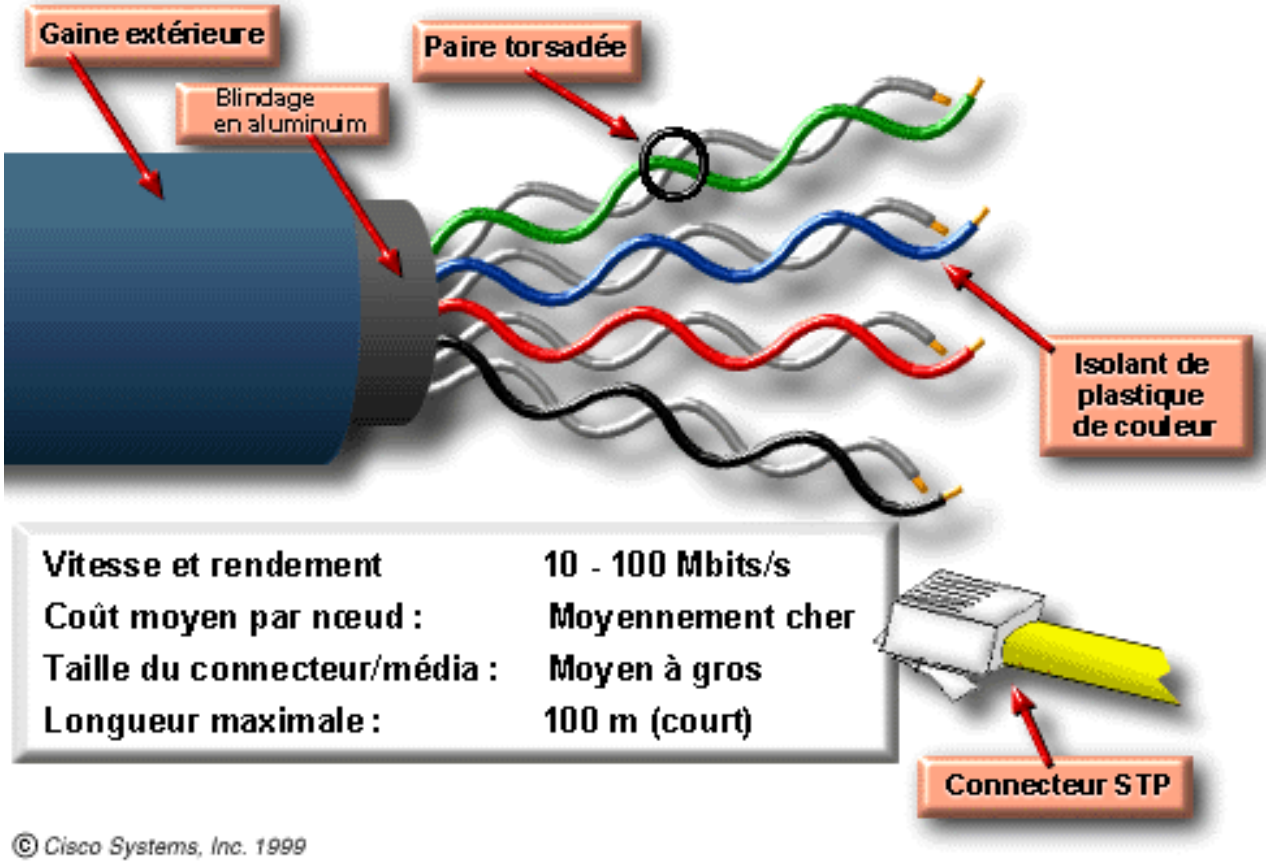
Paire torsadée non blindée (UTP)



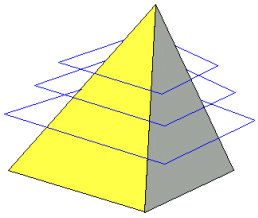
Les types de média - 2/3



Paire torsadée blindée (STP)

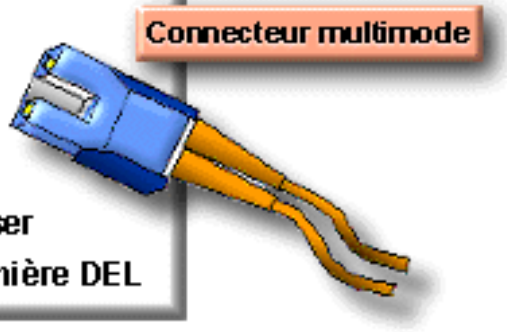


Les types de média - 3/3



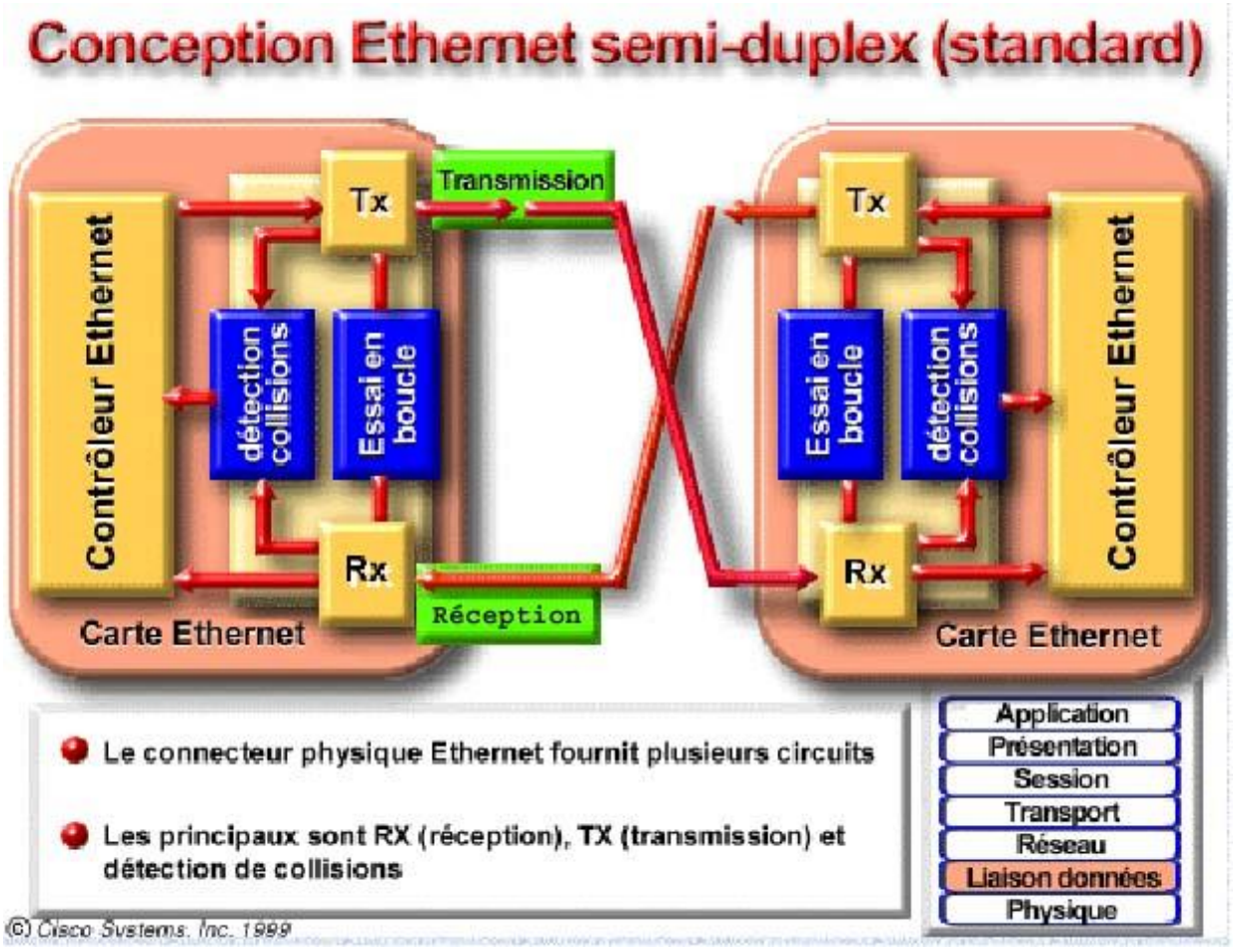
Câble à fibre optique

Vitesse et rendement:	100+ Mbits/s
Coût moyen par nœud :	Le plus cher
Taille du connecteur/média :	Petit
Longueur maximale :	jusqu'à 2 km
Monomode :	Un faisceau de lumière laser
Multimode :	Plusieurs faisceaux de lumière DEL

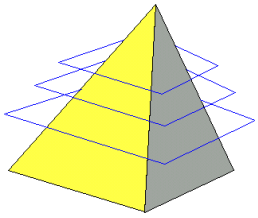


Structure d'une carte NIC

- Les ports des Hubs et des Switchs croisent les circuits.
- Un câble droit relie les hosts à ces matériels.
- Pour relier deux hosts entre eux il faut un câble croisé.



Ethernet / Token Ring (digression)



Ethernet a été développé à l'origine par Xerox (1970), puis a été intégré aux travaux de l'OSI. La méthode d'accès au média (CSMA/CD) est définie dans la sous-couche MAC de OSI 2. Token Ring est une technologie déterministe arrivée trop tard sur le marché.

Ethernet est non déterministe
Token Ring est déterministe

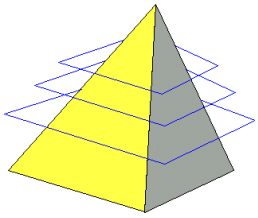
Ethernet est simple
Token Ring est plus complexe

ALOHA !!!
a préfiguré
Ethernet

Le succès d'Ethernet le fait évoluer vers une technologie plus simple, plus rapide et déterministe !

L'évolution de Token Ring a conduit à une complexité de moins en moins gérable.

Trame Ethernet



Structures de trame Ethernet et IEEE 802.3

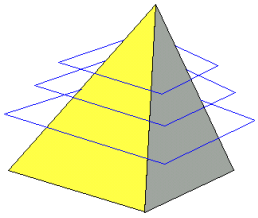
Ethernet

Longueur des champs, en octets						
?	1	6	6	2	46-1500	4
Préambule	Délimiteur de début de trame	Adresse de destination	Adresse source	Type	Données	Séquence de contrôle de trame

IEEE 802.3

?	1	6	6	2	46-1500	4
Préambule	Délimiteur de début de trame	Adresse de destination	Adresse source	Longueur	En-tête 802.2 et données	Séquence de contrôle de trame

COUCHE 2 : Liaison de Données



- **Couche MAC (Media Access Control)**

  La Méthode d'Accès : CSMA / CD vient de l'algorithme radiophonique Aloha, elle est non déterministe.

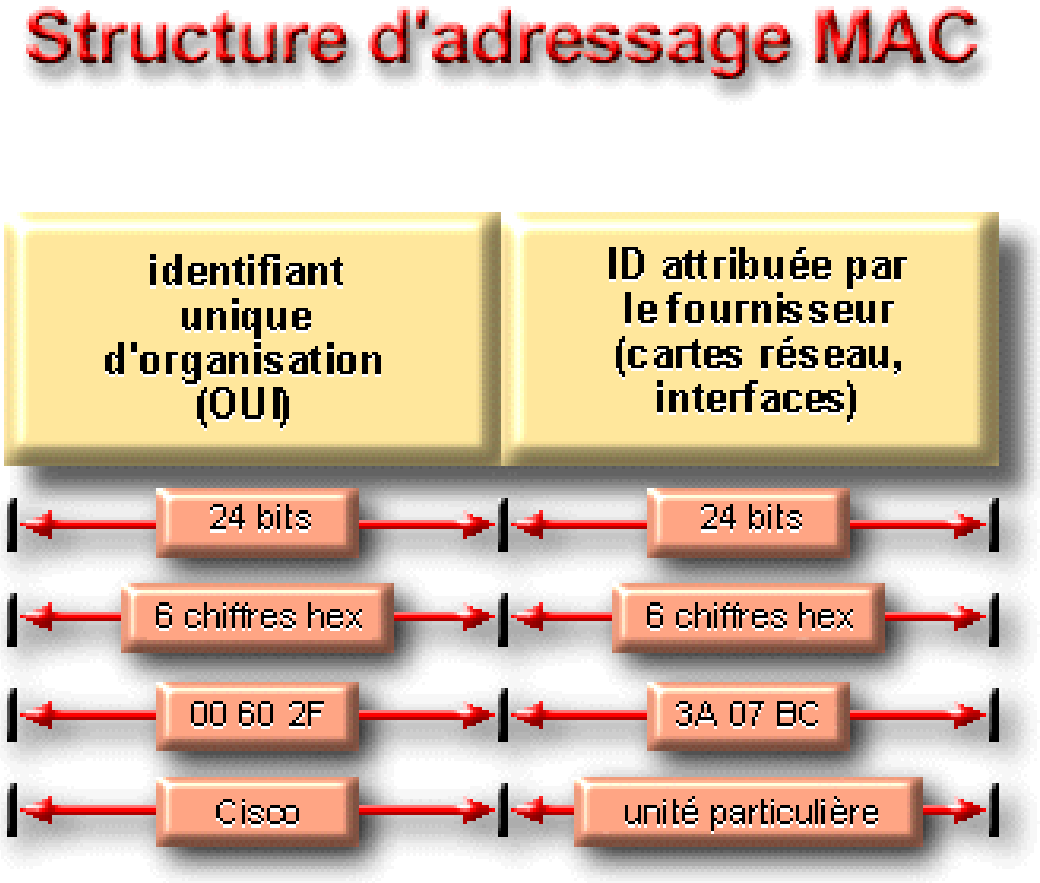
  La méthode d'accès d'un Toking Ring est déterministe.

- **Couche LLC (Type et utilisation)**

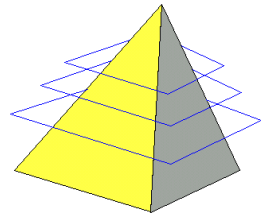
Type 1 :	sans connexion ni acquittement
Tous	point à point ou multipoint
Type 2 :	connexion, acquittement, contrôle de
NetBios	flux, ordonnancement des trames …
SNA	point à point uniquement
Type 3 :	service sans connexion, acquitté …
	Qualité du service intermédiaire

Adressage Physique (MAC)

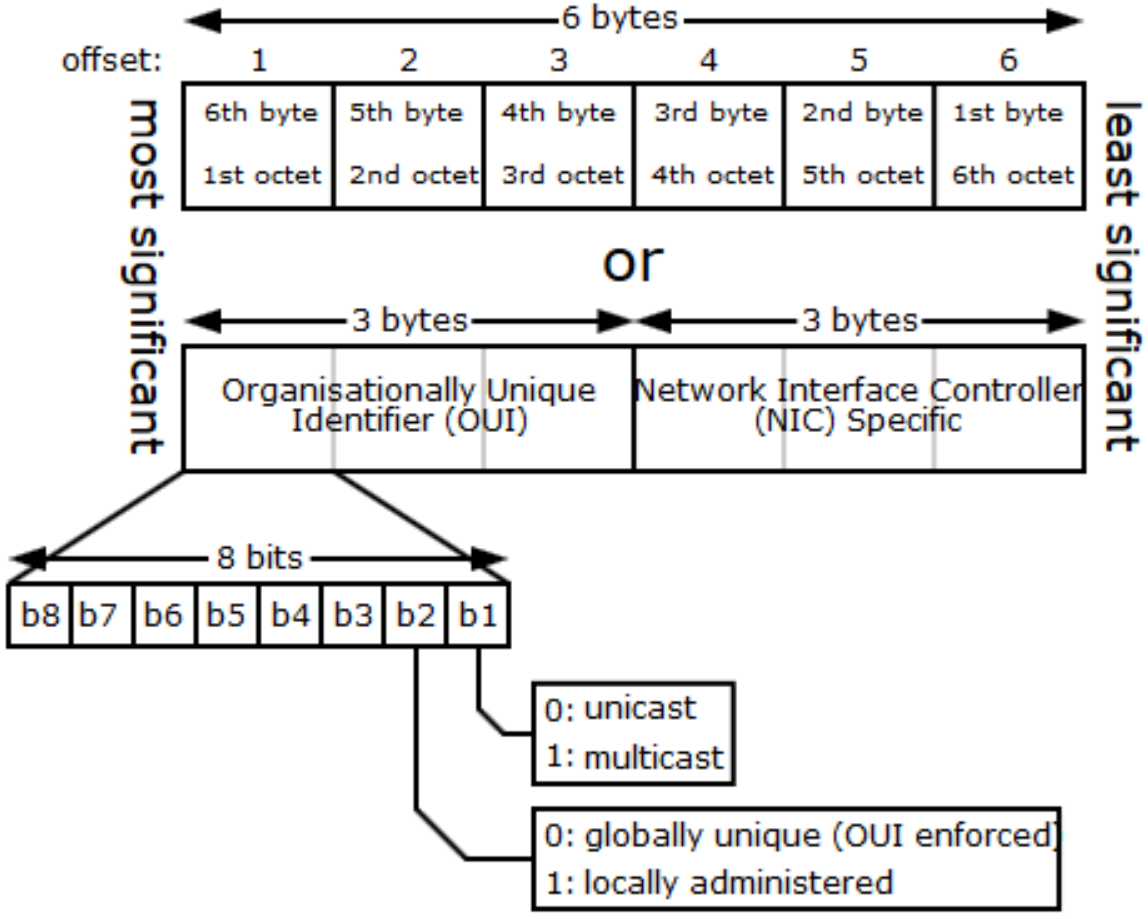
- Bit 0
  - Diffusion
- Bit 1
  - Local
- Bits 2-23
  - N° constructeur



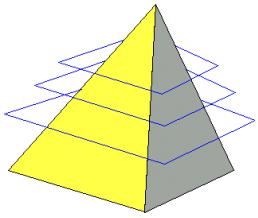
Adressage Physique (MAC)



- Bit 0
  - Diffusion
- Bit 1
  - Local
- Bits 2-23
  - N° constructeur



Adresses Multicast de couche 2

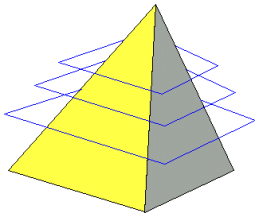


- Multicast MAC : recouvrement possible sur 5 bits
  - Adresses IP : 224.0.0.1 à 239.255.255.254
  - Les adresses 224.128.5.5 et 239.0.5.5 vont être associées aux mêmes adresses MAC

01	00	5E	0	23 derniers bits : 224.128.5.5		
00000001	00000000	01011110	0	0000000	00000101	00000101

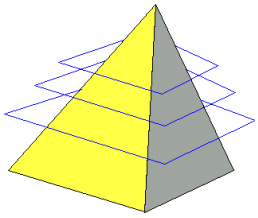
01	00	5E	0	23 derniers bits : 239.0.5.5		
00000001	00000000	01011110	0	0000000	00000101	00000101

Adressage de niveau 2



- Les adresses MAC permettent aux hosts d'un même segment de communiquer entre eux
- Les machines de niveau 3 ou supérieur maintiennent des « Tables ARP »
- Le protocole Address Resolution Protocol permet de connaître l'adresse MAC d'un host à partir de son adresse IP
- Si cette adresse est inconnue la machine émettrice génère un broadcast ARP
- Le protocole RARP permet de retrouver l'adresse IP d'un host à partir de son adresse MAC

Address Resolution Protocol



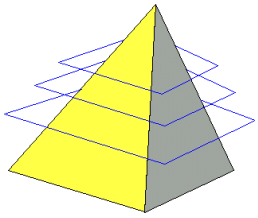
EN-TÊTE MAC	EN-TÊTE IP	MESSAGE DE REQUÊTE ARP
Destination FF-FF-FF-FF-FF-FF Source 02-60-8C-01-02-03	Destination 197.15.22.126 Source 197.15.22.33	Quelle est ton adresse MAC?

STRUCTURE D'UNE REQUÊTE ARP

EN-TÊTE MAC	EN-TÊTE IP	MESSAGE DE REQUÊTE ARP
Destination 02-60-8C-01-02-03 Source 08-00-02-89-90-80	Destination 197.15.22.33 Source 197.15.22.126	Voici mon adresse MAC.

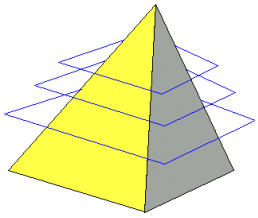
STRUCTURE DE RÉPONSE ARP

Algorithme d'émission



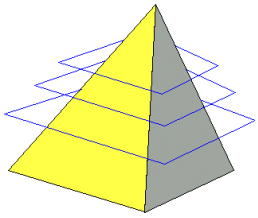
- Le destinataire est-il dans mon réseau IP ?
- Oui
  - Son adresse MAC est-elle dans ma table ARP ?
  - Oui
    - Emission de la trame vers le destinataire
  - Non
    - Emission d'un broadcast ARP pour connaître sa MAC
- Non
  - Emission d'une trame vers ma passerelle. Le paquet IP pour mon destinataire est encapsulé dans cette trame.

Pont / Commutateur



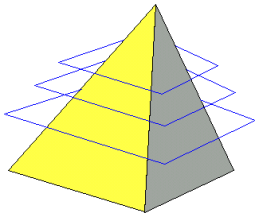
- Un pont est un matériel de couche 2 capable de désencapsuler les trames arrivantes, lire les informations de couches 2 qu'elles contiennent, puis réencapsuler en couche 2 avant de renvoyer les trames sur un port de sortie.
- Un pont peut donc, par exemple, lire des trames Ethernet et renvoyer des trames Token Ring. Il réalise ainsi une fonction d'interface entre des technologies réseaux différentes.
- Un commutateur ou switch est un pont multi ports.
- Les commutateurs Ethernet sont spécialisés dans cette technologie et proposent de nombreuses évolutions.

Commutateur / Switch



- Un commutateur concentre la connectivité et régénère le signal.
- Il permet de « segmenter » le réseau. Chaque port du commutateur est un domaine de collision distinct.
- Il peut fonctionner en modes :
- Cut through : sitôt que l'adresse MAC de destination est lue, la trame est commutée vers le bon port.
- Fragment free : identique au mode précédent, mais le commutateur lit les 64 premiers octets de la trame avant de la commuter. Les trames percutées (les fragments) sont éliminées, ce qui limite le trafic inutile.
- Store and Forward : chaque trame est entièrement mise en mémoire avant d'être commutée. Ce mode autorise des vitesses asymétriques sur les différents ports du switch et permet d'appliquer des stratégies de sécurité.

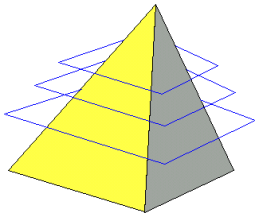
Commutateur / Switch



- Le niveau de prix des switchs dépend de leurs fonctionnalités et du nombre de piles mémoires qui sont gérées (une pile commune, une pile par port, plusieurs piles par port avec gestion des priorités …).
- Les « hosts » connectés directement à un switch peuvent fonctionner en mode Full Duplex (le domaine de collision est réduit au host). Celui-ci peut donc émettre et recevoir en même temps sans avoir besoin d'obéir à la méthode d'accès CSMA/CD.
- Pour connecter un HUB à un swtich ou deux switchs entre eux il faut utiliser un câble croisé.
- Certains switchs disposent d'un (ou plusieurs) ports montants (UpLink), qui peuvent être liés par un câble droit.
- Certains switchs permettent de définir des ports agrégés, c'est-à-dire associés en un seul lien logique, dont la capacité de transmission est la somme des capacité de chaque port (Trunk link).

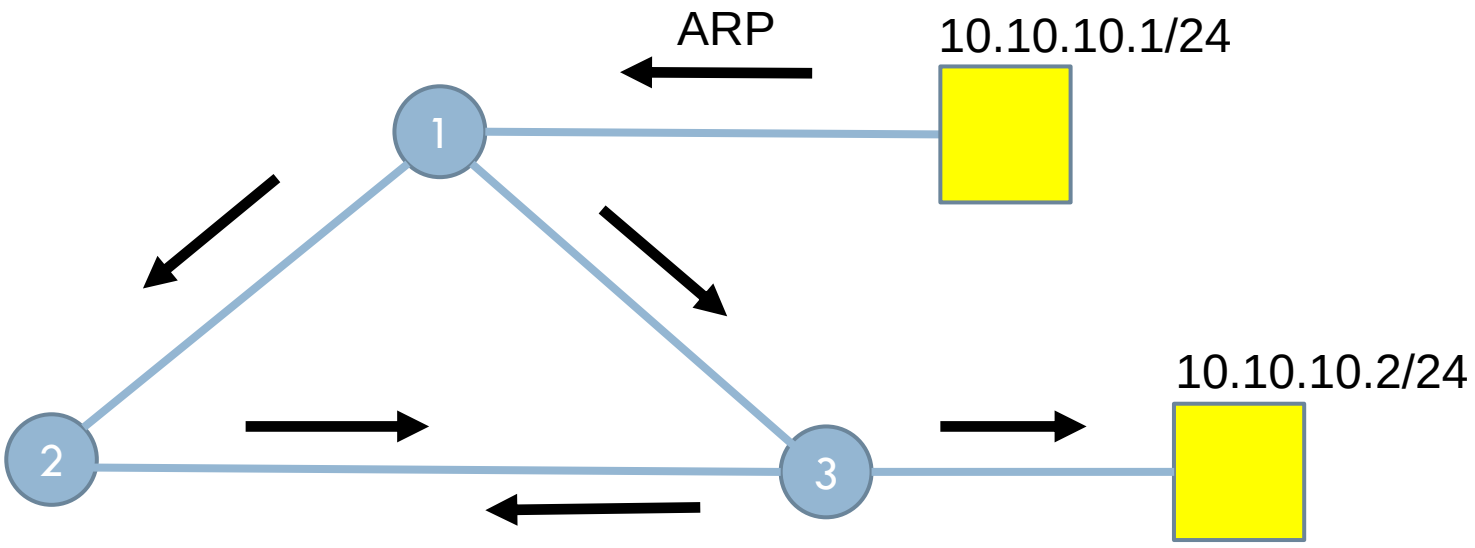
KALYST
INGENIERIE INFORMATIQUE

Spanning tree protocol

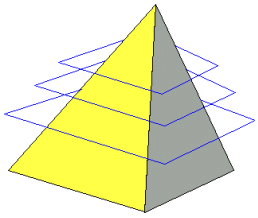


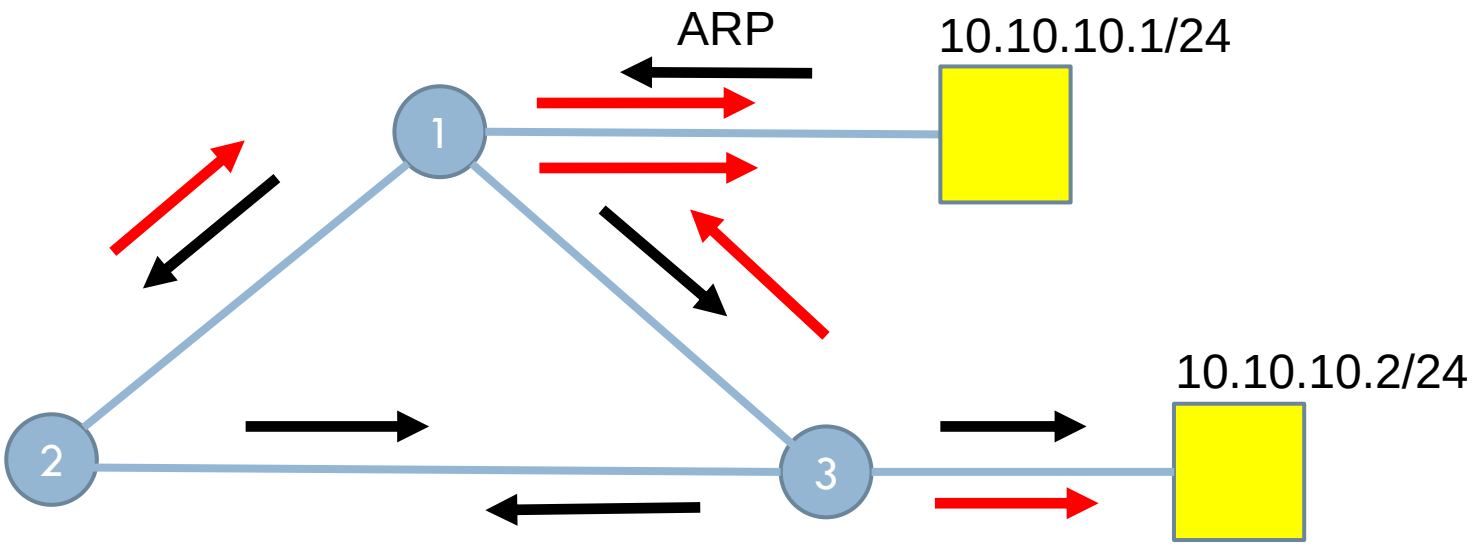
- Protocole qui vérifie l'absence de boucles de couche 2 => tempêtes de broadcast
- Un commutateur est élu « Root Bridge »
- Les liens vers le root sont des « root port »
- Les liens qui mènent au root sont des « designed port »
- Les autres sont « bloqués »
- Pendant le calcul le led est orange, puis passe au vert au bout d'environ 60 secondes
- Spaning tree peut être désactivé, mais attention !!!

Broadcast storm

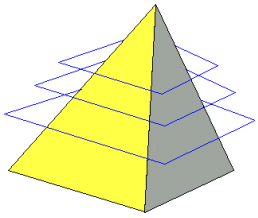


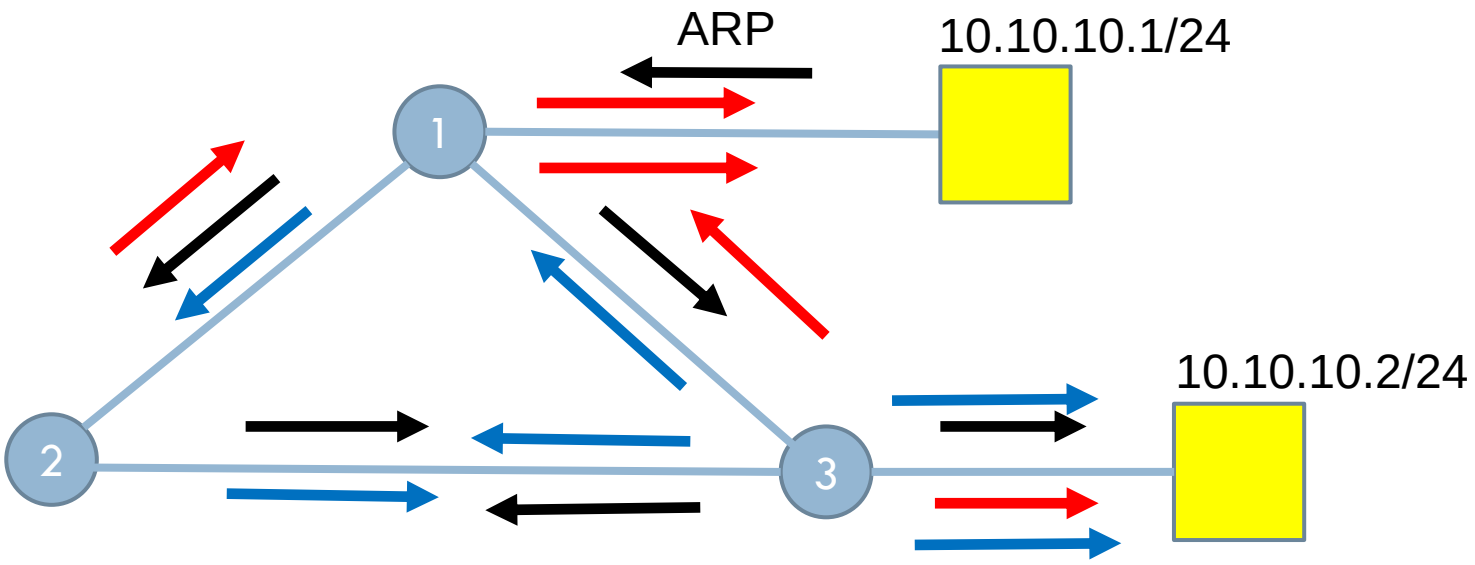
Broadcast storm



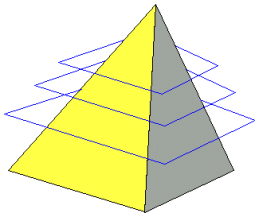


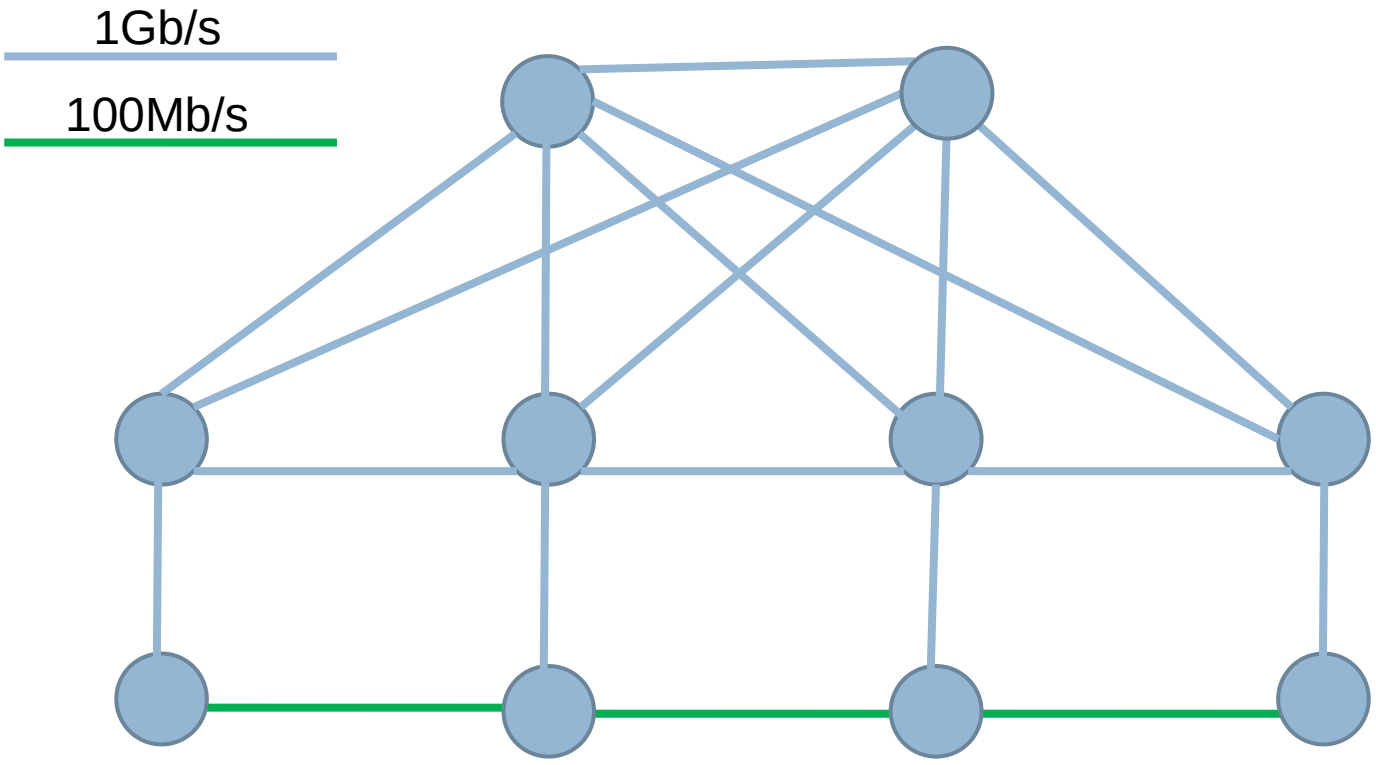
Broadcast storm



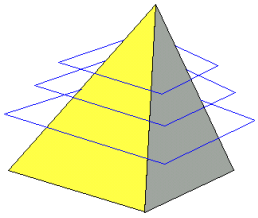


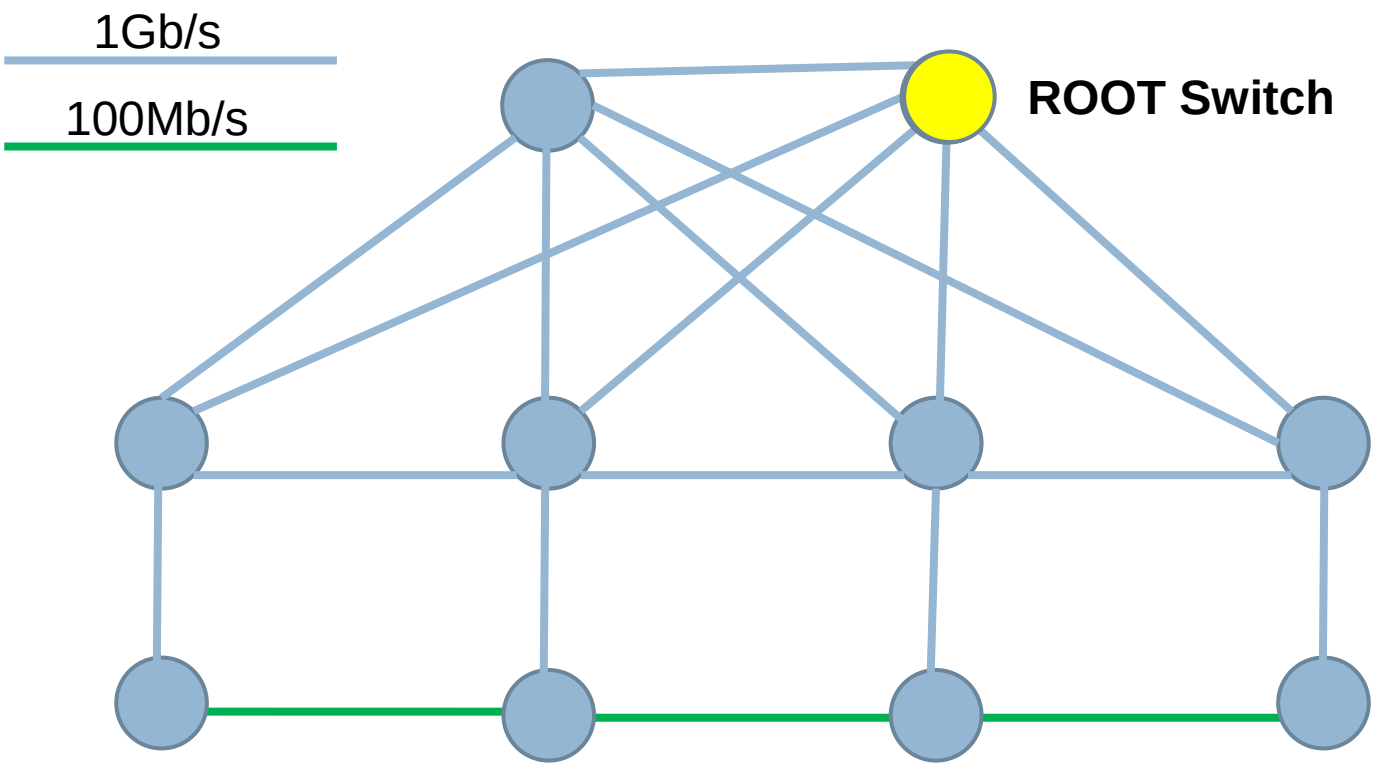
Spanning Tree Protocol



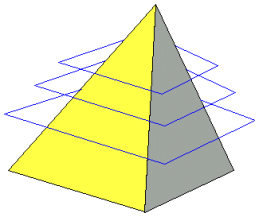


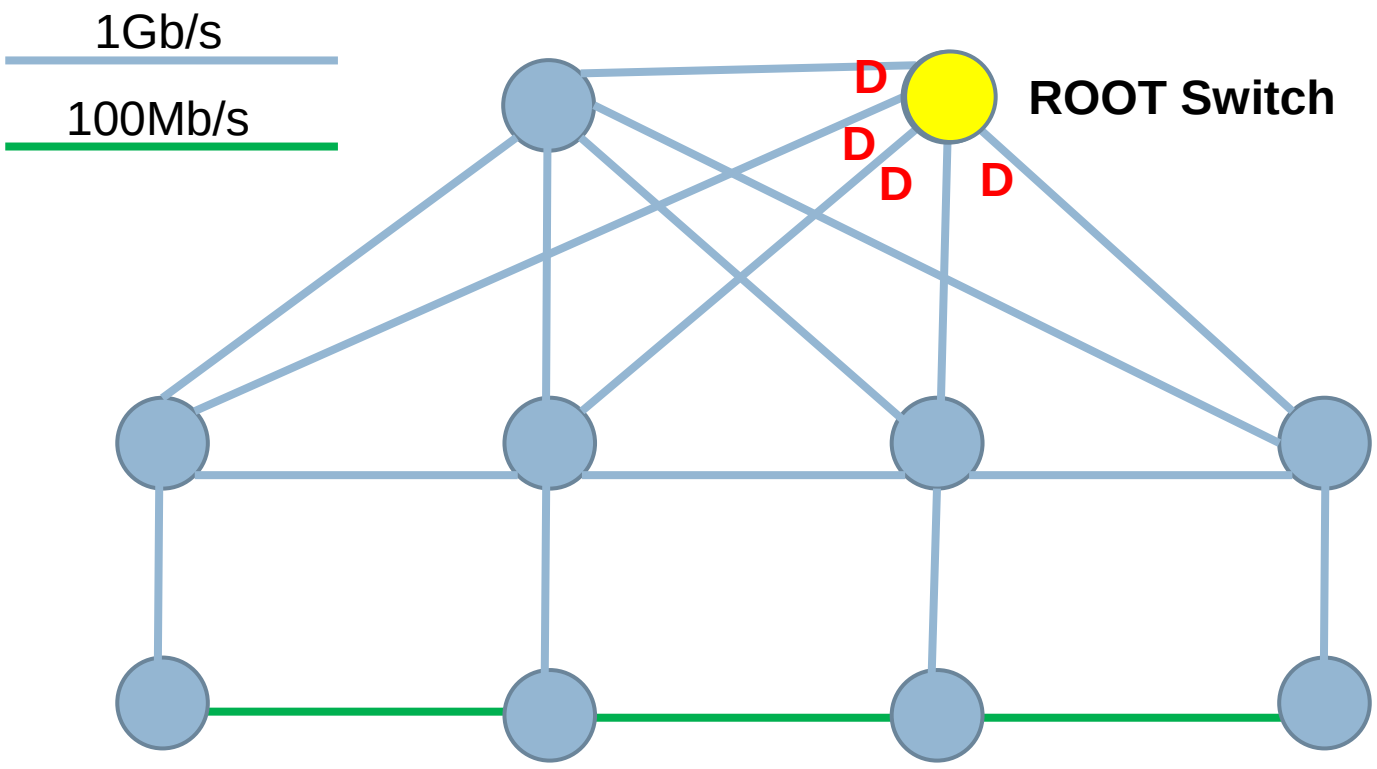
Spanning Tree Protocol



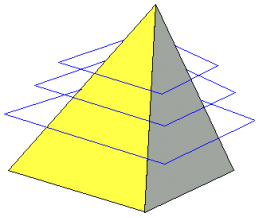


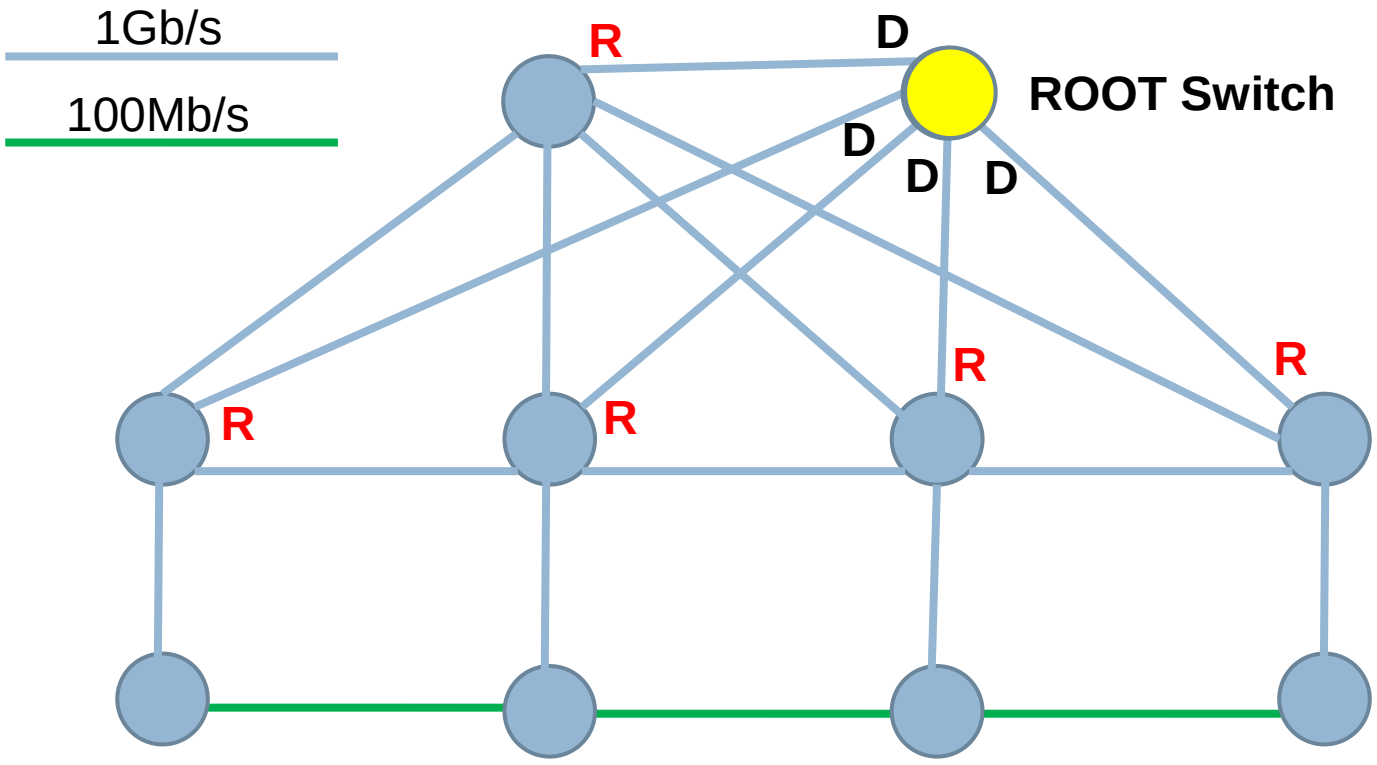
Spanning Tree Protocol





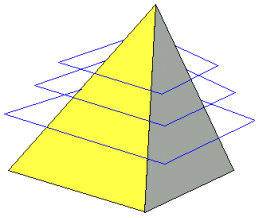
Spanning Tree Protocol

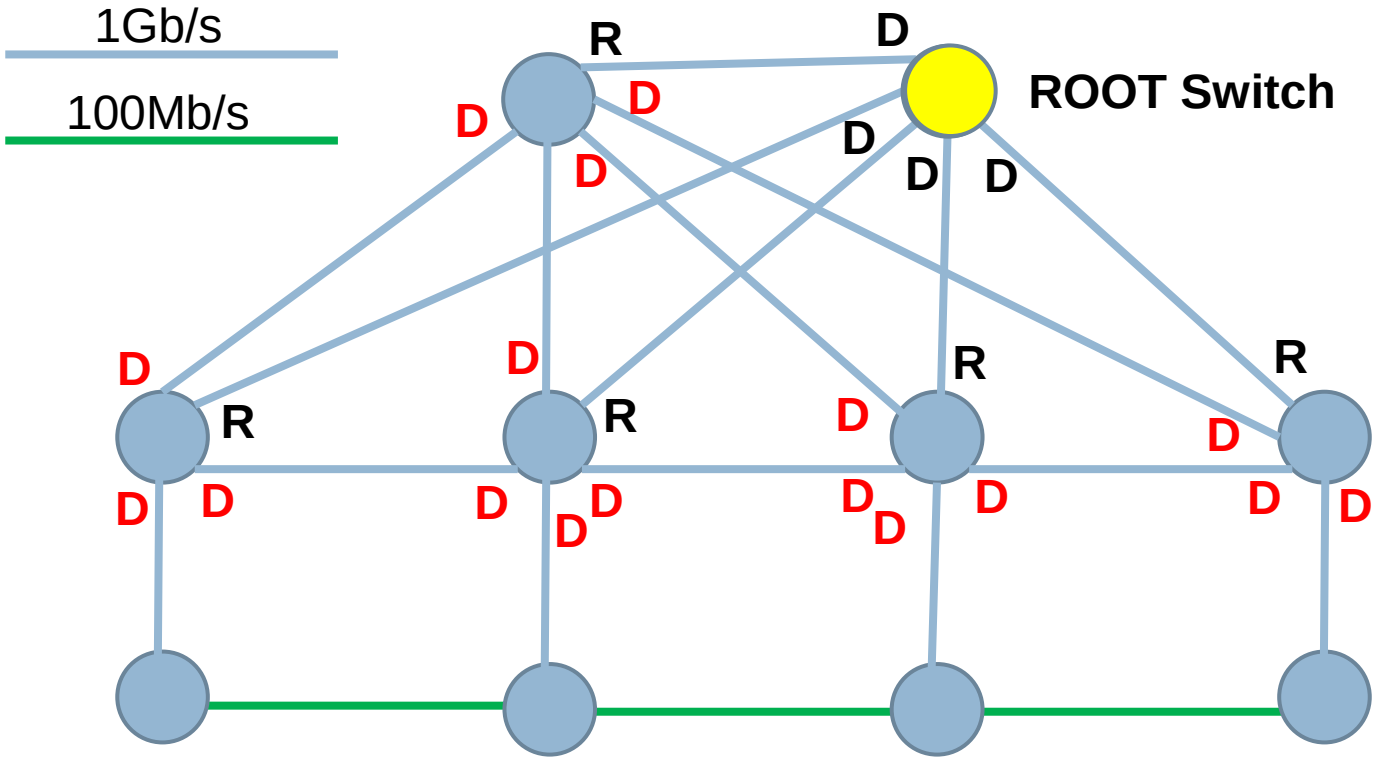




KALYST
INGENIERIE INFORMATIQUE

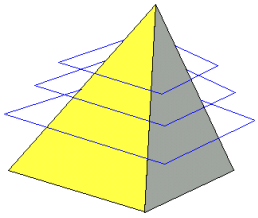
Spanning Tree Protocol

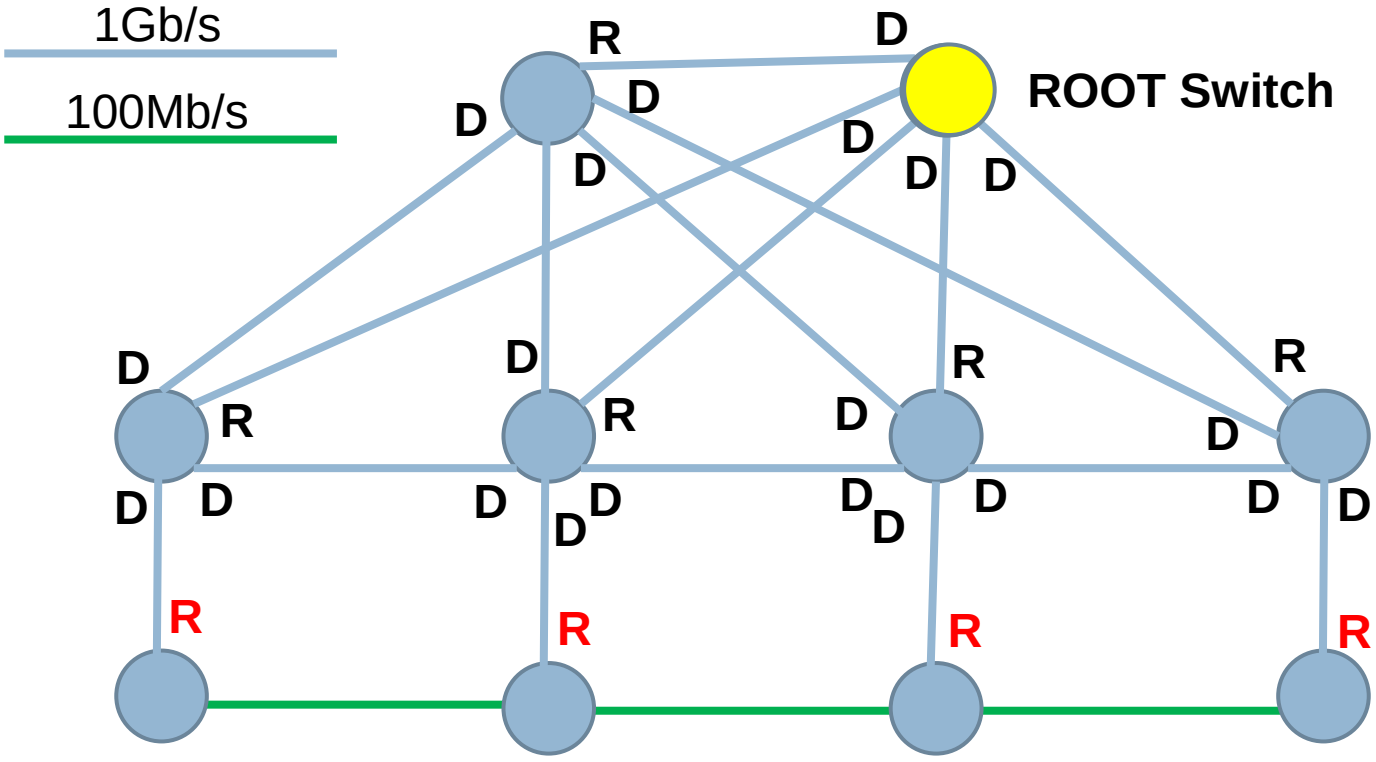




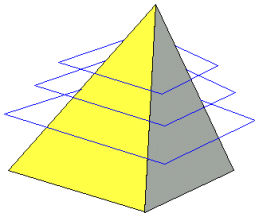
CISCO
Networking Academy

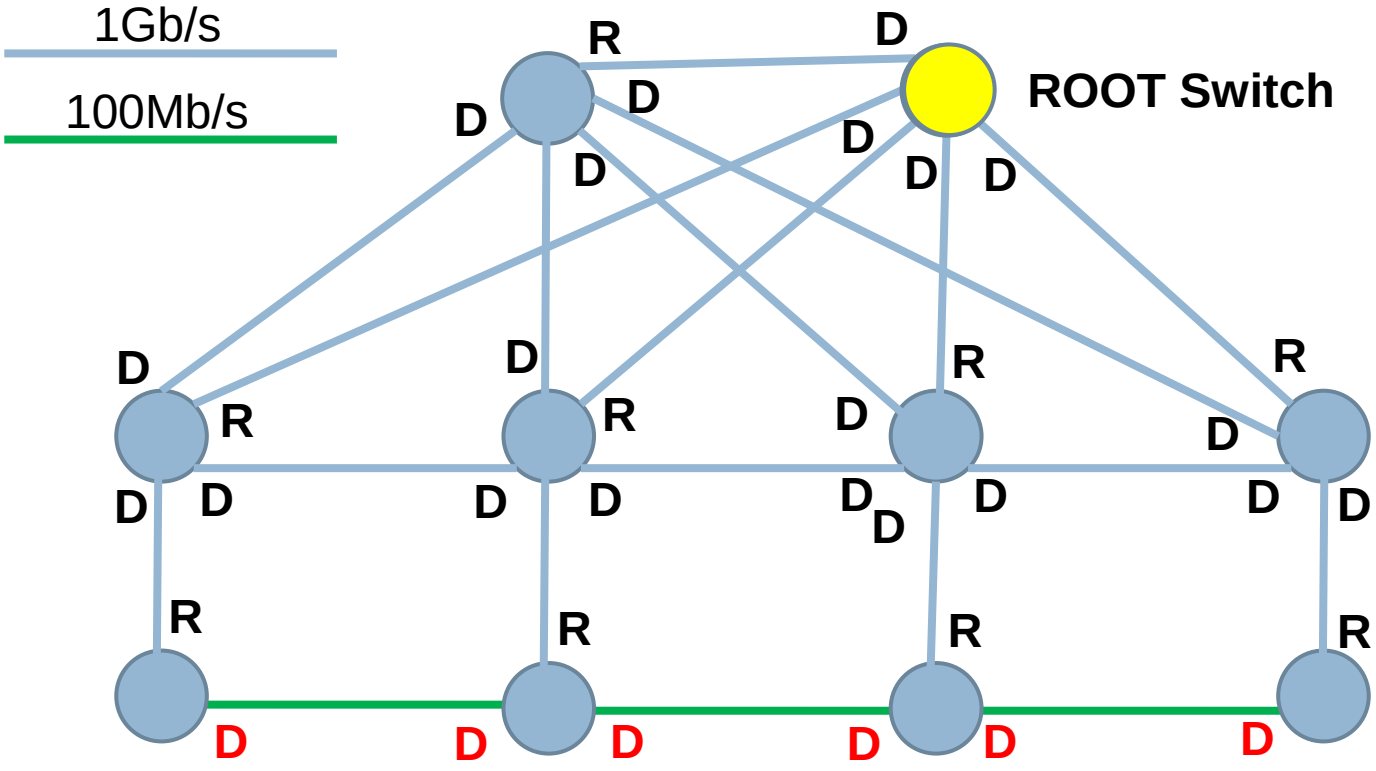
Spanning Tree Protocol



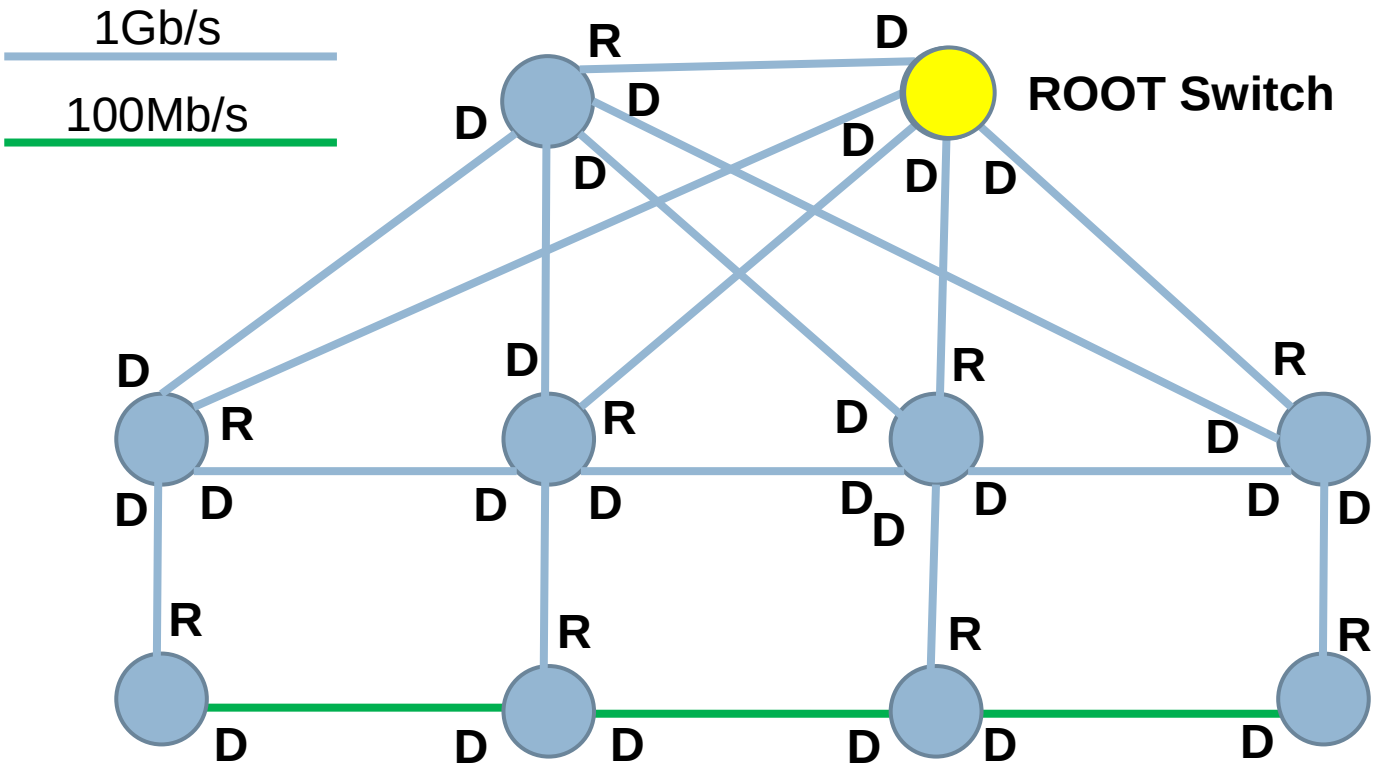


Spanning Tree Protocol

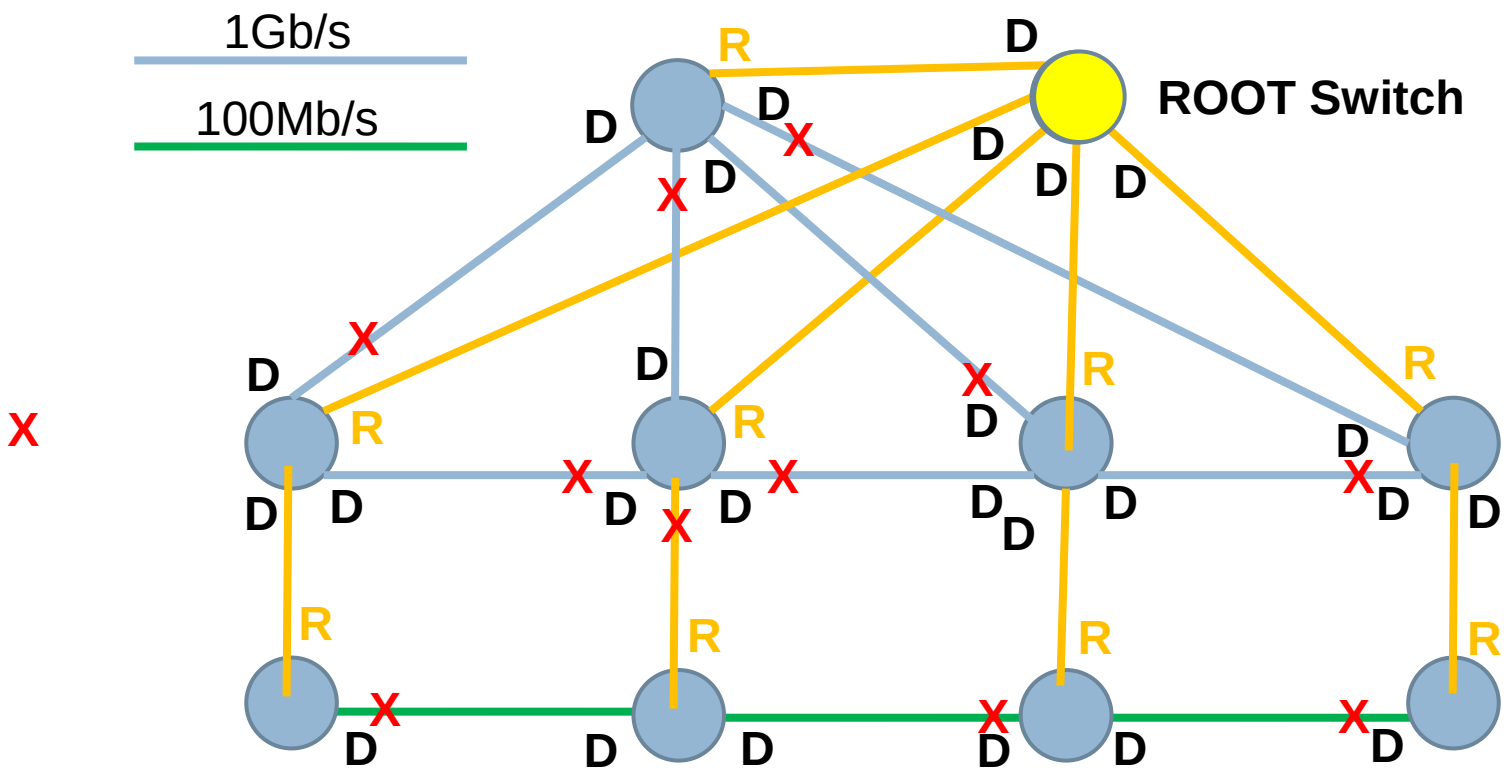




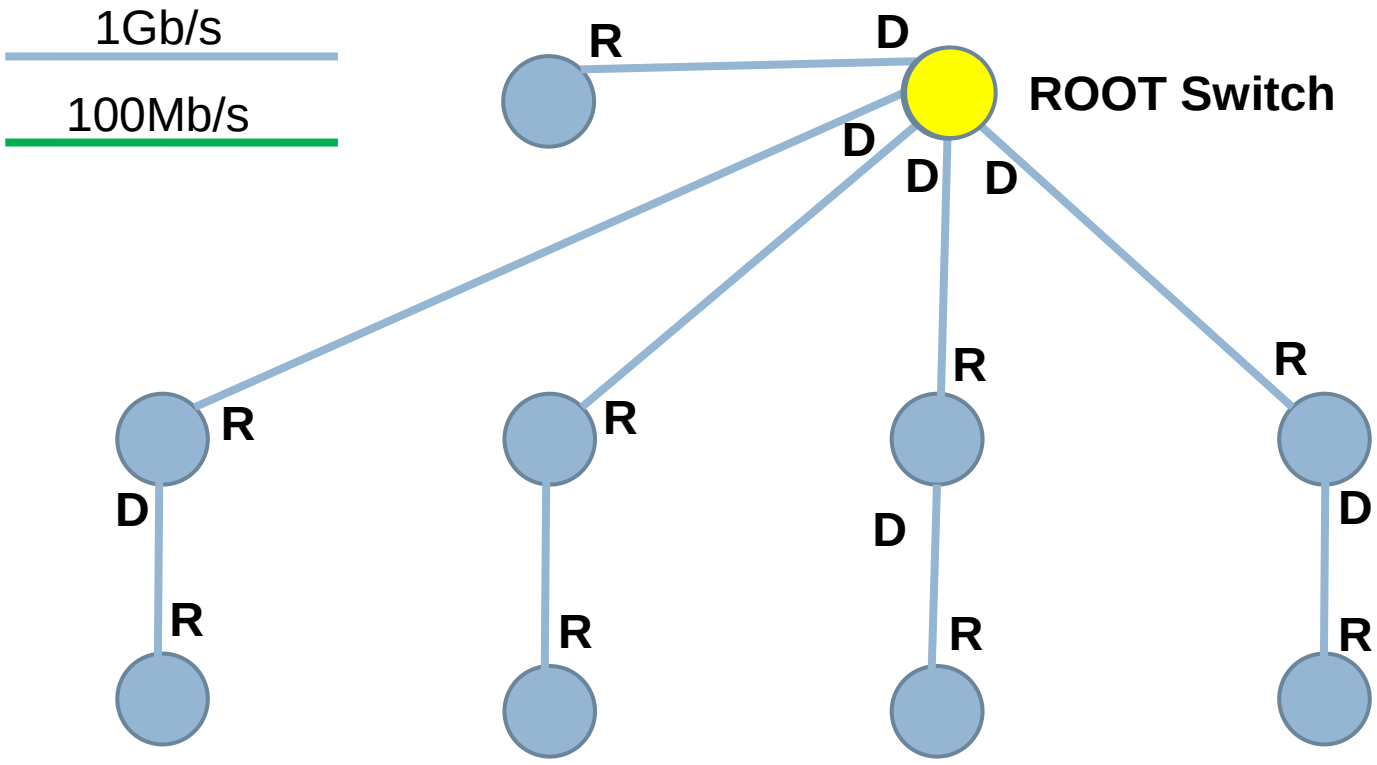
Spanning Tree Protocol



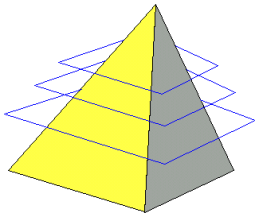
Spanning Tree Protocol

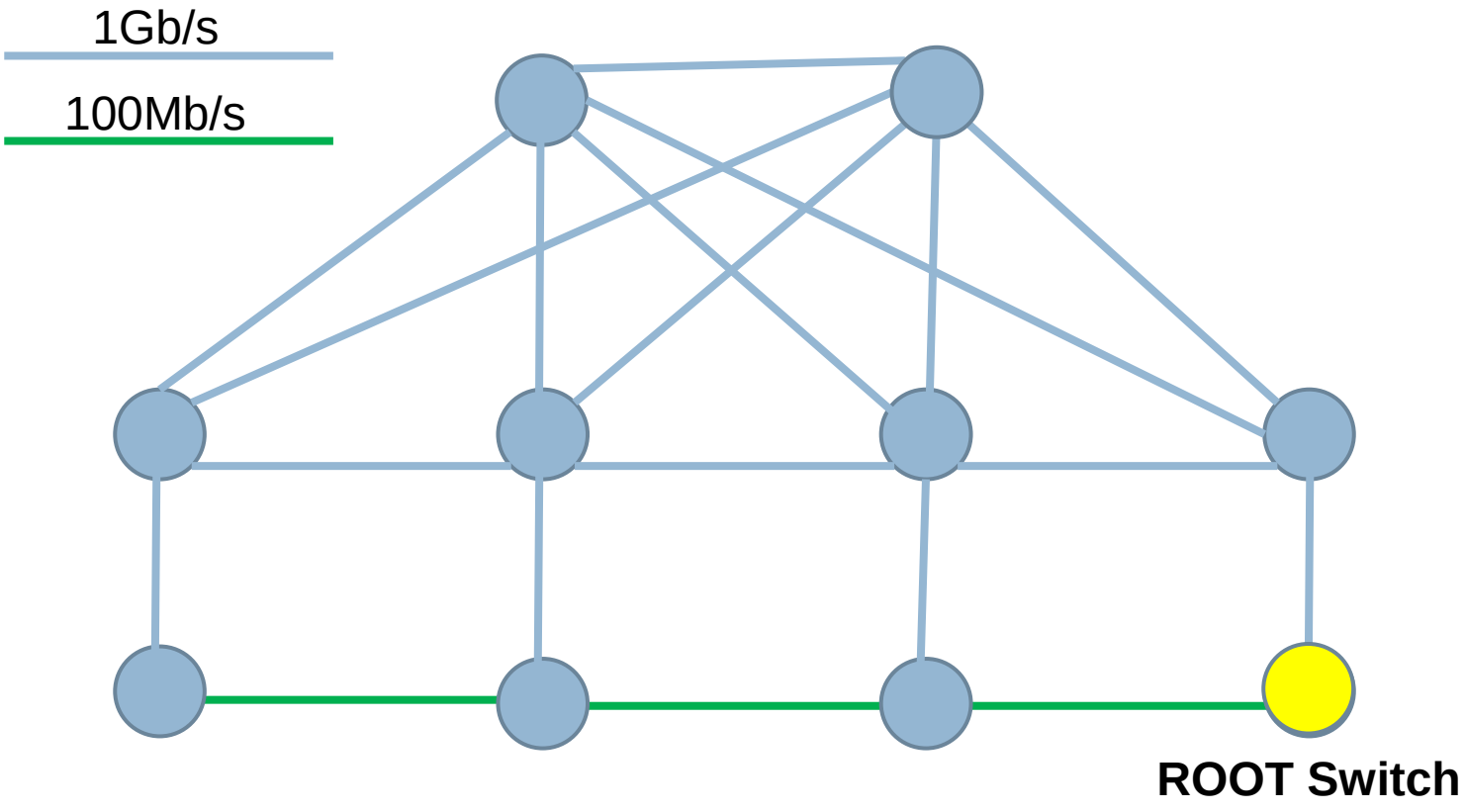


Spanning Tree Protocol

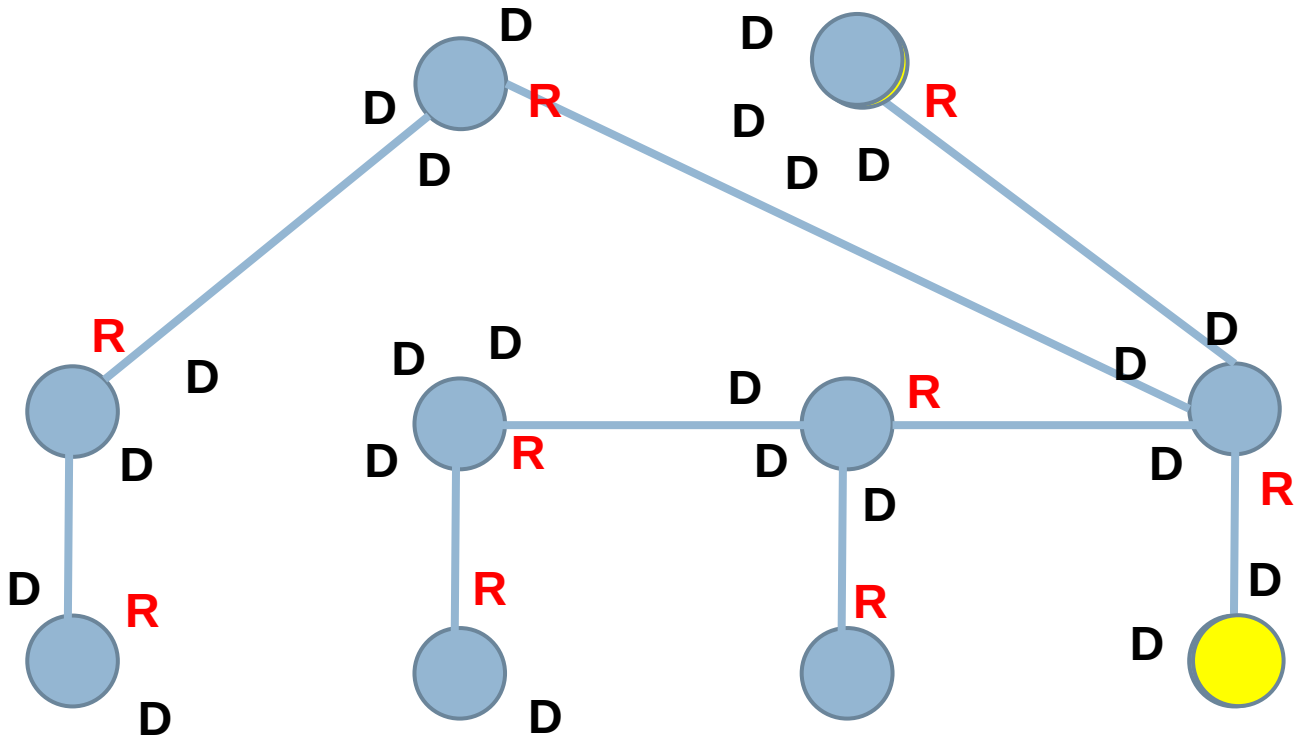


Spanning Tree Protocol

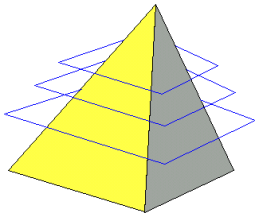




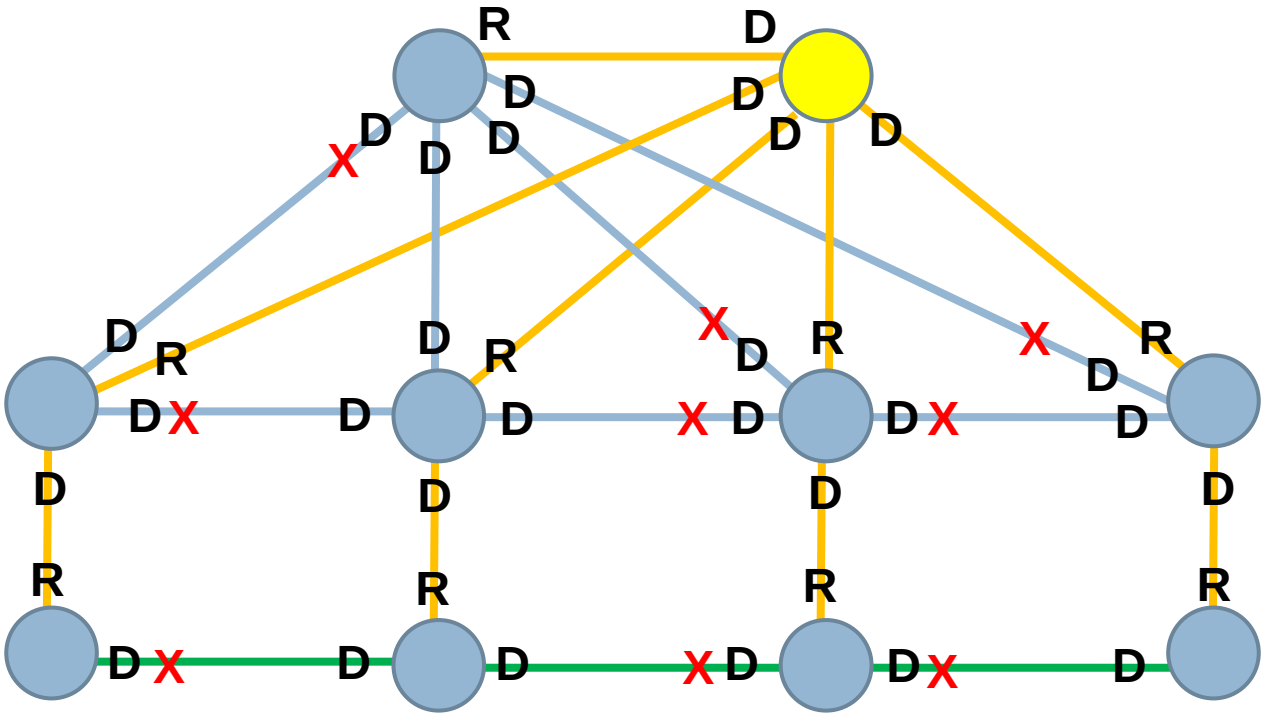
Spanning Tree Protocol



Spanning Tree Protocol

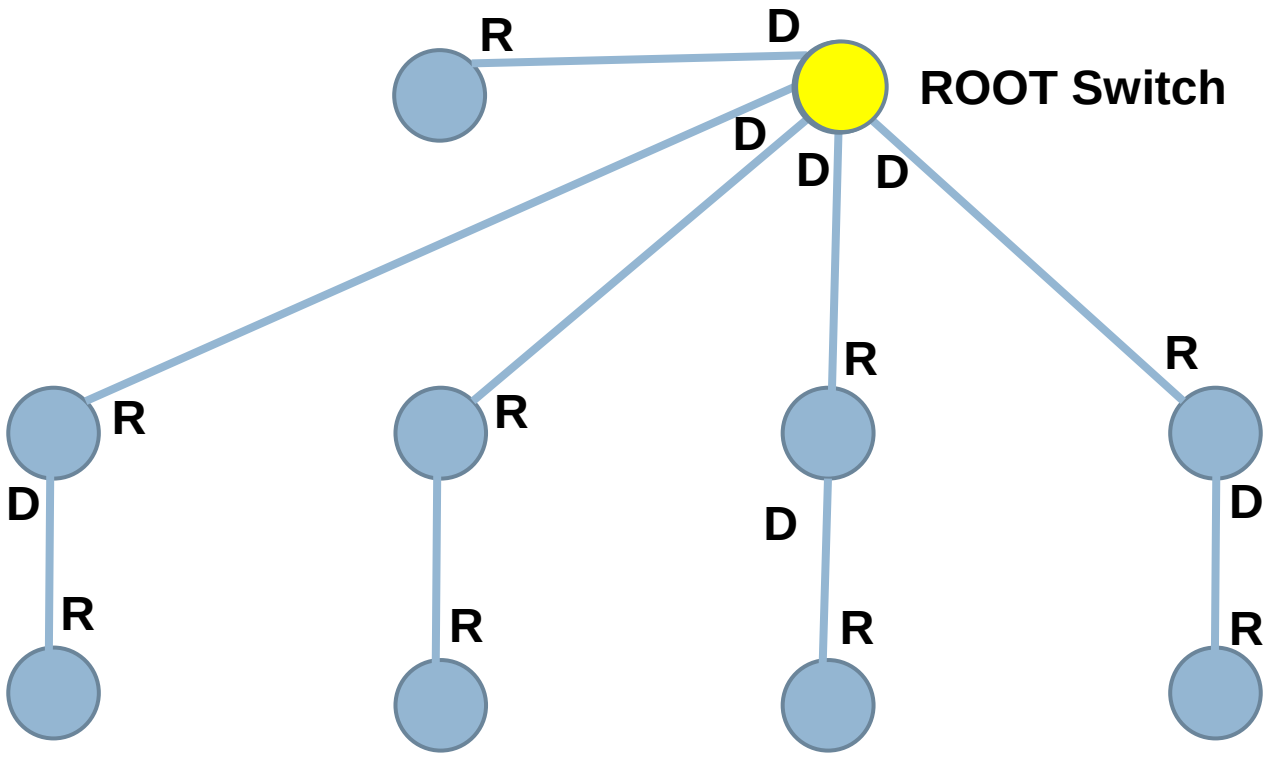


- **Diamètre : doit être ≤ 7 !!!**



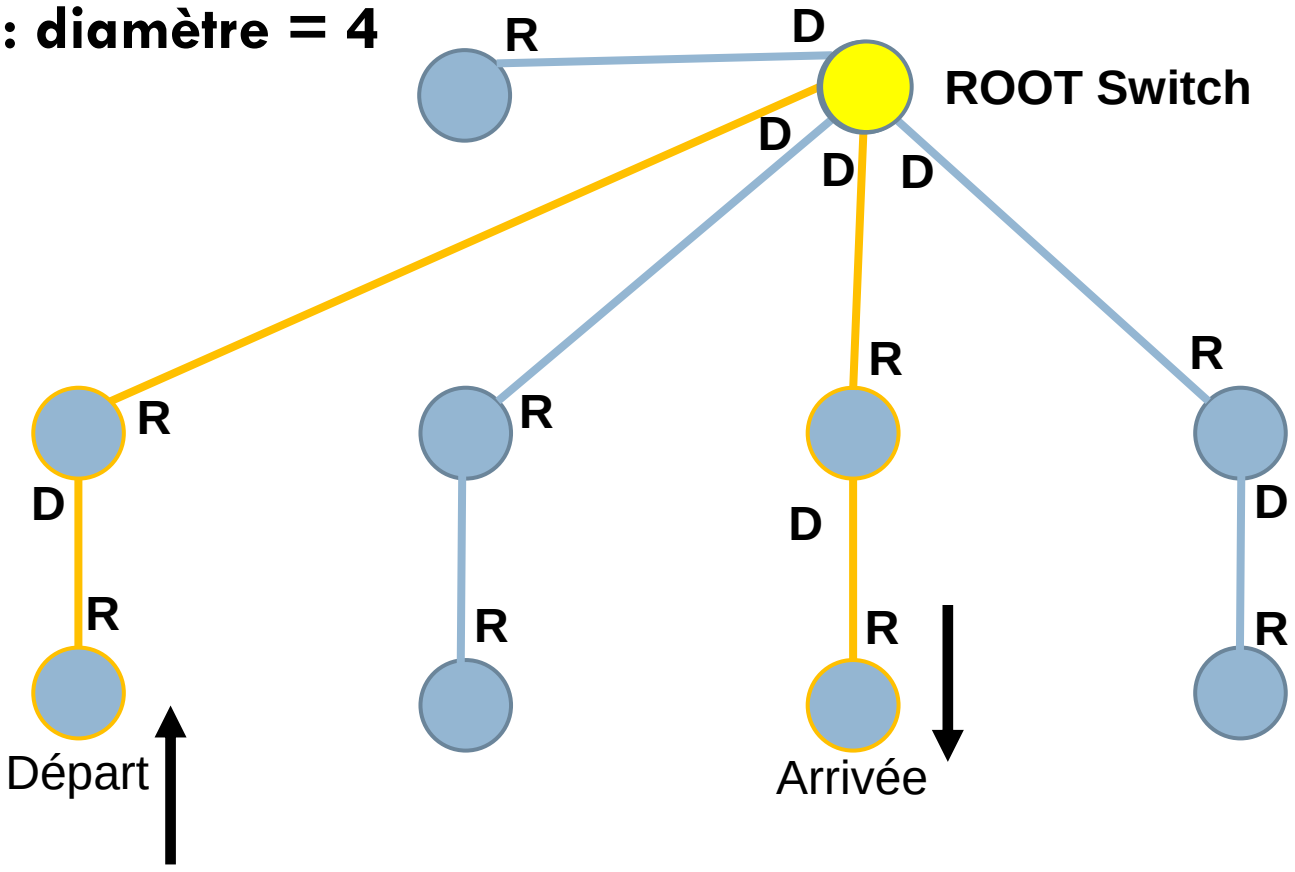
Spanning Tree Protocol

- **Diamètre : doit être ≤ 7 !!!**



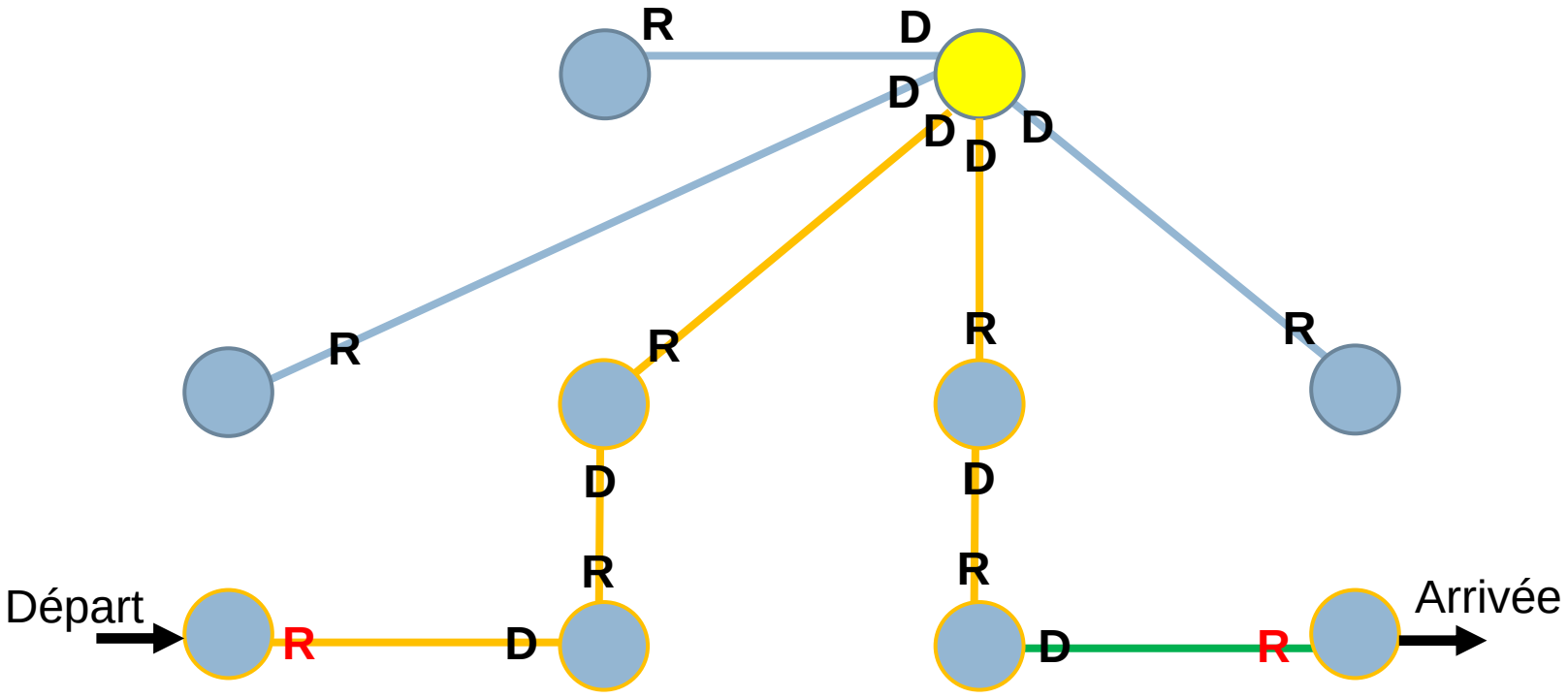
Spanning Tree Protocol

- Diamètre : doit être ≤ 7 !!!
- Ici : diamètre = 4



Spanning Tree Protocol

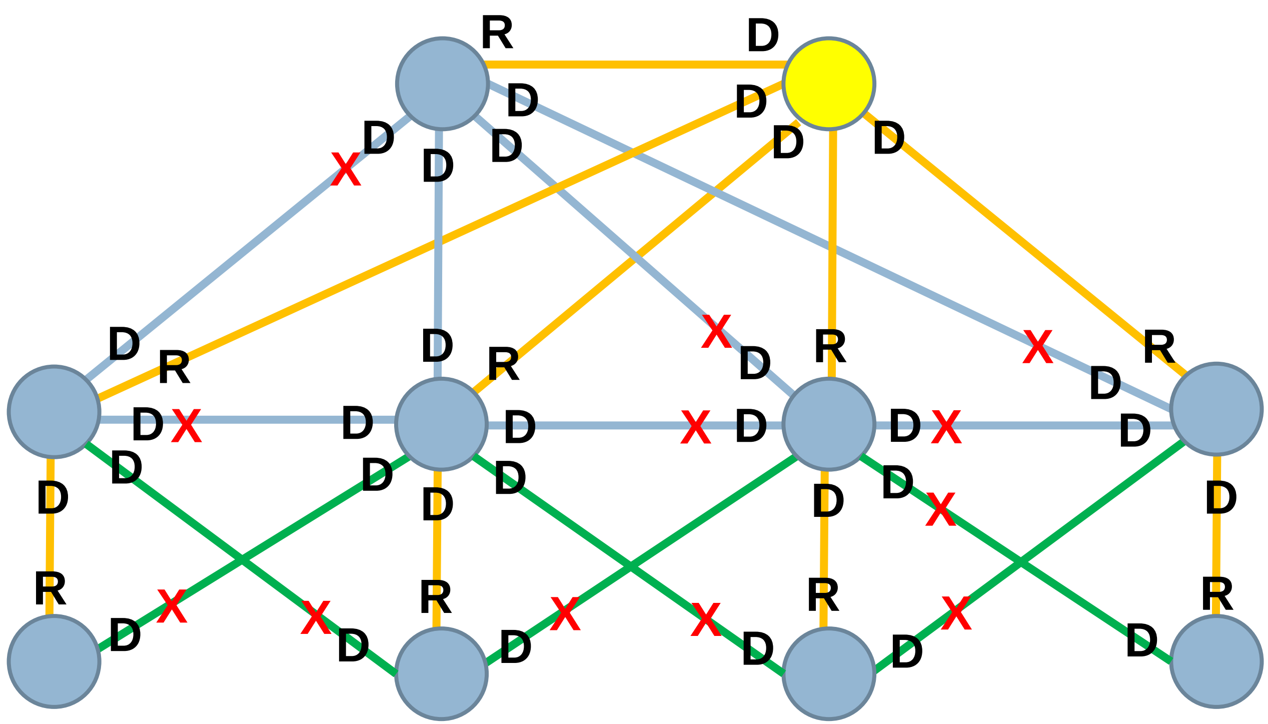
- **Mais, dans cette configuration: 6 switchs traversés**



- **Si des liens tombent, le diamètre est modifié et devient limite !**

Spanning Tree Protocol

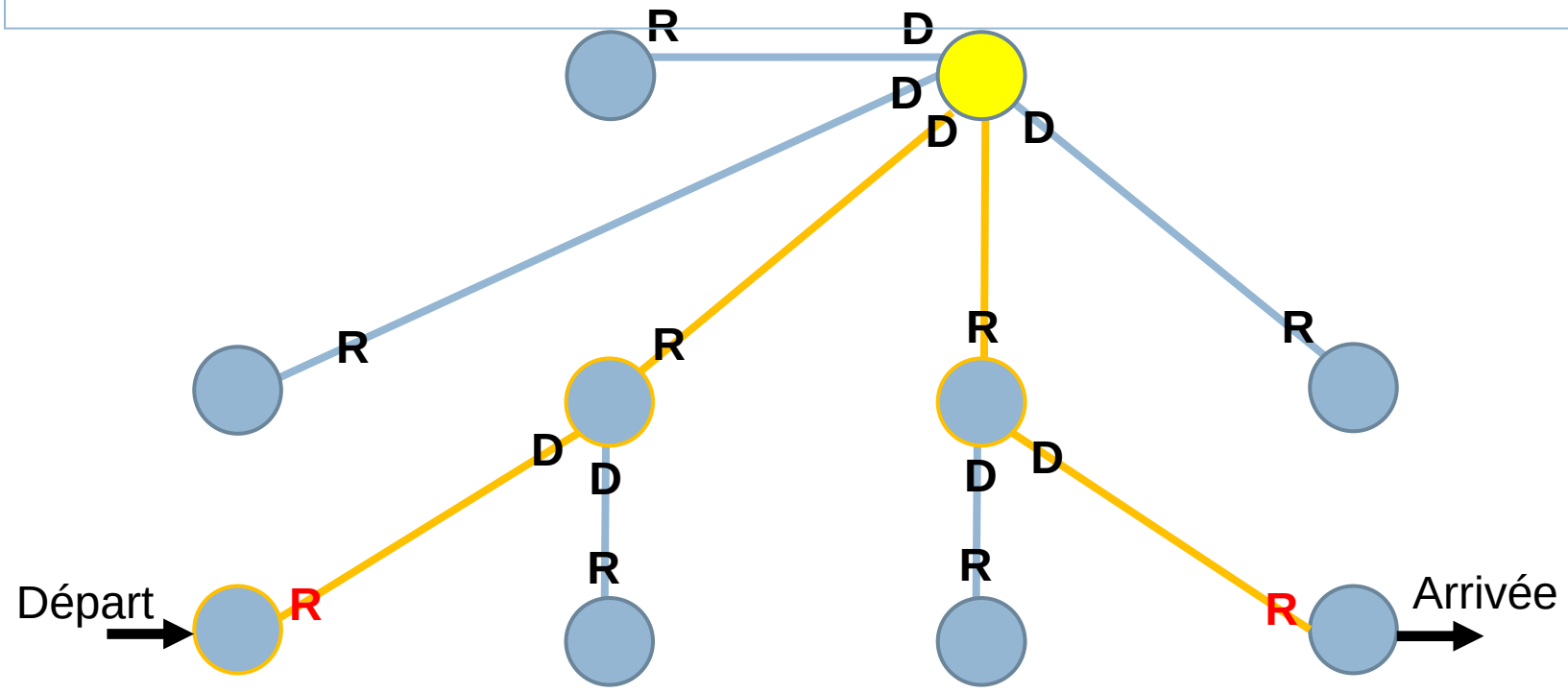
- Une architecture croisée évite ces situations



Cisco
Networking Academy

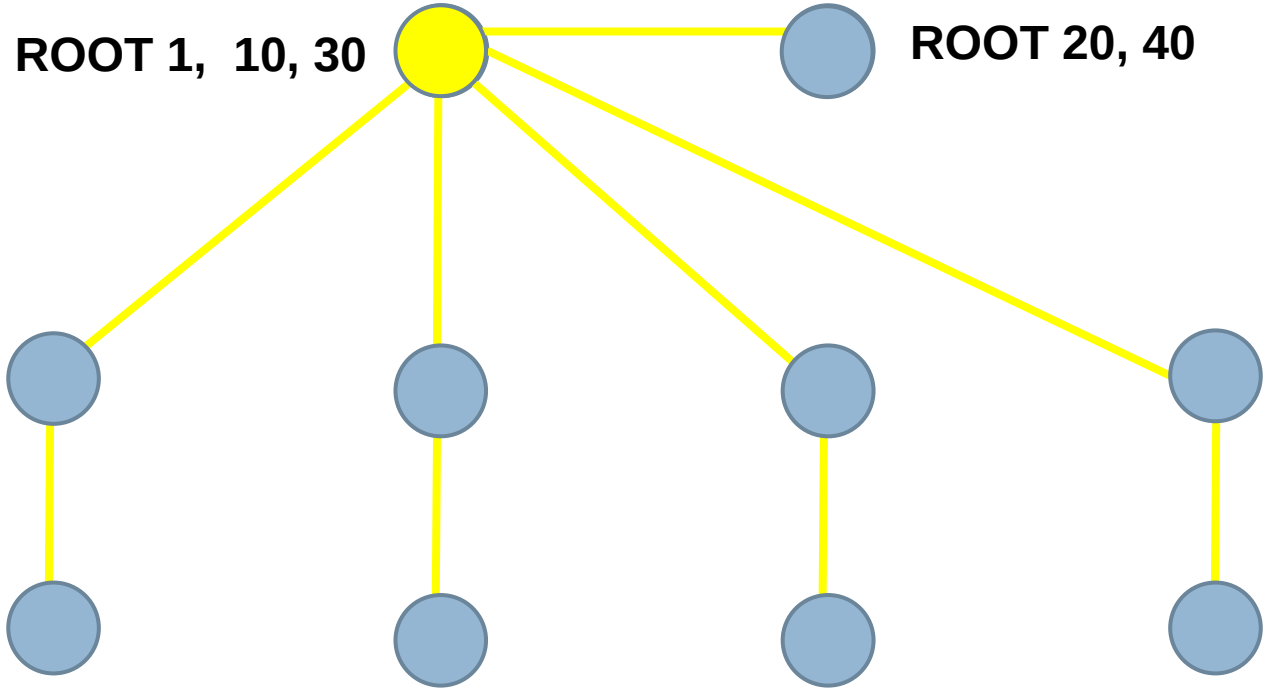
Spanning Tree Protocol

- Diamètre de ce réseau = **4**, quelque soit la situation



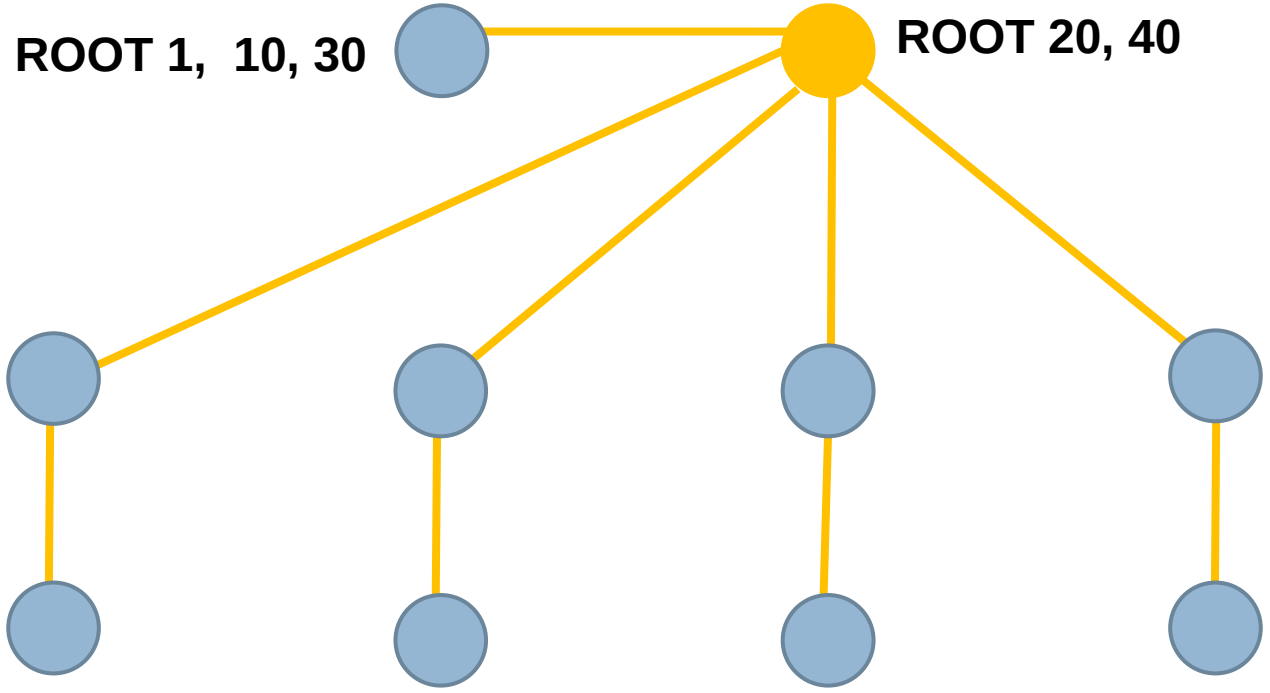
Spanning Tree Protocol

- Load Balancing : Per VLAN Spanning-tree



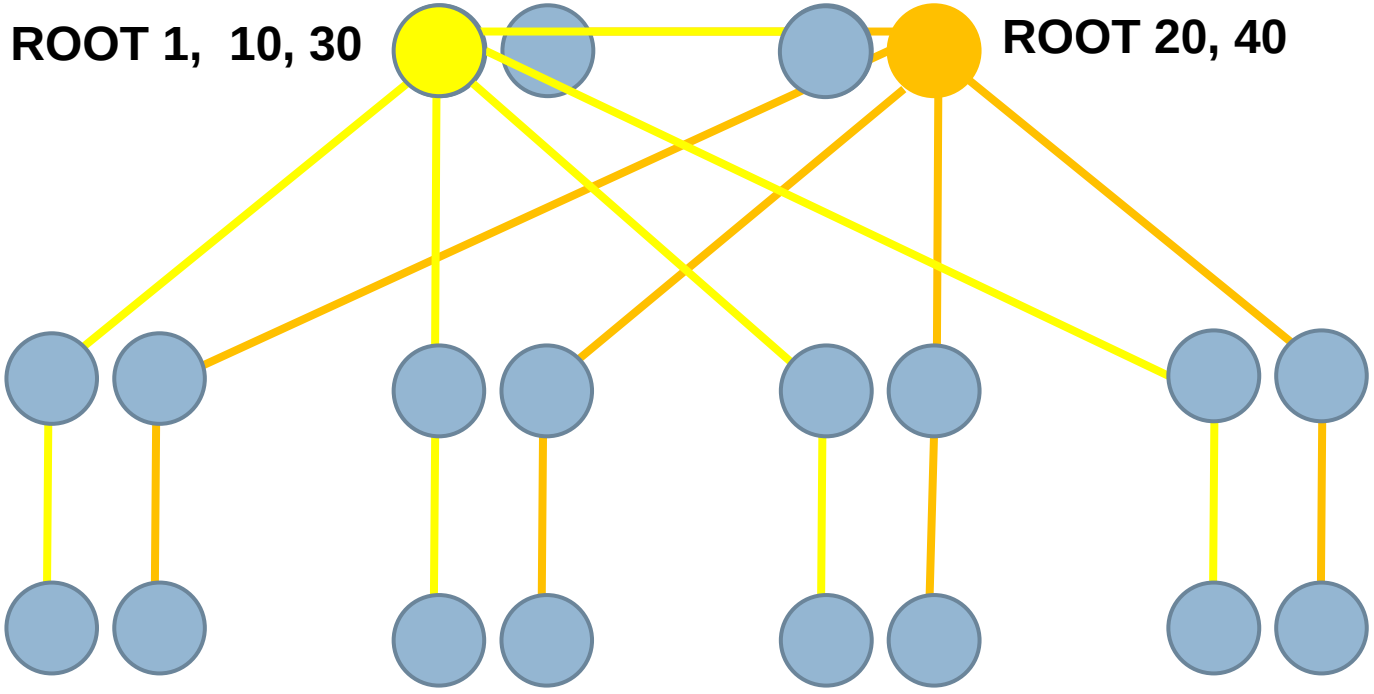
Spanning Tree Protocol

- Load Balancing : Per VLAN Spanning-tree

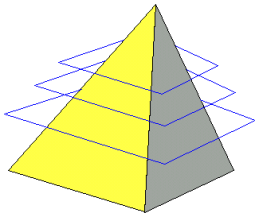


Spanning Tree Protocol

- Load Balancing : Per VLAN Spanning-tree



Spanning Tree Protocol



- Configuration
  - Rien = Grosse Buse

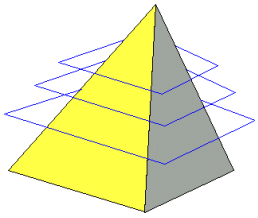
ou

  - CoreL3_1 spanning-tree vlan 1, 10, 30 priority 4096
  - CoreL3_1 spanning-tree vlan 20, 40, 998 priority 8219

  - CoreL3_2 spanning-tree vlan 1, 10, 30 priority 8192
  - CoreL3_2 spanning-tree vlan 20, 40, 998 priority 4096

  - Int fa0/1
  - spanning-tree portfast
  - Bpdu-guard

Spanning Tree Protocol



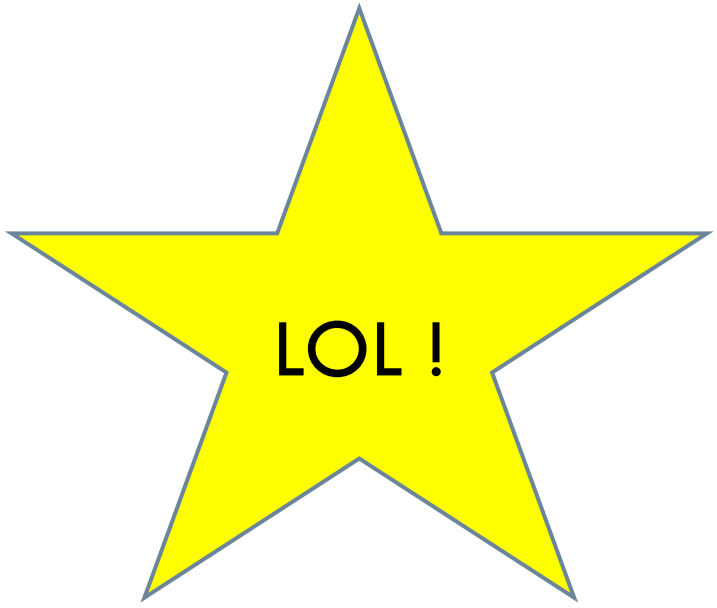
- Configuration
  - Rien

  ou

  - spanning-tree XXX priority 4096

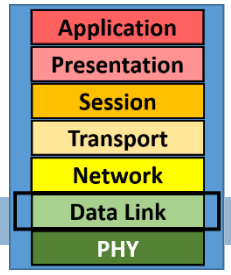
  ou

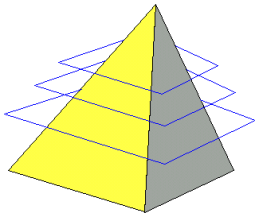
  - spanning-tree XXX priority primary



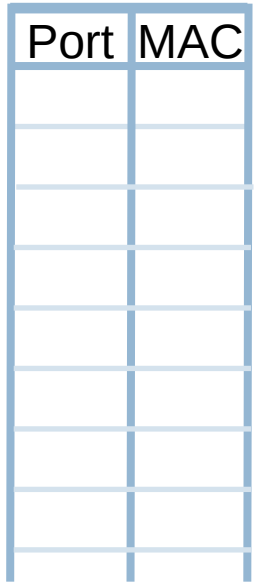
- Nota Bene : il y a en plus une notion de VLAN que nous verrons plus tard

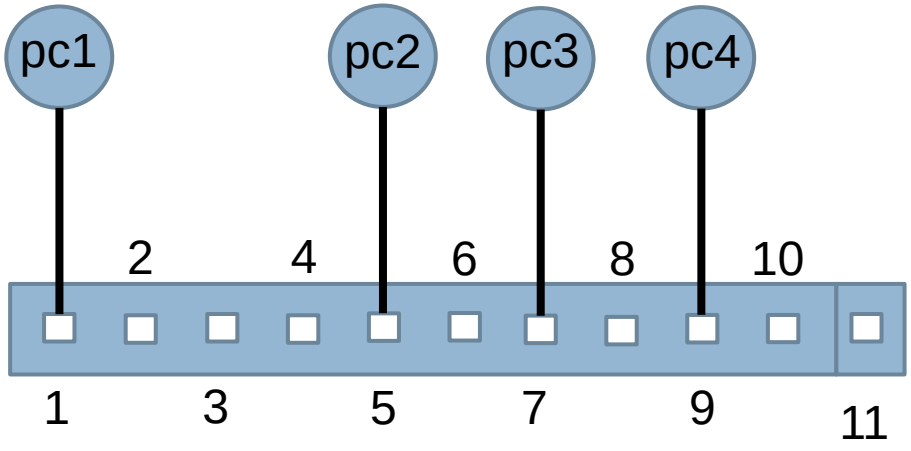
Commutation



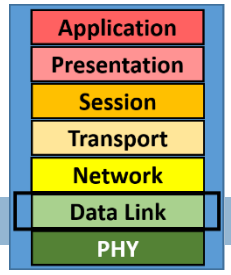


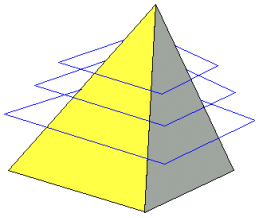
- Le commutateur « apprend » dynamiquement la topologie du réseau : chaque fois qu'il reçoit une trame, il lit l'adresse MAC source et l'associe au port d'entrée.
- Il remplit donc ainsi sa Table de Commutation





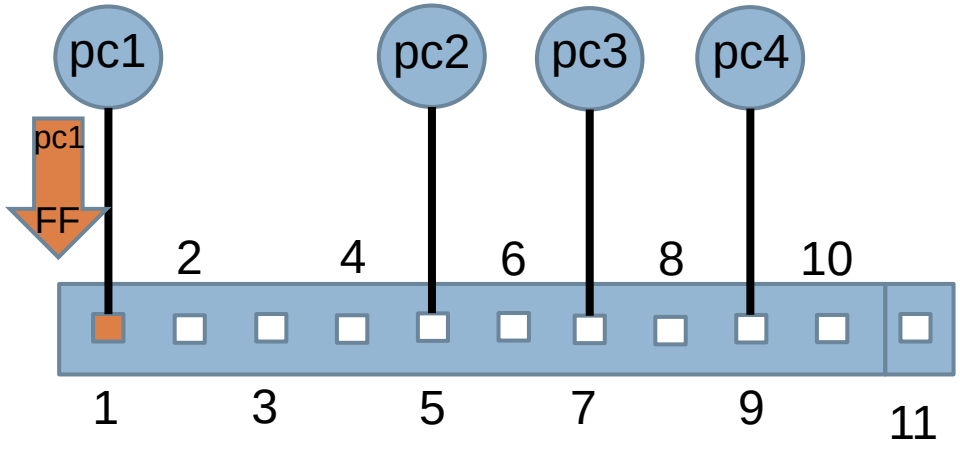
Commutation





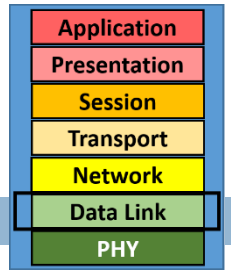
- Par exemple, Pc1 adresse un broadcast ARP pour obtenir l'adresse MAC de Pc2
- La trame est émise par Pc1 à destination de FFFF.FFFF.FFFF
- Le commutateur reçoit la trame, lit l'adresse MAC source

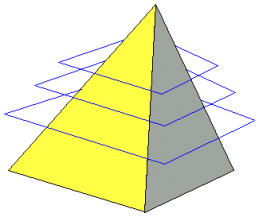
et met à jour sa table de Commutation



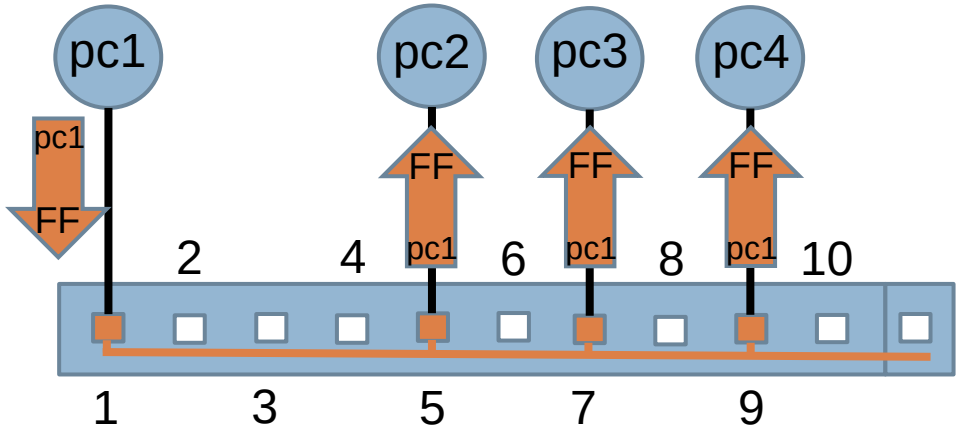
Port	MAC
1	pc1

Commutation



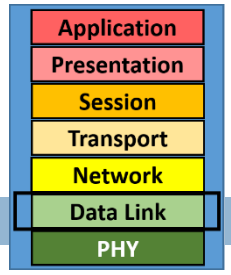


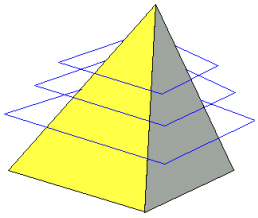
- Le commutateur lit l'adresse de destination
- Comme c'est une adresse de diffusion, il établit un lien entre le port d'entrée et tous les ports actifs (micro segmentation)
- La trame est répliquée sur tous les ports actifs



Port	MAC
1	pc1

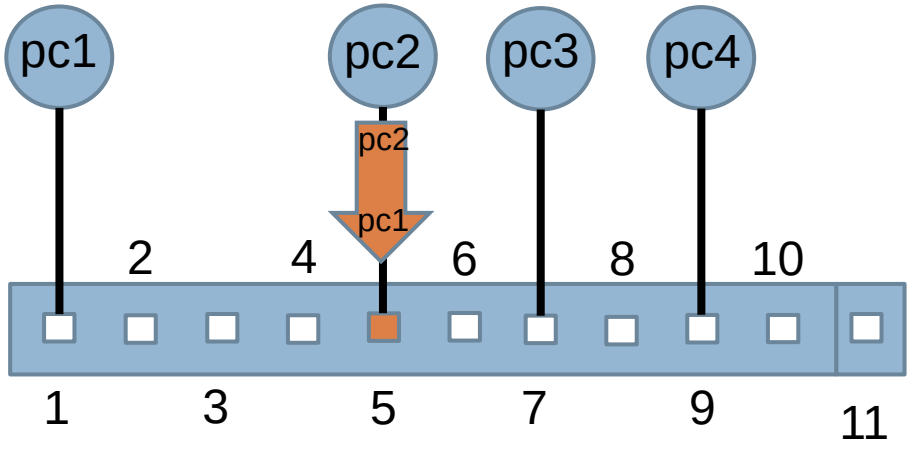
Commutation





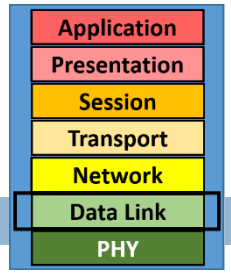
- Seul Pc2 est concerné par la requête ARP
- Pc2 va répondre en émettant une trame à destination de l'adresse MAC de Pc1
- Le commutateur reçoit la trame, lit l'adresse MAC source

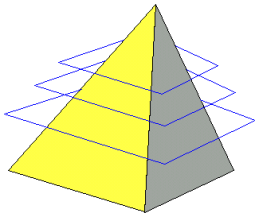
et met à jour sa table de commutation



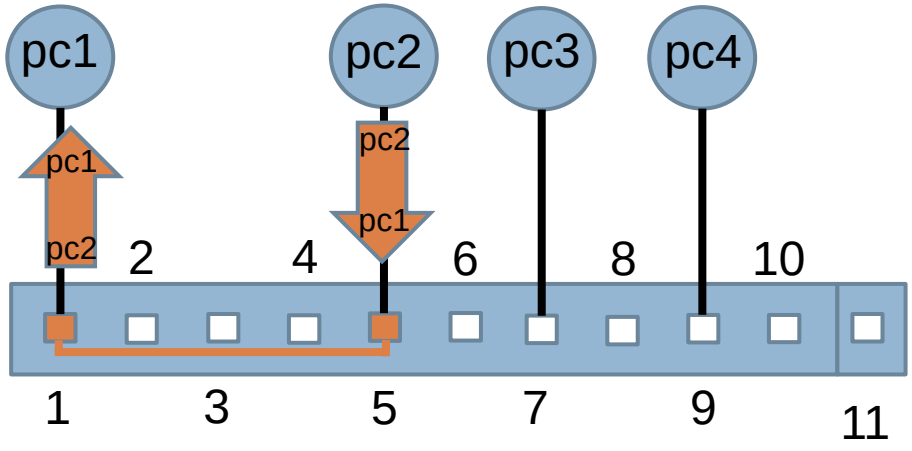
Port	MAC
1	pc1
5	pc2

Commutation





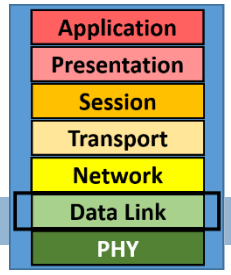
- Le commutateur lit l'adresse MAC de destination (pc1)
- Cette adresse figure dans sa table de commutation sur le port 1
- Le commutateur établit donc un lien (micro segmentation) entre les ports 5 et 1 et diffuse la trame vers PC1.

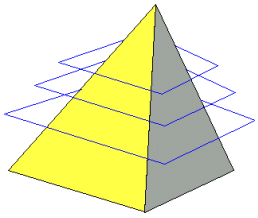


Port	MAC
1	pc1
5	pc2

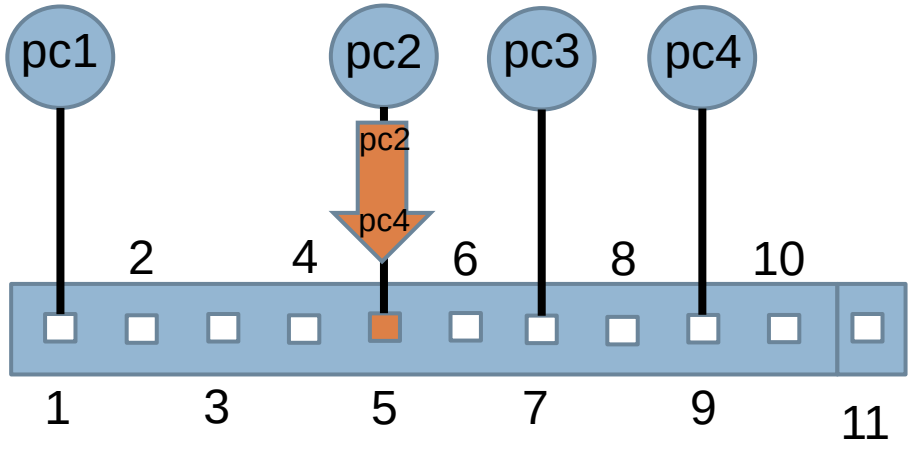
Commutation

Pourquoi l'adresse de Broadcast n'est jamais « apprise » ?





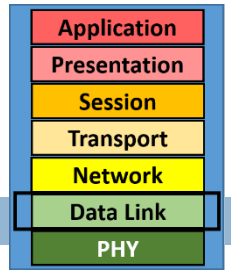
- Que se passe-t-il quand un switch reçoit une trame dont l'adresse de destination n'est pas dans la table de commutation ?
  - C'est le cas notamment de FF:FF:FF:FF:FF:FF (Broadcast)

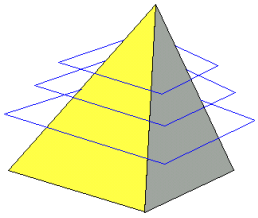


Mise à jour de l'entrée

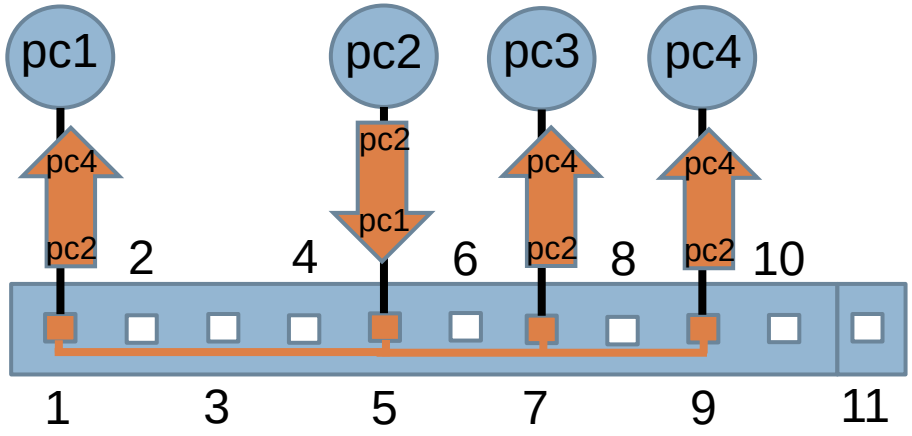
Port	MAC
1	pc1
5	pc2

Commutation





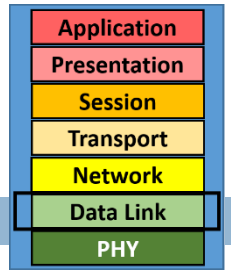
- Que se passe-t-il quand un switch reçoit une trame dont l'adresse de destination n'est pas dans la table de commutation ?
  - Le switch n'a d'autre choix que de commuter la trame vers tous les ports connectés !

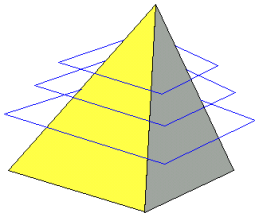


Port	MAC
1	pc1
5	pc2

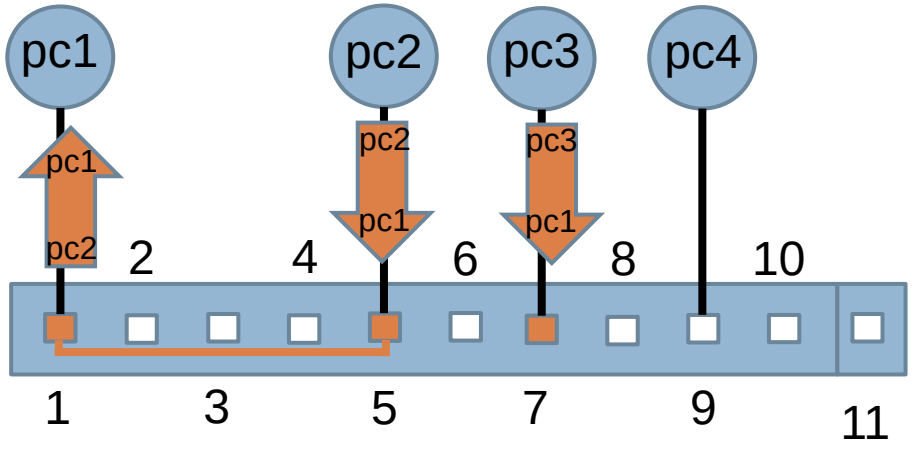
La couche 2 essaye toujours de faire le travail, contrairement à la couche 3 qui est très peu permissive !

Commutation





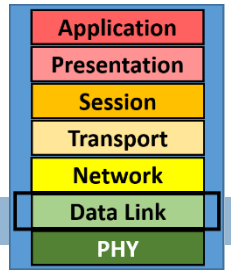
- Que se passe-t-il quand une trame est destinée à un port déjà occupé par un autre trafic ?
  - Que faire de la trame reçue sur le circuit de réception du port 7 et destinée au circuit d'émission du port 1 ?

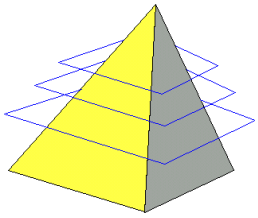


Mise à jour de l'entrée →

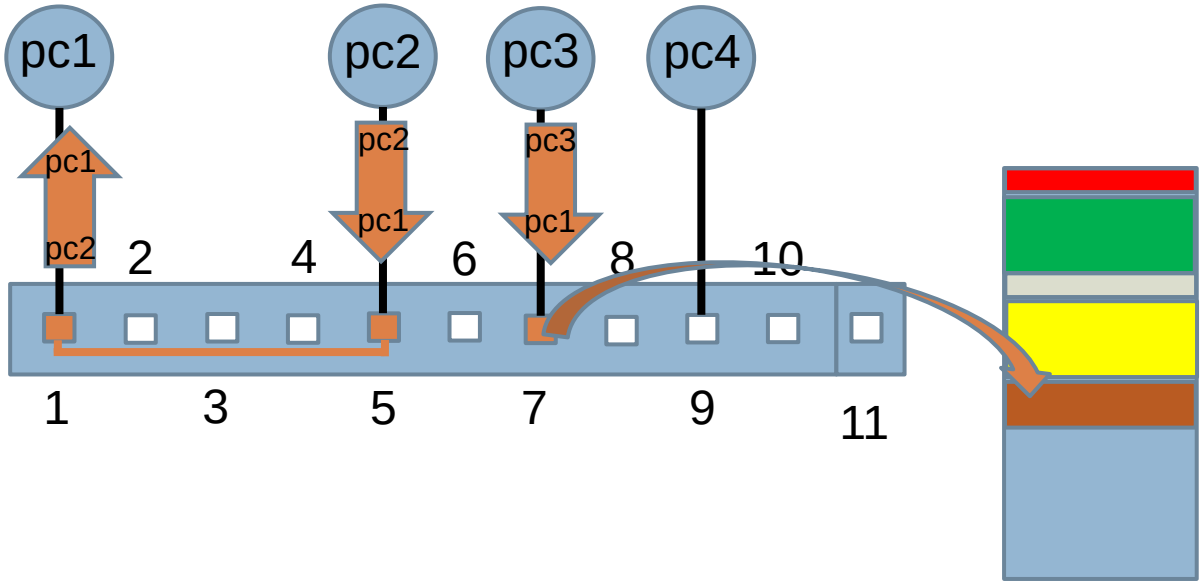
Port	MAC
1	pc1
5	pc2
7	pc3

Commutation



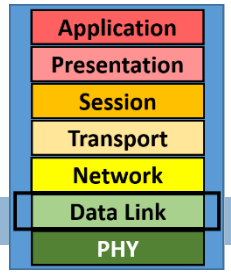


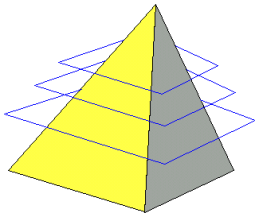
- Que se passe-t-il quand une trame est destinée à un port déjà occupé par un autre trafic ?
  - La trame est stockée dans une mémoire tampon



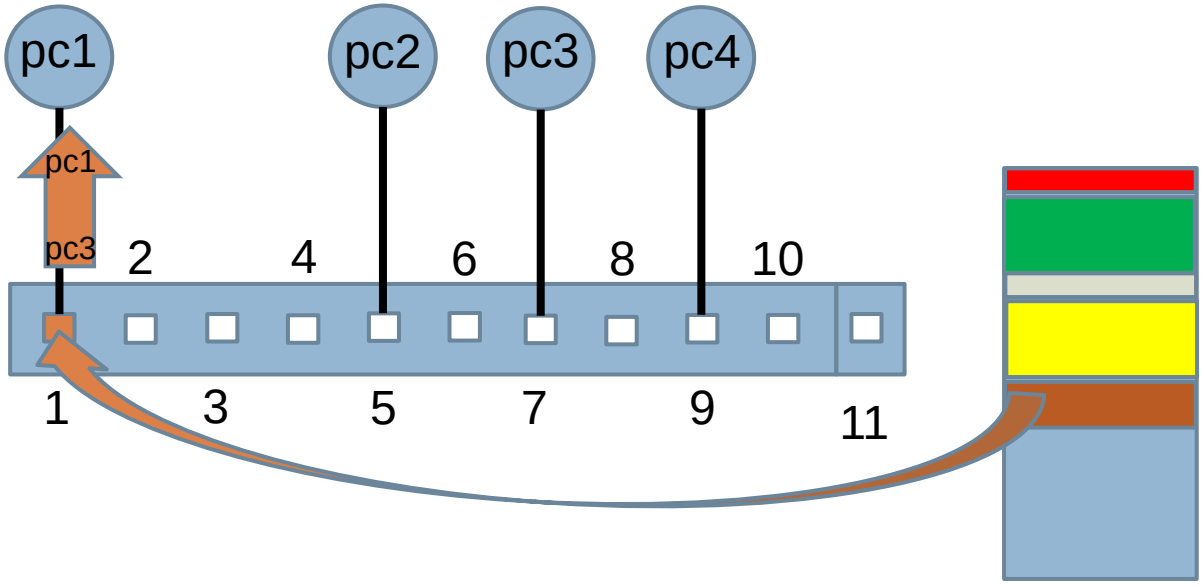
Port	MAC
1	pc1
5	pc2
7	pc3

Commutation



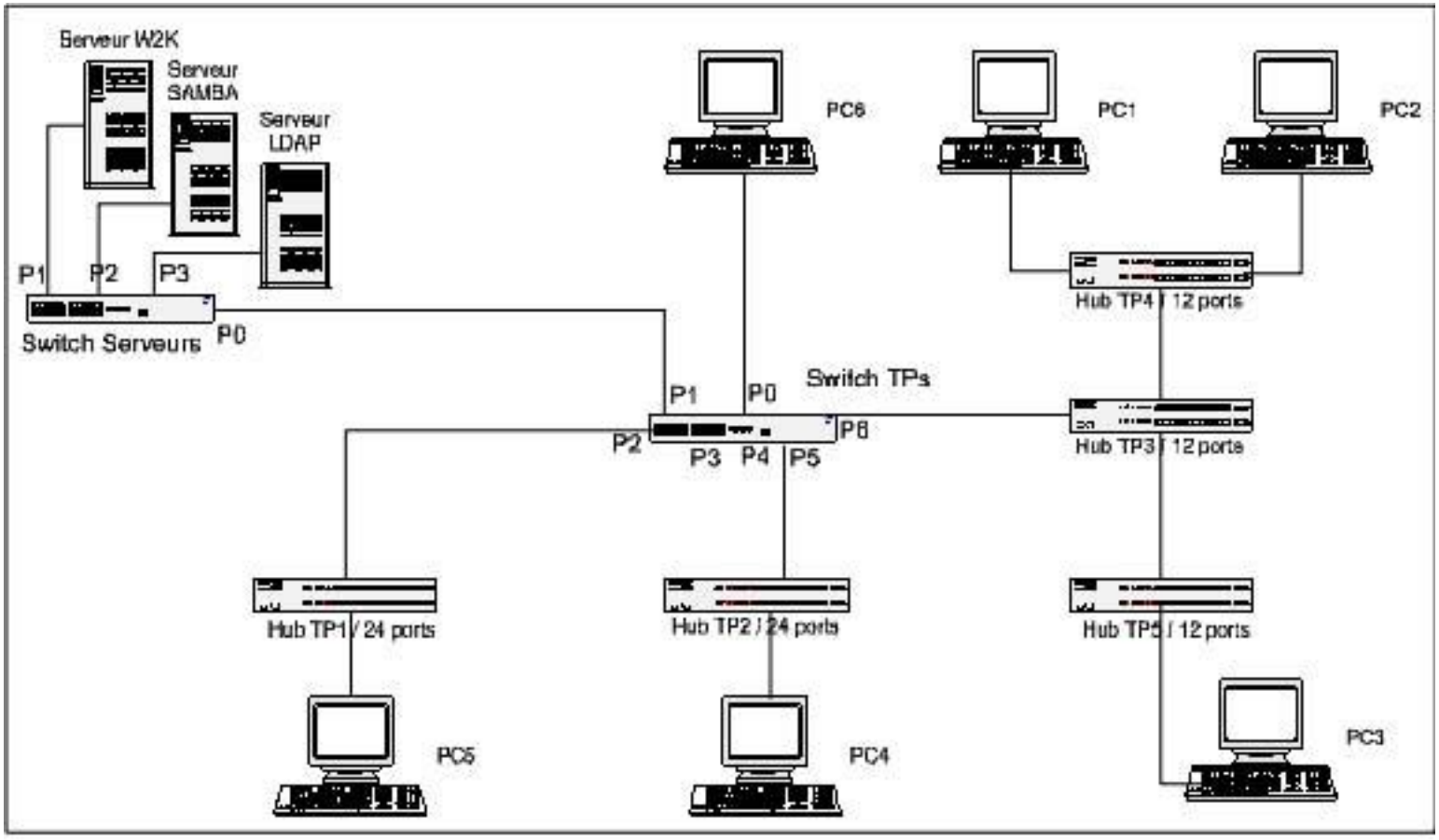


- Que se passe-t-il quand une trame est destinée à un port déjà occupé par un autre trafic ?
  - Puis la trame est transférée sur le circuit d'émission du port 1, sitôt que celui-ci est libre

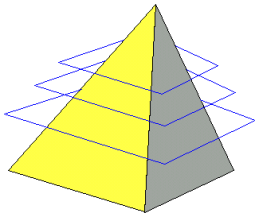


Port	MAC
1	pc1
5	pc2
7	pc3

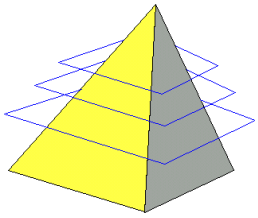
Commutation de niveau 2



Service LAN : DHCP



- Dynamic Host Control Protocol permet de distribuer automatiquement des adresses IP aux clients du réseau
- DHCP fonctionne quatre en étapes
  - Le client émet un **DHCP Discover** en mode diffusion
  - Le serveur DHCP
    - recherche une adresse disponible dans son pool
    - vérifie si cette adresse ne répond pas à un « ping »
      - donc des ARP pour obtenir la MAC d'un host éventuel… qui échouent, si tout va bien !
    - adresse une « offre » au client (**DHCP Offer**) en mode diffusion
  - Le client accepte l'offre et envoie un **DHCP Request** pour obtenir le reste des informations utiles (passerelle, DNS,…) en mode diffusion
  - Le serveur DHCP termine la transaction par un **DHCP Acknowledge** émis en mode diffusion

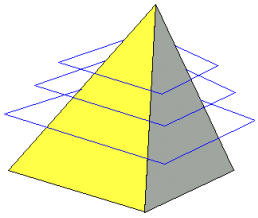


Adresses privées – RFC 1918

- Class A 10.0.0.0 … 10.255.255.255
- Class B 172.16.0.0 … 172.31.255.255
- Class C 192.168.0.0 … 192.168.255.255

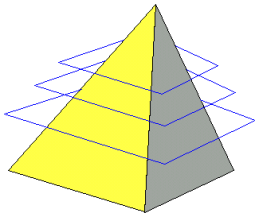
- Adresses internes à un réseau qui peuvent etre gérées par un Network Address Translation

Classes d'adresses

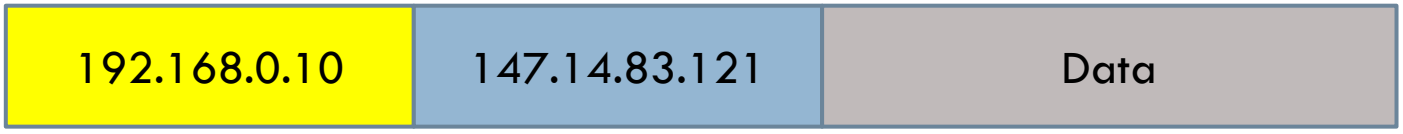


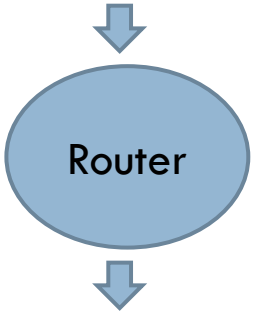
- Taille des réseaux « en classe » (classful)
  - A : 0…127 – Masque : 8 bits – Host : 2^{24}-2 (16 777 214)
  - B : 128…191 – Masque : 16 bits – Host : 2^{16}-2 (65 534)
  - C : 192…223 – Masque : 24 bits – Host : 2^{8}-2 (254)

Translation d'adresse : NAT



- Network Address Translation
  - Le routeur remplace l'adresse privée interne par son IP publique : un seul PC accède à Internet en même temps
  - Il conserve en mémoire la translation opérée

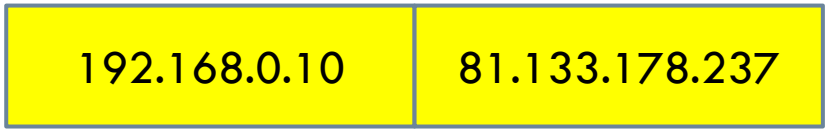


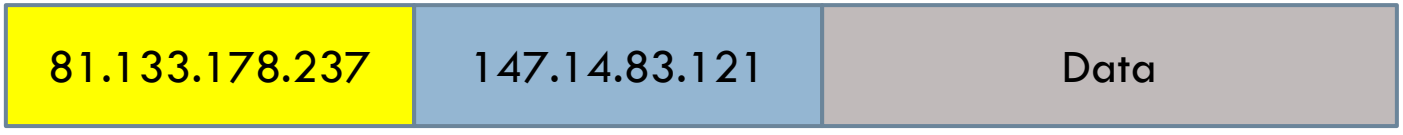


Fa0/0 : 192.168.0.254

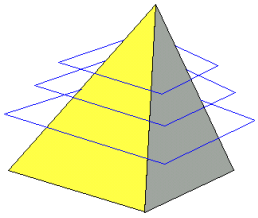
ADSL : 81.133.178.237

Translations actives (sh ip nat trans)





Translation d'adresse : NAT



- Network Address Translation
  - Quand la réponse arrive le routeur consulte sa table de translations actives
  - Il remplace sa propre adresse par celle du client interne

147.14.83.121	81.133.178.237	Data

Router

ADSL : 81.133.178.237

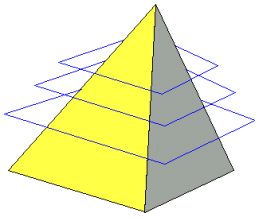
Translations actives (sh ip nat trans)

192.168.0.10	81.133.178.237

Fa0/0 : 192.168.0.254

147.14.83.121	192.168.0.10	Data

Translation d'adresse : PAT



Port Address Translation

- Le routeur remplace les adresses privées interne par son IP publique
- Les différents clients sont identifiés par le port source de couche 4

192.168.0.10	147.14.83.121	65000	80	Data

Fa0/0 : 192.168.0.254

Router

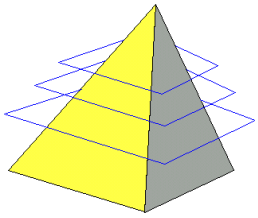
Translations actives (sh ip nat trans)

192.168.0.10:65000	81.133.178.237:65000

ADSL : 81.133.178.237

81.133.178.237	147.14.83.121	65000	80	Data

Translation d'adresse : PAT



Port Address Translation

- Quand la réponse arrive le routeur consulte sa table de translations actives et repère celle qui correspond au port de couche 4 de destination
- Il remplace sa propre adresse par celle du client interne

147.14.83.121	81.133.178.237	80	65000	Data

Router

ADSL : 81.133.178.237

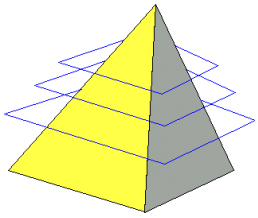
Fa0/0 : 192.168.0.254

Translations actives (sh ip nat trans)

81.133.178.237:65000	192.168.0.10:65000

147.14.83.121	192.168.0.10	80	65000	Data

Translation d'adresse : PAT



- Si deux ports sources identiques ?

192.168.0.10	147.14.83.121	65000	80	Data

Fa0/0 : 192.168.0.254

Router

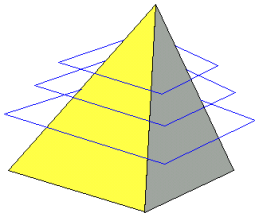
ADSL : 81.133.178.237

Translations actives (sh ip nat trans)

192.168.0.89:65000	81.133.178.237:65000
192.168.0.75:64444	81.133.178.237:64444
192.168.0.10:65000	81.133.178.237:**62222**

81.133.178.237	147.14.83.121	62222	80	Data

Translation d'adresse : PAT



- Si deux ports sources identiques ?

81.133.178.237	147.14.83.121	**62222**	80	Data

ADSL : 81.133.178.237

Router

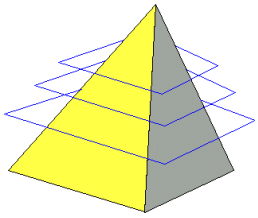
Fa0/0 : 192.168.0.254

Translations actives (sh ip nat trans)

192.168.0.89:65000	81.133.178.237:65000
192.168.0.75:64444	81.133.178.237:64444
192.168.0.50:65000	81.133.178.237:**62222**

192.168.0.10	147.14.83.121	**65000**	80	Data

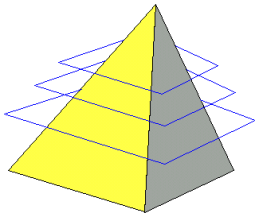
Translation d'adresse : NAT/PAT



Address & Port Address Translation

- Cas d'une entreprise avec plusieurs dizaines ou centaines d'accès à Internet en même temps
- Pour tous les flux en mode déconnecté (HTTP par exemple), le routeur opère un PAT en utilisant son IP publique externe
- Pour les flux en mode connecté (SSH par exemple), le routeur opère un NAT en utilisant un « pool » d'adresses publiques
- NAT STATIQUE : l'adresse privée des serveurs (serveur Web, serveur Mail) est associée de façon statique à des IP publiques référencées dans les serveurs DNS
- **Redirection de Port** : en cas de pénurie d'adresses publiques c'est le port de couche 4 qui permet au routeur de diriger le trafic vers le bon serveur : par exemple port 80 -> serveur Web

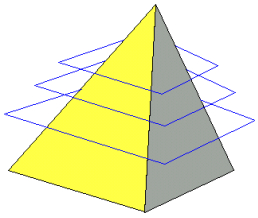
Site à site : Tunnels GRE



- **Generic Routing Encapsulation**. Permet d'établir un « tunnel » entre deux routeurs : les paquets IP sont transportés dans des paquets IP
- L'intérêt est de faire communiquer les différents sites en restant en adressage privé
- **Configuration des routeurs liés par le tunnel**
  - int tunnel 0 — Configuration du routeur 1
    - tunnel source fa0/1 — Interface locale extérieure
    - tunnel destination 81.255.255.49 — IP publique de l'autre routeur
    - ip address 10.1.2.1 255.255.255.252 — Adresse IP du tunnel
  - int tunnel 0 — Configuration du routeur 2
    - tunnel source fa0/1
    - tunnel destination 81.255.255.65
    - ip address 10.1.2.2 255.255.255.252

KALYST
INGENIERIE INFORMATIQUE

Merci de votre attention



- Questions ?

CISCO
Networking Academy