

Formation Transfer 1.2

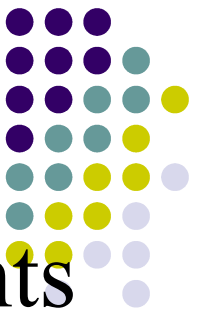
Administration réseaux sous GNU/Linux

Formateurs:

- Olivier-Pascal Bakasanda B. Admin réseau CEDESURK
- Oscar Nsarhaza M. Admin réseau ISTA
- Augustin Kanyimbu M. Admin Backbone réseau UNIKIN

ISTA 20-24 octobre 2008

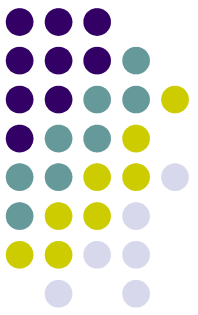
Objectifs



A la fin de ce module de cinq jour, les participants seront en mesure de:

- concevoir et mettre en place le fonctionnement durable d'un réseau local, régional ou national de type TCP/IP, ayant une liaison internet permanente ;
- gérer un réseau local TCP/IP intégrant un ou plusieurs serveurs Unix et offrant les services Internet tels que la messagerie, le web, le DNS, etc. à des utilisateurs de micro-ordinateurs sur un réseau informatique.

Contenu



Chap. 0. Rappels

- 0.1. Système Unix et logiciels libres
- 0.2. Commandes de base, les éditeurs
- 0.3. Droits sur les fichiers et répertoires

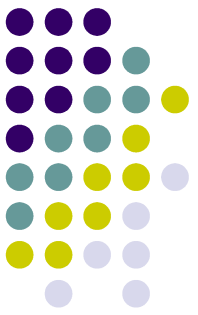
Chap. 1. Généralités des réseaux

- 1.1. Modèle OSI et TCP/IP (les protocoles)
- 1.2. Types et topologies réseaux

Chap. 2. Adressage IP

- 2.1. IPv4: création des réseaux, découpage en sous réseaux;
- 2.2. Ipv6: aperçu général et possibilité d'utilisation;

Contenu (suite)



Chap. 3. Routage IP statique et dynamique

3.1. interconnexion entre réseaux

Chap. 4. Gestion des commandes de base des réseaux

Chap. 5. Installation des serveurs et postes clients
(Debian+Ubuntu)

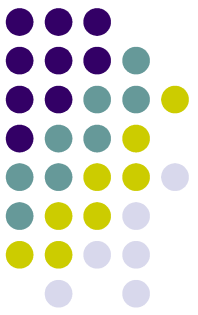
Chap. 6. Installation et configuration des services

6.1. DHCP: dhcp3-server

6.2. DNS: Bind9

6.3. WEB: Apache2 (hôtes virtuels, web sécurisé)

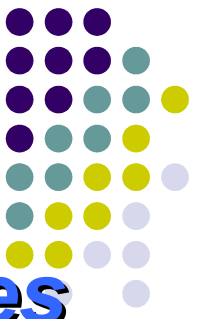
Contenu (suite)



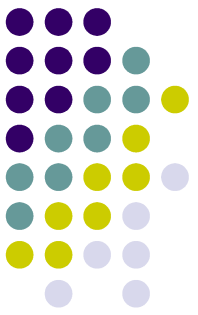
- 6.4. MAIL: Postfix
- 6.5. BD: Mysql
- 6.6. PROXY-CACHE: squid
- 6.7. Backup: Backuppc
- 6.8. Firewall

Chap. 0. Rappels

0.1. Système Unix et logiciels libres

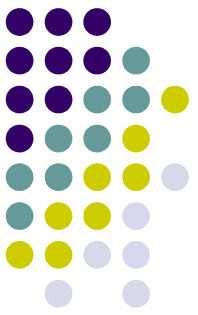


Qu'est-ce qu'un logiciel libre ?



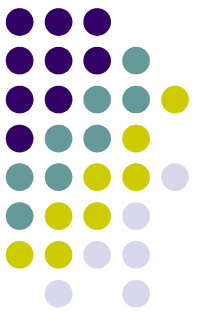
L'expression « **Logiciel Libre** » fait référence à la liberté et non pas au prix.

L'expression « **Logiciel Libre** » fait référence à la liberté pour les utilisateurs d'exécuter, de copier, de distribuer, d'étudier, de modifier et d'améliorer



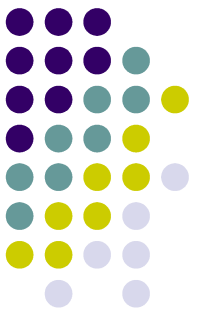
Quatre types de liberté pour l'utilisateur du logiciel :

- **Liberté 0** La liberté d'exécuter le programme, pour tous les usages.
- **Liberté 1** La liberté d'étudier le fonctionnement du programme, et de l'adapter à vos besoins. Pour ceci l'accès au code source est une condition requise.



- **Liberté 2** La liberté de redistribuer des copies, donc d'aider votre voisin.
- **Liberté 3** La liberté d'améliorer le programme et de publier vos améliorations, pour en faire profiter toute la communauté. pour ce faire, l'accès au code source est une condition requise.

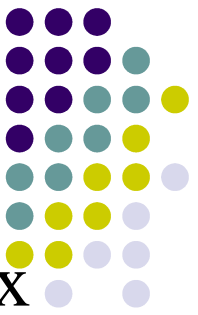
1. Caractéristiques du Linux (Unix)



- Système multi-tâche, multi-utilisateur
- Arborescence de fichiers et de systèmes de fichiers

FS (File system) a une double signification dans le système UNIX.

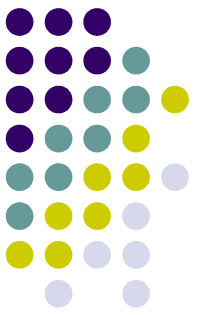
- Pour les utilisateurs et l'administrateur :
 - arborescence des fichiers du système UNIX.
- Pour l'administrateur:
 - structure d'accueil pour une arborescence de fichiers, créée sur un disque.



NB:

Le principe de l'unification des arborescences a été étendu aux réseaux. Un fichier peut résider localement mais aussi sur un disque distant.

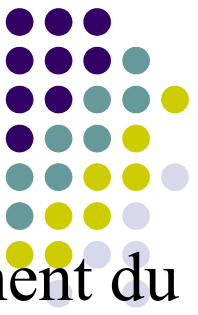
- Processus et noyau, fichiers périphériques
 - Le noyau (« Kernel ») est un fichier chargé au démarrage de l'ordinateur. Il se charge de la gestion des ressources du système UNIX, en particulier des processus qu'il crée pour exécuter les commandes des utilisateurs et des périphériques.
 - Sous UNIX, les périphériques sont vus comme des fichiers



- Shell et commandes, scripts

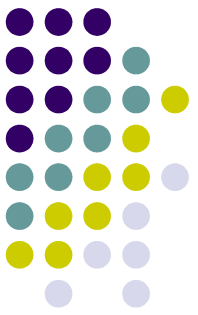
Le shell est associé à une session de travail en mode commande. L'administrateur, plus que les autres utilisateurs, automatisera l'exécution des tâches d'administration en écrivant des procédures, des scripts.

2. Avantages du Linux (Unix)



- Le logiciel libre est un mouvement qui se distingue très clairement du logiciel propriétaire.
- Les enjeux de ce changement de philosophie sont larges :
 - Économie,
 - Politique,
 - Sécurité,
 - Stratégie,
 - La disponibilité du code source,
 - La philosophie de partage de connaissances;
 - La communauté très dynamique sont des atouts de taille pour que le logiciel libre tienne tête au logiciel propriétaire.

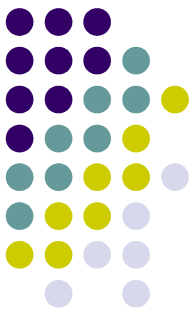
2. Avantages du Linux (Unix) (suite)



- Le prix d'achat n'est pas le seul coût à considérer, il y a aussi :
 - l'installation
 - la prise en main (migration et formation des utilisateurs)
 - l'entretien (mise à jour, maintenance)
 - les coûts impliqués pour la sécurité
 - indépendance par rapport au constructeur

0.2. commandes de base et éditeurs

A. Commandes de base

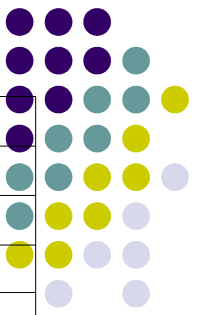


1	adduser Ajout d'un nouvel utilisateur
2	arp Affichage de la table de conversion des adresses MAC
3	catman Mise à jour de la base apropos
4	cd Changement de répertoire
5	chgrp Modification du groupe propriétaire d'un fichier
6	chmod Changement des permissions d'accès sur un fichier
7	chown Modification du propriétaire d'un fichier
8	clear Effacement de l'écran
9	cp Copie de fichiers
10	crontab Execution de commandes à intervalles réguliers
11	date Date et heure du système
12	df Affiche l'espace libre sur support de données
13	du Affiche l'espace occupé par des fichiers pour chaque répertoire
14	dump Sauvegarde des fichiers
15	echo Affiche un texte
16	exit Quitter le shell actuel
17	fdisk Modifie la table de partitions, changement des partitions d'un disque dur
18	find Recherche recursive de fichiers dans un répertoire
19	fsck Contrôle les secteurs défectueux dans un système de fichiers
20	groupadd Ajout d'un groupe
21	groupdel Suppression d'un groupe
22	gzip (De)Comprime les fichiers portant l'extension .gz
23	hostname Fixe ou affiche le nom de l'hôte
24	ifconfig Affiche/configure les interfaces réseau et série (eth, ppp, l) disponibles
25	ifdown Arrête une interface réseau ou série

Les commandes shell UNIX ne sont pas toujours faciles à retenir, mais elles sont tellement pratiques. Une fois que vous connaissez le nom et la fonction de base, man vous aidera pour le reste.



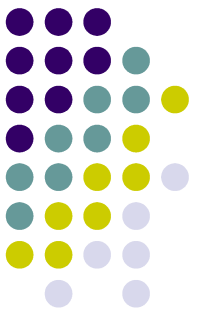
27	iptables le module de filtrage (firewall) des noyaux 2.4
28	kill Envoie des signaux aux processus
29	killall Envoie un signal de fin d'exécution au processus indiqué
30	less Affiche un texte (possibilité de déplacement, de recherche, etc.)
31	ln Crée un lien vers un fichier
32	locate Retrouve rapidement le chemin pour parvenir à un fichier d'après une partie ou l'intégralité de son nom entier
33	logname Affichage du nom d'utilisateur
34	ls Affiche le contenu du répertoire courant
35	lsmod Affiche les modules chargés en mémoire
36	mail Envoi et réception d'e-mail
37	man Affiche de l'aide en ligne
38	mkdir Crée un repertoire
39	mount Montage système de fichier
40	mv Déplace ou renomme un fichier
41	netstat Affiche des infos sur la configuration réseau
42	nslookup Affiche des informations sur la résolution de nom via DNS
43	passwd Change de mot de passe
44	ps Affiche la liste des processus
45	pwd Affiche le chemin courant
46	quotacheck Vérifie les quotas disque
47	quotaon Active les quotas disque
48	quotaoff Désactive les quotas disque



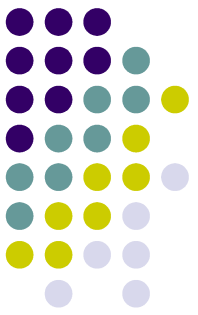
49	reboot Redémarrage
50	rm Efface un fichier
51	shutdown Arrête le système (-h now ou -r 2)
52	startx Démarre le serveur X
53	su Changement d'utilisateur
54	sudo Permet d'exécuter des commandes en tant que super-utilisateur
55	tac Affiche un fichier dans l'ordre inverse
56	tail Affichage de la dernière partie d'un fichier
57	tar Sauvegarde et archivage de fichiers
58	touch Permet de créer un fichier vide
59	traceroute Reconstitue la route qu'emprunte un paquet
60	type Affiche le type du fichier
61	umount Démontage système de fichiers
62	uname Informations (processeur , version) système
63	updatedb Reconstitue la BD des positions de fichiers
64	useradd Ajout d'un nouvel utilisateur
65	userdel Suppression d'un utilisateur
66	vi Editeur texte vi

La liste n'est certes pas exhaustive, les autres commandes interviendront en pleine utilisation du système.

Introduction



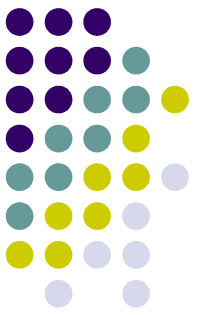
- Cet éditeur, peut être très utile en cas de non fonctionnement de l'interface graphique.
- La syntaxe pour lancer *Vi* est la suivante :
 - **vi nom_du_fichier**
- Une fois le fichier ouvert, il vous est possible de vous déplacer à l'aide des curseurs, et touches *h*, *j*, *k* et *l* .



Les modes de Vi

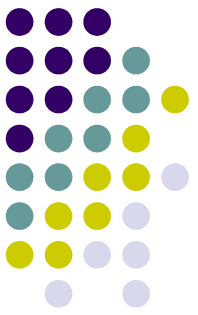
Vi possède 3 modes de fonctionnement :

- **Le mode normal:** mode par défaut, Il permet de taper des commandes
- **Le mode insertion:** Ce mode permet d'insérer les caractères que vous saisissez à l'intérieur du document.
- **Le mode de remplacement:** Ce mode permet de remplacer le texte existant par le texte que vous saisissez.



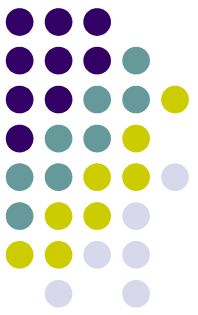
Les commandes de base

Commande	Description
:q	Quitte l'éditeur (sans sauvegarder)
:q!	Force l'éditeur à quitter sans sauvegarder (même si des modifications ont été apportées au document)
:wq	Sauvegarde le document et quitte l'éditeur
:filenom	Sauvegarde le document sous le <i>nom</i> spécifié



Les commandes d'édition

Commande	Description
x	Efface le caractère actuellement sous le curseur
dd	Efface la ligne actuellement sous le curseur
dxd	Efface x lignes à partir de celle actuellement sous le curseur
nx	Efface n caractères à partir de celle actuellement sous le curseur
x>>	Indente x lignes vers la droite à partir de celle actuellement sous le curseur
x<<	Indente x lignes vers la gauche à partir de celle actuellement sous le curseur

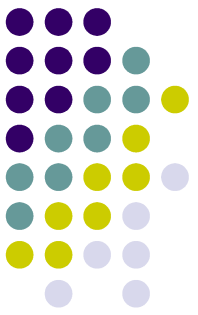


La recherche et le remplacement

- un mot dans un document
 - taper / suivi de la **chaîne à rechercher**, puis valider par la **touche entrée**.
exemple **/passwd** (valider) en mode normal.
- Pour remplacer une chaîne de caractère par une autre sur une ligne.
 - tapez **:s/chaine_a_remplacer/chaine_de_remplacement/** (nécessite d'être sur la ligne)

Il est possible de la généraliser à tout le document grâce à la syntaxe suivante :

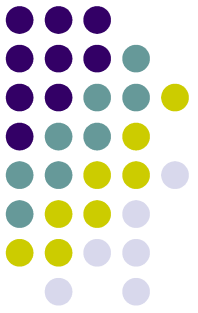
- **:%s/chaine_a_remplacer/chaine_de_remplacement/**



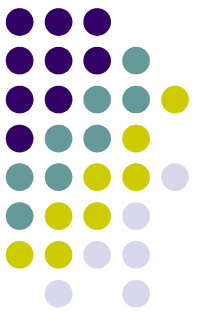
Le copier-coller et couper-coller

- taper la commande suivante pour **copier** *n* lignes :
 - nyy
 - exemple 3yy (copier 3 lignes)
- Pour coller la sélection, il suffit de taper la lettre *p*.
- taper la commande suivante pour **couper** *n* lignes : :
 - ndd
 - Puis *p* pour **coller**.

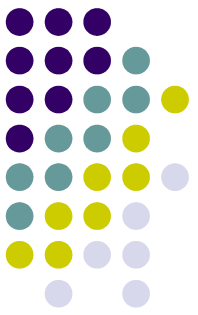
Mouvements du curseur



- `n|` Aller à la colonne `n`
- `Z` Entrée Positionner la ligne courante en haut de l'écran
- `0` ou `|` Place le curseur en début de ligne
- `^` ou `_` Place le curseur sur le premier caractère différent de l'espace et de la tabulation

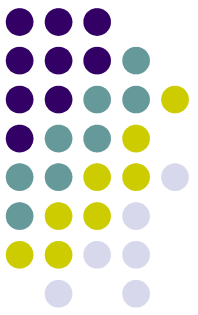


- \$ Place le curseur en fin de ligne
- H Place le curseur en première ligne de la fenêtre (HEAD)
- nH Place le curseur en nième ligne de la fenêtre en partant du haut
- M Place le curseur au milieu de la fenêtre fin de fichier



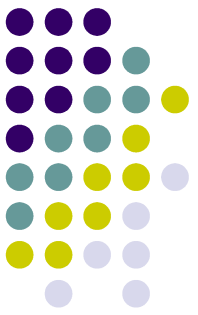
- L Place le curseur en dernière ligne de la fenêtre
- w Place le curseur sur le premier caractère du prochain mot à droite
- b Place le curseur sur le premier caractère du mot courant puis du précédent mot à gauche

- e Place le curseur sur le dernier caractère du mot courant puis du prochain mot à droite
- W Place le curseur sur le premier caractère du prochain mot à droite
- B Place le curseur sur le premier caractère du mot courant puis du précédent mot à gauche
- E Place le curseur sur le dernier caractère du mot courant puis du prochain mot à droite



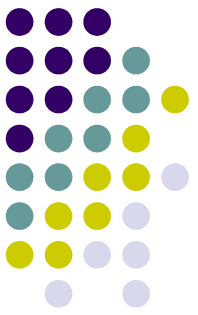
0.2. commandes de base et éditeurs

B. les éditeurs (vi et nano)



L'éditeur nano

- nano est un éditeur petit, sympathique et libre, qui vise à remplacer Pico, l'éditeur par défaut du logiciel non libre Pine. nano ne se contentant pas de copier l'interface et l'ergonomie de Pico, il offre également certaines fonctions manquantes (ou désactivées par défaut) dans Pico.
- Ces fonctionnalités sont, par exemple, les fonctions de recherche et de remplacement, et la possibilité de sauter directement à une ligne et à une colonne précise.
- A vos claviers : ouvrez une console et tapez nano



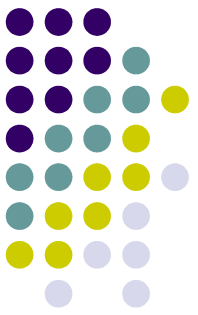
0.3. Manipulation des fichiers et répertoires

Exercices pratiques:

- Énoncé1
- Énoncé2
- Énoncé3
- Énoncé4
- Énoncé5

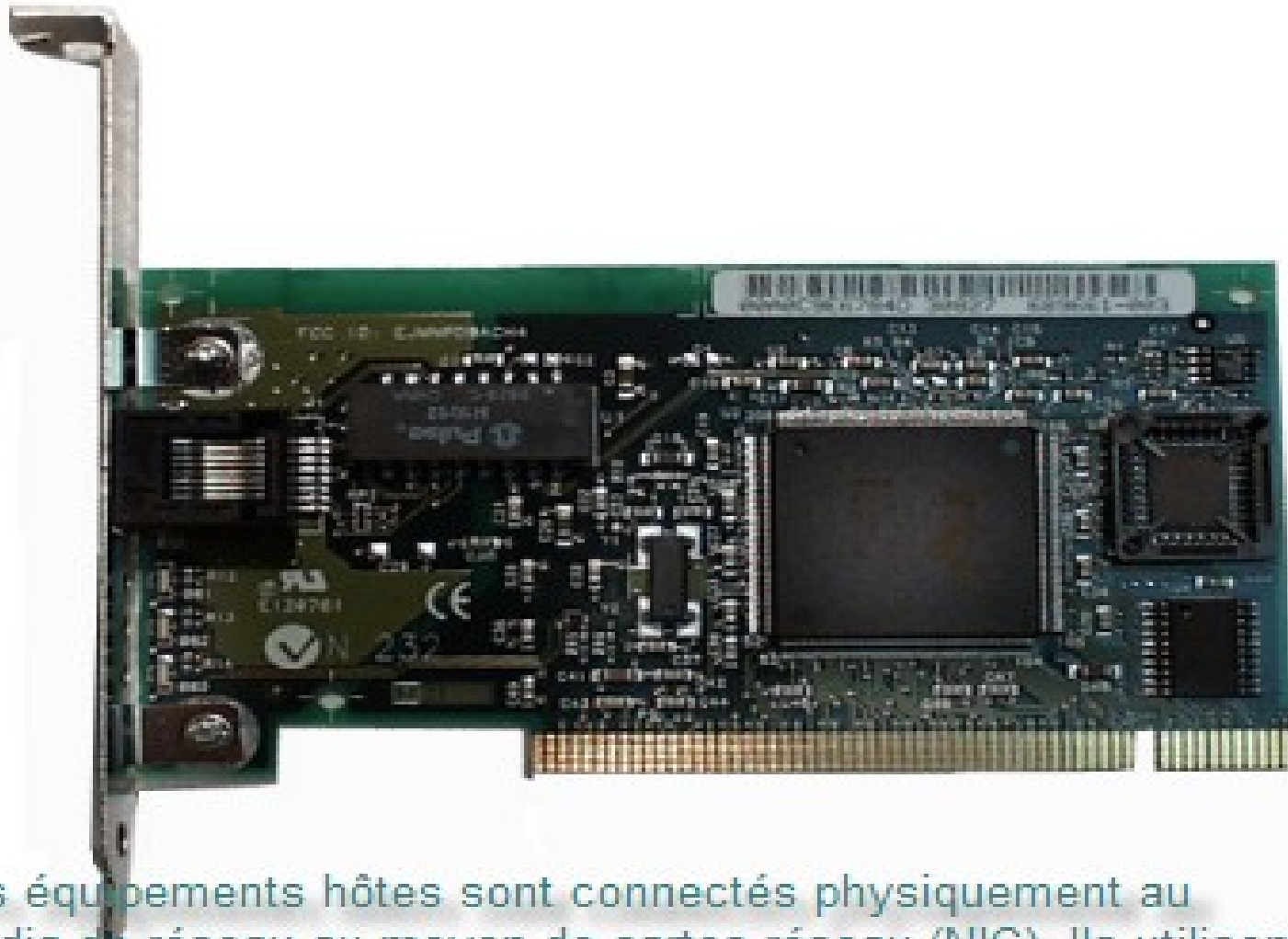
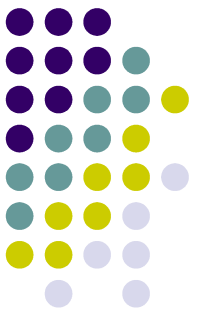
Chap. 1. Généralités des réseaux

1.1. Equipements de réseau



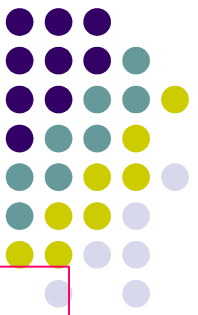
Equipement de l'utilisateur final

Equipements de réseau (suite)



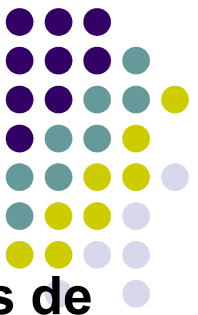
Les équipements hôtes sont connectés physiquement au média de réseau au moyen de cartes réseau (NIC). Ils utilisent cette connexion pour envoyer du courrier électronique, imprimer des rapports, numériser des images ou accéder à des bases de données.









Equipements de réseau (suite)



Une carte réseau est une carte de circuits imprimés qui se loge dans le connecteur d'extension d'un bus sur la carte mère d'un ordinateur. Elles existent également sous forme de périphérique. On emploie également le terme d'adaptateur réseau. Sur les ordinateurs portables, la carte réseau a généralement la taille d'une carte PCMCIA.

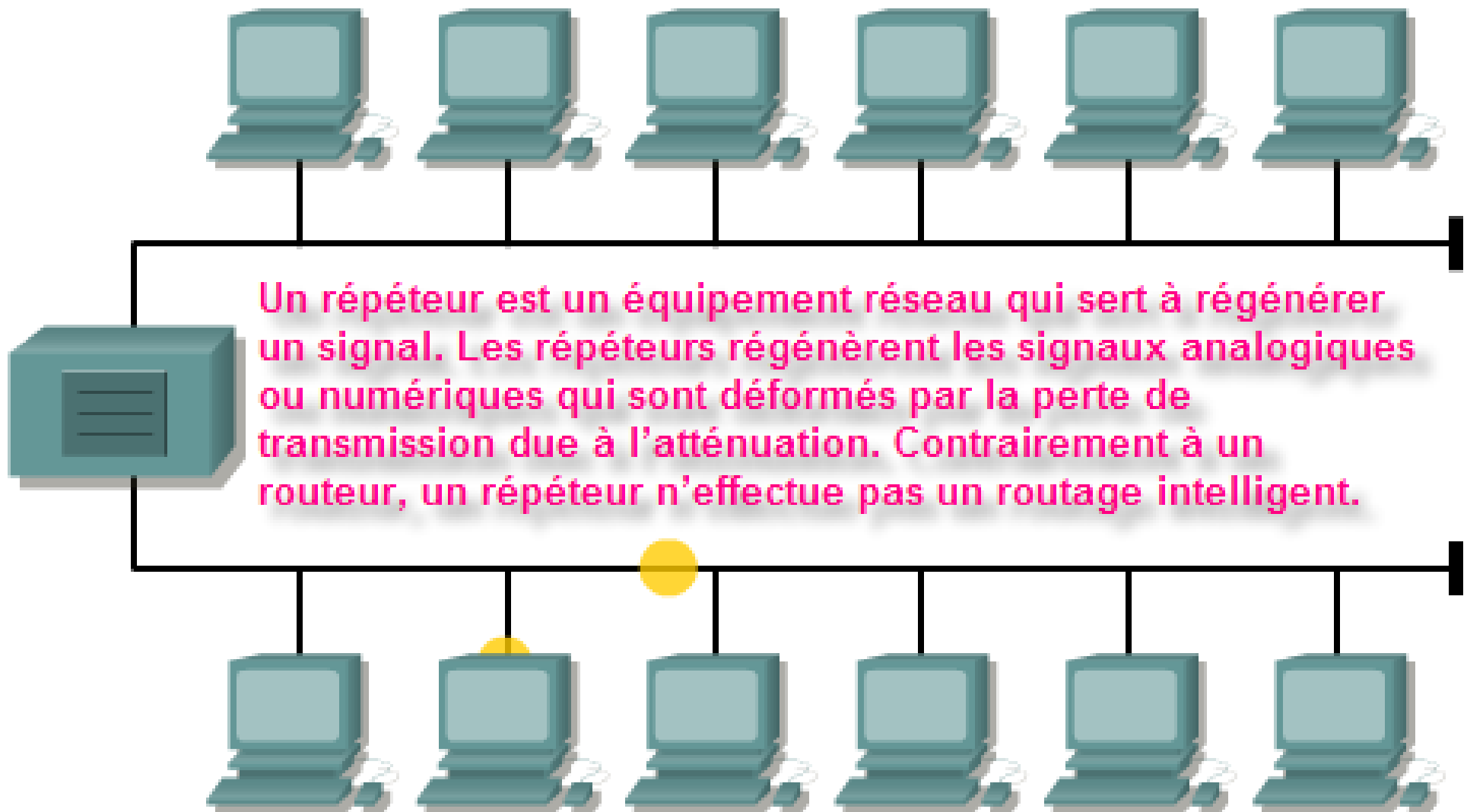
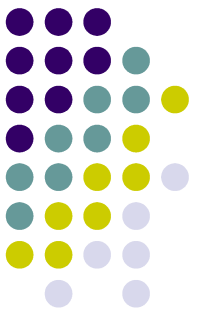
Équipements de réseau (suite)

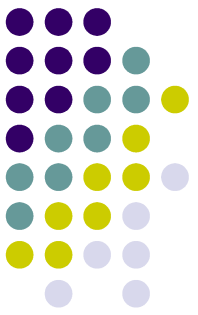


Équipements réseau	
Répéteur 	Pont 
Concentrateur 10BaseT 	Commutateur de groupe de travail 
Concentrateur 100BaseT 	Routeur 
Concentrateur 	Nuage réseau 

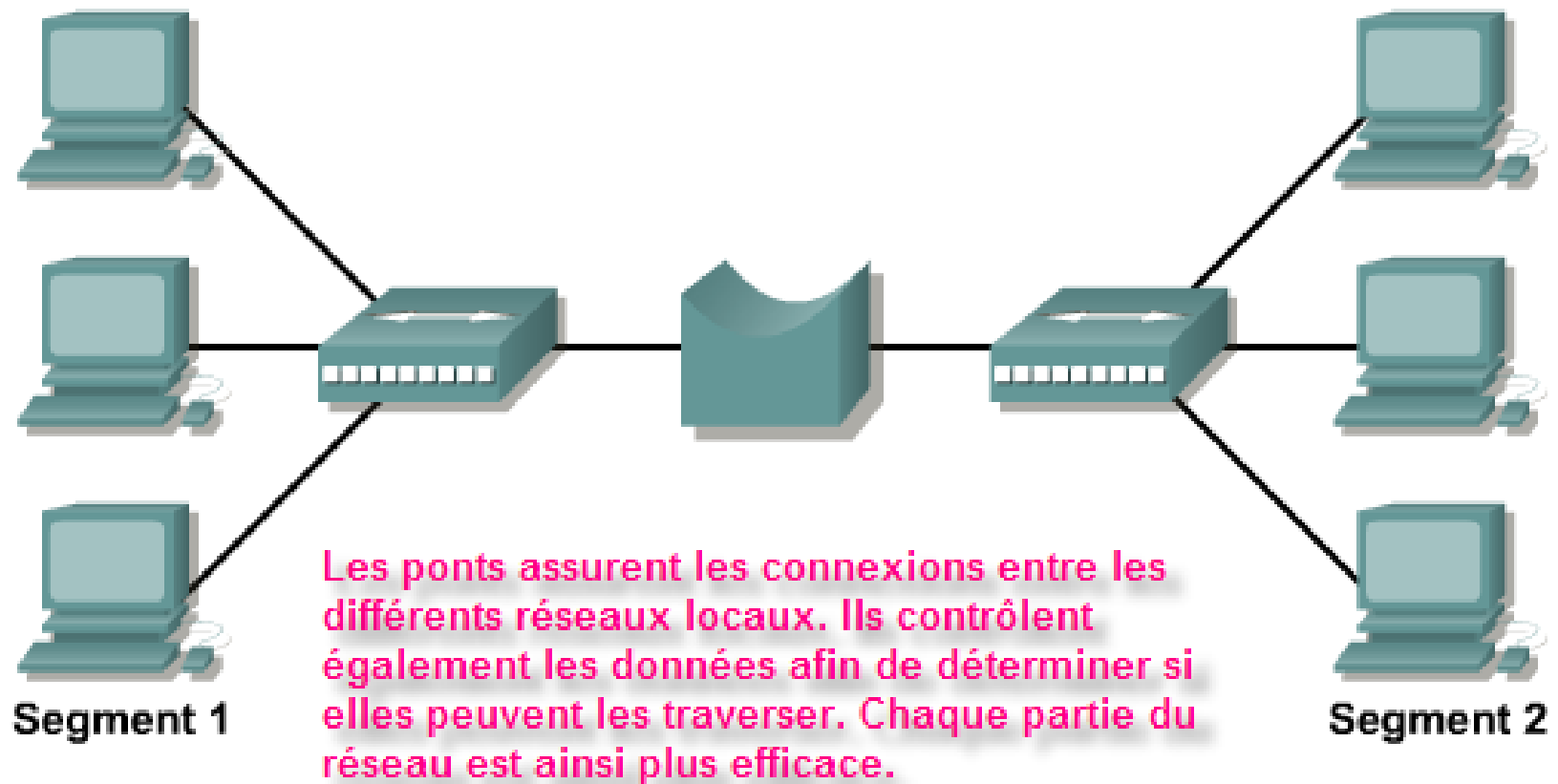
Les équipements de réseau sont utilisés pour étendre les connexions de câbles, concentrer les connexions, convertir les formats de données et gérer les transferts de données. Les répéteurs, concentrateurs, ponts, commutateurs et routeurs sont des exemples d'équipements qui assurent ces fonctions.

Equipements de réseau (suite)

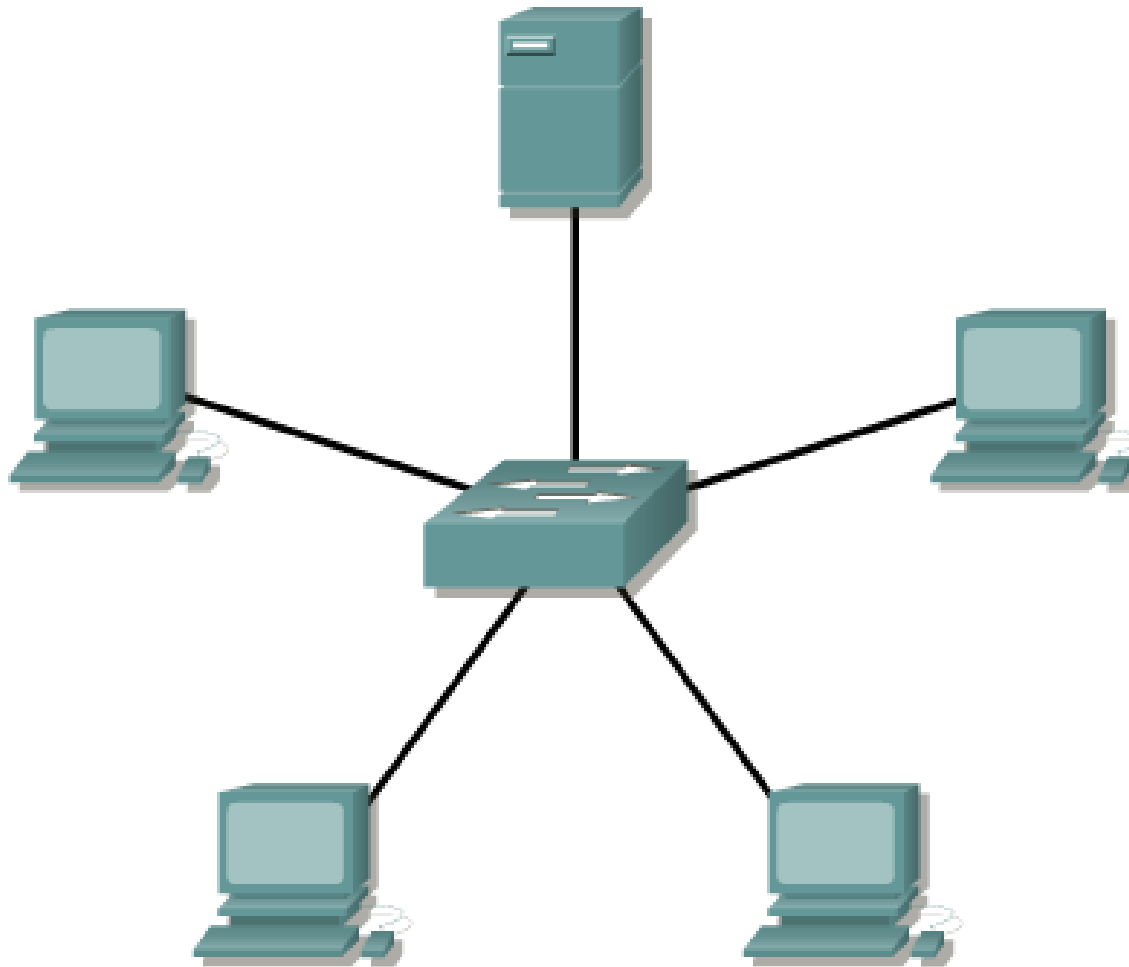
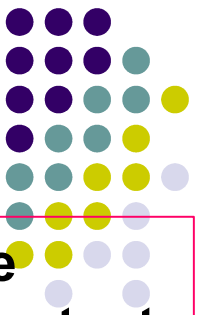




Equipements de réseau (suite)

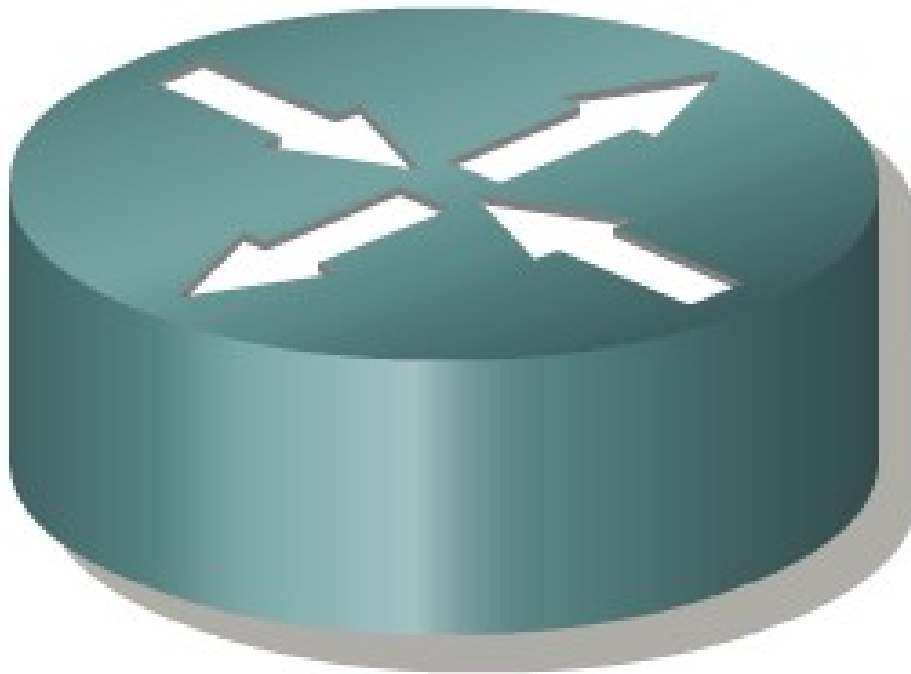
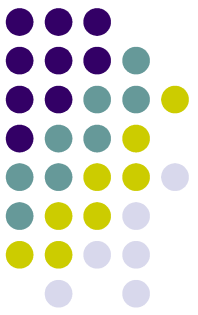


Equipements de réseau (suite)



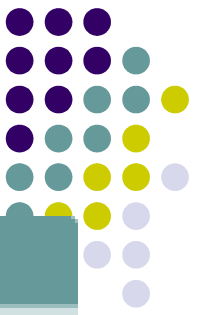
Les commutateurs de groupe de travail apportent de l'intelligence à la gestion du transfert des données. Ils sont capables de déterminer si les données doivent rester sur un réseau local et de ne les transférer que vers la connexion qui en a besoin. Une autre différence entre un pont et un commutateur réside dans le fait qu'un commutateur ne convertit pas les formats de transmission de données.

Equipements de réseau (suite)



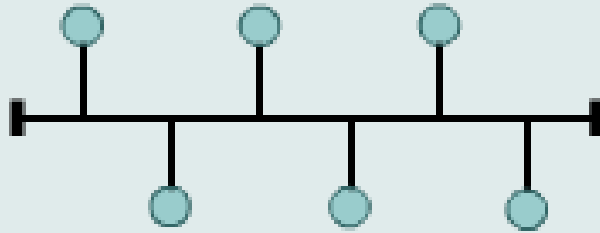
Les routeurs offrent l'ensemble des capacités précédemment citées. Les routeurs peuvent régénérer les signaux, concentrer plusieurs connexions, convertir les formats de transmission de données et gérer les transferts de données. Ils peuvent également se connecter à un réseau étendu, ce qui leur permet d'interconnecter des réseaux locaux séparés par de grandes distances. Aucun des autres équipements ne peut fournir ce type de connexion.

1.2. Topologie des réseaux

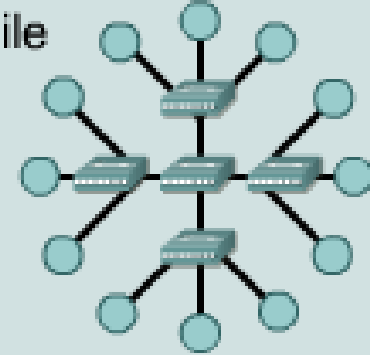


Topologies physiques

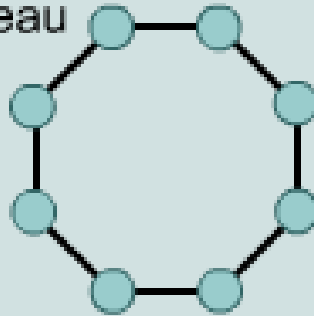
Topologie en anneau
bus



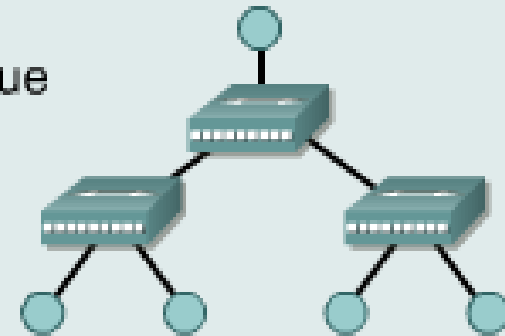
Topologie en étoile
étendue



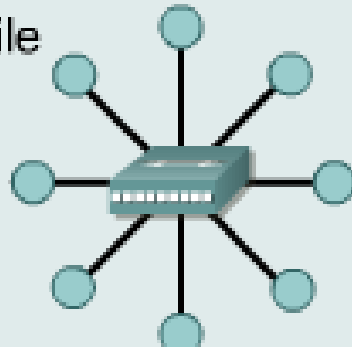
Topologie en anneau



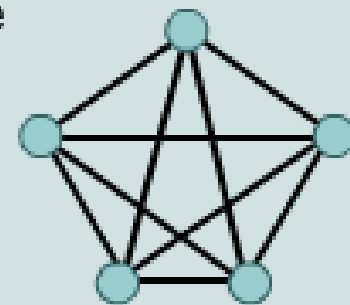
Topologie
hiérarchique



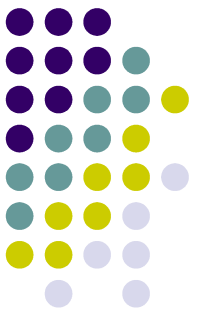
Topologie en étoile



Topologie maillée



1.2.1. *Topologie physique*



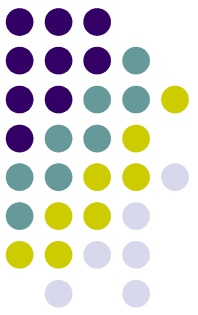
- La topologie réseau définit la structure du réseau. La topologie est définie en partie par la topologie physique, qui est la configuration proprement dite du câblage ou du média. L'autre partie est la topologie logique, qui définit de quelle façon les hôtes accèdent aux médias pour envoyer des données. Les topologies physiques couramment utilisées sont les suivantes:
 - Une topologie de bus fait appel à un câble de backbone unique qui est terminé aux deux extrémités. Tous les hôtes se connectent directement à ce backbone.
 - Dans une topologie en anneau, chaque hôte est connecté à son voisin. Le dernier hôte se connecte au premier. Cette topologie crée un anneau physique de câble.
 - Dans une topologie en étoile, tous les câbles sont raccordés à un point central.

1.2.1. Topologie physique (suite)



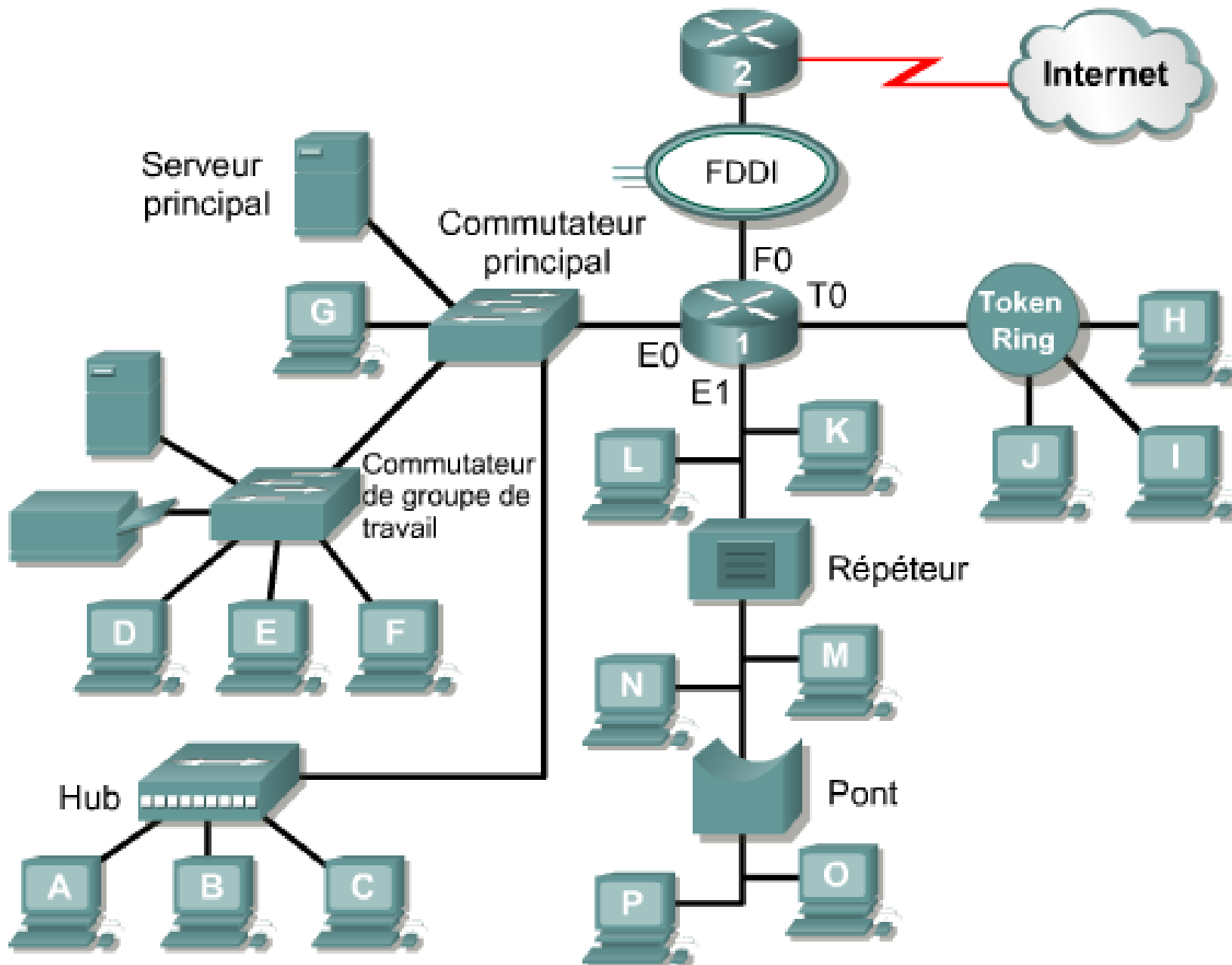
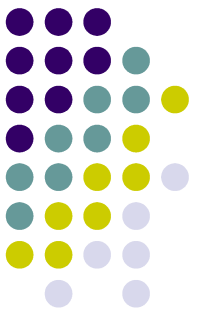
- Une topologie en étoile étendue relie des étoiles individuelles en connectant les concentrateurs ou les commutateurs. Cette topologie peut étendre la portée et la couverture du réseau.
- Une topologie hiérarchique est similaire à une topologie en étoile étendue. Cependant, plutôt que de lier les concentrateurs ou commutateurs ensemble, le système est lié à un ordinateur qui contrôle le trafic sur la topologie.
- On implémente une topologie maillée afin de garantir une protection maximale contre l'interruption de service. Par exemple, une topologie maillée représente une solution idéale pour les systèmes de contrôle en réseau d'une centrale nucléaire. Comme vous pouvez le voir dans le schéma, chaque hôte possède ses propres connexions à tous les autres hôtes. Bien qu'Internet emprunte de multiples chemins pour atteindre un emplacement, il n'adopte pas une topologie complètement maillée.

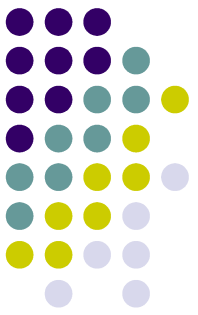
1.2.2. Topologie logique



- La topologie logique d'un réseau détermine de quelle façon les hôtes communiquent sur le média. Les deux types de topologie logiques les plus courants sont le broadcast et le passage de jeton.
 - L'utilisation d'une topologie de broadcast indique que chaque hôte envoie ses données à tous les autres hôtes sur le média du réseau. Les stations peuvent utiliser le réseau sans suivre un ordre déterminé. Ethernet fonctionne ainsi.
 - La deuxième topologie logique est le passage de jeton. Dans ce type de topologie, un jeton électronique est transmis de façon séquentielle à chaque hôte. Dès qu'un hôte reçoit le jeton, cela signifie qu'il peut transmettre des données sur le réseau. Si l'hôte n'a pas de données à transmettre, il passe le jeton à l'hôte suivant et le processus est répété. Token Ring et FDDI (*Fiber Distributed Data Interface*) sont deux exemples de réseaux qui utilisent le passage de jeton. Arcnet est une variante de Token Ring et de FDDI. Il s'agit d'un passage de jeton sur une topologie de bus.

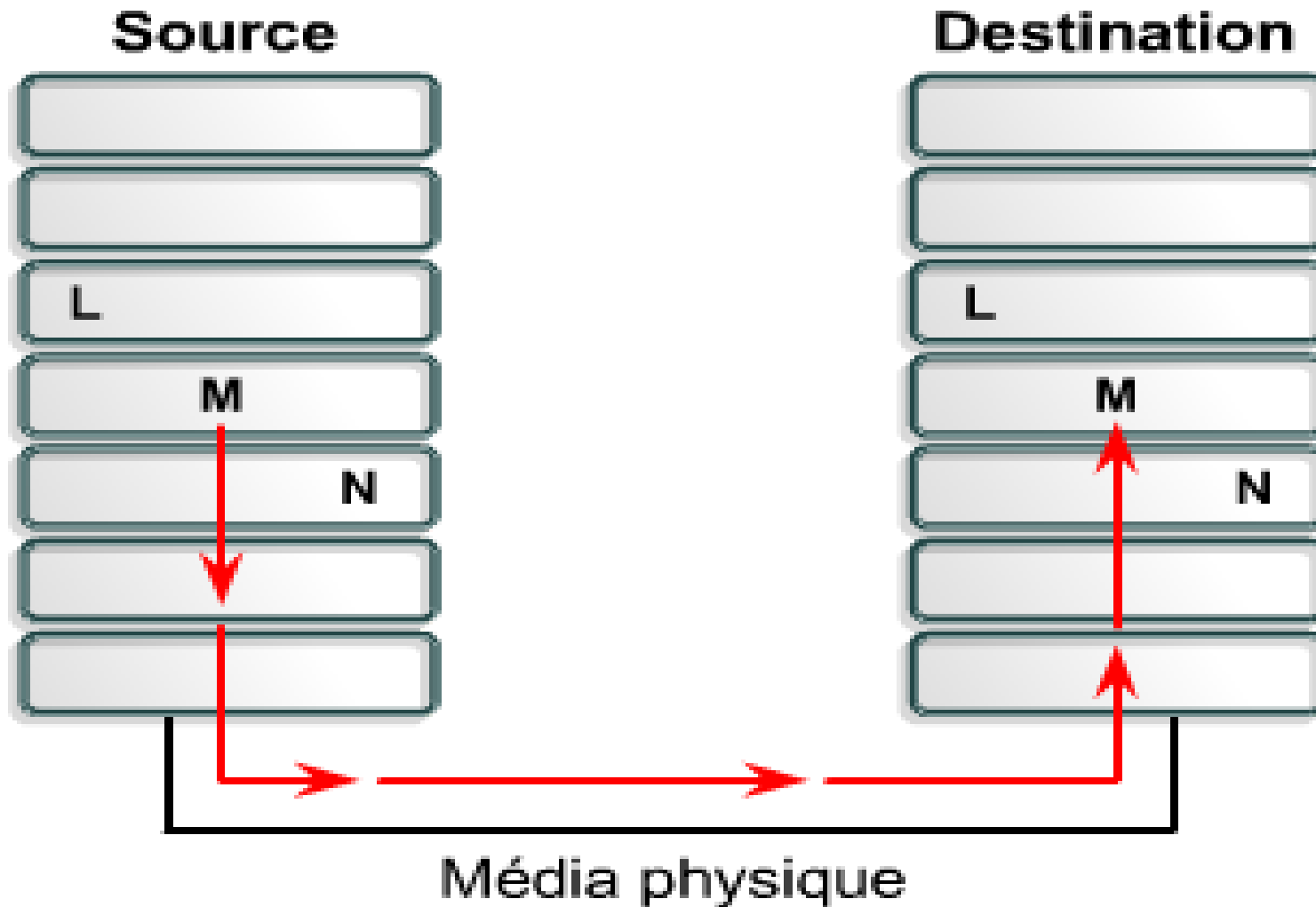
1.2.2. Topologie logique (suite)





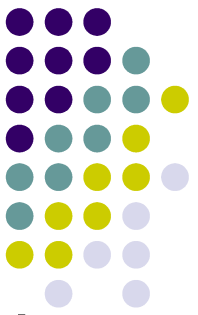
1.3. *Protocoles de réseau*

Protocoles de communication entre ordinateurs



1.3. *Protocoles de réseau*

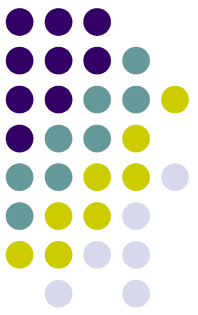
Protocoles de communication entre ordinateurs (suite)



- Les suites de protocoles sont des ensembles de protocoles qui permettent à des hôtes de communiquer sur un réseau. Un protocole est une description formelle d'un ensemble de règles et de conventions qui régissent un aspect particulier de la façon dont les équipements communiquent sur un réseau. Les protocoles déterminent le format, la chronologie, le séquençage et le contrôle d'erreur dans la communication de données. Sans protocole, l'ordinateur ne peut pas constituer ou reconstruire dans le format original le flux de bits entrants provenant d'un autre ordinateur.

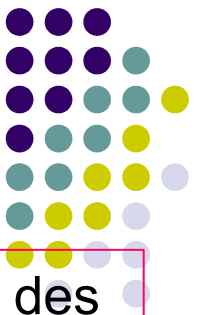
1.3. *Protocoles de réseau*

Protocoles de communication entre ordinateurs (suite)



- Les protocoles contrôlent tous les aspects de la communication de données, dont:
 - Comment est construit le réseau physique
 - Comment les ordinateurs se connectent au réseau
 - Comment les données sont formatées pour la transmission
 - Comment ces données sont envoyées
 - Comment traiter les erreurs

1.4. Modèle OSI

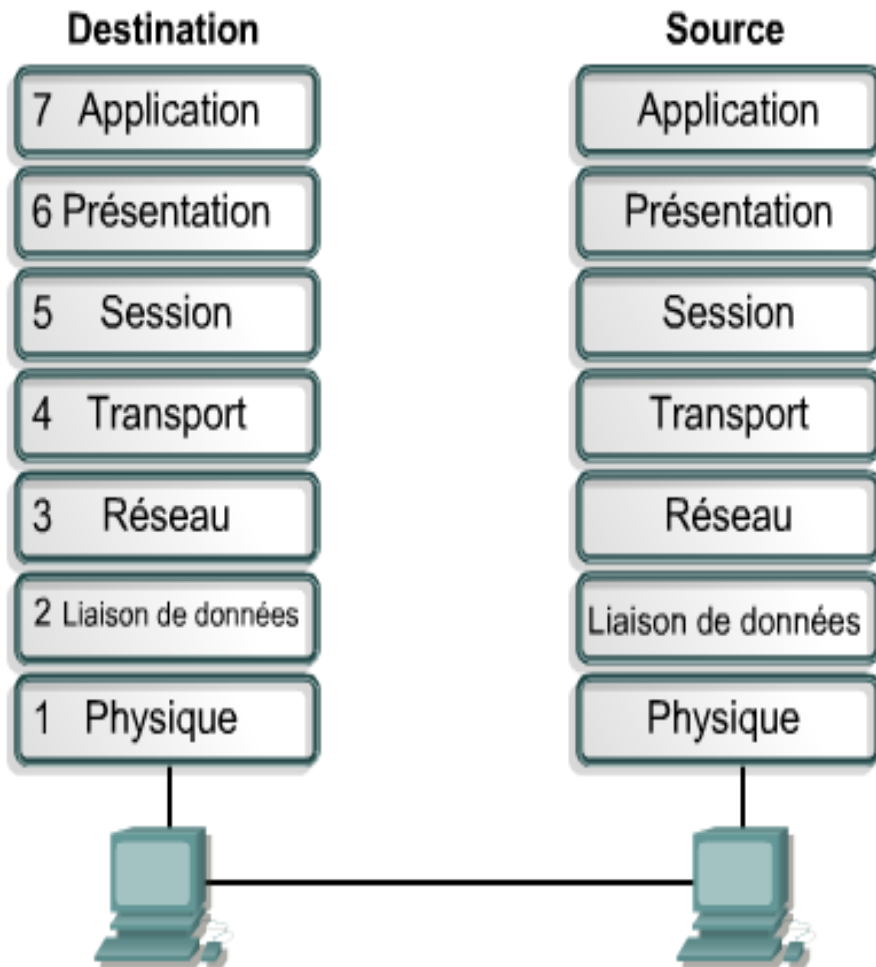
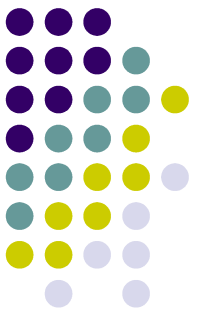


Pour résoudre le problème de l'incompatibilité des réseaux, l'ISO (International Organization for Standardization) examina les modèles réseau tels que DECnet (Digital Equipment Corporation net), SNA (Systems Network Architecture) et TCP/IP afin de trouver un ensemble de règles applicable de façon générale à tous les réseaux. Sur la base de ces recherches, l'ISO a mis au point un modèle de réseau pour aider les fournisseurs à créer des réseaux compatibles avec d'autres réseaux.

Le modèle de référence OSI (Open System Interconnection) publié en 1984 fut le modèle descriptif de réseau créé par l'ISO. Ce modèle propose aux fournisseurs un ensemble de normes assurant une compatibilité et une interopérabilité accrues entre divers types de technologies réseau produites par de nombreuses entreprises à travers le monde.

1.4. Modèle OSI

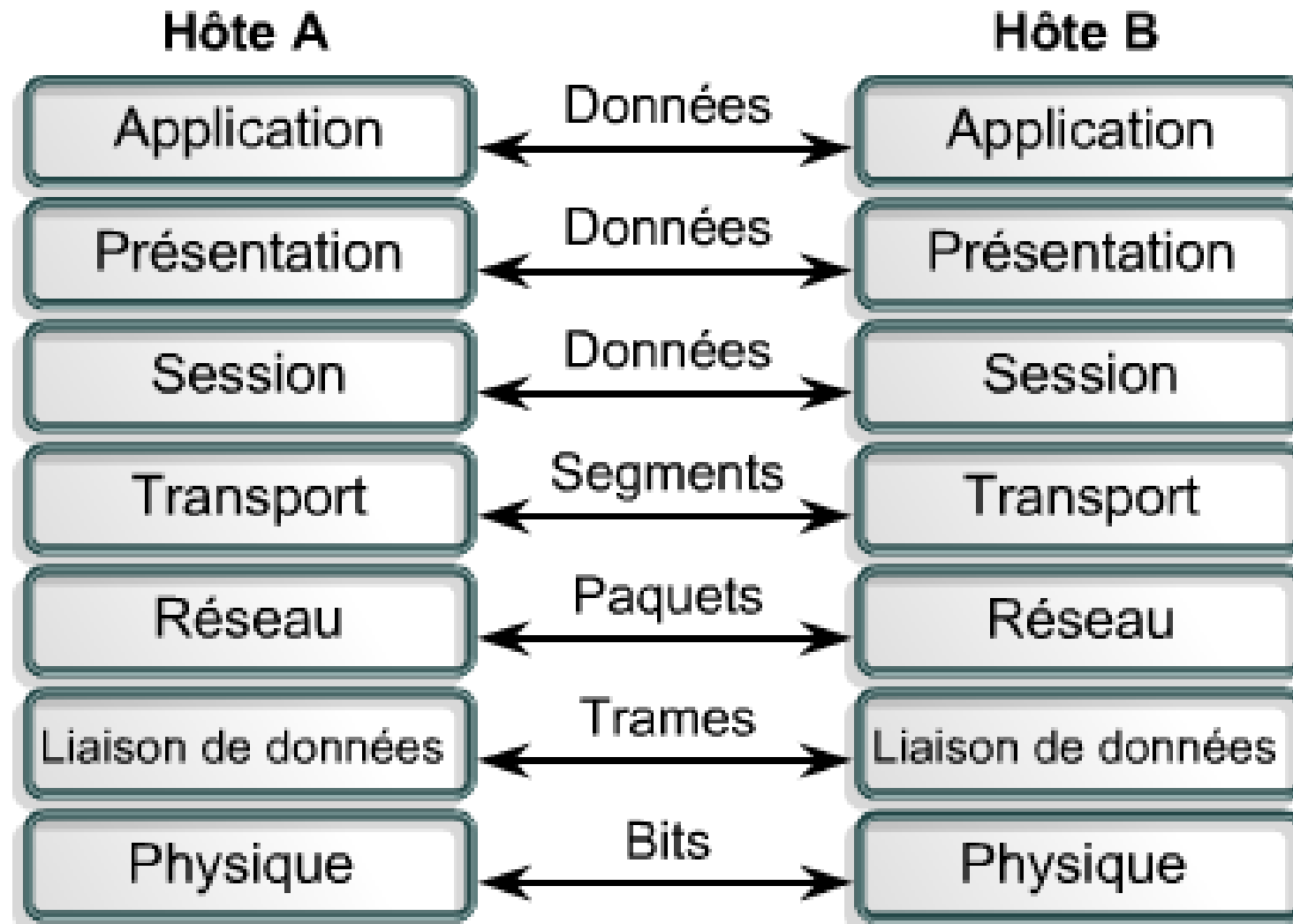
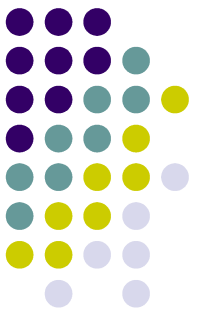
Communications d'égal à égal



Afin de permettre l'acheminement des données entre l'ordinateur source et l'ordinateur de destination, chaque couche du modèle OSI au niveau de l'ordinateur source doit communiquer avec sa couche homologue sur l'ordinateur de destination. Cette forme de communication est appelée communication d'égal à égal. Au cours de ce processus, les protocoles de chaque couche s'échangent des informations, appelées unités de données de protocole (PDU). Chaque couche de communication, sur l'ordinateur source, communique avec l'unité de données de protocole propre à une couche, ainsi qu'avec la couche correspondante sur l'ordinateur de destination, comme l'illustre la figure

1.4. Modèle OSI

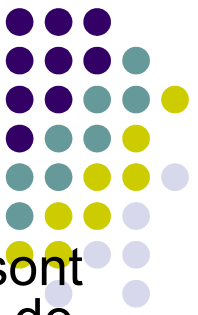
Communications d'égal à égal (suite)

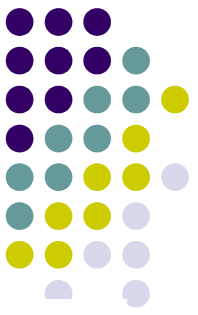


1.4. Modèle OSI

Communications d'égal à égal (suite)

- Dans un réseau, les paquets de données proviennent d'une source et sont acheminés vers une destination. Chaque couche dépend de la fonction de service de la couche OSI sous-jacente. Pour fournir ce service, la couche inférieure utilise l'encapsulation pour placer les PDU de la couche supérieure dans son champ de données. Elle ajoute ensuite les en-têtes et les en-queues de PDU nécessaires à l'exécution de sa fonction. Par la suite, à mesure que les données traversent les couches du modèle OSI, d'autres en-têtes et en-queues sont ajoutés. Dès que les couches 7, 6 et 5 ont ajouté leurs informations, la couche 4 en ajoute d'autres. Ce regroupement des données, ou unité de données de protocole de couche 4, est appelé segment.
- Ainsi, la couche réseau fournit un service à la couche transport, qui présente les données au sous-système de l'interréseau. La couche réseau est chargée de déplacer les données dans l'interréseau. Pour ce faire, elle encapsule les données et leur annexe un en-tête de manière à créer un paquet (soit la PDU de couche 3). L'en-tête contient les informations requises pour effectuer le transfert, notamment les adresses logiques de source et de destination.

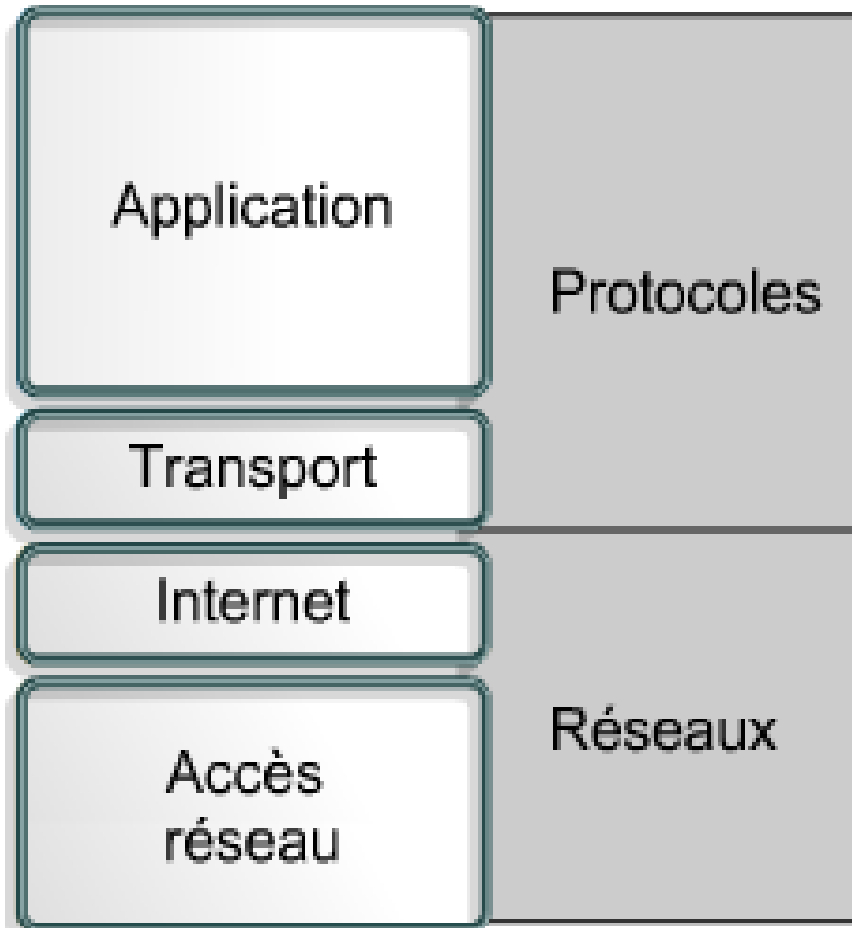




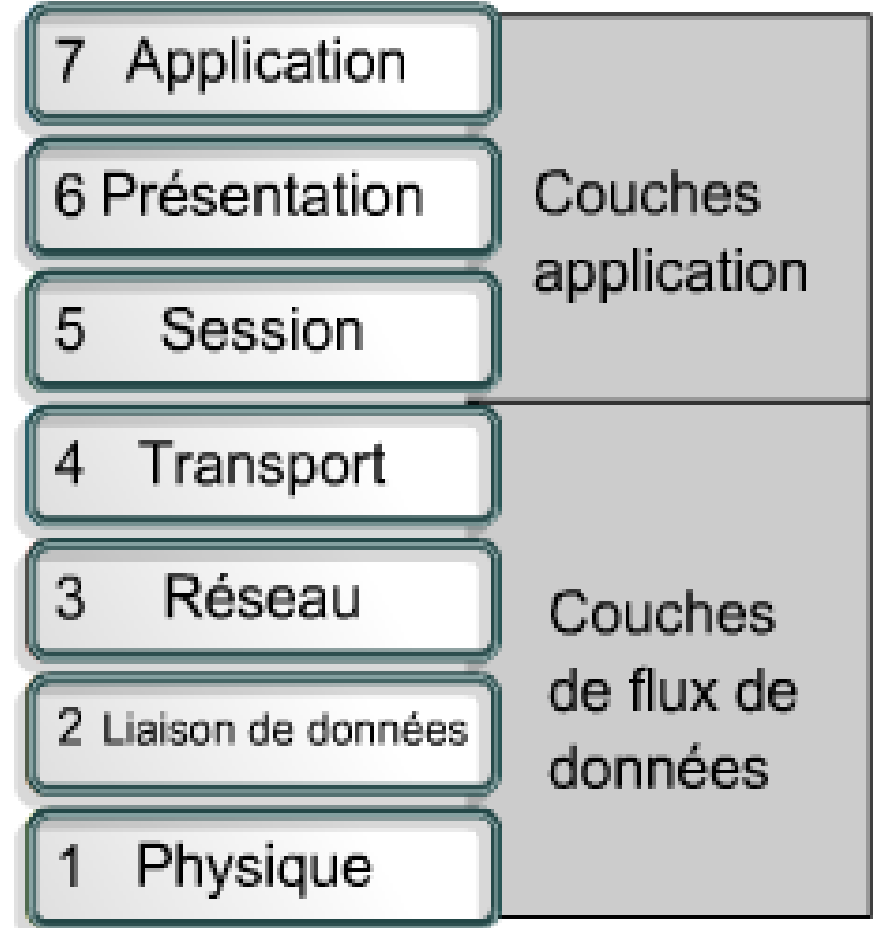
1.5. TCP/IP

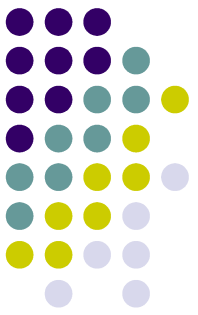
1.5.1. Comparaison entre OSI et TCP/IP

TCP/IP Modèle



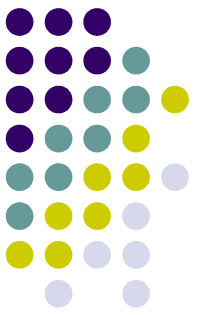
OSI Modèle





1.5.1. Comparaison entre OSI et TCP/IP (suite)

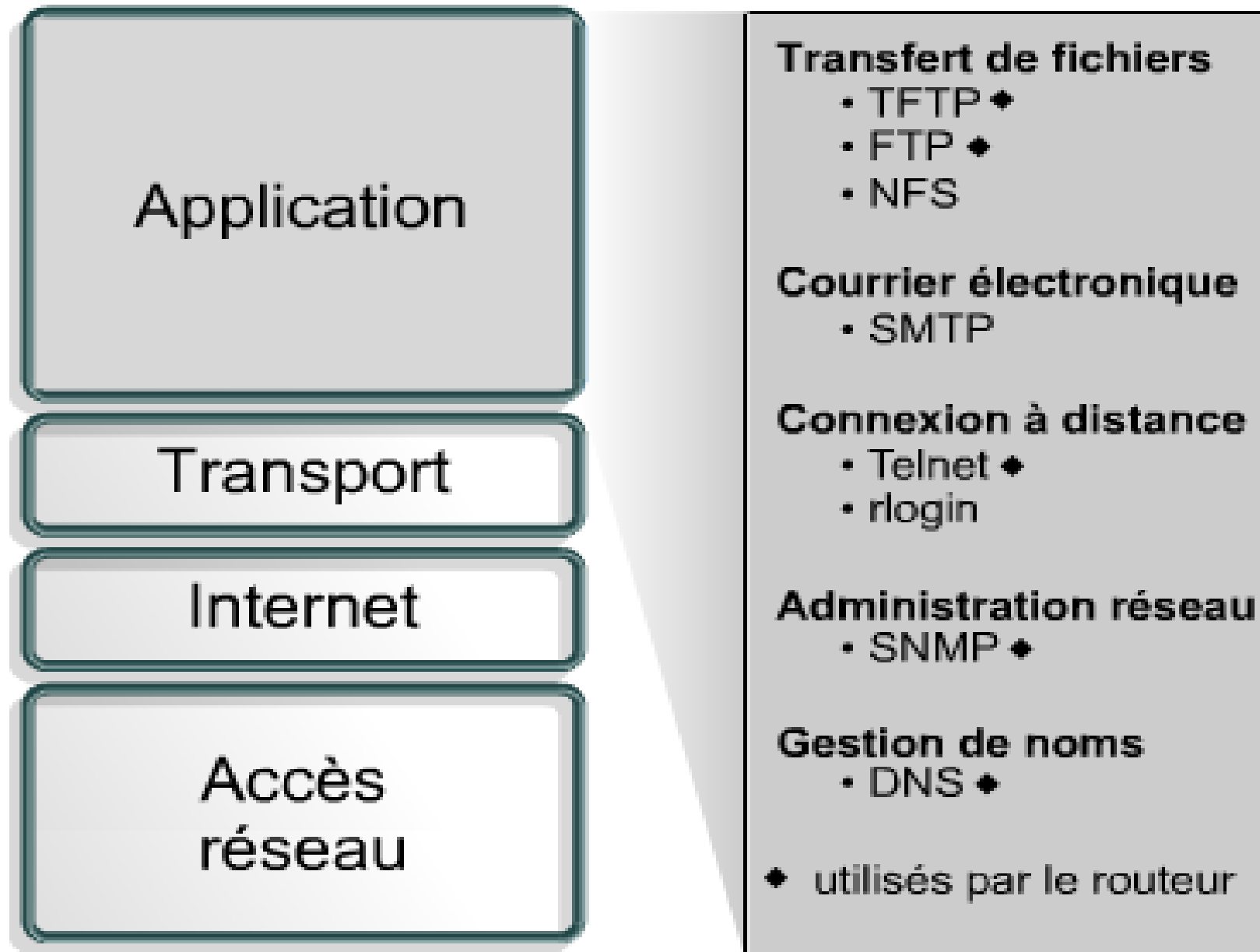
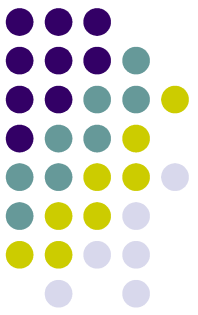
- Les modèles OSI et TCP/IP présentent un grand nombre de similitudes:
 - Tous deux comportent des couches.
 - Tous deux comportent une couche application, bien que chacune fournisse des services différents.
 - Tous deux comportent des couches réseau et transport comparables.
 - Tous deux s'appuient sur un réseau à commutation de paquets, et non sur un réseau à commutation de circuits.

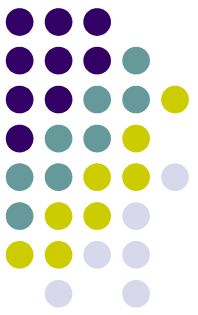


1.5.1. Comparaison entre OSI et TCP/IP (suite)

- Les professionnels des réseaux doivent connaître les deux modèles qui présentent également quelques différences:
 - TCP/IP intègre les couches application, présentation et session du modèle OSI dans sa couche application.
 - TCP/IP regroupe les couches physique et liaison de données du modèle OSI dans sa couche d'accès au réseau.
 - TCP/IP semble plus simple, car il comporte moins de couches.
 - Lorsque la couche transport du protocole TCP/IP utilise le protocole UDP, la transmission des paquets n'est pas fiable tandis qu'elle est toujours fiable avec la couche transport du modèle OSI.

A. Couche application (TCP/IP)

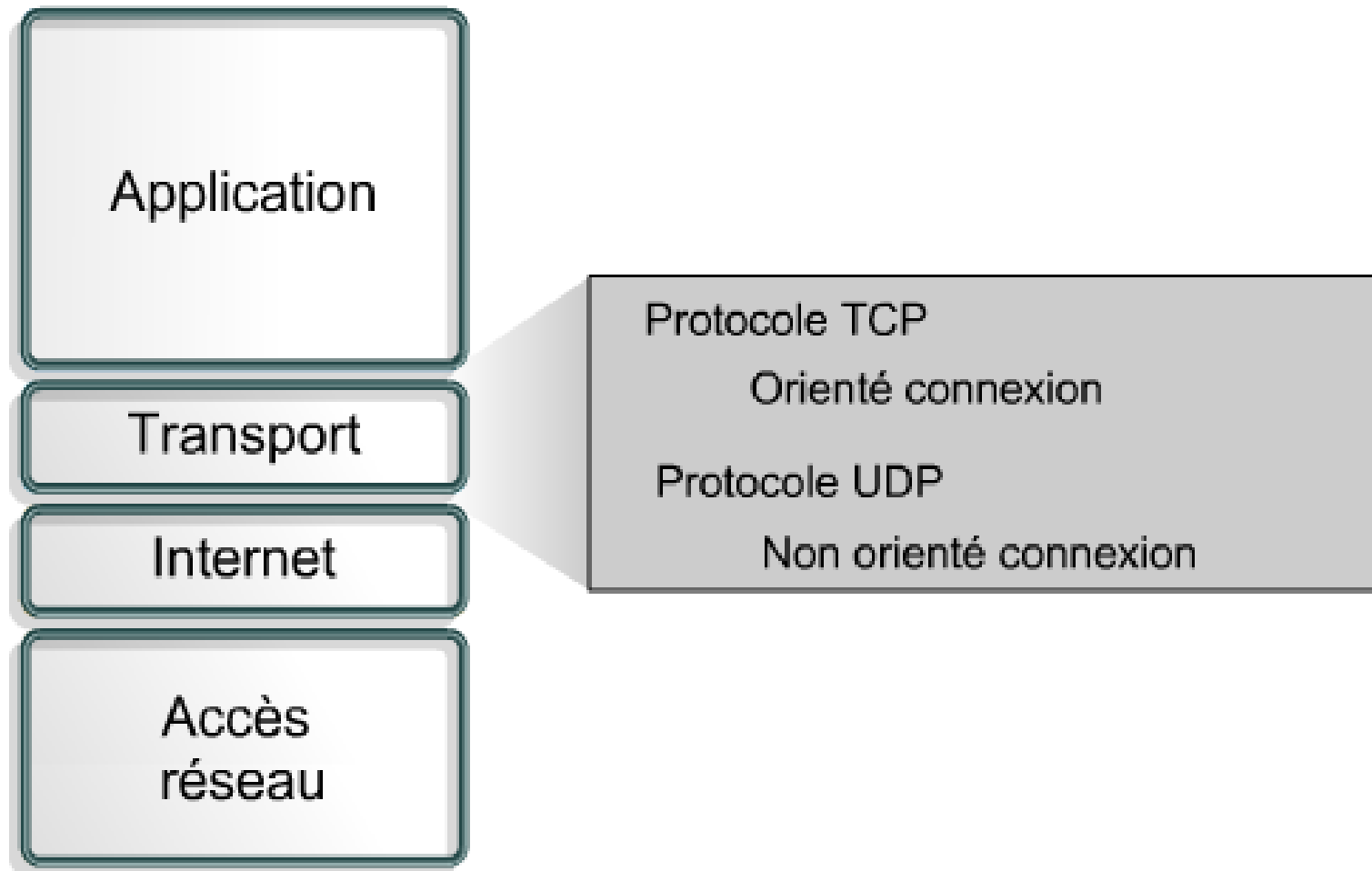
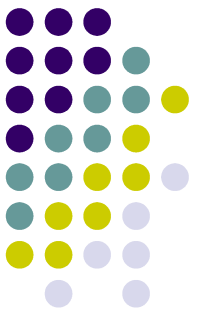




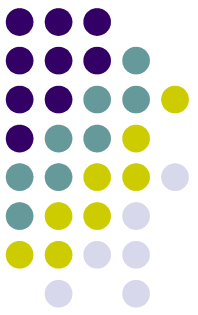
A. Couche application (TCP/IP) suite

- La couche application gère les protocoles de niveau supérieur, les représentations, le code et le contrôle du dialogue. La pile de protocoles TCP/IP regroupe en une seule couche la totalité des aspects liés aux applications et vérifie que les données sont préparées de manière adéquate pour la couche suivante. Le protocole TCP/IP contient des spécifications relatives aux couches transport et Internet, notamment IP et TCP, et d'autres relatives aux applications courantes. Outre la prise en charge du transfert de fichiers, du courrier électronique et de la connexion à distance, le modèle TCP/IP possède des protocoles prenant en charge les services suivants: (voire la figure page précédente)

B. Couche transport (TCP/IP)

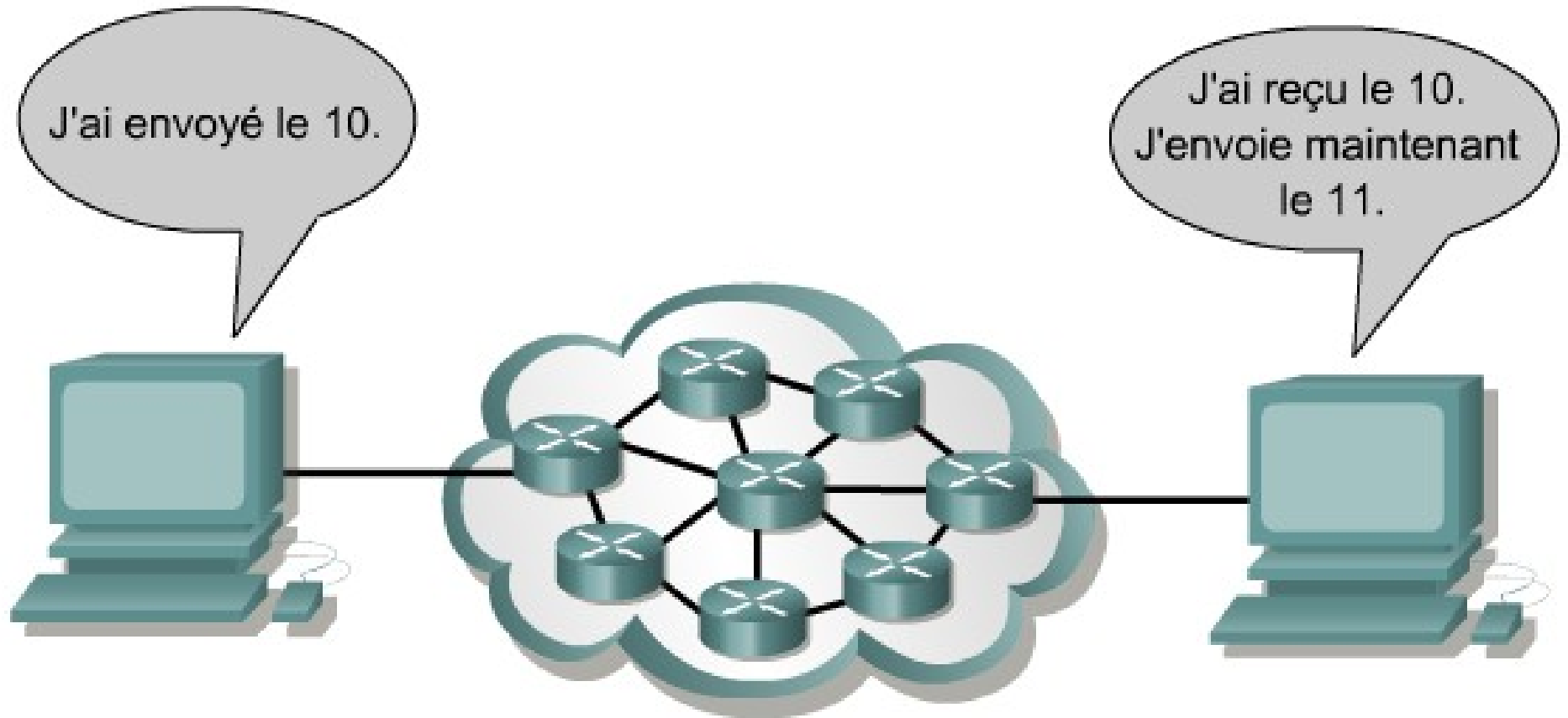
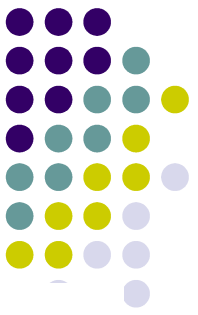


B. Couche transport (TCP/IP) suite

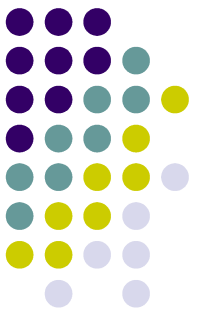


- La couche transport fournit une connexion logique entre les hôtes source et de destination. Les protocoles de transport segmentent et rassemblent les données envoyées par des applications de couche supérieure en un même flux de données, ou connexion logique, entre les deux points d'extrémité.

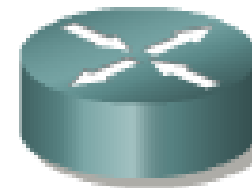
B. Couche transport (TCP/IP) suite



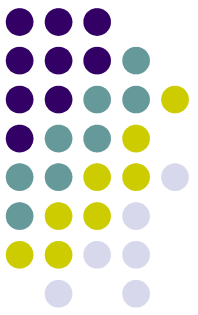
B. Couche transport (TCP/IP) suite



110001010101101100001010010101010

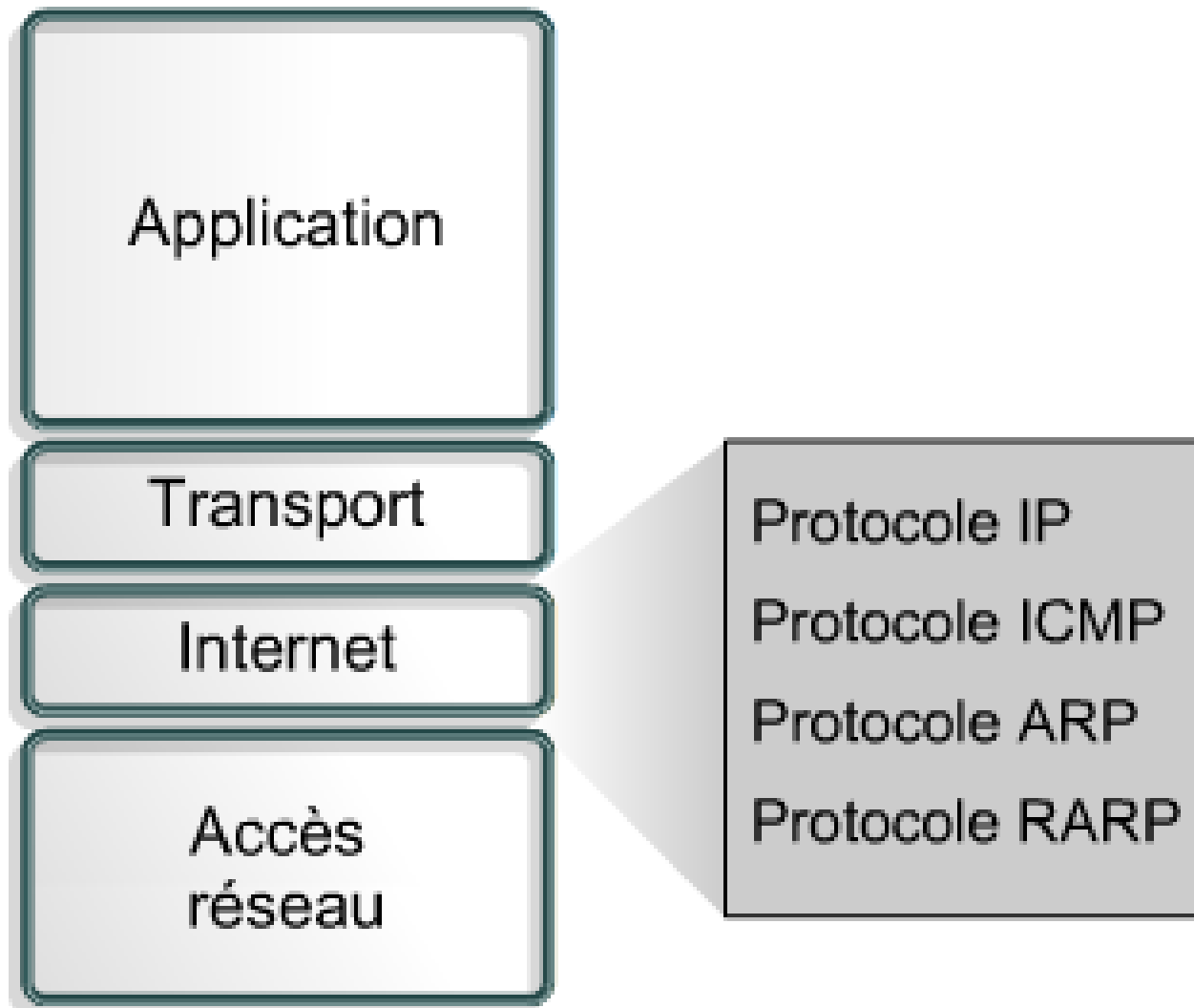
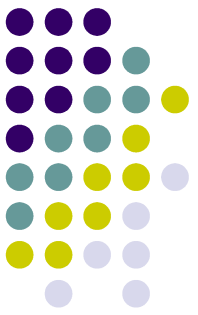


B. Couche transport (TCP/IP) suite

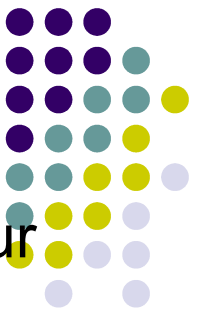


- Internet est souvent représenté par un nuage. La couche transport envoie des paquets de données d'une source à une destination à travers ce nuage.
Le rôle principal de la couche transport est d'assurer une fiabilité et un contrôle de bout en bout lors du transfert des données à travers ce nuage. Les fenêtres glissantes, les numéros de séquençage et les accusés de réception permettent d'obtenir ce résultat. La couche transport définit également une connectivité de bout en bout entre les applications hôtes. Les protocoles de la couche transport incluent les protocoles TCP et UDP.

C. Couche Internet (TCP/IP)

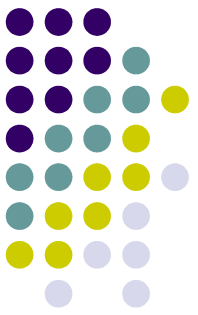


C. Couche Internet (TCP/IP) suite



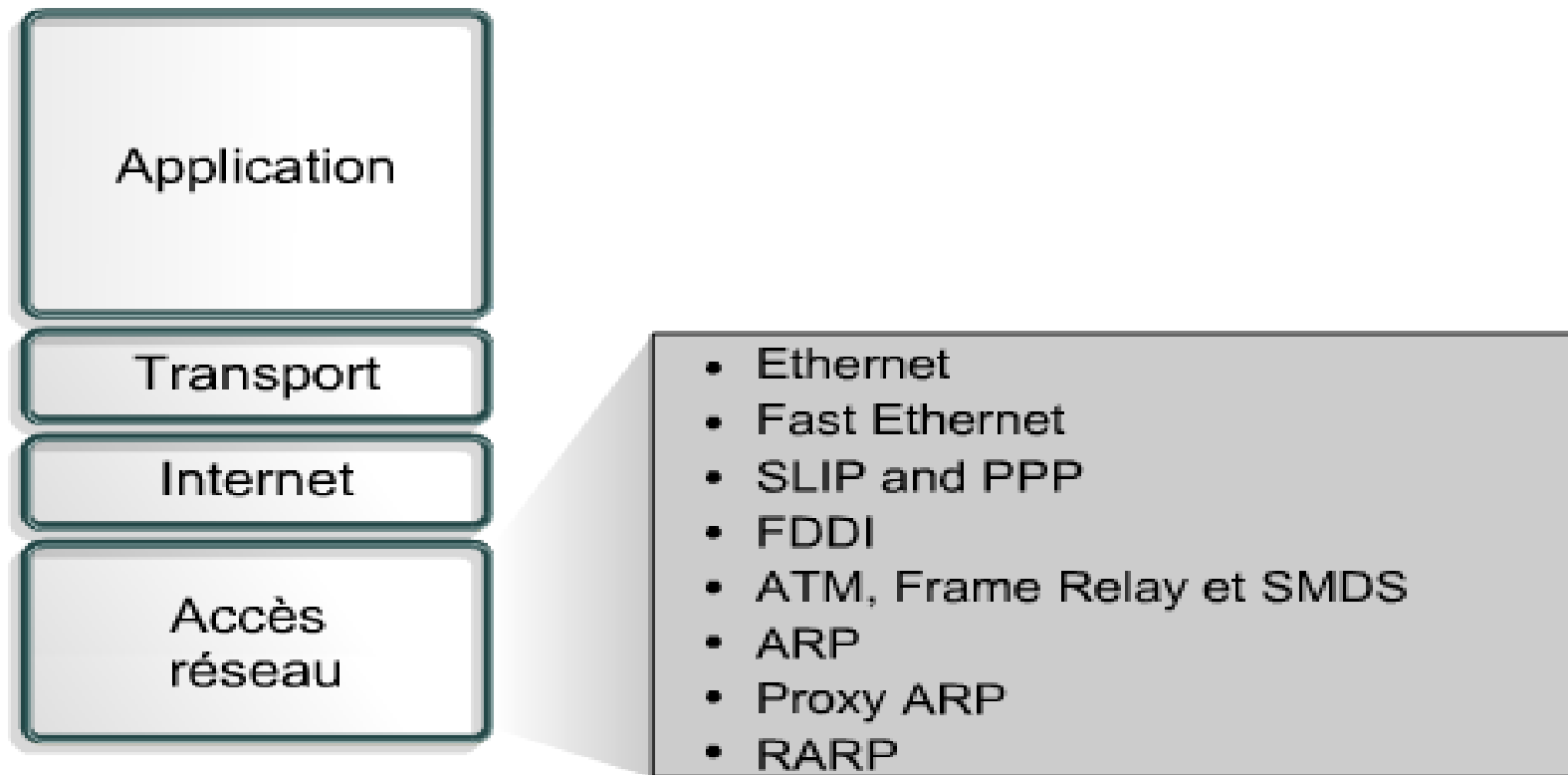
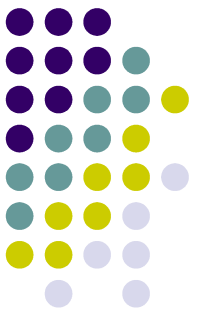
- Le rôle de la couche Internet consiste à sélectionner le meilleur chemin pour transférer les paquets sur le réseau. Le principal protocole de cette couche est le protocole IP. La détermination du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.
- Les protocoles ci-dessous s'exécutent au niveau de la couche Internet du protocole TCP/IP:
 - Le protocole IP assure l'acheminement au mieux (best-effort delivery) des paquets, non orienté connexion. Il ne se préoccupe pas du contenu des paquets, mais il recherche un chemin pour les acheminer à destination.
 - Le protocole ICMP (*Internet Control Message Protocol*) offre des fonctions de messagerie et de contrôle.
 - Le protocole ARP (*Address Resolution Protocol*) détermine les adresses de la couche liaison de données ou les adresses MAC pour les adresses IP connues.

C. Couche Internet (TCP/IP) suite



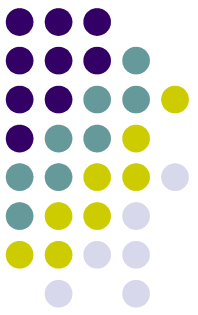
- Le protocole RARP (*Reverse Address Resolution Protocol*) détermine l'adresse IP pour une adresse MAC connue.
- Le protocole IP effectue les opérations suivantes:
 - Il définit un paquet et un système d'adressage.
 - Il transfère des données entre la couche Internet et la couche d'accès au réseau.
 - Il achemine des paquets à des hôtes distants.
- Le protocole IP est parfois qualifié de protocole non fiable.

C. Couche d'accès au réseau (TCP/IP)



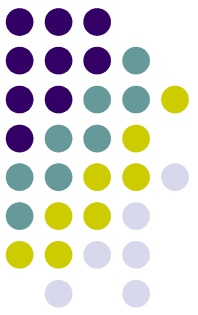
Les protocoles ARP et RARP se situent au niveau des couches d'accès réseau et Internet.

C. Couche d'accès au réseau (TCP/IP) suite



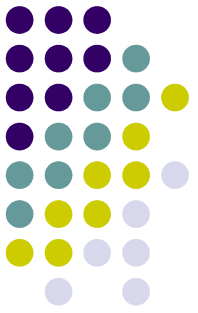
- La couche d'accès au réseau permet à un paquet IP d'établir une liaison physique avec un média réseau. Cela comprend les détails sur les technologies LAN et WAN, ainsi que toutes les informations contenues dans les couches physique et liaison de données du modèle OSI.
- Les pilotes d'application, les cartes modem et les autres équipements s'exécutent au niveau de la couche d'accès au réseau. Cette dernière définit les procédures utilisées pour communiquer avec le matériel réseau et accéder au média de transmission.

C. Couche d'accès au réseau (TCP/IP) suite



- En outre, les protocoles de la couche d'accès au réseau mappent les adresses IP avec les adresses matérielles physiques et encapsulent les paquets IP dans des trames. La couche d'accès au réseau définit la connexion au média physique en fonction de l'interface réseau et du type de matériel utilisés.

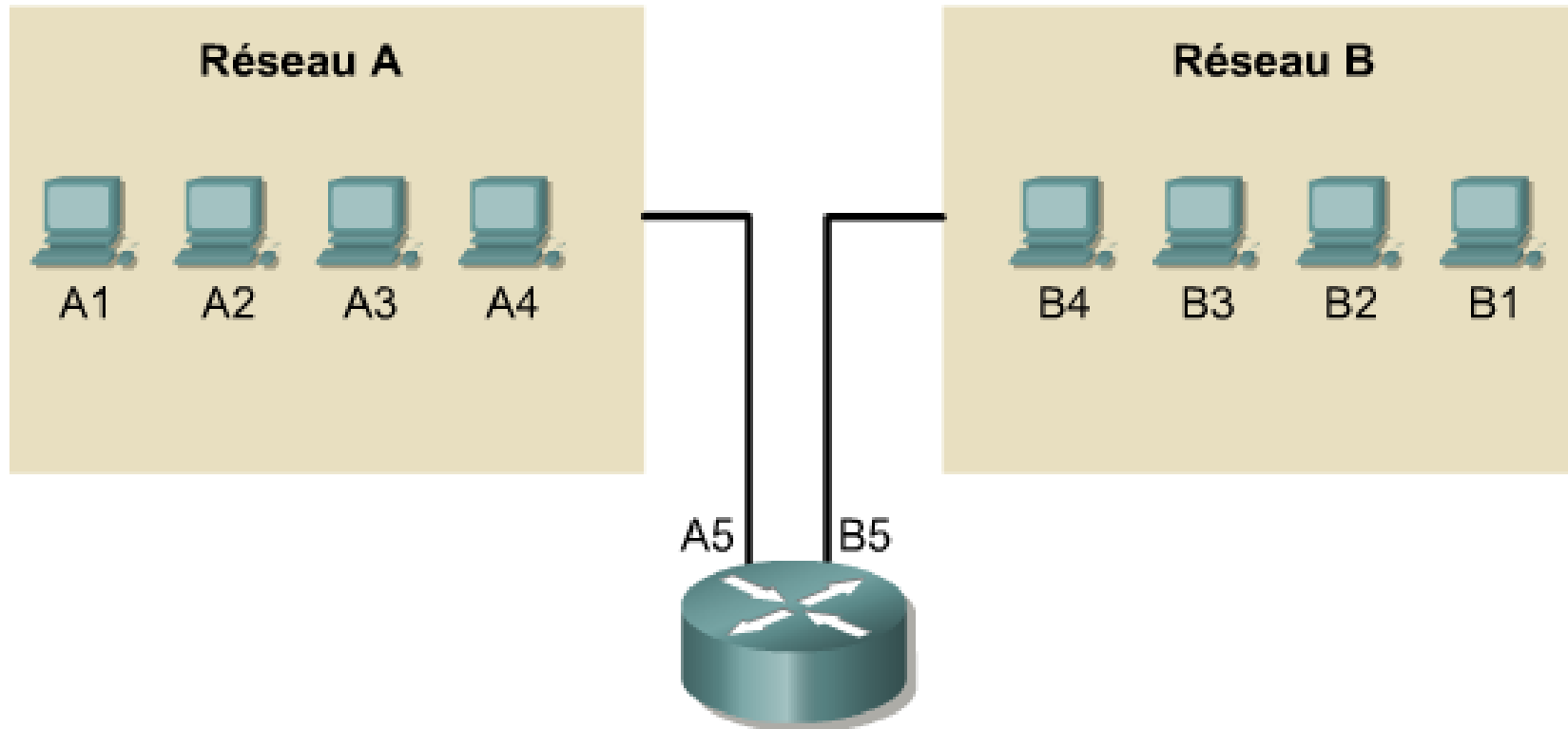
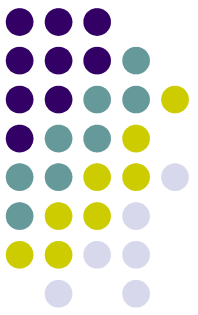
Synthèse



- **Questions???**

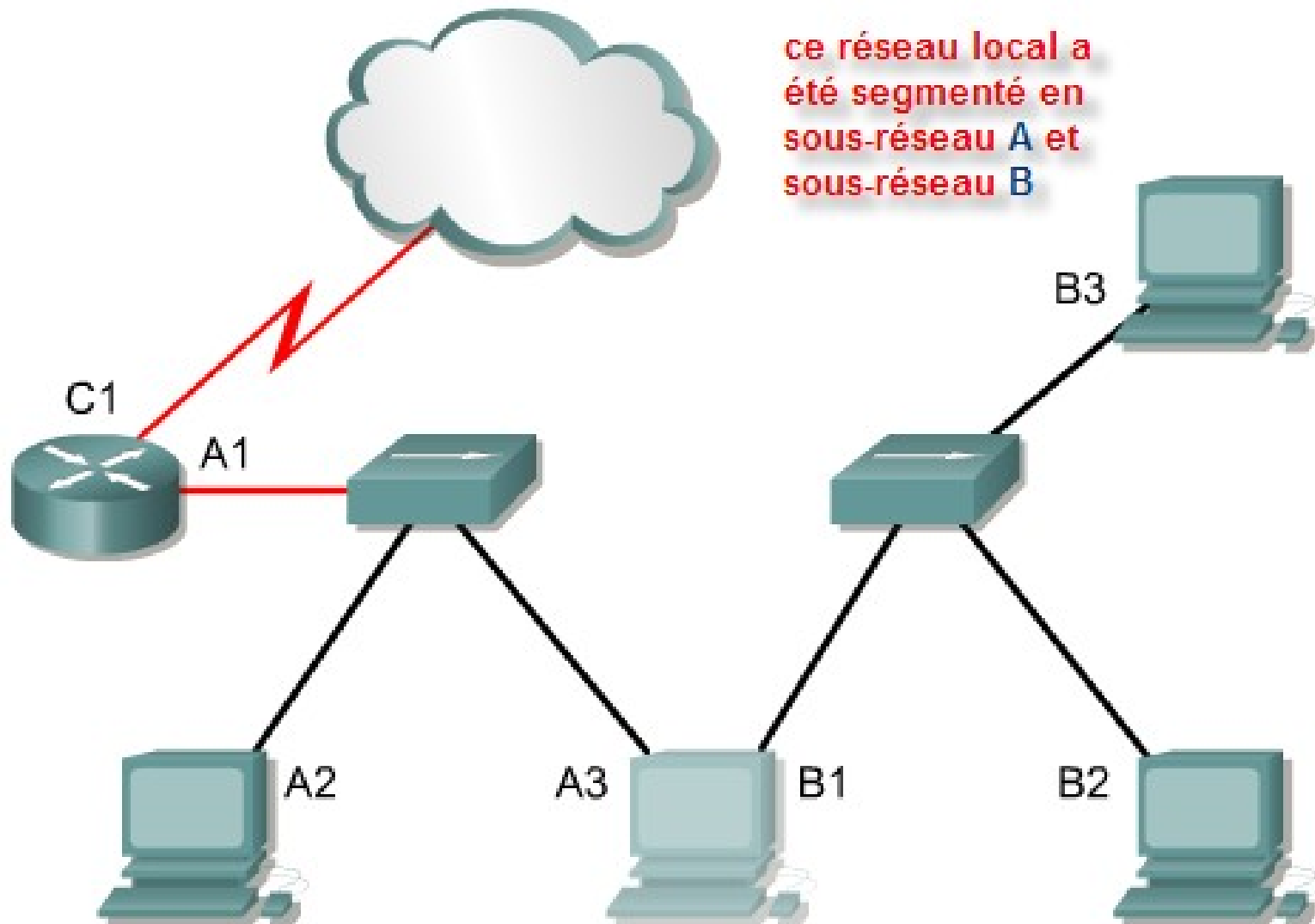
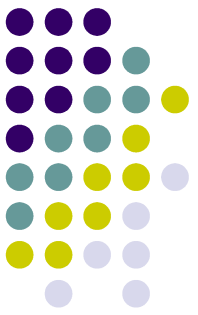
Chap. 2. Adressage IP

2.1. Ipv4



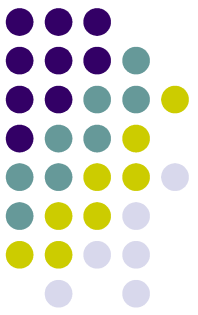
Adressage IP

2.1. Ipv4 (suite)



Adressage IP

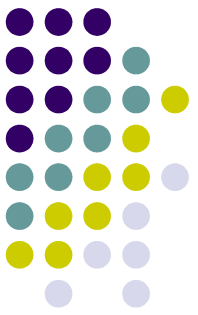
2.1. Ipv4 (suite)



- Un ordinateur peut être connecté à plusieurs réseaux. Si tel est le cas, le système doit recevoir plusieurs adresses. Chaque adresse identifie la connexion d'un ordinateur à un réseau différent. Chaque point de connexion, ou interface, d'un équipement dispose d'une adresse associée à un réseau. Cela permet à d'autres ordinateurs de localiser cet équipement sur un réseau spécifique. La combinaison d'une adresse réseau et d'une adresse hôte crée une adresse unique pour chaque équipement du réseau.

Adressage IP

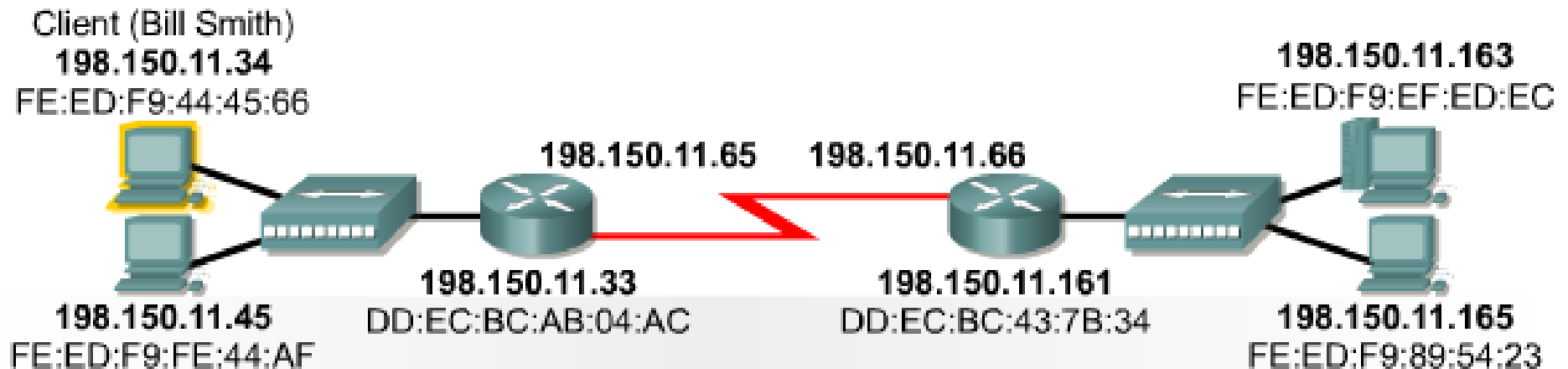
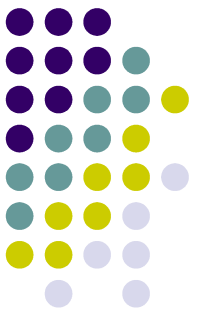
2.1. Ipv4 (suite)



- Tout ordinateur appartenant à un réseau TCP/IP doit disposer d'un identificateur unique, ou adresse IP. Cette adresse, qui intervient au niveau de la couche 3, permet à un ordinateur de localiser un autre ordinateur sur le réseau. Tous les ordinateurs possèdent également une adresse physique unique, également appelée «adresse MAC». Celle-ci est attribuée par le fabricant de la carte réseau. Les adresses MAC opèrent au niveau de la couche 2 du modèle OSI.

Adressage IP

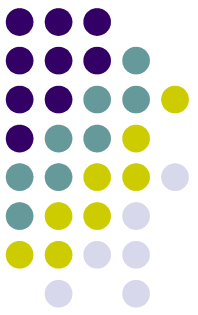
2.1. Ipv4 (suite)



Chaque équipement réseau est identifié par une adresse physique (MAC) et une adresse logique (IP)

Adressage IP

2.1. Ipv4 en binaire(suite)



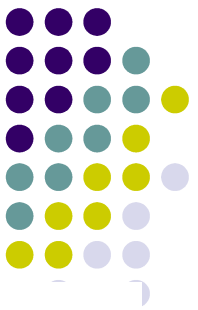
Binaire : 11000000.10101000.00000001.00001000 et 11000000.10101000.00000001.00001001

Décimale : 192.168.1.8 et 192.168.1.9

La figure ci-dessus représente la même valeur sous les formes binaire et décimale. On constate que cette valeur est plus facile à lire exprimée à l'aide de la notation entière avec des points de séparation. Il s'agit d'un des problèmes les plus fréquemment rencontrés avec les nombres binaires. Les longues chaînes de 1 et de 0 répétés sont plus propices aux erreurs.

Adressage IP

2.2.a. (Conversion en binaire)



Exemple de conversion binaire pour la valeur décimale

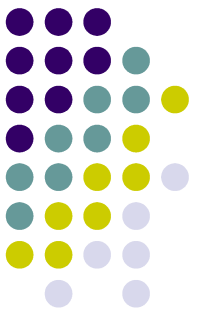
Puissance de la position	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valeur décimale	104	104	40	8	8	0	0	0
Valeur de la position	128	64	32	16	8	4	2	1
Compte binaire	0	1	1	0	1	0	0	0
Reste	104	40	8	8	0	0	0	0

Dans la mesure où le traitement informatique est souvent référencé par des octets, il est plus facile de commencer par définir des plages d'octets et d'effectuer le calcul à partir de ces valeurs. Entraînez-vous à l'aide, par exemple, de la valeur 6 783. Ce nombre étant supérieur à 255 (valeur maximale pour un seul octet), deux octets sont utilisés. Commencez le calcul à 215. L'équivalent binaire de la valeur 6 783 est 00011010 01111111.

Le second exemple utilise la valeur 104. Ce nombre étant inférieur à 255, il peut être représenté par un seul octet. L'équivalent binaire de la valeur 104 est 01101000.

Adressage IP

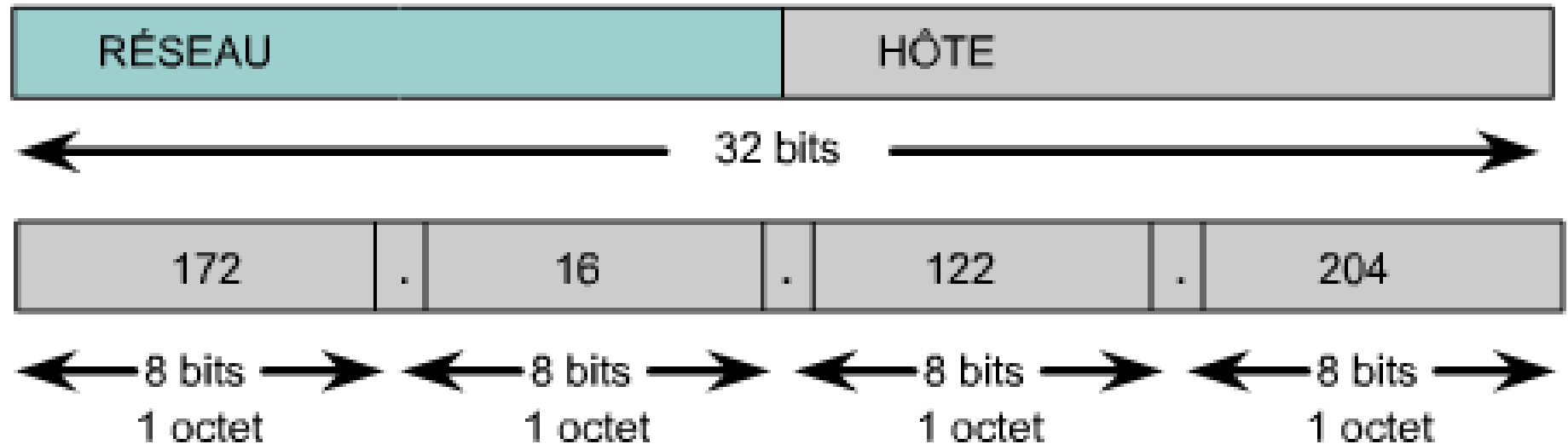
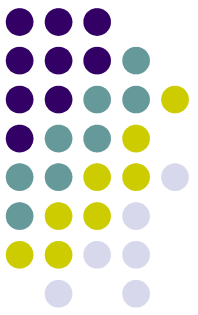
2.2.b. (Conversion en décimal)



- Pour convertir un nombre binaire en nombre décimal, il suffit d'effectuer l'opération en sens inverse. Placez la valeur binaire dans le tableau. Si un 1 est situé dans une position de colonne, ajoutez cette valeur au total. Convertissez le nombre 01110001 en représentation décimale. La bonne réponse est: 113.

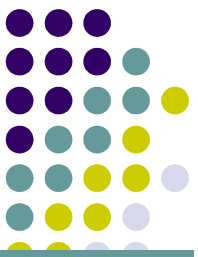
Adressage IP

2.3. Les classes d'adresse



Une adresse IP comporte toujours une partie réseau et une partie hôte.

Adressage IP



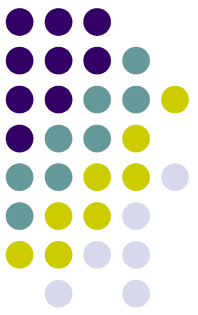
2.3. Les classes d'adresse (suite)

Classe d'adresses IP	Plage d'adresses IP (premier octet)
Classe A	1-126 (00000001-01111110) *
Classe B :	128-191 (10000000-10111111)
Classe C	192-223 (11000000-11011111)
Classe D	224-239 (11100000-11101111)
Classe E	240-255 (11110000-11111111)

Le premier bit d'une adresse de classe A est toujours 0. Par conséquent, le nombre le plus faible pouvant être représenté est 00000000 (0 en décimal) et le plus élevé est 01111111 (127 en décimal). Les valeurs 0 et 127 sont réservées et ne peuvent pas être utilisées comme adresses réseau.

Adressage IP

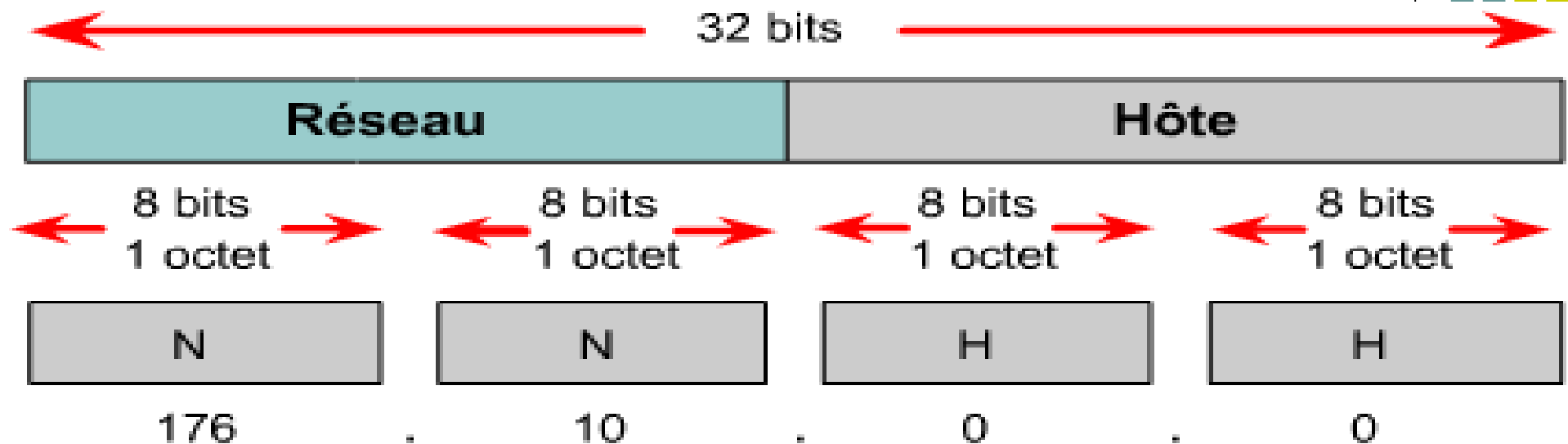
2.3. Les classes d'adresse (suite)



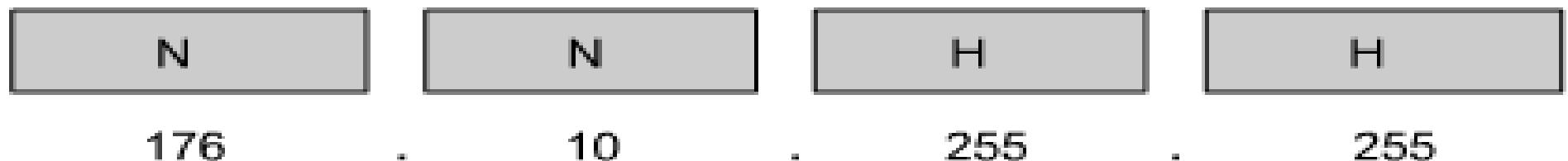
- Les adresses IP sont regroupées en classes afin de permettre l'adaptation à des réseaux de différentes tailles et de faciliter leur classification. Cette opération est connue sous le nom d'adressage par classes. Chaque adresse IP complète de 32 bits est fractionnée en une partie réseau et une partie hôte. Un bit, ou une séquence de bits, situé en début d'adresse détermine la classe de l'adresse. Il existe cinq classes d'adresses IP, comme l'illustre le transparent précédent.

Adressage IP

2.3.1 Les adresses IP interdites



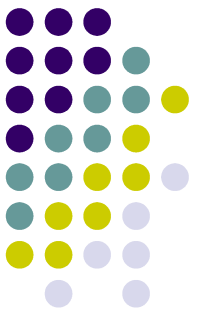
Adresse réseau (bits d'hôte = uniquement des 0)



Adresse de broadcast (bits d'hôte = uniquement des 1)

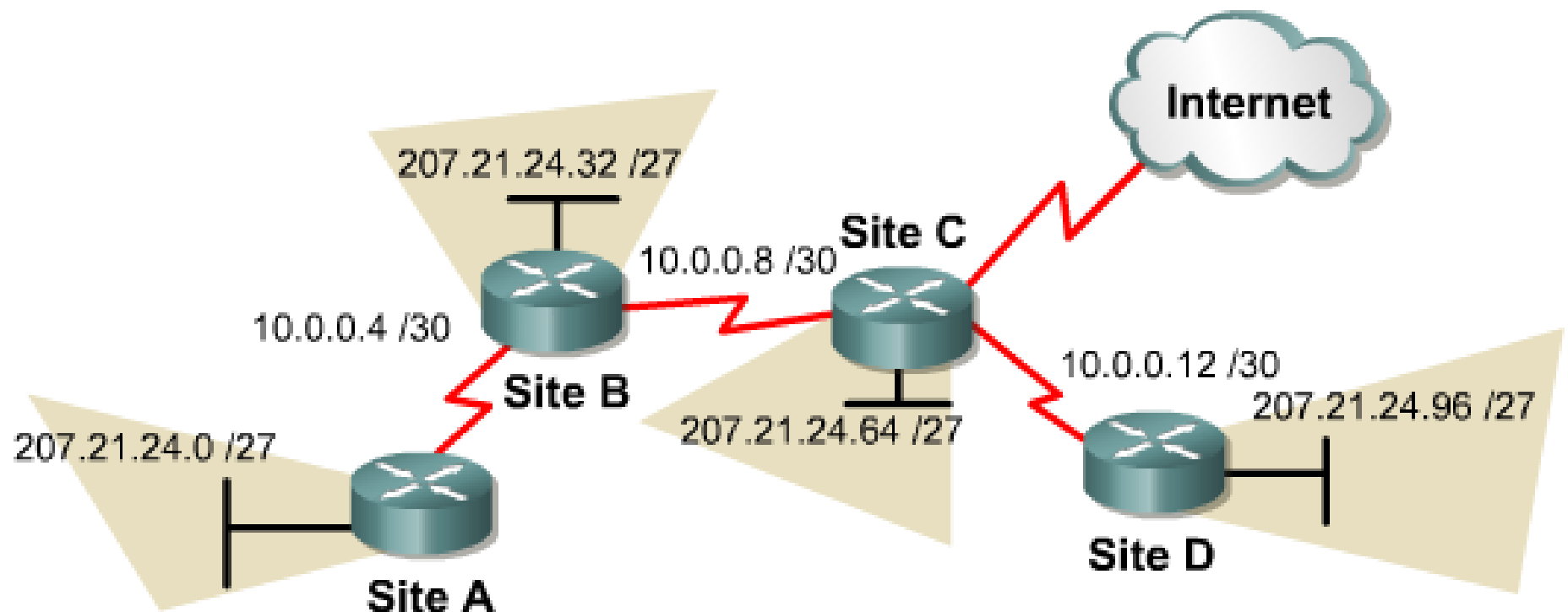
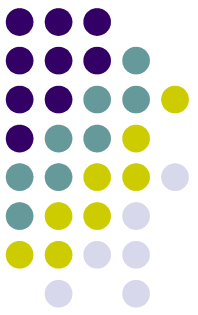
Cette adresse de classe B est l'adresse de broadcast de ce réseau. Lorsque des paquets sont reçus avec cette adresse de destination, les données sont traitées par chaque ordinateur.

2.3.2 adressage *IP Privé*



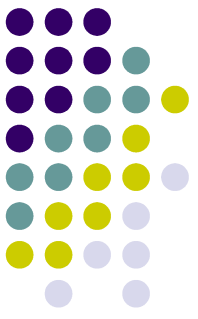
Classe	Plage d'adresses internes RFC 1918
A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.31.255.255
C	192.168.0.0 à 192.168.255.255

2.3.2 adressage IP Privé (suite)



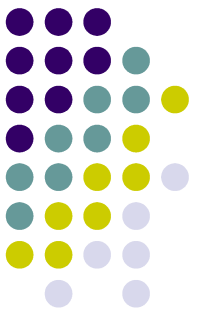
Les adresses privées peuvent être utilisées pour prendre en charge des liaisons séries point à point sans gaspiller les adresses ip réelles (publiques).

2.3.2 adressage IP Privé (suite)



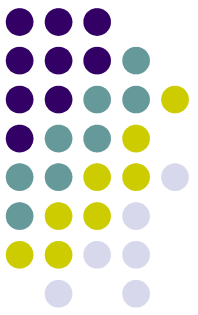
- Les adresses IP privées constituent une solution de rechange au problème de pénurie des adresses IP publiques. Les hôtes d'un réseau public doivent disposer d'une adresse IP unique. Néanmoins, les réseaux privés qui ne sont pas connectés à Internet peuvent utiliser n'importe quelle adresse hôte, dès lors que chacun des hôtes du réseau privé est unique.

2.3.2 adressage IP Privé (suite)



- Un grand nombre de réseaux privés coexistent avec les réseaux publics. La spécification RFC 1918 réserve trois blocs d'adresses IP pour une utilisation privée et interne. Ceux-ci se composent d'une classe A, d'une plage d'adresses de classe B et d'une plage d'adresses de classe C. Les adresses contenues dans ces plages ne sont pas acheminées sur les routeurs du backbone d'Internet. Ces routeurs Internet les rejettent immédiatement.

2.3.3 *Segmentation d'un réseau en sous-réseaux*



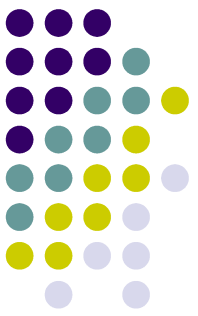
- L'administrateur système doit réfléchir aux problèmes suivants lors de l'évolution d'un réseau: il est essentiel de définir le nombre de sous-réseaux ou de réseaux requis, ainsi que le nombre d'hôtes requis par réseau. En utilisant des sous-réseaux, le réseau n'est pas limité aux masques de réseau de classe A, B ou C par défaut. En outre, la conception du réseau est plus flexible.

2.3.3 *Segmentation d'un réseau en sous-réseaux (suite)*



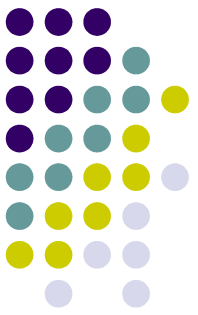
- Les adresses de sous-réseau contiennent une partie réseau, plus un champ de sous-réseau et un champ d'hôte. Le champ de sous-réseau et le champ d'hôte sont créés à partir de la partie hôte d'origine pour l'ensemble du réseau.
- Pour effectuer un découpage en sous-réseaux, des bits de la partie hôte doivent être réattribués au réseau. Cette opération est souvent appelée « emprunt » de bits. Il serait en fait plus juste de parler de « prêt ». L'emprunt se fait toujours à partir du bit d'hôte situé le plus à gauche, à savoir celui le plus proche du dernier octet de la partie réseau.

2.3.3 Segmentation d'un réseau en sous-réseaux (suite)



Nombre de bits emprunté au champ hôte pour créer des sous-réseaux	Nombre de sous-réseaux	Nombre d'hôtes de classe A par sous-réseau	Nombre d'hôtes de classe B par sous-réseau	Nombre d'hôtes de classe C par sous-réseau
2	2	4,194,302	16,382	62
3	6	2,097,150	8,190	30
4	14	1,048,574	4,094	14
5	30	524,286	2,046	6
6	62	262,142	1,022	2
7	126	131,070	510	-
8	254	65,534	254	-

2.3.3 Segmentation d'un réseau en sous-réseaux (exemple 1)



Adresse réseau de classe C 192.168.10.0

11000000.10101000.00001010.00000000

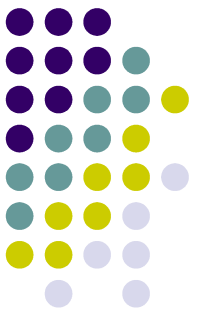
N . N . N . H

11000000.10101000.00001010.00000000

N . N . N . sN H

Dans cet exemple, trois bits ont été alloués pour désigner le sous-réseau.

2.3.3 Segmentation d'un réseau en sous-réseaux (exemple 2)



Adresse réseau de classe B 147.10.0.0

10010011.00001010.00000000.00000000

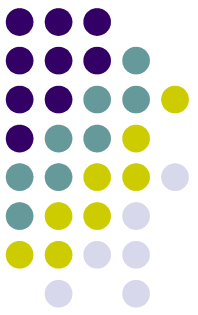
N . N . H . H

10010011.00001010.00000000.00000000

N . N . sN H . H

Dans cet exemple, cinq bits ont été alloués pour désigner le sous-réseau.

2.3.3 Segmentation d'un réseau en sous-réseaux (exemple 3)



Adresse réseau de classe A 28.0.0.0

00011100.00000000.00000000.00000000

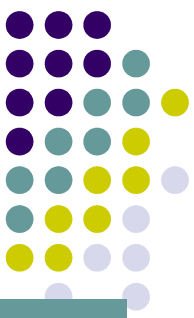
N . H . H . H

00011100.00000000.00000000.00000000

N . sN . sN H . H

Dans cet exemple, douze bits ont été alloués pour désigner le sous-réseau.

2.3.3.a Segmentation d'un réseau en sous-réseaux (Calcul du sous-réseaux)

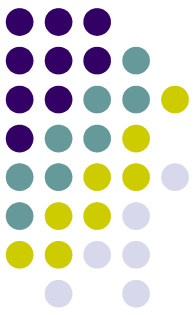


Format /#	/25	/26	/27	/28	/29	/30	N/A	N/A
Masque	128	192	224	240	248	252	254	255
Bits empruntés	1	2	3	4	5	6	7	8
Valeur	128	64	32	16	8	4	2	1
Nombre total de sous-réseaux		4	8	16	32	64		
Sous-réseaux utilisables		2	6	14	30	62		
Nombre total d'hôtes		64	32	16	8	4		
Hôtes utilisables		62	30	14	6	2		

Note:

Une adresse de classe C avec un masque /25 n'emprunte uniquement que 1 bit, comme on le voit ici. Mais une adresse de classe B, avec le même masque, va emprunter 9 bits et on aura un grand nombre de sous-réseaux.

2.3.3.a Segmentation d'un réseau en sous-réseaux (Calcul du sous-réseaux) suite



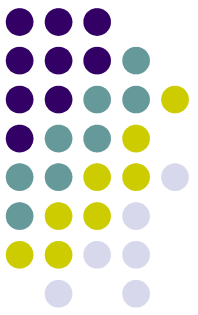
224 dans le quatrième octet représente la valeur de place totale des bits empruntés.

128	64	32	16	8	4	2	1
1	1	1	0	0	0	0	0

3 bits empruntés

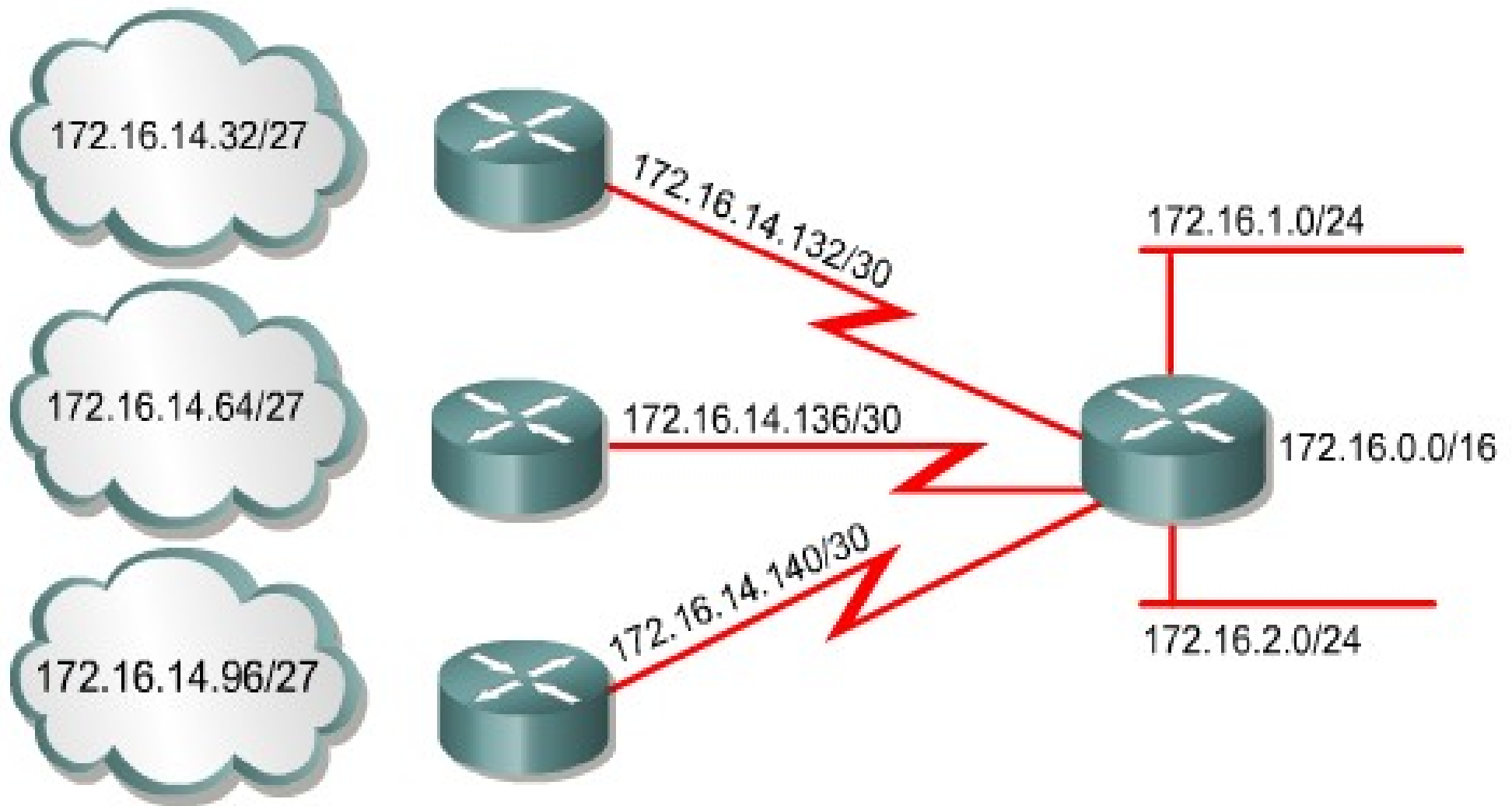
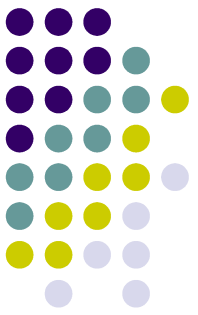
$$128 + 64 + 32 = 224$$

2.3.3.a Segmentation d'un réseau en sous-réseaux (Calcul du sous-réseaux) suite

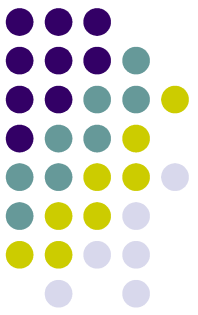


- Nombre de sous-réseaux utilisables = deux à la puissance du nombre de bits attribués au sous-réseau ou nombre de bits empruntés, moins deux. La soustraction correspond aux deux adresses réservées que sont l'adresse du réseau et l'adresse de broadcast du réseau.
- Nombre d'hôtes utilisables = deux à la puissance des bits restants, moins deux (pour les adresses réservées que sont l'adresse du sous-réseau et l'adresse de broadcast du sous-réseau).

2.3.3.b Segmentation d'un réseau en sous-réseaux (Calcul du sous-réseaux par l'opération AND)

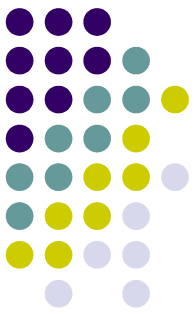


2.3.3.b Segmentation d'un réseau en sous-réseaux (Calcul du sous-réseaux par l'opération AND) suite



- Les routeurs se servent des masques de sous-réseau pour déterminer le sous-réseau de chacun des nœuds. On parle alors d'opération AND logique. Il s'agit d'un processus binaire par lequel le routeur calcule l'ID de sous-réseau d'un paquet entrant. L'opération AND est similaire à une multiplication.
- Ce processus s'effectue au niveau binaire. Il est par conséquent nécessaire d'afficher l'adresse IP et le masque au format binaire. L'opération AND est appliquée à l'adresse IP et à l'adresse du sous-réseau avec pour résultat l'ID du sous-réseau. Cette information permet au routeur de transférer le paquet à l'interface appropriée.

2.3.3.b Segmentation d'un réseau en sous-réseaux (Calcul du sous-réseaux par l'opération AND) suite

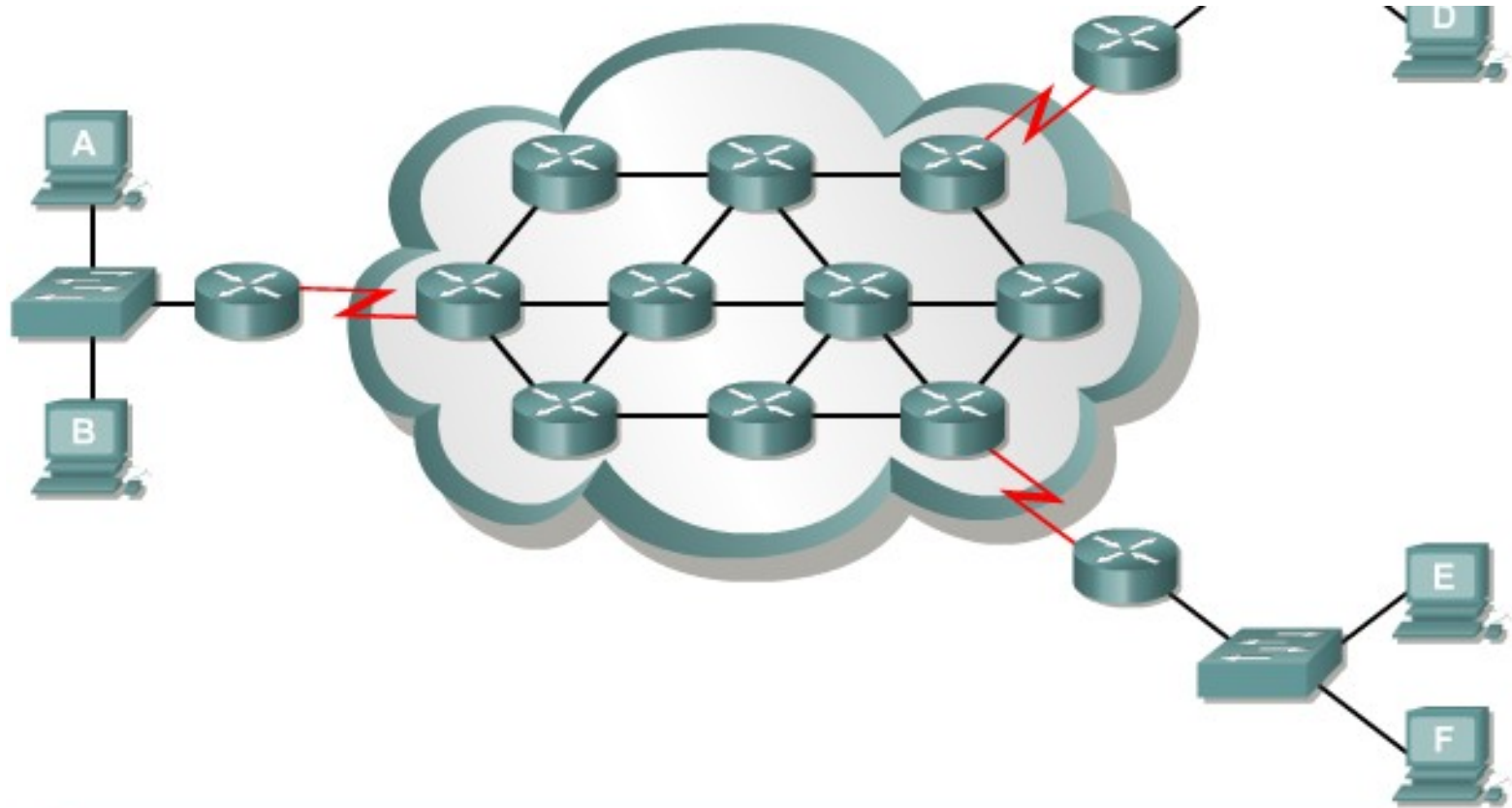
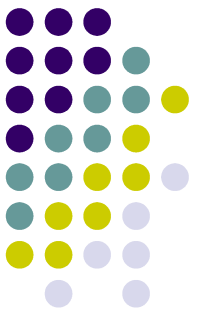


0	AND	0	=	0
0	AND	1	=	0
1	AND	0	=	0
1	AND	1	=	1

Adresse du paquet	201.10.11.65	11001001.00001010.00001011.01000001
AND		
Masque	255.255.255.224	11111111.11111111.11111111.11100000
ID du sous-réseau	201.10.11.64	11001001.00001010.00001011.01000000

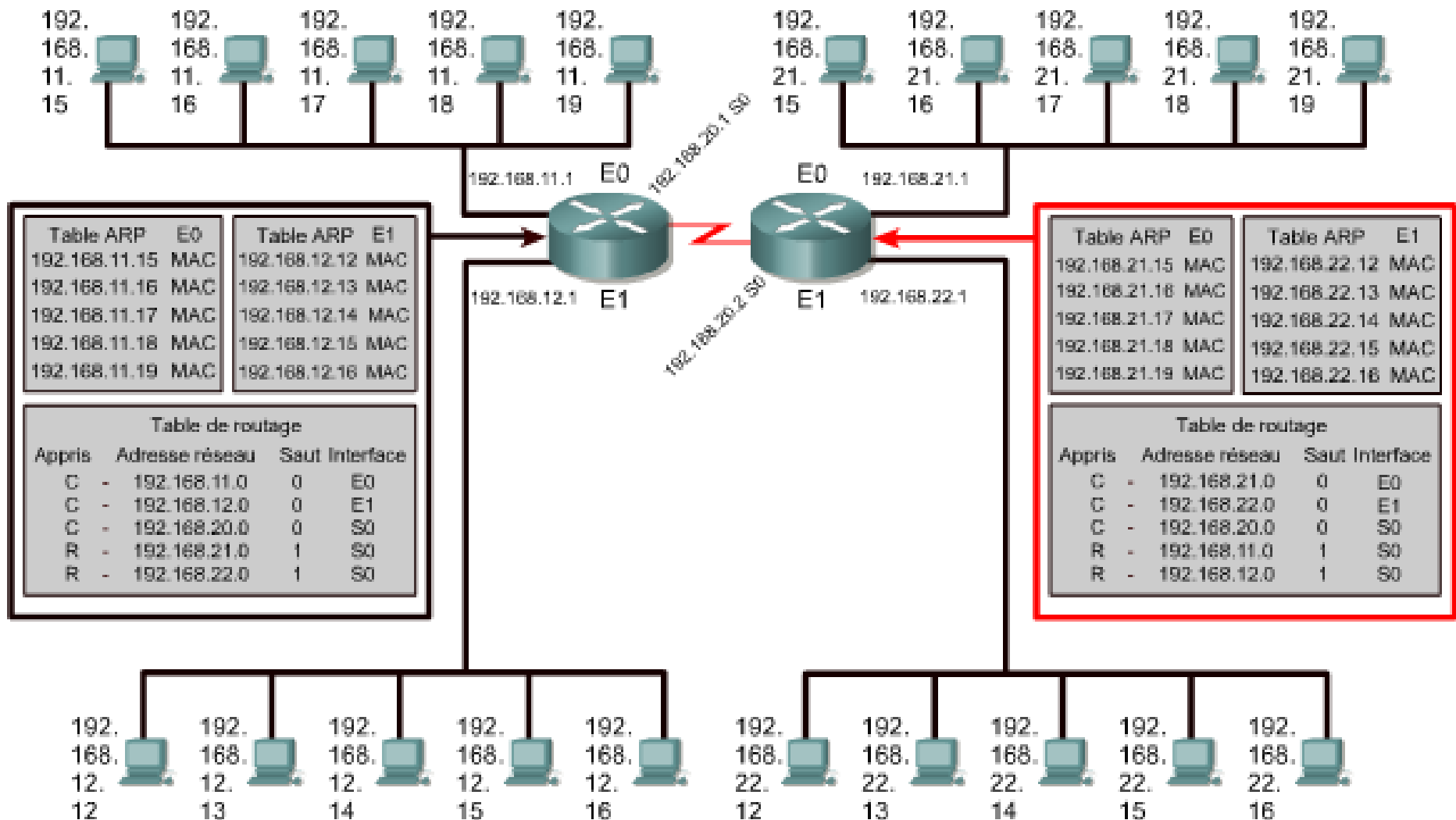
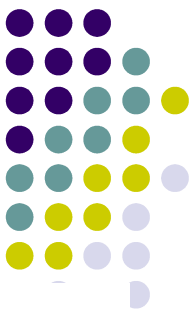
Chap. 3. Routage

3.1. Protocoles routé (IP)

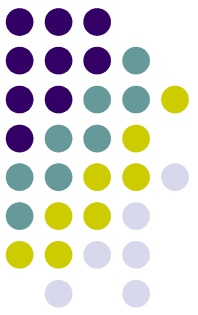


Chap. 3. Routage

3.1. Protocoles de routé (IP)

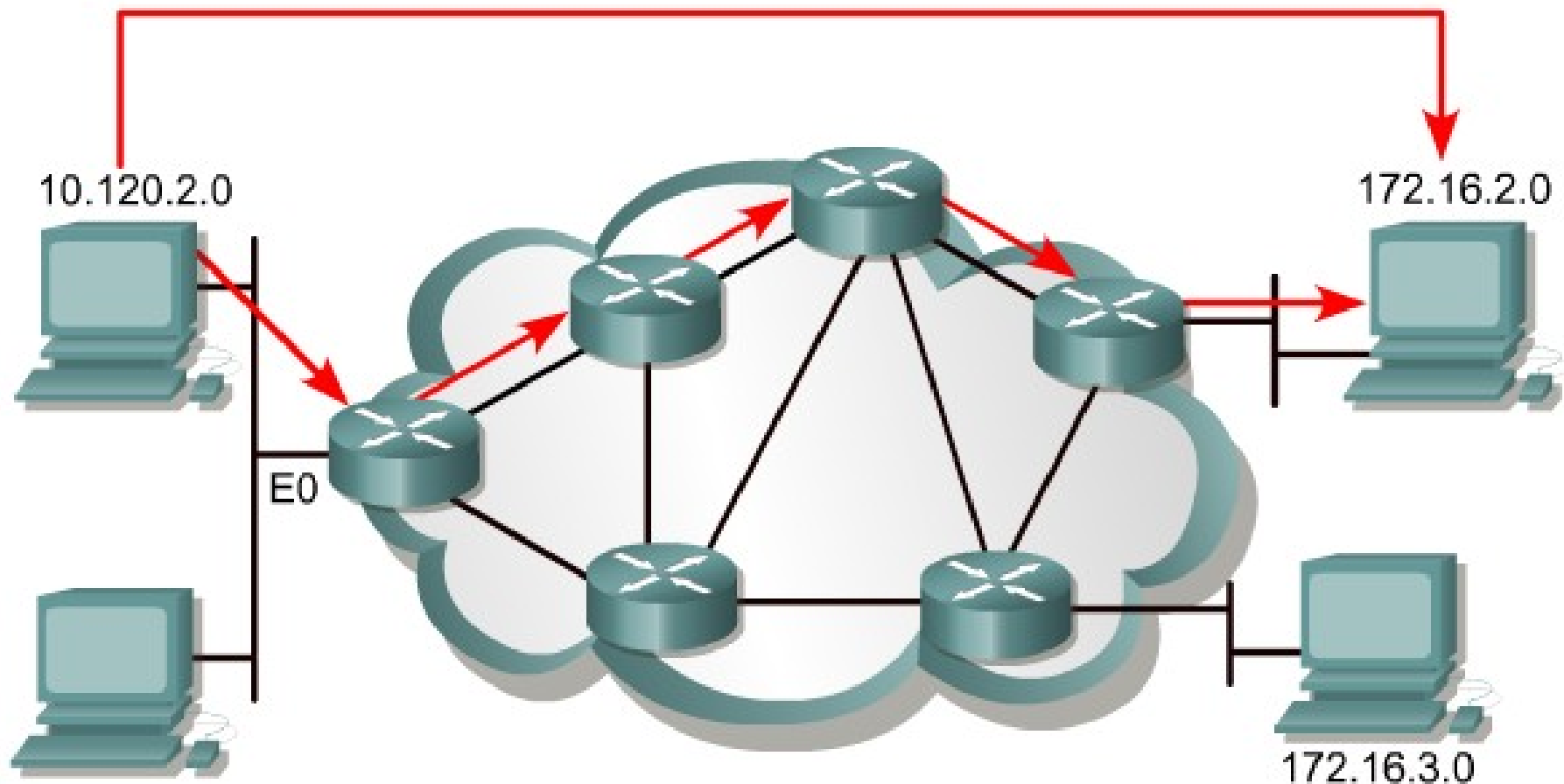
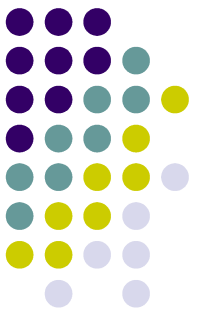


3.1. *Protocoles routé (IP)* (suite)



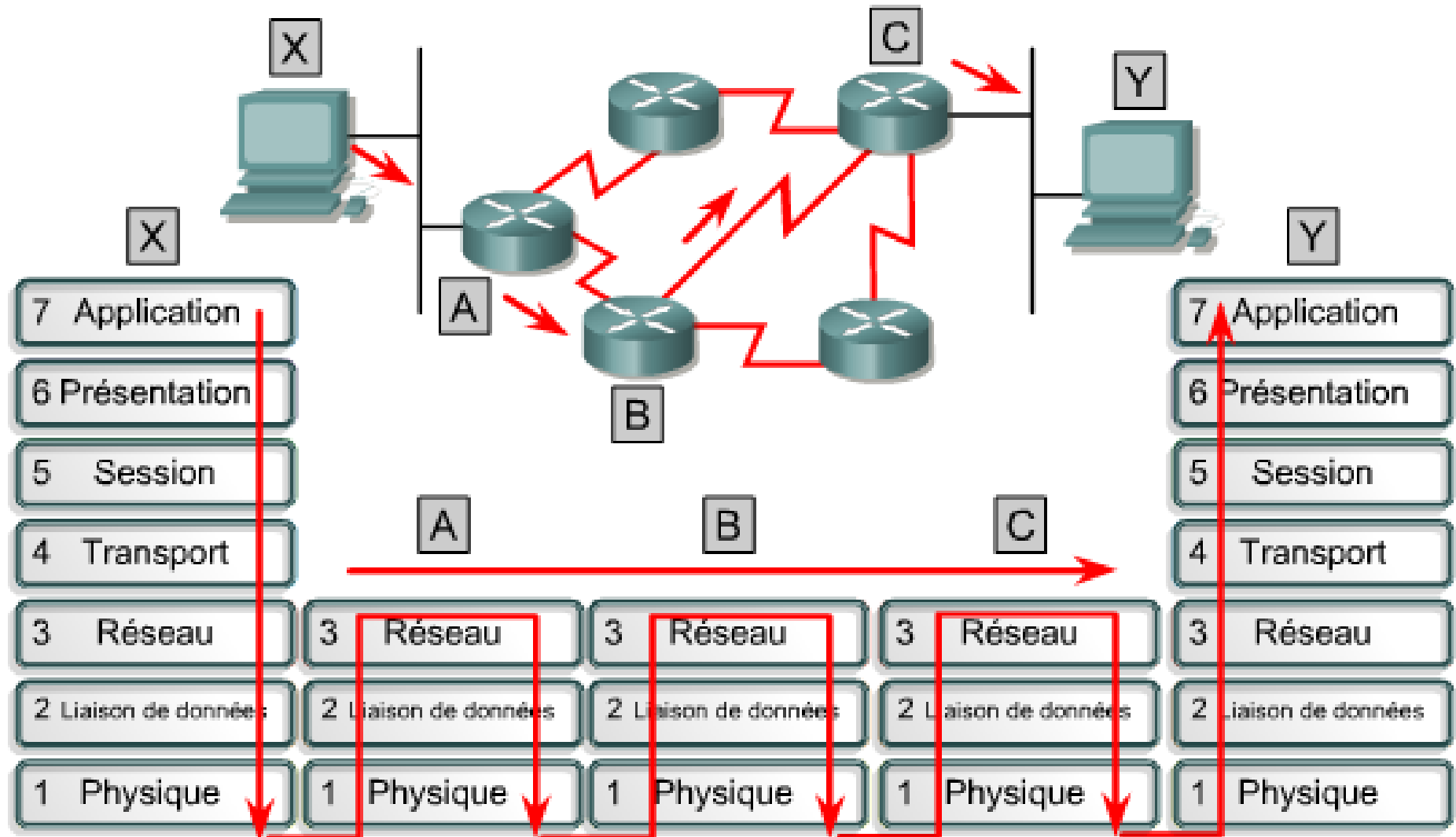
- Le routage est une fonction de la couche 3 du modèle OSI. C'est un système d'organisation hiérarchique qui permet de regrouper des adresses individuelles. Ces dernières sont traitées comme un tout jusqu'à ce que l'adresse de destination soit requise pour la livraison finale des données. Le routage cherche le chemin le plus efficace d'une unité à une autre. Le matériel au centre du processus de routage est le routeur.
- Il possède les deux fonctions principales suivantes:
 - Le routeur gère les tables de routage et s'assure que les autres routeurs ont connaissance des modifications apportées à la topologie du réseau. Il se sert des protocoles de routage pour échanger les informations de réseau.
 - Le routeur détermine la destination des paquets à l'aide de la table de routage lorsque ceux-ci arrivent à l'une de ses interfaces. Il les transfère vers la bonne interface, ajoute les informations de trame de cette interface, puis transmet la trame.

3.1.1. Protocoles routés (IP) (suite)



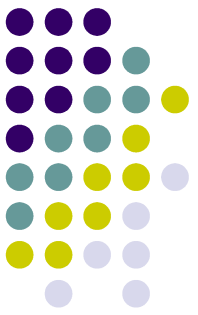
Les protocoles routés transportent les données d'une station d'extrémité à une autre.

3.1.1. Protocoles routés (IP) (suite)



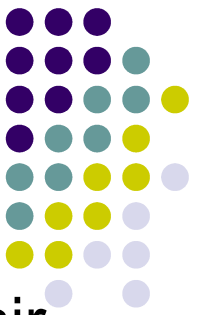
Chaque routeur fournit ses services pour la prise en charge des fonctions de la couche supérieure.

3.1.1. *Protocoles routés (IP) (suite)*



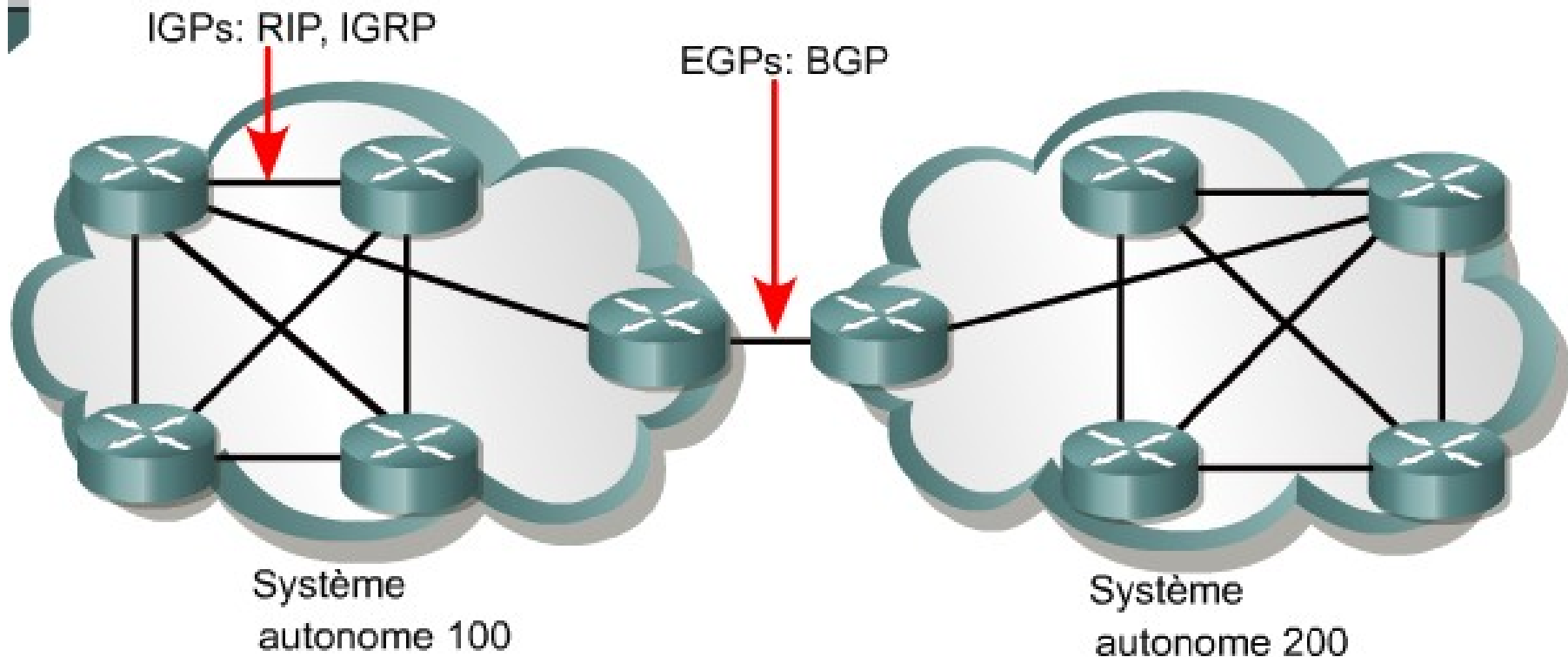
- Les protocoles routés ou routables sont utilisés au niveau de la couche réseau afin de transférer les données d'un hôte à l'autre via un routeur. Les protocoles routés transportent les données sur un réseau.

3.1.2. *Protocoles de routage*



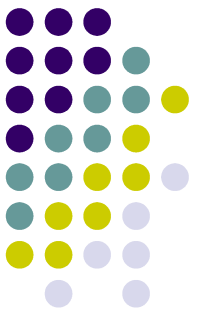
- Les protocoles de routage permettent aux routeurs de choisir le meilleur chemin possible pour acheminer les données de la source vers leur destination.
- Les fonctions du protocole de routage sont en partie les suivantes:
 - Il fournit les processus utilisés pour partager les informations d'acheminement.
 - Il permet aux routeurs de communiquer entre eux afin de mettre à jour et de gérer les tables de routage.
 - Les protocoles de routage prenant en charge le protocole routé IP sont par exemple les protocoles **RIP, IGRP, OSPF, BGP et EIGRP**.
 - Parmi eux il y en a dits “**à Vecteur de Distance**” et d’autres dits “**à Etat de Lien**”, selon les algorithmes.

3.1.2. a. Types de Protocoles de Routage IGP et EGP

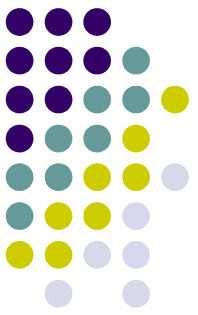


Un système autonome est un ensemble de réseaux placés dans un domaine administratif commun. Les protocoles IGP opèrent au sein d'un système autonome. Les protocoles EGP relient différents systèmes autonomes.

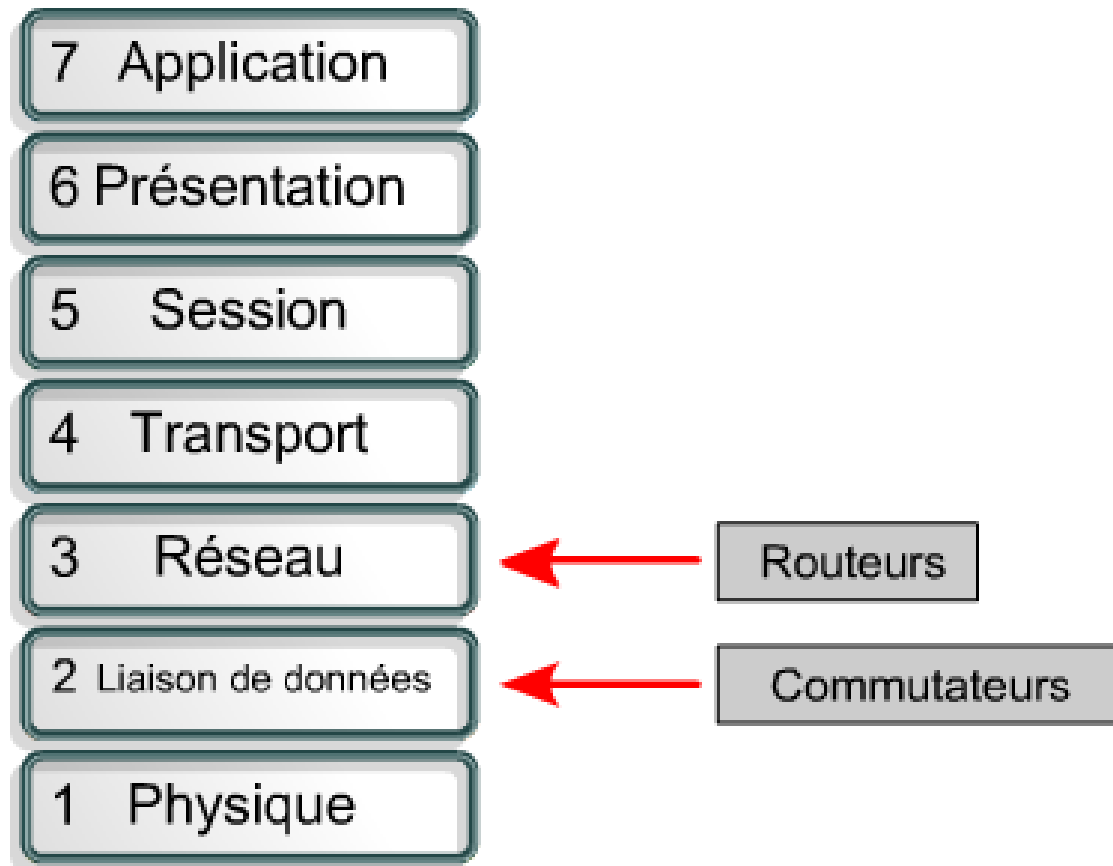
3.1.2. a. Types de Protocoles de Routage IGP et EGP (suite)

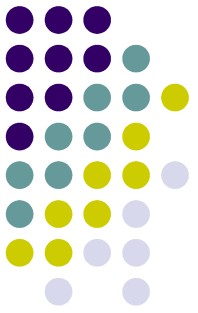


- Les protocoles **IGP** acheminent les données au sein **d'un système autonome**. Il s'agit:
 - Des protocoles RIP et RIPv2.
 - Du protocole IGRP.
 - Du protocole EIGRP.
 - Du protocole OSPF.
 - Du protocole IS-IS (*Intermediate System-to-Intermediate System*).
- Les protocoles **EGP** acheminent les données entre **les systèmes autonomes**. Le protocole BGP est un exemple de ce type de protocole.



3.1.2.b. *Routage et commutation*





Merci de nous avoir suivi...