

Chapitre 1 – Exploration du réseau

- Qu'est-ce qu'un réseau ?
 - Chaque entreprise développe un réseau relationnel qui l'unit à ses clients, ses fournisseurs, ses contacts.
 - Un réseau informatique relie entre eux les ordinateurs, les imprimantes, les serveurs, les téléphones,...



Chapitre 1 – Notions de base

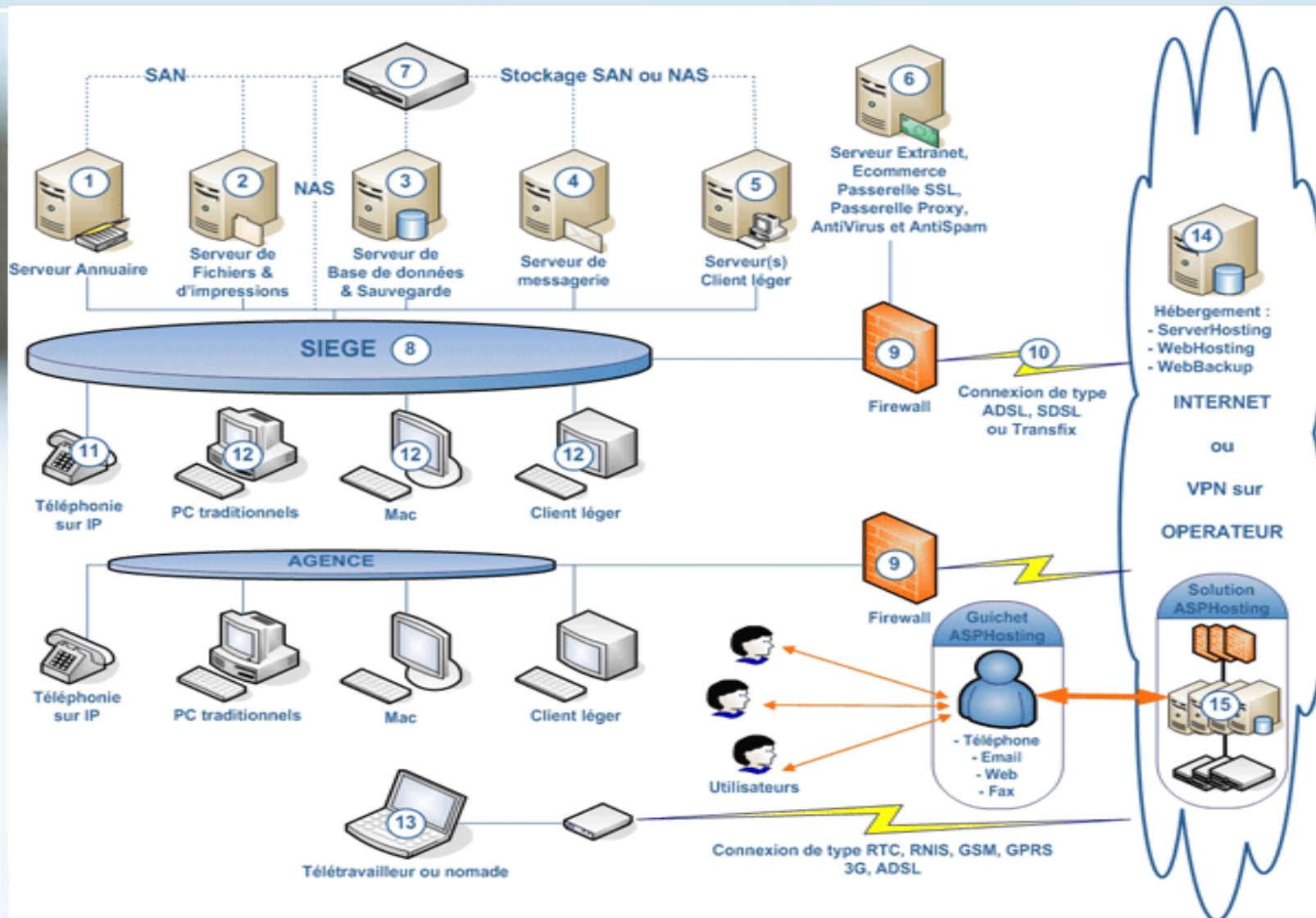
Définition

- Un réseau peut être connecté à d'autres réseaux afin de bénéficier des derniers progrès technologiques
 - la visioconférence
 - le multimédia
 - le transfert de fichiers audio et vidéo
 - les services d'informations en ligne
 - ...



Chapitre 1 – Notions de base

Composants Réseau



Chapitre 1 – Notions de base

Composants Réseau

- Utilisateurs :
 - stations de travail
 - Serveurs
 - Imprimantes
 - Scanners
 - unité de stockage
 - Webcam
 - NAS
 -



Chapitre 1 – Notions de base

Composants Réseau

- Câblage :
 - Câbles cuivre
 - Paires symétriques blindées ou non blindées
 - Fibres optiques
 - Multimode
 - Monomode
 - Liaisons sans-fil
 - WiFi, Infrarouge, Bluetooth, liaisons hertziennes
 - Armoire de brassage (Patch panel)



- Interconnexion LAN :
 - Répéteur (Repeater)
 - Régénère le signal
 - Adapte la connectique
 - Commutateur (Switch)
 - Interconnecte les éléments internes
 - Routeur (Router)
 - Interconnecte les éléments externes



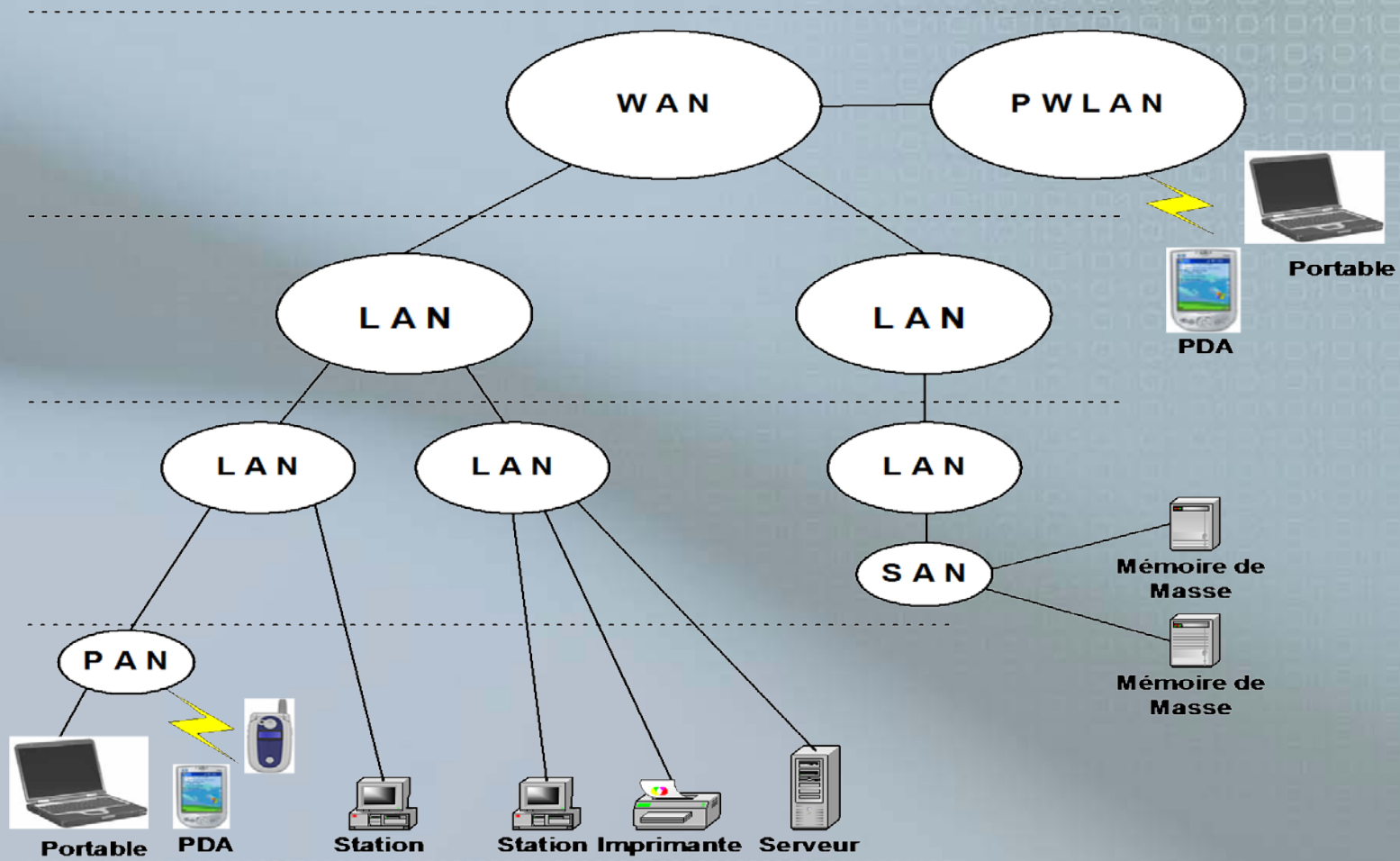
Chapitre 1 – Notions de base Interconnexion Réseau

- Interconnexion WAN :
 - Réseau commuté
 - réseau téléphonique (modem)
 - ADSL, VDSL,...
 - GEthernet, 10 GEthernet,...
 - Liaisons propriétaire (lignes louées)



Chapitre 1 – Notions de base

Structure hiérarchique



Chapitre 1 – Notions de base

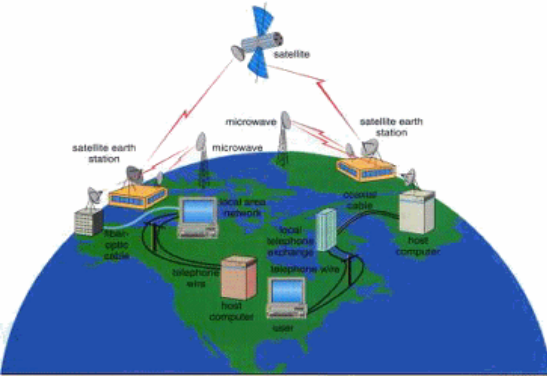
Structure physique

- L'étendue géographique détermine l'organisation physique du réseau :
 - PAN : Personal Area Network
 - LAN : Local Area Network
 - WAN : Wide Area Network
 - SAN : Stockage Area Network
 - PWLAN : Public Wireless Local Area Network

- La taille de l'entreprise détermine l'organisation logique du réseau :
 - Groupe de travail : Interconnexion à l'intérieur d'un bâtiment sur des lignes privées.
 - Entreprise : Interconnexion de plusieurs réseaux de bâtiments sur des lignes privées ou publics.
 - Groupe d'entreprises : Interconnexion de plusieurs réseaux d'entreprises à travers le réseau public.

Chapitre 1 – Notions de base

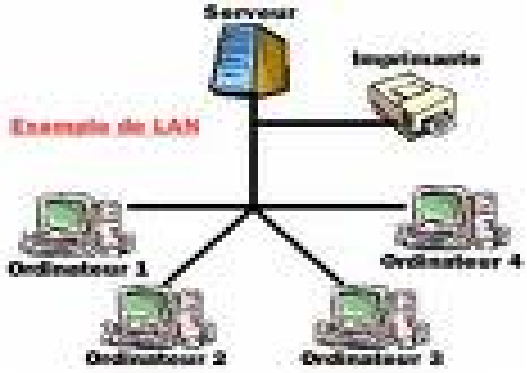
Organisation physique



- WAN : Wide Area Network
 - Réseau étendu (national/international).
 - Généralement sur des lignes publiques.
 - Systèmes de communication publics.
 - Débit de transmission variable selon les technologies utilisées.
 - Topologie maillée, point à point.

Chapitre 1 – Notions de base

Organisation physique



- LAN : Local Area Network
 - Réseau circonscrit dans un environnement restreint.
 - Câblage privé.
 - Systèmes de communications privés.
 - Débits élevés.
 - Topologie en étoile ou arbre.



Chapitre 1 – Notions de base Organisation physique

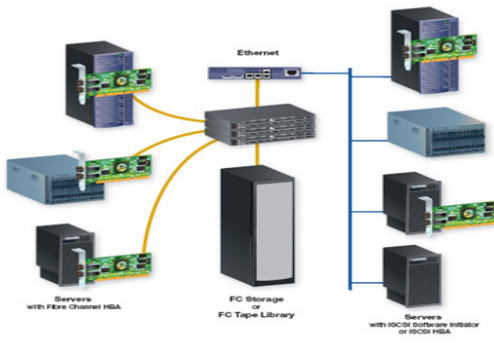
- PWLAN : Public Wireless Local Area Network
 - Réseau d'accès temporaire (Hot Spot).
 - Systèmes de communication publics et privés.
 - Débit de transmission du WiFi.
 - Topologie point à point.




- PAN : Personal Area Network
 - Réseau privé de faible étendue.
 - Débits dépendants la technologie utilisée (Ethernet, Sans fils (WLAN) ou CPL).
 - Systèmes de communications privés.
 - Câblage privé.
 - Topologie point à point ou en étoile.

Chapitre 1 – Notions de base

Organisation physique



- SAN : Storage Area Network
 - Réseau réservé au stockage.
 - Débits très élevés (fiber channel, iSCSI)
 - Interconnexion de systèmes de stockage de masse.
 - Topologie point à point, boucle, étoile



Chapitre 2 – Configuration d'un système d'exploitation

Chapitre 2 – Switch Caractéristiques

- Un commutateur/switch est un équipement qui est défini par les caractéristiques suivantes :
 - Le format
 - Le nombre de ports
 - Le type de port
 - La bande passante
 - Les techniques d'administration
 - La commutation



- **Fonctionnement**

Un commutateur (switch) Ethernet doit permettre :

- Le relayage des trames uniquement aux stations concernées.
- A plusieurs stations de pouvoir commuter en même temps.
- Assurer la redondance des connexions



Chapitre 2 – Switch

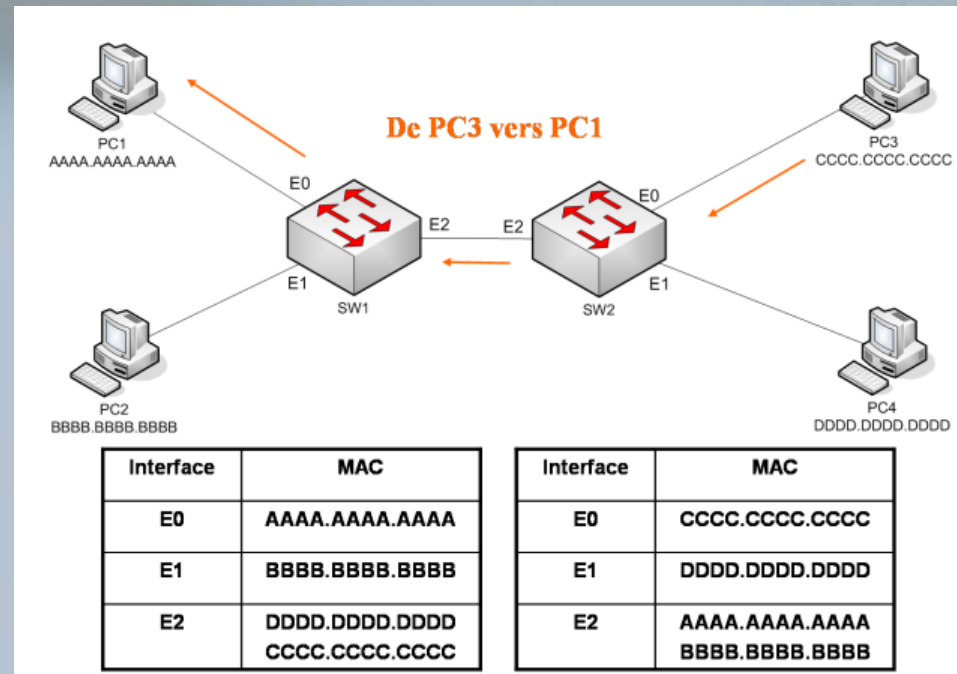
Caractéristiques matériel

- Un switch peut être caractérisé par :
 - Nombre de ports
 - De quelques ports à plusieurs centaines de ports en les cascasant
 - Type de ports
 - Port RJ45 ou fibre optique
 - Panachage de ports RJ45 et de ports fibre optique
 - Bande passante
 - 10, 100 Mb/s, 1 et 10 Gb/s,...
 - Temps et le nombre de commutations



Chapitre 2 – Switch Fonctionnalités

- Fonctionnement
 - Un switch décode l'en-tête Ethernet pour connaître le destinataire et envoie la trame **uniquement** vers sa destination.



- Fonctionnement
 - Chaque adresse MAC connue est associée à un port par lequel on peut l'atteindre.
 - La paire Port/Mac adresse est stockée dans la table de commutation (dynamique).
 - Une demande est diffusée à tout le réseau si l'adresse est inconnue (ARP).
 - La durée des enregistrements dans la table de commutation est limitée.



- On distingue trois catégories de commutateurs :
 - Unmanaged (non administrable)
 - Smart managed (administration intelligente des fonctions principales)
 - Full managed (administration complète - sécurité ou triple play)



- Connexion de deux switchs
 - Croisement de l'émission et de la réception
 - Automatique (Midi/Midi-X auto)
 - Manuel (utilisation d'un câble croisé)
 - Port(s) dédié(s) UpLink
 - Utilisation
 - Ordinateur à switch : Câble droit
 - Ordinateur à routeur : Câble croisé
 - Switch à switch : Câble croisé
 - Routeur à routeur : Câble croisé
 - Routeur à switch : Câble droit



Chapitre 2 – Switch

Principe de fonctionnement

- Trois modes de fonctionnement sont possibles :
 - A la volée
 - Stockage et retransmission
 - A la volée adaptif



Chapitre 2 – Switch

Principe de fonctionnement

- A la volée (on-the-fly ou cut-through)
 - Recopie les trames vers l'interface de sortie dès que l'adresse du destinataire est connue.
 - Avantage :
 - Vitesse de commutation maximale
 - Inconvénients :
 - Pas de vérification du CRC
 - Recopie les trames en erreur

adresse destination	adresse source	protocole/ longueur	données couche supérieure	bourrage	CRC
---------------------	----------------	------------------------	---------------------------------	----------	-----

premier champ de la trame

Chapitre 2 – Switch

Principe de fonctionnement

- Stockage et retransmission (store-and-forward)
 - La trame complète est mise en mémoire
 - Avantage :
 - Fiabilité accrue avec le contrôle du CRC et de la longueur de la trame
 - Inconvénient :
 - Délai de commutation plus grand

adresse destination	adresse source	protocole/ longueur	données couche supérieure	bourrage	CRC
---------------------	----------------	---------------------	---------------------------	----------	-----

dernier champ de la trame

Chapitre 2 – Switch

Principe de fonctionnement

- A la volée adaptif (Adaptive Cut Through)
 - Même principe qu' A la volée.
 - Compte le nombre de trames en erreurs.
 - Si le nombre d'erreurs est trop important -> passage automatique en mode store and forward.
 - Si le taux d'erreur redevient normal -> retour au mode Cut Through.

Chapitre 2 – Switch Configurations

- Pas de configuration possible
- Console sur liaison série RS232 (CLI Command Line Interface)
- Console TelNet sur IP (CLI Command Line Interface)
- Serveur HTTP (Interface graphique)
- Interface graphique propriétaire
- Protocole SNMP (Simple Network Management Protocol)

Chapitre 2 – Switch

Types de commutateur

- Switch de table, compact, non configurable
- Switch configurable



Chapitre 2 – Switch

Types de commutateur

- Switch Professionnel



- Switch industriel



Chapitre 2 – Switch

Types de commutateur

- Datacenter Switch



Chapitre 2 – Switch

Types de commutateur

- Switch optique



- Switch PoE
Power on
Ethernet



Architecture Cisco



Chapitre 2 – Architecture Cisco

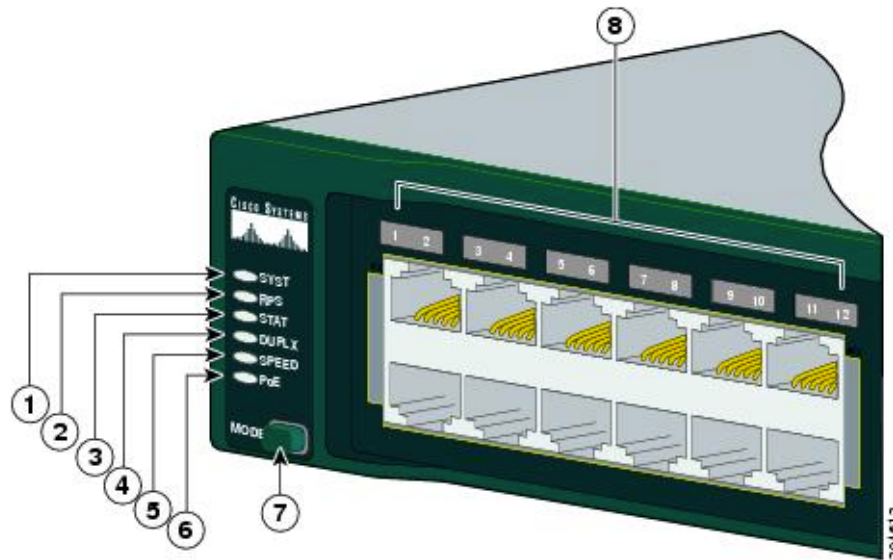
Switch Cisco 2950-2960

- Caractéristiques principales du switch 2960
 - Cisco Catalyst 2960 24 Switch (WS – C2960 - 24)
 - RAM : 16 Ko
 - Mémoire flash : 16 Ko
 - Nombre de ports :
 - 24 x Ethernet 100Base-T / 2 x Ethernet 1000Base-TX
 - Débit de transfert de données :
 - 100 Mbits/s et 1000 Mbits/s
 - Protocole de liaison de données :
 - Ethernet
 - FastEthernet
 - Protocole de gestion à distance :
 - SNMP,
 - RMON
 - Mode de communication :
 - Semi-duplex
 - duplex intégral



Chapitre 2 – Architecture Cisco Switch Cisco 2950-2960

Panneau avant du switch



1	SYST LED	5	Speed LED
2	RPS LED	6	PoE LED ¹
3	Status LED	7	Mode button
4	Duplex LED	8	Port LEDs

¹ The PoE LED is only on the Catalyst 2960 PoE switches.

Chapitre 2 – Architecture Cisco

Switch Cisco 2950-2960

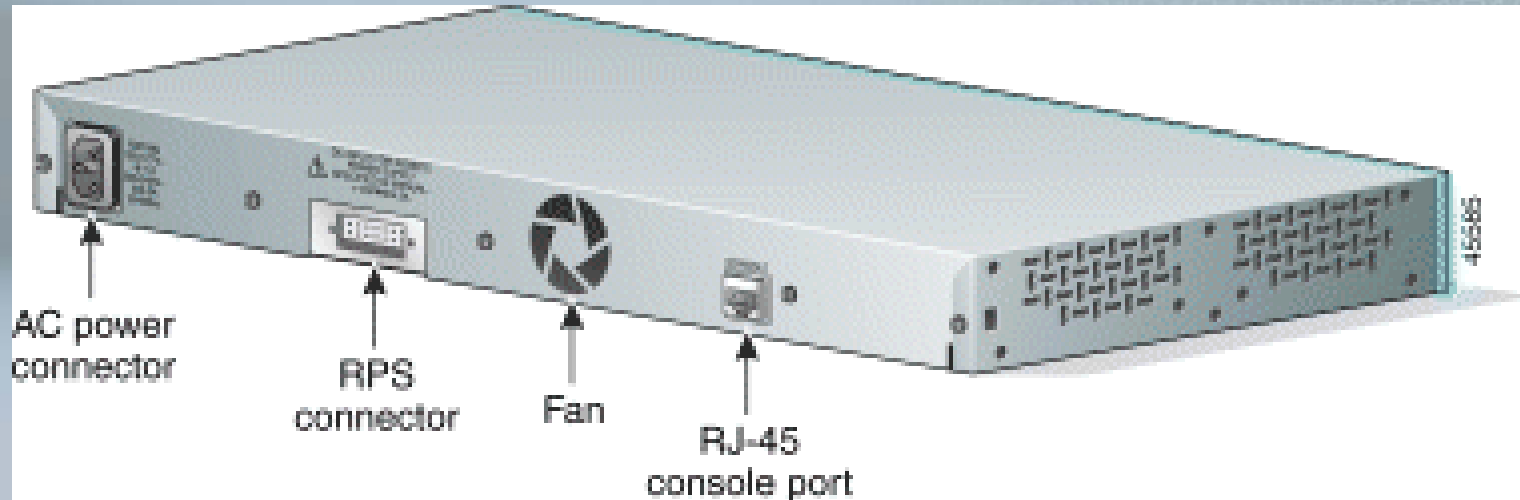
- Signification des LEDs
 - LED 1 : SYST
 - Eteint Le système n'est pas mis sous tension.
 - Vert Le système fonctionne normalement.
 - Ambre Le système est en mode configuration.
 - LED 2 : RPS «**R**edundant **P**ower **S**ystem (Système d'alimentation redondant)
 - LED 3, 4, 5, 6 : Port mode
 - STAT Mode status (défaut).
 - DUPLX Half-duplex ou duplex.
 - SPEED La vitesse de fonctionnement.
 - PoE Power on Ethernet (si disponible)



Chapitre 2 – Architecture Cisco

Switch Cisco 2950-2960

- Panneau arrière

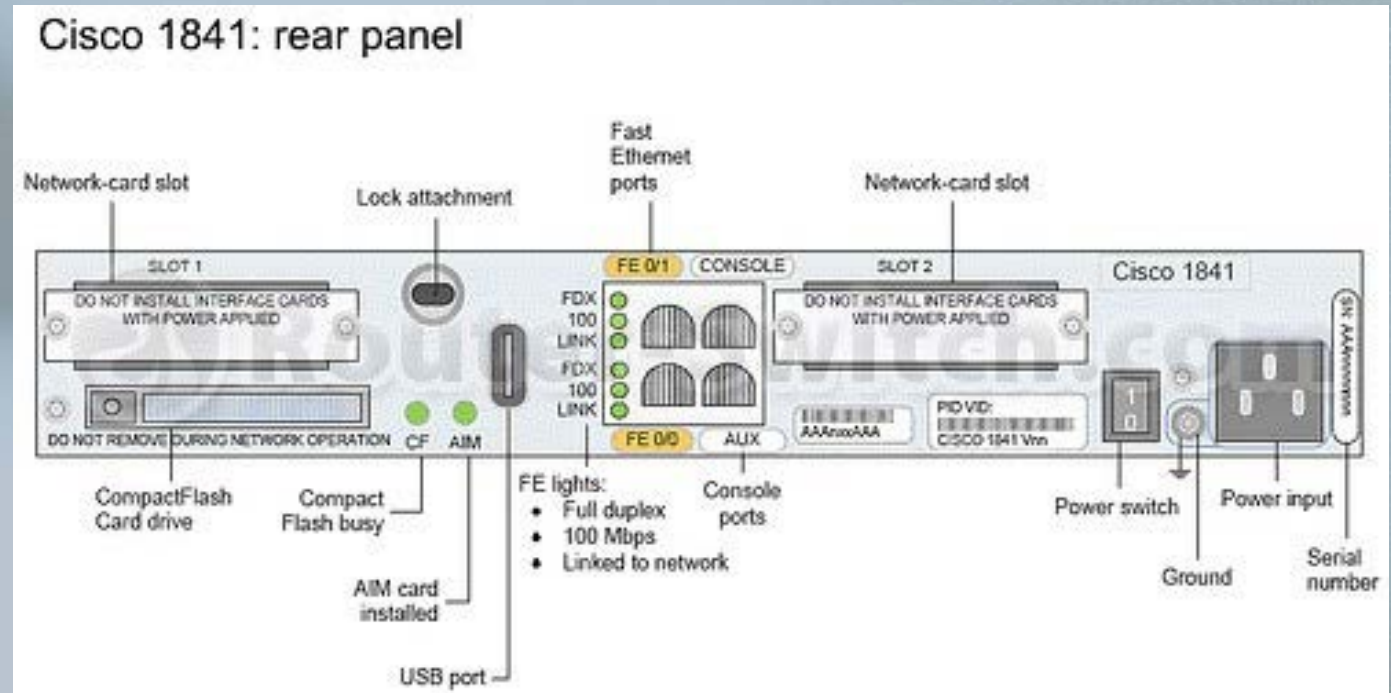


- Alimentation (Power supply)
- Alimentation redondante (RPS)
- Port Console RJ45

Chapitre 2 – Architecture Cisco

Routeur Cisco 1841

- Panneau arrière

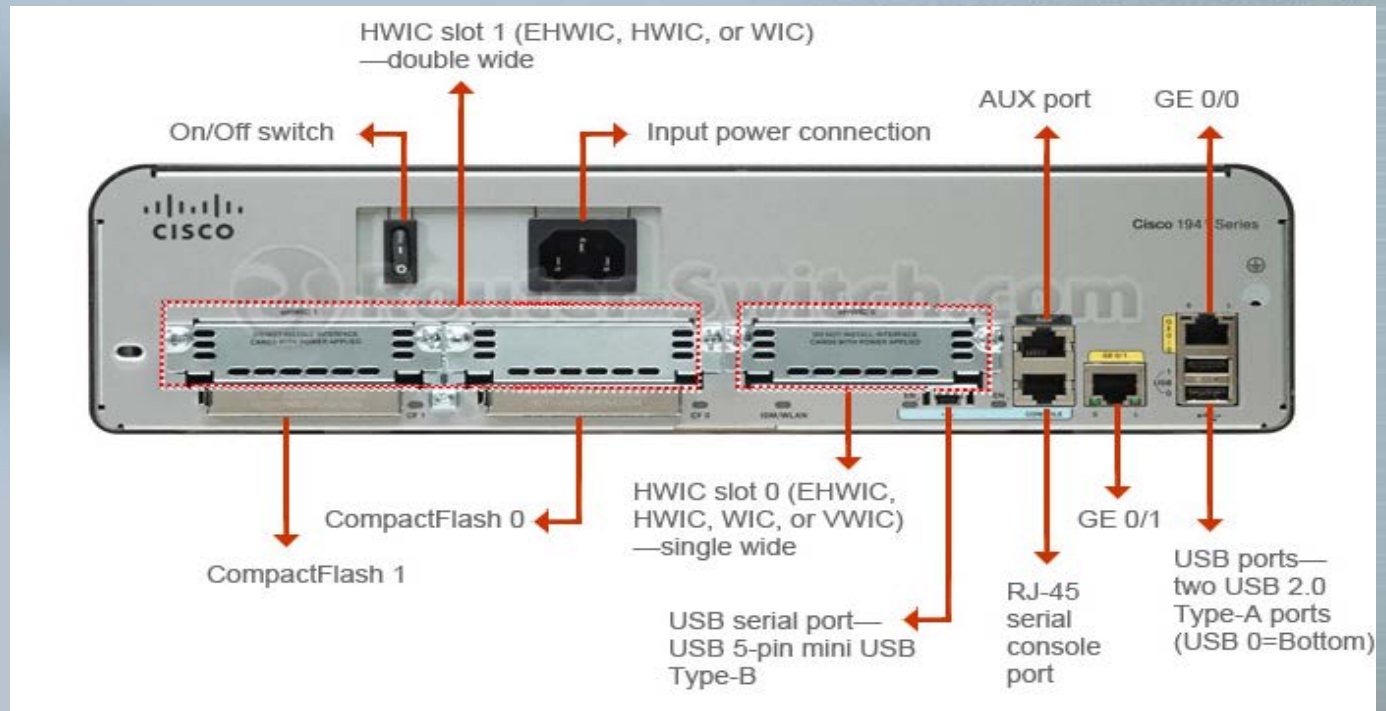


- FastEthernet 0/0 et 0/1
- Port Console RJ45

Chapitre 2 – Architecture Cisco

Routeur Cisco 1941

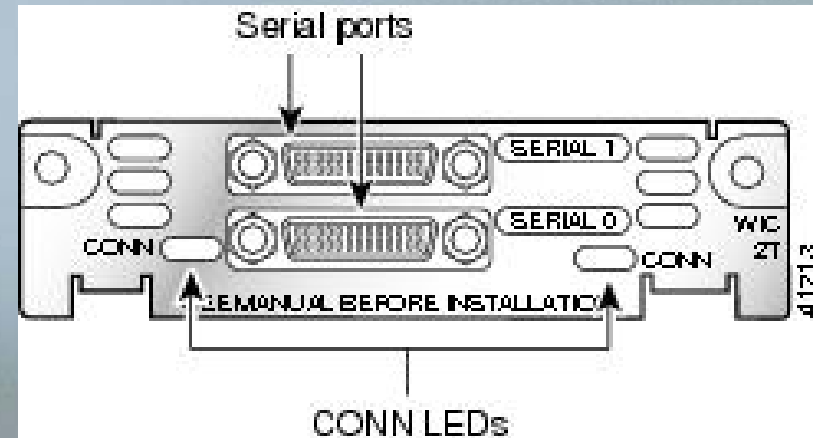
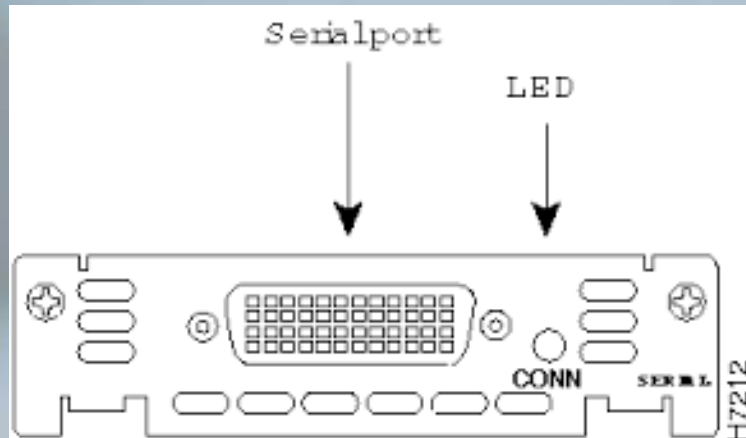
- Panneau arrière



- GigaEthernet 0/0 et 0/1
- Port Console RJ45
- Port USB 5-pin mini USB (à déconnecter si RJ45)

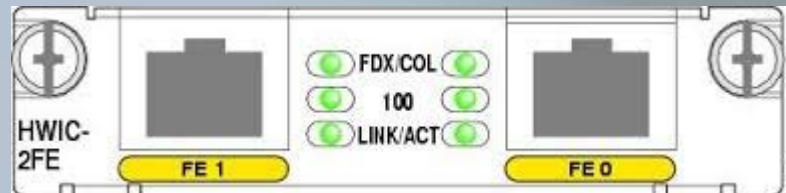
Chapitre 2 – Architecture Cisco Modules d'extension

- Panneau arrière



– serial 0 WIC-1T

serial 0 et 1 WIC-2T



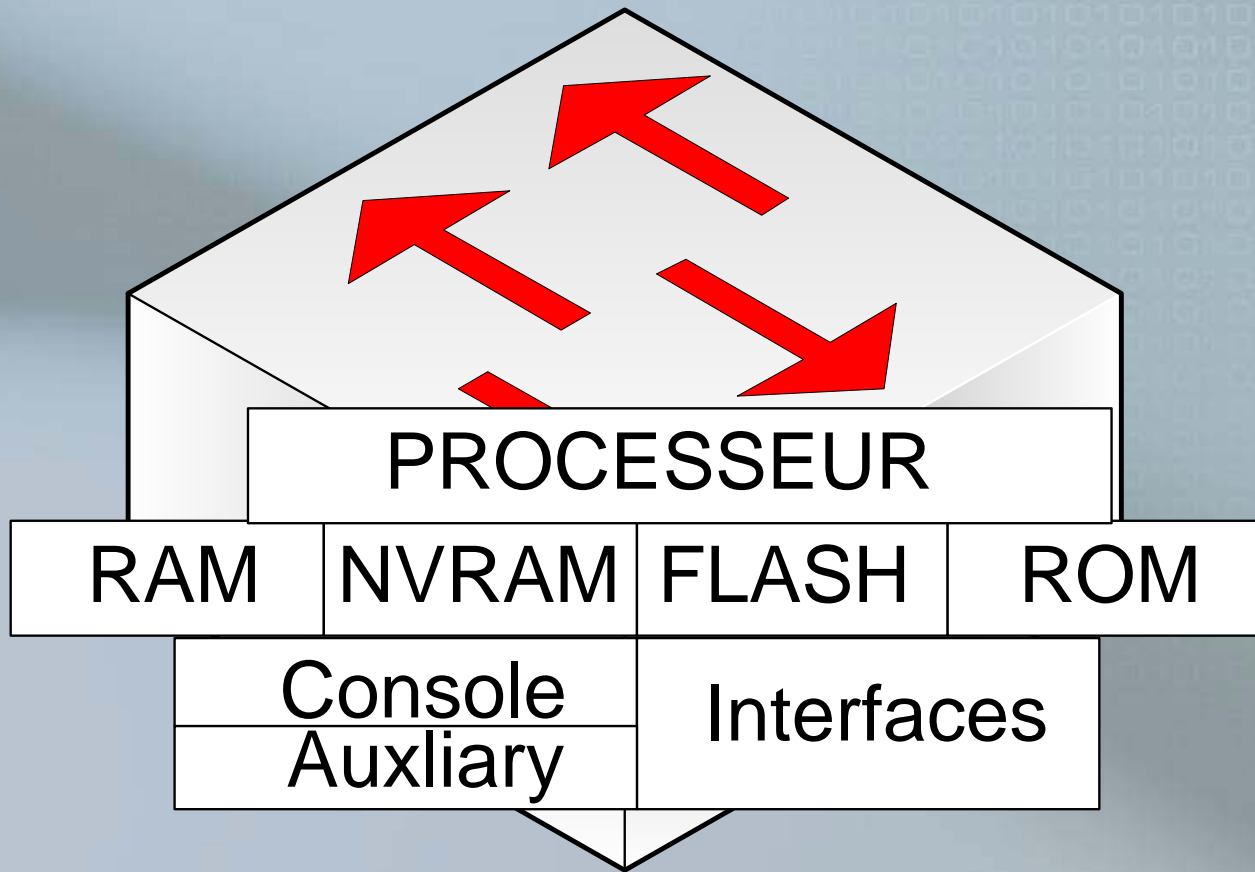
- Ethernet HIC-2FE



Chapitre 2 – Architecture Cisco

Architecture interne

Représentation de l'architecture interne



- Architecture interne du Architecture Cisco
 - Cisco IOS **Internetwork Operating System** est le logiciel qui fonctionne sur le matériel Cisco.
 - L'architecture interne du switch comporte divers éléments :
 - RAM Mémoire volatile
 - NVRAM Mémoire non volatile (fichier utilisateur)
 - FLASH Mémoire de stockage (image IOS, config de démarrage)
 - ROM Contient le BIOS
 - Interfaces Port RJ45
 - Console port série pour administration



- L'interface utilisateur est divisée en 3 modes de commandes :
 - Mode utilisateur : User EXEC mode
 - Mode privilégié : Privileged EXEC mode
 - Mode de configuration global : Global configuration mode

- User EXEC mode
 - visualisation limitée de la configuration
 - Représentation
 - *Switch*> : nom du switch + symbole >
 - *Router*> : nom du router + symbole >
 - Mode par défaut au démarrage



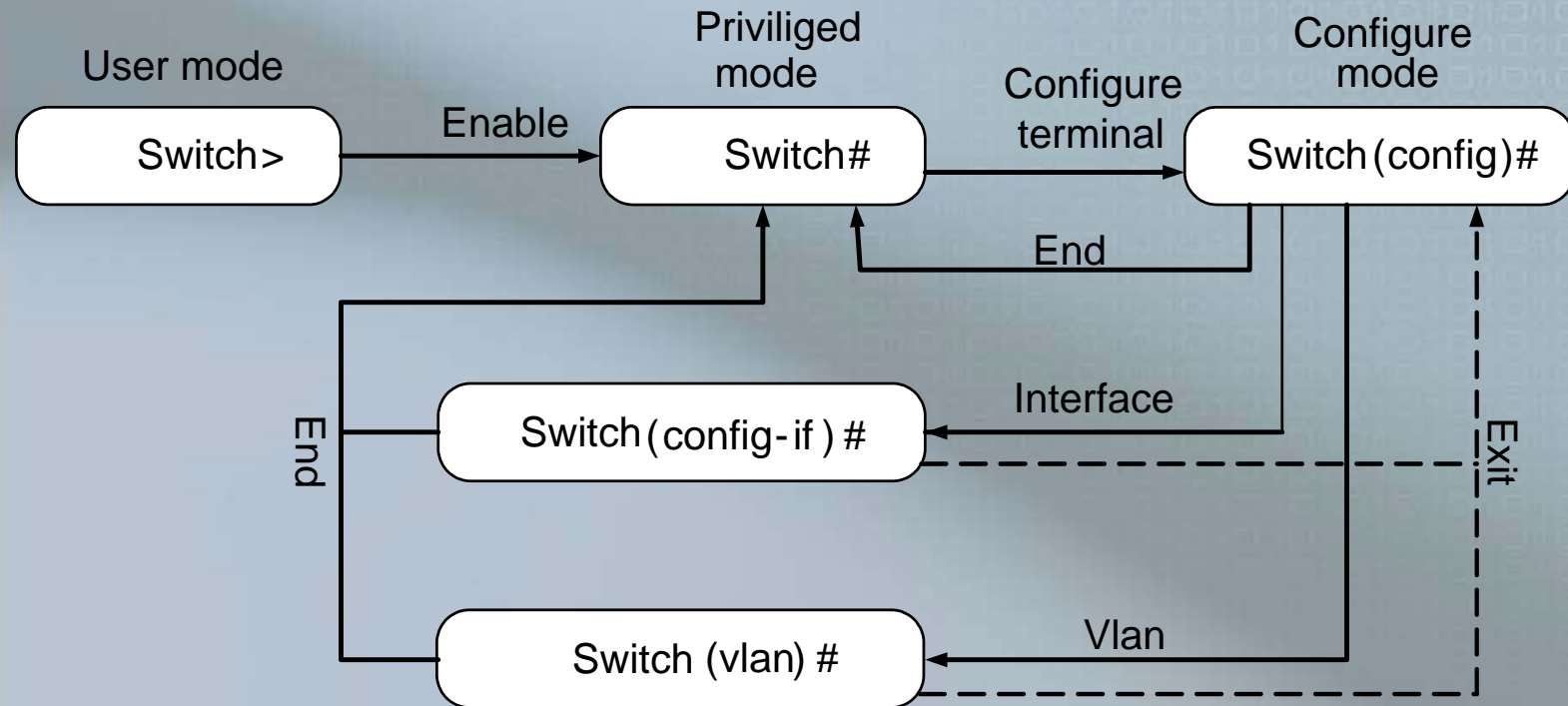
- Privileged EXEC mode
 - Visualisation détaillée
 - Tests
 - Debugging
 - Manipulation de fichiers
 - Représentation
 - *Switch#* : nom du switch + symbole #
 - *Router#* : nom du router + symbole #



- Global configuration mode
 - Commande qui affecte le système dans son ensemble
 - Configuration des interfaces
 - Configuration des VLANs
 - Représentation
 - *Switch(config)#* : nom du switch + (type de configuration) + symbole #
 - *Router(config)#* : nom du router+ (type de configuration) + symbole #

Chapitre 2 – Architecture Cisco Interface utilisateur

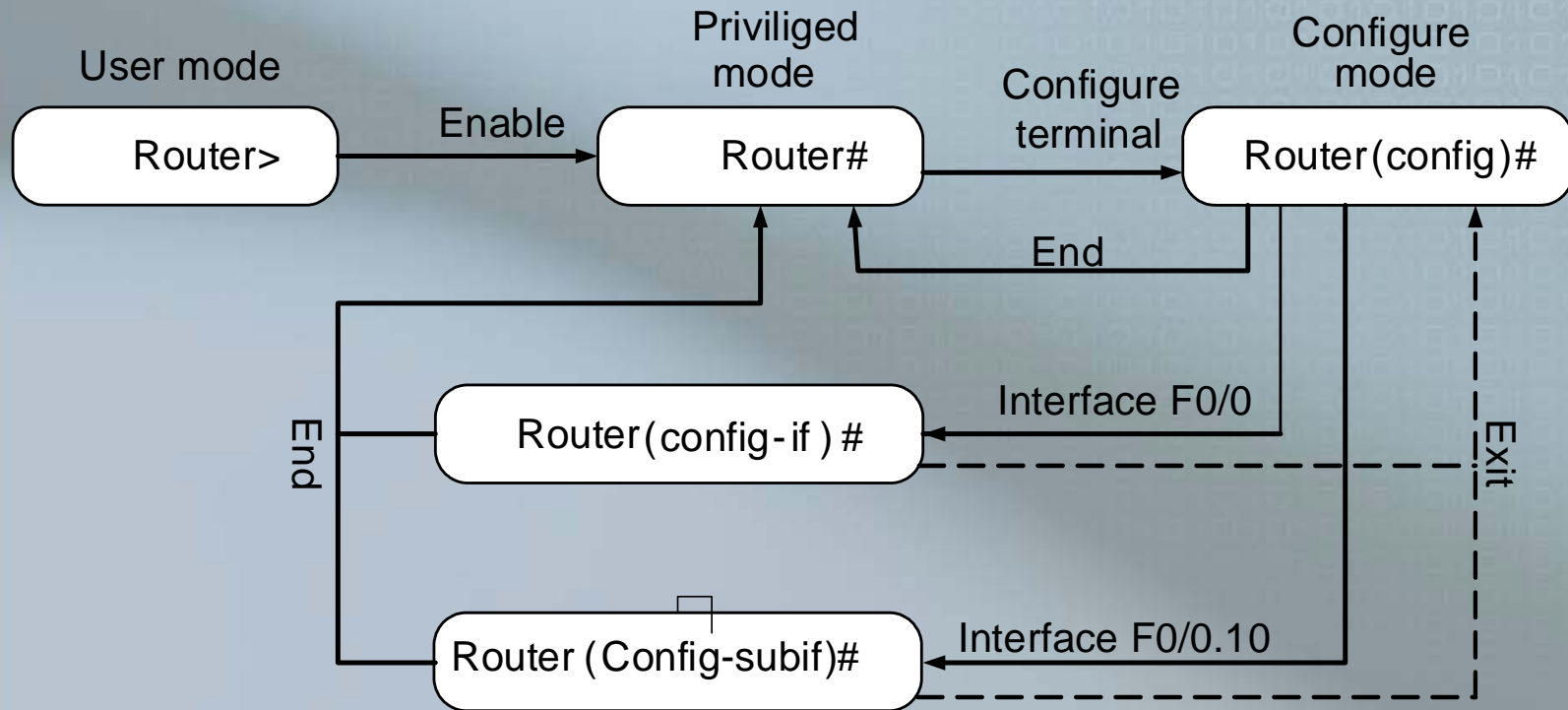
Schéma de principe de fonctionnement



Chapitre 2 – Architecture Cisco

Interface utilisateur

Schéma de principe de fonctionnement



Chapitre 2 – Architecture Cisco


Commande utiles

- ? : Obtenir la liste d'aide
- Show ? : Liste des commandes « show »
- Enable : Accès au mode privilégié
- Configure terminal : Accès au mode configuration global
- Exit : Pour descendre d'un niveau
- End : Pour se retrouver en mode Privilégié
- Tab : Permet de compléter la commande

Chapitre 2 – Architecture Cisco

Méthodes d'accès

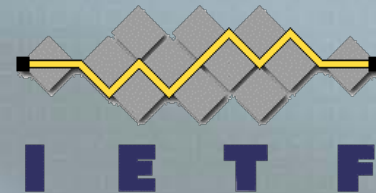
- Ligne de commande CLI
 - Utilisation d'un terminal
 - Port de console
 - Telnet
- Interface graphique
 - SDM Security Device Manager (HTTP)
 - CNA Cisco Network Assistant
- Sauvegarde et restauration
 - FTP / TFTP



Chapitre 3 – Protocoles et communications réseau

Chapitre 3 – Instance de normalisation

Généralités



Chapitre 3 – Instance de normalisation

Généralités

- Une norme désigne un ensemble de spécifications destiné à satisfaire un besoin de manière similaire.
- Il en résulte des règles servant de référence pour les constructeurs.
- Pour le consommateur, la normalisation est une garantie de compatibilité du mode fonctionnement.

Chapitre 3 – Instance de normalisation

Généralités

- La normalisation est issue d'organismes divers, de groupements de constructeurs, d'organismes internationaux.
- Une norme n'est pas obligatoire.
- Certaines sont rendues obligatoires par une réglementation.



Chapitre 3 – Instance de normalisation

Généralités

- Norme ou standard ?
 - Un standard est élaboré entre industriel au sein de consortiums
 - Une norme est établie par des organismes officiels (nationaux, internationaux,...)
 - La différence entre norme et standard est cependant très faible



Chapitre 3 – Instance de normalisation

Groupements de constructeurs

- Association regroupant la plupart des grands constructeurs informatiques
- But recherché :
 - Discussion sur l'élaboration des normes.
 - Emission de recommandations.
 - Statut non officiel.
 - Souvent adoptées au niveau international.



- Principaux groupements de constructeurs
 - ECMA : European Computer Manufactures Association. L'ECMA comprend tous les grands constructeurs (IBM, HP,...)
 - POSI : Promotion Conference for OSI in Japan. Association de six principaux constructeurs japonais.
 - EIA : Electronics Industries Association
 - TIA : Telecommunication Industry Association

Chapitre 3 – Instance de normalisation

Organisme national

- **Organisme suisse**
 - SNV : Schweizerischen Normen Vereinigung
 - La SNV représente directement la Suisse à la normalisation mondiale (ISO) et à la normalisation européenne (CEN)
 - Elle est la plaque tournante pour de nombreux autres réseaux nationaux et internationaux de normalisation

- Principaux organismes nationaux

- ANSI : American National Institute
- DIN : Deutsche Institute für Normung
- BSI : British Standard Institute
- AFNOR : Association Française de
NORmalisation
- IBN : Institut Belge de Normalisation



- Principaux organismes Européens
 - ETSI : European Telecommunication Standards Institute
 - Normalise les réseaux de télécommunications publics
 - CEN (Comité Européen de normalisation)
 - CENELEC (Comité Européen de normalisation pour l'Electrotechnique)



- Principaux organismes internationaux
 - ISO : International Standardization Organization
 - Composant des représentants nationaux de plus de 150 pays
 - CEI : Commission Electrotechnique Internationale
 - UIT-T : Union Internationale des Télécommunications



Chapitre 3 – Instance de normalisation Organismes liés à Internet

- Organismes actifs pour Internet
 - IAB : Internet Activities Board, qui assure par ses publications (RFC : Request For Comments) l'homogénéité de la communauté TCP/IP.
 - IETF : Internet Engineering Task Force, travaille à l'élaboration des protocoles utilisés sur Internet.
 - IRTF : Internet Research Task Force, structurés en groupe de recherches pour les protocoles futurs.

Chapitre 3 – Instance de normalisation Organismes liés à Internet

- Organismes actifs pour Internet
 - IANA : Internet Assigned Number Authorityrting Organization.
 - Responsable de la coordination des DNS root, de l'adressage IP et des protocoles Internet.
 - ICANN : Internet Corporation for Assigned Names and Numbers.
 - Gestion des noms de domaine et distribution des plages IP.
 - W3C : World Wide Web Consortium.
 - Développement des applications (http, HTML)



Chapitre 3 – Instance de normalisation RFC

- RFC : Request For Comments
- Documents officiels décrivant les aspects techniques :
 - D'Internet
 - De différent matériel informatique (routeur, serveur DHCP,...)
- RFC 1 « Logiciel hôte » 7 avril 1969



Chapitre 3 – Instance de normalisation RFC

- L'IAB assigne à chaque RFC un statut et un état.
 - L'état indique le progrès du travail de normalisation (Initial, Standard, Experimental)
 - Le statut indique les conditions dans lesquelles le protocole peut être utilisé (Required, Recommended, elective)



Chapitre 3 – Instance de normalisation RFC

- Principaux protocoles d'Internet et leur RFC respectives.
 - ARP : Statut Elective RFC 826
 - IP : Statut Required RFC 791
 - ICMP : Statut Required RFC 792
 - UDP : Recommended RFC 768
 - TCP : Recommended RFC 793



- Pourquoi a-t-on besoin d'un modèle de communication ?
 - Uniformiser les éléments du réseau afin de permettre le développement et le soutien multi-constructeur.
 - Assurer une parfaite compatibilité des différentes technologies.
 - Diviser les communications sur le réseau en éléments plus petits et plus simples. (Réduit la complexité des systèmes)
 - Permettre à différents types de matériel et de logiciel réseau de communiquer entre eux. (Les interfaces physiques sont uniformisées)



- Utilisation du modèle OSI
 - En 1978, l'organisme ISO (International Standards Organisation) a publié un ensemble de spécifications décrivant une architecture réseau.
 - Prôné pour une utilisation de protocoles et de standards identiques.
 - Publication du modèle de référence OSI en 1984
 - Guide universel de mise en réseau.

Chapitre 3 – Modèles de normalisation

Le modèle OSI

- OSI signifie
Open
Systems
Interconnection

(Systèmes ouverts interconnectés)

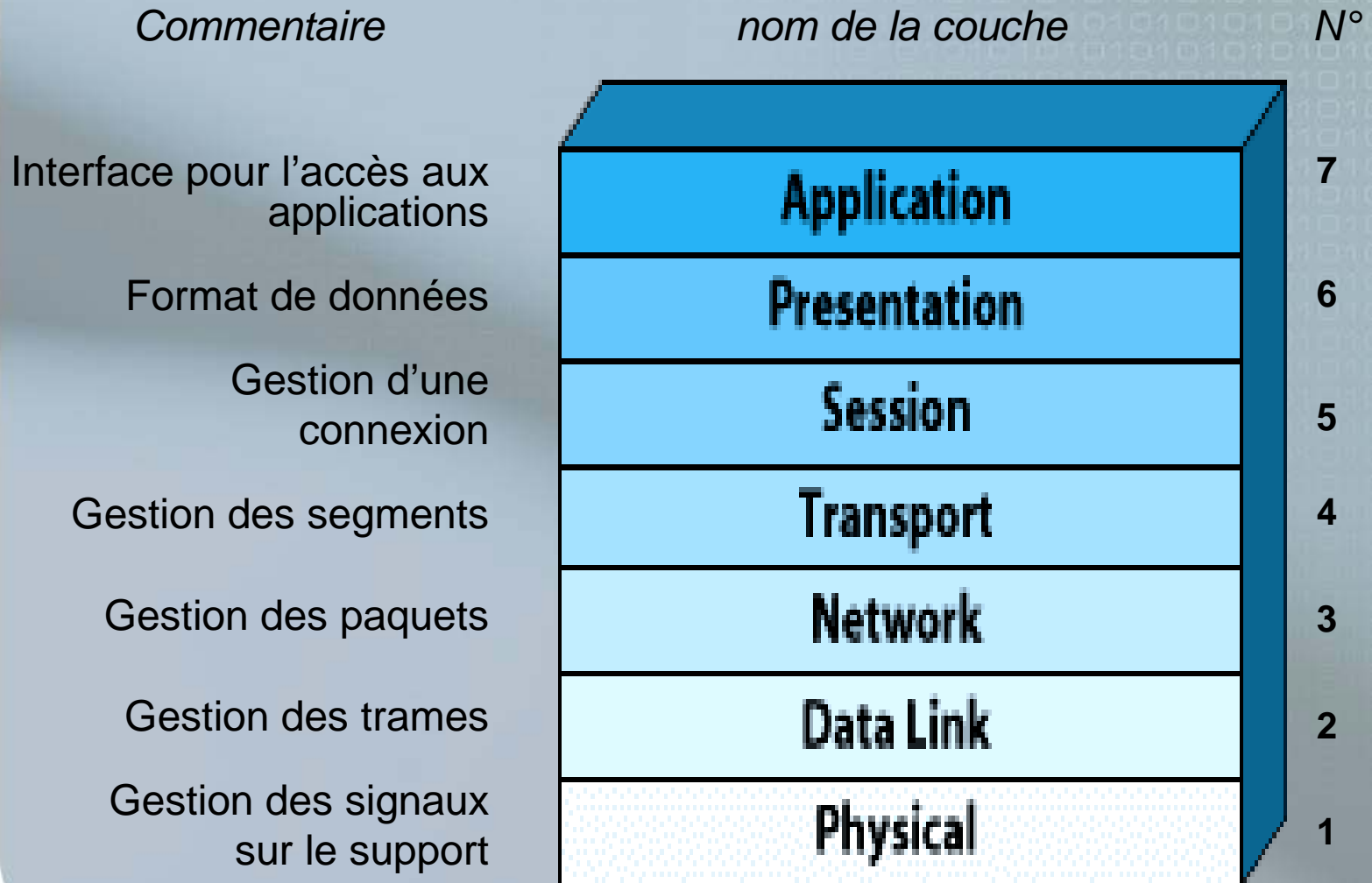


- Principe de l'architecture OSI
 - Division de la communication réseau en sept couches.
 - Chaque couche représentant différentes fonctionnalités et services.
 - Spécifie la manière dont les couches communiquent et coopèrent avec les couches directement voisines.
 - Empêche les changements apportés à une couche d'affecter les autres couches.



Chapitre 3 – Modèles de normalisation

Le modèle OSI



- Couche 1 « Physique »
 - Convertit en signaux électriques, optiques ou hertziens les impulsions qui entrent et sortent du canal de transmission.
 - Transmet le flux de bits, brut et non structuré, par l'intermédiaire d'un canal de transmission.
- Ex : Code Manchester, FHSS,...

- Couche 2 « Liaison de données »
 - Chargée de transférer, sans erreur, les paquets entre ordinateurs, par la couche physique.
 - Détecte tous les problèmes qui auraient pu survenir sur le paquet lors de la transmission.
- Ex: PPPoE, Ethernet, CSMA/CA, ARP,...

- **Couche 3 « Réseau »**
- Se charge de la traduction des adresses physiques en adresses IP et de l'adressage des paquets IP.
- Détermine la route en fonction de l'état du réseau, de la priorité du service et d'autres facteurs.
- Ex: IP, ICMP, OSPF,...



- Couche 4 « Transport »
 - Fournit un circuit point à point entre les applications des utilisateurs finaux.
- Ex: TCP, UDP
 - Gère la transmission de paquets (erreurs, ordre, perte, duplication de données) selon le protocole utilisé.
- Ex: TCP



- Couche 5 « Session »
 - Permet à deux ordinateurs de créer, d'utiliser et de clore une connexion.
 - Effectue la reconnaissance des noms et des fonctionnalités de sécurité nécessaire.
 - Décide qui peut transmettre, quand et pendant combien de temps.
- Ex: EAP, TLS, H323,...



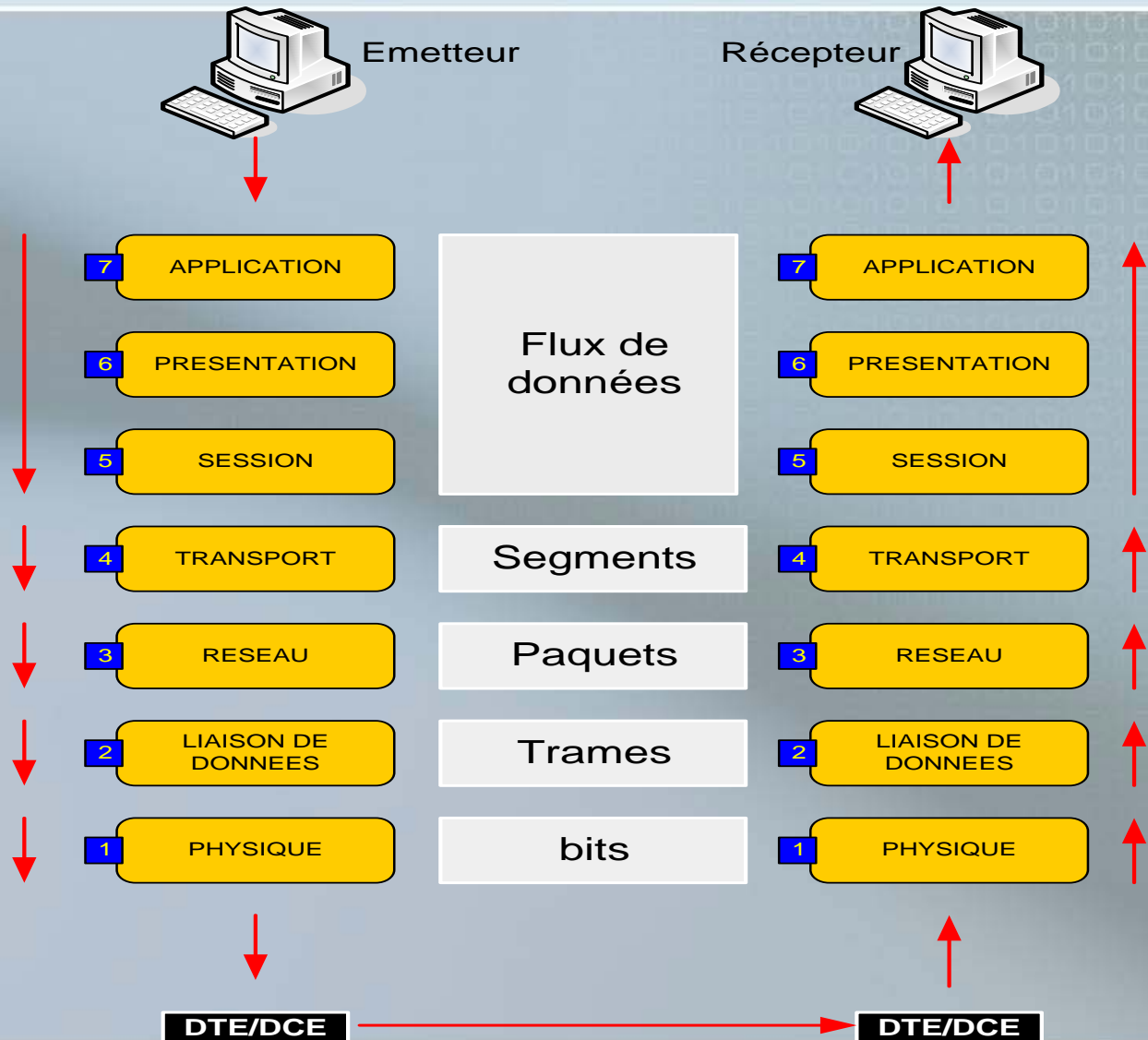
- Couche 6 « Présentation »
 - Détermine le format utilisé pour échanger des données.
 - Crée un format intermédiaire communément reconnu.
 - Se charge de la traduction et du chiffrement des données et de la conversion des jeux de caractères.
- Ex: DES, MIME, ASCII, UNICODE, MIDI,...



- Couche 7 « Application »
 - Services liés directement aux applications utilisateurs.
 - Utilitaires de transfert de fichiers, accès aux bases de données, messagerie,...
 - Peuvent être des programmes protocolaires.
- Ex: FTP, Http, TelNet, DNS, TFTP, SMTP, DHCP, POP3,...

Chapitre 3 – Modèles de normalisation

Le modèle OSI

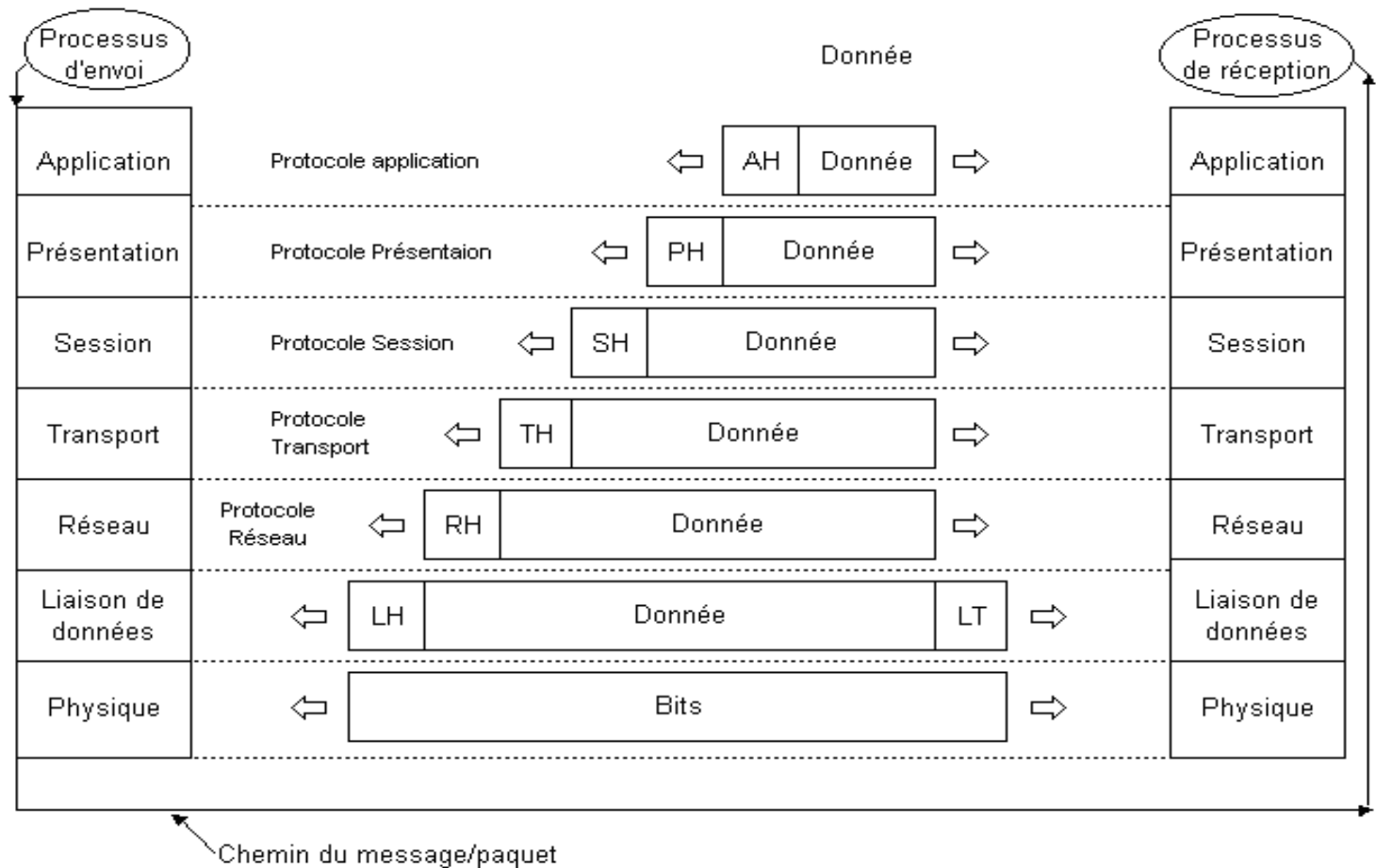


- Principe de fonctionnement
 - Lorsque une information change de couche, le protocole lui rajoute un en-tête spécifique (Header).
 - Elle considère que ce qui provient de la couche supérieure sont des données.
 - Elle encapsule toutes les couches pour l'envoi des données.
 - Elle désencapsule toutes les couches à la réception.



Chapitre 3 – Modèles de normalisation

Le modèle OSI



AH = En-tête application, etc ...

Modèle DoD - TCP/IP



- Généralités
 - Modèle de référence appelé DoD (Department of Defense)
 - Garantir que les paquets de données atteignent à chaque fois un point quelconque à partir de tout autre point.
 - Standard sur lequel repose INTERNET aussi appelé «modèle TCP/IP».



- **Architecture du modèle TCP/IP - DoD**
 - Modèle en 4 couches
 - La couche **Application** qui regroupe les couches application, présentation et session.
 - La couche **Transport**
 - La couche **Internet**
 - La couche d'**Accès au réseau** qui regroupe les couches physique et liaison de données.



Les 4 couches du modèle TCP/IP

- Données
- Segment
- Paquet
- Bit

Application

Transport

Internet

**Accès
réseau**

- **Différences OSI – TCP/IP**

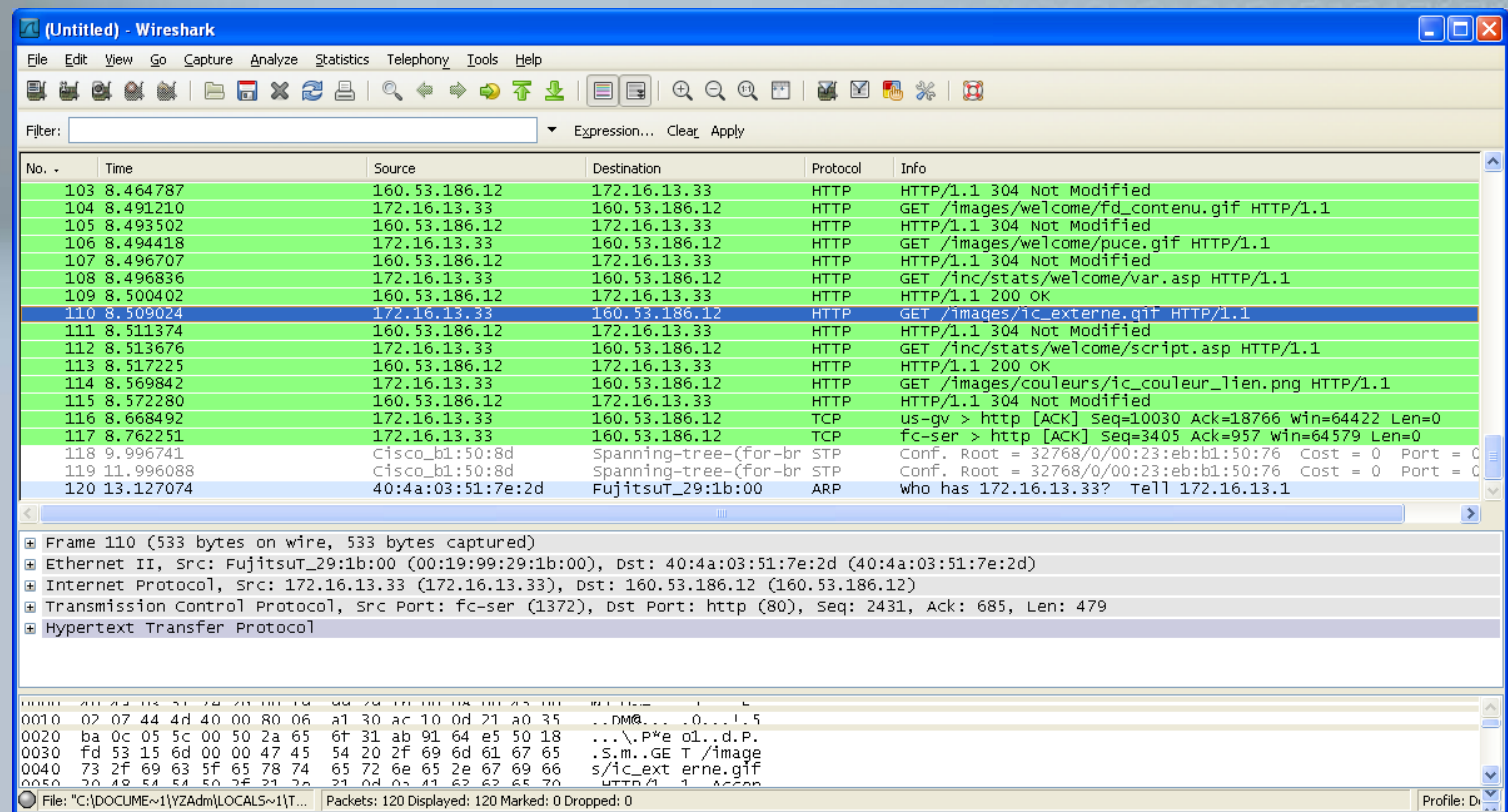
- Le modèle TCP/IP met l'accent sur une souplesse maximale, au niveau de la couche application.
- TCP/IP est plus simple à mettre en œuvre, car il comporte moins de couches.




Chapitre 3 – Modèles de normalisation

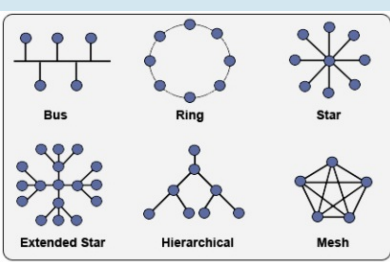
Démonstration

- Analyseur de protocole : Wireshark





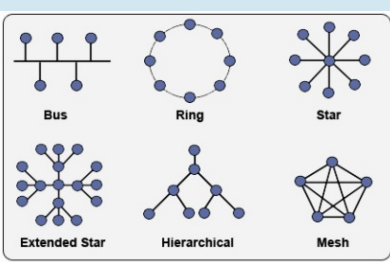
Chapitre 4 – Accès réseau



Chapitre 4 – Méthode d'accès Généralités

- Un réseau repose sur un support de transmission
 - Des câbles
 - Cuivre
 - Fibre optique
 - Les liaisons sans-fil
 - Ondes radio
 - Infrarouge



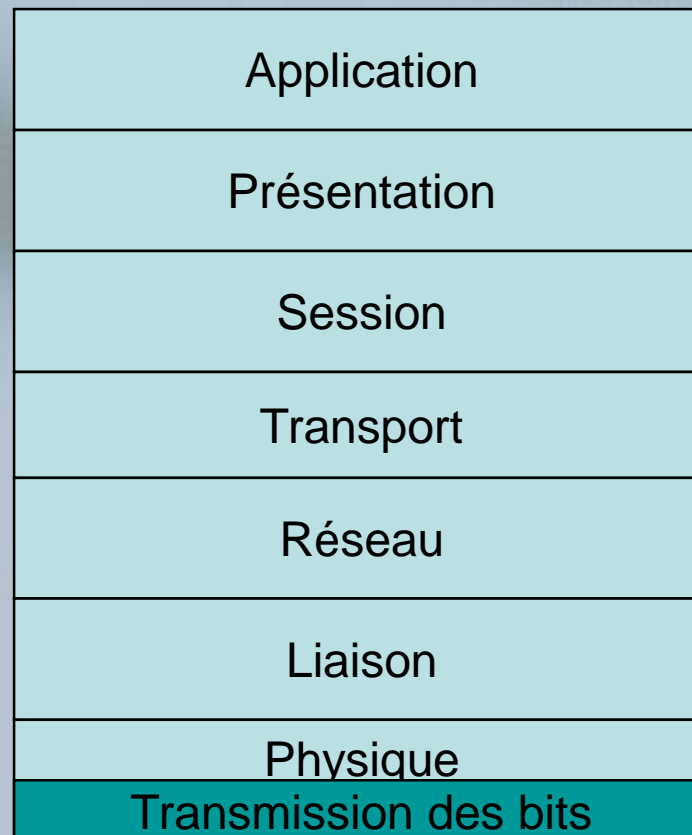


Chapitre 4 – Méthode d'accès Généralités

- Il existe plusieurs topologies
 - **Bus** : les machines sont connectées en série
 - **Anneau** : Interconnexion des opérateurs télécom
 - **Etoile**: les machines sont connectées à un point de distribution.
 - **Etoile étendue ou arbre**: Les switchs et les machines sont interconnectés.
 - **Hiérarchique** : Une arborescence est créée
 - **Maillé** : Plusieurs chemins sont possibles

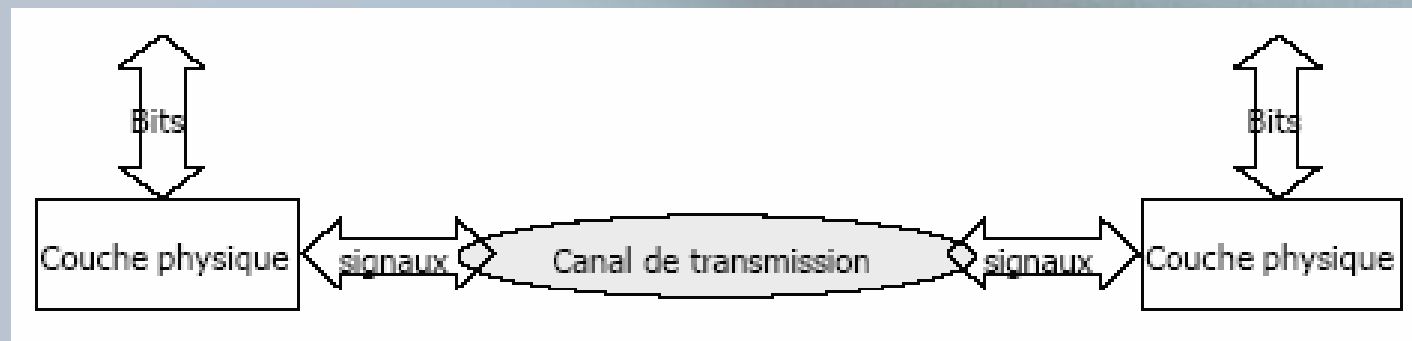
Chapitre 4 – Méthode d'accès Couche physique

Représentation en fonction du modèle OSI



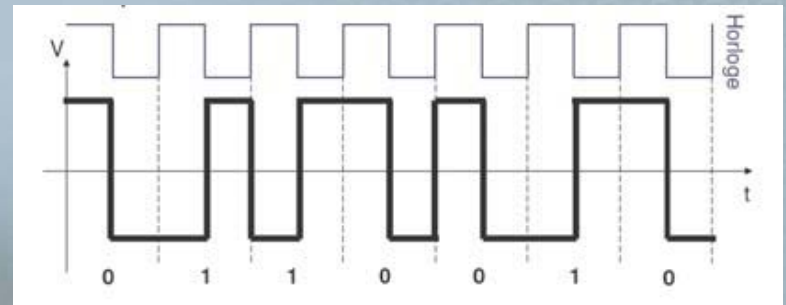
Chapitre 4 – Méthode d'accès Couche physique

- Fonction de la couche physique
 - Transformer une suite de bits en signaux.
 - S'adapter au canal de communication.
 - Partager le canal de communication.



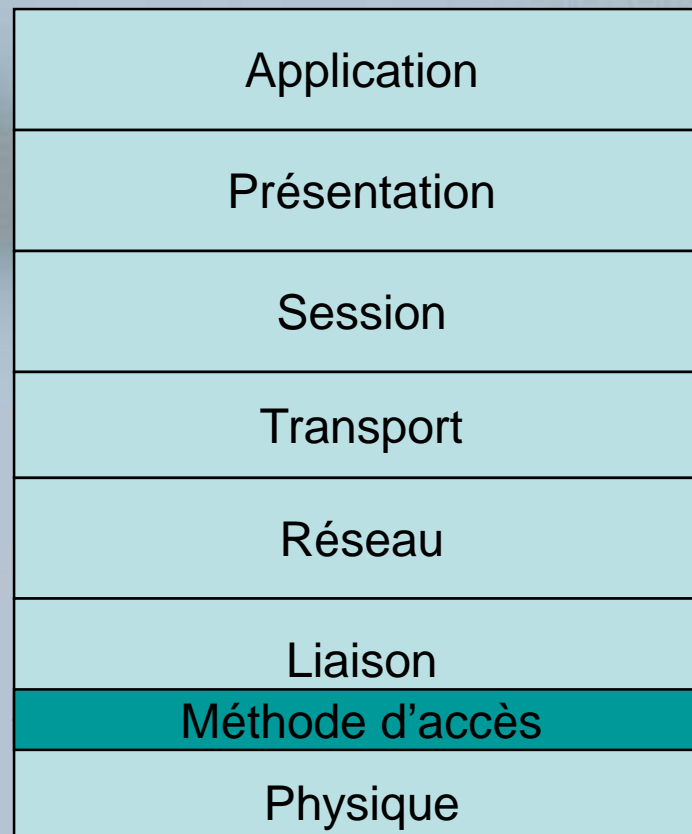
Chapitre 4 – Méthode d'accès Couche physique

- Méthode de codage des bits
 - Code Manchester pour Ethernet

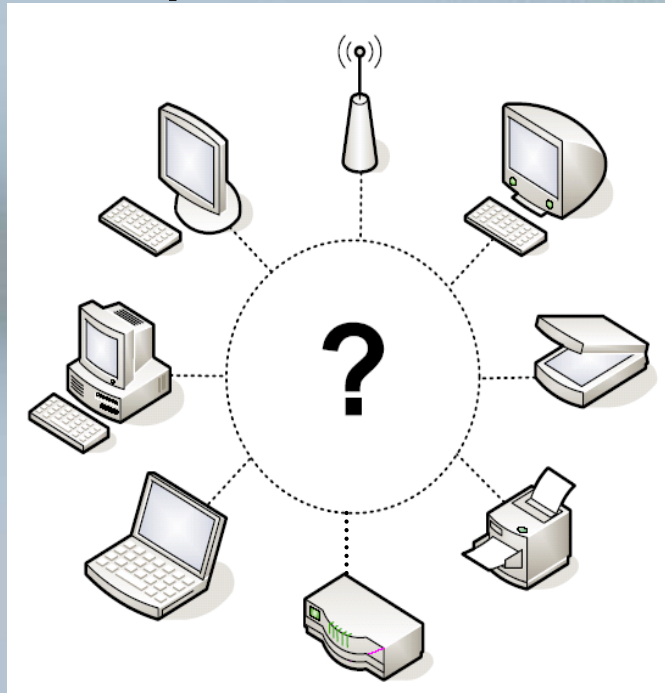


- Méthode WiFi
 - FHSS Frequency Hoping spread spectrum
 - DSSS Direct sequence spread spectrum
- Méthode optique
 - 8B/10B, 64b/66b
 - Tout symbole de 8 bits est codé en un symbole de 10 bits

Représentation en fonction du modèle OSI



- Problématique



- Que faire si toutes les machines veulent accéder au support de transmission en même temps !

- Le rôle des méthodes d'accès
 - Elles représentent un ensemble de règles :
 - Quand et comment placer les données sur le support.
 - Comment récupérer les données.
 - Comment contrôler et réguler le trafic.
 - Elles procurent l'illusion de simultanéité.
 - Elles garantissent les mêmes règles d'accès pour tous les accès au réseau.



Chapitre 4 – Méthode d'accès


Types de méthode d'accès

- Principales méthodes d'accès
- **Méthodes à accès aléatoire dites de « Contention ».**
 - Chaque station peut émettre dès qu'elle le désire ce qui implique un risque de conflit.
 - **Exemple :**
 - CSMA/CD (*Carrier Sense Multiple Access with Collision Detect*)
 - CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*)
 - DCF (*Distributed Coordination Function*) mode ad hoc et infrastructure

- Principales méthodes d'accès
- Méthodes déterministes dites par « Election »
 - La gestion de l'accès est confiée à un arbitre.
 - L'élection de la station peut être effectuée :
 - Par consultation : toutes les stations sont consultées dans un ordre fixe
 - Par sélection : les stations qui veulent émettre envoient une requête.

Exemple :

- Passage de jeton
- Commutation
- PCF (*Point Coordination Function*) mode infrastructure



Chapitre 5 – Ethernet

- Historique :
 - Projet ALOHA
 - Communication radio entre des machines éparpillées (Université de Hawaii, ca. 1970)
 - Ethernet expérimental à 3 Mbit/s (Xerox, 1973)
 - Ethernet à 10 Mbit/s (Digital, Intel et Xerox, 1982)
 - Normalisation 802.3 (IEEE, 1985)
 - Fast Ethernet 100 Mb/s (1997)
 - Giga Ethernet
 - 10G,40 et 100GEthernet



Chapitre 5 – Ethernet Codifications

- Codifications en fonction des vitesses et supports physiques
- Notation classique :
 - <débit> <codage> <type de support>
 - Débit, en Mbits/s ou Gbits/s
 - Codage : *Base* (bande de base) ou *Broad* (modulation)
 - Type de support
- Exemple :
$$100 \text{ BaseT2} = \left\{ \begin{array}{l} \text{débit} = 100 \text{ Mbit/s} \\ \text{codage bande de base} \\ \text{Type de support 2 Twisted pair} \end{array} \right.$$

Chapitre 5 – Ethernet

Codifications

Synthèse des normes Ethernet

Nom commercial	Vitesse	Dénomination physique	Standard	Support, longueur
Ethernet	10 Mbps	10BASE-T	IEEE 802.3	Cuivre, 100 m
Fast Ethernet	100 Mbps	100BASE-TX	IEEE 802.3u	Cuivre, 100 m
Gigabit Ethernet	1000 Mbps	1000BASE-SX, 1000BASE-LX	IEEE 802.3z	Fibre, 550 m, 5 Km
Gigabit Ethernet	1000 Mbps	1000BASE-T	IEEE 802.3ab	Cuivre, 100 m
10Gigabit Ethernet	10 Gbps	10GBASE-SR, 10GBASE-LR	IEEE 802.3ae	Fibre, 300 m, 25 Km
10Gigabit Ethernet	10 Gbps	10GBASE-T	IEEE 802.3an	Cuivre, 100 m

Représentation en fonction du modèle OSI



Chapitre 5 – Ethernet

Format des trames Ethernet

Emission d'une trame



- Préambule : permet la synchronisation du récepteur.
- Début de trame : annonce le début de la transmission.
- Espace inter-frames : permet de bien séparer les trames successives.

Chapitre 5 – Ethernet

Format des trames Ethernet

Trames Ethernet II vs trame IEEE802.3

Ethernet II

Ethernet II					4
6 octets	6 octets	2 octets	de 46 à 1500 octets	octet	
Adresse destination	Adresse source	Type : Protocole	Données	Bourrage	CRC

IEEE 802.3

IEEE 802.3

6 octets	6 octets	2 octets	de 49/54 à 1500 octets		4 octet	
Adresse destination	Adresse source	Type : Longueur données	L L C	Données	Bourrage	FCS

- Sous-couche LLC (link layer controler) applicable

- Taille des trames
 - Taille maximale = 1518 octets
 - Empêche une station de monopoliser le canal pendant trop longtemps
 - Valeur arbitraire
 - Taille minimale = 64 octets
 - Détection des collisions
 - 64 octets = plus petite trame correcte



Chapitre 5 – Ethernet

Champ des en-têtes

Adresse destination	Adresse source	Type : Protocole longueur	Données	Bourrage	CRC
---------------------	----------------	---------------------------------	---------	----------	-----

- **Adresse destination**
 - Adresse physique du destinataire (MAC address)
- **Adresse source**
 - Adresse physique de la source (MAC address)
- **Type**
 - Protocole : Protocole utilisé (Ethernet II)
 - Longueur des données : Total des données (IEEE 802.3)
- **Données + bourrage** : Informations à transmettre
- **Contrôle d'erreur** : CRC (Cyclic Redundancy Check) (Eth II)
FCS (Frame Check Sequence) (IEEE 802.3)

- Format d'une MAC Address
 - Les adresses MAC comportent 6 octets (48 bits)
 - 3 octets administrés par le constructeur.
 - 3 octets représentants le numéro de série de la carte.

00-19-99

-

34-56-CD

3 octets : code constructeur

3 octets : numéro de série

Adresse **unique** (au monde) d'une interface Ethernet / IEEE802.3
(Environ 10^{14} adresses différentes possibles)

Chapitre 5 – Ethernet

La MAC Address

Exemple de numéro de constructeurs

Code fabricant sur 3 octets, en hexadécimal	Vendeur / fabricant
00-00-0C	Cisco
00-03-93	Apple
02-80-8C	3Com
08-00-20	Sun
08-00-5A	IBM

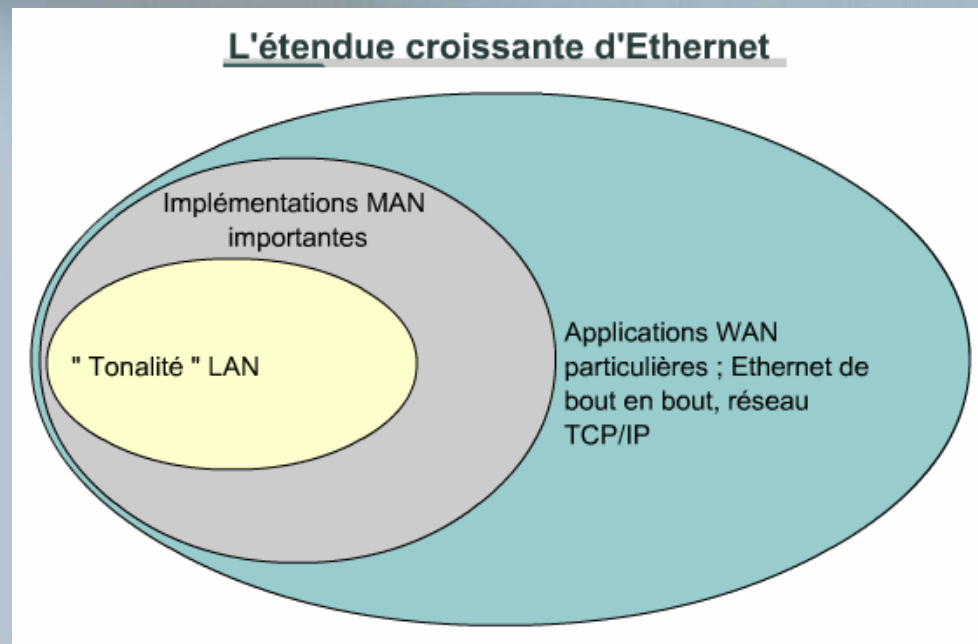
Début d'adresse MAC : exemples
(source :

<http://standards.ieee.org/regauth/oui/index.shtml>)

Chapitre 5 – Ethernet

Evolution future

- Multi Gigabit Ethernet
 - GigaEthernet largement commercialisé
 - 10 GigaEthernet devient abordable
 - 40, 100 GigaEthernet (802.3ba en 2010)
 - Futur 1 TeraEthernet et plus



Protocole ARP



- ARP signifie
Address
Resolution
Protocol

(Protocole de résolution d'adresses)



Représentation en fonction du modèle OSI



Chapitre 5 – ARP Architecture

Application

DHCP

Transport

TCP

UDP

Réseau

IP

ARP

Liaison

Ethernet / IEEE 802.3



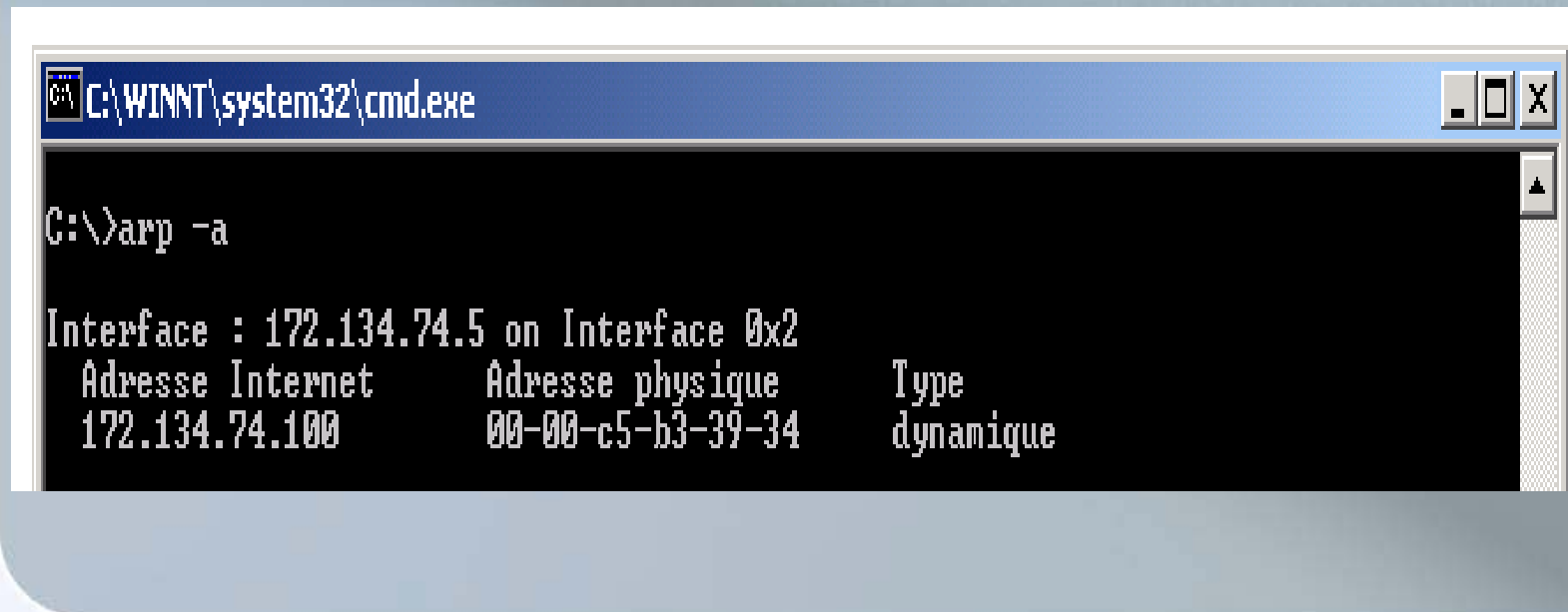
- *Couche liaison (Ethernet)*
 - Les trames sont échangées en utilisant les adresses MAC.
- Couche réseau (IP)
 - Les paquets sont échangés en utilisant les adresses IP.
- Correspondance ARP
 - Adresse MAC \longleftrightarrow Adresse réseau(IP)



Chapitre 5 – ARP

Protocole ARP

- Table de correspondance (*cache*) dynamique
 - Construite et mise à jour par le système
 - Chaque ligne a une durée de vie finie



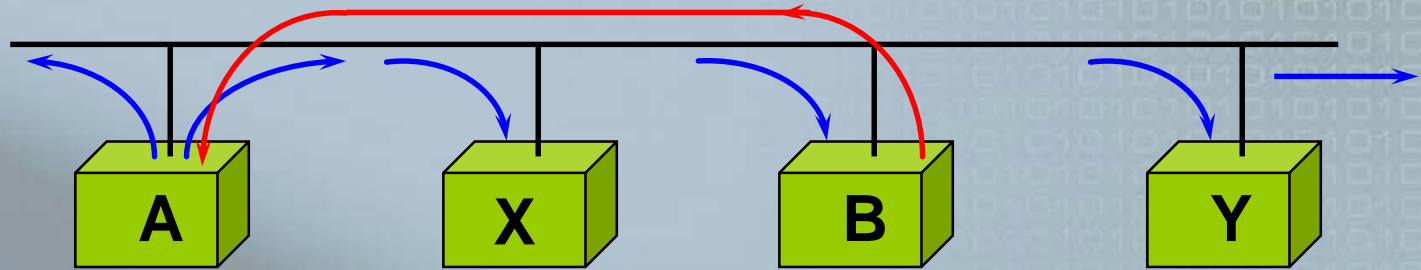
The screenshot shows a Windows command prompt window with the title bar 'C:\WINNT\system32\cmd.exe'. The command 'C:\>arp -a' has been entered. The output displays the ARP table for the interface 172.134.74.5 on interface 0x2. It lists one entry with the Internet address 172.134.74.100, the physical address 00-00-c5-b3-39-34, and the type 'dynamique'.

```
C:\>arp -a

Interface : 172.134.74.5 on Interface 0x2
  Adresse Internet      Adresse physique      Type
  172.134.74.100        00-00-c5-b3-39-34    dynamique
```


Chapitre 5 – ARP

Principe de fonctionnement



- L'association **Adresse physique - Adresse IP** de l'émetteur est incluse dans la requête ARP de manière à ce que les récepteurs enregistrent l'association dans leur propre mémoire cache
- Pour connaître l'adresse physique de B à partir de son adresse IP, la machine A **diffuse une requête ARP** qui contient l'adresse IP de B vers toutes les machines; la machine B **répond avec un message ARP** qui contient la MAC Address.

Chapitre 5 – ARP

Commandes

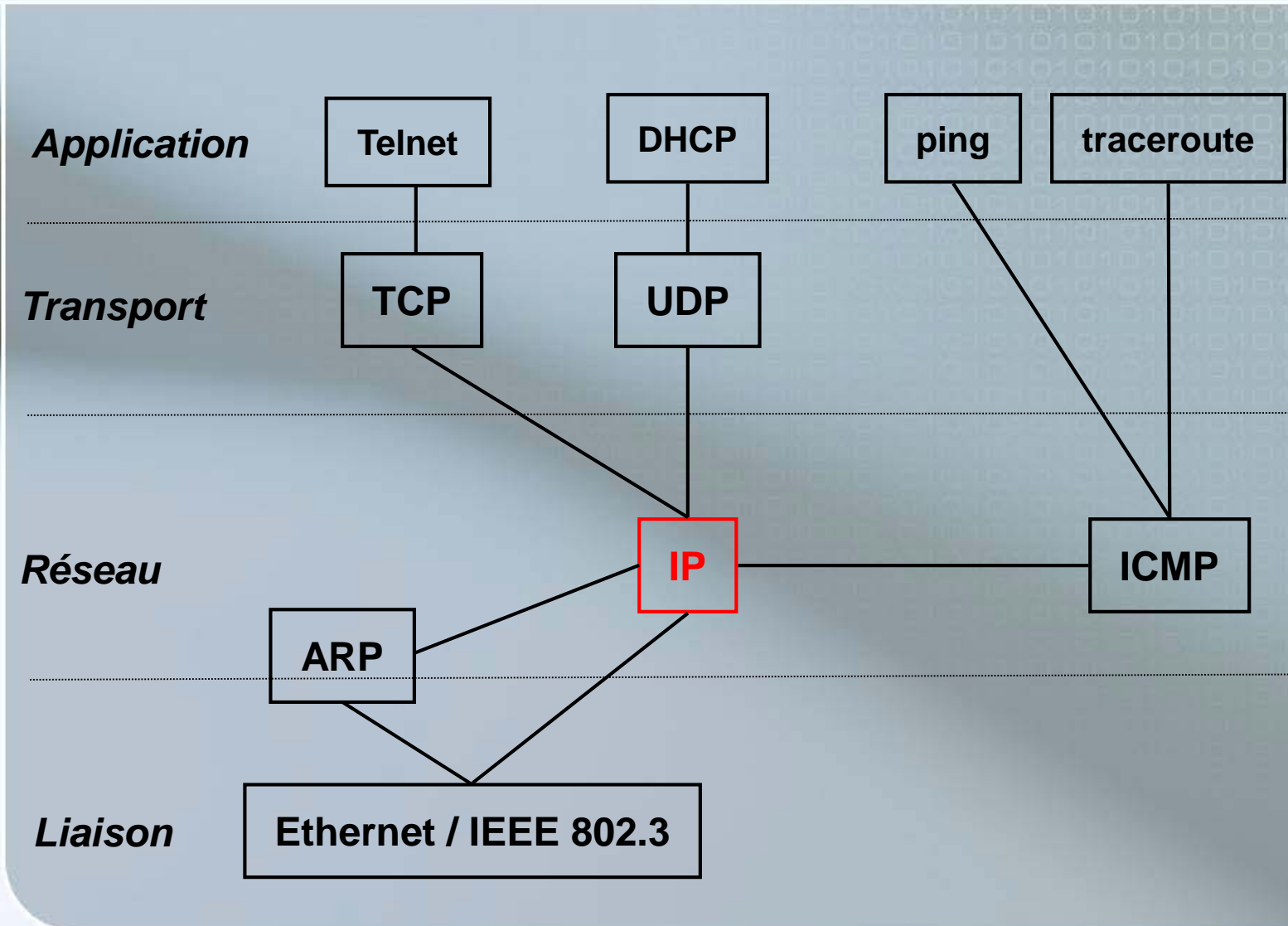
- ARP
- Depuis l'invite de commande de Windows :
 - ARP -a pour visualiser la table de correspondance
 - ARP -d pour vider la table de correspondance
 - ARP -s pour ajouter un hôte
 - ARP /? Pour obtenir l'aide





Chapitre 7 – Adressage IP

Chapitre 7 – Couche Réseau Architecture



Chapitre 7 – Couche Réseau

Généralité

- IP = *Internet protocol*
 - Deux versions :
 - IPv4 : version la plus courante aujourd'hui
 - IPv6 : IP « nouvelle génération »
- Adresse IP :
 - Numéro d'identification attribué lors de la connexion à un réseau informatique.
 - Base pour l'acheminement des message sur Internet.



- Adresse IP
 - Numéro d'identification unique de portée global
- Codée sur 32 bits : (en théorie) 2^{32} adresses différentes.
 - Taille fixe pour simplifier les décisions de routage
 - Structure logique



Chapitre 7 – Couche Réseau

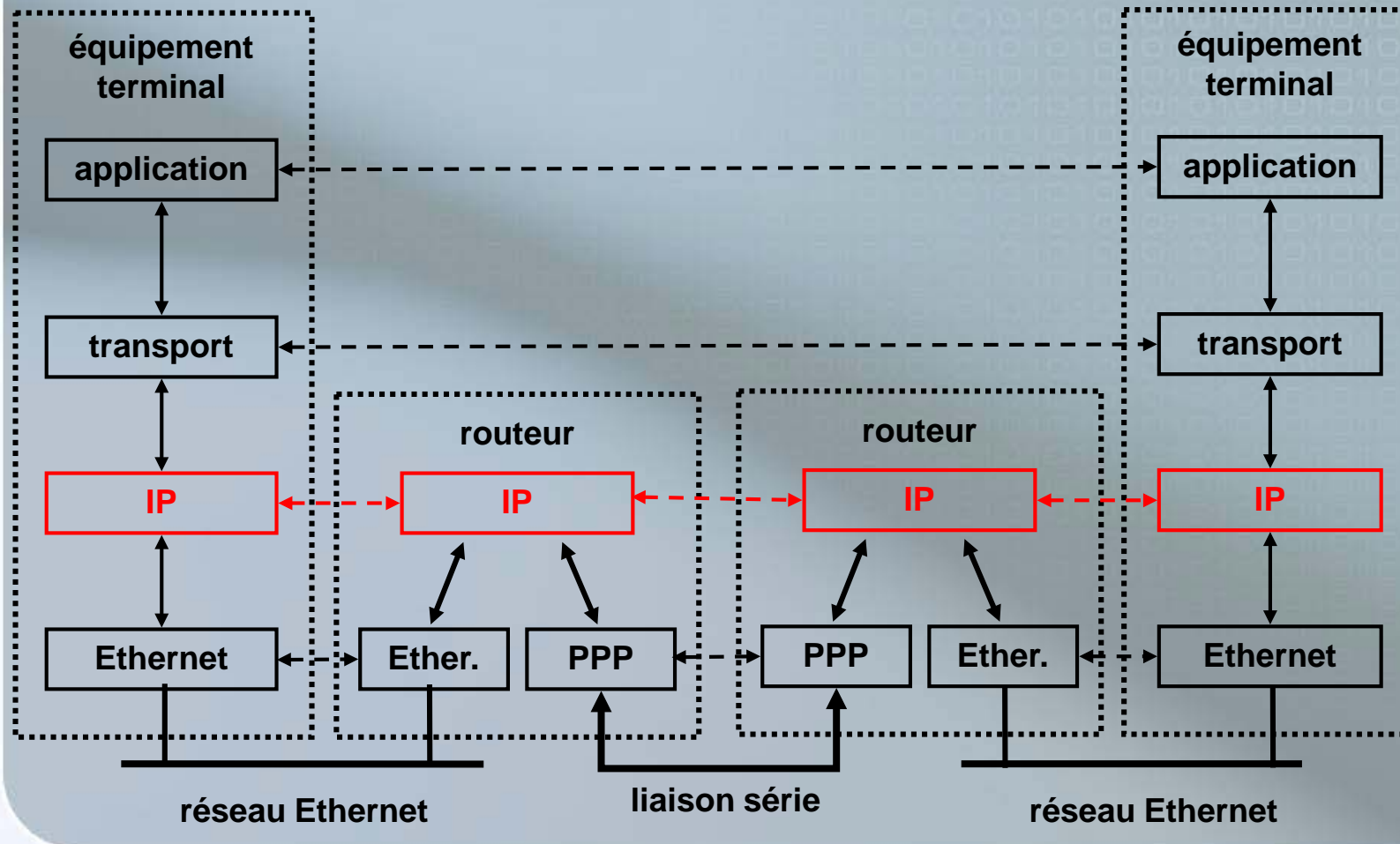
Gestion des adresses IP

- Partie non administrable localement :
 - Numéro de réseaux
- Partie administrable localement :
 - Numéro de host (interface)
- Unicité de l'adresse vis-à-vis des interfaces réseau, pas des machines.
 - Routeur : multiples interfaces (une adresse IP par réseau)
 - Station : (typiquement) une interface donc une adresse pour l'interface



Chapitre 7 – Couche Réseau Interconnexion des réseaux

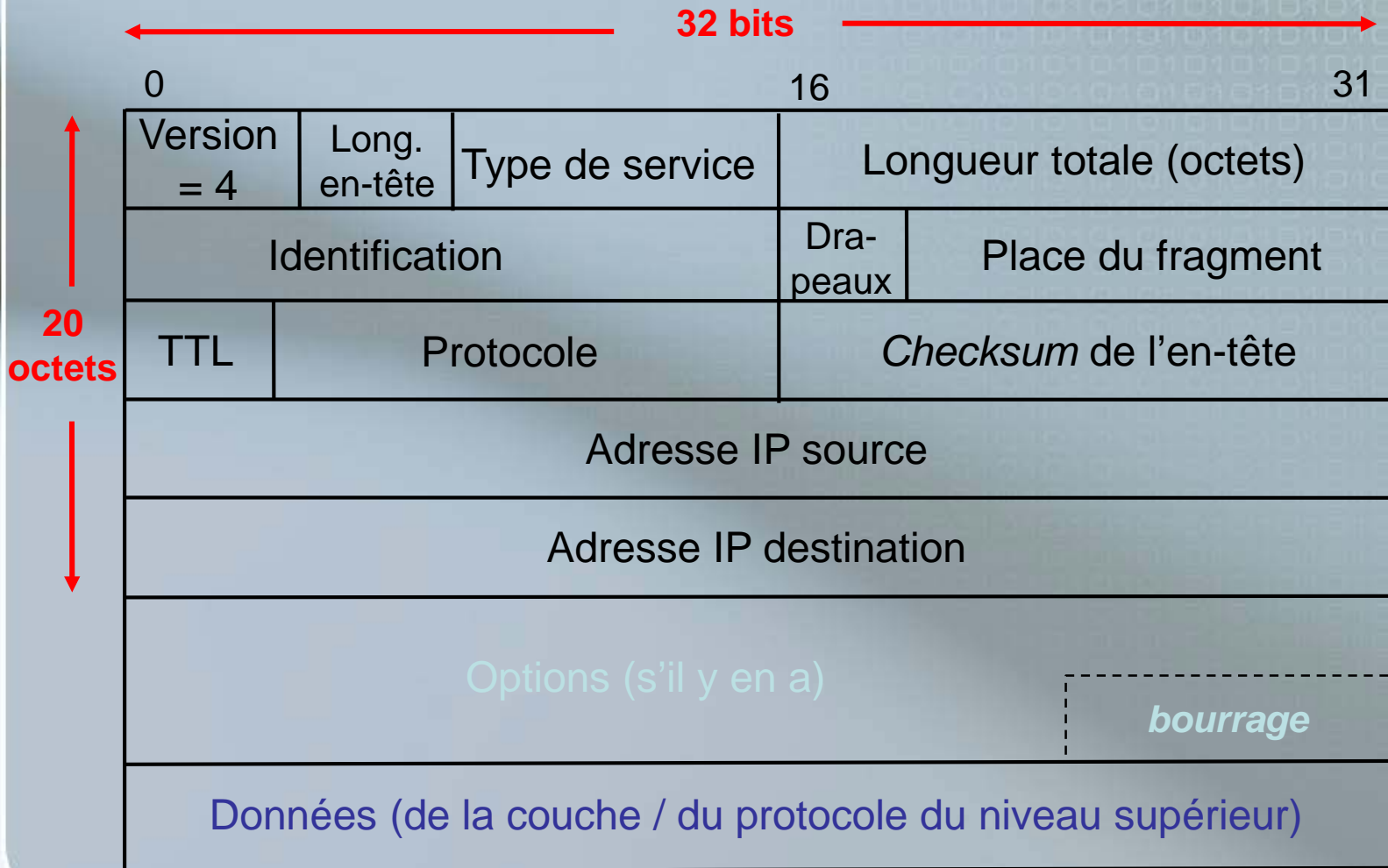
Interconnexion au « Réseau » (niveau) 3 du modèle OSI



- IP offre aux couches supérieures un service (datagramme)
 - Acheminement des paquets de la source à (aux) destination(s)
 - Service ***non orienté connexion***
 - Deux paquets consécutifs peuvent suivre une route différente pour aller de A à B.
 - Service ***non fiable***
 - Perte de paquets : possible
 - Duplication de paquets : possible
 - Séquence d'arrivée des paquets : non garantie

Chapitre 7 – Couche Réseau

Format des paquets IP



Chapitre 7 – Couche Réseau

Champs importants

- Champs importants
- Version
 - Version du protocole IP (IPv4 ou IPv6)
- Identification
 - Numéro du paquet
- TTL
 - Time to Live
- Protocole
 - Protocole utilisé sur la couche supérieur
- Longueur totale
 - Max. théorique = 2^{16}
- Adresses IP source et destination
- Données



Chapitre 7 – Couche Réseau

Champs complémentaires

- Champs complémentaires
- Longueur en-tête
 - Taille maximale (sans options) = 20 octets
- Drapeau
 - Fragmenter ou non
- Place du fragment
 - Où se trouve le fragment
- Type de service
 - QOS
 - RSVP
- Checksum
 - Contrôle de l'intégrité de la trame



Protocole ICMP



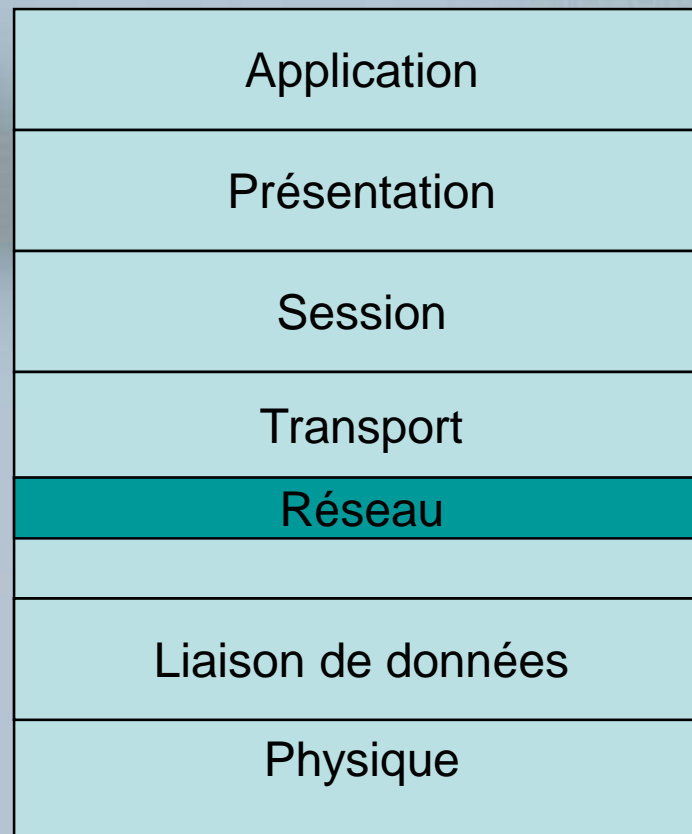
Chapitre 7 – ICMP

Définition

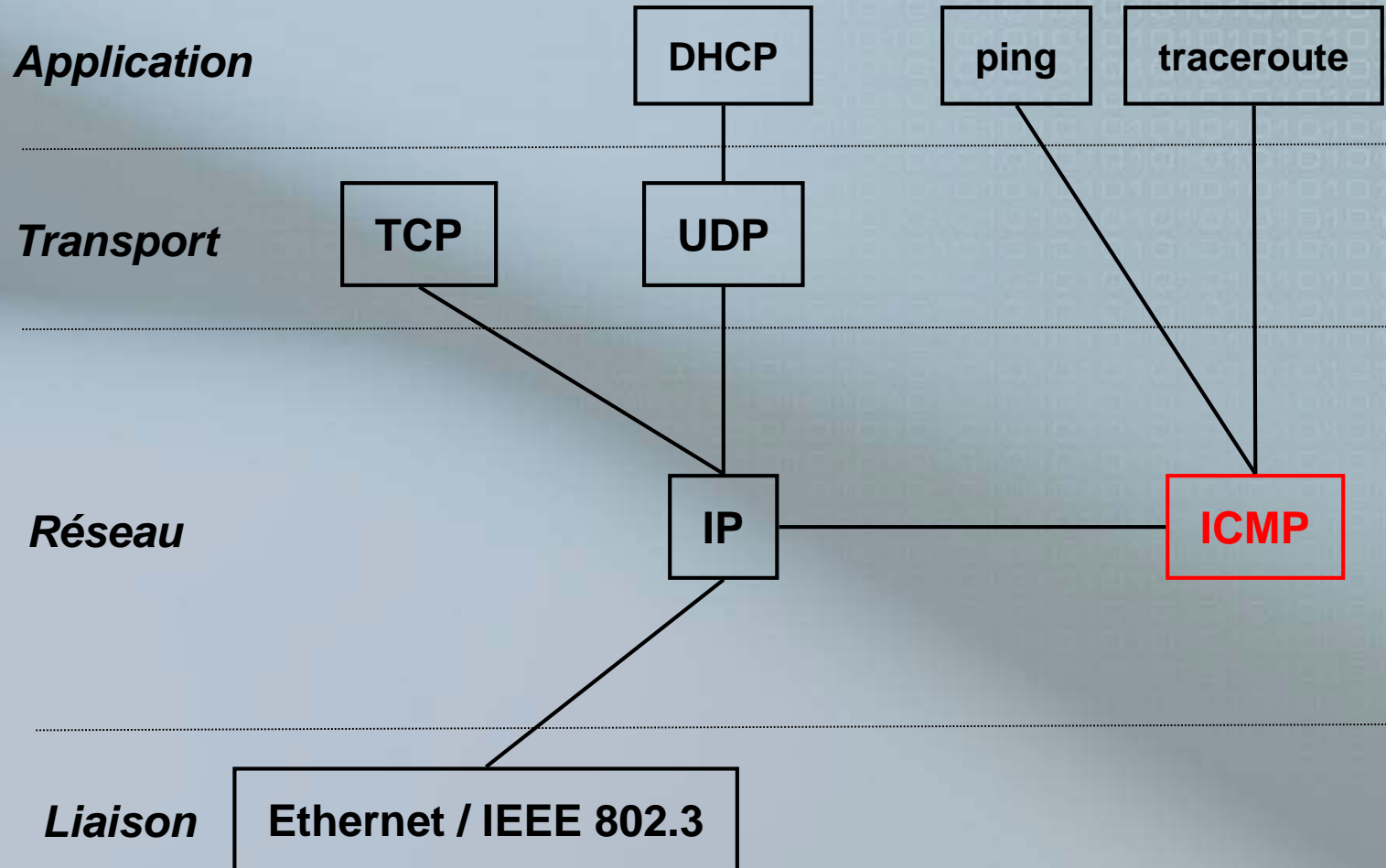
- ICMP signifie
 - **I**nternet
 - **C**ontrol
 - **M**essage
 - **P**rotocol
- (Protocole de contrôle de message Internet)



Représentation en fonction du modèle OSI



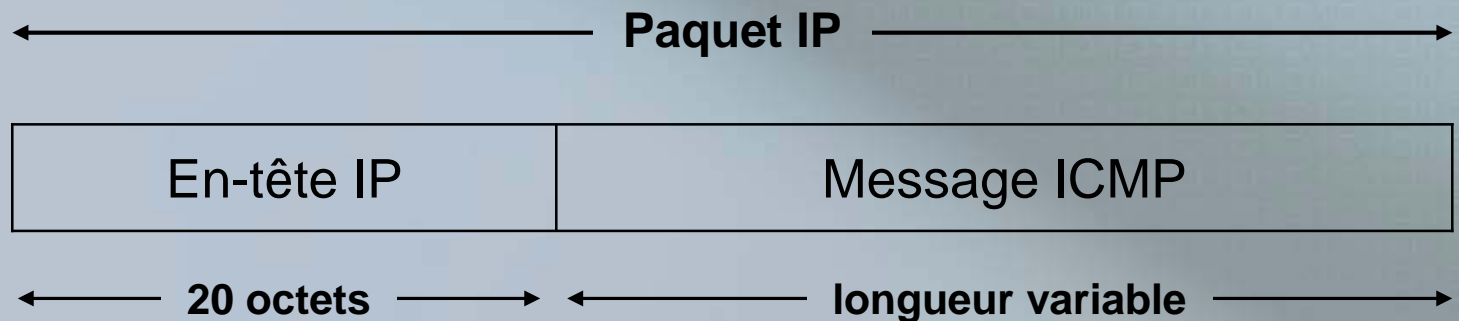
Chapitre 7 – ICMP Architecture



Chapitre 7 – ICMP










Protocole ICMP

- *Internet Control Message Protocol* (RFC 792)
- But : échange de messages d'erreur et de demande d'information
 - Traités soit par IP, soit par une couche supérieure
- Niveau 3, mais encapsulé dans des paquets IP
 - Champ *Protocole* = 1



Chapitre 7 – ICMP

Messages ICMP

Type	Code	Description	Demande	Erreur
0	0	Réponse à une demande d'écho		
3		Destination non accessible :		
	0	Réseau inaccessible		
	1	Station inaccessible		
	2	Protocole inaccessible		
	3	Fragmentation nécessaire mais bit DF = 1		
	4	Port inaccessible		
		etc.		
8	0	Demande d'écho		
11		La durée de vie (TTL) a atteint 0 :		
	0	Durant le transit		
	1	Durant le réassemblage		

Chapitre 7 – ICMP

Commandes

- PING

- Basée sur les messages ICMP de type 8 (*echo request*) et 0 (*echo reply*)
- Réception d'un message type 8 \Rightarrow émission d'un message type 0
- Format des messages :

0	7	8	15	16	23	24	31
Type (0 ou 8)		Code (0)		Checksum			
Identificateur				Numéro de séquence			
(données optionnelles)							

La réponse contient une copie des champs *Identificateur*, *N° de séquence* et les données optionnelles

Chapitre 7 – ICMP

Commande Ping

Exemple d'une réponse «ping»

```
C:\>ping www.sony.com

Envoi d'une requête 'ping' sur www.sony.com [160.33.26.10] avec 32 octets de données :

Réponse de 160.33.26.10 : octets=32 temps=287 ms TTL=242
Réponse de 160.33.26.10 : octets=32 temps=277 ms TTL=242
Réponse de 160.33.26.10 : octets=32 temps=280 ms TTL=242
Réponse de 160.33.26.10 : octets=32 temps=275 ms TTL=242

Statistiques Ping pour 160.33.26.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        minimum = 275ms, maximum = 287ms, moyenne = 279ms
```

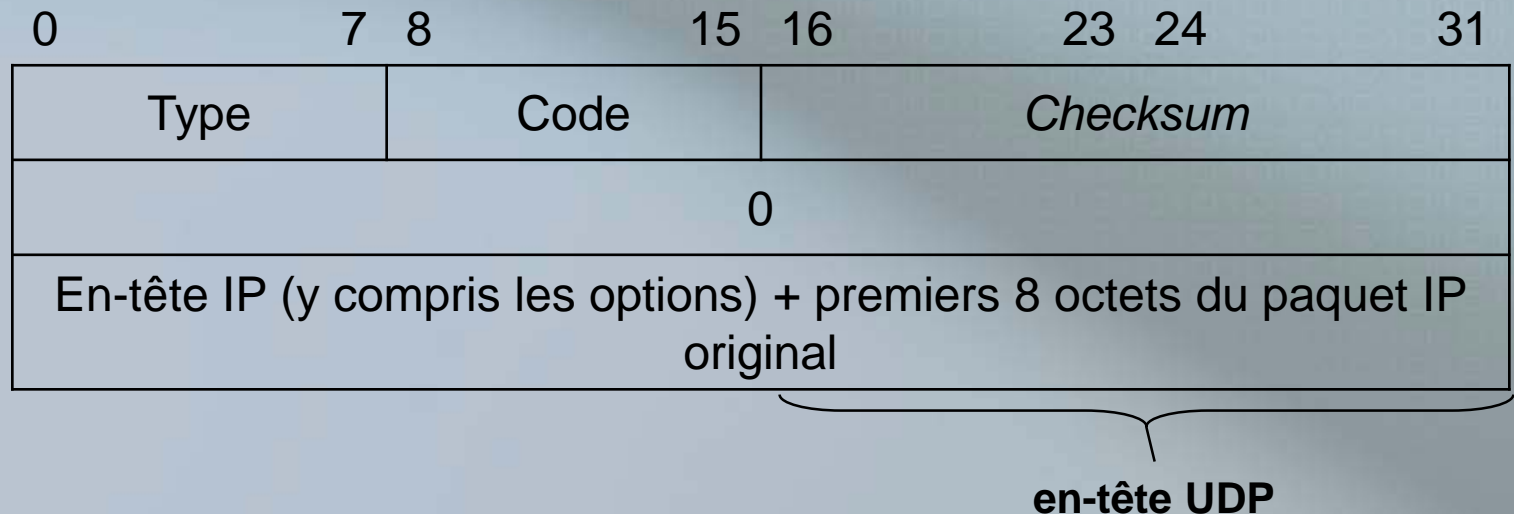
Temps d'aller-retour

Chapitre 7 – ICMP

Commandes

- **TRACERT**

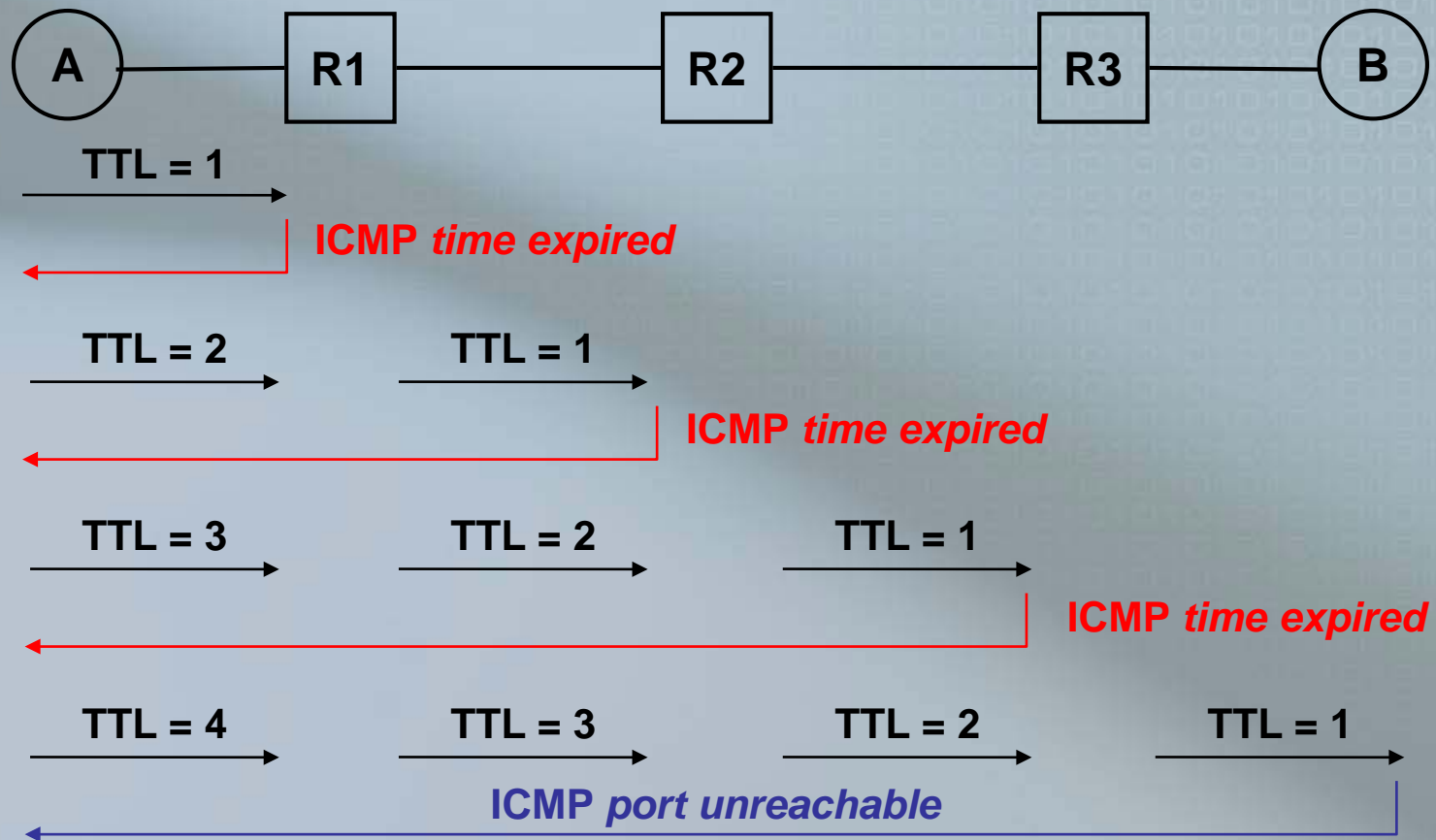
- Basé sur les messages ICMP de type 11 / code 0
 - Envoi de datagrammes UDP qui déclenchent ces messages d'erreur ICMP
- Format des messages :



Chapitre 7 – ICMP

Commande Tracert

Sens A → B : datagrammes UDP (avec N° port destination ≥ 33434)

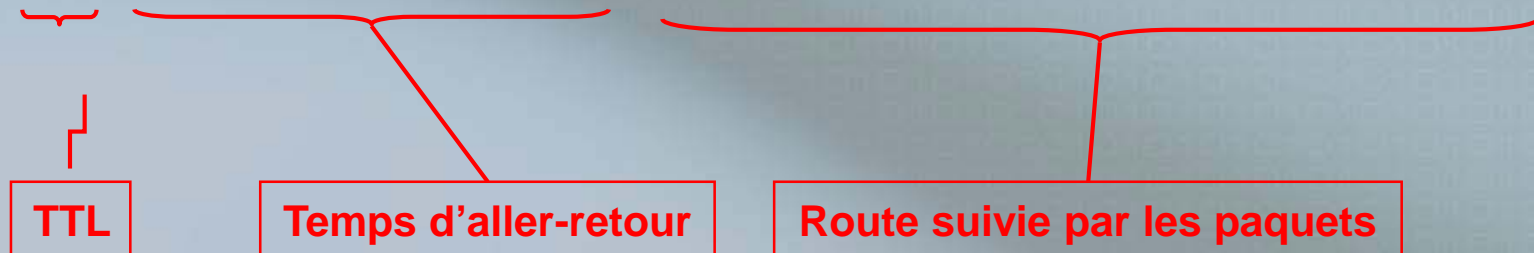



Chapitre 7 – ICMP

Commande Traceroute

Exemple d'une réponse «Tracert»

```
Détermination de l'itinéraire vers www.switch.ch [130.59.10.40]  
avec un maximum de 30 sauts :  
  
 1  <10 ms  <10 ms  <10 ms  AC864A64.ipt.aol.com [172.134.74.100]  
 2   17 ms  22 ms  17 ms  1.96.77.83.cust.bluewin.ch [83.77.96.1]  
 3   17 ms  17 ms  16 ms  net481.bwrt2zhh.bluewin.ch [195.186.123.1]  
 4   17 ms  17 ms  17 ms  net25.bwrt1inh.bluewin.ch [195.186.25.71]  
 5   16 ms  17 ms  17 ms  if234.ip-plus.bluewin.ch [195.186.0.234]  
 6   17 ms  17 ms  17 ms  i79zhh-015-vla201.bb.ip-plus.net [138.187.129.8]
```





Chapitre 6 – Couche réseau

Chapitre 6 – Le routage

Définition

*Le **routage** est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires.*

Source Wikipedia

Chapitre 6 – Le routage

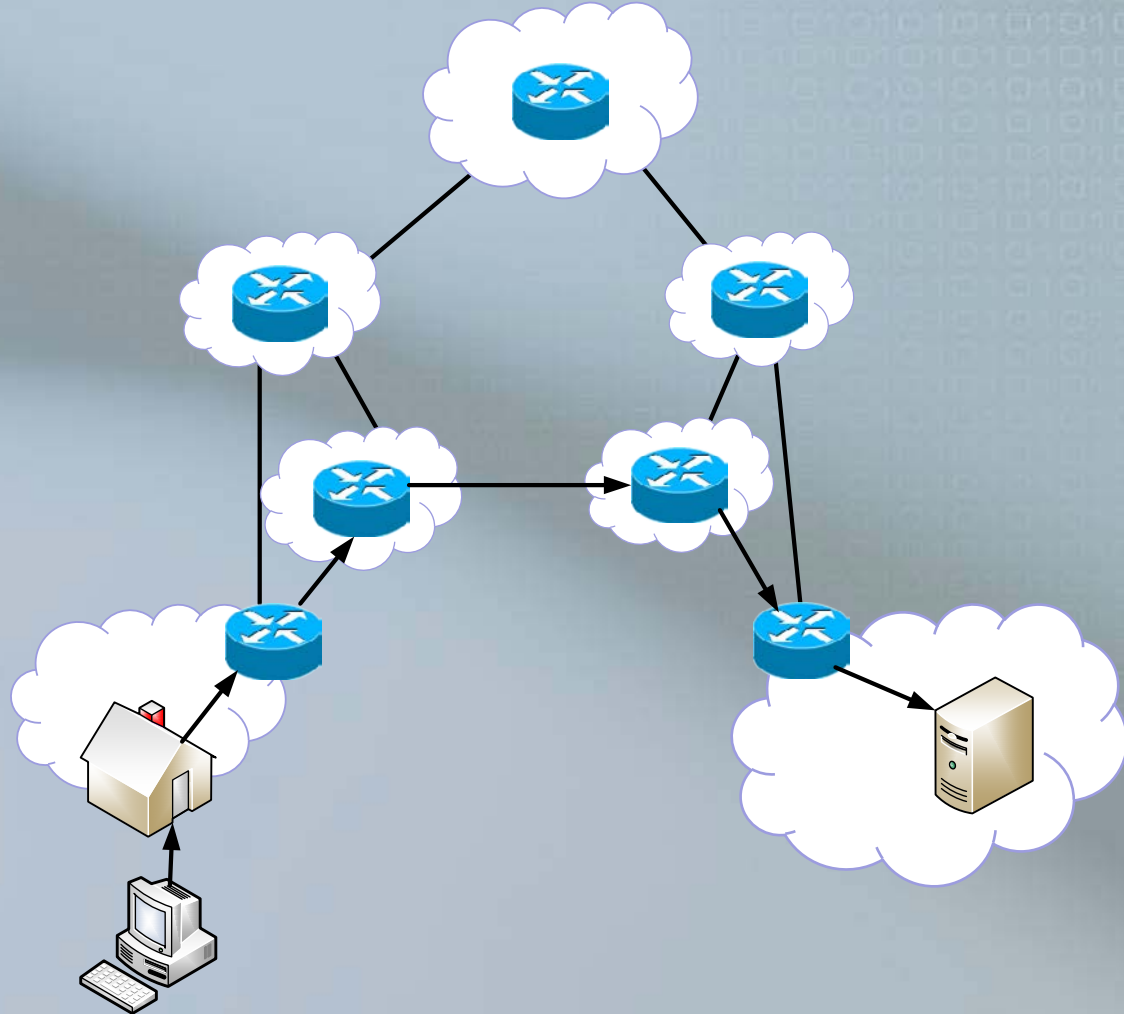
Généralité

- Les réseaux sont interconnectés de natures physiques diverses.
 - Pont, répéteur, Switch, routeur
- L'interconnexion n'a pas la connaissance de la topologie du réseau.
 - Les données sont acheminées par des nœuds intermédiaires.
- L'interconnexion doit pouvoir acheminer les données vers une destination définie.
 - Les données transitent depuis une machine d'un réseau vers une autre machine d'un autre réseau.



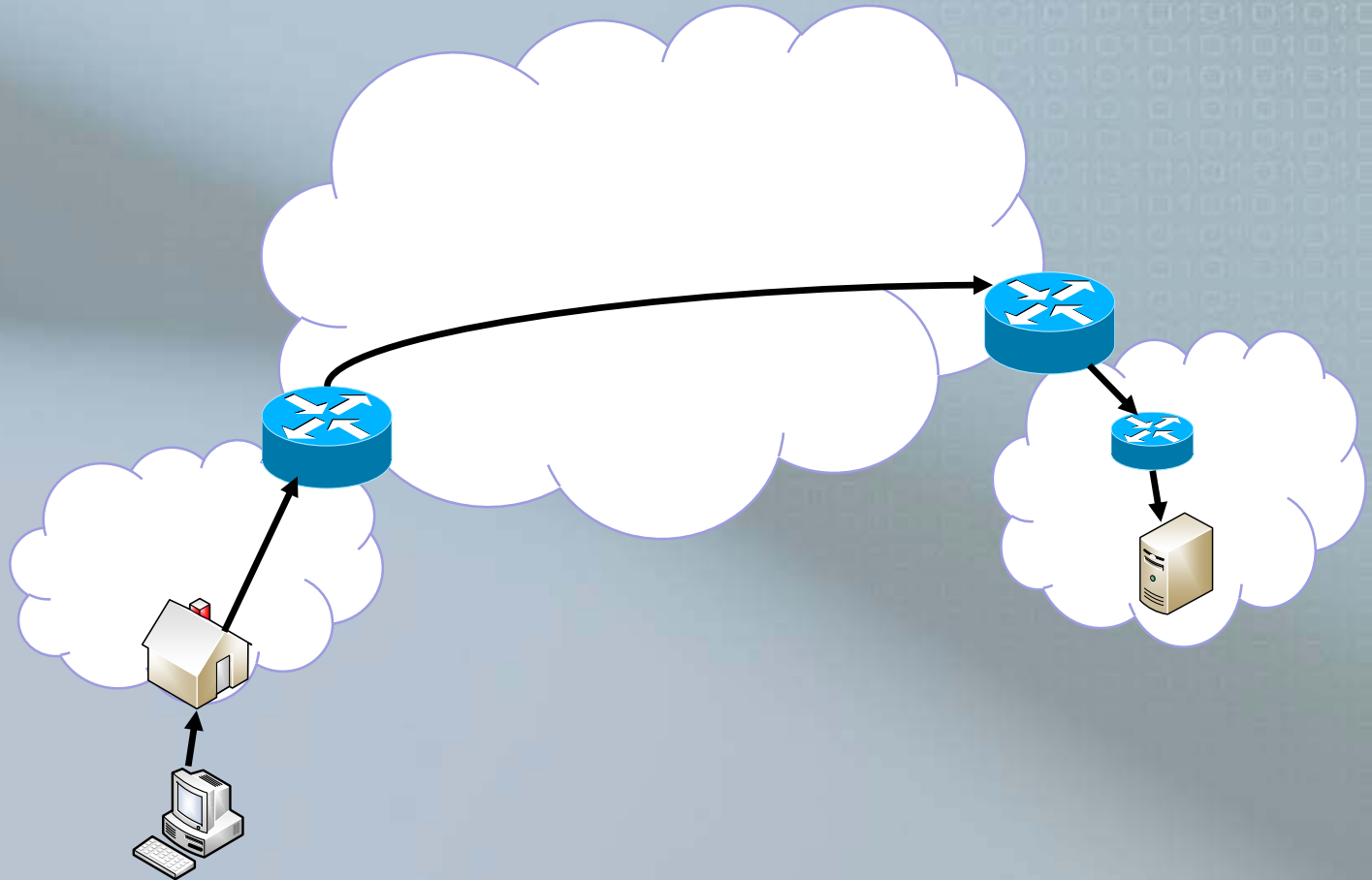
Chapitre 6 – Le routage Interconnexion

Vue « réelle » d'une interconnexion



Chapitre 6 – Le routage Interconnexion

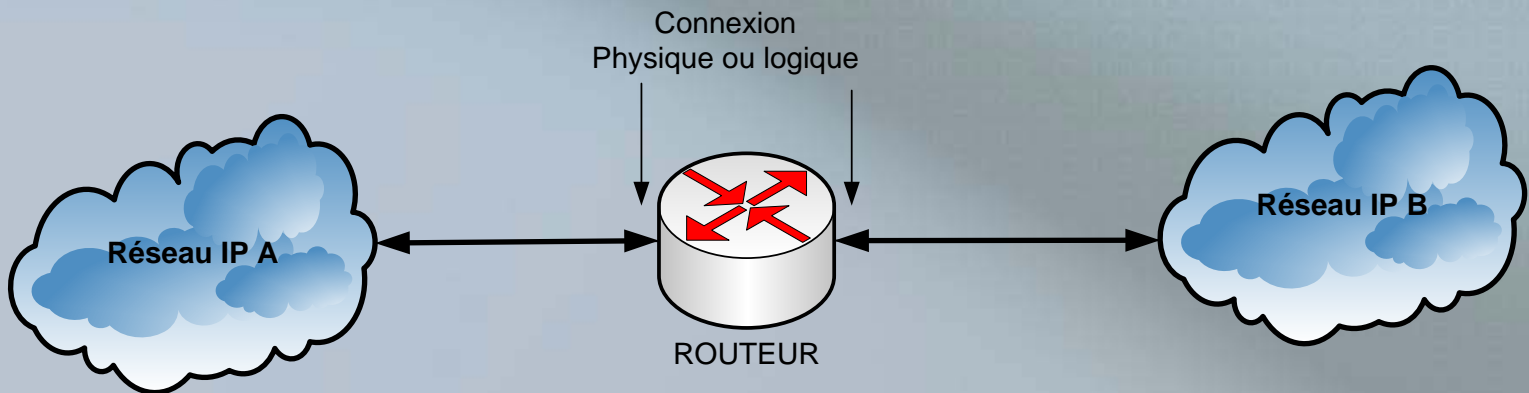
Vue depuis un utilisateur



Chapitre 6 – Le routage

Routage

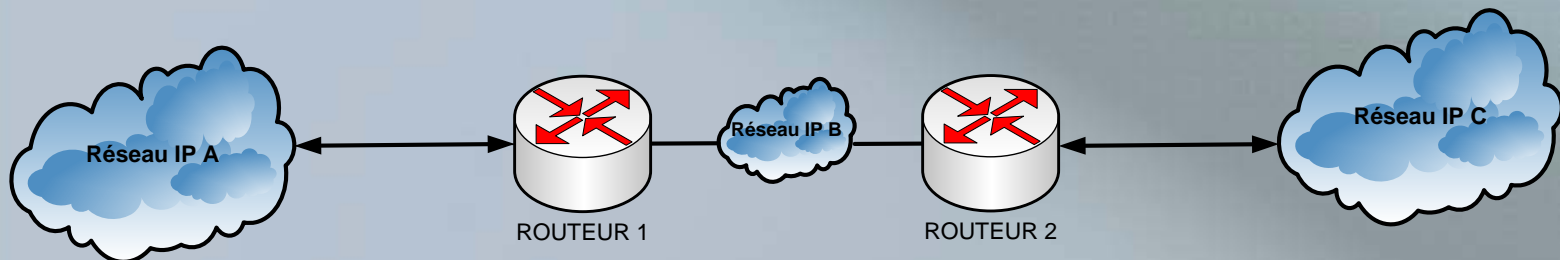
- Un routeur possède une connexion (physique ou logique) sur chacun des réseaux qu'il interconnecte
- Son rôle est de transférer les paquets du réseau IP_A destinés au réseau IP_B et inversement.



Chapitre 6 – Le routage

Routage

- Le routeur 1 se charge du transfert des données du
 - Réseau IP_A vers IP_B et réciproquement
 - Réseau IP_B vers IP_C et réciproquement
- Le Routeur 1 doit avoir la connaissance du chemin vers le réseau IP C
- Le routage s'effectue toujours vers le réseau du destinataire



Chapitre 6 – Le routage

Routage

- Le routage IP est basé sur l'adresse **IP** du destinataire ainsi que sur le masque de son sous-réseau.
- Le routeur ou l'ordinateur possède les informations de routage dans sa **table de routage**
- Une table de routage peut être **fixe** ou **variable**



Chapitre 6 – Le routage

Routage

- Mise à jour de la table de routage :
 - **Manuelle** = **Routage statique**
 - Commande "**route**" des stations « windows »
 - Commande "**ip route**" du langage IOS cisco
 - **Automatique** = **Routage dynamique**
 - Échanges d'informations de routage : P
 - Protocoles de routage (RIP, OSPF, BGP)
 - **Mixte** : Routage statique et dynamique
 - Liaison louée et réseau de site (LL + LAN)

Chapitre 6 – Le routage

Routage

- Une table de routage est constituée des éléments suivants :
 - Méthode de routage : type de protocole qui a appris la route.
 - Réseau et masque de destination.
 - Valeur de métrique : valeur d'une route sur une autre parmi toutes celles apprises par un protocole de routage.
 - Interface de sortie (carte réseau).
 - Interface d'entrée du prochain routeur (Passerelle).



Chapitre 6 – Le routage

Table de routage

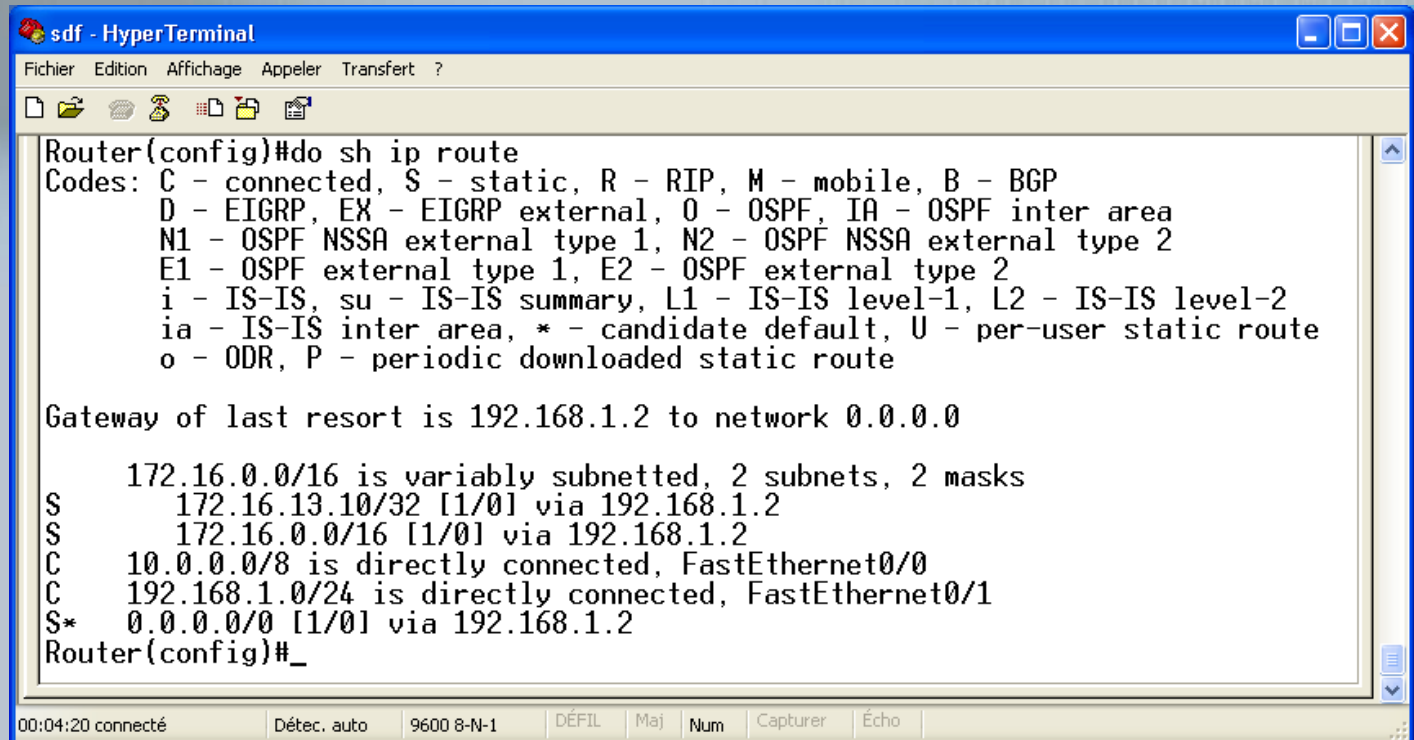
- Accès à la table de routage :
 - D'une station Windows : netstat -r ou route print

```
Table de routage
=====
Liste d'Interfaces
0x1 ..... MS TCP Loopback interface
0x2 ...00 0e e8 09 4a 5f ..... Carte réseau Fast Ethernet PCI Realtek RTL8139 F
amily - Miniport d'ordonnement de paquets
=====
Itinéraires actifs :
Destination réseau      Masque réseau  Adr. passerelle  Adr. interface  Métrique
0.0.0.0                 0.0.0.0       172.134.74.100   172.134.74.30   1
127.0.0.0               255.0.0.0     127.0.0.1        127.0.0.1       1
172.134.74.0            255.255.255.0 172.134.74.30    172.134.74.30   20
172.134.74.30           255.255.255.255 127.0.0.1        127.0.0.1       20
172.134.255.255         255.255.255.255 172.134.74.30    172.134.74.30   20
224.0.0.0               240.0.0.0     172.134.74.30    172.134.74.30   20
255.255.255.255         255.255.255.255 172.134.74.30    172.134.74.30   1
Passerelle par défaut : 172.134.74.100
=====
Itinéraires persistants :
Aucun
```


Chapitre 6 – Le routage

Table de routage

- Accès à la table de routage :
 - D'un **routeur** Cisco : show ip route



```
Router(config)#do sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
S       172.16.13.10/32 [1/0] via 192.168.1.2
S       172.16.0.0/16 [1/0] via 192.168.1.2
C       10.0.0.0/8 is directly connected, FastEthernet0/0
C       192.168.1.0/24 is directly connected, FastEthernet0/1
S*     0.0.0.0/0 [1/0] via 192.168.1.2
Router(config)#_
```


Chapitre 6 – Le routage

Passerelle

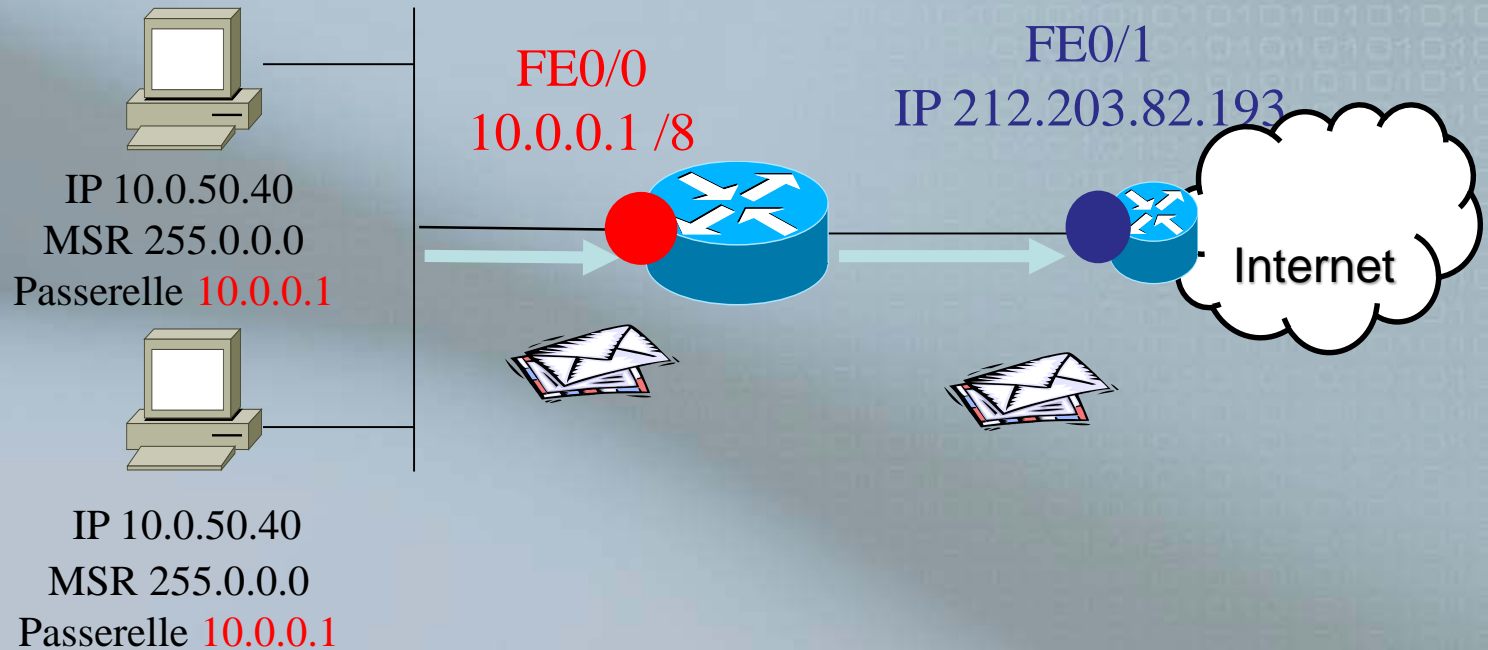
- Pour qu'un poste puisse communiquer sur un réseau IP, il doit posséder au minimum :
 - Une adresse IP
 - Un du masque réseau
 - Une adresse pour la **passerelle (routeur) par défaut**
- Cette dernière adresse désigne l'interface d'un routeur faisant partie du **même réseau** que le poste émetteur.



Chapitre 6 – Le routage

Passerelle

Passerelle par défaut



Chaque élément possède une passerelle par défaut :

Ordinateur : Passerelle par défaut : 10.0.0.1

Routeur : Passerelle par défaut : 212.203.82.193

Chapitre 6 – Le routage

Route statique

- Le routage statique :
 - Mise à jour manuelle de tous les équipements du réseau
 - Gestion de la redondance de routes plus compliquée
 - Si perte de lien la route existe toujours (le paquet est envoyé sur ce lien)



Chapitre 6 – Le routage

Route statique

- Ajout de route statique
 - Permet de construire une table de routage
 - Vers un réseau (network)
 - 192.168.1.0 255.255.255.0 10.0.0.1
 - Vers un sous-réseau (subnet)
 - 192.168.0.64 255.255.255.192 10.0.0.1
 - Vers un équipement (host)
 - 192.168.1.100 255.255.255.255 10.0.0.1
 - Une route par défaut (default)
 - 0.0.0.0 0.0.0.0 10.0.0.1



- Route statique par défaut
 - En général, sur les équipements non routeurs, on définit uniquement une route par défaut.
 - Une route par défaut doit toujours être présente.
 - Acheminement du trafic si aucune autre route n'est valide.



Chapitre 6 – Le routage

Route statique

- Syntaxe pour ajouter une route d'une station windows :

- Route ADD 157.0.0.0 MASK 255.255.0.0 156.55.80.1 METRIC 3 IF 2

```
route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
      destination^          ^masque passerelle^  metrique^
                                   interface^
```

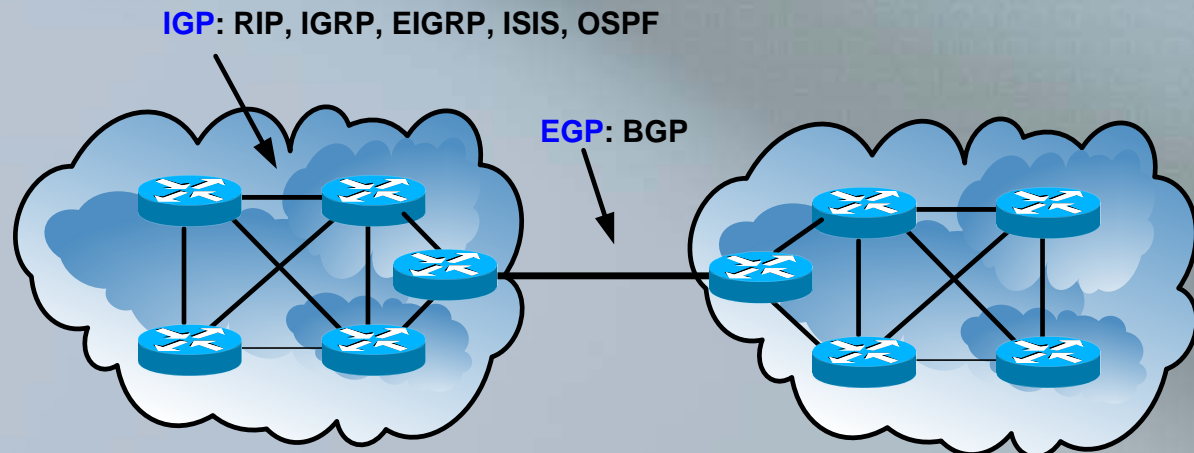
- Syntaxe pour ajouter une route sur un routeur Cisco :

- IP route 157.0.0.0 255.255.0.0 156.55.80.1 120

Chapitre 6 – Le routage

Route dynamique

- Il existe deux types principaux de protocoles de routage dynamique :
 - Les IGP (Interior Gateway Protocol) : échanges d'informations de routage à l'intérieur d'un système autonome.
 - Les EGP (Exterior Gateway Protocol): échanges d'informations de routage entre systèmes autonomes



Chapitre 6 – Le routage

Route dynamique

- Le routage dynamique :
 - Les routes sont automatiquement apprises par le routeur après qu'un **protocole de routage** ait été configuré.
 - Les tables de routage sont **automatiquement** mises à jour.
 - Un protocole de routage opère au niveau de la **couche réseau**.




Chapitre 6 – Le routage

Route dynamique

- Il existe trois grandes classes de protocoles de routage :
 - Vecteur de distance (distance vector)
 - Analyse le chemin le plus court
 - Etat des liaisons (link-state)
 - Analyse l'état de la ligne
 - Hybride équilibré (balanced hybrid)





Chapitre 8 – Segmentation des réseaux IP en sous-réseaux

- Interconnexion de réseaux
 - Subdivision d'un réseau si :
 - atteint une certaine taille
 - réparti sur plusieurs sites
 - Il y a plusieurs raisons à cela :
 - le réseau entier ne dépasse pas la taille de la classe utilisée (récupération d'adresses IP)
 - Meilleure gestion du trafic (broadcast limité)
 - Trafic local confiné dans le sous-réseau (Utilisation des Vlan)



Chapitre 8 – Sous-adressage IP

Généralités

- Le sous-adressage est une extension du plan d'adressage initial (RFC 950)
- Il a été introduit afin de
 - limiter la consommation d'adresses IP
 - simplifier la gestion administrative des adresses IP
- Il implique
 - une taille des tables de routage grandissante
 - un nombre d'informations de routage important
 - un plus grand traitement des paquets IP
- Le découpage d'un réseau en entités plus petites est appelé :
 - Sous-réseaux ou subnets

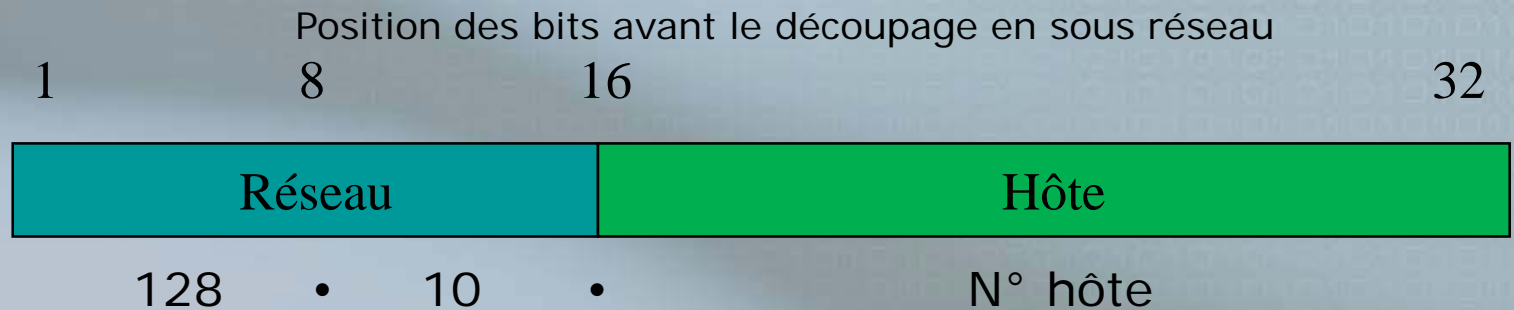
Chapitre 8 – Sous-adressage IP

Sous-réseau SR

- Adresse IP
 - 192.168.0.0
 - Masque de sous-réseau
 - 255.255.255.0
 - Sous-adresse IP
 - 192.168.0.0 et 128
 - Masque de sous-réseau
 - 255.255.255.128
 - Sous-adresse IP
 - 192.168.0.0, 64, 128 et 192
 - Masque de sous-réseau
 - 255.255.255.192
- Diagram illustrating the division of the 192.168.0.0 network into subnets (SR) using VLSM:
- 1 -> ID réseau
254 hosts
1 -> IP broadcast
 - 2 -> ID SR
126 hosts par SR
2 -> IP broadcast
 - 4 -> ID SR
62 hosts par SR
4 -> IP broadcast

- Adresse IP de classe B

- Nombre de réseaux possible ?
- Nombre d'hôtes possible ?



- Nombre de réseaux : 16384
- Nombre d'hôtes : 65534

Chapitre 8 – Sous-adressage IP

Principe

- A l'intérieur d'une entité associée à une adresse IP de classe A, B ou C, plusieurs réseaux physiques partagent cette adresse IP.



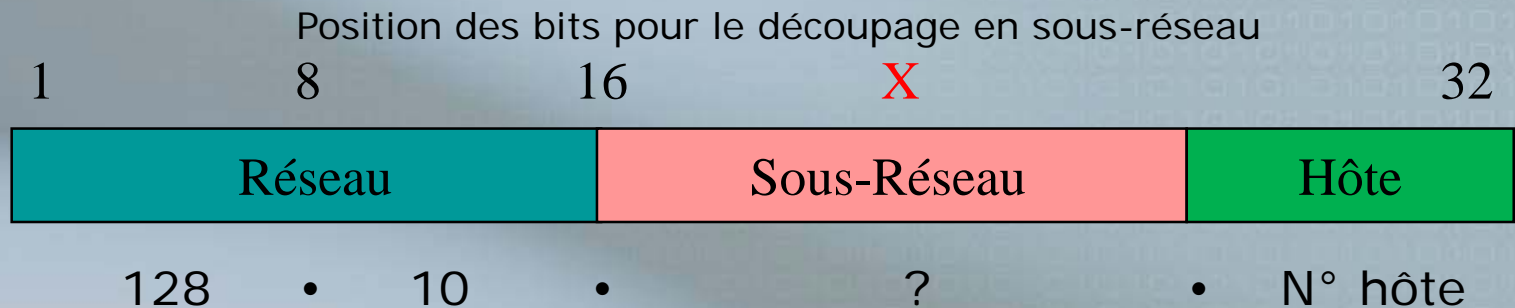
- La partie locale de l'adresse initiale est subdivisée en sous-réseau (subnet) et hôte (HostId).
- Les champs sous-réseau et hôte sont de tailles variables
- La longueur des 2 champs étant toujours égale à la longueur de la partie locale initiale.

Chapitre 8 – Sous-adressage IP

Découpage en sous-réseau

- Le « subnetting »

- Nombre de sous-réseaux possible ?



- 0 bit : pas de subnet
- 1 bit : 2^1 2 sous-réseaux
- 2 bits : 2^2 4 sous-réseaux
- 3 bits : 2^3 8 sous-réseaux
- 4 bits : 2^4 16 sous-réseaux
- etc
- 14 bits : 2^{14} 16384 sous-réseaux

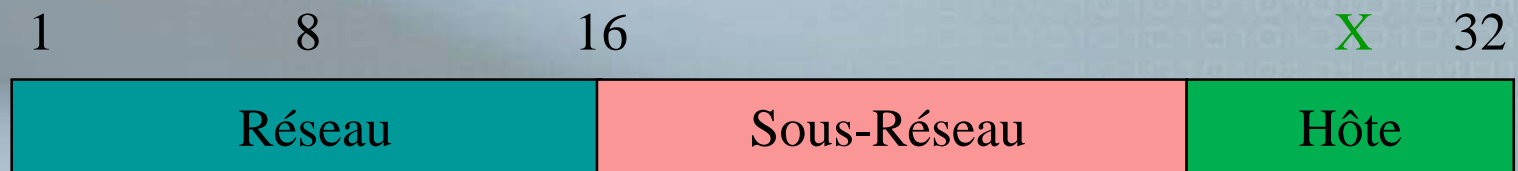
Chapitre 8 – Sous-adressage IP

Découpage en sous-réseau

- Le « subnetting »

- Nombre d'hôtes possible ?

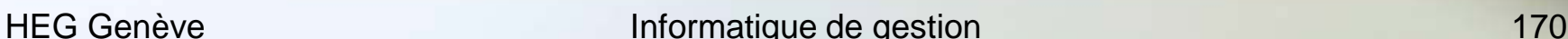
Position des bits pour le découpage en sous-réseau



128 • 10 • 1 • nbre hôte

- 16 bits : pas de subnet
- 15 bits : 2^{15} 32766 hôtes
- 14 bits : 2^{14} 16382 hôtes
- 13 bits : 2^{13} 8190 hôtes
- 12 bits : 2^{12} 4094 hôtes
- etc
- 2 bits : 2^2 2 hôtes

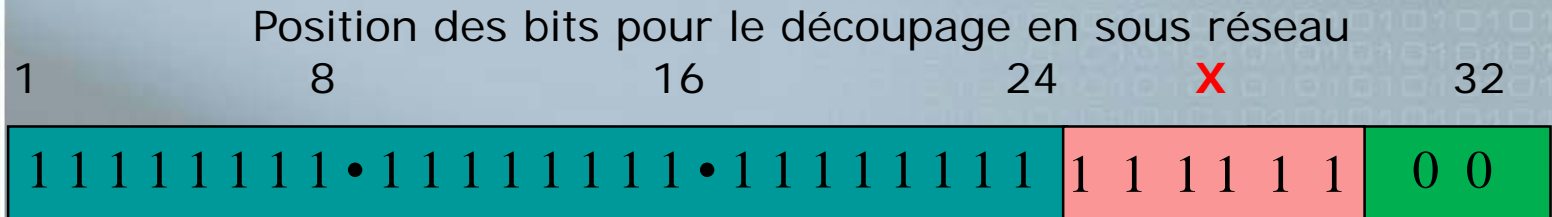
- Dans la pratique, on utilise un **masque de sous-réseau** ou **subnet mask**.
- **Masque** : 4 octets scindé en 2 parties (bits contigus) :
 - 1^{ère} partie = masque de sous-réseau par défaut
 - 2^{ème} partie = masque de sous-réseau personnalisé
 - **Suite de bit à 1** : bits "réseau", suivis de **bit à 0** : bits « hôtes »



Chapitre 8 – Sous-adressage IP

Découpage en sous-réseau

- Exemple pour une classe C



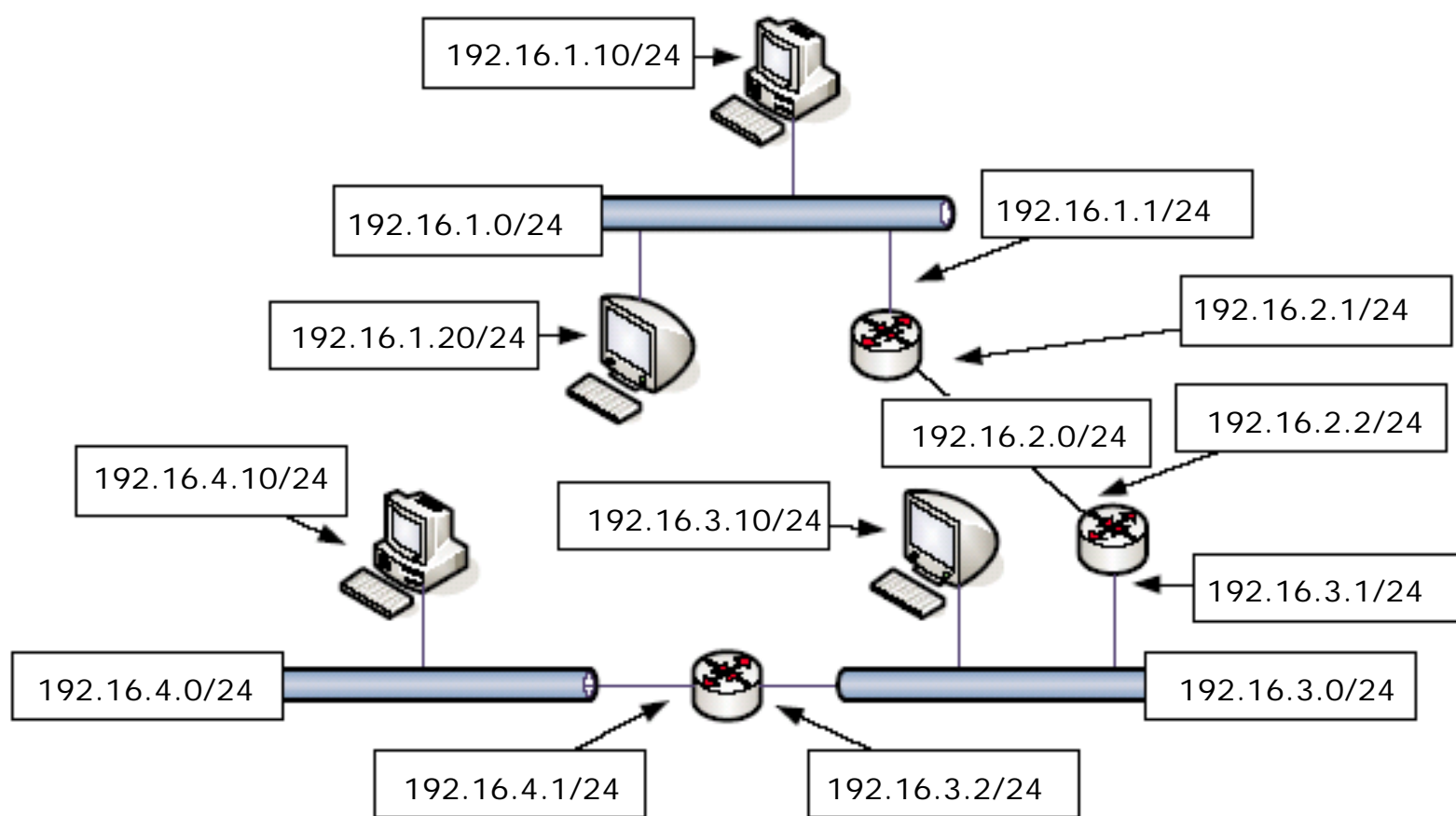
- Masque classe C : Nombre de bit à 1 ≥ 22
 - Toujours de type **255.255.255.X**

Nb de bit utilisé	Masque	Nb de subnet	Nb de machine par subnet	Nb Total de machines
0	255.255.255.0	0	254	254
1	255.255.255.128	2	126	252
2	255.255.255.192	4	62	248
3	255.255.255.224	8	30	240
4	255.255.255.240	16	14	224
5	255.255.255.248	32	6	192
6	255.255.255.252	64	2	128

Chapitre 8 – Sous-adressage IP

Exemple

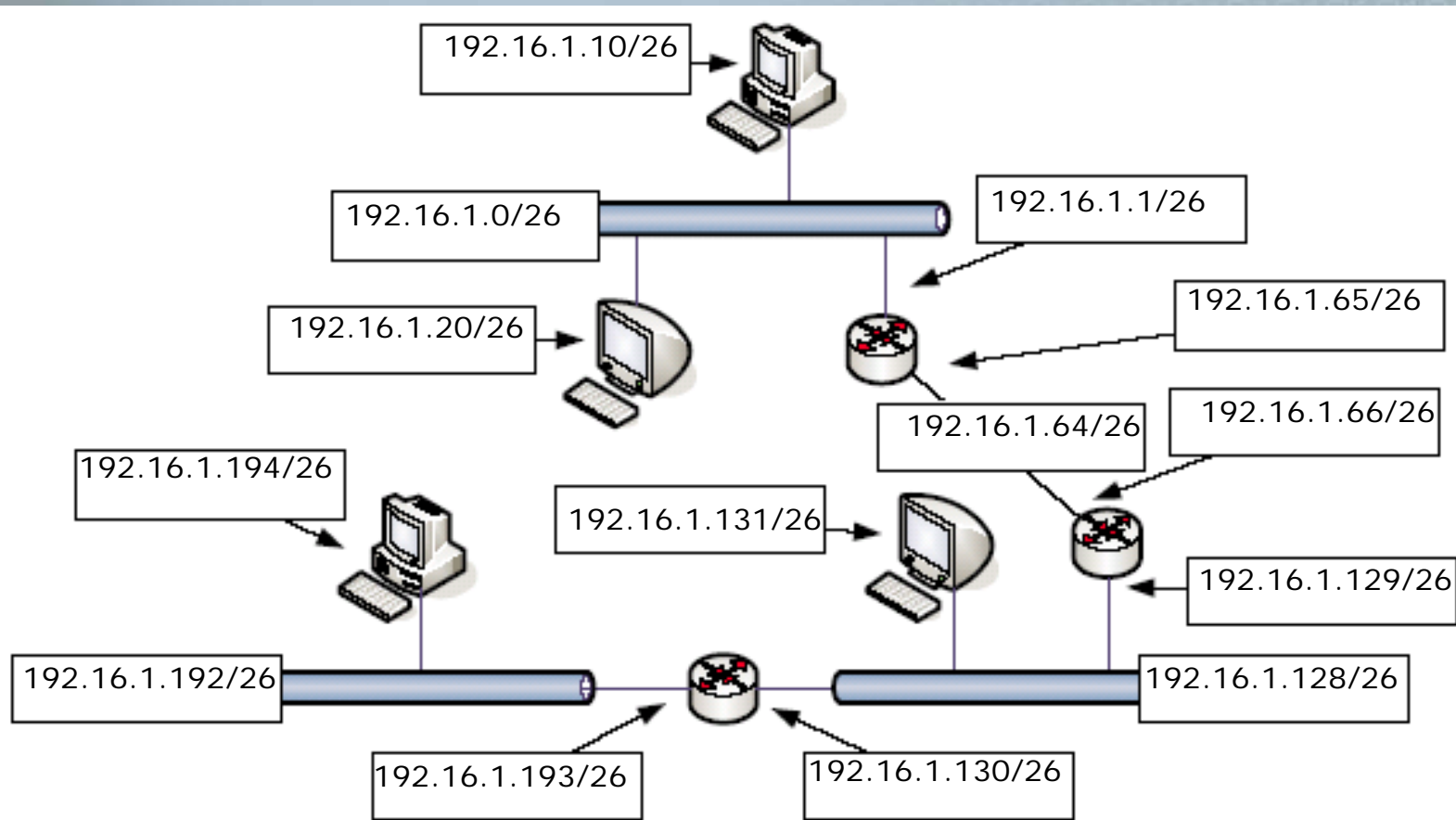
- Exemple d'interconnexion avec des réseaux
 - 4 réseaux : 1016 IP (10 utilisées)




Chapitre 8 – Sous-adressage IP

Exemple

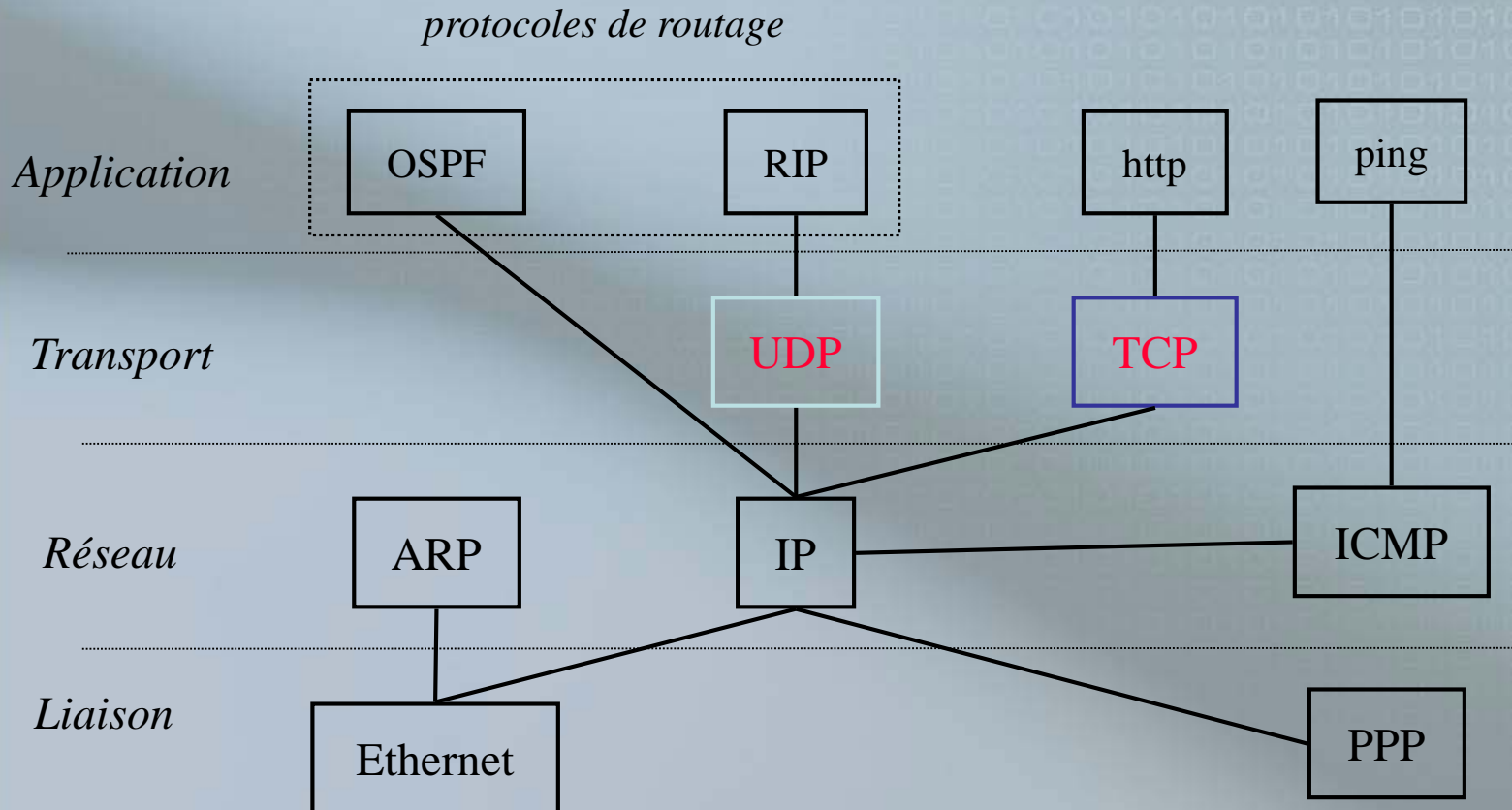
- Exemple d'interconnexion avec des sous-réseau
 - 4 sous-réseaux : 248 IP (10 utilisées)





Chapitre 9 – Couche Transport

Chapitre 9 – TCP et UDP Architecture



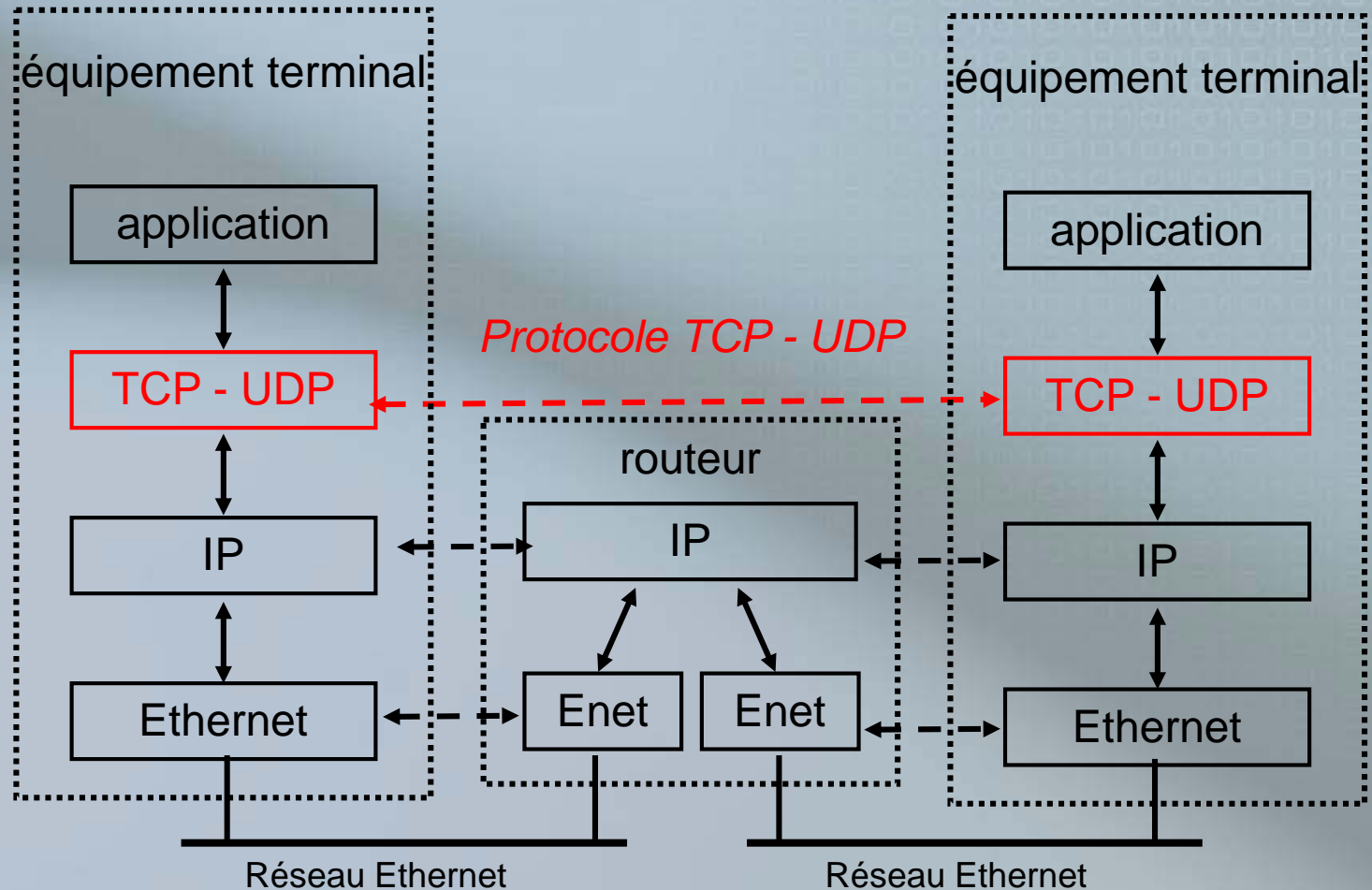
- La couche transport offre deux types de service:
 - UDP (User Datagram Protocol)
 - un service non fiable et non connecté.
 - Pas de garantie de livraison, les erreurs ne sont pas corrigées,...
 - TCP (Transmission Control Protocol)
 - Un service fiable et connecté.
 - Contrôle complet de la communication



Chapitre 9 – TCP et UDP

Protocole de transport

Interconnexion au « Transport » (niveau) 4 du modèle OSI



Chapitre 9 – TCP et UDP

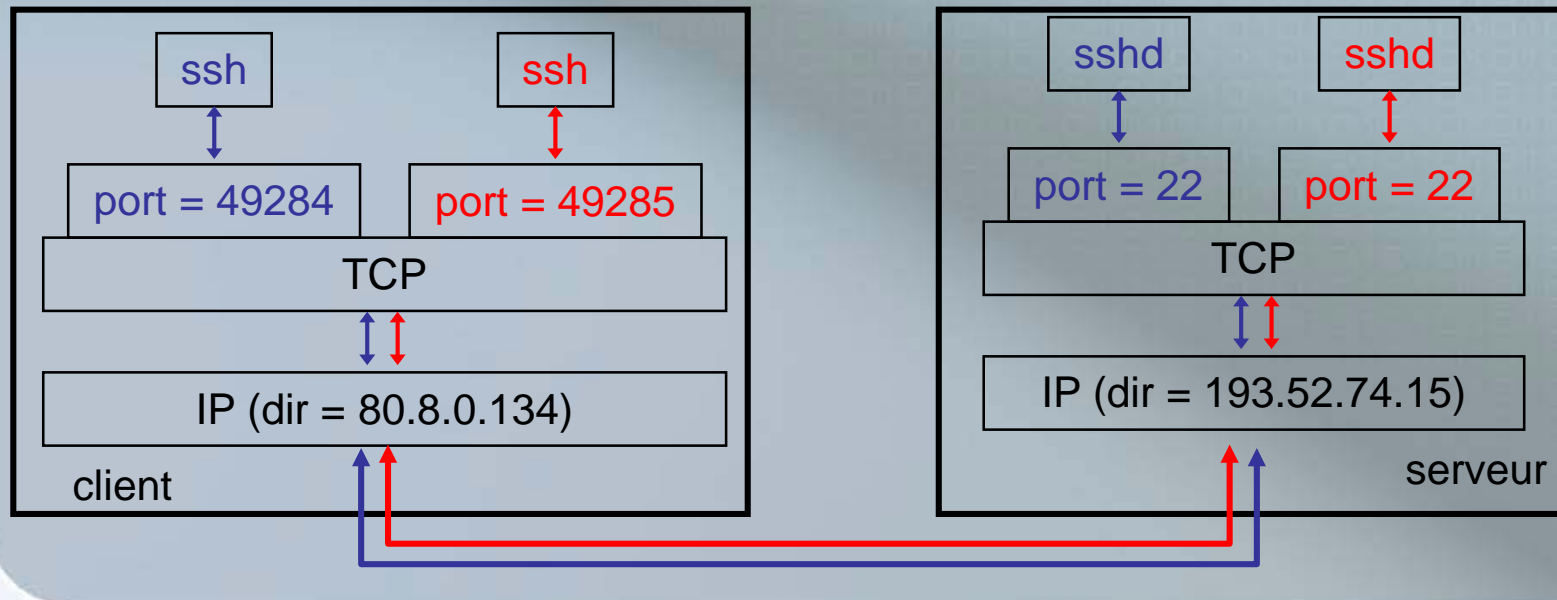
Protocole TCP

- Connexion TCP/IP ou UDP/IP
 - une connexion de type « circuit virtuel » est établie avant que les données ne soient échangées.
 - Une extrémité de connexion = couple (adresse IP, N° de port) est appelé « Socket »
 - Exemple de connexion : ((12.32.12.1, 1034), (19.24.67.2, 21))
 - Une extrémité de connexion peut être partagée par plusieurs autres extrémités de connexions (multi-instanciation)

Chapitre 9 – TCP et UDP

Multiplexage de ports

- Identification = (direction IP de A, port de A) + (direction IP de B, port de B) = *socket A* + *socket B*
 - Exemple : deux connexions « en parallèle » à un serveur ssh
 - Serveur : port bien connu (22)
 - Client : ports éphémères



Chapitre 9 – TCP et UDP

Protocole UDP

- UDP signifie
 - User
 - Datagram
 - Protocol
 - (Protocole d'utilisateur de datagrammes)



Chapitre 9 – TCP et UDP

Protocole UDP

- Protocole de transport sans connexion de service applicatif :
 - émission de messages applicatifs : sans établissement de connexion au préalable
 - l'arrivée des messages ainsi que l'ordonnancement ne sont pas garantis.
- Identification du service : les ports
 - Les adresses IP désignent les machines entre lesquelles les communications sont établies.
 - Les ports désignent les services (processus) applicatifs auxquels on veut accéder.

Chapitre 9 – TCP et UDP

Protocole UDP

- En-tête UDP

- Port Source et destination
- Longueur du message
- Checksum
- Données

0	16	31
Port UDP Source	Port UDP dest.	
Longueur message UDP	Checksum UDP	

- *User Datagram Protocol (RFC 768)*
- Applications/protocoles qui utilisent UDP
 - NFS (*Network File System*)
 - DNS (*Domain Name System*)
 - DHCP (*Dynamic Host Configuration Protocol*)
 - *Streaming* multimédia



Chapitre 9 – TCP et UDP

Protocole UDP

- Certains ports sont réservés (*RFC 1700*) :

<u>No port</u>	<u>Mot-clé</u>	<u>Description</u>
13	DAYTIME	Daytime
37	TIME	Time
53	DOMAIN	Domain Name Server
69	TFTP	Trivial File transfert protocol
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol

- D'autres numéros de port (non réservés) peuvent être assignés dynamiquement aux applications.

Chapitre 9 – TCP et UDP

Protocole TCP

- TCP signifie
 - Transmission
 - Control
 - Protocol
 - (Protocole de contrôle de transmission)



Chapitre 9 – TCP et UDP

Protocole TCP

- Transport fiable de la technologie TCP/IP.
 - fiabilité = illusion assurée par le service
 - transferts tamponnés : découpage en segments
 - connexions bidirectionnelles et simultanées
- Service en mode connecté
- Garantie de non-perte de messages ainsi que de l'ordonnancement des segments composant les messages



Chapitre 9 – TCP et UDP

Protocole TCP

- En-tête TCP

- Port source et destination : Port TCP
- Numéro de séquence : Numéro du segment TCP
- Numéro d'acquittement : Segment reçu ?
- Drapeaux : longueur, offset, réservé,...
- Pointeur d'urgence : données urgentes (flag URG)

0	4	10	16	24	31
Port source			Port destination		
Numéro de séquence					
Numéro d'acquittement					
Drapeaux			Fenêtre		
Checksum			pointeur urgence		
Options éventuelles				padding	

Chapitre 9 – TCP et UDP

Protocole TCP

- *Transmission Control Protocol* (RFC 1180)
- Applications/protocoles qui utilisent TCP
 - HTTP
 - SMTP
 - FTP
 - telnet, rlogin, ssh



Chapitre 9 – TCP et UDP

Protocole TCP

- Segment TCP :
 - unité de transfert du protocole TCP
- Utilisation :
 - Echange pour établir les connexions
 - Transfert de données
 - Emission des acquittements
 - Clôture des connexions



Comme pour UDP, il existe des ports réservés:

<u>No port</u>	<u>Mot-clé</u>	<u>Description</u>
20	FTP-DATA	FileTransfer [Default Data]
21	FTP	File Transfer [Control]
23	TELNET	Telnet
25	SMTP	Simple Mail Transfer
53	DOMAIN	Domain Name Server
80	HTTP	WWW
110	POP3	Post Office Protocol - Version 3

- D'autres numéros de port (non réservés) peuvent être assignés dynamiquement aux applications.

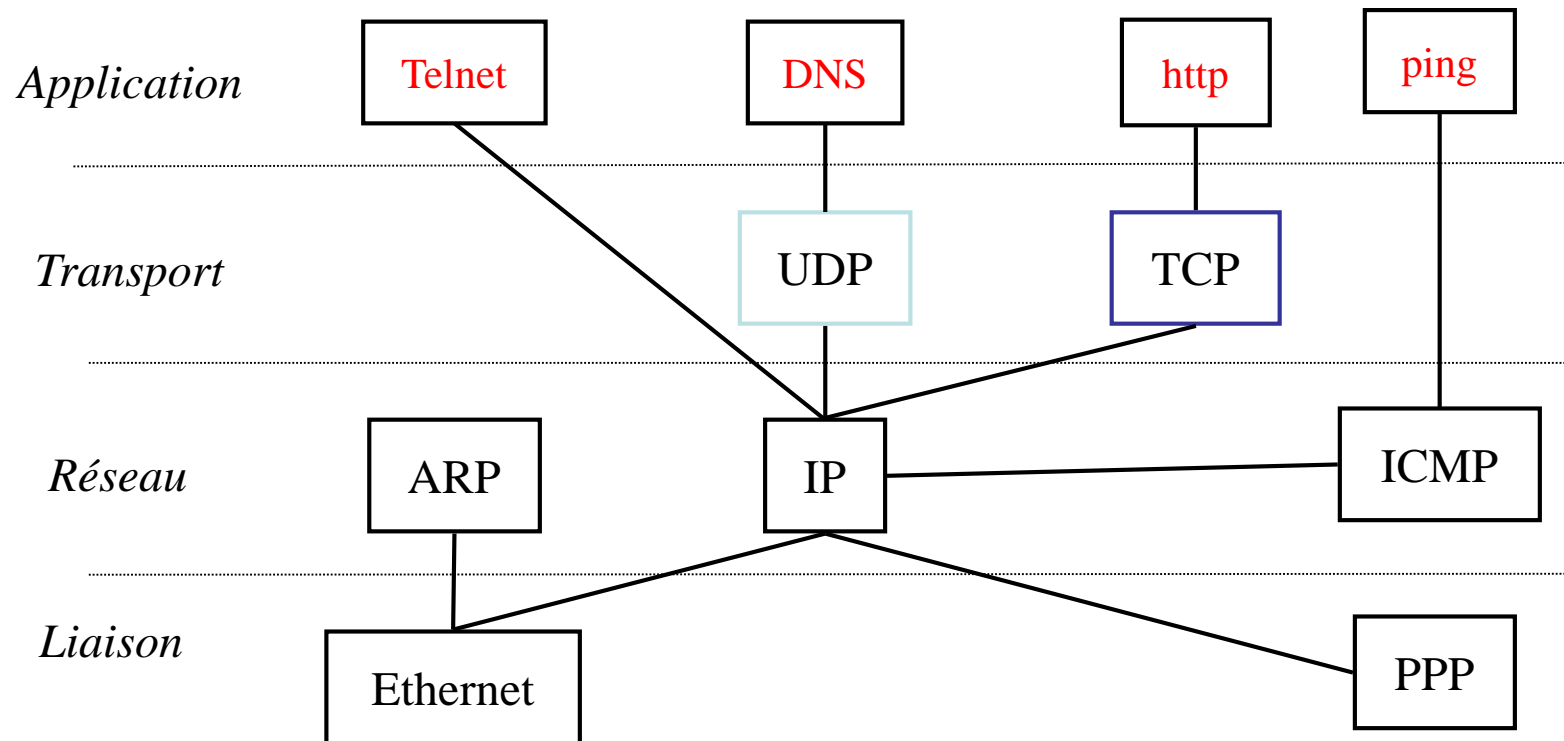
- NETSTAT
- Depuis l'invite de commande de Windows :
 - NETSTAT -a pour visualiser l'ensemble des connexion
 - NETSTAT -e pour visualiser les statistiques Ethernet
 - NETSTAT -o détaille le numéro de processus associé
 - NETSTAT -s affiche les statistiques détaillées par protocole
 - NETSTAT -? Affiche l'aide



Chapitre 10 – Couche Application

Chapitre 10 – Application Architecture

Représentation dans le modèle OSI



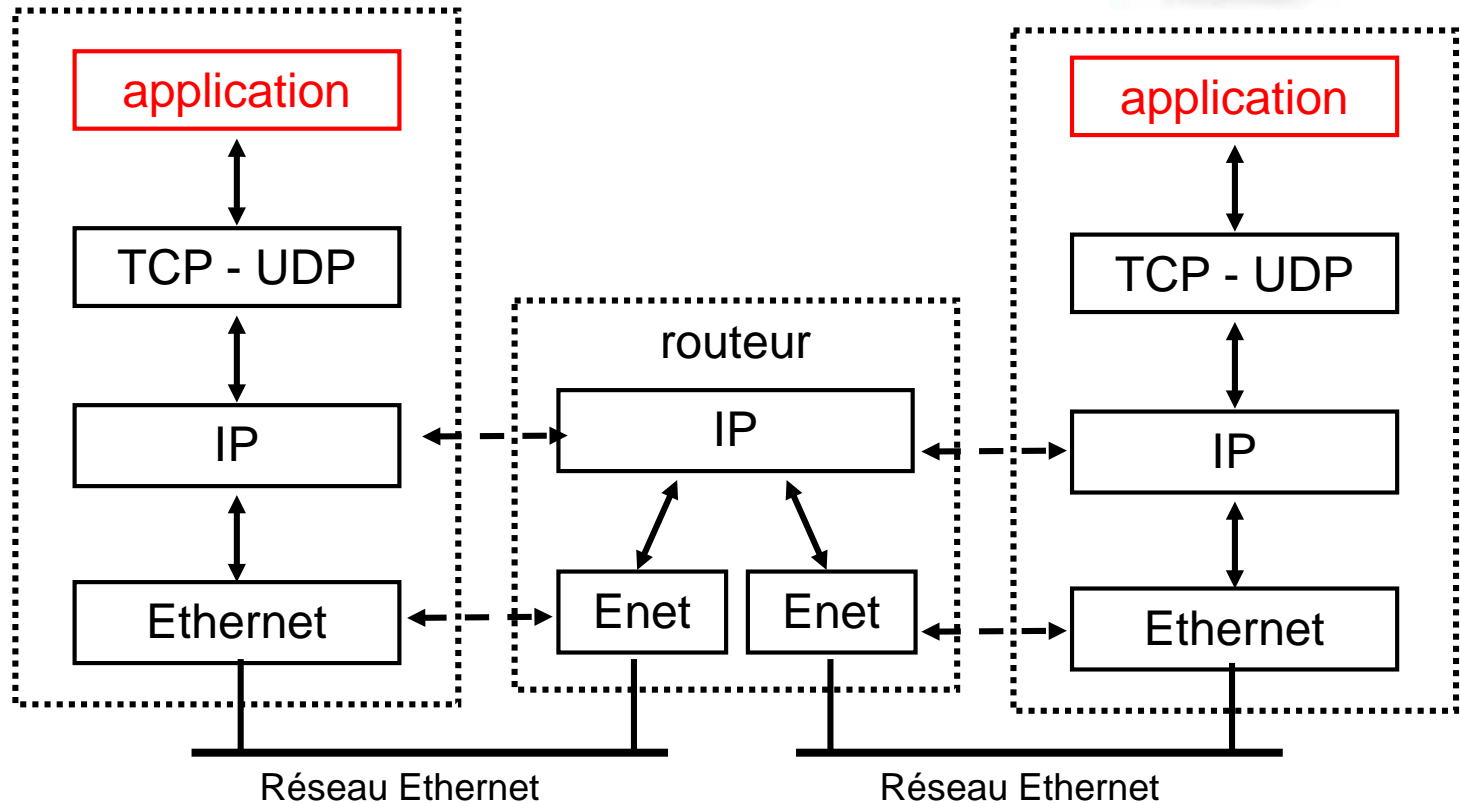
Chapitre 10 – Application

Couche application

- La couche Application est :
 - La source des données à transporter
 - La destination des données transportées
- La couche Application gère :
 - Les programmes de l'utilisateur
 - Fournit des applications et services (Telnet, FTP,...)

Chapitre 10 – Application Protocole d'application

Interface de l'utilisateur vers le réseau



- Un protocole d'application doit spécifier :
 - Le type et le contenu des messages échangées
 - Les règles déterminant quand ces messages peuvent être envoyés ou reçus
 - L'agent utilisateur, c'est-à-dire quelle interface utiliser entre le protocole d'application et l'utilisateur (Messagerie, navigateur,...)

- Principe du client/serveur
- Client :
 - Initie la connexion
 - Demande un service
- Serveur
 - Fournit un service (Web/mail,...)
- Il peut y avoir des systèmes simultanés où chacun est «client et serveur»

Chapitre 10 – Application exemple

- Exemple :

Vous devez envoyer un message à un correspondant. Quelles seront les étapes ?

- Vous rédigez votre message dans votre application (Outlook par exemple) sans savoir quelle sera l'application utilisée par votre correspondant.
- Vous envoyez votre message qui va commencer son chemin par la couche application qui va utiliser un protocole adéquat.

Chapitre 10 – Application exemple

- La couche Application va donc le coder en utilisant le protocole SMTP (Simple Mail Transfert Protocol)
- Le mail va poursuivre son chemin dans les différentes couches OSI, puis être transmis.
- Il arrivera à destination et à la couche Application, le protocole SMTP sera reconnu.
- Finalement, le message pourra être adapté sur la messagerie du destinataire (Thunderbird par exemple)