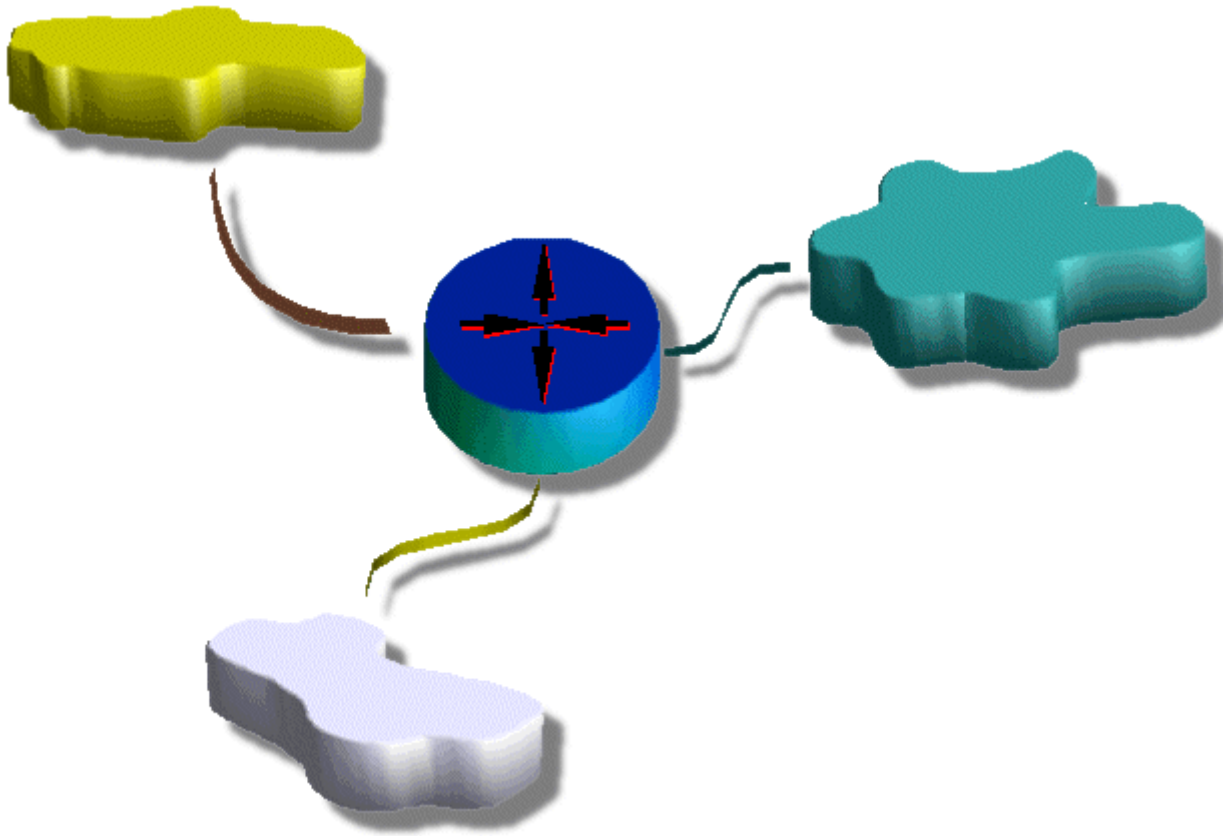
Introduction à l'Interconnexion de réseaux

Yann Duchemin
E-mail: yann.duchemin@free.fr – http://yann.duchemin.free.fr



Pré-requis :

- *Notions de bases sur les réseaux*
- *Topologie des réseaux*
- *Notions TCP/IP, IPX/SPX*

Objectifs :

Apporter un minimum d'autonomie à un administrateur réseau pour la configuration, la supervision, le diagnostique et la résolution de problèmes courants.

Version 1.1 - mars 2001

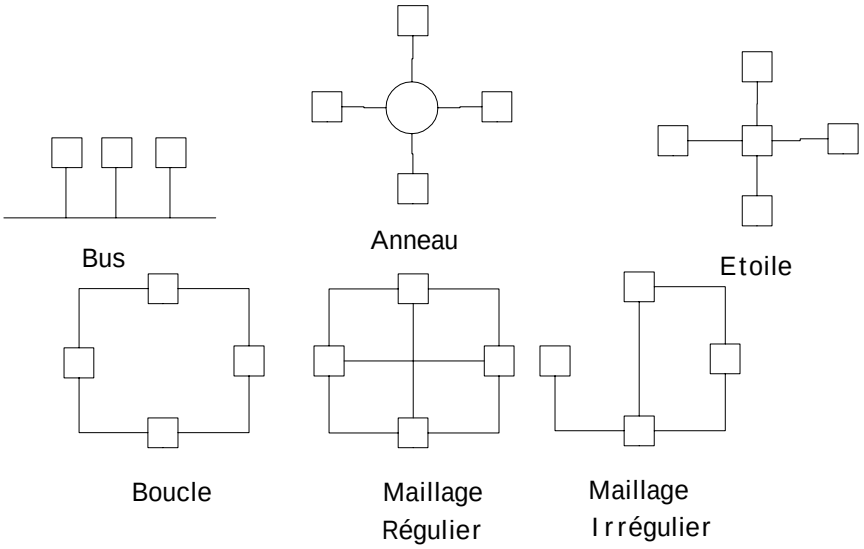
Table des matières

Introduction

Les réseaux informatiques peuvent se classer hierarchiquement de part leur taille. En effet si on part des « bus » internes vers le microprocesseur qui communique aux périphériques d'un ordinateur via les 3 bus que sont celui d'adresse, de données et de contrôle, nous pouvons les considérer comme des « réseaux » particuliers, réservés aux taches spécifiques de «l 'outil » informatique. Aussi on peut assimiler cette schématique de fonctionnement aux structures d'interconnexions d'aujourd'hui.

Le réseau local (Local Area Network) peut aller de quelques mètres (2 machines par exemple) à quelques kilomètres, en passant par une multitude de technologies reliant même plusieurs batiments.

Le réseau métropolitain (Metropolitan Area Network) interconnecte pour sa part plusieurs sites d'une même ville (universités, administrations, ...) constitués chacun d'un réseau local.
Le réseau étendu ou WAN (Wide Area Network) sert à faire communiquer ces infrastructures à tous niveaux supérieurs (pays, planète, ..?).



On peut, selon sa structure, déterminer la topologie d'un réseau. On y retrouve 2 classes d'un niveau physique:

- *Mode de Diffusion*

- *Mode Point à Point*

Dans le *mode de diffusion*, un seul support de transmission est partagé pour la communication entre 2 équipements. Dans ce cas, tous les équipements recoivent le message de la source, et c'est à chacun de déterminer s'il est concerné ou pas. Ceci implique qu'un seul élément du réseau doit utiliser le support, ainsi en cas du rupture de ce support, c'est le réseau entier qui est perturbé. Cependant, chacun des noeuds du réseau est indépendant des autres, il n'y a généralement pas de problème si aucun d'entre eux n'est en panne.

Dans le *mode point à point*, le support physique ne relie pas tous les noeuds d'un même réseau, ainsi pour faire communiquer 2 noeuds indirectement, le message devra passer par un ou plusieurs intermédiaires du réseau.

On appelera Interconnexion de réseaux la possibilité de faire dialoguer plusieurs sous-réseaux initialement isolés, par l'intermédiaire de périphériques spécifiques (concentrateur, pont, commutateur, et routeur), pour former un réseau étendu. Toutes sortes de technologies (topologies) peuvent êtres connectées.

Modes de communication

Quelque soit le principe physique de l'interconnexion, il existe 2 modes de fonctionnement différents :

- *Le mode connecté*

- *Le mode non-connecté*

Processus de communication du mode connecté :

1. L'émetteur demande l'établissement d'une connexion avec un hôte.
2. Si le recepteur (ou le gestionnaire du service) refuse la connexion, celle-ci n'a pas lieu.
3. Sinon un « lien » s'établit entre l'emetteur et le recepteur.
4. Les données transitent d'un point a l'autre.
5. La connexion est libérée.

Tout ce schéma est similaire à une communication téléphonique, l'avantage principal de ce mode de fonctionnement est l'identification de l'émeteur et du recepteur ainsi que la possibilité de définir une qualite de service à l'avance. L'inconvénient est la gestion « bavarde » pour de tout petits échanges de données, d'autre part une gestion complexe, mais aussi la complication des communications multipoints.

Processus de communication du mode non-connecté :

1. Envoi d'un message sur un support.
2. Le message contient les coordonnées du destinataire.
3. Chaque recepteur potentiel possède des coordonnées uniques.
4. Le contenu de l'information est inconnu de l'émetteur.
5. Le support est inconnu des utilisateurs (applicatifs).

Ce principe rappelle davantage celui du courrier postal, aucune vérification de la disponibilité du destinataire et des intermédiaires éventuels n'est effectuée avant l'envoi. Ce sont les équipements réseaux qui s'occupent de cette gestion.
Les blocs de données sont appelés « Datagrammes ».

Principes de commutation

Les communications (quel que soit leur mode : connecté ou non) sont basées sur un principe de commutation (création de circuits temporaires) pour acheminer un message d'un client vers un autre. Plusieurs types existent :

La **commutation de circuits** : la plus ancienne (réseau téléphonique commuté : RTC) qui crée des « lignes » le temps de la communication et les libère ensuite. Si pendant un temps T variable, rien n'est échangé sur cette ligne, on peut l'utiliser entièrement ou en partie pour un autre service. Cela améliore le fonctionnement global, mais complique la gestion des files d'attente, des priorités, ...

La **commutation de messages** : consiste à envoyer un ensemble d'informations (un message) d'un émetteur vers un récepteur en passant par un ou plusieurs noeuds de commutation. Chacun de ces noeuds attend la réception complète du message avant de le réémettre, cela demande des buffers sur chaque équipement, ainsi qu'un contrôle de flux pour éviter les engorgements. De plus le taux d'erreurs pour des messages de taille importante doit être très bas.

La **commutation de paquets** : celle-ci reprend la méthode précedente, mais en découpant le message en un nombre de fragments défini. Chaque noeud redirige ces fragments selon ses propres lois (tables de routage), la reprise sur erreur est donc plus simple, cependant le récepteur final doit être capable de réassembler tous ces paquets dans un ordre souvent différent de celui dans lequel il les a reçu.

La **commutation de cellules** : c'est une commutation de paquets particulière, puisque dans ce cas la taille du paquet est figée (à 53 octets pour ATM-asynchronous transfert mode), pour une émission en mode connecté via un chemin fixe pour toutes les cellules. C'est un mélange de la commutation de circuits et de la commutation de paquets, elle a pour avantage de simplifier le travail des commutateurs et d'autoriser des débits plus élévés.

Rappels sur le Modèle OSI

L'***O**pen **S**ystem **I**nterconnection* est une norme établie par L'*International Standard Organisation* , afin de permettre aux *systèmes ouverts* (ordinateur, terminal, réseau, ...) d 'échanger des informations avec d'autres équipements hétérogènes. Cette norme est constituée de 7 couches, dont les 4 premières sont dites *basses* et les 3 supérieures dites *hautes*. Le principe est simple, la couche la plus basse (directement au dessus du support physique) ne peut communiquer directement avec une couche n+1: chacune des couches est composée d'éléments matériels et/ou logiciels chargés de « transporter » le message à la couche immédiatement supérieure.

```
7 - Application
6 - Présentation  - : Passerelle
5 - Session
4 - Transport     - : TCP
3 - Réseau        - : Routeur
2 - Liaison       - : Pont
1 - Physique      - : Répeteur
```

1 - La Couche Physique

Cette couche définit les caractéristiques techniques, éléctriques , fonctionnelles et procédurales nécessaires à l'activation et à la désactivation des connexions physiques destinées à la transmission de bits entres deux entités de liaisons de données.

2 - La Couche Liaison

Cette couche définit les moyens fonctionnels et procéduraux nécessaires à l'activation et à l'établissement ainsi qu'au maintien et à la libération des connexions de liaisons de données entre les entités du réseau. Cette couche détecte et corrige, quand cela est possible, les erreurs de la couche physique et signale à la couche réseau les erreurs irrécupérables.

3 - La Couche Réseau

Cette couche assure toutes les fonctionnalités de relais et d'amélioration de services entre les entités du réseau, c'est à dire : l'adressage, le routage, le contrôle de flux, la détection et la correction d'erreurs non résolues par la couche 2 (liaison) pour préparer le travail de la couche 4.

4 - La Couche Transport

Cette couche définit un transfert de données transparent entre les entités en les déchargeant des détails d'éxecution (contrôle entre l'OS et le support de transmission). Son rôle est d'optimiser l'utilisation des services de réseau disponibles afin d'assurer à moindre coût les performances requise par la couche 5 (session).

5 - La Couche Session

Cette couche fournit aux entités de la couche présentation les moyens d'organiser et de synchroniser les dialogues et les échanges de données. Il s'agit de la gestion d'accès, de sécurité et d'identification des services.

6 - La Couche Présentation

Cette couche assure la transparence du format des données à la couche 7 (application).

7 - La Couche Application

Cette couche assure aux processus d'application le moyen d'accès à l'environnement OSI et fournit tous les services directement utilisable par l'application (transfert de données, allocation de ressources, intégrité et cohérence des informations, synchronisation des applications).

Le modèle OSI

<table>
<tr><td>Couche Application
7</td><td colspan="2">Programmes,
Applications Réseau</td><td colspan="4">Messagerie, Navigateur Internet, ping, ftp, bootp, ...</td></tr>
<tr><td>Couche Présentation
6</td><td colspan="2">Utilitaire de conversion, de cryptage,...</td><td colspan="4">Interpréteurs ASCII/EBCDIC, Emulateurs,...
(telnet, nfs, ...)</td></tr>
<tr><td rowspan="2">Couche Session
5</td><td colspan="6">Système d'exploitation</td></tr>
<tr><td colspan="2">Network
Operating
System</td><td colspan="4">Netware IP/IPX - NetBios - DEC - snmp, ftp, smtp, telenet</td></tr>
<tr><td>Couche Transport
4</td><td colspan="6">SPX, PCLAN, LanManager, DecNet, PC/TCP
TCP (connecté -> ftp,http,smtp,...) - UDP (non connecté -> dns, tftp, ...)</td></tr>
<tr><td rowspan="2">Couche Réseau
3</td><td colspan="6">IEEE 802.1
(ip, ipx, rip, icmp, igmp,...)</td></tr>
<tr><td colspan="6">Drivers Réseau</td></tr>
<tr><td rowspan="4">Couche Liaison
2</td><td rowspan="2">Logical
Link
Control</td><td colspan="5">IEEE 802.2</td></tr>
<tr><td>CSMA/CD</td><td>Token Bus</td><td>Token Ring</td><td>DQDB</td><td>ISO 9314
ANSI X3T9.5</td></tr>
<tr><td>Medium
Acces
Control</td><td>IEEE 802.3</td><td>IEEE 802.4</td><td>IEEE 802.5</td><td>IEEE 802.6</td><td>FDDI</td></tr>
<tr><td colspan="6">isdn, lan, ppp, slip, ...</td></tr>
<tr><td rowspan="3">Couche Physique
1</td><td rowspan="2">Physical
Layer
Signaling</td><td rowspan="2">MTU
64/1518bytes</td><td rowspan="2">MTU
32b/16Kb</td><td rowspan="2">MTU
32b/16Kb</td><td rowspan="2"></td><td rowspan="2">MTU
32b/4400b</td></tr>
<tr><td>AUI</td></tr>
<tr><td colspan="6">Ethernet, paire torsadée, ...</td></tr>
</table>

Acheminement des données

Quatre types d'équipements distincts permettent d'acheminer les données :

Les répéteurs et concentrateurs (ou « hubs » qui ne sont pas des répéteurs)
Les ponts (ou « *bridges* »)
Les routeurs (ou « *routers* »)
Les paserelles (ou « *gateways* »)

1 - Les Répéteurs

Les répéteurs possèdent exactement 2 interfaces, et agissent au niveau de la **couche physique**. Ils retransmettent le signal capté sur une interface et le retransmettent en le régénérant, ils ne possèdent pas d'adresse physique, et sont connectés à 2 réseaux distincts (point de liaison).

De manière générale, les répéteurs permettent d'augmenter de manière simple l'étendue des segments Ethernet ou des anneaux Token-Ring. En effet, sur ces types de topologies, l'affaiblissement du signal sur les câbles est lié directement à la longueur du segment qui gêne proportionellement la propagation du signal. La solution est donc de recréer un/des segments ou un/des anneaux dès que l'on tend vers les limites physiques de la solution choisie, et ceci grâce aux répéteurs.

Le cas particulier du concentrateur, qui intervient également sur la couche physique, est en fait l'utilisation d'un bus interne à lui-même, de ce fait il émule une topologie en bus par une topologie en étoile. L'avantage est que dans certains équipements évolués (dit manageables), on peut contrôler les communications. Par exemple limiter les émissions de messages, en renvoyant des trames erronnées pour faire intervenir l'algorithme csma/cd, mais aussi sécuriser les accès, le concentrateur permettant de lire l'adresse physique des stations de tous les segments raccordés. Attention cependant de ne pas vérouiller à une adresse mac unique un port sur lequel serait raccordé un autre hub.

On reconnaît 2 type principaux de concentrateurs baptisés *classe I* et *classe II* :

Pour la première classe : connexion de postes réseau avec une distance maximale de 100 mètres (diamètre de collision de 200m) pour ethernet. On ne peut pas interconnecter un autre concentrateur.

Pour la seconde classe : connexion de postes réseau avec une distance maximale de 100 mètres, avec la possibilité de connecter avec un câble un autre concentrateur de classe II. Le diamètre de collision est de 205m, ce qui signifie que si le câble mesure 10m, la distance maximale entre 2 noeuds actifs du même concentrateur ne doit dépasser 195m.

Pour la norme ethernet ou fast-ethernet, il est autorisé dans le cas d'utilisation de concentrateurs (et éviter l'emploi de répéteurs) d'employer un bus interne (dit *bus de fond de panier*) entre plusieurs concentrateurs. Ceci permet de multiplier le nombre de bus, ils sont alors empilables (ou *stackables*) par un ou des connecteurs particuliers (propriétaire) généralement à plein débit, ou par la face avant (croisement du media) au débit standard. Cependant, attention à la normalisation pour conserver des segments de longueur correcte.

2 - Les Ponts

Les ponts possèdent au moins 2 interfaces, et agissent au niveau de la **couche liaison**. Leur rôle est de récupérer les trames qui arrivent sur une de leurs interfaces, et de les retransmettre sans les modifier sur une ou plusieurs autres interfaces. Un pont dit « pont filtrant » examine les paquets en circulation sur ses interfaces afin de déterminer le ou les destinataires, ceci permet une économie de la bande passante, mais en utilisant un protocole dédié, les temps d'accès sont légérement allongés. Les ponts travaillent au niveau MAC et de manière indépendante des protocoles de niveau supérieur, ils ne permettent donc pas d'interconnecter 2 topologies distinctes : exemple, les trames 802.2 et 802.5 étant différentes, il est impossible de passer d'un segment ethernet à un segment token-ring via un pont. D'autre part de manière générale, 2 segments interconnectés par un pont doivent être dans le même espace d'adressage (protocole de niveau supérieur) TCP/IP, IPX, ... Sauf cas particuliers que nous verrons par la suite avec les commutateurs et la notion de réseaux virtuels.

Dans le principe, un pont analyse toutes les trames des segments auxquels il est directement raccordé. Il identifie en permanence les stations présentes pour stocker leur adresse physique. Chacune de ces entrées est stockée dans une table de correspondance (adresse/numéro de port) valide pour une période de temps donnée. Dans le cas d'un commutateur (on parle de réseau commuté), l'ensemble des noeuds ne se partage plus la même bande passante (comme dans le cas du concentrateur). Le commutateur après avoir repéré le destinataire dans sa table de routage (il analyse préalablement la trame pour déterminer l'adresse physique), crée ensuite une « liaison » directe entre les 2 noeuds (on parle par exemple de matrice de commutation) avec une bande passante maximale à cet instant. Des paramètres optionnels comme le contrôle de flux, la gestion de files d'attente, agrégations de segments, peuvent êtres implémentés : on parle de micro-segmentation. Le plus de cette technologie est son utilisation dans les réseaux à hauts débits, en utilisant des commutateurs fédérateurs, par exemple pour segmenter un service en fonction de son besoin en bande passante, ou pour connecter des serveurs, les stations de travail étant connectées sur des concentrateurs eux-même reliés au commutateur. Ainsi certains modèles peuvent accepter indifférement des connexions à 10Mbs, 100Mbs, ... et bien entendu les mixer (ex : serveurs à 100Mbs, stations à 10Mbs, sur le même commutateur).

Pour acheminer les trames, il existe 3 principes :

- Le « **store and forward** » : la trame est entièrement mémorisée par le commutateur, l'entête est analysée, si la trame est correcte, elle est acheminée vers le destinataire. Cette technique n'est pas la plus rapide, mais seules les trames sans erreurs sont reémises (vérification du checksum, de l'alignement, de la longueur, ...). Il y a dans de cas 1 domaine de collision par port.

- Le « **cut through** » : l'entête est immédiatement analysée et le paquet est alors envoyé au destinataire avant même que la fin de la trame n'arrive au commutateur. Tous les ports sont dans le même domaine de collision. Cette technique est rapide, mais inadaptée si l'on raccorde un concentrateur sur l'un des ports, car cela engendre des collisions qui sont remontées jusqu'au commutateur. Le commutateur (étoile) doit executer l'algorithme du CSMA/CD ou du BEB afin de limiter le droit de parole des stations du réseau pour gérer le flux sur les bus. Le contrôle du flux peut alors se faire en envoyant un début de trame d'information de collision aux stations qui encombrent le segment, avant le remplissage total des buffers. Autre technique si des serveurs sont connectés sur ce port, c'est le « *load balancing* », ou répartition de la charge en regroupant plusieurs

ports pour une même machine (autant d'interfaces réseau que de ports), c'est de l'agrégation de liens.

- La « **transmission adaptative** » : certains commutateurs analysent le taux d'erreurs et commutent d'un mode à l'autre selon la valeur.

Le concentrateur qui émule le bus sur une topologie en étoile permet la gestion des collisions par émulation (ce qui permet aux stations d'auto-gérer correctement la bande passante) mais n'a pas cette capacité qu'a le commutateur à doubler si on le désire la bande passante.
En effet, le commutateur utilise deux modes de transmission : le half-duplex et le full-duplex. En mode commuté, il n'y a plus de collisions possibles (en théorie), donc nous n'avons plus besoin de recopier les messages sur la paire en reception. On peut donc émettre simultanément sur la paire qui sert à l'émission et sur celle qui sert à la réception, la bande passante normalisée est alors doublée.

3 - Les Routeurs

Les routeurs possèdent au moins 2 interfaces, et agissent au niveau de la **couche réseau**. Leur rôle est de récupérer les trames MAC qui arrivent sur une de leur interface, d'en extraire les datagrammes IP, et de les renvoyer sur une autre interface en les encapsulant dans de nouvelles trames MAC. Pour déterminer sur quelle interface un paquet doit être réémis, les routeurs consultent une table de routage qui est en fait la cartographie des réseaux auquels ils sont connectés.

Un routeur est constitué de 2 éléments essentiels :

- Une composante matérielle : des ports (ou interfaces) qui recoivent et génèrent des trames au format adapté à la topologie raccordée.Cette partie a en charge le raccordement de n'importe quel type de réseau (Ethernet, Ligne Serie, ...)

- Une composante logicielle : Un système d'exploitation est en place afin de dédier des processus de traitement des paquets. Cette partie a en charge de déterminer vers quelle interface envoyer un paquet reçu, et de convertir les trames.

Un routeur *structure* donc un réseau en le découpant de manière logique. Les paquets (donc les trames qui les encapsulent) restent au sein d'un même réseau logique tant qu'ils n'ont pas besoin d'être réémis vers un autre. La conséquence directe de ce fait est que les flux sont mieux gérés : les broadcast mac ne sont pas retransmis, ceux de niveau supérieur peuvent l'être selon la configuration et pour les besoins particuliers de service liés (TCP et DHCP, DNS,...).

4 - Les Passerelles

Les passerelles agissent au niveau de la **couche application**. Leur rôle est d'intercepter les informations au plus haut niveau, et de les rettransmettre vers une autre machine.

Résumé

Matériel	Application	Caractéristiques	Technologies	Particuliarités
Répéteur	Petits réseaux adressages plats mise en oeuvre simple	1 domaine de collision 1 domaine de broacast	Extension de bus Extension (limitée) de segments	
Pont / Commutateur TTR 800µs-15µs	Petits réseaux adressages plats mise en oeuvre simple	Interconnecte 2 réseaux de même topologie Utilise les adresses physiques (MAC) des interfaces réseaux Plusieurs domainne de collision 1 domaine de broacast	Spanning tree (Ethernet) évite les boucles dans des réseaux maillés par determination statique des chemins Source routing (Token Ring) permet aux stations de choisir le chemin à emprunter	Identifie les adresses mac sur chaque segments retransmet les broacasts & multicast et les adresses mac inconnues
Routeur TTR 800µs à 1800µs	Grands réseaux structurés Conversion de protocoles, encapsulation, routage,...	Plusieurs domaines de collision 1 domaine de broacast Interconnecte toutes les topologies Utilise un adressage logique indépendant des couches physiques Adressage découpé	Routage dépendant des protocoles (ospf pour tcp/ip, nlsp pour ipx,...) Chaque paquet est transmis par les adresse src/dest Le routeur décide du meilleur chemin, à l'aide d'un protocole de routage	Un O.S. Et un processus par protocole à gérer Adressage logique (n° de réseau+n° de machine) Indépendant de l'adresse MAC Résolution de l'adresse MAC/logique
Passerelle	Conversion de protocoles			

Principe de fonctionnement du routage

Attention de ne pas confondre protocole routable et protocole de routage. Par protocole routable on sous-entend un protocole de niveau 3 du modèle OSI, tel que IP, IPX, DecNet, ...
Une station qui veut communiquer vers une autre station n'appartenant pas à un même réseau logique doit solliciter un routeur afin de déterminer le chemin pour y parvenir. Cette station doit au moins bénéficier d'un logiciel réseau lui permettant de traiter des informations de niveau 3. On a alors plusieurs choix pour y parvenir : soit il existe un système dynamique permettant de découvrir le routeur, soit la station connaît l'adresse du routeur par défaut. On parle alors de routage **statique** ou de routage **dynamique**. Un protocole routable est en fait un protocole d'encapsulation qui provient de la couche transport afin d'assurer les services de la couche réseau.

Quoi qu'il en soit le routeur par défaut et la station émettrice doivent être sur le même domaine de broacast mac (physiquement liés par un média), un routeur ne prend en compte que les trames mac qui lui sont destinées (contrairement au pont qui lit systématiquement toutes les trames en circulation sur le média).

La communication entre 2 noeuds peut se faire de manière *directe*, c'est l'adresse réseau qui est comparée, si elle est identique alors la transmission du datagramme est réalisée. Si l'adresse réseau est différente, on parle de routage *indirect* alors au moins une passerelle sera traversée. Dans ce dernier cas, le datagramme est émis à la paserelle, celle-ci extrait les données, selectionne le prochain noeud (recepteur des données, ou passerelle par défaut), remet en forme la nouvelle trame et la réémet.

Un mécanisme spécifique de résolution d'adresse (ARP), est mis en oeuvre lors de l'établissemnent de la session de niveau 3. La station émettrice diffuse alors un paquet de broacast, à l'aide de l'adresse réseau du routeur (niveau 3), qui demande de renvoyer l'adresse mac du routeur qui détient l'adresse logique de la station réceptrice. Une fois l'adresse mac connue, la station émettrice envoie toutes les trames suivantes à cette adresse mac, donc au routeur, mais avec l'adresse logique de la station cible. Sur l'autre réseau logique (destination), la station reçoit les trames en provenance du routeur, croyant qu'il s'agit directement de la station émettrice (l'adresse mac connue est celle du routeur, et l'adresse physique est celle de la station émettrice).

Les stations associent donc l'adresse mac du routeur à l'adresse logique de toutes les stations se trouvant sur les réseaux situés de l'autre côté du routeur.

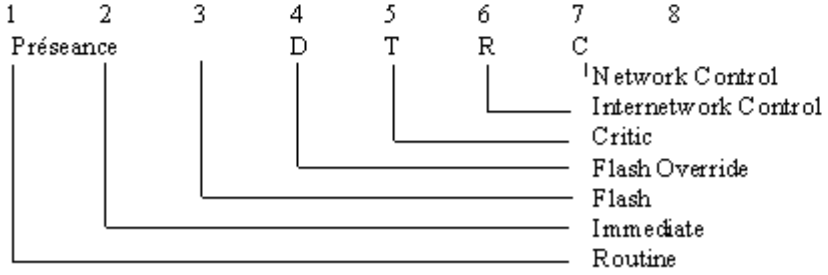
Des fonctions évoluées peuvent être mises en place par la composante logicielle. Par exmple, le contôle de flux, qui analyse les paquets (voir les champs des datagrammes) et affecte ainsi une priorité forte aux sessions transactionnelles (ex.: telnet tcp-port 23) et moins forte pour les messages liés à un transfert de données (ex.: http tcp-port 80). On peut également effectuer des filtrages pour augmenter la sécurité, que ce soit sur les adresses, les protocoles, ou encore le type d'application.

Tout comme les trames *mac* ou *llc* permettent de connaître le protocole transporté dans le champ de données, les paquets disposent d'un champ identifiant le type d'application. Ce type de filtrage dépend donc du niveau 3 (cf. schéma page suivante).

Exemple d'un Datagrammes IP :

Version Type d'enveloppe	Longueur de l'entête en mots de 32bits mini 5 max 15	Type de service Indication de priorité sur le routage (1)	Longueur Totale du datagramme = entête + données Taille du champs données : LongTot - Long Entete soit 2E16 = 65535
Identification Unique pour réassembler les fragments d'un même datagramme		Flags 000: frag sur le dernier 001: frag intermédiaire 010: frag interdite	Offset de fragmentation taille en octet des données du datagramme dans le segment (2)
Time To Live si = 0 alors destruction du datagramme (désincrémentation a chaque passage d'un routeur)		N° de protocole 1 icmp 5 stream 2 igmp 6 tcp 3 gcp 8 egp 4 ip 17 udp ...	CRC champ de contrôle de l'enveloppe uniquement
Adresse IP Source			
Adresse IP Destination			
Options			PAD
Données			

(1) Paramètre de gestion de la file d'attente des routeurs - de 0 à 7



(2) Sert lors de la fragmentation, ainsi lorsqu'un fragment est perdu, tous les autres sont détruits. Les réseaux hétérogènes utilisant des paquets de tailles différends, des débits différents, des taux d'erreurs variables, ...

Comparaison des techniques d'interconnexions

Pont / Commutateur	***Routeur***
Traite les adresses mac (niveau 2)	Traite les paquets des protocoles (niveau 3)
Adressage MAC (lié à la carte réseau)	Adressage propre à chaque protocole
Découpage par segments physiques	Découpages par réseaux logiques
Interconnexion de même topologie	Interconnexion de différentes topologies
Pas de contrôle de flux (standard)	Contrôle de flux par priorité, non diffusion des broacast mac et filtrage
Composante matériel forte, mise en oeuvre simple	Composante logicielle forte, nombre important d'interfaces supportées
Temps de traitement performant	Temps de traitement +/- performant

Notons que le répéteur n'est pas considéré comme un matériel d'interconnexion puisqu'il agit au niveau des signaux (transparent aux trames mac) en régénérant le signal.

Familles de routage

Le routage est divisé en 2 familles, d'une part le routage entre 2 systèmes autonomes différents, baptisé **EGP** pour *Exterior Gateway Protocol* (les exemples les plus courants sont EGP, BGP). L'autre famille réalise le routage entre 2 routeurs du même segment autonome, il s'agit d'**IGP** pour *Interior Gateway Protocol*. Cette dernière famille, IGP, est elle-même divisée en 2 types de protocoles :

- Les protocoles à **vecteur distance** (tels que le sont *RIP, IGRP, EIGRP*, ...)

Ils sont simples à utiliser, et nécessitent peu de ressources.

- Les protocoles à **état de liens** (tels que le sont *OSPF, ES-IS, IS-IS,* ...)

Leur convergence est rapide, la création de boucle est bien contrôlée, il est possible d'avoir des chemins d'accès multiples.

Le principal point de contrôle déterminant le chemin à emprunter pour transmettre les données est ce que l'on nomme le **métrique** :

Le métrique est implémenté dans les tables de routage, et utilisé par les protocoles de transmission de paquets, c'est un critère de comparaison.

- *Path Length* **:**
  L'administrateur d'un site peut attribuer des coûts à chacun des liens de son réseau. La longueur d'un lien est égale à la somme des coûts de tous les liens qui le composent. Certains protocoles de routage comme RIP se contentent de compter le nombre de routeurs traversés pour attribuer un coût. Cette variable est statique.

- *Reliability* :
  Selon les technologies choisies, les liens d'un réseau sont plus ou moins sensibles aux perturbations extérieures. De plus certains liens sont plus ou moins faciles à être réparés ou secourus. Cette métrique tient compte de la fiabilité, en termes de pourcentage d'erreurs de chaque lien de réseau traversé, ou de la charge du processeur en rapport avec le nombre de processus à traiter. Ce taux est habituellement assigné à la ligne par l'administrateur système d'un site, et est une valeur arbitraire et donc statique.

- *Delay* :
  Le temps de réponse de la ligne fait référence au temps nécessaire pour transmettre un paquet d'un point à un autre à travers un réseau. Ce facteur dépend de plusieurs paramètres comme la largeur de bande des réseaux intermédiaires, le taux de congestion de chaque routeur et leur capacité à y faire face, ainsi qu' à la longueur du chemin choisi . Cette métrique, tenant compte de beaucoup des caractéristiques de la ligne, est donc représentative de son coût. De ce fait c'est une des plus utilisées. Cette valeur est statique.

- *Bandwidth* :

La largeur de bande représente le débit de la ligne. Ce débit ne représente pas forcément le débit instantané de la ligne. Une ligne à débit instantané moyen mais fiable est préférable à une ligne à haut débit complètement congestionnée. Cette valeur est statique.

- *Load* :

La disponibilité représente le degré de disponibilité des ressources du réseau. Elle peut-être calculée à partir du taux d'utilisation de CPU, du débit de paquets par secondes...
Malheureusement, le contrôle de ces paramètres contribue à l'utilisation de ces ressources. Cette valeur est dynamique.

- *Cost* :

Certains utilisateurs peuvent accorder plus d'importance au prix de la transaction qu'à la vitesse. Ils préfèrent donc employer des lignes lentes leur appartenant plutôt que des lignes publiques rapides mais chères.

- *Emplacement géographique* :

Un paramètre important peut être l'emplacement géographique de passage des lignes. Pour des applications militaires par exemple, il peut être nécessaire de pouvoir éviter certains passages à risques.

Exterior Gateway Protocol

Il s'agit là de l'un des plus anciens protocoles de routage inter-domaines, ses fonctionnalités le rendent peu pratique pour les réseaux actuels. Il a été conçu pour rallier des sous-ensembles à un réseau unique (topologie en étoile), qui était ARPANET. Le calcul des routes se fait en communiquant la découverte de segments au voisin direct (1 seul saut) le plus proche. La gestion des boucles est donc inexistante.

Border Gateway Protocol

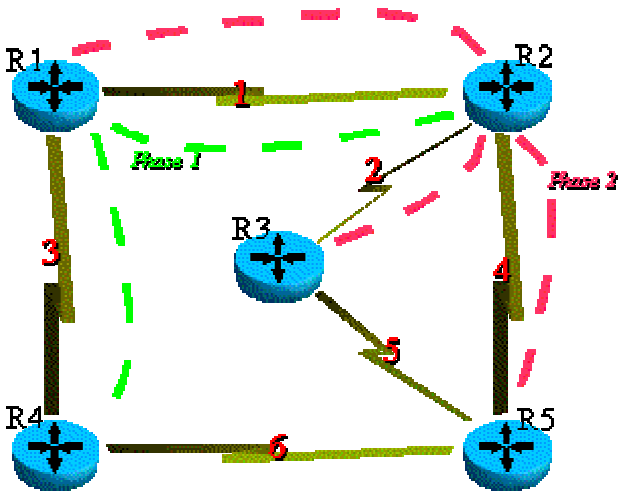
BGP est l'évolution directe d'EGP avec tout d'abord une gestion des boucles. Pour éviter une boucle dans le réseau, BGP fait transiter toute la "carte" du réseau à tous les routeurs qui composent ce réseau, notamment avec le chemin emprunté pour relier les noeuds entre eux. Si un des composants du réseau est présent plus d'une fois dans la liste, il y a vraisemblement une boucle, donc une erreur à traiter. On peut lui reconnaître d'autres avantages (fiabilité, rapidité, ...).
Le problème de TCP est son mode de contrôle de flux : en effet en cas de problème, TCP réduit immédiatement son débit d'émission en réduisant sa fenêtre de congestion, c'est à dire le nombre d'octets qui peuvent être émis sur une connexion sans attendre un acquittement. Ce principe fonctionne bien pour la plupart des communications, mais pas dans le cas d'un protocole de routage dont la vitesse de convergence est directement dépendante. On fixera donc dans un paquet IP un code de préséance « Internetwork Control », qui modifie la priorité de traitement. A noter qu'en utilisant TCP (mode connecté, donc communication fiable), la mise à jour des tables de routage peut se faire de manière non cyclique.

Protocoles à Vecteur Distance

Dans ce cas chaque routeur d'un réseau est doté d'un numéro, on affecte également un numéro à un lien physique utilisé comme coût (en général la valeur est de 1). Au départ chaque routeur ne connaît que lui même, son vecteur de distance équivaut alors à la valeur 0, et la valeur « infinie » pour toutes les autres destinations.

- A intervale régulier (ou quand l'état du réseau a changé) les routeurs transmettent leur vecteur distance à chacun de leurs voisins.
- Chaque routeur conserve le vecteur distance le plus récent reçu de la part de chacun de ses voisins.
- Chaque routeur examine le vecteur reçu, et recalcule son propre vecteur distance, en minimisant le coût de chaque destination.
- Le vecteur distance est recalculé à la suite des événements suivants :
  - Envoi par un voisin d'un vecteur distance contenant une information différente de la précédente.
  - Découverte de l'interruption d'une liaison vers un voisin.

Voici les différentes phases d'apprentissage:



Phase 1 : Chaque noeud résume sa propre table en diffusant son vecteur distance à son voisin.

Phase 2 : Chaque noeud qui reçoit une information de mise à jour, conserve la plus petite valeur pour mettre sa propre table de routage à jour, et réémets les modifications.

Etc...

Résumé des différentes phases des tables de routage :

R1	*Lien*	*Coût*	*R2*	*Lien*	*Coût*	*R3*	*Lien*	*Coût*	*R4*	*Lien*	*Coût*	*R5*	*Lien*	*Coût*	*Phase*
R1	-	0	R2	-	0	R3	-	0	R4	-	0	R5	-	0	0
			R1	1	1				R1	3	1				1
R2	1	1				R2	2	1				R2	4	1	
R4	3	1				R1	2	2				R1	4	2	2
												R4	6	1	
			R4	1	2	R5	5	1	R2	3	2	R3	5	1	
			R3	2	1	R4	5	2	R5	6	1				3
			R5	4	1										

Exemple avec RIP

A l'origine il s'agit d'un protocole de routage *LAN* basé sur un principe de diffusion, le routage se fait par le saut le plus faible jusqu'à la destination avec un seuil maxi de 15. Le fonctionnement normal de RIP consiste à diffuser les vecteurs à intervalles réguliers de 30 secondes. Si un routeur voisin ne reçoit pas de nouveau cette même information au bout de 180 secondes, on suppose alors que la liaison concernée n'est plus valable. Cette liaison prend un valeur infini (16) dans la table de routage du routeur. Lorsqu'un routeur détecte que l'état du réseau a changé, il n'attend pas le délai défini pour réémettre le vecteur. Il procède à des « *mises à jour déclenchées* », en n'envoyant que la l'information sur la liaison concernée; ce mode à une convergence rapide, mais le risque de créer une boucle est important. La taille maximale d'un message est de 512 octets, ce qui permet de transmettre 25 entrées. Le véhicule d'information utilise les datagramme *UDP* sur le port *520*.

Pour minimiser les effets de boucle différentes techniques sont mise en pratique :

1. *Horizon partagée* : Les mise à jour se font partout, sauf d'où provient l'information.
2. *Horizon partagée avec retour empoisonné* : C'est un variante de la précédente méthode, mais l'on renvoie à l'émetteur de l'information une métrique de 16.
3. *Le gel* : Si un lien est inaccessible, la mise à jour est interrompue pour une durée T (~60s)

La version 1 était très simple à utiliser, mais il n'y avait pas de procédure d'authentification, impossibilité de router à partir des préfixes de sous-réseau ou d'adresses sans classe (CIDR, voir plus loin). C'est pourquoi arriva la version 2, qui reste **compatible**. Un routeur, ou une âme malveillante, pouvait émettre des vecteurs distances absurdes. La version 2 a donc introduit une **procédure d'authentification**.

Exemple avec IGRP - Interior Gateway Routing Protocol

Il s'agit là d'un protocole propriétaire de *Cisco*, pour palier les défauts de RIP : une seule métrique, nombre de sauts limité,.... . De plus les protocoles "remplaçant" tel qu'OSPF tardaient. Il utilise comme RIP la diffusion périodique de mises à jour, mais 90 secondes au lieu de 30 secondes pour RIP, encombre moins le réseau.

Le processus de routage et le choix d'une route est basé sur la prise en compte des paramètres suivants :

- Largeur de bande
- Charge sur les lignes
- Délais dus à la topologie
- Fiabilité du chemin
- Taille maximale des paquets (MTU)

IGRP permet de partager le trafic entre les chemins dont les coûts sont presque égaux (load splitting), sans risquer de créer des boucles. Il utilise pour cela un coefficient de variance V : Un deuxième meilleur chemin peut être sélectionné si sa métrique M2 n'est pas plus de V fois supérieur à la métrique M1 du meilleur chemin.

IGRP utilise plusieurs timers, dont les temps de fonctionnement sont configurables :

- Le *Update Timer* gère la fréquence d'envoi de messages de mise à jour aux routeurs voisins.
- Le *Invalid Timer* contrôle le temps au bout duquel, en l'absence de message de la part d'un routeur, on peut le déclarer down (par défaut 3 fois le temps d'attente de l'update timer).
- Le *Hold Timer* gère le temps pendant lequel les mises à jour sont refusées en cas de hold down (3 fois le temps d'attente de l'update timer plus 10 secondes).
- Et enfin le *Flush Timer* gère le temps de vie d'une route non confirmée (par défaut 7 fois le temps d'attente de l'update timer).

IGRP utilise d'autres méthode afin d'éviter les boucles, comme la "retenue" et "l'empoisonnement" des routes. Ce qui a pour effet de rendre les destinations temporairement indisponibles.

Cependant IGRP a quelques problèmes pour la détection des boucles :

Les techniques de retenue ou d'empoisonnement des routes ne peuvent prévenir les boucles qu'en rendant des destinations inaccessibles pour une période qui peut-être assez longue. IGRP ne supporte pas non plus les masques de sous-réseaux de longueurs variables, ni les agrégations de réseaux. Cisco a donc développé une autre version de IGRP : Extended IGRP. EIGRP garantit l'absence total de boucles même transitoire grâce à l'algorithme *DUAL*, bien qu'il rende certaines destinations transitoirement inaccessibles.

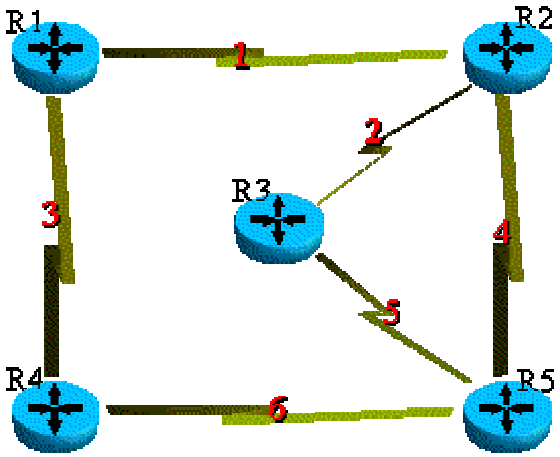
Pour diminuer les besoins en transmission des protocoles à vecteur de distance, EIGRP fait appel aux mises à jour incrémentales, c'est à dire que toutes les mises à jour seront acquittées et que chaque routeur conservera en mémoire les distances et destinations annoncées par chacun des ses voisins. On ne peut s'appuyer sur l'échange périodique des mises à jour incrémentales, pour tester la continuité de la liaison. C'est pour cela qu'il y a cinq types de messages dans EIGRP :

- Hello:
  Les paquets sont envoyés à « tous les routeurs EIGRP du réseau » à intervalles réguliers. Les routeurs voisins les acquitteront en envoyant leurs propres paquets « Hello ».
- Mise à jour:
  Pour envoyer les modifications du vecteur de distance d'un routeur passif
- Demande:
  Pour envoyer les mises à jour du vecteur de distance d'un routeur actif et déclencher le processus de diffusion,
- Réponse :
  envoyé en réponse à une demande,
- Requête :
  Similaires aux requêtes d'IGRP.

Le format des entrées de la table de routage a été modifié pour permettre le routage d'après des masques de sous-réseau arbitraires ou d'après des masques d'agrégats selon « CIDR ».

Protocoles à Etat de Liens

Dans cette configuration, chaque routeur a la responsabilité de rentrer en contact avec les routeurs voisins et d'apprendre leurs noms. Chaque routeur construit un paquet connu sous le nom de « paquet d'état de liaison », ou **LSP** (*Link State Packet*) qui contient une liste des noms et des coûts de ses voisins. Le LSP est transmis d'une manière ou d'une autre à tous les autres routeurs, et chaque routeur enregistre le LSP généré le plus récemment par chaque autre routeur. Chaque routeur, qui possède maintenant une carte complète de la topologie, calcule les routes vers chaque destination.



Dans ce cas, chacun des routeurs interroge son voisin afin de connaître son nom, après quoi il construit un paquet particulier dit paquet de liaison (Link State Packet) qui contient la liste des noms connus associés à leur coût. Chaque routeur enregistre alors le LSP le plus récent généré par un routeur donné, pour une liaison connue, ensuite chacun effectue un calcul des routes pour chacune des destinations ainsi découvertes.

On obtient dans cet exemple :

De	***À***	***Lien***	***Coût***
R1	*R2*	*1*	*1*
R1	*R4*	*3*	*1*
R2	*R1*	*1*	*1*
R2	*R3*	*2*	*1*
R2	*R5*	*4*	*1*
R3	*R2*	*2*	*1*
R3	*R5*	*5*	*1*
R4	*R1*	*3*	*1*
R4	*R5*	*6*	*1*
R5	*R2*	*4*	*1*
R5	*R3*	*5*	*1*
R5	*R4*	*6*	*1*

Exemple avec OSPF - Open Shortest Path Find

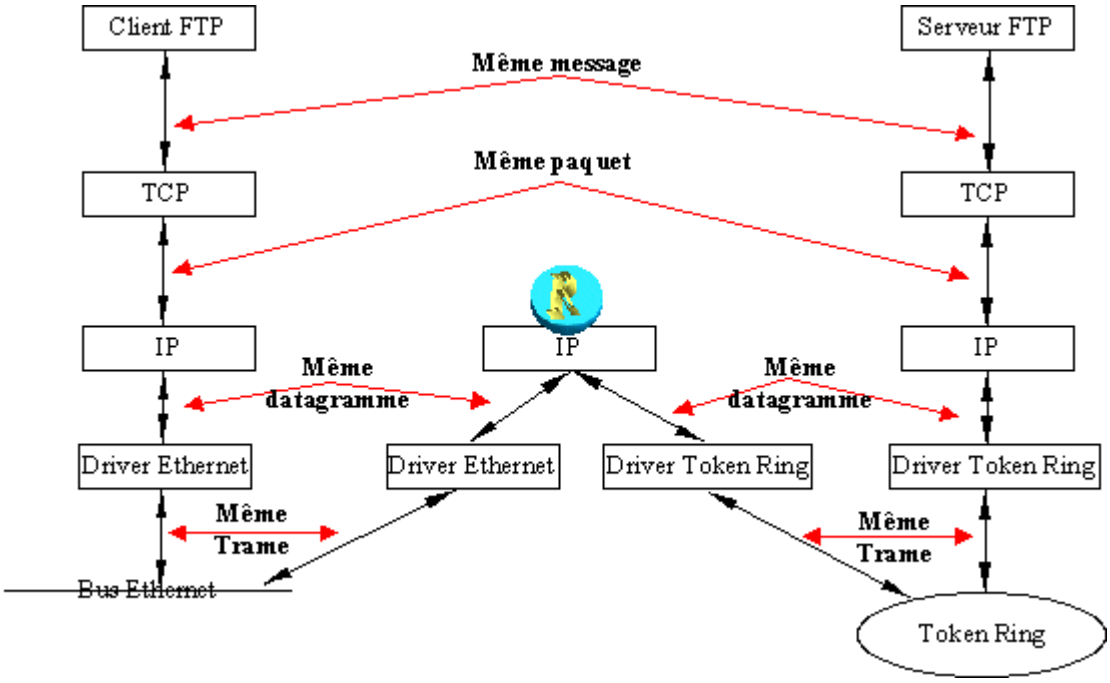
OSPF est un protocole de routage développé pour IP par l'IETF car RIP ne suffisait plus pour des interconnexions de réseaux hétérogènes. OSPF est ouvert et est basé sur l'algorithme SPF.

La taille de la base de données (table de routage), la durée des calculs des routes augmentent avec la taille du réseau. La réponse à ce problème est le routage hiérarchique. OSPF peut gérer un réseau organisé hiérarchiquement, et il est capable d'échanger des trames avec l'extérieur.

Le routage hiérarchique consiste à découper le réseau en un ensemble de parties indépendantes, connectées par une partie centrale.

Le réseau est donc divisé en zones ou aires (area). Les routeurs d'une zone ne calculent que les routes correspondant à leur zone, ainsi le coût du routage est ainsi proportionnel à la taille de la zone et non plus à la taille du réseau. Chaque zone est connectée à une aire centrale appelée backbone, pour faire la liaison entre les zones et le backbone, OSPF utilise des routeurs appelés « area border routers » ou « routeurs interzones » . Ces routeurs disposent de plusieurs interfaces, et appartiennent à la fois à une zone et au backbone. Ils possèdent une topologie séparée pour chaque aire. Il faut au moins un routeur interzone par aire. Les *liaisons externes* partent des points d'accès et décrivent les connexions vers l'extérieur. Les *liaisons récapitulatives* partent des routeurs interzones et décrivent les routes vers l'intérieur.

Schématique d'interconnexion de réseaux



CIDR

Ceci est un autre concept de routage, on parle de routage sans classe (Classeless InterDomain Rounting). En effet, normalement on peut associer à chaque réseau un masque de sous réseau afin de distinguer des entités plus petites. CIDR permet de faire l'inverse, on appelle cela des agrégats de réseaux, la notion de classe disparaît par la même occasion.

R*écapitulatif Ethernet*

	10Base-5 (802.3)	**10Base-2** (802.3)	**10Base-T** (802.3)	**100Base-T** (802.3u)	**100VG** (802.12)	**1000BaseT** (802.3z)fbr (802.3ab)cu
Bande Passante (théorique/estimméé)	*10 /7 Mbs*	*10 / 7 Mbs*	*10 / 7 Mbs*	*100 / 90 Mbs*	*100 / 96Mbs*	*1000 / ? Mbs*
Méthode d'accès	*CSMA/CD*	*CSMA/CD*	*CSMA/CD*	*CSMA/CD*	*Priorité*	*CSMA/CD*
Type de câbles: UTP STP Coax Fibre	 - - *épais* -	 - - *fin* -	*3,4,5* *1,2* - *10Base-fl*	*5(TX),3,4(T4)* *1,2* - *100Base-fl*	*3,4,5* - - *Supportée*	*6* - - *Supportée**
Paires utilisées	-	-	*2 (1,2) & 3 (3,6)*	*2,3,1(4,5), 4(7,8)*	*2,3,1,4*	*2, 3, 1, 4*
Segment - Nbr. de noeuds	*500m - 30*	*200m - 30*	*100m - 64*	*100m - 64*	*100m - ?*	*100m - ?*
Répéteur entre 2 noeuds (de classe 2)	*4 - ø500m*	*4 - ø200m*	*4 - ø500m*	*2 - ø200m*	*5*	*1 - ø205m*
Les câbles UTP ne doivent pas exéder 100m. Un seul hub de classe 1 ou 2 entre deux noeuds.			(*) Fibre: 9µ = 3km/1300nm 62,5µ = 300m/850nm 62,5µ = 550m/12300nm 50µ = 550m Cuivre: 250Mbs/paire/125Mhz			

Problème de routage	Solution

Interface down	**1)** Utiliser la commande **show interfaces privileged exec** pour vérifier l'état de l'interface :
	`Router#show interface serial 0`
	`Serial0 is administratively down, line protocol is down`
	`Hardware is HD64570`
	`Internet address is 10.1.1.5 255.255.255.252`
	`[...]`
	2) Si l'interface est "administratively down," l'activer par un **no shutdown** de l'interface en mode configuration.
	`Router(config)#int serial0`
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
	3) Utiliser la commande **show interfaces** commde ci dessus et vérifier qu'elle est UP.
	4) Si ce n'est pas le cas, c'est peut être un problème matériel ou de liaison.

Le réseau a routé est erroné ou indéfini	**1)** Utiliser la commande **show running-config privileged exec** pour voir la configuration active sur le routeur. **2)** S'assurer qu'il y a un réseau spécifié pour l'interface concernée. Exemple, si l'on assigne un nouvelle interface IP avec l'adresse 192.168.52.42 : `c4500(config)#`**`router rip`** `c4500(config-router)#`**`network 192.168.52.0`**

Pas d'interface active configurée avec une adresse IP (OSPF)	OSPF utilise une adresse IP sur le routeur comme ID. Seulement, pour configurer OSPF sur un routeur, vous avez besoins de la dernière interface active configurée avec une adresse IP. Si il n'y a pas d'interface active avec une adresse IP, le routeur, renvoie un erreur :
	`2509(config)#`**`router ospf 100`**
	
	`2509(config)#`
	`OSPF: Could not allocate router id`
	1) Utiliser la commande **show ip interfaces privileged exec** que l'interface est active avec un adresse IP.
	2) Si il n'y a pas d'interface active avec un adresse IP, en configurer une, si nécéssaire utiliser la commande no shutdown pour l'activer :
	`Router#conf t`
	`Enter configuration commands, one per line.`
	`End with CNTL/Z.`
	`Router(config)#interface serial 0`
	`Router(config-if)#ip address 10.1.1.5 255.255.255.252`
	`Router(config-if)#no shutdown`
	`Router(config-if)#`

Erreur de restriction ou de filtrage	**1)** Utiliser la commande **show running-config** afin de vérifier que les routeurs utilisent des access-list ou non.
	2) Si il y a des adresse en accès limité, les arrêter avec la commande appropriée. Par exemple pour stopper le filtrage du port 80 tcp ou udp :
	`C4000(config-if)#`**`no ip access-group 80 in`**
	
	3) Après cette étape refaire un test de communication, si les applications refonctionne, les access-list sont probablement inadaptés.
	5) Pour isoler le problème, créer des accès petits à petits.
	6) Si les access list interdisent le traffic spécifique aux ports TCP ou UDP , vérifier qu'il ne sont pas utilisées par des application.
	Entrer explicitement la commande **permit** pour les ports utilisés sur votre réseau. L'exemple qui suit autorise les service DNS et Telnet dans les 2 sens de communication à tous le monde:
	`access-list 101 permit udp 0.0.0.0 255.255.255.255`
	`0.0.0.0 255.255.255.255 eq 53`
	
	`access-list 101 permit tcp 0.0.0.0 255.255.255.255`
	`0.0.0.0 255.255.255.255 eq 23`

UDP broadcast	**1)** Utiliser la commande **show running-config privileged exec** afin de vérifier la configuration concernant la retransimssion des broadcast.
	Par exemple, si l'on entre **no ip forward-protocol udp 53** dans la configuration globale on desactive la retransmission du traffic UDP sortant sur le port 53 (DNS broadcasts).
	2) Par exemple, pour acticiver les DNS broadcasts :
	`C4500(config)#ip forward-protocol udp domain`
	
	Pour autoriser la retransmission des BOOTP broadcasts :
	`C4500(config)#ip forward-protocol udp bootp`
	
	Pour tous les UDP broadcasts :
	`C4500(config)#ip forward-protocol udp`

Access list ou les filtres erronés	**1)** Utiliser la commande **show running-config**. **2)** Si des access lists sont activés, les desactiver. Par exemples pour desactiver les acces définis pour le groupe 10 : `C4000(config-if)#no ip access-group 10 in`

Problèmes de connexion au réseau local	**Solution**
Câble défectueux ou inadapté	**1)** vérifier que la diode du port du commutateur où est connectée la station, est active **2)** Si la diode est inactive, s'assurer que le câble utilisé est le bon (qu'il n'est pas croisé, dans la bonne catégorie, bien en cliqué, ...) **3)** Vérifier que le câblage est correct (paire par paire). **4)** Utiliser un reflectomètre ou un testeur de câble pour vérifier que le signal est présent sur toutes les paires. **5)** Remplacer le câble par un autre du même modèle. Si la connexion se fait, c'était un câble défectueux.
Alimentation insuffisante	**1)** Vérifier les témoins du commutateur, si ils ne sont pas actif, vérifier le raccordement électrique. **2)** Vérifier les fusibles si l'alimentation parvient au commutateur, sans témoins actifs.
Matériel	**1)** Vérifier les témoins de contrôle du commutateur. **2)** Si le témoin du port concerné est inactif mais le câble intact, il se peut que ce soit un problème matériel. **3)** Vérifier le paramétrage du port qui pause problème (vitesse, type, ...). **4)** Si la diode est toujours inactive, essayer un redémarrage du module. **5)** Si cela ne marche toujours pas remplacer le module ou le commutateur.
Adresse IP manquante ou erronée	**1)** Vérifier que l'adresse IP est paramétrée pour le réseau local pour le commutateur est connecté. Pour cela vérifier par exemple que vous "pinguiez" le commutateur ou la routeur par défaut. **2)** Si l'adresse IP semble ne pas être la bonne, la modifier.
Masque de sous réseau erroné	**1)** Vérifier que l'on atteint bien les autres nœud du même sous réseau. **2)** Vérifier le masque de sous réseau utilisable sur le réseau local. **3)** Déterminer lequel des nœuds possède le bon masque de sous réseau, et reconfigurer l'autre.
Pas de routeur pas défaut sur le commutateur ou sur le serveur	**1)** Vérifier quel est le bon routeur par défaut sur le réseau local. **2)** Toutes les stations qui n'ont pas de routeur par défaut sur le réseau local, doivent avoir l'adresse IP de celui-ci.
Réseau virtuels mal configurés	**1)** Assurez vous que tous les nœuds qui doivent communiquer ensemble sont sur le même vlan du commutateur. **2)** Si un port doit communiquer avec plusieurs vlan, utiliser un port dédié ou le vlan correspondant pour assurer la stabilité du système.

Problèmes d'accès au port de management	Solution
Mauvais débit	**1)** Vérifier la configuration du mode terminale entre la station d'administration et le matériel. **2)** Tester la connexion en utilisant différents paramètres.
Câble incorrect	Un câble null-modem est nécessaire pour connecter un commutateur, routeur, directement entre un terminal et une station de configuration (vt, pc, ...)

Problèmes de performances en environnement commuté	Solution
Sélection du mode Full- or Half-Duplex	**1)** Vérifier les statistiques du port. **2)** Si il y a checksum error ou des erreurs d'alignements (trame non divisible par 8), vérifier que le port ne soit pas en mode full-duplex. **3)** Si le port du commutateur est en full-duplex, vérifier que le périphérique raccordé n'est pas un répéteur ou un périphérique half-duplex. Sinon basculer dans le mode approprié. **4)** Si des collisions tardives, vérifier que le port n'est pas en mode half-duplex. **5)** Si le port est en half-duplex, vérifier que l'autre périphérique n'est pas en full-duplex, sinon le reconfigurer.
Câble trop long	**1)** Vérifier les statistiques du commutateurs. Si l'on constate des erreurs de crc, des collisions tardives ou des erreurs d'alignement, il se peut que le câble soit trop long. **2)** Vérifier la longueur du câble à l'aide d'un réflectomètre ou d'un testeur de câble. Vérifier que les réseaux virtuels correspondent à la même norme. **3)** Sinon réduire la longueur du câble.

Mode de Commande

Exemple :
Ce qui suit est un exemple de ce qu'affiche la commande **show interfaces** pour l'interface Ethernet 0 :

```
Router# show interfaces ethernet 0

Ethernet 0 is up, line protocol is up
   Hardware is MCI Ethernet, address is aa00.0400.0134 (via 0000.0c00.4369)
      Internet address is 131.108.1.1, subnet mask is 255.255.255.0
      MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
             Encapsulation ARPA, loopback not set, keepalive set (10 sec)
             ARP type: ARPA, PROBE, ARP Timeout 4:00:00
             Last input 0:00:00, output 0:00:00, output hang never
             Output queue 0/40, 0 drops; input queue 0/75, 2 drops
             Five minute input rate 61000 bits/sec, 4 packets/sec
             Five minute output rate 1000 bits/sec, 2 packets/sec
          2295197 packets input, 305539992 bytes, 0 no buffer
          Received 1925500 broadcasts, 0 runts, 0 giants
          3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
           0 input packets with dribble condition detected
          3594664 packets output, 436549843 bytes, 0 underruns
          8 output errors, 1790 collisions, 10 interface resets, 0 restarts
```

Descriptions des champs affichés par "show interfaces":

Champ	Description
Ethernet...is up...is administratively down	Indique si l'interface matérielle est actuellement active et si elle a été coupée par un administrateur. "Disabled" indique que le routeur a reçu plus de 5000 erreurs sur une intervalle donnée (par défaut 10 secondes).
line protocol is {*up* | *down* | *administratively down*}	Indique si le logiciel qui gère le protocole de la liaison estime que l'interface est utilisable ou pas, ou si elle a été coupée par un administrateur.
Hardware	Type de matériel (par exemple, MCI Ethernet, SCI, cBus Ethernet) et adresse.
Internet address	Adresse IP suivie du masque de réseau.
MTU	Taille maxi de l'unité de transmission (Maximum transmission unit) de l' interface.
BW	Largeur de bande de l'interface en Kilobits par seconde. (Bandwidth)
DLY	Délai de l'interface en microsecondes. (Delay)
rely	Disponibilité de l'interface en fraction de 255 (255/255 : 100% de disponibilité), calculée d'après une moyenne sur 5 minutes. (Reliability)
load	Charge de l'interface en fraction de 255 (255/255 : complètement saturée), calculée d'après une moyenne sur 5 minutes.
Encapsulation	Méthode d'encapsulation attachée à l'interface.
ARP type:	Type d'ARP (Address Resolution Protocol) assigné à l'interface.
loopback	Indique si le rebouclage est activé ou non.
keepalive	Indique si les " keepalives " sont activés. (l'interface se désactive en cas d'erreurs trop nombreuses)
Last input	Nombre d'heures, minutes, secondes écoulées depuis le dernier paquet correctement reçu par l'interface. Utile pour connaître le moment où l'interface est tombée .
Last output	Nombre d'heures , minutes, secondes écoulées depuis le dernier paquet correctement transmis par l'interface.
output	Nombre d'heures , minutes, secondes écoulées depuis le dernier paquet correctement transmis par l'interface. Utile pour connaître le moment où l'interface est tombée.
output hang	Nombre d'heures, minutes et secondes depuis la dernière réinitialisation de l'interface due à une transmission ayant pris trop de temps. (si pas de réinitialisation : never)

Last clearing	Moment auquel les compteurs qui mesurent des statistiques cumulées (comme par exemple le nombre d'octets transmis et reçus) ont été remis à zero pour la dernière fois . Remarque : les variables telles que Load et Reliability (voir plus haut) qui affectent le routage ne sont pas effacées quand les compteurs sont remis à zero. *** indique que le temps écoulé est trop important pour être affiché.
Output queue, input queue, drops	Nombre de paquets dans les files d'attente (en entrée et en sortie). Chaque nombre est suivi par un / et par la taille maxi de la file d'attente ainsi que le nombre de paquets perdus à cause d'une file d'attente pleine.
Five minute input rate, Five minute output rate	Nombre moyen de bits et de paquets transmis par seconde sur les cinq dernières minutes. Si l'interface n'est pas en mode de proximité, ceci permet de recenser le trafic réseau qu'elle reçoit et qu'elle transmet, plutôt que le trafic réseau global. Les " five-minute input et output rates " doivent être utilisées seulement comme approximation du trafic par seconde sur une période donnée de cinq minutes.
packets input	Nombre total de paquets non–erronés reçus par le système.
bytes input	Nombre total d'octets, (données plus encapsulation MAC) compris dans les paquets non-erronés reçus par le système.
no buffers	Nombre de paquets reçus rejetés à cause du manque de place dans les buffers du système. (=ignored counts, voir plus bas dans le tableau). Les " tempêtes de broadcast " sur les réseaux ethernet et la présence soudaine de bruit sur les lignes série sont souvent la cause du manque de place dans les buffers.
Received...broadcasts	Nombre total de paquets broadcasts et multicasts reçus par l'interface.
runts	Nombre de paquets rejetés parce que plus petits que la taille minimum autorisée pour un paquet. Par exemple, tout paquet ethernet inférieur à 64 octets est considéré comme un " runt ".
giants	Nombre de paquets rejetés parce que trop grands. Par exemple, tout paquet ethernet supérieur à 1518 octets est considéré comme un " giant ".
input error	Somme des erreurs ayant perturbé la reception : inclut les runts, giants, no buffer, CRC, frame, overrun, et les ignored counts.
CRC	Le Cyclic redundancy checksum généré par la station émettrice ne correspond pas au CRC calculé avec la donnée reçue. Sur un LAN, ceci indique habituellement des problèmes de transmission ou du bruit. Un grand nombre de CRC est souvent le résultat de collisions ou d'une station qui transmettrait des données erronées.
frame	Nombre de paquets reçus avec une erreur de CRC et un nombre d'octets non intègre. Habituellement le résultat de collisions ou d'un matériel ethernet endommagé.
overrun	Nombre de fois où une donnée reçue n'a pas pu être traitée par le matériel destinataire car sa taille excédait celle des buffers.
ignored counts	Nombre de paquets reçus ignorés par l'interface à cause du manque de place dans les buffers internes. Les tempêtes de Broadcast et l'apparition de bruit peuvent causer une augmentation du nombre d'ignored counts.
input packets with dribble condition detected	Le bit " dribble " indique une trame légérement trop longue. Toutefois, le routeur acceptera la trame.
packets output	Nombre total de paquets transmis par le système.
bytes	Nombre total d'octets (data plus encapsulation MAC) transmia par le système.
underruns	Nombre de fois l'emetteur a été plus rapide que le routeur ne pouvait traiter les données.
output errors	Nombre total d'erreurs survenue avant la fin d'une transmission complète d'un datagramme. Cependant cette valeur peu ne pas être égale avec la somme de toutes les erreurs en sortie, du fait qu'un datagramme peu comprendre plus d'une erreur qui n'entrerait pas à un paramètre affichable.
collisions	Nombre de message transmis du fait d'une erreur ethernet (collision). Ce peu être du à un segment trop étendu (câble ou segment trop long, plus de deux répéteurs entre 2 stations, trop de concentrateurs en cascade,... .

interface resets	Nombre de fois ou une interface a été complètement redémarrée. Cela peut se produire lorsque la file d'attente en transmission n'a pu se vider dans les délai prévus. Une ligne série deffectueuse (problème de modem, de synchronisation,...) peut en être la cause. Si le système indique que le signal de porteuse est bon, mais que la ligne est coupée, génère ces reset.
restarts	Nombre de fois ou une interface Ethernet a été redémarrée en raison d'erreurs.

Lorsque vous cherchez à résoudre des problèmes liés au support ethernet dans un environnement routeur Cisco, la commande **show interfaces ethernet** vous donne des informations susceptibles de vous aider à isoler les problèmes. Voici une description détaillée de la commande **show interfaces ethernet** et des informations qu'elle donne :

show interfaces ethernet

Utilisez **show interfaces ethernet privileged exec** pour afficher les infos concernant les interfaces ethernet sur le routeur.

Syntaxe :

show interfaces ethernet unit [**accounting**]
show interfaces ethernet [*slot* | *port*] [**accounting**] (pour les Cisco série 7200 & Cisco 7500)
show interfaces ethernet [*type slot* | *port-adapter* | *port*]

Description de la syntaxe :

- **unit**--- A remplacer par un numéro de port sur l'interface sélectionnée.
- **accounting**---(Optionnel) Affiche le nombre de paquets envoyés via l'interface sélectionnée pour chaque protocole
- **slot**--- Voir le manuelde référence pour les informations complémentaires.
- **port**--- Voir le manuelde référence pour les informations complémentaires.
- **port-adapter**--- *Voir le manuelde référence pour les informations complémentaires*.

Problèmes liés au support physique	Solutions
Bruit excessif	**1)** Utilisez la commande **show interfaces ethernet** pour déterminer l'état des interfaces ethernet du routeur. La présence de nombreuses erreurs CRC mais de peu de collisions indique un bruit excessif. **2)** Vérifiez l'état des câbles. **3)** Vérifiez l'état des connecteurs. **4)** Si vous utilisez du 100BaseTX, assurez vous que vous utilisez du câble de catégorie 5 exclusivement.
Collisions excessives	**1)** Utilisez la commande **show interfaces ethernet** afin de vérifier le taux de collisions. Le nombre total de collisions par rapport au nombre total de paquets sortants doit être aux alentours d'1 pour 1000. **2)** Utilisez un testeur de câbles pour trouver les éventuels câbles ethernet non bouclés.
Trames erronées excessives	**1)** Dans un environnement ethernet partagé, les trames erronées (runts,…) sont presque toujours causées par des collisions. Donc vérifiez le taux de collisions, et si il est élevé référez-vous à la rubrique précédente du tableau. **2)** Si les trames erronées sont présentes alors que le taux de collisions est faible ou dans un environnement ethernet commuté, alors elles sont le fruit d' underruns ou d'un mauvais microcode constructeur sur une carte réseau ou d'une carte réseau défaillante. **3)** Utilisez un analyseur de protocoles pour tenter de déterminer l'adresse qui émet les trames erronées.

Collisions tardives	**1) Utilisez un analyseur de protocoles pour chercher la présence de collisions tardives. Celles-ci ne devraient jamais exister dans un réseau ethernet convenablement conçu. Elles apparaîssent habituellement quand les câbles sont trop longs ou quand il y a trop de répéteurs sur le réseau.** **2)** Vérifiez le diamètre du réseau et assurez vous qu'il reste dans les normes. Une collision tardive est une collision qui a lieu au delà des premiers 64 octets d'une trame ethernet.
Liens non intègres sur 10BaseT, 100BaseT4, ou 100BaseTX	**1)** Assurez-vous que vous n'utilisez pas de 100BaseT4 alors que seulement 2 paires sont disponibles. Le 100BaseT4 requiert quatre paires… **2)** Vérifiez la concordance entre la configuration des cartes réseau sur les hôtes et la configuration du concentrateur, par exemple. (mode de transmission : half ou full duplex ; vitesse de transmission) **3)** Vérifiez que l'hôte n'est pas connecté sur le port cascadé du concentrateur. **4)** Vérifiez la présence de bruit excessif (voir la rubrique " Bruit excessif ")

Configuration de base d'un liaison ISDN

Configuration of Remote Router	Configuration of Main Router
hostname branch1 ! username main password secret1 ! isdn switch-type basic-dms100 ! interface Ethernet 0 ip address 131.108.64.190 255.255.255.0 ! interface BRI 0 encapsulation PPP ip address 131.108.157.1 255.255.255.0 isdn spid1 415988488501 9884885 isdn spid2 415988488602 9884886 ppp authenticate chap dialer idle-timeout 300 dialer map IP 131.108.157.2 name main 4883 dialer-group 1 ! ip route 131.108.0.0 255.255.0.0 131.108.157.2 ip route 0.0.0.0 0.0.0.0 131.108.157.2 ! dialer-list 1 protocol ip permit	hostname main ! username branch1 password secret1 username branch2 password secret2 ! isdn switch-type basic-dms100 ! interface Ethernet 0 ip address 131.108.38.1 255.255.255.0 ! interface BRI 0 encapsulation PPP ip address 131.108.157.2 255.255.255.0 isdn spid1 415988488201 9884882 isdn spid2 415988488302 9884883 ppp authenticate chap dialer idle-timeout 300 dialer map IP 131.108.157.1 name branch1 4885 dialer-group 1 ! ip route 131.108.64.0 255.255.255.0 131.108.157.1 ! dialer-list 1 prot ip list 101 access-list 110 deny igrp any any access-list 110 permit ip any any

hostname *name*
Il s'agit du nom logique du routeur sur le réseau local, qui est utilisé pour son identification sur l'autre routeur lors de l'envoi du "challenge" d'authentification par chap.
username *name* **password** *secret*
Un nom d'utilisateur est requis avec un mot de passe qui sera utilisé par les routeur pour la négociation de la communication sécurisée. Les deux routeurs doivent utiliser le même nom d'utilisateur.
isdn switch-type *switch-type*
isdn spid1 *spid-number [ldn],* **isdn spid2** *spid-number [ldn]*
Ces commandes sont spécifiques au fournisseur télécom, et pas toujours utiles, ils faut vérifier lors de la création de ligne avec le constructeur.

dialer-group *group number*
dialer-list *dialer-group* **protocol** *protocol-name* {**permit | deny**}
dialer-list *dialer-group* **protocol** *protocol-name* **list** *access-list-number*
Ceci permet de définir le type de paquets qui traffiquent sur la ligne, ainsi que le délai de déconnexion.
ppp authentication chap
Specifie que l'on utilise CHAP pour la sécurisation des accès. Voir les commandes **dialer map** pour plus de détails.
dialer idle-timeout *seconds*
Cette commande défini le délai de deconnexion quand un traffic jugé non-usuel est présent (ou pas).
dialer map *protocol* **name** *remote-name broadcast* **speed 56** *phone-number*
Le dialer map est utilisé pour la différenciation de plusieurs sites distant. Une "map" est nécéssaire pour chaque siteet chaque protocol utilisé. Le nom est le nom du routeur distant. Le champ de broadcast specifie quand un packet de broadcast, tel qu'une mise à jour des tables de routage, sont envoyées pour ce protocol, pour ce site. Le champ vitesse est nécéssaire pour les connexions qui ne seraient pas de bout en bout sur un même média (ici numérique).
Le Dialer maps fournit la liaison afin que le router encapsule et envoie correctement le packets sortant d'une interface.
ip route *network [mask] {address | interface} [distance]*

On peut très facilement sauvegarder la configuration d'un routeur via un serveur *tftp.* Pour cela, il faut démarrer un serveur tftp sur une machine du reseau de ce routeur, on utilise la commande *« write net »,* après quoi vous n'avez plus qu'à répondre aux questions posées (nom du fichier de destination, adresse du serveur, ...) Au final le fichier se retrouve sur la machine ou attendait le serveur tftp. Pour la restauration c'est la commande *« copy tftp »* après quoi il faut choisir entre *running_config* (qui ajoute la configuration à l'existante) et *startup_config* pour créer une nouvelle configuration. Après quoi on redémarre le routeur et c'est tout.

Exemple de routeur Cisco

http://www.cisco.com/

Cisco 2500

Exemples d'outils d'administration et de supervision réseaux

Sniffer Ethernet :

EtheReal (GNU ethereal.zing.org) - Unix et Windows
Sniffit (GNU www.linuxapps.com) - Unix
TcpDump, Snoop - Unix en standard

Sniffer Pro (payant NetworkAssociates) - DOS / Windows
NetXRay (payant NetworkAssociates) - Windows

Analyseurs de performances :

MIBbrowser (www.adventnet.com) - Java
CiscoCPULoad (payant www.solarwind.com) - Windows
NetXRay
Transcend (payant www.3com.com) - Windows
PaketShaper (payant www.iperformance.com) - Matériel

Surveillance globale :
Cheops (www.linuxapps.com) - Unix GNU
Scotty Management - Unix GNU
HP OpenView - Payant Unix et Windows

- ... Liste non exhaustive ...-

Glossaire

AB

ARP : *Adress Resolution Protocol, partie du protocol de TCP/IP qui permet de "lier" une adresse IP ou adresse logique avec une adresse MAC ou adresse physique.*

AUI : *Attachement Unit Interface, connecteur universel 15 broches.*

Bandwidth: *Bande Passante mesurée en milliers de bits par seconde Kbps ou en millions de bits par seconde Mbps, mesure relative au débits de liaisons particulières (T1=1,544 Mbps, numéris 64kbps,...).*

BGP : *Border Gateway Protocol.*

BRI : *Basic Rate Interface. Interface numéris (ISDN=RNIS) composée de 2 cannaux à 64kbps et d'un canal à 16kbps.*

CDE

Classes d'adresses:

A

```
0 1 ...126        . 0-255     . 0-255     . 0-255
|----- RESEAU -----|---------- HÔTES ----------|
```

B

```
1 0 1 ...128-191              . 0-255     . 0-255
|---------- RESEAU ----------|----- HÔTES -----|
```

C

```
1 1 0 ... 192-223                         . 0-255
|--------------- RESEAU ---------------| HÔTES |
```

D

```
Réservée au Multicast ( 224 à 239 )
```

E

```
Réservée à un usage particulier. ( 240 à 255 )
```

CHAP : *Challenge Handshake Authentification Protocol, protocole destiné à securiser la connexion entre deux machines.*

CSMA/CD: Carrier Sense Multiple Acces / Collision Detection

CIDR : *Classless Inter-Domain Routing.*

Datagramme: Message concernant la couche 3 du modèle OSI

DHCP : *Dynamic Host Configuration Protocol. Permet d'obtenir de manière dynamique une adresse IP avec différends critères tels que l'authentification, la durée de bail, ...*

DNS : *Domain Name Server. Permet d'attribuer des noms logiques à des machines à la place d'une adresse IP.*

Ethernet : *Est un réseau local qui connecte un ensemble d'hôte (ordianteurs, imprimantes, ...) à l'aide de câble coaxial, ou de paire torsadée.*

EGP : *Exterior Gateway Protocol.*

FGH

FTP : File Transfert Protocol

IJK

ICMP : *Internet Control Messaging Protocol, utilisé par les composants actifs d'un réseau pour rapporter les éventuelles erreurs et contrôles, lors de communications IP*

IGMP : *Internet Group Management Protocol.*

IGP : *Interior Gateway protocol.*

IP : *Internet Protocol, fait partie de TCP/IP. C'est un protocole de routage adapté à la plupart des infrastructure réseau, en terme de taille, de complexité,... . L'adresse IP permet d'identifier un hôte de manière logique sur un réseau. Elle est codée sur 4bytes soit 32bit, divisée en 2 champs, qui identifie d'une part le Réseau, et l'hôte (unique pour un même réseau).*

IPX : *Internet Packet eXchange, protocole dédiée de Netware.*

ISDN : *Integrated Services Digital Network, permet d'envoyer des données et de la voix simultannément à partir d'un même média. Celui-ci utilise plusieurs canaux de communications, 2 baptisés B pour la data d'une taille de 64kbps, puis 1 autre, le D de 16kbps pour le contrôle et la synchronisation.*

LMN

LAN : *Local Area Network*
MAC : *Media Access Control, ensemble de règles permettant la communication entre différends noeuds d'un réseau.*
MAU : Media Attachement Unit.
MAN : *Metroplolitan Area Network*
MIB : *Management Information Base, sorte de répertoire utilisant un certains nombre de conversions en noms logiques des paramètres de configuration d'un équipement informatique.*
MISSALIGNED: Collision en cours d'émission, elle est non divisible par 8, et le crc est faux
NFS : *Network File System*

OPQ

OSI : *Open System Interconnection, références à un modèle standardisé utilisé pour la description définissant le nombre de "composants" d'un réseau ainsi et du rôle des couches fonctionnelles ainsi définies.*
OSPF : *Open Shortest Path First*
Out Of Band: *Canal de communication indépendant*
PAP : *Password Authentification Protocol, utilisé pour définir un nom d'utilisateur et un mot de passe afin de sécuriser un accès.*
Paquet : Message concernant la couche 4 du modèle OSI.
Port : *TCP/IP utilise une information logique définissant une sorte d'emplacement réservé au fonctionnement d'un applicatif ou d'un processus.Ex: 21-FTP, 23-Telnet, ...*
PPP : *Point to Point Protocol, protocole de communication encapsulant (définissant) des paquets de données afin de les envoyer vers un lien unique WAN, ou par des connexions appel du client vers un host (RTC).*

RST

RARP : *Reverse Address Resolution Protocol.*
RIP : *Rounting Informatin Protocol. Protocole d'echange de table de routage basé sur le coût de chaque destination, appelé "saut".*
RPC : *Remote Procedure Call.*
RTC : *Réseau téléphonique commuté.*
SLIP : *Serial Line Internet Protocol, permet d'envoyer des paquets IP par liaison série.*
SMTP : *Simple Message Transfert Protocol, est un protocol de communication dédié à l'échange de message électronique entre utilisateurs de réseaux interconnectés.*
SNMP : *Simple Network Management Protocol, est un protocol de communication dédié à la supervision de la plupart des équipements réseaux (intégré par le constructeur). Celui-ci permet de récupérer diverses informations et de les stocker dans une base de donnée dédiée appelée MIB. Ce protocol intervient par UDP.*
Socket : *Définit un ensemble adresse IP + numéro de port + processus pour une communication TCP/IP.*
Spanning Tree: *Partie importante du "transparent bridging" pour la detection de boucles.*
TACACS: *Terminal Access Concentrator Access Control Server, protocole tres simple d'authentification (uniquement PAP) par question/reponse.*
TCP : *Transmission Control Protocol :*
Protocoles de transports :
- Transmission Control Protocol
- User Datagram Protocol

Protocoles de routage : Contrôler l'adresse et le format d'un paquet pour déterminer le meilleur chemin entre l'émetteur et le récepteur:
- Internet Protocol
- Internet Control Message Protocol
- Rounting Information Protocol
- Open Shortest Path first

Protocoles de routeurs : Permet d'échanger les informations de routage
- Exterior Gataway Protocol
- Gateway to Gateway Protocol
- Interior Gateway Protocol

.../...

Protocoles et services de réseaux : Permet de d'identifier et d'utiliser les noeuds d'un réseau :
- Domain Name Server / System
- Address Resolution Protocol
- Reverse Address Resolution Protocol

Services Utilisateurs :
- BootP
- File Transfer Protocol
- Telnet
- Network File System
- Network Information service
- Remote Procedure Call
- Simple Mail Tranfer Protocol
- Simple Network Management Protocol

TFTP : *Trivial File Tranfer Protocol*
Trame : Message concernant la couche 1.
Transparent Bridging: *Permet de relier 2 réseau de même topologie.*
Translational Bridging: *Permet de relier 2 réseau de topologie différentes.*

UVWXYZ

UDP : *User Datagram Protocol, sous partie de TCP/IP.*
Communique en mode non connecté
WAN : *Wide Area Network*
WINS : *Windows Internet Name Service, produit par MicroSoft afin de permettre aux utilisateurs d'utiliser les noms logiques de machine locales dynamiquement, ce que ne permet pas DNS.*

AB

arp : Permet de modifier le cache su système
Liaison adresse physique et adresse logique

CDE

du / df : estime l'utilisation de l'espace disque des fichiers

FGH

ftp : Permet de tranferer des fichiers d'une machine vers une autre (via le protocole ftp)
commandes : binary / ascii : change le mode de transfert
cd : changer de répertoire sur la machine distante
lcd : change de répertoire sur la machine locale
get : rapatrie un fichier distant : src dst
put : envoie un fichier distant : src dst
ls : liste les entrées distante ...

IJKLMN

netstat : Affiche les connexions actives, tables de routage, statistique sur les interfaces
options : -i Si taux d'erreurs en entrée important : probléme de câbles ?
taux d'erreurs en sortie important : problème de contrôleur ?
rapport collision/paquets.sec supérieur à 1/1000 : Surcharge réseau.
-s Si retourne des erreurs de crc, vérifier le routeur.

nfsstat : affiche les statistiques sur les connexions NFS (Network File System)
les appels RPC = taux d'erreur < 5%

nbtstat : Affiche les statistiques du protocole et les connexions TCP/IP actuelles
utilisant NBT (NetBIOS sur TCP/IP)
options : -a Nom_Machine
-A @IP_machine
-c affiche le cache
-r Nom_machine par WINS

OPQ

ping : Permet de connaître les temps de réponses entre 2 noeuds d'un réseau (via ICMP)

ps : Status des process actifs

RST

rarp : Permet de modifier le cache su système - Liaison adresse logique et adresse physique

route : Permet de modifier la table de routage
ex: route ADD @equipement MASK @subnet @Routeur -p : ajoute une entrée permanente.

telnet : Permet de se connecter pour utiliser une machine distante (via le protocole telnet)

tftp : Permer de tranférer des fichiers, en envoi et en reception, via TFTP (udp)

tracert : Permet d'afficher les liens empruntés par des paquets ICMP

UVWXYZ

Vmstat : Statistiques sur la mémoire virtuelle d'un système

Câblage

```
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
                   Cable RJ45
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
                                                       (>
+--------------+
|+--------+    |   +----------------------+
||=8      |    |   |           --------[1]-|--- blanc/orange --
||=7      +--+ |   +--------+  --------[2]-|--- orange --------
||=6         | |   |         \ --------[3]-|--- blanc/vert ----
||=5         | |   |          +-----+--[4]-|--- bleu ----------
||=4         | |   |          +-----+--[5]-|--- blanc/bleu ----
||=3         | |   |         / --------[6]-|--- vert ----------
||=2      +--+ |   +--------+  --------[7]-|--- blanc/marron --
||=1      |    |   |           --------[8]-|--- marron --------
|+--------+    |   +----------------------+
+--------------+

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
                   Norme 258A
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Cables     Paires              DB25        DB9   Signal
------     ------              ----        ---   ------

(1)-------+                     5           8      Ready To Send
          |[2]
(2)-------+                     8           1      Carrier Detect

(3)---------------+             3           2      Data Received
                  |
(4)-------+       |             7           5      Ground Signal
          |[1]    |[3]
(5)-------+       |             7           5      Ground Signal
                  |
(6)---------------+             2           3      Data Send

(7)-------+                     20          4      Ready Data Terminal
          |[4]
(8)-------+                     4           7      Send Request
```

Types de câble :

- Catégorie 1 : Téléphonie et transfert de donnée a basse vitesse
- Catégorie 2 : ISDN, T1, E1
- Catégorie 3 : Transfert de donnée jusqu'à 16Mhz (inclue le 10BT et 100BT4)
- Catégorie 4 : Transfert de donnée jusqu'à 20Mhz (TokenRing 16Mbs - 100BT4)
- Catégorie 5 : Transfert de donnée jusqu'à 100Mhz
- Catégorie 6 : Transfert de donnée jusqu'à 250Mhz
- Catégorie 7 : Transfert de donnée jusqu'à 600Mhz ???