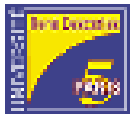
Université René Descartes – Paris 5
UFR de mathématiques et Informatique



LICENCE MIA
Année L3

Année scolaire 2005-2006

Support de cours

RESEAUX et TELECOMMUNICATIONS

Dominique SERET
Ahmed MEHAOUA
Neilze DORTA

Réseaux et Télécommunications

Auteur(s) : Dominique SERET

Dernière modification : 09/10/2005
Pré-requis : notion de bases en architecture et système d'exploitation
Description du module
- Volume horaire : 30 heures
- Objectif général : comprendre rapidement l'environnement réseau de l'entreprise
- Objectifs d'apprentissage
§ savoir identifier les natures et modes de transmissions
§ savoir situer les différents équipements de l'architecture d'un réseau
§ savoir reconnaître les protocoles de communication utilisés et les services rendus
§ comprendre les services réseau implémentés et les utiliser
§ comprendre les éléments de configuration d'un réseau
§ appréhender la sécurité dans les environnements réseaux

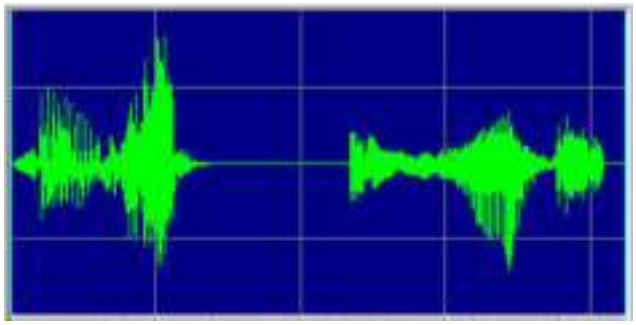
- Résumé : ce cours présente de manière très progressive les éléments de réseau et leurs architectures. Il décrit les principes de base et s'attache à présenter les solutions les plus fréquentes d'Ethernet à Internet.
- Mots clés : protocoles, TCP/IP, applications, Ethernet, interconnexion.

Sommaire

Toute entreprise possède aujourd'hui un ou plusieurs systèmes de télécommunication qui véhiculent les différentes informations nécessaires à sa vie et à son développement. Ces systèmes sont organisés en réseaux, qu'on peut définir comme des ensembles d'équipements et de supports de transmission dont une des fonctions est de permettre le transfert d'informations. Nous sommes entrés dans l'ère de la communication où le volume et la diversité de ces informations se font de plus en plus grands.
Dans les années 80, cette diversité conduisait à l'adoption de solutions de communication distinctes et différentes suivant la nature des informations à transmettre : réseau téléphonique pour la transmission de la voix, réseau spécialisé dans la transmission de données sur longue distance comme Transpac en France ou sur courte distance comme les réseaux locaux d'entreprise, réseau hertzien ou câblé pour la télévision.
Aujourd'hui les progrès de l'informatique rendent possible le traitement d'informations de natures différentes sur le même ordinateur : séquences vidéos et sonores, présentation de documents. C'est le domaine du *multimédia*.
De plus, les progrès des techniques de transmission permettent de transférer sur un même support (une fibre optique par exemple) ces informations variées. Les frontières entre les différents réseaux tendent à s'estomper. Par exemple, le réseau mondial Internet, initialement destiné exclusivement à la transmission de données, transmet des communications téléphoniques sur. Les solutions à un besoin de communication sont multiples et les progrès techniques rendent foisonnant le domaine des réseaux.

Nature des informations transmises

Nous parlerons d'applications téléphoniques, informatiques et téléinformatiques quelconques dans la mesure où la nature des informations peut être très variée :
– parole humaine et son haute fidélité,
– données alphanumériques, textes et autres données structurées en un ensemble de caractères,
– images fixes en noir et blanc ou en couleur,
– images animées, images de télévision par exemple,
– informations *multimédia* qui intègrent plusieurs types d'informations, telles que textes, sons, images fixes ou animées.
Par *nature* même, certaines informations sont *analogiques*, c'est-à-dire qu'elles correspondent à des signaux qui varient continûment dans le temps et qui peuvent prendre une infinité de valeurs distinctes. La parole, la musique, les images animées de la télévision sont des informations de nature analogique.
D'autres informations sont par nature *numériques*. D'une façon générale, on considère qu'elles correspondent à des signaux qui varient de manière discrète dans le temps et qui prennent un ensemble fini de valeurs distinctes. Par exemple, un texte est une suite de caractères appartenant à un alphabet d'un nombre fini de symboles : c'est une information de nature numérique.



ci-dessus une information analogique : quatre syllabes de parole

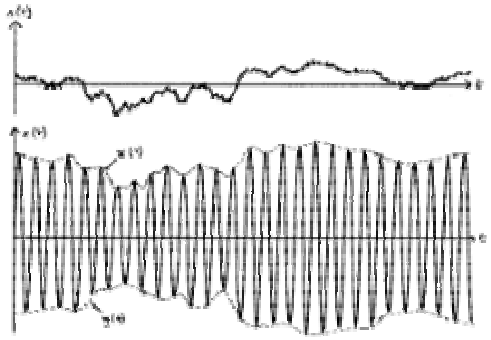
ci-dessous une information numérique : une suite de 0 et de 1

```
01111010100010111010000011010101000101010
```

Les informations numériques sont facilement transformées en une suite de données binaires grâce à une opération de *codage* qui fait correspondre à chaque symbole de l'alphabet une configuration binaire particulière. Plusieurs codes existent pour l'ensemble des caractères courants (les vingt-six lettres de l'alphabet, les chiffres, les symboles de ponctuation, les symboles mathématiques,…), on en imagine également pour des symboles graphiques afin de créer des images fixes.

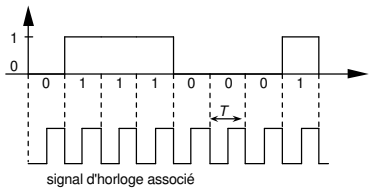
Nature des transmissions

La transmission des informations sur un support peut être analogique ou numérique selon que le signal transporté varie de manière continue ou discrète dans le temps, et que son espace de valeurs est infini ou non.
Un signal de parole module de manière analogique l'amplitude ou la fréquence d'une onde porteuse avec des variations dans le temps qui sont continues. On parle de *transmission analogique.*



en haut un signal analogique, en bas une onde porteuse dont l'amplitude est celle du signal du haut

Une suite de données binaires permet de construire un signal qui prend, par exemple, deux valeurs 0 et 1 et qui varie dans le temps à des intervalles de temps réguliers kT où k est un entier. On parle de *transmission numérique.*
Mais la correspondance entre nature de l'information et nature de la transmission ne se réduit pas à une telle bijection. On sait transformer une information analogique pour la mettre sous forme numérique et ensuite la transmettre. Cette opération s'applique aussi bien à un signal de parole qu'à une image fixe, une bande son haute fidélité ou des images de télévision animées et en couleur.
Aujourd'hui la quasi-totalité des transmissions sont numériques. Seul l'accès au réseau téléphonique, c'est-à-dire la liaison entre le poste téléphonique et le réseau, est encore majoritairement analogique.



ci-dessus un signal numérique transportant la suite 01110001 et le signal d'horloge (rythme) associé

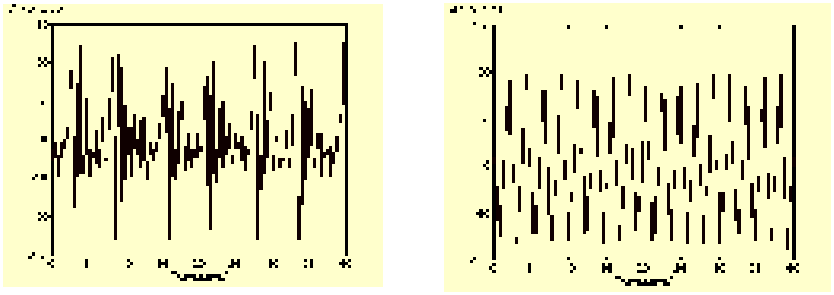
Exemple d'informations à transmettre : données alphanumériques

La transmission de données alphanumériques répond à de multiples besoins. Dans le cadre du courrier électronique, on cherche à transmettre le plus souvent de courts textes constitués de caractères. La méthode la plus simple pour le codage associe à chaque caractère un mot de 7 ou 8 bits comme avec le code ASCII. Si un caractère est codé par un octet, un courrier électronique de 40 lignes de 40 caractères tient en 1600 octets, soit 12,8 kbit. Une page de textes d'un livre imprimé fait typiquement 2400 octets. Un chapitre de livre d'une trentaine de pages est codé en environ 600 kbit sans considérer la mise en forme. Le roman *Les misérables* comprend de l'ordre de 3 millions de caractères, soit 24 Mbit.

On voit donc que la taille de l'information peut considérablement varier. Dans certains cas, il est intéressant d'utiliser des techniques de compression pour réduire la taille des données à transmettre. Dans d'autres cas, on désire privilégier la simplicité en adoptant un codage très simple comme le code ASCII sans compression.

Exemple d'informations à transmettre : la voix et sa numérisation

Le flux d'air en provenance des poumons est modulé par les cordes vocales, créant des ondes de pression qui se propagent à travers le conduit vocal. Ce dernier, constitué des cavités orales et nasales, se comporte comme un " filtre " caractérisé par des fréquences de résonance.
Les sons de parole sont classés en 3 catégories :
les sons voisés : les cordes vocales vibrent de façon quasi-périodique. Le signal de parole est alors quasi-périodique et est caractérisé par sa fréquence fondamentale. Typiquement, la période fondamentale des différents sons voisés varie entre 2 et 20 ms.

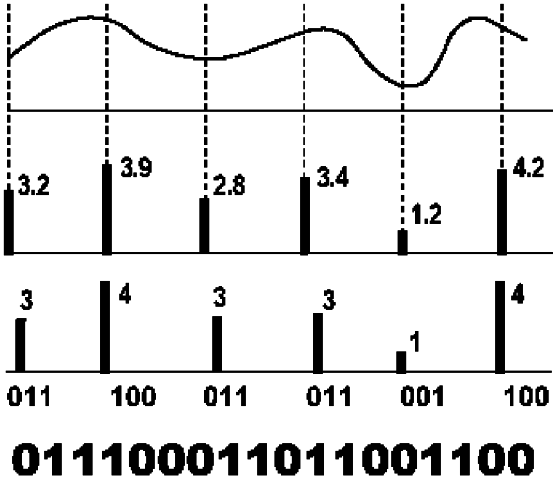


'a' *'ou'*

Sons voisés

les sons non voisés : les cordes vocales ne vibrent pas. L'air passe à haute vitesse entre les cordes vocales. Le signal produit est équivalent à un bruit blanc.
les plosives : ces sons sont obtenus lorsqu'on libère soudainement l'air comprimé par fermeture totale du conduit vocal.
La première étape de numérisation consiste à échantillonner, c'est-à-dire prendre en compte seulement l'amplitude du signal à des intervalles de temps régulier T. La fréquence d'échantillonnage est donc de $f=1/T$. Pour être capable de reconstituer le signal d'origine, le théorème de l'échantillonnage fourni par la théorie du signal dit que la fréquence d'échantillonnage doit être supérieure ou égale à $2f_{max}$, soit dans notre exemple 2*4000 = 8000 Hz. La période d'échantillonnage est donc de 1/8 ms soit 125 µs. Il faut ensuite quantifier le signal échantillonné, c'est-à-dire lui associer une valeur parmi un ensemble fini de valeurs. La quantification peut se faire sur 256 niveaux ; le codage du niveau, troisième étape, est finalement effectué sur 1 octet. La numérisation d'un signal vocal produit donc un flux régulier d'informations numériques de 1 octet toutes les 1/8 ms, soit un débit de 64 kbit/s. Cette technique, appelée MIC (Modulation par Impulsion et Codage), est utilisée dans le réseau téléphonique.
En résumé, la numérisation consiste en trois **étapes** fondamentales :
L'**échantillonnage** : le signal analogique est un signal continu qui par définition contient un nombre infini d'éléments. L'échantillonnage consiste à prélever un nombre déterminé d'éléments (échantillons) qui seront suffisants pour reconstituer à l'arrivée un signal analogique de qualité. Les différentes études ont montré qu'il suffit d'échantillonner à deux fois la fréquence supérieure contenue dans le signal. Ainsi, pour un signal de la parole où l'information est contenue dans une bande de 4000 Hz (0-4000), un échantillonnage à **8000 Hz** suffit (c'est-à-dire **toutes les 125 µs**). Pour la musique haute fidélité où l'information est contenue dans la bande audible (20-2000 Hz), l'échantillonnage a été défini à 44,1 kHz. Echantillonner à une fréquence plus faible conduit à un signal restitué de mauvaise qualité, et un

échantillonnage plus élevé augmente le volume de données à transmettre sans augmentation significative de la qualité.
La **quantification** : elle attribue à chaque échantillon une valeur prise dans une échelle finie de valeurs. L'erreur effectuée dans l'approximation est appelée bruit de quantification. Ce bruit ayant une répercussion importante pour les faibles niveaux, l'échelle n'est pas une échelle linéaire. Pour le signal de parole dans le réseau téléphonique, **256 niveaux** ont été retenus.
Le **codage** : chaque échantillon sera codé sur un ensemble de bits. Pour permettre le codage des différentes valeurs, **8 bits** sont nécessaires si l'on a retenu 256 niveaux.



un exemple simple (sur 3 bits donc 8 niveaux)

Une étude approfondie des caractéristiques de la parole montre qu'il est possible de la numériser à beaucoup plus faible débit. Dans les réseaux de téléphonie mobile GSM, la voix est ainsi transmise sur 13 kbit/s. Des codeurs récents atteignent 8 kbit/s avec une bonne qualité de restitution, voire 2400 bit/s pour des applications militaires où les contraintes de qualité sont moindres.
De plus, au cours d'une conversation, un interlocuteur parle statistiquement la moitié du temps. Les pauses au sein des phrases, le détachement des syllabes (voir schéma de l'échantillon de parole) montrent que le signal vocal est fréquemment réduit à un silence. La voix n'est donc plus numérisée comme un flux continu d'informations mais comme un flux *sporadique* : des périodes d'activités durant en moyenne 1,4 s suivies de silence de 1,75 s en moyenne. Avec un codage à 8 kbit/s, le flux obtenu a ainsi un débit moyen d'environ 4 kbit/s.

Exemple d'informations à transmettre : images fixes

Une image est une information de type analogique facilement numérisable par découpage en *pixel*s, (contraction de " picture element ") puis association d'un niveau de gris ou d'une couleur à chaque pixel. La taille d'un pixel est de 21x21 μm^2 pour rendre la numérisation non détectable (résolution utilisée par les journaux). Une photographie de 15x10 cm^2 contient donc 7000x4700 pixels environ.
La représentation la plus simple, appelé bit-map, associe à chaque pixel un niveau de gris ou une couleur. En supposant la couleur codée sur 8 bits, notre photographie tient sur 260 Mbit environ ! Si une qualité moyenne est acceptée (taille du pixel plus importante), le codage est réduit à 1 Mbit.

Trois images avec des pixels de tailles différentes !

Un écran d'ordinateur 800x600 contient 480000 pixels ; si chaque pixel est codé sur 24 bits (8 bits pour chaque couleur rouge, vert et bleu), une image sur tout l'écran est numérisée en 11,5 Mbit. On imagine alors l'importance de la capacité d'une carte graphique dans des applications vidéo, voire des jeux.
Nous voyons que la taille des données peut être considérable, mais, de même que pour la voix, des techniques de compression sont possibles. En général, la couleur d'un pixel est corrélée avec la couleur du pixel voisin. De façon très simplifiée, il est plus économique de coder la différence de couleur entre un pixel et son voisin plutôt que la couleur de celui-ci. La norme JPEG (*Joint Photographic Experts Group)* représente des images fixes de qualité photographique en réduisant la taille de l'image d'un facteur 20 par rapport à une représentation bit-map.

Exemple d'informations à transmettre : images animées

Les séquences animées sont obtenues par une succession d'images fixes à un rythme typique de 25 images par seconde. Celui-ci est suffisamment rapide pour donner à l'œil une impression de variation continue (ce rythme fournit un mouvement sans saccades, par opposition aux premiers films tournés à 12 images/s, à la création du cinéma). En prenant une image non compressée à 11,5 Mbit, la séquence animée produit alors 25x11,5=288 Mbit/s. Le débit nécessaire est considérable.
En utilisant les techniques de compression de type JPEG combinés avec l'exploitation des corrélations temporelles, la norme MPEG-1 (*Motion Picture Experts Group*) réduit le débit produit à 1,2 Mbit/s. Si les images varient rapidement, le flux d'information est plus important ; si les images sont quasiment fixes, le flux est moins important.

Définition de la qualité de service

Le transfert d'une information élémentaire entre deux équipements fait intervenir de multiples autres équipements et provoquer la transmission de signaux de nature variée sur des supports également variés. La grande réussite des télécommunications est celle de la transparence : l'utilisateur final ne connaît pas la nature des supports de transmission utilisés, il n'est concerné que par la *qualité du service* qui lui est offert et exprime des exigences dans ce domaine. La qualité de service est souvent appelée QOS, *Quality of Service*.
Quelques éléments de qualité de service peuvent être donnés :
– la *disponibilité* des moyens de transfert de l'information qui est liée au taux de panne des équipements et des liaisons,
– le *taux d'erreur maximal*, exprimé comme le rapport entre le nombre de bits dont la valeur est modifiée par rapport au nombre total de bits d'information émis,
– le *débit* de transfert,
– le *délai*, c'est-à-dire la durée entre la décision d'émettre l'information et la réception par le destinataire.
La qualité de service n'est pas une notion absolue. Elle est généralement liée à la nature des informations transmises et du type de besoin. Nous illustrons cette variété de la notion de qualité de service à l'aide de divers exemples.

Données alphanumériques, textes et images fixes

Un courrier électronique est une information en général courte. Il n'y a pas de contraintes de débit importantes. De plus on tolère que le courrier mette plusieurs minutes à être transmis. En revanche, l'usager exige que son message ne soit pas perdu par suite de la défaillance d'un équipement.

Imaginons que Victor Hugo écrive de nos jours *Les misérables* sur son ordinateur personnel et le transmette sous forme d'un fichier texte à son éditeur. Le fichier a une taille de 24 Mbit, sans aucune compression. Supposons qu'il utilise un moyen de télécommunication dont le taux d'erreur binaire (i.e. la probabilité qu'un bit soit mal transmis) soit 10^{-6}. Si au cours de la transmission, un seul élément binaire est mal reçu, le texte est modifié. La probabilité que l'ensemble du livre soit bien transmis en une seule fois est de $(1-10^{-6})^{24000000} = 4.10^{-11}$. Il est pratiquement certain qu'il y a une ou plusieurs erreurs dans le texte reçu par l'éditeur, si aucune vérification n'est faite. Si V. Hugo transfère le fichier pendant la nuit, un débit modéré peut convenir : à 9600 bit/s, le transfert dure une quarantaine de minutes. Le moyen de télécommunication rajoute un délai de plusieurs dizaines de minutes sans impact important pour l'éditeur. Cet exemple illustre que le taux d'erreur est généralement le facteur principal de qualité de service pour la transmission de fichiers et que le délai n'a pas d'importance (l'importance du débit dépend étroitement de l'utilisation).

Les journaux sont maintenant composés directement par ordinateur. Ils comportent du texte et des images fixes mais, dans certaines parutions, textes comme photographies sont considérés comme des images et transmis tels quels (en bit-map). Un quotidien tient ainsi sur 220 Mo soit 1,8 Gbit. Comme dans l'exemple précédent, il y a une nécessité que l'information soit correctement transmise de l'atelier de composition à l'imprimeur. Notons cependant que la solution bit-map permet de supporter des erreurs de transmission isolées : un pixel erroné parmi des pixels corrects est non détectable. Un taux d'erreur de 10^{-6} est acceptable. L'exigence principale s'exprime avec la disponibilité : l'impression ne doit pas être retardée à cause de l'indisponibilité du réseau informatique. La qualité de service prend en compte ce facteur. Le transfert doit de plus être rapide, il faut donc un débit assez élevé : avec un liaison à 2 Mbit/s, le transfert du journal demande environ 15 minutes.

Lorsqu'on consulte un serveur Web, on est dans le cas d'une application interactive : on transmet quelques informations pour demander d'afficher une page d'écran que le serveur transfère ensuite. La qualité de service dépend de plusieurs paramètres : disponibilité, délai, rapidité de transmission de la page. Notons que les flux générés sont largement dissymétriques : une commande transmise vers le serveur peut être codée sur quelques dizaines d'octets ; en revanche, le chargement de la page peut demander la transmission de plusieurs centaines de kilo-octets s'il y a des images (à 64 kbit/s, le chargement est de 13 secondes pour 100 kilo-octets). Les flux sont de plus très sporadiques : on demande le chargement d'une page, puis on la regarde pendant quelques minutes au bout desquelles on consulte une nouvelle page. Le débit moyen exigé peut être faible (environ 500 bit/s si l'usager charge 1 page de 100 kilo-octets toutes les 2 minutes) mais le débit instantané doit être relativement important si on ne veut pas impatienter l'usager !

La voix

La voix est un flux produit par le locuteur, puis numérisé. Le débit produit peut être faible si les techniques de compression sont utilisées. Il est essentiel que le flux soit régénéré à l'arrivée avec le même rythme, sans quoi la conversation est inaudible. Cependant, on tolère un taux d'erreur assez important en conservant une bonne compréhension : l'auditeur entend, par exemple, des claquements ou un son métallique qui peuvent être désagréables mais n'empêche pas la communication.

Dans le cas d'une communication téléphonique, le délai doit être le plus réduit possible ; dans le cas, par exemple, d'une diffusion d'émission radiophonique, il a une valeur plus élevée mais doit être constant.

Un autre élément de la qualité de service pour les communications téléphoniques est la disponibilité des moyens de transmission. Un usager est empêché de téléphoner à cause de la panne d'un équipement mais aussi par manque de ressource dans le réseau. Pour faire un appel depuis un portable, il faut disposer d'un canal radio (une fréquence radio). Si au moment, où on tente de faire l'appel, aucun canal n'est disponible, l'appel échoue. La probabilité d'échec d'un appel intervient ici fortement dans la qualité de service.

Les images animées

De la même façon que pour la voix, la transmission d'images animées exige que le flux d'origine soit restitué au même rythme. Il y a donc des contraintes de délais. En revanche, le débit requis est beaucoup plus important.

En conclusion, définir la qualité de service nécessite une analyse précise du type d'utilisation recherchée et de la nature des informations à transmettre. La qualité de service dépend généralement de la disponibilité, du débit, du délai, du taux d'erreur mais l'importance respective de chaque aspect peut grandement varier suivant les applications.

Historique : les systèmes centralisés

Les circuits logiques et la mémoire qui supportaient l'intelligence des ordinateurs centraux ont longtemps été des éléments coûteux par rapport aux lignes de transmission et aux terminaux. On cherchait donc à les rentabiliser au mieux en les mettant en commun au service d'un nombre maximal d'utilisateurs dans des systèmes centralisés. La distribution des fonctions au sein d'un tel système était simple : le maximum dans le *système central.*

Dans les premiers systèmes téléinformatiques, les terminaux ne contenaient que des fonctions de gestion des transmissions et d'interface avec les utilisateurs. Le logiciel du système central assurait le contrôle du partage des ressources (mémoire, fichiers…) entre les différentes applications. L'accès à distance impliquait des outils de contrôle d'accès et de partage de mémoire ou de données.

D'autre part, le système central devait faire face à des défaillances éventuelles et donc contenir des mécanismes de reconfiguration. Il assurait également la gestion des terminaux qui lui étaient connectés et offrait des fonctions de protection des données. Les communications étaient gérées par des procédures de communication.

Le nombre de terminaux augmentant, la connexion directe de terminaux à l'ordinateur central devint problématique :

– le matériel nécessaire à la connexion d'un terminal à l'ordinateur représentait un coût non négligeable et la gestion des terminaux mobilise la puissance de l'ordinateur pour des tâches auxquelles il n'est pas toujours adapté ;

– les lignes de transmission elles-mêmes commençaient à représenter un coût important alors qu'elles avaient un faible taux d'utilisation (un terminal d'interrogation de bases de données est inactif entre 30 et 70% du temps où il est en communication).

On vit donc apparaître tout d'abord des *liaisons multipoints* où plusieurs terminaux partagent un même support, mais qui gardent l'ensemble des traitements au niveau du système central, puis des *multiplexeurs* et des *concentrateurs* et enfin des ordinateurs *frontaux.*

Les multiplexeurs ou les concentrateurs assurent à un moindre coût les fonctions de communication et de transport en " concentrant " le trafic de plusieurs terminaux (dits *basse vitesse*) sur un même support de transmission (dit *haute vitesse*). Le multiplexeur est souvent un équipement câblé qui conserve le trafic de chaque terminal tel quel (avec les silences, par exemple). Le concentrateur est un équipement plus " intelligent " qui assure plusieurs fonctions de contrôle de transmission sur la liaison haute vitesse (stockage, traitement des informations, compression, protection contre les erreurs …).

Les frontaux sont des mini-ordinateurs assurant les fonctions de contrôle des communications pour le compte de l'ordinateur central, déchargeant ainsi celui-ci. Le frontal est relié au système central par une liaison particulière, très rapide. Il assure des fonctions de stockage momentané des messages, il gère automatiquement les ordres d'échange d'informations vers les différents terminaux et les incidents liés aux transmissions.

Historique : les réseaux de transmission

L'introduction d'un *réseau* de données maillé permet de constituer des réseaux généraux dans lesquels :

– un terminal accède à différents ordinateurs pour bénéficier d'une variété de services ;

– il existe de multiples communications simultanées, les ressources du réseau étant partagées entre elles ;

– les communications entre ordinateurs autorisent des applications informatiques distribuées.

Cette étape coïncide avec l'apparition de terminaux intelligents capables d'assurer eux aussi des fonctions de traitement local des données et de mettre en œuvre des procédures de communication complexes. Dans un réseau maillé, on distingue donc :

– le sous-réseau de communication mettant en correspondance tout un ensemble d'usagers (munis d'équipements informatiques très variés) et partageant ainsi les ressources de communication entre ces usagers ;
– les usagers eux-mêmes, " abonnés " à un service de communication donné ou clients passagers et dûment identifiés.
Le sous-réseau de communication est formé d'un ensemble de lignes de transmission et de *nœuds de commutation.* Ceux-ci sont des mini-ordinateurs spécialisés : ils assurent des fonctions de surveillance du réseau, de collecte de statistiques, de choix des chemins… Ils sont donc généralement constitués d'un processeur spécialisé dans les fonctions de commutation et de gestion des transmissions et d'un processeur général chargé des autres fonctions (taxation par exemple).
Dans les années 70 et 80, on identifiait trois types de réseaux au sein d'une entreprise : le réseau informatique, le réseau bureautique et le réseau téléphonique.
Le *réseau informatique* reliait plusieurs terminaux ou mini-ordinateurs à une machine centrale sur laquelle s'exécutaient généralement tous les programmes (informatique de gestion de l'entreprise : paie, factures, bons de commande, gestion de stocks …). Cette structure centralisée était calquée sur l'organisation de l'entreprise elle-même et faisait apparaître des matériels souvent homogènes, provenant d'un même constructeur.
Le *réseau bureautique* était constitué de micro-ordinateurs semblables reliés en réseau local pour partager des ressources comme les imprimantes. Les informations circulant sur ce réseau local étaient le plus souvent saisies et traitées indépendamment de celles traitées par le réseau informatique, les deux réseaux étant séparés.
Le *réseau téléphonique* était une troisième infrastructure, souvent administrée par une autre direction que celle de l'informatique, utilisant des moyens techniques autonomes.
Devant la très grande variété de produits offerts par les constructeurs, chacun proposant des solutions de communication adaptées à sa propre gamme de machines et généralement incompatibles avec celles des autres, un besoin très fort de normalisation s'est fait sentir. En 1976 est né un *modèle conceptuel pour l'interconnexion des systèmes ouverts* structuré en sept couches pour construire une architecture de réseaux entre des machines hétérogènes. Ce modèle, normalisé au plan international par l'ISO (organisation internationale de normalisation), est appelé aussi modèle de référence ou modèle OSI (*Open Systems Interconnection*). Il s'applique principalement aux réseaux informatiques et bureautiques.
L'informatique a évolué dans le même temps vers une diversification des machines (concentrateurs, frontaux, ordinateurs, super-ordinateurs) avec, pour chacune d'entre elles, des logiciels puissants et aux nombreuses fonctionnalités. Remarquons enfin que l'entreprise s'est trouvée souvent malgré elle face à une informatique hétérogène du simple fait des fusions, rachats, réorganisations de sociétés. Le modèle de référence est alors une solution théorique au problème de l'hétérogénéité des installations réseaux et informatiques.

Historique : le numérique et les réseaux multimédia

De nombreux progrès techniques et technologiques ont fait évoluer les réseaux depuis le début des années 80 : l'apparition d'infrastructures de télécommunication numériques avec de hauts débits et le codage d'une information sous des formes de plus en plus réduites. La parole au début des années 80 était systématiquement codée sur 64 kbit/s et les débits possibles sur des liaisons longues distances étaient de l'ordre de 2 Mbit/s. La parole peut être codée à 8 kbit/s sans perte de qualité et une fibre optique offre un débit de 155 Mbit/s. Là où 30 communications téléphoniques étaient envisageables, on pourrait en faire passer maintenant plus de 15 000 !
Il est donc envisageable à l'heure actuelle d'avoir un même réseau pour transmettre des informations variées (communications téléphoniques, fichiers, images fixes ou animées,…). Celles-ci empruntent des artères de transmission à très haut débit, appelées souvent *autoroutes de l'information.*
Les solutions techniques ont donc évolué. Cependant, du point de vue architectural, elles reprennent toujours la philosophie en couches, concept de base des réseaux développé dans le modèle de référence qu'il est important de bien comprendre.
Les avantages de la numérisation sont nombreux :
- la fiabilité de la transmission : l'information transmise étant une séquence binaire, les valeurs représentées appartiennent à un ensemble discret et limité. Ainsi, contrairement à une source

d'information analogique, on utilise des techniques à seuil lors de la déformation du signal transmis. Après reconnaissance par discrimination, le signal est régénéré (répété) offrant ainsi une transmission fiable.

- la banalisation de l'information transmise : indépendamment de la source, l'information transmise correspond à des séquences binaires. Ainsi, le support véhicule des bits. Ces derniers représentent aussi bien du texte, de la parole, de l'image (fixe ou animée). Par conséquent, il est possible de constituer un réseau " multi-usages ".

- la compression : les algorithmes de compression informatiques sont utilisés dès la phase de numérisation terminée. Dans ce cas, il est possible de choisir entre tel ou tel algorithme selon le contenu informationnel d'origine.

- le cryptage : de la même façon que la compression, on applique des techniques de cryptage issues du monde informatique, et tout type de manipulation sur les données (effets spéciaux sur les images,…).

- la protection contre les erreurs : lorsque l'application le permet (pas de contrainte temporelle élevée), des techniques de protection contre les erreurs sont mises en œuvre offrant ainsi encore plus de fiabilité.

Exercices

Exercice 1

Citer les codes ou alphabets que vous connaissez ! Quels sont les symboles représentables? Comment représente-t-on la parole, la musique, les images pour les applications que vous connaissez : le téléphone, la télévision, les CD audio ou vidéo ? Quels sont les intérêts du numérique par rapport à l'analogique ?

Exercice 2

Dans un système à disque compact, chaque canal stéréo est échantillonné à 44,1 kHz avec une résolution de 16 bits par échantillon. Déterminer le volume de données stockées sur le CD pour l'enregistrement de la 9ème symphonie de Beethoven (durée 74 mn).

Exercice 3

Dans le réseau Télex, on utilisait une transmission asynchrone avec un alphabet qui contient 5 bits par caractère. Comment pouvait-on coder les lettres de notre alphabet, les chiffres et les autres symboles (ponctuation, par exemple) qui constituent cette page ?

Exercice 4

Un fichier est codé en ASCII et transcrit ci-dessous en hexadécimal. Ecrire son contenu en clair.
4C 65 20 44 45 55 47 20 50 61 72 69 73 20 35 20 65 73 74 20 75 6E 65 20 22 65 78 63 65 6C 6C 65 6E 74 65 22 20 46 6F 72 6D 61 74 69 6F 6E 2E

Exercice 5

Une imprimante noir et blanc a une résolution de 600 dpi (dot per inch). Un point est supposé représenté par un bit (0 pour un point blanc, 1 pour un point noir). Quel est le volume d'informations dans une page A4 ? Quelle doit être la capacité de traitement de cette imprimante pour une impression de 4 pages à la minute ?
Rappel 1 inch = 2,54 cm ; A4 = 21 x 29,7 cm

Exercice 6

Soit un ensemble de 26 symboles à coder en binaire pour la transmission et le traitement informatique.
a) Combien de bits sont nécessaires pour chaque symbole, si l'on choisit un code de longueur fixe ?
b) Si 6 symboles ont une même probabilité d'occurrence de 0,1 et les 20 autres une même probabilité (à calculer...), montrer qu'avec un code à longueur variable on peut optimiser la représentation par rapport à la question a). Quel est le gain obtenu ?
c) Si tous les symboles sont équiprobables, peut-on imaginer un code à longueur variable ?

Exercice 7

Soit à coder, en binaire pour la transmission et le traitement informatique, une page au format A4. On choisit de représenter chaque pixel par un bit (0 s'il est blanc, 1 s'il est noir).
a) Sachant qu'il y a (pour le fax) 1728 pixels par ligne et 3,85 lignes de pixels par mm, quel est le volume de données binaires pour représenter ainsi une page ?
b) Combien de temps faut-il pour transmettre cette page à 9600 bit/s, à 64 kbit/s ?
c) Mêmes questions si l'on veut transmettre l'image avec 256 couleurs (possibles pour chaque pixel).

Exercice 8

Pour les longues suites de zéros (qui sont obtenues dans le fax pour les plages blanches...), on choisit de faire de la compression en utilisant le codage par plages. Chaque symbole de k bits indique combien de zéros séparant deux 1 consécutifs. Pour traiter les longues plages, le symbole plein 1 signifie qu'une plage de 2^k-1 plus la valeur du (ou des) symbole(s) suivant(s) sépare les deux 1.Soit la chaîne suivante
0 0 0 1 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 1 1 0 1 0 0 0 0 1 0 1
a) Quelle est la suite des longueurs de plages séparant les 1 ?
b) Coder cette suite sur k = 3 bits. Comment se représente 15 ?
c) Quelle est la suite obtenue ? quel est le taux de compression ?
d) Peut-on décoder la suite ?
e) Et s'il y a une erreur au cours de la transmission ?
f) Recommencer la même opération une deuxième fois. Qu'obtient-on ?

Exercice 9

On considère une suite de données binaires, issues de la numérisation d'un document papier. Chaque pixel blanc est codé par 0, chaque pixel noir est codé par 1.Les données sont regroupées par octets pour faciliter la lecture.

```
00000000 00000000 00000000 00000000 00001000 00011100 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00001000 00011000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000100 00010000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000110 00010000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000011 00010000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000001 10010000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 11100000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 01100000 00000000 00000000 00000000
```

Il y a huit lignes de neuf octets ce qui représente une surface d'environ 2mn x 8 mn (pour un télécopieur par exemple). Quel est le nombre de bits utilisés pour le codage de cette petite surface ?
Remarquant que cette suite de données contient beaucoup de zéros, on choisit de la compresser de la façon suivante : on remplace la suite des données par la concaténation des longueurs de plages de zéros consécutifs. Ainsi la première ligne devient 36, 6 , 0 ,0 , 26 qui se comprend : 36 zéros, 1 un, 6 zéros, 1 un, 0 zéro, 1 un, 0 zéro, 1 un, 26 zéros
Donner de la même façon les sept lignes suivantes.
Combien de plages de zéros trouve-t-on, en moyenne par ligne ?
Les données effectivement stockées sont donc le codage en binaire des longueurs de plages avec la règle suivante : les longueurs comprises entre 0 et 30 sont codées en binaire naturel sur 5 bits, les longueurs entre 31 et 63 sont codées sur 10 bits dont les 5 premiers sont toujours 11111 et les cinq suivants représentent le codage en binaire naturel de la longueur -31; les longueurs comprises entre 64 et 95 sont codées sur 15bits dont les 10 premiers sont 11111 11111 et les 5 suivants représentent le codage en binaire naturel de la longueur -64, etc.
Ainsi la première ligne devient

```
          11111 00101 00110 00000 00000 11010
          <-- 36  --> <-6-> <-0-> <-0-> <-26->
```

Sans donner les autres lignes, quel est le nombre total de bits nécessaire à cette représentation ?
Quel est le gain de la compression ?

Annexe

Les préfixes multiplicateurs et diviseurs pour les unités

kilo (k)	1000= 10^3	milli (m)	10^{-3}
Méga (M)	1000000= 10^6	micro (μ)	10^{-6}
Giga (G)	10^9	nano (n)	10^{-9}
Téra (T)	10^{12}	pico (p)	10^{-12}
Péta (P)	10^{15}	femto (f)	10^{-15}
Exa (E)	10^{18}	atto (a)	10^{-18}
Yotta (Y)	10^{21}	yocto (y)	10^{-21}
Zéta (Z)	10^{24}	zepto (z)	10^{-24}

kilo ou Kilo ?

En informatique, on substitue souvent Kilo (avec un K majuscule) à kilo (avec un k minuscule).

Kilo représente 2^{10} soit 1024 qui est très proche de 1000. Par la suite les autres préfixés (qui ne sont pas différenciés par l'initiale) s'entendent dans le même sens, c'est-à-dire comme des puissances de 2 :

Méga = 2^{20} soit 1048576 au lieu de 1000000, ce qui fait 4,8% d'écart

Giga = 2^{30} soit 1073741824 au lieu de 1000000000, ce qui fait 7,3% d'écart

et ainsi de suite….

Les unités de volumes d'informations

Le bit est l'unité normalisée d'information : c'est l'information élémentaire qui peut prendre deux valeurs 0 ou 1 (vrai ou faux, noir ou blanc, ouvert ou fermé…). L'octet est un ensemble de huit bits. En anglais byte (prononcer baït et ne pas confondre avec bit !).

On utilisera le Kilooctet (1024 octets), le Mégaoctet (1048576 octets), le Gigaoctet, le Téraoctet,…. comme unité de volume de données binaires dans un fichier, voire un système de stockage de données.

Références

Sites utilisés

Les illustrations de ce chapitre sont extraites des deux sites suivants :

http://www.httr.ups-tlse.fr/pedagogie/

http://www.rennes.supelec.fr/ren/perso/ pleray/audio/audio_0.htm

http://membres.lycos.fr/imgnum/intro.html

pour en savoir plus

http://web.ccr.jussieu.fr/urfist/image_numerique/Image_numerique1.htm
http://www.tcom.ch/Tcom/Laboratoires/digivox2000/chap/chap4/mod_diff.htm

Quelques corrigés

Exercice 1

Citer les codes ou alphabets que vous connaissez ! réponses possibles : ASCII, EBCDIC, Unicode, UCS = ISO 10646 ...
Quels sont les symboles représentables ? réponses possible selon les codes : les 26 lettres de l'alphabet (parfois minuscules ET majuscules), les chiffres, les symboles de ponctuation, les symboles mathématiques, les symboles de monnaie, des éléments graphiques..., des caractères de mise en page et de structures (non imprimables)
Il y a parfois problème pour représenter les spécificités de chaque langue (lettres accentuées du français, par exemple)
Comment représente-t-on la parole, la musique, les images pour les applications que vous connaissez : le téléphone, la télévision, les CD audio ou vidéo ?
téléphonie classique : accès = analogique, transport dans le réseau = numérique
téléphonie sans fil, RNIS : numérique
télévision classique ; analogique
studios : numérique
CD Audio, DVD : informations numériques
Quels sont les intérêts du numérique par rapport à l'analogique ? question de cours : revoir le chapitre

Exercice 2

musique stéréo = 2 bandes son (gauche et droite) chacune est numérisée : il faudra multiplier par 2 le résultat
44,1 kHz = 44100 Hz ; il y a donc 44100 échantillons par seconde de musique, chacun codé sur 16 bits, sur chaque bande son
74 minutes = 74 * 60 = 4440 secondes
nombre de bits total = 2 * 44100 * 4440 * 16 = 6 265 728 000 bit
Calculons en Méga octets : il faut diviser par (8*1024*1024). On obtient 747 Mo

Exercice 5

1 page A4 = 21cm * 29,7 cm
horizontalement, il y a donc 21*600/2,54 pixels
[21 cm, 600 pixels par pouce et 2,54 cm par pouce]
verticalement c'est pareil : il y a 29,7*600/2,54 pixels
soit en tout, 21*600*29,7*600/(2,54 *2.54) = 34 802 530 pixels

ensuite 1 pixel = 1 bit (codage noir et blanc) donc le volume de la page est de 34802530 bits
pour obtenir le résultat en Mégaoctet il faut diviser par 8*1024*1024 (et non par 8*1000000)
on obtient 4,15 Mo
pour pouvoir imprimer 4 pages par minutes, l'imprimante doit avoir une capacité de 4,154*4 = 16,6 Mo/minute ou 2,2 Mbit/s.

Exercice 7

a) volume d'information dans une page numérisée
1768 * 3,85 * 297 = 2021619,6 bits soit 246,78 Kilooctets

b) temps de transmission
2021619,6/ 9600 = 210,6 s = 3 minutes 30 secondes
2021619,6/ 64000 = 31,6 s

conclusion : que le débit soit 9600 ou 64000bit/s, le temps de transmission est inacceptable !
Dans la pratique, les télécopieurs effectuent une compression de l'image de la plage avant de transmettre ==> le temps de transmission devient acceptable (et il est variable, suivant le contenu de la page)

c) s'il y a des couleurs, 256 couleurs nécessitent un codage sur 8 bits.
Il faut multiplier les résultats précédents par 8....

Exercice 9

il y a huit lignes de neuf octets soit 8 * 9 = 72 octets donc 72 * 8 = 576 bits

la ligne 1 est représentée par 36, 6, 0, 0, 26
- ligne 2 : 36, 6, 0, 27
- ligne 3 : 37, 5, 28
- ligne 4 : 37, 0, 4, 28
- ligne 5 : 38, 0, 3, 28
- ligne 6 : 39, 0, 2, 28
- ligne 7 : 40, 0, 0, 29
- ligne 8 : 41, 0, 29

Il y a en moyenne 4 plages de 0 par ligne (5 sur la première ligne et 3 seulement sur les lignes 3 et 8)

Pour calculer la longueur du fichier compressé, il faut ajouter la longueur de tous les codes des nombres ci-dessus.
- ligne 1 : 30 bits (10+5+5+5+5)
- ligne 2 : 25 bits (10+5+5+5)
- ligne 3 : 20 bits ...
- ligne 4 : 25 bits
- ligne 5 : 25 bits
- ligne 6 : 25 bits
- ligne 7 : 25 bits
- ligne 8 : 20 bits

soit en tout 195 bits nécessaires pour cette représentation . Le gain obtenu est alors (576 -195) / 576 = 66 %
Remarque : cette compression est d'autant plus efficace que le fichier initial contient beaucoup de blanc (pixel 0).

Constitution d'une liaison simple

Caractéristiques d'une transmission locale

L'introduction d'une distance entre les équipements informatiques a un tel impact sur les communications qu'une architecture complète de règles d'échanges a dû être définie et normalisée au plan international.
Supposons qu'un ordinateur échange des données avec son périphérique, déroulant ainsi une entrée/sortie.
L'échange met en jeu :
– un bus d'adresse (permettant de véhiculer l'adresse du périphérique qui peut ainsi reconnaître qu'il est concerné par l'échange), ce bus ayant autant de " fils " qu'il y a de bits d'adresse ;
– un bus de données (permettant de véhiculer les données dans un sens ou dans l'autre, données qui sont souvent échangées en parallèle, sur un bus de 8 fils) ;
– des fils de contrôle, véhiculant chacun un signal particulier, nécessaires au bon déroulement de l'entrée/sortie.
Les caractéristiques d'un tel échange sont :
– la vitesse à laquelle on peut transférer des données entre l'ordinateur et son périphérique est très grande, elle s'exprime typiquement en milliards d'octets par seconde ;
– la qualité de ce transfert est généralement excellente, il est très rare qu'un bit d'information soit erroné à la réception, l'ordre de grandeur du taux d'erreur est de 10^{-12}, 10^{-13} … voire moins ;
– plusieurs sortes d'informations sont échangées, (données, adresses, contrôle) dans les deux sens, même si le transfert des données n'a lieu que dans un sens précis. Ces informations sont identifiées par le fil ou le bus sur lequel elles circulent. Ces différentes informations sont émises en parallèle, chacune sur son support.

Caractéristiques d'une transmission à distance

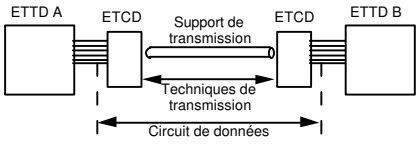
Le problème de la transmission à distance est donc de reproduire le même échange en introduisant un moyen de transporter l'information sur des dizaines ou des milliers de kilomètres. On utilise un support de transmission et un signal qui doit transporter, sous une forme ou sous une autre, les informations.
L'introduction du support a de nombreuses conséquences.
– Le support est généralement une ressource chère que l'on cherchera à rentabiliser au maximum. Un support de transmission unique doit véhiculer *en série* toutes les informations précédentes (qu'il s'agisse d'adresses, de données ou de contrôle). Il faudra donc imaginer un moyen d'identifier ces informations correctement.
– Le support a une bande passante limitée, il ne peut pas transmettre n'importe quels signaux, ni n'importe quelle quantité d'information sur ces signaux. Tous supports confondus, le débit d'une transmission à grande distance peut varier de 50 bit/s à quelques centaines de Mbit/s. Un échange à grande distance se fait en général *plus lentement* qu'un échange local et il faut en tenir compte dans les programmes des différentes machines informatiques.
– Le support n'est pas parfait. Même si les signaux sont correctement adaptés à la bande passante, ils sont toujours affectés par des distorsions, des affaiblissements et surtout du bruit qui perturbent leur propagation et créent une qualité de réception *nettement moindre*. Il faudra donc imaginer un moyen de détecter les erreurs de transmission et les corriger si le taux d'erreur sur le support est insupportable pour l'application, c'est-à-dire pour les besoins de l'utilisateur : une liaison téléphonique peut être considérée de très bonne qualité pour transmettre de la parole et se révéler de médiocre qualité pour la transmission de données bancaires.
– La transmission des signaux sur n'importe quel support suppose un certain délai de propagation, incompressible, qui peut atteindre des valeurs très grandes (des centaines de millisecondes dans le cas de transmissions par satellite). Il faudra tenir compte de ce paramètre dans le déroulement de la communication.
Nous venons donc de voir que de nombreux paramètres de la communication sont changés : le taux d'erreur est plus élevé, le débit plus faible et le délai de propagation plus grand. Enfin, toutes les informations sont transmises en série.

Eléments de base

Il est d'usage de structurer la transmission en un ensemble de " boîtes noires ", chacune remplissant une fonction particulière.

– L'ETTD, *Équipement Terminal de Traitement des Données*, désigne l'équipement informatique qui génère les données à transmettre et traite les données reçues. L'ETTD est, par exemple, un ordinateur personnel.

– L'ETCD, *Équipement de Terminaison du Circuit de Données*, reçoit en entrée la suite de données binaires et fournit en sortie un signal dont les caractéristiques sont adaptées au support de transmission. Il effectue également l'opération inverse : recevant le signal qui s'est propagé dans le support, il en extrait une suite de données binaires. L'ETCD rend ainsi transparente à l'utilisateur la nature du support de transmission réellement utilisé.



Constitution d'un circuit de données

Le nom ETCD est normalisé. L'importance de la normalisation dans ce domaine ainsi que les différentes instances qui réglementent les transmissions aux niveaux international, européen et national sont présentées plus loin. En anglais, l'ETCD est appelé DCE, *Data terminating Circuit Equipment* et l'ETTD est désigné par DTE, *Data Terminating Equipment.* Il est possible de représenter la fonction de l'ETCD en deux transformations successives. Un ou plusieurs bits successifs sont convertis en un *symbole* choisi à l'intérieur d'un alphabet limité. Ce symbole est alors transformé en un signal particulier (électrique, électromagnétique ou optique) pendant une durée élémentaire. Dans le cas le plus simple, un bit est associé de façon bi-univoque à un symbole.

L'ETCD est couramment appelé *modem* pour modulateur-démodulateur. Il est souvent intégré aux ordinateurs (le minitel, par exemple, est un terminal très simple muni d'un modem intégré). Pour permettre une indépendance entre les ordinateurs et les ETCD, une interface a été définie sous le nom de V24. Cette interface peu performante mais relativement simple s'est considérablement développée. La grande majorité des ordinateurs en sont pourvus. L'ensemble constitué par le support et les deux ETCD placés à chaque extrémité constitue un *circuit de données.* Compte tenu des caractéristiques du support que nous venons de voir, on peut dire que le circuit de données est une entité capable d'écouler une suite de données binaires à un débit donné avec un délai donné, mais sans garantie de qualité. Si la transmission simultanée dans les deux sens est possible, le circuit est dit *full-duplex* ou *duplex intégral* Lorsqu'elle n'est possible que dans un seul sens à un moment donné — on parle de transmission à l'alternat —, le circuit est dit *half-duplex* ou *semi duplex.* Enfin, lorsqu'elle n'est possible que dans un seul sens prédéfini, le circuit est dit *simplex.*

La qualité du circuit de données

La qualité du circuit de données est mesurée à l'aide de différents critères.

– Le *taux d'erreurs* est le rapport du nombre de bits erronés reçus au cours d'une période d'observation, au nombre total de bits transmis pendant cette période.

– La *disponibilité* permet d'évaluer la proportion de temps pendant lequel la transmission est possible (absence de panne ou de coupure). Dans certains cas, on s'intéresse également au nombre d'incidents et à leur durée cumulée, afin d'en déterminer la durée moyenne et, le cas échéant, le coût.

– Le *débit binaire* D représente le nombre de bits transmis par seconde. On précise éventuellement si ce débit est possible en duplex intégral, en semi duplex ou en simplex.

– La *rapidité de modulation* R indique le nombre de symboles transmis par unité de temps et s'exprime en *bauds*. Le mot baud vient d'Emile BAUDOT (1845-1903), ingénieur français. Si d représente la durée exprimée en secondes de l'intervalle significatif le plus court séparant deux symboles successifs, alors $R = 1/d$ bauds.

La relation liant la rapidité de modulation au débit binaire est la suivante :

$D = R \cdot \log_2 V$
où V est la valence des signaux émis, c'est-à-dire le nombre de symboles utilisés. Pour des signaux de valence 2, donc pour lesquels chaque intervalle d transporte un bit, les valeurs numériques du débit et de la rapidité de modulation sont égales.

Caractéristiques des supports de transmission

Les supports de transmission, quels qu'ils soient, ne sont malheureusement pas parfaits. Ils ont une bande passante limitée, supportent divers bruits et ont de ce fait une capacité à transmettre les signaux limitée.

Bande passante

Ils ont une *bande passante* limitée c'est-à-dire que certains signaux se propagent correctement dans le support (ils sont affaiblis mais encore reconnaissables à l'autre extrémité), mais d'autres ne le traversent pas du tout (ils sont tellement affaiblis ou déformés qu'on ne les retrouve plus du tout à la sortie). La bande passante d'un support est la bande de fréquences des signaux dont la puissance à la sortie, après la traversée du support, est supérieure à un seuil donné. En général, on caractérise un support par sa bande à 3 dB (décibels), c'est-à-dire par la plage de fréquence à l'intérieur de laquelle la puissance de sortie d'un signal sinusoïdal est au pire divisée par deux (en notant P_S la puissance de sortie et P_e la puissance d'entrée, l'affaiblissement en dB s'exprime comme $10 \log_{10} P_e/P_S$. Pour $P_e/P_S = 2$, on trouve $10 \log_{10} P_e/P_S = 3$ dB). Intuitivement, plus un support a une bande passante large et plus il pourra transporter d'informations par unité de temps.

Bruits et distorsions

Les supports de transmission déforment les signaux qu'ils transportent même lorsque ceux-ci ont des fréquences adaptées. En effet, plusieurs sources de *bruit* perturbent les signaux et des *distorsions* (d'amplitude ou de phase) peuvent s'avérer gênantes pour la reconnaissance des signaux en sortie.
Par ailleurs, la distance est un facteur d'affaiblissement, particulièrement important pour les liaisons par satellite. Enfin, certaines perturbations de l'environnement peuvent également introduire des bruits (foudre, orages pour le milieu aérien, champs électromagnétiques dans des ateliers pour les supports métalliques…). Même lorsque les signaux sont adaptés aux supports de transmission, on ne pourra pas garantir à 100% leur exactitude à la réception.

Capacité limitée

L'ensemble des caractéristiques que nous venons de voir fait que la capacité d'un support de transmission est limitée. Par capacité, nous entendons la quantité d'information transportée par unité de temps.
Un théorème dû à *Shannon (*Claude Shannon, mathématicien américain du XX^{ème} siècle qui a développé la théorie de l'information) donne une borne maximale de cette capacité, notée Cap_{Max} et exprimée en bits par seconde :
$Cap_{Max} = W \log_2 (1 + S/B)$
où W est la largeur de la bande passante exprimée en Hertz, S/B est la valeur du rapport puissance du signal à puissance du bruit, la base deux du logarithme servant pour exprimer l'information en bits.
A titre d'exemple, sur une liaison téléphonique dont la bande passante a une largeur de 3100 Hz et avec un rapport S/B correspondant à 32 dB (valeurs courantes), on obtient :
$10 \log_{10} S/B = 32$ donc $\log_{10} S/B = 3,2$ soit $S/B = 1585$
$Cap_{Max} = 3100 \log_2 (1 + 1585)$ soit avec $1586 = 2^{10,63}$
$Cap_{Max} = 3100 \times 10,63 = 33000$ bit/s.

Les supports de transmission

Pour de nombreuses applications, il est nécessaire de disposer d'une liaison directe et permanente entre deux ordinateurs éloignés. Le plus ancien support de transmission employé à cette fin, et encore le plus largement utilisé aujourd'hui, est la paire torsadée. Les câbles coaxiaux et les fibres optiques sont également fréquents. Enfin, les communications sans fils sont en plein essor.

La paire torsadée

Une *paire torsadée* non blindée (UTP, *Unshielded Twisted Pair*) est composée de deux conducteurs en cuivre, isolés l'un de l'autre et enroulés de façon hélicoïdale autour de l'axe de symétrie longitudinal. Cet enroulement permet de réduire les conséquences des inductions électromagnétiques parasites provenant de l'environnement. L'utilisation la plus courante de la paire torsadée réside dans la desserte des usagers du service téléphonique ou des usagers de réseaux privés. Les abonnés sont reliés à l'autocommutateur local par de simples paires de fils métalliques dont les diamètres sont compris entre 0,4 et 0,8 mm. Ces fils sont en cuivre ou quelquefois en aluminium.

Le principal inconvénient des fils métalliques téléphoniques est leur affaiblissement, d'autant plus important que le diamètre est faible. Il peut donc être nécessaire de placer dans la paire à intervalles réguliers des éléments, appelés répéteurs ou régénérateurs, qui régénèrent le signal transmis. En outre, quand plusieurs paires sont rassemblées dans un même câble, les signaux électriques qu'elles transportent interfèrent plus ou moins les uns avec les autres par rayonnement ; ce phénomène porte le nom de *diaphonie.* La bande passante d'une liaison téléphonique est d'environ 3,1 kHz entre les fréquences 300 et 3 400 Hz. Les débits permis par les liaisons téléphoniques sont de l'ordre de 10 kbit/s : 9 600 bit/s en duplex intégral, voire 14 400 bit/s. L'utilisation de techniques d'adaptation dynamique aux caractéristiques réelles de la liaison permet d'atteindre un débit de 28800 bit/s, voire 56 kbit/s.

Sur des distances relativement courtes de quelques dizaines de kilomètres, par une transmission en bande de base, on atteint 72 kbit/s. Si l'on se limite à une distance de plusieurs centaines de mètres, le débit peut atteindre plusieurs centaines de Mbit/s. A l'extrême, sur les bus d'ordinateurs, des Goctets/s peuvent être obtenues facilement.

Pour les réseaux locaux d'entreprise, où les distances sont limitées à quelques kilomètres, la paire torsadée peut être suffisante. Les avantages sont nombreux : technique très bien connue, facilité de connexion, ajout de nouvelles entrées sans problème, coût faible. Certains constructeurs proposent des paires torsadées blindées (STP, *Shielded Twisted Pair*) c'est-à-dire " enrobés " d'un conducteur cylindrique protégeant mieux des parasites.

Les câbles coaxiaux

Pour éviter les perturbations dues aux bruits externes, on utilise souvent deux conducteurs cylindriques de même axe, séparés par un isolant, et qui forment un ensemble appelé *câble coaxial.* On peut montrer que le rapport entre les diamètres des deux conducteurs doit être de 3,6. Les différents câbles sont désignés par des diamètres en mm ; les deux plus courants sont le 2,6/9,5 et le 1,2/4,4. L'atténuation varie de 2 à 18 dB/km suivant le type de câble et les fréquences utilisées. Des amplificateurs doivent être disposés tous les 4,5 km et 3 km respectivement pour les deux exemples donnés.

Le câble coaxial présente de meilleures caractéristiques que le câble à paire torsadée. Il offre en outre un bon compromis entre la largeur de la bande passante qu'il présente et la protection contre les rayonnements électromagnétiques parasites. Sa bande passante dépend des caractéristiques des conducteurs et des isolants et de sa longueur utile. Pour les câbles utilisés en transmission en bande de base, il est possible d'atteindre un débit de 10 Mbit/s sur une longueur d'un kilomètre. Des débits plus élevés peuvent être obtenus sur des distances plus courtes. De même, il est possible de transmettre à des débits inférieurs à 10 kbit/s sur des distances supérieures à 10 km.

La fibre optique

Une *fibre optique* est constituée d'un fil de verre très fin, à base de silice. Elle comprend un cœur dans lequel se propage la lumière. Une impulsion lumineuse représente l'information binaire 1 tandis que l'absence de lumière représente l'information binaire 0.

Les avantages de la fibre optique sont nombreux. Le diamètre extérieur est de l'ordre de 0,1 mm et son poids de quelques grammes au kilomètre. Cette réduction de taille et de poids la rend facilement utilisable. Autre avantage technique : la largeur de la bande passante utilisée (1 GHz pour un km) qui permet le multiplexage sur un même support de très nombreux canaux de télévision, de hi-fi, de téléphone,… La faible atténuation des fibres conduit par ailleurs à envisager un espacement plus important des points de régénération des signaux transmis. Les meilleures fibres optiques présente une atténuation de 0,3 dB/km, ce qui permet d'envisager des pas de régénération de plus de 500 km. A titre de

comparaison, le câble coaxial en cuivre Paris-Lyon utilisé à 60 MHz possédait des répéteurs tous les 2 km. Lorsque l'on connaît les inconvénients que présentent les amplificateurs régénérateurs intermédiaires sur une ligne de transmission, on comprend l'importance de cet aspect technique pour les télécommunications.
De surcroît, l'insensibilité des fibres aux parasites électromagnétiques constitue un avantage particulier pour la transmission de données, dans la mesure où elle leur permet de supporter sans difficulté la proximité d'émetteurs radioélectriques.
L'inconvénient des fibres optiques tient au coût des ETCD, appelés dans ce contexte coupleurs optiques. Cet aspect limite leur généralisation dans le cadre des réseaux locaux d'entreprise.

L'éther

L'utilisation des ondes électromagnétiques permet la transmission de signaux sur un support immatériel, désigné par le terme d'*éther*, qui peut être l'atmosphère ou le vide. Elle est pratiquement indispensable dans le cas de liaisons très longues distances. De plus, l'absence de support matériel permet d'apporter une certaine souplesse et convient bien aux applications ponctuelles. Ce type de transmission comprend principalement les faisceaux hertziens, les rayons infrarouges et les rayons laser.
Les transmissions par rayons laser ou infrarouges sont entièrement numériques et à faisceaux très directifs, ce qui les protège contre la plupart des interceptions frauduleuses. Toutefois, les conditions météorologiques peuvent, selon les fréquences de travail choisies, altérer la qualité des communications entre les immeubles.
Les faisceaux hertziens reposent sur l'utilisation de fréquences très élevées (fréquences de 2 GHz à 15 GHz voire jusqu'à 40 GHz qui correspondent à des longueurs d'onde centimétriques à décimétriques) et de faisceaux directifs produits par des antennes rayonnant principalement dans une direction donnée. La propagation est limitée à l'horizon optique. La transmission se fait entre des stations placées en hauteur (par exemple sur une tour ou au sommet d'une colline) pour éviter les obstacles dus aux constructions environnantes. Dans les fréquences élevées (au-dessus de 12 GHz), la pluie et la neige introduisent un affaiblissement supplémentaire, ce qui conduit à rapprocher les stations. Les faisceaux hertziens sont utilisés pour la transmission de chaînes de télévisions et pour constituer des artères de transmission longue distance dans les réseaux téléphoniques sans avoir recours à la pose coûteuse de câbles. Ils sont utilisés également dans les transmissions par satellite.
Les ondes dites radioélectriques correspondent à des fréquences comprises entre 10 kHz et 2 GHz. Ces ondes sont diffusées, c'est-à-dire que, d'un émetteur, on peut les capter avec des récepteurs dispersés géographiquement. Contrairement aux faisceaux hertziens, il n'est pas nécessaire d'avoir une visibilité directe entre l'émetteur et le récepteur car le récepteur utilise l'ensemble des ondes réfléchies et diffractées. En revanche, la qualité de la transmission est faible.

Utilisation des différentes gammes de fréquences

L'attribution de telle ou telle bande de fréquence (ou longueur d'onde) à tel ou tel service exploitant est faite en tenant compte de la situation existante, du désir de contenter tout le monde et de réserver les longueurs d'onde les mieux appropriées à l'utilisation envisagée. Elle varie suivant les continents et fait l'objet d'accords internationaux. Les grandes lignes de la répartition des ondes sont données dans le tableau. Au-delà de 960 MHz, on trouve un partage complexe entre radiotéléphonie, transmission par faisceaux hertziens, radars, communication par satellite.

Gamme de fréquence	Type d'utilisation
10 kHz - 150 kHz	Communications radiotélégraphiques
150 kHz - 300 kHz	Radiodiffusion (grandes ondes)
510 kHz - 1605 kHz	Radiodiffusion (petites ondes)
6 MHz - 20 MHz	Radiodiffusion (ondes courtes)
29,7 MHz - 41 MHz	Radiotéléphonie
47 MHz - 68 MHz	Télévision
68 MHz - 87,5 MHz	Liaisons radio en modulation de fréquences
87,5 MHz - 108 MHz	Radiodiffusion
108 MHz - 162 MHz	Radiotéléphonie
162 MHz - 216 MHz	Télévision
216 MHz - 470 MHz	Radiotéléphonie
470 MHz - 860 MHz	Télévision et radar
860 MHz - 960 MHz	Radiotéléphonie
Autour de 1800 MHz	Radiotéléphonie
Entre 6 et 30 GHz	Services satellites en fixe

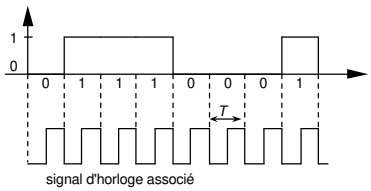
Utilisation des différentes gammes de fréquences

Techniques de transmission

Après la conversion parallèle/série, l'ETTD peut délivrer ses caractères accolés les uns à la suite des autres en une succession régulière, dans le temps, de symboles binaires, sous forme d'un signal électrique bivalent appelé *message de données synchrone*. Il peut aussi délivrer des suites de caractères séparés par des intervalles de temps variables et aléatoires pour lesquels la durée de chaque état est multiple ou non d'un intervalle de temps élémentaire T_e. Le message de données sera alors dit *asynchrone*.

Transmission synchrone

Un signal numérique est *synchrone* si les intervalles de temps alloués à chaque symbole sont égaux et coïncident avec les périodes successives d'un signal appelé base de temps ou horloge. Le signal d'horloge associé est indispensable à l'interprétation du signal de données. L'interprétation est effectuée en échantillonnant le signal de données aux instants qui coïncident avec les fronts du signal d'horloge. Ce signal est périodique de période T. L'ETTD délivre, chaque seconde, un nombre de symboles égal à $1/T$, fréquence du signal d'horloge.
Les transmissions synchrones sont utilisées pour acheminer des volumes importants d'information (transfert de fichiers par exemple). En transmission synchrone, la synchronisation se fait au niveau des éléments binaires et, éventuellement, au niveau des caractères. Elle est fondée sur l'utilisation de combinaisons spéciales : les caractères de synchronisation.

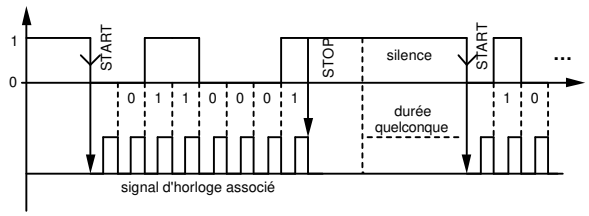


Transmission synchrone

Transmission asynchrone

Lorsque la source produit des caractères, à faible débit et à des instants aléatoires, il est parfois plus simple de transmettre ces caractères au moment où la source les délivre, sans tenir compte des caractères

précédents ou suivants. On a alors des successions de trains de symboles binaires synchrones pour la durée de transmission d'un caractère, qui se succèdent à des instants aléatoires.



Le délimiteur de début START dure une période et prend l'état 0.
Le délimiteur de fin STOP dure deux périodes et prend l'état 1.

Transmission asynchrone

Au repos, la ligne de transmission reste à l'état 1, utilisé comme état d'inactivité. Il est nécessaire d'adjoindre au caractère des délimiteurs de début (START) et de fin (STOP) permettant une reconnaissance du caractère. Le délimiteur START correspond à un état actif 0 pendant un temps-bit : il provoque nécessairement une transition qui marque ainsi le début de transmission. Le délimiteur STOP correspond à un état inactif 1 pendant un ou deux temps bits suivant la configuration choisie : il permet de s'assurer que la ligne revient bien au repos à la fin du caractère (Il est possible d'intervertir les états 1 et 0 dans le texte et d'utiliser l'état 0 comme état inactif entre les caractères. On présente ici la configuration la plus courante). Le caractère lui-même est généralement transmis en commençant par les bits de poids faible. Une telle transmission est dite *asynchrone* ou *arythmique* ou encore *START/STOP*. L'avantage d'une telle transmission est sa simplicité, l'inconvénient majeur provient de l'allongement du délai de transmission : pour chaque caractère, il faut transmettre au moins deux bits supplémentaires.

Transmission en bande de base

Les supports de transmission sont caractérisés par le fait qu'ils ont une bande passante limitée. Certains peuvent être assimilés à des filtres passe-bas, c'est-à-dire qu'ils ne laissent passer que les basses fréquences, d'autres se comportent comme des filtres passe-bande, c'est-à-dire qu'ils ne laissent passer les fréquences que dans un certain intervalle.

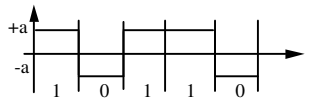
Lorsqu'un signal numérique traverse un filtre, il subit des modifications qui ont pour effet, entre autres, d'atténuer la raideur des fronts. Ces déformations ne sont pas gênantes si l'information numérique contenue dans le signal, en sortie du filtre, peut encore en être extraite. L'estimation des informations contenues dans les signaux reçus permettra de régénérer localement des signaux identiques aux signaux originaux. La condition pour que cette estimation soit correcte est qu'en échantillonnant les signaux à un rythme correspondant aux intervalles significatifs, on mesure sans ambiguïté des valeurs égales à celles des impulsions qui constituent le signal initial.

Certains supports de transmission autorisent la transmission directe des signaux numériques, dite *transmission en bande de base* , qui conduit à des réalisations simples et économiques.

Les principales difficultés rencontrées dans la transmission directe d'une information en ligne sont dues à la limitation de la bande passante dans les basses et les hautes fréquences ainsi qu'à la transparence vis-à-vis des données. Par ailleurs, le signal d'horloge associé aux données doit pouvoir être correctement reconstitué, quelle que soit la séquence de données binaires transmise, les distorsions d'amplitude et de phase doivent pouvoir être corrigées.

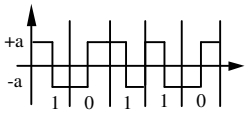
La transmission du signal d'horloge peut être réalisée de deux façons : indépendamment du signal de données ou en utilisant les transitions du signal codé.

Le mode de représentation le plus habituel de l'information numérique est le signal binaire sans retour à zéro (*NRZ, No Return to Zero*). Un niveau de tension (+*a* sur la figure) pendant une période complète est utilisé pour représenter un 1. Un autre niveau (–*a* sur la figure) est utilisé pour le 0. Le signal avec retour à zéro (*RZ, Return to Zero*) utilise le même principe mais la durée du niveau de tension est inférieure à la période.



Représentation d'une information numérique en NRZ

Le code biphase fréquemment appelé Manchester est une représentation à deux niveaux obtenue en transmettant pendant chaque intervalle de temps correspondant à un symbole binaire, deux polarités opposées : un front montant ou un front descendant, au milieu de l'intervalle de temps significatif. Les états logiques 0 et 1 peuvent être affectés à chacun de ces symboles.



Code biphase

Les codes biphases assurent au moins une transition à chaque période d'horloge quelle que soit la séquence transmise. La puissance au voisinage de la fréquence zéro est nulle, ce qui est intéressant pour la transmission en bande de base. En revanche, le spectre du signal est plus étalé que celui d'un signal NRZ. Une succession de 1 en codage biphase correspond à un signal de fréquence fondamentale $2f$ pour une fréquence d'horloge f.

Principe de la transmission par transposition en fréquence

La plupart des supports de transmission, les lignes téléphoniques en particulier, ne permettent pas la transmission directe d'un signal numérique en bande de base. Ils aboutissent à des pertes de symboles au cours de la transmission. D'autre part, il est nécessaire que le spectre de fréquence des signaux émis coïncide avec la bande passante du support, afin que ces derniers ne soient pas filtrés.

On utilise alors la *transmission par transposition de fréquence* qui consiste à moduler une onde sinusoïdale porteuse de fréquence convenable par le signal à transmettre L'opération de modulation équivaut à une translation du spectre du signal dans le domaine des fréquences. Cette opération permet de centrer son énergie autour de la fréquence de la porteuse donc à l'intérieur de la bande passante du support de transmission.

Les différentes techniques de modulation utilisées en transmission numérique consistent à manipuler un ou deux des paramètres de l'onde sinusoïdale : l'amplitude, la phase, la fréquence. L'utilisation de ces techniques sur le réseau téléphonique est normalisée par l'ITU dans les recommandations de la série V.

Transmission en modulation d'amplitude

Soit une porteuse $v(t)$ de fréquence f_0. Sans limiter la généralité de la présentation, on peut considérer une phase nulle et une amplitude égale à 1 :

$v(t) = \cos(2\pi f_0 t)$

En modulation d'amplitude, l'amplitude du signal modulé varie linéairement en fonction du signal d'entrée $x(t)$:

$m(t) = (a+k\,x(t)) \cos(2\pi f_0 t)$ où $k<1$ est appelé indice de modulation.

La modulation d'amplitude présente l'inconvénient d'être sensible au bruit car la puissance du signal modulé est fonction du signal d'entrée. Le spectre du signal modulé contient une raie à la fréquence f_0 due au facteur a. Lorsqu'il est nul, cette raie disparaît : c'est la modulation avec suppression de porteuse ou modulation sans porteuse.

De plus, le spectre du signal modulé est doublé par rapport au spectre du signal d'entrée. C'est pourquoi, on l'appelle la *modulation d'amplitude à double bande (DB).* Elle n'est pas utilisée telle quelle dans les transmissions numériques mais essentiellement pour la transmission de radiodiffusion analogique (et la transmission du son de la télévision hertzienne) car la fabrication d'un récepteur est extrêmement simple.

Transmission par modulation de phase

En *modulation de phase,* le signal à transmettre est utilisé pour faire varier la phase de l'onde porteuse utilisée pour décaler le spectre de fréquence du signal à transmettre. Elle peut s'écrire sous la forme :

$m(t) = \cos(2\pi f_0 t + k\, x(t))$

Il existe deux types de codage utilisés en modulation de phase. Dans le premier type, la valeur du symbole transmis suffit pour déterminer la valeur des données transmises ; la démodulation doit alors être cohérente. Dans le second, c'est la différence entre les deux symboles consécutifs qui porte l'information ; on parle alors de modulation de phase *différentielle* ; la démodulation peut être cohérente ou non cohérente.

En cas de transmission numérique, l'ensemble des phases possibles prend valeur dans un ensemble dénombrable d'au moins deux éléments. Elle est appelée PSK, *Phase Shift Keying*.

Transmission par modulation de fréquence

En *modulation de fréquence,* le signal est obtenu en utilisant le signal à transmettre pour faire varier la fréquence de l'onde porteuse utilisée :

$m(t) = \cos(2\pi\, [f_0 + k\, x(t)]\, t + \varphi)$

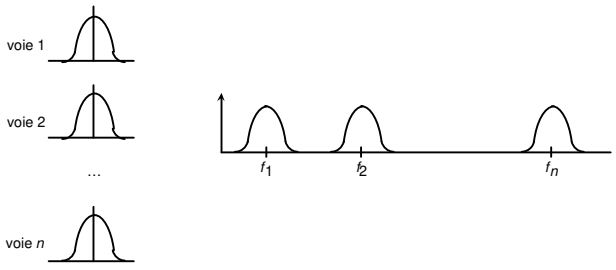
Le spectre du signal modulé en fréquence ne s'exprime pas facilement en fonction du spectre du signal à transmettre. En théorie, il est même infini. Lorsque le rapport $\Delta f/R$ vaut 1/4, une grande partie de l'énergie est concentré autour de la fréquence porteuse et il est facile d'assurer une continuité de phase. La modulation est alors appelée MSK (*Minimum Shift Keying*). Elle est fréquemment utilisée dans les systèmes radio-mobiles.

Multiplexage

Lorsque la bande passante d'un support est nettement plus large que le spectre du signal à transmettre, il est intéressant d'utiliser un même support pour transmettre parallèlement plusieurs signaux. On parle alors de *multiplexage*. Le démultiplexage consiste à reconstituer les différents signaux à partir du signal multiplexé.

Multiplexage fréquentiel

Le multiplexage fréquentiel est utilisable dans les transmissions analogiques et numériques. Il consiste à transposer les *n* signaux d'entrée en fréquence — ce qui revient à une modulation —, chacun ayant une fréquence porteuse différentes. On parle alors d'Accès Multiple à Répartition en Fréquence (AMRF) ou *Frequency Division Multiple Access* (FDMA).

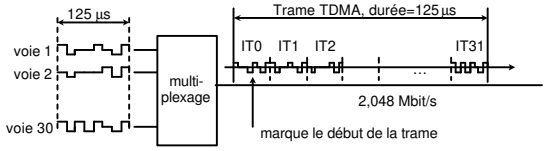


Multiplexage en fréquence

Le multiplexage fréquentiel est utilisé pour les transmissions sur fibre optique. Les opérations de multiplexage/démultiplexage peuvent se faire de manière complètement optique en jouant sur les phénomènes de réfraction qui sont fonctions des longueurs d'onde : un démultiplexeur est similaire à un prisme. On parle alors de multiplexage en longueur d'onde.

Multiplexage temporel

Le multiplexage temporel est en général utilisé dans les transmissions numériques. Il est appelé Accès Multiple à Répartition dans le Temps (AMRT) ou *Time Division Multiple Access* (TDMA).
Si on considère *n* signaux numériques : le multiplexage consiste à transmettre d'abord un ou plusieurs bits de la voie 1, puis de la voie 2 et ainsi de suite jusqu'à la voie *n* pour former une *trame TDMA* et de répéter ce cycle. Si le débit des entrées est de *b* bit/s alors le débit en sortie de la voie multiplexée est de $n \cdot b$ bit/s, ce qui signifie que le spectre de cette dernière est étalée. Pour pouvoir démultiplexer, il est nécessaire de transmettre des éléments de synchronisation afin de réaffecter correctement l'entrée à la voie correspondante.
L'AMRT est utilisé dans le réseau téléphonique pour les transmissions des communications. On parle alors de voie MIC, Modulation par Impulsions Codées. La voix humaine est numérisée sous la forme d'un signal à 64 kbit/s, 1 octet transmis toutes les 125 µs, puis codé en bande de base. En Europe, on multiplexe temporellement 30 voies. Le signal multiplexé contient 30 intervalles de temps ou IT contenant chacun une voie auxquels on rajoute un élément de synchronisation (dans l'IT 0) et un élément de signalisation (en général dans l'IT 16). On obtient donc un total de 32 IT et un débit brut de 32x64=2048 kbit/s capable de transporter 30 communications. On parle alors de MIC 30 voies (dans le langage courant, un MIC désigne en fait l'ensemble des 30 voies multiplexées temporellement).



Les voies 1 à 15 sont placées dans les IT 1 à 15 ; les voies 16 à 30 dans les IT 17 à 31.

Exemple de multiplexage temporel

Il est possible de multiplexer plusieurs voies déjà multiplexées si le support est capable de transmettre des débits plus élevés. Dans le cadre du réseau téléphonique, différents niveaux de multiplexage sont définis, en multiple de 2,048 Mbit/s, produisant ce qu'on appelle une *hiérarchie de multiplexage*.
Le multiplexage de *n* signaux, occupant chacun une largeur de bande *B*, génère un signal de largeur supérieure ou égale à $n \cdot B$, pour le multiplexage fréquentiel comme pour le multiplexage temporel. Il n'y a aucune économie faite sur la bande consommée mais seulement économie sur l'aspect matériel (un seul support au lieu de *n*).

Synthèse

Pour relier deux " équipements " informatiques distants l'un de l'autre, on utilise :
– un *support de transmission* pour franchir la distance séparant les équipements, ce support est loin d'être parfait ;
– des " modems " ou des " codeurs " qui ont pour rôle de fabriquer les meilleurs signaux adaptés à la nature du support de transmission, on constitue ainsi un *circuit de données*.
Les supports de transmission sont de nature très différente les uns des autres : paires métalliques, câbles coaxiaux, fibre optique, éther. Ils sont caractérisés par leur *bande passante* qui limite le débit maximal auquel on peut transmettre et le *taux d'erreur* qu'ils introduisent sur les signaux transportés. Les *techniques de transmission* (en bande de base ou par transposition de fréquence) ont pour objet d'adapter au mieux les signaux aux caractéristiques de ces supports. Elles sont normalisées au niveau international et mises en œuvre dans un *" modem "*. Ce dernier est relié aux équipements informatiques par une *interface* elle-même normalisée. La plus classique est V24, alias RS 232C.

Exercices

Exercice 1

Soit la suite d'éléments binaires 0 1 1 1 1 1 1 0.

Représenter les signaux transmis lorsqu'on transmet en bande de base avec les codes NRZ, code biphase et bipolaire. Citer des exemples d'application de ce type de transmission.
Représenter les signaux transmis lorsqu'on transmet en transposition de fréquence avec une modulation d'amplitude à deux niveaux, une modulation de phase à deux niveaux, une modulation de fréquence à deux niveaux. Si le débit D est donné, quelle est la rapidité de modulation ? Citer des exemples d'application de ce type de transmission.
Représenter les signaux transmis lorsqu'on transmet en transposition de fréquence avec une modulation d'amplitude à quatre niveaux, une modulation de fréquence à quatre niveaux. Si le débit D est donné, quelle est la rapidité de modulation ? Citer des exemples d'application de ce type de transmission.

Exercice 2

Exprimer et comparer les valeurs du débit binaire et de la rapidité de modulation du modem V23 (1200 bit/s avec une modulation de fréquence (FSK) à deux niveaux) et du modem V29 (9600 bit/s avec une modulation combinée d'amplitude à deux niveaux et de phase à huit niveaux).

Exercice 3

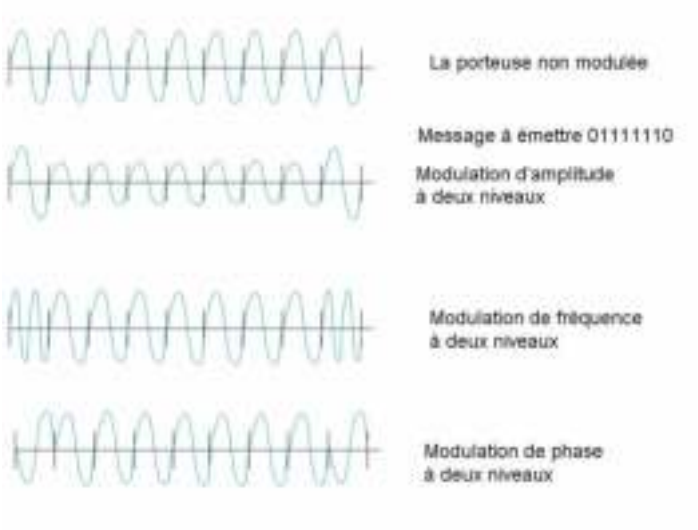
Dans le réseau Télex, on utilisait une transmission asynchrone avec un alphabet qui contient 5 bits par caractère. Comment pouvait-on coder les lettres de notre alphabet, les chiffres et les autres symboles (ponctuation, par exemple) qui constituent cette page ?

Exercice 4

Un terminal est relié à un ordinateur par une liaison asynchrone. La transmission utilise 7 bits de données, 1 bit de START et 2 bits de STOP. Chaque frappe sur une touche du clavier provoque l'émission du caractère correspondant codé en ASCII. Représenter le signal obtenu lorsqu'on appuie sur la touche H.

Quelques corrigés

Exercice 1



Exercice 2

Le modem V23 est le "vieux" modem que l'on trouve dans le Minitel : débit = 1200 bit/s, modulation de fréquence simple, rapidité de modulation = 1200 bauds, c-à-d un intervalle de temps (=1/1200 seconde) transporte 1 bit
Le modem V29 utilise dans le même intervalle une modulation d'amplitude à 2 niveaux et modulation de phase à 8 niveaux

exemple
il y a deux amplitudes A1 et A2
il y a huit phases P1, P2, P3, P4 P5, P6, P7, P8
un intervalle de temps utilise une amplitude et une phase donc une valeur significative parmi les 16 possibles
les informations à transmettre sont groupées par 4 :
0000 ==> A1 et P1
0001 ==> A1 et P2
0010 ==> A1 et P3
0011 ==> A1 et P4
0100 ==> A1 et P5
0101 ==> A1 et P6
0110 ==> A1 et P7
0111 ==> A1 et P8
1000 ==> A2 et P1
1001 ==> A2 et P2
1010 ==> A2 et P3
et ainsi de suite

Comme le débit est de 9600 bit/s, l'intervalle de temps est de 4/9600 s soit 1/2400 s et la rapidité de modulation de 9600/4 = 2400 bauds

Les protocoles de liaison de données

Généralités sur les protocoles de liaison de données

Un *protocole* est un ensemble de règles à respecter pour échanger des données dans de bonnes conditions entre deux équipements. Un protocole *de liaison de données* a pour objet de rendre fiable le circuit de données qui peut altérer les informations transportées.
Un protocole de liaison de données fournit un service spécifique supplémentaire par rapport au circuit de données : principalement la fiabilisation de la transmission. L'implantation d'un protocole sur un équipement peut être vu comme la réalisation d'un ensemble de procédures informatiques : celles-ci acceptent les données que veut transmettre l'utilisateur, prennent totalement en charge la transmission puis avertissent l'utilisateur lorsque la transmission est effectuée. En réception, ces mêmes procédures transfèrent à l'utilisateur les données reçues et signifient à l'émetteur que la réception s'est bien déroulée. Cet ensemble de procédures est désigné sous le terme général d'*entité.* Ici, il s'agit d'une *entité de liaison de données* offrant un service de transmission fiable sur un circuit de données. L'utilisateur du service peut être un autre logiciel ou un opérateur humain.

Rôles et fonctions d'un protocole de liaison de données

Alors que le circuit de données est capable de transmettre des éléments binaires, les protocoles de liaison de données travaillent sur des blocs d'éléments binaires appelés *trames*. La trame est l'unité de base que gère le protocole de liaison de données.
La trame transporte les données de l'utilisateur mais elle contient aussi des informations de contrôle qui sont nécessaires au protocole pour le bon déroulement du dialogue. Certaines trames sont d'ailleurs réduites à ces seules informations de contrôle. Dans une trame, on définit différents champs. Un *champ* est un bloc d'éléments binaires dont la signification est précisée dans la définition du protocole. En général, chaque champ est défini par sa place dans la trame.
Il faut ensuite définir les règles de dialogue. Le circuit de données introduisant des perturbations, il faut pouvoir détecter les erreurs. Ceci est réalisé en introduisant une redondance dans la transmission et en vérifiant à la réception que cette redondance est conservée. Si des erreurs arrivent, il est nécessaire de spécifier des procédures de correction des erreurs détectées. Enfin, il est utile de détecter les pannes d'équipement et les ruptures complètes de liaison pour avertir l'utilisateur de l'indisponibilité du service.
Définir un protocole de liaison de données consiste donc à préciser :

– le format des trames,
– le critère de début et de fin de trames,
– la place et la signification des différents champs dans une trame,
– la technique de détection d'erreur utilisée,
– les règles de dialogue : les procédures après détection d'erreur ou de panne et la supervision de la liaison.

Mise en forme des données

En théorie, le critère de début et de fin de trame est indépendant de la technique de transmission utilisée. En pratique, cela est faux car certains procédés utilisent des particularités du codage en ligne pour délimiter les trames. Les solutions les plus fréquentes sont la délimitation par un séquence binaire spéciale ou l'indication directe de la longueur de la trame.

• Délimitation par séquence binaire

Les trames sont des blocs composés d'un nombre quelconque de bits et on parle de *protocole orienté bit.* Une séquence spécifique de bits sert à délimiter les trames, elle est souvent appelée *fanion (flag).* Un mécanisme de transparence rend la transmission indépendante du codage utilisé.
En général, la suite d'éléments binaires 01111110 est utilisée comme fanion. Un mécanisme de transparence est nécessaire pour éviter l'apparition de la séquence du fanion à l'intérieur de la trame. Il consiste, en émission, à insérer dans le corps de la trame un élément binaire de valeur 0 après avoir rencontré 5 éléments binaires consécutifs de valeur 1. En réception, il faut donc supprimer un élément

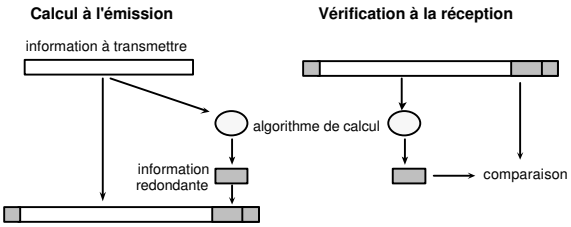
binaire de valeur 0 après avoir rencontré 5 éléments binaires consécutifs de valeur 1. Avec un tel mécanisme, on interdit donc l'émission de plus de 5 éléments binaires de valeur 1 sauf pour la délimitation de trames.
Cette méthode a l'avantage de permettre la transmission de trames de longueur variable, sans limitation, mais elle introduit des variations sur la durée de transmission des données utilisateur : cette durée dépend très légèrement de la valeur des données transmises et pas seulement de la taille de celles-ci.
Trame contenant les données utiles suivantes : 0110 1111 1110 1001.
La trame réellement émise est la suivante : *01111110* 0110 1111 1**0**110 1001 *01111110*
où les fanions sont marqués en italique et le bit inséré est souligné en gras.

• Délimitation par transmission de la longueur

Une autre méthode consiste à indiquer dans un champ particulier le nombre d'octets contenus dans la trame. On peut utiliser une séquence particulière pour indiquer le début de la trame. Ensuite, un octet (ou éventuellement plusieurs), dont la place est fixée dans la définition du protocole par rapport au début de trame, indique la longueur de la trame. Cette longueur est généralement exprimée en octets mais pourrait l'être en bits ou en nombre de mots de 16, 32... bits.
Ce procédé induit une limitation dans la taille de la trame. Si la longueur est exprimée en octets et codée sur un octet, on est limité à des trames de 256 octets. Elle a l'avantage d'éviter les problèmes de transparence : le récepteur n'interprète en aucun cas les données reçues comme des délimiteurs. Il ne se met en attente d'une séquence de début de trame qu'à la fin de réception d'une trame. En revanche, elle est sensible à des erreurs de transmission : si le champ de longueur est mal reçu, le récepteur risque de perdre son cadrage par rapport à l'émetteur. Pour remédier à ce problème, certains protocoles introduisent alors une protection supplémentaire sur les champs de contrôle.
Cette méthode revient en force sur les liaisons de radiotéléphonie. La trame est ajustée à une longueur fixe par ajout d'éléments binaires de bourrage. Un champ précise la longueur utile.

Principe du contrôle de validité de l'information

Pour contrôler la validité de l'information transmise, on adjoint à celle-ci une *redondance* calculée avec un algorithme spécifié dans le protocole. A la réception, le même algorithme est appliqué pour vérifier que la redondance est cohérente : s'il y a cohérence, on considère qu'il n'y a pas eu d'erreur de transmission et on traite l'information reçue ; s'il n'y a pas cohérence, on est certain que l'information est invalide et on ne la traite pas.



Principe général de la détection d'erreurs

Il est toujours possible qu'une erreur de transmission apparaisse et que la cohérence par malchance reste vraie : on est alors dans le cas d'une erreur résiduelle. Le contrôle aura pour objet de minimiser le taux d'erreurs résiduelles.
Il est également possible que l'erreur se produise uniquement sur la redondance et non sur l'information mais le récepteur n'a aucun moyen de le détecter : l'information reçue est déclarée non valide et n'est donc pas traitée.

Méthode de contrôle de la validité : protection au niveau du code

Une protection au niveau du code consiste à organiser une redondance interne au code où quelques-unes des combinaisons binaires possibles sont retenues comme valides. Ce type de protection est donc lié au codage. Une protection au niveau du caractère est possible lorsque l'émission des données se fait par

caractère : on introduit une redondance à chaque caractère transmis. Par exemple, on rajoute à chaque caractère un *bit de parité* ; on parle alors de *parité longitudinale LRC* (*Longitudinal Redundancy Checking*). Pour chaque caractère, on fait la somme des bits représentant ce caractère. En cas de parité dite paire, si cette somme est paire, on rajoute un 0 à la fin du caractère, si elle est impaire on rajoute un 1. La séquence binaire obtenue, appelée *mot de code,* est ainsi toujours paire. A la réception, il suffit de vérifier cette parité pour considérer ou non le mot comme valide.
Le contrôle de validité par parité longitudinale est fréquemment utilisé avec le code CCITT n° 5 sur les liaisons asynchrones. Par exemple, le caractère M est codé par 1001101, le bit de parité est donc 0. On transmettra dans cet ordre le mot de code 10110010 (7 bits en commençant par les poids faibles puis parité). L'inconvénient général aux contrôles par parité est que les erreurs doubles ne sont pas détectées.

Méthode de contrôle de la validité : protection au niveau de la trame

La protection au niveau des trames est la plus classique : une redondance est rajoutée à chaque trame en fonction de l'ensemble des éléments binaires qui la constituent. Plusieurs techniques sont utilisables, nous verrons ici la parité transversale et le contrôle polynomial.

• Contrôle de parité transversale

On forme un mot de contrôle en faisant la somme modulo 2 des bits de même rang. On parle alors de *parité verticale* (VRC, Vertical Redundancy Checking).
On associe souvent la parité longitudinale et la parité verticale (VRC + LRC). A chaque caractère, on rajoute un bit de parité (LRC) et un caractère de VRC comportant également un bit de parité. Cette double parité permet d'améliorer la détection d'erreurs.

Exemple
Soit la suite de caractères L, 2, M à transmettre. Elle est codée en CCITT n°5 par les valeurs 4C, 32 et 4D. En parité paire, les bits de parité pour chaque caractère sont respectivement 1, 1 et 0. Le caractère de parité vertical est calculé suivant le tableau ci-dessous :
1 1 0 0 1 1 0 0 caractère L + parité LRC
1 0 1 1 0 0 1 0 caractère 2 + parité LRC
0 1 0 0 1 1 0 1 caractère M + parité LRC
0 0 1 1 0 0 1 1 caractère du VRC
La suite des éléments binaires émise est donc 0011 0011 0100 1101 1011 0010 1100 1100 si on transmet en commençant par les poids faibles.

• Contrôle polynomial

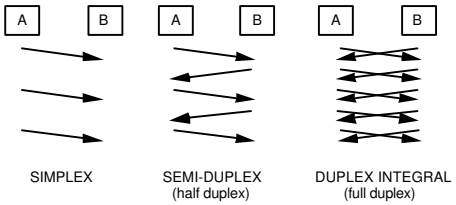
Le *contrôle polynomial* est très utilisé dans les protocoles modernes car il permet de détecter les erreurs sur plusieurs bits. Il est appelé couramment (par abus de langage…) *contrôle cyclique* (CRC, *Cyclic Redundancy Checking*). Le propos de ce paragraphe n'est pas d'en faire la théorie mais d'en décrire le processus.
On considère la trame à transmettre comme un groupe de bits. On lui fait correspondre un polynôme $P(x)$ tel que le coefficient de degré i correspond à la valeur du $i^{ème}$ bit. Les algorithmes de calcul se font modulo 2 sur les polynômes. [par exemple, $(x^7 + x^3) + (x^3 + x) = x^7 + x$].
On choisit un polynôme $G(x)$ de degré r, appelé *polynôme générateur.* Ce polynôme est caractéristique du contrôle. A l'émission, on multiplie $P(x)$ par x^r et on divise le polynôme obtenu par $G(x)$ (division euclidienne). On obtient un reste de degré inférieur strictement à r noté $R(x)$:
$x^r . P(x) = G(x).Q(x) + R(x)$. (1)
On transmet le polynôme $T(x)$ constitué à partir de $P(x)$ et du reste $R(x)$ défini par l'équation (2) :
$T(x) = x^r . P(x) + R(x)$. (2)
D'après les équations (2) et (1) et du fait des calculs modulo 2, ce polynôme vérifie :
$T(x) = G(x).Q(x)$, il est donc divisible par $G(x)$.
Le circuit de données peut modifier l'information. Soit $E(x)$ le polynôme associé aux erreurs apportées par le circuit. Les données reçues ont pour polynôme associé $S(x)$, lequel est défini par $S(x) = T(x) + E(x)$.
A la réception, on divise $S(x)$ par $G(x)$ et on obtient un reste $R_1(x)$ qui vérifie l'équation suivante :
$S(x) = G(x).Q_1(x) + R_1(x)$.

Si $R_1(x)$ est nul, on considère que $E(x)$ est nul et que l'information reçue correspond à celle émise. Si $R_1(x)$ est non nul, le polynôme $E(x)$ n'est donc pas nul : le circuit de données a introduit une ou plusieurs erreurs et l'information reçue n'est pas prise en compte.

Exemple
L'information 1000001110000100 est associée à $P(x) = x^{15} + x^9 + x^8 + x^7 + x^2$.
Soit le polynôme générateur de degré 12 : $G(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$.
La division de x^{12} .$P(x)$ par $G(x)$ donne : $R(x) = x^{11} + x^9 + x^8 + x^7 + x^6 + x^4 + 1$.
On transmet : 1 0 0 0 0 0 1 1 1 0 0 0 0 1 0 0 1 0 1 1 1 1 0 1 0 0 0 1.
x^{12} . $P(x)$ $R(x)$
A la réception, on vérifie que le reste de la division par $G(x)$ est nul.

Modes d'exploitation de la liaison

Le *mode d'exploitation* peut être simplex, semi-duplex, duplex intégral. Dans le mode *simplex,* l'échange de données se fait dans un seul sens. En *semi-duplex* (*half-duplex).* il se fait dans les deux sens mais alternativement : les deux stations ne transmettent jamais simultanément. En *duplex intégral* (*full-duplex),* les stations peuvent transmettre simultanément sans aucune contrainte.



Mode d'exploitation de la liaison

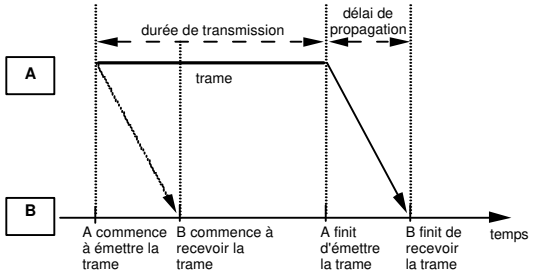
Il est à noter que le mode d'exploitation peut être différent des caractéristiques du circuit : on peut par exemple exploiter une liaison en semi-duplex alors que le circuit permet des transmissions en duplex intégral.

Du protocole utopique au protocole à fenêtre

En considérant un exemple simple de dialogue entre deux équipements, nous introduisons les différents types de protocoles de liaisons de données.

Représentation des échanges

Le temps s'écoule suivant un axe horizontal. La transmission d'une trame est schématisée par un trait gras. La longueur du trait représente donc la durée d'émission de la trame. La propagation est schématisée par une flèche légèrement inclinée par rapport à une verticale. L'instant d'arrivée de la seconde flèche au destinataire représente donc l'instant où la trame est totalement reçue. Lorsqu'une trame est mal reçue par le récepteur, la transmission est représentée par un trait pointillé sans flèche.



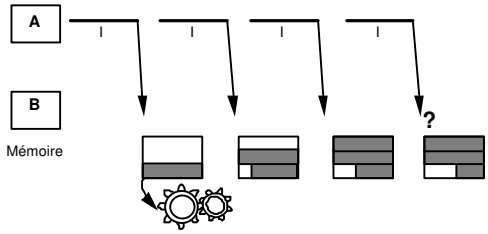
Représentation des échanges

Les temporisations sont symbolisées par un sablier, le traitement des informations par un petit engrenage et la non prise en compte des informations par le récepteur par une poubelle !

Contrôle de flux

Considérons deux équipements A et B reliés via un circuit de données parfait. A veut envoyer des données à B.

L'équipement A découpe les données en trames et transmet les trames les unes à la suite des autres. Ces trames sont appelées *trames d'information* et sont notées par la lettre I. Elles respectent un certain format permettant de déterminer le début des données utilisateurs, la fin de la trame et le type de trame. Le circuit étant parfait, toutes les données sont délivrées sans erreur à B qui les stocke pour les exploiter.



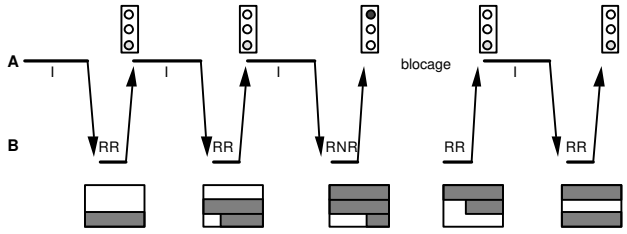
Exemple d'une transmission sans contrôle de flux

Supposons que A soit un calculateur et B une imprimante lente avec une capacité mémoire limitée. L'imprimante B doit garder en mémoire toutes les informations envoyées par A tant qu'elles ne sont pas imprimées. Mais le rythme d'envoi des informations est bien supérieur au rythme d'impression : il y a donc rapidement saturation de la mémoire de B et perte d'information par B qui n'a plus moyen de les stocker.

Il faut donc mettre en place un mécanisme pour contrôler le rythme d'envoi des informations. Ce mécanisme s'appelle le *contrôle de flux.*

Pour réaliser ce contrôle de flux, on introduit deux trames, dites de *supervision*, RR (*Receiver Ready*) et RNR (*Receiver Not Ready*). Ces trames ne transportent aucune information utile. Elles sont générées et exploitées seulement par le protocole de liaison de données pour la gestion du dialogue : elles sont donc invisibles pour un utilisateur.

Le mécanisme est le suivant : à chaque réception de trame, la station B envoie une trame RR si elle est prête à accepter d'autres trames et une trame RNR si elle ne peut plus en recevoir de nouvelles. Dans ce dernier cas, B envoie RR dès qu'elle est à nouveau prête à accepter des trames.

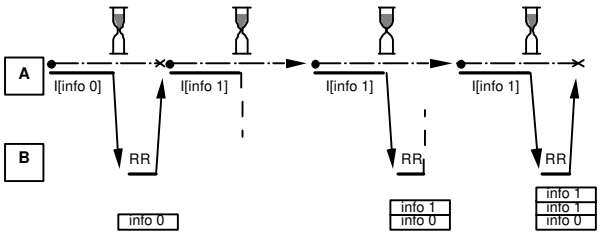


Mécanisme du contrôle de flux

Il existe des variantes de ce mécanisme : la station B peut s'abstenir d'envoyer des trames RR dans le cas général. Lorsque la mémoire disponible descend au-dessous d'un certain seuil, elle génère une ou plusieurs trames RNR suivies de trames RR lorsqu'une partie de la mémoire est libérée. A contrario, il est possible de transmettre en continu des trames RR quand la station B a de la mémoire disponible (quelle que soit l'action de la station A) et des trames RNR quand la mémoire est pleine. Un tel processus est couramment utilisé pour les liaisons entre micro-ordinateur et imprimante. Les trames sont alors réduites à un seul caractère, RNR est codée par le caractère XOFF (Contrôle-S) et RR par XON (Contrôle-Q).

Gestion d'acquittement

Supposons maintenant que le circuit ne soit pas totalement fiable et introduise des erreurs. Un mécanisme de détection d'erreur comme décrit précédemment est implanté dans les stations. Il faut ajouter un processus d'*acquittement.* Plusieurs options sont possibles, par exemple :
– lorsqu'une trame est bien reçue, la station réceptrice envoie une trame d'acquittement et ne fait rien en cas de mauvaise réception,
– lorsqu'une trame est mal reçue, la station réceptrice envoie une *demande de retransmission* à l'émetteur et ne fait rien en cas de bonne réception.
Dans la deuxième stratégie, l'absence de réponse est considérée comme un acquittement : à chaque trame, la station émettrice lance une *temporisation* correspondant à l'attente maximale d'une demande de retransmission. Si elle reçoit une telle demande, elle répète la dernière trame ; dans le cas contraire, à échéance de la temporisation, elle considère que la transmission s'est bien effectuée. Cette stratégie est peu fiable — la demande de retransmission peut elle-même être mal transmise — et peu efficace — elle provoque une attente systématique en cas de bonne transmission.
On utilise donc, le plus souvent, une stratégie d'acquittement positif à l'aide des trames de supervision précédentes (RR et RNR). Le fonctionnement de la station B devient le suivant :
– si la station B reçoit une trame correcte alors elle renvoie un acquittement à l'aide de la trame RR ou RNR suivant l'état de sa mémoire (on garde le mécanisme de contrôle de flux),
– si elle reçoit une trame erronée, elle ne mémorise pas la trame et ne renvoie aucune trame. A fortiori, si la station B ne reçoit pas une trame émise par A, elle ne réagit pas et ne renvoie rien !
Le fonctionnement de la station A est le suivant : à l'émission de chaque trame, A lance une temporisation correspondant à l'attente maximale d'un acquittement de B. Dès que A reçoit un acquittement, elle arrête la temporisation et émet la trame suivante. En cas de non réponse de B à l'échéance de cette temporisation ou en cas de réponse brouillée, A émet la trame à nouveau et réitère le processus précédent. Le nombre de répétitions autorisées est limité. Au-delà d'un certain seuil, on considère qu'un incident grave s'est produit (rupture totale de la liaison, panne de la station B, panne d'un élément de transmission sur A ou B...). Il faut avertir l'utilisateur que la liaison est rompue.
Ce protocole n'est pas encore satisfaisant. En effet, le circuit de transmission peut corrompre les trames émises par A et aussi les trames émises par B.



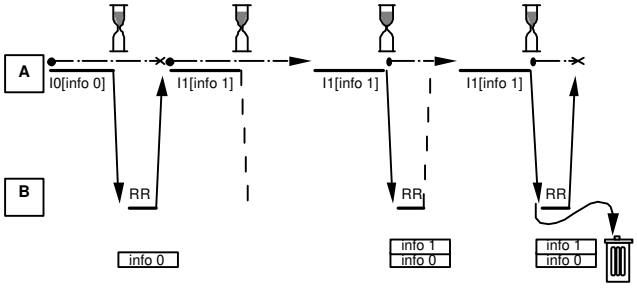
I[info 0] signifie que la trame I transporte l'information " info 0 ".
Dans cet exemple l'" info 1 " est dupliqué.

Protocole avec acquittement simple

Supposons que A envoie une trame contenant l'information 1, vers B. Cette trame est bien reçue par B qui émet en réponse une trame d'acquittement RR mais cette trame RR est mal transmise. La station A ne la détecte pas et va réémettre sa trame d'information : cette dernière va donc être dupliquée dans B. La station B n'a aucun moyen de détecter cette duplication. En aucun cas, elle ne doit analyser le contenu de l'information pour détecter une duplication : A peut très bien décider de transférer deux fois de suite la même information. Le protocole de liaison de données doit être *complètement indépendant du contenu* des trames transférées.
Il faut donc introduire un mécanisme supplémentaire pour distinguer deux trames successives différentes : un champ supplémentaire de *numérotation* ou d'*indication de retransmission* est introduit dans la trame.

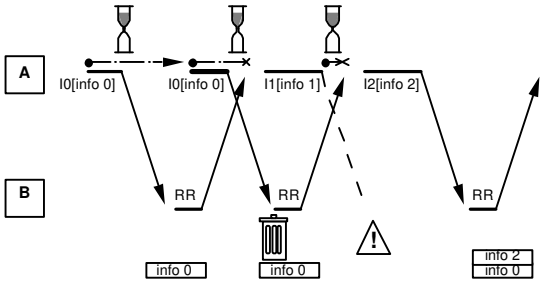
Numérotation des trames

Chaque trame d'information est numérotée par le protocole. Cette numérotation est placée dans un en-tête tout comme le type de trame. Deux trames correspondant à des numéros différents sont considérées comme transportant deux données de l'utilisateur distinctes. Cet en-tête est utilisé par le protocole du récepteur pour vérification, puis l'information contenue dans la trame est délivrée à l'utilisateur.
La variable donnant le numéro de la trame est appelée *N*(S) (S pour *send*). Cette variable est codée sur quelques bits ; elle est prise modulo *M* où *M* est un entier, en général de valeur 2 (valeur minimale pour distinguer deux trames successives différentes), 8 ou 128.
L'introduction de numéros dans les trames impose des compteurs dans chaque station et une initialisation du dialogue pour que les deux stations se mettent d'accord sur les valeurs initiales des compteurs. On a alors un protocole dit *orienté connexion*.
Le processus fonctionne de la façon suivante. A possède un compteur interne donnant le numéro de la trame à émettre :
– pour toute nouvelle émission, A émet la trame en plaçant la valeur du compteur dans l'en-tête, puis incrémente ce compteur,
– pour toute répétition, A émet la trame sans modification du numéro.



Protocole à numérotation de trames

Sur réception d'une trame, B teste la valeur du compteur de la trame : si elle est égale à la valeur de la trame précédente, la trame est dupliquée et B l'ignore. Il envoie cependant une trame de supervision pour acquitter la trame reçue.
Ce mécanisme possède une grosse faiblesse. La valeur de la temporisation est un paramètre critique dont un mauvais choix peut entraîner un dysfonctionnement du protocole.

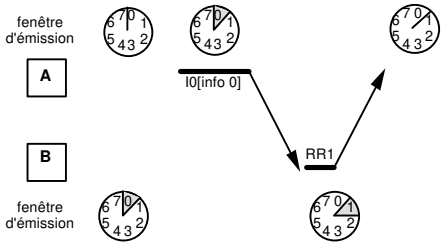


Exemple de mauvais fonctionnement en cas de numérotation des trames

Considérons le scénario où la station A envoie une trame I_0 qui est bien reçue par B. La station B l'acquitte mais l'acquittement arrive après l'expiration de la temporisation de A. Celle-ci émet donc à nouveau la trame I_0. Lorsque A reçoit l'acquittement de sa première trame I_0, il croit qu'il s'agit d'un acquittement pour la dernière trame émise. Il émet donc la trame suivante I_1. Puis il reçoit l'acquittement de la deuxième trame I_0 qu'il interprète comme un acquittement de la trame I_1. Si, par malheur, cette trame est mal transmise, elle va manquer à B car A croit qu'elle est acquittée alors qu'en réalité elle n'a pas été reçue par B.
On est donc obligé de préciser dans une trame d'acquittement quelle trame d'information elle acquitte.

Protocole à fenêtre

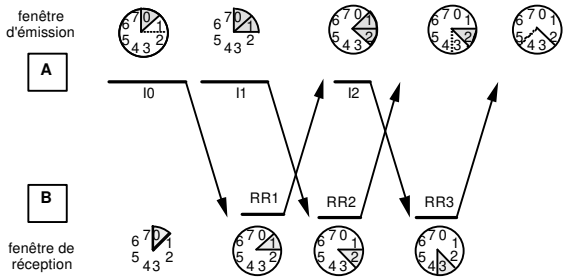
Afin d'augmenter l'efficacité du dialogue, on introduit la notion d'*anticipation,* c'est-à-dire la possibilité d'émettre plusieurs trames à la suite sans avoir réception d'acquittement. De même, une trame de supervision pourra acquitter non plus une seule trame mais un ensemble de trames.
Le nombre de trames successives qu'on peut émettre sans réception d'acquittement est limité par une valeur notée *k*. Considérons une numérotation des trames modulo 8. Intuitivement, on perçoit que la valeur maximale de *k* est au plus de 8. Nous montrerons qu'elle est en fait de 7.



Représentation des fenêtres d'émission et de réception

Adoptons une représentation circulaire des trames en attente d'acquittement. On représente sur un disque l'ensemble des trames distinguées par leur numéro. Chaque trame occupe donc une part du disque. Un trait gras représente la valeur du compteur interne de A donnant le prochain numéro de trame que la station A va émettre. A l'instant initial, A est au repos. Dès qu'elle démarre l'émission de la trame 0, cette trame est considérée comme émise et elle est non acquittée : on grise la portion 0 du disque. Si A émet plusieurs trames successives, on grise l'ensemble des trames en attente d'acquittement. Lorsqu'un

acquittement est reçu, les portions correspondant aux trames acquittées sont blanchies. L'ensemble des portions grisées représente l'état de la *fenêtre d'émission.*
On représente également par un disque l'état du récepteur en noircissant les numéros que B s'attend à recevoir. A l'initialisation, B s'attend à recevoir une trame numérotée 0 : la case 0 est grisée. Lorsque cette trame est bien reçue, B se met en attente de la trame 1 et la case 1 est par conséquent grisée à son tour.
Le fonctionnement, dans les cas exempts d'erreur de transmission, est le suivant : quand la station B reçoit une trame, elle enregistre le numéro *N*(S) de cette trame, l'incrémente de 1, le mémorise puis le place dans une trame de supervision qu'elle renvoie à A. La station A émet ses trames successivement jusqu'à ce qu'elle n'ait plus de trames à transmettre ou jusqu'à ce que le nombre de trames autorisées sans réception d'acquittement soit atteint. Elle lance une temporisation à l'émission de la première trame.
On remarque que ce protocole suppose des équipements " duplex-intégral " car les acquittements sont reçus pendant le cours des émissions de A.



Lorsque A a émis les trames I_0 et I_1, sa fenêtre est fermée. Elle attend la réception d'un acquittement pour pouvoir émettre la trame I_2.

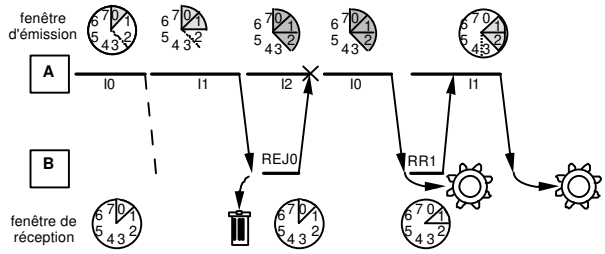
Scénario pour un protocole à fenêtre d'anticipation de largeur 2

Déterminons, par un exemple, la taille maximale de la fenêtre d'anticipation lorsque les trames sont numérotées sur 3 bits (donc de 0 à 7). Considérons les deux scénarios suivants.
Scénario 1) la station A transmet une trame numérotée 0 qui est acquittée par la station B. L'acquittement n'est pas bien reçu par A qui émet à nouveau la trame 0 à l'expiration de la temporisation de garde.
Scénario 2) la station A transmet une trame numérotée 0 qui est acquittée par la station B à l'aide d'un message RR 1 puis 8 trames successives (trames 1 à 7 puis trame 0) dont les 7 premières ne sont pas reçues par B.
Pour la station B, les deux scénarios se caractérisent par la réception de deux trames successives portant l'indice 0 mais dans le scénario 2 il s'agit d'une trame différente de la précédente. Il est donc nécessaire de limiter l'anticipation à 7 trames pour éviter toute confusion.
De façon générale, si les trames sont numérotées de 0 à *n*, la taille maximale de la fenêtre est de *n*. Graphiquement, il doit toujours y avoir une part du disque non grisée.

Protocole Go-back-N

Quand une trame reçue est erronée, elle n'est pas prise en compte. Le récepteur fait comme s'il n'avait rien reçu : une erreur n'est détectée que **si une trame suivante est correctement reçue** parce que son numéro n'est pas celui attendu.
L'émetteur retransmet soit toutes les trames depuis la trame mal transmise, soit seulement la trame qui a été erronée. La première stratégie s'appelle le *Go-back-N* (retour au *n* ième) alors que la seconde porte le nom de *rejet sélectif* ou Selective Reject. Pour demander la retransmission des trames suivant la trame erronée (comprise), une nouvelle trame de contrôle appelée REJ, *Reject*, est nécessaire.
Le *Go-back-N* est illustré par le scénario suivant : A envoie la trame 0, mal reçue, suivie de la trame 1, bien reçue. A la réception de la trame 1, B constate une rupture de séquencement c'est-à-dire qu'il reçoit la trame 1 sans avoir reçu de trame 0, il ne mémorise pas la trame 1 et envoie un rejet REJ avec le numéro

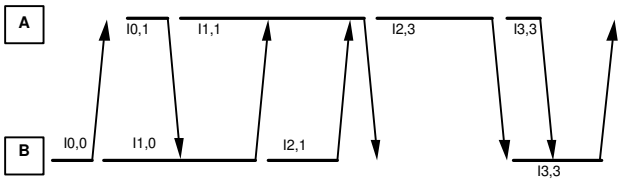
0 demandant à A de reprendre l'émission à partir de la trame 0. La station A, recevant la trame REJ, interrompt éventuellement l'émission en cours et reprend le processus d'émission comme demandé.



Scénario d'un protocole Go-back-N

Le " piggy-backing "

Considérons des échanges bidirectionnels. On peut entrelacer dans le temps les scénarios précédents : pour transmettre des données, la station A envoie des trames d'information numérotées et pour acquitter elle envoie des trames de supervision RR, RNR ou REJ dont les numéros correspondent aux trames envoyées par B. Un tel mécanisme n'est pas très efficace. On convient donc d'utiliser les trames I à la fois comme des trames d'information classiques et comme trames RR.
Chaque trame I possède donc deux numéros : un numéro *N*(S), véritable numéro de la trame I, et un numéro *N*(R) acquittant les trames émises dans le sens opposé. Ce mécanisme est appelé *piggy-backing* la trame I portant (sur son dos) l'acquittement RR. Notons que les trames RNR ou REJ sont toujours transportées explicitement. Enfin, lorsqu'une station n'a pas de trame I à transmettre, elle peut toujours utiliser explicitement des trames RR pour acquitter le trafic qu'elle reçoit.



Une trame I*N*(S),*N*(R) a comme signification I*N*(S) et RR*N*(R).
La fenêtre d'anticipation à l'émission est de taille au moins 3 dans cet exemple.

Scénario d'un protocole duplex avec piggy-backing

Description du protocole HDLC

En conclusion, un protocole de liaison de données peut offrir plusieurs services suivant la qualité de la transmission :
– service sans acquittement ni connexion ni contrôle de flux lorsqu'il est nécessaire d'avoir un protocole très simple ou lorsque le support de transmission est d'excellente qualité,
– service avec acquittement mais sans connexion ni contrôle de flux qui permet de fiabiliser un peu la liaison mais n'offre pas de garantie de non duplication des messages,
– service avec acquittement, connexion et contrôle de flux qui comporte donc une numérotation des trames et des acquittements. Ce dernier service est le seul à offrir une réelle garantie de fiabilité, mais il est plus complexe à implanter. Plusieurs stratégies peuvent être distinguées dans la gestion des acquittements : le *Stop-and-Wait*, le *Go-back-N* et le *Selective Reject*. Le *Go-back-N* est le plus utilisé. Le *Stop-and-Wait* est peu efficace tandis que le *Selective Reject* est trop complexe à implanter, sans gain flagrant dans la majorité des cas.
De multiples protocoles de liaison de données ont été développés. Nous nous contenterons ici de la présentation détaillée d'un seul protocole : HDLC, recommandation internationale.

HDLC (High level Dta Link Control) repose sur la transmission synchrone orientée bit. Elle met en œuvre un mécanisme de transparence par fanion identique à celui décrit au début du chapitre qui rend le protocole totalement indépendant du codage des données transportées : HDLC peut transporter des informations utilisant des codes de longueur variable.
Sa variante la plus connue est de type *Go-back-N* avec un mécanisme de contrôle de flux. Il est équilibré ou symétrique : les deux stations ont les mêmes prérogatives. Il utilise des moyens de transmission duplex intégral sur une liaison point à point exploitée en full-duplex ; il possède en outre un mode half-duplex.

Structure de la trame

Toutes les informations sont transportées dans une structure unique : la *trame*. Celle-ci est de longueur variable ; elle est délimitée par une séquence binaire spécifique appelée *flag* ou fanion. Le même fanion est utilisé pour marquer le début et la fin d'une trame. En cas d'émission consécutive de trames, le fanion marque la fin d'une trame et le début de la suivante. Les différents champs sont décrits ci-après dans l'ordre d'émission.
Le champ *Address* s'étend sur un octet et identifie une des extrémités de la liaison.
Le champ *Control* décrit le type de la trame : il s'étend sur 1 octet mais peut être porté à 2 octets dans le mode appelé *mode étendu.*
Le champ *Information* est un champ facultatif contenant un nombre quelconque d'éléments binaires représentant les données de l'utilisateur.
Le champ *FCS* (Frame Check Sequence) est une séquence de contrôle de trame (elle est obtenue par un contrôle polynomial de polynôme générateur $x^{16} + x^{12} + x^5 + 1$).

Flag	Address	Control	Information	FCS	Flag
01111110	8 bits	8 bits	*N* bits	16 bits	01111110

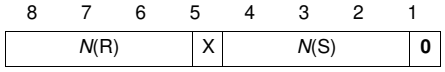
Le champ de gauche est le premier transmis, le champ de droite est le dernier.

Format de base des trames

Les bits sont émis en transmission synchrone en commençant par les poids faibles : bit 1 à bit 8 de chaque champ. Le mécanisme de transparence décrit précédemment est mis en œuvre (insertion d'un bit 0 après 5 bits consécutifs à 1, dans le corps de la trame). La transmission d'éléments binaires est continue ; en l'absence d'émission spécifique, les équipements émettent des fanions consécutifs.

Types de trame

Il existe trois types de trames qui sont identifiés par le champ *Control*. La trame d'information ou trame I permet la transmission de données de l'utilisateur. Les trames de supervision ou trames S permettent l'acquittement et le contrôle de flux. Elles ne transportent pas de données. Les trames non numérotées ou trames U (*Unnumbered*) sont utilisées pour toutes les fonctions de contrôle de la liaison telles que l'initialisation, la libération... Elles ne transportent pas de données.
La trame I permet la transmission des données. Elle est numérotée par la variable *N*(S). Elle permet également l'acquittement des trames échangées dans le sens inverse (procédé *piggy-backing*) grâce au numéro *N*(R).



format général aux trames I

le bit 1 de valeur 0 est spécifique à la trame I

Format de l'octet " Control " pour les trames I

Les trames S permettent l'acquittement et l'indication de l'état de disponibilité des stations (aptitude ou non à recevoir de nouvelles trames). Elles servent au contrôle d'erreur et au contrôle de flux. Elles contiennent un numéro *N*(R).

Les trois trames de supervision sont :
– la trame RR (*Receiver Ready*) indique que l'équipement est prêt à recevoir de nouvelles trames d'information. Le numéro de séquence *N*(R) indique le numéro de la prochaine trame attendue. Il indique donc que *toutes* les trames d'information de numéro *N*(S) strictement inférieur à *N*(R) ont été bien reçues.
– la trame RNR (*Receiver Not Ready*) indique que l'équipement n'est pas en mesure de recevoir de nouvelles trames d'information. Le numéro *N*(R) a la même signification que pour RR.
– la trame REJ (*Reject*) indique que l'équipement demande l'arrêt immédiat des émissions en cours de trame d'information et la reprise de la transmission. Le numéro de séquence *N*(R) indique où reprendre la transmission.

8	7	6	5	4	3	2	1	
N(R)			X	**S**	**S**	**0**	**1**	format général aux trames S
N(R)			X	0	0	**0**	**1**	RR : Receiver Ready
N(R)			X	0	1	**0**	**1**	RNR : Receiver Not Ready
N(R)			X	1	0	**0**	**1**	REJ : Reject

les bits 1 et 2 sont spécifiques des trames de supervision S
les bits 3 et 4 définissent le type de trame de supervision

Format de l'octet " Control " pour les trames de supervision

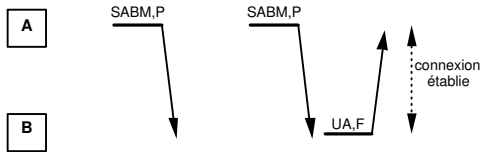
Un équipement peut envoyer des trames RR pour indiquer son état de réception ou pour demander l'état de la station en vis-à-vis.
Les trames U sont utilisées pour effectuer des fonctions supplémentaires de commande de la liaison :
– SABM (*Set Asynchronous Balanced Mode*) permet d'initialiser le fonctionnement en mode équilibré ;
– DISC (*DISConnect*) permet de rompre logiquement la liaison entre deux stations ;
– UA (*Unnumbered Acknowledgement*) permet d'acquitter les commandes SABM ou DISC ;
– FRMR (*FRaMe Reject*) permet de rejeter une commande (voir §III.3.3.a) invalide (correcte du point de vue de la détection des erreurs mais incohérente par rapport à l'état du dialogue) ;
– DM (*Disconnect Mode*) permet d'indiquer l'état de déconnexion d'une station. Il est utilisé, en particulier, pour répondre négativement à une initialisation SABM.

8	7	6	5	4	3	2	1	
U	**U**	**U**	X	**U**	**U**	**1**	**1**	format général pour trames U
0	0	1	X	1	1	**1**	**1**	SABM : *Set Asynchronous Balanced Mode*
0	1	0	X	0	0	**1**	**1**	DISC : *DISConnect*
0	1	1	X	0	0	**1**	**1**	UA : *Unnumbered Acknowledgment*
1	0	0	X	0	1	**1**	**1**	FRMR : *FRaMe Reject*
0	0	0	X	1	1	**1**	**1**	DM : *Disconnect Mode*

Format de l'octet " Control " pour les trames non numérotées

Établissement et libération

HDLC est un protocole orienté connexion : il faut d'abord effectuer une procédure d'établissement avant d'envoyer des informations ou de pouvoir en recevoir. Lorsqu'un des équipements veut terminer le dialogue, il doit engager une procédure de libération.



La station A tente d'établir une connexion vers B.
La station B ne détecte pas la première trame mais acquitte la seconde.

Établissement d'une connexion

L'une quelconque des 2 stations peut initialiser la liaison, elle envoie la trame non numérotée SABM et se met en attente d'une réponse. En cas d'absence de réponse, elle réitère son envoi jusqu'à un nombre maximal de répétitions. En cas de non réponse, elle considère la liaison comme ne pouvant pas être établie. A la réception de SABM,P, la station réceptrice transmet une trame UA,F si son utilisateur est prêt à initialiser le dialogue, une trame DM,F sinon. La connexion est alors établie : tous les compteurs et les temporisateurs sont initialisés. Les premières trames émises porteront un *N*(S) égal à 0.
Le processus de libération est identique avec l'échange des commandes DISC et UA.

Le protocole PPP

Le protocole PPP,*Point to Point Protocol*, est une version très simplifée d'HDLC qui ne comprend (sauf options) ni contrôle de flux, ni mécanisme de reprise sur erreur. Il est utilisé dans l'environnement Internet sur des liaisons point à point, typiquement entre un ordinateur personnel et le fournissuer d'accès à Internet. La seule trame définie alors est une trame *UI*, Unnumbered Information, qui transporte une information mais n'est pas numérotée.
L'absence de mécanisme de reprise sur erreur ne signifie pas que le circuit est parfait : le champ FCS est utilisé pour valider les trames reçues et les trames erronées sont retransmises grâce à d'autres mécanismes.

Synthèse

Un *protocole de liaison de données* est un ensemble de règles pour échanger des données de manière fiable alors que le circuit de données altère les informations transportées. Il définit le format de transmission des *trames*, leur délimitation, les techniques utilisées pour contrôler leur validité (parité, code polynomial,…) et le mode de correction des erreurs ainsi détectées (retransmission…). Le *contrôle de flux* et la *gestion des acquittements* sont deux fonctions importantes d'un protocole de liaison de données. *HDLC* est un exemple de protocole très répandu, orienté bit, transparent à tous les codes, dans lequel toutes les trames ont le même format. Il permet d'exploiter une liaison bidirectionnelle simultanée avec contrôle d'erreur, contrôle de séquencement et contrôle de flux. *PPP* est une version très simplifiée utilisée sur les liaisons point à point dans Internet.

Exercices

Exercice 1

Calculer le VRC et le LRC pour le message « HELLO » en utilisant la parité paire sachant que H est codé par 0001001, E par 1010001, L par 0011001 et O par 1111001. Précisez l'ordre de transmission du message construit.

Exercice 2

Soit la suite d'éléments binaires *0 1 1 1 0 1 0 0 0 0 1 0 1 0 1 0*. Calculer le bloc de contrôle d'erreur pour ces données, en supposant que l'on utilise un code polynomial de générateur $x^5 + x^3 + 1$. Le bloc suivant est reçu : *0 0 0 1 0 1 0 0 0 0 1 0 1 0 1 0 0 0 1 0*. Le contrôle d'erreur utilisant le même polynôme générateur, quelle est la décision prise par le récepteur concernant ce bloc ?

Exercice 3

Représenter le schéma du circuit calculant le CRC correspondant au polynôme générateur $G'(x) = x^6 + x^4 + x + 1$.

Exercice 4

Dans un transfert de fichier entre deux ordinateurs, on imagine deux stratégies d'acquittement, en supposant que le fichier est découpé en paquets pour sa transmission. La première consiste à faire acquitter chaque paquet individuellement par le récepteur, le fichier complet n'étant pas acquitté lui-même. La seconde consiste simplement à acquitter le fichier entier une fois que la transmission est faite. Que peut-on penser de ces deux stratégies ?

Exercice 5

On désire transmettre une suite de seize données binaires : 2BE3 (en hexadécimal), le premier élément transmis correspondant au 2. La protection contre les erreurs se fait par parité longitudinale.
a) Donner la forme polynomiale du message émis.
b) Donner la suite binaire complète transmise au récepteur.

c) En supposant que, par suite d'une erreur de transmission, le 19e bit de la suite trouvée en a) est modifié, calculer la valeur du reste trouvée par le récepteur.
6. On considère la suite de données binaires : *0 1 0 1 1 0 1 1 0 0 0 0 1 1 1 1 0 1 0 1 0 1 0 0* constituée par une suite de deux caractères de huit bits (parité paire) suivis par un bloc de contrôle d'erreur calculé avec un code polynomial (polynôme générateur $x^8 + 1$). La suite considérée est reçue : comment réagit le récepteur ? Détecte-t-il des erreurs de transmission ? Pourquoi ?

Exercice 6

Les premiers bits à transmettre dans une trame d'informations d'une procédure de type HDLC sont : *1 0 1 0 1 1 1 0*.
a) Sachant que le polynôme générateur utilisé est le polynôme V41, trouver le reste de la division polynomiale du message par ce polynôme.
b) En supposant que la transmission des 8 bits s'est effectuée sans erreur, représenter la suite des opérations effectuée par le récepteur depuis le premier bit de données jusqu'à la réception du dernier bit de contrôle.
c) En déduire la"valeur magique" utilisée dans une procédure de type HDLC. Donner sa représentation polynomiale.

Exercice 7

Dans un protocole de liaison de données, on suppose que chaque émetteur peut utiliser au maximum *Maxseq* + 1 numéros de séquence différents numérotés de 0 à *Maxseq*. Expliquer pourquoi la taille de la fenêtre en émission doit rester inférieure à *Maxseq*. Mettre en évidence un cas d'ambiguïté.

Exercice 8

Écrire la suite des bits transmis sur la ligne pour l'émission de la trame SABM émise par un équipement d'adresse A (03 en hexadécimal) vers un équipement d'adresse B (01 en hexadécimal). Le bit P est mis à 1. On admettra que le FCS pour cette trame est *1 1 0 1 0 1 1 1 1 1 1 1 1 0 1 1* en binaire dans le sens de transmission.
Par quelle trame répond l'équipement B ?

Exercice 9

La suite de données binaires suivante correspond au contenu du champ d'information d'une trame HDLC : *0 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 1 0 0.*
Quelle est la suite réellement fournie au support physique (pour ces données seulement) ?

Que se passe-t-il si le sixième bit de la suite fournie précédemment est erroné au cours de sa transmission ?

Exercice 10

On considère un échange de données bidirectionnel simultané entre deux stations A et B, géré par le protocole LAP-B (sous-ensemble d'HDLC sans rejet sélectif). La liaison est déjà initialisée et aucun temporisateur n'est en cours. La station A a cinq trames d'information à transmettre à la station B, la station B a dix trames d'information à transmettre à la station A, ces trames sont de même longueur. Les deux stations démarrent leur transmission à des instants très visins l'un de l'autre.
Donnez le schéma des échanges en indiquant le numéro des trames émises et reçues avec la nomenclature classique **I, N(S), N(R)** pour une trame d'information dont les deux numéros sont N(S) et N(R). On supposera
- qu'il n'y a aucune erreur de transmission sur les trames de A,
- qu'il y a une erreur de transmission sur les sixième et septième trames de B,
- que les trames retransmises ne sont pas une nouvelle fois erronées,
- que le temps de propagation est équivalent au quart de la durée de transmission d'une trame I,
- que la taille de la fenêtre d'anticipation est maximale,
- que les accusés de réception (dont la durée de transmission est égale au quart de la durée d'une trame I) sont transmis dès que possible et en tout cas inclus dans des trames d'information s'il y en a.

Que se passerait-il si les trames de A étaient dix fois plus longues que celles de B ?

Exercice 11

Un équipement A dialogue avec un équipement B suivant le protocole LAP-B via une liaison satellite. Le satellite réémet les signaux reçus sans aucun traitement. Son altitude est de 200 km. Tous les délais dus aux traitements sont négligeables. Les équipements dialoguent à 9600 b/s et limitent les trames d'information échangées à 64 octets d'information. Tout équipement recevant une trame d'information correcte l'acquitte immédiatement si il n'a aucune information à transmettre. En faisant l'hypothèse qu'il n'y a aucune erreur de transmission, quelle est la taille minimale de la fenêtre d'anticipation pour une transmission efficace lorsque A, seul, envoie des données vers B ?
Le satellite est maintenant à 36 000 km et on garde les mêmes hypothèses. Même question.

Exercice 12

On considère une trace relevée par un analyseur de protocole pour une station A qui émet et reçoit à travers un réseau. (On ne s'intéresse pas au contenu des trames).
La syntaxe est la suivante : colonne 1 : R = reçu par la station, E = émis par la station ; colonne 2 : longueur de la trame en octets (adresse + commande + données) sans compter le bloc de contrôle d'erreur ; colonne 3 : champ adresse (hexadécimal) ; colonne 4 : type de trame (pour les trames contenant des données utilisateurs, les numéros N(S) et N(R) sont précisés) ; colonne 5 : contenu de la trame

1	2	3	4	5
E	2	01	SABM	
R	2	01	UA	
R	7	03	I 0,0	1000 RES 07 00
E	5	01	I 0,1	1000 RES C
R	2	01	RR 1	
R	21	03	I 1,1	1000 CALL 05 191040420 01 00 02 99 01 00
E	5	01	I 1,2	1000 CALL C
R	2	01	RR 2	
E	12	01	I 2,2	1013 CALL 191050189
R	2	01	RR 3	
R	5	03	I 2,3	1013 CALL C
E	2	03	RR 3	
R	14	03	I 3,3	1013 D 0,0 42 CF 4E CA CF 55 D2 0A 8D
E	5	01	I 3,4	1013 RR 1
R	2	01	RR 4	
R	10	03	I 4,4	1000 D 0,0 62 32 30 0D 0A

E	5	01	I 4,5	1000 RR 1
R	2	01	RR 5	
R	21	03	I 5,5	1001 CALL 04 191040420 01 00 02 99 01 00
E	5	01	I 5,6	1001 CALL C
R	2	01	RR 6	
E	12	01	I 6,6	1013 D 0,1 53 41 4C 55 0D 0A
R	2	01	RR 7	
R	5	03	I 6,7	1013 RR 1
E	2	03	RR 7	
E	14	01	I 7,7	1001 D 0,0 42 4F 4E 4A 4F 55 0D 0A
R	2	01	RR 0	
R	5	03	I 7,0	RR 1
E	2	03	RR 0	
R	11	03	I 0,0	1001 D 0,1 72 65 63 75 0D 0A
E	11	01	I 0,1	1001 D 1,1 72 65 63 75 0D 0A
R	2	01	RR 1	
R	5	03	I 1,1	1001 RR 2

Que remarque-t-on pour le champ d'adresse ? Comment expliquer le fait que la station A qui a initialisé le dialogue soit la première à recevoir des données ? En supposant que la transmission a lieu à l'alternat, reconstituez le diagramme temporel des échanges. Toutes les trames sont-elles acquittées ? Terminer l'échange.

Quelques corrigés

Exercice 1

```
          LRC
H       0001001         0
E       1010001 1
L       0011001 1
L       0011001 1
0       1111001 1
--------------      -
VRC = 0100001         0
```

Message transmis (bits de poids faible en premier):
VRC + O + L + L + E + H -->
01000010 11110011 00110011 00110011 10100011 00010010

Exercice 6

a) Notons *M(x)* le message à émettre sous forme polynômiale. Il vaut :

$$M(x) = x^7+x^5+x^3+x^2+x$$

La division polynômiale à effectuer est donc : $x^{16}M(x)$ par $G(x)$, soit :
$x^{23}+x^{21}+x^{19}+x^{18}+x^{17}$divisé par $x^{16}+x^{12}+x^5+1$. Ce qui donne un reste :

$$R(x) = x^{14}+x^{12}+x^{10}+x^5+x^2$$

b) Le tableau ci-dessous donne les restes successifs calculés par le récepteur.

c) La "valeur magique" du reste d'un message transmis sans erreur est donc :

$$R(x) = x^{12}+x^{11}+x^{10}+x^8+x^3+x^2+x+1$$

c'est-à-dire en binaire sur 16 bits : *0 0 0 1 1 1 0 1 0 0 0 0 1 1 1 1*.

n° bit	DI	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	1
		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
2	0	1	0	1	1	1	0	1	1	1	1	1	1	1	0	1	
4	0	1	0	1	0	1	0	1	0	1	1	1	1	0	1	0	
5	1	0	1	0	1	0	1	0	1	0	1	1	1	1	0	1	
6	1	1	0	1	0	1	1	1	0	1	0	1	1	0	1	0	
7	1	0	1	0	1	0	1	1	1	0	1	0	1	1	0	1	
8	0	0	0	0	1	0	0	0	1	1	1	0	1	1	1	1	
10	1	1	1	0	0	1	1	0	0	1	1	1	0	0	1	1	
11	0	1	1	1	0	0	0	1	0	0	1	1	1	1	0	1	
12	0	1	1	1	1	0	1	0	1	0	0	1	1	0	1	0	
13	1	0	1	1	1	1	0	1	0	1	0	0	1	1	0	1	
14	0	0	0	1	1	1	1	0	1	0	1	0	0	1	1	0	
15	1	0	0	0	1	1	1	1	0	1	0	1	0	0	1	1	
16	0	0	0	0	0	1	1	1	1	0	1	0	1	0	0	1	
17	0	1	0	0	0	0	0	1	1	1	0	1	0	0	0	0	
18	0	1	1	0	0	0	1	0	1	1	1	0	1	1	0	0	
19	1	1	1	1	0	0	1	1	0	1	1	1	0	0	1	0	
20	0	0	1	1	1	0	0	1	1	0	1	1	1	0	0	1	
21	1	1	0	1	1	1	1	0	1	1	0	1	1	0	0	0	
22	0	1	1	0	1	1	0	1	0	1	1	0	1	0	0	0	
23	1	1	1	1	0	1	0	0	1	0	1	1	0	0	0	0	
24	1	1	1	1	1	0	0	0	0	1	0	1	1	1	0	0	

Tableau des restes du récepteur

Exercice 7

Si la taille de la fenêtre (W) est supérieure à la largeur du champ de numérotation (N), il y aura une confusion entre un message portant un numéro donné k et le message numéroté k+N soit encore k avec le modulo.
W < N sinon il y a des problème similaire à la gestion du tampon circulaire et ses pointeurs (P). Pour être plus précis : lorsque Pdébut = Pfin → Comment est l'état du tampon ? (plein ou vide).

Un cas d'ambiguïté :
Prenons l'exemple d'un modulo 8 donc 0, 1, 2,… 7 sont les numéros possibles (Maxseq = 7)
Définissons une taille de fenêtre maximale à (Maxseq +1) autrement dit à 8.
Imaginons qu'une station X émette une trame numérotée 7 qui est acquittée par une station Y : l'acquittement est RR0. Puis la station X émet 8 trames consécutives dont les 7 premières (0 1 2 3 4 5 et 6) ne sont pas reçues. Il ne reste plus que la trame 7 qui est une trame différente de la précédente ! La station Y peut croire à un doublon de la trame 7 précédente et donc l'ignorer… ainsi que les trames entre deux qu'elle n'a de fait pas reçues…
Donc nous pouvons conclure par cet exemple que la taille maximum de la fenêtre doit être Maxseq.

Exercice 8

a) Le corps de la trame est :

1000 0000 1111 1100 1101 0111 1111 1011
adresse=B SABM(P=1) FCS

Après insertion des zéros pour la transparence au fanion (indiqué en italique gras) et ajout des fanions de délimitation de la trame, la suite d'éléments binaires réellement transmise est :
01111110 1000 0000 1111 1***0*** 100 1101 0111 11***0*** 11 1011 01111110
Fanion adresse=B SABM(P=1) FCS Fanion
b) L'équipement répond par une trame UA avec le bit F mis à 1. Son champ adresse contient celle de B.

Exercice 9

soit la suite des données à transmettre

0 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 1 0 0
pour l'intégrer dans un corps de trame HDLC, il faut utiliser le mécanisme d'insertion de 0. Derrière cinq 1 successifs, on insère un 0.
On obtient
0 1 1 1 1 0 1 1 1 1 1 0 0 1 1 1 1 1 0 1 0 0.

Si le sixième bit de cette suite est erroné, on reçoit donc
0 1 1 1 1 1 1 1 1 1 1 0 0 1 1 1 1 1 0 1 0 0.
qui fait apparaître la succession impossible de dix 1. Le prochain fanion servira à découper une trame dont on sait d'ores et déjà qu'elle est erronée, elle sera donc ignorée.

Exercice 11

T = l / D

T est le temps de transmission
l est la longueur en bits du message
D est le débit en ligne en bit/s

t(p) = distance/vitesse de la lumière

t(p) est le temps de propagation
distance en mètre
vitesse de la lumière 300 000 000 m/s

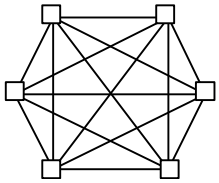
- A transmet un message à B, B finit de recevoir à T + t(p).
- Sur réception il renvoie immédiatement une réponse.
- Le temps que A recoive la fin du message de réponse, il faut que la taille de la fenêtre soit plus grande que T + le temps d'attente de la réponse, sinon on perd du temps.

Temps de transmission d'un message à 64 octets:
T = (48 + 64*8)/9600 = 58,33 ms
200 km d'altitude: temps de propagation
t(p) = 2*200 000 / 300 000 000 = 1/750 = 0.001333333 = 1,333 ms
Temps d'attente pour recevoir le RR (delta):
(delta) = 2*t(p) + t(RR) = 2*t(p) + (48 / 9600) = 2*1.33 + 5 = 7,66 ms
=> pendant que l'on envoie le second message par anticipation, on recevra le RR, donc on n'aura jamais de problème de taille de fenêtre.
36 000km d'altitude:
t(p) = 2*36 000/ 300 000 = 240 ms
Temps d'attente (delta):
(delta) = 2*t(p) + t(RR) = 485 ms
nombre de messages écoulés avant que l'on finisse de recevoir la réponse
n = (delta) / T = 8,31
=> dans un protocole comme HDLC, les numéros de séquence sont modulo 8 et donc la taille de la fenêtre maximale est de 7 (valeurs), il y aura donc un silence à chaque fois que la fenêtre est pleine. On pourrait améliorer le système si le modulo de la numérotation pouvait être plus grand
ou si les messages envoyés étaient plus longs.

Les concepts généraux des réseaux

Nous généralisons ici l'échange entre deux équipements à un ensemble de *N* équipements. Nous étudions les matériels et les procédures à mettre en place pour permettre un dialogue entre deux équipements quelconques de cet ensemble. Les équipements considérés ici peuvent être des ordinateurs ou bien tout équipement susceptible de communiquer comme un simple téléphone. Ils seront désignés par le terme générique d'*équipements terminaux.*

Étudions le nombre de liaisons point à point à mettre en place pour permettre tous les dialogues au sein d'un ensemble de *N* équipements terminaux. Il y a C_N^2 paires possibles d'équipements, soient $N(N-1)/2$ liaisons nécessaires. Chaque équipement doit alors gérer *N*-1 liaisons ! Pour 100 stations, il faut environ 5000 liaisons. Ceci montre l'impossibilité d'envisager des liaisons exclusives entre équipements terminaux.

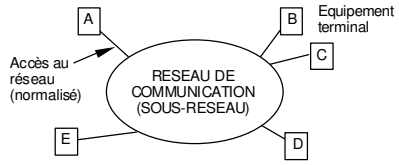


Tous les équipements sont reliés 2 à 2 : il y a $N(N-1)/2$ liaisons pour N terminaux.

Il est donc nécessaire de grouper les moyens de communication et de les *partager* entre les équipements terminaux pour réaliser un réseau. Ces moyens de communication peuvent être soit des liaisons point à point ou multipoint, soit des équipements capables de stocker et d'aiguiller l'information.

Un *réseau de communication* est donc un ensemble de ressources mis à la disposition d'équipements pour leur permettre d'échanger de l'information. Le terme réseau désigne suivant le contexte soit l'ensemble des ressources y compris les équipements terminaux, soit seulement le réseau de communication. On parle parfois de *réseau de transport* ou de *sous-réseau.*

La présence d'une multitude d'équipements terminaux oblige à définir un système d'identification cohérent au sein du réseau pour les différencier : c'est l'*adressage.* De plus, le réseau doit être capable d'acheminer une information vers tout destinataire en fonction de son adresse : c'est la fonction de *routage*.

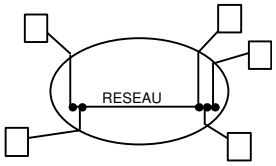


Réseau de communication

Un réseau de communication est généralement la propriété d'un *opérateur* qui met cette ressource à la disposition de tiers moyennant rétribution. C'est le cas des grands réseaux : en France, réseau téléphonique géré par *France Télécom*, réseau de transmission de données par paquets géré par la société *Transpac*. Dans ce cas, l'organisation du réseau est du ressort exclusif de l'opérateur. L'accès au réseau doit être normalisé tant pour les caractéristiques mécaniques et électriques que pour les procédures de dialogue. Cet accès au réseau peut être très différent de la nature interne du réseau : dans le cas des réseaux radio-mobiles, l'accès se fait par transmission sur la voie hertzienne alors que toutes les transmissions au sein du réseau se font sur des liaisons filaires. De plus, un même réseau de communication peut avoir différents types d'accès : un réseau radio-mobile et le réseau téléphonique peuvent être organisés comme un seul réseau avec des accès classiques par fils et des accès par voie hertzienne.

Un réseau peut être aussi la propriété exclusive de l'utilisateur. C'est le cas des *réseaux locaux d'entreprise* dont tous les équipements et les moyens de communications sont gérés entièrement par

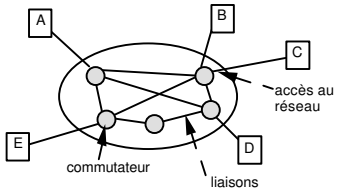
l'entreprise utilisatrice. Appelés aussi *LAN* (*Local Area Network),* ils peuvent accueillir plusieurs centaines d'équipements sur une distance de quelques kilomètres. La ressource partagée dans ce cas est le support de transmission qui est de type *diffusif* : tous les équipements sont reliés à ce support commun et tout message émis est reçu par l'ensemble des équipements. Cette caractéristique amène à des architectures spécifiques qui seront traitées dans le chapitre sur les réseaux locaux.



Exemple de réseau local

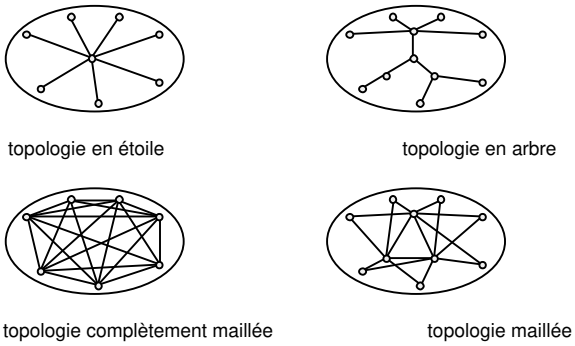
Réseaux à commutation

Dans le cas des réseaux grande distance, appelés aussi *WAN* (*Wide Area Network),* reliant plusieurs centaines de milliers voire millions d'équipements terminaux sur un territoire national, il n'est pas possible de partager un même support de transmission. On utilise un réseau à commutation. Les équipements terminaux sont reliés à des *commutateurs*. Ces derniers sont les " carrefours " du réseau et ont pour fonction de concentrer, d'éclater et de rediriger les informations. Les commutateurs sont reliés entre eux par des *circuits* point à point qui constituent des artères de communication.
Un réseau de communication peut ainsi se définir comme un graphe ou un ensemble de nœuds, les *commutateurs*, et d'arcs, les *circuits*. Ces circuits sont quelquefois appelés canaux, jonctions, lignes de transmission ou même liaisons selon les cas.



Réseau à commutation

La *topologie* du réseau définit la façon dont sont reliés les différents commutateurs.
Dans le cas d'une *topologie en étoile*, l'ensemble des commutateurs sont reliés à un même commutateur central. Certaines opérations comme le routage sont alors très simples. Cependant, un tel réseau est très fragile car tout dépend du bon fonctionnement du commutateur central.
La *topologie en arbre* peut être vue comme une généralisation du cas précédent avec l'introduction d'une hiérarchie : chaque commutateur est relié à un ensemble de commutateurs de niveau inférieur. Dans les topologies en arbre ou en étoile, il n'y a toujours qu'un chemin possible entre deux commutateurs : toute rupture d'une liaison entre deux commutateurs empêche donc le dialogue entre certains équipements terminaux.
Dans une topologie complètement *maillée*, chaque commutateur est relié à tous les autres. On atteint alors un haut niveau de sécurité au prix d'une augmentation considérable du nombre de liaisons et donc des coûts.
Dans la plupart des réseaux, la solution choisie est un mélange des précédentes : le réseau est hiérarchisé suivant une topologie en arbre avec un certain degré de maillage.

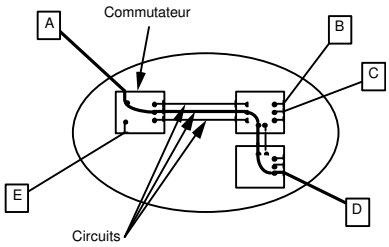


Topologie des réseaux

L'adressage au sein d'un réseau peut être lié à la localisation, c'est-à-dire à l'équipement lui-même ou au commutateur sur lequel est connecté l'équipement. On parle quelquefois d'*adresse physique*. C'est le cas du réseau téléphonique où les premiers chiffres d'un numéro indiquent le commutateur auquel est relié l'équipement de l'abonné. L'adresse peut être totalement décorrélée de la localisation et on peut parler d'*adresse logique*. Par analogie, le numéro de sécurité sociale peut être considéré comme l'adresse logique d'un individu : il est unique mais n'est pas lié au lieu de résidence de celui-ci.
La fonction de *routage* prend une importance particulière dans un réseau à commutation puisqu'il n'y a pas, en général, de lien direct entre équipements terminaux mais une multitude de chemins possibles mettant en œuvre plusieurs liaisons et plusieurs commutateurs.

Différents types de commutation : la commutation de circuits

Dans les réseaux à *commutation de circuits,* de multiples supports de transmission sont installés entre les différents commutateurs. Pour échanger des informations entre deux équipements terminaux, il est nécessaire de déterminer un chemin à travers le réseau et de réserver un support de transmission entre chaque paire de commutateurs situés sur ce chemin. Chaque commutateur ré-émet les signaux qu'il reçoit suivant ce chemin. Le réseau fournit donc l'équivalent d'un support de transmission point à point entre les équipements terminaux. Le réseau téléphonique est un exemple classique de réseau à commutation de circuits. Dans le contexte de la téléphonie, le mot *circuit* désigne une liaison entre 2 commutateurs.
Tout dialogue se décompose en 3 phases : une première phase d'établissement du circuit entre les équipements terminaux par réservation de l'ensemble des circuits nécessaires à l'intérieur du réseau, la phase classique de transfert des informations puis une phase de libération pour permettre la réutilisation des différents circuits par d'autres équipements terminaux. La libération se fait à la demande d'un des équipements terminaux (ou si le réseau détecte qu'un équipement est en panne). Tant qu'elle n'a pas eu lieu, les circuits restent réservés à l'intérieur du réseau, même s'il n'y a aucun transfert d'information.
Ce type de commutation présente l'inconvénient de monopoliser les circuits entre commutateurs pendant la durée entière du dialogue. Il est donc nécessaire de multiplier les circuits entre commutateurs, on parlera dans ce cas de *faisceaux* (ou trunks). Il nécessite, de plus, la disponibilité simultanée des deux équipements terminaux pour tout dialogue. En revanche, il présente l'avantage d'être assez simple : la commutation de circuits peut s'appliquer sur un réseau analogique ou bien numérique. Dans le cas d'un réseau numérique, la mémoire nécessaire dans les commutateurs est réduite et il n'y a aucun traitement à faire sur l'information transmise.



Principe de la commutation de circuits

Un faisceau peut correspondre à plusieurs supports physiques différents (par exemple une paire torsadée par circuit) ou bien à un seul support physique sur lequel les circuits sont multiplexés en temps ou en fréquence mais la philosophie reste la même : il y a toujours réservation d'une partie de la capacité de transmission pendant tout le dialogue.

Différents types de commutation : commutation de messages

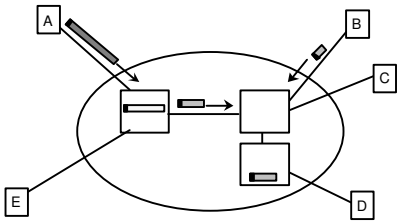
La *commutation de messages* s'applique aux seuls réseaux numériques. Un *message* est défini comme une suite de données binaires formant un tout logique pour les équipements terminaux. C'est, par exemple, un fichier complet, un courrier électronique ou une page d'écran.

Lorsqu'un équipement veut transmettre un message, il lui ajoute l'adresse du destinataire et le transmet au commutateur. Celui-ci attend la réception complète du message, le stocke, analyse son adresse et le réémet alors vers le commutateur voisin adéquat. Le message transite ainsi à travers le réseau par réémissions successives entre les commutateurs (on utilise quelquefois le terme anglais *store-and-forward.*

Les commutateurs sont reliés deux à deux par une liaison de données. Celle-ci est occupée uniquement pendant la durée de transmission du message mais elle n'est jamais monopolisée par un équipement indépendamment de toute transmission. De plus, si un équipement terminal est temporairement indisponible, le réseau peut stocker le message jusqu'au rétablissement de l'équipement.

Dans un tel réseau, chaque commutateur doit être capable de stocker le message en entier. Comme un commutateur supporte simultanément plusieurs dialogues et que la taille d'un message est déterminée par les équipements, la mémoire nécessaire peut être importante. De plus, le délai de transmission à travers le réseau est fonction du nombre de commutateurs traversés et de la taille du message. Il peut donc être assez important. Enfin, pour un taux d'erreur donné par bit transmis, la probabilité d'une erreur sur un message augmente avec la taille du message. La transmission de longs messages dans le réseau est donc très pénalisante.

Le réseau *Télex* est un réseau à commutation de messages. La commutation de messages n'étant plus l'objet de développements aujourd'hui, elle n'est pas traitée ici.



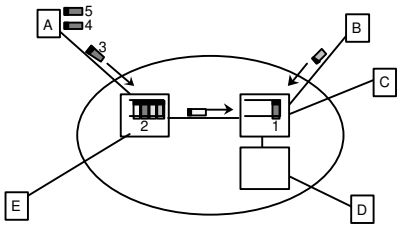
Principe de la commutation de messages

Différents types de commutation : commutation par paquets

Les inconvénients de la commutation de messages sont liés à la taille des messages.

La *commutation par paquets* consiste à découper les messages en morceaux appelés segments. Ce découpage est la *segmentation.* Il est fait par l'expéditeur. A chaque segment sont ajoutées des

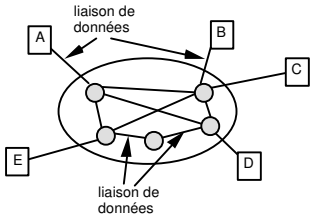
informations permettant d'identifier l'expéditeur et le destinataire : l'ensemble forme un *paquet.* La taille maximale d'un paquet est fonction du réseau. Les paquets sont acheminés par le réseau comme dans un réseau à commutation de messages jusqu'au destinataire. Celui-ci attend la réception de tous les paquets pour reconstituer le message et le traiter. Cette opération est le *réassemblage.*
Un paquet ne forme pas un tout logique pour l'équipement terminal. Il n'a de sens que comme " atome d'information " acheminé par le réseau par réémissions successives entre les commutateurs. Sa petite taille permet de réduire le délai global d'acheminement des messages à travers le réseau.
Une liaison entre commutateurs n'est pas monopolisée par un équipement mais supporte la transmission de paquets de multiples utilisateurs. Si le débit de la liaison est supérieur au flux transmis par l'ensemble des utilisateurs, elle peut supporter de multiples dialogues simultanés tout en donnant l'impression à chacun d'être seul sur le réseau. Le flux généré par un utilisateur donné peut augmenter subitement, l'impact sera faible sur le flux global. On a donc un effet de *multiplexage statistique.*



Le message émis par A est segmenté en 5 paquets, qui sont acheminés un par un par le réseau.

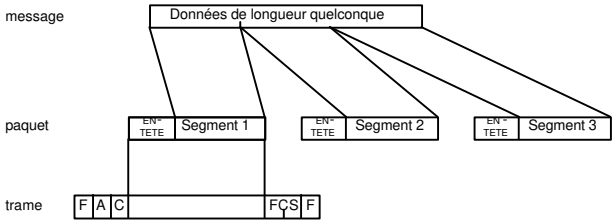
Principe de la commutation par paquets

Comme chaque paquet doit traverser le réseau, il est nécessaire qu'il contienne un *en-tête* comportant des informations de contrôle. Ces informations sont utilisées par les commutateurs pour un aiguillage correct. Le format de l'en-tête est défini par l'opérateur du réseau. Chaque paquet reçu par un commutateur est stocké puis son en-tête est analysé
En fonction des informations de contrôle, le paquet est aiguillé vers un autre commutateur ou le cas échéant vers l'équipement terminal. Si la liaison vers le commutateur concerné est occupée, le paquet est conservé en mémoire : chaque commutateur se comporte donc comme une mémoire tampon. Le dimensionnement de la mémoire des commutateurs est un des éléments déterminant la capacité et les performances d'un réseau à commutation par paquets. Si la mémoire d'un commutateur est entièrement utilisée, celui-ci n'est plus en mesure de recevoir de nouveaux paquets. Il peut, dans certains cas, détruire des paquets et dégrader les performances du réseau. L'ensemble des techniques mises en œuvre pour éviter la saturation de la mémoire des commutateurs s'appelle le *contrôle de congestion.*
De plus, les liaisons entre les commutateurs ne sont pas d'une fiabilité totale. Il est donc nécessaire de mettre en œuvre des protocoles de liaison de données entre chaque paire d'équipements. Les commutateurs gèrent donc autant de liaisons de données que le nombre d'équipements auxquels ils sont reliés.
L'approche utilisée pour la structuration des équipements est une approche hiérarchique : pour chaque liaison dans le réseau, une *entité de liaison de données* s'occupe de fournir un dialogue fiable. La gestion de l'aspect réseau, c'est-à-dire l'aiguillage des paquets, est réalisée par une autre entité, *l'entité réseau* qui utilise l'entité de liaison de données comme une boîte noire fournissant un service. L'entité réseau est la seule entité à interpréter l'en-tête des paquets. En revanche, l'entité de liaison de données considère les paquets comme un tout logique à transmettre, c'est-à-dire comme de l'information à placer dans une trame, par exemple HDLC (le paquet constitue donc le champ Information de la trame). Ce processus s'appelle l'*encapsulation.*



Entre toutes les paires d'équipements, sont mises en œuvre des liaisons de données.

Liaisons de données dans un réseau



Le message est coupé en trois segments dans cet exemple. A chaque segment est adjoint un en-tête pour former un paquet. Chaque paquet est transmis dans une trame (ici trame HDLC).

Message, paquets et trames

Le protocole normalisé pour le format des paquets dans l'accès à un réseau à commutation de paquets offrant le service circuit virtuel est X25. Transpac fut l'un des premiers réseaux à utiliser et promouvoir X25.

Différents types de commutation : commutation de trames

La commutation de trames ou *relais de trames* est une évolution de la commutation par paquets avec service circuit virtuel. Le réseau offre toujours un service en mode connecté, utilisant des principes identiques à X25 pour le routage des informations, mais n'assure pas l'intégrité totale ni le contrôle de flux sur les données. Dans un réseau utilisant X25, chaque paquet (élément vu par l'entité réseau) est transporté dans une *trame* (élément vu par l'entité liaison de données). Le paquet possède ses informations de contrôle (référence à la connexion établie, numéros de paquet,...) et la trame qui le transporte possède elle aussi ses informations de contrôle (adresse, numéros de trame, bloc de contrôle d'erreur...).

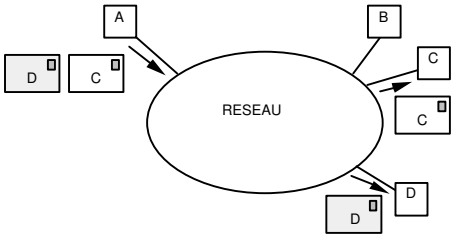
Le relais de trames consiste à assurer les fonctions de routage à travers le réseau directement sur les *trames* (il compacte les couches 2 et 3 en une seule) et supprime les fonctions de contrôle d'erreur et de contrôle de flux entre les commutateurs du réseau : ces fonctions sont reportées sur les utilisateurs, qui les assureront, s'ils en ont besoin. Typiquement, pour le contrôle d'erreur, on conserve les mécanismes de détection mais il n'y a aucune correction des erreurs dans le réseau : l'utilisateur sera obligé de commander lui-même les retransmissions. Cette simplification des procédures *dans le réseau* est d'autant plus acceptable que les transmissions utilisent des fibres optiques de très bonne qualité. Il s'agit donc d'une solution intéressante pour offrir des débits plus élevés. Le relais de trames offre ainsi un service en mode connecté avec établissement de *liaisons virtuelles rapides* (similaires au circuit virtuel d'X25). La taille des trames est quelconque. Transpac a fait évoluer son protocole X25 vers le relais de trames. Dans un premier temps, le relais de trame a été utilisé à l'intérieur du réseau, ce qui reste transparent pour les utilisateurs. Puis, Transpac a offert aux utilisateurs d'accéder au réseau en relais de trames.

Différents types de commutation : commutation de cellules

Une nouvelle technique de commutation émerge aujourd'hui, en particulier pour le réseau numérique à intégration de services large bande. Il s'agit d'une commutation hybride, qui allie commutation de circuits et commutation par paquets. Elle utilise une technique de transfert dite ATM (*Asynchronous Transfer Mode*). Les informations (voix, données, images…) sont toutes découpées en paquets de taille fixe, baptisés *cellules* et contenant 48 octets d'informations utiles. Mode de transfert asynchrone défini par une norme l'ITU, ATM (Asynchronous Transfer Mode) est une technologie de télécommunication basée sur le principe de la commutation par *cellules* qui sont des paquets de taille *fixe* et *petite* (53 octets), ce qui lui permet d'être très rapide et efficace.
ATM a été développé à l'origine par des chercheurs français (CNET, Centre National d'Etudes des Télécommunications). L'objectif est de transmettre sur le même réseau des données, de la parole, des images, en temps réel. Les problèmes posés par les autres technologies sont multiples : trop faible capacité des réseaux, faibles vitesses de transmission, rigidité des services offerts, interconnexion difficile entre différents types de réseaux, coût élevé des solutions performantes, incapacité de transmettre parole et images en temps réel, qualité de service insuffisante. La commutation de cellules pousse le raisonnement précédent (évolution d'X25 vers le relais de trames) encore plus loin. Elle supprime la détection d'erreur sur les données et réduit les contrôles au seul en-tête des cellules. L'unique traitement dans les commutateurs du réseau est alors la commutation et le routage (il n'y a plus de liaison de données et le niveau réseau est réduit au strict minimum). Le fait que les liaisons soient des fibres optiques, que les cellules soient petites et de taille fixe, qu'elles passent toutes par le *même chemin virtuel* sont des atouts de la technologie ATM qui peut ainsi offrir une excellente qualité de service et apporter un confort d'utilisation tel que les qualités des liaisons commutées et des liaisons permanentes sont équivalentes. Les débits peuvent être quelconques et en particulier variables. Ceci apporte une très grande souplesse par rapport au RNIS *bande étroite* du fait qu'il est entièrement construit sur la base de l'unique débit 64 kbit/s. Par ailleurs, les délais de traversée du réseau sont garantis très faibles (commutateurs puissants et dimensionnés pour le traitement de cellules de taille fixe). Ceci permet la mise en œuvre d'applications d'images avec compression en temps réel et fait d'ATM l'unique technologie pour le multimédia.

Notion de services dans un réseau à commutation

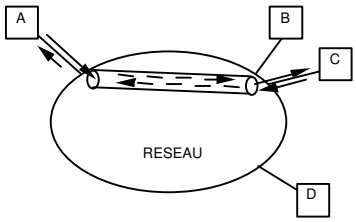
Dans un service *sans connexion,* chaque paquet est considéré comme totalement indépendant des précédents par l'équipement expéditeur. Il doit donc comporter l'adresse complète du destinataire et éventuellement celui de l'expéditeur. L'équipement terminal peut délivrer au réseau à tout moment un paquet à transmettre sans procédure préalable. Un tel service est par exemple fourni par le réseau postal : une lettre peut être postée à tout moment !



Service sans connexion

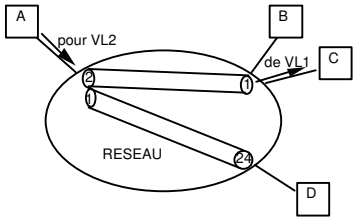
Dans un service *avec connexion* ou *orienté connexion*, l'équipement terminal doit d'abord indiquer le correspondant avec lequel il veut dialoguer : le réseau établit un lien logique entre les deux équipements et constitue un " tube " de dialogue. Cette procédure est appelée *ouverture de la connexion*. Tout paquet délivré par un équipement au réseau est alors transmis jusqu'au destinataire sans qu'il soit besoin de préciser une quelconque adresse : seule une référence au " tube " de communication suffit. Lorsque le dialogue est terminé, un des deux équipements peut indiquer au réseau qu'il souhaite fermer la connexion. Pour dialoguer avec un autre équipement, il est nécessaire d'établir une nouvelle connexion. Un tel service est illustré par le réseau téléphonique : il est nécessaire de décrocher le téléphone et d'appeler son

correspondant pour pouvoir dialoguer avec lui. Dès qu'on raccroche, il faut le rappeler pour communiquer avec lui.



Service avec connexion

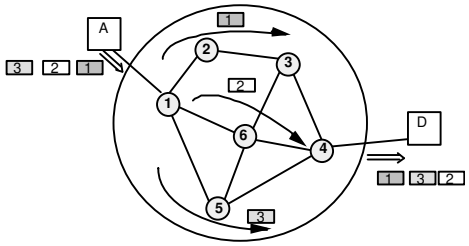
Il est possible pour un équipement terminal de gérer plusieurs connexions en parallèle. Celles-ci sont distinguées par leur référence : numéro appelé souvent *numéro de voie logique*. A l'établissement d'une connexion, l'équipement précise l'adresse du destinataire. Un numéro de voie logique est attribué localement à l'expéditeur. Pour envoyer un paquet vers le destinataire, l'équipement place ce numéro de voie logique dans l'en-tête et transmet ainsi le paquet au commutateur d'accès du réseau. Il est ensuite acheminé jusqu'au destinataire. Ce destinataire lors de l'établissement de la connexion s'est vu attribuer lui aussi un numéro de voie logique associé à l'adresse de l'expéditeur. Le paquet reçu porte ce numéro. Il faut remarquer que les numéros des deux extrémités de la connexion sont totalement indépendants.



La connexion entre A et C est référencée par la voie logique 2 pour A et 1 pour C.
La connexion entre A et D est référencée par la voie logique 1 pour A et 24 pour D.
L'équipement A dispose de deux voies logiques 1 et 2 multiplexées sur la liaison entre A et le premier commutateur.

Multiplexage de voies logiques

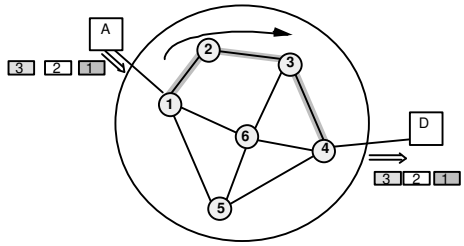
Dans un réseau à *datagramme*, les paquets (appelés datagrammes) sont considérés comme totalement indépendants les uns des autres. Chaque paquet transite à travers le réseau avec l'ensemble des informations nécessaires à son acheminement et notamment les adresses complètes de l'expéditeur et du destinataire. Le routage est effectué pour chaque paquet. Deux paquets successifs échangés entre les mêmes équipements peuvent donc suivre des chemins différents et être reçus par l'expéditeur dans un ordre différent de l'ordre d'émission. De plus, en cas de problème (rupture de liaison, manque de mémoire dans un commutateur), des paquets peuvent être perdus. L'équipement terminal doit donc réordonner les paquets pour reconstituer les messages et doit contrôler qu'aucun paquet n'est perdu. L'avantage d'un tel réseau est sa simplicité de réalisation interne : les fonctions de contrôle sont mises en œuvre par les équipements terminaux et non pas dans le réseau lui-même..



A envoie successivement les paquets 1, 2, 3.
Le paquet 1 emprunte le chemin passant par les commutateurs 1, 2, 3, 4.
Les paquets 2 et 3 empruntent respectivement 1, 6, 4 et 1, 5, 4.
C reçoit dans l'ordre 2, 3 puis 1.

Service de datagramme

Le service avec connexion est fréquemment couplé avec la notion de *circuit virtuel*. A l'ouverture de la connexion, le réseau détermine un chemin qu'emprunteront ensuite tous les paquets : ce chemin est appelé circuit virtuel. Circuit car on utilise les mêmes principes que pour la commutation de circuits. Virtuel car une liaison entre commutateurs n'est pas monopolisée par un chemin mais peut être utilisée par plusieurs circuits virtuels entre des équipements totalement différents. De ce fait, l'utilisation du support de transmission est beaucoup plus efficace que dans le cas de la commutation de circuits.
L'avantage d'un réseau à circuit virtuel est sa fiabilité : comme les paquets d'un même circuit virtuel empruntent le même chemin, il suffit de conserver l'ordre des paquets sur chaque tronçon du chemin pour conserver globalement l'ordre sur un circuit virtuel. En revanche, ce type de réseau est plus compliqué à réaliser. Sur le circuit virtuel, l'opérateur de réseau peut garantir une certaine qualité de service : taux d'erreur, séquencement, contrôle de flux.



Tous les paquets empruntent le chemin défini par les commutateurs 1, 2, 3, 4.

Réseau à circuit virtuel

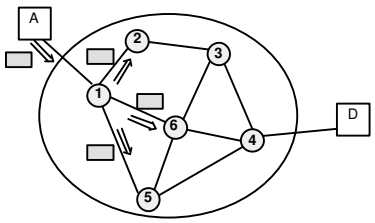
Le réseau *Transpac* est un réseau à commutation par paquets à circuits virtuels.

Fonctions de contrôle interne dans un réseau

Le routage

Le *routage* est la détermination d'un chemin permettant d'orienter à travers le réseau des paquets vers le correspondant désigné. Cette opération se fait à l'établissement d'un circuit virtuel ou réel, ou pour chaque paquet dans un réseau datagramme. Dans un réseau maillé, il y a une multitude de chemins possibles. Trouver le meilleur chemin peut avoir plusieurs significations : le moins coûteux pour l'opérateur, pour le client, le plus rapide, le plus sûr...
Deux grandes catégories de routage existent. Avec un routage *non adaptatif*, le choix du chemin entre deux équipements est fixé à l'avance et mémorisé dans un ou plusieurs nœuds du réseau. Le routage peut être *adaptatif* : le chemin varie en fonction de l'état du réseau (panne de liaisons ou de commutateurs...)

ou du trafic écoulé par le réseau. Les routages adaptatifs sont nécessaires pour utiliser au mieux les ressources du réseau et améliorer sa défense en cas d'incident.
De plus, l'algorithme de routage peut être plus ou moins *réparti* sur le réseau. On peut avoir un routage centralisé, isolé ou distribué. Dans le cas du routage *centralisé*, un organe est dédié à cette fonction. Il est interrogé par l'ensemble des commutateurs à chaque opération de routage. En cas de routage adaptatif, il doit connaître en permanence l'état complet du réseau.
Dans un routage *isolé*, chaque commutateur détermine le chemin, uniquement en fonction de son état : taille des files d'attente, occupation des lignes. Il n'a pas connaissance de l'environnement c'est-à-dire des commutateurs voisins ou des liaisons voisines.
Dans un routage *distribué*, chaque nœud diffuse à ses voisins des indications sur son état. Un nœud peut donc déterminer un chemin en fonction de son propre état et de l'état de ses proches voisins.
La description de l'ensemble des algorithmes de routage sort du cadre de ce module car ils sont variés et peuvent être assez complexes. Donnons juste l'exemple simple du *routage par inondation* dans un réseau à commutation par paquets : un paquet reçu par un commutateur est réémis sur toutes les liaisons hormis celle où ce paquet a été reçu. Un tel algorithme provoque une multiplication, infinie en théorie, du nombre de paquets. Il est donc nécessaire d'en détruire pour éviter une congestion du réseau. Pour ce faire, on place un compteur dans l'en-tête de chaque paquet. Ce compteur est décrémenté par les commutateurs à chaque réémission. Lorsqu'il devient nul, le paquet est détruit. La valeur minimale initiale doit être égale au nombre de commutateurs minimum à traverser pour joindre le correspondant. Si celle-ci est inconnue de l'expéditeur, on peut prendre le nombre maximal de commutateurs séparant deux équipements quelconques.
Le routage par inondation est de type isolé. Son avantage principal est la simplicité et la fiabilité. Il trouve toujours le chemin le plus court quel que soit l'état du réseau. Il est utilisé dans les réseaux militaires où il est nécessaire d'assurer un fonctionnement du réseau (transmission d'alarmes) même lorsqu'un grand nombre de commutateurs ou de liaisons sont détruits.



Routage par inondation

Un autre algorithme de routage très simple est celui de la " patate chaude " (*hot potatoe*) qui consiste pour un commutateur à se débarrasser d'un paquet reçu le plus rapidement possible en le transmettant sur la liaison la moins chargée (hormis celle où ce paquet a été reçu). Un tel algorithme est adaptatif puisqu'il prend en compte l'état du réseau. Pour améliorer son efficacité, il peut être combiné avec un routage statique où plusieurs routes possibles sont mémorisées.

Le contrôle de congestion

Le *contrôle de congestion* est l'ensemble des opérations effectuées pour éviter que les ressources des commutateurs ne soient surchargées. La fonction de routage est, à ce titre, fondamentale car elle doit répartir le trafic entre les commutateurs du réseau. Plusieurs méthodes peuvent être évoquées : perte de paquets en cas de congestion, limitation des connexions et contrôle isarythmique.
Dans les réseaux à commutation de circuits, lorsque la capacité de communication entre deux commutateurs est saturée, on peut refuser de nouveaux appels. De même lorsque la mémoire d'un commutateur de paquets arrive à saturation, celui-ci ne stocke plus les nouveaux paquets qui arrivent : ceux-ci sont perdus et l'équipement terminal doit les émettre à nouveau. Le réseau peut donc perdre des paquets indépendamment de tout problème de transmission. De tels mécanismes sont présents dans les réseaux à datagrammes. Ils sont très simples mais il n'y a pas à proprement parler contrôle de congestion.

La description précédente n'est pas exhaustive. D'autres méthodes de contrôle de congestion existent. De plus, les méthodes précédentes peuvent être combinées et raffinées.

Administration de réseaux

Administrer un réseau revient à se poser le problème de la faisabilité et de la mise en œuvre opérationnelle de ce réseau. Or, les architectures actuelles ne sont pas homogènes : il n'existe pas de système permettant de répondre à l'ensemble des besoins d'un utilisateur. Ainsi, une architecture est constituée de différents types de réseaux : réseaux locaux, PABX, réseaux grandes distances publics ou privés. Les informations véhiculées sont de types différents : images, voix, données, et les modes d'exploitation variés, avec ou sans connexion. De plus, pour l'utilisateur, la gestion de réseau. Il ne suppose pas seulement la bonne gestion du service de transport de l'information, mais également la gestion correcte de son traitement.
L'utilisateur a donc besoin d'une gestion puissante, prenant en compte l'hétérogénéité de l'architecture du réseau, fournissant un véritable " système d'exploitation réseau " prenant en charge les aspects distribués du système.
Les besoins, en matière de gestion, se situent à deux niveaux : celui de l'*utilisateur* et celui de l'*opérateur* du réseau.
Les besoins de l'utilisateur sont très variés et s'expriment en :
– *connexion aux différentes applications.* L'utilisateur demande tout d'abord de pouvoir se connecter aux différentes applications. Il doit avoir à sa disposition un ensemble d'outils permettant de lui rendre transparentes les différentes méthodes d'accès et de connexions aux applications.
– *accès aux serveurs de noms.* L'utilisateur a besoin, dans certains cas, d'accéder aux serveurs de noms afin de trouver la localisation d'une ressource ou même l'existence d'une ressource.
– *confidentialité des échanges et sécurité des informations* dans le réseau.
– *assistance technique et service SVP réseau*. L'utilisateur, derrière sa console, n'a aucune connaissance a priori de l'architecture du système distribué sur lequel il est connecté. Il se peut que pour des raisons de pannes ou pour des raisons personnelles, il ait besoin de conseils pour le débloquer d'une situation anormale ou inconnue. Il apprécie alors les aides et les modes opératoires qui lui sont fournis pour sortir de ces cas d'exceptions.
– *qualité de service*. La qualité de service est un élément important dans une gestion de réseau car elle est directement ressentie par l'utilisateur. Ceci correspond aux notions de disponibilité du système et de performances.
Les besoins de l'opérateur sont également variés et se déclinent de multiples façons.
– *planification*. L'opérateur d'un réseau est constamment confronté à l'adéquation de son système par rapport aux besoins. Le rôle de la planification est d'harmoniser l'ensemble des ressources disponibles par rapport aux demandes tout en optimisant les coûts. Il est nécessaire de disposer d'une vue globale du système. Ceci permet d'effectuer la répartition des ressources offertes et de suivre l'évolution dans le temps du système.
– *exploitation*. Cette phase correspond au suivi permanent du réseau. Elle représente l'ensemble des actions journalières menées par une équipe réseau. L'exploitation s'effectue par la surveillance des différents composants constituant le réseau. C'est, en général, dans cette phase que sont détectées les anomalies de fonctionnement.
– *maintenance.* Lorsqu'une anomalie, logicielle ou matérielle, a été détectée, il est nécessaire d'y remédier. L'opération est plus ou moins aisée, suivant les outils mis à disposition (outils de test logiciel ou matériel). Le but est de réparer au plus vite les éléments défectueux. En général, l'exploitation intervient pour localiser au mieux la cause de l'anomalie, et, si possible, proposer une solution de secours. Après réparation par la maintenance, l'exploitation réintègre l'ensemble des composants.
– *hétérogénéité.* La prise en compte de l'hétérogénéité d'un réseau est un véritable problème pour le gestionnaire. En effet, il faut être capable de corréler l'ensemble des états de systèmes différents afin d'établir des relations de cause à effet ou de mettre en évidence des situations de fonctionnement anormal et d'analyser finement les événements qui y ont conduit. La complexité provient du fait que les différents éléments constituant l'architecture d'un réseau ne fonctionnent pas nécessairement suivant les mêmes normes et ne fournissent donc pas des informations directement comparables.

– *intégrité*. Ce besoin impose de structurer de façon fiable une gestion de réseau. En effet, l'utilisateur peut accéder à certaines fonctionnalités, mais doit être protégé contre toutes tentatives de violation sur les autres fonctionnalités. Ceci permet de spécifier les différentes responsabilités, leurs autorités et leurs limites qui peuvent intervenir au sein d'une gestion de réseau.
– *résistance aux pannes.* La qualité d'une gestion provient de ce qu'elle est capable de continuer sa surveillance en tout état de cause. Ceci implique qu'une panne isolée ne puisse rendre impuissante cette gestion. En effet, il serait dérisoire d'avoir implanté une application bloquante, surtout si le but de cette application est de fournir des remèdes à ces blocages.
– *connaissance des chaînes de liaison.* La connaissance des chaînes de liaison est importante car elle fournit un suivi dynamique des différents échanges intervenant dans le système distribué. On peut ainsi suivre une ou plusieurs communications. Cette connaissance permet, entre autres, de faire des reprises de connexions et de rendre ainsi transparent à l'utilisateur le chemin d'accès à son application.

Synthèse

Pour relier un grand nombre d'équipements informatiques, on fait appel à une *infrastructure de réseau* dont les ressources sont partagées entre les différents dialogues mis en œuvre. La *commutation de circuits* permet de réserver des ressources physiques à chaque couple d'équipements qui désire établir une communication, c'est la technique utilisée dans le *réseau téléphonique*. La *commutation par paquets* est utilisée pour des échanges de type données informatiques, découpées en paquets, œ fut la technique du *réseau Transpac*. Un service simple baptisé *datagramme* est utilisé à l'échelle internationael dans Internet. Des fonctions de *contrôle interne* sont nécessaires à la gestion d'un réseau, pour assurer le meilleur contrôle des ressources et donc le meilleur partage entre les utilisateurs : routage, contrôle de congestion et administration de réseaux.

Exercices

Exercice 1

Un message de taille 40 octets doit être transmis entre deux équipements A et B. On suppose que ces 2 équipements peuvent être reliés à 3 réseaux : (1) réseau à commutation de circuits, (2) réseau à commutation par paquets offrant un service orienté connexion, (3) réseau datagramme offrant un service sans connexion. Quel est le réseau que vous choisissez pour réaliser ce transfert ?

Exercice 2

Deux entités A et B communiquent à travers un réseau X25. Un circuit virtuel est établi entre A et B. Il est identifié comme voie logique numéro 152 du côté de A. Peut-on déduire le numéro de voie logique qui est affecté à ce circuit virtuel du côté B ?

Exercice 3

Un réseau X25 relie trois ETTD. Est-il possible d'ouvrir plusieurs circuits virtuels entre deux ETTD donnés ? Dans le cas d'une réponse positive, quel intérêt y aurait-t-il à ouvrir plusieurs circuits virtuels entre deux ETTD ?

Exercice 4

Etablir un tableau de comparaison, selon le modèle suivant, pour des réseaux de données.

Eléments de comparaison	**Mode connecté**	**Mode non connecté**
fonctionnalités		
complexité		
performance		
Coût du réseau		
Exemple de réseau		

Exercice 5

Soit un ETTD A communiquant avec un ETTD B via un réseau dont le protocole d'accès est X25. Les ETTD A et B sont reliés à des ETCD numérotés respectivement 1 et 2. Si A reçoit une trame LAP-B de type RR avec un numéro *N*(R) envoyée par l'ETCD 1, cela signifie-t-il que toutes les trames d'information dont le numéro *N*(S) est strictement inférieur à *N*(R) ont été bien reçues par B ?

Exercice 6

Soit un ETTD A conforme à la norme X25, chargé d'envoyer à un ETTD B un fichier de 3 Mégaoctets par le réseau Transpac. On suppose que le transfert de données s'effectue sans erreur et que la taille des paquets de données est de 128 octets. La taille de la fenêtre du circuit virtuel commuté est prise égale à 7. Décrire les différentes phases nécessaires à l'échange en indiquant la nature et le nombre des paquets échangés.

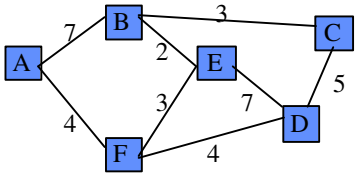
Exercice 7

Dans un réseau à commutation par paquets où la taille maximale des paquets est de 128 octets, la durée de vie maximale d'un paquet est fixée à 30 s. On utilise une numérotation séquentielle des paquets sur 8 bits. Quel est le débit maximal par connexion ? Pourquoi ? Que doit-on faire si l'on veut un débit beaucoup plus important ?

Exercice 8

Etablir les tables de routage de tous les nœuds de ce réseau en minimisant le coût des liaisons. Pour chaque destination, on déterminera le nœud suivant.

Exercice 9



Indiquez quels sont les paquets échangés entre deux ETTD A et B, depuis l'établissement du CVC jusqu'à leur libération, sachant que chaque ETTD désire émettre 3 paquets de données vers l'autre ETTD. Nous supposons en outre que A ouvre et libère le CVC ; l'acquittement des paquets de données est local et la fenêtre de niveau 3 est égale à 2.

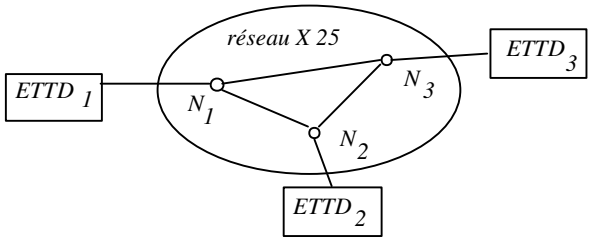
Exercice 10

On considère un réseau à commutation. Deux stations A et B ont établi une communication à travers ce réseau et on note *S* le nombre de commutateurs du réseau traversés par la communication entre A et B.
Le débit de toutes les liaisons est *D* bit/s. Le protocole de communication utilisé est le même sur toutes les liaisons, il rajoute un en-tête de *H* bits à chaque unité de données. On néglige les temps de propagation et les temps de traitement dans les commutateurs du réseau ainsi que les accusés de réception.
La station A doit transférer un fichier de taille *L* bits à la station B.
a) Le réseau utilise la commutation de message et le fichier est transmis en un seul message sur chaque liaison. Donner l'expression T_{fic1} du temps de transmission du fichier sur ce réseau.
b) Le réseau utilise la commutation par paquets et le fichier est découpé en paquets contenant *P* bits de données. Montrer que l'expression T_{fic2} du temps de transmission du fichier sur ce réseau est donnée par $T_{fic2} = (S + L/P)(P + H)/D$
c) *Application numérique :* L = 64 000 octets ; H = 9 octets ; S = 2 commutateurs ; D = 64 kbit/s ; pour la taille du paquet, on prendra deux valeurs : P_a = 128 octets et P_b = 16 octets. Calculer et comparer les

valeurs obtenues pour T_{fic1} et T_{fic2} (pour la commutation par paquets, on comparera les deux tailles possibles de paquets).
d) Quels sont les avantages et inconvénients de la commutation de paquets par rapport à la commutation de message ?
e) Les liaisons sont affectées d'un taux d'erreur binaire noté τ. Montrer que la probabilité pour qu'une trame de longueur l soit reçue correcte est donnée par $p = (1 - \tau)^l$. En déduire que le nombre moyen N de transmissions d'une trame (en supposant que le protocole de contrôle répète la trame indéfiniment, sans anticipation, jusqu'à ce qu'elle soit correcte) est donné par $N = 1 / p$.
f) Refaire l'application numérique de la question c) en tenant compte du taux d'erreur $\tau = 10^{-4}$. Pour la commutation de message, il y a une trame unique contenant tout le fichier ; pour la commutation par paquets, une trame transporte un paquet.
g) Conclure. Ces techniques sont-elles adaptées aux hauts débits ? Pourquoi ? Quelles solutions existent pour de tels environnements ?

Exercice 11

Chaque ETTD veut envoyer 4 paquets de données aux deux autres. Le plus grand numéro de voie logique disponible est 7 pour tous les ETTD. L'$ETTD_1$ a ouvert les circuits virtuels avec l'$ETTD_2$ et l'$ETTD_3$; l'$ETTD_3$ a ouvert le circuit virtuel avec l'$ETTD_2$. Représentez la suite des paquets échangés entre les ETTD et les ETCD, en supposant que :
– les circuits virtuels sont des circuits permanents (CVP) déjà ouverts,
– les fenêtres des différents circuits virtuels sont respectivement :
entre l'$ETTD_1$ et l'$ETTD_2$: W = 1
entre l'$ETTD_1$ et l'$ETTD_3$: W = 2
entre l'$ETTD_2$ et l'$ETTD_3$: W = 3
– l'acquittement des paquets de données est local,
– on entrelace les données des différents circuits virtuels pour minimiser le temps de transfert global des données.



Exercice 12

Soit un terminal ($ETTD_A$) conforme à la norme X25, chargé d'envoyer à un ordinateur ($ETTD_B$) un fichier de 4 Mégaoctets par le réseau Transpac. On suppose que le transfert de données s'effectue sans erreur et que la taille des paquets de données est de 128 octets. La taille de la fenêtre du CVC est prise égale à 7.
a) Décrivez les différentes phases nécessaires à l'échange en indiquant la nature des paquets échangés.
b) Décrivez les équipements nécessaires entre l'$ETTD_A$ et le réseau, ainsi que les caractéristiques de chacun d'eux.

Exercice 13

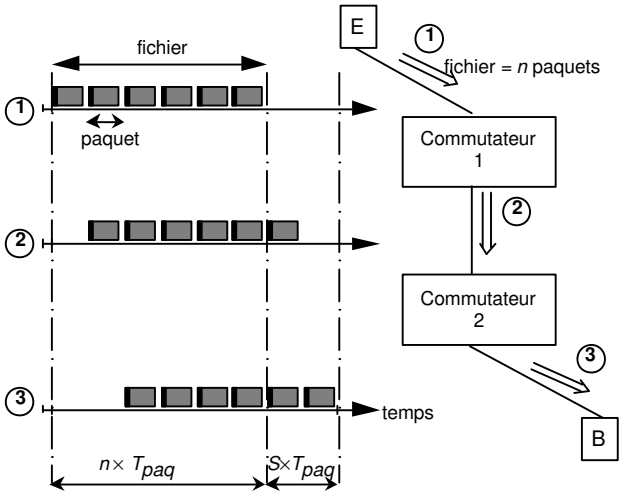
On considère trois réseaux à commutation de paquets ayant n nœuds. Le premier a une topologie en étoile avec un nœud central auquel sont connectés les n–1 autres nœuds, le second a une topologie en anneau, chaque nœud étant connectés à deux nœuds voisins, le troisième a un maillage complet. Toutes les

liaisons entre les nœuds sont bidirectionnelles simultanées. Comparer ces trois topologies (efficacité, routage, complexité, …).

Quelques corrigés

Exercice 10

1) Soient L la taille du fichier en bits, P la taille du paquet dans le réseau, H la taille de l'en-tête et d le débit d'une liaison. Soit S le nombre de commutateurs traversés pour une communication entre A et B.
La durée de transmission T_{paq} d'un paquet sur une liaison est :
$T_{paq} = (P+H)/d$
La durée de transmission T_{fic} d'un fichier est égale à la durée de transmission des paquets jusqu'au premier commutateur plus le délai nécessaire au dernier paquet pour parvenir jusqu'à l'équipement B.
Le nombre n de paquets transmis est égal à L/P. On en déduit :
$T_{fic} = (S + n)\ T_{paq} = (S + n)\ (P+H)/d$



Application numérique
cas 1.1
$P = L = 64\ 000 * 8 = 512\ 000$ bits
$T_{fic} = (2+1)*(64\ 000+9)*8/64\ 000 = 24$ s

cas 1.2
$P = 128 * 8 = 1024$ bits
$n = L/P = 500$ paquets
$T_{fic} = (2+500)*(128+9)*8/64\ 000 = 8{,}6$ s

cas 1.3
$P = 16 * 8 = 128$ bits
$n = L/P = 4000$ paquets
$T_{fic} = (2+4000)*(16+9)*8/64\ 000 = 12{,}5$ s
Conclusion : le découpage en paquets permet de réduire le délai d'acheminement à travers le réseau. Cependant, il a pour effet d'augmenter la part relative des en-têtes par rapport au message total. Une taille de paquet trop petite provoque ainsi un allongement du délai d'acheminement.
2) Pour qu'une trame de longueur l soit reçue sans erreur, il faut que tous les bits soient bien reçus donc le taux d'erreur trame est P_t :
$P_t = 1-(1-P_b)^l$

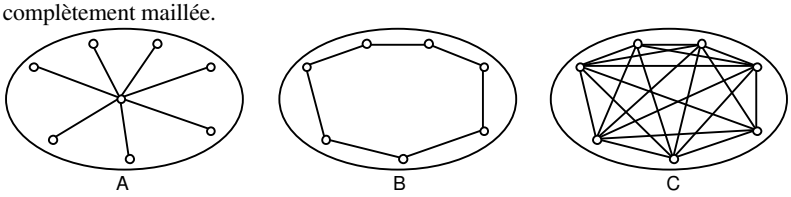
où P_b désigne le taux d'erreur bit.
La longueur d'une trame est due à la longueur des en-têtes et du contenu et vaut
$l = P+H$.
Le nombre moyen d'émissions est donc
$1.(1-P_t) + 2(1-P_t)P_t + 3(1-P_t)P_t^2 + \ldots = 1/(1-P_t)$
On peut appliquer la formule précédente en tenant compte des répétitions, d'où
$T'_{fic}=T_{fic}/(1-P_t) = T_{fic} / (1-P_b)^l$
Application numérique
cas 1.1
$P = L = 64\,000 * 8 = 512\,000$ bits
$T'_{fic} = 16848$ s soit plus de 4 heures !

cas 1.2
$P = 128 * 8 = 1024$ bits
$T'_{fic} = 9{,}6$ s soit une dégradation de 11,6 % par rapport au cas parfait

cas 1.3
P = 16 ∗8 = 128 bits
$T'_{fic} = 12{,}75$ s soit une dégradation de 2 % par rapport au cas parfait
Conclusion : la prise en compte du taux d'erreur dans les liaisons renforce l'intérêt du découpage en paquets. Il est visiblement hors de question d'envisager dans ce cas la commutation de messages. Cependant, il reste peu judicieux d'utiliser des paquets de trop faible taille. La taille de 128 octets reste un bon compromis.

Exercice 13

Appelons A le réseau à topologie en étoile, B le réseau à topologie en anneau et C le réseau à topologie complètement maillée.



Comparaison des trois réseaux, voir tableau ci-contre.

	Réseau A	Réseau B	Réseau C
nb de liaisons coût	n-1 faible	n faible	$n(n-1)/2$ très élevé
routage	très simple	simple : chaque nœud doit connaître ses voisins de droite et de gauche	immédiat : deux nœuds sont directement reliés
fiabilité	mauvaise : la panne du nœud central coupe **toutes** les communications	bonne mais limitée à une ou deux pannes	excellente, même avec un grand nombre de pannes, il y a toujours un moyen d'atteindre le destinataire
complexité	faible, sauf pour le nœud central qui supporte tout	faible	grande si on souhaite une efficacité maximale
lg moyenne des chemins	≅ 2	≅ $n/4$	1
efficacité	bonne	moyenne	très grande

Réseaux locaux d'entreprise et interconnexion

Pour répondre à leurs besoins propres en informatique distribuée, les entreprises ont commencé à mettre en œuvre, au sein de leurs établissements des *réseaux locaux d'entreprise,* les RLE ou LAN (*Local Area Network*). Ces réseaux utilisent des protocoles assez simples. Les distances couvertes sont courtes, de quelques centaines de mètres à quelques kilomètres, et les débits peuvent être importants, jusqu'à plusieurs dizaines de Mbit/s.

Ces réseaux se sont prolongés par la suite, surtout aux États-Unis, par des réseaux plus étendus, entre établissements d'une même ville, ou MAN (*Metropolitan Area Network*), ou interurbains, les WAN (*Wide Area Network*).

Les réseaux locaux informatiques ont été introduits pour répondre aux besoins de communication entre ordinateurs au sein d'une entreprise. Dans une structure commerciale, le réseau local est utilisé pour des applications de gestion. Dans un environnement bureautique, il sert à la création de documents, à la gestion d'agenda, à l'analyse de données, etc. Il s'agit de relier un ensemble de ressources devant communiquer entre elles et d'en assurer le partage à haut débit : stations de travail, imprimantes, disques de stockage, ordinateurs, équipements vidéo. L'accès aux réseaux publics de données est recherché dans un stade ultérieur.

Les réseaux locaux peuvent aussi être utilisés dans un environnement de production automatisée ; ils prennent alors le nom de *réseaux locaux industriels*, ou RLI, pour la Conception et la Fabrication Assistée par Ordinateur, la CFAO. Il s'agit d'interconnecter divers équipements de contrôle et de mesure, des capteurs et des actionneurs, pour échanger des informations qui doivent être exploitées très rapidement. Ces réseaux locaux doivent avoir un haut degré de fiabilité et traiter certaines informations en temps réel.

Un réseau local est caractérisé par des stations géographiquement proches les unes des autres et, en général, par son aspect diffusif : tout bit émis par une station sur le réseau local est reçu par l'ensemble des stations du réseau.

Les principales caractéristiques fonctionnelles attendues des réseaux locaux informatiques sont la capacité, la connectivité, l'interconnexion, la configuration, la diffusion et la fiabilité :

– la capacité se définit par le débit que fournit le réseau local et le type d'information qu'il transporte : voix, données, images ;

– la connectivité est la capacité de raccorder physiquement des équipements au support physique, et d'assurer leur compatibilité au niveau du dialogue ;

– l'interconnexion traduit la possibilité de relier le réseau local à d'autres réseaux locaux et aux réseaux publics par des ponts, des routeurs et des passerelles ;

– la configuration représente la capacité du réseau local à s'adapter aux changements de sa structure d'accueil (déplacement, ajout, retrait d'équipements) et à la définition des accès aux ressources ;

– la diffusion, ou *broadcast*, permet à toute station d'envoyer un message à l'ensemble ou à un sous-ensemble de stations du réseau ;

– la fiabilité prend plus ou moins d'importance selon le type d'application supportée par le réseau local.

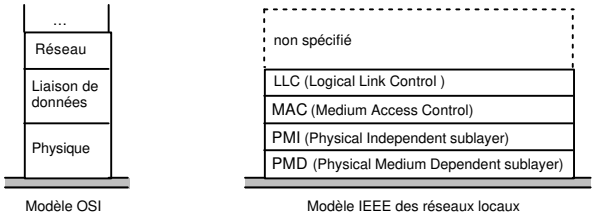
Les architectures de réseaux locaux

Dans les réseaux locaux informatiques, les protocoles d'accès sont assez simples. Ils respectent le principe de la structuration en couches. Ils ne requièrent cependant qu'une partie des fonctionnalités des 7 couches normalisées et peuvent ne mettre en jeu qu'une partie de ces couches, généralement les deux premières.

En revanche, on ajoute une sous-couche qui n'existe pas dans le modèle normalisé: la sous-couche MAC (*Medium Access Control*), dont le rôle est de permettre le partage du support, c'est-à-dire celui de la bande passante, par plusieurs utilisateurs. Cette sous-couche est située entre la couche 1 (Physique) et la couche 2 (Liaison de données) ; elle est souvent considérée comme une sous-couche de la couche Liaison, celle-ci étant appelée LLC, *Logical Link Control*. Grâce à la couche MAC, la couche LLC peut se comporter comme si les stations du réseau étaient toutes reliées deux à deux. La couche MAC a pour fonction de régler l'accès au médium partagé et de filtrer les trames reçues pour laisser passer celles réellement destinées à la station.

L'adoption d'une architecture en couches permet de disposer d'une même couche LLC quelle que soit la technique de partage du support utilisée. La normalisation ne concerne pas les couches au-dessus de

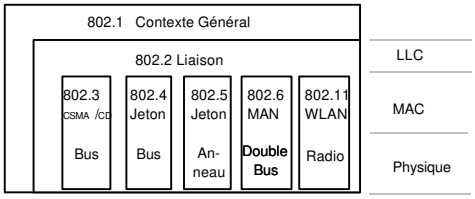
LLC ; il est possible d'implanter directement des protocoles applicatifs ou des protocoles d'interconnexion de réseaux .
La couche physique est quelquefois découpée en une couche PMI, *Physical Media Independent sub-layer*, qui assure le codage en ligne indépendamment du type de support de transmission utilisé, et une couche PMD, *Physical Media Dependent sub-layer*, qui assure l'émission physique du signal.



Modèle en couches des réseaux locaux

Normalisation

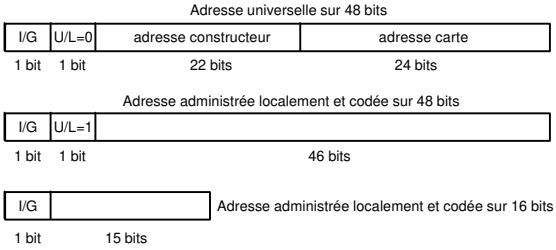
Les travaux de normalisation ne concernent que les deux premières couches. Ils sont menés par le comité 802 de l'IEEE (Institute for Electricity and Electronics Engineers. Le comité 802 de cette société savante s'est occupé de normalisation des réseaux locaux. Il est essentiellement constitué de constructeurs américains), repris par l'ISO sous le numéro 8802 :
– la norme 802.1 définit le contexte général des réseaux locaux informatiques,
– la norme 802.2 définit la couche liaison de données,
– les normes 802.3, 802.4, 802.5 et 802.6, définissent différents protocoles d'accès au support, pour les différents types de supports physiques, la paire symétrique, le câble coaxial ou la fibre optique, qui sont considérés comme fiables et offrant un débit de transmission important,
– la norme 802.11 définit un protocole d'accès pour les réseaux locaux sans fils (WLAN, *Wireless LAN*).



Portée des différentes normes

Adressage

Pour différencier les stations reliées sur un même réseau local, il est nécessaire de les repérer par une adresse. Celle-ci est gérée au niveau MAC et possède un format défini par l'IEEE sur 16 bits ou sur 48 bits. Ce dernier format permet un adressage universel des équipements : il correspond à un numéro de série avec un champ donnant le constructeur qui est attribué par l'IEEE, et le numéro de la carte librement choisi par le constructeur. De cette façon, toute carte réseau d'un ordinateur possède une adresse unique dans le monde. Le format universel sur 48 bits est le plus utilisé.
Il est possible de définir des adresses de groupe qui englobent plusieurs utilisateurs. Lorsque tous les bits sont positionnés à 1 (sur 16 bits ou sur 48 bits), il s'agit d'une adresse de diffusion correspondant à l'ensemble des stations d'un réseau local.



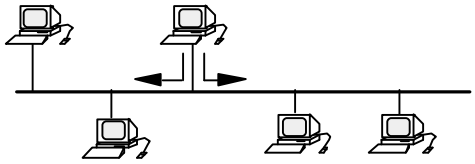
Le bit I/G=0 pour une adresse individuelle, I/G=1 pour une adresse de groupe.

Adressages dans les réseaux locaux

Topologie

La topologie d'un réseau décrit la façon dont ses stations sont reliées. On distingue trois types de topologie : en *bus,* en *anneau,* en *étoile.*

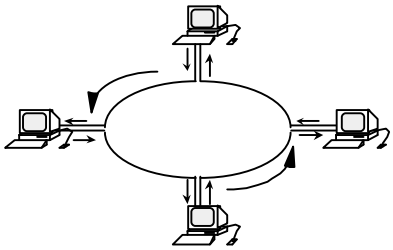
Dans la topologie en bus, tous les éléments sont reliés à un support physique commun. Une structure en " arbre sans racine " est utilisée. Les topologies en bus sont conçues de façon à ce qu'il n'y ait qu'un seul chemin entre deux éléments du réseau. Il n'y a pas de boucles. Le support est de type bidirectionnel, il permet l'émission d'informations sur le bus vers les stations " amont " et " aval ". La topologie en bus permet de faire des communications de point à point et se prête naturellement à la diffusion.



Topologie en bus

Dans la topologie en anneau, le support relie toutes les stations deux à deux, de façon à former un anneau. Le support est utilisé de façon unidirectionnelle et l'information circule dans un seul sens. Toute station, hormis celle qui génère la trame, réémet le signal reçu provoquant la diffusion de la trame dans l'anneau. On parle quelquefois de *topologie active* ou d'*anneau actif* pour souligner le fait que la diffusion est prise en charge par chaque station au contraire du bus qui est intrinsèquement diffusif.

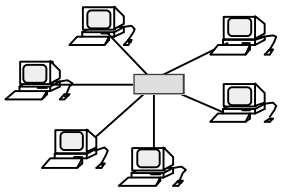
Le problème de cette topologie est son manque de fiabilité en cas de rupture du support. C'est pour cette raison que l'on double parfois le support. Les deux anneaux peuvent transmettre dans le même sens ou en sens inverse. La seconde solution est préférable car elle permet de reconfigurer le réseau en cas de rupture des deux anneaux.



Topologie en anneau

Dans la topologie en étoile qui est aussi la topologie des centraux multiservices, tous les éléments du réseau sont reliés à un nœud central. Cette topologie présente également des fragilités : en cas de panne

du nœud central, le réseau est inutilisable. Le point de concentration central peut aussi constituer un goulet d'étranglement s'il est mal dimensionné et entraîner la dégradation des performances du réseau.



Topologie en étoile

Politique de câblage

Le support physique des réseaux locaux informatiques représente le système nerveux de l'installation. La mise en place du câblage constitue un service de base, au même titre que l'infrastructure électrique des bâtiments. C'est pourquoi il est nécessaire de disposer d'un système de câblage universel, adapté à la diversité des équipements et permettant la mise en œuvre de toutes les architectures de réseaux. Il existe deux possibilités de câblage.

Le *post-câblage* consiste à installer l'infrastructure de communication au fur et à mesure des besoins, dans des bâtiments généralement non prévus pour cela. L'accroissement du parc des stations informatiques connectées aux réseaux locaux et les restructurations-déménagements donnent lieu à des modifications de câblage continuelles et coûteuses.

Le *précâblage* conçu dès la construction, consiste à poser un réseau de conducteurs en grande quantité, offrant une grande souplesse d'arrangement. Le précâblage est évidemment moins coûteux mais il n'est réalisable que dans de nouveaux locaux. Le précâblage deviendra probablement systématique et apportera une présence de câbles à tous les étages, même si l'on ne connaît pas l'affectation des bâtiments.

L'organisation du câblage repose sur l'existence de locaux de sous-répartition dans les étages ou les couloirs, et une distribution semblable depuis les sous-répartiteurs jusqu'aux postes de travail des différents bureaux. Les sous-répartiteurs sont reliés par des câbles de plus forte capacité à un répartiteur central avec un câblage en étoile, qui est compatible avec une organisation du réseau en bus ou en anneau. Une gestion technique du système de câblage est prévue par certains constructeurs.

Les principaux supports de transmission des réseaux locaux sont, comme nous l'avons vu au chapitre II, des câbles, constitués de paires symétriques, de câbles coaxiaux ou de fibres optiques.

La paire torsadée est le support le plus couramment employé. Ses avantages sont le faible coût et la facilité d'installation ; ses inconvénients sont la mauvaise immunité aux bruits. Les paires torsadées permettent des débits de l'ordre du Mégabit par seconde, certains constructeurs proposent 10 voire 100 Mbit/s, mais sur de courtes distances. Certains constructeurs proposent des paires torsadées blindées (*Shielded Twisted Pair)* plus résistantes aux interférences mais plus coûteuses.

Le câble coaxial, largement utilisé, présente des caractéristiques très intéressantes, mais à un coût plus élevé que la paire torsadée. Deux types de transmission sont possibles : la transmission numérique en *bande de base* et la transmission analogique par *étalement de bande* avec laquelle plusieurs communications simultanées utilisent chacune une porteuse particulière. Les avantages du câble coaxial sont des performances supérieures à la paire torsadée et une meilleure immunité aux bruits ; son inconvénient, une installation moins souple.

La fibre optique est de plus en plus utilisée malgré un coût plus élevé. Les avantages en sont une totale immunité aux bruits, un très faible poids, un encombrement minimal et une très large bande passante ; les inconvénients, le coût et la complexité de connectique.

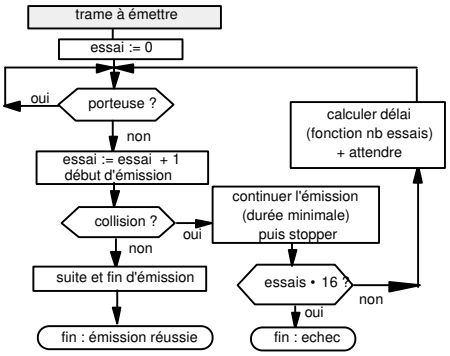
Techniques d'accès au support

Les réseaux locaux informatiques nécessitent un partage de la bande passante utile entre les différents utilisateurs du réseau. Il existe différentes techniques d'accès au support. Elles peuvent être déterministes ou aléatoires.

Les techniques déterministes sont celles où l'allocation de la bande se fait dynamiquement en fonction de l'activité des stations ; c'est le cas du contrôle centralisé par *polling,* où une station maîtresse interroge tour à tour les autres stations pour leur donner l'occasion d'émettre ou de recevoir. C'est aussi le cas des protocoles à *jeton* où le droit d'utiliser la bande est donné explicitement par la remise d'une trame particulière appelée jeton.
Dans les techniques à accès aléatoire, chaque station tente sa chance pour obtenir l'accès à la bande et il existe plusieurs protocoles basés sur une telle technique comme Aloha (La plus ancienne méthode de contrôle des accès à un support physique. Elle consiste à envoyer l'information sans s'occuper de ce qui se passe sur le support et à retransmettre l'information au bout d'un temps aléatoire en cas de collision. Son nom provient d'un génie des légendes hawaïennes car c'est dans l'archipel d'Hawaï que cette technique a été expérimentée pour la première fois, avec un réseau hertzien reliant les différentes îles…) et CSMA/CD, qui doivent résoudre des problèmes de collisions.

Techniques d'accès aléatoire au support

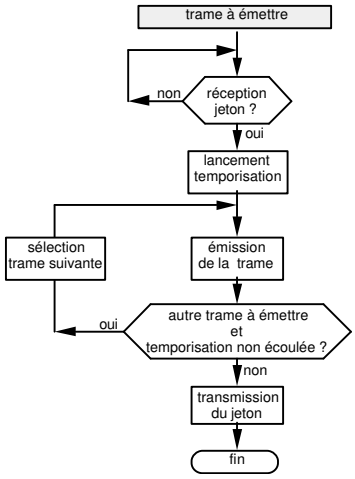
Dans les méthodes de type CSMA, pour *Carrier Sense Multiple Access*, (IEEE 802.3), les stations se mettent à l'écoute du canal et attendent qu'il soit libre pour émettre. Les transmissions ne sont pas instantanées par suite des délais de propagation, et une collision peut se produire au moment où une station émet, même si elle a écouté le canal au préalable et n'a rien entendu. Plus le délai de propagation est grand, plus le risque de collision est important.
Il existe différentes variantes du protocole. La plus classique est celle des réseaux 802.3 : CSMA/CD, pour CSMA with *Collision Detection*. Sa particularité est que la station *continue* à écouter le canal après le début de l'émission et *arrête* immédiatement l'émission si une collision est détectée. Le temps pendant lequel on écoute ainsi, alors qu'on est en train de transmettre, est limité à quelques microsecondes (temps de propagation aller retour entre les deux stations les plus éloignées). La durée de la collision est ainsi réduite au minimum. Le temps nécessaire pour émettre une trame ne peut pas être garanti avec le CSMA/CD. En effet, les retransmissions sont effectuées après une durée aléatoire qui dépend du nombre de tentatives et après 16 tentatives infructueuses, on abandonne. L'intérêt de cette technique est qu'elle ne nécessite pas la présence d'une station maîtresse.



Algorithme d'émission CSMA/CD

Techniques d'accès déterministe au support

La méthode du jeton peut être utilisée sur un bus ou sur un anneau. Le jeton circule de station en station. Une station qui reçoit et reconnaît le jeton émis par la station précédente peut alors accéder au support. En fonctionnement normal, une phase facultative de transfert des données alterne avec une phase de transfert du jeton. Chaque station doit donc être en mesure de gérer la réception et le passage du jeton, en respectant le délai maximum défini par la méthode. Les stations doivent également prendre en compte l'insertion d'une nouvelle station. Enfin, elles doivent réagir à l'altération voire à la perte du jeton en mettant en œuvre un mécanisme de régénération du jeton.



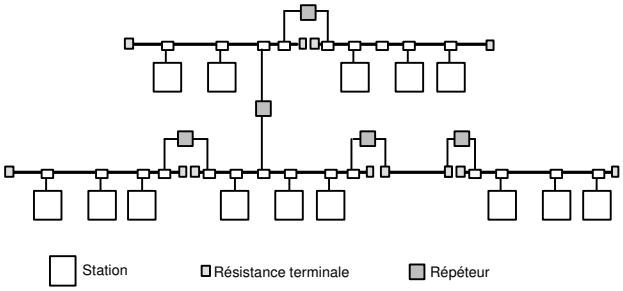
Principe général de l'accès par jeton

Description des réseaux de première génération

Le premier réseau local utilisant le CSMA/CD sur un bus a été développé par la société Xerox pour le produit appelé Ethernet. Il a eu un succès considérable et les sociétés Xerox, DEC et Intel ont décidé d'en faire un standard qui a servi de base au comité IEEE 802.3 pour sa norme. Toutefois, le produit Ethernet et le standard IEEE 802.3 diffèrent sur des points mineurs. Il est d'usage courant de appeler Ethernet tout réseau local utilisant le CSMA/CD. Nous présentons ici la norme IEEE 802.3 dans ses grandes lignes.

Caractéristiques physiques des réseaux IEEE 802.3 CSMA/CD

Les réseaux IEEE 802.3 utilisent une transmission en bande de base avec un code Manchester. Afin que toutes les stations reçoivent un signal de niveau suffisant, la longueur du bus est limitée à 500 mètres. Pour atteindre des longueurs supérieures, il est possible d'utiliser des *répéteurs*, qui décodent les signaux reçus et les régénèrent mais ne les interprètent jamais (ils n'ont pas de couche MAC mais juste une couche physique).
Les répéteurs introduisent un retard de quelques bits et contribuent à augmenter le délai de propagation. Ils permettent de relier entre eux différents segments de façon à former un seul bus logique et un seul domaine de collision. Pour limiter les risques de collision, le délai de propagation aller-retour du signal entre les deux stations les plus éloignées doit être inférieur à 51,2 µs ce qui limite à 4 le nombre de répéteurs traversés pour relier 2 stations (soit au plus 5 segments reliés en série). La structure d'un réseau peut donc être plus compliquée qu'un simple bus reliant toutes les stations.
Chaque extrémité d'un bus est muni d'une résistance terminale ou " terminateur" qui présente une impédance de 50 Ω, impédance caractéristique du bus. Son rôle est de d'absorber le signal électrique qui se propage, l'empêchant au maximum d'être réfléchi en sens inverse et de provoquer un brouillage du signal par lui-même.



Exemple de réseau IEEE 802.3

Format de la trame dans les réseaux IEEE 802.3 CSMA/CD

Le format de la trame de base comporte un long préambule (101010…) provoquant l'émission d'un signal rectangulaire de fréquence 10 MHz et permettant à l'ensemble des stations du réseau de se synchroniser sur l'émetteur. Le champ SFD, *Start Frame Delimitor*, contient une séquence particulière (10101011) et marque le début de la trame. La trame contient également l'adresse du destinataire DA, *Destination Address*, et de l'expéditeur SA, *Source Address*. Un champ de longueur précise le nombre d'octets des données de niveau supérieur (i.e. données LLC) dans la trame. Celle-ci est complétée par des octets de bourrage si la taille est inférieure ou égale à 64 octets. La validité des trames reçues est contrôlée par un bloc de contrôle d'erreur placé dans le champ FCS, *Frame Check Sequence.*

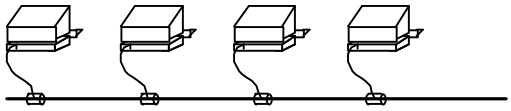
10101010	10101010	10101010	10101010	10101010	10101010	10101010	10101011
DA- Adresse Destination (48 bits)							
SA- Adresse Source (48 bits)							
Protocole ou longueur (16 bits)							
Données (de 46 à 1500 octets) et bourrage éventuel							
FCS- Bloc de contrôle d'erreur (32 bits)							

La taille de la trame (moins les 8 octets de préambule) doit être comprise entre 64 et 1518 octets, ce qui laisse de 46 à 1500 octets "utiles". Un contenu plus court que 46 octets est complété par des caractères de remplissage.
Dans la norme, le champ protocole était supposé indiquer la longueur effective du contenu de la trame. Dans la pratique, le contenu de la trame (IP, ARP, etc) décrit implicitement la longueur et le champ est utilisé pour dénoter le protocole utilisé.
Le champ "protocole" peut prendre les valeurs suivantes (en hexadécimal) :
0800 protocole IP
0806 protocole ARP
0835 protocole RARP

Plan de câblage des réseaux IEEE 802.3 CSMA/CD

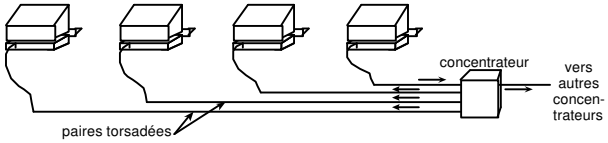
Le plan de câblage définit la façon dont on organise physiquement les connexions des stations. Il peut suivre la topologie en bus, ou bien être en étoile.
La nomenclature usuelle désigne le type de câblage et de topologie physique par sous la forme *X*Base*t* où *X* désigne le débit exprimé en Mbit/s, Base indique une transmission en bande de base et *t* renseigne sur le type de câble ou la longueur maximale d'un segment.
Les câblages les plus anciens sont le 10 Base 5 et le 10 Base 2 :
– 10 Base 5 est un coaxial de 500 mètres maximum par segment, généralement blanc, permettant un débit en bande de base de 10 Mbit/s, utilisé dans l'Ethernet classique,

– 10 Base 2 est un coaxial fin de 180 mètres maximum par segment, généralement jaune, permettant un débit en bande de base de 10 Mbit/s, utilisé dans Cheapernet.



Câblage en bus

La grande faiblesse d'un câblage en bus est sa sensibilité aux incidents : si le bus est coupé, on se retrouve en présence de deux bus ayant chacun une extrémité sans répéteur. La désadaptation d'impédance provoque un " auto-brouillage " dû aux phénomènes d'écho.
On a massivement recours au câblage en étoile : toutes les stations sont branchées sur un " concentrateur" ou *hub,* qui retransmet sur l'ensemble des ports tout signal reçu sur un port quelconque. La topologie logique reste donc celle d'un bus et le fonctionnement de l'accès par CSMA/CD est inchangé. Les câblages dans ce cas sont les suivants :
– 10 Base T (T pour *Twisted pair*) est une paire en bande de base de 100 m par segment, à 10 Mbit/s,
– 10 Base F (T pour *Fiber*) est une fibre optique de 2,5 km, en bande de base à 10 Mbit/s,
– 10 Broad 36 est un câble de télédistribution de 3,6 km, avec étalement de bande, à 10 Mbit/s par canal (impédance 75Ω).
Le câblage en étoile a été initialement introduit par ATT dans le produit Starlan sous la référence 1 Base 5. Il est constitué de paires symétriques téléphoniques de 2 km, permet un débit de 1 Mbit/s et 5 concentrateurs. Le principal intérêt est son très faible coût.

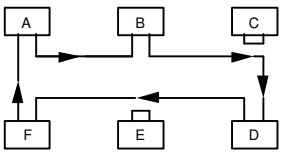


Câblage en étoile avec paire torsadée

La grande force de 802.3 est sa simplicité : l'utilisation d'un médium diffusif (ou d'un concentrateur) rend l'ajout et le retrait de station très simple. A faible charge, l'accès est quasiment immédiat. En revanche, le réseau supporte mal les fortes charges qui peuvent provoquer un effondrement du débit utile. De plus, le délai d'accès est non borné. En conclusion, 802.3 est surtout orienté vers la bureautique. Sa simplicité d'utilisation en fait le réseau d'entreprise le plus utilisé pour ces applications.

Principe général des réseaux IEEE 802.5 ou anneau à jeton

L'anneau à jeton ou *Token Ring* a été principalement développé par la société IBM et normalisé par l'IEEE dans le standard 802.5.
L'anneau à jeton est un anneau simple unidirectionnel : chaque station est reliée à deux autres, en point à point. Une station en service est normalement insérée dans l'anneau. Elle peut s'extraire de l'anneau — elle se met en *by-pass* — en cas de panne ou de mise hors tension. Des dispositifs électroniques ou électromagnétiques permettent à l'anneau de se reconfigurer automatiquement en cas d'incident.



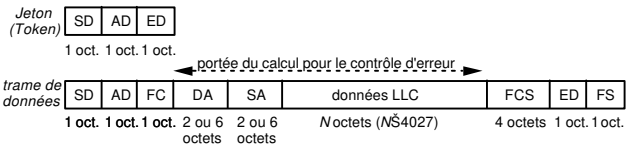
Les stations C et E sont en *by-pass.*

Constitution d'un anneau

Une station qui ne détient pas le jeton se comporte comme un répéteur physique : elle régénère bit à bit le signal reçu et prend copie du message reçu. L'équipement qui détient le jeton émet une trame vers son successeur qui le retransmet au suivant et ainsi de suite jusqu'à l'équipement émetteur. Ce dernier peut ainsi vérifier en comparant la trame reçue et la trame émise que celle-ci a correctement fait le tour de l'anneau. Lorsqu'un équipement a transmis sa ou ses trames il transmet un jeton et se met en réémission.

Format de la trame dans les réseaux IEEE 802.5 anneau à jeton

Le format des trames est différent. Le jeton est une trame particulière écourtée dont le format correspond au début d'une trame normale. Lorsqu'aucune station n'a de trame à transmettre, le jeton circule dans l'anneau, chaque station se comportant comme un répéteur. Il est donc nécessaire que la durée τ entre l'émission d'un bit et la réception de ce même bit après un tour d'anneau soit supérieure à la durée de transmission du jeton c'est-à-dire que la latence soit supérieure à la longueur du jeton, soit 24 bits. Si l'anneau est trop petit, une station particulière appelée moniteur de boucle ou *Monitor*, gère une petite mémoire tampon pour retarder la réémission et porter la latence à 24 bits.
Le champ SD, *Start Delimitor*, marque le début le trame. Le champ AD, *Access Control*, indique s'il s'agit d'un jeton libre ou d'une trame. Il comporte de plus un bit M géré par le moniteur, et deux groupes de 3 bits chacun, donnant la priorité du jeton ou de la trame transmise et la priorité des trames en attente dans les stations de l'anneau. Le champ FC, *Frame Control*, donne le type de trame. Les champs DA, SA, données LLC et FCS sont définis comme dans IEEE 802.3. Le champ ED, *End Delimitor*, délimite la fin du jeton ou de la trame de données. Pour cette dernière, il est suivi d'un champ FS, *Frame Status*, permettant de surveiller l'anneau.



Format de trame 802.5

Le champ FS contient deux fois deux bits A et S qui sont positionnés à 0 par l'émetteur de la trame. Toute station qui reconnaît son adresse (individuelle ou de groupe) positionne à 1 un des bits A qui était à 0. Elle positionne le bit S si elle a pu correctement décoder la trame et la stocker. Ces deux bits permettent donc de détecter la duplication d'une adresse individuelle (possible seulement en cas d'administration locale des adresses) et de s'assurer que la trame a été reçue par au moins une station.
La transmission se fait en bande de base suivant un code Manchester différentiel, caractérisé par une transition au " centre " du bit. Les délimiteurs de début et de fin comportent des codes appelés J et K qui sont caractérisés par une absence de transition et ne correspondent donc ni à un 0 ni à 1. Ils permettent de délimiter les trames en résolvant les problèmes de transparence

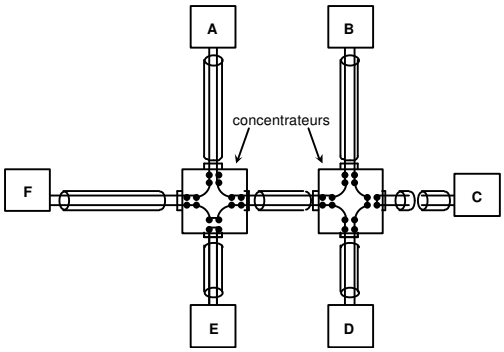
Gestion de l'anneau dans les réseaux IEEE 802.5

Lorsqu'une station détient le jeton, elle peut émettre une trame. Celui-ci fait le tour de l'anneau et lui revient : par le jeu des différents indicateurs (champ AD, bits A, S…), elle vérifie que l'anneau n'est pas coupé, qu'il n'y a pas duplication du moniteur, que la trame a été recopiée par le destinataire, et détecte la demande de jeton de plus haute priorité exprimée par une des stations du réseau. Elle peut ensuite émettre une autre trame ou transmettre un jeton libre à son successeur. Il est nécessaire que la station reçoive le début de sa trame avant de pouvoir émettre un jeton libre.
Afin d'éviter toute utilisation abusive du support, chaque station arme un temporisateur au début la phase d'émission et doit obligatoirement passer le jeton lorsque celui-ci arrive à échéance. On peut affecter différentes priorités aux stations. Celle qui a une trame en attente de priorité inférieure à celle du jeton ne peut capturer le jeton. Elle doit attendre un passage du jeton avec un priorité inférieure ou égale à celle de sa trame.
Le fonctionnement d'un anneau à jeton est assez compliqué quand on considère les cas d'incidents et de mise en service : à l'initialisation, il faut créer un jeton ; la mise hors service d'une station qui possède le

jeton provoque la disparition de celui-ci. Une station appelée moniteur, élue par ses paires, surveille la présence des stations, régénère le jeton en cas de perte, détecte les messages ayant fait plus d'un tour, assure la synchronisation bit, etc. Le moniteur fournit une méthode de correction de la contenance de l'anneau, qui permet à l'anneau initial, quelle que soit sa taille, de contenir le jeton. Toutes les stations peuvent jouer le rôle de moniteur, pour suppléer le moniteur actif en cas de panne.

Plan de câblage dans les réseaux IEEE 802.5

Le plan de câblage généralement proposé pour l'anneau à jeton comprend un ensemble d'étoiles. Un concentrateur actif AWC, *Active Wire ring Concentrator*, permet de constituer l'anneau. Par des dispositifs électroniques ou électromécaniques, il surveille la présence active de chaque station (détection d'une station hors station, d'un câble coupé…) et reconfigure automatiquement l'anneau en cas d'incident en excluant la station concernée (mise en *by-pass*). Il est possible de relier plusieurs concentrateurs entre eux pour augmenter la taille de l'anneau et le nombre des stations.
Le câble de raccordement entre la station et le concentrateur est généralement une paire torsadée blindée d'impédance 150 Ω. Les débits possibles sont de 1, 4 et 16 Mbit/s. Le nombre maximal de stations dans l'anneau peut aller jusqu'à 260.



La station E, hors-service, est mise en by-pass par le concentrateur 1. Le concentrateur 2 détecte la rupture du câble avec C et reboucle l'entrée-sortie correspondante.

Câblage physique

Le débit réel d'un anneau de 4 Mbit/s est très légèrement inférieur à 4 Mbit/s. Il résiste bien à la charge et le débit utile ne s'effondre jamais comme c'est possible avec 802.3. De plus, comme il est possible de borner le délai d'accès au médium, il permet d'envisager des dialogues entre machines sur lesquelles tournent des applications temps réel. Cependant la couche MAC est plus compliquée que pour 802.3 et à faible charge le délai d'accès est non nul puisqu'il faut attendre le jeton avant d'émettre (alors que l'accès est immédiat en CSMA/CD sur un bus libre).

Couche Liaison de données

La Couche Liaison de données, dans les réseaux locaux, définit le format, la structure et la succession des trames qui sont échangées. La norme IEEE 802.2 définit un protocole de commande, LLC pour Logical Link Control, qui est basé sur les formats du protocole normalisé HDLC. Trois types de LLC ont été définis :
– LLC1 est sans connexion et fournit un service de type *datagramme* sans aucun contrôle, en point à point, en multipoint ou en diffusion ;
– LLC2 assure un service avec connexion entre deux points d'accès et possède les fonctionnalités complètes d'une procédure telle que LAP-B, qui assure contrôle de flux et contrôle d'erreur ;
– LLC3, adapté au monde des réseaux industriels, rend un service sans connexion, mais avec acquittement. Il a l'avantage de LLC1 pour la rapidité avec la garantie du bon acheminement grâce à l'acquittement.

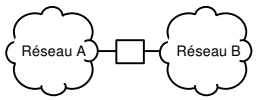
LLC1 est le protocole le plus courant. LLC1 possède trois trames différentes :
– UI *(Unnumbered Information)*, trame d'information non numérotée, correspondant à la notion de datagramme ;
– XID *(eXchange IDentifier),* trame de contrôle pour échanger des identifications ;
– TEST.

Format des trames LLC 1

Le champ *Control* est codé conformément au LAPB. Les champs " Address DSAP " (*Destination SAP*) et " Address SSAP " (*Source SAP*) sont les adresses des SAP (*Service Access Point*) source et destination, lesquelles, associées avec l'adresse physique de la couche MAC, désignent de manière unique l'origine et le destinataire de l'échange.

Interconnexion

Physiquement, deux réseaux ne peuvent être reliés que par l'intermédiaire d'une machine connectée à chacun d'eux et qui sait acheminer des paquets d'un réseau à l'autre. De telles machines sont appelées *passerelles*.



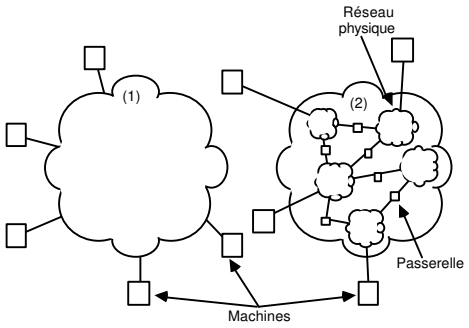
La passerelle doit accepter, sur le réseau A, les paquets destinés aux machines du réseau B et transmettre les paquets correspondants. De façon analogue, elle doit accepter, sur le réseau B, les paquets destinés aux machines du réseau A et transmettre les paquets correspondants.

Une passerelle reliant deux réseaux

Lorsque les interconnexions de réseaux deviennent plus complexes, les passerelles doivent connaître des informations relatives à la topologie de l'interconnexion, au-delà du réseau auquel elles sont connectées.

Trois réseaux reliés par deux passerelles

Les passerelles doivent bien évidemment savoir comment router les paquets vers leur destination. Ce sont souvent des mini-ordinateurs qui conservent des informations relatives à chacune des machines de l'interconnexion à laquelle ils sont reliés. Pour minimiser la taille des passerelles, les paquets sont acheminés en fonction du réseau destination et non en fonction de la machine destination. La quantité d'information gérée par une passerelle devient alors proportionnelle au nombre de réseaux de l'interconnexion et non au nombre de machines.
L'utilisateur voit une interconnexion comme un réseau virtuel unique auquel les machines sont connectées. Les passerelles, pour acheminer des paquets entre des paires quelconques de réseaux peuvent être obligées de leur faire traverser plusieurs réseaux intermédiaires. Les réseaux de l'interconnexion doivent accepter que des données extérieures les traversent. Les utilisateurs ordinaires ignorent l'existence du trafic supplémentaire acheminé par leur réseau local.

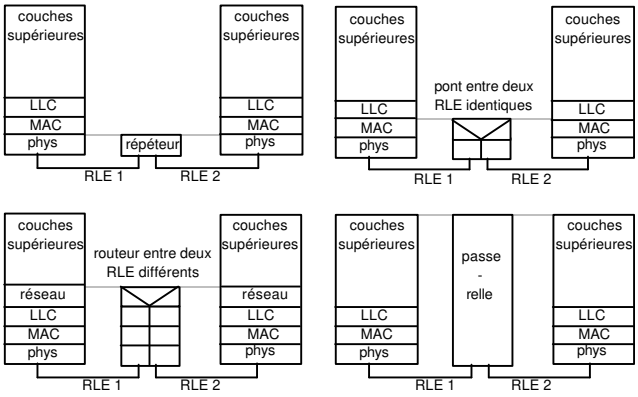


Une interconnexion de réseaux vue par l'utilisateur (1) : chaque machine semble être raccordée à un seul et immense réseau : le réseau virtuel unique.
La structure réelle (2) : des réseaux physiques interconnectés par des passerelles

Réseaux interconnectés

Interconnexion de réseaux locaux

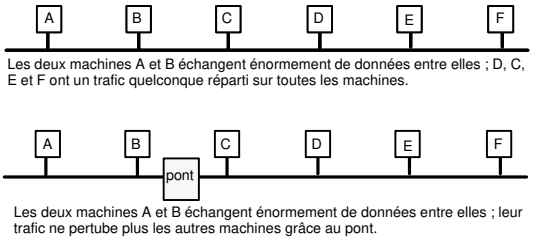
On ne conçoit plus désormais un réseau local sans une ouverture vers le monde extérieur, il devient nécessaire d'interconnecter les réseaux entre eux et de pouvoir les raccorder aux moyens de communication publics ou privés à grande distance. Plusieurs dispositifs d'interconnexion peuvent être mis en jeu



Niveaux d'interconnexion de réseaux locaux

Les *répéteurs* ne font que prolonger le support physique, en amplifiant les signaux transmis. Ils propagent donc les collisions.
Les *ponts* ou bridges en anglais, sont conçus pour construire un réseau local logique à partir de plusieurs réseaux locaux homogènes distants. Ce sont des connecteurs évolués qui interviennent au niveau de la couche MAC. Deux demi-ponts peuvent être reliés par une liaison grande distance. Les ponts ont progressivement évolué vers des équipements plus sophistiqués, appelés parfois *ponts filtrants*, ou brouter pour bridge-router en anglais, qui effectuent un filtrage des données et possèdent des fonctions de sécurité et de contrôle du trafic particulières. Les ponts filtrants permettent, par exemple, de détecter les chemins redondants entre deux réseaux locaux grâce à un échange d'informations de gestion interne. Les ponts sont transparents aux protocoles des couches supérieures.
Les ponts permettent également de segmenter un réseau local en deux sous-réseaux pour améliorer les performances. Dans un réseau Ethernet par exemple qui approche de la saturation, on peut chercher les couples de machines qui ont un gros trafic entre elles et les isoler de chaque côté du pont. Le pont

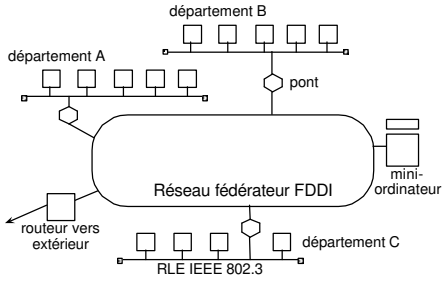
travaille alors par apprentissage : progressivement, il apprend à situer les stations sur chacun des sous réseaux (au fur et à mesure de leur activité). Dès qu'une trame se présente sur le pont et qu'elle est destinée au sous-réseau d'où elle vient, le pont la filtre : le deuxième sous-réseau ne la reçoit pas.



Introduction d'un pont dans un réseau local

Les *routeurs,* ou routers en anglais, sont destinés à relier plusieurs réseaux de technologies différentes. Ils opèrent au niveau de la couche Réseau et effectuent le routage des informations à travers l'ensemble des réseaux interconnectés. Ils sont plus chers et généralement moins performants que les ponts et ils sont liés à l'architecture des protocoles utilisés.

Les *passerelles,* ou gateways, entrent en scène dans les cas les plus complexes pour assurer une compatibilité au niveau des protocoles de couches hautes entre réseaux hétérogènes. Elles permettent à des postes situés sur le réseau local de dialoguer avec l'application située sur un ordinateur avec une architecture propriétaire.



Exemple de réseau fédérateur

Les grandes entreprises sont généralement structurés en départements qui sont dans des étages différents d'un bâtiment voire sur plusieurs bâtiments d'un même site. Le trafic global généré peut être important avec de gros échanges de données au sein des départements. Il est fréquent de constituer des réseaux pour chaque département (ou groupe de départements) et de relier tous ces réseaux par un réseau à haut débit qui fonctionne en réseau fédérateur ou *backbone.* La liaison de chaque réseau au réseau fédérateur se fait par un pont. Le trafic interne à un département reste cirsconcrit à son réseau propre. De plus, certains moyens informatiques communs à l'ensemble de l'entreprise peut être mis sur le réseau fédérateur et devenir accessible à tous de même que les accès à des réseaux externes (on met par exemple un routeur IP connecté à l'Internet).

L'évolution des réseaux locaux

L'intégration des réseaux locaux dans le système d'information et de communication de l'entreprise conduit au concept plus général de réseau d'entreprise, avec une transparence des accès pour l'utilisateur et donc la nécessité d'offrir les mêmes informations et les mêmes ressources informatiques, grâce à une réelle distribution des applications. L'évolution des réseaux tend vers des débits toujours plus élevés qui ont un impact sur l'efficacité.

Réseaux de type Ethernet

Si Ethernet a été initialement conçu pour fonctionner sur des câbles coaxiaux à un débit de 10 Mbit/s, il est devenu le réseau local le plus répandu dès que le câblage téléphonique a pu être utilisé. Fast Ethernet, une version à 100 Mbit/s compatible avec les réseaux à 10 Mbit/s, est maintenant largement diffusée. Gigabit Ethernet, une version à 1 Gbit/s (1000 Mbit/s) se répand de plus en plus. Les équipements Gigabit combinent généralement des ports à 10 et 100 Mbit/s avec une ou plusieurs connexions sur des fibres optiques à 1 Gbit/s. Gigabit Ethernet s'est développé dans les environnements commutés et possède deux modes de fonctionnement : les modes *duplex intégral* et *semi-duplex*.

Le duplex intégral permet à une station d'émettre et de recevoir simultanément des données, chaque station utilisant une voie pour chaque sens de communication. Il n'y a donc plus de collision possible avec les émissions des autres stations.

Le semi-duplex est employé lorsque les stations sont raccordées par un hub. Des collisions entre trames émises simultanément par différentes stations peuvent alors se produire. À cause du débit employé, le temps d'émission d'une trame est très faible. Des fonctionnalités supplémentaires dans la méthode d'accès ont dû être apportées : l'*extension de trame* et le *mode rafale*. La première consiste à porter la longueur minimale de la trame à 512 octets (au lieu de 64 octets dans l'Ethernet classique). La seconde permet à un émetteur d'envoyer en une seule fois plusieurs trames consécutives.

Réseaux locaux à commutateur et réseaux locaux virtuels

La limitation du débit utile dans un réseau Ethernet est due aux nombreuses collisions qui apparaissent à forte charge. Une solution pour améliorer l'efficacité consiste à abandonner le principe du médium diffusant et à utiliser un commutateur. Le commutateur stocke les trames émises par les stations et les retransmet ensuite. Il a une capacité de stockage permettant d'éviter tout conflit. Cette solution est appelée *Ethernet Commuté*.

Le passage d'Ethernet classique avec un concentrateur et un câblage en étoile à Ethernet commuté est transparent pour les stations. Elles restent à 100 Mbit/s par exemple (à 10 Mbit /s, quand cela existe encore…) et écoutent toujours le canal avant d'émettre. Chaque station dispose de la totalité de la bande de 100 Mbit/s entre elle et le commutateur, ce qui constitue une amélioration considérable. Les commutateurs proposent quelques ports rapides à 1Gbit/s.

L'introduction des commutateurs dans un réseau local a permis de construire des réseaux logiques indépendants les uns des autres. Ces réseaux sont définis en fonction des centres d'intérêt de leurs utilisateurs et non en fonction de la situation géographique des stations au sein de l'entreprise. On parle alors de *réseaux virtuels* ou *VLAN* (Virtual LAN). Un réseau virtuel regroupe une communauté d'usagers répartis dans toute l'entreprise, comme s'ils appartenaient au même réseau physique. Les échanges à l'intérieur d'un VLAN sont sécurisés et les communications entre VLAN contrôlées. Par exemple, le réseau virtuel réservé à la direction de l'entreprise fournit un espace de communication sécurisé à l'équipe directoriale. Celui-ci est logiquement distinct du réseau virtuel affecté aux services de production, même si les machines sont reliées aux mêmes commutateurs.

Plusieurs de niveaux de VLAN sont possibles, selon la manière dont les différentes stations du VLAN sont identifiées. Le *niveau 1* relie des machines connectées au même port du commutateur ; le *niveau 2* définit les machines d'un VLAN en fonction de leurs adresses MAC et le *niveau 3* regroupe les machines en fonction de leurs adresses IP. Avec les VLAN de niveaux 2 et 3, les machines peuvent appartenir à plusieurs VLAN et le commutateur contient une table de correspondance entre les VLAN et la liste des adresses associées. L'identification du VLAN utilisé est contenue dans un champ supplémentaire de la trame émise par la station.

Réseaux locaux sans fil

Les réseaux locaux sans fil WLAN s'utilisent comme les réseaux filaires et couvrent quelques centaines de mètres. Les technologies sans fil évoluant très rapidement, on trouve toute une série de normes physiques, repérées par la lettre suivant le terme générique 802.11. Elles se distinguent par la bande de fréquences utilisée, les débits binaires et la portée dans un environnement dégagé. Le *Wi-Fi* (802.11b) est l'une des premières solutions du standard 802.11. Il utilise la bande de fréquences 2,4 GHz sur une portée maximale de 300 mètres.

Les débits disponibles pour les réseaux sans fil varient de 11 Mégabit/s pour le 802.11b à 54 Mégabit/s pour le 802.11g. Deux autres solutions plus récentes coexistent dans la bande des 5 GHz (*Wi-Fi5* ou 802.11a et *HiperLan2* ou 802.11h).
Le protocole d'accès utilisé dans les réseaux locaux sans fil est CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), une variante des algorithmes de la famille CSMA. Ce protocole est destiné à limiter les risques de collisions entre émissions provenant de machines qui ne se « voient » pas, c'est-à-dire entre machines se trouvant hors de portée l'une de l'autre.
L'organisation interne d'un réseau local sans fil est soit indépendante de toute infrastructure (*réseaux ad hoc*), soit elle est structurée en domaines indépendants appelés *cellules* (*réseaux cellulaires*). Dans un réseau ad hoc, les communications sont directes, de machine à machine (connexions point à point). Les équipements d'un tel réseau sont de ce fait à la fois hôte et relais pour les stations hors de portée ; les règles topologiques des réseaux filaires sont alors inapplicables car la validité d'un itinéraire peut changer brusquement. De plus, les algorithmes de routage ont dû être adaptés pour tenir compte de la bande passante limitée et de la faible durée de vie des batteries.

Synthèse

Dans le domaine des communications locales à un bâtiment, un site, un campus (domaine privé), les solutions de communications sont nombreuses : *réseau local informatique* ou PABX.
L'utilisation d'un support unique partagé entre plusieurs utilisateurs dans un réseau local nécessite la mise en œuvre de protocoles spécifiques (accès aléatoire avec *détection de porteuse* ou mécanisme de *jeton*) ; par ailleurs, ces réseaux permettent la *diffusion* d'information et doivent être reliés au monde extérieur par des *passerelles* (relais, ponts, routeurs, selon le niveau de l'interconnexion).

Exercices

Exercice 1

Pourquoi la trame IEEE 802.3 (Ethernet) ne contient-elle pas de fanion de fin comme une trame type HDLC ? Pourquoi la trame IEEE 802.5 (Token Ring) ne contient-elle pas un long préambule comme la trame IEEE 802.3 ?

Exercice 2

Soit un réseau Ethernet en bus de 8 stations. La distance moyenne entre stations est de 15 mètres. La vitesse de propagation est de 250 m/µs. Quelle est la durée de la période de vulnérabilité ?
Lors de la reprise de la surveillance du jeton par un nouveau moniteur, celui-ci émet une trame AMP. La première station située en aval du moniteur récupère cette trame et émet à la place une trame SMP qui sera traitée par toutes les stations, afin que le moniteur puisse connaître la station qui le précède sur l'anneau. Cette méthode permet-elle de détecter la défaillance d'une station intermédiaire ? Sinon, comment peut-on diagnostiquer la défaillance d'une telle station ?

Exercice 3

Que se passe-t-il dans un réseau local en bus s'il n'y a pas de bouchon terminateur ?

Exercice 4

Dans un réseau local dont le débit binaire est de 5 Mbit/s, les signaux se propagent à la vitesse de 250 m/µs. Un bit transmis est équivalent à quelle longueur de câble ? Ceci a-t-il une influence sur le choix de la longueur des messages ?

Exercice 5

Une entreprise dispose d'un réseau Ethernet. Un nouvel employé dans l'entreprise est doté d'un ordinateur ayant une carte Ethernet d'adresse universelle 3E 98 4A 51 49 76 (en hexadécimal). A quel niveau cette adresse est-elle gérée ? Est-il nécessaire de vérifier qu'aucun autre ordinateur ne dispose de la même adresse dans le réseau local ?

Exercice 6

Déterminer le débit utile maximal sur un réseau Ethernet. On rappelle que le débit nominal est de 10 Mbit/s et que les trames contiennent un préambule de 8 octets, deux champs d'adresse de 6 octets chacun, un champ longueur de 2 octets, des données dont la longueur est obligatoirement comprise entre 46 et 1500 octets et un bloc de contrôle d'erreur de 4 octets. Par ailleurs, un intervalle de silence entre trames est obligatoire : sa durée est de 9,6 ms. Que pensez-vous du résultat obtenu ? Pourquoi ne peut-on pas l'atteindre ?
Quel est le degré du polynôme générateur utilisé pour le contrôle d'erreur ?

Exercice 7

Soit un anneau à jeton constitué de 4 stations A, B, C et D. A un instant donné, A émet une trame MAC avec la priorité 3. C veut émettre une trame avec la priorité 4 et D veut émettre avec la priorité 5. Sachant que chaque station s'occupe de retirer de l'anneau la trame qu'elle a émise et qu'elle doit remplacer celle-ci par une trame comportant un jeton libre, indiquez comment vont opérer les stations pour répondre aux besoins du trafic (la fin de l'opération demandée correspond à la circulation d'une trame avec un jeton libre à la priorité initialement utilisée par A).

Exercice 8

Un réseau local en bus de type 802.3 a un débit de 10 Mbit/s et mesure 800 mètres. La vitesse de propagation des signaux est de 200 m/µs. Les trames MAC contiennent 256 bits en tout et l'intervalle de temps qui suit immédiatement une transmission de données est réservé à l'émission de l'accusé de réception de 32 bits.
a) Quel est le nombre de bits en transit sur le bus à un instant déterminé ?
b) Quel est le débit efficace du réseau, en supposant qu'il y a 48 bits de service (champs MAC et LLC) dans chaque trame ?

Exercice 9

Un réseau local en anneau comprend 10 stations uniformément réparties. La vitesse de propagation des signaux est de 200 m/µs. Les trames MAC ont une longueur totale de 256 bits. Calculez le nombre de bits en transit sur l'anneau pour les configurations suivantes :
a) Pour une longueur de 10 km et un débit binaire de 5 Mbit/s ?
b) Pour une longueur de 1 km et un débit binaire de 500 Mbit/s ?
c) Comparez les deux anneaux du point de vue du nombre de trames en transit et du débit utile, si la station émettrice attend le retour de sa propre trame pour réinjecter le jeton sur l'anneau.

Exercice 10

Quels sont les objets comparés en haut des deux colonnes ? Justifiez votre réponse.

Eléments de comparaison	?	?
Simplicité d'installation et de configuration	Oui	Non
Filtrage	Sur les adresses physiques	Sur les adresses IP
Trafic de service	Non sauf « Spanning Tree Algorithm »	Important « Routing Information Protocol »
Protocoles traités	Indépendant des protocoles	Une version de logiciel par protocole traité
Filtrage du trafic de diffusion	Non	Oui
Gestion de la sécurité du réseau	Non	Oui

Quelques corrigés

Exercice 1

La trame Ethernet 802.3 ne contient pas de fanion de fin car elle est suivie d'un signal obligatoire (intervalle inter-trames) et que sa longueur est codée dans le champ longueur.
[Dans le cas où le champ longueur est remplacé par un champ « type », il faut extraire la longueur du contenu lui-même].
Dans Ethernet n'importe quelle station peut à un moment donné prétendre prendre la parole. Pour une station qui reçoit, l'émetteur est inconnu et se situe à une distance quelconque, il est variable d'une transmission à la suivante : il est nécessaire de se re-synchroniser sur à chaque réception de trame.
Dans Token Ring, une station reçoit toujours de la part de son prédécesseur sur l'anneau (point à point), la synchronisation est beaucoup plus simple à acquérir.

Exercice 3

Aucune transmission n'est possible. Le bouchon a un rôle électrique, il doit avoir une impédance bien adaptée de telle sorte que les signaux ne soient pas réfléchis en arrivant aux extrémités du câble. La réflexion est source de bruit et perturbe toutes les transmissions.

Exercice 4

Si le débit est de 5 Mbit/s, un bit occupe $1/5.10^6 = 0{,}2$ µs soit avec la vitesse de propagation de 250 m/µs, une longueur équivalente à 50 m de câble. Dans un réseau local dont la longueur est en général inférieure au kilomètre, cela suppose qu'il y a, à un instant donné, 1000/50 = 20 bits. Cette longueur est donc très petite : le message est à la fois en cours de transmission et en cours de réception, il est inutile de prévoir des protocoles complexes avec anticipation.

Exercice 5

L'adresse MAC est l'adresse physique de la carte Ethernet. C'est le numéro de série de cette carte, il est défini par le constructeur de la carte. [Les constructeurs ont des préfixes uniques au monde (3 octets) et numérotent ensuite leurs cartes sur les 3 octets suivants : deux cartes ne peuvent jamais avoir le même numéro de série.] Il est donc inutile de vérifier qu'aucun autre ordinateur ne possède la même adresse (MAC) dans le réseau local.

Exercice 6

Le débit utile maximal est obtenu de manière théorique si une station unique émet en permanence (en respectant l'espace inter-trames) des trames de longueur maximale. On obtient alors
Longueur totale équivalente d'une trame en octets
= 8 (préambule) + 6 (adresse dest) +6 (adresse émet) +2 (lg ou type) + 1500 (contenu utile) + 4 (BCE) + 12 (inter-trames) = 1528 octets
Débit utile = 10 * (1500 / 1528) = 9,82 Mbit/s
Soit un rendement de 98,2%.
Ceci est bien évidemment un calcul théorique : il est impossible d'attendre un tel rendement dans la pratique, dès lors qu'il y a plusieurs stations qui tentent d'émettre. Il y aura des silences et des collisions lesquelles entraîneront d'éventuels silences et/ou collisions supplémentaires. En pratique, on considère qu'un rendement de 50 à 60 % est une valeur limite. Si le trafic devait être plus important, les performances s'effondrent. De l'intérêt des commutateurs dans les réseaux locaux.

Introduction à Internet

Internet est un réseau international constitué de l'interconnexion de multiples réseaux permettant la mise en relation de plusieurs centaines de millions d'ordinateurs. Initialement destiné à la recherche, il s'est considérablement développé. Conçu aux Etats-Unis, il repose sur des solutions pragmatiques : service réseau sans connexion non fiable (principe du datagramme) et fiabilisation du dialogue par les extrémités.
Une application conviviale permettant la consultation à distance de pages d'informations contenant du texte, des images et du son a été développée sur Internet. Il s'agit du WWW pour *World Wide Web* couramment appelé *Web*. La grande force du *Web* est de permettre à partir d'une page de consulter d'autres pages stockées sur des ordinateurs éventuellement très éloignés. La convivialité et l'esthétique soignée du *Web* ont contribué à sa popularité et par là même à la diffusion d'Internet dans le grand public.

Historique

En 1969, fut créé aux États-Unis le réseau Arpanet sous l'impulsion du DARPA (*Defense Advanced Research Projects Agency*). Ce réseau avait un double objectif : permettre aux universités, aux militaires et à certains centres de recherche d'échanger des informations et d'expérimenter les techniques de commutation par paquets. Il permettait notamment d'étudier comment des communications pouvaient être maintenues en cas d'attaque nucléaire. Largement subventionnés, le réseau et la recherche sur les protocoles se sont considérablement développés.
Devant le déploiement parallèle d'autres réseaux et des réseaux locaux d'entreprise, il apparut intéressant de pouvoir les relier entre eux, indépendamment de leurs technologies respectives pour offrir un service de réseau global. Deux protocoles furent alors développés et prirent leur forme définitive dans les années 77-79 : TCP, *Transport Control Protocol*, et IP, *Internet Protocol* . Ces protocoles furent implantés sur le réseau Arpanet qui devint la base du réseau Internet au début des années 80. La DARPA sépara d'Arpanet le réseau militaire qui prit le nom de Milnet.
Pour favoriser l'adoption des nouveaux protocoles, la DARPA créa une société chargée de les développer et subventionna l'université de Berkeley pour qu'elle les intègre à son système d'exploitation Unix, lui-même distribué à bas prix aux universités. TCP, IP et l'ensemble des protocoles et applications développés autour d'eux touchèrent ainsi rapidement 90% des universités américaines, ce qui créa un effet d'entraînement sur l'ensemble de la communauté scientifique. Cet ensemble de protocoles est souvent baptisé *architecture TCP/IP* ou modèle TCP/IP.

Objectifs et hypothèses de bases d'Internet

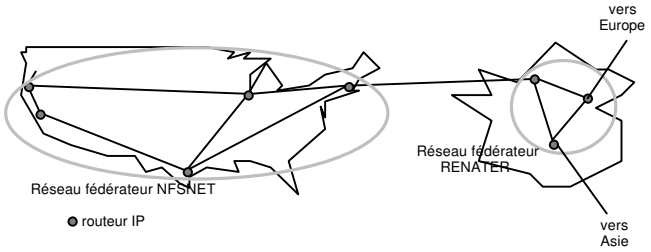
Internet ne constitue pas un nouveau type de réseau physique. Il offre, par l'interconnexion de multiples réseaux, un service de réseau virtuel mondial basé sur les protocoles TCP et IP. Ce réseau virtuel repose sur un adressage global se plaçant au-dessus des différents réseaux utilisés. Les divers réseaux sont interconnectés par des routeurs.
Lorsque des données empruntent plusieurs réseaux, la qualité de l'échange est globalement donnée par le réseau le plus faible : il suffit qu'un seul des réseaux empruntés perde des paquets pour que l'échange ne soit pas fiable. Internet offre donc un *service non fiable* de remise de paquets en mode *sans connexion*. Soulignons que la commutation par paquets permet une utilisation efficace des lignes de transmission au sein du réseau grâce à l'aspect " multiplexage statistique " comme il a été expliqué au chapitre IV. Le service sans connexion fait qu'il est possible à tout moment d'échanger des informations avec n'importe quel ordinateur du réseau : les dialogues sont donc beaucoup plus souples et faciles que sur les réseaux téléphoniques ou Transpac. La fiabilisation des dialogues, lorsqu'elle est nécessaire, est réalisée aux niveaux des extrémités par TCP qui est un protocole de transport fiable. D'autres applications qui n'ont pas besoin de cette fiabilité peuvent utiliser un autre protocole de transport : UDP, *User Datagram Protocol.*
La grande force d'Internet est d'offrir un service de communication universel entre ordinateurs. L'adoption généralisée des protocoles TCP/IP offre un service indépendant des constructeurs, de l'architecture matérielle et des systèmes d'exploitation des ordinateurs. Par ailleurs, le choix d'une architecture de protocoles en couches permet une indépendance vis-à-vis des technologies des réseaux qu'Internet utilise.

Internet s'est développé comme un réseau coopératif. Si une société est reliée à Internet par deux liaisons différentes grâce à des routeurs, elle accepte qu'une partie du trafic Internet transite par son propre réseau et ses routeurs. Internet s'est développé de façon très rapide et non contrôlée.

Architecture matérielle

Internet est un réseau international réalisant l'interconnexion de multiples réseaux. Certains de ces réseaux sont des réseaux locaux, d'autres des réseaux fédérateurs (appelés aussi épines dorsales ou *backbone* d'autres encore de simples liaisons spécialisées. En connectant un réseau local à Internet, une entreprise y connecte *de facto* l'ensemble des ordinateurs du réseau pourvu qu'ils soient munis des logiciels adéquats. On conçoit donc que la croissance du nombre d'ordinateurs connectés à Internet soit très forte.

Les réseaux fédérateurs sont déployés sur de grandes distances pour permettre les communications au sein d'un pays. Aux États-Unis, la NSF, *National Science Foundation*, a installé le réseau NSFNET composé de 13 nœuds de commutation reliés par des liaisons à 45 Mbit/s. En France, le réseau RENATER (REseau NAtional pour la Technologie, l'Enseignement et la Recherche) peut être utilisé comme réseau fédérateur. Les différents réseaux sont connectés entre eux par des routeurs.



Exemple de réseaux fédérateurs Internet

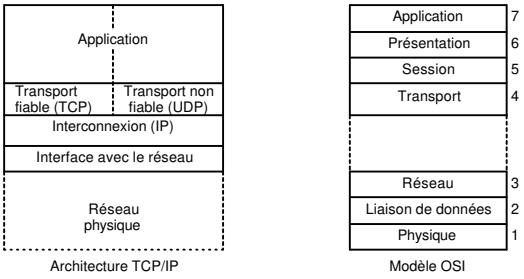
Différents acteurs

Initialement développé par des centres de recherches, Internet se développe maintenant sous l'impulsion d'opérateurs privés. Les opérateurs déploient des réseaux dorsaux mondiaux constitués de routeurs IP interconnectés par des liaisons numériques. Ces liaisons ne sont pas nécessairement installées par l'opérateur Internet mais peuvent être louées à des opérateurs de télécommunications.
Les réseaux des différents opérateurs sont reliés entre eux en de multiples points. Afin de minimiser les échanges de trafic, les opérateurs signent entre eux des accords de *peering* qui consiste à ne laisser passer à travers les réseaux que le trafic propre à chacun d'eux de la façon la plus efficace. Considérons deux réseaux, A et B, proches l'un de l'autre et reliés entre eux. Plutôt que de laisser le trafic échangé entre A et B passer par de multiples routeurs et des réseaux tiers, A et B installent un routeur appelé routeur croisé : tous les datagrammes IP émis par A et destinés à B sont routés vers le réseau B et réciproquement. Si A et B sont deux opérateurs Internet français, cela permet d'éviter par exemple que les datagrammes émis par une machine IP française de A à destination de B ne transitent par les Etats-Unis. La qualité de service du réseau s'en trouve améliorée.
Les grandes entreprises sont généralement reliées directement au réseau Internet. Par exemple, un routeur IP situé dans l'entreprise sur son résau local est relié à un routeur IP d'un opérateur Internet généralement par une liaison spécialisée permanente numérique. Suivant la quantité d'information à écouler, le débit de cette liaison peut être plus ou moins élevé.
Le coût de location d'une telle liaison est prohibitif pour les particuliers ou les petites entreprises. Ils se connectent généralement à Internet par l'intermédiaire du réseau téléphonique. Un certain nombre d'organismes, appelés *fournisseurs d'accès Internet* ou IAP (*Internet Access Provider*), disposent d'ordinateurs reliés d'une part à Internet et d'autre part au réseau téléphonique grâce à des modems ou une liaison ADSL. Il suffit de disposer d'un micro-ordinateur, d'un modem et de souscrire un abonnement auprès de ces prestataires pour avoir un accès à Internet. Notons que le fournisseur d'accès

peut être un câblo-opérateur (ou un partenaire d'un câblo-opérateur) ; il utilise alors le réseau câblé de distribution de télévision pour la transmission entre ses routeurs et l'équipement du particulier.
Lorsque le fournisseur d'accès proposent à ses abonnés des services additionnels comme par exemple un annuaire, le développement de pages Web, on parle de *fournisseur de services Internet* ou ISP (*Internet Service Provider*). Un opérateur Internet peut, bien évidemment, être aussi IAP et ISP.

Architecture en couches

L'architecture globale d'Internet comporte quatre couches. Celle-ci est différente de la normalisation mais se base sur la même philosophie globale :
– découpage en différents niveaux de détail, chacun assurant un service spécifique indépendamment des autres,
– principe d'encapsulation.
Le niveau le plus haut comprend les applications. Il correspond globalement à l'ensemble des couches hautes du modèle OSI. Le niveau le plus bas comprend les opérations à effectuer pour s'adapter aux réseaux physiques utilisés. Il correspond donc aux protocoles des couches basses : 1 et 2 pour un réseau local ou une liaison spécialisée, 1, 2 et 3 pour un réseau grande distance. L'ensemble des opérations effectuées par les réseaux traversés n'est pas pris en compte dans le modèle. Le protocole IP a pour rôle principal le routage ou l'acheminement des données à travers l'interconnexion. TCP et UDP sont des protocoles de transport, ils se situent au niveau intermédiaire entre IP et les applications. Ils ont pour objectif d'offrir aux applications la qualité de service dont elles ont besoin.



Architectures en couches TCP/IP et OSI

Adresse IP

Chaque équipement sur le réseau est repéré par une adresse, appelée adresse IP, codée sur 32 bits avec deux champs principaux précisant une identité de réseau et une identité de machine. Plusieurs classes d'adresses sont définies suivant la longueur des champs d'identité. Un réseau comportant beaucoup de machines dispose d'une adresse avec un court champ d'identité de réseau mais un long champ d'identité de machines. En revanche, dans un petit réseau local, l'identité de machine sera codée sur peu d'éléments binaires. La classe d'adresse et l'identifiant de réseau sont attribués par l'I.C.A.N.N., qui gère le plan d'adressage Internet et garantit l'unicité des identifiants de réseau au niveau international. L'identifiant de machine dans le réseau est déterminé de façon autonome par l'administrateur responsable de ce réseau.
L'identité de machine dans le réseau est déterminée de façon autonome par l'administrateur du réseau. Cette séparation en deux identités permet de réduire la taille des tables de routage car un datagramme est d'abord aiguillé vers le réseau destinataire, puis vers l'ordinateur concerné.
Il est possible de diffuser des messages au sein d'un réseau en positionnant à 1 les bits du champ de numéro de machine. De plus, un format spécifique permet de définir des adresses de diffusion de groupe (*multicast*).

Protocole IP

Le protocole IP assure un service non fiable sans connexion de remise des données. Il comprend la définition du plan d'adressage, la structure des informations transférées (le *datagramme IP)* et les règles

de routage. L'envoi de messages d'erreur est prévu en cas de destruction de datagrammes, de problèmes d'acheminement ou de remise.
Les datagrammes sont constitués d'un en-tête et d'un champ de données ; ils sont indépendants les uns des autres et sont acheminés à travers l'Internet, en fonction des adresses IP publiques (origine et destination) que contient l'en-tête. Les différents routeurs assurent le choix d'un chemin à travers les réseaux ; ils fragmentent, si nécessaire, les datagrammes lorsqu'un réseau traversé n'accepte que des messages de plus petite taille. Une fois le datagramme morcelé, les fragments sont acheminés comme autant de datagrammes indépendants jusqu'à leur destination finale où ils doivent être réassemblés. L'en-tête de ces différents fragments contient alors les indications nécessaires pour reconstituer le datagramme initial.
Pour trouver un chemin jusqu'au destinataire, les routeurs s'échangent, dans des messages spéciaux, des informations de routage concernant l'état des différents réseaux. Ces informations sont véhiculées par IP dans le champ de données d'un datagramme. Elles sont régulièrement mises à jour dans les tables de routage et indiquent, pour chaque identifiant de réseau, si les machines situées dans le réseau sont accessibles directement ou non. Le routage est *direct* si les machines appartiennent au même réseau, sinon il est *indirect*. Lorsque le routage est indirect, le routeur émetteur envoie le datagramme au routeur le plus proche ; la coopération des deux routeurs permet de bien acheminer le datagramme. Des protocoles comme GGP (Gateway to Gateway Protocol), EGP (Exterior Gateway Protocol), RIP (Routing Information Protocol), OSPF (Open Shortest Path Protocol) sont utilisés entre les différents types de routeurs pour échanger et effectuer la mise à jour des informations de routage.

Protocoles de transport

Les protocoles de transport TCP et UDP sont implantés exclusivement dans les ordinateurs connectés (ils ne sont pas installés dans les équipements intermédiaires des réseaux). Ils contrôlent l'acheminement des données de bout en bout, c'est-à-dire depuis la station d'origine jusqu'à la station de destination. Ils offrent également leurs services à de nombreuses applications. Pour distinguer ces dernières, les protocoles de transport utilisent la notion de *port* et de *socket*.
Toute machine est identifiée par son adresse IP et chaque application est reconnue par un numéro de port unique. Le numéro de port est un identifiant attribué par le système d'exploitation de la machine au moment du lancement de l'application. Le couple « adresse IP, numéro de port » sur la machine considérée s'appelle le *socket*. La communication entre deux applications exécutées sur des machines distantes est identifiée de manière unique par les deux sockets « adresse IP source, numéro de port source, adresse IP destination, numéro de port destination ». Les applications les plus courantes utilisent un numéro de port connu de toutes les machines. Par exemple, un serveur web utilise le port 80, un serveur FTP (File Transfer Protocol) les ports 21 et 22.
Le protocole TCP fonctionne en mode connecté ; il est utilisé pour les échanges de données qui nécessitent une grande fiabilité. Pour les autres échanges, le protocole UDP, fonctionnant sans connexion, suffit. UDP assure un échange de données entre les processus communicants, sans contrôle supplémentaire par rapport à IP ; il ne fait que gérer localement les sockets. Le protocole TCP offre de nombreux services supplémentaires : il détecte les datagrammes dupliqués et les détruit ; il récupère les datagrammes perdus et les remet dans l'ordre d'émission, grâce aux acquittements fournis par le récepteur. TCP possède en outre des fonctions de contrôle de flux pour réguler l'échange des données entre les ordinateurs qui dialoguent. Les délais d'attente d'acquittement de bout en bout sont calculés de manière dynamique, en fonction des statistiques de charge du réseau acquises par les machines. Par ailleurs, TCP gère un flot de données urgentes, non soumis au contrôle de flux.

Applications

Dans l'architecture TCP/IP, un grand nombre d'applications simples ont été initialement développées sous le système d'exploitation Unix. Elles permettaient de gérer des ressources distantes (imprimantes, disques durs etc.), comme si elles étaient situées dans la machine de l'utilisateur. De nos jours, tous les systèmes d'ordinateurs font de même. L'application la plus populaire est le web. Son fonctionnement sera traité plus loin. Quelle que soit l'application utilisée, la *netiquette* définit un ensemble de règles de bonne conduite des utilisateurs du réseau Internet.

Dans toutes les applications, les machines sont connues le plus souvent par leur nom symbolique, qui se réfère à l'organisation que l'on cherche à contacter. La connaissance du nom symbolique est suffisante pour permettre la communication avec la machine souhaitée. Le nom symbolique désigne une machine sous la forme d'une chaîne de caractères alphanumériques, dont la structure hiérarchisée reflète l'espace d'adressage. Celui-ci est divisé en domaines, eux-mêmes subdivisés en sous-domaines, selon une structure arborescente dans laquelle le nom le plus à droite désigne le domaine le plus vaste. Par exemple, le nom symbolique *www.linux.org* signifie que la machine à atteindre est un serveur web qui se trouve dans le sous-domaine *linux* du domaine *org*, lequel regroupe des organisations non commerciales. Pour assurer la correspondance entre le nom symbolique et l'adresse IP de la machine, on fait appel à un ou plusieurs *serveurs de noms* (les DNS, Domain Name Servers) qui font office d'annuaires.
Utilisé d'abord dans les entreprises, puis chez les particuliers, *la messagerie électronique* (encore appelée *e-mail -pour electronic mail-, mail, courriel*,…) joue un rôle essentiel dans les demandes de raccordement à Internet. C'est une application qui fonctionne en mode non connecté : le courrier est déposé et stocké dans une « boîte aux lettres » que le destinataire viendra consulter à loisir depuis n'importe quelle machine. Ce service est fourni par SMTP (Simple Mail Transfer Protocol) et utilise les services de TCP. Un message électronique possède un en-tête -contenant l'adresse d'un ou plusieurs destinataires, des destinataires de copies et un sujet de message- et un corps de message. Il est possible d'annexer des documents (les documents attachés), transmis au destinataire en même temps que le message, mais en dehors du corps de celui-ci.
Une *messagerie instantanée* (*chat*) permet à des individus connectés au réseau de discuter directement par des échanges de textes très courts, écrits dans un jargon à base d'abréviations et de symboles graphiques.
Les *news* sont des forums de discussion ayant une durée de vie déterminée, portant sur des sujets précis. Chaque utilisateur s'inscrit aux forums qui l'intéressent pour participer aux discussions. Les questions posées sont placées dans une boîte aux lettres consultable par tous les participants et chacun peut y répondre. Un forum constitue souvent une mine d'informations pratiques et pertinentes. Les questions les plus fréquemment posées sont regroupées sous la rubrique F.A.Q. (Frequently Asked Questions, ou foire aux questions). Elles sont associées à leurs réponses pour que l'on puisse retrouver rapidement les informations cherchées. Dans certains forums, un modérateur valide les informations avant de les publier.
Le *transfert de fichiers* est assuré très souvent par FTP et utilise les services de TCP. L'utilisateur est alors un « client » s'adressant à un « serveur » de fichiers. Des milliers de serveurs sont connectés sur Internet et proposent toutes sortes de logiciels au public ; les logiciels à prix modiques sont appelés des *shareware*, les logiciels gratuits sont des *freeware*. FTP nécessite une connexion avec identification et authentification de l'utilisateur par *login* et mot de passe. Un compte personnel sur un serveur permet d'y déposer des fichiers (des pages web, par exemple). En pratique, tous les serveurs offrent un accès dit *anonyme*. Dans ce cas, le *login* de l'utilisateur est *anonymous.* La netiquette recommande que l'on mette son adresse électronique comme mot de passe. Les fichiers téléchargés depuis un serveur sont très souvent compressés, pour limiter l'espace de stockage nécessaire sur le serveur et les temps de transfert vers l'utilisateur. Ce dernier doit donc disposer des utilitaires adaptés pour effectuer la décompression des fichiers importés sur sa machine.
Parmi *les services de connexion à distance*, Telnet permet à tout ordinateur de se comporter, sur n'importe quel ordinateur du réseau doté de cette application, comme une simple unité clavier-écran. L'utilisateur se connecte alors par TCP. Telnet est un protocole général qui définit un terminal virtuel, indépendant du type de machine et de son système d'exploitation. Actuellement SSH (Secure SHell), une version sécurisée de cette application, lui est souvent préférée car elle vérifie l'identité des correspondants et crypte les données transmises sur le réseau.

Les *logiciels d'échanges Peer-to-Peer* (ou P2P), popularisés durant les années 1990, proposent une alternative au modèle client/serveur. Les données échangées sont réparties dans les machines de tous les participants. Chacun peut télécharger des fichiers à partir de n'importe quelle machine connectée au réseau et proposer ses propres fichiers aux autres. Ce mode de communication est l'un des modes de diffusion les plus rapides : il peut ainsi propager les nouveaux virus à un très grand nombre de machines en un très court laps de temps ! Les échanges de ce type sont associés dans l'esprit du public au piratage de logiciels, de fichiers musicaux ou de films.

Présentation du web

Le web s'appuie sur un langage de description, le html (HyperText Markup Language), qui permet d'afficher sur l'écran de l'utilisateur des documents mis en forme à partir de commandes simples. Html utilise la notion d'hypertexte, c'est-à-dire que les documents sont parcourus dans l'ordre choisi par l'utilisateur à l'aide de sa souris. Dans un hypertexte, chaque document appelé page web ou encore page html est un fichier repéré par son URL (Uniform Resource Locator), un lien spécifique improprement dénommé adresse http (HyperText Transfer Protocol).
À l'intérieur d'un document, des objets particuliers contiennent des *liens* vers d'autres documents que l'utilisateur peut activer comme il le souhaite. Le clic sur un lien provoque le chargement du document associé dans la machine de l'utilisateur. Les liens sont affichés de façon spéciale : par exemple, si l'objet est un texte, les mots sont souvent soulignés et de couleur bleue. Aux abords de la zone où se situe le lien, l'utilisateur constate un changement de forme du curseur de sa souris, attirant ainsi son attention.

Considérons l'URL http://www.linux.org/news/2005/index.htm qui représente le lien vers un fichier de la machine linux vue plus haut. http désigne le nom du protocole de transfert des données ; www.linux.org est le nom symbolique de la machine contactée, news est un répertoire de ce site, 2005 un sous-répertoire du répertoire news. Enfin, index.htm est le nom du fichier écrit en langage html. Autrement dit, le fichier recherché est situé dans le sous-répertoire 2005 du répertoire news de la machine www.linux.org. Une URL peut contenir des informations complémentaires comme des mots de passe ou des numéros de port, lorsque les serveurs utilisent des techniques d'identification des clients ou des numéros de ports particuliers.
Les pages web contiennent aussi bien du texte que des images, des sons ou des fichiers vidéo ; le web est donc un outil multimédia. Un lien peut pointer vers des pages stockées sur d'autres ordinateurs. Le passage d'une page stockée sur un ordinateur aux États-Unis à une autre située en Australie peut se faire rapidement. L'utilisateur « surfe » sur le réseau et voyage virtuellement à travers le monde. Les logiciels d'accès au web, baptisés *navigateurs* (Netscape, Internet Explorer, Mozilla,…), intègrent aujourd'hui d'autres applications comme la messagerie électronique ou le transfert de fichiers.

Un serveur web (on parle également de site web) est une machine capable d'envoyer simultanément plusieurs pages html aux utilisateurs connectés. Certaines pages web sont créées spécialement en réponse à la requête d'un utilisateur (ou d'un client) ; elles possèdent alors une forme et un contenu variables, adaptés à ses besoins. Le serveur filtre les utilisateurs qui se connectent et conserve une trace de toutes les connexions. Les *cookies* sont des informations engendrées par le serveur dès qu'un client visite le site. Ils sont stockés sur les machines des utilisateurs, à leur insu, et sont exploités par le serveur lors des connexions suivantes des clients. Certains sites marchands vont jusqu'à conserver un profil de chaque client en repérant ses habitudes de navigation et d'achats.
Les *moteurs de recherches* (Google, Yahoo!, Voila, AltaVista,…) sont des serveurs spécialisés dans la recherche d'informations à partir de mots-clés. Des banques de données textuelles sont alimentées en permanence par des programmes automatiques d'indexation qui regroupent par thèmes les informations recueillies.
Un *blogue* (en anglais *blog,* contraction de *weblog*), est un site web personnel, évolutif et non conformiste, présentant des réflexions de toutes sortes, généralement sous forme de courts messages. Le blogue est mis à jour par son auteur, qui tient compte des commentaires de ses lecteurs. À la différence d'un blogue, qui exprime la pensée d'un individu, le w*iki* est un site web collaboratif matérialisant les idées d'un groupe qui partage une philosophie ou des intérêts communs.

Standardisation

L'Internet doit aussi son succès aux organisations réactives qui pilotent le développement, l'évolution du réseau, en définissent les axes de développement et réagissent rapidement aux problèmes :
L'Internet Society, créée en 1992, a pour but de développer l'usage de l'Internet dans le monde. Elle ne traite pas des aspects techniques, mais organise des séminaires pour favoriser l'échange d'expérience.
L'IAB (*Internet Activities Board*) est constitué d'un petit groupe d'experts qui conseille techniquement l'Internet Society et qui a réfléchi sur les évolutions à long terme de l'Internet.

L'IESG (*Internet Enginiering Steering Group*) pilote le développement des standards de l'Internet. Il gère les travaux effectués par l'IETF (*Internet Engeniering Task Force* : Force de Travail pour l'Ingénierie de l'Internet) qui publie des documents appelées RFC (*Request For Comments*) définissant les protocoles employés dans l'Internet. Une grande partie des informations relatives à Internet se trouve dans ces RFC, lesquels sont des textes plutôt informels et peu structurés, retraçant les différents débats qui ont permis d'aboutir à tel ou tel choix ou telle ou telle définition. Plus de 2000 documents sont aujourd'hui répertoriés et certains en rendent d'autres obsolètes. L'IAB publie donc régulièrement la liste des RFC à jour : liste officielle des protocoles standardisés par l'IAB. Les protocoles standardisés par l'IAB ont un état qui évolue au cours du temps et définit leurs niveaux d'agrément : expérimental, proposition de standard, projet de standard, et enfin standard.

RFC 768 UDP	RFC 791 IP	RFC 792 ICMP	RFC 793 TCP	RFC 821 SMTP	RFC 854 TELNET	RFC 959 FTP	RFC 1034/35 DNS

RFC 783 TFTP	RFC 1058 RIP	RFC 1171 PPP

Principaux documents RFC

Les principaux standards officiels ou propositions sont indiqués dans le tableau. Les RFC sont disponibles sous forme électronique sur de nombreux sites.

Synthèse

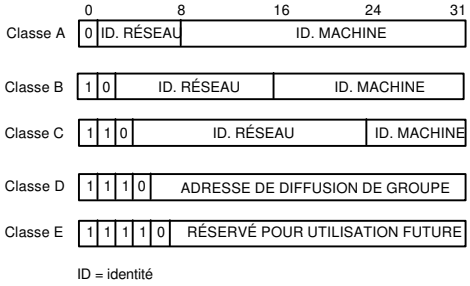
Grâce à Internet, le modèle d'architecture TCP/IP, conçu selon les mêmes principes que l'OSI, s'est répandu et a été adopté dans la plupart des réseaux d'entreprise. Ce modèle permet une interconnexion de réseaux hétérogènes avec un service minimal : le service de remise non fiable de datagramme en mode sans connexion. Ce service est apporté par le protocole IP implanté sur tous les équipements terminaux et dans tous les routeurs de l'interconnexion. TCP est un protocole de transport utilisé pour fiabiliser les échanges chaque fois que cela est nécessaire. De nombreuses applications ont été développées au dessus de TCP et IP. Parmi elles, le courrier électronique et le Web ont provoqué une croissance explosive du nombre de connexions et du trafic sur le réseau Internet.

Le protocole IP

Le protocole IP (*Internet Protocol*) assure un service de remise non fiable sans connexion. Il comprend la définition du plan d'adressage, de la structure de l'unité de données transférée appelé *datagramme IP* et des règles de routage. Enfin, il inclut un protocole ICMP de génération de messages d'erreur en cas de destruction de datagrammes ou de problèmes d'acheminement ou de remise.

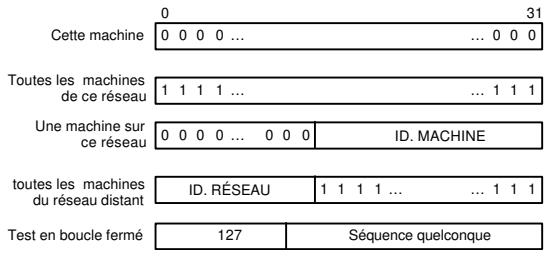
Les classes d'adresse IP

La classe d'une adresse IP peut être déterminée à partir des bits de poids fort. Les adresses de classe A affectent 7 bits à l'identité de réseau et 24 bits à l'identité de machine. Les adresses de classe B affectent 14 bits à l'identité de réseau et 16 bits à l'identité de machine. Enfin, les adresses de classe C allouent 21 bits à l'identité de réseau et 8 bits à l'identité de machine. Les adresses de classe D sont réservées pour mettre en œuvre le mécanisme de diffusion de groupe.



Structure générale d'une adresse IP

Les très grands réseaux ont des adresses de classe A. Une adresse de classe A comporte 8 bits d'identifiant de réseau dont le premier bit est à 0. Les 7 autres bits servent à identifier 126 réseaux différents. Chaque réseau de classe A possède 24 bits d'identifiant de machine, ce qui permet d'adresser $2^{24} - 2$, soit 16 777 214 machines (les deux identifiants 0 et 16 777 215 sont, par convention, réservés à un autre usage)**.** Les réseaux de taille moyenne ont des adresses de classe B, commençant en binaire par 10 et affectant 14 bits à l'identifiant de réseau. Il reste 16 bits pour identifier les machines, soit au maximum 65 534 (pour la même raison que précédemment, les identifiants 0 et 65 535 ne sont pas attribués à une machine). Enfin, pour les petits réseaux, les adresses de classe C commencent en binaire par 110 et allouent 21 bits à l'identifiant de réseau, 8 bits à l'identifiant de machine. On peut ainsi adresser jusqu'à 254 machine (les identifiants 0 et 255 ne sont pas utilisés). Les adresses de classe D, commençant en binaire par 1110, sont réservées à la mise en œuvre d'un mécanisme de diffusion de groupe.
L'adresse IP sur 32 bits peut être vue comme une suite de quatre octets. Elle est écrite pour l'être humain en représentation dite *décimale pointée* : quatre octets écrits en décimal et séparés par un point. Ainsi 10001001 11000010 110000000 00010101 s'écrit 137.194.192.21. Il s'agit en l'occurrence d'une adresse de classe B.



Adresses IP particulières

Pénurie d'adresses

Le formidable succès d'Internet a mené à l'épuisement des adresses de classes A et B et à l'explosion des tables de routage des routeurs situés dans les réseaux de transit. Si beaucoup d'organisations possèdent plus de 254 ordinateurs, peu en possèdent quelques milliers (or une adresse de classe B permet d'identifier jusqu'à 65 534 machines). À cause de la pénurie d'adresses, il est devenu impossible d'attribuer à chaque réseau de plus de 254 machines une adresse de classe B. Désormais l'ICANN attribue plusieurs adresses de classe C contiguës, pour ajuster le nombre d'adresses IP allouées aux besoins du réseau à connecter. Si l'allocation de plusieurs adresses de classe C freine la consommation de l'espace d'adressage disponible, elle augmente d'autant la taille des tables de routage. La mise à jour régulière des tables de routage devient une tâche irréalisable quand celles-ci contiennent des milliers d'entrées mémorisant les routes vers des milliers de réseaux différents. Il faut donc procéder à une allocation intelligente des adresses, afin de les grouper par blocs de numéros, par continents, par régions… Cela aboutit à la notion d'*agrégation de routes.* Les autorités continentales délèguent une partie de leurs plages d'adresses à des autorités de niveau inférieur. Par exemple, l'association RIPE (Réseaux IP européens) confie une partie de son espace d'adressage à des autorités nationales (l'INRIA -Institut national pour la recherche en informatique et en automatique- pour la France). Si le plan de répartition des adresses est bien respecté, tous les réseaux gérés par RIPE sont représentés par une seule entrée dans les tables des autres continents. D'autres solutions sont utilisées pour économiser les adresses IP : l'utilisation d'adresses privées et la distribution dynamique des adresses.

Notion de sous-réseaux et de masque

La hiérarchie à deux niveaux (réseau et machine) de l'adressage IP s'est rapidement révélée insuffisante à cause de la diversité des architectures des réseaux d'organisation connectés. La notion de sous-réseau fut introduite en 1984 et a conservé le format de l'adresse IP sur 32 bits. Dans un réseau subdivisé en plusieurs sous-réseaux, on exploite autrement le champ identifiant de machine de l'adresse IP. Celui-ci se décompose désormais en un identifiant de sous-réseau et un identifiant de machine. Remarquons que ce découpage n'est connu qu'à l'intérieur du réseau lui-même. En d'autres termes, une adresse IP, vue de l'extérieur, reste une adresse sur 32 bits. On ne peut donc pas savoir si le réseau d'organisation est constitué d'un seul réseau ou subdivisé en plusieurs sous-réseaux.
Le masque de sous-réseau (netmask) est alors utilisé pour différencier les bits réservés à l'adressage des sous-réseaux de ceux qui correspondent à la machine. Il contient des 1 sur toute la partie identifiant le réseau et les bits de sous-réseau et des 0 sur la partie réservée au numéro de machine dans le sous-réseau.
Lorsqu'une station d'un (sous-)réseau veut émettre un message à une autre, elle compare sa propre adresse à celle du destinataire, bit à bit en utilisant le masque de sous-réseau. Si sur toute la partie identifiée par les 1 du masque de sous-réseau, il y a égalité, les deux stations se trouvent dans le même (sous-)réseau, le message peut donc être transmis directement, sinon, il est envoyé à la machine qui assure l'acheminement du message vers l'extérieur : le routeur.

Exemple
adresse IP de réseau de classe C 193.27.45.0
masque de sous-réseau 255.255.255.224

soit en binaire 11111111 11111111 11111111 11100000
Dans l'octet réservé au champ identificateur de machine, il y a donc trois bits utilisés pour identifier des sous-réseaux interconnectés par des routeurs.
Sur le sous-réseau 1, l'adresse du sous-réseau est 193.27.45.32, l'adresse 193.27.45.33 peut être celle du routeur, côté sous-réseau 1; l'adresse 193.27.45.63 est l'adresse de diffusion dans le sous-réseau, il reste donc 29 adresses disponibles sur les 32 possibles pour les stations du sous-réseau 1.
De la même façon dans le sous-réseau 2, l'adresse de sous-réseau est 193.27.45.64, l'adresse 193.27.45.65 est celle du routeur B, côté sous-réseau 2; l'adresse 193.27.45.95 est l'adresse de diffusion dans le sous-réseau, il reste de même 29 adresses disponibles sur les 32 possibles pour les stations du sous-réseau 2.
Bilan : sans notion de sous-réseau, on peut mettre 254 stations sur un réseau de classe C, avec 6 sous-réseaux physiques comme dans cet exemple, on ne peut en mettre que 174, mais on dispose d'une identification plus fine et d'une possibilité de diffusion limitée à chaque sous-réseau.
L'administrateur local choisit le nombre de bits à consacrer à l'identifiant de sous-réseau grâce au *masque de sous-réseau*. Celui-ci, également codé sur 32 bits, définit le découpage de l'identifiant machine en deux champs (sous-réseau et machine). Dans un réseau subdivisé, chaque machine connaît son adresse IP et le masque, ce qui lui permet de savoir dans quel sous-réseau elle se trouve. Il suffit de faire l'addition entre l'adresse IP de la machine et le masque :
193.27.45.33 = 11000001 00011011 00101101 00100001
255.255.255.224 = 11111111 11111111 11111111 1110000
addition (ou exclusif)

```
11000001  00011011  00101101  00100001
11111111  11111111  11111111  11100000
--------------------------------------
11000001  00011011  00101101  00100000
```

résultat = 193.27.45.32 l'adresse du sous-réseau auquel appartient la machine 193.27.45.33

Association des adresses Internet et des adresses physiques

Soit deux machines, 1 et 2, reliées dans Internet à un même réseau. Chaque machine a une adresse IP, respectivement IP1 et IP2, et une adresse physique (le terme adresse physique s'applique ici à une adresse MAC (numéro de série de la carte Ethernet, par exemple)), respectivement PH1 et PH2. Le problème, nommé problème de résolution d'adresse (*address resolution problem*), consiste à faire la correspondance entre les adresses IP et les adresses physiques, sachant que les programmes d'application ne manipulent que des adresses IP. Des tables, dans chaque machine, contiennent des paires adresse de haut niveau / adresse physique, mais elles ne peuvent maintenir qu'un petit nombre de paires d'adresses. Un protocole de résolution d'adresses (*ARP: Address Resolution Protocol*) fournit un mécanisme efficace et simple. Il permet à une machine de trouver l'adresse physique d'une machine cible située sur le même réseau physique, à partir de sa seule adresse IP. Lorsqu'une machine 1 veut résoudre l'adresse IP2, elle diffuse (en utilisant l'adresse 11…11 comme identité de machine) un datagramme spécial. Celui-ci demande à la machine d'adresse IP2 de répondre, en indiquant son adresse physique PH2. Toutes les machines, y compris 2, reçoivent ce paquet, mais seule la machine 2 reconnaît son adresse IP. Elle renvoie donc un message contenant son adresse physique PH2. Lorsque 1 reçoit cette réponse, elle peut alors communiquer directement avec 2. Les messages spéciaux que nous venons de voir, ceux du protocole ARP, sont véhiculés dans les données du protocole IP que nous allons voir ci-dessous. Un protocole similaire, baptisé RARP (*Reverse Address Resolution Protocol*), permet, de la même façon, pour une machine sans disque, de connaître son adresse IP auprès d'un serveur d'adresses.

Adresses physiques

les adresses Ethernet s'écrivent sur 6 octets (48 bits) en notation héxadécimale, souvent écrits séparés par le caractère ':' (sous Linux) et '–' sous Windows :
les 3 premiers octets correspondent à un code constructeur (3Com, Sun, ...) ;
les 3 derniers octets sont attribués par le constructeur.

Ainsi, une adresse Ethernet est supposée être unique. Sous Unix, la commande `ifconfig` révèle l'adresse Ethernet associée à une carte :
Sous Linux
/sbin/ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:90:27:6A:58:74
inet addr:192.168.1.3 Bcast:192.168.1.255 Mask:255.255.255.0

Sous Windows
ipconfig /all
    Description . . . . . :
    Adresse physique. . . . . : 52-54-05-FD-DE-E5
Signalons enfin que `FF:FF:FF:FF:FF:FF` correspond à l'*adresse de diffusion* (*broadcast*) qui permet d'envoyer un message à toutes les machines, et que `00:00:00:00:00:00` est réservée.

Le protocole ARP

Le protocole ARP (*Address Resolution Protocol* RFC 826) fournit une correspondance dynamique entre adresses physiques et adresses logiques (adresses respectivement de niveau 2 et 3) : l'émetteur connaît l'adresse logique du destinataire et cherche à obtenir son adresse physique. La requête/réponse ARP contient :
l'*adresse physique de l'émetteur*. Dans le cas d'une réponse ARP, ce champ révèle l'adresse recherchée.
l'*adresse logique de l'émetteur* (l'adresse IP de l'émetteur).
l'*adresse physique du récepteur*. Dans le cas d'une requête ARP, ce champ est vide.
l'*adresse logique du récepteur* (l'adresse IP du récepteu)r.
Le message ARP est transporté dans une trame Ethernet. Lors d'une demande ARP, l'adresse de destination est l'adresse de diffusion `FF:FF:FF:FF:FF:FF` de sorte que tout le réseau local reçoit la demande. En revanche, seul l'équipement possédant l'adresse IP précisée dans la requête répond en fournissant son adresse physique.
Un mécanisme de cache permet de conserver les informations ainsi acquises : chaque système dispose d'une table qui sauvegarde les correspondances (adresse MAC, adresse IP). Ainsi, une requête ARP est émise uniquement si le destinataire n'est pas présent dans la table.
La commande `arp -a` affiche le contenu de la table, aussi bien sous Windows que sous Unix :

```
sous Linux
arp -a
poste1(192.168.1.2) at 02:54:05:F4:DE:E5 [ether] on eth0
poste2(192.168.1.1) at 02:54:05:F4:62:30 [ether] on eth0
```

Adresses IP privées et mécanisme NAT

Plusieurs plages d'adresses IP ont été réservées dans chaque classe d'adresses et sont d'utilisation libre. Elles sont appelées « adresses IP privées » et sont décrites dans la RFC 1918. Ces adresses ne peuvent être attribuées par l'ICANN à une organisation. Ainsi, des réseaux d'organisation différents peuvent utiliser les mêmes adresses IP privées, pourvu qu'ils restent isolés les uns des autres. Pour relier à l'Internet les machines d'un réseau utilisant des adresses privées, on met en place une traduction, gérée par le routeur, entre adresses IP privées (internes au réseau de l'organisation, inaccessibles de l'extérieur) et adresses IP publiques (visibles de l'extérieur, c'est-à-dire accessibles par Internet). Une adresse IP publique est unique ; elle est dite « routable », car elle seule autorise l'accès à Internet. La correspondance entre les deux types d'adresses est assurée par le NAT (Network Address Translation), un mécanisme de conversion d'adresse décrit par la RFC 3022. De plus, les adresses IP privées garantissent une meilleure sécurité d'accès aux réseaux d'organisation, dans la mesure où les adresses réelles utilisées par les machines du réseau ne sont pas connues de l'extérieur. .

classe	Information	Nombre maximum de machines
A	**10.x.y.z**, où 0 <= x <= 255	(256*256*256) - 2 = 16 777 214

	0 <= y <= 255 et 0 <= z <= 255	
B	**172.x.y.z**, où 16 <= x <= 31 0 <= y <= 255 et 0 <= z <= 255	(15*256*256) - 2 = 1 048 574
C	**192.168.x.y**, où 0 <= x <= 255 et 0 <= y <= 255	(256*256) - 2 = 65 534

Le NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur permet donc d'associer à une adresse IP privée (par exemple *192.168.0.1*) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP. Le NAT statique permet ainsi de connecter des machines du réseau interne à internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où *n* adresses IP routables sont nécessaires pour connecter *n* machines du réseau interne

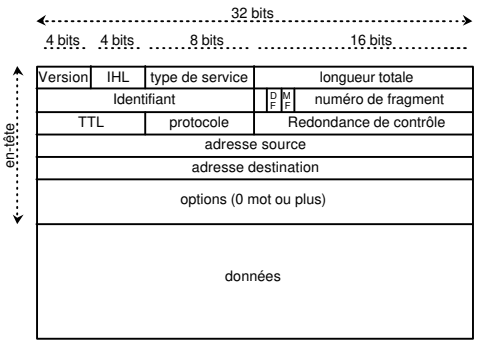
Le NAT dynamique partage une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP

Les avantages des adresses IP privées sont donc la garantie d'une sécurité accrue et la résolution du manque d'adresses IP. Les inconvénients sont le travail supplémentaire lors de la configuration du réseau et la renumérotation à envisager lors de la fusion d'entreprises qui utiliseraient les mêmes adresses IP privées.

Pour assurer la distribution dynamique des adresses, le protocole DHCP (Dynamic Host Configuration Protocol) fournit automatiquement à un ordinateur qui vient d'être installé dans le réseau de l'entreprise ses paramètres de configuration réseau (adresse IP et masque de sous-réseau). Cette technique simplifie la tâche de l'administrateur d'un grand réseau, en évitant par exemple les doublons d'adresses. Un autre avantage de cette solution est que l'entreprise dispose d'une plage d'adresses IP utilisables sur le réseau plus faible que son parc de machines. Les adresses IP utilisables sont alors temporairement affectées aux seules machines connectées à Internet.

Format du datagramme IP

Le format d'un datagramme IP comprend un en-tête et des données. L'en-tête contient principalement les adresses IP de la source et du destinataire, et un champ identifiant la nature des données transportées.



IHL, *Intenet Header Length* indique la longueur de l'en-tête en mots de 32 bits.
La longueur totale est la longueur du datagramme en octets, en-tête compris.
L'identification est un numéro permettant d'identifier de manière unique les fragments d'un même datagramme.
DF, *Don't Fragment*, interdit la fragmentation du datagramme (toute machine doit accepter les fragments de 476 octets ou moins).
MF, *More Fragments*, est mis à 1 pour tous les fragments d'un même datagramme initial sauf pour le dernier fragment.
Le numéro de fragment permet de reconstituer, dans l'ordre, le datagramme initial à partir de l'ensemble des fragments.
TTL, *Time To Live*, indique le nombre de secondes qui restent à vivre au datagramme. Ce champ est modifié par les routeurs IP au cours de la traversée du réseau par le datagramme.
Le champ protocole indique le protocole de la couche supérieur (UDP, TCP,…).
La redondance de contrôle permet de détecter les erreurs éventuels sur l'en-tête.

Format d'un datagramme IP

Les datagrammes sont indépendants les uns des autres, ils sont acheminés à travers l'interconnexion en fonction des adresses IP qu'ils contiennent. Ce sont les différents routeurs qui assurent le choix d'un chemin à travers le réseau et éventuellement fragmentent les datagrammes, lorsqu'un réseau traversé n'accepte que des petites tailles de messages. La MTU (*Maximum Transfer Unit*) d'un réseau Ethernet, par exemple, est de 1500 octets, celle d'un réseau de type X25 peut être de 128 octets. Une fois le datagramme fragmenté, les fragments sont acheminés comme autant de datagrammes indépendants jusqu'à leur destination finale où ils doivent être réassemblés. L'en-tête de ces différents fragments doit contenir l'information nécessaire pour reconstituer correctement le datagramme initial.
L'intérêt des datagrammes IP réside également dans les options qui peuvent être utilisées. Les options de routage et d'horodatage sont particulièrement intéressantes. Elles constituent un bon moyen de surveiller ou de contrôler la traversée des datagrammes dans le réseau. L'*enregistrement de route* est une option qui demande à chaque routeur traversé d'indiquer dans le datagramme lui-même sa propre adresse. Le destinataire reçoit ainsi un datagramme qui contient la liste des adresses des routeurs par lesquels il est passé. Le *routage défini par la source* est une autre option qui permet à l'émetteur de forcer le chemin par lequel doit passer un datagramme. L'*horodatage* est une option qui demande à chaque routeur d'estampiller le datagramme de la date et l'heure à laquelle il a été traité. Ces différentes options sont transportées dans l'entête du datagramme.

Protocole ICMP

Internet est un réseau décentralisé. Il n'y a pas de superviseur global du réseau. Chaque routeur fonctionne de manière autonome. Des anomalies, dues à des pannes d'équipement ou à une surcharge temporaire, peuvent intervenir. Afin de réagir correctement à ces défaillances, le protocole de diagnostic ICMP, *Internet Control Message Protocol*, a été développé. Chaque équipement surveille son environnement et échange des messages de contrôle lorsque c'est nécessaire. Ces messages sont transportés par IP dans la partie données des datagrammes.
Pour contrôler le trafic dans le réseau, un champ, dans l'en-tête du datagramme, indique, en secondes, la *durée maximale de transit* dans l'interconnexion. Chaque routeur qui traite le datagramme décrémente sa

durée de vie. Le datagramme est détruit lorsque sa durée de vie vaut zéro, on envoie alors un message d'erreur à l'émetteur du datagramme. Ce message d'erreur est un exemple typique du protocole ICMP.

Evolution d'Internet : le protocole IPv6

La croissance exponentielle du nombre d'ordinateurs connectés à l'Internet pose de nouveaux problèmes. Le plan d'adressage IP atteint un seuil de saturation, les adresses disponibles commencent à manquer. Une nouvelle version d'IP dite IPv6 (IP version 6) prévoit une champ d'adressage beaucoup plus large pour faire face à cette explosion.

IPv6 prévoit des adresses sur 128 bits, ce qui est gigantesque : chaque habitant de la planète pourrait utiliser autant d'adresses que l'ensemble utilisé aujourd'hui sur Internet ! Cet espace sera surtout utilisé pour améliorer la flexibilité et faciliter la tâche des administrateurs, ainsi que pour assurer la compatibilité avec les systèmes existants.

Les types d'adresses sont globalement conservés, à part la disparition des adresses de diffusion (broadcast) qui sont remplacées par une généralisation du *multicast* (adressage multi-points).

On ne parle plus de classes d'adresses mais il existe de nombreux nouveaux types, déterminés par un préfixe. Le préfixe 0000 0000 binaire sera utilisé pour la compatibilité avec les adresses IP classiques.

L'adressage IPv6 résout non seulement le problème de la saturation des adresses mais offre, en plus, de nouvelles possibilités comme une hiérarchisation à plusieurs niveaux ou l'encapsulation d'adresses déjà existantes qui facilite la résolution des adresses.

IPv6 utilise un format de datagramme incompatible avec IP classique. Il est caractérisé par un en-tête de base de taille fixe et plusieurs en-têtes d'extension optionnels suivis des données. Ce format garantit une souplesse d'utilisation et une simplicité de l'en-tête de base.

Regardons maintenant la structure de l'en-tête IPv6. Il y a 16 niveaux de priorité qui sont respectés par les routeurs. Ceci permet par exemple de traiter différemment les applications interactives et les transferts de fichiers.

Un identificateur de flot permet de relier les datagrammes d'une même connexion applicative afin de leur garantir une même qualité de service.

L'utilisation combinée de la priorité et de l'identificateur de flot permet d'ajuster la qualité de service offerte par le routage aux besoins de l'application. Elle répond donc à la demande des nouvelles applications (temps réel, multimédia...).

Le nombre de routeurs que peut traverser le datagramme avant d'être détruit remplace le champ durée de vie d'IP. Sa gestion est plus simple. La fragmentation est désormais effectuée de bout en bout : un algorithme PMTU (*Path Maximum Transfer Unit*) détermine la taille maximale des datagrammes sur le chemin prévu, les paquets sont ensuite fragmentés par la source et rassemblés par le destinataire.

Grâce à l'utilisation d'en-têtes optionnels, le routeur n'a qu'à extraire l'en-tête de base ainsi que l'en-tête optionnel *hop by hop* (littéralement saut par saut) qui suit l'en-tête de base et qui contient des options devant être traitées aux nœuds intermédiaires.

Il est intéressant, avec le développement des portables, de pouvoir rediriger les messages adressés à la station fixe habituelle vers sa localisation actuelle en cas de déplacement. Ceci va désormais se faire au niveau du protocole IPv6 (et non au niveau de protocoles de couches supérieures comme c'est le cas avec la redirection des courriers électroniques). Un redirecteur placé à l'entrée du réseau connaît l'adresse IPv6 de la personne en déplacement. Il encapsule le datagramme dans un nouveau datagramme IPv6 et l'expédie à la nouvelle adresse. Le destinataire peut ainsi connaître l'identité de l'émetteur.

Les routeurs mettent également en œuvre un mécanisme de réservation de ressources adapté aux exigences stipulées dans les champs priorité et identificateur de flot des datagrammes, dans le cas de contraintes de délai et de débit (temps réel).

IPv6 tente d'apporter des éléments d'authentification et de confidentialité, thèmes qui n'étaient pas abordés dans IP. IPv6 permet d'accompagner le datagramme d'un en-tête d'authentification et de confidentialité.

Synthèse

Exercices

Exercice 1

L'adresse de ma machine est 193.48.200.49. Puis-je en déduire si le réseau est de classe A, B ou C ?

Exercice 2

Considérons deux machines, 1 et 2, reliées à un même réseau local. Chaque machine a une adresse IP, respectivement IP1 et IP2, et une adresse MAC, respectivement PH1 et PH2. Comment la machine 1 désirant envoyer un datagramme vers la machine 2 dont elle ne connaît que l'adresse IP2, peut-elle mettre en correspondance l'adresse IP2 avec l'adresse physique PH2 ? Et si la machine 2 est sur un autre réseau local à distance, comment le datagramme est-il transmis dans le réseau local de la machine 1 : quelles adresses porte la trame qui le transporte, d'où viennent-elles ?

Exercice 3

Soit une entreprise disposant d'un réseau Ethernet relié à Internet. L'entreprise dispose d'une adresse IP de classe B, d'une identité réseau égale à 29 C2 (écrite en hexadécimal). Sur le réseau il y a déjà deux cents ordinateurs dont l'adresse IP a été choisie dans l'ordre croissant en commençant par 1. Vous branchez un nouvel ordinateur disposant d'une carte Ethernet d'adresse universelle 3E 98 4A 51 49 76.
Proposer une adresse IP pour l'ordinateur et l'écrire sous forme décimale hiérarchique.
L'ordinateur est déplacé vers un autre réseau Ethernet de la même entreprise, ce réseau étant également branché sur Internet. Est-il nécessaire de changer l'adresse de la carte Ethernet ? Est-il nécessaire de changer l'adresse IP de l'ordinateur ?

Exercice 4

Etablir un tableau comparatif entre les équipements d'interconnexion (répéteur, pont et routeur) en abordant les aspects suivants : niveau d'interconnexion, filtrage d'adresses, filtrage des collisions, filtrage du trafic de diffusion, génération de trafic de gestion, dépendance vis-à-vis des protocoles de communication, évolutivité, performances, impact sur la sécurité du réseau, reconfiguration, coût, temps de traitement interne, simplicité d'installation et de maintenance...

Exercice 5

Deux entreprises A et B sont équipées l'une d'un réseau local de type Ethernet, l'autre d'un réseau local de type Token Ring.
a) Proposer des solutions d'interconnexion pour que chaque station de l'entreprise A puisse dialoguer avec toutes les stations de l'entreprise B.
b) A quoi pourraient être dus le goulet d'étranglement et la dégradation éventuelle des débits utiles au niveau de chaque station du réseau A ?

Exercice 6

Un site local est composé de deux sous-réseaux physiques, reliés par l'intermédiaire d'une même passerelle au reste du monde. Ce site possède une adresse IP de classe B. Proposez un mode d'adressage des différentes stations sur le site pour que la passerelle n'ait pas à diffuser systématiquement tous les messages reçus du reste du monde sur chacun des deux sous-réseaux.

Exercice 7

Un datagramme IP peut être segmenté en plusieurs fragments.
a) De quelles informations dispose-t-on pour savoir qu'un datagramme contient un fragment ?
b) Comment reconstitue-t-on un datagramme à l'arrivée ?

c) Une passerelle peut-elle confondre deux fragments qui ont les mêmes éléments suivants : source, destination et numéro de fragment ?

Exercice 8

Deux sociétés S1 et S2 situées à 100 km l'une de l'autre fusionnent et désirent mettre en commun leurs moyens informatiques. La société S1 possède un réseau Ethernet E1 et les transferts de données utilisent TCP/IP, avec une adresse IP de classe C. La société S2 possède un réseau: Ethernet E2 sous TCP/IP, avec une adresse IP de classe B. Que faut-il faire pour que tous les utilisateurs de E1 puissent accéder aux machines du réseau de E2 et vice-versa ? Quelle est la structure de l'équipement d'interconnexion pour passer de E1 à E2 ? Quels sont les problèmes potentiels dus à l'interconnexion ?

Exercice 9

Dans un réseau local Ethernet 100 Mbit/s, on dispose de 50 machines d'utilisateurs réparties en 5 groupes de 10 et de serveurs : un serveur spécifique dans chaque groupe et 2 serveurs communs à l'ensemble des utilisateurs. Dans chacun des 5 groupes, les machines des utilisateurs sont reliées à un concentrateur 12 ports.
L'entreprise possède l'adresse IP 193.22.172.0, peut-on répartir les adresses en faisant apparaître les 5 groupes ? Si oui, comment ? Proposez un plan d'adressage.

Exercice 10

Vous avez lancé une commande traceroute (tracert sous Windows). Cette commande permet de connaître le chemin suivi par un datagramme entre votre machine et une machine destination quelconque. Vous avez obtenu le résultat suivant :

1	193.51.91.1	1ms	1ms	1ms
2	2.0.0.1	23ms	23ms	23ms
3	11.6.1.1	105ms	35ms	35ms
4	11.6.13.1	37ms	35ms	34ms
5	189.52.80.1	37ms	60ms	36ms
6	193.48.58.41	51ms	39ms	46ms
7	193.48.53.49	39ms	47ms	44ms
8	193.220.180.9	44ms	*	*
9	195.48.58.43	48ms	38ms	44ms
10	195.48.58.50	145ms	170ms	64ms
11	194.206.207.18	61ms	146ms	44ms
12	194.207.206.5	166ms	261ms	189ms

Pourquoi le délai est-il (inférieur à) 1 milliseconde pour la première ligne ? Que peuvent signifier les étoiles ? Comment expliquez-vous que pour la même destination les délais varient ? Combien de réseaux différents ont été traversés ? Peut-on connaître les protocoles utilisés ?

Exercice 11

A et B sont deux utilisateurs de la même entreprise. L'utilisateur A a pour adresse 143.27.100.101 et lit sur sa machine : masque de sous-réseau 255.255.192.0 et adresse passerelle 143.27.105.1.
1) Quelle est l'adresse du sous-réseau auquel appartient A ? Quelle est l'adresse de diffusion sur ce sous-réseau ?
2) L'utilisateur B a pour adresse 143.27.172.101 et lit sur sa machine : masque de sous-réseau 255.255.192.0.
B est-il sur le même réseau que A ? Peut-il utiliser la même adresse de passerelle que A ? S'il ne connaît pas l'adresse à utiliser, que doit-il faire ?

Exercice 12

Soit un routeur d'entreprise qui relie 4 sous-réseaux R1, R2, R3 et R4 et offre l'accès à l'Internet. L'entreprise a un adresse IP de classe C, d'identité réseau égale à 195.52.100. Dans le sous-réseau R1, il y a 15 postes de travail, dans R2 20 postes , R3 25 postes, R4 30 postes.
Peut-on imaginer un plan d'adressage avec quatre sous-réseaux distincts ? Quel sera alors le masque de sous-réseau ?

Exercice 13

1/ Quelles sont les propriétés indispensables des adresses dans un réseau de communication ?
2/ Quel est l'avantage de la séparation de l'adressage en 2 parties dans l'adressage Internet ?
3/ Pourquoi l'adresse IP ne peut pas être affectée à un périphérique réseau par son fabricant ?

Exercice 14

compléter le tableau

adresse IP	124.23.12.71	124.12.23.71	194.12.23.71
masque de sous-réseaux	255.0.0.0	255.255.255.0	255.255.255.240
classe			
Adresse du réseau auquel appartient la machine			
Adresse de diffusion dans le réseau			
adresse du sous-réseau auquel appartient la machine dont l'adresse est donnée sur la première ligne			
adresse de diffusion dans le sous-réseau			

Exercice 15

Décoder le datagramme IPv4 suivant (hexadécimal) et en extraire toutes les informations possibles.

```
45 00 00 50 20 61 00 00 80 01 C5 64 C7 F5 B4 0A C7 F5 B4 09
08 00 00 1C 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10
11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24
25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38
```

Exercice 16

Décoder la trame Ethernet suivante (hexadécimal) et en extraire toutes les informations possibles.

```
AA AA AA AA AA AA AA AB 08 00 02 4B 01 C3 08 00 02 4B 02 D6 08 00
45 00 00 50 20 61 00 00 80 01 C5 64 C7 F5 B4 0A C7 F5 B4 09
08 00 00 1C 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10
11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24
25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38
5F A6 8C 04
```

Quelques corrigés

Exercice 3

L'adresse Ethernet est gérée dans la sous-couche MAC.

Il n'est pas nécessaire de vérifier l'unicité de l'adresse. Celle-ci est garantie par le constructeur. Au niveau international, chaque constructeur a son préfixe et numérote ensuite chacune de ses cartes dans l'absolu.
L'adresse IP est de classe B donc commence par 10. L'identité réseau s'écrit sur 14 bits : 29C2 (hexadécimal) = 10 1001 1100 0010. Donc la partie réseau vaut 1010 1001 1100 0010 soit en décimal 169.194. L'identité de la machine peut être (par exemple) choisie égale à 201 (décimal). L'adresse IP est donc 169.194.0.201.
Par définition de l'adresse Ethernet : la carte a conservé son adresse. Il faut, par contre, lui donner une nouvelle adresse IP avec la nouvelle identité réseau et une nouvelle identité de machine dans ce réseau.

Exercice 6

Adresse de classe B : x .y.0.0 avec x compris entre 128 et 191. En absence d'hypothèse précise sur le nombre de machines dans chacun des réseaux, on considèrera qu'il suffit de créer deux sous-réseaux (ce qui nécessite 4 bits si l'on veut éviter le sous-réseau « plein 0 » et le sous-réseau « plein 1 ») donc un masque 255.255.192.0. Dans les adresses IP des stations, les 16 premiers bits représentent le réseau (x.y), les deux bits suivants le sous-réseau (01 et 10) et les 14 bits restant la machine elle-même.
Sous-réseau 01 a pour adresse de sous-réseau x.y.64.0 ; les adresses des machines vont de x.y.64.1 à x.y.127.254 ; l'adresse de diffusion dans ce sous-réseau est x.y.127.255. Tout message parvenant à la passerelle avec une adresse IP dans l'intervalle ci-dessus est diffusé exclusivement dans ce sous-réseau.
Sous-réseau 10 a pour adresse de sous-réseau x.y.128.0 ; les adresses des machines vont de x.y.128.1 à x.y.191.254; l'adresse de diffusion dans ce sous-réseau est x.y.191.255. . Tout message parvenant à la passerelle avec une adresse IP dans l'intervalle ci-dessus est diffusé exclusivement dans ce sous-réseau.

Exercice 7

Un datagramme IP peut être découpé en plusieurs fragments.
a) le bit M (More fragments) est à 1 dans tous les fragments sauf le dernier et le champ « deplacement offset » n'est pas nul sauf dans le premier fragment. Un datagramme non fragmenté a un bit M à 0 ET un champ deplacement offset à 0.
b) tous les fragments portent le même identificateur (celui du datagramme initial), on utilise alors le champ deplacement offset pour reconstituer le datagramme. Le bit M à 0 indique la fin.
c) Un routeur peut-il confondre deux fragments qui ont les mêmes éléments suivants : source, destination et place de fragment ? non le champ identificateur du datagamme est forcément différent !

Exercice 13

1/ unicité, homogénéité
2/ Le fait de séparer l'adresse en deux parties permet de réduire la taille mémoire des passerelles car elles ne conservent que l'adresse des (sous)réseaux (et celle des stations des (sous)réseaux directement rattachées). En effet, la séparation entre l'adresse du (sous)réseau et celle de la station attachée à ce (sous)réseau permet un routage effectif dans les routeurs uniquement d'après l'adresse du (sous)réseau. L'adresse complète n'est utilisée qu'une fois le paquet arrivé au routeur auquel est connecté le (sous)réseau destinataire.
Il est facile d'envoyer un paquet sur toutes les stations d'un (sous)réseau. Il suffit d'utiliser une adresse de station particulière qui signifie que le paquet doit être diffusé sur tout le (sous)réseau. On peut garder par exemple l'adresse de station avec tous les bits à 1 pour envoyer un paquet à toutes les stations d'un (sous)réseau.
Enfin, cela permet une décentralisation de la gestion des « host id ».
3/ L'adresse IP ne doit pas être seulement unique mais elle doit aussi refléter la structure de l'interconnexion. Elle est constituée par une partie réseau qui dépend donc du réseau auquel est connecté la station. Toutes les machines connectées au réseau physique ont le même préfixe réseau.

Exercice 14

adresse IP	124.23.12.71	124.12.23.71	194.12.23.71

masque de sous-réseaux	255.0.0.0	255.255.255.0	255.255.255.240
classe	A	A	C
Adresse du réseau auquel appartient la machine	124.0.0.0	124.0.0.0	194.12.23.0
Adresse de diffusion dans le réseau	124.255.255.255	124.255.255.255	194.12.23.255
adresse du sous-réseau auquel appartient la machine dont l'adresse est donnée sur la première ligne	pas de sous-réseaux	124.12.23.0	194.12.23.64
adresse de diffusion dans le sous-réseau		124.12.23.255	194.12.23.79

Exercice 15

`45` → 4 = protocole IP version 4; 5 = longueur de l'entête du datagramme = 5 * 4 octets = 20 octets = longueur par défaut d'un entête sans options
`00` → Type Of Service = 0 = pas de service particulier; en fait avec Ipv4 il n'y a pas de service particulier, ce champ est donc toujours nul !!
`00 50` → longueur totale = 0*4096 + 0*256 + 5*16 + 0*1 = 80 octets donc la longueur du contenu est de 80-20 = 60 octets
`20 61` → identificateur du datagramme (ne sera utile que plus tard, au cas où il serait fragmenté)
`00 00` → drapeaux et déplacement tout à zero = datagramme non fragmenté
`80` → durée de vie = 80 = 8*16 +0*1 = 128 routeurs que le datagramme pourrait encore traverser…
`01` → protocole transporté dans le datagramme : 1 = code du protocole ICMP
`C5 64` → Bloc de contrôle d'erreur de l'entête
`C7 F5 B4 0A` → adresse IP émetteur = 199.245.180.10
`C7 F5 B4 09` → adresse IP destinataire =199.245.180.9
Les deux machines sont dans le même réseau de classe C, le réseau 199.245.180.0
-------fin de l'entête IP----------
pour décoder le contenu il faut connaître le format d'un message ICMP
`08` → type : 8
`00` → code : 0
l'ensemble type = 0 et code = 0 signifie demande d'écho (couramment appelée ping)
`00 1C` → bloc de contrôle d'erreur sur l'entête du message ICMP
-----fin de l'entête ICMP----------
contenu quelconque destiné à être renvoyé par le destinataire s'il répond à cette demande décho.

```
01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10
11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20
21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30
31 32 33 34 35 36 37 38
```

longueur du contenu ICMP = 56 octets
------fin du contenu ICMP------
--- fin du contenu IP-------
Conclusion : le datagramme est au format IPv4. Il a été émis par la machine d'adresse IP 199.245.180.10 vers la machine d'adresse IP 199.245.180.9. Ces deux machines sont dans le même réseau de classe C, le réseau 199.245.180.0. La datagramme possède une longueur totale de 60 octets, il transporte une requête ICMP de demande d'echo et dont la longueur du contenu est de 56 octets:L'émetteur envoie un ping au récepteur pour connaître son état.

Exercice 16

---------- début d'une trame Ethernet ----------
AA AA AA AA AA AA AA AB -> Synchronisation
08 00 02 4B 01 C3 -> @mac destinataire (constructeur = 080020)
08 00 02 4B 02 D6 -> @mac émetteur (même constructeur)
08 00 -> Type (ici IP). Si < à 1500 c'est une longueur
[ici 08 00 = 2048, cette valeur ne peut donc pas être la longueur des données de la trame]
---------- 46 <= contenu (ici datagramme IP)<= 1500 ----------
le contenu de cette trame est le « ping » de l'exercice précédent
----------fin du contenu----------
5F A6 8C 04 ➔ bloc de contrôle d'erreur Ethernet

Conclusion. Cette trame Ethernet a été capturée dans le réseau de classe C 199.245.180.0. Deux machines sont concernées par cet échange : la machine X d'adresse MAC 08 00 02 4B 02 D6 et d'adresse IP 199.245.180.10 a envoyé une requête d'écho (ping) à la machine Y d'adresse MAC 08 00 02 4B 01 C3 et d'adresse IP 199.245.180.9, située sur le même réseau local. Les cartes Ethernet sont du même constructeur. Les protocoles utilisés sont IP et ICMP.

Le routage

Le but d'un protocole de routage est très simple : fournir l'information nécessaire pour effectuer un routage, c'est-à-dire la détermination d'un chemin à travers le réseau entre une machine émettrice et une machines réceptrices, toutes deux identifiées par leur adresse. Les protocoles de routages établissent des règles d'échange des messages d'état entre routeurs pour mettre à jours leurs tables selon des critères de coût comme, par exemple, la distance, l'état de la liaison, le débit, et ainsi améliorer l'efficacité du routage.

Le réseau Internet est organisé comme une collection de « systèmes autonomes», chacun d'entre eux étant en général administré par une seule entité. Un système autonome, ou SA , est constitué d'un ensemble de réseaux interconnectés partageant la même stratégie de routage , plus précisément tous routeurs internes à ce système obéissent à un même protocole de routage , régi par une autorité administrative (un département responsable spécifique comme un fournisseur d'accès ou toute autre organisation).

Le protocole de routage utilisé à l'intérieur d'un système autonome est référencé en tant que protocole interne à des passerelles, ou IGP. Un protocole séparé, appelé EGP (protocole externe à des passerelles, est utilisé pour transférer des informations de routage entre les différents systèmes autonomes.

RIP

RIP (Routing Information Protocol) a été conçu pour fonctionner en tant qu'IGP dans des systèmes autonomes de taille modérée. RIP utilise un algorithme d'une classe connue sous le nom d'«algorithmes à vecteurs de distance», il recherche le plus court chemin au sens d'un critère de coût où seul le nombre de routeurs traversés intervient, un coût unitaire étant associé à la traversée de chaque réseau.

Le protocole est limité aux réseaux dont le plus long chemin (le diamètre du réseau) implique 15 routeurs maximum. Il est mal adapté au traitement de boucles dans les chemins et utilise des « métriques » fixes pour comparer les routes alternatives. Cela n'est pas toujours approprié pour les situations où les routes doivent être choisies en fonction de paramètres temps réel comme un délai, une fiabilité ou une charge mesurés.

OSPF

Basé sur un algorithme conçu par le chercheur en informatique néerlandais Dijkstra , l'algorithme SPF (Shortest Path First) calcule le plus court chemin vers toutes les destinations de la zone ou du SA en partant du routeur où s'effectue le calcul (à partir de sa base de données topologiques) au sens d'un critère de coût où entrent de multiples paramètres. Ce calcul est effectué de manière indépendante par tous les routeurs « OSPF » internes au SA. C'est par l'intermédiaire de cet algorithme que s'effectue la mise à jour de la table de routage : ayant trouvé les plus courts chemins d'un point à un autre, en terme de coût, le routeur est apte à connaître le prochain routeur à qui il doit transmettre le message, pour que ce dernier arrive de manière optimum à son destinataire (ce routeur étant évidement un routeur adjacent au routeur qui effectue sur le calcul et se trouvant sur ce chemin). Chaque mise à jour de la base de données entraîne la mise à jour de la table de routage. C'est ici qu'intervient la communication même entre les routeurs , communication régie par le protocole OSPF. Elle définit des règles et des formats de messages que doivent respecte les routeurs « OSPF » internes à un système autonome. OSPF a la particularité de s'appuyer directement sur IP et non sur UDP comme le protocole RIP. On distingue 5 types de messages : « Hello », « Description de base de données », « Requête d'état de liaison », « Mise à jour d'état de liaison », « Acquittement d'état de liaison ». qui permettent aux différents routeurs de s'echanger des informations sur l'état des liaisons et déterminer ainsi une fonction de coût plus réaliste que dans RIP.

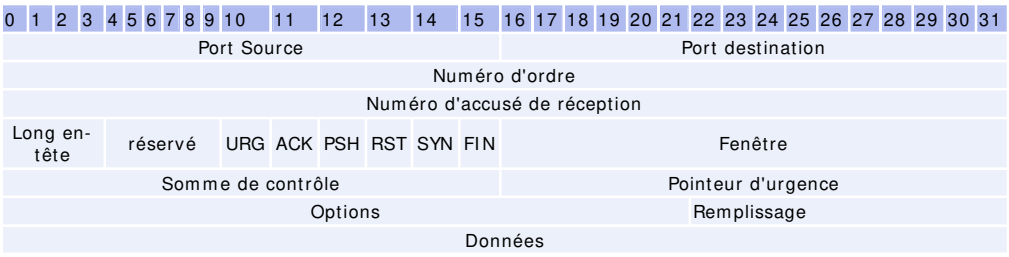
Protocoles TCP et UDP

Pour les échanges qui ont besoin d'une grande fiabilité, le protocole de Transport TCP**Erreur ! Signet non défini.** (*Transport Control Protocol*) est utilisé dans les stations d'extrémité. Pour les échanges qui ne nécessitent pas une telle fiabilité, un protocole de Transport plus simple UDP (*User Datagram Protocol*) fournit les services de bout en bout en mode sans connexion. Le protocole UDP ne possède pas de fonction de contrôle de flux, il essaye toujours de transmettre les données quelque soit l'état de congestion du réseau.

Le protocole TCP est implanté au-dessus du protocole IP pour assurer un transfert fiable en mode connecté : il fournit le même service que le protocole de transport, dit de *classe 4*, défini dans le modèle OSI. Il est capable de détecter les datagrammes perdus ou dupliqués, et de les remettre dans l'ordre dans lequel ils ont été émis. Il repose sur le principe de numérotation et d'acquittement des données, et de fenêtre d'anticipation. Il possède des fonctions de contrôle de flux par fenêtre glissante pour réguler les échanges de données entre équipements. Ce contrôle de flux pourrait être utilisé comme méthode de contrôle de congestion lorsque le protocole ICMP indique une saturation d'une partie du réseau. En fait, TCP ne tient pas compte d'ICMP. Les temporisateurs d'attente maximale d'acquittement de bout en bout sont dimensionnés de manière dynamique en fonction de la connaissance acquise sur le fonctionnement du réseau. Par ailleurs, TCP gère un flot de données urgentes, non soumises au contrôle de flux.

Le protocole TCP utilise des mécanismes plutôt complexes et des recherches sont en cours pour améliorer son efficacité dans des environnements à haut débit.

Le protocole TCP



Signification des différents champs:

Port Source (16 bits): port relatif à l'application en cours sur la machine source

Port Destination (16 bits): port relatif à l'application en cours sur la machine de destination

Numéro d'ordre (16 bits): lorsque le drapeau SYN est à 0, le numéro d'ordre est celui du premier octet du segment en cours

Lorsque SYN est à 1, le numéro de séquence est le numéro de séquence initial utilisé pour synchroniser les numéros de séquence (ISN)

Numéro d'accusé de réception (32 bits): numéro d'ordre du dernier octet reçu par le récepteur

Longueur en-tête (4 bits): il permet de repérer le début des données dans le segment. Ce décalage est essentiel car le champ d'options est de taille variable

Réservé (6 bits): Champ inutilisé actuellement mais prévu pour l'avenir

Drapeaux (flags) (6x1 bit)

URG: si ce drapeau est à 1 le paquet doit être traité de façon urgente

ACK: si ce drapeau est à 1 le paquet est un accusé de réception

PSH (PUSH): si ce drapeau est à 1, le paquet fonctionne suivant la méthode PUSH

RST: si ce drapeau est à 1, la connexion est réinitialisée

SYN: si ce drapeau est à 1, les numéros d'ordre sont synchronisés (ouverture de connexion)

FIN: si ce drapeau est à 1 la connexion s'interrompt

Fenêtre (16 bits): champ permettant de connaître le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception

Somme de contrôle (Checksum): la somme de contrôle est réalisée en faisant la somme des champs de données et de l'en-tête, afin de pouvoir vérifier l'intégrité

Pointeur d'urgence (16 bits): indique le numéro d'ordre à partir duquel l'information devient urgente

Options (Taille variable): options diverses
Remplissage: On remplit l'espace restant après les options avec des zéros pour avoir une longueur multiple de 32 bits

Le protocole UDP

L'en-tête du paquet UDP est très simple:

Port Source (16 bits)	Port Destination (16 bits)
Longueur (16 bits)	Somme de contrôle (16 bits)
Données (longueur variable)	

Port Source: il s'agit du numéro de port correspondant à l'application émettrice du paquet. Ce champ représente une adresse de réponse pour le destinataire.
Port Destination: ce champ contient le port correspondant à l'application de la machine émettrice à laquelle on s'adresse
Longueur: ce champ précise la longueur totale du paquet, en-tête comprise, exprimée en octets
Somme de contrôle: il s'agit d'une somme réalisée de telle façon à pouvoir contrôler l'intégrité de l'en-tête du paquet

Synthèse

Exercices

Exercice 1

Sachant qu'un segment TCP contient 20 octets d'en-tête et qu'il est transporté dans un datagramme IP qui contient lui aussi 20 octets d'en-tête, déterminez le débit utile maximum d'une application utilisant TCP/IP sur Ethernet.

Exercice 2

Quel intérêt y a-t-il pour un protocole (comme TCP) à ne posséder qu'un seul format d'en-tête ?

Exercice 3

Exploitez la trame Ethernet ci-dessous et donnez toutes les informations que vous pouvez en extraire. Les différentes couches de protocoles seront explicitement indiquées.

```
AA AA AA AA AA AA AA AB 00 A0 00 00 8D 20 00 40 95 AA A4 3D 08 00 45
00 00 48 2F B1 00 00 40 11 C6 F7 84 E3 3D 17 84 E3 3D 1F 06 58 00 A1
00 34 39 4F 30 82 00 28 02 01 00 04 06 70 75 62 6C 69 63 A0 1B 02 01
01 02 01 00 02 01 00 30 10 30 82 00 0C 06 08 2B 06 01 02 01 01 05 00
05 00 15 A7 5C 89
```

Exercice 4

La fragmentation et le réassemblage étant pris en charge par IP, pourquoi TCP se préoccupe-t-il de l'ordre d'arrivée des datagrammes ?

Exercice 5

Comment sont traités les en-têtes des datagrammes dans les deux cas suivants :
a) L'émetteur et le récepteur sont connectés au même réseau de type TCP/IP.
b) L'émetteur et le récepteur sont connectés à deux réseaux TCP/IP, qui sont interconnectés grâce à un routeur IP.

Quelques corrigés

Réseau d'entreprise - Intranet et Extranet

L'ensemble des protocoles utilisés dans l'Internet s'est généralisé et est devenu un standard de fait. La plupart des équipements disposent des protocoles IP, UDP, TCP,… Cependant, la connexion à l'Internet présente des risques non négligeables d'intrusion. Il peut être intéressant pour une entreprise de disposer d'un serveur Web, d'un système de messagerie électronique,… réservés à ses membres sans connecter tout son réseau à l'Internet mais en réutilisant les mêmes protocoles. On parle alors d'intranet. Ce concept est apparu à la fin des années 90. Notons qu'un réseau intranet n'est pas forcément local à un site, il s'appuie généralement sur un ensemble de réseaux locaux interconnectés entre eux par des liaisons (ou un réseau) protégées contre les intrusions.
Le concept d'intranet permet à une entreprise de disposer des services de type Internet de façon sécurisée mais seulement en interne. Lorsqu'on fournit les moyens d'échanger des informations de façon sécurisée avec des fournisseurs, des partenaires (en gardant les protocoles de l'Internet), on parle alors d'Extranet.

Architecture Client / Serveur

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, ...
Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi de client FTP, client de messagerie, ..., lorsque l'on désigne un programme, tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès du serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client messagerie il s'agit de courrier électronique).
Dans un environnement purement client/serveur, les ordinateurs du réseau (les clients) ne peuvent voir que le serveur, c'est un des principaux atouts de ce modèle. Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont:
des ressources centralisées: étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction ;une meilleure sécurité: car le nombre de points d'entrée permettant l'accès aux données est moins important ; une administration au niveau serveur: les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés ; un réseau évolutif: grâce à cette architecture ont peu supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeures.
L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles:
un coût élevé dû à la technicité du serveur et un maillon faible: le serveur lui-même, étant donné que tout le réseau est architecturé autour de lui! Heureusement, le serveur a souvent une grande tolérance aux pannes.

Les serveurs DNS

Chaque station possède une adresse IP propre. Cependant, les utilisateurs ne veulent pas travailler avec des adresses numériques du genre *192.163.205.26* mais avec des noms explicites plus faciles à mémoriser (appelées noms symboliques) du style http://www.math-info.univ-paris5.fr ou dominique.seret@math-info.univ-paris5.fr
Un système appelé DNS (Domain Names Service) permet de faire l'association entre les adresses IP et les noms symboliques. On appelle *résolution de noms de domaines* (ou *résolution d'adresses*) la corrélation entre les adresses IP et le nom de domaine associé.
Aux origines de TCP/IP, les réseaux étaient très peu étendus, le nombre d'ordinateurs connectés à un même réseau était faible, les administrateurs réseau créaient des fichiers appelés *tables de conversion manuelle* (fichiers généralement appelé *hosts* ou *hosts.txt*), associant sur une ligne, l'adresse IP de la machine et le nom littéral associé, appelé *nom d'hôte*. Ce système à l'inconvénient majeur de nécessiter la mise à jour des tables de tous les ordinateurs en cas d'ajout ou modification d'un nom de machine. Ainsi, avec l'explosion de la taille des réseaux et de leur interconnexion, il a fallu mettre en place un système plus centralisé de gestion des noms. Ce système est nommé *Domain Name System (DNS).*

Ce système consiste à une hiérarchie de noms permettant de garantir l'unicité d'un nom dans une structure arborescente. On appelle nom de domaine, le nom à deux composantes, dont la première est un nom correspondant au nom de l'organisation ou de l'entreprise, le second à la classification de domaine (.fr, .com, ...). Chaque machine d'un domaine est appelée hôte. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré (le serveur web d'un domaine porte généalement le nom *www*).
L'ensemble constitué du nom d'hôte, d'un point, puis du nom de domaine est appelé *adresse FQDN* (*Fully Qualified Domain*). Cette adresse permet de repérer de façon unique une machine. Ainsi *www.commentcamarche.net* représente une adresse FQDN.
Des machines appelées *serveurs de nom de domaine* permettent d'établir la correspondance entre le nom de domaine et l'adresse IP sur les machines d'un réseau. Chaque domaine possède ainsi un serveur de noms de domaines, relié à un serveur de nom de domaine de plus haut niveau. Ainsi, le système de nom est une architecture distribuée, c'est-à-dire qu'il n'existe pas d'organisme ayant à charge l'ensemble des noms de domaines.
Le système de *noms de domaine* est transparent pour l'utilisateur, mais chaque ordinateur doit être configuré avec l'adresse d'une machine capable de transformer n'importe quel nom en une adresse IP. Cette machine est appelée Domain Name Server. (Dans le cas d'une connexion à un fournisseur d'accès Internet, celui-ci va automatiquement jouer le rôle de DNS et fournir une adresse utilisable pour ce service)
L'adresse IP d'un second Domain Name Server (secondary Domain Name Server) peut également être introduite: il peut relayer le premier en cas de panne.
La classification du domaine correspond généralement a une répartition géographique. Toutefois, il existe des noms, créés pour les Etats-Unis à la base, permettant de classifier le domaine selon le secteur d'activité, par exemple:

- .com correspond aux entreprises à vocation commerciales (devenu international maintenant, .com ne correspond pas forcément à des entrprises commerciales...)
- .edu correspond aux organismes éducatifs
- .gov correspond aux organismes gouvernementaux
- .mil correspond aux organismes militaires
- .net correspond aux organismes ayant trait aux réseaux
- .org correspond aux entreprises à but non lucratif

La communication avec les protocoles TCP/IP requiert à chaque instant l'adresse IP du destinataire. Les aplications d'une machine hôte contactent donc le « client DNS » installé sur la machine et lui font la requête de correspondance voulue. Le client DNS transfère la requête au serveur DNS (port 53) dont l'adresse IP est donnée par la configuration de la machine. Les serveurs DNS constituent un ensembnle coopératif qui permet d'obtenir la réponse à la requête en question, le client DNS récupère (et enregistre) cette réponse et la fournit à l'application qui peut alors communiquer. Quelques microsecondes ont été nécessaires, sans que l'utilisateur final ne s'aperçoive de rien !

Gestion de la sécurité

Risques et menaces sont deux concepts fondamentaux pour la compréhension des techniques utilisées dans le domaine de la sécurité. Le *risque* est une fonction de paramètres que l'on peut maîtriser, les principaux sont la vulnérabilité et la sensibilité. La *menace* est liée à des actions et opérations émanant de tiers, elle est indépendante de la protection dont on peut se doter.
La *vulnérabilité* désigne le degré d'exposition à des dangers. Un point de vulnérabilité d'un réseau est le point le plus facile pour l'approcher. Un élement de ce réseau peut être très vulnérable tout en présentant un niveau de sensibilité très faible: le poste de travail de l'administrateur du réseau, par exemple, dans la mesure où celui-ci peut se connecter au système d'administration en tout point du réseau.
La *sensibilité* désigne le caractère stratégique, au sens valeur, d'un composant du réseau. Celui-ci peut être très sensible, vu son caractère stratégique mais quasi-invulnérable, grâce à toutes les mesures de protection qui ont été prises pour le prémunir contre les risques potentiels. Exemples : le câble constituant le média d'un réseau local lorsqu'il passe dans des espaces de service protégés, l'armoire de sauvegarde des logiciels de tous les commutateurs du réseau, ...
On peut classer les risques en deux catégories : les risques *structurels* liés à l'organisation et la démarche d'une entreprise, les risques *accidentels* indépendants de l'entreprise.

Enfin, selon leur niveau de sensibilité et de vulnérabilité, on distingue souvent quatre niveaux de risques.
– Les *risques acceptables* n'induisent aucune conséquence grave pour les entités utilisatrices du réseau. Ils sont facilement rattrappables : pannes électriques de quelques minutes, perte d'une liaison, ...
– Les *risques courants* sont ceux qui ne portent pas un préjudice grave au réseau. Ils se traduisent, par exemple, par une congestion d'une partie du réseau. La mauvaise configuration d'un équipement peut causer la répétition des messages émis, un opérateur peut détruire involontairement un fichier de configuration, ...
– Les *risques majeurs* sont liés à des facteurs rares, mais pouvant causer des préjudices de nature à causer des dégats importants, mais toujours rattrappables. Un incendie a ravagé le centre de calcul d'une entreprise. La conséquence se traduit par le remplacement de l'ensemble du matériel, mais, heureusement, tous les logiciels et les données sont sauvegardés et archivés dans un local anti-feu.
– Les *risques inacceptables* sont, en général, fatals pour l'entreprise, ils peuvent entraîner son dépot de bilan. Exemple : la destruction du centre de calcul et de l'ensemble des sauvegardes des programmes et données.
Les *menaces passives* consistent essentiellement à copier ou à écouter l'information sur le réseau, elles nuisent à la *confidentialité* des données. Dans ce cas, l'information n'est pas altérée par celui qui en prélève une copie, d'où des difficultés pour détecter ce type de malveillance. Elles ne modifient pas l'état du réseau. La méthode de prélèvement varie suivant le type de réseau. Sur les réseaux cablés, on peut imaginer un branchement en parallèle grâce à des appareils de type analyseurs de protocole ou une induction (rayonnement électromagnétique). Sur les faisceaux hertziens, des antennes captent les lobes secondaires des faisceaux ; dans les transmissions par satellites, des antennes avec sytèmes de poursuite existent, …
Les *menaces actives* nuisent à l'*intégrité* des données. Elles se traduisent par différents types d'attaques. On distingue le brouillage, le déguisement (modification des données ou de l'identité), l'interposition (déguisement en émission ou en réception). Les niveaux de piratage sont très variables, puisque la gamme des pirates s'étend de l'amateur sans connaissances particulières du réseau qu'il pénêtre ou tente d'infiltrer au professionnel, souvent membre de l'entreprise, et au courant des procédures clés du réseau. Les mécanismes de sécurité doivent donc prendre en considération aussi bien le sondage aléatoire que pratique l'amateur à la recherche d'un mot de passe, que la lecture, aux conséquences désastreuses, du catalogue central des mots de passe, des codes de connexion ou des fichiers. Les menaces actives sont de nature à modifier l'état du réseau.
Les menaces *dues aux accidents* (26%) sont le fait d'incendies, d'inondations, de pannes d'équipements ou du réseau, de catastrophes naturelles, ... Les menaces *dues aux erreurs* (17%) sont liées à l'utilisation et l'exploitation, la conception et la réalisation, le défaut de qualité, ... Les menaces *dues à la malveillance* (57% dont 80% sont d'origine interne) concernent les actes tels que le vol des équipements, les copies illicites de logiciels et de documents techniques, le sabotage matériel et l'attaque logique (virus, modification, …), les intrusions et l'écoute, les actes de vengeance...

Services de sécurité

L'ISO a défini plusieurs services de sécurité. Ceux-ci sont assurés par différents types de mécanismes et diffèrent par leur sophistication, leurs coûts, les efforts nécessaires pour leur implantation, leur maintenance et leurs besoins en ressources humaines.

Authentification

Ce service permet d'authentifier les partenaires qui communiquent, au moyen d'un protocole donné, indépendamment de l'émission d'un message. L'authentification a pour but de *garantir l'identité* des correspondants. On distingue :
– l'authentification de l'entité homologue qui assure que l'entité réceptrice qui est connectée est bien celle souhaitée. Son action peut intervenir à l'établissement de la communication et pendant le transfert des données. Son objectif principal est donc la lutte contre le déguisement.
– l'authentification de l'origine qui assure que l'entité émettrice est bien celle prétendue. Le service est inopérant contre la duplication d'entité. Comme le prédédent, il s'agit d'authentification simple
– l'authentification mutuelle qui assure que les deux entités émettrice et réceptrice se contrôlent l'une l'autre.

Le service d'authentification est inutilisable dans le cas d'un réseau fonctionnant en mode "sans connexion".

Contrôle d'accès

Ce service empêche l'utilisation non autorisée de ressources accessibles par le réseau. Par "utilisation", on entend les modes lecture, écriture, création ou suppression. Les ressources sont les systèmes d'exploitation, les fichiers, les bases de données, les applications, … Ce service utilise le service d'authentification vu ci-dessus afin de s'assurer de l'identité des correspondants transportée dans les messages d'initialisation des dialogues.

Confidentialité des données

L'objet de ce service est d'empêcher des données d'être compréhensibles par une entité tierce non autorisée, le plus souvent en état de fraude passive.

Intégrité des données

Contre les fraudes actives, ce service détecte les altérations de données entre émetteur et récepteur. On distingue :
– l'intégrité des données en mode connexion *avec récupération* (c'est sur l'ensemble des données transmises que se fait la vérification d'intégrité : le service relève les modifications, les insertions, les suppressions et les répétitions de données et assure la remise en état des données) ;
– l'intégrité des données en mode connexion *sans récupération* ;
– l'intégrité d'un champ spécifique, ce service n'agit que sur quelques données incluses dans une transmission (les modifications, suppressions, insertions et répétitions sont détectées) ;
– l'intégrité des données en mode sans connexion (la détection de modification est toujours fournie, par contre les détections d'insertions et de répétitions ne sont que partielles et optionnelles) ;
– l'intégrité d'un champ spécifique en mode sans connexion, ce service n'assure plus que la détection de modification dans un champ de données sélectionné.

Non-répudiation

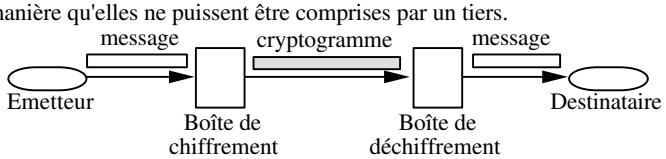
La non-répudiation de l'origine fournit au récepteur une preuve empêchant l'émetteur de contester l'envoi ou le contenu d'un message effectivement reçu. La non-répudiation de la remise fournit à l'émetteur une preuve empêchant le récepteur de contester la réception ou le contenu d'un message effectivement émis.

Protection contre l'analyse de trafic

Le secret du flux lui-même empêche l'observation du flux de transmission de données, source de renseignements pour les pirates. Ce cas s'applique aux situations où l'on a besoin de garder la confidentialité sur l'existence même de la relation entre les correspondants.
Mécanismes de sécurité
Plusieurs mécanismes réalisent les services de sécurité énumérés ci-dessus.

Chiffrement

Le chiffrement transforme tout ou partie d'un texte dit *clair* en *cryptogramme*, message chiffré ou protégé. Si une ligne utilise des dispositifs de chiffrement, les données sont transmises sous une forme "brouillée", de manière qu'elles ne puissent être comprises par un tiers.



Le mécanisme de chiffrement émet un message X sous une forme secrète au moyen d'une clé K. L'émetteur dispose d'une fonction algorithmique E, qui à X et K associe $E(K,X)$. Le récepteur reçoit $E(K,X)$ (message chiffré émis) et le déchiffre au moyen de sa clé K' avec sa fonction D, qui à $E(K,X)$ et K' associe X. On a alors : $D(K', E(K,X)) = X$

Les fonctions *E* et *D* peuvent être secrètes ou publiques. Il en est de même pour les clés *K* et *K'*. L'existence d'un déchiffrement tient à la définition de l'algorithme donnant *E* et *D*, et de la méthode produisant et répartissant les clés *K* et *K'*.
Le mécanisme de chiffrement existe typiquement à deux niveaux : *voie par voie* ou *de bout-en-bout*. L'ensemble repose, dans tous les cas, sur un algorithme donné, un couple de clés associées et un mécanisme de distribution des clés.
Le *chiffrement voie par voie* est le résultat de la mise en place de boîtes noires sur les lignes, qui laissent les données en clair au niveau des hôtes et des nœuds du réseau. Le message est chiffré/déchiffré indépendamment à chaque changement de ligne. Le chiffrement de voie appartient à la couche Liaison de Données. L'intrusion sur une ligne si on connaît sa clé n'aboutit pas à l'accès des autres lignes qui sont susceptibles de posséder des clés différentes. De plus, un texte complet, en-têtes et informations d'acheminement, peut être chiffré sur la ligne. Enfin, cette solution libère le logiciel des tâches de chiffrement puisque ce dernier est réalisé par une boîte de chiffrement placée du côté numérique du modem aux deux extrémités de la ligne. Dans ce cas, le service est fourni par l'infrastructure du réseau utilisé.
Le *chiffrement de bout-en-bout* laisse en clair les informations de routage. Seules les données constituant l'information transmise sont chiffrées. Dans un réseau multi-nœuds, le message traverse plusieurs nœuds et garde le même chiffrement depuis son émetteur jusqu'à son destinataire final. Le chiffrement de bout-en-bout appartient logiquement à la couche Présentation. Les données restent brouillées dans les nœuds. La distribution des clés est plus aisée dans un système de bout-en-bout.

Signature numérique et fonction de condensation

La production d'une signature numérique est obtenue par l'application d'un algorithme au message transmis qui devient *signé*. Le plus souvent, cette signature numérique est le résultat d'une transformation cryptographique du message, indépendante de la taille de ce dernier, et de taille réduite. Le propre de la signature est qu'elle est vérifiable par tous, mais inimitable. Les algorithmes qu'on utilise en matière de signature numérique sont asymétriques. L'expression théorique d'un message signé sera de la forme $E[K,h(M)]$ où *M* représente le message, $h(M)$ l'image de *M* par une fonction de condensation et $E[K,h(M)]$ la signature proprement dite.

Contrôle d'accès

Ce mécanisme utilise l'identité authentifiée des entités ou des informations fiables pour déterminer leurs droits d'accès au réseau ou aux ressources sur le réseau. De plus, il est susceptible d'enregistrer sous forme de trace d'audit et de répertorier les tentatives d'accès non autorisées.
Les informations utilisées sont :
– les listes de droits d'accès, maintenues par des centres,
– les mots de passe,
– les jetons de droits d'accès,
– les différents certificats,
– les libellés de sensibilité des données.
Le mécanisme de contrôle d'accès peut avoir lieu aux deux extrémités de la communication (équipement d'accès et ressource du réseau).

Intégrité des données

L'intégrité d'une unité de données ou d'un champ spécifique de données se fait par les codes de contrôle *cryptographique*, dont le mécanisme est identique à celui des signatures numériques.
L'intégrité d'un flot de données peut être assurée par le même mécanisme de cryptographie auquel s'ajoutent des codes de détection d'erreurs ainsi que la numérotation des unités de données par horodatage.

Echange d'authentification

Lorsque les entités homologues et les moyens de communication sont sûrs, l'identification des entités homologues peut se faire par des *mots de passe*. Par mots de passe, on entend aussi bien les véritables mots de passe que l'utilisateur physique donne pour accéder à un système, que les codes de connexion qu'un terminal utilise. Un mot de passe est souvent composé de deux parties : le mot de passe proprement dit, plus un identificateur d'utilisateur qui permet le contrôle du mot de passe. L'identificateur n'est pas

approprié pour la sécurité car il est habituellement de notoriété publique, tel le numéro d'identification de l'employé, et ne peut être changé facilement du fait que beaucoup d'informations s'y rattachent.
Dans certaines applications, l'utilisateur ne connaît même pas son mot de passe qui est inscrit sur une piste magnétique contenant un Numéro d'Identification Personnel. Dans d'autres applications, seul l'utilisateur connaît son numéro, et une fonction lui permet de changer son mot de passe. Le cas des guichets bancaires est particulier : le client doit introduire une carte contenant son code, plus une clé secrète, certains ordinateurs désactivant ce code tous les mois pour forcer un changement.
Lorsque les moyens de communication ne sont pas sûrs, les mots de passe ne suffisent plus à réaliser le mécanisme ; il faut alors y adjoindre des procédures de chiffrement.

Bourrage

Ce mécanisme sert à simuler des communications dans le but de masquer les périodes de silence et de banaliser les périodes de communication réelles. Ceci permet de ne pas attirer l'attention des pirates lors des démarrages de transmission.
Un mécanisme de bourrage de voie est obtenu en envoyant sur la ligne, entre deux émissions de messages utiles, des séquences de messages contenant des données dépourvues de sens. Le générateur de messages respectera la fréquence des lettres et des diagrammes de l'alphabet employé.

Contrôle de routage par gestion dynamique de la bande passante

Après détection d'une attaque sur une route donnée, ou tout simplement pour prévenir cette attaque, les systèmes d'extrémités ou les réseaux peuvent, par ce mécanisme, sélectionner une route plus sûre. Dans certains cas, la modification périodique est programmée afin de déjouer toutes les tentatives malveillantes.

Notarisation

Une garantie supplémentaire peut être apportée par la *notarisation* : les entités font confiance à un tiers qui assure l'intégrité, l'origine, la date et la destination des données. Le processus sous-entend que ce tiers doit acquérir les informations par des voies de communication très protégées.

Les aspects opérationnels de la sécurité

Les techniques de sécurité décrites ci-dessus permettent de réduire les risques de manière significatives. Elles ne peuvent pas les éliminer totalement. Des mécanismes de détection d'intrusion ou de violation doivent être implantés pour surveiller de façon continue la sécurité. Le flot général des messages, événements et alarmes est similaire à celui de la gestion des pannes. Cependant des actions spécifiques sont à prendre pour la gestion de la sécurité. Elles doivent, en particulier, avoir un impact minimal sur le fonctionnement opérationnel du réseau et maximiser les chances de "coincer" le pirate.
Les journaux sont les sources d'information les plus utiles. Ils contiennent :
– tous les événements et incidents de communication présélectionnés par le responsable de la sécurité (refus d'accès, tentatives de connexion, …);
– les identificateurs des usagers, émetteur, récepteur avec une indication de l' initateur de la connexion,
– la date, heure,…
– les ressources impliquées dans la communication,
– les mots de pase et/ou clés utilisées,
– les fonctions de sécurité appelées, manuellement ou automatiquement.
Les équipements et instruments de collectes de mesures et de gestion des pannes participent à la gestion de la sécurité. Certains équipements sont spécifiques : les boîtes de chiffrement, les contrôleurs d'accès, les contrôleurs d'authentification, les solutions de sécurité pour les LAN…
Parmi les outils classiques, nous pouvons citer le standard DES, l'algorithme RSA, l'algorithme MD5, Kerberos et les pare-feux *(firewalls*).

Le standard de chiffrement DES

Le mécanisme de cryptage le plus utilisé est basé sur le standard américain DES (Data Encryption Standard) adopté par le NIST en 1977. Les blocs de données sont découpés en 64 bits et l'algorithme

transforme chaque bloc en un autre bloc de 64 bits à l'aide d'une clé (limitée par les instances fédérales américaines) de 56 bits. Le même algorithme et la même clé sont utilisés pour le déchiffrement. Il s'agit d'un algorithme dont toutes les opérations sont connues (permutations, additions, substitutions) dont la sécurité réside dans la clé (secrète) c'est-à-dire dans la complexité des calculs nécessaires pour analyser toutes les clés possibles, en l'absence de toute autre information.
Pour augmenter la sécurité d'un tel système, on utilise fréquemment plusieurs opérations en cascade (double DES voire Triple DES), ayant des clés différentes.

L'algorithme de chiffrement RSA

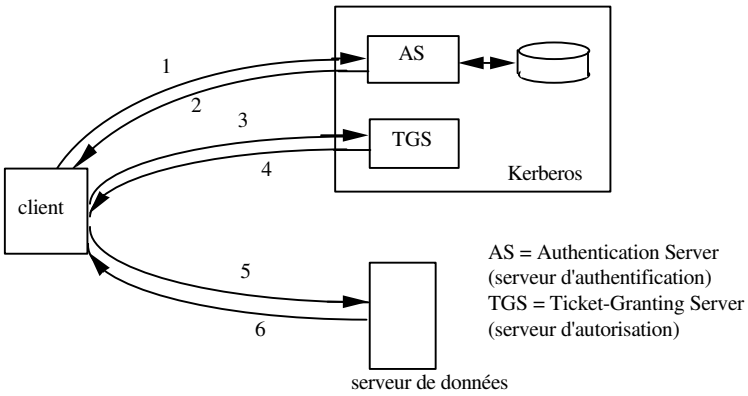
L'algorithme RSA (Rivest, Shamir, Adleman, du nom de ses concepteurs) est un alorithme à clé publique conçu au MIT en 1978. Il est basé sur des problèmes NP complets : par exemple, la décomposition d'un nombre en facteurs premiers (le nombre en question a 100 ou 200 chiffres…). Celui qui cherche à protéger ses communications rend ce nombre public (dans un annuaire…), mais le résultat de la décomposition est connu de lui seul. Même si un espion intercepte un message, il ne peut donc pas le déchiffrer. Un tel algorihtme permet au seul récepteur autorisé de lire les messages qui lui sont destinés.

L'algorithme de signature MD5

Egalement conçu par Rivest, cet algorithme à clé publique utilisé pour la confidentialité et l'authentification. MD5 (Message Digest 5, défini en 1992 dans le RFC 1321, successeur de MD4…) prend en entrée des messages de longueur quelconque qu'il découpe en blocs de 512 bits pour produire en sortie un bloc de 128 bits grâce à une fonction de condensation. Les calculs sont basés sur des opérations simples, faites sur des blocs de 32 bits, pour une implémentation rapide.

Le service Kerberos

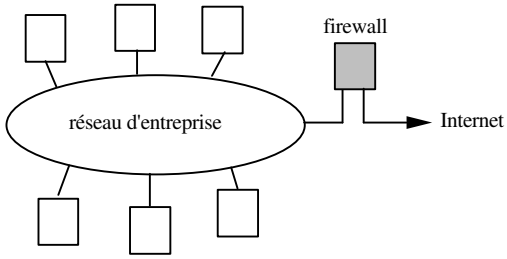
Kerberos est un service d'authentification développé au MIT pour fournir des services de sécurité dans un environnement client/serveur distribué. Le principe de fonctionnement est illustré sur la figure suivante. Pour utiliser un service, un client doit tout d'abord fournir auprès du serveur d'authentification un certificat, preuve de son identité et de ses droits. Il reçoit en retour des données ayant une durée de vie limitée : un ticket et une clé. Armé de ces données, le client adresse alors au serveur d'autorisation un message chiffré et daté contenant une demande d'autorisation d'accès à un serveur donné et reçoit en retour un nouveau ticket et une nouvelle clé. Il utilisera ces dernières informations pour se connecter sur le serveur de données, lequel vérifiera la validité des informations fournies. L'algorithme de chiffrement utilisé est le DES.



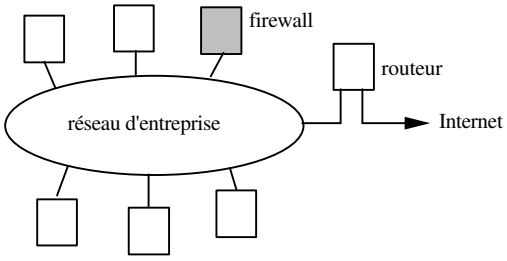
Kerberos repose sur une station du réseau, il est responsable de la génération de toutes les clés et gère les certificats d'identité et les tickets d'autorisation. Tous les serveurs de données et les applications du réseau doivent être déclarés auprès de Kerberos. Notons que celui-ci ne gère pas l'accès aux fichiers ordinaires et suppose que l'environnement est un réseau local utilisant les protocoles de la famille TCP/IP.

Les pare-feux

La connexion d'un réseau d'entreprise à l'Internet est la porte ouverte à toutes les intrusions. On protège alors le réseau en filtrant les accès depuis ou vers l'Internet dans un routeur appelé "firewall**Erreur ! Signet non défini.**" ou pare-feu**Erreur ! Signet non défini.** ou encore bastion. Ce filtrage doit offrir en toute tranparence aux utilisateurs du réseau d'entreprise tous les services dont ils ont besoin à l'extérieur et protéger els accès aux applications et aux données à l'intérieur du réseau d'entreprise.
Le filtrage peut se faire au niveau des datagrammes sur leur entête (filtrage sur les adresses ou sur le contenu (type de protocole, par exemple). Le filtrage peut aussi se faire au niveau applicatif (ftp et telnet, par exemple, sont des applications interdites), ceci suppose que le firewall connaît toutes les applications… Dans les deux cas, le filtrage peut être positif ou négatif : tout ce qui n'est pas explicitement interdit est autorisé ou tout ce qui n'est pas explicitement autorisé est interdit ! Il est judicieux d'interdire par défaut tout ce qui n'est pas explicitement autorisé…
Le pare-feu à séparation de réseaux (*dual homed firewall)* est un routeur qui possède deux cartes réseaux, séparant physiquement le réseau d'entreprise de l'Internet : tout le trafic inter-réseau passe donc par le firewall qui peut exécuter son filtrage sur chaque requête entrante ou sortante… .



Le pare-feu peut être une machine du réseau, distincte du routeur qui assure l'accès à l'Internet. On parle alors de *screened host firewall,* de "pare-feu au fil de l'eau" ou encore de bastion. C'est le routeur qui agit activement en faisant transiter tout le trafic venant d'Internet vers la machine pare-feu. Il bloque tout trafic destiné à l'Internet qui est émis par une machine quelconque du réseau autre que le pare-feu. Les machines internes du réseau doivent donc connaître le pare-feu et lui adresser tout leur trafic effectivement destiné à l'Internet.



Réseaux privés virtuels

On désigne par *réseau privé virtuel* (VPN, *Virtual Private Network*) un réseau d'entreprise constitué de plusieurs sites reliés par Internet. La traversée d'Internet est vue comme un *tunnel*, dans lequel les données de l'entreprise sont chiffrées et transitent d'un bout à l'autre. L'entreprise ne peut avoir connaissance des autres données qui circulent sur les liaisons empruntées. Pour mettre en oeuvre ce mécanisme de tunnel, on utilise un protocole spécial pouvant assurer plusieurs services selon les besoins de l'entreprise : confidentialité, intégrité des données, authentification des machines d'extrémité. Le principal protocole de tunnel est utilisé au niveau Réseau : il s'agit d'*IPSec*, une version sécurisée d'IP définie par la RFC 2246. L'entreprise reçoit donc le même service que si les liaisons lui appartenaient. C'est pourquoi on parle de réseau virtuel.
Deux machines passerelles, situées à chaque extrémité du tunnel, négocient les conditions de l'échange des informations : quels algorithmes de chiffrement, quelles méthodes de signature numérique ainsi que les clés utilisées pour ces mécanismes. Elles traitent ensuite les données avec la politique de sécurité associée. A titre d'exemple, il est possible d'authentifier les adresses IP utilisées ainsi que les données

grâce à une signature numérique puis chiffrer l'ensemble du paquet IP en l'« encapsulant » dans un nouveau paquet, ce qui a pour effet de rendre le paquet inexploitable par un utilisateur non autorisé.

Synthèse

Exercices

Exercice 1

Une entreprise possédant un siège et plusieurs filiales à distance souhaite mette en place un Intranet avec un Web interne situé au siège, la messagerie électronique, le transfert de fichier et des groupes de discussions. Le fournisseur d'accès à l'Internet est choisi et le raccordement se fait par le réseau téléphonique commuté pour les filiales et par liaison spécialisée pour le siège. Proposer une architecture matérielle et logicielle pour cet Intranet. Sachant que le serveur Web transfère des pages de 20 koctets simultanément vers 25 utilisateurs situés dans les filiales et que l'on souhaite que le temps de réponse (le temps de transmission et affichage d'une page) soit inférieur à 10 seconde, quel débit faut-il choisir pour la ligne ?

Exercice 2

Une entreprise largement déployée sur la région parisienne possède environ 250 sites et 12000 postes de travail identiques auxquels il faut ajouter 250 serveurs (un par site). Les deux sites les plus éloignés sont distants de 123 km.
Peut-on imaginer un réseau Ethernet pour cette entreprise ? Pourquoi ?
Le directeur du système d'information (DSI) décide d'implanter un réseau Ethernet par site et un réseau fédérateur FDDI auquel est relié chacun des Ethernet (directement ou indirectement...). Quels matériels d'interconnexion sont nécessaires ? Combien ? Proposer une solution d'interconnexion.
L'administrateur réseau demande une adresse IP pour son entreprise ? Quelle classe lui faut-il ? Il obtient 145.87.0.0. Ceci lui convient-il ? Peut-il prévoir un plan d'adressage avec autant de numéros de sous-réseaux qu'il y a de réseaux physiques existants ?
Le DSI voudrait mettre en œuvre un serveur Web accessible depuis l'extérieur de l'entreprise. Proposer une localisation possible et un modèle de sécurité pour ce serveur.
Seuls 3% des utilisateurs sont effectivement autorisés par la direction de l'entreprise à sortir de l'entreprise et naviguer sur l'Internet (toutes applications confondues). Le plan d'adressage précédent est-il utile ? Pourquoi ? Proposer une solution.

Exercice 3

Soit deux réseaux locaux RL1 et RL2, interconnectés par une passerelle. Deux stations, STA sur le réseau RL1 et STB sur le réseau RL2, communiquent grâce aux protocoles TCP/IP. La taille des datagrammes IP dans le réseau RL2 est 2 fois inférieure à celle des datagrammes dans le réseau RL1.
a) Expliquez la procédure d'échange et le séquencement des opérations lors d'un transfert de fichiers entre STA et STB.
b) Proposez des types de passerelle que l'on puisse utiliser dans les cas suivants:
Cas 1 : les 2 réseaux sont situés sur le même site.
Cas 2 : les 2 réseaux sont utilisés par deux entités d'une même société, situées aux deux extrémités d'une grande ville.
Cas 3 : les 2 réseaux relient 2 structures situées dans des villes différentes.
Cas 4 : le premier réseau se trouve en France, le deuxième aux États-Unis.

Exercice 4

Une station A souhaite accéder à une page Web sur une machine B. Les caractéristiques de A et B sont

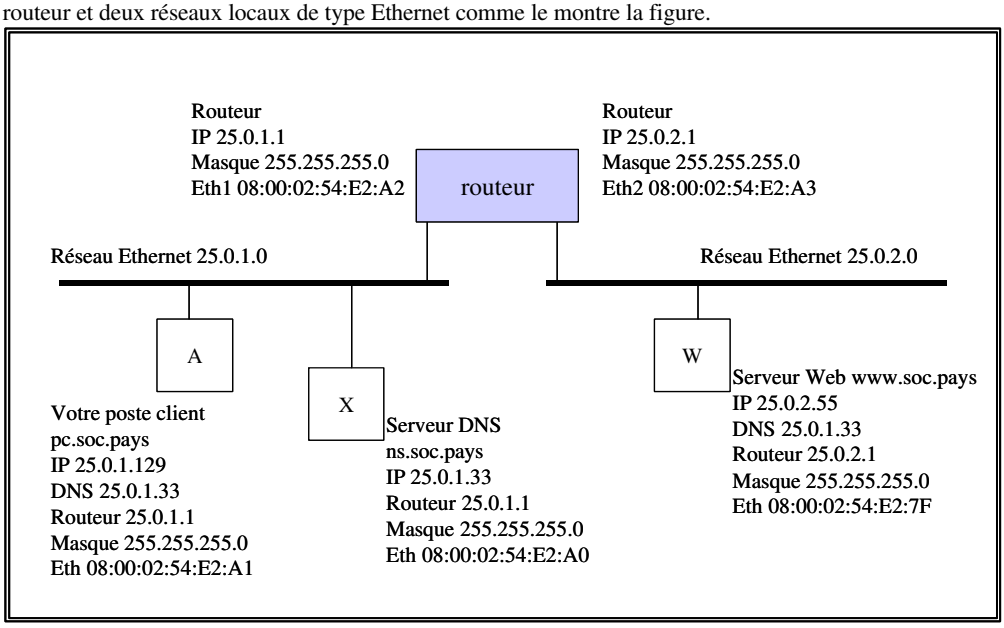
Machine	Nom logique	Adresse IP
A	topaze.univ-paris5.fr	194.132.6.9
B	dizzie.univ-tahiti.fr	192.41.8.1

Indiquer :

a/ Quel est l'élément de la machine A qui fait la résolution nom logique / adresse IP
b/ Comment sait-on que le destinataire B n'est pas situé sur le même réseau que la source ?
c/ Qui est responsable de la détermination de la route à suivre ?

Exercice 5

On considère un réseau composé de trois ordinateurs (votre PC, un serveur DNS et un serveur Web), un routeur et deux réseaux locaux de type Ethernet comme le montre la figure.



Donnez les différentes trames échangées sur les deux réseaux Ethernet lorsque la machine A (pc.soc.pays) cherche à établir une session www sur le serveur W (www.soc.pays).
On supposera que les trois machines et le routeur sont correctement configurés. Ils viennent d'être installés et sont allumés lorsque le client commence sa requête. On supposera également que la machine X (ns.soc.pays) se trouvant sur le même réseau que le client dispose de l'information permettant de résoudre directement le nom www.soc.pays en une adresse IP.
La réponse à cette question se présentera sous la forme d'un tableau donnant les trames Ethernet dans l'ordre chronologique. On indiquera pour chaque trame le réseau sur lequel elle a été émise (1 pour le réseau 25.0.1.0 et 2 pour le réseau 25.0.2.0), les adresses physiques de la source et de la destination de la trame, les adresses IP de la source et de la destination (si nécessaire) et un bref commentaire sur le contenu ou la fonction de cette trame ou de son contenu. La dernière trame à indiquer dans la table est celle contenant l'arrivée de la confirmation d'établissement de la connexion TCP utilisée entre A et W.
Modèle attendu pour la réponse

#	Réseau	Ad. phy source	Ad. phy dest	IP source	IP dest.	Commentaire
1						
2						
3						
...						

Exercice 6

Pour protéger des données confidentielles, on utilise un système de chiffrement dit de César (qui consiste à décaler les lettres de l'alphabet d'une constante). Montrer qu'il est très aisé de déchiffrer le message suivant (écrit en français) :

Zsgashwsfrwbhsfbsh

Exercice 7

Ecrire en pseudo langage les règles de filtrage nécessaires à refuser en entrée d'un routeur pare-feu pour le réseau 195.45.3.0 (de masque 255.255.255.0) les attaques en déni de service : inondation de requêtes de connexion TCP ou de messages ICMP avec des adresses IP usurpées.

Quelques corrigés

Exercice 2

La distance entre les sites est trop importante pour faire un seul réseau ethernet. Il faut donc mettre en place autant de réseaux Ethernet que de sites donc 250 réseaux Ethernet.
Il faudrait 250 routeurs, 1 pour chaque réseau, or pour une entreprise cela revient trop cher. On regroupe donc les sites par 10, et ces regroupements sont reliés au FDDI par des gros routeurs, ce qui en réduit le nombre a 25 et donc ce qui réduit le coût pour l'entreprise.
Il lui faut une adresse de classe B car il y a 12 000 postes, une adresse de classe C étant insuffisant pour couvrir tous les postes (254 postes seulement)
145.87.0.0 est une adresse de classe B, elle couvre 65534 postes, ce qui est largement suffisant. Plan d'adressage : de 145.87.1.0 à 145.87.252.0 : une adresse par site + une adresse pour le FDDI
Le serveur Web serait idéalement placé à mi-chemin entre les deux sites les plus éloignés. En effet l'un ne sera pas désavantagé dans l'accès aux pages Web par rapport à l'autre. Le modèle de sécurité à envisager dans le cas d'accès extérieur est le modèle DMZ couplé à un firewall. Il permet une protection du réseau interne vis-à-vis de l'extérieur, mais permet aussi à des serveurs et/ou des applications à se connecter à l'extérieur (après configuration).
Le plan d'adressage précédent n'est plus utile. En effet une adresse de classe C composée de sous-réseaux aurait été suffisante puisque le réseau ne sert qu'en interne. Pour le serveur Web, il faudrait le placer sur le site qui a le plus d'accès externe vers Internet (le plus d'utilisateurs autorisés). Un routeur et un firewall bien configurés suffisent à protéger le réseau interne.

Exercice 4

a /le résolveur DNS ou client DNS
b/ parce que les préfixes 194 et 192 sont différents !
c/ le module IP situé dans le routeur de sortie du réseau de la machine A

Exercice 6

Lesmetiersdinternet
le code est le suivant : décalage de 14 lettres
clair : abcdefghijklmnopqrstuvwxyz
chiffré : opqrstuvwxyzabcdefghijklmn
En français la lettre la plus fréquente est le e : ici il y a 5s et 3h. Il est logique de tester y=e. Le reste vient tout seul ensuite puisque le décalage est constant…
Le système est donc très facilement cassable dès lors que l'on connaît les fréquences des lettres dans la langue utilisée !

Exercice 7

Usurpation d'adresse : des messages proviendraient de l'extérieur du réseau avec une adresse d'émetteur qui est une adresse interne
Définition des paramètres :
ouraddr = 195.45.3.0/24 (toutes les adresses de notre réseau)
anyaddr = n'importe quelle adresse
Effacer toutes les règles en entrée

Refuser les messages en entrée dont l'adresse source est ouraddr, l'adresse destination est ouraddr, le protocole est TCP et le bit SYN est mis à 1
Refuser les messages en entrée dont l'adresse source est ouraddr, l'adresse destination est ouraddr et le protocole est ICMP