Réseaux et Protocoles (partie 2)

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

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 ;

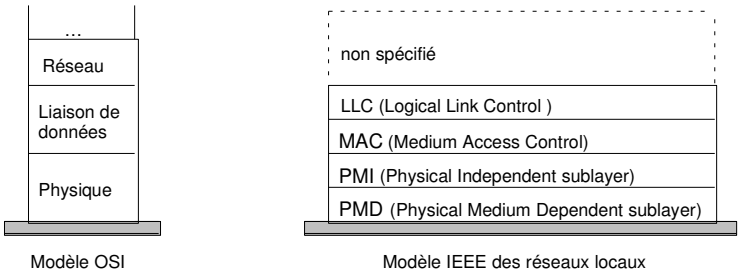
– la fiabilité prend plus ou moins d'importance selon le type d'application supportée par le réseau local.

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.

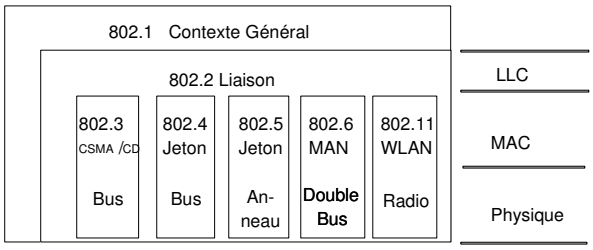
L’adoption d’une architecture en couches permet de disposer d’une même couche LLC quelle que soit la technique de partage du support utilisée. La normalisation ne concerne pas les couches au-dessus de LLC ; il est possible d’implanter directement des protocoles applicatifs ou des protocoles d’interconnexion 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

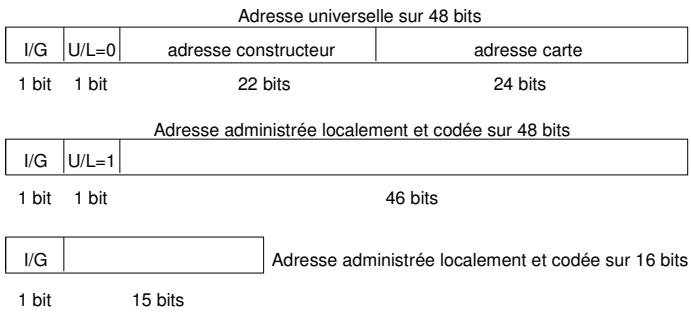
Les travaux de normalisation ne concernent que les deux premières couches. Ils sont menés par le comité 802 de l’IEEE (Institute for Electricity and Electronics Engineers. Le comité 802 de cette société savante s'est occupé de normalisation des réseaux locaux. Il est essentiellement constitué de constructeurs 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.



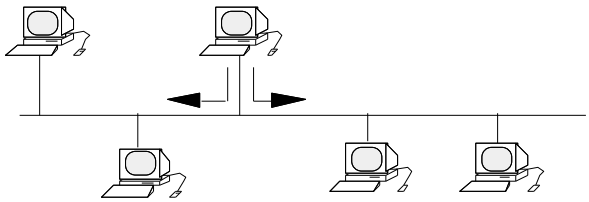
Le bit I/G=0 pour une adresse individuelle, I/G=1 pour une adresse de groupe.

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.*

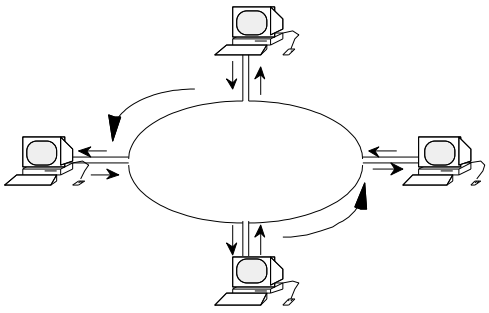
Dans la topologie en bus, tous les éléments sont reliés à un support physique commun. Une structure en " arbre sans racine " est utilisée. Les topologies en bus sont conçues de façon à ce qu'il n'y ait qu'un seul chemin entre deux éléments du réseau. Il n'y a pas de boucles. Le support est de type bidirectionnel, 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

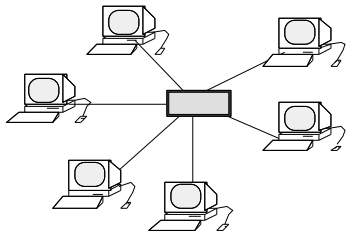
Dans la topologie en anneau, le support relie toutes les stations deux à deux, de façon à former un anneau. Le support est utilisé de façon unidirectionnelle et l'information circule dans un seul sens. Toute station, hormis celle qui génère la trame, réémet le signal reçu provoquant la diffusion de la 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.

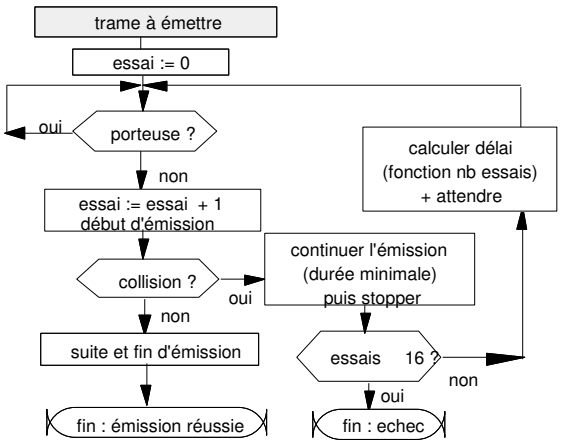
La fibre optique est de plus en plus utilisée malgré un coût plus élevé. Les avantages en sont une totale immunité aux bruits, un très faible poids, un encombrement minimal et une très large bande passante ; les inconvénients, le coût et la complexité de connectique.

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.

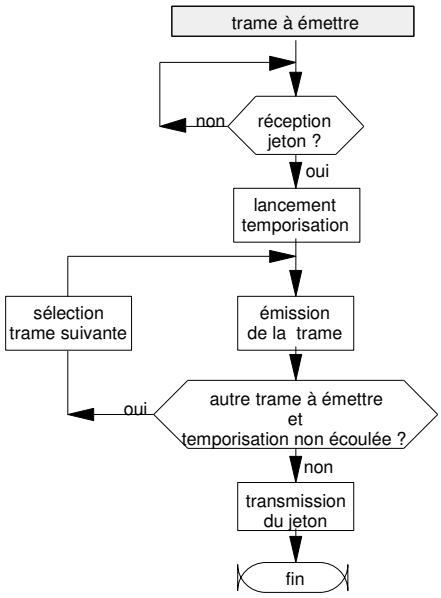


Algorithme d’émission CSMA/CD

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.



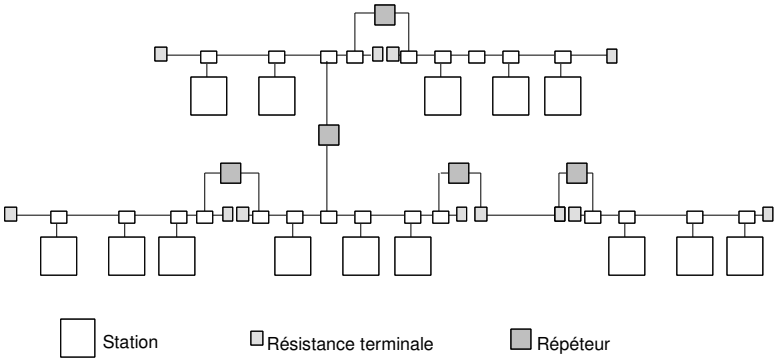
Principe général de l'accès par jeton

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.

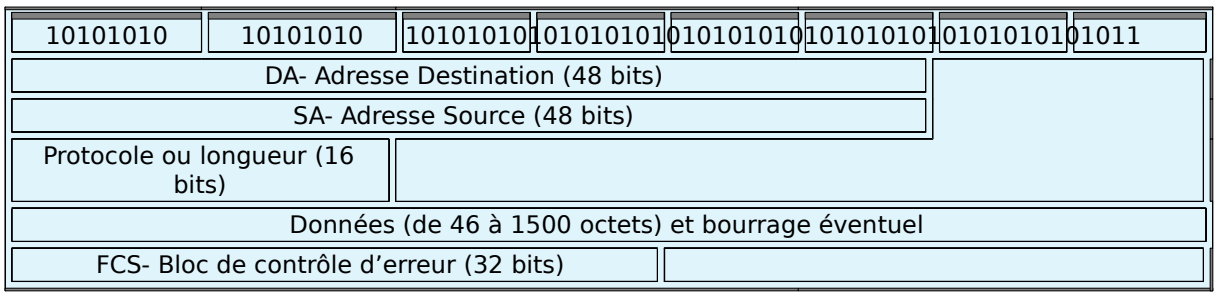


Entre deux stations, on traverse au plus 5 segments.

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.*

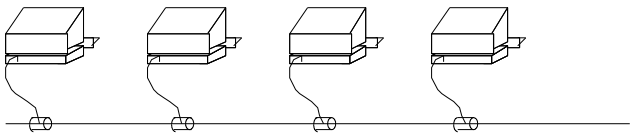


La taille de la trame (moins les 8 octets de préambule) doit être comprise entre 64 et 1518 octets, ce qui laisse de 46 à 1500 octets "utiles". Un contenu plus court que 46 octets est complété par des caractères de remplissage.
Dans la norme, le champ protocole était supposé indiquer la longueur effective 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

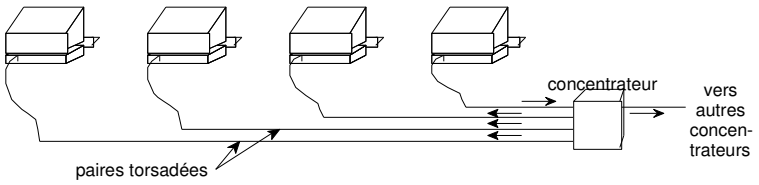
Le plan de câblage définit la façon dont on organise physiquement les connexions des stations. Il peut suivre la topologie en bus, ou bien être en étoile.
La nomenclature usuelle désigne le type de câblage et de topologie physique par sous la forme *X*Base*t* où *X* désigne le débit exprimé en Mbit/s, 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.

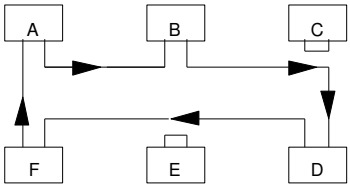


Câblage en étoile avec paire torsadée

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.



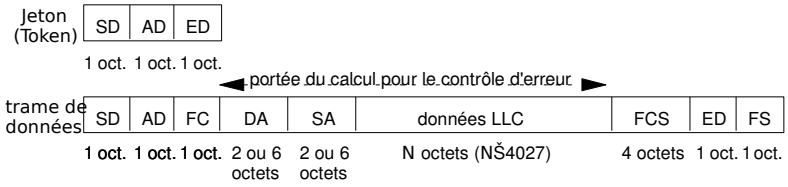
Les stations C et E sont en by-pass.

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

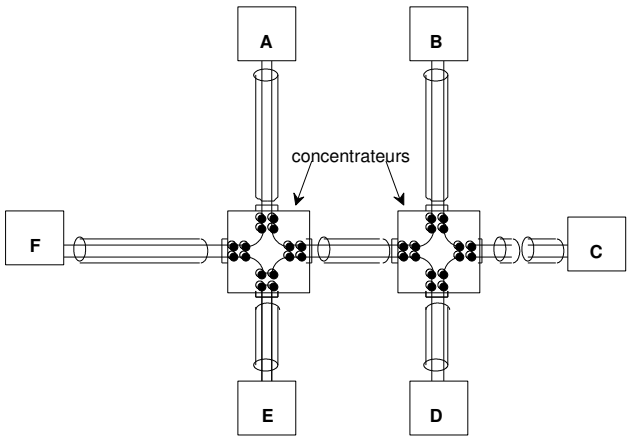
Gestion de l'anneau dans les réseaux IEEE 802.5

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

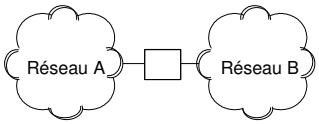
Logical Link Control, qui est basé sur les formats du protocole normalisé HDLC. Trois types de LLC ont été définis :
– LLC1 est sans connexion et fournit un service de type *datagramme* sans aucun contrôle, en point à point, en multipoint ou en diffusion ;
– LLC2 assure un service avec connexion entre 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.

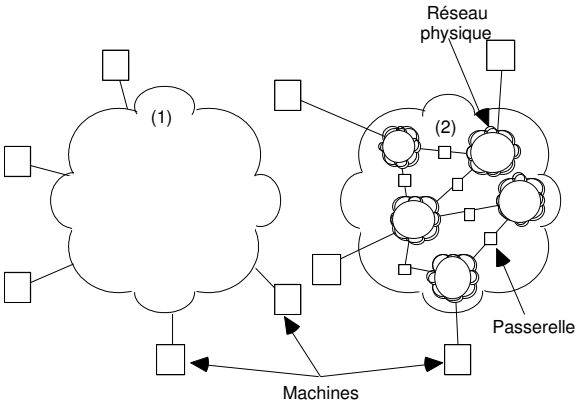
Une passerelle reliant deux réseaux

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.

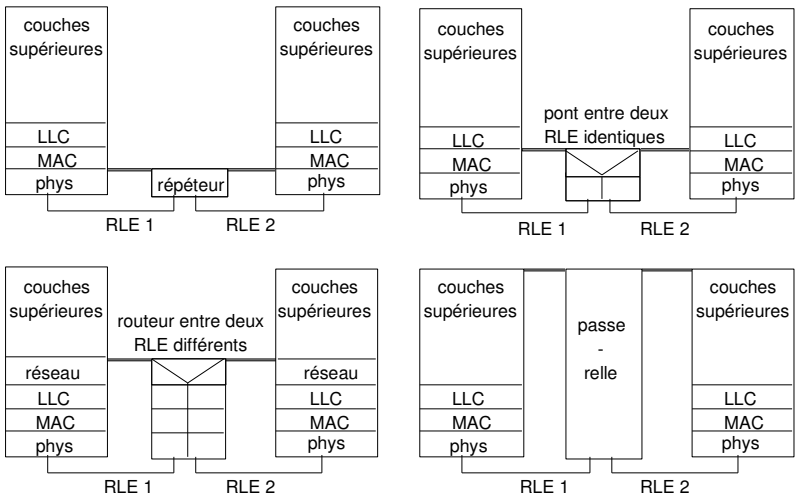


Une interconnexion de réseaux vue par l'utilisateur (1) : chaque machine semble être raccordée à un seul et immense réseau : le réseau virtuel unique.
La structure réelle (2) : des réseaux physiques interconnectés par des passerelles

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

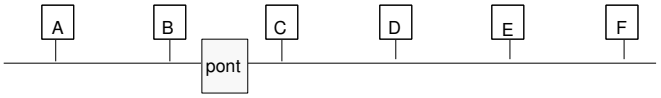


Niveaux d'interconnexion de réseaux locaux

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.

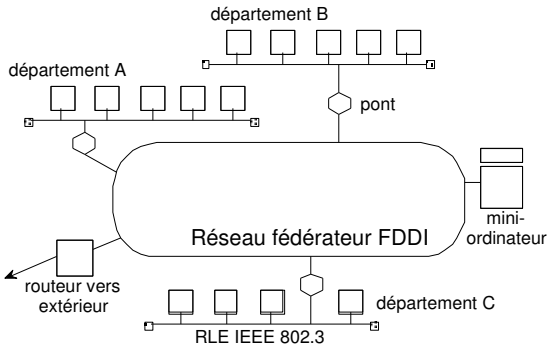
Les deux machines A et B échangent énormement de données entre elles ; D, C, E et F ont un trafic quelconque réparti sur toutes les machines.



Les deux machines A et B échangent énormement de données entre elles ; leur trafic ne pertube plus les autres machines grâce au pont.

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

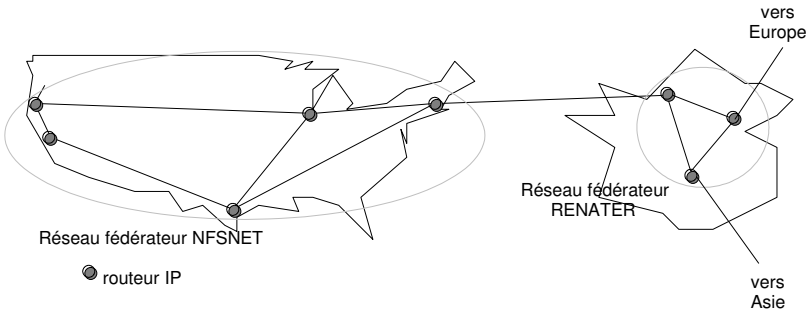
Internet ne constitue pas un nouveau type de réseau physique. Il offre, par l'interconnexion de multiples réseaux, un service de réseau virtuel mondial basé sur les protocoles TCP et IP. Ce réseau virtuel repose sur un adressage global se plaçant au-dessus des différents réseaux utilisés. Les divers 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

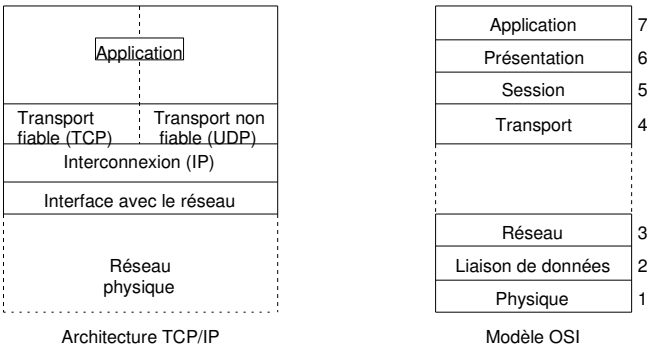
Différents acteurs

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

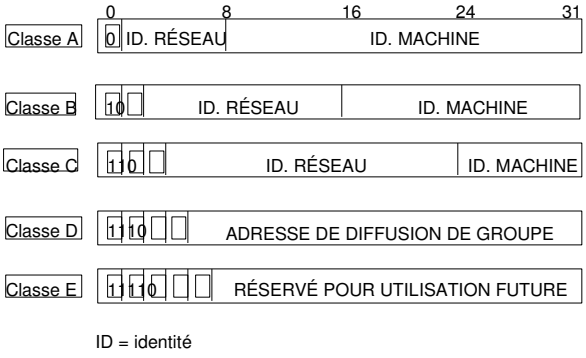
Grâce à Internet, le modèle d'architecture TCP/IP, conçu selon les mêmes principes que l'OSI, s'est répandu et a été adopté dans la plupart des réseaux d'entreprise. Ce modèle permet une interconnexion de réseaux hétérogènes avec un service minimal : le service de remise non fiable de datagramme en mode 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.

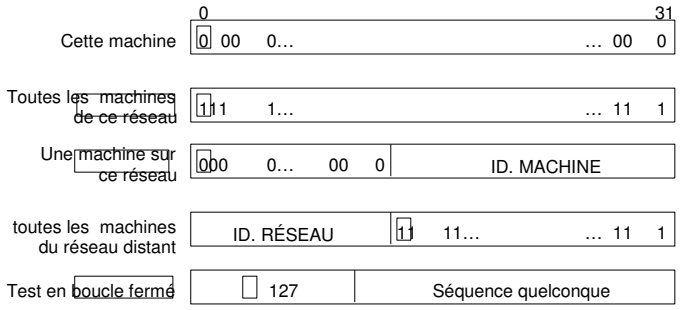
Les classes d'adresse IP

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. .

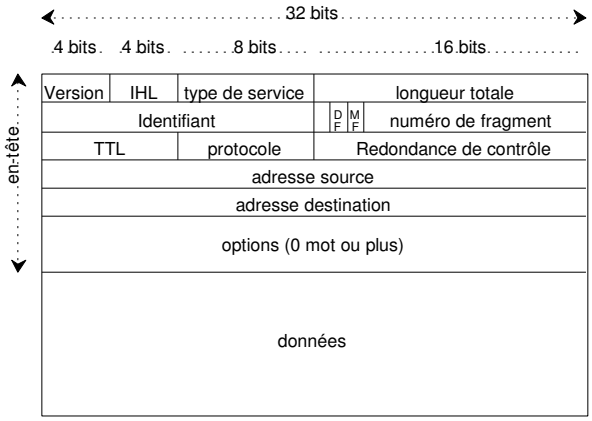
classe	Information	Nombre maximum de machines
A	**10.x.y.z**, où 0 <= x <= 255 0 <= y <= 255 et 0 <= z <= 255	(256*256*256) - 2 = 16 777 214

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.

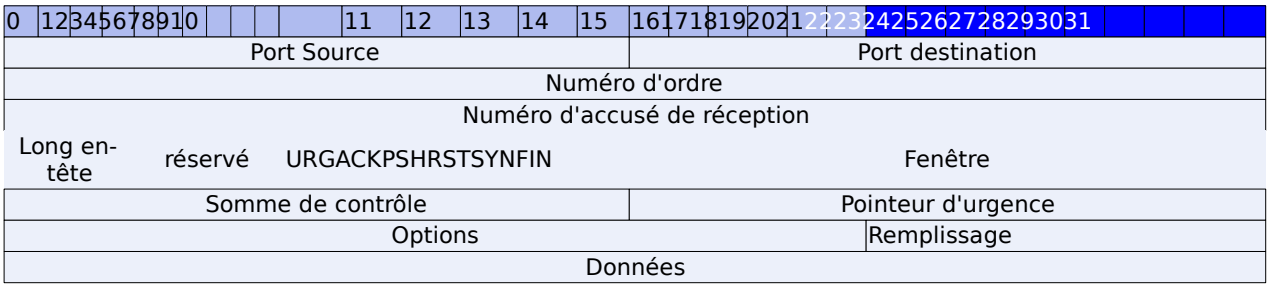
OSPF

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

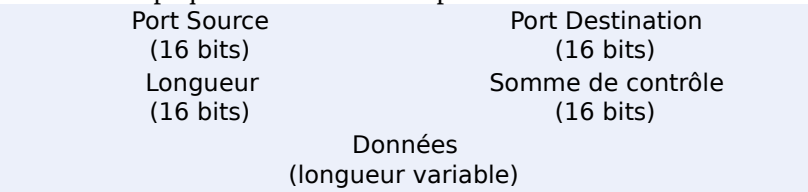


Signification des différents champs:
Port Source (16 bits): port relatif à l'application en cours sur la machine source
Port Destination (16 bits): port relatif à l'application en cours sur la machine de destination
Numéro d'ordre (16 bits): lorsque le drapeau SYN est à 0, le numéro d'ordre est celui 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: 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 utailisable 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

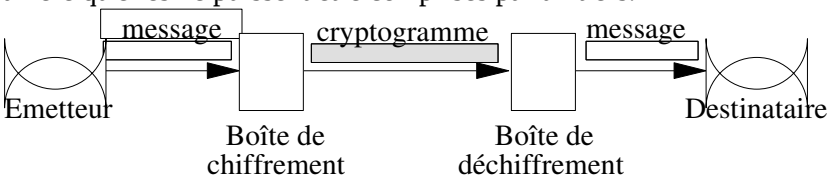
La non-répudiation de l'origine fournit au récepteur une preuve empêchant l'émetteur de contester l'envoi ou le contenu d'un message effectivement reçu. La non-répudiation de la remise fournit à l'émetteur une preuve empêchant le récepteur de contester la réception ou le contenu d'un message effectivement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

Échange 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

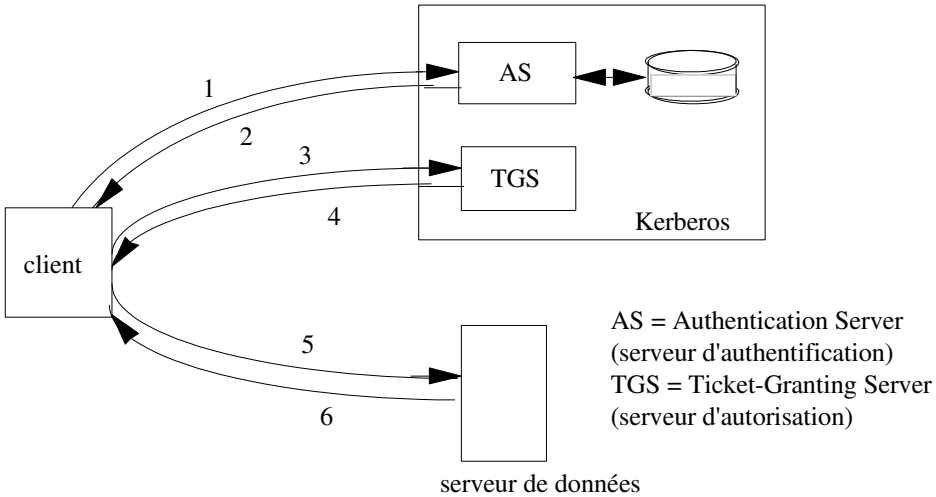
L'algorithme RSA (Rivest, Shamir, Adleman, du nom de ses concepteurs) est un alorithme à clé publique conçu au MIT en 1978. Il est basé sur des problèmes NP complets : par exemple, la décomposition d'un nombre en facteurs premiers (le nombre en question a 100 ou 200 chiffres…). Celui qui cherche à protéger 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.

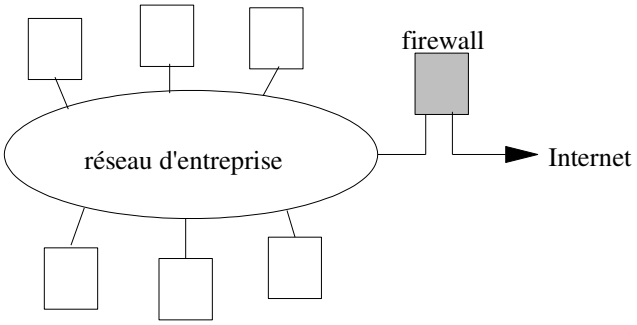


Kerberos repose sur une station du réseau, il est responsable de la génération de toutes les clés et gère les certificats d'identité et les tickets d'autorisation. Tous les serveurs de données et les applications du réseau doivent être déclarés auprès de Kerberos. Notons que celui-ci ne gère pas l'accès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

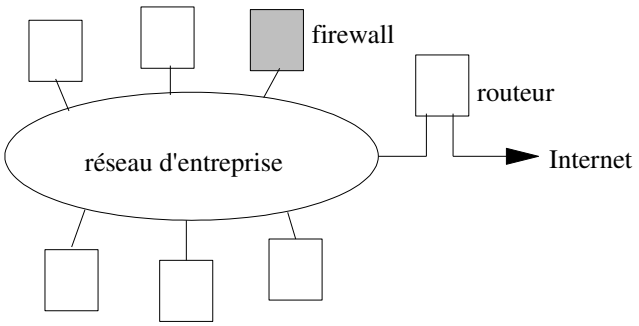
Les pare-feux

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

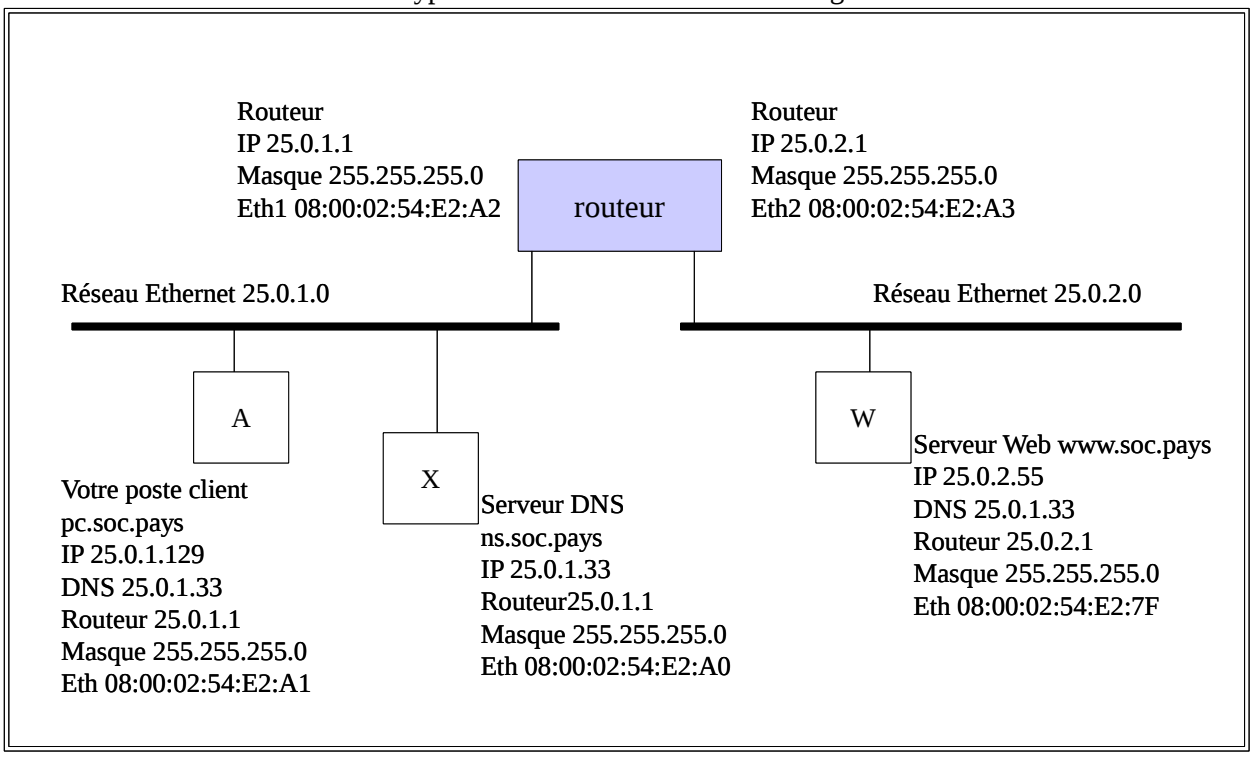
Une station A souhaite accéder à une page Web sur une machine B. Les caractéristiques de A et B sont

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