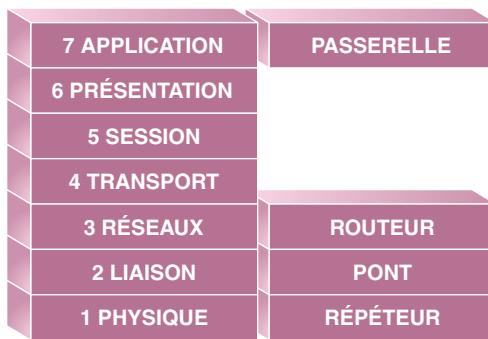


1 Matériel réseaux

1•1 Besoins d'interconnexion

- La méthode d'accès à un réseau Ethernet (CSMA/CD) engendre des collisions. Plus le nombre de machines augmente, plus le débit diminue et le réseau devient vite inexploitable. Afin de pallier le problème, des solutions existent pour segmenter le réseau en plusieurs sous-réseaux.
- Il faut pouvoir connecter des réseaux locaux utilisant des méthodes d'accès et des protocoles différents.
- Il est également nécessaire de procurer au réseau local une ouverture vers les réseaux étendus (ex. : Internet via Numéris).

Les moyens d'interconnexion



Pour résoudre ces problèmes les constructeurs proposent différents moyens d'interconnexion. Selon les couches du modèle OSI concernées ces modules portent le nom :

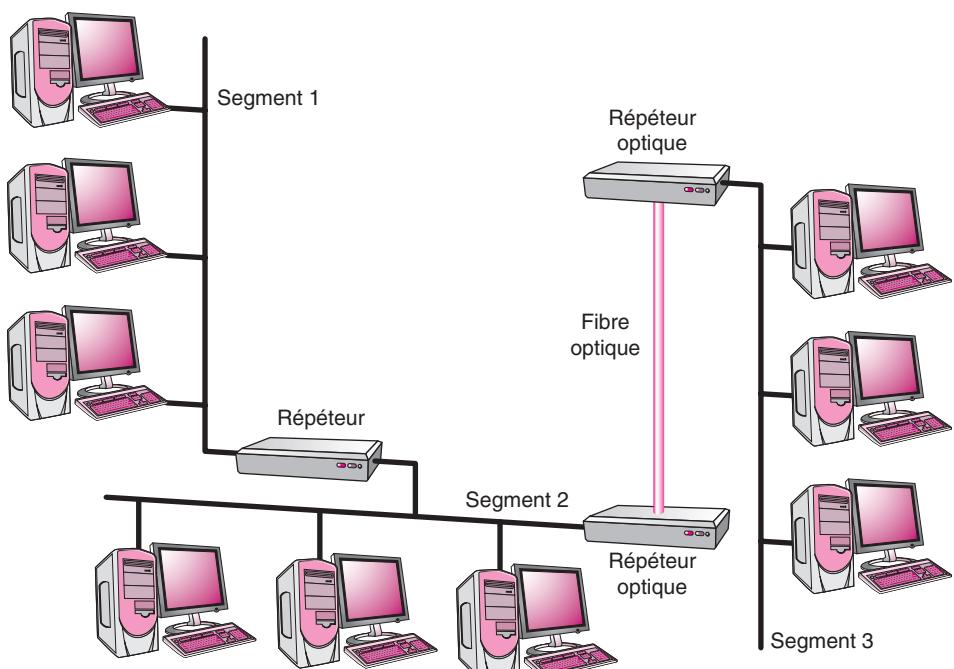
- Répéteur
- Pont, commutateur
- Routeur
- Passerelle.

C

Les réseaux et les serveurs

1•2 Les répéteurs et concentrateurs

Moyens d'interconnexion



Moyens d'interconnexion (suite)

DÉFINITION

- Un répéteur assure l'**interconnexion de niveau 1**, (couche physique).
- Il relie différents segments d'un **même réseau**, après avoir régénéré les signaux, ce qui permet d'augmenter la longueur globale du réseau.
- Ils peuvent aussi assurer l'interconnexion de segments éloignés par des fibres optiques.

FONCTION DES RÉPÉTEURS

- Retransmission des trames bit par bit (sans lecture des adresses ni vérification du CRC).
- Re-synchronisation des paquets.
- Transmission des conditions de collision.
- Mise à l'arrêt de segments au terme de 32 collisions consécutives.
- Re-branchement automatique de segments sélectionnés après la bonne réception ou transmission d'une trame.

LES CONCENTRATEURS

Ils interviennent aussi sur la couche physique mais ils émulent une topologie en bus par une topologie en étoile.

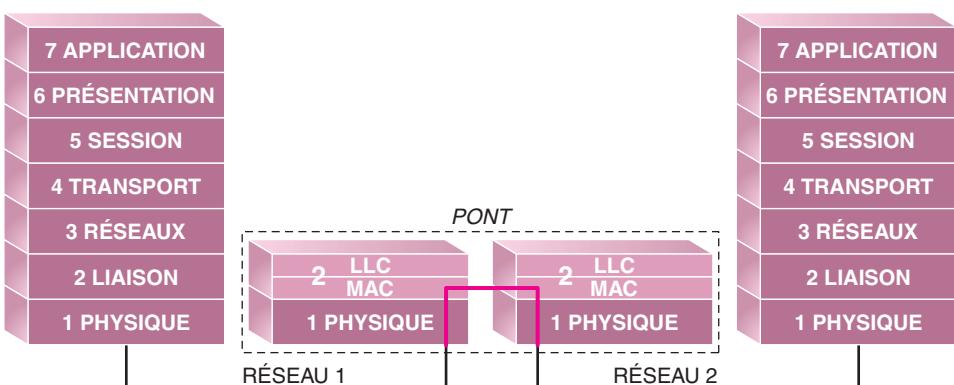
Il existe 2 types de concentrateurs :

- Classe I : distance maximum 100 m ; on ne peut connecter aucun autre concentrateur.
- Classe II : distance maximum 100 m ; on peut connecter un autre concentrateur.

1•3 Le pont

- Le pont (*bridge* en anglais) assure l'interconnexion de niveau 2 (couche liaison).
- Un pont permet donc d'interconnecter des réseaux possédant des supports de transmission et des techniques d'accès différents.
- Un pont filtrant détermine le ou les destinataire(s) de la trame en analysant les adresses source et destination **au niveau liaison (adresses MAC)**.
- 2 segments d'un pont doivent être dans un même domaine d'adressage (IP, IPX...).
- Les broadcasts traversent le pont.

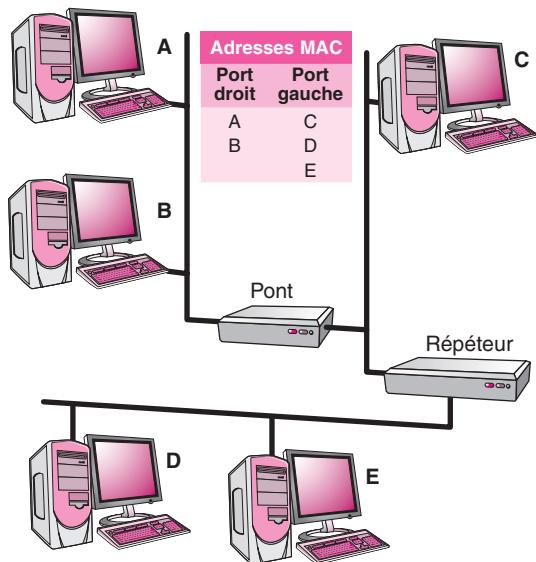
Liaison par pont



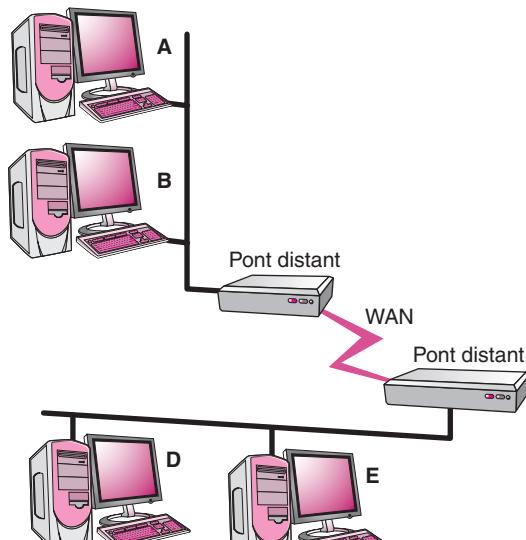
Il existe des ponts locaux qui travaillent sur un même réseau local ou des ponts distants qui permettent de relier 2 réseaux locaux distants.

Liaisons par pont (suite)

FONCTIONNEMENT



Liaison par pont local



Liaison par pont distant

FONCTIONS DES PONTS

- Ils jouent le rôle de « frontière » entre deux domaines physiques avec transparence vis-à-vis des stations et permettent ainsi un **isolement du trafic**.
- Ils forment un réseau logique à partir de plusieurs réseaux physiques.
- Ils permettent d'étendre les distances en local (4 répéteurs de chaque côté du pont).
- Ils permettent d'interconnecter des réseaux éloignés (ponts distants).

On réalise donc avec les ponts des groupes de travail.

• Trame de A vers B

– La trame est relevée par le pont (port droit).

– En lisant les zones d'adresse (source et destination), si le pont remarque que les deux stations se trouvent sur le même LAN, il éliminera la trame par filtrage. La trame n'étant pas transmise, le risque de collision sur l'autre LAN (2) s'en trouve diminué.

• Trame de A vers C (ou D ou E)

– Le pont constate que les deux stations se trouvent sur deux LAN différents, il l'acheminera.

– Plusieurs techniques peuvent être retenues :

1. Donner à chaque station une adresse dont certains bits correspondent au numéro du segment sur lequel elles sont connectées.

2. Implanter dans chaque pont une table de correspondance entre l'adresse des stations et le numéro du segment sur lequel elles sont connectées.

3. Constituer automatiquement la table de correspondance par apprentissage.

Lorsqu'une trame est destinée à une station non connue du pont, celui-ci laisse passer la trame sur les autres segments, puis note lors de la réponse de la station si elle se situe sur le segment d'origine ou sur les autres.

1•4 Commutateurs, switchs

PRÉSENTATION

On a vu avec les ponts que l'on améliore le rendement en segmentant le réseau, mais il reste toujours le fait que toutes les stations situées sur le même port du pont se partagent la bande passante.

Afin d'améliorer le rendement, pour les utilisateurs gourmands en bande passante, il est possible d'incorporer un commutateur ou switch.

Chaque utilisateur disposera alors de toute la bande passante.

FONCTIONNEMENT

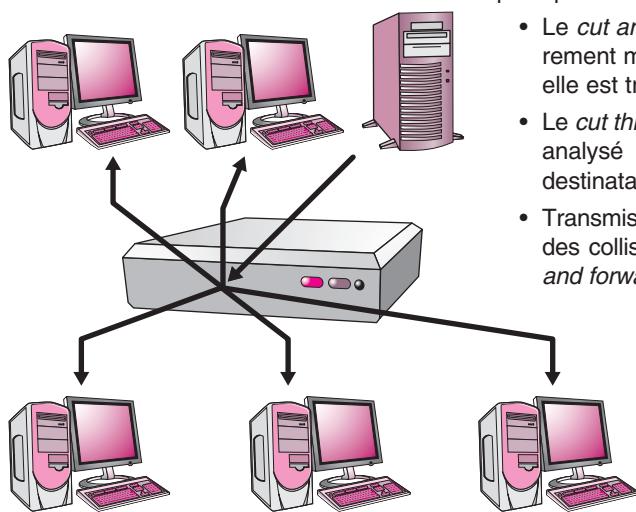
Le commutateur travaille au niveau 2 : il examine donc les adresses MAC.

Après lecture de l'adresse de destination, le concentrateur met en relation la machine émettrice et la machine réceptrice. Le transfert des données dispose donc de toute la bande passante. Simultanément une autre liaison station à station peut être établie et disposer aussi de toute la bande passante.

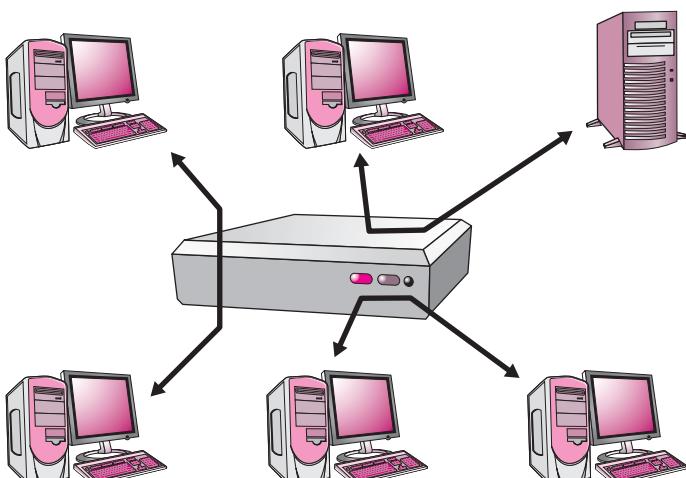
Pour réaliser ces liaisons, il existe trois principes de fonctionnement :

- Le *cut and forward* : la trame est entièrement mémorisée ; si elle est correcte elle est transmise au destinataire.
- Le *cut through* : l'en-tête de la trame est analysé et immédiatement envoyé au destinataire.
- Transmission adaptative : après analyse des collisions, on bascule en mode *cut and forward* ou en mode *cut through*.

Commuteurs



Solution avec concentrateur :
la bande passante
est partagée entre
tous les utilisateurs.



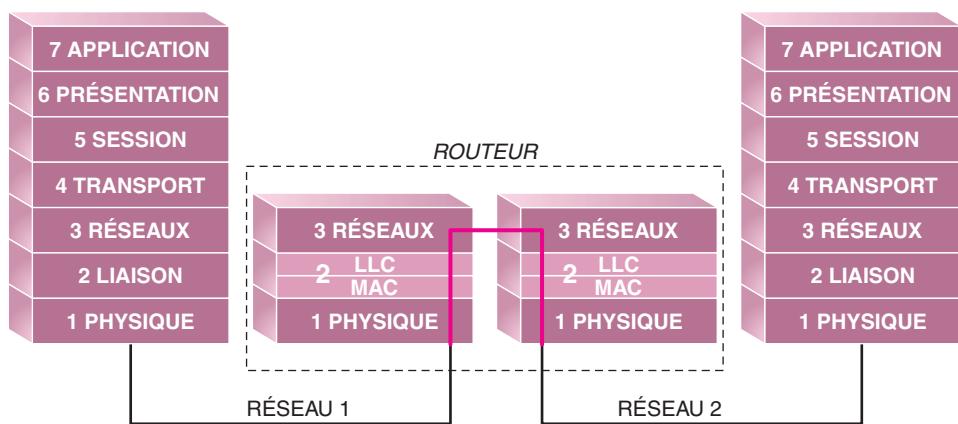
Solution avec commutateur

1•5 Le routeur

DÉFINITION

- Le routeur assure l'interconnexion de niveau 3, c'est-à-dire jusqu'à la couche réseau.
- Les routeurs gèrent de multiples protocoles.
- Les broadcasts MAC (niveau 2 ne traversent pas un routeur).
- Seuls les protocoles routables (IP, IPX...) le traversent, les autres (NETBEUI) ne passent pas le routeur.
- Ils permettent de subdiviser le réseau en domaines ou régions.
- Ils permettent à chaque nœud de définir le meilleur chemin pour transmettre les informations d'une station à une autre.

Routeurs



FONCTIONNEMENT

- Le routeur décompacte les trames et extrait les datagrammes de niveau 3 contenant l'adresse réseau.
- Suivant la table de routage il convertit si nécessaire le protocole et re-compacte la trame avant de la transmettre.
- Les stations devant traverser le routeur auront l'adresse réseau de la station réceptrice et l'adresse Mac du port du routeur.
- Si il existe plusieurs routeurs sur le réseau, un calcul du meilleur chemin peut être réalisé suivant le type de routage.

Il existe 2 façons d'effectuer un routage :

- Le routage statique : c'est l'administrateur qui introduit manuellement les adresses réseaux et les routes dans les tables de routage.
- Le routage dynamique : il y a détection automatique des routes et adresses par apprentissage.

Les chemins empruntés dans le réseau peuvent être modifiés en fonction du trafic sur certaines branches du réseau.

**UN PONT SEGMENTE LES DOMAINES DE COLLISION
UN ROUTEUR SEGMENTE LES DOMAINES DE DIFFUSION**

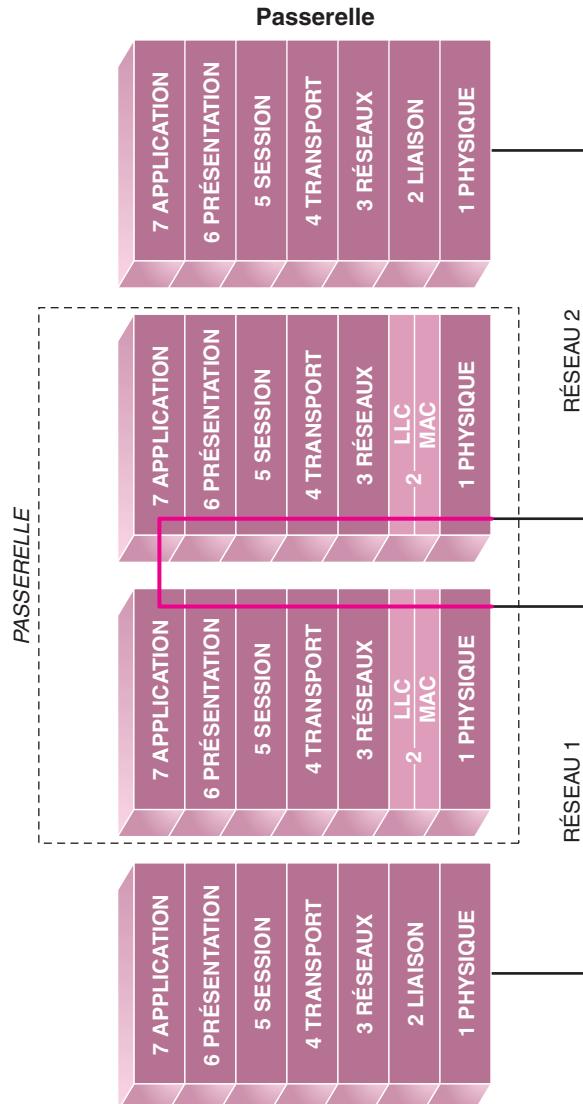
C

Les réseaux et les serveurs

1•6 La passerelle

La passerelle assure l'interconnexion jusqu'au niveau 7.

Passerelles

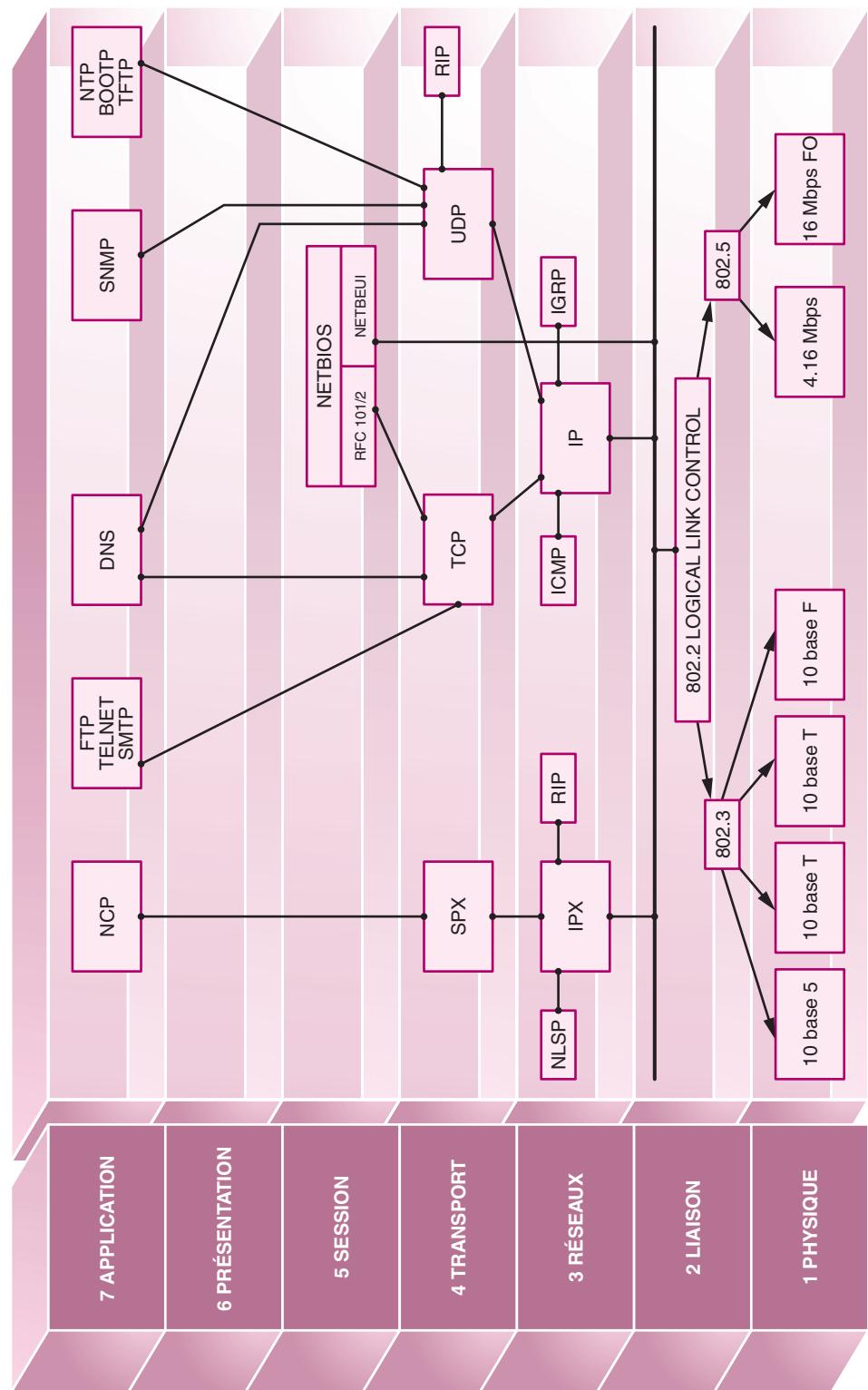


→ Une passerelle permet donc d'adapter l'ensemble des caractéristiques d'un réseau à celles d'un autre réseau.

→ Une passerelle constitue le système d'interconnexion le plus sophistiqué pour faire passer les informations d'une architecture réseau donnée à une autre totalement différente.

→ La passerelle est plus lente et nécessite généralement un micro-ordinateur dédié. Son utilisation est donc plus rare.

Passerelles (suite)



2 Du réseau local à Internet

Sur un réseau local, les différents postes peuvent communiquer entre eux. Pour dialoguer avec un autre réseau, l'usage d'un routeur devient nécessaire. En connectant tous ces réseaux ensemble, on obtient Internet, le réseau des réseaux.

Le routeur permet de changer de réseau. Lorsque la distance séparant les postes est importante, on fait appel à un modem chargé de moduler et démoduler les signaux à envoyer ou à recevoir. Il existe différents types de modems suivant le type de connexion choisie : modem RTC, ADSL ou spécifique au câble ou à la fibre optique.

Pour rendre plus parlante la référence aux sites Web, on utilise le plus souvent une URL à la place d'une adresse IP mettant en œuvre un serveur DNS. Ce dernier peut être vu comme un véritable annuaire faisant la correspondance entre les URL des sites Web et leurs adresses IP.



TLD

TLD : Top Level Domain

Depuis février 2011, l'attribution d'une adresse IP s'effectue en IPV6. L'enregistrement d'un nom de domaine passe par un « registrar » et ne coûte que quelques euros à quelques dizaines d'euros suivant le TLD choisi. Il est possible de faire appel à l'hébergement et aux autres services proposés par le FAI ou le registrar.

Via une interface Web, le registrar propose d'associer le nom de domaine précédemment réservé à l'adresse IP correspondant au serveur de l'hébergeur ou à celui de votre choix. Il est possible aussi de se lancer dans la mise en place d'un serveur DNS en installant et en paramétrant l'application Bind. Les DNS des FAI peuvent faire l'objet d'un filtrage et retourner en conséquence une adresse IP locale...

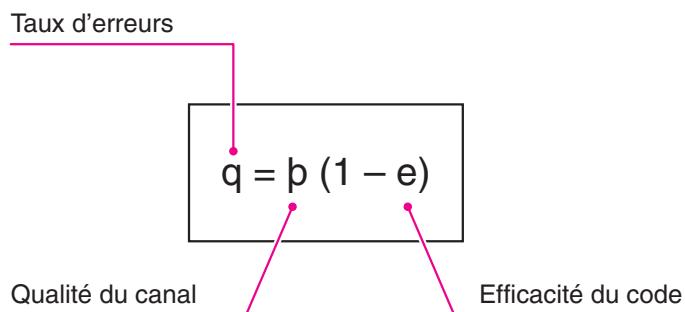


3 Gestion des erreurs

Taux d'erreurs

Les systèmes électroniques ne sont pas exempts d'erreurs liées à la qualité du support de transmission et au bruit environnant. Le système le plus simple de gestion des erreurs consiste à ajouter un bit de parité. Certains systèmes se contentent de détecter et de signaler une erreur tandis que d'autres assurent une correction.

Le **taux d'erreurs global** indique la proportion de messages faux. Il s'exprime à l'aide de l'égalité suivante :


$$q = p(1 - e)$$

Pour la gestion des erreurs, un système de codage optimal ne l'est jamais de manière permanente. Cela explique en partie le nombre impressionnant de systèmes de codage.

La simplicité de certaines gestions des erreurs, comme par exemple celle reposant sur la parité, provient le plus souvent de leur facilité d'intégration à moindre coût.

Lorsqu'une transmission est interrompue, il peut être possible dans certains cas de récupérer partiellement des informations. Ce n'est pas le cas par exemple avec certains fichiers PDF qui semblent privilégier l'intégralité du document à une représentation erronée.

C

Les réseaux et les serveurs

3.1 Codes simples

Parité

Le code à parité simple : il consiste à ajouter un bit supplémentaire permettant d'obtenir un nombre de bits pair.

Exemple de codage à parité paire :

Le bit de parité est à zéro de manière à obtenir un nombre total pair de bits à 1

Nombre pair de bits à 1
0 0 1 0 0 1 1 1 0 0
Nombre pair de bits à 1 Bit de parité

Parité

Le code à parités entrelacées : il repose sur le code à parité simple mais le principe est étendu dans le plan.

Exemple :

0	1	0	1	0	1	1	0	0
0	1	0	0	0	0	1	0	0
0	1	1	1	0	0	1	0	0
0	1	1	0	0	1	0	1	0
0	1	1	1	0	1	0	0	0
0	1	1	0	1	1	1	1	0
0	1	1	0	1	1	1	0	1
0	0	1	0	0	0	0	0	1
0	1	0	1	0	1	1	0	0

Bits de parité pour chaque ligne

Bits de parité pour chaque colonne

On peut citer aussi le code de **Van Duuren** qui procède à une répétition du caractère télégraphique lors d'une détection d'erreur.

3•2 Le code CRC

CRC

Le code CRC (*Cyclic Redundancy Code*) consiste à placer à intervalles réguliers une signature. La signature est générée à partir d'une opération sur les données.

À la réception, le CRC est recalculé avant d'être comparé avec la valeur de la signature reçue. En cas de différence, les données nécessitent une retransmission.

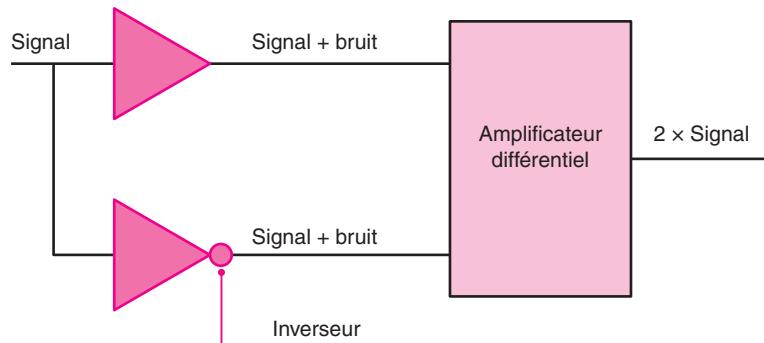
Parmi les opérations simples on peut envisager par exemple d'additionner un certain nombre de données ; le résultat sans retenue forme le CRC.

En pratique, le calcul par additions successives demeure assez simple à réaliser à partir d'un langage de programmation. Cette façon de faire présente toutefois l'inconvénient de consommer du temps de calcul.

Pour améliorer le processus, on fait plutôt appel à une division modulo 2 dont le reste constitue le CRC. En effet, la division modulo 2 se résume à l'utilisation d'un registre à décalage. Dans ce cas, l'électronique au niveau composant trouve pleinement son sens en remplaçant une solution logicielle pénalisante en termes de temps par un dispositif particulièrement bien adapté ; seulement quelques dizaines de portes logiques sont nécessaires dans un FPGA qui en compte quelques centaines de milliers.

3•3 Identification d'une erreur (trois états)

Pour améliorer la qualité d'une transmission, on peut faire appel au mode différentiel. Sur un fil, le signal utile est envoyé. Sur un second câble, l'information en opposition de phase est transmise. En bout de ligne, l'un des deux câbles est branché à un inverseur puis les deux signaux sont additionnés. On récupère ainsi l'information utile tandis que les parasites sont retranchés.



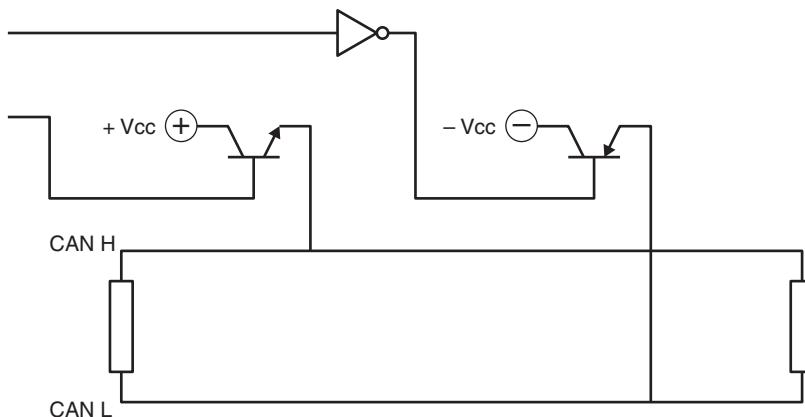
L'amplificateur différentiel effectue l'opération suivante :

$$(Signal + Bruit) - (-Signal + Bruit)$$

Bruit

Chaque élément est constitué de composants électroniques de base. Une fois de plus l'électronique vient au secours du traitement automatique de l'information, l'informatique ne constituant qu'un sous-ensemble de l'électronique.

Le Bus CAN représenté ci-dessous repose sur un système en opposition de phase (mode différentiel) et comporte un troisième état (état haute impédance) permettant d'indiquer ou d'identifier facilement l'absence de communication.



C

Les réseaux et les serveurs

4 CSMA/CD

Cette technique a comme origine la technique ALOHA implantée sur un réseau reliant les îles Hawaï. Elle est principalement utilisée sur les réseaux à diffusion.

4•1 Principe

La technique du CSMA

- Lorsqu'une station désire transmettre une information, elle l'envoie, sans se préoccuper des autres usagers.
- S'il y a collision, les trames sont perdues, puis retransmises ultérieurement.

4•2 Accès aléatoire avec écoute de la porteuse

La technique du CSMA (suite)

Cette technique est connue sous le nom de **CSMA** (*Carrier Sense Multiple Access*).

On écoute le canal avant d'entreprendre une émission.

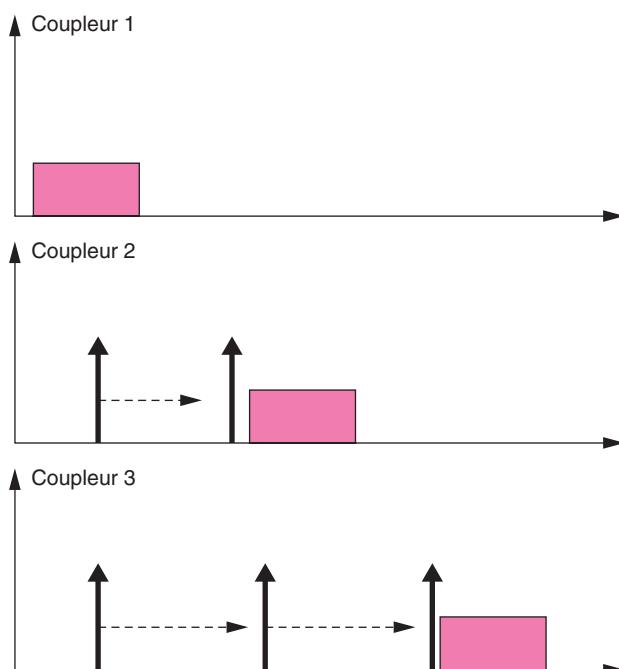
Le nombre de collisions est réduit mais pas totalement évité car si 2 stations écoutent et émettent en même temps il y a collision.

4•2•1 CSMA non persistant

On écoute le canal avant d'entreprendre une émission.

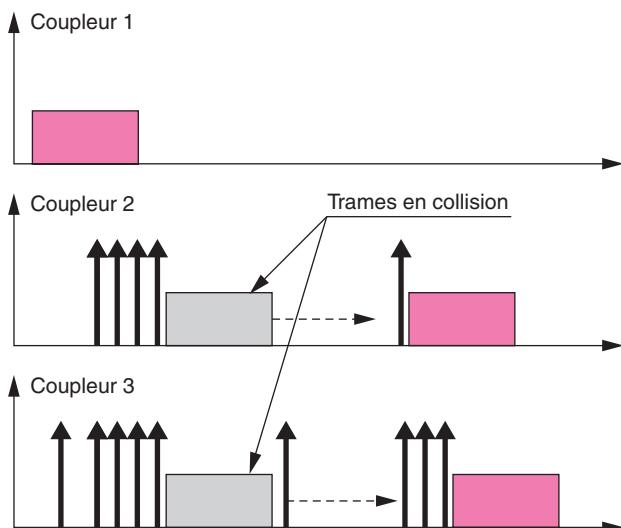
- Si le canal est libre, le communicateur émet.
- Si le canal est occupé on réécoute après un temps aléatoire.

La technique du CSMA (suite)



4•2•2 CSMA persistant

On écoute le canal avant d'entreprendre une émission.
 → Si le canal est libre, le communicateur émet.
 → Si le canal est occupé il continue à écouter jusqu'à ce que le canal soit libre et émet à ce moment-là.

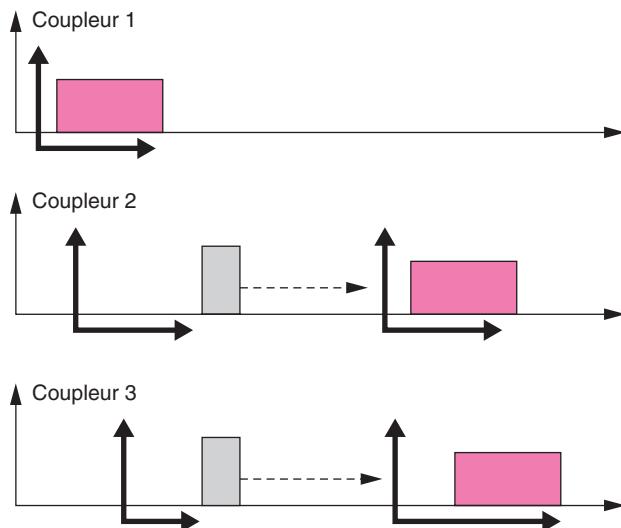
La technique du CSMA (suite)

Cette technique est plus rapide que la précédente, mais elle augmente la probabilité de collision.

**4•2•3 CSMA/CD (avec détection de collision)
(Carrier Sense Multiple Access / Collision Detect)**

Cette méthode à accès est utilisée par le réseau local ETHERNET.

- À l'écoute préalable du réseau s'ajoute l'écoute pendant la transmission.
- S'il se produit une collision, la station annule sa transmission et envoie des signaux spéciaux appelés « bits de bourrage » afin que toutes les stations soient prévenues de la collision.
- Il retentera son émission ultérieurement.

La technique du CSMA (suite)

Cette technique donne un gain d'efficacité par rapport aux précédentes puisqu'il y a détection immédiate des collisions.

Dans le cas du réseau Ethernet, quand on atteint 30 collisions, on abandonne.

5 L'ADSL

5•1 Présentation de l'ADSL

Généralités

L'*Asymmetric bit rate Digital Subscriber Line* signifie « débit numérique asymétrique sur ligne de client ».

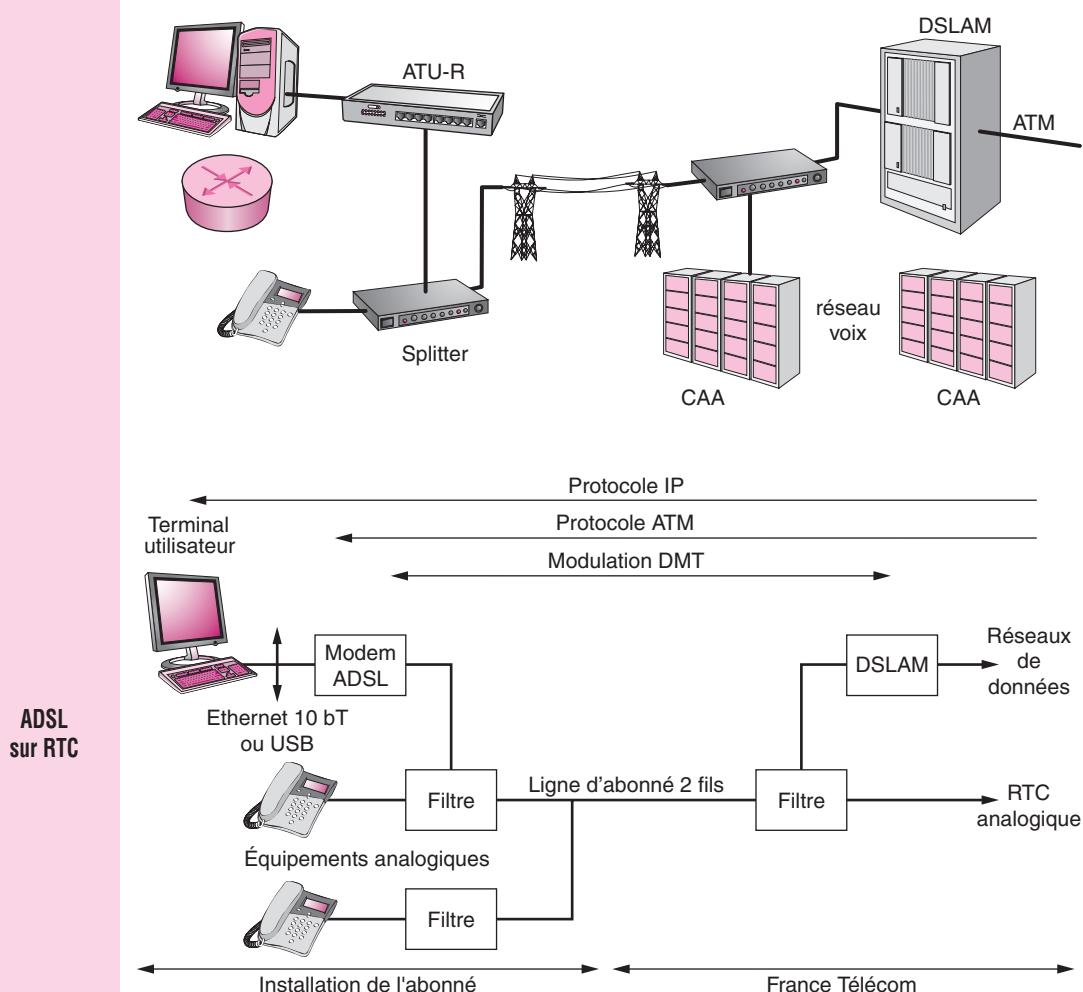
Cette technique de transmission appartient à la famille xDSL qui a pour fonction d'optimiser les débits sur les liaisons cuivre.

- Le HDSL (*High bit rate DSL*). Transmission bidirectionnelle et symétrique sur 2 paires pour les lignes à 2 Mbps.
- Le SDSL (*Single bit rate DSL*). Transmission bidirectionnelle et symétrique sur 1 paire pour les lignes à 2 Mbps mais pour des distances inférieures à l'HDSL.
- Le VDSL (*Very High Data rate DSL*). Transmission pouvant atteindre 52 Mbps en symétrique ou asymétrique ; cette technique est utilisée derrière des terminaisons de réseau optique.
- Le RADSL (*Rate Adaptative DSL*). C'est une variante de l'ADSL qui permet d'adapter le débit en fonction de la qualité de la ligne. En réalité, aujourd'hui la plupart des modems ADSL en sont déjà capables. Cependant, la différence essentielle réside dans la mise en œuvre d'une couche logicielle supplémentaire.

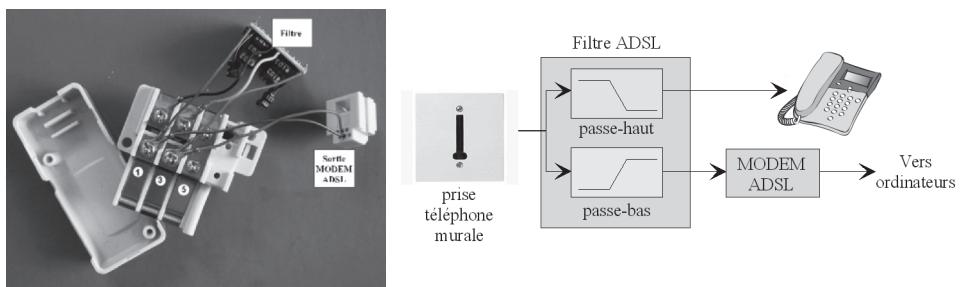
→ Le ADSL2+, la bande de fréquence étendue jusqu'à 2,2 MHz. Nouveau projet de recommandation G992, l'ADSL2+ s'enrichit d'autres facilités : choix du transport (STM / IP / ATM), possibilité d'une référence de temps, procédure d'initialisation rapide, adaptation de débit, Reed Solomon à 3 mots de code par symbole. Cette norme complète la G.992.3 (G.dmt.bis) par une extension de la bande utile à 2,208 MHz (512 porteurs) et de la bande montante 276 kHz (64 porteurs). Elle augmente aussi sa portée jusqu'à 5 km et son débit (350 à 800 kbit/s dans le sens montant et jusqu'à 12 ou 25 Mbit/s dans le débit descendant à 1,5 km du DSLAM). Le mode de repos est défini de façon à consommer moins d'énergie.

Technologies	Mode de transmission	Débit descendant	Débit montant	Distance maximale
HDSL	symétrique	1,544 Mbps 2,048 Mbps	1,544 Mbps 2,048 Mbps	3,6 km
SDSL	symétrique	768 kbps	768 kbps	3,6 km
ADSL	asymétrique	de 1,544 Mbps à 9 Mbps	de 16 kbps à 640 kbps	5,4 km
ADSL+	asymétrique	de 12 Mbps à 25 Mbps	de 350 kbps à 800 Mbps	5 km
RADSL	asymétrique	de 0,6 Mbps à 7 Mbps	de 128 kbps à 1 Mbps	5,4 km
VDSL	asymétrique	de 15 Mbps à 53 Mbps	de 1,544 Mbps à 2,3 Mbps	1,3 km

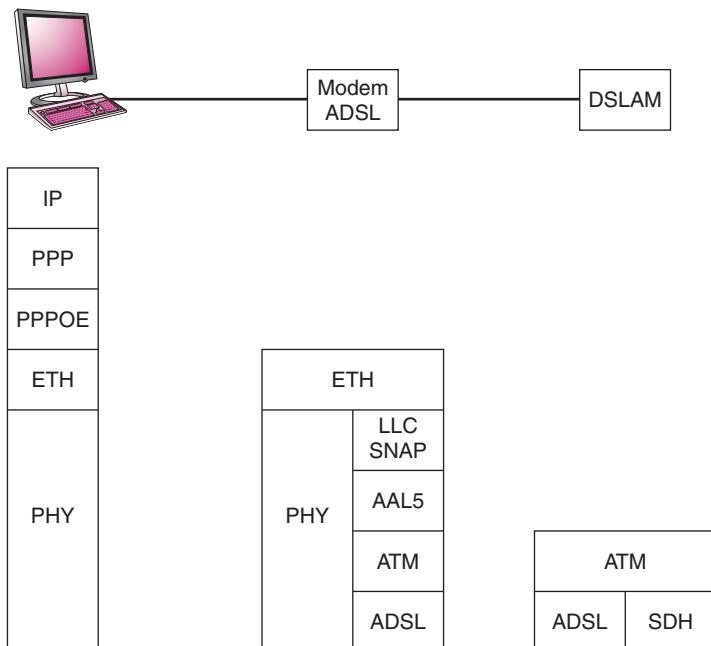
5•2 Connexion ADSL sur le réseau RTC



Les filtres permettent l'utilisation simultanée du téléphone analogique dans la bande de fréquence 0-4 kHz et les données sur IP dans la bande 20 kHz-1,1 MHz.
Pour chaque poste téléphonique de l'installation un filtre doit être ajouté.



Le modem va encapsuler / désencapsuler les données dans des cellules ATM puis utiliser le support ADSL pour le transport des données.



La technique du CSMA (suite)

Deux modems ADSL ne peuvent fonctionner sur une même ligne (côté abonné) car la synchronisation du signal serait impossible.

La jonction ou interface utilisée entre le terminal et le modem est du type Ethernet 10 bT ou USB. L'interface série asynchrone du PC est dans ce cas inutilisable car limitée en débit (115 kbps).

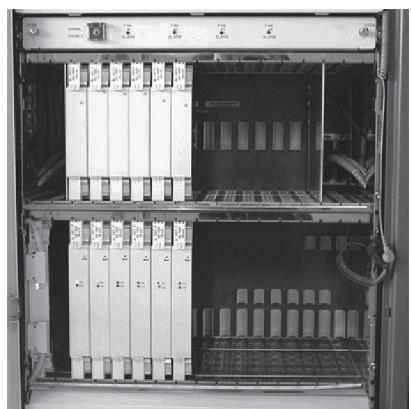
Les téléphones analogiques fonctionnent de façon permanente en mode commuté ; en revanche la liaison ADSL se comporte comme une ligne louée. Ceci implique que la facturation des services soit différente :

- Facturation à la durée pour le téléphone.
- Facturation mensuelle pour la ligne louée.

Le DSLAM (*DSL Access Multiplexer*), est un équipement situé à l'autre bout de la ligne téléphonique, reliant tous les modems ADSL reliés à ce central. Pour équiper ces répartiteurs, Orange a choisi les DSLAMs de marque Alcatel et ECI (un troisième constructeur de DSLAMs devrait apparaître en France, il s'agit de Lucent). Le type de DSLAM, ainsi que sa version sont un point très important car tous les modems ADSL ne sont malheureusement pas compatibles avec tous les DSLAMs.

Il est donc important, avant de choisir son modem, de bien vérifier si celui-ci est bien compatible avec votre DSLAM. Vous pourrez vérifier la plaque (zone composée d'un même type de DSLAM) de laquelle votre ville dépend, sur <http://www.ligne-adsl.fr>.

DSLAM Alcatel



La technique du CSMA (suite)

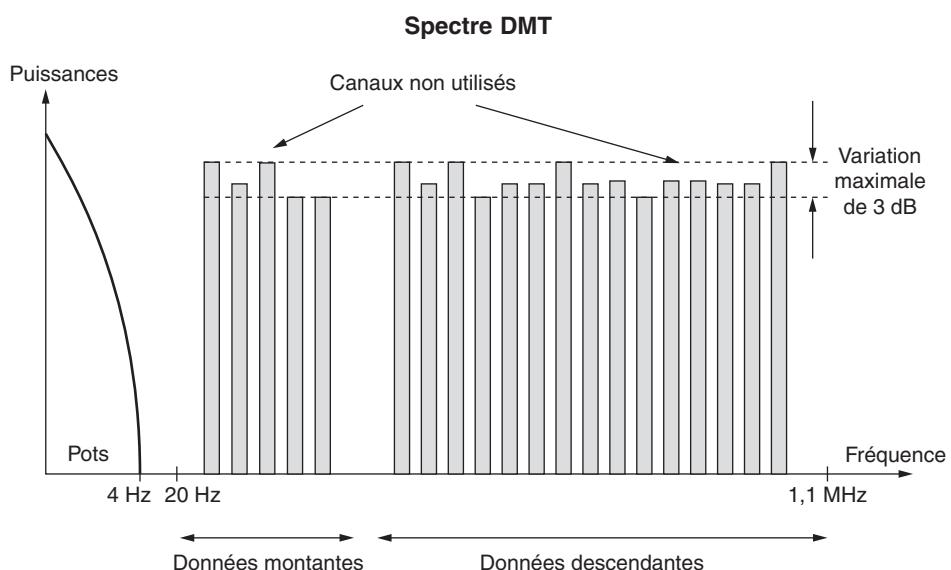
Aujourd'hui, de nombreuses mises à jour ont été effectuées sur les DSLAMs afin que les différents modems proposés soient interopérables sur tous les DSLAMs.

La modulation DMT (*Discrete Multi Tone*) est du type multiporteuse.

La technique consiste à partager la bande passante disponible en un nombre élevé de canaux. Ces canaux reçoivent une modulation de type QAM et sont transmis en parallèle. Cette technique multiporteuse, nécessite de forts traitements numériques et n'a donc vu le jour qu'à partir du moment où les DSP sont devenus à des coûts abordables.

La normalisation ANSI T1.413 spécifie l'utilisation de 256 porteuses pour le canal de réception, chacun des sous-canaux ayant une bande passante de 4 kHz. Chacune des porteuses peut être modulée, ce qui permet un débit de 60 kbps pour chacun de ces canaux de transmission.

En émission, la norme spécifie l'utilisation de 20 porteuses.



- Les signaux compris entre 300 et 4 kHz sont destinés à la communication téléphonique sur réseau commuté (RTC).
- Les signaux compris entre 20 kHz et 1,1 MHz sont destinés à la transmission de données (ADSL) sur ligne louée.
- Ces signaux sont séparés par un « splitter », filtre placé sur chaque prise téléphonique afin de séparer les deux services.
- Entre 20 kHz et 200 kHz, on trouve les canaux qui serviront à l'émission des données.
- Entre 200 kHz et 1,1 MHz, nous avons les canaux réservés à la réception des données.
- Une liaison DSL sur une ligne RNIS est impossible pour des raisons de bande passante. La bande passante du RNIS empiète sur celle du DSL.

6 Protocole PPP D'après la RFC 166

6•1 Introduction

Généralités

Le protocole Point-à-Point est utilisé pour des liaisons simples transportant des paquets de données entre deux éléments. Ces liens permettent une communication simultanée bidirectionnelle (*full-duplex*), et sont supposés transmettre des paquets dans l'ordre. PPP propose une solution commune pour un raccordement aisément d'une grande variété d'hôtes, de ponts et de routeurs.

L'encapsulation PPP permet le multiplexage de différentes connexions protocolaires au niveau réseau simultanées sur la même liaison physique. Cette encapsulation a été conçue dans l'exigence d'une excellente compatibilité avec la plus grande variété de matériels.

6•1•1 Protocole de contrôle de liaison (*Link Control Protocol*)

Généralités (suite)

Afin d'être suffisamment souple pour pouvoir être porté dans de nombreux environnements, le protocole PPP dispose d'un protocole de contrôle de liaison (*Link Control Protocol* – LCP). Le LCP est utilisé pour effectuer la négociation automatique des options de format d'encapsulation, la gestion de tailles variables de paquets, la détection d'un rebouclage de liaison ainsi que d'autres erreurs courantes de configuration, ainsi que pour gérer la rupture de liaison. Les autres fonctionnalités apportées concernent l'authentification de l'identité de l'hôte dans lequel il est implémenté, ainsi que la détection de fautes de fonctionnement sur la liaison.

6•1•2 Protocole de gestion réseau (*Network Control Protocol*)

Généralités (suite)

Les liaisons Point-à-Point tendent à mettre en exergue de nombreux problèmes vis-à-vis de protocoles réseaux communs. Par exemple, l'assignation et la gestion des adresses IP, pouvant poser des problèmes y compris dans l'environnement limité d'un LAN, est particulièrement délicate lorsque la liaison passe par un réseau de type circuit communiqué (par exemple une connexion modem via réseau téléphonique). Ces problèmes sont gérés par une famille de protocoles de gestion réseau (*Network Control Protocols* – NCPs), chacun traitant des aspects particuliers à la gestion de tel ou tel type de protocole de niveau réseau.

6•2 Encapsulation PPP

Encapsulation

L'encapsulation PPP est utilisée pour lever l'ambiguïté sur des datagrammes provenant de protocoles différents. Cette encapsulation nécessite l'usage d'un tramage dont le but principal est d'indiquer le début et la fin de l'encapsulation.

Protocole 8 ou 16 bits	Information	Bourrage
------------------------	-------------	----------

6•2•1 Champ protocole

Encapsulation (suite)

Le Protocole comprend un ou deux octets, et sa valeur identifie le datagramme encapsulé dans le champ Information du paquet. Ce champ est transmis et reçu, l'octet le plus significatif en tête.

La structure de ce champ est conforme aux mécanismes définis par l'ISO 3309 pour l'extension des champs d'adresse. Tous les Protocoles DOIVENT être impairs ; le bit le moins significatif de l'octet le moins significatif DOIT être égal à « 1 ». De plus, tous les Protocoles DOIVENT être codés de sorte que le bit le moins significatif de l'octet le plus significatif soit égal à « 0 ». Les trames reçues qui ne se conforment pas à ces règles DOIVENT être considérées comme transportant un Protocole non identifié.

Les valeurs du champ Protocole comprises dans la plage « 0*** » à « 3*** » identifient un protocole de niveau réseau de paquets spécifiques, et des valeurs entre « 8*** » et « b*** » identifient des paquets appartenant aux Network Control Protocols (NCPs) associés, le cas échéant.

Des valeurs de champ de protocole comprises entre « 4*** » et « 7*** » sont utilisées pour des protocoles de faible trafic et ne disposant pas de NCP associé. Les valeurs entre « c*** » et « f*** » identifient des paquets appartenant aux Link Control Protocols (comme LCP).

Les valeurs les plus récentes établies pour ce champ Protocole sont listées dans le document « Assigned Numbers » [2]. La spécification suivante réserve les valeurs :

Valeur (en hexa)	Nom de protocole
0001	Protocole de bourrage
0003 à 001f	réservé (non transparents)
007d	réservé (Control Escape)
00cf	réservé (PPP NLPIID)
00ff	réservé (non comprimables 1000)
8001 à 801f	non utilisé
807d	non utilisé
80cf	non utilisé
80ff	non utilisé
c021	Link Control Protocol
c023	Password Authentication Protocol
c025	Link Quality Report
c223	Challenge Handshake Authentication Protocol

Les développeurs de nouveaux protocoles DOIVENT obtenir un numéro de protocole de l'Internet Assigned Numbers Authority (IANA), à IANA@isi.edu.

6•2•2 Champ information

Le champ Information contient zéro octet au minimum. Il contient le datagramme du protocole spécifié dans le champ Protocole.

La longueur maximum du champ Information, y compris le bourrage, mais hors champ Protocole, est limité à l'Unité de Réception Maximale (URM), par défaut 1500 octets. Par négociation, des implémentations de PPP plus « libérales » pourront utiliser d'autres valeurs d'URM.

BOURRAGE

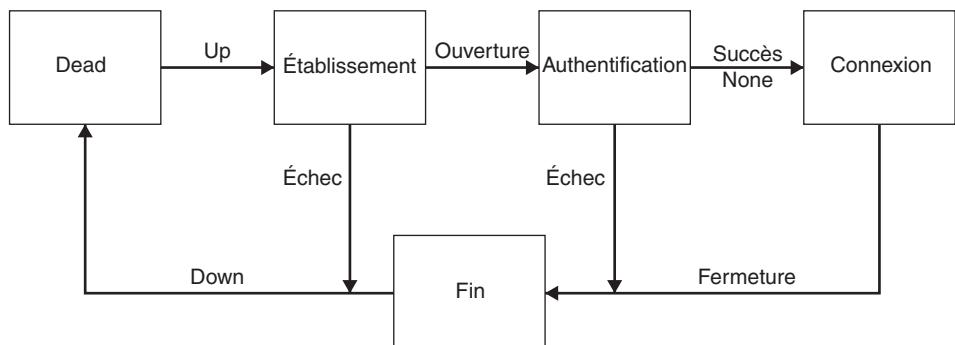
En transmission, le champ Information PEUT être complété d'un nombre arbitraire d'octets de « bourrage » dans la limite de la règle de l'URM. C'est à chaque protocole que revient le travail de dissocier les octets de bourrage de l'information utile.

Encapsulation
(suite)Encapsulation
(suite)

6•3 Fonctionnement d'une liaison PPP

Principe de fonctionnement

Dans les processus de configuration, de maintien et de clôture de liaison point-à-point, le lien PPP rencontre un certain nombre d'états décrits de façon sommaire par le schéma suivant :



6•3•1 « Link Dead » (couche physique non prête)

Principe de fonctionnement (suite)

Une communication débute et se termine nécessairement dans cet état. Lorsqu'un événement extérieur (comme une détection de porteuse ou la configuration par l'administrateur réseau) indique que le niveau physique est en état pour un processus de connexion, PPP passera la liaison en phase d'établissement.

Durant cette phase, l'automate LCP (décris plus loin) sera dans l'état Initial ou Démarrage. Le passage à l'état Établissement sera signalé par un événement Up à l'automate LCP.

NOTES D'IMPLÉMENTATION

Typiquement, une liaison doit retomber dans cet état après toute déconnexion du modem. Dans le cas d'une liaison filaire permanente, cet état pourra n'être maintenu que pendant une très courte durée – cependant suffisamment longue pour pouvoir simuler un état de repos effectif.

6•3•2 Établissement

Principe de fonctionnement (suite)

Le protocole de liaison *Link Control Protocol* (LCP) est utilisé pour établir la connexion grâce à l'échange de paquets de Configuration. Cet échange est totalement résolu, et l'automate LCP entre dans l'état Ouvert, lorsque des paquets d'acquittement *Configuration-Acquittée* (décris plus loin) ont été reçus des deux côtés.

Toutes les options de Configuration sont supposées être à leur valeur par défaut avant d'être modifiées par l'échange de configuration. Voir le chapitre sur les options de configuration LCP pour plus de détails.

Il est important de noter que seules les options de configuration indépendantes de tout protocole réseau sont configurées par LCP. La configuration de chacun des protocoles réseau est réalisée via des protocoles *Network Control Protocols* (NCPs) spécifiques durant la phase de configuration réseau. Tout paquet non-LCP reçu pendant cette phase DOIT être ignoré.

La réception d'une requête pour configuration LCP provoque un retour à l'état d'établissement de liaison à partir de l'état de configuration réseau ou de la phase d'authentification.

6•3•3 Authentification

Principe de fonctionnement (suite)

Sur certaines liaisons il peut être pertinent d'imposer une authentification du correspondant avant de permettre toute négociation protocolaire au niveau réseau.

Par défaut, l'authentification n'est pas demandée. Lorsqu'une implémentation impose que le correspondant s'authentifie à l'aide d'un protocole d'authentification particulier, alors il DOIT explicitement demander l'usage de ce protocole d'authentification pendant la phase d'établissement de la liaison.

L'authentification DEVRAIT être faite le plus tôt possible après la conclusion de la phase d'établissement. La détermination de la qualité de la liaison POURRA être réalisée dans le même temps. Toutefois, une implémentation correcte NE DOIT PAS permettre un échange de paquets de mesure de la qualité de liaison, dans le but de retarder indéfiniment le processus d'authentification.

Le passage de la phase d'authentification à la phase de négociation de protocole réseau NE DOIT PAS être accepté avant que l'authentification n'ait abouti avec succès. Si l'authentification échoue, l'authémificateur DEVRAIT plutôt entamer une phase de fermeture de liaison.

Les paquets LCP, d'authentification, et de mesure de qualité de liaison sont les seuls autorisés pendant cette phase. Toute autre forme de paquet DOIT être ignorée.

NOTES D'IMPLÉMENTATION

Une implémentation NE DOIT PAS faire échouer un processus d'authentification sur une simple temporisation ou une absence de réponse. L'authentification DEVRAIT permettre un certain nombre de tentatives, et ne conclure à un échec que lorsque le nombre de tentatives maximum est « consommé ».

C'est dans tous les cas l'implémentation qui a refusé d'authentifier son correspondant qui doit entamer la phase de fermeture de liaison.

6•3•4 Phase de négociation réseau

Principe de fonctionnement (suite)

Une fois que PPP a achevé les procédures précédentes, chaque protocole réseau (tels qu'IP, IPX, ou AppleTalk) DOIT être configuré séparément via un protocole *Network Control Protocol* (NCP). Chaque NCP DEVRAIT pouvoir être Ouvert et Fermé à tout moment.

NOTES D'IMPLÉMENTATION

Comme il se peut que certaines implémentations demandent un temps non négligeable pour mesurer la qualité de liaison, les modules PPP DEVRAIENT éviter l'utilisation de temporisations à durée fixe entre la fin de l'authentification et le début d'une négociation NCP.

Lorsqu'un NCP atteint l'état Ouvert, la liaison PPP est alors prête à véhiculer les paquets du protocole réseau associé. Tout paquet dans un protocole géré par NCPs arrivant alors que le NCP associé (ou associable) est en état fermé doit être ignoré.

Lorsque le LCP est dans son état ouvert, tout paquet protocolaire non supporté par l'implémentation DOIT être retourné à l'émetteur dans un paquet Protocole-Rejeté (décrit plus loin). Seuls les protocoles gérés (mais de NCP fermés) sont ignorés.

Dans cet état, le trafic sur le lien est composé de toute combinaison de paquets LCP, NCP, et datagrammes réseau.

6•3•5 Fermeture de liaison**Principe de fonctionnement (suite)**

PPP peut fermer la liaison à tout moment. Ceci peut survenir suite à une perte de portée, l'échec d'une authentification, la détection d'une qualité de liaison insuffisante, la chute d'une temporisation d'attente, ou la fermeture de la liaison du fait d'une décision humaine.

Le protocole LCP est utilisé pour procéder à la clôture de la liaison par l'échange de paquets de clôture. Lors de la fermeture, PPP en informe tout d'abord les couches réseau afin que ces dernières puissent prendre leurs dispositions.

Après l'échange des paquets de Clôture, l'implémentation DEVRAIT signaler à la couche physique de procéder à la déconnexion physique, particulièrement utile dans le cas de l'échec d'une authentification. L'émetteur d'une Requête pour Clôture DEVRAIT se déconnecter juste après avoir reçu un acquittement de Clôture, ou au plus tard après que la temporisation de Reprise soit écoulée. Le récepteur d'une Requête pour Clôture DEVRAIT attendre la déconnexion du correspondant, et NE DOIT PAS se déconnecter pendant au moins la durée d'une temporisation de Reprise comptée à partir de l'émission de l'acquittement de Clôture. PPP DEVRAIT passer en état « *Link Dead* ».

Tout paquet autre que LCP reçu durant cette phase DOIT être ignoré.

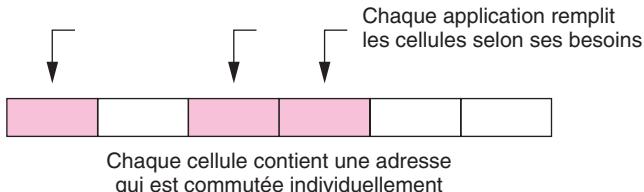
NOTES D'IMPLÉMENTATION

La fermeture d'une liaison par LCP est suffisante. Les différents NCP actifs n'ont pas l'obligation d'envoyer chacun leur salve de paquets de clôture. Inversement, la rupture d'une communication réseau par un NCP n'est pas une raison suffisante pour la coupure de la liaison PPP, même s'il s'agit du dernier NCP actif sur la liaison.

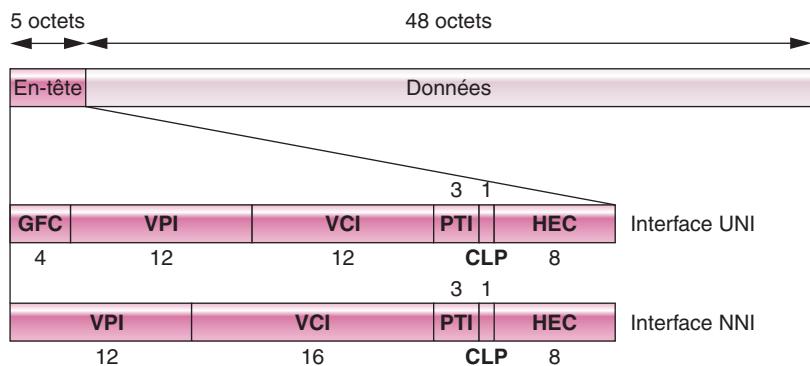
7 Les bases de l'ATM

7•1 Généralités

La vocation de l'ATM (*Asynchronous Transfer Mode*) est de transporter tout type de service grâce à la longueur fixe de sa cellule (53 octets) et le multiplexage dynamique de celle-ci.



La cellule ATM comprend un en-tête de 5 octets et un champ de données de 48 octets. Ce format est fixe.



Généralités

Significations des champs

→ **GFC (Generic Flow Control)**

Champ de 4 bits permettant d'affecter une priorité à une cellule. Ce champ peut également être utilisé pour distinguer plusieurs stations qui partagent une même interface ATM.

→ **VPI (Virtual Patch Identifier)**

Permet de créer 256 chemins virtuels au sein des commutateurs ATM.

→ **VCI (Virtual Chanel Identifier)**

Permet d'identifier de manière unique toutes les voies virtuelles au sein d'un chemin virtuel (216 possibilités soit 16 536).

→ **PTI (Payload Type Indicator)**

Le premier bit indique si la cellule transporte des données de contrôle ou des données utilisateurs. Pour les données utilisateurs le deuxième bit appelé EFCI (*Explicit Forward Congestion Indication*), indique à l'application qu'il faut prévoir des délais d'acheminement pour les cellules à venir (suite à une congestion par exemple). Positionné à 1, le troisième bit indique que le champ d'information contient des données utilisées par les applications de l'administration OAM (*Operation Administration And Maintenance*).

→ **CLP (Cell Loss Priority)**

Ce bit indique que la cellule peut être ignorée par le commutateur si cela s'avère nécessaire (en cas de congestion par exemple).

→ **HEC (Header Error Control)**

Cet octet permet à la couche TC (*Transmission Convergence*) d'opérer un contrôle d'erreur sur l'en-tête de la cellule.

L'en-tête de l'interface NNI ne comprend pas de champ GFC et fait passer ce champ à 16 bits.

C

Les réseaux et les serveurs

8 La trame HDLC

8•1 Généralités

HDLC, ADCCP et SDLC

Depuis quelques années sont apparus des protocoles de liaison nouveaux, plus performants que leurs prédecesseurs en « mode de base », et permettant des échanges duplex de séquences de bits.

Parmi ces protocoles, les principaux sont les suivants :

- HDLC (*High-level Data Link Control*) normalisé par l'ISO (*International Standards Organization*).
- ADCCP (*Advanced Data Communications Control Procedure*) normalisé par l'ANSI (*American National Standards Institute*).
- SDLC (*Synchronous Data Link Control*) défini par IBM.

Ces protocoles sont très voisins. HDLC (ainsi que ADCCP) prévoit plusieurs classes de procédure, ainsi qu'un vaste répertoire de commandes et de réponses. SDLC est un sous-ensemble de HDLC, et offre par ailleurs des possibilités complémentaires, telles que le support des liaisons configurées en boucles.

La description qui suit concerne plus précisément HDLC. La documentation de référence comporte plusieurs parties :

- Structure de trame ISO 3309
- Éléments de procédure ISO 4335
- Classes de procédure ISO 7809.

8•2 Caractéristiques essentielles

Protocoles Famille HDLC

Les points suivants sont à rapprocher de ceux relatifs aux limitations des protocoles en mode de base.

1. Les protocoles de la famille HDLC permettent une exploitation duplex de la liaison de données.
2. Les messages, appelés trames, peuvent contenir à la fois des données et des informations de service, telles que des accusés de réception.
3. Plusieurs trames peuvent être émises en séquence, sans qu'un accusé de réception soit renvoyé pour chacune d'elles.
4. Toutes les trames, même sans données, sont protégées des erreurs de transmission par un FCS (*Frame Check Sequence*).
5. Toutes les trames ont un format unique, avec un seul type de délimiteur de début et de fin appelé fanion.
6. Les protocoles de la famille HDLC assurent la transmission de suites d'éléments binaires, et non de caractères. Le transfert de l'information s'effectue sans aucune interprétation de son contenu, ce qui assure une transparence totale par rapport aux codes éventuellement utilisés.

8•3 Types de liaisons

Liaison non-équilibrée

Une liaison non-équilibrée, point-à-point ou multipoint, comporte une station primaire qui gère la liaison et assure l'échange de données entre elles et une ou plusieurs stations secondaires (fig. 1). Les trames qu'émettent la station primaire sont des commandes, celles qu'elle reçoit sont des réponses.

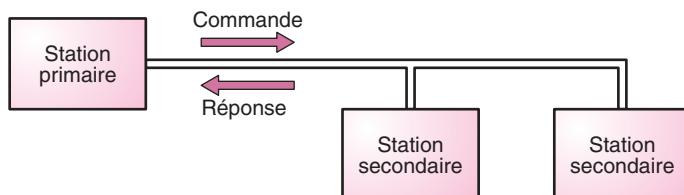


Fig. 1
Liaison non-équilibrée

Le jeu des commandes de la station primaire est plus riche que le jeu des réponses des stations secondaires. La station primaire est en effet responsable de l'activation et la désactivation de la liaison, et aussi des reprises en cas d'anomalies.

Liaison équilibrée

Une liaison équilibrée est du type point-à-point, et comporte deux stations mixtes. Celles-ci ont des responsabilités égales et peuvent toutes les deux émettre des commandes et des réponses (voir figure 2). Une station mixte assure donc les fonctions d'une station primaire et d'une station secondaire.

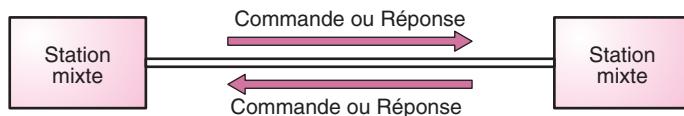


Fig. 2
Liaison équilibrée

8•4 Modes de fonctionnement des stations

Mode de réponse normal

Dans ce mode, (*NRM-Normal Response Mode*) qui ne s'applique qu'aux liaisons non-équilibrées, une station secondaire ne peut émettre que si elle a été invitée par la station primaire. Elle doit aussi indiquer la fin de sa transmission afin de rendre le contrôle à la station primaire.

Une station secondaire est mise dans ce mode opérationnel par la commande SNRM (*Set Normal Response Mode*) ou SNRME (*Set Normal Response Mode Extended*).

Elle peut aussi être déconnectée logiquement de la liaison en étant mise en mode NDM (*Normal Disconnected Mode*) par la commande DISC (*Disconnect*). Enfin, elle peut être mise en mode d'initialisation (IM) par la commande SIM (*Set Initialisation Mode*).

Mode de réponse asynchrone

Sur une liaison non-équilibrée, une station secondaire en mode ARM (*Asynchronous Response Mode*) peut émettre à son gré, sans avoir à être sollicitée par la station primaire. Ce mode s'applique quasi exclusivement à des configurations point-à-point, bien que HDLC n'en interdise pas l'usage sur une liaison multipoint. Une station secondaire est mise dans ce mode opérationnel par la commande SARM (*Set Asynchronous Response Mode*) ou SARME.

Sur une liaison équilibrée, les stations mixtes fonctionnent en mode asynchrone équilibré (ABM – *Asynchronous Balanced Mode*). Chacune des stations peut émettre la commande SABM (*Set Asynchronous Balanced Mode*) ou SABME.

Dans les deux cas, les stations peuvent être mises en mode ADM (*Asynchronous Disconnected Mode*) par la commande DISC, ainsi que, sur option, en mode d'initialisation par la commande SIM.

HDLC définit donc trois classes de procédure :

- la classe UNC (*Unbalanced Normal Class*),
- la classe UAC (*Unbalanced Asynchronous Class*),
- la classe BAC (*Balanced Asynchronous Class*).

9 Wi-Fi

9•1 Présentation

Norme
802.11

Basé sur la norme 802.11 un réseau WI-FI (*Wireless Fidelity*) permet de créer des réseaux locaux sans fils à haut débit.

Le logo WIFI est le suivant :



9•2 La norme

Norme
802.11
(suite)

La norme 802.11 a subi plusieurs révisions suivant les débits et des détails de sécurité.

Le tableau ci-dessous récapitule les quatre différentes principales révisions :

Norme	Nom	Débits (Mbps)	Bande de fréquence (GHz)	Nombre de canaux	Portée (m)
802.11a	Wifi5	54	5	8	30
802.11b	Wifi	11 (6 réels)	2,4	3	100
802.11g		54 (30 réels)	2,4		100
802.11n		200 (max 540)	2,4 ou 5		125

Il est à noter que les équipements 802.11a ne sont pas compatibles avec ceux équipés 802.11b.

Note : la norme 802.11e ajoute les mécanismes QoS dans les réseaux 802.11.

9•3 Méthode d'accès CSMA

Principe
de
fonctionnement

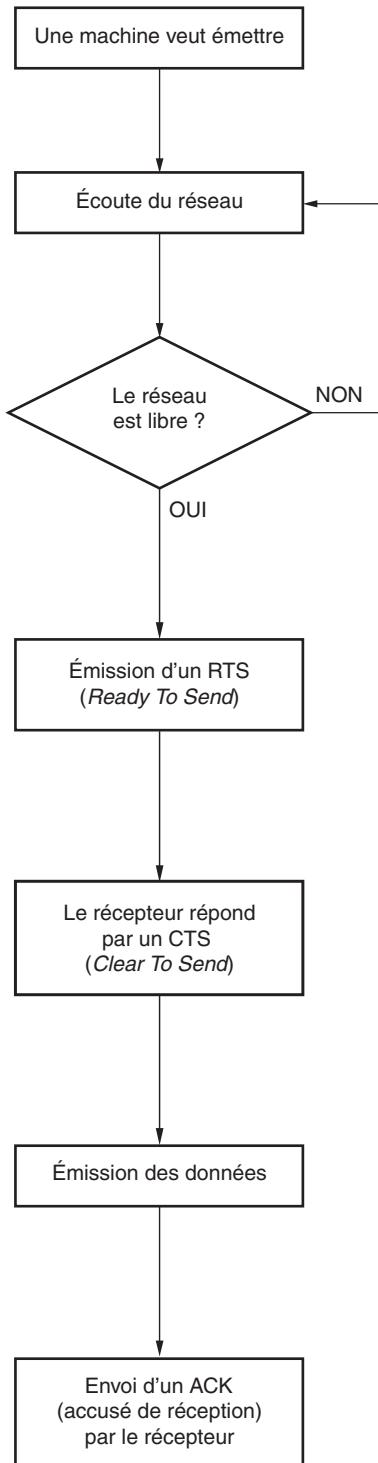
Dans un réseau sans fil la détection de collision n'est pas possible en raison des rayons de portée.

Le CSMA utilise donc un système d'accusé de réception.

La différence avec le réseau Ethernet réside en ce que la couche MAC du 802.11 possède un mécanisme de contrôle d'erreur (le contrôle d'erreur étant géré par TCP pour un réseau Ethernet).

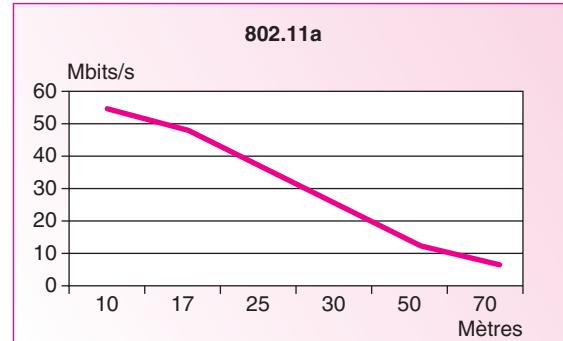
Principe de fonctionnement (suite)

Principe d'émission d'une station sur le réseau

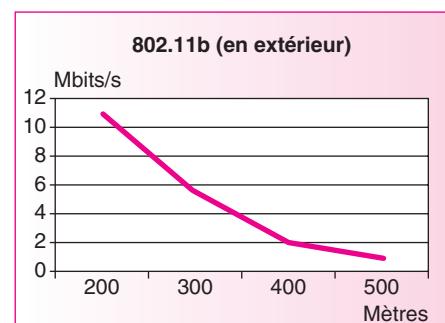
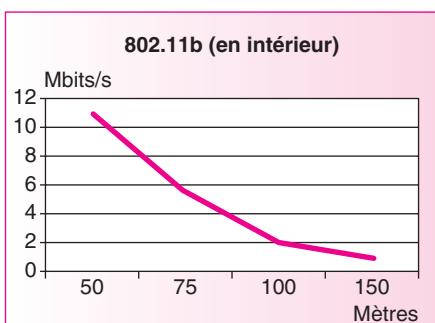


9•4 Portées et débits

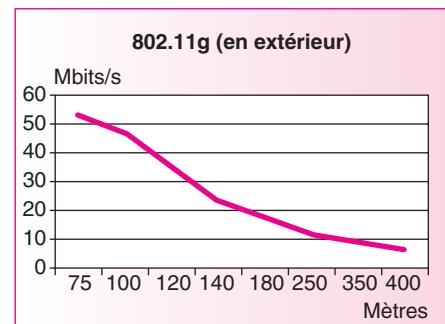
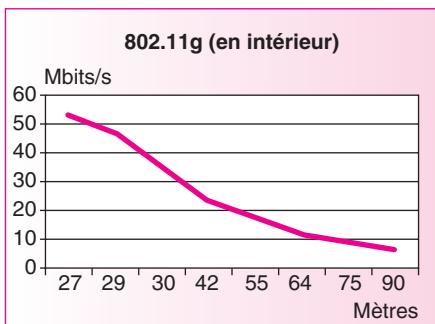
Performances



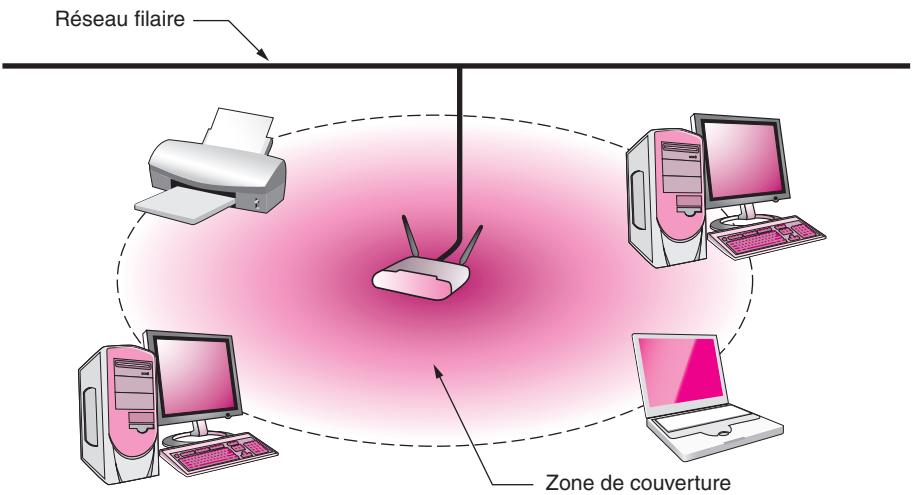
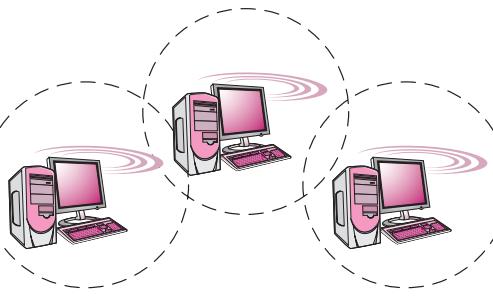
802.11b



802.11g



9•5 Les modes de fonctionnement

Modes de fonctionnement	<p>Il existe 2 modes de fonctionnement pour les réseaux WI-FI :</p> <ul style="list-style-type: none"> → le mode infrastructure, → le mode ad hoc.
Principe de fonctionnement (suite)	<p>9•5•1 Le mode infrastructure</p> <p>Les ordinateurs ou périphériques voulant rejoindre le réseau doivent se connecter à un point d'accès.</p> <p>Ce point d'accès couvre une certaine zone que l'on nomme zone de couverture.</p>  <p>L'ensemble point d'accès+ordinateurs (ou périphériques) connectés forment un ensemble de services de base (BSS Basic Service Set).</p> <p>Chaque ensemble de services de base est identifié grâce à 6 octets. Cet identifiant est noté BSSID et dans le mode infrastructure il correspond à l'adresse mac du point d'accès.</p> <p>Dans ce mode de fonctionnement le point d'accès et les ordinateurs (ou périphériques) doivent être configurés pour avoir le même nom de réseau. Ce nom est le SSID (Service Set Identifier).</p>
Principe de fonctionnement (suite)	<p>9•5•2 Le mode ad hoc</p> <p>Dans ce mode de fonctionnement les ordinateurs se connectent directement entre eux, il n'existe pas de point d'accès.</p> <p>Il suffit de configurer les machines en mode ad hoc, de sélectionner un canal et le nom de réseau (SSID).</p> <p>On peut dans ce cas créer un réseau "maille" dont la dimension ne dépend que de l'existence d'une machine voisine. Il faut pour cela implanter un logiciel de routage, chaque machine jouera le rôle de routeur.</p> 

9•6 La sécurité

Sécurité Il faut en premier modifier tous les paramètres par défaut.

9•6•1 Sécurité d'accès au réseau

Sécurité (suite) Il est possible de limiter l'accès au réseau en activant le filtrage par adresses mac sur la borne d'accès. Seuls les ordinateurs dont l'adresse mac aura été enregistrée par l'administrateur pourront accéder au réseau.

Cette protection ne rend pas les données confidentielles ; il faut, pour cela, appliquer d'autres techniques.

9•6•2 Le WEP

Sécurité (suite) Le WEP (*Wired Equivalent Privacy*) est un mécanisme de chiffrement des données. Les clés sont 40 ou 128 bits et doivent être enregistrées sur le point d'accès et sur les clients.

Plus le nombre de bits utilisés pour la clé est faible, plus la protection est vulnérable. Il vaut donc mieux utiliser une clé de 128 bits.

9•6•3 Le WAP

Sécurité (suite) Le WAP nécessite un serveur d'authentification et utilise un algorithme de cryptage, TKIP, qui est capable de modifier la clé de chiffrement plusieurs fois par seconde.

Le WAP ne permet de sécuriser que les réseaux en mode infrastructure.

Pour pouvoir sécuriser un réseau en mode ad hoc (et infrastructure) il faut utiliser le **WAP2**.

10 Bluetooth

10•1 Présentation

Normes

C'est une technologie de communication sans fils (WPAN : *Wireless Personnal Aera Network*).

Contrairement aux systèmes infrarouges les matériels n'ont pas besoin d'être en vue directe pour communiquer.

La portée étant relativement faible on parlera dans ce cas de picoréseaux.

Le logo Bluetooth est le suivant :



10•2 Normes Bluetooth

Norme 802.15

Norme

802.15.1 Bluetooth v1.x, débit : 1 Mbit/s

802.15.2 Utilisation de la bande de fréquence 2,4 GHz (en cours de validation)

802.15.3 Haut débit (20 Mb/s) (en cours de développement)

802.15.4 Bas débit (en cours de développement)

10•3 Portée et puissance

Performances

Il existe trois classes d'émetteur :

	Classe	Puissance	Portée
	I	100 mW	100 m
	II	2,5 mW	15/20 m
	III	1 mW	10 m

Les faibles puissances mises en jeu expliquent que l'on préfère la technologie Bluetooth au WI-FI pour les appareils autonomes.

10•4 Principe de fonctionnement

Principe

Bluettooth utilise la technique FHSS (*Frequency Hope Spread Spectrum*) qui découpe la bande de fréquences en 79 canaux de 1 MHz.

Afin d'éviter des interférences avec d'autres appareils radio, un changement de canal est régulièrement effectué (jusqu'à 1 600 fois par seconde).

RÉSEAU MAÎTRE/ESCLAVE

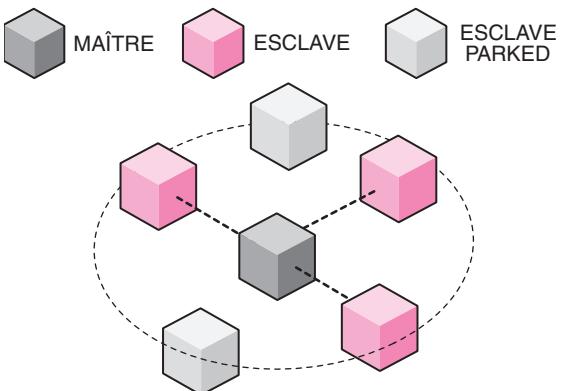
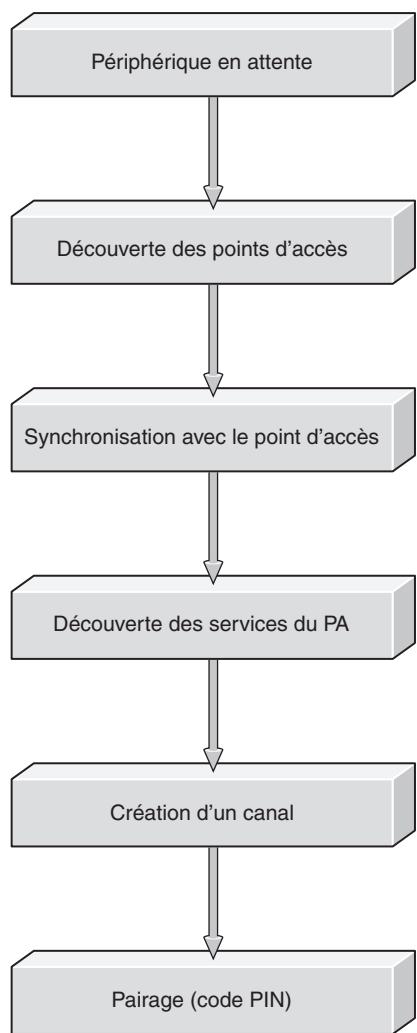
Bluethooth est un réseau « maître/esclave ».

Principes (suite)

Le maître permet aux périphériques esclaves de se connecter (7 au maximum, 255 en mode parked).

En mode parked les périphériques sont connectés mais ne possèdent pas d'adresse réseau.

L'ensemble maître/esclave(s) forme un picoréseau (10 au maximum dans une zone de couverture).

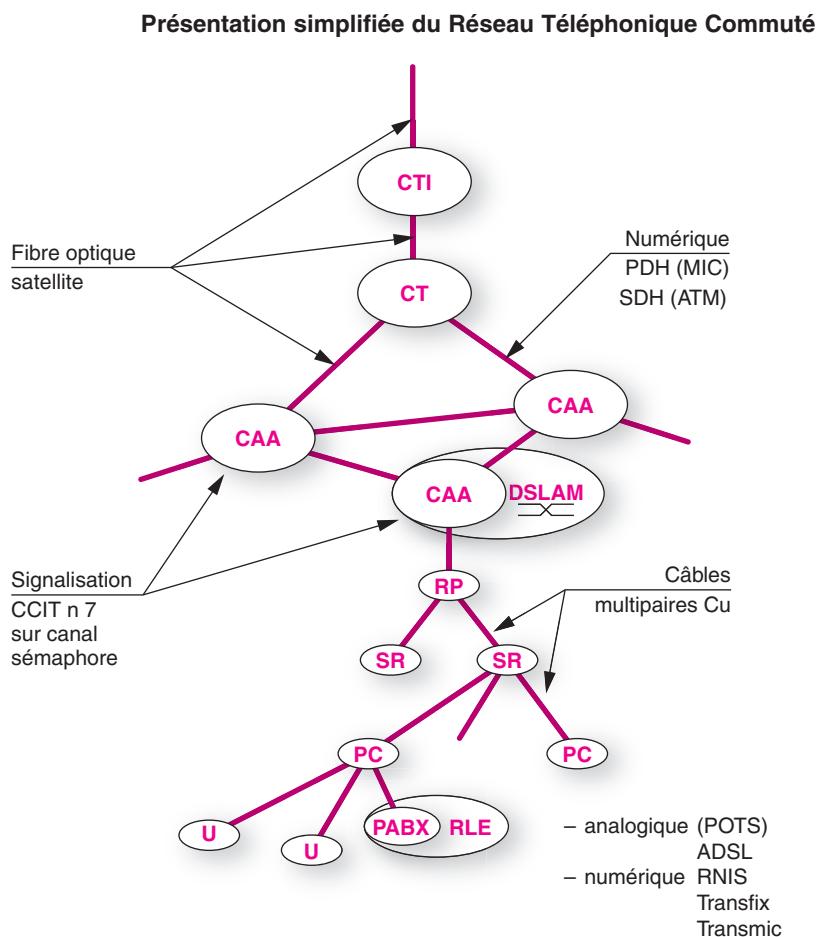
**10•5 Établissement d'une connexion****Principes (suite)**

11.1 Présentation

Normes

C

Les réseaux et les serveurs



CTI Centre de Transit International

CT Centre de Transit

CAA Centre à Autonomie d'Acheminement

RP Répartiteur Général

SR Sous-Répartiteur

PC Point de Connexion

U Utilisateur final

PABX Autocommutateur privé

DSLAM Multiplexeur de liaison ADSL

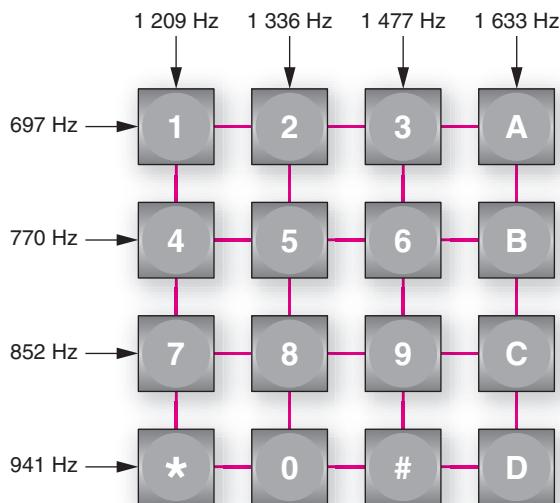
RLE Réseau local d'entreprise

11•2 La numérotation sur le réseau RTC

11•2•1 La numérotation par tonalité

Numérotation DTMF

Le principe du signal DTMF (*Dual Tone Multi Frequency*) consiste à superposer, pour un chiffre donné, deux fréquences sinusoïdales parfaitement définies en valeur de fréquence. Ces fréquences doivent se situer à l'intérieur de la bande passante du réseau téléphonique RTC (300-3 400 Hz).



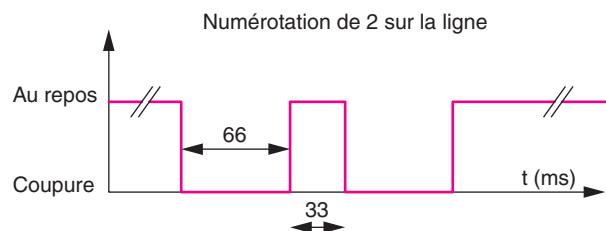
À titre d'exemple, le chiffre 5 est déterminé par un signal résultant de la superposition des deux fréquences 770 Hz et 1 336 Hz.

11•2•2 La numérotation par impulsion

Numérotation par impulsion

Elle consiste à créer des coupures brèves sur la ligne pour effectuer une numérotation.

Chiffre	Coupure
0	10
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9

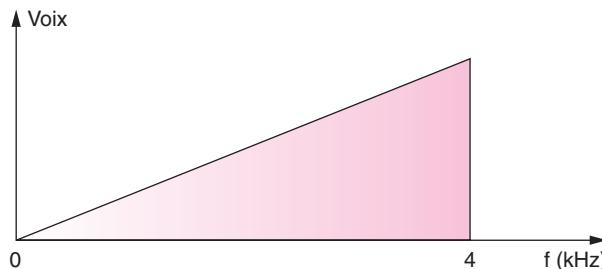


Numérisation de la voix

- Un signal électrique analogique est un signal dont le nombre d'états électriques est indéfini donc sensible aux perturbations électromagnétiques ; il est très délicat à transporter.
- Un signal électrique numérique est un signal dont le nombre d'états électriques est fini donc facile à régénérer. Il peut être transporté sur de longues distances sans altération.

La bande passante d'une ligne téléphonique classique du réseau commuté s'étend de 300 à 3 400 Hertz. Sans parler de qualité HIFI, cette bande est amplement suffisante pour rendre les conversations parfaitement intelligibles.

Le maximum d'énergie dans cette bande se situe approximativement à 800 Hertz. Avant de numériser la voix, on admet que la bande utile s'étend de 0 à 4 000 Hertz.



Le théorème de **SHANNON** fixe la fréquence d'échantillonnage à **2 fois la fréquence maximale** contenue dans le signal à échantillonner. On déduit que la fréquence d'échantillonnage doit être :

$$f_e = 8 \text{ kHz} \text{ soit } T_e = 125 \mu\text{s}$$

Ainsi, il faut prélever un échantillon toutes les 125 micro-secondes. Chaque échantillon est ensuite codé sur 8 bits.

La transmission de la voix est une transmission de données particulière au sens où la restitution du signal vocal au destinataire impose le strict respect d'une contrainte de temps : la voix est numérisée à raison d'un échantillon (1 octet) toutes les 125 micro-secondes, il faut donc absolument transporter un octet en 125 micro-secondes, ni plus, ni moins.

Ceci équivaut à transporter un débit binaire de **64 kbits/s** (8 000 échantillons/s × 8 bits).

Ainsi le signal transportant la voix doit être isochrone. On peut dire également qu'il s'agit d'un **transport temps réel**.

11•4 Le multiplexage des voies MIC

11•4•1 Objectif de la trame MIC

Généralités

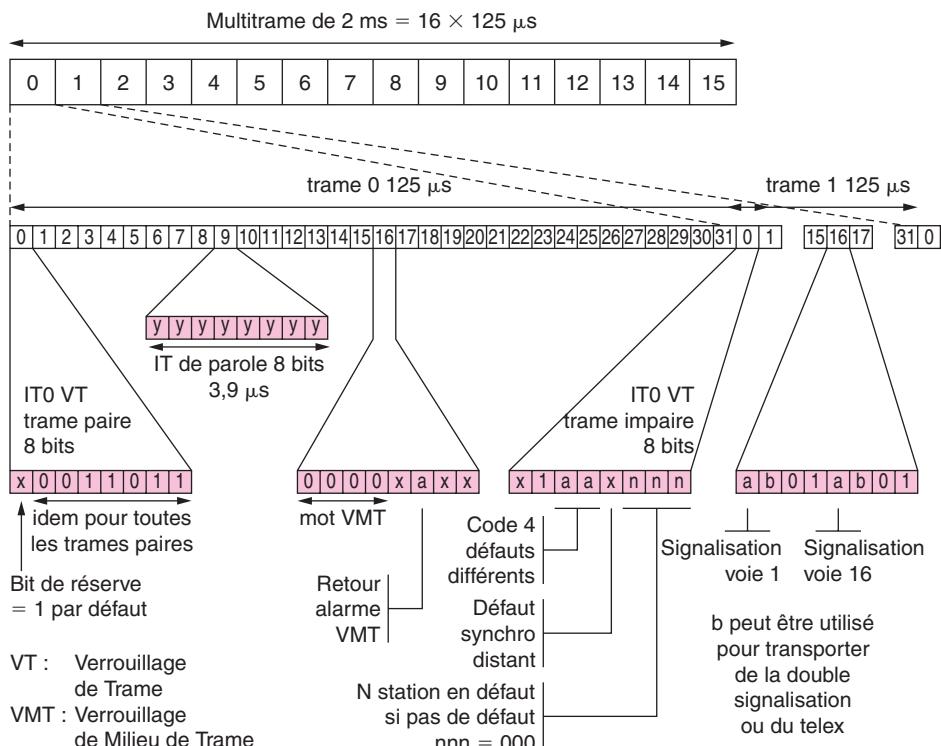
On profite de la faible bande passante des lignes téléphonique pour multiplexer dans le temps les différentes voies téléphoniques. La bande passante d'une voie téléphonique étant de : $3\ 400 - 300 = 3\ 100$ Hz, on a choisi 4 000 Hz comme bande passante utile.

Les différentes administrations européennes, regroupées dans le CEPT (Commission Européenne des Postes et Télécommunications) ont normalisé un multiplexeur téléphonique à 30 voies. Ce multiplexeur téléphonique a une structure de trame de 32 IT de 8 bits, numérotés de 0 à 31.

L'IT0 est utilisé pour le verrouillage des trames et la transmission des différents signaux d'alarme et de service. L'IT16 porte la signalisation correspondant aux 30 voies téléphoniques.

11•4•2 Structure de la trame d'un multiplexeur MIC 1G à 2 Mbps

La trame MIC



12 Le RNIS

12·1 Généralités

Le réseau NUMÉRIS est un réseau numérique permettant essentiellement de faire de la commutation de circuits (il s'agit donc d'un réseau commuté comme le RTC). Ce réseau offre avant tout un service support disponible en tout point du territoire.

Les services offerts peuvent être uniquement numériques ou mixtes (numériques et analogiques).

– En communication de type téléphonique (voies numérisées par MIC), le support offert peut être mixte (signaux issus de dispositifs Vidéotex, de teletex, de télécopieur, de poste téléphonique...).

Ces services « support » ont été rendus possible grâce au RTC constitué des CAA, CTS...

Ce qui change donc du RTC classique est :

- **La numérisation de la communication jusque chez l'abonné.**
- **La possibilité de transmettre des données à 64 kbit/s ou simplement de téléphoner à partir du même accès.**

D'autre part NUMÉRIS permet d'établir des circuits entre deux abonnés grâce à une signalisation très riche utilisant le réseau sémaaphore. Cette signalisation est directement fournie ou reçue par les terminaux de l'abonné.

Ce réseau sémaaphore est un réseau supervisant le réseau de commutation de circuits. Les informations circulant sur ce réseau sont a priori des informations de signalisation.

Le réseau sémaaphore est un réseau à commutation de paquets ; cela permet de transporter sur un même circuit des informations de signalisation relatives à plusieurs communications distinctes.

L'abonné peut ainsi bénéficier directement de la signalisation et de ses compléments de service associés (indication du coût, double-appel, va-et-vient, identification d'appel, minimesse, portabilité, présentation d'appel, renvoi de terminal, SDA, sous-adresse, etc.).

Le réseau Numéris offre plusieurs types d'accès :

- **L'accès de base**

L'abonné dispose de :

- Deux canaux de transmission pour la parole ou les données à 64 kb/s utilisant la commutation de circuits. Ces canaux sont appelés « canaux B ».
- Un canal de signalisation utilisé pour la supervision des communications sur les canaux B. Ce canal utilise la commutation par paquets avec un débit de 16 kb/s. Il est appelé « canal D ». Les informations de signalisation transmises sur le canal D vont ensuite emprunter le réseau sémaaphore. Comme les informations de signalisation sont loin de saturer ce réseau, on permet aux abonnés de faire également de la transmission de données (en mode paquet) sur ce canal D (exemple : connexion des terminaux « jeux rapido » de la Française des jeux).

- **Le groupement d'accès de base**

Ce groupement permet d'associer plusieurs accès de base.

- **L'accès primaire**

Cet accès est obligatoire à partir de 13 canaux B.

On peut alors souscrire à 15, 20, 25 ou 30 canaux B et un canal D qui dans ce cas a un débit de 64 kb/s.

C

Les réseaux et les serveurs

Généralités
sur Numéris

12•2 La couche physique

L'interface S0 est réservée au débit de 144 kb/s (accès 2B + D) et l'interface S2 au débit de 1984 kb/s. Le bus de l'interface S0 est réalisé par un câble à 4 paires symétriques. L'interface S est constituée d'un connecteur 8 broches (RJ45) défini par la norme ISO/DIS 8877.

- 2 paires obligatoires**

Transmission dans les deux sens (1 paire par sens)

Activation du terminal

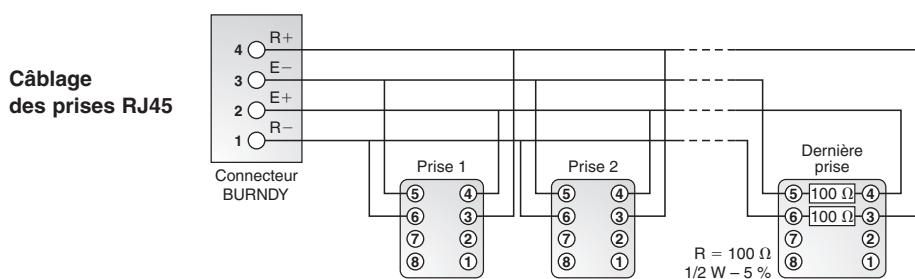
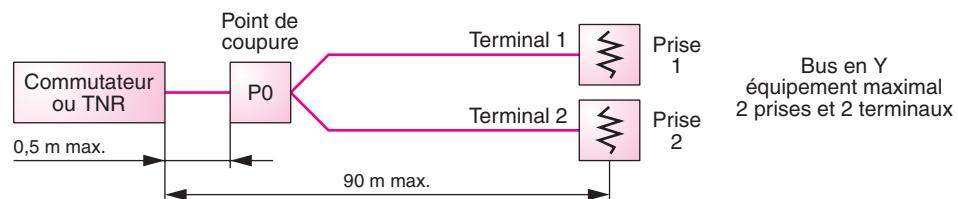
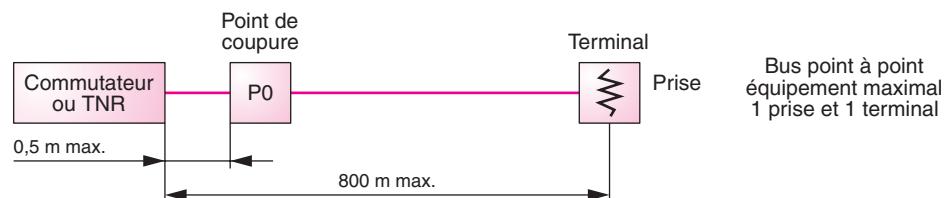
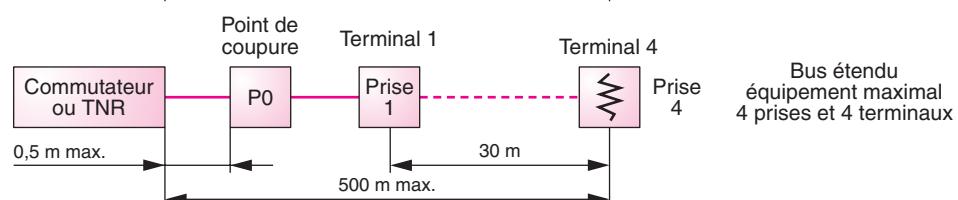
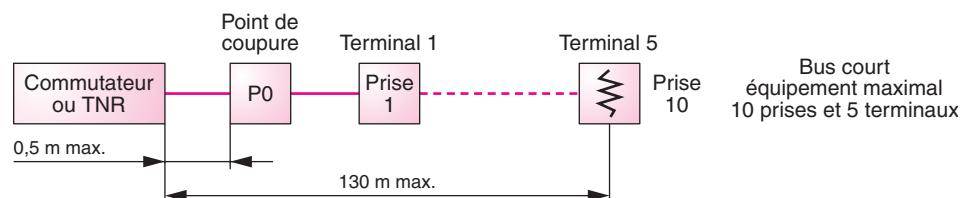
Téléalimentation du terminal

- 2 paires facultatives**

Sécurisation de l'alimentation des terminaux

Alimentation de la régie par le terminal

Les différentes configurations pour les petites installations sont :

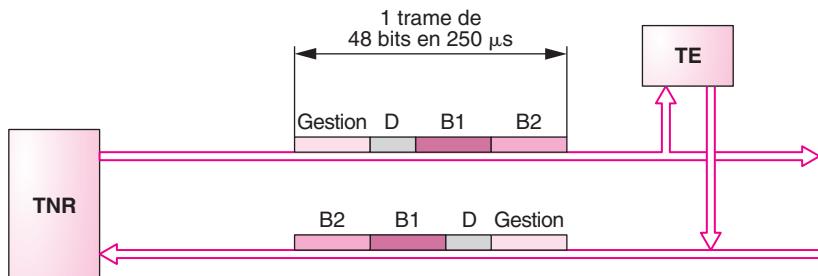


Configuration du bus S

Câblage des prises RJ45

12•2•1 Mécanisme d'accès au canal D

Le rôle du niveau 1 est de gérer l'accès des terminaux au canal D sur le support physique et de multiplexer l'information contenue dans le canal D avec d'autres informations (cet aspect sera étudié lors de l'étude des niveaux supérieurs).



Sachant que la liaison au niveau physique est de type point à multipoint, il nous faut considérer les deux cas suivants :

- **Sens TE → TNR** (paire réception de la TNR)

Deux terminaux peuvent envoyer des informations en même temps sur le canal D, ce qui (si rien n'est fait) engendre une collision des deux informations et rend donc celles-ci incompréhensibles.

- **sens TNR→ TE** (paire émission de la TNR)

Le problème ne se pose pas car seule la TNR est susceptible d'émettre des données sur le canal D.

Mécanisme d'accès au canal D

La méthode choisie pour résoudre ce problème est **CSMA/CR** (*Carrier Sense Multiple Access / Contention Resolution*) (Accès multiple avec écoute de porteuse / résolution de contention).

Le principe de cette méthode d'accès est simple. Il consiste pour la TNR à renvoyer en écho sur un canal E, en direction des terminaux, la copie parfaite des informations que la TNR avait reçues sur le canal D en provenance des terminaux.

Grâce à cet écho chaque terminal peut vérifier bit par bit que l'information qu'il envoie est bien celle que reçoit la TNR.

Dès qu'un terminal constate une différence entre le bit envoyé et le bit indiqué en écho (donc celui effectivement reçu par la TNR), il arrête aussitôt l'émission.

- Un « 1 » logique est codé par une tension nulle.
- Un « 0 » logique est codé en alternance par une tension positive ou négative.
- Chaque terminal envoie des « 1 » entre les trames qu'il envoie ou lorsqu'il n'envoie rien (bourrage).
- Le bit réellement envoyé sur le canal D est le résultat de l'opération logique ET de tous les bits envoyés par chacun des terminaux sur le canal D.

C

Les réseaux et les serveurs

Nous venons de voir comment étaient résolus les problèmes de contention (c'est-à-dire lorsque plusieurs terminaux se décident à envoyer des données en même temps).

Nous venons d'étudier le « **CR** », reste à aborder le « **CSMA** ».

TOUS les terminaux connectés sur le bus prennent en compte en permanence les informations présentes sur le canal D par le biais de l'écho (canal E).

Grâce à cela un terminal peut savoir avant d'émettre des données si le canal D est déjà occupé.

En effet, si un terminal constate qu'il y a eu au moins sept « 1 » consécutifs, il en déduit qu'aucun terminal n'est en train d'émettre des informations sur le canal D.

Il y a 6 états « 1 » consécutifs pour un fanion (7Eh) et il ne peut jamais y avoir plus de 5 états « 1 » consécutifs à l'intérieur d'une trame.

Pour cela on applique un dispositif d'insertion de « 0 » pour assurer la transparence de l'information.

Mécanisme d'accès au canal D (suite)

Donc a priori un terminal qui aurait compté sept « 1 » consécutifs sur le canal E pourrait émettre ses informations sur le canal D.

Mais dans la réalité ce n'est pas le cas : les informations de signalisation sont prioritaires sur toutes les autres.

En outre, pour éviter que ce soient toujours les mêmes terminaux qui envoient leurs informations, il a été mis en place des classes de priorité et des niveaux de priorité dans ces classes.

Mécanismes de priorité

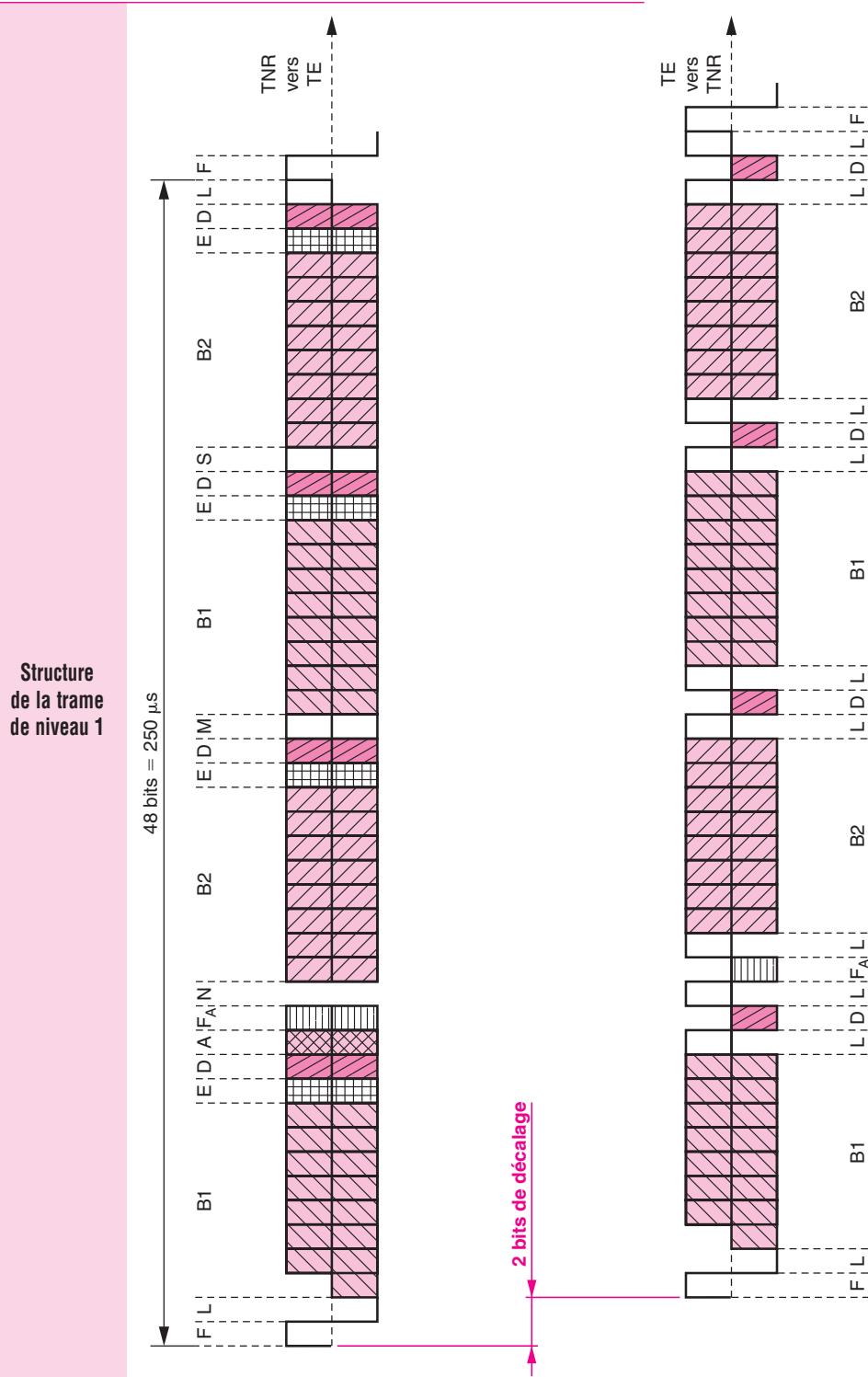
Les trames de la couche 2 qui transitent de l'information de signalisation ont priorité absolue (classe 1) sur les autres trames d'information (classe 2).

De plus, pour que les terminaux de même classe de priorité puissent avoir un accès équitable sur le canal D, un terminal qui a effectué avec succès la transmission d'une trame aura pour la trame suivante un niveau de priorité inférieur (dans la même classe de priorité).

Ce mécanisme de priorité est fondé sur le fait qu'un terminal ne peut commencer à émettre sa trame de niveau 2 sur le canal D qu'à partir du moment où le nombre de « 1 » consécutifs comptés sur le canal E est supérieur ou égal à :

- 8 pour la classe 1, niveau normal (info de signalisation),
- 9 pour la classe 1, niveau inférieur (info de signalisation),
- 10 pour la classe 2, niveau normal (autre info),
- 11 pour la classe 2, niveau inférieur (autre info).

12•3 Structure de la trame de niveau 1



C

Les réseaux et les serveurs

Structure de la trame de niveau 1 (suite)

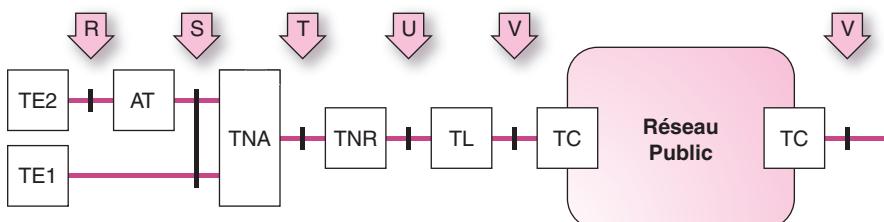
F	bit de verrouillage
L	bit d'équilibrage de composante continue
B1	bits dans la voie B1
E	bit de la voie D en écho
D	bit de la voie D
A	bit utilisé pour l'activation des TE
F_A	bit de verrouillage de trame auxiliaire (voir ci-après)
N	bit à l'état binaire inverse de F_A (= 1)
B2	bit dans la voie B2
M	bit de multitrame (non utilisé actuellement)
S	bit non utilisé actuellement (= 0)

Afin de garantir la sécurité du verrouillage de trame, on introduit un couple de bits de verrouillage de trame auxiliaire F_A et N dans le sens TNR vers TE et un bit de verrouillage de trame auxiliaire F_A associé à son bit d'équilibrage L dans le sens TE vers TNR.

- Dans le sens TNR vers TE, la valeur de F_A = 0 et la valeur de N = 1.
- Dans le sens TE vers TNR, la valeur de F_A est égale à la valeur du dernier bit F_A .

Les terminaux se synchronisent à partir de la trame reçue. Cela explique le décalage de 2 bits entre les trames reçues et émises.

LES GROUPEMENTS FONCTIONNELS ET LES POINTS DE RÉFÉRENCE



Architecture générale

Groupements fonctionnels

- TE : terminal
- AT : adaptateur de terminal
- TNA : terminaison numérique d'abonné
- TNR : terminaison numérique de réseau
- TL : terminal de ligne
- TC : terminal de commutation

Points de référence

- R : point de référence
- T : marque la frontière entre domaine public et domaine privé
- S et T peuvent être confondus (fonctionnement sans TNA)
- U correspond pratiquement à la boucle d'abonné

12•4 La couche réseau

Caractéristiques générales

Le protocole niveau 3 définit les procédures portant sur la signalisation relatives aux communications mode circuit à l'interface S/T du RNIS.

Le champ de commande des messages utilisés possède un SAPI de valeur 0 (signalisation).

Les procédures définies permettent :

- l'établissement, la supervision et la rupture des communications utilisant les canaux B exploités en communication circuit ;
- la mise en œuvre des compléments de service ;
- le transfert d'informations usager à usager.

La longueur des messages est variable, mais est toutefois limitée par le niveau 2 (260 octets maxi).

L'ensemble des services et compléments de service utilise 24 types de message.

La définition d'un message tient compte :

- du contenu ;
- du sens d'utilisation ;
- de l'état des interfaces émettrices ou réceptrices ;
- du service traité ;
- du contexte d'appel (simple, multiple) et de la configuration utilisée à chaque extrémité.

Le service transfert d'information non numéroté n'est utilisé que dans le cas point à multipoint de la couche 3, lors de la présentation de l'appel à l'interface Destination.

Les différents types de messages utilisés

MESSAGES D'ÉTABLISSEMENT D'APPEL

- ALERTE
- APPEL ACHEMINÉ
- APPEL EN COURS
- CONNEXION
- ACCUSÉ DE RÉCEPTION DE CONNEXION
- ÉTABLISSEMENT
- ACCUSÉ DE RÉCEPTION D'ÉTABLISSEMENT.

MESSAGES DE DÉCONNEXION

- DÉCONNEXION
- LIBÉRATION
- FIN DE LIBÉRATION.

MESSAGES EN PHASE D'ÉCHANGE D'INFORMATION

- REPRISE
- ACCUSÉ DE RÉCEPTION DE REPRISE
- REFUS DE REPRISE
- SUSPENSION
- ACCUSÉ DE RÉCEPTION DE SUSPENSION
- REFUS DE SUSPENSION.

MESSAGES DE COMMANDE DE FACILITÉS

- FACILITÉ
- ACCEPTATION DE FACILITÉ
- REFUS DE FACILITÉ
- ENREGISTREMENT
- ACCEPTATION D'ENREGISTREMENT
- REFUS D'ENREGISTREMENT.

MESSAGES DIVERS

- INFORMATION
- ÉTAT.

C

Les réseaux et les serveurs

La mise en œuvre des procédures de niveau 3 implique que la liaison de données soit établie entre le terminal et le réseau.

1^{re} PHASE : DEMANDE D'APPEL

L'usager déclenchant l'appel transmet un message « ÉTABLISSEMENT » à travers l'interface usager-réseau. Dès la transmission du message, l'usager arme une temporisation en attente de réponse.

L'usager se trouve alors dans l'état d'initialisation d'appel.

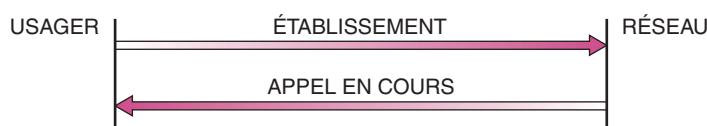
Dans le message établissement, l'usager peut indiquer dans le champ « Identification de canal » s'il désire utiliser un canal particulier.

En ce qui concerne la numérotation, celle-ci peut être envoyée par le terminal en « bloc » ou par « chevauchement ».

Numérotation en bloc

Tous les paramètres concernant l'adresse du demandé sont contenus dans « ÉTABLISSEMENT ».

Si ces valeurs sont acceptables par le réseau, ce dernier émet vers l'usager le message « APPEL EN COURS ».



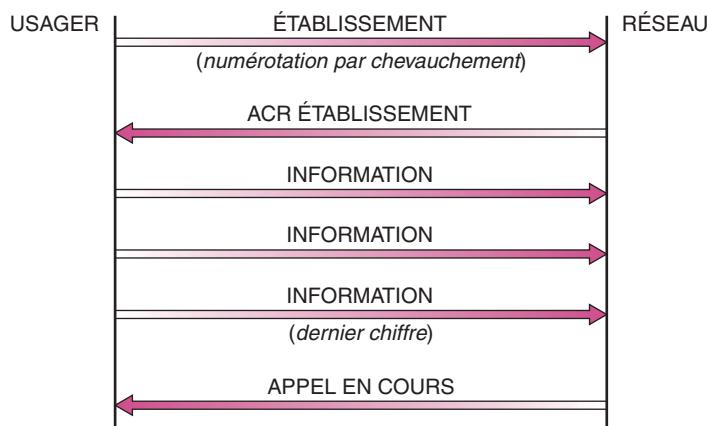
Établissement d'un appel

Numérotation par chevauchement

Si l'« ÉTABLISSEMENT » indique que la numérotation est émise par chevauchement, et qu'il est correct, le réseau émet un « ACCUSÉ DE RÉCEPTION D'ÉTABLISSEMENT » autorisant l'usager à émettre la numérotation.

Dès réception d'« ACR d'ÉTABLISSEMENT », l'usager se connecte sur le canal indiqué (réception des tonalités) et émet unitairement ou par groupe, le numéro de destination dans des messages « INFORMATION ».

Lorsque le réseau a reconnu la numérotation complète, le message « APPEL EN COURS » est émis.



Établissement d'un appel (suite)

2^e PHASE : APPEL EN COURS

Dès réception du message « APPEL EN COURS », l'appel entre dans l'état « Appel sortant en cours ».

Les opérations de sélection de l'abonné demandé vont être déclenchées par le central. Suite à la recherche entreprise une indication va être émise vers l'usager demandeur :

- Indication d'émission de tonalité ou d'annonce parlée.
- Indication d'interfonctionnement.
- Indication de confirmation d'appel.
- Indication d'acceptation d'appel par l'usager distant.
- Indication de rejet d'appel.

Si la temporisation d'attente expire avant la réception d'une de ces indications, l'usager émet un message « DÉCONNEXION » vers le réseau.

Indication d'émission de tonalité ou d'annonce parlée

Lorsque, en cours d'établissement de communication, le réseau veut imposer une tonalité ou un film de dissuasion, il émet vers l'usager le message « APPEL ACHEMINÉ » avec la cause. L'usager effectue la connexion au canal B s'il ne l'a déjà réalisée. Cette procédure sera suivie par :

- une indication d'interfonctionnement,
- une indication de confirmation d'appel,
- une indication d'acceptation d'appel par l'usager distant,
- une indication de rejet de l'appel.

Établissement de l'appel par le Central arrivée

Le réseau présente à l'interface usager-réseau un message « ÉTABLISSEMENT ».

Le nombre d'appels présenté à un usager n'est pas limité (référence d'appel). Dans le cas de surcharge, l'appel n'est pas reconnu et ne donne pas lieu à une réponse. Le message « ÉTABLISSEMENT » est présenté à tous les terminaux.

Un terminal ne répond à la présentation d'un appel que s'il est compatible avec l'élément d'information (compatibilité des couches supérieures et compatibilité des couches inférieures).

Le message « ÉTABLISSEMENT » peut également comporter une information de sous-adresse de destination. Le terminal alors ne répond que s'il se reconnaît dans les informations d'adresse reçues.

La réponse au message de présentation d'appel « ÉTABLISSEMENT » sera fonction du type de terminal :

- terminal à réponse manuelle (téléphone...),
- terminal à réponse automatique (télécopie).

Réponses pour un terminal

Le message « ALERTE » est émis par un terminal à réponse manuelle disposant d'un contexte à allouer si un canal est disponible ou s'il a la possibilité d'en disposer d'un (libération ou mise en garde).

Le message « CONNEXION » est émis en première réponse par un terminal à réponse automatique.

ACCEPTATION D'APPEL

Un usager acceptant l'appel entrant émet un message « CONNEXION » à travers l'interface usager-réseau.

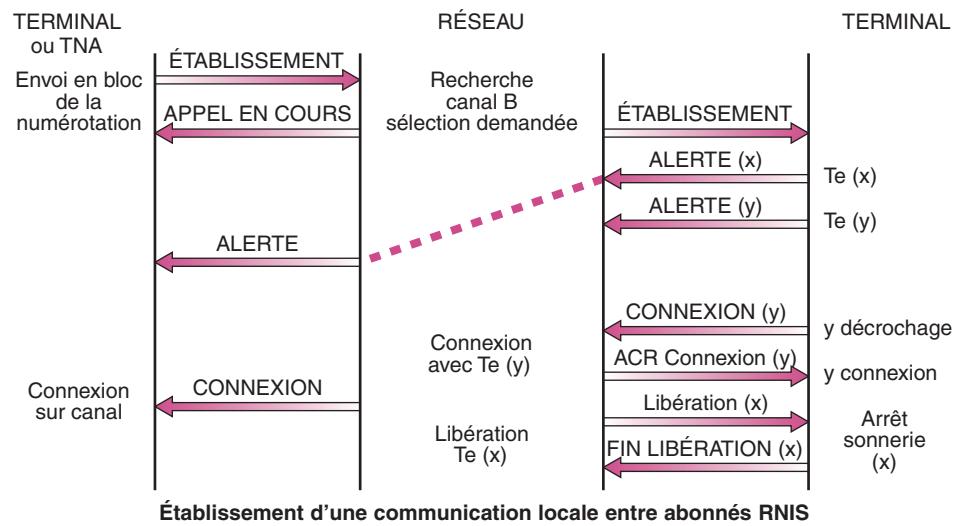
Le message « CONNEXION » peut être utilisé pour négocier un canal. Deux cas peuvent se présenter :

a) Aucun canal disponible n'est spécifié dans « ÉTABLISSEMENT ». Seuls les terminaux en conversation sont concernés et peuvent alors :

- Libérer une communication en cours (donc un canal), le message « CONNEXION » ne comportant pas le numéro du canal. Le réseau allouera donc le canal libéré dans le message de réponse « ACCUSÉ DE RÉCEPTION DE CONNEXION ». Si aucun canal n'est trouvé libre, le réseau émet le message « LIBÉRATION » vers le terminal concerné avec la cause.
- Mettre en garde une communication en cours. Le message « CONNEXION » identifie alors le canal réservé au terminal par la suite de la mise en garde. Le réseau, en réponse envoie « ACCUSÉ DE RÉCEPTION DE CONNEXION » sans identification du canal.

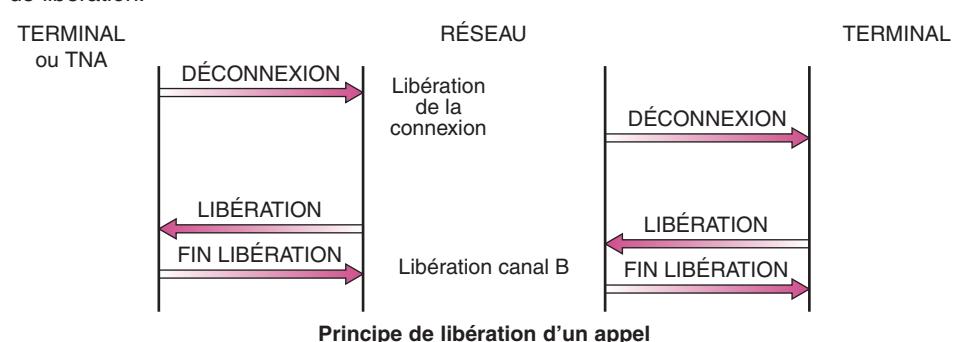
b) Spécification d'un canal dans « ÉTABLISSEMENT »

Un terminal libre ou se libérant accepte le canal proposé. « CONNEXION » est alors émis en réponse sans identification de canal.



LIBÉRATION DE L'APPEL

L'envoi du message « DÉCONNEXION » par l'usager ou le réseau déclenche la procédure de libération.



Libération en fonction de l'état de l'appel**a) Procédure de libération côté départ**

État de l'appel	Message émis pour initialiser la libération	
	par l'usager	par le réseau
Demande d'appel émise ou reçue	Déconnexion	Fin de libération
Message émis ou reçu ⁽¹⁾ , en réponse à la demande d'appel	Déconnexion	Déconnexion
Message alerte émis ou reçu	Déconnexion	Déconnexion
Appel actif, connexion établie	Déconnexion	Déconnexion

Libération côté départ

Nota 1: Ce message peut être ACCUSÉ DE RÉCEPTION ÉTABLISSEMENT ou APPEL EN COURS.

b) Procédure de libération côté arrivée

État de l'appel	Message émis pour initialiser la libération			
	par le réseau	par l'usager		
		rejet avec SUU	renvoi	rejet
Demande d'appel émise ou reçue		Libération	Libération	Libération
Message ALERTE émis ou reçu	Libération	Libération	Libération	
Appel actif, connexion établie ⁽¹⁾	Déconnexion	Déconnexion		Déconnexion

Libération côté arrivée

Nota 1 : La connexion n'est établie que pour un seul équipement d'usager, à savoir celui auquel un message AR CONNEXION a été émis.

La signalisation d'usager à usager (mini-message) permet l'échange d'informations entre deux usagers. Les terminaux peuvent échanger de la signalisation d'usager à usager lors de la phase d'établissement ou de libération dans les messages ci-après :

- ÉTABLISSEMENT
- ALERTE
- CONNEXION
- DÉCONNEXION
- LIBÉRATION.

La longueur maximum de 128 octets introduite au niveau de la spécification du protocole pour les terminaux est actuellement limitée par le réseau public à 32 octets utiles. Toute information dépassant cette longueur est ignorée par le réseau.

Le réseau ne contrôle pas le contenu de cet élément d'information mais assure uniquement son transfert.

La spécification impose que lors de la mise en œuvre de ce complément de service, les usagers s'assurent de l'aptitude de leur correspondant à traiter la signalisation usager à usager.

L'usager demandé sait à partir du message « ÉTABLISSEMENT » reçu si le demandeur l'autorise à émettre de la signalisation usager à usager (3 octets dans champ IUU).

Lors de la phase d'établissement, le demandeur émet de l'IUU sous son entière responsabilité.

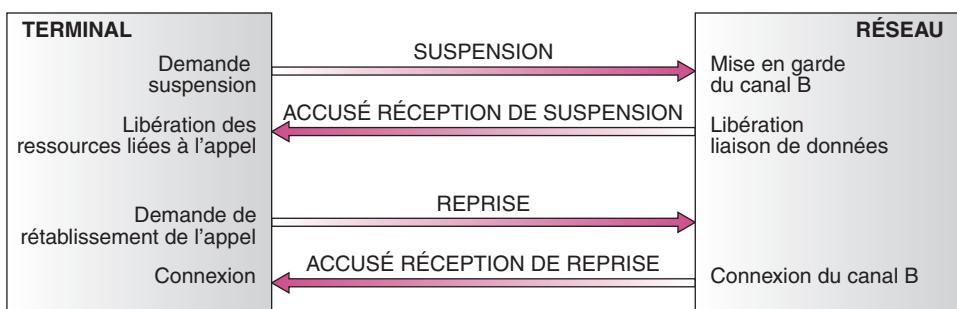
La mise en œuvre de cette procédure à l'interface usager-réseau correspond à un certain nombre d'événements :

- déconnexion physique de l'équipement d'usager et connexion à un point différent ;
- remplacement physique d'un équipement d'usager par un autre point ;
- passage d'un équipement d'usager à un autre ;
- suspension de l'appel et reprise sur le même équipement d'usager.

Le réarrangement d'appel est fourni comme élément de base du service RNIS.

Toutefois, actuellement, la reprise d'un appel suspendu doit être effectuée sur le canal utilisé avant la suspension.

Réarrangement d'appel



Exemple de suspension et reprise d'un appel

Lorsqu'un message « REPRISE » reçu ne peut être traité par le réseau, un message « FIN DE REPRISE », ou « FIN DE LIBÉRATION » est envoyé à l'usager demandeur. L'appel est alors libéré.

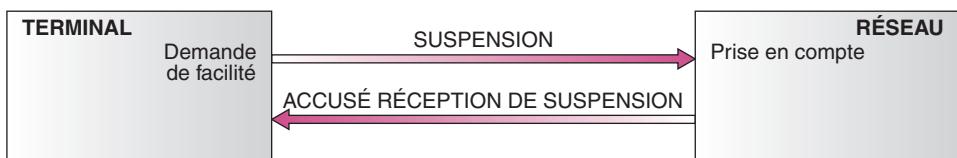
Deux procédures de commande des services complémentaires sont définies :

- Commande des services complémentaires concernant l'appel, associés à une procédure de commande de l'appel ;
- Enregistrement ou annulation des services complémentaires, indépendamment des procédures de commande de l'appel et de tout appel particulier.

Les messages utilisés pour la commande des services complémentaires sont :

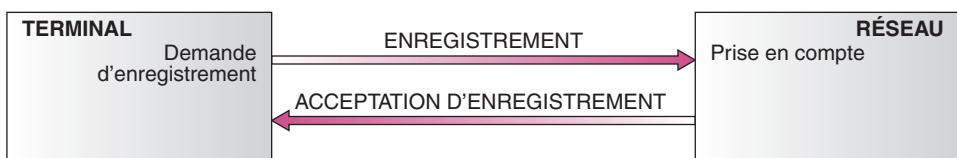
- FACILITÉ
- ACCEPTATION DE FACILITÉ
- REFUS DE FACILITÉ

Commande de services complémentaires d'usager



Les messages utilisés pour l'enregistrement, l'annulation ou la vérification d'enregistrement de compléments de service sont :

- ENREGISTREMENT
- ACCEPTATION D'ENREGISTREMENT
- REFUS D'ENREGISTREMENT.



Messages utilisés par les compléments de service

PROCÉDURE DE REJET DE COMPLÉMENT DE SERVICE

Un certain nombre de raisons peuvent entraîner le rejet de la demande de l'usager :

- interdiction d'accès à l'usager (complément de service non souscrit) ;
- ressources indisponibles ;
- complément de service non mis en oeuvre dans le réseau ou dans la TNA ;
- demande incohérente ;
- etc.

Signalisation usager à usager : ÉTABLISSEMENT, ALERTE, CONNEXION, DÉCONNEXION, LIBÉRATION :

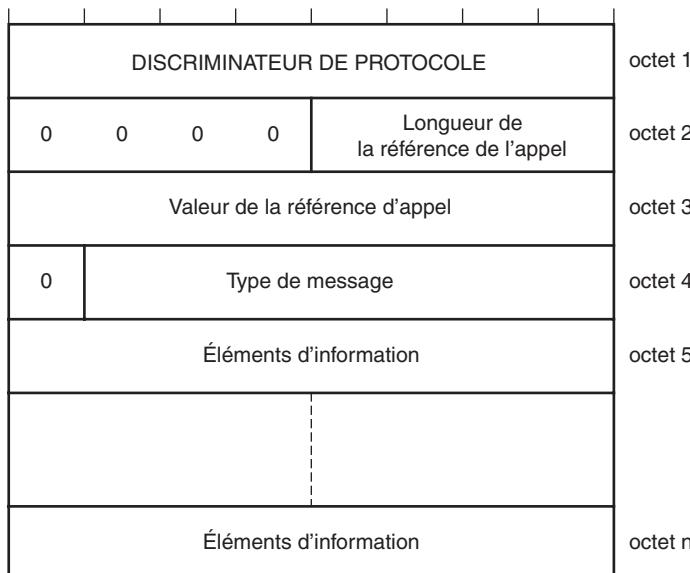
- identité de l'usager demandeur : ÉTABLISSEMENT ;
- SDA RNIS : ÉTABLISSEMENT ;
- indication de coût : demande dans ÉTABLISSEMENT émission de une ou plusieurs INFORMATIONS à chaque incrémentation du compteur ;
- coût total : DÉCONNEXION ou LIBÉRATION ;
- transfert d'appel national : ENREGISTREMENT de renvoi temporaire (enregistrement, modification, interrogation et annulation) ;
- renvoi du terminal : réponse au message ÉTABLISSEMENT par le message LIBÉRATION contenant la demande de renvoi du terminal ainsi que l'adresse de réacheminement ;
- mise en garde et passage en double appel :
 - mise en garde et levée de garde : FACILITÉ ;
 - prise appel en instance : FACILITÉ, CONNEXION ;
 - établissement second appel : FACILITÉ, ÉTABLISSEMENT ;
- va-et-vient : FACILITÉ ;
- conférence additive : FACILITÉ et DÉCONNEXION pour libération de la conférence ;
- identification d'appel malveillant : FACILITÉ.

Structure des messages

Chaque message est structuré de la manière suivante et dispose de :

- discriminateur de protocole ;
- référence d'appel ;
- type de message ;
- des éléments d'information fonction des besoins.

STRUCTURE GÉNÉRALE D'UN MESSAGE



DISCRIMINATEUR DE PROTOCOLE

Le discriminateur de protocole permet d'établir une discrimination entre les messages servant à la commande d'appel usager-réseau et d'autres messages. Il sert également à distinguer les messages figurant dans cette spécification des unités de données de protocole de niveau réseau OSI qui sont codées conformément à d'autres recommandations du CCITT et à d'autres normes.

RÉFÉRENCE D'APPEL

Elle permet l'identification au niveau interface locale usager-réseau l'appel ou la demande d'enregistrement / annulation à laquelle s'applique le message. La référence d'appel n'a qu'une signification locale.

La valeur référence d'appel est attribuée par le côté de l'interface origine de l'appel. Elle est affectée au début de la communication et reste pendant la durée (sauf durant les suspensions).

TYPE DE MESSAGE

Le type de message identifie la fonction du message.

	8	7	6	5	4	3	2	1	TYPE
Structure des messages (suite)	0	0	0	Message d'établissement de l'appel
				0	0	0	0	1	Alerte
				0	0	0	1	0	Appel en cours
				0	0	0	1	1	Appel acheminé
				0	0	1	1	1	Connexion
				0	1	1	1	1	Accusé de réception de connexion
				0	0	1	0	1	Établissement
				0	1	1	0	1	Accusé de réception d'établissement
	0	0	1	Message en phase d'information de l'appel
				0	0	1	1	0	Reprise
0	0	1	1	1	1	0			Accusé de réception de reprise
		0	0	0	1	0			Refus de reprise
		0	0	1	0	1			Suspension
		0	1	1	0	1			Accusé de réception de suspension
		0	0	0	0	1			Refus de suspension
	0	1	0	Message de libération de l'appel
0	0	0	1	0	1				Déconnexion
		0	1	1	0	1			Libération
		1	1	0	1	0			Fin de libération
	0	1	1	Messages divers
0	1	1	0	1	1	1			Informations
	0	0	0	1	0	0			Facilité
	0	1	0	1	0	0			Acceptation de facilité
	1	0	0	1	0	0			Refus de facilité
	0	0	1	0	0	0			Enregistrement
	0	1	1	0	0	0			Acceptation d'enregistrement
	1	0	1	0	0	0			Refus d'enregistrement
	1	1	1	0	1				État

13 Téléphonie sur IP

13•1 Présentation

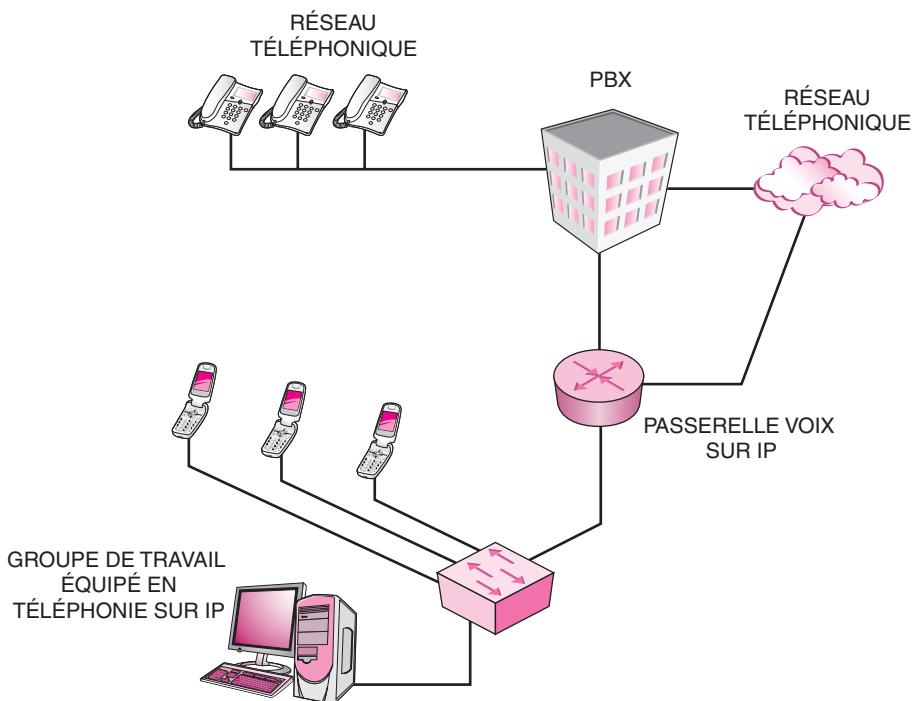
La « Voix sur IP » est la technologie utilisée pour transporter le service de téléphonie sur IP.

La téléphonie sur IP est un service de téléphonie fourni sur un réseau de télécommunications ouvert au public ou privé utilisant principalement le protocole de réseau IP.

Cette technologie permet d'utiliser une infrastructure existante de réseau IP pour raccorder des terminaux IP que l'on nomme IP-PHONE, ainsi que des logiciels sur PC raccordés sur le même réseau IP que l'on nomme SOFTPHONE.

La téléphonie sur IP peut :

- 1) Se rajouter en complément sur un réseau téléphonique traditionnel existant avec une passerelle.



- 2) S'utiliser en full-IP pour une nouvelle infrastructure (nouvel immeuble par exemple avec uniquement du câblage catégorie 5 ou 6).

- 3) S'utiliser en multisites full IP avec l'aide d'un opérateur adéquat et parfois des serveurs centralisés.

- 4) S'utiliser sur un ordinateur relié au réseau Internet à destination d'un autre ordinateur relié lui aussi au réseau Internet, mais en utilisant absolument le même logiciel (les communications seront donc gratuites de PC à PC).

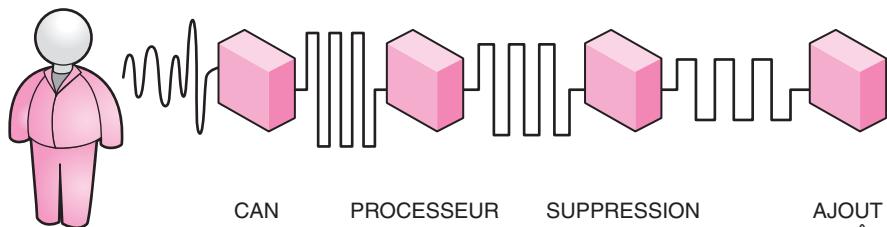
La téléphonie sur IP est une transmission de la voix en mode paquets au format TCP/UDP.

C

Les réseaux et les serveurs

13•2 Traitement de la voix analogique

La voix
sur IP
(suite)



La bande voix, qui est un signal électrique analogique utilisant une bande de fréquences de 300 à 3 400 Hz, est d'abord échantillonnée numériquement par un convertisseur puis codée sur 8 bits, puis compressée par les fameux codecs (il s'agit de processeurs DSP) selon une certaine norme de compression variable selon les codecs utilisés.

Ensuite on peut éventuellement supprimer les pauses de silences observés lors d'une conversation, pour être ensuite habillé RTP, UDP et enfin en IP.

13•3 Généralités sur la transmission

La transmission

Le transport des signaux voix numérisés par paquets impose des contraintes majeures :

1) Optimisation de la bande passante (attention aux autres applications informatiques qui monopolisent la majeure partie de la bande passante disponible).

2) Délai de transmission

Il comprend le codage, le passage en file d'attente d'émission, la propagation dans le réseau, la bufférisation en réception et le décodage. Le délai de transmission optimal est de 150 ms (UIT-T G114). Les délais parfois tolérables sont entre 150 et 400 ms.

3) Le phénomène d'écho (réverbération du signal)

C'est le délai entre l'émission du signal et la réception de ce même signal en réverbération. Cette réverbération est causée par les composants électroniques des parties analogiques. Un écho < 50 ms n'est pas perceptible. Plus il est décalé dans le temps, plus il est insupportable.

4) La gigue ou Jitter (variation de l'écart initial entre deux paquets émis)

Elle correspond à des écarts de délais de transmission entre des paquets consécutifs et nécessite la mise en place de buffers en réception qui lisent ces écarts pour retrouver le rythme de l'émission.

Effet néfaste des buffers de réception ==> augmentation du délai de transmission.

5) La gestion de la qualité de service des réseaux IP de transport

d'un bout à l'autre. Elle peut être une solution propriétaire (Qos constructeur), DiffServ, RSVP ou MPLS.

Rappelons enfin que le mode de fonctionnement de l'acheminement sur l'Internet est du type Best Effort : chaque équipement constituant le réseau (en particulier les routeurs) fait de son mieux pour acheminer les informations.

En conclusion, le transport de la téléphonie sur l'IP ne doit souffrir d'aucun retard de transmission, ni d'altérations (attention aux *firewall*), ni de perte de paquets.

13•4 Les transmissions CODECs et taux de compression

Taux de compression	Les codecs sont des chipsets qui font office de codeurs/décodeurs. Certains terminaux IP-PHONES n'acceptent qu'une partie ou même un seul codec, tout dépend du modèle de terminal et du constructeur.	
	Les principaux taux de compression de la voix sont les codecs officiels suivants :	
	Méthode de compression	Débit en kBits/s
	G.711 PCM	64
	G.726 AD PCM	32
	G.728 LD CELP	16
	G.729 CS ACELP	8
	G.729 × 2 Encodings	8
	G.729 × 3 Encodings	8
	G.729a CS ACELP	8

13•5 Les différents protocoles utilisés

Caractéristiques générales	Les différents protocoles non propriétaires sont les trois suivants :	
	H323	Le protocole H323 est le plus connu et se base sur les travaux de la série H.320 sur la visioconférence sur RNIS. C'est une norme stabilisée avec de très nombreux produits sur le marché (terminaux, gatekeeper, gateway, logiciels). Il existe actuellement 5 versions du protocole (V1 à V5).
	SIP	Le protocole SIP (<i>Session Initiation Protocol</i>) a été initié par le groupe MMUSIC (<i>Multiparty Multimedia Session Control</i>) et est désormais repris et maintenu par le groupe SIP de l'IETF donnant la Rfc 3261 rendant obsolète la Rfc 2543 . SIP est un protocole de signalisation appartenant à la couche application du modèle OSI . Son rôle est d'ouvrir, modifier et libérer les sessions. L'ouverture de ces sessions permet de réaliser de l'audio ou vidéoconférence, de l'enseignement à distance, de la voix (téléphonie) et de la diffusion multimédia sur IP essentiellement. Un utilisateur peut se connecter avec les utilisateurs d'une session déjà ouverte. Pour ouvrir une session, un utilisateur émet une invitation transportant un descripteur de session permettant aux utilisateurs souhaitant communiquer de s'accorder sur la compatibilité de leur média ; SIP permet donc de relier des stations mobiles en transmettant ou redirigeant les requêtes vers la position courante de la station appelée. Enfin, SIP possède l'avantage de ne pas être attaché à un médium particulier et est sensé être indépendant du protocole de transport des couches basses.
	MGCP	Le protocole MGCP est complémentaire à H.323 ou SIP, et traite des problèmes d'interconnexion avec le monde téléphonique.

C

Les réseaux et les serveurs

13•6 L'alimentation des postes IP

L'alimentation

Un poste IP (ou iP-PHONE) a besoin d'une alimentation externe DC de 48 volts ou d'une télé-alimentation par le port Ethernet.

Il y a deux solutions pour se passer d'un petit transformateur 220 V~/48 VDC.

Ces deux solutions ont été normalisées par un document officiel de IEEE Computer Society (norme : 802.3af) et elles sont décrites ci-dessous :

SOLUTION 1

Les téléphones IP sont directement connectés aux switchs d'étages qui intègrent l'alimentation 48 V nécessaire sur les paires LIBRES ! C'est donc un switch dernière génération compatible 802.3af.

SOLUTION 2

Si le Switch n'est pas équipé, il faut installer un *Patch Power Panel* pour pouvoir alimenter quand même les téléphones IP. Les cordons réseaux sortent du Switch, vont au *power panel* puis ressortent sur un autre port vers le PC de l'étage.

Si vous n'avez pas un Switch qui assure la télé-alimentation ou un *power patch panel*, il est obligatoire de disposer d'un transformateur externe par téléphone IP (IP-PHONE). Il est à noter qu'en cas de panne secteur, il n'y a plus de téléphone et aucun appel d'urgences n'est donc possible.

14 Les postes DECT

14•1 Définition

Principe du DECT

C'est une norme de téléphonie sans fil fonctionnant sur une gamme de fréquences allant de 1 880 à 1 900 MHz.

DECT = *Digital Enhanced Cordless Telephone*

14•2 Généralités

C'est une technologie d'accès radio-numérique qui se compose au minimum de deux éléments : la base et le combiné.

La base est reliée à un réseau (RTC, RNIS...).

Si on possède plusieurs combinés il est alors possible de communiquer entre combinés.

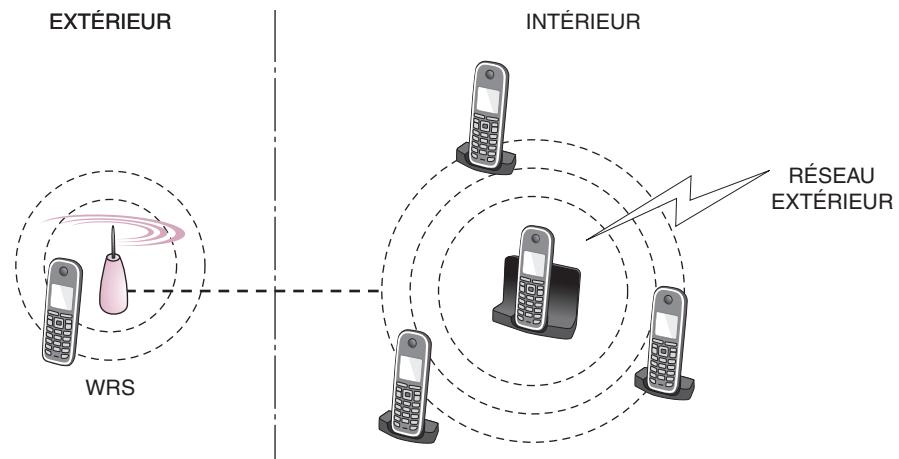
Il est possible de connecter 12 combinés (6 sur les modèles économiques).

LA PORTÉE

Elle est généralement d'environ 50 mètres à l'intérieur et de 300 m en zone dégagée.

Pour augmenter la zone de couverture il est possible d'ajouter un amplificateur appelé *Wireless Relay Station*.

L'alimentation



14•3 Le fonctionnement

Principe du DECT (suite)

À la mise sous tension de la base, celle-ci émet des signaux courts sur le canal temporel qu'elle aura préalablement choisi pour sa qualité.

Chaque signal transporte les informations sur la capacité de la base et permet au mobile de se connecter. Ce signal est émis toutes les 10 ms et dure 52 µs.

À la mise sous tension de la partie mobile celle-ci détecte le signal et peut alors se connecter à la base.

C

Les réseaux et les serveurs

14•4 La norme

Norme EN 300175

Cette norme est définie par l'ETSI sous la référence EN 300 175.

Radio :

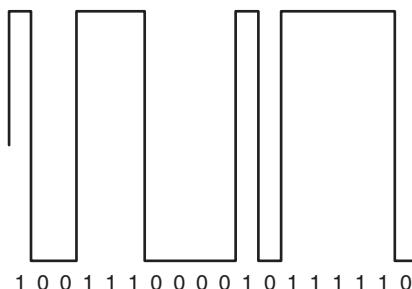
- Modulation GFSK.
- FDMA : 10 porteuses de 1 880 à 1 900 MHz en Europe.
- TDMA : 2 fois 12 intervalles de temps (*time slots*) (12 dans chaque sens). Chaque intervalle de temps permet un débit de 32 kbit/s. Ces *time slots* peuvent être groupés pour offrir un débit binaire supérieur.
- L'allocation des canaux et *time slots* se réalise de façon dynamique permettant théoriquement l'établissement de 120 communications simultanées. Ceci n'est toutefois pas réalisable en général si les bases ne sont pas synchronisées.
- Voix codée en ADPCM (Sigle anglais correspondant à Modulation par impulsion et codage différentiel adaptatif). C'est une méthode de codage des fichiers sonores à 32 kbit/s selon G.726.
- Chiffrage activable pour assurer une plus grande confidentialité.

MODULATION GSFK

Les signaux passent dans un filtre Gaussien (G) avant de transiter par le modulateur SFK.

SFK

C'est une modulation qui, à un élément binaire à 1, fait correspondre une déviation de fréquence positive (maximale comprise entre 140 et 175 kHz) et à un 0 une déviation négative.



Les signaux logiques sont représentés par une variation de fréquence de la porteuse.

FDMA

Frequency Division Multiple Access

C'est une technique qui à chaque message octroie une bande de fréquence.

TDMA

Time Division Multiple Access

Dans cette technique toute la bande de fréquence est allouée mais pendant un temps très court.

15 Réseaux Ethernet

15•1 Couche physique

Caractéristiques	Vitesse de transmission	10 Mbits/s
	Mode de transmission	série synchrone
	Type de transmission	bande de base, codage Manchester
	Support de transmission	câble coaxial 50 ohms ou paires torsadées
	Structure topologique	multipoints non arborescent
	Nombre de stations	1 024 max.
	Longueur maximum	500 m sans répéteur (coaxial épais) 185 m sans répéteur (coaxial fin) 100 m sans répéteur (paire torsadée)
	Long. max. entre 2 stations	2,5 km (avec répéteurs)
	Nombre max. de répéteurs	pas plus de 4 répéteurs entre deux équipements

15•2 Le RTD (*Round Trip Delay*)

Aller-retour du signal

Lors de l'émission d'une trame par une station, celle-ci écoute pendant toute la durée de l'émission afin de s'assurer qu'aucune autre trame n'entre en collision.

Le cas le plus critique se situe lorsqu'on émet la trame la plus courte sur le réseau (64 octets).

On calcule donc le temps mis par la trame pour faire un aller / retour sur le réseau avec Q = nombre de bits transmis.

$$T = \frac{Q}{\text{Débit}} = \frac{64 \times 8}{10 \times 10^6} = 51,2 \mu\text{s} \text{ avec } Q = \text{nombre de bits transmis.}$$

CONCLUSION

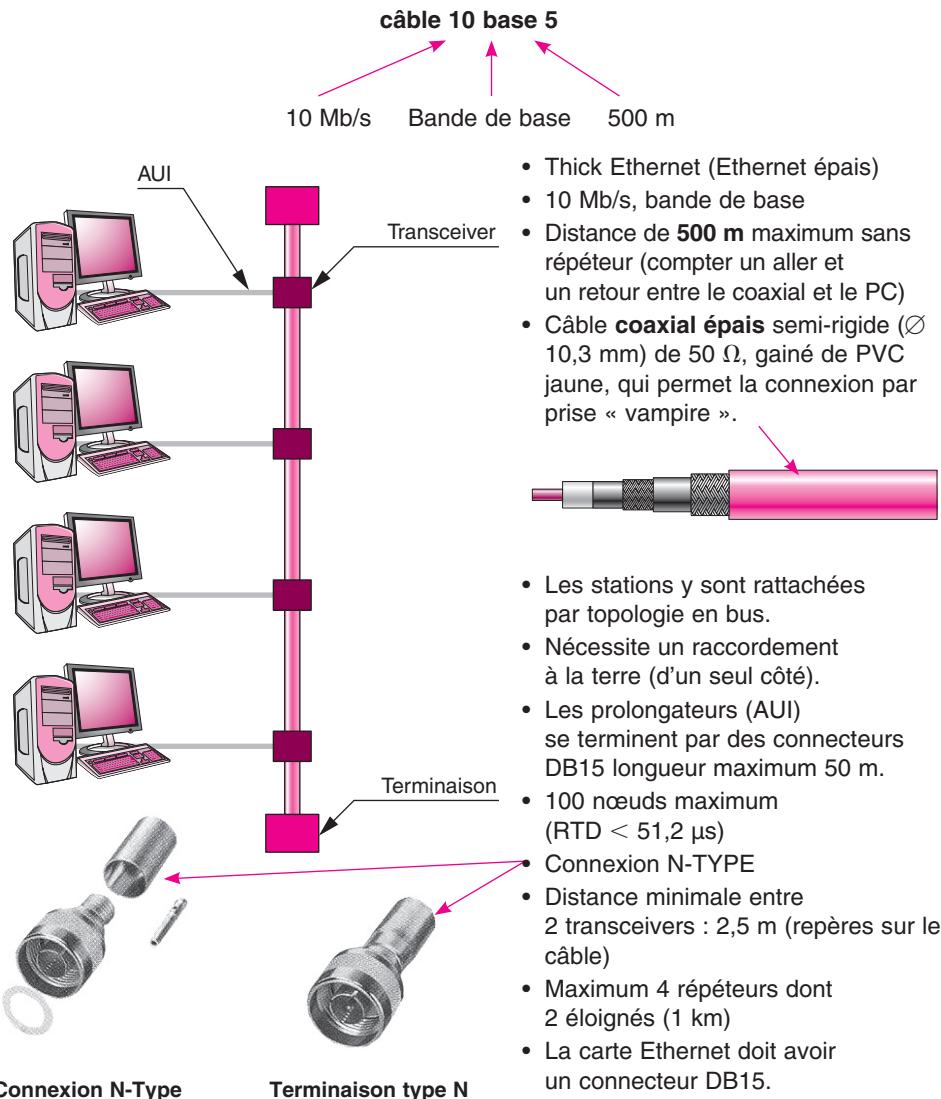
La durée d'un **aller / retour du signal** entre deux points extrêmes doit toujours être inférieure à 51,2 µs. Cette durée est le **RTD**.

C

Les réseaux et les serveurs

15•3 Différents types de réseaux Ethernet

10 Base 5



Les transceivers

Ils peuvent être équipés de prises type N ou de prises vampire.
La prise vampire permet de connecter un transceiver sur le coaxial sans le couper (il faut alors percer la gaine et l'isolant pour permettre l'établissement des contacts).



Transceiver avec prise type N



Transceiver avec prise vampire

Réseaux Ethernet

- 10 Mb/s, bande de base.
- Distance de **185 m** maximum sans répéteur.
- Câble **coaxial fin** (\varnothing 4,6 mm) de 50Ω , dit « coaxial noir » appelé également *Cheapernet*. Les stations y sont rattachées par topologie en bus.
- Vitesse de propagation : 0,65 c.
- Ne nécessite pas de raccordement à la terre.
- 30 nœuds maximum (RTD < 51,2 μ s).
- Connexion BNC.

10 Base 2



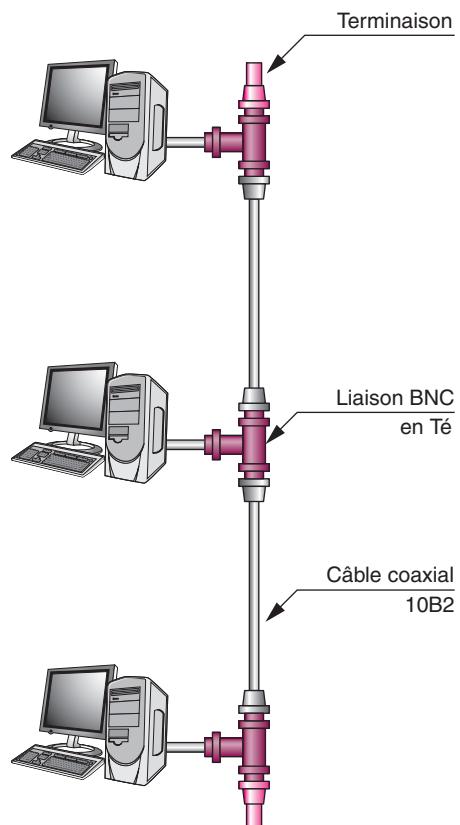
Terminaison 10 base 2



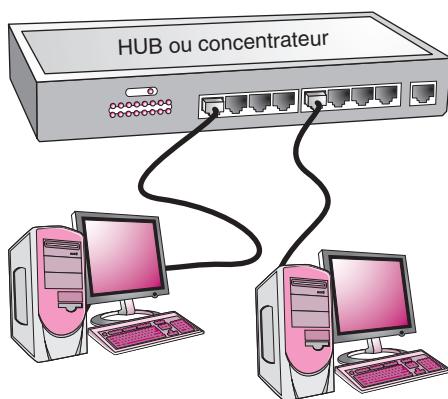
Té 10 base 2



Cordon 10 base 2



10 Base T



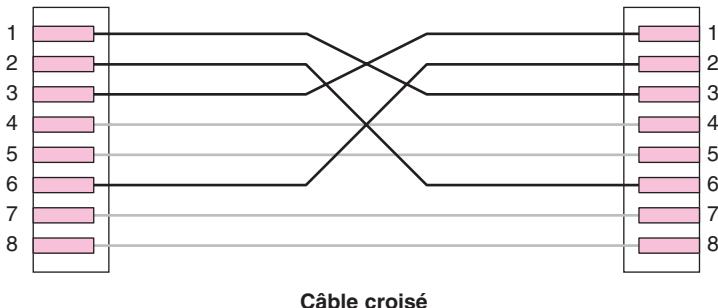
Connecteur RJ 45

- 10 Mb/s.
- Bande de base.
- Câble sur **paires torsadées téléphoniques non blindées** (UTP).
- Câblage d'Ethernet en étoile au moyen de hubs.
- Distance de 100 m maximum sans répéteur. Il contient 2 paires (émission et réception)
- 5 segments maximum (RTD < 51,2 μ s).
- Connexion sur prise RJ 45.
- Le hub est généralement équipé de LED indiquant l'état de la liaison avec la station.

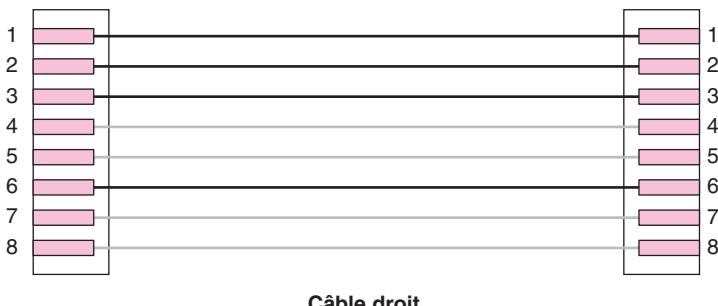
Broche n°	SIGNAL
1	Tx+
2	Tx-
3	Rx+
6	Rx-
4 & 5	Réservés au téléphone

10 Base T
(suite)**CÂBLE DROIT OU CÂBLE CROISÉ ?**

Si on relie directement deux ordinateurs sans passer par un HUB, il faudra utiliser un câble croisé afin que la paire émission de la machine 1 soit reliée à la paire réception de la machine 2 et vice versa.

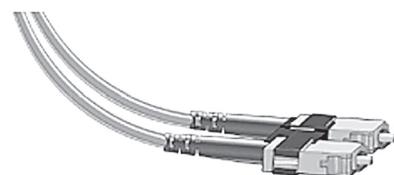


Si on relie plus de deux machines on utilisera alors un HUB ; il faudra employer des câbles droits, le croisement étant réalisé par le HUB.



Types de connecteurs

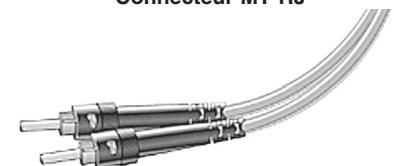
- FOIRL (*Fiber Optic Inter Repeater Link*) (ancien standard) : portée 1 km.
- 10 base FL (*Fiber Link*) : portée 2 km.
- 10 base Fb (*Fiber backbone*) : liaison inter-répéteurs.
- 10 base Fp (*Fiber passive*) : segment optique passif.
- Connecteur ST ou SMA
Il faut une fibre émission et une fibre réception (2 fibres par liaison).
C'est aussi un standard pour l'interconnexion de réseaux locaux.
La fibre optique transportant de la lumière, il n'y a pas de problèmes de masse ni d'isolation aux champs magnétiques.
- On emploie des fibres multimodes (à saut d'indice 50 Mb/s maximum ou à gradient d'indice 1 Gb/s) ou monomode.



Connecteurs SC



Connecteur MT-RJ



Connecteurs ST

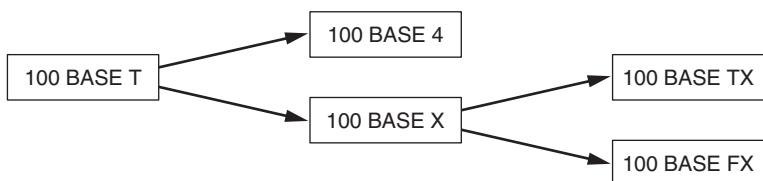
15•4 Ethernet 100 Mb/s ou Fast Ethernet

15•4•1 Présentation

Les différents supports normalisés

- Le principe d'accès reste, comme en 10 Mb/s, le CSMA/CD.
- Il a été normalisé IEEE 802.3u.
- Il existe plusieurs types de réseaux 100 Mb/s suivant le support utilisé.

15•4•2 Supports normalisés 100 Base T



Les différents supports normalisés (suite)

100 BASE 4

- Câble UTP catégorie 3 ou 4.
- Utilisation de 4 paires.
- Codage 8B6T (8 bits pour 6 transmissions).

100 BASE TX

- Câble UTP catégorie 5.
- Utilisation de 2 paires.
- Codage 4B/5B.
- 100 m maximum.

100 BASE FX

- 2 fibres optiques multimodes à gradient d'indice.
- Codage 4B/5B.

15•4•3 Les HUBs

Généralités

LES HUBS DE CLASSE I

- Peuvent relier des câblages différents.
- Pas de mise en cascade.

LES HUBS DE CLASSE II

- Relient des câblages de même type.
- Temps de transfert plus court que les HUBs de classe I.
- Nombre maximum de HUBs entre 2 nœuds : 2.
- Il faut utiliser des HUBs empilables de manière à ce que la pile obtenue ne compte que pour un seul HUB.

15•4•4 RTD et diamètre de collision

Diamètres des domaines de collision

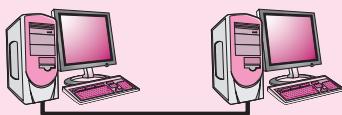
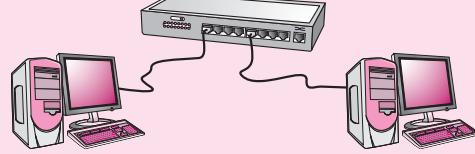
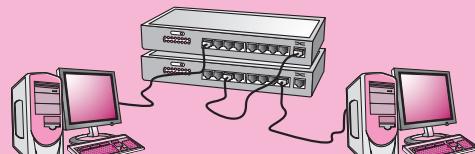
LE RTD

En 10 Mb/s le RTD était de 51,2 µs, en 100 Mb/s il sera de **5,12 µs**.

LES DIAMÈTRES DE COLLISION

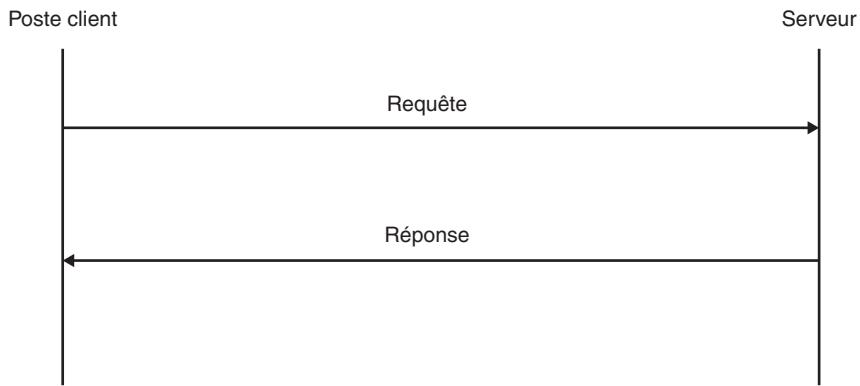
Diamètres des domaines de collision

Diamètres
des domaines
de collision
(suite)

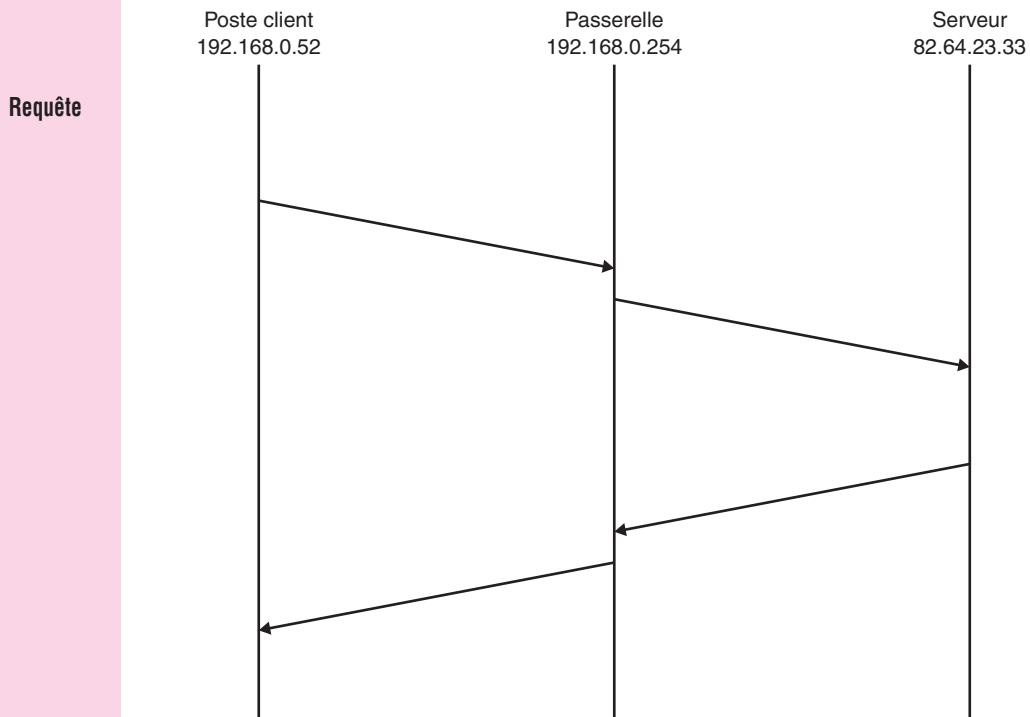
	Cuivre	Fibre	T4 + TX	TX + FX
	100 m	412 m		
1 hub classe I 	200 m	272 m	231 m	260 m
1 hub classe II 	200 m	320 m		308 m
2 hubs classe II 	205 m	228 m		216 m

16 Les serveurs

Un serveur est un système électronique en mesure de distribuer de l'information à un ou plusieurs postes appelés clients. Le poste client effectue une requête au serveur. En retour, il reçoit l'information demandée.



Entre le poste client et le serveur, il est fréquent que s'intercalent différents dispositifs. Le temps de propagation peut être mis en évidence par une flèche oblique : l'axe des temps est en ordonnée. Sur l'axe horizontal on place le matériel.



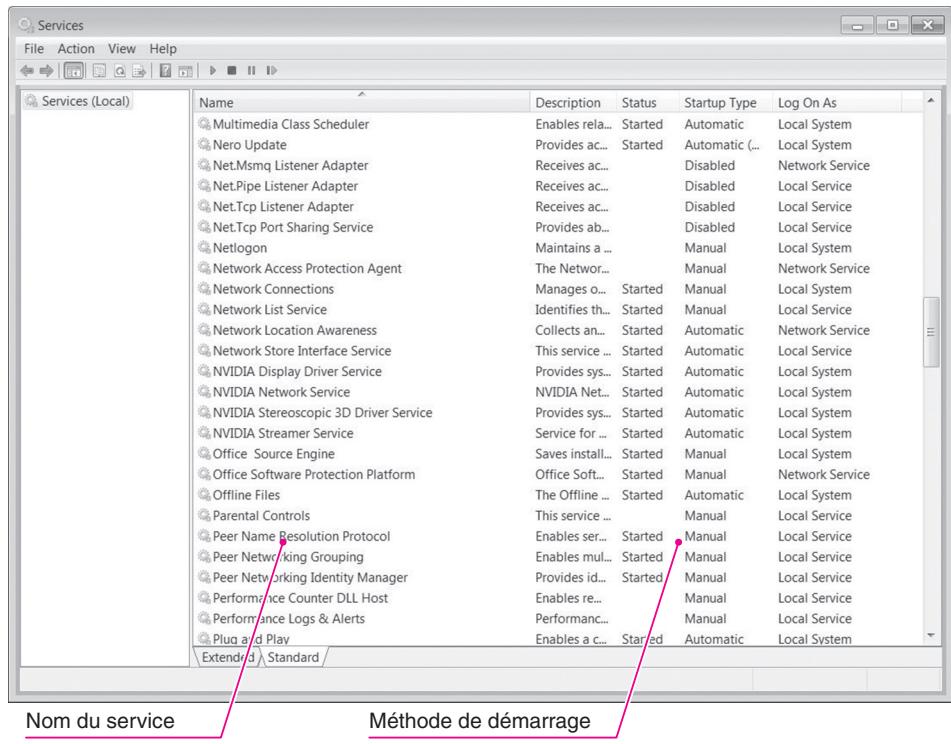
En dessous de chaque matériel, on précise l'adresse IP correspondante. Sur une même machine, un serveur fournit généralement plusieurs services (partage de fichiers, partage d'imprimantes, accès aux pages Web, courrier électronique...).

C

Les réseaux et les serveurs

16•1 Services

Les services sont des applications fonctionnant sur un serveur. Sous l'invite de commande Windows, la commande NET START permet d'afficher leur liste. On peut aussi lancer l'exécutable services.msc pour en obtenir une représentation graphique.



Name	Description	Status	Startup Type	Log On As
Multimedia Class Scheduler	Enables rela...	Started	Automatic	Local System
Nero Update	Provides ac...	Started	Automatic (...)	Local System
Net.Msmq Listener Adapter	Receives ac...	Disabled	Network Service	
Net.Pipe Listener Adapter	Receives ac...	Disabled	Local Service	
Net.Tcp Listener Adapter	Receives ac...	Disabled	Local Service	
Net.Tcp Port Sharing Service	Provides ab...	Disabled	Local Service	
Netlogon	Maintains a ...	Manual	Local System	
Network Access Protection Agent	The Networ...	Manual	Network Service	
Network Connections	Manages o...	Started	Manual	Local System
Network List Service	Identifies th...	Started	Manual	Local Service
Network Location Awareness	Collects an...	Started	Automatic	Network Service
Network Store Interface Service	This service ...	Started	Automatic	Local Service
NVIDIA Display Driver Service	Provides sys...	Started	Automatic	Local System
NVIDIA Network Service	NVIDIA Net...	Started	Automatic	Local System
NVIDIA Stereoscopic 3D Driver Service	Provides sys...	Started	Automatic	Local System
NVIDIA Streamer Service	Service for ...	Started	Automatic	Local System
Office Source Engine	Saves install...	Started	Manual	Local System
Office Software Protection Platform	Office Soft...	Started	Manual	Network Service
Offline Files	The Offline ...	Started	Automatic	Local System
Parental Controls	This service ...	Manual	Local Service	
Peer Name Resolution Protocol	Enables ser...	Started	Manual	Local Service
Peer Networking Grouping	Enables mul...	Started	Manual	Local Service
Peer Networking Identity Manager	Provides id...	Started	Manual	Local Service
Performance Counter DLL Host	Enables re...	Manual	Local Service	
Performance Logs & Alerts	Performanc...	Manual	Local Service	
Plug and Play	Enables a c...	Started	Automatic	Local System

Liste des services sous Windows

Sous Linux, le terme service est rarement employé au profit du mot daemon. La liste des services réseau s'obtient par la ligne de commande suivante :

netstat -a

Le répertoire /etc/rc.d/init.d contient un ensemble de scripts permettant de démarrer les différents daemons.

/etc/rc.d/init.d/network start permet par exemple de démarrer le service réseau. On peut remplacer start par stop pour effectuer un arrêt. En choisissant restart on force le redémarrage du service en question. On peut aussi utiliser à la place des commandes précédentes celles-ci qui assurent un rôle équivalent :

service network start

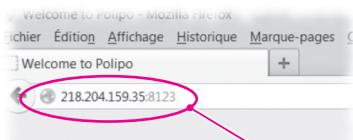
service network stop

service network restart

16•2 Ports

Si on utilise par exemple un même ordinateur pour consulter des pages Web et pour travailler avec un logiciel de messagerie, on peut se demander comment le système arrive à diriger les flux de données à la bonne application. En effet, l'ordinateur ne possède qu'une seule adresse IP. Il est donc indispensable d'avoir un autre élément permettant d'assurer un lien entre un paquet reçu et son application à laquelle il est destiné. Cette opération s'effectue grâce au PORT. Un port n'est rien d'autre qu'un numéro codé sur 16 bits intégré au paquet IP. En pratique il est compris entre 1 et 65535.

Par défaut votre navigateur utilise pour les pages Web le port 80. On peut très bien écouter sur un autre port en le précisant tout simplement dans la barre d'URL du navigateur. Pour les pages sécurisées, il est d'usage de faire appel au port 443 ou de s'appuyer sur un port libre tel que par exemple 8080.



Welcome to Polipo

[The Polipo manual.](#)

[The configuration interface.](#)

URL représentée sous la forme d'une adresse IP suivie de son numéro de port

netstat (suite)

La commande netstat fonctionnant aussi bien sous Linux que Windows permet d'obtenir des informations intéressantes. Par exemple son option –b sous Windows facilite le repérage des applications associées aux différents ports.

```
C:\Windows\system32>netstat -b
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1052	Poste27:65000	ESTABLISHED
[thunderbird.exe]			
TCP	127.0.0.1:1198	Poste27:1197	
[thunderbird.exe]			Le logiciel de messagerie fait appel au port 1198
TCP	127.0.0.1:1258	Poste27:1259	
[firefox.exe]			ESTABLISHED
TCP	127.0.0.1:1259	Poste27:1258	
TCP	127.0.0.1:23401	Poste27:1241	
TCP	127.0.0.1:23401	Poste27:1245	Ici, le « Poste27 » correspond au poste local. Thunderbird utilise aussi le port 1259

C

Les réseaux et les serveurs

16•2•1 Les principaux ports

Sous Linux, pour observer les ports ouverts, on peut s'appuyer sur la commande `ss` et ses options `a`, `l`, `n`, `p`, `u` et `t`.

Le tableau ci-dessous met en avant quelques-uns des principaux ports utilisés.

Port	Description
20	Données FTP (transfert de fichiers)
21	Commandes FTP
22	SSH (sécurité)
23	Telnet
25	SMTP (courrier électronique)
43	Whois
53	DNS (nom de domaine)
69	TFTP (transfert de fichiers)
80	HTTP (Pages Web)
110	POP3 (courrier électronique)
119	NNTP (usenet)
143	IMAP4
443	HTTPS (Pages Web sécurisées)
513	Connexion à distance
531	Chat
1521	Base de données Oracle
3306	MySQL (Base de données)
5060	SIP (établissement d'une communication téléphonique)
8080	http (serveur cache Web)

nmap

Sous Windows, la liste des ports utilisés est placée dans le fichier `\Windows\System32\drivers\etc\services`. Sous Linux, on consultera le fichier `/etc/services`.

L'écoute de ports peut être effectuée à l'aide de la commande Linux `nmap`.

```
nmap -sT 127.0.0.1
```

On peut aussi faire appel à la commande Linux `ss` :

```
ss -ap
```

Affiche tous les ports

Indique le processus associé

Les numéros de ports (source et destination) sont inscrits au début du segment TCP ou UDP.

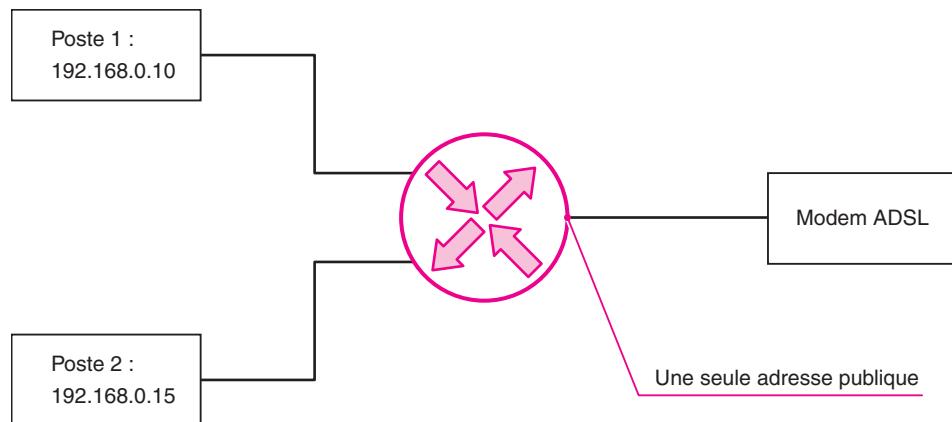
TCP est un protocole fiable agissant en mode connecté appartenant à la couche transport du système OSI.

UDP est un protocole non-fiable, c'est-à-dire qu'il accepte un certain nombre d'erreurs. Par rapport à TCP il présente une vitesse de transfert plus grande.

16•2•2 Redirections d'adresses et de ports

Pour connecter plusieurs postes informatiques sur Internet avec une seule adresse publique, il est nécessaire de procéder à une translation d'adresses (NAT pour *Network Address Translator*) . Cette opération est effectuée par le routeur.

NAT



La redirection de port permet de rediriger une communication venue de l'extérieur sur un poste local précis. Par exemple, tous les flux de données entrant sur le port 80 seront redirigés sur le poste local servant de serveur Web. L'adresse IP de ce dernier est précisée au niveau du routeur.

On peut aussi prévoir d'autres scénarios en matière d'utilisation. Une batterie de serveurs Web tous configurés sur le port 80 seront accessibles par exemple de l'extérieur à partir d'une même adresse publique mais avec des ports différents.

16•3 Serveurs de noms de domaines

DNS

Pour accéder à un serveur Web, on entre généralement une URL constituée d'un nom de domaine. On peut dans certaines situations le remplacer en faisant directement appel à l'adresse IP du serveur.

Internet repose sur le protocole TCP/IP ; les serveurs comme les autres dispositifs en réseau sont identifiables à l'aide de leur adresse IP. Afin d'accéder à un système à partir d'un nom de domaine, il a fallu créer un annuaire faisant correspondre chaque domaine à une adresse IP. Cette opération est réalisée à partir d'un serveur DNS (*Domain Name Server*) que l'on peut assimiler à un véritable annuaire.

L'utilisation d'un serveur DNS à la place de la saisie d'une adresse IP présente plusieurs avantages :

- il est généralement plus facile de mémoriser un nom de site que son adresse IP ;
- le changement d'adresse IP du serveur lors d'opérations de maintenance est transparent pour l'internaute ;
- l'hébergement de plusieurs sites sur un même serveur est envisageable.

On peut toutefois noter une difficulté supplémentaire importante : la mise en place de systèmes intermédiaires ouvre la porte à de nouvelles attaques. On peut citer par exemple la technique du phishing qui consiste à rediriger l'utilisateur vers un autre site. Cette redirection s'effectuant au niveau du serveur DNS, même avec un système à jour, l'internaute n'est pas à l'abri d'une telle pratique.

whois

Le système de noms de domaines est hiérarchisé ; dans une URL, le point permet de passer d'un niveau à l'autre : « org », « com » et « fr » représentent trois sous-domaines.

Pour effectuer des recherches sur les bases de données de noms de domaines, on peut interroger différents organismes. L'AFNIC propose en ligne l'accès aux bases de données de noms de domaines en .fr en s'appuyant sur l'outil « whois ». Elle restreint toutefois l'accès à certaines informations personnelles et interdit une interrogation massive.

L'achat d'un nom de domaine implique de vérifier au préalable sa disponibilité. Il entraîne des coûts facturés à l'année. Pour obtenir un .fr, il suffit d'une simple adresse en Europe. D'autres pays adoptent des règles différentes distinguant les particuliers, les professionnels et les ressortissants étrangers. Par exemple la Norvège impose d'être norvégien pour l'obtention d'un .no. Les étrangers peuvent toutefois obtenir un .co.no. On appréciera pour ce pays souvent montré en exemple en matière économique sa distinction des sites professionnels des particuliers : .no pour les entreprises et .priv.no pour les particuliers. De telles différences peuvent justifier des variations de tarifs d'une extension à l'autre.

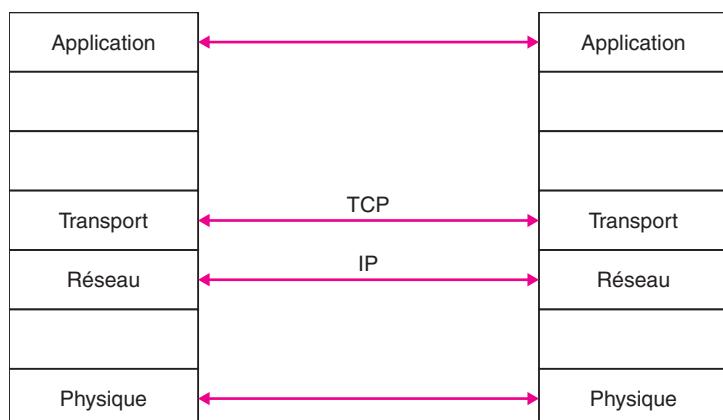
Afin d'améliorer sa visibilité sur Internet, il est possible de faire l'acquisition de plusieurs domaines et de les rattacher à une même machine.

Bind est une application permettant de mettre en place son propre serveur DNS. On peut aussi mettre en place un DNS local en faisant tout simplement usage du fichier host présent sur les systèmes Windows et Linux. En renseignant la table host, on peut améliorer la vitesse de résolution de noms de domaines et bloquer ou rediriger facilement des sites.

16•4 Serveur Web

Apache

La communication entre un navigateur Web et un serveur http est représentée par le diagramme suivant modélisant les couches OSI et les interactions mises en œuvre :



Le protocole **HTTP** employé pour émettre et recevoir des requêtes est décrit dans le document **RFC 2616**.

Pour une mise en place complète d'un serveur Web, le lecteur se reportera au premier chapitre de l'ouvrage « *La pratique de l'électronique sur systèmes numériques – Tome 2* ; Vincent Breton – Editions Casteilla ».

16•5 Serveur de fichiers (FTP)

FTP

Le **FTP** (*File Transfer Protocol*) est un protocole de transfert de fichiers permettant d'assurer la création, la copie ou le déplacement de fichiers sur un réseau **TCP/IP** en mode **TCP**. Un port est dédié aux commandes FTP (port 21) et l'autre (port 20) est réservé au transport des données.

Sous Windows et sous Linux il est possible de dialoguer à l'aide de l'interpréteur de commandes et de l'outil FTP. Le document **RFC 959** décrit le protocole FTP.

Pour une mise en place complète d'un serveur FTP, le lecteur se reportera au deuxième chapitre de l'ouvrage « *La pratique de l'électronique sur systèmes numériques – Tome 2 ; Vincent Breton – Editions Casteilla* ».

16•6 Serveur de courrier électronique (SMTP)

SMTP

Les serveurs de courrier électronique utilisent plusieurs protocoles. Pour l'envoi de courrier on fait généralement appel au protocole **SMTP** (*Simple Mail Transfer Protocol*) décrit dans la **RFC 2821**.

Pour la réception de courriers électroniques, les applications clientes s'appuient sur le protocole **POP3** décrit dans la **RFC 1939**. Le protocole **IMAP** décrit dans la **RFC 3501** offre de nouvelles possibilités en permettant par exemple la manipulation des courriers électroniques situés sur le serveur.

Pour la sécurisation des données, les outils de messagerie sont souvent couplés avec le protocole de cryptage SSL (TLS).

16•7 Serveur d'impression

Samba

Le serveur d'impression vise à faire partager une ou plusieurs imprimantes par différents utilisateurs. Dans un parc hétérogène on peut citer le serveur Samba capable de mettre à disposition de stations Windows et Linux une même imprimante. Samba offre aussi la possibilité de partager des fichiers. Il repose sur le protocole **SMB** (*Server Message Block*).

Dans sa dernière version, la norme SMB est décrite dans un document comptant pas moins de 441 pages.

Pour une intégration plus simple et plus rapide d'une solution de serveur d'impression, on pourra se tourner vers la solution CUPS développée par Apple. CUPS repose sur le protocole **IPP** (*Internet Printing Protocol*) décrit dans la **RFC 2911**. IPP s'appuie sur le protocole HTTP. L'installation et le paramétrage d'une nouvelle imprimante sont facilités par une interface Web.

L'accès à la console d'administration s'effectue à l'aide de l'URL suivante :

<http://localhost:631/admin>

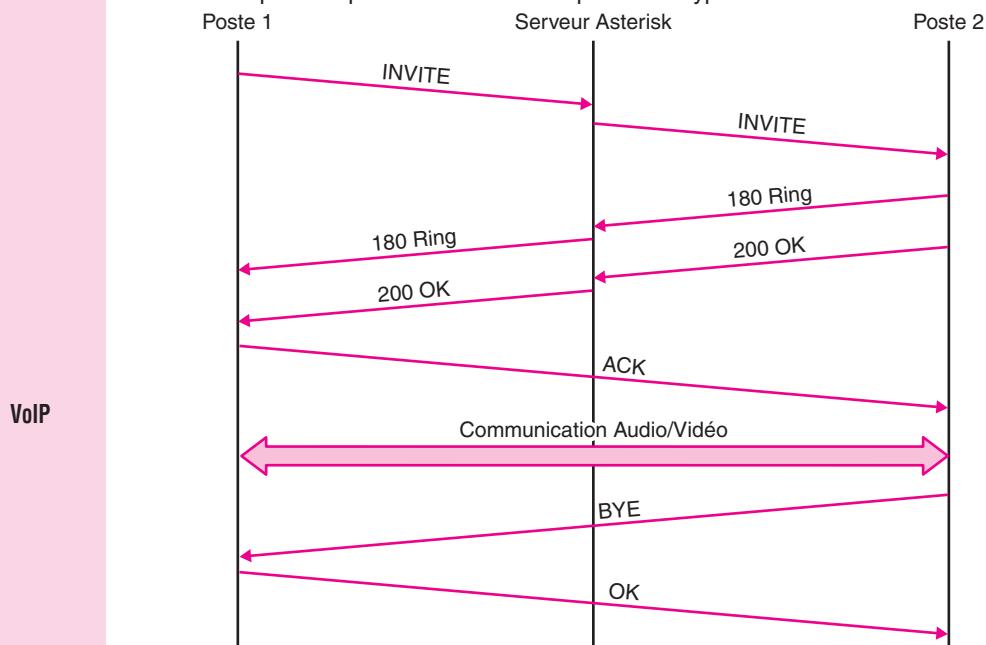
Avec un serveur d'impression, on privilégiera des gestionnaires d'imprimantes au format PostScript car il est alors possible d'effectuer des modifications automatiques intéressantes comme par exemple le changement d'échelle automatique ou la conversion au format PDF. L'écriture de scripts et leur mise en place au niveau du serveur d'impression accroissent les capacités de l'ensemble.

16•8 Serveur de téléphonie

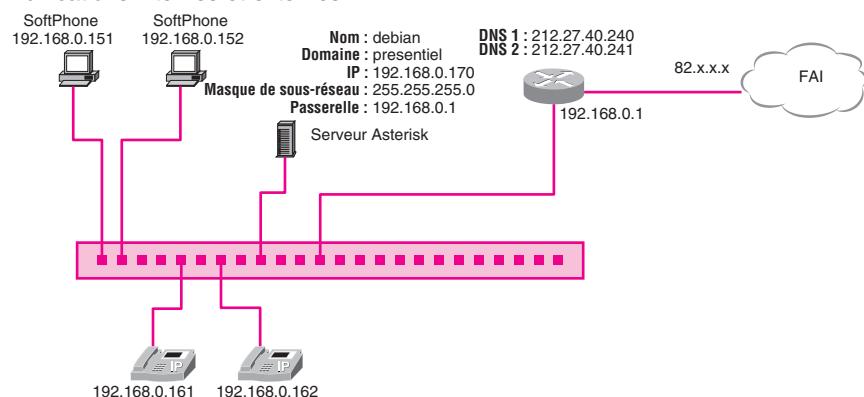
La VoIP (*Voice Over Internet Protocol*) ou « Voix sur IP » repose sur plusieurs protocoles incluant aussi bien le transfert de la voix que de la vidéo. Les systèmes de téléphonie par Internet reposent sur la VoIP et font généralement appel au protocole **SIP** (*Session Initiation Protocol*) chargé d'établir et de gérer les sessions.

Contrairement à ce que laisse supposer l'acronyme SIP, ce protocole appartient à la couche application. Pour le transport de l'audio et de la vidéo, la norme H.323 dérivée de la norme H.320 est très souvent employée. Le diagramme ci-dessous représente une communication entre deux postes faisant appel à un serveur de téléphonie. Les commandes et les messages représentés font partie du protocole SIP.

L'initialisation d'une communication téléphonique via le réseau Internet entre deux usagers s'effectue en passant par un serveur de téléphonie de type Asterisk.



Le plan de câblage représenté ci-dessous fournit un exemple d'installation permettant les communications internes et externes.



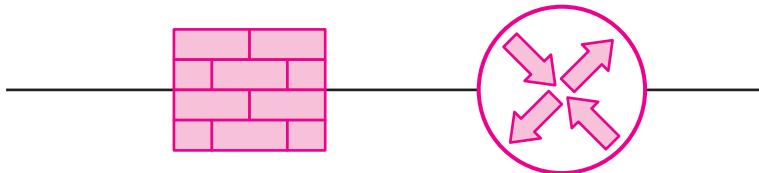
Le système IVR

16.9 Les pare-feu

Il existe deux grandes catégories de pare-feu (*firewall*) :

- les pare-feu matériel ;
- les pare-feu logiciel.

Dans tous les cas de figures, le pare-feu agit comme un filtre. Avec les pare-feu matériel, les données transitant par un port ou une adresse IP déterminée au préalable sont exclues du trafic. Le pare-feu logiciel agit sur l'analyse du paquet et en fonction des signatures préenregistrées et détectées, il rejette lui aussi des communications.



Pare-feu et routeur sont souvent intégrés dans un même boîtier.

Pare-feu matériel et pare-feu logiciel sont indissociables dans le sens où ils assurent une complémentarité au niveau du filtrage des données sur le réseau. Le pare-feu matériel se distingue par un fonctionnement transparent dans le sens où il n'influence pas les débits. Le pare-feu logiciel nécessite du temps processeur pour l'analyse détaillée du contenu des paquets entraînant ainsi un décalage ou un ralentissement dans les communications.

netfilter

Pour pallier les inconvénients respectifs des deux grandes catégories de pare-feu, certains constructeurs rassemblent les deux techniques dans un même boîtier. Les routeurs offrent bien souvent des possibilités intéressantes de pare-feu mais elles demeurent rudimentaires par rapport aux véritables solutions de filtrage.

Avec la récente affaire des écoutes de la NSA, en matière de sécurité il convient d'être vigilant sur la provenance et le choix des composants constituant les systèmes électroniques. Pour ne rien arranger au problème, la DARPA, l'Agence américaine pour les projets avancés de Défense, a réservé pas moins de 17 millions de dollars pour la conception et le développement de composants électroniques destructibles à distance ou dégradables (d'après ElectroniqueS – www.electroniques.biz – en date du 14 février 2014). Avec un Internet issu de l'ARPANET, la programmation de pannes risque bien d'être le prochain défi auquel seront confrontés les administrateurs et toutes les personnes en charge de la sécurité des équipements et des systèmes informatiques.

Pour des raisons de coût mais aussi de facilité d'installation et de configuration, l'acquisition d'un logiciel pare-feu permet de protéger rapidement son ordinateur de flux de données indésirables. En aucune manière ce type de produit ne saurait se substituer à un antivirus qui agit principalement sur l'analyse de fichiers présentant des risques d'altération ou de destruction. Windows dispose d'un pare-feu intégré mais l'utilisation de la solution OutpostPro d'Agnitum facilite la mise en place. Les utilisateurs de systèmes Linux bénéficient depuis la version 2.0 du noyau d'outils pare-feu intégrés :

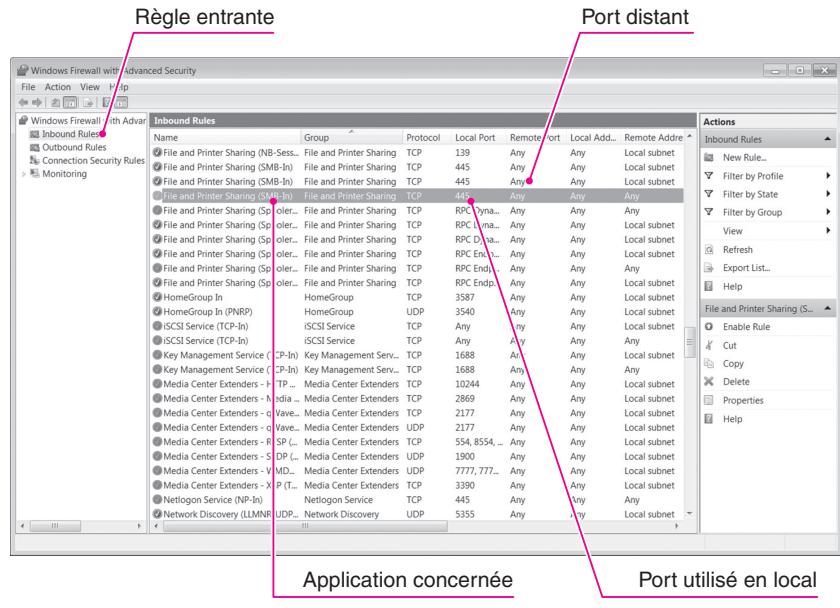
Outil pare-feu	Version du noyau Linux
ipfwadm	2.0
ipchains	2.2
netfilter	≥ 2.3

C

Les réseaux et les serveurs

Les serveurs

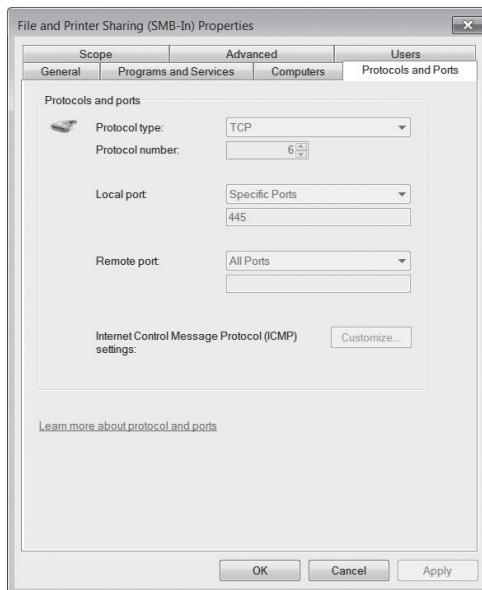
L'accès au pare-feu Windows s'effectue à partir du panneau de configuration. Pour des raisons de sécurité, on privilégiera la solution consistant à bloquer tous les ports puis à en ouvrir seulement quelques-uns.



Pare-feu logiciel intégré à Windows

Règles

Un double-clic sur la ligne souhaitée permet d'obtenir l'interface de configuration. Les règles prédéfinies ne permettent pas le changement de certains paramètres. L'onglet « Protocoles et Ports » précise le type de protocole et les ports employés. Le numéro de protocole fait référence à une classification des différents protocoles par Microsoft.



Sous Linux, la commande `root iptable` permet la mise en place des règles de filtrage.

16•10 Interface Web

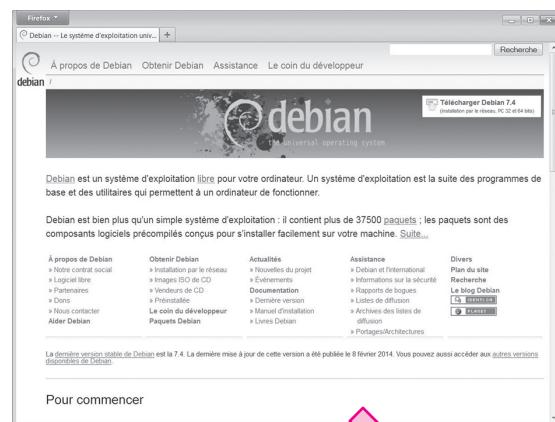
Un grand nombre d'applications s'appuient sur une interface de gestion en ligne. La consultation à distance à travers un simple navigateur Web devient possible. On peut citer par exemple les services de courrier électronique en ligne proposés par les fournisseurs d'accès internet et les registrars. Parfois l'interface Web complexifie la prise de contact ; c'est par exemple le cas avec le serveur de téléphonie Trixbox qui apporte une surcouche graphique à Asterisk. Au premier abord, l'écran peut s'apparenter à un tableau de bord d'un avion tant il y a de boutons, de zones de texte... On peut aussi citer l'exemple plus répandu de la base de données MySQL et de son Interface graphique optionnelle phpMyAdmin.

Certains ne jurent que par le mode commande, d'autres se contentent uniquement d'un environnement graphique. Pour un technicien, ce dernier est l'arbre qui cache la forêt. L'étude d'une application uniquement par son interface Web s'apparente plus à une démonstration du produit qu'à l'apprentissage réel des technologies qui en découlent.

IDENTIFICATION DES PRINCIPALES TECHNOLOGIES ASSOCIÉES À UNE PAGE WEB :

Les pages Web reposent sur le langage **HTML** défini par le W3C. Sous Firefox, un simple « **Ctrl + U** » permet d'afficher le code source d'une page.

HTML



Ctrl + U (Firefox)

```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html lang="fr">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <title>Debian - Le système d'exploitation universel</title>
  <link rev="made" href="mailto:root@devel.ardorid.debian.org">
  <meta name="Generator" content="WML 2.0.12 (16-Apr-2008)">
  <meta name="Modified" content="2014-03-04 23:49:54" type="text/wml">
  <meta name="viewport" content="width=device-width" type="text/wml">
  <meta name="author" content="Aldo Deblieck" type="text/wml">
  <meta name="HandheldFriendly" content="true" type="text/wml">
  <link rel="alternate" type="application/rss+xml" title="Actualités Debian" href="News/news" type="text/rss" />
  <link rel="alternate" type="application/rss+xml" title="Nouvelles du projet Debian" href="News/weekly/dwn" type="text/rss" />
  <link rel="alternate" type="application/rss+xml" title="Annonces de sécurité Debian (résumé)" href="security/dsa-long" type="text/rss" />
  <link href="/debhome.css" rel="stylesheet" type="text/css" media="all" />
  <link href="/debian-fr.css" rel="stylesheet" type="text/css" media="all" />
  <link rel="shortcut icon" href="favicon.ico" />
  <meta name="Keywords" content="debian, GNU, linux, unix, open source, libre, DFSG" />
  <link rel="search" type="application/opensearchdescription+xml" title="Recherche sur le site web Debian" href=".search.fr.xml" />
</head>
<body>
  <div id="header">
    <div id="upperheader">
      <div id="logo">
        <a href="/" title="Accueil Debian"></a>
      </div>
      <div id="logos">
        <div id="searchbox">
          <form name="p" method="get" action="http://search.debian.org/cgi-bin/omega">
            <input type="text" name="q" value="" />
          </form>
        </div>
      </div>
    </div>
  </div>

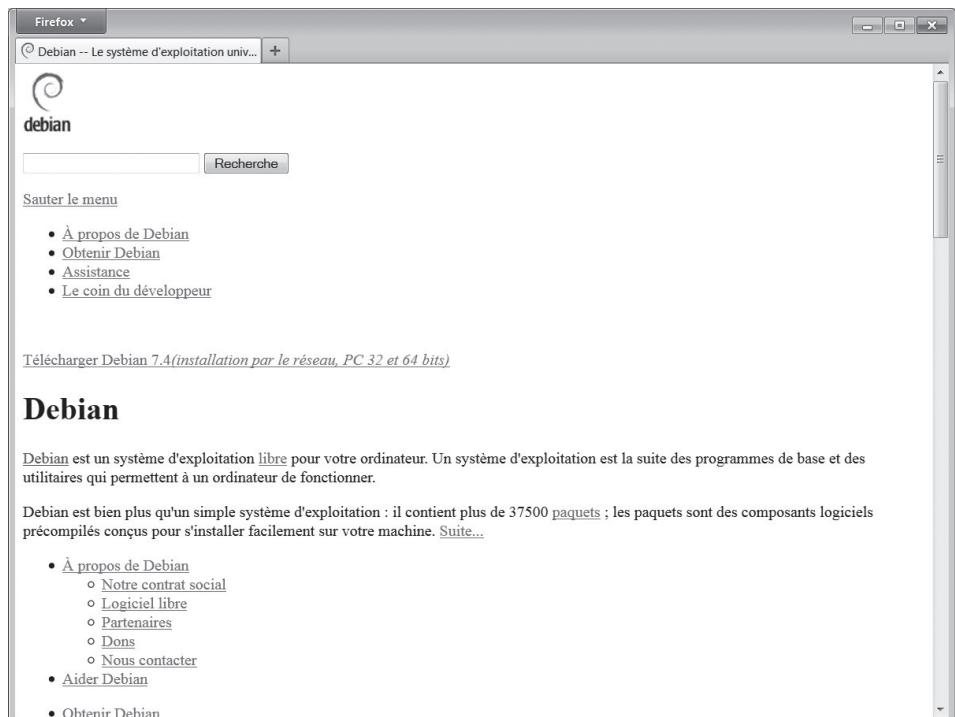
```

Ligne 2, Colonne 14

Dans les premières lignes d'un fichier source HTML, le mot « **stylesheet** » montre la présence d'une feuille de style associée à la page écrite en **CSS** (*Cascading style sheets*). Les éléments du CSS sont définis par le W3C.

```
<link href=>./debian-fr.css> rel=>stylesheet type=>text/css media=>all>>
```

L'affichage d'une page Web sans la technologie CSS est facilement réalisable. En la désactivant il est ainsi possible de se rendre compte de son influence



Page d'accueil du site Debian sans sa feuille de style

De plus en plus de sites Web utilisent le langage JavaScript permettant d'étendre les possibilités d'HTML. JavaScript permet de créer des boucles. Il est aussi capable de modifier les propriétés du CSS. Pour une exécution du code au niveau du serveur, le langage Php est souvent employé. En retour, le navigateur reçoit des pages HTML.

Au niveau de la sécurité, l'usage d'un front-end plus connu sous le terme d'interface en ligne, matérialisé par un formulaire, pose de nouvelles difficultés : injection de code et phishing mettent en danger les données personnelles de l'utilisateur ainsi que celles des autres. Pour s'en prémunir, tout administrateur digne de ce nom doit bannir la plupart des opérations d'administration et de maintenance des serveurs par la voie d'une interface en ligne et se limiter à la ligne de commande. Loin d'être une limite, la ligne de commande apporte davantage de sécurité tout en allant plus loin comme par exemple la création de fichiers batch.

On retrouve aussi l'usage d'interfaces en ligne dans les outils de blog et de CMS comme par exemple Wordpress et Spip.

16•11 Les machines virtuelles

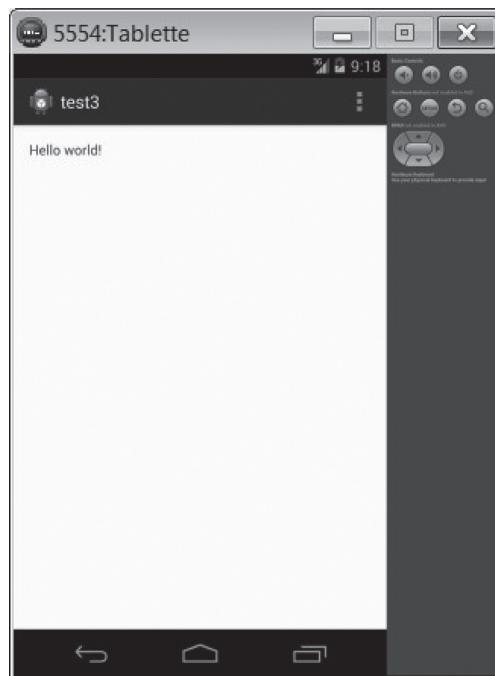
Android

Les machines virtuelles permettent de disposer de plusieurs systèmes d'exploitation en même temps. Que ce soit par le réseau ou par le partage d'un périphérique, la communication d'un système à l'autre devient envisageable. Un autre avantage indéniable réside dans le gain de place car un seul ordinateur suffit.

Faire tourner une machine virtuelle nécessite un peu d'espace mémoire. 2 Go de RAM est un minimum pour travailler avec l'environnement graphique des distributions Linux actuelles. Pour faire cohabiter une deuxième machine virtuelle, mieux vaut prévoir tout de suite 4 Go. Chaque machine virtuelle se présente sous la forme d'un fichier de la taille de son disque virtuel. Plus il y a de machines et plus l'espace disque occupé devient critique. La puissance du processeur est un élément tout aussi important.

Le déploiement de postes clients légers permet de réduire le coût global d'acquisition mais la prise à distance du bureau peut augmenter considérablement la bande passante du réseau. La démocratisation du *cloud computing* est intimement liée à l'évolution de l'infrastructure du réseau Internet. Un des éléments qui ne facilite pas son adoption est le risque lié à l'extériorisation des informations.

Un usage plus récent des machines virtuelles vise à tester le développement d'applications sur d'autres architectures. L'environnement de développement Android met à la disposition du programmeur toute une série d'appareils.



Machine virtuelle Android dans une fenêtre Windows

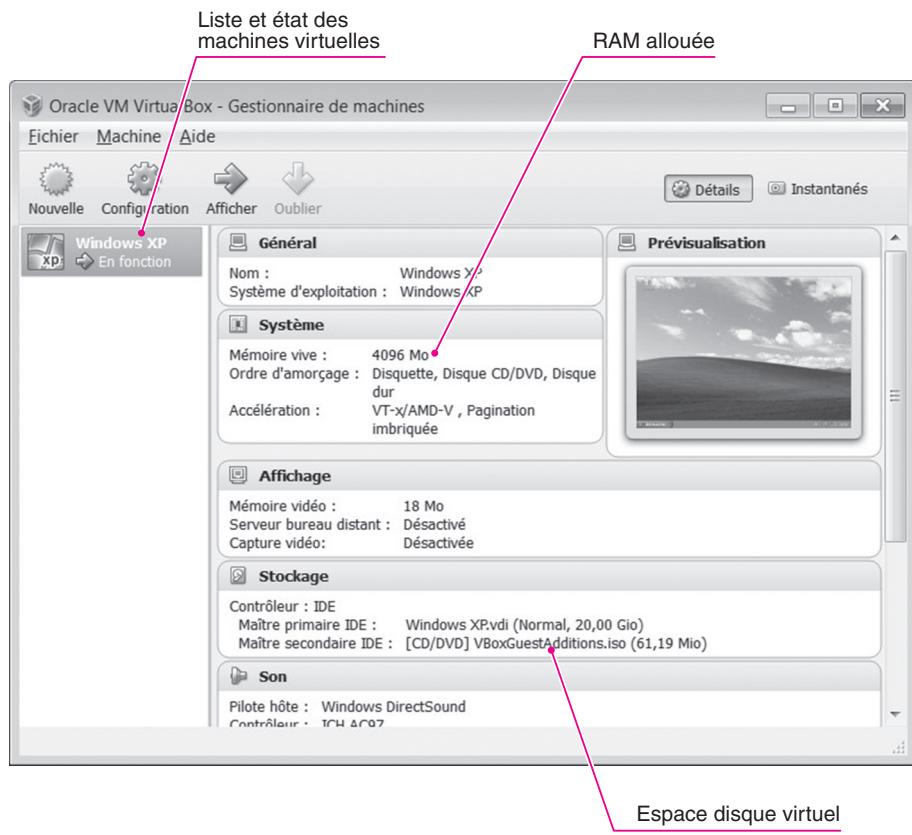
On retrouve la notion de virtualisation au sein même de certains langages comme par exemple Java. Le code généré est un pseudo code interprété par la JVM (Java Virtual Machine). Réputé à l'origine pour sa sécurité, Java est à présent pointé du doigt par la plupart des navigateurs qui lui réservent une confiance toute relative.

Les serveurs

VirtualBox

Parmi les nombreux outils de virtualisation, on peut citer Bochs, QEMU, Xen, VirtualPC, VirtualBox et VMware.

La figure ci-dessous représente le superviseur de VirtualBox chargé de gérer l'ensemble des machines virtuelles.



Des interfaces réseau virtuelles permettent de faire communiquer plusieurs machines entre elles avec la possibilité de choisir ses propres adresses MAC. Par défaut, l'interface réseau assure une translation d'adresse pour faire usage de la connexion Internet. VirtualBox propose aussi la redirection de ports.

Pour une mise en pratique d'une machine virtuelle, le lecteur se reportera au chapitre 4 de l'ouvrage « *La pratique de l'électronique sur systèmes numériques – Tome 2* ; Vincent Breton – Editions Casteilla ».

16•12 Les VLANS

VLAN = Virtual Local Area Network

16•12•1 Présentation

Généralités

- Avec les réseaux Ethernet classiques (tous les équipements recevant une trame émise sur le réseau) le nombre de collisions augmente très rapidement lorsque le nombre d'équipements s'accroît : il s'ensuit rapidement une saturation du réseau.
- Un VLAN est un groupement logique de stations ou d'utilisateurs qui forme ainsi un domaine de diffusion.
- Les VLANs sont définis par le standard IEEE 802.1Q.
- Il est réalisé à l'aide de commutateurs que l'on configure (soit par logiciel soit en mode console) pour créer des groupes.

16•12•2 Avantages des vlans

Généralités (suite)

- Sécurité accrue.
- Performances accrues.
- Mobilité des utilisateurs : les droits d'accès aux ressources restent les mêmes quel que soit l'endroit de connexion.
- Administration simplifiée.

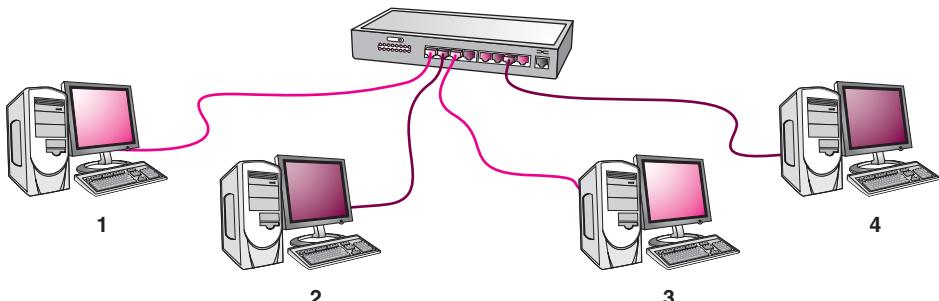
16•12•3 Différents types de vlans

DÉFINIS PAR GROUPES DE PORTS

- Toutes les stations connectées sur un port du groupe appartiennent au VLAN.
- Ce type est à utiliser quand les équipements sont raccordés directement sur les ports du commutateur.
- Les utilisateurs ne peuvent se déplacer qu'en se connectant à un port appartenant à leur VLAN.

**VLAN 1 : Ports 1, 3, 5, 8
VLAN 2 : Ports 2, 4, 6, 7**

Différents types de réseaux



Dans ce cas :

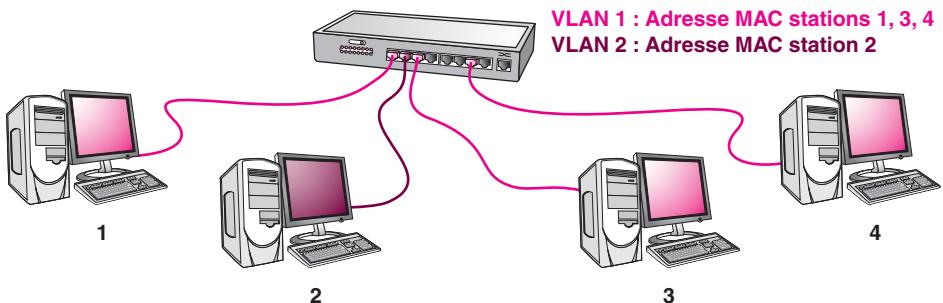
- Les stations 1 et 3 appartiennent au VLAN 1
- Les stations 2 et 4 appartiennent au VLAN 2

C

Différents types de réseaux

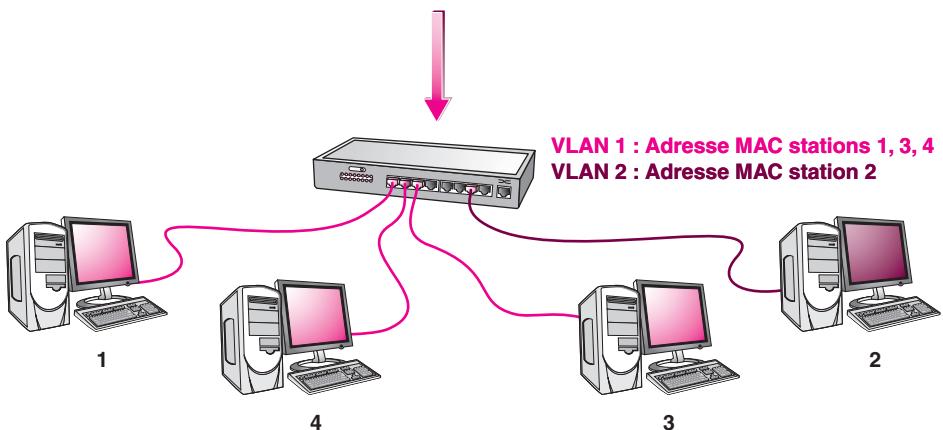
DÉFINIS PAR LES ADRESSES MAC

- Dans ce type de VLAN on peut se connecter à un port quelconque du commutateur : on fera toujours partie du même VLAN.
- Ces VLANs sont difficiles à administrer.



Dans ce cas :

- Les stations 1, 3 et 4 appartiennent au VLAN 1
- La station 2 appartient au VLAN 2

SI ON CHANGE LES STATIONS DE PORT

Dans ce cas :

- Les stations 1, 3 et 4 appartiennent toujours au VLAN 1
- La station 2 appartient toujours au VLAN 2

LES VLANs DE NIVEAU TROIS

Le VLAN est constitué de toutes les machines utilisant le même protocole de niveau 3 ou appartenant au même réseau logique.

16•12•4 Communication entre les VLANs

Différents types de réseaux (suite)

Le routage est nécessaire pour passer d'un VLAN à l'autre. On utilise alors un routeur ou un commutateur intégrant la fonction de routage. Il existe un protocole inter-VLANs : c'est NHRP (*Next Hop Resolution Protocol*).

16•13 Les réseaux virtuels : les VPNs

16•13•1 Présentation

Généralités

Il arrive souvent que des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même du personnel géographiquement éloignés via internet.

Ces réseaux locaux d'entreprise (LAN ou RLE) sont de plus en plus souvent reliés à Internet par l'intermédiaire d'équipements d'interconnexion.

Les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.

La première solution pour répondre à ce besoin de communication sécurisée consiste à relier les réseaux distants à l'aide de liaisons spécialisées.

Toutefois la plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée ; il est parfois nécessaire d'utiliser Internet comme support de transmission.

Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole d'encapsulation (en anglais *tunneling*, d'où l'utilisation impropre parfois du terme « tunnellation »), c'est-à-dire encapsulant les données à transmettre de façon chiffrée.

On parle alors de **réseau privé virtuel** (noté *RPV* ou **VPN**, acronyme de *Virtual Private Network*) pour désigner le réseau ainsi artificiellement créé.

Ce réseau est dit *virtuel* car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et *privé* car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données.

Le système de *VPN* permet donc d'obtenir une liaison sécurisée à moindre coût.

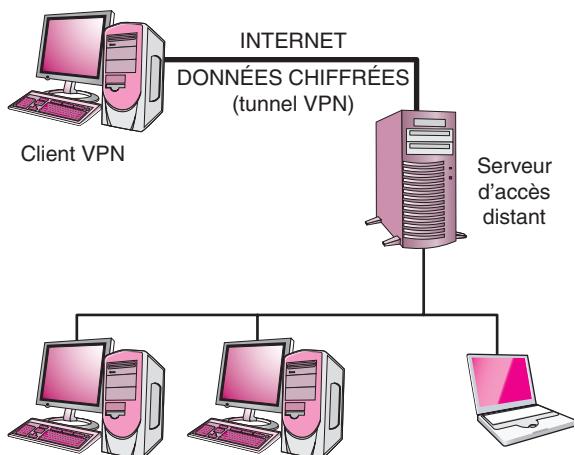
C

Les réseaux et les serveurs

16•13•2 Fonctionnement d'un VPN

Protocole de tunnellation

Un réseau privé virtuel repose sur un **protocole de tunnellation** (*tunneling*), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.



Protocole de tunnelling

Entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel.

Dans le cas d'un VPN établi entre deux machines, on appelle *client VPN* l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et *serveur VPN* (ou plus généralement **serveur d'accès distant**) l'élément chiffrant et déchiffrant les données du côté de l'organisation.

De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. À réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur ...

16•13•3 Les protocoles de tunnelling

Protocole de tunnelling (suite)

Les principaux protocoles de *tunneling* sont les suivants :

- **PPTP** (*Point-to-Point Tunneling Protocol*) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- **L2F** (*Layer Two Forwarding*) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète.
- **L2TP** (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'IETF pour faire converger les fonctionnalités de *PPTP* et *L2F*. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- **IPSec** est un protocole de niveau 3 permettant de transporter des données chiffrées pour les réseaux IP.