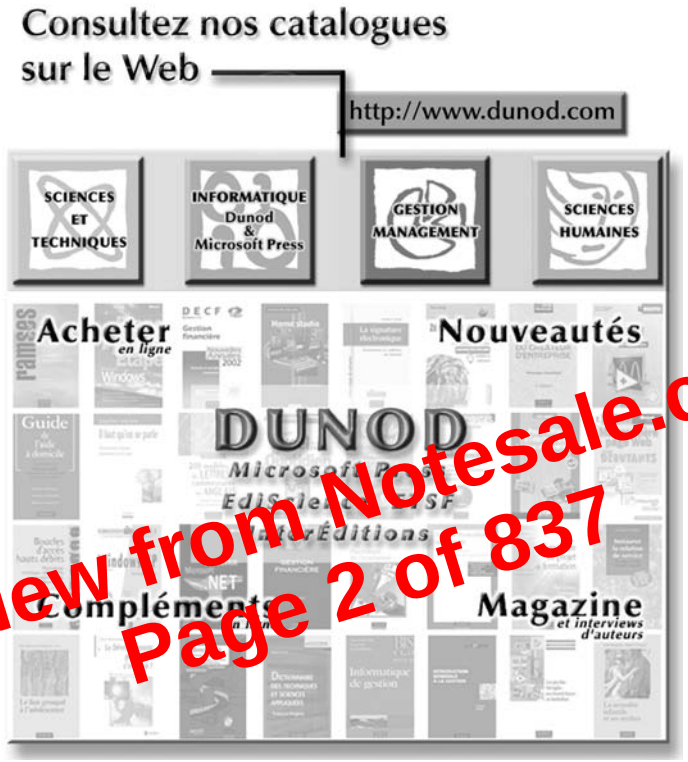
19,5x25 Page II Jeudi, 22. juin 2006 12:02 12



Preview from Notesale.co.uk
Page 2 of 837

Preview from Notesale.co.uk
Page 4 of 837

Ce pictogramme mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du **photocopillage**.

Le Code de la propriété intellectuelle du 1er juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.

Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation du Centre français d'exploitation du droit de copie (**CFC**, 20 rue des Grands-Augustins, 75006 Paris).

Nouveau tirage corrigé
© Dunod, Paris, 2003
ISBN 2 10 007986 7

Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite selon le Code de la propriété intellectuelle (Art L 122-4) et constitue une contrefaçon réprimée par le Code pénal. • Seules sont autorisées (Art L 122-5) les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, ainsi que les analyses et courtes citations justifiées par le caractère critique, pédagogique ou d'information de l'œuvre à laquelle elles sont incorporées, sous réserve, toutefois, du respect des dispositions des articles L 122-10 à L 122-12 du même Code, relatives à la reproduction par reprographie.

Preview from Notesale.co.uk
Page 32 of 837

Chapitre **2**

L'information et sa représentation dans les systèmes de transmission

Preview from Notesale.co.uk
Page 33 of 837

2.1 GÉNÉRALITÉS

2.1.1 Les flux d'information

L'acheminement, dans un même réseau, d'informations aussi différentes que les données informatiques, la voix ou la vidéo implique que chacune de ces catégories d'information ait une représentation identique vis-à-vis du système de transmission et que le réseau puisse prendre en compte les contraintes spécifiques à chaque type de flux d'information (figure 2.1).

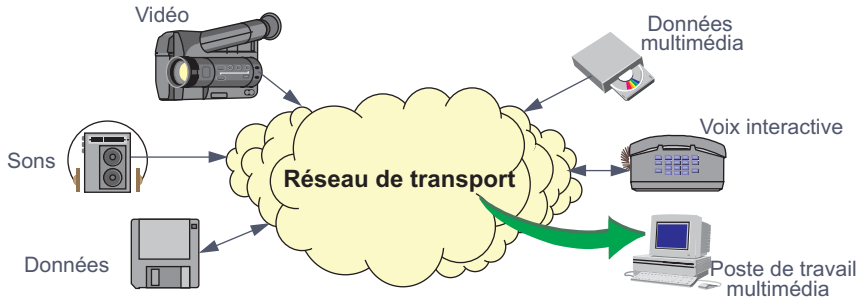


Figure 2.1 Le réseau et les différents flux d'information.

Afin de qualifier ces différents flux vis-à-vis du système de transmission, nous définirons succinctement les caractéristiques essentielles d'un réseau de transmission[1]. Nous examinerons ensuite le mode de représentation des informations. Enfin, nous appliquerons les résultats

1. Ces différentes notions seront revues et appronfondies dans la suite de cet ouvrage.

aux données, à la voix et à l'image pour en déduire les contraintes de transfert spécifiques à chaque type de flux.

2.1.2 Caractéristiques des réseaux de transmission

Notion de débit binaire

Les systèmes de traitement de l'information emploient une logique à deux états ou binaire. L'information traitée par ceux-ci doit être traduite en symboles compréhensibles et manipulables par ces systèmes. L'opération qui consiste à transformer les données en éléments binaires s'appelle le **codage** ou **numérisation** selon le type d'information à transformer.

On appelle débit binaire (D) le nombre d'éléments binaires, ou nombre de bits, émis sur le support de transmission pendant une unité de temps. C'est l'une des caractéristiques essentielles d'un système de transmission. Le débit binaire s'exprime par la relation :

$$D = \frac{V}{t}$$

avec D (débit) en bits par seconde (bit/s[2]), V le volume à transmettre exprimé en bits et t la durée de la transmission en seconde.

Le débit binaire mesure le nombre d'éléments binaires transitant sur le canal de transmission pendant l'unité de temps (figure 2.2).

Preview from Notesale.co.uk
Page 34 of 837

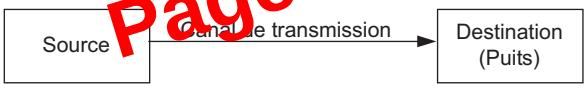


Figure 2.2 Schématisation d'un système de transmission.

Notion de rapport signal sur bruit

Les signaux transmis sur un canal peuvent être perturbés par des phénomènes électriques ou électromagnétiques désignés sous le terme générique de **bruit**. Le bruit est un phénomène qui dénature le signal et introduit des erreurs.

Le rapport entre la puissance du signal transmis et celle du signal de bruit qualifie le canal vis-à-vis du bruit. Ce rapport, appelé rapport signal sur bruit (S/N avec N pour *Noise*), s'exprime en dB (décibel[3]) :

$$S/N_{dB} = 10 \log_{10} S/N_{(\text{en puissance})}$$

Notion de taux d'erreur

Les phénomènes parasites (bruit) perturbent le canal de transmission et peuvent affecter les informations en modifiant un ou plusieurs bits du message transmis, introduisant ainsi des

2. L'unité officielle de débit est le bit/s (invariable). L'abréviation bps pouvant être confondue avec byte par seconde ne sera pas utilisée dans cet ouvrage. Rappelons que le terme bit provient de la contraction des termes « binary digit ».

3. Le décibel ou dB (10^e du bel) est une unité logarithmique sans dimension. Elle exprime le rapport entre deux grandeurs de même nature. Le rapport Signal/Bruit peut aussi s'exprimer par le rapport des tensions, la valeur est alors $S/N_{\text{dB}} = 20 \log_{10} S/N_{(\text{en tension})}$.

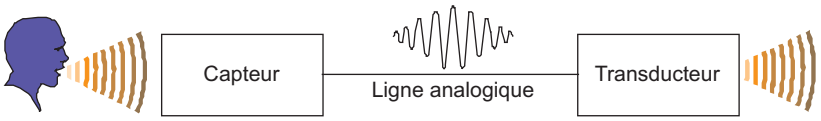


Figure 2.3 Le signal analogique.

2.2.2 Codage des informations

Définition

Coder l'information consiste à faire correspondre (bijection) à chaque symbole d'un alphabet (élément à coder) une représentation binaire (mot code). L'ensemble des mots codes constitue le code (figure 2.4). Ces informations peuvent aussi bien être un ensemble de commandes d'une machine outil que des caractères alphanumériques... C'est à ces derniers codes que nous nous intéresserons. Un code alphanumérique peut contenir :

– Des chiffres de la numérotation usuelle [0..9] ;
– Des lettres de l'alphabet [a..z, A..Z] ;
– Des symboles nationaux [é, è,...] ;
– Des symboles de ponctuation [, ; : . ? ! _] ;
– Des symboles sémi-graphiques [ ] ;
– Des commandes nécessaires au système [Saut de ligne, Saut de page, etc.].

Preview from Notesale.co.uk
Page 36 of 837

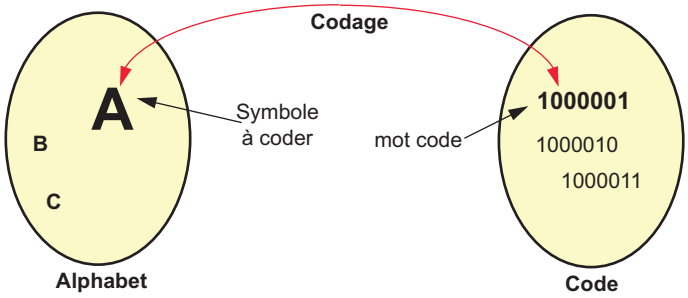


Figure 2.4 Principe du codage des données.

Les différents types de code

Le codage des différents états d'un système peut s'envisager selon deux approches. La première, la plus simple, considère que chacun des états du système est équiprobable. La seconde prend en compte la fréquence d'apparition d'un état. Cette approche conduit à définir deux types de code : les codes de longueur fixe et les codes de longueur variable.

➤ Les codes de longueur fixe

Chaque état du système est codé par un certain nombre de bits, appelé longueur du code, longueur du mot code ou encore code à n moments.

Symbole	Signification	
ACK	Acknowledge	Accusé de réception
BEL	Bell	Sonnerie
BS	Backspace	Retour arrière
CAN	Cancel	Annulation
CR	Carriage Return	Retour chariot
DC	Device control	Commande d'appareil auxiliaire
DEL	Delete	Oblitération
DLE	Data Link Escape	Caractère d'échappement
EM	End Medium	Fin de support
ENQ	Enquiry	Demande
EOT	End Of Transmission	Fin de communication
ESC	Escape	Echappement
ETB	End of Transmission Block	Fin de bloc de transmission
ETX	End Of Text	Fin de texte
FE	Format Effector	Commande de mise en page
FF	Form Feed	Présentation de formule
FS	File Separator	Séparateur de fichiers
GS	Group Separator	Séparateur de groupes
HT	Horizontal Tabulation	Tabulation horizontale
LF	Line Feed	Interligne
NAK	Negative Acknowledge	Accusé de réception négatif
NUL	Null	Nul
RS	Record Separator	Séparateur d'articles
SI	Shift IN	En code
SO	Shift Out	Hors code
SOH	Start Of Heading	Début d'en-tête
SP	Space	Espace
STX	Start Of Text	Début d'en-tête
SYN	Synchronous idle	Synchronisation
TC	Transmission Control	Commande de transmission
US	Unit Separator	Séparateur de sous-article
VT	Vertical Tabulation	Tabulation verticale

Figure 2.5 Le code ASCII.

Preview from Notesale.co.uk
Page 39 of 837

➤ Les codes de longueur variable

Lorsque les états du système ne sont pas équiprobables, la quantité d'information apportée par la connaissance d'un état est d'autant plus grande que cet état a une faible probabilité de se réaliser. La quantité moyenne d'information apportée par la connaissance d'un état, appelée **entropie**, est donnée par la relation :

$$H = \sum_{i=1}^{i=n} p_i \log_2 \frac{1}{p_i}$$

où p_i représente la probabilité d'apparition du symbole de rang i.

L'entropie représente la longueur optimale du codage des symboles du système. Déterminons la longueur optimale du code (entropie) pour le système décrit par le tableau ci-dessous. À des fins de simplicité, chaque état est identifié par une lettre.

© Dunod – La photocopie non autorisée est un délit

Figure 2.9 Structure élémentaire d'un convertisseur analogique/numérique.

Application à la voix

Un canal téléphonique utilise une plage de fréquence ou Bande Passante (**BP**) allant de 300 Hz à 3 400 Hz. Si on prend 4 000 Hz comme fréquence maximale à reproduire, la fréquence d'échantillonnage minimale est de :

$$F_e \geqslant 2 \cdot F_{\max} = 2 \cdot 4\,000 = 8\,000 \text{ Hz}$$

Soit 8 000 échantillons par seconde, ce qui correspond, pour chaque échantillon à une durée de 125 µs (1/8 000). Pour une restitution correcte (dynamique[6] et rapport signal à bruit), la voix devrait être quantifiée sur 12 bits (4 096 niveaux). Les contraintes de transmission en rapport avec le débit conduisent à réduire cette bande. L'utilisation d'une loi quantification logarithmique permet de ramener la représentation numérique de la voix à 8 bits (7 bits pour l'amplitude et un bit de signe), tout en conservant une qualité de reproduction similaire à celle obtenue avec une quantification linéaire sur 12 bits. Cette opération dite de compression est différente en Europe (loi A) et en Amérique du Nord (loi μ). En codant chaque échantillon sur 8 bits, il est nécessaire d'écouler :

$$8\,000 \cdot 8 = 64\,000 \text{ bits par seconde sur le lien}$$

Ce qui correspond à un débit de 64 000 bit/s. Ce choix correspond à celui du **RNIS** (Réseau Numérique à Intégration de Service ou **ISDN**, *Integrated Service Digital Network*) qui utilise des voies à 64 kbit/s.

Le codage de l'image vidéo

La voix est un phénomène vibratoire, l'oreille perçoit des variations de pression successives qu'elle interprète. L'image est interprétée globalement par l'œil alors qu'elle ne peut être transmise et reproduite que séquentiellement. La discrétisation de l'image nécessite 2 étapes : d'abord une transformation espace/temps qui se concrétise par une analyse de celle-ci, ligne par ligne, puis une décomposition de chaque ligne en points, enfin la quantification de la valeur lumineuse du point, valeur qui est ensuite transmise.

Une image colorée peut être analysée selon 3 couleurs dites **primaires** de longueur d'onde (λ) déterminée. Pour reconstituer l'image d'origine, il suffit de superposer les trois images, c'est la synthèse additive. La figure 2.10 représente le principe de la synthèse additive, le dosage de chacune des sources lumineuses permet de reproduire toutes les couleurs.

6. La dynamique exprime le rapport entre les puissances maximale et minimale du signal.

© Dunod – La photocopie non autorisée est un délit

Preview from Notesale.co.uk
Page 43 of 837

code, non la valeur absolue de l'échantillon, mais son écart par rapport au précédent. Des techniques plus élaborées prédisent la valeur future à partir des 4 derniers échantillons (**CELP**, *Code Excited Linear Prediction*).

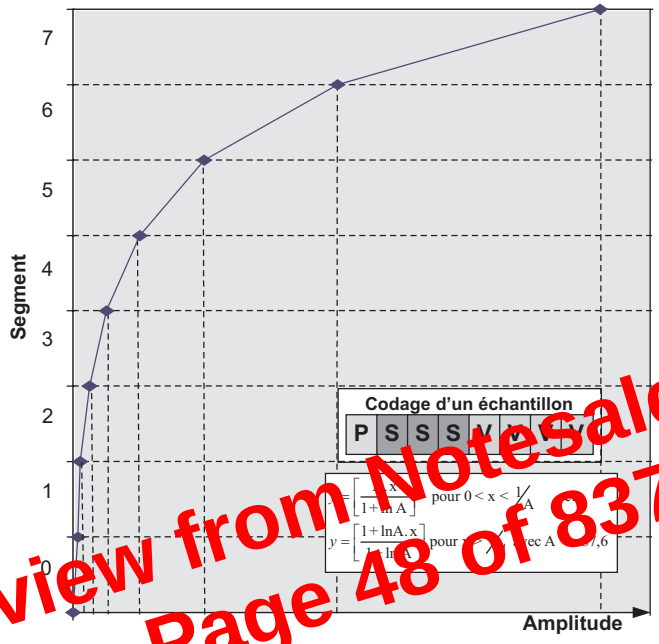


Figure 2.11 La loi de codage A.

Preview from Notesale.co.uk
Page 48 of 837

La figure 2.12 compare différents algorithmes de compression en fonction du débit qu'ils nécessitent et de la qualité de restitution de la parole. La norme G.711 est utilisée dans la téléphonie fixe traditionnelle. La norme G.729 est mise en œuvre dans la voix sur IP, elle modélise la voix humaine par l'utilisation de filtres.

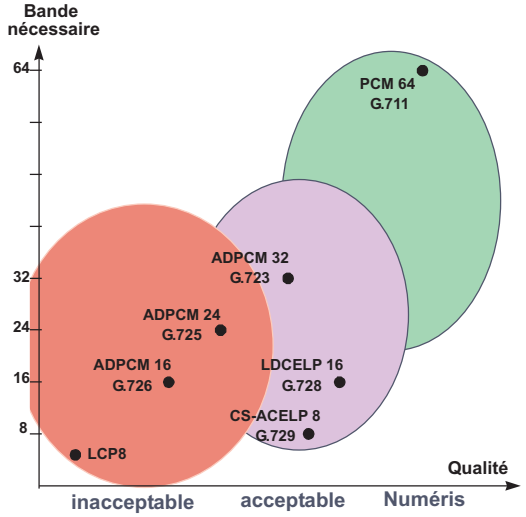


Figure 2.12 Les différents algorithmes de compression du son.

Services	Noms	Caractéristiques	Application types
CBR	Constant Bit Rate	Débit constant Flux isochrone	Voix, vidéo non compressée
VBR-rt	Variable Bit Rate real time	Débit variable Flux isochrone	Applications audio et vidéo compressées
VBR-nrt	Variable Bit Rate non real time	Débit variable mais prévisible	Application de type transactionnel
ABR	Available Bit Rate	Débit sporadique Sans contrainte temporelle	Interconnexion de réseaux locaux
UBR	Unspecified Bit Rate	Trafic non spécifié Best Effort	Messagerie, sauvegarde à distance (remote backup)

Figure 2.16 Les classes de service de l'ATM Forum.

réel (**VBR-rt**, *VBR Real Time*), les variations maximales du délai de transfert sont fixées à la connexion. La classe VBR correspond aux applications de type voix ou vidéo compressées.

Les classes CBR et VBR garantissent aux applications une certaine qualité de service, le réseau devant s'adapter aux besoins des applications. Certaines applications, notamment les applications de type données, sont moins exigeantes en terme de débit. Afin de mieux utiliser les capacités du réseau, il semble préférable que ce soient les applications qui s'adaptent aux capacités de transfert de ce dernier et non l'inverse. La classe de service **ABR** (*Available Bit Rate*) ne spécifie, à la connexion, qu'un débit minimal et maximal, il n'y a aucun débit moyen garanti. Les applications utilisent le débit disponible sur le réseau (entre les deux bornes prédéfinies).

Preview from Notesale.co.uk
Page 52 of 837

De même, une classe de service de type datagramme[16] ou *best effort* a été définie : **l'UBR** (*Unspeciefied Bit Rate*). L'UBR ne fournit aucune garantie ni de débit ni de remise des données. Si l'état du réseau le permet, toutes les données introduites dans le réseau sont transmises, en cas de saturation du réseau elles sont éliminées.

2.4.3 Conclusion

La notion de qualité de service est au cœur de la recherche de nouveaux protocoles et des développements des réseaux. Des solutions ont été apportées à ce problème dans les protocoles de dernières générations tels qu'**ATM** (*Asynchronous Transfer Mode*), tandis que les protocoles plus anciens comme **TCP/IP** (*Transmission Control Protocol/Internet Protocol*) ont été adaptés et enrichis pour en tenir compte.

16. Un datagramme est une unité de données constituant un tout et acheminé tel quel sur le réseau sans aucune garantie de délivrance.

En transmission asynchrone, les caractères émis sont précédés d'un signal de synchronisation : le **bit de start**. Entre chaque caractère, pour garantir la détection du bit de start suivant, la ligne est remise à l'état zéro. Ce temps de repos minimal varie de 1 à 2 temps bit, il constitue le ou les **bits de stop** (figure 3.13). Le niveau de repos de la ligne ou niveau zéro est fixé à un certain potentiel (V) et non pas au zéro électrique pour ne pas confondre un zéro binaire avec une rupture de la ligne. Cette tension de repos signale aux systèmes que les terminaux sont actifs.

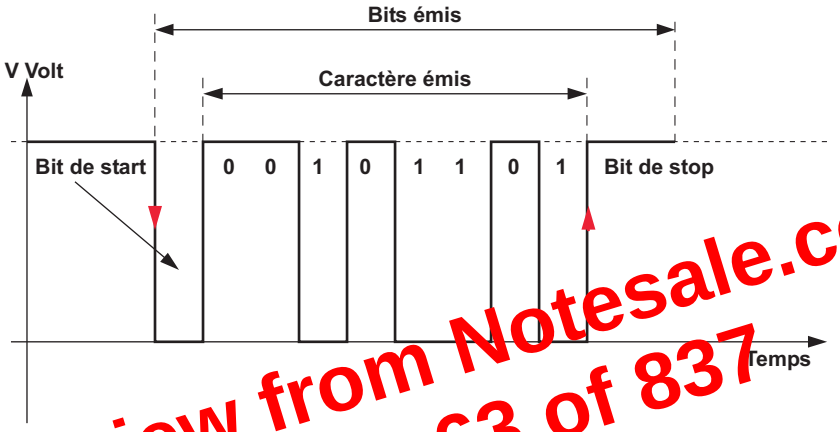


Figure 3.14 Caractère asynchrone.

Preview from Notesale.co.uk
Page 63 of 837

Le bit de start et celui ou ceux de stop servent de délimiteur de caractères (figure 3.14). Les transmissions asynchrones s'effectuent selon un ensemble de règles régissant les échanges (protocole). On distingue deux types de protocoles asynchrones (figure 3.15) :

– Le mode caractères : la transmission a lieu caractère par caractère. L'intervalle de temps qui sépare chaque caractère peut être quelconque (multiple de la fréquence d'horloge).

– Le mode blocs : les caractères sont rassemblés en blocs. L'intervalle de temps entre l'émission de 2 blocs successifs peut être quelconque (multiple de la fréquence d'horloge).

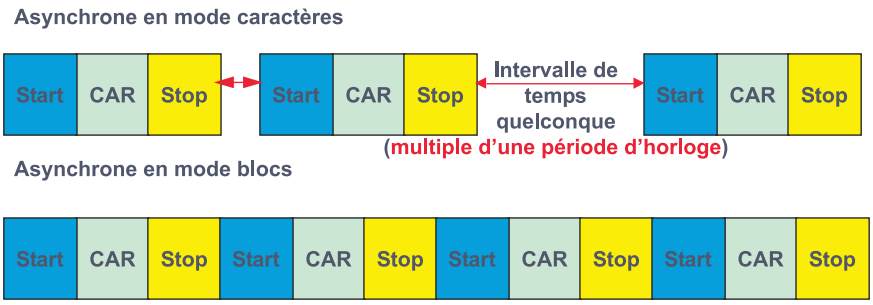


Figure 3.15 Mode caractères et mode blocs.

Le principe des protocoles de transmission sera étudié au chapitre 6. Les principaux protocoles asynchrones sont :

– **XON-XOFF**, protocole orienté caractères, le terminal réactive la ligne quand il est prêt à émettre, il la désactive quand il n'a plus de données disponibles ;

© Dunod – La photocopie non autorisée est un délit

Fanion 0x7E	Adresse 0xFF	Contrôle UI = 0x	Protocole 2 octets	Données 1 500 octets	FCS 2 octets	Fanion 0x7E

Figure 3.18 Trame PPP.

La trame PPP (figure 3.18) comporte 8 octets de service[6] (2 fanions d'un octet, 1 octet pour le champ adresse, 1 pour le champ contrôle, 2 pour le champ protocole et 2 pour le champ FCS) pour une charge utile de 1 500 octets d'information (*payload*).

L'efficacité dans le mode synchrone correspond au rapport du nombre d'octets utiles au nombre d'octets transmis soit :

$$Eff = \frac{1500}{1508} = 0{,}994$$

En mode asynchrone, il faut, à chaque octet ajouter un bit de start et un bit de stop soit 10 bits pour 8 d'utiles. L'efficacité dans ces conditions est :

$$Eff = \frac{1500 \cdot 8}{1508 \cdot 10} = 0{,}795$$

Essentiellement pour des raisons de dérive d'horloge et d'efficacité, les systèmes de transmission à bas débit constituent le domaine de prédilection du mode asynchrone. Cependant, compte tenu des coûts plus faibles des systèmes asynchrones par rapport aux coûts des systèmes synchrones, ils sont mis en œuvre dans les systèmes grand public pour les accès à Internet à 56 000 bit/s via le réseau téléphonique commuté.

Attention : les termes synchrone et asynchrone ont, selon ce qu'ils qualifient, des significations différentes. Un tableau en annexe résume les différentes utilisations de ces termes dans le monde des télécommunications.

Preview from Notesale.co.uk
Page 66 of 837

3.2.3 Selon le mode de transmission électrique

Les zéros ou les uns sont différentiés par un niveau électrique différent. On distingue deux modes selon la manière dont sont lus les niveaux électriques.

Le mode dissymétrique

Dans le mode asymétrique (ou dissymétrique), l'information d'état est fournie par la différence de potentiel entre le conducteur concerné et un conducteur de retour. Le fil de retour peut être commun à plusieurs fonctions. Ce conducteur commun est souvent désigné sous le terme de **terre de signalisation**. La figure 3.19 représente les variations de potentiel (+V, −V) autour d'une valeur de référence dite « zéro électrique ».

Ce mode de transmission est simple à réaliser au niveau de l'électronique, il ne nécessite que 2 conducteurs mais est très sensible aux parasites.

Le mode symétrique

Dans le mode symétrique appelé aussi **transmission différentielle**, l'information d'état est déduite de la différence de potentiel entre deux conducteurs. La figure 3.20 illustre ce mode de

6. Pour la signification de chacun de ces champs voir chapitre 6.

EXERCICES

Exercice 3.1 Organisation des échanges

Donnez un exemple de la vie courante pour chacun des modes de contrôle des échanges.

Exercice 3.2 Transmission parallèle

Combien de conducteurs sont nécessaires pour réaliser une transmission en parallèle de mots machines de 32 bits si on utilise ou non un retour commun ?

Exercice 3.3 Transmission synchrone et asynchrone

Rappeler brièvement ce qui distingue ces deux modes de transmission.

Preview from Notesale.co.uk
Page 69 of 837

Exercice 3.4 Élément d'accès aux réseaux

Un DTE peut-il être raccordé directement au réseau d'un opérateur ?

Exercice 3.5 Transmission asynchrone

En transmission asynchrone, l'horloge du récepteur n'est synchronisée qu'en début de transmission. Une source a une horloge de 1 000 Hz (1 000 bit/s) avec une stabilité de 10^{-2}. Sachant que pour lire correctement un bit on ne peut admettre qu'une dérive maximale de 10 % par rapport à un temps bit et que le débit binaire est égal à la rapidité de modulation, quel est le nombre de bits que l'on peut émettre en une fois ?

Exercice 3.6 Durée d'un transfert d'information

Une entreprise désire réaliser la sauvegarde de ses données sur un site distant. Le volume de données à sauvegarder est estimé à 10 Go/jour. La sauvegarde doit s'effectuer la nuit de 22 h 00 à 6 h 00. Les deux sites sont reliés par une ligne à 2 Mbit/s. On vous demande de vérifier si cette solution est réalisable et le cas échéant de proposer une solution qui permette cette sauvegarde. Pour ce problème on admettra que 1ko = 1 000 octets.

© Dunod – La photocopie non autorisée est un délit

Chapitre **4**

Les supports de transmission

Preview from Notesale.co.uk
Page 71 of 837

L'infrastructure d'un réseau, la qualité de service offerte, les solutions logicielles à mettre en œuvre dépendent largement des supports de transmission utilisés. Les supports de transmission exploitent les propriétés de conductibilité des métaux (paires torsadées, coaxial), celles des ondes électromagnétiques (faisceaux hertziens, guides d'onde, satellites) ou encore celles du spectre visible de la lumière (fibre optique). Généralement on classe les supports en deux catégories :

– les supports guidés (supports cuivre et supports optiques) ;
– les supports libres (faisceaux hertziens et liaisons satellites).

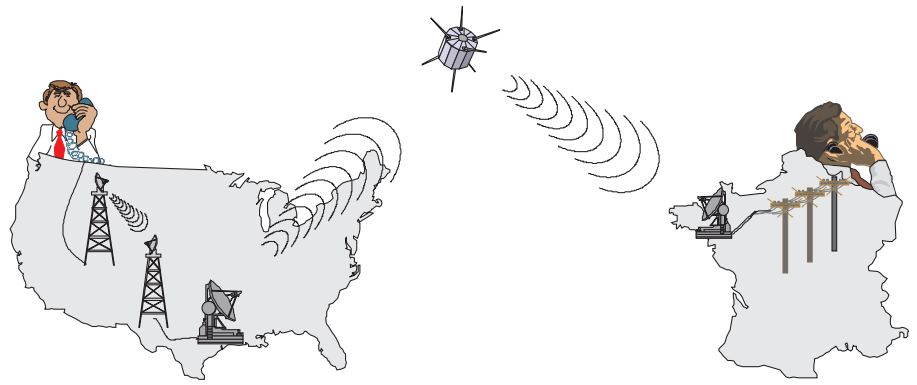


Figure 4.1 Une liaison informatique peut mettre en œuvre plusieurs types de support.

La complexité des systèmes provient généralement du fait qu'une liaison peut emprunter différents supports (figure 4.1). Le système de transmission devra alors réaliser l'adaptation du signal à transmettre au support utilisé. Les caractéristiques des supports diffèrent selon la nature physique du support et le mode de propagation choisi. Cependant, certaines caractéris-

tiques sont communes à tous les types de support (bande passante...), d'autres sont spécifiques (impédance caractéristique...). Après l'étude générale de ces caractéristiques, nous examinerons et qualifierons chaque type de support.

4.1 CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION

4.1.1 Bande passante et système de transmission

Généralités

L'impulsion électrique représentative d'un élément binaire est affaiblie et déformée par le système de transmission (figure 4.2).

Figure 4.2 Déformation du signal par le support de transmission.

Preview from Notesale.co.uk
Page 72 of 837

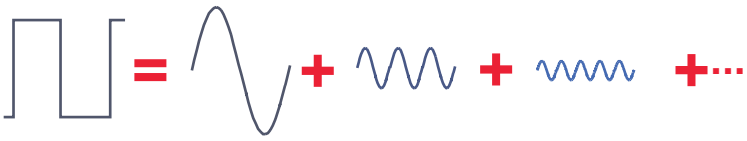
À l'extrémité de la ligne, le récepteur doit identifier et décoder le signal. Cette fonction ne peut valablement être réalisée que si le signal n'a pas été exagérément modifié pendant la transmission. Ces modifications dépendent d'une part de la nature du signal (spectre du signal) et, d'autre part, de la réponse en fréquence du système (bande passante).

Notions d'analyse spectrale

L'impulsion électrique est un phénomène discontinu qui ne peut être modélisé. L'étude du comportement des circuits en régime impulsionnel est essentiellement due aux travaux du mathématicien et physicien Fourier qui a montré que tout signal périodique non sinusoïdal peut être considéré comme la somme d'une composante continue (A_0) et d'une infinité de signaux sinusoïdaux d'amplitude et de phase convenablement choisies. Le théorème de Fourier peut s'exprimer sous la forme de :

$$u(t) = A0 + \sum_{i=1}^{i=\infty} Ui \cos(i\omega t + \varphi i)$$

La composante de même fréquence que le signal d'origine est appelée **fondamental**. Les autres composantes, multiple de la fréquence du signal fondamental, sont appelées **harmoniques**. La figure 4.3 illustre la décomposition d'un signal carré.



$u(t) = 4\,U / \pi\,(\sin \omega t + 1/3 \sin 3\omega t + 1/5 \sin 5\omega t + \ldots)$

Figure 4.3 Décomposition d'un signal carré symétrique par rapport au 0 volt.

– faible affaiblissement (0,2 à 0,5 dB/km) ;
– faible encombrement et poids ;
– vitesse de propagation élevée (monomode) ;
– sécurité (absence de rayonnement à l'extérieur et difficulté de se mettre à l'écoute) ;
– légèreté.

Ces caractéristiques font des fibres optiques le support privilégié dans le domaine des télécommunications à haut débit et grande distance, dans les applications aéronautiques et navales (sous-marin) et dans les transmissions de données en milieu perturbé.

Si la pose de la fibre optique est aisée (pas de contraintes particulières), la connectique est assez délicate, elle nécessite un outillage particulier et un savoir-faire certain.

4.2.4 Les liaisons hertziennes

Principe

Un conducteur rectiligne alimenté en courant haute fréquence ou radiofréquence peut être assimilé à un circuit oscillant ouvert. Un tel circuit ou antenne d'émission rayonne une énergie (onde électromagnétique). Cette énergie électromagnétique recueillie par un autre conducteur distant ou antenne de réception est transformée en un courant électrique similaire à celui d'excitation de l'antenne d'émission (théorème de réciprocité). La figure 4.26 illustre le principe d'une liaison radioélectrique.

Preview from Notesale.co.uk
Page 85 of 837

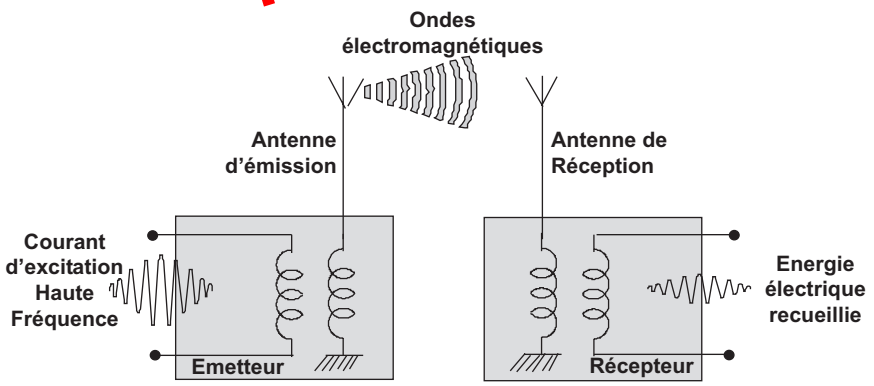


Figure 4.26 Principe d'une liaison radioélectrique.

Contrairement aux supports étudiés dans les paragraphes précédents, la liaison entre les deux entités émetteur et récepteur s'effectue sans support physique. Les ondes électromagnétiques (OEM) se propagent dans le vide à la vitesse de la lumière. On appelle longueur d'onde (λ), la distance parcourue pendant une période du phénomène vibratoire.

Une antenne est un conducteur dont la longueur est un sous-multiple de la longueur d'onde. Le rayonnement d'une source ponctuelle est omnidirectionnel, l'énergie se diffuse selon une sphère. Le rayonnement d'un conducteur rectiligne s'effectue selon un demi-tore. Afin d'utiliser au mieux l'énergie rayonnée, on réalise des réflecteurs. Les réflecteurs peuvent être actifs (rideaux d'antennes) ou passifs (brins, réflecteur plan ou parabolique).

© Dunod – La photocopie non autorisée est un délit

Exercice 4.3 Bande passante d'une fibre optique

Une fibre optique multimode à saut d'indice a une ouverture numérique de 0,22 (l'ouverture numérique correspond au sinus de l'angle d'ouverture) et un indice de réfraction du cœur de $n_1 = 1{,}465$. Déterminer la bande passante en bit/s de cette fibre pour une longueur de 1 km (BP/km).

Preview from Notesale.co.uk
Page 91 of 837

© Dunod – La photocopie non autorisée est un délit

Chapitre **5**

Les techniques de transmission

Preview from Notesale.co.uk
Page 93 of 837

5.1 GÉNÉRALITÉS

Chaque machine participant à une transmission de données est reliée à la terre locale. Si la terre constitue une référence locale, son potentiel est différent en divers points. De ce fait, réaliser une liaison cuivre directe entre les deux calculateurs provoquerait un courant d'équilibrage qui peut ne pas être supporté par la ligne (intensité) et qui risque de perturber la transmission. Ce problème conduit à distinguer deux références électriques :

– une référence pour la transmission : la terre de signalisation ;

– une référence pour les équipements : la terre de protection.

Cependant, rien ne garantit que dans un équipement les deux terres ne soient pas confondues[1]. Pour pallier ce défaut, on réalise l'isolement galvanique des deux machines par des transformateurs dits *transformateurs d'isolement* (figure 5.1). Ces transformateurs réduisent la bande passante et sont perturbés par la composante continue du signal.

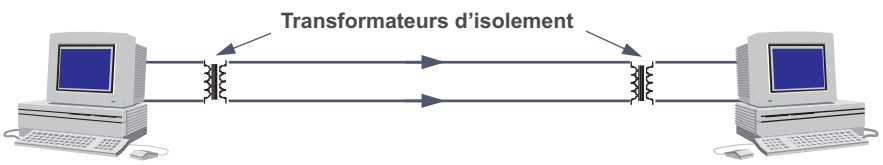


Figure 5.1 Insertion de transformateurs d'isolement sur le lien de transmission.

1. Certaines réglementations nationales imposent la confusion des deux terres.

La rapidité de modulation maximale de ce canal est :

$$R_{\max} = 2 \cdot BP = 2(3\,400 - 300) = 6\,200\text{bauds}$$

La capacité de transmission est donnée par la relation de Shannon :

$$\begin{aligned} C &= BP \cdot \log_2[1 + (S/N)] \\ &= (3\,400 - 300)\log_2(1 + 1\,000) \approx 3\,100 \cdot 3,32 \log_{10}(1\,000) \\ &= 3\,100 \cdot 3,32 \cdot 3 \\ &= 30\,876 \text{ bit/s} \end{aligned}$$

Ce débit maximal théorique correspond aux performances maximales que l'on peut obtenir sur une ligne téléphonique[6].

➤ Conclusion

La bande passante ou encore la rapidité de modulation et le rapport signal sur bruit limitent les possibilités de transmission en bande de base. La transmission bande de base occupe la totalité de la bande passante du canal interdisant l'utilisation de techniques de multiplexage (voir chapitre 7, *Mutualisation des ressources*).

Les techniques dites « bande de base » restent utilisées sur des liaisons spécialisées privées, les liaisons louées par les opérateurs aux entreprises pour se constituer des réseaux privés, les liaisons d'accès aux réseaux des opérateurs et les réseaux locaux d'entreprise. En l'absence de normalisation concernant les ERBdB, il est impératif d'associer ces équipements par paire de même référence chez un même constructeur. Les ERBdB couvrent une gamme de débits allant de 2 400 bit/s à 2 Mbit/s. La distance maximale d'utilisation dépend essentiellement de la qualité du support utilisé et du débit en ligne, elle varie de quelques kilomètres à quelques dizaines de kilomètres.

Preview from Notesale.co.uk
Page 104 of 837

5.3 LA TRANSMISSION EN LARGE BANDE

5.3.1 Principe

Transmission bande de base et large bande

En transmission large bande, le spectre du signal numérique est translaté autour d'une fréquence centrale appelée **porteuse**. La translation de spectre résout les deux problèmes posés par la transmission en bande de base : dispersion du spectre (étalement du signal) et la monopolisation du support qui interdit le multiplexage. Elle est réalisée par un organe appelé modulateur. En réception le signal doit subir une transformation inverse, il est démodulé. Le modem, contraction de **mod**ulation/**dém**odulation, est un équipement qui réalise la modulation des signaux en émission et leur démodulation en réception.

6. Le débit maximal sur ligne téléphonique ordinaire (BP = 300 – 3 400 Hz) est aujourd'hui atteint par les modems V34 bis (33 600 bit/s).

porteuse. Chaque demi-spectre ou bande latérale contient l'intégralité de l'information à transmettre. Aussi, pour réduire la largeur de bande et la dispersion du spectre, certains équipements n'utilisent qu'une seule des deux bandes latérales (**BLU**, Bande Latérale Unique). La porteuse, nécessaire à la démodulation, est régénérée par le récepteur.

L'amplitude étant représentative de l'information, la modulation d'amplitude est très sensible aux bruits parasites, elle n'est pratiquement utilisée qu'en combinaison avec la modulation de phase.

➤ La modulation de fréquence

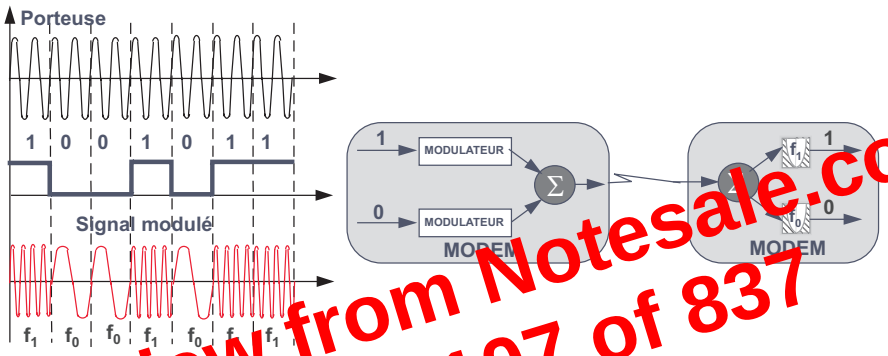


Figure 5.21 Principe de la modulation de fréquence.

Preview from Notesale.co.uk
Page 107 of 837

Dans ce type de modulation, on associe à une valeur binaire (0,1, ou 01,10...) une fréquence particulière (figure 5.21). En réception, un filtre permet la restitution de la valeur binaire d'origine. La technique de la modulation de fréquence est particulièrement simple à mettre en œuvre. Elle est très résistante aux bruits, mais la grande largeur du spectre du signal résultant la limite au faible débit comme pour le modem V.23 utilisé par le Minitel.

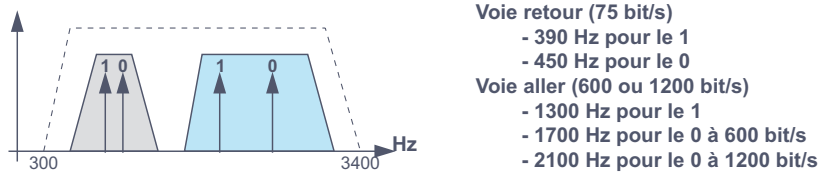


Figure 5.22 Spectre du modem V.23.

Le modem V.23 est conçu pour fonctionner sur ligne téléphonique ordinaire (Bande Passante 300-3 400 Hz). Il permet de réaliser des liaisons *full duplex* asymétriques (la voie aller et la voie retour ont des débits différents). La figure 5.22 indique les fréquences affectées à chaque valeur binaire.

➤ La modulation de phase

En modulation de phase, on associe une valeur binaire à un signal dont la phase est fixée par rapport à un signal de référence. Dans la figure 5.23, la valeur binaire 1 est associée à un signal en phase avec le signal de référence, et la valeur binaire 0 à un signal déphasé de 180°. La représentation est bivalente : modulation de phase à deux états ou **BPSK**, *Binary Phase Shift Keying*.

© Dunod – La photocopie non autorisée est un délit

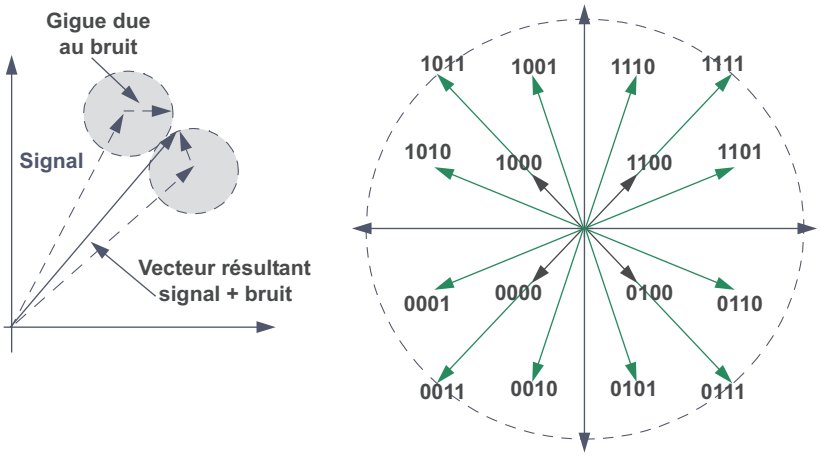


Figure 5.24 Principe de la modulation MAQ (MAQ16) et ses limitations.

Preview from Notesale.co.uk
Page 109 of 837

5.3.2 Les liaisons full duplex

Les liaisons *full duplex* (figure 5.25) peuvent être réalisées simplement par l'utilisation de 2 voies de communications distinctes (liaisons 4 fils) ou par mise en œuvre de techniques spécifiques (liaison 2 fils).

Figure 5.25 Liaisons *full duplex* à 4 et 2 fils.

En transmission large bande, il est facile de réaliser une liaison full duplex sur deux fils par simple décalage des porteuses comme, par exemple dans le modem V.23 (figure 5.22). En transmission bande de base, cette technique est inapplicable. L'émetteur et le récepteur sont raccordés à la liaison 2 fils par un système hybride permettant le passage de 4 en 2 fils, ce système n'isole pas parfaitement les deux voies. Une partie du signal d'émission se retrouve sur la voie de réception (écho local et écho distant). Le système annuleur d'écho évalue la valeur de ces signaux parasites et les ajoute en opposition de phase au signal reçu. La figure 5.26 illustre ce système.

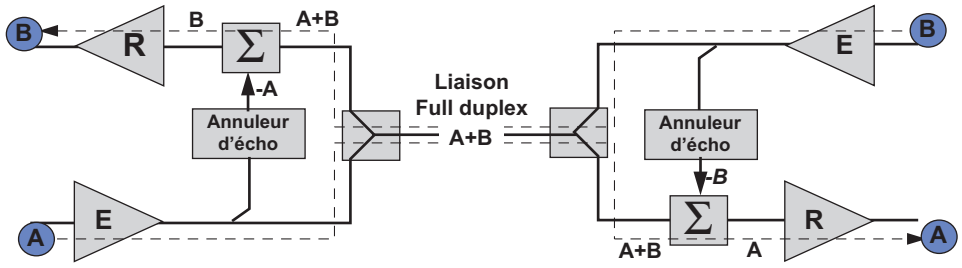


Figure 5.26 Système hybride de passage de 4 à 2 fils.

Les systèmes à annulation d'écho sont aussi utilisés dans les modems large bande.

© Dunod – La photocopie non autorisée est un délit

L'interface d'accès aux réseaux publics

➤ L'interface X.21

Afin d'optimiser l'accès aux réseaux publics de données une nouvelle interface a été définie : l'avis X.21. Cette interface autorise des débits synchrones pouvant atteindre 10 Mbit/s sur quelques mètres et un temps d'établissement de la connexion d'environ 200 à 300 ms contre 3 à 15 s pour l'interface V.24.

L'avis X.21 définit l'interface d'accès entre un ETTD et un réseau public de transmission de données (figure 5.47), il fixe les règles d'échange pour :

– l'établissement de la connexion avec un ETTD distant à travers un ou plusieurs réseaux,

– l'échange des données en mode duplex synchrone,

– la libération de la connexion.

Preview from Notesale.co.uk
Page 124 of 837

Figure 5.47 Le réseau X.21.

L'avis X.21 prévoit deux modes électriques de fonctionnement. Côté ETCD seul le mode équilibré peut être utilisé (2 fils par circuits), côté ETTD les deux modes sont possibles : le mode équilibré ou le mode non équilibré (retour commun). Il n'utilise que 8 circuits, les commandes ne sont pas matérialisées par des tensions sur un circuit spécifié mais par une combinaison de signaux. L'état de l'interface est indiqué par la combinaison des quatre circuits Transmission (T), Contrôle (C), Réception (R) et Indication (I). Le circuit C est activé par le terminal pour émettre l'appel et le circuit I par le réseau pour indiquer la connexion.

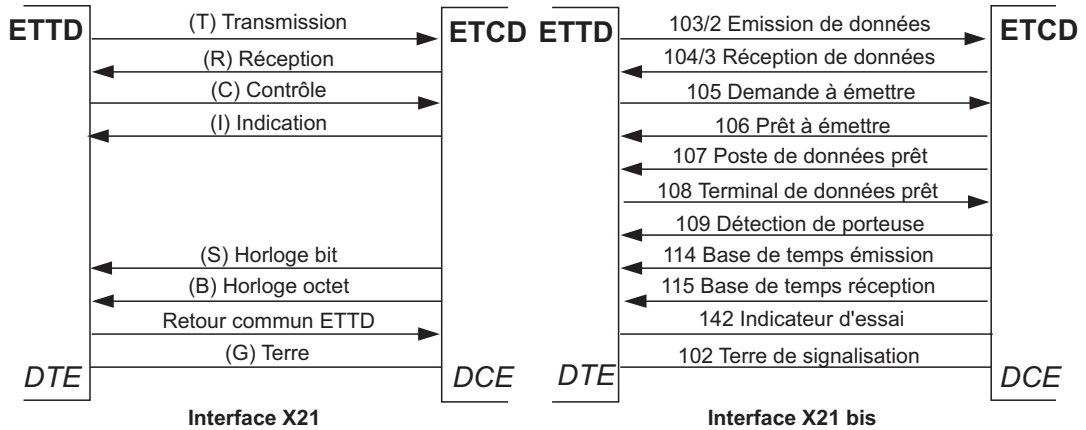


Figure 5.48 L'interface X.21 et X.21bis.

Exercice 5.7 Rapidité de modulation

Quelle est la rapidité de modulation en bauds du signal sur un réseau local 802.3 10 base 5 (Ethernet, codage Manchester) lorsqu'il émet une suite continue de 1 ou de 0 ?

Preview from Notesale.co.uk
Page 128 of 837

Chapitre **6**

Notions de protocoles

Preview from Notesale.co.uk
Page 129 of 837

Dans les chapitres précédents nous avons étudié tous les mécanismes à mettre en œuvre pour transmettre un flot de bits entre deux systèmes distants. Cependant, il ne suffit pas de lire correctement les bits reçus, encore faut-il les traduire en données utilisables par les applications. On appelle protocole un ensemble de conventions préétablies pour réaliser un échange fiable de données entre deux entités (figure 6.1).

Figure 6.1 Un protocole organise l'échange de données.

Lors de l'échange de données, le protocole de transfert doit assurer :

- la délimitation des blocs de données échangés ;
- le contrôle de l'intégrité des données reçues[1] ;
- l'organisation et le contrôle de l'échange ;
- éventuellement le contrôle de la liaison.

1. Dans ce chapitre, le terme intégrité sera utilisé dans son sens le plus restrictif, il ne concernera que le contrôle d'erreur.

division $R_{(x)}$ constitue le CRC parfois appelé aussi **FCS** (*Frame Check Sequence*). Le CRC calculé est transmis à la suite du bloc de données (figure 6.12). En réception, le destinataire effectue la même opération sur le bloc reçu (figure 6.13). Le CRC transmis et celui calculé par le récepteur sont comparés, si les valeurs diffèrent une erreur est signalée.

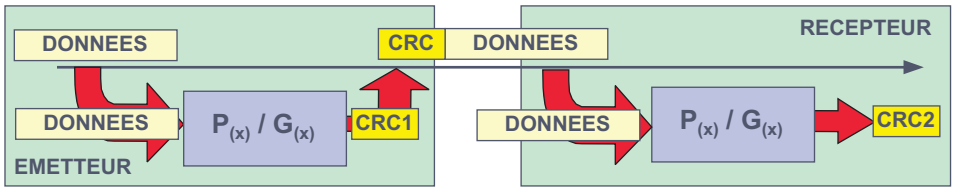


Figure 6.13 Principe de la détection d'erreur par clé calculée.

En réalité la méthode utilisée est quelque peu différente. En effet, si D est le dividende, d le diviseur et R le reste, la division $(D - R)/d$ donne un reste nul. En arithmétique booléenne, l'addition et la soustraction sont la même opération (figure 6.14), l'opération $(D - R)$ est équivalente à l'opération $(D + R)$.

Preview from Notesale.co.uk
Page 136 of 837

Addition

+	0	1
0	0	1
1	1	0

Soustraction

−	0	1
0	0	1
1	1	0

Multiplication

×	0	1
0	0	0
1	0	1

Figure 6.14 Les opérations booléennes.

Dans ces conditions (figure 6.15), la division par le polynôme générateur $(G_{(x)})$ de l'ensemble bloc de données et du CRC soit $P_{(x)} + R_{(x)}$ donne un reste égal à zéro. En réception, l'automate effectue la division sur l'ensemble du bloc de données y compris la clé calculée, lorsque le calcul du reste donne zéro et que le caractère suivant est le fanion, le bloc est réputé exact.

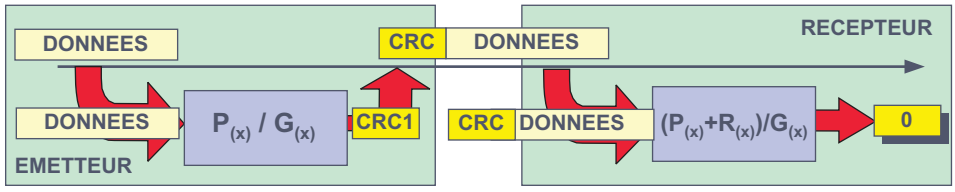


Figure 6.15 Détection d'erreur par CRC.

L'arithmétique modulo 2 est une arithmétique sans retenue, l'affirmation précédente n'est donc exacte que si le reste est ajouté à une séquence binaire nulle. Pour réaliser cette condition, avant d'effectuer la division, on multiplie le polynôme $P_{(x)}$ par x^m où m est le degré du polynôme générateur, ce qui correspond à une translation de m positions. Rappelons que le reste de la division par un diviseur de degré *m* est de degré *m – 1*, il comporte donc *m* termes. Cette opération a pour effet d'insérer *m* bits à zéro, pour y ajouter les termes du reste. L'exemple développé ci-dessous devrait éclairer le lecteur.

Exemple : on désire protéger le message « 110111 » par une clé calculée à l'aide du polynôme générateur $x^2 + x + 1$.

6.3 LE CONTRÔLE DE L'ÉCHANGE

6.3.1 Du mode *Send and Wait* aux protocoles à anticipation

Les mécanismes de base

Le principe de base de toute transmission repose sur l'envoi (*Send*) d'un bloc d'information. L'émetteur s'arrête alors (*Stop*) dans l'attente (*Wait*) d'un accusé de réception. À la réception de l'acquittement, noté **ACK** pour *Acknowledge*, l'émetteur envoie le bloc suivant (figure 6.17 gauche).

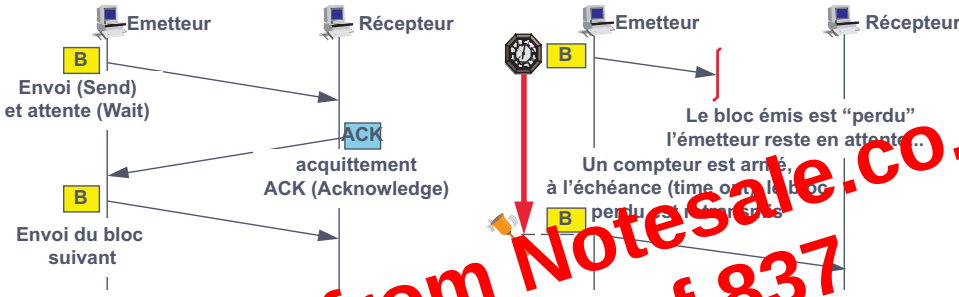


Figure 6.17 Le mode *Send et Wait* et la reprise sur temporisation.

Preview from Notesale.co.uk
Page 140 of 837

En cas d'erreur de transmission, le bloc reçu est rejeté. Le bloc est dit perdu, il n'est pas acquitté. L'émetteur reste alors en attente. Pour éviter un blocage de la transmission, à l'émission de chaque bloc de données, l'émetteur arme un temporisateur (*Timer*). À l'échéance du temps imparti (*Time Out*), si aucun accusé de réception (ACK) n'a été reçu, l'émetteur retransmet le bloc non acquitté, cette technique porte le nom de reprise sur temporisation (**RTO**, *Retransmission Time Out*) ou correction d'erreur sur temporisation (figure 6.17 droite).

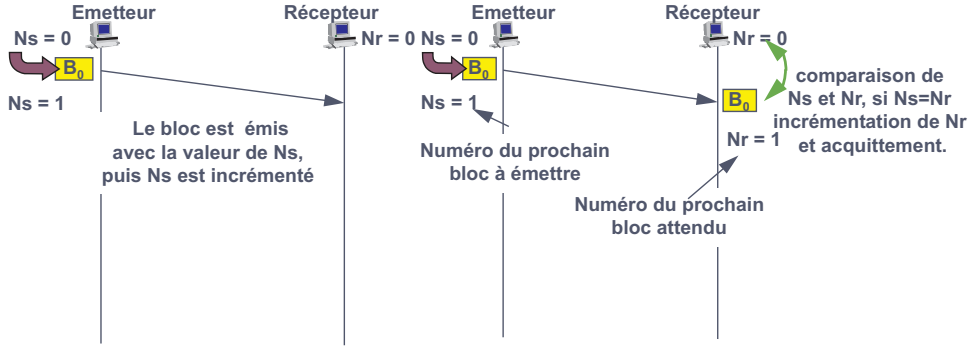


Figure 6.18 Numérotation des blocs de données.

Une difficulté survient si la perte concerne l'ACK. En effet, bien que les données aient été correctement reçues, l'émetteur les retransmet sur temporisation. Les informations sont ainsi reçues 2 fois. Pour éviter la duplication des données, il est nécessaire d'identifier les blocs. À cet effet, l'émetteur et le récepteur entretiennent des compteurs (figure 6.18). Les compteurs Ns (Ns, Numéro émis, s pour *send*) et Nr (Numéro du bloc à recevoir, r pour *receive*) sont

Dans ces conditions, les données reçues peuvent ne pas être acquittées à temps. L'émetteur effectue alors une retransmission sur temporisation. Le récepteur ayant déjà reçu ces informations les élimine et les acquitte. En effet, pour le récepteur, s'il y a eu une retransmission, c'est que l'émetteur n'a pas reçu le précédent ACK. Ainsi, figure 6.20, à la réception du premier ACK (acquittant le bloc 0) l'émetteur envoie le bloc suivant (B1).

Supposons que ce bloc se perde, l'émetteur à la réception du second ACK (concernant le second envoi de B0) considère que cet ACK est relatif au bloc B1, il envoie le bloc suivant (B2). Ce bloc comporte un Ns différent du numéro attendu, il est rejeté. Pour éviter cette confusion d'interprétation, il est aussi nécessaire de numéroter les ACK.

Efficacité du protocole de base

Pour déterminer l'efficacité d'un protocole, il faut non seulement tenir compte des informations de contrôle (figure 6.21), mais aussi du délai d'acquittement. D'une manière générale, l'efficacité d'un protocole mesure le rapport du temps effectivement consacré à l'émission d'informations utiles au temps pendant lequel le support a été occupé ou encore le rapport du nombre de bits utiles transmis au nombre de bits qui auraient pu être émis.

Preview from Notesale.co.uk
Page 142 of 837

Figure 6.21 Structure de base d'un bloc d'information.

➤ La transmission étant considérée sans erreur

Considérons l'échange représenté par le diagramme temporel de la figure 6.22, on distingue les phases suivantes :

– l'émission du bloc de données, ou **U** représente les données utiles, **G** les données de gestion du protocole ;
– un temps mort pendant lequel l'émetteur attend l'acquittement qui correspond au temps de transit aller et retour sur le support et au temps de traitement des données reçues par le récepteur. Ce temps, généralement désigné sous le terme de temps de traversée des équipements, noté **RTT** (*Round Trip Time*, temps aller et retour), équivaut à l'émission de $(D \cdot RTT)$ bits où **D** représente le débit nominal du système ;
– enfin, la réception de l'accusé de réception de **K** bits.

Le temps entre l'émission du premier bit du bloc N et le premier bit du bloc suivant $(N + 1)$ est appelé temps d'attente et noté Ta.

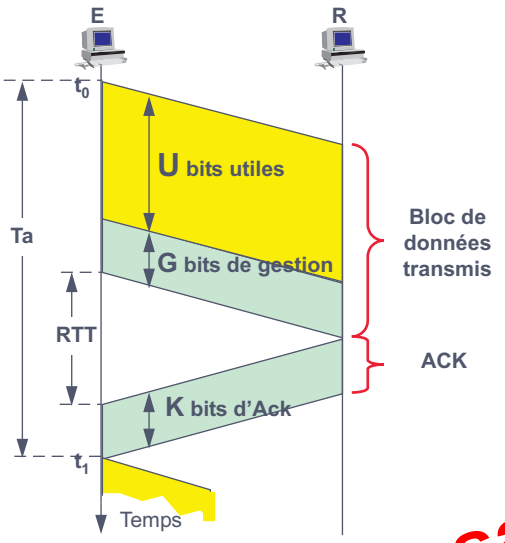


Figure 6.22 Efficacité du mode de base

Preview from Notesale.co.uk
Page 143 of 837

Établissons l'efficacité du protocole dans une transmission sans erreur. Rappelons que l'efficacité d'un protocole (E) est le rapport entre le nombre de bits utiles transmis (U) au nombre de bits total transmis ou qui auraient pu être transmis (N) :

$$E = U/N \qquad (1)$$

Le nombre de bits qui auraient pu être transmis entre t_0 et t_1 (Ta) s'exprime par la relation :

$$N = U + G + K + D \cdot RTT$$

Dès lors, on peut déterminer l'efficacité du protocole dans le cas où aucune erreur ne se produit, posons :

$$S = G + K + D \cdot RTT$$

$D \cdot RTT = Nb.$ de bits représentatifs du temps de traversée des équipements

G : bits de gestion (contrôle, adresse...)

K : bits d'accusé de réception

Soit, en reprenant l'équation (1) :

$$E_0 = U/N = U/(U + S)$$

E_0 : efficacité du protocole sans erreur

➤ Cas d'une transmission avec erreur

Si t_e (taux d'erreur) est la probabilité pour qu'un bit transmis soit erroné, $1 - t_e$ est la probabilité pour qu'un bit soit correctement transmis. Si la transmission porte sur N bits, la probabilité pour que N bits soient correctement transmis, est :

$$p = (1 - t_e)^N \quad \text{avec} \quad N = U + G.$$

© Dunod – La photocopie non autorisée est un délit

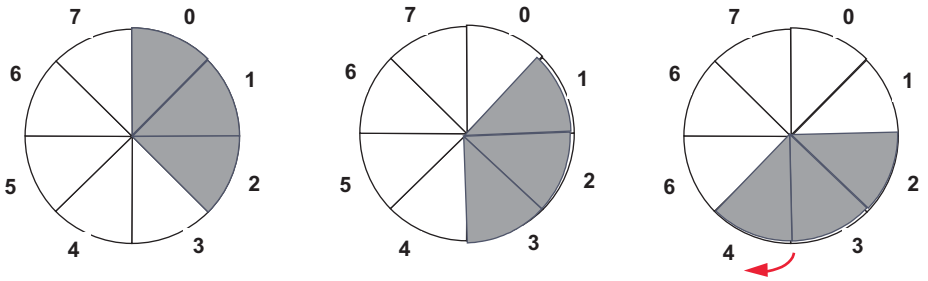


Figure 6.25 Gestion de la fenêtre dite « glissante ».

Cependant, chaque bloc n'a pas nécessairement besoin d'être acquitté individuellement. L'acquittement peut être différé et concerner plusieurs blocs. La figure 6.26 illustre ce propos. La fenêtre est de 3, l'acquittement du troisième bloc reçu (Nr = 3) acquitte les blocs 0, 1 et 2 et demande l'émission du quatrième bloc qui portera le numéro 3. Nr représente le numéro du prochain bloc attendu. L'acquittement est dit global ou différé.

Preview from Notesale.co.uk
Page 147 of 837

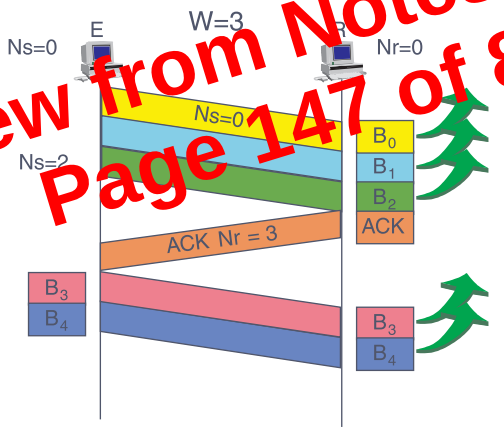


Figure 6.26 Principe de l'acquittement global ou différé.

Dans ce mode de fonctionnement, il y a arrêt des émissions quand le crédit d'émission est consommé. À la réception d'un ACK, la fenêtre se rouvre de tout le crédit, elle est dite **sautante** (figure 6.28).

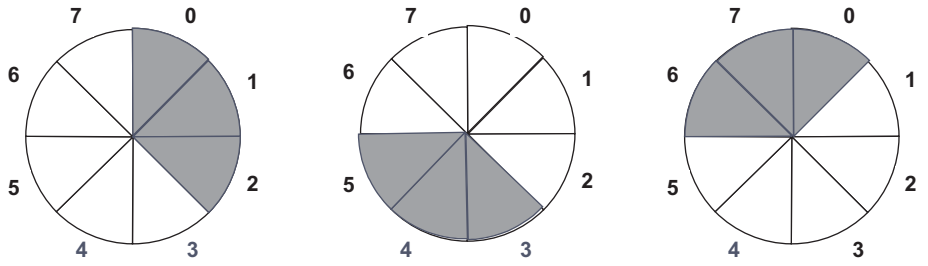


Figure 6.27 Gestion de la fenêtre dite « sautante ».

© Dunod – La photocopie non autorisée est un délit

le même support physique, on parle alors de **voies virtuelles**[10]. Dans un tel système, illustré figure 6.37, le canal de signalisation est établi en permanence, alors que le canal de données peut n'être établi qu'à la demande.

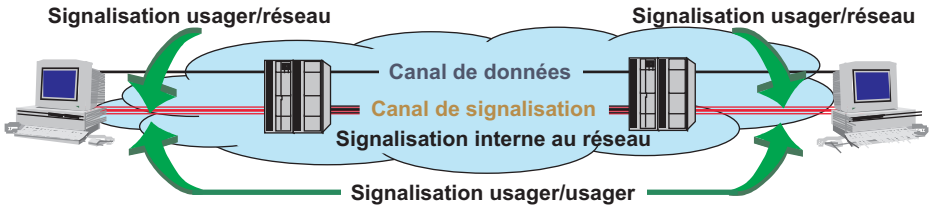


Figure 6.37 Signalisation par canal dédié à la signalisation.

La signalisation par canal dédié utilise un protocole différent du protocole de transfert de données : le protocole de signalisation. L'indépendance de ce protocole permet de multiplexer les informations transmises. Ainsi, il devient possible de distinguer différentes signalisations :

– la **signalisation usager/réseau**, chargée essentiellement de l'établissement de la liaison usager/réseau et de sa supervision ;
– la **signalisation interne au réseau** qui permet l'établissement d'une liaison à travers le réseau (routage ou acheminement) et de la contrôler durant l'échange ;
– la **signalisation usager/usager** dite aussi de **bout en bout**. Cette signalisation permet aux entités distantes de s'échanger des informations hors du protocole de transmission. C'est ainsi qu'il est possible de transmettre, via le protocole usager/usager de petites quantités d'information en l'absence de toute communication établie.

Preview from Notesale.co.uk
Page 154 of 837

Le Réseau téléphonique Numérique à Intégration de Service (**RNIS**) met aussi en œuvre ce type de signalisation. Cette approche est aussi utilisée dans tous les protocoles haut débit comme le **Frame Relay**[11] ou l'**ATM** (protocoles issus des travaux sur le RNIS Large Bande).

Figure 6.38 La signalisation par canal dédié.

Lorsque le support de communication est capable d'acheminer plusieurs communications, la signalisation des différentes communications peut être acheminée par un canal associé à chaque voie de communication. On parle alors de signalisation voie par voie ou **CAS**, *Channel Associated Signalling* (figure 6.38 gauche). Elle peut aussi être acheminée dans un canal

10. Nous montrerons au chapitre 7, lors de l'étude du multiplexage, comment sur une même voie physique on peut réaliser plusieurs canaux de communication (voies logiques).
11. Voir chapitre 11, section 11.2.4 et 11.2.5.

commun à toutes les voies de communication, on parle alors de signalisation par **canal sémaphore** ou **CCS**, *Common Channel Signalling*.

Le réseau téléphonique commuté utilise une signalisation de type CAS, alors que le réseau téléphonique à intégration de service met en œuvre une signalisation de type CCS.

6.5 ÉTUDE SUCCINCTE D'UN PROTOCOLE DE TRANSMISSION (HDLC)

6.5.1 Généralités

HDLC (*High Level Data Link Control*) est un protocole ligne dit de **point à point**. Dérivé de SDLC (*Synchronous Data Link Control*) d'IBM, il a été normalisé par le CCITT (UIT-T) en 1976.

L'unité de transfert d'HDLC est la trame (*Frame*), chaque trame est délimitée par un caractère spécifique : le fanion ou *Flag*. Ce caractère est le seul caractère spécial utilisé par le protocole. Le fanion est aussi employé pour maintenir, en l'absence de données à transmettre, la synchronisation entre les trames. La figure 6.39 représente le principe d'une liaison HDLC. Les symboles « F » représentent les fanions envoyés durant les silences pour maintenir la synchronisation. L'entité primaire désigne celui qui a initialisé la communication. Quand chaque entité peut initialiser la communication et émettre des commandes, le mode de fonctionnement est dit **équilibré**.

Preview from Notesale.co.uk
Page 155 of 837

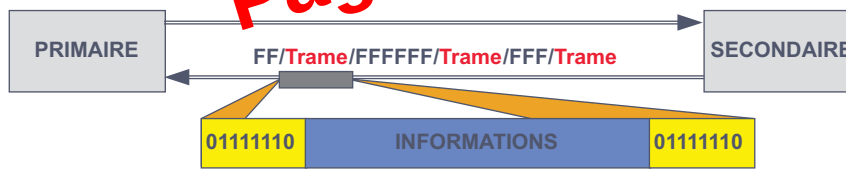


Figure 6.39 La liaison HDLC.

HDLC est un protocole qui utilise un mode de signalisation dans la bande. À cet effet, on distingue trois types de trames (figure 6.40).

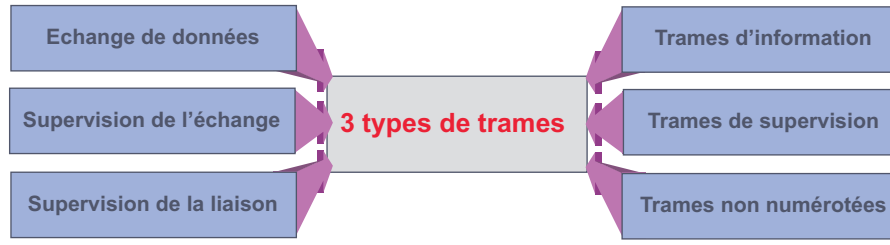


Figure 6.40 Les fonctions et trames correspondantes d'HDLC.

Les trames d'information ou trames **I** assurent le transfert de données ; les trames de supervision ou trames **S** (*Supervisor*) le contrôlent (accusé de réception...), les trames non numérotées ou trames **U** (*Unnumbered*) supervisent la liaison. Les trames U sont des trames de signalisation.

© Dunod – La photocopie non autorisée est un délit

Gestion des erreurs

La figure 6.48 illustre la reprise sur erreur. Supposons la trame 2 erronée, elle est ignorée par le récepteur. La trame 3 est alors reçue hors séquence, elle est rejetée. La machine B émet alors une trame de supervision de rejet (REJ, *Reject*) en indiquant à A à partir de quelle trame il doit reprendre la transmission [N(r) = 2]. Toutes les trames dont la valeur de Ns est supérieure à 2 sont alors rejetées (rejet simple).

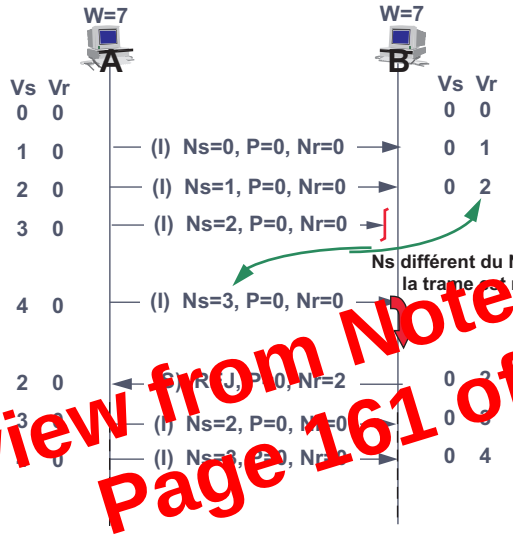


Figure 6.48 Gestion des erreurs.

Preview from Notesale.co.uk
Page 161 of 837

La machine A reprend la transmission à partir de la trame 2 (Ns = 2). Si, suite à la trame erronée, A n'avait plus de données à émettre, B n'aurait pas détecté le déséquencement. C'est A qui, à l'échéance du temporisateur T1, aurait pris l'initiative de retransmettre la trame 2.

Gestion du contrôle de flux

HDLC utilise le contrôle de flux implicite. La fenêtre est paramétrée à l'installation du logiciel ou négociée lors de la connexion par le protocole de niveau supérieur. En cas de saturation des tampons de réception, le récepteur, ici dans la figure 6.49 la machine B, rejette la trame en excès et informe A de son incapacité temporaire à accepter de nouvelles données. Il émet la trame « S » **RNR** (*Receive Not Ready*) avec le compteur Nr positionné au numéro de la trame reçue et rejetée.

La machine A prend en compte cette demande et interroge (*poll*) régulièrement (tous les T1) la machine B, pour d'une part signaler sa présence et d'autre part formuler auprès de B une demande de reprise de transmission à l'aide de la trame « S » **RR**, *Receive Ready*, avec le bit P à 1.

Lorsque B peut reprendre la réception, il le signale à l'émetteur en accusant réception à l'aide de la trame « S » RR. Le compteur N(r) contient le numéro à partir duquel la retransmission doit reprendre. A avait positionné le bit P à 1, la réponse de B est émise avec le bit F à 1.

© Dunod – La photocopie non autorisée est un délit

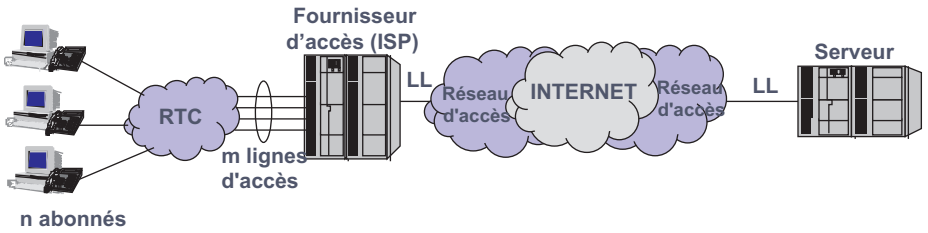


Figure 7.3 Détermination du nombre de lignes.

S'il dispose d'autant de lignes (m) que d'abonnés (n) aucun problème d'exploitation ne se présentera, mais il y aura vraisemblablement un « gâchis » de ressources. Si le nombre de lignes m est petit devant n, il y aura un taux de refus de mise en relation important. Le problème consiste donc à déterminer la valeur optimale du nombre de lignes nécessaires m pour que les abonnés aient une qualité de service acceptable (taux de refus faible et prédéterminé).

La relation entre intensité de trafic et ressources nécessaires a été étudiée par Erlang (mathématicien danois). Le dimensionnement des ressources nécessite de quantifier le trafic à écouler (Intensité de trafic), puis en fonction d'un taux de refus prédéterminé (probabilité que toutes les ressources soient utilisées quand l'utilisateur $n + 1$ désire se connecter) à définir le nombre de lignes m nécessaires.

Preview from Notesale.co.uk
Page 169 of 837

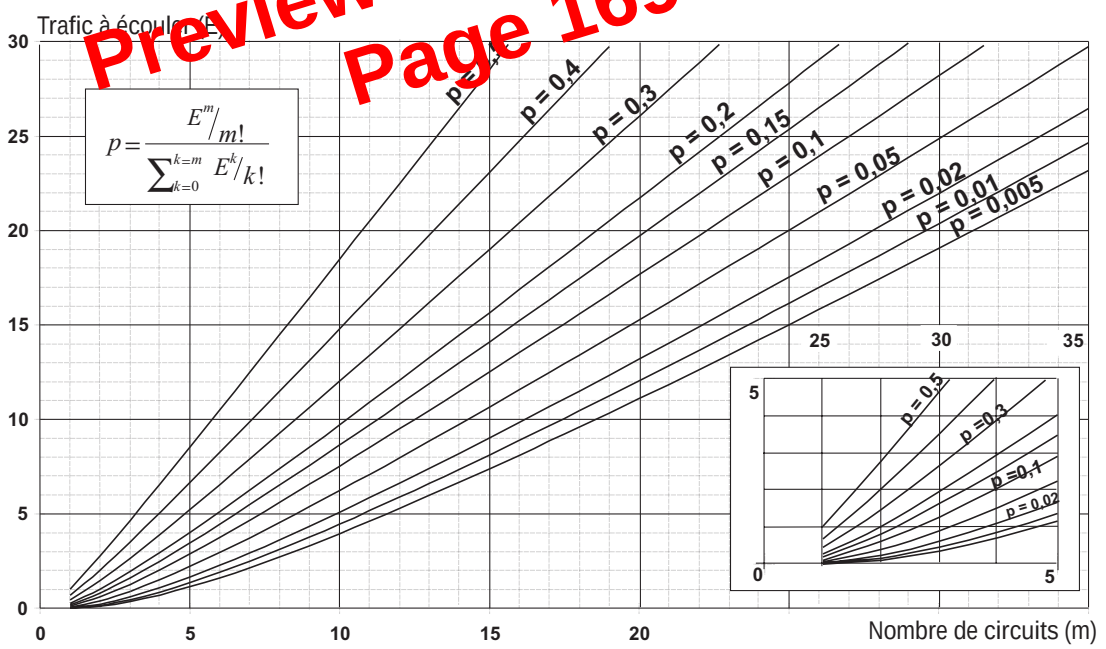


Figure 7.4 Abaque d'Erlang dit à refus.

Ce problème peut être résolu par l'utilisation de tables dites **tables d'Erlang** ou dites d'abaques d'Erlang. La figure 7.4 représente un abaque d'Erlang. Connaissant le trafic (E), la probabilité de refus (ou taux de blocage) choisie (p), il est possible de déterminer le nombre de lignes (m).

© Dunod – La photocopie non autorisée est un délit

capable d'analyser les données qu'il transmet. Il dispose, pour cela, d'une logique programmée.

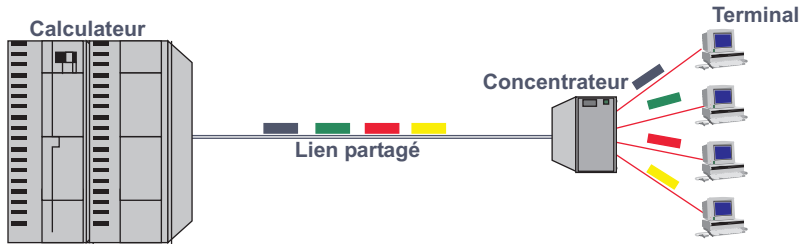


Figure 7.7 Principe de la concentration de terminaux.

Avec le développement des réseaux locaux, le concentrateur en tant que tel tend à disparaître. Un micro-ordinateur, désigné sous le terme de passerelle, assure la fonction de concentration. Un logiciel spécifique, chargé sur un micro-ordinateur, poste de travail émule le terminal passif traditionnel. Cette utilisation est illustrée par la figure 7.8.

Preview from Notesale.co.uk
Page 171 of 837

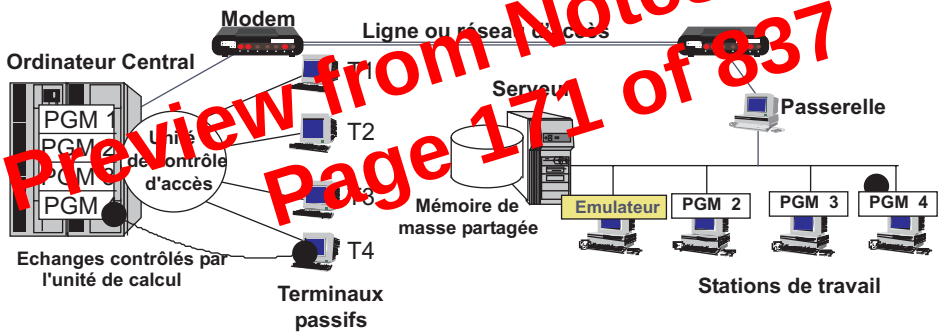


Figure 7.8 L'accès aux ordinateurs centraux via un réseau local.

7.2.2 Fonctionnalités complémentaires, exemple d'application

Le concentrateur, lorsqu'il reçoit un message l'analyse, interprète les données d'aiguillage et retransmet vers le destinataire les informations reçues en effectuant, éventuellement, une conversion de protocole. C'est le cas notamment des points d'accès vidéotex (**PAVI** figure 7.9).

Le PAVI est un concentrateur qui, outre les fonctions de concentration, assure :

– La conversion de protocole, les caractères reçus, en mode asynchrone en provenance du terminal Minitel (terminal asynchrone) sont regroupés en blocs de données (paquets) et émis en mode synchrone selon le protocole X.25[1] sur le réseau Transpac. De manière inverse, les données reçues sous forme de paquets par le PAVI, en provenance de l'ordinateur serveur, via le réseau X.25, sont désassemblées et transmises caractère par caractère au terminal Minitel (fonction **PAD**, *Packet Assembler Dissassembler*). Ce procédé évite que sur le réseau X.25 on ne fasse 1 caractère = 1 paquet.

1. Le protocole X.25 est étudié à la section 11.2.2. La société Transpac a mis en service en 1978 le premier réseau public de transmission en mode paquets X.25.

© Dunod – La photocopie non autorisée est un délit

Chapitre **8**

Le concept de réseau

Preview from Notesale.co.uk
Page 183 of 837

8.1 GÉNÉRALITÉS

8.1.1 Définition

Un réseau est un ensemble de moyens matériels et logiciels géographiquement dispersés destinés à offrir un service, comme le réseau téléphonique, ou à assurer le transport de données. Les techniques à mettre en œuvre diffèrent en fonction des finalités du réseau et de la qualité de service désirée.

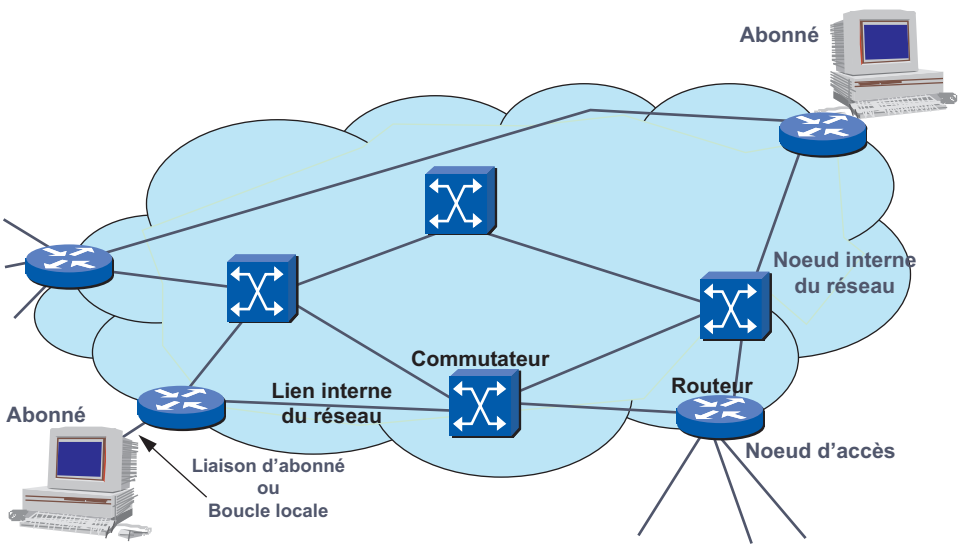


Figure 8.1 Le réseau : ensemble de ressources mises en commun.

Le réseau illustré par la figure 8.1 est composé de nœuds. Les nœuds d'accès, situés à la périphérie du réseau, permettent le raccordement des usagers par une liaison dénommée **liaison d'abonné**. L'ensemble des moyens mis en œuvre pour raccorder un usager est souvent désigné par le terme de **boucle locale**[1]. Les nœuds sont généralement des routeurs au point d'accès et des commutateurs au cœur du réseau.

8.1.2 Classification des réseaux

Le langage courant distingue les réseaux selon différents critères. La classification traditionnelle, fondée sur la notion d'étendue géographique, correspond à un ensemble de contraintes que le concepteur devra prendre en compte lors de la réalisation de son réseau. Généralement, on adopte la terminologie suivante :

- **LAN** (*Local Area Network*), réseau local d'étendue limitée à une circonscription géographique réduite (bâtiment...), ces réseaux destinés au partage local de ressources informatiques (matérielles ou logicielles) offrent des débits élevés de 10 à 100 Mbit/s.
- **MAN** (*Metropolitan Area Network*), d'une étendue de l'ordre d'une centaine de kilomètres, les MAN sont généralement utilisés pour fédérer les réseaux locaux ou assurer la desserte informatique de circonscriptions géographiques importantes (réseau de campus).
- **WAN** (*Wide Area Network*), ces réseaux assurent généralement le transport d'information sur de grande distance. Lorsque ces réseaux appartiennent à des opérateurs, les services sont offerts à des abonnés contre une redevance. Les débits offerts sont très variables de quelques kbit/s à quelques Mbit/s.

Preview from Notesale.co.uk
Page 184 of 837

D'autres classifications, plus proches des préoccupations quotidiennes, peuvent être adoptées. Le critère organisationnel prédomine. Le réseau est accessible à tous moyennant une redevance d'usage, il est alors dit public ; s'il n'est qu'à une communauté d'utilisateurs appartenant à une même organisation, il est alors dit privé. Un réseau public peut être géré par une personne privée (opérateur de télécommunication de droit privé), et un réseau privé peut être sous la responsabilité d'une personne de droit public (réseau d'un ministère...). Un réseau privé est dit **virtuel** lorsqu'à travers un réseau public on simule (émule) un réseau privé.

Les réseaux se différencient, aussi, selon les modes de diffusion de l'information (figure 8.2). On distingue trois modes :

- La source diffuse ses informations vers des stations réceptrices. La relation est unidirectionnelle de *1 à N* (réseau de diffusion). Les réseaux de radiodiffusion constituent un exemple de ce type de réseau. Les réseaux locaux sont aussi assimilés à cette catégorie.
- À l'inverse, un ensemble de stations peut envoyer les informations à un seul destinataire. La relation est aussi unidirectionnelle, mais de *N à 1* (réseaux de collecte). Les réseaux de télémesure constituent un exemple de ce mode de fonctionnement.
- D'une manière plus générale, un abonné d'un réseau désire pouvoir atteindre tous les autres abonnés ou une partie de ceux-ci. Le réseau doit établir une relation de *1 à 1* parmi *N*. Ces réseaux, de mise en relation, sont dits **réseaux de commutation**, le réseau téléphonique (RTC) en est un exemple.

1. Pour certains la boucle locale ne comprend que la liaison cuivre qui relie l'abonné au PoP (*Point of Presence*).

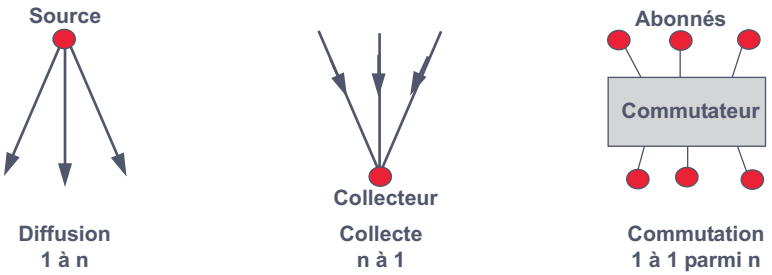


Figure 8.2 Classification selon les modes de diffusion de l'information.

Enfin, une autre distinction (approche temporelle) applicable à tous les réseaux décrit comment les différents nœuds (éléments actifs) d'un réseau sont synchronisés entre eux (figure 8.3) :

– Si chaque nœud a une horloge indépendante, le réseau est dit **plésiochrone**. Les horloges réception et émission sont différentes mais proches (plésio).

– Si les horloges des différents nœuds sont toutes asservies à une même horloge, le réseau est dit **synchrone**. L'horloge principale peut être une horloge atomique ou une horloge pilotée par les tops horaires d'un GPS.

Preview from Notesale.co.uk
Page 185 of 837

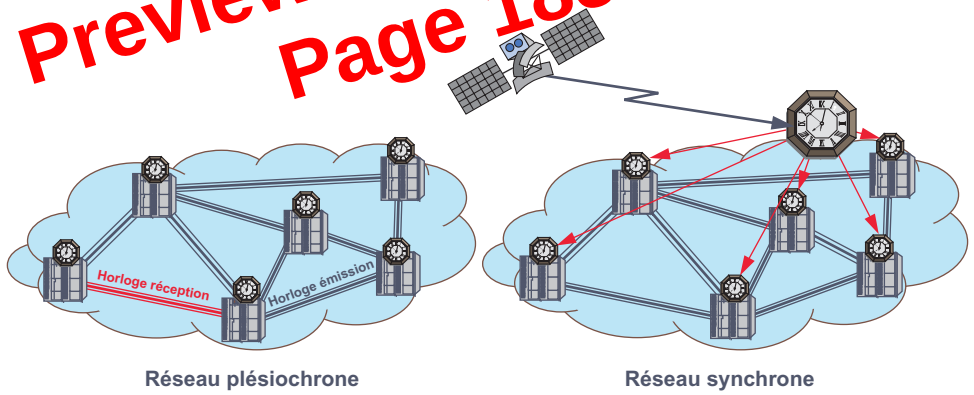


Figure 8.3 Distinction des types de réseaux selon le mode de synchronisation.

La synchronisation des réseaux et les problèmes en relation avec la distribution des horloges constituent un problème majeur de conception d'un réseau. L'étude de ces techniques sort du cadre de cet ouvrage.

8.1.3 Topologies physiques des réseaux

La topologie d'un réseau décrit la manière dont les nœuds sont connectés. Cependant, on distingue la **topologie physique**, qui décrit comment les machines sont raccordées au réseau, de la **topologie logique** qui renseigne sur le mode d'échange des messages dans le réseau (**topologie d'échange**).

© Dunod – La photocopie non autorisée est un délit

Dans ce contexte où la ressource est rare vis-à-vis de la demande potentielle (si simultanément tous les abonnés du réseau désiraient joindre un autre abonné...), il est indispensable de rechercher des techniques particulières pour optimiser le partage des ressources, c'est l'objectif des techniques de commutation. Selon la technique employée pour « relier » deux utilisateurs, on distingue la commutation de circuits, de messages ou de paquets.

Un réseau à commutation assure une connectivité totale. Dans ses conditions, la topologie logique ou interconnexion totale, vue du côté des utilisateurs, est différente de la topologie physique réelle (figure 8.10).

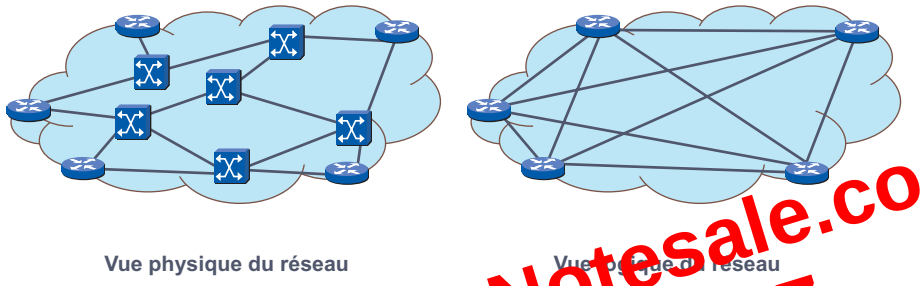


Figure 8.10 Conséquence de la commutation sur la vision du réseau

Preview from Notesale.co.uk
Page 189 of 837

8.2.2 La commutation de circuits

Dans la commutation de circuits, un chemin physique est établi par juxtaposition de différents supports physiques afin de construire une liaison de bout en bout entre une source et une destination (figure 8.11). La mise en relation physique est réalisée par les commutateurs avant tout échange de données et est maintenue tant que les entités communicantes ne la libèrent pas expressément. Le taux de connexion est important, alors que le taux d'activité peut être faible.

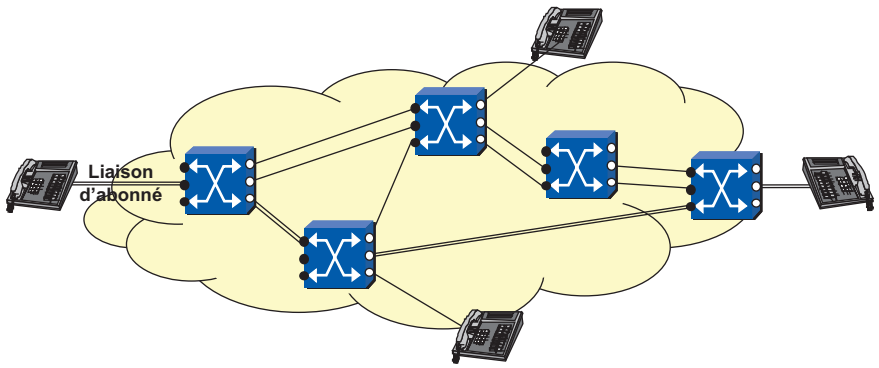


Figure 8.11 Réseau à commutation de circuits ou spatiale.

La constitution d'un chemin physique, emprunté par la suite par toutes les données transférées, garantit l'ordonnancement des informations. Elles sont reçues dans l'ordre où elles ont été émises. Cependant, les deux entités correspondantes doivent être présentes durant tout l'échange de données, il n'y a pas de stockage intermédiaire. Les débits de la source et du destinataire doivent être identiques. Les abonnés monopolisent toute la ressource durant la connexion. Dans ces conditions, la facturation est généralement dépendante du temps et de la distance (exemple : le Réseau Téléphonique Commuté ou **RTC**).

© Dunod – La photocopie non autorisée est un délit

ce mode d'adressage est utilisé dans les relations du type maître/esclave où le maître est toujours identifié. Seule l'adresse du terminal apparaît dans les échanges, elle désigne celui à qui on parle (adresse destination) ou celui qui répond (adresse source).

– Adresse source uniquement, le récepteur n'est pas identifié, toutes les stations à l'écoute reçoivent les informations (messages de diffusion, broadcast ou mode de contrôle maître/esclave).
– Adresse Source/Destination, cas le plus fréquent, l'adressage est alors dit distribué ou encore global distribué.
– L'adresse est absente du bloc de données, on lui a substitué un label. L'adressage est alors dit en cascade ou adressage de convention. La convention est établie pendant une phase d'initialisation, c'est le cas par exemple de l'attribution du numéro de voie logique dans le mode connecté.

Preview from Notesale.co.uk
Page 202 of 837

8.4 NOTIONS DE NOMMAGE

8.4.1 Le nommage

La notion de nommage est complémentaire de celle d'adressage, l'un désigne l'objet, l'autre précise sa localisation. Indépendamment qu'il est plus aisé de manipuler des noms que des adresses, l'avantage du nommage est essentiellement de dissocier l'objet de sa localisation géographique. Le déplacement de l'objet nommé est transparent à l'utilisateur. De manière similaire à l'adressage, le nommage attribue deux modes de représentation :

– Le **nommage à plat ou horizontal**, ce type de nommage impose une démarche rigoureuse pour garantir l'unicité d'un nom sur l'ensemble du réseau. NetBios, protocole allégé mis en œuvre dans les réseaux locaux, utilise un nommage à plat.

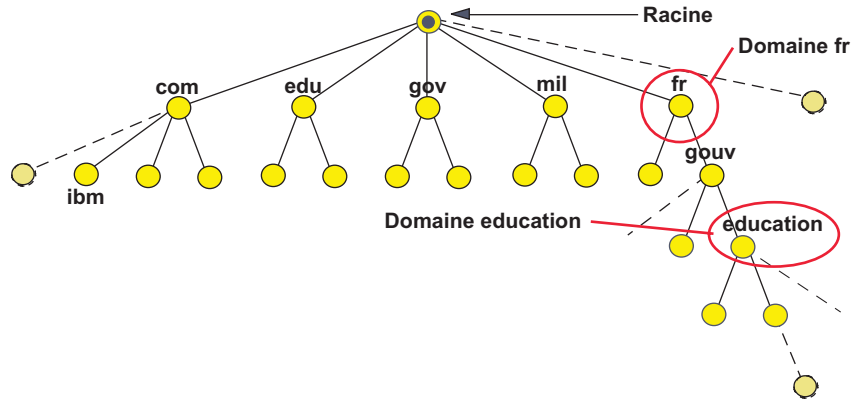


Figure 8.31 Arbre de nommage d'Internet.

– Le **nommage hiérarchique ou arborescent**, plus souple, organise le nommage en domaines. Cette technique autorise une représentation des objets calquée sur l'organisation de l'entreprise. Chaque nœud peut être un domaine dont la gestion peut être confiée à une

autorité particulière. Ce mode de représentation et d'administration convient parfaitement à la gestion d'un annuaire très important comme celui d'Internet (figure 8.31).

8.4.2 Notion d'annuaire

La localisation d'un objet nommé nécessite de mettre en relation son nom et son adresse : résolution de nom. L'association nom/adresse est résolue selon deux techniques (figure 8.32) :

– la consultation d'un fichier local, le nommage est alors dit local ;

– la consultation d'une base de données centralisée ou répartie sur un système local ou des systèmes distants, le nommage est, alors, dit **décentralisé**.

Figure 8.32 Principe de la résolution de nom.

Preview from Notesale.co.uk
Page 203 of 837

8.5 L'ACHEMINEMENT DANS LE RÉSEAU

8.5.1 Définitions

Acheminer les informations, dans un réseau, consiste à assurer le transit des blocs d'un point d'entrée à un point de sortie désigné par son adresse. Chaque nœud du réseau comporte des tables, dites **tables d'acheminement** couramment appelées **tables de routage**, qui indiquent la route à suivre pour atteindre le destinataire (figure 8.33). En principe, une table de routage est un triplet <Adresse destination>/<Route à prendre>/<Coût>.

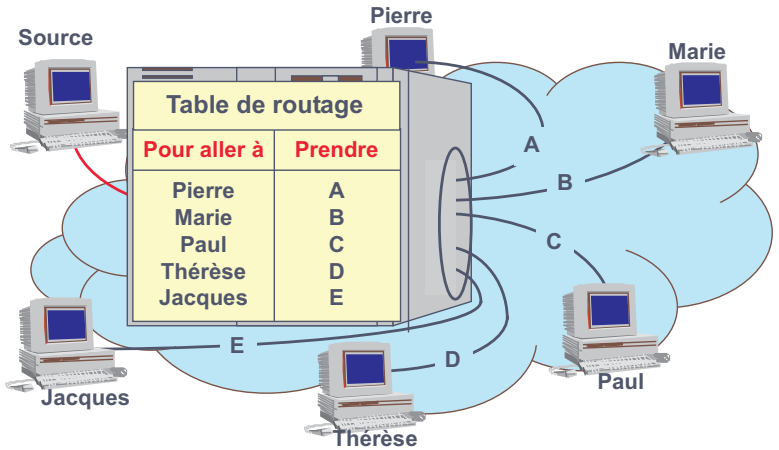


Figure 8.33 Principe d'une table de routage.

© Dunod – La photocopie non autorisée est un délit

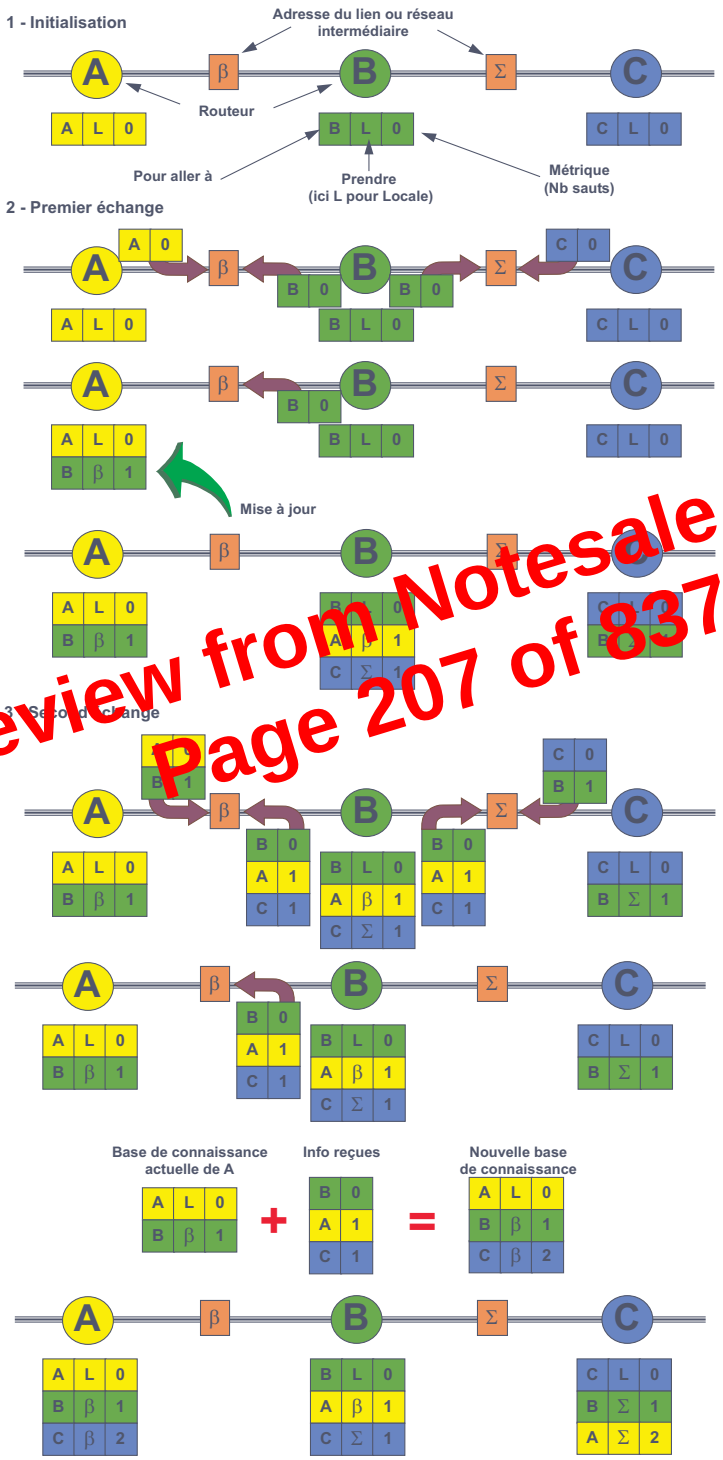


Figure 8.34 Échange des tables en routage vecteur distance.

Preview from Notesale.co.uk
Page 207 of 837

© Dunod – La photocopie non autorisée est un délit

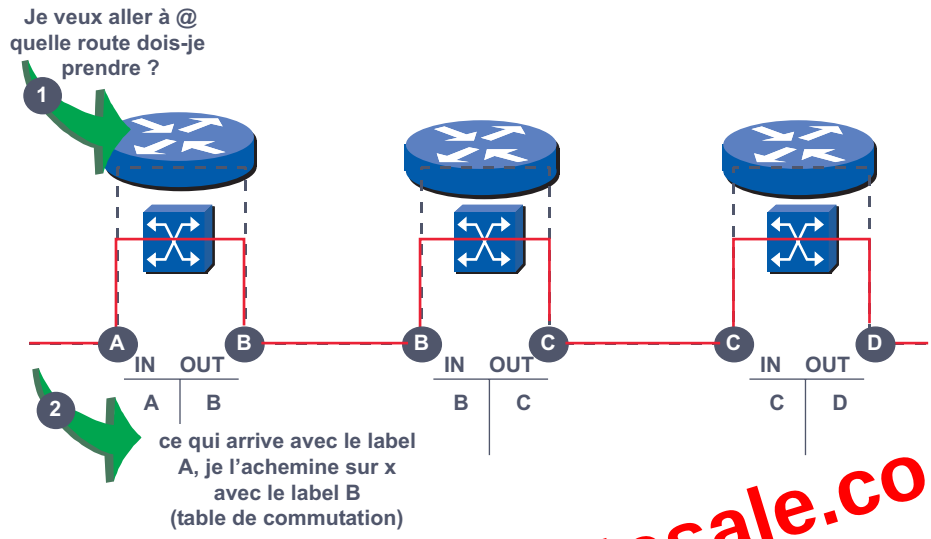


Figure 8.41 Après la phase d'établissement (1), la commutation (2).

Preview from Notesale.co.uk
Page 212 of 837

La décision de commutation est plus rapide que la décision de routage, les protocoles récents dits à haut débit comme le Frame Relay ou l'ATM (*Asynchronous Transfer Mode*) utilisent ce principe. Devant l'efficacité de ce mode d'acheminement dans les réseaux, l'IETF a défini, pour les protocoles réseaux en mode non connecté, le protocole **MPLS** (*MultiProtocol Label Switching*).

➤ MPLS

MPLS permet un acheminement commuté de datagrammes. À cet effet, un protocole de distribution d'identifiants de route ou labels prédétermine des routes en établissant une correspondance entre une destination IP et un label. En fonction de son adresse destination, chaque datagramme en entrée du réseau se voit affecter, par le routeur de périphérie d'entrée (*Edge Label Switching Router* ou **eLSR**), un identifiant de route (label). Il est ensuite acheminé dans le réseau par rapport à cet identifiant et non plus en fonction de l'adresse destination. Comme dans les réseaux en mode connecté, l'identifiant n'a qu'une valeur locale. Le routeur de sortie supprime le label et achemine le datagramme vers sa destination. L'ensemble forme un réseau MPLS (figure 8.42).

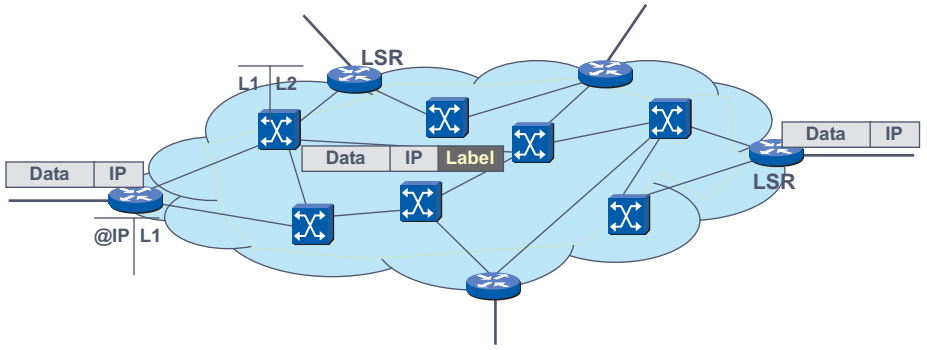
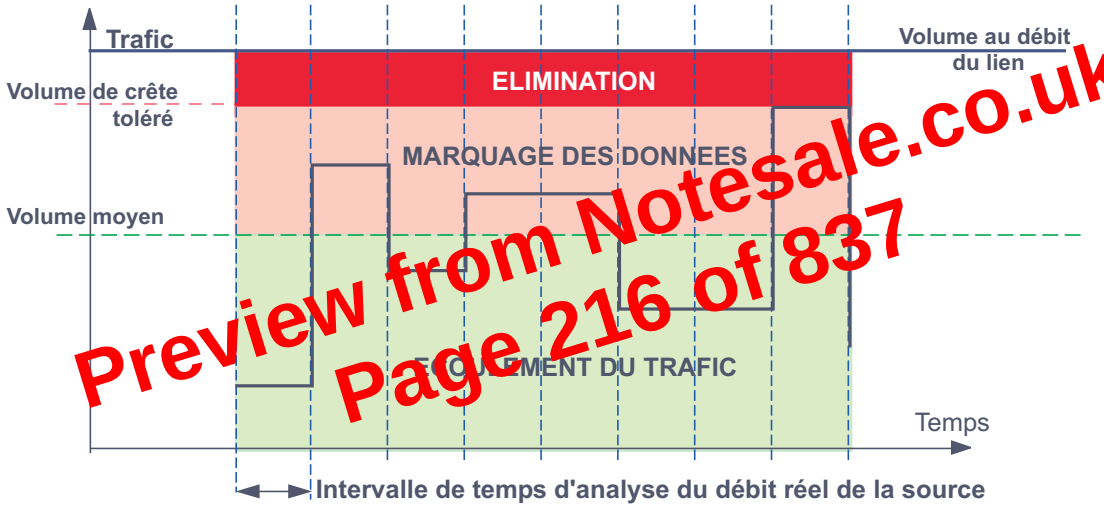


Figure 8.42 Principe de la commutation MPLS.

Cependant, le contrôle de flux est un mécanisme insuffisant. Compte tenu de la taille de la fenêtre, dans les réseaux haut débit, le contrôle de flux a été abandonné. Il ne subsiste que de bout en bout, c'est-à-dire entre machines d'extrémité.

Contrôle d'admission

Les réseaux en mode circuits sont naturellement protégés contre la congestion. En cas de manque de ressource dans le réseau, la connexion est purement et simplement refusée. Ce mode de prévention se heurte au principe de mutualisation des ressources. Une politique plus souple peut être utilisée : le contrat de service (figure 8.48).



Preview from Notesale.co.uk
Page 216 of 837

Figure 8.48 Principe du contrat de trafic.

Chaque abonné du réseau spécifie, à l'abonnement ou à la connexion, la description du trafic qu'il va soumettre au réseau (**CAC**, *Connection Admission Control*). Trois zones de fonctionnement peuvent alors être définies. La première correspond à un trafic garanti. Ce trafic, dit **trafic moyen**, est toujours écoulé dans le réseau quel que soit son état. La seconde zone correspond à une zone de tolérance, le trafic soumis est acheminé mais repéré (*Cell tagging*). En cas de congestion, il sera éliminé. Enfin, la troisième zone définit un trafic excédentaire, ou hors contrat, ce trafic est purement et simplement éliminé, il n'est jamais acheminé par le réseau. C'est le nœud d'entrée dans le réseau qui assure le contrôle d'admission.

Le lissage de trafic

Même si chaque source respecte son contrat de service, la congestion peut résulter d'une simultanéité de soumission de rafales par les différentes sources. Pour éviter cet afflux sporadique, on effectue, à l'entrée du réseau, un lissage du trafic (technique du seau percé, *leaky bucket algorithm*). Dans ce système, les données sont mises en file d'attente et délivrées régulièrement. Le mécanisme du seau percé est un mécanisme de prévention utilisé dans ATM, ce n'est pas un mécanisme de résolution, la figure 8.49 illustre ce principe.

EXERCICES

Exercice 8.1 Évaluation du nombre de liaisons

Déterminez le nombre de liaisons nécessaires à la réalisation d'une interconnexion totale entre 100 équipements.

Exercice 8.2 Table de routage

En reprenant la matrice de routage de la figure 8.36, établissez la table de routage du nœud B et déterminez la topologie du réseau.

Exercice 8.3 Temps de transfert sur un réseau

Deux réseaux LAN de type Ethernet (MTU 1 500 octets) sont interconnectés par un WAN. On vous demande de calculer le temps nécessaire à l'envoi d'un message de 4 500 octets dans les conditions suivantes :

- le protocole réseau nécessite 20 octets d'en-tête (In) ;
- le protocole de ligne utilisé sur les liens du WAN rajoute 8 octets d'en-tête (Hl).

et pour les différents modes suivants :

a) En mode commutation de circuits.

b) En mode commutation de messages (dans les mêmes conditions, c'est-à-dire par blocs de 1 500 octets). Le réseau comporte 5 nœuds hors organes d'extrémité.

c) En mode commutation de paquets (mode non connecté, mais les datagrammes seront supposés emprunter le même chemin). Le réseau comporte 5 nœuds hors organes d'extrémité. Faire le calcul pour un MTU de 57, 168, 316 octets. Rappelons que le LAN transmet au routeur des trames de MTU 1 500 octets, c'est le routeur qui a en charge l'adaptation des unités de données au réseau (segmentation).

Le débit des liens sera supposé de 64 kbit/s, les temps de traitement et des stockages intermédiaires seront considérés comme nul. On ne tiendra pas compte des temps d'émission sur les réseaux locaux, seul sera pris en compte le temps de traversée du WAN. Quels commentaires pouvez-vous faire ?

Preview from Notesale.co.uk
Page 220 of 837

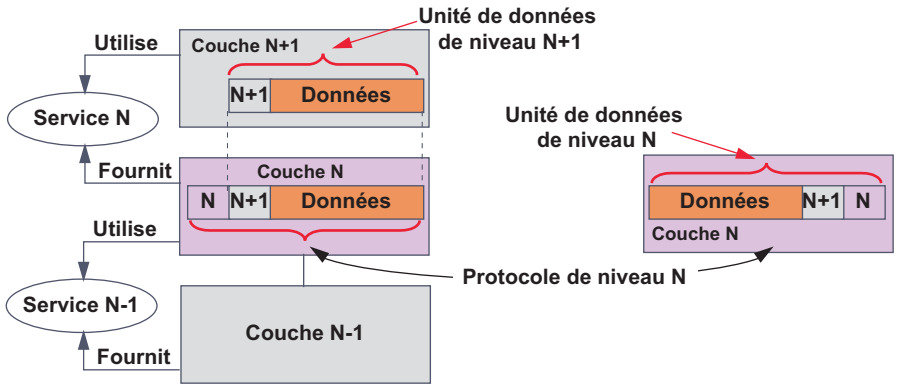


Figure 9.4 Service et encapsulation de données.

Preview from Notesale.co.uk
Page 224 of 837

Les services de la couche (N) sont offerts par une entité de niveau N et accessibles via une interface désignée par un identificateur ou point d'accès au service (SAP, *Service Access Point*). Un SAP ne peut être rattaché qu'à une seule entité, mais une même couche peut mettre en œuvre plusieurs occurrences de l'entité de niveau N.

Le dialogue OSI est un dialogue entre entités homologues distantes via une mise en relation ou connexion de niveau (N–1).

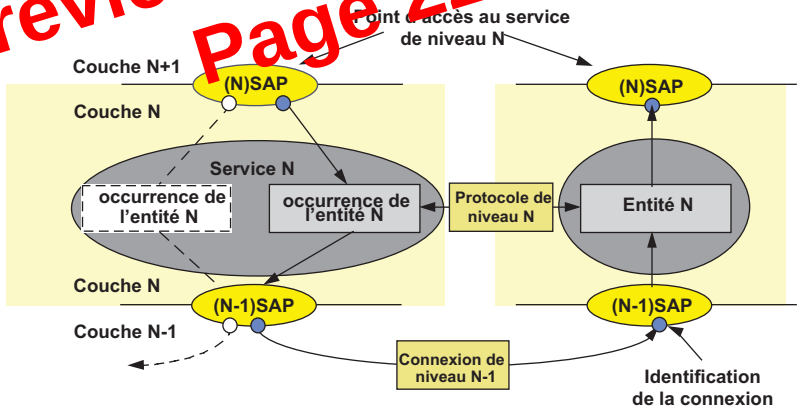


Figure 9.5 L'identification des services.

Les unités de données manipulées

Les données manipulées par une couche et envoyées à l'entité homologue constituent une unité de données (*Data Unit*). La couche de niveau (N + 1), utilisatrice des services de niveau (N), adresse à la couche (N), des unités de données de service notées (N)SDU[3] (*Service Data Unit*). Pour la couche (N), les données entrantes sont considérées comme utilisatrices du service (N).

3. Les notations OSI utilisent, pour désigner les couches, les notations suivantes :
– (N) SDU désigne une SDU de niveau (N) générique ;
– N_SDU désigne une SDU d'un niveau particulier, ici le niveau 3 (Network).

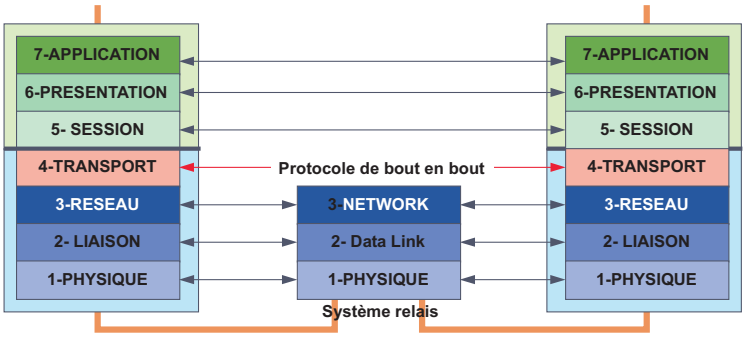


Figure 9.11 Le modèle de référence.

C'est ainsi, qu'après de nombreux débats, le modèle de référence a été défini en 7 couches (compromis entre 6 et 8 !). Le modèle de référence (figure 9.11) ne définit pas seulement des fonctionnalités de couche mais précise aussi la dénomination des unités de données (figure 9.13). La figure 9.12 détaille les fonctionnalités de chacune des couches composant le modèle.

Preview from Notesale.co.uk
Page 229 of 837

COUCHES	FONCTIONS
NIVEAU 1 **Couche Physique** ***Physical Layer***	La couche physique assure un transfert de **bits** sur le canal physique (support). À cet effet, elle définit les supports et les moyens d'y accéder : spécifications mécaniques (connecteurs), spécifications électriques (niveau de tension), spécifications fonctionnelles des éléments de raccordement nécessaires à l'établissement, au maintien et à la libération de la ligne. Elle détermine aussi les moyens d'adaptation (ETCD).
NIVEAU 2 **Couche Liaison de données** ***Data Link Layer***	La couche liaison assure, sur la ligne, un service de transfert de blocs de données (**trames**) entre deux systèmes adjacents en assurant le contrôle, l'établissement, le maintien et la libération du lien logique entre les entités. Les protocoles de niveau 2 permettent, en outre, de détecter et de corriger les erreurs inhérentes aux supports physiques.
NIVEAU 3 **Couche Réseau** ***Network Layer***	La couche réseau assure, lors d'un transfert à travers un système relais, l'acheminement des données (**paquets**) à travers les différents nœuds d'un sous-réseau (routage). Les protocoles de niveau 3 fournissent les moyens d'assurer l'acheminement de l'appel, le routage, le contrôle de congestion, l'adaptation de la taille des blocs de données aux capacités du sous-réseau physique utilisé. Elle offre, en outre, un service de facturation de la prestation fournie par le sous-réseau de transport.
NIVEAU 4 **Couche Transport** ***Transport Layer***	La couche transport est la couche pivot du modèle OSI. Elle assure le contrôle du transfert de bout en bout des informations (**messages**) entre les deux systèmes d'extrémité. La couche transport est la dernière couche de contrôle des informations, **elle doit assurer aux couches supérieures un transfert fiable quelle que soit la qualité du sous-réseau de transport utilisé**.
NIVEAU 5 **Couche Session** ***Session Layer***	La couche session gère l'échange de données (**transaction**) entre les applications distantes. La fonction essentielle de la couche session est la synchronisation des échanges et la définition de points de reprise.
NIVEAU 6 **Couche Présentation** ***Presentation Layer***	Interface entre les couches qui assurent l'échange de données et celle qui les manipule, cette couche assure la mise en forme des données, les conversions de code nécessaires pour délivrer à la couche supérieure un message dans une syntaxe compréhensible par celle-ci. En outre, elle peut, éventuellement, réaliser des transformations spéciales, comme la compression de données.
NIVEAU 7 **Couche Application** ***Application Layer***	La couche application, la dernière du modèle de référence, fournit au programme utilisateur, l'application proprement dite, un ensemble de fonctions (entités d'application) permettant le déroulement correct des programmes communicants (transferts de fichiers, courrier électronique...).

Figure 9.12 Brève description des fonctionnalités de chaque couche.

© Dunod – La photocopie non autorisée est un délit

9.3 ÉTUDE SUCCINCTE DES COUCHES

Nous limiterons cette étude aux fonctionnalités et particularismes essentiels de chacune des couches. Les protocoles et techniques en relation avec ces couches ont déjà fait l'objet d'étude ou le feront lors de l'étude des services qui les mettent en œuvre.

9.3.1 La couche physique

La couche physique (figure 9.17) fournit l'interface avec le support physique sur lequel elle transmet un train de bits en assurant, éventuellement, la transparence de binaire. Elle est chargée de la synchronisation entre les horloges source et destination. La couche physique ne distingue pas le mode connecté du mode sans connexion. Elle prend en charge les transmissions synchrones ou asynchrones en fonctionnement simplex, semi-duplex ou duplex que la liaison soit en mode point à point ou multipoint.

Les services fournis, à la couche liaison, sont :

– l'établissement et la libération de la connexion physique ;
– la transmission série et ou parallèle de « n » bits ;
– l'identification des extrémités de la connexion physique, qui peut être unique (liaison point à point) ou multiple (liaison multipoint) ;
– l'identification du circuit de données, cette identification pouvant être utilisée par les entités réseaux pour identifier un circuit de données (voie logique) ;
– le maintien en séquence des bits émis ;
– l'horloge et la récupération d'horloge (synchronisation) :
– la notification de dérangement.

Preview from Notesale.co.uk
Page 233 of 837

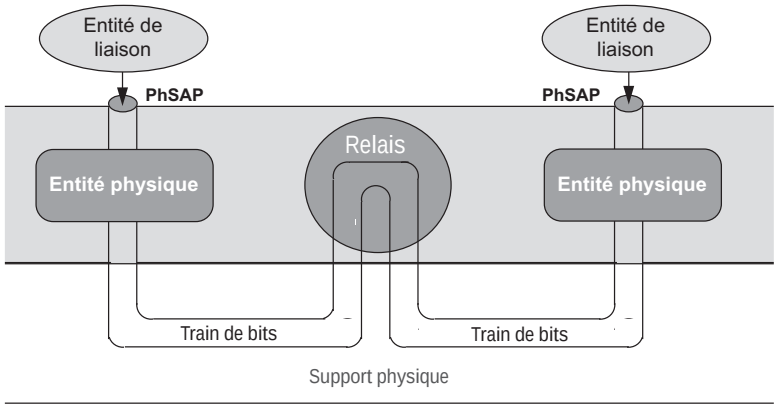


Figure 9.17 La couche physique.

La qualité de service fournie dépend essentiellement des supports utilisés, elle est caractérisée par le débit offert, le débit effectif, le taux d'erreur et la disponibilité.

Les normes couvertes par la couche physique comprennent principalement les normes relatives aux jonctions (V.24, V.35, X.21...) et aux ETCD (Modem, TNR – Terminaison Numérique de Réseau – ...).

© Dunod – La photocopie non autorisée est un délit

ROSE (*Remote Operation Service Element*)**,** ISO 9072, CCITT X.219 et X.229, comprend un ensemble de fonctions supportant les opérations interactives. ROSE est notamment utilisé dans le modèle client/serveur.

➤ Les principaux ASE fonctionnels

MHS (*Message Handling System***,** système de messagerie), ISO 10021, CCITT X.400/MOTIS, implémente un service de messagerie en mode non connecté. En cas d'absence du destinataire, le message est délivré dans sa boîte à lettres. X.400 offre les services de création, envoi, réception et stockage de messages.

DS (*Directory Service*), ISO 9594, CCITT X.500, offre un service d'annuaire, c'est une base de données permettant la localisation géographique (adresse) des équipements adressables connectés au réseau. La norme prévoit un seul annuaire mondial, en fait, il s'agit de réaliser un ensemble d'annuaires locaux coopérants. Les éléments sont adressés selon une organisation hiérarchique ou en arbre (**DIT**, *Directory Information Tree*). X.500 assure la correspondance entre un nom mnémonique et une adresse physique.

FTAM (*File Transfer, Access and Management*), ISO 8571, assure les opérations d'accès, de transfert et de gestion de fichiers distants. FTAM travaille sur des fichiers virtuels ou documents, c'est le système d'exploitation qui manipule les fichiers physiques. Trois types génériques de fichiers sont décrits dans FTAM :

– Les fichiers non structurés, dans ce type de fichiers, les applications ne connaissent pas la structure de ceux-ci, seules les opérations de lecture et d'écriture portant sur l'intégralité du fichier sont admises.
– Les fichiers structurés, constitués d'une suite d'enregistrements éventuellement associés à une clé. Il est possible d'accéder à un enregistrement spécifique, séquentiellement ou à l'aide de la clé associée. Toutes les opérations sur les fichiers sont autorisées : lecture, écriture, modification suppression ou ajout d'enregistrement.
– Les fichiers hiérarchisés, modèle plus général, ce type de fichier peut être représenté par un arbre, à chaque nœud est associée une clé.

DTP (*Distributed Transaction Processing*), ISO 10026, cet ASE est spécialement dédié à la gestion de transactions s'exécutant sur des terminaux répartis. DTP utilise la notion de transaction atomique afin de garantir l'intégrité des données (fichiers cohérents).

VT (*Virtual Terminal*), ISO 9040 et 9041, définit un terminal virtuel (nombre de lignes, nombre de caractères par ligne, attributs de caractères, fontes...). Il assure la correspondance entre les caractéristiques du terminal virtuel et le terminal du système physique réel. VT gère les différents types de terminaux :

– terminal en mode défilement ou rouleau ;
– terminal en mode page ;
– terminal en mode masque d'écran et données ;
– terminal graphique simple ou multifenêtre.

ODA (*Office Document Architecture*), ISO 8613, CCITT T.400, normalise une architecture de documents, ODA concerne le traitement de textes. ODA spécifie une structure générale de document comprenant :

Preview from Notesale.co.uk
Page 248 of 837

Taille du segment de données échangé

Chaque réseau, en fonction de ses caractéristiques spécifiques admet des unités de données de taille plus ou moins grande (**MTU**, *Maximum Transfer Unit*). Pour certains réseaux, cette taille est normalisée. C'est le cas, par exemple, pour les réseaux de type Ethernet où la MTU est fixée à 1 500 octets. Dans les réseaux étendus (WAN), la taille est déterminée par l'opérateur en fonction des caractéristiques de ses éléments actifs (buffers...). Un datagramme peut, pour atteindre sa destination, traverser plusieurs réseaux dont les MTU sont différentes. Si le datagramme à transférer a une taille supérieure à la MTU du réseau, le commutateur d'accès devra fractionner (segmenter) l'unité de données pour la rendre compatible avec les capacités de transport du réseau (figure 10.7).

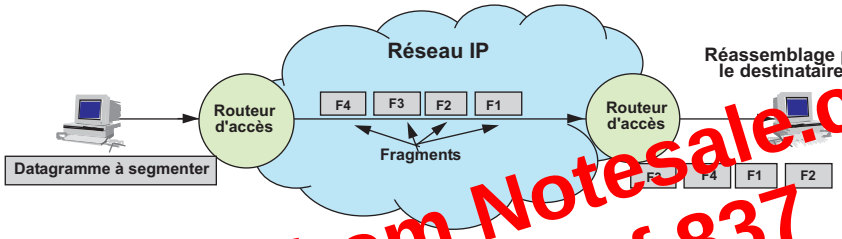


Figure 10.7 Principe de la segmentation sous IP

Preview from Notesale.co.uk
Page 264 of 837

Le routage de chaque fragment étant indépendant du précédent et du suivant, aucun nœud n'a la certitude de recevoir tous les fragments, dans ces conditions, seul le destinataire a la capacité de réassembler les différents fragments.

En mode datagramme la perte d'un seul fragment implique une retransmission complète du segment TCP d'origine. Si la connexion est locale, afin d'éviter la reprise d'un segment complet, on cherche à définir une taille de segment correspondant à la taille maximale que peut supporter le réseau. Pour l'interconnexion, via des réseaux de transport, cette taille est fixée à 576 octets, dont 536 utiles. Les passerelles interréseaux doivent être capables de traiter des segments de 576 octets sans avoir à les fragmenter. Néanmoins, cette taille n'est pas nécessairement compatible avec celle admissible par tous les sous-réseaux physiques traversés. Dans ces conditions, la couche IP fragmentera le bloc de données (datagramme IP), chaque fragment constituant un nouveau datagramme IP.

Lors de l'établissement de la connexion de transport, une option de TCP permet l'annonce, et non la négociation, de la taille maximale de segment que le système d'extrémité peut admettre (**MSS**, *Maximum Segment Size*). La figure 10.8 illustre la relation entre MSS et MTU pour la valeur par défaut de 576 octets de MTU. La MTU de 576 octets garantit une charge utile minimale de 512 octets aux données de l'application.

10.1.5 Les instances de normalisation

Plusieurs organismes contribuent à la cohérence des développements des protocoles liés à TCP/IP. Ce sont principalement **l'IAB** (*Internet Activities Board*) qui assure les relations avec les autres organismes de normalisation et définit la politique d'évolution à long terme. L'**IETF**

(*Internet Engineering Task Force*) se préoccupe des évolutions à court et moyen terme. Enfin, l'**IANA** (*Internet Assigned Number Authority*) gère l'attribution d'adresses IP. Des orga-

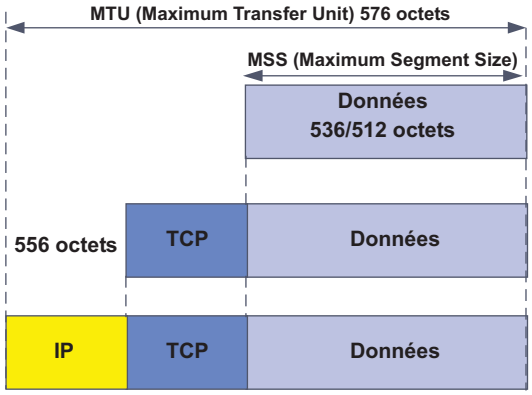


Figure 10.8 Relation entre MTU et MSS (Valeur implicite).

nismes régionaux agissent par délégation de l'IANA, c'est par exemple le **RIPE** (Réseaux IP Européens) représenté en France, depuis le 1er janvier 1998, par l'AFNIC (Association Française pour le Nommage Internet en Coopération). Les standards ou normes TCP/IP sont publiés sous forme de **RFC** (*Request For Comments*). La RFC 2026 décrit le processus d'élaboration (*The Internet Standards Process*).

Preview from Notesale.co.uk
Page 265 of 837

10.2 L'ADRESSAGE DU RÉSEAU LOGIQUE

10.2.1 Principe de l'adressage IP

Chaque machine (host), raccordée au réseau logique IP, est identifiée par un identifiant logique ou adresse IP (@IP) indépendant de l'adressage physique utilisé dans le réseau réel (figure 10.9). Le réseau logique IP masquant le réseau physique, pour assurer l'acheminement des données, il est nécessaire de définir des mécanismes de mise en relation de l'adresse logique, seule connue des applications, avec l'adresse physique correspondante (résolution d'adresses).

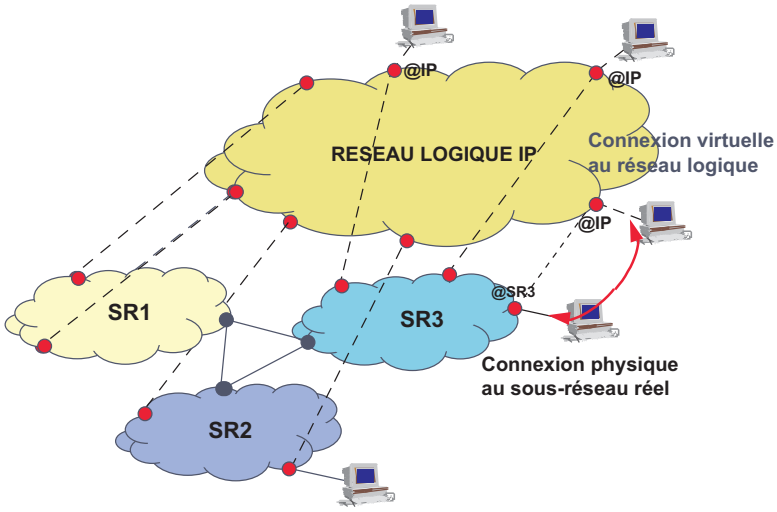


Figure 10.9 Nécessité d'une résolution d'adresses.

© Dunod – La photocopie non autorisée est un délit

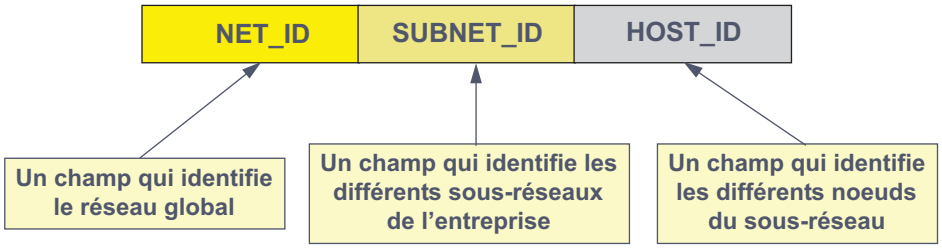


Figure 10.19 La technique du *subnetting* décompose l'adresse IP en 3 champs.

En principe, l'acheminement est réalisé à partir du champ <Net_ID> dont la taille, dépendant de la classe d'adressage, est connue de chaque routeur. L'utilisation d'un identifiant supplémentaire de longueur variable nécessite d'indiquer à chaque host du réseau quels sont les bits de l'adresse IP à prendre en compte pour définir l'acheminement dans le réseau. Cette information est fournie sous forme d'un champ de bits à 1 appelé **masque de sous-réseau** (figure 10.20).

Preview from Notesale.co.uk
Page 272 of 837

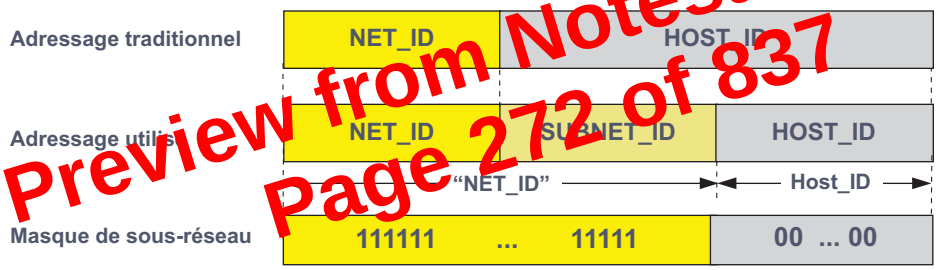


Figure 10.20 Principe du masque de sous-réseau.

Il existe deux méthodes d'écriture des masques de sous-réseaux, qui sont équivalentes :

– Réseau : 10.0.0.0, masque de sous-réseau 255.255.240.0 ;
– ou plus simplement 10.0.0.0/20, le préfixe 20 indique la longueur en bits du masque de sous-réseau (longueur du préfixe réseau ou simplement préfixe). Cette dernière écriture, plus simple, est à préférer à la précédente.

➤ Utilisation du masque de sous-réseau

Lorsqu'une station émet un datagramme à destination d'une autre station, la couche IP locale vérifie, à l'aide du masque de sous-réseau, si le datagramme appartient au même sous-réseau que celui de l'émetteur. Si le datagramme est destiné à une station située sur un sous-réseau distant, le datagramme est envoyé à la passerelle par défaut, charge à celle-ci d'adresser le datagramme vers le bon sous-réseau. Ainsi, une station d'un réseau logique IP doit connaître (figure 10.21) :

– son adresse IP ;
– le masque de sous-réseau ;
– l'adresse de la passerelle locale (routeur).

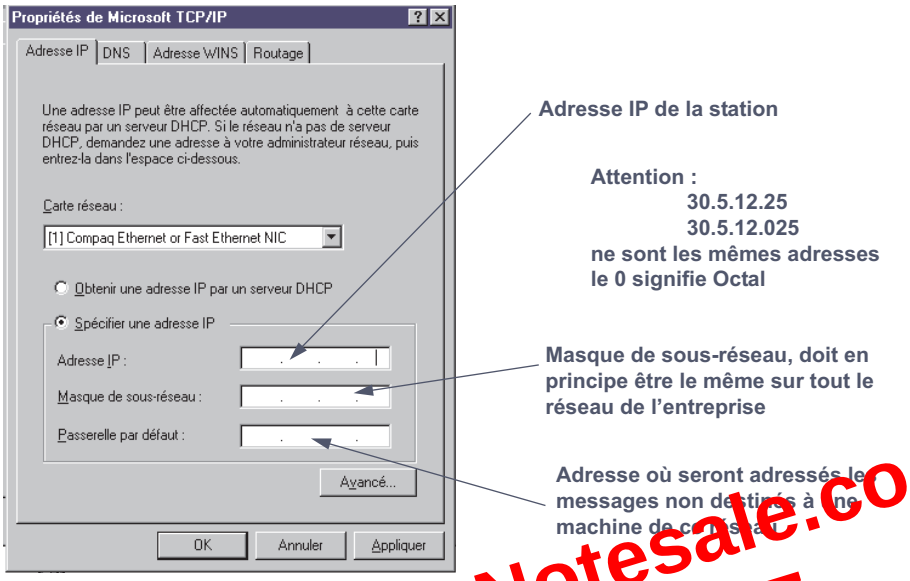


Figure 10.21 Informations de configuration d'une machine NT.

Preview from Notesale.co.uk
Page 273 of 837

Pour déterminer si la machine cible est localisée sur le même sous-réseau, la machine source réalise un « ET » logique entre les bits de l'adresse source et ceux du masque de sous-réseau, elle procède de même avec l'adresse destination. Si le résultat donne une valeur identique les deux machines sont sur le même sous-réseau, sinon le datagramme est adressé au routeur (figure 10.22).

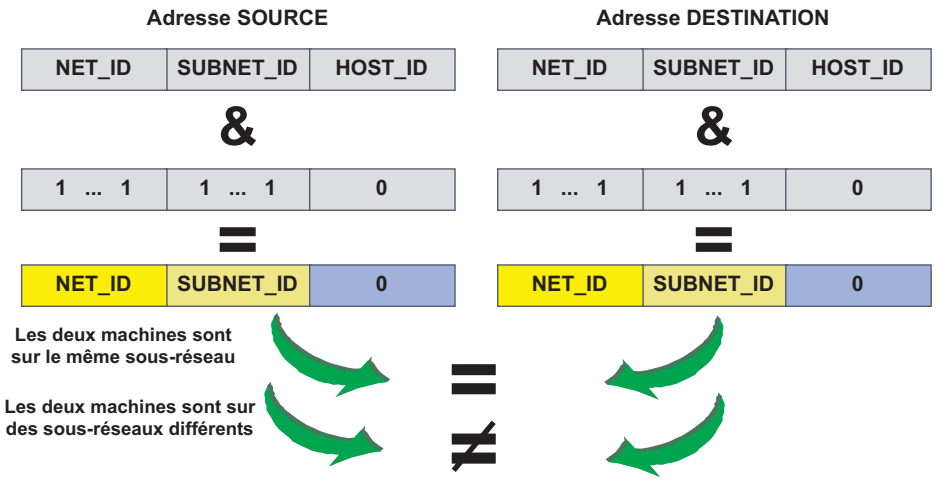


Figure 10.22 Détermination du sous-réseau cible à l'aide du masque de sous-réseau.

© Dunod – La photocopie non autorisée est un délit

Dans ces conditions les valeurs tout à <0> et tout <1> du champ <SubNet_ID> sont interdites. La capacité de numérotation (C_n) d'un masque de sous-réseau de n bits est de :

$$C_n = 2^n - 2$$

La première conséquence est que pour distinguer deux sous-réseaux il faut au moins 2 bits (figure 10.24) :

Valeur	Ordre du S/R
00	Interdit
01	1er S/R
10	2e S/R
11	Interdit

Figure 10.24 Capacité de numérotation de 2 bits.

Preview from Notesale.co.uk
Page 275 of 837

Ainsi, les critères à prendre en considération pour la détermination d'un masque de sous-réseau sont :

– l'espace de numérotation des hosts, c'est-à-dire le nombre de machines à numéroter et l'évolution probable de ce nombre (nombre de bits du champ <Host_ID>) ;
– l'espace de numérotation des sous-réseaux, c'est-à-dire le nombre de sous-réseaux à distinguer et l'évolution probable de ce nombre (nombre de bits du champ <SubNet_ID>) ;
– la lisibilité, c'est-à-dire permettre par simple lecture d'identifier facilement le sous-réseau concerné.

L'adressage géographique ou CIDR

Une adresse IP désigne une organisation, elle ne permet pas d'en déterminer la localisation, c'est un adressage à plat. Dans ces conditions, chaque routeur du réseau Internet doit tenir à jour la liste de toutes les adresses attribuées (Net_ID) et la route à suivre. Cet encombrement des tables de routage a conduit, lors de la recherche de solutions pour palier la prévisible pénurie d'adresses, à mettre en œuvre un mécanisme d'affectation géographique des adresses de classe C non attribuées.

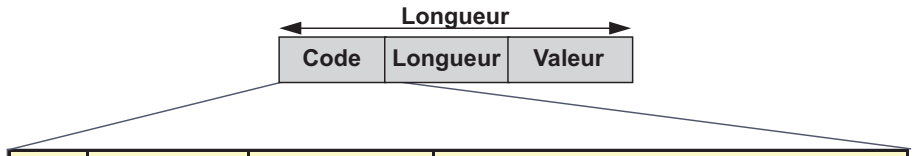
D'autre part, il a été décidé de n'attribuer qu'exceptionnellement les adresses de classes B restantes et d'attribuer en lieu et place des adresses contiguës de classe C, de leur faire coïncider une seule entrée dans les tables de routage et de réaliser une affectation géographique. La figure 10.25 indique les plages d'adresses géographiques (RFC 1466).

Ainsi, pour l'Europe les adresses 194 et 195 ont les 7 premiers bits identiques. Il suffit donc d'indiquer aux routeurs que le champ <Net_ID> à prendre en compte est de 7 bits et non de considérer ces adresses comme des adresses de classes C. Une seule entrée suffit alors dans la table de routage. Cette technique, issue de celle du masque de sous-réseau, porte le nom de *supernetting* ou routage interdomaine sans tenir compte de la classe d'adressage (**CIDR**, *Classless InterDomain Routing*).

Le nombre de bits servant à coder la partie commune, ou préfixe d'adresse, est représenté à la fin de l'écriture de l'adresse comme suit : 194.0.0.0/7, ainsi cette adresse indique tous les sous-réseaux européens.

© Dunod – La photocopie non autorisée est un délit

Le champ option, de longueur variable, est codé : code option (type), longueur, valeur. Le premier octet, l'octet code, est un champ de bits dont les différentes valeurs et leur signification sont indiquées dans le tableau de la figure 10.33.



Bit	Fonction	Valeur		Commentaire	
0	Copie	0		En cas de fragmentation, l'option n'est pas recopiée.	
		1		L'option est recopiée dans le fragment.	
1-2	Classe Option	00		Datagramme ou supervision de réseau.	
		01		Réservé pour une utilisation future.	
		10		Test.	
		11		Réservé.	
3-7	Numéro d'option	Classe	Valeur	Longueur	
		0	0		Fin de la liste d'options.
		0	1		Alignement d'octet.
		0	2	11	Restrictions de sécurité.
		0	3	var	Routage lâche par la source.
		2	4	var	Horodatage.
		0	7	var	Enregistrement route.
		0	8	4	Identificateur de connexion.
		0	9	var	Routage strict par la source.

Figure 10.33 Codage et options IP.

Preview from Notesale.co.uk
Page 281 of 837

La longueur du champ option étant variable, celui-ci peut-être suivi de bits de bourrage pour assurer l'alignement de l'en-tête sur des mots de 32 bits. Coûteux en terme de traitement pour les passerelles, le champ option est peu utilisé.

10.4.3 Contrôle de la fragmentation sous IP

La fragmentation d'un segment TCP est contrôlée par les champs : longueur totale (LEN), offset (Offs) dans le segment, et le bit MF du datagramme IP. Le champ offset indique, en multiples de 8 octets, la position du fragment dans le datagramme initial. Le fragment, ainsi constitué, ne peut avoir, pour longueur, que le multiple de 8 le plus proche de la MTU, sauf pour le dernier fragment.

Ainsi, pour une MTU de 128 octets (MTU d'un paquet X.25), la charge utile (niveau IP) ne peut être que de 108 octets (128 - 20 d'en-tête IP), soit une taille effective de 104 octets (13×8), si l'on tient compte de l'en-tête TCP (20 octets), la charge du premier fragment n'est que de 84 octets. La figure 10.34 illustre cette fragmentation pour un segment TCP de 576 octets. Pour faciliter la lecture les valeurs des champs Len et Offset sont exprimées en décimal.

Pour assurer le réassemblage, IP doit attendre l'arrivée de tous les fragments. Les opérations de fragmentation et de réassemblage sont coûteuses en terme de puissance de calcul et de mémoire. De plus, la perte d'un seul fragment provoque une reprise par la couche TCP du segment fragmenté.

© Dunod – La photocopie non autorisée est un délit

Les différents champs du segment sont :

– Numéro de port (2 fois 16 bits), valeurs spécifiées à la connexion, et identifiant celle-ci. Le port destinataire est soit connu, soit défini lors d'une phase d'identification (login) et passé à l'appelant en réponse.

– Numéro de séquence sur 32 bits, une valeur initiale et aléatoire (**ISN**, numéro de séquence initial) est définie et acquittée par les deux systèmes d'extrémité lors de la phase de connexion. Le numéro de séquence indique le rang du premier octet du segment transmis, les octets sont décomptés depuis le début de la connexion (Ns = ISN + Nb octets transmis + 1). Le numéro de séquence du premier octet transmis est (ISN +1).

– Le numéro de séquence acquitté indique le numéro du prochain octet attendu, c'est-à-dire le numéro de séquence du dernier segment reçu, incrémenté de la taille des données reçues.

– Longueur de l'en-tête ou *offset* (4 bits) indique la longueur de l'en-tête du segment TCP en multiples de 4 octets. La valeur 5 correspond à taille minimale de l'en-tête TCP (20 octets). Le champ longueur d'en-tête pointe sur le début des données.

– Un espace de 6 bits est disponible.

– Le champ drapeau contient 6 indicateurs[10] :

  – **URG** valide le champ pointeur sur données urgentes.

  – **ACK**, le bit ACK à 1 valide le champ numéro de séquence acquitté.

  – **PSH** TCP peut, pour des raisons d'efficacité du protocole, attendre d'avoir suffisamment de données à transmettre pour former un segment. L'indicateur PUSH permet de demander au destinataire de délivrer immédiatement les données en attente. Par exemple, l'application terminal virtuel associe, au caractère retour chariot (CR), la commande PSH.

  – **RST**, suite à la détection d'une anomalie grave sur le réseau, RST demande au destinataire de réinitialiser la connexion.

  – **SYN**, à 1 ce bit correspond à une demande de connexion, cet indicateur valide l'échange et l'acquittement des numéros de séquence initiaux (ISN).

  – **FIN**, ce drapeau correspond à une demande de déconnexion émise par l'un des interlocuteurs. Le destinataire d'une demande de déconnexion n'est pas obligé de s'exécuter (rupture de connexion négociée).

– Le champ fenêtre (2 octets) indique, en octets, la valeur de la fenêtre en réception, cette valeur varie dynamiquement en fonction de l'état du récepteur.

– Le total de contrôle est calculé sur l'ensemble du segment TCP, en-tête compris.

– Le pointeur sur données urgentes pointe sur le dernier octet urgent du champ de données. Dans TCP, il n'y a pas de notion de données express, les données comprises entre le début du champ données et la valeur du pointeur données urgentes sont traitées, en priorité, par le destinataire.

Preview from Notesale.co.uk
Page 290 of 837

10. Un segment TCP où les bits SYN, URG, PSH et FIN sont à 1 et qui ne contient qu'un octet de données est nommé « paquet Kamikaze ».

10.6 LES PROTOCOLES DE LIAISON (POINT À POINT)

10.6.1 Généralités

Bien que défini à l'origine pour s'appuyer sur des réseaux physiques existants, très vite la nécessité de définir des protocoles de niveau 2 est apparue (figure 10.55).

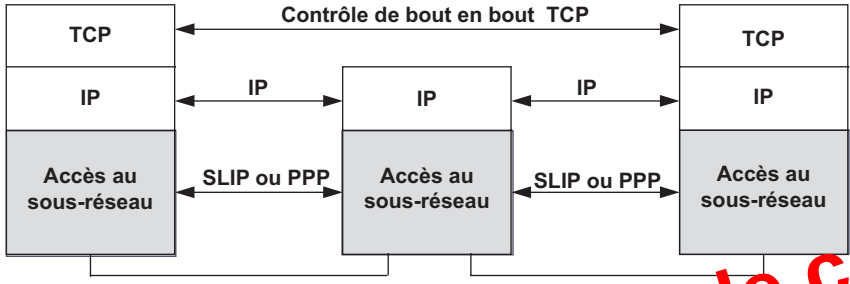


Figure 10.55 Position des protocoles de liaison.

Preview from Notesale.co.uk
Page 298 of 837

Les paquets IP ne peuvent être émis directement sur une liaison série. En effet, il convient au minimum d'assurer la délimitation des blocs de données (datagrammes), c'est l'un des rôles essentiels des protocoles de liaison (10.56).

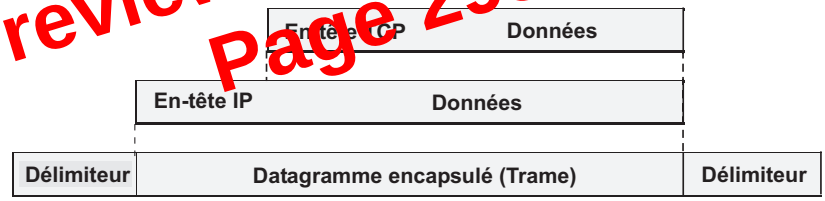


Figure 10.56 Délimitation des blocs de données.

Deux protocoles de liaison ont été spécifiés : **SLIP** (*Serial Line IP*) et **PPP** (*Point-to-Point Protocol*), le premier n'est utilisé que dans des liaisons point à point locales, car il suppose une ligne fiable, le second est notamment utilisé pour accéder, à travers le réseau téléphonique, à Internet.

10.6.2 SLIP, Serial Line Internet Protocol (RFC 1055)

SLIP est un protocole asynchrone orienté bloc. Très simple, il n'effectue que la délimitation de trames, et n'offre aucun mécanisme de détection et de reprise sur erreur (figure 10.57). Seule, la transparence aux caractères de délimitation est réalisée.

END 0xC0	Caractères à transmettre	END 0xC0

Figure 10.57 Format de la trame SLIP.

Le caractère END (192 ou 0xC0) est utilisé comme délimiteur de début et de fin. La transparence de caractère (un caractère END dans le champ données ne doit pas être interprété comme

Commande	Valeur dec.	Valeur Hex.	Signification
IAC	255	FF	Interpréter le caractère suivant comme une commande
DON'T *xx*	254	FE	Refus d'une option, le caractère suivant '*xx*' identifie l'option refusée
DO *xx*	253	FD	Acceptation de l'option '*xx*' (Start Use)
WON'T *xx*	252	FC	Acquittement négatif de l'option '*xx*'
WILL *xx*	251	FB	Acquittement positif de l'option '*xx*' (Will Use)
GA	249	F9	Continuer (Go Ahead)
EL	248	F8	Effacer une ligne (Erase Line)
EC	247	F7	Effacer un caractère (Erase Character)
AO	245	F5	Arrêter l'édition (Abort Ouput)
IP	244	F4	Interrompre le processus (Interrupt Process)
BRK	243	F3	Break
NOP	241	F1	Opération nulle (Non OPeration)
EOR	239	EF	Fin d'enregistrement (End of Record)

Commande	Valeur dec.	Valeur Hex.	Signification
Transmit Binaire	00	00	Transmission en mode 8 bits
Echo	01	01	Écho des données introduites au clavier (Echo Data)
Suppress go ahead	03	03	Passage en mode caractère
Linemode	34	22	Passage en mode ligne
Carriage Return	10	0A	Retour chariot, Positionne le curseur en début de ligne
Line Feed	13	10	Passage à la ligne suivante

Preview from Notesale.co.uk
Page 309 of 837

Figure 10.71 Principales commandes et options Telnet.

10.8 D'IPv4 À IPv6

10.8.1 Les lacunes d'IPv4

IPng (*next generation*) ou IPv6 répond au besoin d'évolution de la communauté Internet et comble les faiblesses d'IPv4. La plus connue concerne l'espace d'adressage, IPv4 met en place un adressage à plat (Net_ID) ce qui a conduit à l'explosion des tables de routage (certains routeurs Internet ont plusieurs dizaines de milliers d'entrées dans leur table de routage). Le CIDR (voir section 10.2.2) a partiellement répondu à ce problème en faisant disparaître la notion de classe d'adresses, en autorisant l'agrégation d'adresses de réseaux contigus en un seul préfixe réseau et en organisant une affectation géographique des adresses. La seconde concerne la prévisible pénurie d'adresses, l'utilisation d'un adressage privé associé à la translation d'adresses (NAT) résout partiellement ce problème mais pénalise fortement les performances.

Enfin, l'arrivée de nouvelles applications comme le multimédia et le besoin de services sécurisés ont motivé l'étude d'un nouveau protocole permettant d'augmenter l'espace d'adressage tout en conservant les grands principes qui ont fait le succès du protocole IP.

Les principales caractéristiques d'IPv6 sont :

– adressage étendu (128 bits au lien de 32) ;
– en-tête simplifié autorisant un routage plus efficace ;

© Dunod – La photocopie non autorisée est un délit

gigue s'exprime en amplitude (variation autour de la fréquence moyenne), de l'ordre de 10^{-5} à 10^{-6}, et en fréquence.

La seconde, beaucoup plus lente, s'appelle dérapage ou glissement, son cycle peut être très grand, c'est par exemple la variation de fréquence due aux variations de température durant la journée.

Pour remédier à ces écarts d'horloge et donc de débit, plusieurs solutions sont envisageables. La plus simple consiste à régénérer périodiquement le signal, les **répéteurs** ou **régénérateurs**, non seulement restaurent le signal (forme et amplitude) mais peuvent aussi recalibrer le signal autour d'une fréquence moyenne (figure 11.5).

Figure 11.5 Régénération du signal par un répéteur.

Preview from Notesale.co.uk
Page 324 of 837

Cependant, les bits sont reçus par les éléments actifs au rythme de l'horloge source. Si celle-ci est supérieure à celle de l'horloge émission, il est nécessaire de mémoriser les bits excédentaires en attente d'une période inverse de l'horloge source. En moyenne, les bits reçus ne peuvent excéder les bits émis. Pour limiter la taille des mémoires tampons, l'UIT-T a fixé des limites aux dérives d'horloge, la stabilité des horloges devant être d'autant plus grande que les débits sont importants.

La figure 11.6 représente un système de correction de gigue. La mémoire tampon (*buffer*) de réception est constituée par un registre à décalage « élastique ». Le *buffer* est plus ou moins rempli selon les écarts de rythme entre l'horloge de réception (Hr) et l'horloge d'émission (He). Ce dispositif est efficace mais introduit un retard (temps de rétention des bits).

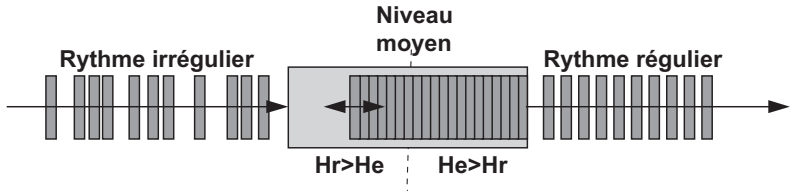


Figure 11.6 Principe de la correction de gigue d'horloge.

Lors des opérations de multiplexage, les différentes voies incidentes peuvent avoir des rythmes d'horloge différents. Les dispositifs précédents ne suffisent plus. La seule solution envisageable est alors de prévoir dans le train d'émission un cadrage variable des débits affluents. Ce principe, illustré par la figure 11.7, est utilisé aussi bien dans la hiérarchie plésiochrone (justification au niveau bit) que dans la hiérarchie synchrone (justification au niveau octet). Un pointeur permet de déterminer où débutent les données.

---

tifiable et engendre des décalages temporels entre les bits provoquant éventuellement des erreurs (saut de bits). L'autre, dépend essentiellement de la charge du réseau et de ses variations, elle n'engendre pas d'erreur binaire mais peut rompre, éventuellement, l'isochronie des paquets de données.

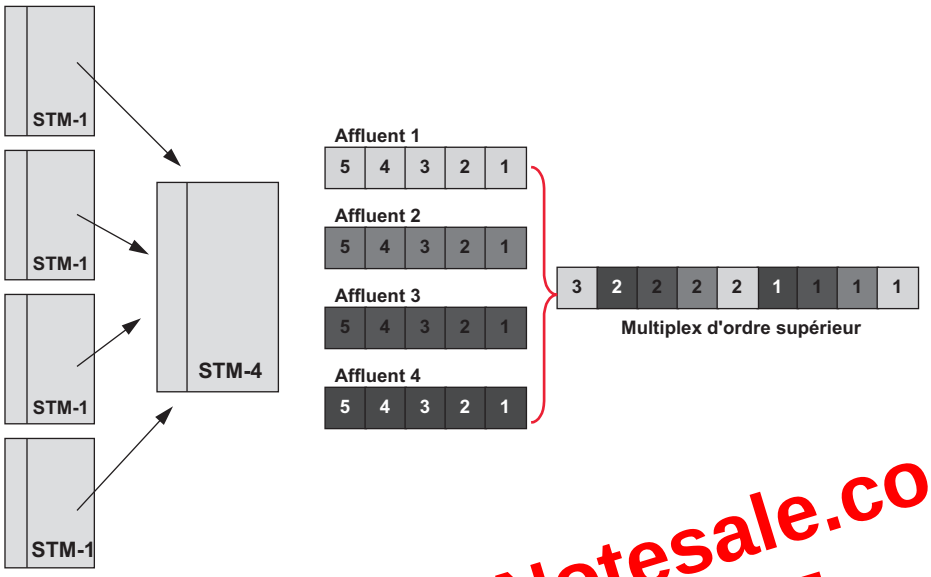


Figure 11.18 Principe du multiplexage d'octets.

Preview from Notesale.co.uk
Page 331 of 837

Un autre avantage des infrastructures SDH concerne les mécanismes de sécurisation automatique qui permettent le rétablissement du trafic dans des délais d'environ 50 ms. Ce mécanisme, dit **d'autocicatrisation** (*APS : Automatic Protection Swiching*), est basé sur l'utilisation d'informations de supervision contenues directement dans l'en-tête SDH (surdébit de section, SOH).

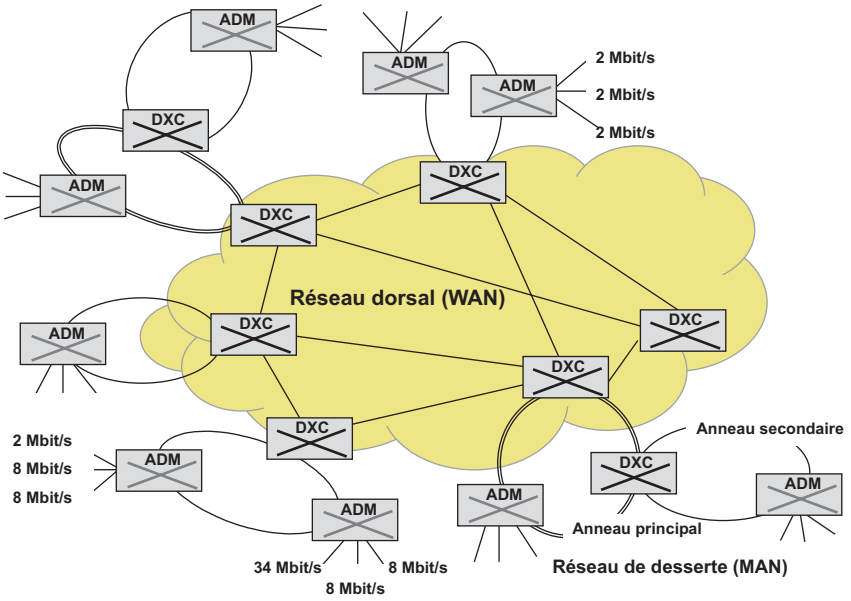


Figure 11.19 Principe d'un réseau SDH.

© Dunod – La photocopie non autorisée est un délit

Virtual Circuit). Elle résout les problèmes d'adressage et de multiplexage des connexions virtuelles sur la même liaison d'abonné. Le protocole X.25-3 assure le transfert de données, le contrôle de flux, la fragmentation et le réassemblage des paquets.

La procédure d'établissement des CVC établit une relation entre un numéro de voie entrante d'une part et le numéro de voie sortante d'autre part. Cette relation correspond à un lien virtuel entre les entités connectées (connexion virtuelle) similaire à la constitution d'un circuit en commutation de circuits. Le mode de mise en relation est dit orienté connexion. Ce procédé (figure 11.33) qui identifie une liaison, autorise le multiplexage des connexions sur une même voie physique et l'utilisation d'un adressage abrégé : le Numéro de Voie Logique (**NVL**).

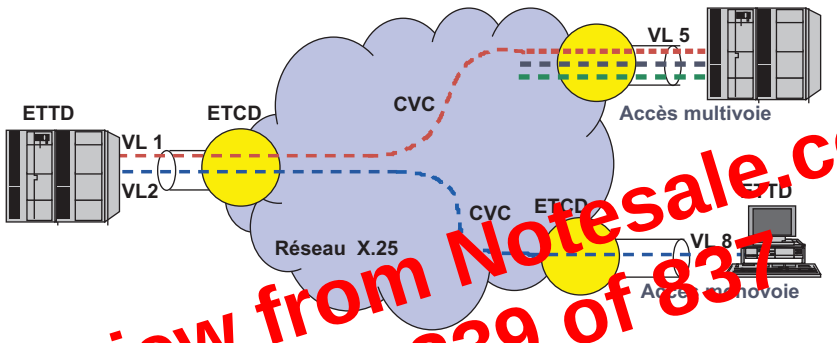


Figure 11.33 Mise en relation d'abonnés.

Preview from Notesale.co.uk
Page 339 of 837

➤ Format des unités de données

Les paquets X.25-3 comportent les informations relatives à l'adressage : le numéro de voie logique utilisée (adressage de convention), des informations de contrôle et éventuellement des données. Les paquets sont transmis à la couche trame qui les encapsule (figure 11.34).

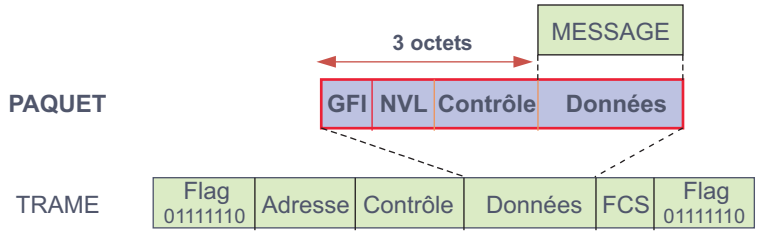


Figure 11.34 Encapsulation des paquets X.25 dans les trames LAPB.

Un paquet X.25, illustré figure 11.35, comporte au moins 3 octets. Le premier champ de 4 bits, dit champ **GFI** (*General Format Identifier*) définit certains paramètres de l'échange. Le premier bit a deux significations. Dans les paquets de données il est dit bit **Q** (*Qualified*), dans les paquets d'établissement bit **A** (*Address*). Le bit Q (bit à 1) est, par exemple, utilisé pour indiquer au PAD (accès asynchrone à X.25) que le paquet est une commande à son intention et non un paquet de données à transmettre à ETTD. Le bit A, dans les paquets d'établissement (ou d'appel) identifie le format du champ adresse. Si le bit A est à 0, l'adresse est au format X.121, sinon le format de l'adresse est indiqué dans le champ adresse. Le bit **D** (*Delivery*) détermine la portée des acquittements. Si le bit D est à 1 l'acquittement a une signification de bout en

© Dunod – La photocopie non autorisée est un délit

➤ Échange de données

Chaque circuit virtuel établi peut supporter un transfert de données bidirectionnel limité, en débit, par le paramètre **classe de débit**. La figure 11.41 illustre les paquets utilisés lors d'un échange de données.

Figure 11.41 Format des paquets de données, d'acquittement et de contrôle de flux.

La taille du champ de données est définie à l'abonnement ou par l'opérateur, cette taille est fixée par la norme X.25 à 16, 32, 64, 128, 256, 512, 1024, 2 048 ou 4 096 octets. L'échange de données s'effectue selon un mécanisme similaire à celui étudié pour HDLC. Les compteurs $P_{(s)}$ et $P_{(r)}$ des paquets de données permettent de vérifier le séquencement des paquets (perte éventuelle d'un paquet) et d'acquitter ceux-ci ($P_{(r)}$, numéro du paquet attendu). Les paquets **RR** (*Receive Ready*) et **RNR** (*Receive Not Ready*), (figure 11.41) assurent l'acquittement et le contrôle de flux.

Preview from Notesale.co.uk
Page 344 of 837

➤ Gestion des incidents

Lorsque le réseau, ou l'un des ETTD, détecte une désynchronisation des échanges (Numéros $P_{(s)}$, et $P_{(r)}$, il demande une réinitialisation des compteurs par l'émission d'un paquet de demande de réinitialisation. Les données en cours de transfert sont abandonnées, les compteurs sont remis à zéro. La demande de réinitialisation ne concerne que le CV sur lequel elle a été émise. Le mécanisme de la réinitialisation est illustré par la figure 11.42.

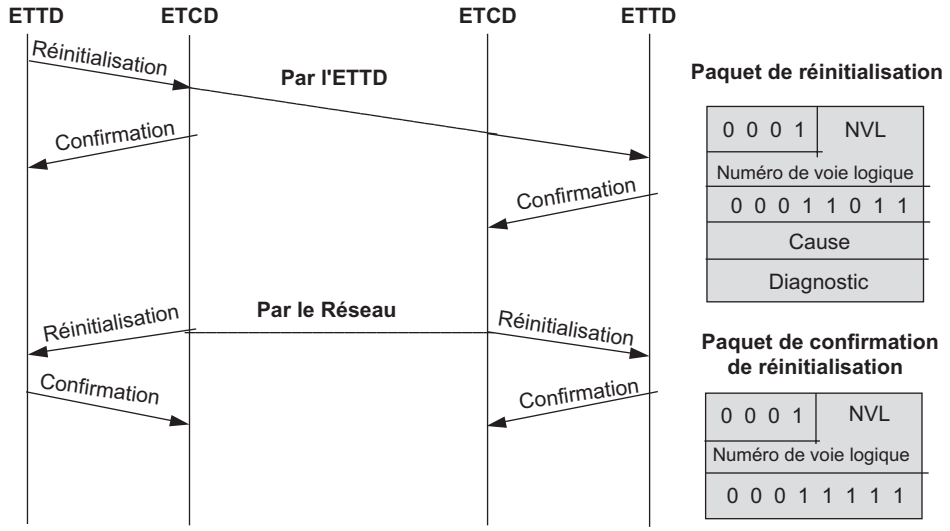


Figure 11.42 Mécanisme de la réinitialisation.

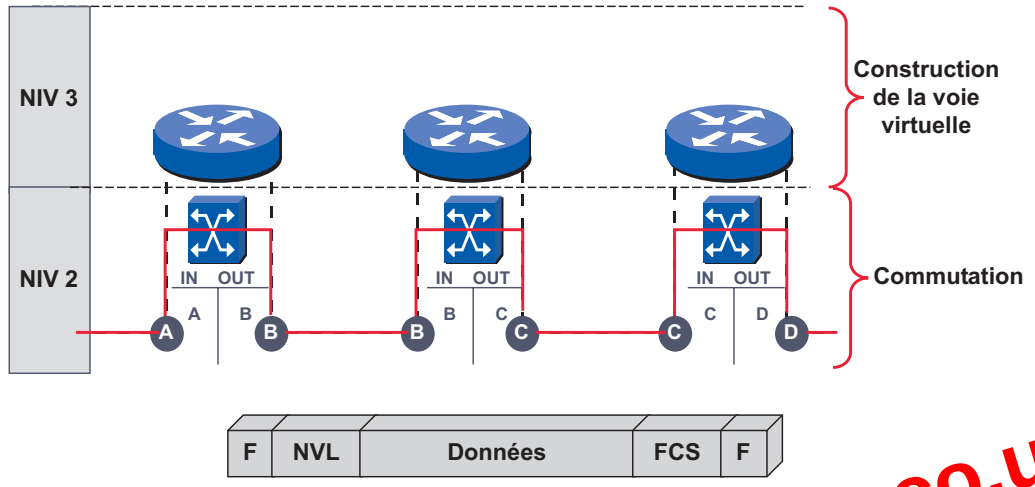


Figure 11.50 Première approche du Frame Relay.

Preview from Notesale.co.uk
Page 351 of 837

Par la suite, toutes les fonctions, non liées directement à l'acheminement furent abandonnées pour donner naissance au **relais de trames** (*Frame Relay*) ou encore **LAP-F**. Initialement prévue pour une utilisation sur le RNIS (Canal D ou sur un ou plusieurs canaux B), la technologie Frame Relay a rapidement évolué, sous l'égide du Frame Relay Forum[8], vers un service de liaison virtuelle permanentes, puis commutées utilisables sur tout support numérique hors RNIS.

Le relais de trames offre un service réseau en mode connecté conforme à l'avis Q.922 de l'UIT-T. La signalisation est du type canal sémaphore conforme à l'avis Q.933 (évolution de l'avis Q.931, protocole D du RNIS). Elle établit un service de liaison virtuelle entre les deux extrémités, qui peut être permanent (PVC, *Permanent Virtual Circuit*) ou établi à la demande (SVC, *Switched Virtual Circuit*). Actuellement, les opérateurs n'offrent qu'un service de circuits virtuels permanents.

Le relais de trames couvre les couches 1 et 2 du modèle OSI, mais n'est pas conforme à ce dernier. La couche physique émet un train de bits sur le support en assurant la transparence binaire (technique dite du *bit stuffing* ou de transparence binaire)

La couche 2 est subdivisée en deux sous-couches : le noyau (*Core*) et une sous-couche (**EOP**, *Element of Procedure*) complémentaire facultative. Non normalisée, ses fonctionnalités sont laissées à la discrétion de l'utilisateur. Cette sous-couche 2 supérieure peut, par exemple, être HDLC LAP-B. La répartition des fonctions essentielles est schématisée par la figure 11.51.

Format de l'unité de données

Le relais de trames utilise une trame de type HDLC (*High Level Data Link Control*) dérivée du LAP-D, délimitée par deux fanions (0x7E, 01111110B), elle comporte un champ adresse

8. Afin d'harmoniser les solutions, de combler les vides des normes et de proposer rapidement des solutions techniques cohérentes, les constructeurs se regroupent autour d'une technologie pour édicter leur propre règles : ce sont les forums constructeurs.

© Dunod – La photocopie non autorisée est un délit

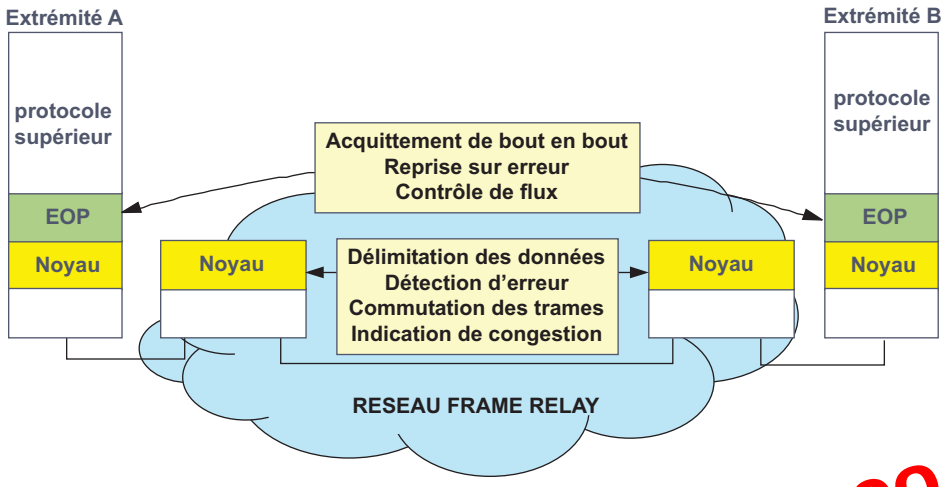


Figure 11.51 Architecture du relais de trames.

Preview from Notesale.co.uk
Page 352 of 837

de 2 à 4 octets, un champ données et un champ de contrôle d'erreur (FCS). Le champ contrôle (commande) d'HDLC est absent, il est inutile puisqu'il n'existe qu'un seul type de trame (signalisation par canal sémaphore). La figure 11.52 représente la trame Frame Relay.

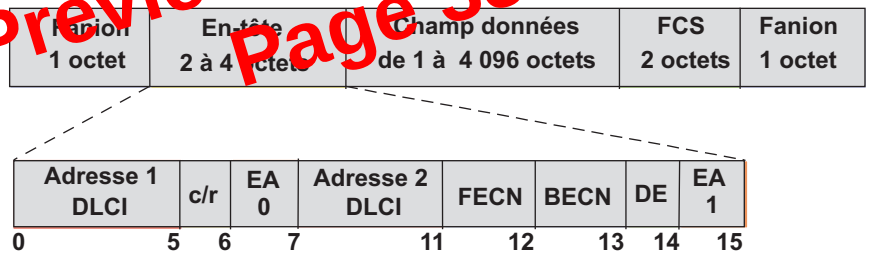


Figure 11.52 Trame Frame Relay.

Le champ adresse (**DLCI**, *Data Link Connection Identifier*) du relais de trames est subdivisé en plusieurs éléments. Dans la version de base, il est composé d'un premier bloc de 6 bits et d'un second de 4 bits (10 bits au total). Le champ **EA** (*End Address*) indique si le champ adresse a une suite (EA = 0) ou s'il est le dernier (EA = 1). Dans les versions étendues, le champ adresse est incrémenté de 1 octet (7 bits et le bit EA). L'adresse peut donc être exprimée sur 10 bits (version de base), 17 bits (en-tête de 3 octets) ou 24 bits (en-tête de 4 octets).

Le champ **C/R** (*Commande/Response*) a la même signification que le bit P/F (*Poll/Final*) d'HDLC. Les bits **FECN** (*Forward Explicit Congestion Notification*) et **BECN** (*Backward Explicit Congestion Notification*) sont utilisés pour signaler aux organes d'extrémité l'état de congestion d'un élément du réseau. Le bit **DE** (*Discard Eligibility*) est positionné par le réseau ou par les organes d'accès (**FRAD**, *Frame Relay Access Device*) il indique les trames à éliminer en priorité lors d'une congestion. Le FRAD est l'équipement interface entre le réseau de l'utilisateur et le réseau *Frame Relay*.

Une capacité d'adressage sur 10 bits ne permet d'identifier que 1 024 (2^{10}) voies logiques, ce qui est suffisant pour la plupart des utilisateurs mais peut s'avérer faible pour l'identification des voies en interne dans le réseau. Aussi, un adressage étendu sur 17 et 24 bits est prévu (figure 11.54). Le format représenté correspond au format du Frame Relay Forum (les bits FCEM et BCEM ont une position fixe). Le tableau de la figure 11.55 décrit l'utilisation des diverses plages d'adressage pour l'adressage normal (10 bits).

DLCI	Utilisation
0	Établissement de circuits (Q.931)
1-15	Réservés
16-1007	DLCI utilisateurs (PVC, SVC)
1008-1018	Réservés
1019-1022	Multicast
1023	Signalisation de la congestion (CLLM ou LMI) et état des liens

Figure 11.55 Fonctions des différents DLCI à l'interface usager.

Preview from Notesale.co.uk
Page 354 of 837

L'adressage des terminaux n'est pas fixé par la norme, le réseau peut spécifier des adresses de type E.164 (RNIS), X.121 (X.25) ou encore IP (TCP/IP).

➤ Le traitement des erreurs

Le traitement des erreurs n'est pas réalisé dans le réseau : chaque commutateur n'assure qu'une vérification d'intégrité de la trame :

- délimitation de la trame ;
- validation du DLCI ;
- contrôle d'erreur (FCS).

Toutes les trames non valides sont purement et simplement éliminées. Le traitement des erreurs est reporté sur les organes d'extrémité, il est confié aux protocoles de niveau supérieur, qui devront éventuellement mettre en œuvre des mécanismes de :

- numérotation des blocs de données pour la détection de perte ;
- reprise sur temporisation ;
- reprise sur erreur.

➤ Le contrôle d'admission

La simplification du protocole a conduit à la suppression de tout contrôle de flux dans le réseau et à fragiliser celui-ci face aux problèmes de congestion. Aussi, toute nouvelle connexion ne doit être acceptée que si le réseau est apte à la satisfaire sans préjudice pour les connexions déjà établies. Dans les réseaux de type X.25, le contrôle d'admission est effectué à l'établissement du circuit : dans chaque nœud sont réservées les ressources nécessaires au traitement des données (buffer), si il n'y a plus de ressources disponibles la connexion est refusée. Cependant, la réservation statique des ressources est incompatible avec l'admission d'un trafic en rafale qui rend le dimensionnement du réseau difficile. En Frame Relay, toute demande de connexion est accompagnée d'un descripteur de trafic définissant en particulier le débit moyen et le débit de pointe demandé. Un contrat de trafic est passé entre la source et le réseau ; il comporte trois paramètres :

	X.25	Frame Relay
Niveau 1	Délimitation des trames Transparence binaire	Délimitation des trames Transparence binaire
Niveau 2	Type de trames Validité de la trame (contrôle d'erreurs) Contrôle de séquencement Gestion de la fenêtre Gestion des temporisations Acquittement éventuel	Validité de la trame (contrôle d'erreurs) Validité du DLCI (DLCI connu) Acheminement Éventuellement positionnement des bits ED, EFCN, BFCN.
Niveau 3	Type de paquets Contrôle de séquencement Gestion de la fenêtre Gestion des temporisations Acquittement éventuel Routage	

Figure 11.62 Comparaison des traitements X.25/Relais de trames

Preview from Notesale.co.uk
Page 361 of 837

des trafics sporadiques (réseaux locaux, applications client serveur), il a été adapté au transport des flux isochrones comme la voix[10] (FRF.11 et FRF12).

11.2.5 L'ATM (Asynchronous Transfer Mode)

Généralités

Le relais de trames n'est qu'une évolution d'HDLC (LAP-D). Peu adapté, en natif, au transfert des flux isochrones, il n'est parfois perçu que comme une solution temporaire au besoin de haut débit. Ses limitations sont essentiellement dues au traitement d'unités de données de taille variable. Pour pallier cet inconvénient, la recommandation FR11 (Frame Relay Forum 11) introduit, pour le traitement de la voix, la notion de trames de longueur fixe.

En traitant des unités de données de taille réduite et fixe (cellules), les temps de traitements sont considérablement réduits. On peut alors assurer leur commutation par des systèmes matériels (*hardware*) et non plus logiciels, ce qui autorise des débits de plusieurs centaines de Mbit/s.

C'est sur ces bases que le CNET (Centre Nationale Etude et de Télécommunication) a décrit, en 1982, une technique de multiplexage asynchrone (**ATD**, *Asynchronous Time Division*) qui allait donner naissance à l'ATM. L'ATM supporte des liaisons point à point, ou point à multipoint, il comporte trois couches dont les fonctions essentielles sont (figure 11.63) :

– assurer l'adaptation des cellules au système de transport physique utilisé (couche physique),
– effectuer la commutation et le multiplexage des cellules (couche ATM à proprement parler),
– adapter les unités de données (segmentation et réassemblage) des protocoles supérieurs à la couche ATM (couche **AAL**, *ATM Adaptation Layer*) et mettre en place des mécanismes spécifiques à chaque type de données transportées.

10. Voir section 16.6.

© Dunod – La photocopie non autorisée est un délit

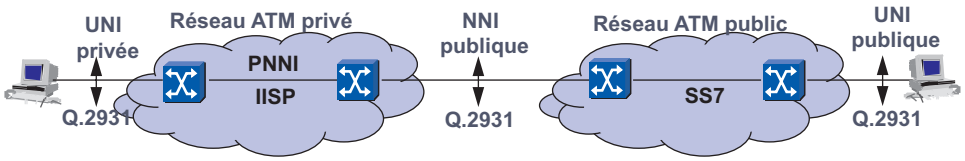


Figure 11.82 La signalisation dans ATM.

À l'interface usager (**UNI**, *User Network Interface*) ou entre réseaux (**NNI**, *Network to Network Interface*) une signalisation de type canal sémaphore (PVC 0/5) utilise le protocole Q.2931. Les réseaux publics utilisent la signalisation définie pour le RNIS, SS7 (*Signaling System 7*) ou CCIT N°7. En interne, les réseaux privés utilisent **PNNI** (*Private Network to Network Interface*) qui autorise l'établissement de SVC et assure un routage en fonction de la qualité de service. Précédemment **IISP** (*Interim Inter Switch Protocol*) ne permettait qu'une configuration statique du réseau, ce qui le réservait aux petits réseaux

➤ Architecture générale de la signalisation

La signalisation à l'interface usager (UNI) dérive des spécifications Q.2931, protocole de niveau 3, elle s'appuie sur une AAL sécurisée définie à cette intention : la **SAALL** (*Signaling AAL*, Q.2100). De type canal sémaphore, la signalisation utilise le couple VPI/VCI réservé : 0/5 (VPI = 0, VCI = 5). La figure 11.83 représente l'architecture de signalisation telle que l'a définie l'ATM Forum.

Preview from Notesale.co.uk
Page 376 of 837

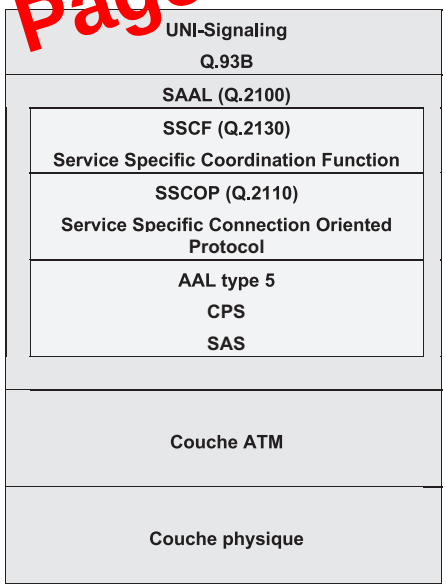


Figure 11.83 L'architecture générale de la signalisation NNI.

En mode commuté, l'établissement d'un SVC est préalable à l'envoi de données. Le message *Setup* est émis par l'appelant, il comporte tous les éléments nécessaires à l'établissement d'un SVC (bidirectionnel). Compte tenu de sa taille, ce message est composé de plusieurs cellules ATM émises sur le VPI/VCI réservé : 0/5.

L'accès au réseau haut débit de l'opérateur via la ligne téléphonique nécessite l'installation d'un équipement spécifique chez l'utilisateur final qui assure la séparation des canaux : le *splitter* (séparateur vocal), ou coupleur **POTS** (*Plain Old Telephon Service*, service téléphonique traditionnel) et le modem ADSL. Le *splitter* est généralement intégré au modem. Le modem offre un accès de type Ethernet, USB ou ATM. Du côté opérateur, le **DSLAM** (*Digital Subscriber Line Access Multiplex*) est un multiplexeur statistique assurant l'interface entre les connexions utilisateurs et le réseau haut débit de l'opérateur (figure 11.96)

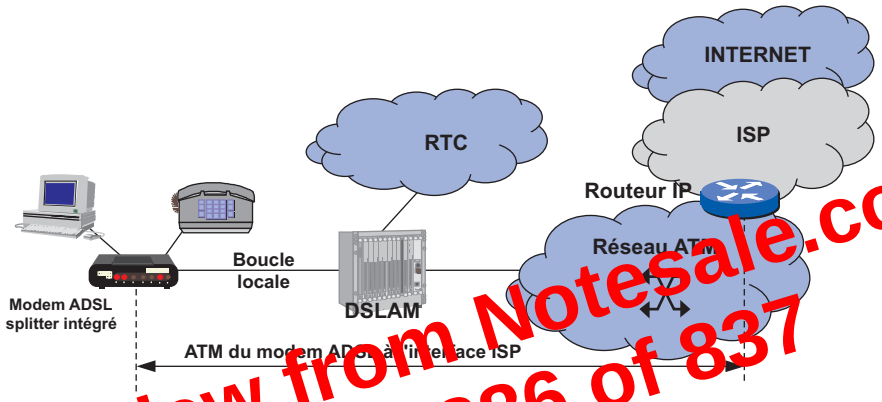


Figure 11.96 Architecture d'un réseau ADSL.

Preview from Notesale.co.uk
Page 386 of 837

ADSL est normalisé par l'ANSI et l'ETSI. Cependant, compte tenu des investissements nécessaires au déploiement d'un réseau ADSL, les constructeurs et opérateurs ont constitué un groupe de travail, le UAWG (*Universal ADSL Working Group*), pour définir une version allégée. L'ADSL G.Lite intègre le *splitter* (séparateur de voies) au modem autoconfigurable (*Plug and Play*), limite les débits à 1,5 Mbit/s en flux montant et à 512 kbit/s en flux descendant en réduisant les sous-canaux.

Appellation	Débit descendant	Débit montant	Distance	Utilisation
ADSL	32 kbit/s à 8 Mbit/s	32 kbit/s à 1,1 Mbit/s	5,5 km	Accès professionnel à Internet Interconnexion de LAN Vidéo à la demande (VoD)
UADSL G.Lite	64 kbit/s à 1,5 Mbit/s	32 kbit/s à 512 kbit/s	5,5 km	Accès résidentiel à Internet
SDSL	1,54 Mbit/s (T1) 2,048 Mbit/s (E1)	1,54 Mbit/s (T1) 2,048 Mbit/s (E1)	6,5 km	Interconnexion de LAN Serveur Internet Vidéoconférence
IDSL	144 kbit/s à 1,5 Mbit/s	32 kbit/s à 512 kbit/s	11 km	Accès RNIS
VDSL	13 à 52 Mbit/s	1,5 à 2,3 Mbit/s	1,2 km	Accès Internet, VoD TV haute définition
HDSL	1,5 Mbit/s (T1) 2,048 Mbit/s (E1)	1,5 Mbit/s (T1) 2,048 Mbit/s (E1)	4,5 km	Accès professionnel E1 Raccordement PABX Interconnexion de LAN

Figure 11.97 Les différentes technologies xDSL.

d) Quel est le rendement du protocole (rapport entre le nombre de bits utiles et le nombre de bits transmis) ?

e) Quel est alors le taux de transfert d'information (bit/s) ?

f) En supposant un taux d'erreur de 10^{-6} quel est le taux de transfert d'information réel (bit/s) ?

g) Quel est le rendement global du système (TTI/Possibilité du modem)

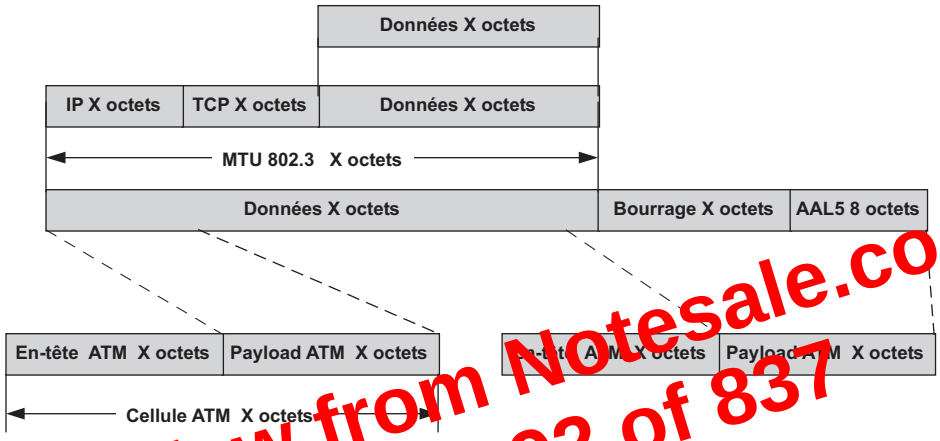


Figure 11.101 Encapsulation de données dans ATM.

Preview from Notesale.co.uk
Page 392 of 837

Exercice 11.8 Évolution de l'encapsulation d'IP

Veuillez compléter le tableau ci-dessous (figure 11.102) qui résume les différentes possibilités d'encapsulation du protocole IP pour en assurer le transport sur un réseau WAN.

Type d'encapsulation	Mise en œuvre	Caractéristiques
IP/ATM/SDH/WDM		
IP/SDH/WDM		
IP/WDM		

Figure 11.102 Encapsulation IP.

données...). Le terme de réseau local (**LAN**, *Local Area Network*) qui définit un LAN comme un système de communication entre unités centrales sur une étendue géographique limitée est restrictif. Faisant abstraction de la notion d'étendue géographique, le terme de réseau local d'entreprise (**RLE**) semble mieux approprié.

12.1.2 Distinction entre réseau local et informatique traditionnelle

Entre un terminal passif, par exemple un terminal Telnet, en informatique traditionnelle centralisée, et un poste client d'un réseau local, le plus souvent un micro-ordinateur, la différence essentielle concerne la localisation des traitements et de la politique d'accès (figure 12.2).

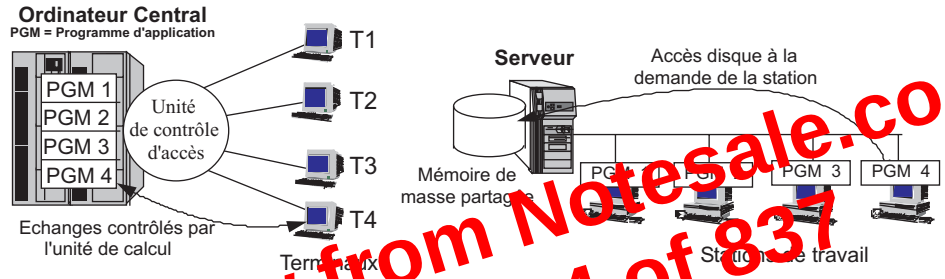


Figure 12.2 Localisation de la puissance de calcul.

Preview from Notesale.co.uk
Page 394 of 837

Un terminal passif ne dispose d'aucune puissance de calcul, les diverses applications partagent le temps CPU de l'ordinateur central. Celui-ci contrôle le traitement et organise les accès (politique d'accès centralisé : *polling/selecting* ou relation maître/esclave). Un poste client (**station**) d'un réseau local dispose d'une puissance de calcul autonome, le programme principal s'exécute en local, il n'émet des requêtes au serveur que pour utiliser les ressources partagées et offertes par ce dernier. Il n'y a pas de subordination entre les différents constituants du réseau. Dans ces conditions, ceux-ci partageant le même média, une discipline d'accès (**protocole d'accès**) doit être implémentée dans chaque unité (politique ou contrôle d'accès décentralisé).

Un réseau local distingue deux types de machines, celles qui offrent des ressources en partage : les serveurs, et celles qui utilisent ces ressources : les postes clients, postes de travail ou stations. Dans les réseaux locaux de la dernière génération toutes les machines peuvent offrir des ressources en partage et utiliser celles offertes par les autres stations du réseau. Ce type de réseau est désigné sous le nom de *peer to peer* ou poste à poste ou encore d'égal à égal. En fait, dans les réseaux importants, une machine dédiée aux fonctions traditionnelles de serveur subsiste. Celle-ci assure la gestion des utilisateurs, la sécurité d'accès, la distribution des logiciels...

12.1.3 Réseaux locaux et accès aux systèmes traditionnels

Pour l'utilisateur, la distinction entre les systèmes est masquée. Une station d'un réseau local peut donner accès aux applications d'un ordinateur central (mini ou *mainframe*). Le programme client émule alors un terminal de l'autre système. L'une des stations assure les fonctions de passerelle vers le système central (figure 12.3).

L'adresse de diffusion restreinte ou multicast

Une adresse de multicast ou de groupe (bit G = 1) désigne un ensemble de stations. Les applications fournissent à la station (couche MAC) la liste des adresses de groupe auxquelles elle doit répondre (abonnement). Ces adresses sont utilisées, par exemple, pour la diffusion vidéo. Des plages d'adresses multicasts ont été définies pour permettre l'encapsulation d'adresses IP multicast, cette plage s'étend de :

01-00-5E-00-00-00 à 01-00-5E-7F-FF-FF (RFC 1112)

La figure 12.17 montre comment est réalisée la construction d'une adresse multicast IEEE (adresse MAC) à partir d'une adresse IP multicast (classe D).

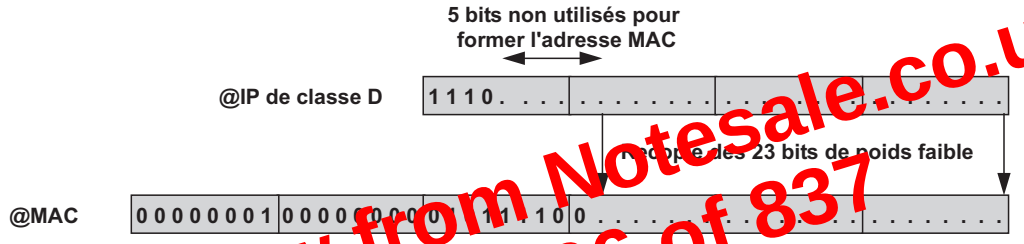


Figure 12.17 Construction d'une @MAC multicast à partir d'une @IP de classe D.

Preview from Notesale.co.uk
Page 406 of 837

➤ Format canonique et non canonique.

Les bits d'adresse sont toujours transmis bits de poids faible en premier (figure 12.15), ce qui ne correspond pas à l'écriture naturelle des valeurs. Lorsque l'adresse est écrite au format IEEE (bit de poids faible en tête, octet de poids fort devant) l'adresse est dite au format canonique, les valeurs des différents octets s'écrivent en les séparant par « : », dans le cas inverse (écriture naturelle), le format est dit non canonique et les différents octets sont écrits en les séparant par un tiret (figure 12.16). Les réseaux de type Ethernet utilisent le format canonique, les réseaux Token Ring le format non canonique.

Le contrôle d'erreur

L'en-queue contient le champ de contrôle d'erreur par CRC[6] sur 32 bits (**FCS**, *Frame Control Sequence*). Le polynôme générateur, identique pour tous les types de réseaux normalisés par IEEE, est :

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + 1$$

La couche MAC rejette toute trame erronée mais n'effectue aucune reprise sur erreur. Cette tâche sera éventuellement réalisée par les couches supérieures. La figure 12.18 représente le format général de la trame MAC. L'en-tête et l'en-queue sont spécifiques à chaque type de réseau.

6. Voir section 6.2.1 pour le mode de calcul du CRC ou FCS.

Le champ longueur des données utiles, sur deux octets, différentie les spécifications Ethernet V2 et IEEE 802.3, en conséquence, les deux réseaux sont incompatibles. Dans la version Ethernet V2, ce champ identifie le protocole supérieur, c'est à ce dernier que revient la tâche d'extraire les données utiles du champ données.

Dans l'exemple de la figure 12.28, la station **B** a cessé son émission immédiatement après avoir détecté la collision, son message est donc très court. Pour être certain qu'un message minimal arrive à **A** et que celui-ci détecte bien la collision, **B** émet une séquence de brouillage de 32 bits à 1 (3,2 μs) appelée *jam interval*.

Les évolutions récentes d'Ethernet vers des débits plus élevés ont posé le problème du maintien de cette fenêtre à 51,2 μs. Par exemple, à 100 Mbit/s, la trame minimale devient de 640 octets, c'est-à-dire que compte tenu des données de bourrage l'augmentation du débit vu des applications serait quasiment nulle pour les petits messages. Dans ces conditions et pour assurer la compatibilité entre les différentes versions, la trame minimale de 64 octets a été maintenue. Si le débit croît, la fenêtre de collision décroît dans les mêmes proportions et par conséquent la distance maximale entre deux stations aussi (diamètre du réseau). Le tableau de la figure 12.30 illustre cette relation.

Preview from Notesale.co.uk
Page 414 of 837

Débit	Fenêtre de collision	Diamètre du réseau
10 Mbit/s	51,2 μs	2500 m
100 Mbit/s	5,12 μs	250 m
1000 Mbit/s	0,512 μs	25 m

Figure 12.30 Relation débit et diamètre du réseau.

Algorithme du BEB

Le **BEB** (*Binary Exponentiel Backoff*) ou encore algorithme de ralentissement exponentiel, détermine le délai aléatoire d'attente avant que la station ne réessaie, après collision, une émission (figure 12.31). Après une collision, une station ne peut émettre qu'après un délai défini par :

$$T = K \cdot TimeSlot$$

K est un nombre aléatoire entier généré par l'émetteur et compris dans l'intervalle :

$$K = \left[0, 2^n - 1\right] \text{ avec } n \leqslant 10$$

où n représente le nombre de collisions successives détectées par la station pour l'émission d'un même message. Après 16 tentatives, l'émetteur abandonne l'émission.

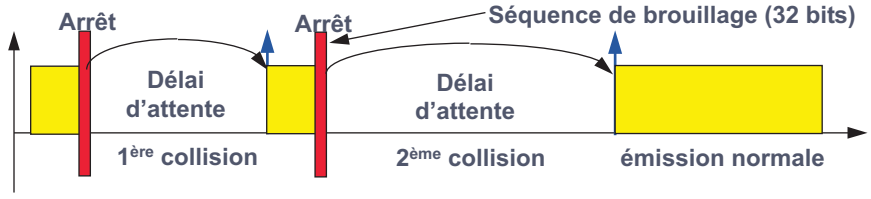


Figure 12.31 Principe du BEB.

connecté directement sur la carte par l'intermédiaire d'un T vissé BNC (*Barrel Neck Connector*). La longueur maximale d'un segment est de 185 m et chaque segment peut accueillir un maximum de 30 stations. La figure 12.34 présente cette version du réseau Ethernet.

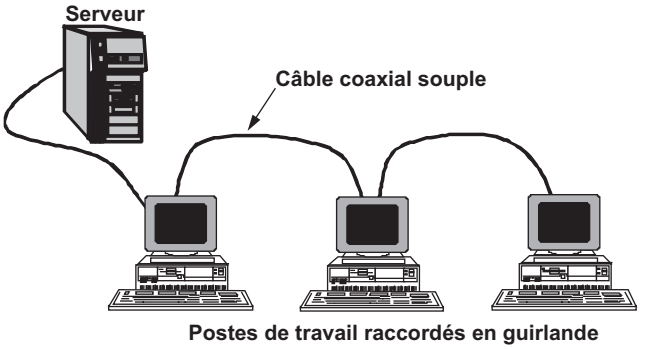


Figure 12.34 L'Ethernet fin.

Preview from Notesale.co.uk
Page 417 of 837

Cette architecture physique de réseau est recommandée pour la réalisation de petit réseau d'une dizaine de machines, c'est la plus économique.

Ethernet sur paires torsadées : IEEE 802.3 10 base T

➤ Origine

Compte tenu des problèmes en relation avec le câblage, AT&T a imaginé de réutiliser le câblage téléphonique préexistant dans les immeubles de bureaux pour la réalisation de réseau. Le réseau devait alors passer d'une topologie bus à une topologie physique étoile, assurer la diffusion des messages et la détection des collisions. La solution adoptée par AT&T consiste simplement à émuler un bus dans un boîtier : le hub, chargé d'une part de concentrer les connexions et d'autre part d'assurer la diffusion des messages (figure 12.35).

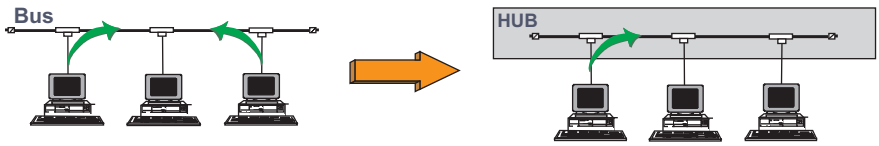


Figure 12.35 Passage du bus à l'étoile.

La liaison hub/station était réalisée en paires torsadées (1 paire émission, 1 paire réception), cela imposait deux contraintes : l'une de débit, l'autre de distance. Ce réseau fonctionnait à 1 Mbit/s, les stations étaient connectées sur des concentrateurs répéteurs (**hub**) et la distance entre le hub et une station était limitée à 250 m. Cette architecture (802.3 1 base 5 ou Starlan), complètement obsolète, est à l'origine de la version à 10 Mbit/s (802.3 10 base T, T pour *Twised pair*) qui en reprend les principes.

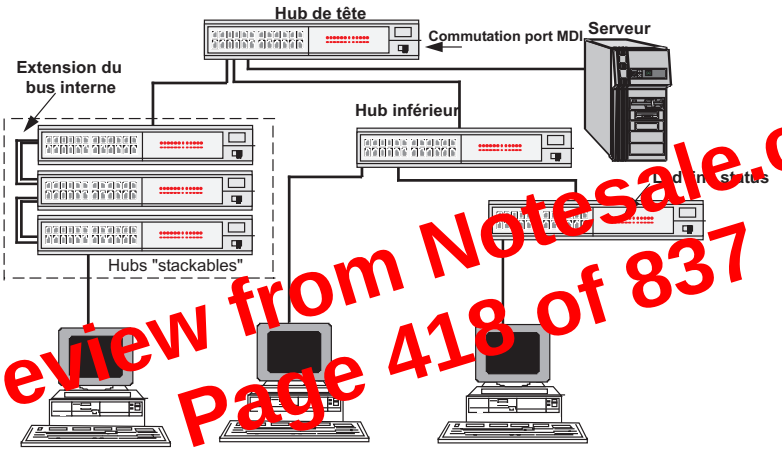
➤ Ethernet, 802.3 10 base T

La version 10 base T reprend les principes architecturaux du réseau Starlan, c'est un réseau en étoiles hiérarchisées (figure 12.36). Les hubs assurent :

© Dunod – La photocopie non autorisée est un délit

– les fonctions de diffusion des messages (émulation de bus, deux stations connectées au même hub ne reçoivent le signal de l'autre que via le hub de tête) ;
– la détection des collisions (le hub diffuse un signal de collision vers les autres stations) ;
– la détection de stations bavardes (fonction *Jabber* : message d'une durée supérieure à 150 ms).

En cas de collisions multiples, le hub segmente le réseau. Le débit est de 10 Mbit/s, la longueur d'un brin est limitée à 100 m (distance entre un hub et une station ou entre deux hubs), cette longueur est portée à 150 m si l'atténuation est inférieure à 11,5 dB, le nombre de niveaux est fixé à trois.



Preview from Notesale.co.uk
Page 418 of 837

Figure 12.36 Architecture du réseau 10 base T.

Un signal particulier, le *link status* (état de la ligne), permet, par la visualisation de diodes **LED** (*Light Emitting Diode*), de contrôler la continuité du lien entre le hub et la station (*link integrity test function*). En l'absence d'émission, le hub et la carte réseau émettent, toutes les 8 secondes, des impulsions de test de 100 ms (impulsions de test de lien ou **LTP**, *Link Test Pulses*). En l'absence de données (données utilisateur ou signal LTP) ou de réception du signal de remplissage (**TP_IDL**, *Twisted Pair Idle Signal*), le hub et la carte considèrent le lien défectueux, le voyant *link status* est alors positionné à « OFF » et le port du hub est inhibé.

Sur chaque hub, un interrupteur permet la commutation de la fonction d'un des ports (**MDI**, *Medium Dependent Interface*) en port de répétition vers un hub de niveau supérieur (croisement des paires émission et réception). C'est la fenêtre de collision qui limite le nombre de niveaux admissibles (distance maximale). Pour franchir la barrière des trois niveaux et autoriser un plus grand nombre de stations connectées, les hubs peuvent aussi être empilés par l'extension du bus interne (figure 12.36). Ces hubs, dits « stackables », sont vus par le système comme un seul niveau.

Ethernet à 100 Mbit/s

➤ Généralités

Évolution de la version 10 base T, l'Ethernet 100 Mbit/s (ou Fast Ethernet) résulte des travaux du groupe de travail IEEE 802.14. La compatibilité avec la version 10 base T est assurée par

  - 100, trame d'apprentissage, celle-ci n'emprunte que les branches établies, précédemment, par le *Spanning Tree Protocol*[10] ;
- **longueur**, ce champ, de 5 bits, spécifie la longueur du champ RI (32 octets maximum) ;
- **sens**, ce bit indique si la route à suivre doit être lue de gauche à droite ou de droite à gauche ;
- **MTU** (*Maximum Transfer Unit*), ce champ de 4 bits indique la taille maximale des unités de données qui peuvent être transférées sur le réseau traversé, les valeurs sont codifiées (576, 1500, 2052, 4472, 8144, 11407, 17820, 65535) ;
- enfin, le champ **route** qui contient *n* sous-champs *Route Designator*. Le sous-champ *Route Designator* sur 16 bits identifie le réseau, ou port, sur 12 bits et le pont traversé sur 4 bits. Les identificateurs sont initialisés par l'administrateur de réseau.

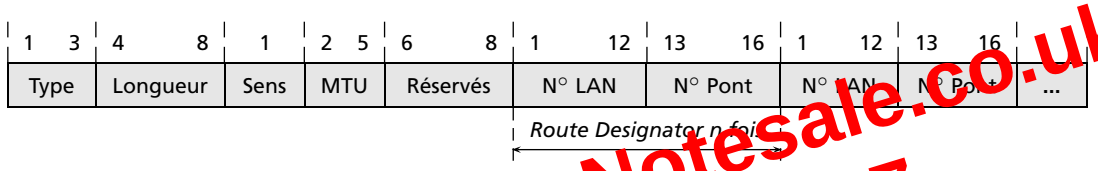


Figure 12.50 Structure du champ RI.

Preview from Notesale.co.uk
Page 427 of 837

12.4.3 Comparaison Ethernet/Token Ring

Lorsque l'on compare deux types de réseaux, les critères à retenir sont principalement :

- les performances en termes de débit et temps d'accès ;
- les types de transferts et applications informatiques envisageables ;
- l'infrastructure requise et les distances maximales admissibles ;

En termes de débit et temps d'accès

Le débit d'un réseau peut s'exprimer selon 3 valeurs. Le **débit nominal** qui correspond au débit physique sur le lien. Le **débit utile** qui représente les données effectivement transmises sur le réseau, tandis que le **débit effectif** correspond à celui vu des applications. Le premier est effectivement lié au choix du réseau, le second dépend non seulement du débit physique mais aussi de la charge du réseau et des protocoles empilés. Seuls, nous intéressent ici les débits nominaux et la tenue en charge du réseau (débit utile).

La figure 12.51 superpose l'évolution des débits en fonction de la charge de chaque réseau. Il est intéressant de constater qu'à faible charge, les réseaux de type Ethernet présentent, vis-à-vis des couches supérieures, une meilleure efficacité. En effet, en Ethernet, si le trafic est faible, dès qu'une station veut émettre, elle émet. En *Token Ring*, même à faible charge, la station doit attendre le jeton.

Cependant, à forte charge dans le réseau Ethernet, les collisions se multiplient et le débit utile sur le support s'effondre, alors que dans le cas du réseau *Token Ring*, même si le débit effectif de chaque station diminue, le débit utile sur le support tend vers le débit nominal.

10. Voir section 14.3.4.

© Dunod – La photocopie non autorisée est un délit

– l'octet de contrôle de trame (**FC**, *Frame Control*) indique le type de trame (jeton, données...) ;
– les champs d'adresse spécifient les adresses destination (DA) et source (SA) ;
– le champ de données peut contenir de 0 à 8 191 octets ;
– enfin, le FCS protège les champs FC, DA, SA et données.

Préambule	SD Start Delimiter	FC Frame Control	DA Destination Address	SA Source Address	Information 0 à 8 181 octets	FCS	ED End Delimiteur

Figure 12.56 Trame IEEE 802.4.

Preview from Notesale.co.uk
Page 433 of 837

12.6 LE RÉSEAU 100 VG ANY LAN, 802.12

12.6.1 Généralités

D'origine HP et AT&T et normalisé par le groupe de travail IEEE 802.12, le 100 VG *Any Lan*[11] implémente un nouveau protocole d'accès fondé sur la méthode du polling. Les trames peuvent être au format Ethernet ou Token Ring, selon la configuration, d'où l'appellation *d'Any Lan*. Se contentant de simples paires torsadées de qualité vocale (**VG**, *Voice Grade*), le 100 VG *Any Lan* offre un débit de 100 Mbit/s et a mode déterministe. Il admet du trafic de type isochrone.

Les distances couvertes dépendent du type de câble utilisé. Elles sont de 100 m (hub/station ou hub/hub) avec du câble catégorie 3 (*Voice Grade*) et catégorie 4. Elles atteignent 150 m (voire 200 m) avec du câble catégorie 5 UTP (non blindé, *Unshielded Twisted Pair*).

Le réseau 100 VG *Any Lan*, en raison de son protocole d'accès, utilise au maximum la bande passante (bande utile de 80 Mbit/s contre 40 à 50 Mbit/s pour l'Ethernet). Concurrent malheureux de l'Ethernet 100 Mbit/s, le 802.12 est resté très confidentiel. Seule, la description de sa méthode d'accès justifie son étude.

12.6.2 Le DPAM

Principe

Les stations sont raccordées à un concentrateur intelligent selon une topologie physique identique à celle du réseau 10 base T (réutilisation du câblage existant). Lorsqu'une station a des données à émettre, elle formule une requête au hub, qui lui alloue ou non le support (*Demand Priority Access Method* ou **DPAM**).

Les schémas de la figure 12.57 illustrent succinctement le principe de DPAM :

– Le hub informe les stations et celles-ci informent le hub de leur disponibilité (émission du signal *IDLE*).
– La station ayant des données à émettre le signale au hub en lui envoyant une requête selon

11. Le 100 VG LAN est une proposition commune d'Heweltt Packard, IBM et d'AT&T.

© Dunod – La photocopie non autorisée est un délit

le niveau de priorité des données. Ici, ce sont des données de priorité normale, signal **NPR** (*Normal Priority Request*).

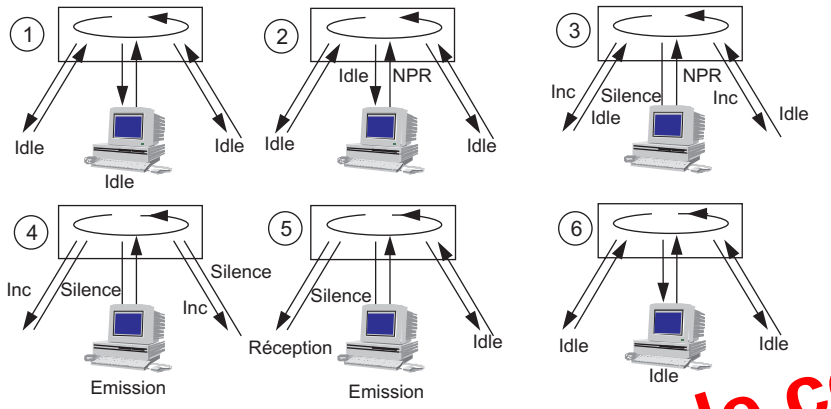


Figure 12.57 Principe du DPAM.

Preview from Notesale.co.uk
Page 434 of 837

– Le hub scrute en permanence ses différents ports (*round robin*). Durant cette phase de polling, le hub détecte la demande de la station. Il informe les autres stations qui lui sont raccordées de se mettre en état de recevoir (signal *Incoming*, **INC**) et cesse son émission de Idle vers la station demanderesse (silence).
– Les stations signalent au hub qu'elles sont prêtes à recevoir en cessant leur émission de Idle. La station demanderesse interprète la non-réception de Idle comme une autorisation d'émettre, elle transmet sa trame.
– Le hub, à réception de cette dernière, examine l'adresse destination et retransmet la trame sur le seul port intéressé. Ce processus nécessite l'implémentation d'un protocole d'apprentissage d'adresses. Le hub reprend, vers les autres stations, l'émission de Idle.
– À la fin du cycle, après émission et réception de la trame toutes les stations et le hub émettent les signaux Idle.

Principe de la signalisation

Tonalité	Hub vers station		Station vers Hub	
Silence	Prêt à émettre ou à recevoir			
1 et 1	IDLE	Rien à envoyer	IDLE	Rien à transmettre
1 et 2	Incoming INC	Demande de passage en état réception	NPR	Requête de priorité normale
2 et 1			HPR	Requête de priorité haute
2 et 2	Initialisation INIT	Signal d'initialisation, déclenché notamment pour l'apprentissage des adresses MAC des stations raccordées à un HUB.		

Figure 12.58 Signalisation du réseau 100 VG *Any Lan*.

La signalisation utilisée dans les différentes phases du processus décrit précédemment est réalisée à partir de l'émission continue de signaux de fréquences différentes (0,9375 MHz pour

affectation statique. Ce mode de fonctionnement est le moins performant, le commutateur devant accéder à l'adresse de niveau 3 pour définir le VLAN d'appartenance. L'adresse de niveau 3 est utilisée comme étiquette, il s'agit bien de commutation et non de routage. L'en-tête n'est pas modifié.

Il est aussi envisageable de réaliser des VLAN par :

– protocole (IP, IPX...), la communication ne pouvant s'établir qu'entre stations utilisant le même protocole ;

– par application (N° de port TCP), la constitution des VLAN est alors dynamique, un utilisateur pouvant successivement appartenir à des VLAN différents selon l'application qu'il utilise ;

– par mot de passe (constitution dynamique des VLAN au login de l'utilisateur).

La figure 12.65 illustre ces différentes approches. Les VLAN peuvent être définis sur un ou plusieurs commutateurs, que ceux-ci soient locaux ou distants. Cependant, il devra y avoir autant de liens intercommutateurs (physiques ou virtuels) que de VLAN interconnectés.

Preview from Notesale.co.uk
Page 441 of 837

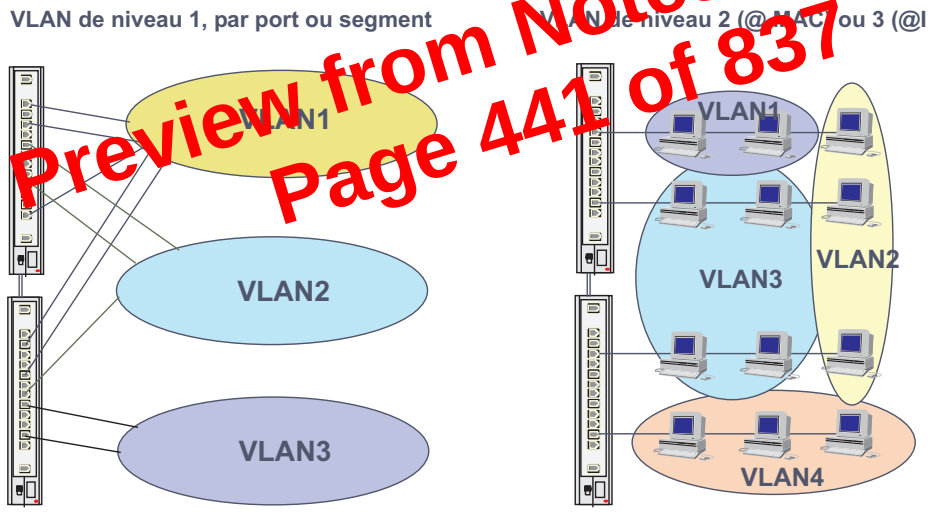


Figure 12.65 Les différents niveaux de VLAN.

12.8.3 L'identification des VLAN (802.1Q)

Principe

Lorsqu'un réseau comporte plusieurs commutateurs, chaque commutateur doit pouvoir localiser toutes les machines (table d'acheminement) et connaître le VLAN d'appartenance de la source et du destinataire (filtrage de trafic). Lorsque le réseau est important les tables peuvent devenir très grandes et pénaliser les performances. Il est plus efficace d'étiqueter les trames (figure 12.66). L'étiquette identifie le VLAN de la station source, le commutateur n'a plus alors qu'à connaître les VLAN d'appartenance des stations qui lui sont raccordées. La norme IEEE 802.1Q définit l'étiquetage des trames.

© Dunod – La photocopie non autorisée est un délit

champ Ethertype de la trame 802.3, il identifie le format 802.1 p/Q, sa valeur est fixée à 0x8100. Les deux octets suivants permettent de définir huit niveaux de priorité (*User Priority*). Les commutateurs de dernière génération disposent de plusieurs files d'attente les trames sont affectées à telle ou telle file suivant leur niveau de priorité.

Le bit **CFI** (*Canonical Format Identifier*) est, en principe, inutilisé dans les réseaux 802.3, il doit être mis à 0. Dans les réseaux Token Ring, à 1, il indique que les données du champ routage par la source sont au format non canonique. Le champ **VID** (*VLAN IDentifier*) identifie sur douze bits le VLAN destination. L'introduction de quatre octets supplémentaires implique que les commutateurs d'entrée et de sortie recalculent le FCS. On commence à trouver des cartes transporteurs capables de supporter le tagging.

12.9 LES RÉSEAUX SANS FIL

12.9.1 Généralités

S'affranchissant d'une infrastructure câblée et autorisant la mobilité, les réseaux sans fils, sous des appellations génériques différentes, sont en plein essor. On distingue :

- les **WPAN** (*Wireless Personal Network*), de la simple liaison infrarouge à 100 kbit/s au Bluetooth à environ 1 Mbit/s, ces technologies peu coûteuses devraient se développer rapidement. Elles sont essentiellement utilisées pour raccorder un périphérique informatique (imprimante...), un agenda électronique...
- les **WLAN** (*Wireless Local Area Network*), prolongent ou remplacent un réseau local traditionnel. Ces réseaux, objet de ce paragraphe, devraient connaître un développement important. Ils autorisent des débits allant de 2 à 54 Mbit/s ;
- les **WMAN** (*Wireless Metropolitain Area Network*) utilisés pour l'accès aux réseaux d'infrastructure (boucle locale), ils offrent des débits de plusieurs dizaines de Mbit/s ;
- enfin, les **WWAN** (*Wireless Wide Area Network*), recouvrent essentiellement les réseaux voix avec ses extensions données (GSM, GPRS et UMTS), les débits sont relativement faibles de quelques dizaines de kbit/s (10 à 384 kbit/s).

Le tableau de la figure 12.69 présente une synthèse des principales technologies.

Nom	Fréquence	Débit	Portée	Commentaires
Bluetooth	2,4 GHz	1 à 10 Mbit/s	10-100 m	Utilisation personnelle
Wi-Fi (802.11b)	2,4 GHz	11 Mbit/s	300 m	Liaison point à point à haut débit
Home RF	2,4 GHz	1,6 et 10 Mbit/s	50 m	Domotique
IEEE 802.11g	2,4 GHz	54 Mbit/s		Successeur du 802.11b
IEEE 802.11a	5 GHz	54 Mbit/s		Idem.
HiperLan 2	5 GHz	54 Mbit/s		Concurrent du 802.11a

Figure 12.69 Les principales solutions de réseaux sans fil.

© Dunod – La photocopie non autorisée est un délit

Preview from Notesale.co.uk
Page 443 of 837

nical and Office Protocol), d'origine Boeing, prend en compte les besoins bureautiques, il s'appuie sur des couches MAC 802.4, 802.3 et 802.5. La figure 12.76 présente ces architectures.

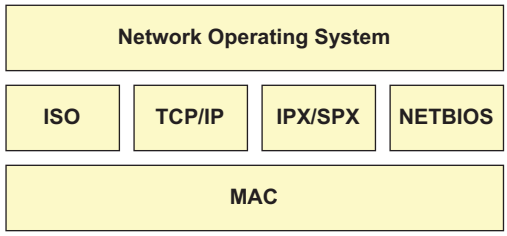


Figure 12.75 Les principales piles de protocoles utilisées dans les LAN.

De manière générale, les piles ISO utilisent TP4 et **CLNP** (*ConnectionLess Network Protocol*, ISO 8473). L'adressage résulte de la concaténation d'une adresse X.121 (*Net_Id*) et de l'adresse MAC (*Host_Id*).

Preview from Notesale.co.uk
Page 448 of 837

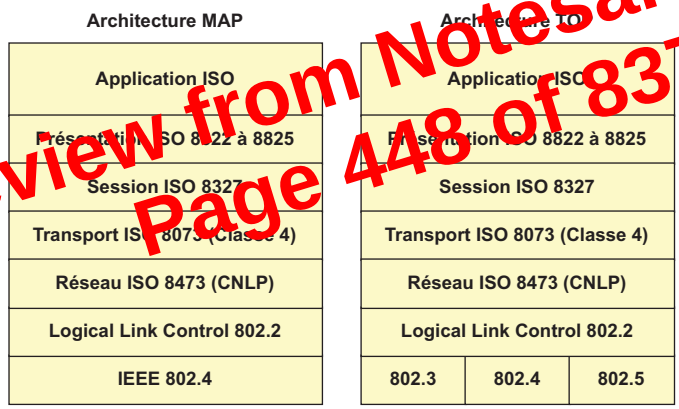


Figure 12.76 Les réseaux MAP et TOP.

12.10.3 La pile IPX/SPX

Présentation

En voie de disparition, mais encore présente dans de nombreux réseaux, la pile **IPX/SPX** (*Internet Packet eXchange/Sequenced Packet eXchange*) est une adaptation par Novell de l'architecture **XNS** (*Xerox Network System*) de Xerox. La similitude des deux architectures représentées figure 12.77 est très apparente.

Le protocole *Echo* sert à vérifier l'existence d'une route pour atteindre une station (Ping de TCP/IP). Le protocole *Error* sert à signaler à l'émetteur d'un paquet une erreur sur celui-ci (ICMP de TCP/IP). Le protocole SPX (**SPP**, *Sequenced Packet Protocol de XNS*) assure un service de transport en mode connecté (TCP de TCP/IP). Le protocole **PEP** (*Packet Exchange Protocol*) est un service de transport en mode non connecté, cependant celui-ci est capable d'effectuer une reprise sur erreur. Le protocole **RIP** (*Routing Information Protocol*) achemine les paquets à travers un réseau (protocole de routage).

atteint 16, le paquet est détruit. Le champ type de datagramme précise le protocole encapsulé (00 type inconnu, 01 RIP...). Suivent les champs d'adressage.

Adressage IPX

Le datagramme IPX contient toutes les données nécessaires à l'adressage complet des données. Le champ adresse réseau permet de déterminer le réseau sur lequel est située la machine (Net_ID). Cette information est complétée par l'indication de l'adresse MAC de la station. Le fait d'avoir choisi comme Host_ID l'adresse physique du coupleur garantit l'unicité d'adresse et simplifie la tâche de l'administrateur de réseau lors de la configuration. Cette approche a été reprise dans IPv6 (EUI-64).

La notion d'unicité d'adressage réseau est absente dans IPX, il n'y a pas d'organisme international de gestion de l'espace d'adressage. Celle de plan d'adressage est très réduite, et peut poser quelques problèmes lors de l'interconnexion de plusieurs réseaux. L'adresse réseau zéro indique le réseau sur lequel on est. De ce fait, si le réseau n'est interconnecté à aucun autre, ce champ n'a pas besoin d'être renseigné. Ces informations sont complétées par l'indication du *socket*, notion équivalente à celle de port TCP/IP ou à celle de TSAP d'ISO.

Preview from Notesale.co.uk
Page 450 of 837

12.10.4 La pile NETBIOS

Présentation

NetBIOS (*Network Basic Input/Output System*) est un ensemble de protocoles réseaux. Non conforme au modèle de référence, NetBios a été développé par la société Sytek pour le réseau IBM PC NetWork. Adopté par Microsoft, NetBios devint vite, malgré ses faiblesses, un standard du marché. La pile NetBios est représentée figure 12.79.

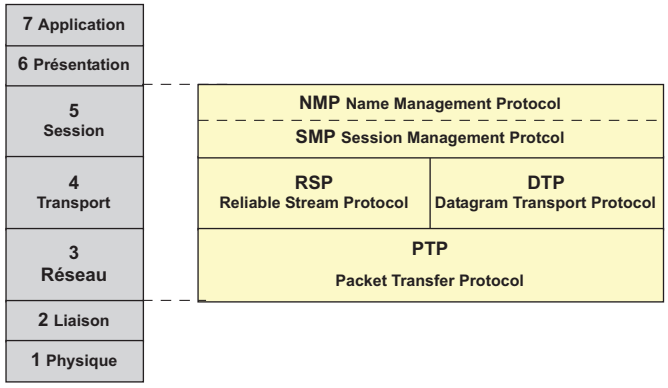


Figure 12.79 L'architecture NetBIOS.

NetBios couvre les couches 3 à 5 du modèle de référence. La couche 3, **PTP** (*Packet Transfer Protocol*) implémente un service de datagramme. Il n'y a pas, dans NetBIOS, de notion d'adressage réseau. Prévu initialement pour de petits réseaux, NetBIOS n'utilise que l'adresse MAC. Le service transport offre les deux types de service, un service en mode non connecté (**DTP**, *Datagram Transport Protocol*), et un service en mode connecté (**RSP**, *Reliable Stream Protocol*). RSP établit un circuit entre les deux participants à l'échange, il offre un service

MPOA exploite la technologie LANE (LAN *Emulation*) et pallie ses limites en offrant une émulation transparente des protocoles réseaux s'exécutant au-dessus d'ATM. MPOA assure une connectivité de niveau 3 de bout en bout entre les systèmes d'extrémité, qu'ils soient directement raccordés à une infrastructure ATM ou à un sous-système de technologie antérieure.

L'avantage primordial de l'approche MPOA réside dans le fait que chaque système intégrant une interface MPOA peut établir des connexions ATM directes (sans intermédiaire) de type unicast, multicast et broadcast.

Fonctionnement de MPOA

➤ Architecture de MPOA

À l'instar de LANE, MPOA fonctionne selon le modèle client/serveur. Il comporte deux éléments :

– le client (*MPOA client*, **MPC**), élément logiciel résident dans l'équipement terminal ou le commutateur de bordure[5] (*edge device*) raccordé à ATM. Le client MPC inclut les services de la RFC 1 483 pour assurer un transfert de données hors LEC ;

– le serveur (*MPOA server*, **MPS**), est une extension logicielle résidente dans les routeurs interréseaux.

MPOA ne fonctionne que sur LANE2. La communication entre MPC (MPOA *Client*) et MPS (MPOA *Serveur*) s'effectue via les LAN Emulation Clients (LEC). La communication entre serveurs MPOA (MPS) utilise le protocole NHRP (*Next Hop Routing Protocol*). La figure 13.36 schématise cette architecture.

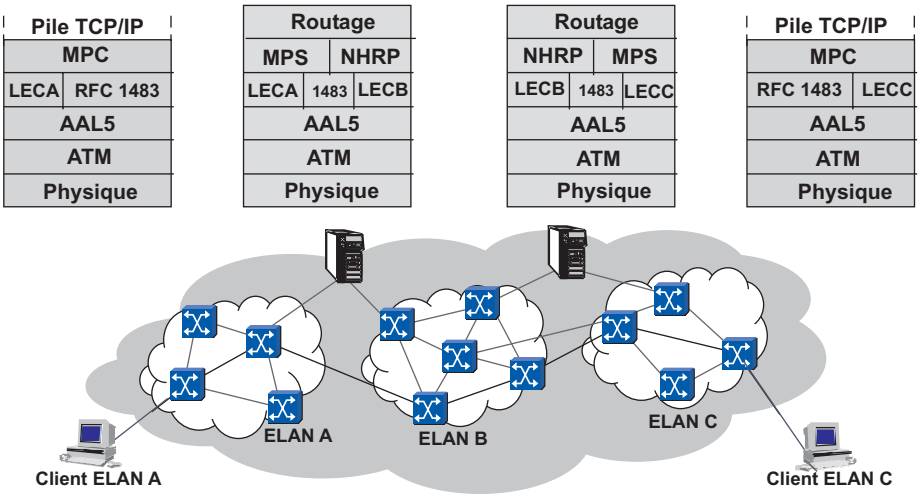


Figure 13.36 Architecture d'une interconnexion MPOA.

5. C'est par exemple le cas d'un commutateur Ethernet disposant d'un raccordement ATM.

© Dunod – La photocopie non autorisée est un délit

Preview from Notesale.co.uk
Page 485 of 837

EXERCICES

Exercice 13.1 FDDI et Token Ring

Comparez les caractéristiques physiques et fonctionnelles des réseaux Token Ring et FDDI

Exercice 13.2 Données de la classe Isochrone

Est-il envisageable d'émettre des données Isochrone sur un réseau FDDI-1

Exercice 13.3 L'acquittement dans FDDI

Dans FDDI le champ FS comporte les informations en relation avec l'indication de détection d'erreur, d'adresse reconnue et de trame recopiée. Donnez la structure de ce champ lors de l'envoi d'une trame multicast alors que trois stations ont reconnu leur adresse mais seulement deux ont correctement recopié la trame.

Preview from Notesale.co.uk
Page 487 of 837

Exercice 13.4 Rotation des données sur le réseau FDDI

Supposons un réseau FDDI ne comportant que 4 stations. Représenter la circulation des données sur l'anneau en admettant que :

- avant l'échange seul le jeton circule sur l'anneau ;
- la station 1 acquiert le jeton et transmet des données à la station 3 ;
- la station 2 acquiert le jeton et transmet des données à la station 4.

On considérera que la trame est très petite devant la taille de l'anneau.

Exercice 13.5 État des compteurs dans DQDB

Une station a le compteur RQ positionné à 5 et le compteur CD positionné à 2, elle désire émettre des données. Aucune nouvelle requête en amont n'étant formulée combien de slots vides devra-t-elle décompter avant de pouvoir émettre ses données ?

© Dunod – La photocopie non autorisée est un délit

Preview from Notesale.co.uk
Page 488 of 837

Chapitre **14**

Interconnexion des réseaux

Preview from Notesale.co.uk
Page 489 of 837

14.1 GÉNÉRALITÉS

14.1.1 Définition

Le déploiement des réseaux d'établissement a permis le traitement local des informations. Cependant, pour assurer la cohérence du système d'information de l'entreprise, il s'avère nécessaire d'assurer l'échange d'information entre ses différentes composantes. Tel est l'objet de l'interconnexion des réseaux. Fonctionnellement, l'interconnexion consiste à mettre en relation, indépendamment de la distance qui les sépare et des protocoles qu'elles utilisent, des machines appartenant à des réseaux physiquement distincts.

Physiquement, elle se réduit à la mise en relation de deux réseaux via un organe, appelé relais dans la terminologie OSI. Le relais peut n'être qu'un simple élément physique mais aussi un réseau (figure 14.1).

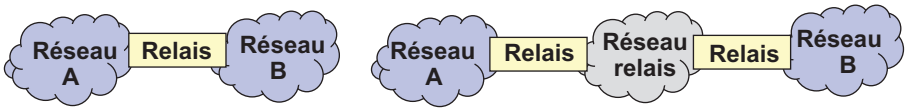


Figure 14.1 Principe de l'interconnexion des réseaux.

14.1.2 Problématique de l'interconnexion

La mise en relation d'un système A avec un système B peut se réaliser très simplement si A, B et le relais utilisent les mêmes protocoles, comme par exemple l'interconnexion de deux réseaux locaux utilisant TCP/IP via un réseau IP. Cependant, dans la plupart des cas, le protocole du réseau relais est différent du protocole local, par exemple l'interconnexion de deux réseaux locaux TCP/IP via un réseau de transport X.25, FR ou ATM. L'hétérogénéité peut aussi être de bout en bout, quand les deux éléments à raccorder mettent en œuvre des tech-

rement une machine spécifique, une station d'un réseau local peut participer à l'acheminement des données (UNIX, LINUX, Windows NT...).

14.4.2 Les techniques de routage

Généralités

Ces techniques ont été étudiées au chapitre 8. Rappelons-en le principe, les routeurs orientent les paquets selon des informations contenues dans des tables dites tables de routage. Ils utilisent essentiellement deux modes de routage :

– le routage statique ou fixe, dans ce type de routage, les tables de routage sont introduites par l'administrateur de réseau à l'initialisation du réseau ;

– le routage par le chemin le plus court, dans ce type de routage, les tables de routage indiquent pour chaque destination le coût le moins élevé. Périodiquement, des échanges d'informations entre les routeurs permettent de maintenir ces tables à jour. Les algorithmes de vecteur distance (*Distance Vector Routing*) et à état des liaisons (*Link State Routing*) sont de cette nature.

Preview from Notesale.co.uk
Page 506 of 837

La station qui a des données à transmettre connaît le routeur auquel elle est rattachée (routeur ou passerelle par défaut). Ce routeur doit ensuite déterminer le prochain nœud à atteindre pour trouver le destinataire. Ce choix est effectué par consultation d'une table de routage en fonction d'une politique de routage. Rappelons qu'un protocole de routage n'indique pas comment est prise la décision de routage (politique de routage), il détermine seulement comment sont échangées les informations de routage. Dans la pratique ces notions sont confondues. Un protocole de routage résout essentiellement trois problèmes :

– il découvre les autres routeurs du réseau ;

– il construit les tables de routage ;

– il maintient les tables de routage à jour.

Si on veut réaliser l'interconnexion de réseaux d'opérateurs différents, il est nécessaire de définir un protocole commun d'échange des informations de routage. Chaque opérateur peut alors utiliser le mode de routage qui lui convient. Aussi, outre l'aspect de limitation du trafic de gestion, le domaine global de routage (**Internet**) a été subdivisé en domaines de routage autonomes (**AS**, *Autonomous System*). Cette division conduit à distinguer deux familles de protocoles de routage (figure 14.29) :

– les protocoles de routage intradomaine, pour le routage à l'intérieur d'un même domaine (**IGP**, *Interior Gateway Protocol*). Les paquets de service du protocole de routage identifient le domaine d'appartenance, tout paquet qui n'appartient pas au même domaine est ignoré. Cette technique limite la diffusion à l'intraréseau ;

– les protocoles de routage interdomaine (**EGP**, *Exterior Gateway Protocol*). Ces protocoles routent les paquets d'informations dans l'interréseau. Ces protocoles doivent prendre en compte les accords commerciaux ou politiques entre les systèmes autonomes. Notons que les machines d'accès à l'interréseau mettent en œuvre les deux types de protocoles, un protocole intradomaine sur leur lien intradomaine, et un protocole interdomaine sur le lien interréseaux.

– *Poison reverse*, complète le *split horizon*. Si, après avoir détecté une route coupée, un routeur reçoit une information d'accessibilité avec un coût important par rapport au coût initial il ignore cette information. Il estime alors que le message lui est revenu par une boucle,

Lorsqu'une nouvelle route est annoncée, si le routeur contient déjà une entrée de même coût dans sa table, il ignore cette information. De ce fait, non seulement RIP ne peut faire d'équilibrage de charge mais, dans un réseau maillé, le chemin est dépendant de l'ordre de mise en marche des routeurs.

Les messages ne sont pas authentifiés. Il est alors possible à un individu malveillant de générer des messages RIP avec des coûts tels que toutes les routes passent par un même routeur. Le nœud ainsi attaqué devient alors un véritable goulet d'étranglement, le réseau peut ainsi être complètement paralysé (congestion).

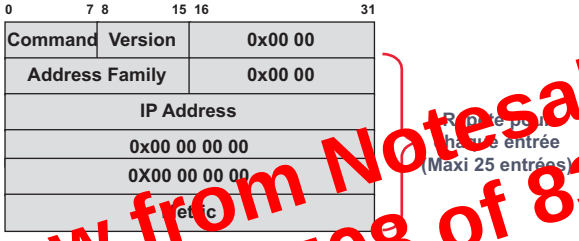


Figure 14.30 Message RIP v1.

Preview from Notesale.co.uk
Page 508 of 837

La taille maximale d'un message RIP (figure 14.30) est de 512 octets de charge utile, auxquels il convient d'ajouter 28 octets pour l'en-tête UDP (port 520) et IP. Cette taille limite le nombre d'entrées dans un message à 25. Le message comporte les informations suivantes :

– le champ *command* permet de distinguer les différents types de message
  – 1, *Request*, permet de demander à un système distant d'envoyer tout ou partie de sa table de routage. Ce message permet, à un routeur, lors de son démarrage d'acquérir rapidement les informations de routage sans attendre une diffusion ;
  – 2, *Response*, message contenant tout ou partie d'une table de routage. Ce message peut être envoyé en réponse au message précédent (*Request*), ou lors d'une simple mise à jour périodique ;
  – 3 et 4 *traceon* et *traceoff*, ces messages aujourd'hui obsolètes, doivent être ignorés ;
  – 5, réservé à Sun Microsystems ;
  – 6, réservé à d'éventuelles nouvelles commandes ;
– le champ *Version* identifie la version du protocole, il doit être mis à 1 ;
– l'ensemble des champs suivants contient les informations en relation avec les routes :
  – *Address Family* identifie la famille d'adresse, cette valeur est à 2 pour IP. Toute autre valeur doit être ignorée. Les deux octets suivants doivent être mis à zéro ;
  – *IP Address* contient l'adresse IP d'un réseau, d'un sous-réseau ou d'une station ou un routeur par défaut (0.0.0.0) ;
  – les deux champs suivants doivent être mis à zéro ;

– Type 5, (**ASBR**, *Autonomous System Boudary Router*), le routeur est en bordure de système autonome. L'ID d'état des liaisons correspond à l'adresse IP de la liaison. Dans les messages d'état des liaisons, cet en-tête est suivi de la liste des liens connus et de leurs caractéristiques.

Dans les différents messages échangés, l'association de l'identifiant du routeur annonçant (celui à l'origine des informations concernant ce lien), de l'identifiant d'état des liens et du type d'état des liens distingue de manière unique un enregistrement. Le champ numéro de séquence identifie une annonce. Le total de contrôle porte sur tout le message d'annonce d'état d'un lien. Dans le message de description de la base de données le champ données étant absent, le total de contrôle ne porte que sur les 20 octets d'en-tête LSA.

Chacun des routeurs participant à l'échange construit, pour les liens dont il n'a pas le descriptif ou pour lesquels l'information est trop vieille, une liste d'état des liens à demander. La structure de ce message (OSPF type 3) est représentée figure 14.37, la signification des champs est identique à celle du message de description de la base de données.

Preview from Notesale.co.uk
Page 516 of 837

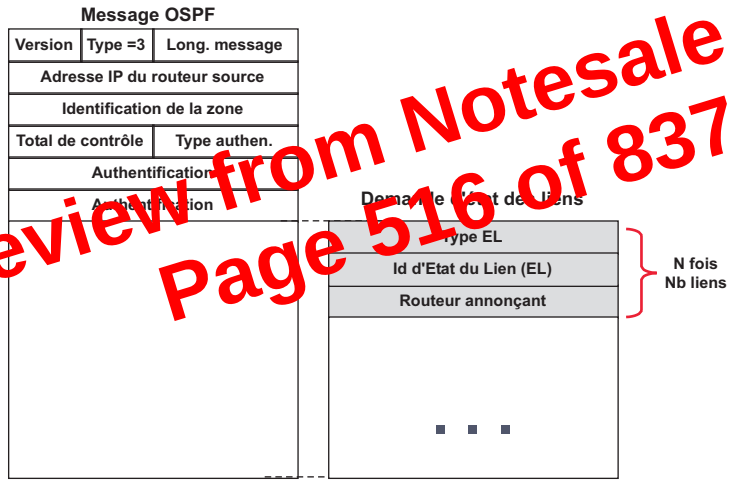


Figure 14.37 Message de demande d'état des liens.

Le routeur cible renvoie un message de mise à jour des liens (*Link State Update*) dont le contenu dépend du type d'état des liens. Les messages de mise à jour de l'état des liens des types EL = 1 décrivent les liens, les messages LSA des types EL = 2, 3, 4 donnent une liste de réseaux et les masques associés, le type EL = 5 décrivent les liens externes. La figure 14.38 donne le format d'un message de mise à jour pour un EL de type 1.

L'en-tête de description d'un lien précise la nature du routeur annonçant (bit **V** pour *Virtual*, routeur en extrémité d'un lien virtuel ; bit **E** pour *External*, routeur en frontière d'un système autonome ; **B** pour *Border*, routeur en bordure d'aire). Le champ significatif suivant indique le nombre de liens décrits pour ce routeur. Le tableau de la figure 14.39 indique en fonction de la valeur du champ *Type*, la signification du champ d'identification du lien et du champ données du lien.

Enfin, la métrique est indiquée. OSPF peut gérer plusieurs tables de routage et router en fonction du TOS. Les routeurs qui ont cette possibilité positionnent à 1 le bit T de l'en-tête du message d'état des liens (champ option). La partie descriptive du message d'état des liens fournit, pour chaque lien, une métrique par TOS géré. Le routage sera déterminé selon la valeur du champ TOS du datagramme IP (figure 14.40).

boucle...), le monde des réseaux d'entreprise est encore largement dominé par des protocoles du type vecteur distance que ceux-ci soient normalisés (RIP) ou d'origine constructeur par exemple **IGRP** (*Interior Gateway Routing Protocol*) et **EIGRP** (*Enhanced Interior Gateway Protocol*) de chez Cisco.

Le choix, pour une entreprise de tel ou tel protocole de routage est un choix stratégique. Quelles que soient les qualités des protocoles propriétaires, ils sont et demeurent propriétaires ce qui peut constituer un handicap lors de l'évolution du réseau ou du renouvellement des équipements.

Le routage interdomaine

Un système autonome (AS) correspond à un domaine de routage[8] sous le contrôle d'une autorité d'administration unique. Les différents systèmes autonomes composant l'Internet doivent s'échanger leurs informations d'accessibilité. Ainsi, chacun des routeurs de bordures des deux systèmes autonomes de la figure 14.42 doit d'une part établir une connectivité entre eux et, d'autre part informer leur voisin des réseaux qu'ils savent atteindre.

Preview from Notesale.co.uk
Page 519 of 837

Figure 14.42 – Connectivité de deux systèmes autonomes.

Ainsi, le routeur de bordure de l'AS « A » annonce au routeur de bordure de l'AS « B » par l'intermédiaire d'un protocole de routage interdomaine (**EGP**, *External Gateway Protocol*) les informations (liste d'accessibilité) qu'il a acquises, par un protocole de routage intradomaine (**IGP**, *Interior Gateway Protocol*), sur les réseaux accessibles par transit dans sa zone. Le routeur B va diffuser ces informations au format de l'IGP utilisé dans sa zone.

Le protocole de routage externe doit résoudre de nombreux problèmes spécifiques. Le premier concerne le routage politique. Supposons qu'une entreprise internationale dispose d'un réseau privé. Afin de minimiser le trafic sur son réseau, elle dispose d'un accès à Internet dans chacun des pays desservis par son réseau (figure 14.43). Cette entreprise s'oppose évidemment à ce que le trafic Internet transite par son réseau.

Le second, mis en évidence par la figure 14.42, concerne les métriques. Quelle métrique utiliser dans les annonces puisque chacun des AS peut utiliser un protocole de routage interne différent et transparent à l'EGP ? Le coût annoncé est donc forfaitaire (distance arbitraire), il permet en outre aux administrateurs de favoriser le transit par tel ou tel réseau en fonction d'accords commerciaux ou autres. Ce qui répond à la préoccupation précédente.

De nombreux protocoles de routage externes ont été testés. Actuellement Internet met en œuvre **BGP 4** (*Border Gateway Protocol*). Les informations de routage échangées comprennent : le numéro de système autonome, la liste des réseaux de chaque système autonome, la distance relative vers chacun des sous-réseaux de l'AS et l'adresse IP du routeur d'accès à ces réseaux. BGP prend en compte des critères extérieurs aux domaines de routage

8. Le concept de systèmes autonomes a été défini à la section 8.5.2.

© Dunod – La photocopie non autorisée est un délit

Les adresses de groupe les plus connues sont :

– 224.0.0.1, tous les hôtes multicast de ce sous-réseau ;
– 224.0.02, tous les routeurs multicast de ce sous-réseau ;
– 224.0.0.4, tous les routeurs exécutant le protocole de routage multicast DVMRP ;
– 224.0.1.11, applications audio (IETF) ;
– 224.0.1.12, application vidéo (IETF) ;
– 224.0.1.16, diffusion de musique (Music-Service) ;
– 224.0.1.17, *Audionew* (bulletins d'information radio) ;

Le protocole local IGMP (RFC 2236)

Le protocole **IGMP** (*Internet Group Management Protocol*) est le protocole d'apprentissage utilisé par les routeurs multicast pour découvrir l'existence, dans les sous-réseaux auxquels ils sont raccordés, de membres d'un groupe multicast (figure 14.51).

Preview from Notesale.co.uk
Page 526 of 837

Figure 14.51 Principe du protocole IGMP.

Le protocole IGMP version 2 utilise quatre types de messages et un seul format (figure 14.52) :

– Les messages de demande d'adhésion (*Host Membership Query*, type = 0x11) destinés à demander régulièrement aux stations à quel groupe multicast elles appartiennent. Un seul routeur multicast du réseau envoie régulièrement ces messages (routeur dominant), c'est celui de plus petite adresse IP. Le champ *Multicast Group Address* est à 0.
– Les messages de réponse (*Host Membership Report*, type = 0x16) sont envoyés par tout hôte appartenant à un groupe de diffusion multicast. Chaque hôte répond après un délai aléatoire avant le délai imposé (*Max response Time*). Le champ *Multicast Group Address* est alors renseigné sur le groupe d'appartenance. Si un hôte a déjà répondu pour ce groupe, les autres hôtes du même groupe s'abstiennent alors de répondre.
– Lorsqu'un hôte quitte une session multicast, il envoie un message d'abandon de groupe (*Leave Group Message*, type 0x17) à l'adresse multicast 224.0.0.2 (tous les routeurs multicast du sous-réseau).
– En réponse à ce message, le routeur demandeur envoie un message de demande d'adhésion spécifique au groupe qui vient d'être quitté (*Group Specific Query Message*, type = 0x11 mais avec le champ *Multicast Group Address* renseigné du groupe multicast abandonné). En l'absence de réponse, le groupe est supprimé de sa liste d'adhésion et plus aucun message concernant ce groupe ne sera relayé sur le sous-réseau.

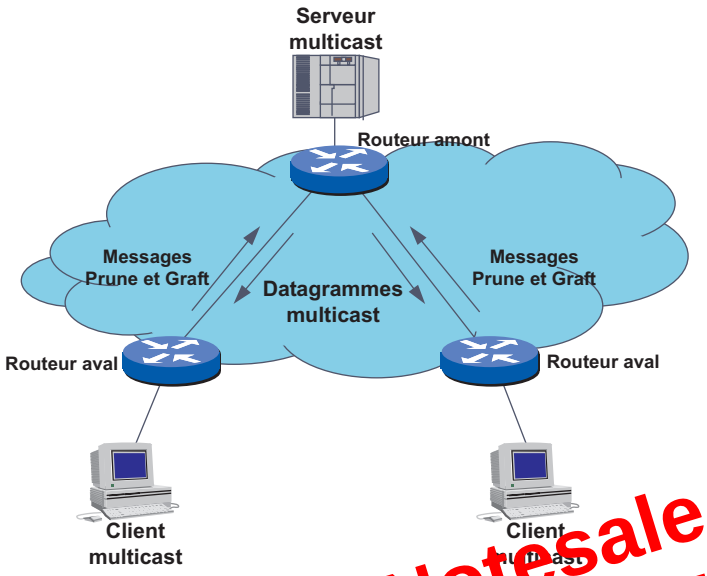


Figure 14.54 Diffusion de messages dans un réseau DVMRP

Preview from Notesale.co.uk
Page 528 of 837

À l'instar de RIP, le protocole DVMRP échange ses tables de routage avec ses voisins DVMRP (message *route report* toutes les 60 s à l'adresse de diffusion 224.0.0.4). Les voisins DVMRP sont découverts par l'émission, toutes les 10 s, de messages *probe message*.

➤ Internet et le multicast

La composante d'Internet qui assure la diffusion de messages en multicast sur le réseau est désignée sous le nom de **Mbone** (*Multicast Backbone*). Il s'agit d'un réseau virtuel reliant les différents routeurs multicast (mrouteurs) par des tunnels (tunnels multicast), mais le service rendu est du type datagramme.

Diverses applications sont offertes téléconférences, programmes radio, jeux... Un annuaire des sessions en cours permet aux utilisateurs de rejoindre un groupe de diffusion.

14.4.5 Fonctions annexes des routeurs

Les routeurs multiprotocoles

Dans des environnements complexes, il arrive que plusieurs protocoles réseaux soient utilisés en même temps (IP, IPX...). Les routeurs capables d'assurer l'acheminement de données de différents protocoles sont dits routeurs multiprotocoles.

Dans ces environnements, se pose la question de la reconnaissance du protocole à router. Digital, Intel et Xerox ont résolu ce problème en introduisant dans la trame Ethernet (Ethernet V2) le champ type de protocole (*Ethertype*). ISO identifie le protocole supérieur par les champs DSAP et SSAP de la trame LLC. Certaines implémentations de réseaux locaux utilisent la trame LLC mais des protocoles de niveau supérieur non ISO (Token Ring...). Pour résoudre le problème d'identification, une encapsulation supplémentaire a été introduite : l'encapsulation **SNAP** (*SubNetwork Access Protocol*). La figure 14.55 rappelle ces différents formats pour les réseaux de type Ethernet.

Exercice 14.7 Masque de sous-réseau

Deux réseaux (A et B) utilisent le protocole TCP/IP, ils sont reliés via un routeur. L'entreprise a défini le masque de sous-réseau : 255.255.0.0. Un utilisateur du réseau A sur la machine 100.64.0.102 se plaint de ne pouvoir joindre un correspondant d'adresse 100.64.45.102 du réseau B. Expliquez pourquoi, donnez une solution simple pour que ces machines puissent communiquer ?

Exercice 14.8 Routage statique

En reprenant le plan d'adressage de la solution de l'exercice 12.11, établissez les tables de routage (routage fixe) du réseau. Pour répondre aux Ping, les adresses des LL (liaisons louées) seront incluses dans les tables. Vous vous aiderez de la figure 14.64 ci-dessous.

Preview from Notesale.co.uk
Page 535 of 837

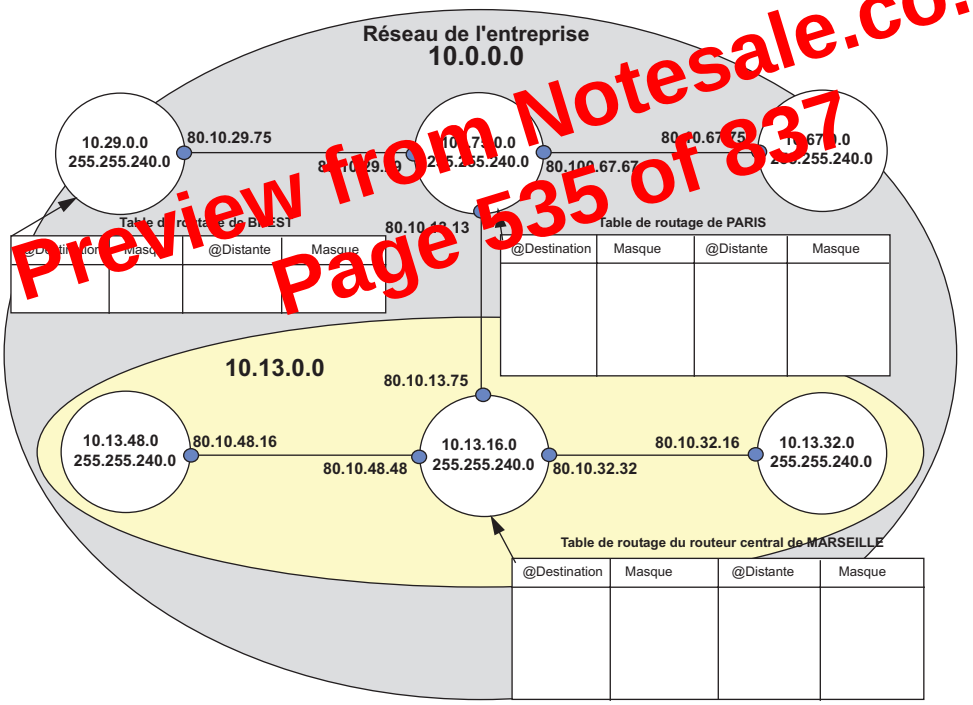


Figure 14.64 Plan d'adressage et tables de routage du réseau 10.0.0.0.

© Dunod – La photocopie non autorisée est un délit

La commutation de circuits ou commutation spatiale consiste à juxtaposer bout à bout des voies physiques de communication, la liaison étant maintenue durant tout l'échange. La numérisation de la voix a permis le multiplexage temporel des communications. La commutation spatiale a été remplacée par la commutation d'intervalles de temps (IT) ou commutation temporelle. Ce concept est illustré figure 15.2. En mettant en relation un IT d'une trame en entrée avec un IT d'une autre trame en sortie, la commutation temporelle émule un circuit. La communication est *full duplex*, une bande passante de 64 kbit/s, dans chaque sens, est donc réservée durant toute la communication.

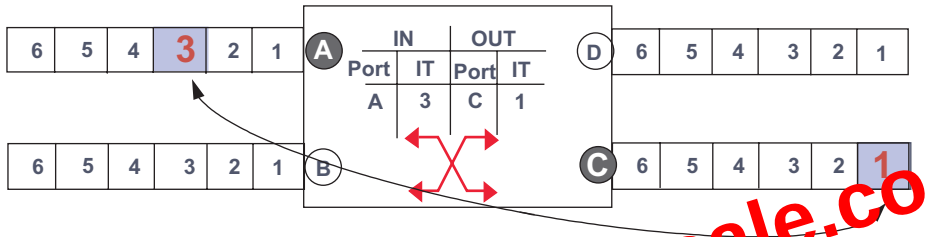


Figure 15.2 Principe de la commutation temporelle.

Preview from Notesale.co.uk
Page 538 of 837

Les supports de transmission sont constitués de voies numériques multiplexées selon une hiérarchie appelée hiérarchie plésiochrone (*Plesiochronous Digital Hierarchy*, **PDH**). Malgré la numérisation du réseau, la liaison des abonnés résidentiels est restée essentiellement analogique. C'est le commutateur de rattachement qui réalise la fonction de numérisation et de dénumérisation de la voix (figure 15.3).

Figure 15.3 Les modes de raccordement.

15.2 ORGANISATION DU RÉSEAU TÉLÉPHONIQUE

15.2.1 Architecture traditionnelle

Le réseau téléphonique a une organisation hiérarchique à trois niveaux (figure 15.4). Il est structuré en zones, chaque zone correspond à un niveau de concentration et en principe de taxation. On distingue :

– Zone à Autonomie d'Acheminement (**ZAA**), cette zone, la plus basse de la hiérarchie, comporte un ou plusieurs Commutateurs à Autonomie d'Acheminement (**CAA**) qui eux-mêmes desservent des Commutateurs Locaux (**CL**). Les commutateurs locaux ne sont que de simples concentrateurs de lignes auxquels sont raccordés les abonnés finals. La

ZAA (Zone à Autonomie d'Acheminement) est un réseau étoilé, elle constitue le réseau de desserte ;

– Zone de Transit Secondaire (**ZTS**), cette zone comporte des Commutateurs de Transit Secondaires (**CTS**). Il n'y a pas d'abonnés reliés directement aux CTS (Commutateurs de Transit Secondaires). Le réseau étant imparfaitement maillé lorsqu'un CAA (Commutateur à Autonomie d'Acheminement) ne peut atteindre directement le CAA destinataire, ils assurent le brassage des circuits ;

– Zone de Transit Principal (**ZTP**), cette zone assure la commutation des liaisons longues distances. Chaque ZTP (Zone de Transit Principal) comprend un Commutateur de Transit Principal (**CTP**). Au moins un Commutateur de Transit Principal (**CTP**) est relié à un Commutateur de Transit International (**CTI**).

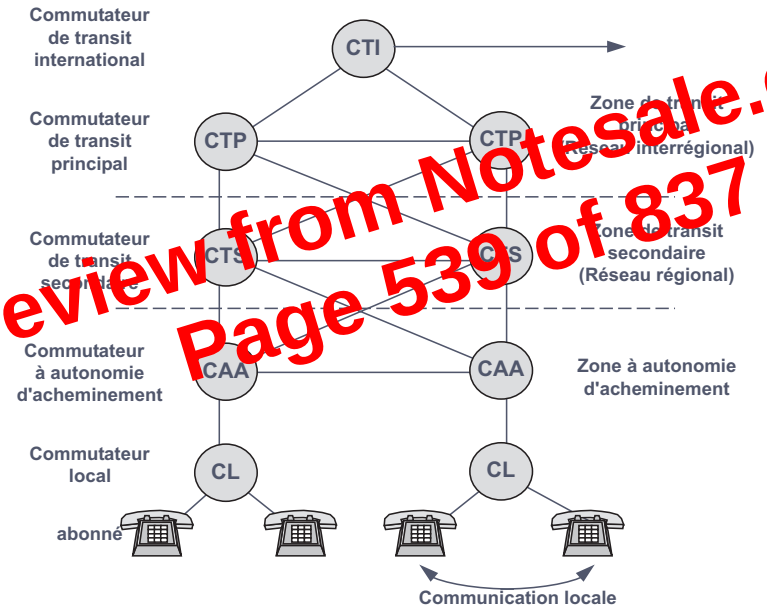


Figure 15.4 Organisation du réseau téléphonique.

Preview from Notesale.co.uk
Page 539 of 837

Le réseau étant partiellement maillé, plusieurs itinéraires sont généralement possibles pour atteindre un abonné. Afin d'optimiser l'utilisation des faisceaux, on distingue deux types de faisceaux : les faisceaux de premier choix et les faisceaux de second choix ; les faisceaux de second choix constituent des faisceaux de débordement. Pour un numéro donné, le faisceau de premier choix est choisi de telle manière qu'il conduise l'appel vers le commutateur le plus proche de l'abonné appelé en empruntant les faisceaux de plus faible hiérarchie.

15.2.2 Gestion du réseau

La gestion générale du réseau discerne trois fonctions :

– **la distribution**, celle-ci comprend essentiellement la liaison d'abonné ou boucle locale (paire métallique) qui relie l'installation de l'abonné au centre de transmission de rattachement. Cette ligne assure la transmission de la voix (fréquence vocale de 300 à 3 400 Hz), de

© Dunod – La photocopie non autorisée est un délit

la numérotation (10 Hz pour la numérotation décimale – au cadran – et 697 à 1 633 Hz pour la numérotation fréquentielle) et de la signalisation générale (boucle de courant, fréquences vocales) ;

– **la commutation**, c'est la fonction essentielle du réseau, elle consiste à mettre en relation deux abonnés, maintenir la liaison pendant tout l'échange et libérer les ressources à la fin de celui-ci. C'est le réseau qui détermine les paramètres de taxation et impute le coût de la communication à l'appelant ou à l'appelé ;

– **la transmission**, c'est la partie support de télécommunication du réseau, cette fonction est remplie soit par un système filaire cuivre, par de la fibre optique ou par des faisceaux hertziens. Aujourd'hui, le réseau français est intégralement numérisé, seule la liaison d'abonné est encore, la plupart du temps, analogique et sur support cuivre, notamment pour les abonnés résidentiels.

Preview from Notesale.co.uk
Page 540 of 837

15.3 ÉTABLISSEMENT D'UNE COMMUNICATION TÉLÉPHONIQUE

15.3.1 Principe d'un poste téléphonique

Établir une communication téléphonique c'est mettre en relation deux terminaux téléphoniques. Le poste téléphonique doit remplir plusieurs fonctions, chacune est réalisée par un organe spécifique. Le terminal téléphonique élémentaire comporte cinq organes (figure 15.5) :

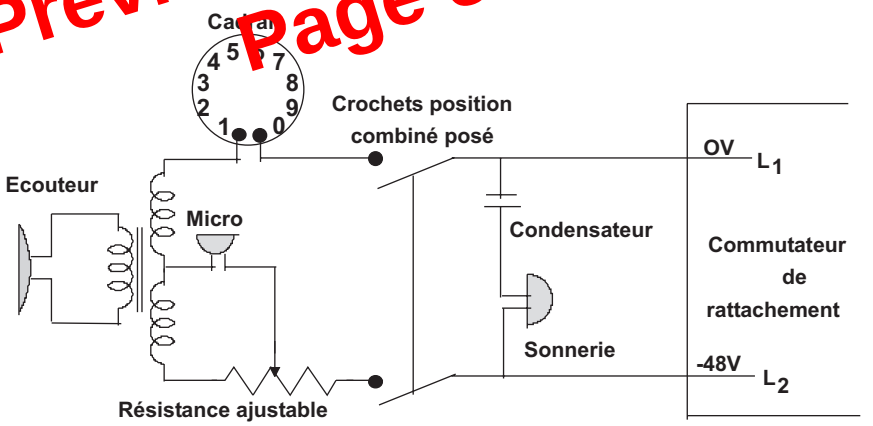


Figure 15.5 Le terminal téléphonique S63.

– les crochets ou supports sur lesquels repose le combiné ; lorsque le combiné est soulevé les contacts se ferment. Le circuit électrique est alors fermé, le commutateur de rattachement détecte le courant et en déduit que l'abonné désire entrer en communication. Un potentiomètre permet d'ajuster ce courant à 30 mA. De même, lors du raccroché, le commutateur détecte l'ouverture de la boucle de courant. L'ouverture ou la fermeture de cette boucle permet, très simplement, au commutateur de rattachement de détecter le changement d'état du terminal (signalisation) ;

– le micro ou capteur, constitué d'une simple membrane qui par ses vibrations, sous l'effet de la pression acoustique (voix), fait varier la résistance interne de celui-ci (micro au charbon).

– lorsque l'appelant décroche le combiné, le réseau (le commutateur de rattachement) détecte la fermeture de la boucle de courant ;
– il envoie à l'usager l'invitation à numéroter (signal à 440 Hz). Dans le même temps, il arme une temporisation ;
– le demandeur n'effectuant aucune opération, à l'échéance du compteur (Timer, de 15 à 20 secondes) le commutateur de rattachement inhibe le poste en lui envoyant la tonalité d'occupation (signal de décroché malencontreux) pendant environ une minute.

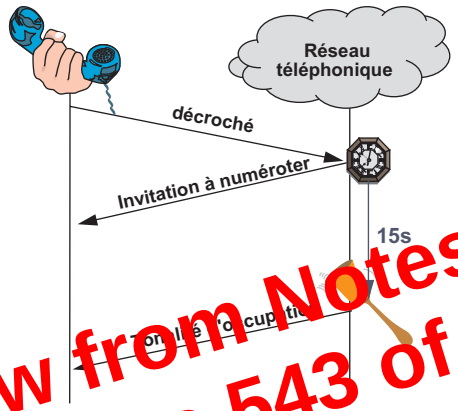


Figure 15.8 Diagramme des événements lors d'un décroché malencontreux.

Preview from Notesale.co.uk
Page 543 of 837

15.3.4 La numérotation

Préfixe international	Indicatif Pays	Numéro national demandé		
		EZ	AB PQ	MC DU
Pour sortir du réseau national, en France 00	Par exemple France = 33	Exploitant Zone	Numéro du commutateur de rattachement	Numéro de la ligne d'abonné

Valeur E	Signification
0	Opérateur de boucle locale
1	Numéros d'urgence
2	Siris
3	Numéros spéciaux (téléservices)
4	Télétel 2
5	Omnicom
6	Esprit Telecom
7	Cegetel
8	France Télécom
9	9 Télécom

Figure 15.9 Structure d'un numéro d'abonné et valeur du préfixe E.

Le numéro d'abonné (Numéro international au format E.163 ou E.164) correspond à l'identification du point d'accès au réseau (prise terminale). L'adresse est du type hiérarchique, la structure en est donnée par la figure 15.9. Les différents éléments qui la constituent sont :

© Dunod – La photocopie non autorisée est un délit

(H_0), 1 536 kbit/s (H_{11}) ou de 1 920 kbit/s (H_{12}). La figure 15.16 illustre le principe de raccordement d'un terminal au réseau RNIS.

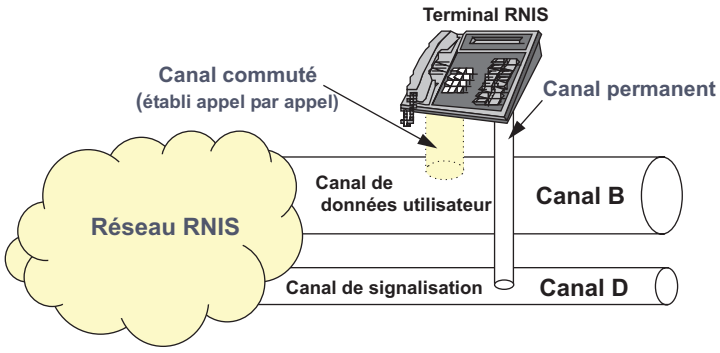


Figure 15.16 Connexions d'un terminal RNIS.

Preview from Notesale.co.uk
Page 548 of 837

La connexion permanente du terminal au canal de signalisation rend obsolète la notion de terminal occupé : le terminal pourra toujours être alerté d'un appel entrant et recevoir, via le canal D, des messages (mini-messages). RNIS est donc un système de transmission utilisant deux réseaux distincts : un réseau de transmission (commutation de circuits) et un réseau de signalisation (commutation de paquets). Les réseaux sont fonctionnellement différents. Cependant, ils utilisent les mêmes capacités de transport (multiplexage) mais les commutateurs sont différents bien que situés sur les mêmes sites. La figure 15.17 illustre ce concept.

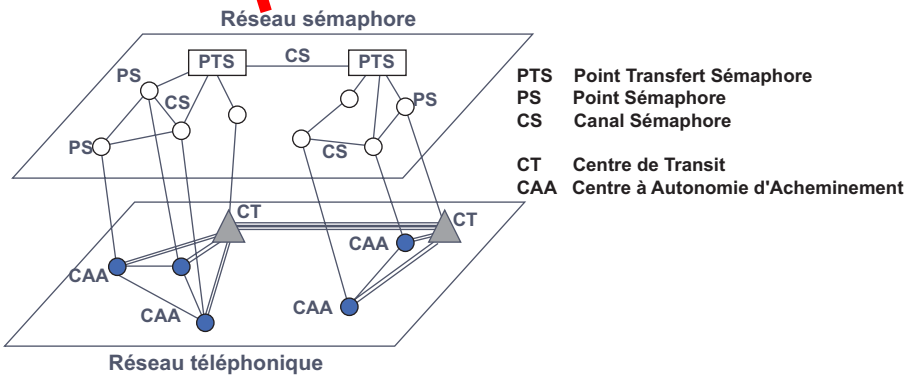


Figure 15.17 Réseau téléphonique et réseau sémaphore.

15.4.4 Le raccordement d'usager

Les accès RNIS

L'accès au réseau RNIS s'effectue par l'intermédiaire d'interfaces normalisées appelées points de référence (recommandation I 411 du CCITT) et dépendant du type de terminal à raccorder. Les terminaux n'accèdent pas directement au réseau, ils y sont raccordés via des interfaces. L'équipement d'interfaçage entre l'installation d'abonné et le réseau porte le nom de **TNR** (Terminaison Numérique de Réseau) ou de **TNL** (Terminaison Numérique de Ligne) selon le

type d'abonnement au réseau. La **TNA** (Terminaison Numérique d'Abonné) est un équipement facultatif, généralement un commutateur téléphonique privé (**PABX**, *Private Branched eXchange*). Lorsque l'installation d'abonné ne comporte pas de TNA, les points de référence S et T sont confondus.

Les divers points de référence (figure 15.18) sont, par ordre alphabétique, du privé vers le réseau public :

– **Point R**, interface pour les terminaux non RNIS, c'est notamment le cas des terminaux dotés d'une interface V.24/28, X.21, V.35...

– **Point S**, point d'accès universel pour les équipements compatibles RNIS,

– **Point T** matérialise la limite entre le réseau public et l'installation d'abonné, c'est aussi la frontière de responsabilité entre l'opérateur et l'abonné,

– **Point U**, il symbolise la limite entre le réseau de transport et la liaison d'abonné.

Preview from Notesale.co.uk
Page 549 of 837

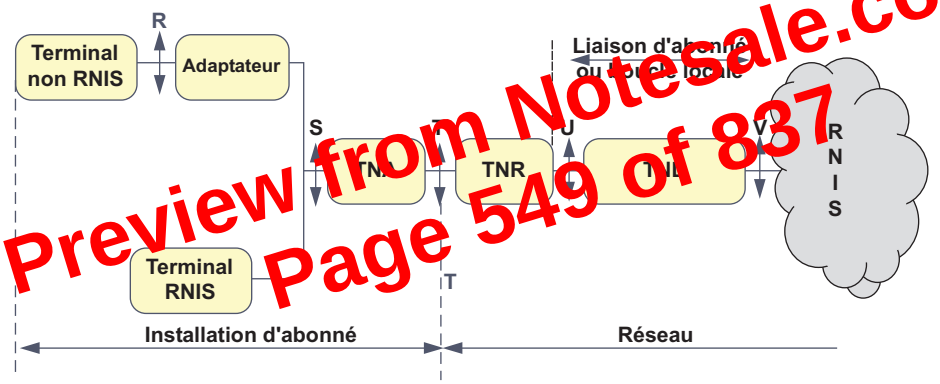


Figure 15.18 Les points de référence des accès au RNIS.

L'offre RNIS se décline selon la combinaison des trois types de canaux mis à disposition :

– les **canaux B** sont les canaux de transfert d'information, le débit nominal est de 64 kbit/s ;

– le **canal D**, à 16 ou 64 kbit/s selon le nombre de canaux B offerts, est dédié au transfert de la signalisation (protocole D). La bande non utilisée par la signalisation peut être utilisée pour transférer des données en mode paquet (accès aux réseaux X.25) ;

– les **canaux H**, combinaison de n canaux à 64 kbit/s offrent un débit de n · 64 kbit/s. On distingue les canaux H_0 à 384 kbit/s, H_{11} à 1 536 kbit/s et H_{12} à 1 920 kbit/s. Les canaux B sont commutés et établis appel par appel sans garantie du chemin.

Selon le nombre de canaux offerts, on définit trois types d'accès, dont seuls deux sont disponibles en France :

– **T0**, ou accès de base (**BRI**, *Basic Rate Interface*), offre un débit de 192 kbit/s dont 144 utiles, soit 2 canaux B et un canal D à 16 kbit/s,

– **T1**, non disponible en France,

– **T2**, ou accès primaire (**PRI**, *Primary Rate Interface*) offre 15, 20, 25 ou 30 canaux B et un canal D à 64 kbit/s. Soit, pour 30 canaux B un débit de 2 048 kbit/s dont 1 920 utiles.

© Dunod – La photocopie non autorisée est un délit

➤ Présentation d'appel, double appel, va-et-vient

Durant la communication, si un nouvel appel survient, l'usager en est averti (Présentation d'appel). Celui-ci peut achever la communication en cours et prendre la nouvelle, ou mettre la communication en cours en attente et prendre la nouvelle (Double appel). L'usager peut aussi passer alternativement de l'une à l'autre (Va-et-vient). L'usager ne peut prendre une troisième communication, celle-ci lui est cependant présentée.

➤ Identification d'appel, non-identification, identification d'appel malveillant

Un appel entrant est présenté avec l'identification de l'appelé (Identification d'appel) sauf si l'appelant a souscrit au complément de service « non-identification d'appel ». L'identification d'appel malveillant permet à un usager de faire identifier par l'opérateur l'auteur d'un appel malveillant.

➤ Portabilité

C'est la faculté dont dispose l'usager, durant un appel, de suspendre une communication et de reprendre celle-ci plus tard sur le même poste au même endroit ou sur le même poste déplacé dans l'installation ou encore sur un autre poste de la même installation. La suspension de l'appel n'interrompt pas la facturation. Elle est limitée à 3 minutes.

Preview from Notesale.co.uk
Page 552 of 837

➤ Renvoi du terminal, transfert d'appel national

Un utilisateur peut faire réacheminer ses appels sur un autre poste de l'installation (Renvoi d'appel) ou sur un autre poste d'une autre installation (Transfert d'appel national). Le renvoi d'appel peut être inconditionnel, sur occupation ou sur non-réponse.

➤ Mini-message (Signalisation d'usager à usager)

Cette facilité permet aux usagers de s'échanger des messages de 32 caractères (Mini-message) en dehors de toute communication lors des phases d'établissement ou de libération de la communication.

➤ Services restreints

Ce complément de service permet de limiter l'usage d'un poste aux communications locales, de voisinage ou nationales.

➤ Sous-adresse

Cette information complète l'adresse du terminal, soit pour distinguer celui-ci, soit pour sélectionner sur celui-ci un service particulier (exemple : terminal multimédia). La sous-adresse peut contenir jusqu'à 40 caractères IA5. La sous-adresse est transportée de manière transparente sur le réseau.

➤ Sélection Directe à l'Arrivée (SDA)

La sélection directe à l'arrivée permet de joindre directement un terminal de l'installation sans nécessiter le recours à un(e) standardiste. C'est l'équipement local de l'abonné (PABX) qui effectue la relation entre le numéro SDA appelé et le numéro interne du poste demandé.

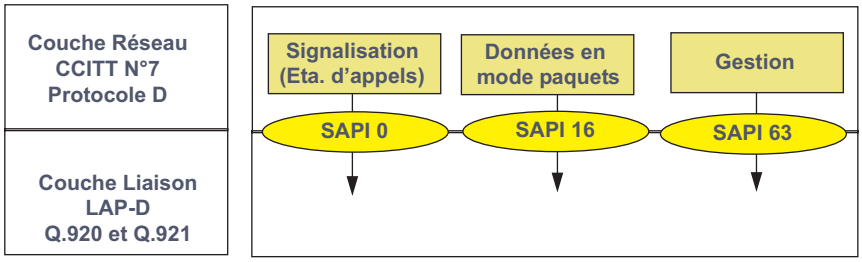


Figure 15.23 Affectation des principaux SAPI.

Le principe général de l'accès au canal D est similaire à celui utilisé dans les réseaux locaux de type « Ethernet ». Cependant, le support physique étant multiplexé, il peut y avoir une activité électrique sur celui-ci (canal B) alors que le canal D est libre. L'écoute doit se faire au niveau du canal et non du support. Pour détecter et prévenir une éventuelle collision toutes les données émises sur le canal D sont retransmises par la TNR sur un **canal d'écho** (**canal E**, figure 15.24). La station vérifie en permanence que ce qu'elle reçoit sur le canal E correspond bien à ce qu'elle a émis sur le canal D. Si ce n'est pas le cas la station s'arrête (collision). En l'absence d'émission, un terminal émet des « 1 » (potentiel électrique 0). Lorsqu'il désire accéder au canal D, le terminal écoute celui-ci, s'il ne détecte aucune activité durant un certain délai (8 à 11 temps bit selon le message à émettre), il émet sa trame LAP-D.

Preview from Notesale.co.uk
Page 555 of 837

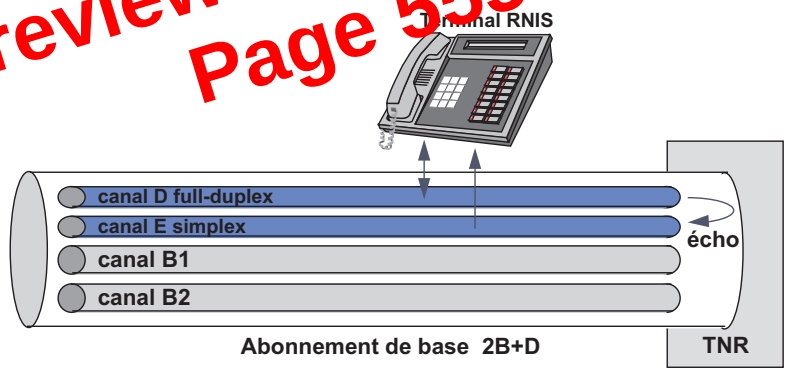


Figure 15.24 Le terminal émet sur le canal D écoute l'écho le canal E.

Afin d'éviter que toutes les stations en conflit ne s'arrêtent, un mécanisme de résolution de la contention (CSMA/CR) assure qu'une station, et une seule, pourra poursuivre son émission. Le système repose sur le codage retenu pour les signaux électriques, les zéros logiques correspondent à l'émission d'une tension alternativement positive ou négative (élimination de la composante continue), tandis que les 1 logiques correspondent à une tension nulle. Ce codage, appelé codage pseudo-ternaire, est représenté figure 15.25.

La répétition, par le canal E, des données du canal D est telle que, pour tout 1 émis, le canal E retransmet un 1 (tension nulle), pour tout 0 émis, le canal E retransmet un 0. C'est-à-dire que l'émission d'un 0 par une station masque l'émission d'un 1 par une autre. Ce mécanisme, illustré figue 15.25, autorise la résolution des conflits d'accès. Au temps d'horloge 1, 2, 3 et 4 les signaux émis sur le canal E correspondent à ceux émis par les divers terminaux, ceux-ci poursuivent leur émission.

© Dunod – La photocopie non autorisée est un délit

Principe général de fonctionnement

Chaque BTS diffuse en permanence sur un canal de signalisation (**BCCH**, *Broadcast Control CHannel*) des informations générales sur le type de réseau auquel la cellule est rattachée. Lorsqu'un mobile est mis sous tension, il recherche (*scanning*) un canal BCCH. Le mobile sélectionne alors la BTS (cellule) dont le niveau de réception est le plus élevé en acquittant le signal de BCCH sur le canal d'accès aléatoire de la cellule (**RACH**, *Random Access CHannel*) et s'y inscrit. Le réseau lui attribue alors un canal de signalisation (**SACCH**, *Slow Associated Control CHannel*). Les données utilisateurs de la HLR (base de données centrale) sont recopiées dans la VLR (base de données locale des visiteurs de la cellule). À la demande de la BSC, la HLR enregistre la localisation du mobile pour être en mesure d'y acheminer les appels entrants. En principe, la base HLR est unique par réseau (**PLMN**, *Public Land Mobile Network*).

Preview from Notesale.co.uk
Page 565 of 837

15.5.2 Gestion de l'abonné et du terminal

On distingue plusieurs types de terminaux selon leur taille (terminaux portables et portatifs), leur bande de fréquences (GSM 900 MHz, DCS 1 800 MHz et les terminaux bi-bandes). L'utilisation de systèmes portables miniaturisés, facilement « empruntables » et d'une interface air a nécessité l'introduction de mécanismes d'identification garantissant une certaine sécurité et préservant l'anonymat des communications. C'est ainsi, que les identifications de l'abonné et du terminal ont été dissociées.

L'abonné est identifié par un module spécifique dans lequel sont inscrites toutes les données propres à l'utilisateur (carte **SIM**, *Subscriber Identity Module*). Cette carte, délivrée par l'opérateur, mémorise un nombre important d'informations :

- des données propres à l'opérateur (réseau...) ;
- des données propres à l'utilisateur (identification, services optionnels, annuaire...) ;
- des données propres à l'usage du terminal (dernière zone de localisation, listes des réseaux utilisés...) ;
- les informations de sécurité (mots de passe utilisateur, compteurs d'erreur, clé de déblocage, clé d'authentification, clé de cryptage propre au terminal...) ;
- les mini-messages reçus (**SMS**, *Short Message Service*)...

L'utilisation du portable est protégée par un mot de passe utilisateur demandé à l'initialisation du système (CHV1, *Card Holder Verification* ou code **PIN**, *Personnal Identity Number*), certaines fonctions ne sont accessibles qu'après l'introduction d'un mot de passe de second niveau (CHV2 ou PIN2).

La carte SIM permet de dissocier les données utilisateurs de celles du terminal et permettre à l'opérateur de bloquer l'un indépendamment de l'autre. Le terminal est identifié par **l'IMEI** (*International Mobile Equipement Identity*). À chaque utilisateur est associé un numéro d'appel international (**MSISDN**, *Mobile Station ISDN*) par lequel l'abonné peut être appelé et un identifiant utilisé par le réseau pour le localiser (**IMSI**, *International Mobile Subscriber Identity*). Lorsqu'un utilisateur est présent dans une zone, pour ne pas transporter dans le réseau son identifiant personnel (confidentialité), un identifiant temporaire lui est attribué (**TMSI**, *Tempo-*

© Dunod – La photocopie non autorisée est un délit

rary Mobile Station Identity). La figure 15.37 illustre l'utilisation de ces identifiants lors d'un appel entrant depuis le réseau public commuté (RTC).

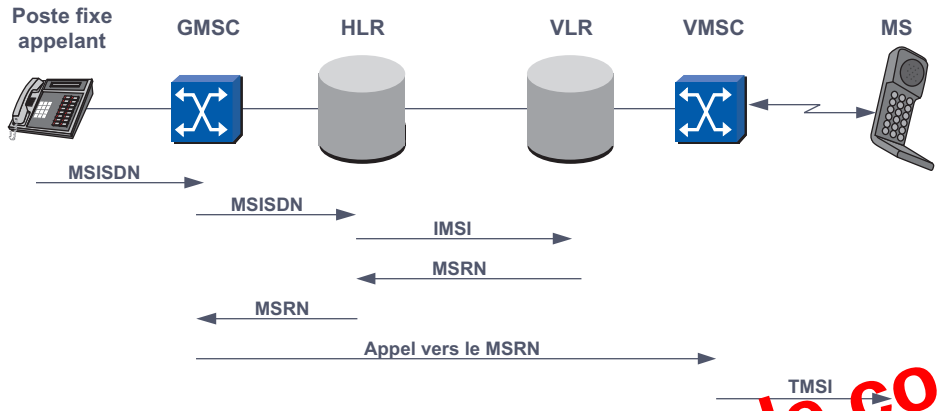


Figure 15.37 Echange des différents identifiants

Le poste appelant numérote le MSISDN (06 xx xx xx xx), cet appel est acheminé par le réseau téléphonique fixe vers le commutateur du réseau de mobile le plus proche (MSC) qui fera office de passerelle entre les deux réseaux (**GMSC**, *Gateway MSC*). Le GMSC interroge le HLR pour connaître la localisation de l'appelé. Le HLR substitue au MSISDN le IMSI (N° attribué pour localiser l'appelé) et interroge la base VLR qui lui attribue alors un **MSRN** (*Mobile Station Roaming Number*, Numéro permettant le routage des appels, ce numéro est composé du code pays du VLR, de l'identifiant du VLR et du N° d'abonné). Le GMSC établit alors l'appel vers le **VMSC** (*Visited MSC*). Enfin, le VMSC établit l'appel vers le mobile en utilisant l'identité temporaire (TMSI).

Preview from Notesale.co.uk
Page 566 of 837

L'affectation des canaux de communication est dynamique. Elle suit les procédures décrites ci-après. Lors d'un appel entrant, la base radio diffuse sur un canal d'appel (*paging*) l'identification de la station appelée. Le mobile qui reconnaît son identification accuse réception du message sur le canal de retour d'appel. La base radio affecte alors au mobile un canal de trafic (fréquence et IT). Lors d'un appel sortant, le canal de trafic n'est attribué par la base radio qu'après que l'appelant ait décroché. Cette technique dite du rappel du demandeur évite d'affecter des ressources à un appel non abouti.

15.5.3 L'interface radio

Organisation cellulaire du réseau

On appelle cellule, la zone géographique couverte par un émetteur (figure 15.38). La taille des cellules doit tenir compte de nombreux facteurs, notamment :

– des conditions de propagation. Les systèmes de téléphonie mobile utilisent des fréquences de l'ordre du GHz, la propagation de telles fréquences se fait uniquement par onde directe. Les obstacles créent des zones d'ombre ;

– de la limitation de la puissance d'émission du mobile. Un des éléments essentiels de la téléphonie mobile est le poids du terminal, ce facteur impose des batteries de faible capacité et donc, afin de disposer d'une autonomie suffisante, une puissance d'émission limitée ;

et un arrêt immédiat faute d'abonné, Iridium a été remis en service en mars 2001. Il offre des services de voix, données, fax et messagerie.

L'une des particularités essentielles d'Iridium est de permettre une communication intersatellite : les communications, entre deux mobiles, peuvent être acheminées directement dans le réseau Iridium sans emprunter de liens terrestres. Les communications sont établies en *full duplex* à 2,4 kbit/s (bande passante identique pour la transmission de données et les fax).

➤ Le système Globalstar

Globalstar, soutenu par Alcatel et France Télécom, utilise 48 satellites en orbite basse (1 410 km) répartis sur 8 plans orbitaux. À la différence d'Iridium les communications intersatellites ne sont pas possibles. Pour mettre en relation deux utilisateurs non desservis par le même satellite, Globalstar utilise les réseaux traditionnels des opérateurs terrestres.

Globalstar offre les mêmes services qu'Iridium mais autorise, en plus, une fonction de localisation de type GPS. Chaque satellite peut établir 28 800 communications simultanées.

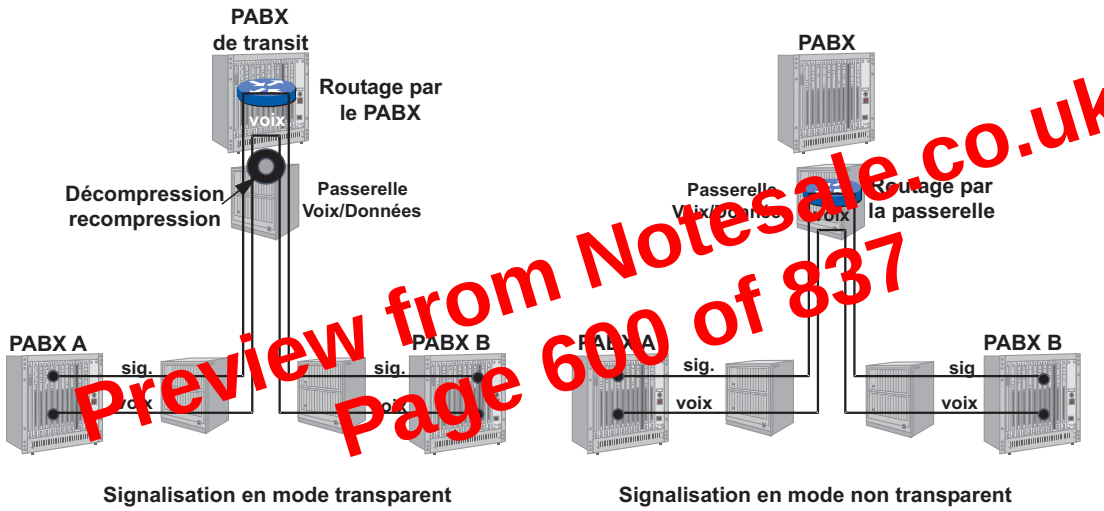
15.6 CONCLUSION

Phénomène de ce début de XXIe siècle, la mobilité envahit tous les domaines des télécommunications. Que ce soit en milieux professionnels ou privés la connectivité des équipements et leur communication feront vraisemblablement l'objet de développements et d'applications que l'on ne peut encore imaginer.

Preview from Notesale.co.uk
Page 573 of 837

© Dunod – La photocopie non autorisée est un délit

Dans un réseau voix/données deux modes d'établissement des communications sont envisageables. Le premier, le plus simple consiste à transporter la signalisation de manière transparente. Les informations de signalisation ne sont alors pas interprétées par les passerelles voix/données et sont acheminées comme de simples données. Le routage des communications est alors réalisé par les PABX dit PABX de transit. Cette opération conduit à une décompression et à une recompression de la voix. Indépendamment des délais introduits, ce mode d'établissement des communications (figure 16.34) par les opérations de compression et de décompression altère fortement la qualité de la voix et limite le nombre de bonds dans le réseau.



Preview from Notesale.co.uk
Page 600 of 837

Figure 16.34 Communication entre les PABX A et B.

Dans le deuxième mode, dit non transparent, l'acheminement de la communication est réalisé par les passerelles voix/données qui interprètent la signalisation et assurent alors le routage de la communication. Le signal de voix n'a pas à être décompressé et recompressé. L'élongation du réseau n'est alors limitée que par les temps de transfert et de traitement.

➤ Limitation et correction de la gigue

Le temps total de transfert ou temps de bouche à oreille intervient dans l'interactivité de la communication téléphonique, alors que la variation de ce temps ou gigue est un processus réducteur de la qualité auditive de la communication. La gigue dans un réseau voix/données a deux origines. La première est liée aux délais variables de traitements des données par chaque élément du réseau, elle dépend de la charge de celui-ci et du dimensionnement du réseau (files d'attente). La seconde est liée directement à la nature des flux. Compte tenu de la spécificité des différents flux, dans les équipements voix/données les flux voix et données sont séparés et mis, en attente de traitement, dans des files d'attente différentes. Le traitement de la voix bénéficie d'une priorité absolue, tant qu'un paquet voix est présent, la file d'attente données est bloquée. Ce n'est qu'en l'absence de voix, ou entre 2 paquets voix que les paquets données sont traités et émis. La figure 16.35 illustre ce mécanisme. Les paquets de voix sont émis avec une période de récurrence constante (flux isochrone), cependant l'insertion d'un paquet

de données engendre un retard dans l'émission du paquet voix suivant. Ce retard dépend de l'instant d'arrivée du paquet voix et de sa taille.

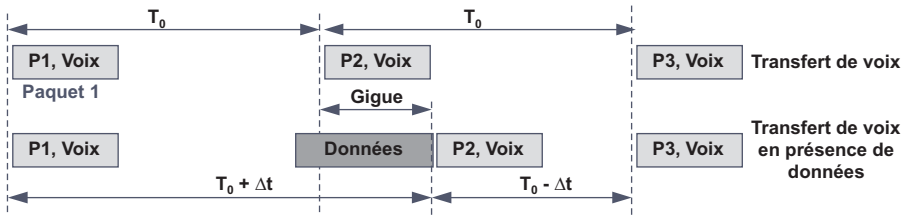


Figure 16.35 Introduction d'une gigue par l'émission d'un paquet voix.

Pour limiter la gigue, les paquets de données devront être aussi petits que possible (fragmentation des paquets de données en présence de paquets voix). Chaque nœud intermédiaire franchi introduit, en présence de données, une variation de délai de transit. La gigue totale résulte de la somme des variations de délai introduits par chacun des nœuds. En sortie du réseau, la passerelle voix/données doit insérer un buffer « élastique » pour corriger cette gigue (figure 16.36). Si le buffer de gigue résout le problème de variation des délais, il allonge le temps de transfert de bout en bout.

Preview from Notesale.co.uk
Page 601 of 837

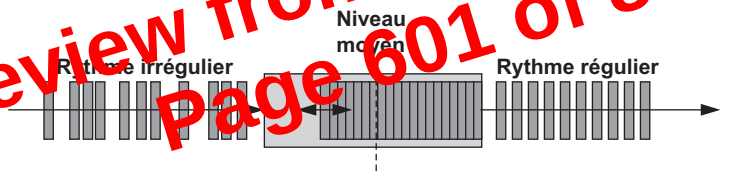


Figure 16.36 Principe de la correction de gigue par buffer « élastique ».

➤ Traitement des télécopies

La voix, même dégradée en qualité, est reconnaissable, il n'en est pas de même des données de télécopie. La solution généralement adoptée consiste à reconnaître les modulations, détecter la porteuse (exemple pour le V.29 porteuse à 2 100 Hz), la démoduler et transmettre les données numériques issues du Fax comme une donnée ordinaire. Le système récepteur opérera à l'inverse en remodulant avant de remettre le signal au PABX destinataire.

➤ Traitement de l'écho

Le poste de l'usager est raccordé par deux fils (boucle locale), la liaison distante comporte généralement quatre fils (paire émission et paire réception). Un transformateur différentiel assure le passage de deux à quatre fils. Si l'adaptation d'impédance est mal réalisée, une partie de l'énergie est réfléchie : c'est l'écho. Les différents types d'écho sont représentés figure 16.37.

L'écho local est peu gênant. À partir d'un certain délai de transmission, fonction de la distance séparant les deux PABX, l'écho distant peut devenir gênant. Supérieur à 45 ms, il constitue un véritable trouble de la conversation[9].

9. L'IUT limite à 24 ms le temps de propagation dans un réseau. Au-delà, l'emploi d'annulateur d'écho est obligatoire.

© Dunod – La photocopie non autorisée est un délit

detection) détecte les silences, la voix est ensuite compressée. Enfin, l'ensemble des informations est mis en paquets (paquets de voix ou paquets de silence). Les paquets de silence ne transportent aucune donnée, ils ne sont utilisés que pour signaler une absence de paquets voix, et non une perte, et permettre au destinataire de générer un bruit aléatoire de fond.

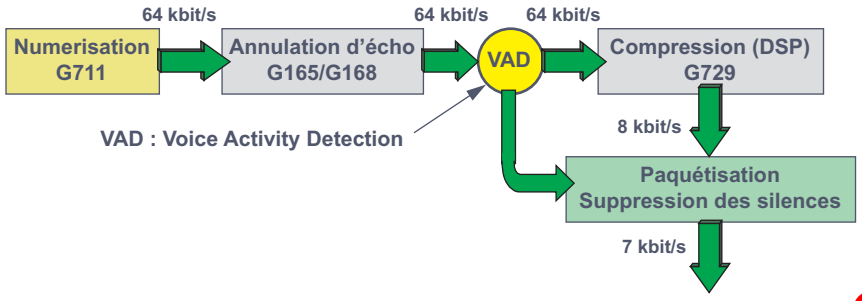


Figure 16.39 Exemple de système de traitement des silences.

Preview from Notesale.co.uk
Page 603 of 837

Dans l'exemple de la figure 16.39, le débit minimal d'environ 7 kbit/s correspond au débit de ligne après les diverses encapsulations du signal. Lors du dimensionnement d'un système voix/données, il ne faut pas tenir compte de cette récupération de bande pour définir les canaux voix, ils doivent l'être au maximum de la bande requise, soit dans notre exemple 17,8 kbit/s (encapsulation RTP/UDP/IP/PPP, voir section 16.7, voix sur IP).

Modes de relation téléphonique dans les réseaux paquets

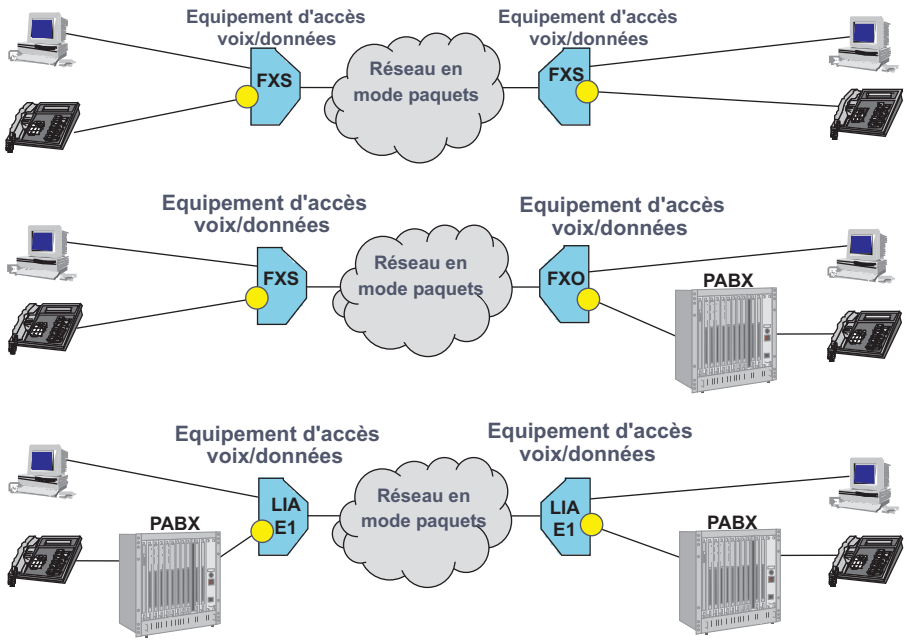


Figure 16.40 Mode de mise en relation à travers un réseau en mode paquets.

© Dunod – La photocopie non autorisée est un délit

– **RTP** (*Real Time Protocol*, RFC 1889 et RFC 1890) qui assure l'horodatage et le contrôle de séquencement des paquets ;
– **RSVP** (*Resource reSerVation Protocol* de l'IETF, Q.397 de l'UIT) qui autorise, pour les flux multimédias, une réservation de ressources réseau de bout en bout. Ce protocole permet la cohabitation de flux multimédia et de flux sporadiques non prioritaires ;
– **MPPP** (*Multilink PPP*, extension de la RFC 1717) qui assure la segmentation des paquets de données longs (*jumbogram*) en petits paquets et autorise le multiplexage de ces paquets avec des paquets temps réel (*Multilink fragmentation and interleaving*).

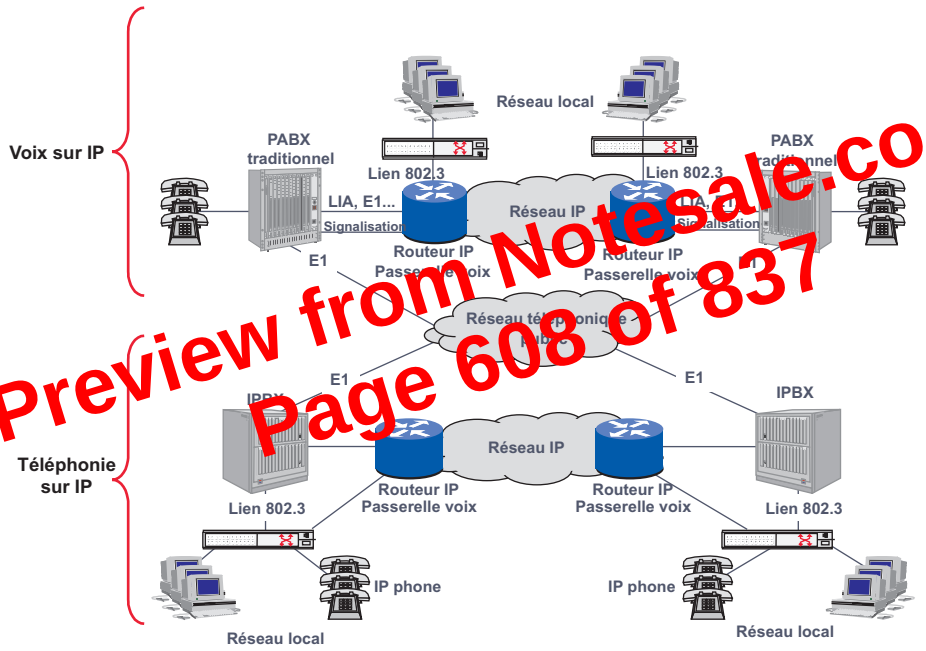


Figure 16.46 Voix sur IP.

L'ensemble s'intégrant dans un modèle architectural décrit par l'UIT, le modèle H.323. Ce modèle permet l'établissement de communication entre terminaux IP/IP (IP phone) et des terminaux IP/Traditionnel. H.323 détermine les protocoles de signalisation interne au réseau et assure la conversion de signalisation vers les réseaux publics.

16.7.2 TCP/IP et le temps réel

Pour des raisons d'efficacité le protocole **UDP** (*User Datagram Protocol*) s'impose pour le transfert des flux multimédia :

– pas d'ouverture, ni de fermeture de session ;
– pas d'acquittement, ni de reprise sur erreur ;
– pas de contrôle de flux et de congestion ;
– faible temps de latence.

Preview from Notesale.co.uk
Page 608 of 837

Deux protocoles complémentaires ont été adjoints à UDP, le premier **RTP** (*Real Time Protocol*) a essentiellement pour objet de fournir les informations nécessaires à la correction de gigue. Le second, intégré dans RTP, **RTCP** (*Real Time Control Protocol*) fournit périodiquement des informations sur la qualité du réseau. La figure 16.47 illustre les différents flux protocolaires.

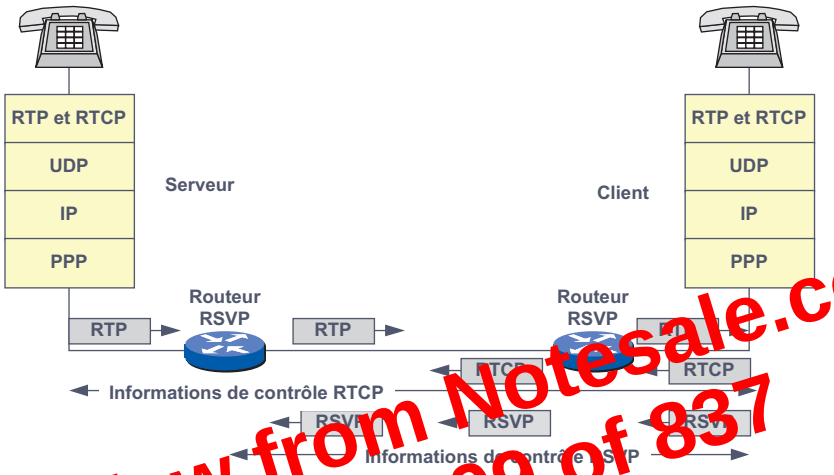


Figure 16.47 Le contrôle de session par RTP et RTCP.

Preview from Notesale.co.uk
Page 609 of 837

Dans une session multimédia, chaque flux est transporté par une session RTP distincte. De même, à chaque session RTP est associé un flux de contrôle RTCP. Une session RTP est une association de plusieurs communicants, au moins 2, une session est identifiée par le couple port/adresse. L'en-tête RTC contient les informations d'identification, de séquencement, de type de charge utile et d'horodatage (figure 16.48).

Ver	P	X	CC	M	PT (type de charge)	Numéro de séquence
RTP Time Stamp						
Identifiant de la source de synchronisation (SSRC)						
Identifiant des flux (CSRC)						

Figure 16.48 En-tête RTP.

Sur 2 bits, le champ Ver indique la version de RTP (actuellement 2). Le bit P indique s'il y a (1) ou non (0) des octets de bourrage. Le nombre d'octets de bourrage est précisé dans la charge utile. Le X précise s'il y a des extensions d'en-tête. Le bit M (*Marker*) définit un profil RTP, par exemple, si la récupération des silences est activée, dans chaque premier paquet d'un échange ce bit est à 1. Le champ PT (*Payload Type*) indique le type de charge utile et le format de codage. Le numéro de séquence est incrémenté de 1 à chaque paquet, le numéro de séquence initial est aléatoire. Le champ *Time Stamp* indique sur 32 bits l'instant d'échantillonnage du premier octet du paquet RTP. Cette information permet la récupération de la gigue, sa valeur initiale est aléatoire. Le champ SSRC (*Synchronisation Source Report Count*), unique au sein d'une session RTP, identifie la source sur laquelle les paquets de données sont synchronisés. Le champ CSRC (*Contributing Source*) est utilisé quand plusieurs sources fournissent des

© Dunod – La photocopie non autorisée est un délit

informations et que le paquet contient des informations reconstituées à partir de ces différentes sources.

L'encapsulation IP/UDP/RTP ajoute 20 octets au paquet de données, sans compter l'en-tête de niveau 2. Le tableau de la figure 16.49 indique la bande passante, arrondie au kbit/s le plus proche, requise en fonction du type de protocole de niveau 2.

Algorithme	Débit Codec kbit/s	Charge utile/ Nb paquets seconde	Niveau 3	Niveau 2			
			IP/UDP/RTP	Ethernet	PPP	Frame Relay	ATM
Octets overhead			40	26	6	6	5
G.711	64	160/50	80	90	82	82	88
G.711	64	240/33	74	81	76	76	84
G.723.1	6,3	24/33	17	24	18	18	28
G.729	8	20/50	24	34	26	26	42

Figure 16.49 Bande utile après encapsulation

Preview from Notesale.co.uk
Page 610 of 837

Le rapport charge utile/données de service est tel qu'un mécanisme de compression d'en-tête (**CRTP**, *Compressed Real Time Transport Protocol*, RFC 1144), basé sur la redondance des informations d'en-tête, permet de réduire d'un facteur d'environ 10 (en-tête de 2 à 4 octets) la taille des données de service (figure 16.50). Par exemple, la compression CRPT associée à la récupération des silences réduit le débit du G.723.1 de 18 à 6 kbit/s. La compression CRTP compresse les données lien par lien, ce qui signifie d'une part que tous les équipements intermédiaires doivent supporter la compression CRTP et d'autre part que ce traitement induit un délai supplémentaire d'autant plus important que le nombre de bonds l'est.

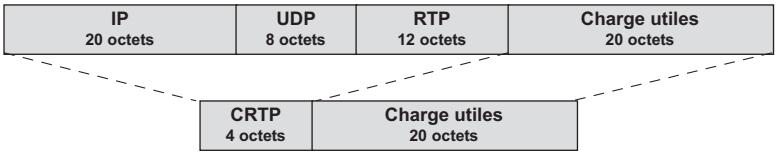


Figure 16.50 Compression d'en-tête CRTP.

Pour limiter la gigue, le protocole **MLPPP** (*MultiLink PPP*, RFC 1144) fragmente les paquets longs. Les petits paquets, notamment ceux de voix, sont encapsulés normalement et entrelacés (multiplexés) avec le flux fragmenté (figure 16.51).

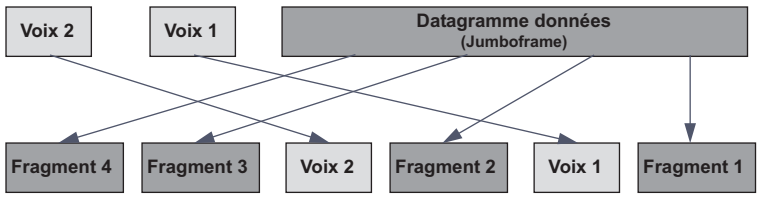


Figure 16.51 Entrelacement des paquets voix et données (MLPPP).

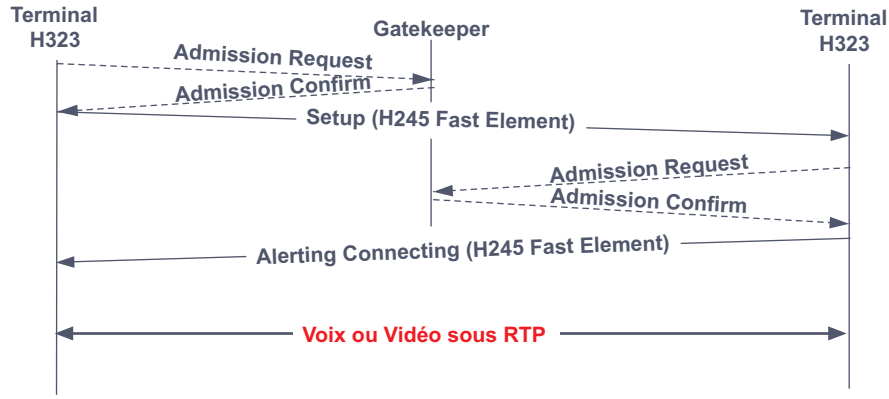


Figure 16.57 Établissement d'un appel sous H.323v2.

Preview from Notesale.co.uk
Page 614 of 837

16.7.4 Le protocole SIP de l'IETF (RFC 2543)

Actuellement la plupart des solutions développées utilisent la signalisation H.323 (v1, v2 ou v3) d'origine UIT-T. Développé au sein du groupe de travail **MMUSIC** (*Multiparty Multimedia SessIon Control*) de l'IETF, le protocole **SIP** (*Session Initiation Protocol*) beaucoup simple que H.323 pourrait, à terme, remplacer H.323. Les messages SIP sont au format texte, ce qui confère au protocole une grande évolutivité. La figure 16.58 illustre l'architecture SIP.

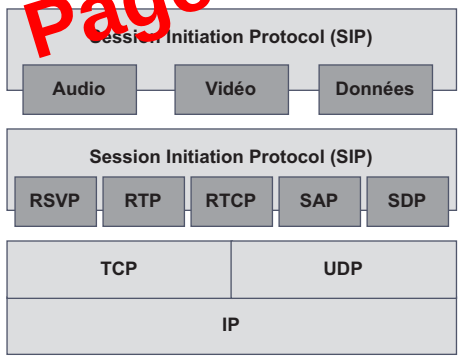


Figure 16.58 Architecture protocolaire SIP.

À l'instar d'H.323, SIP s'appuie sur les protocoles temps réel (RTP et RTCP), il peut éventuellement utiliser RSVP pour obtenir une certaine qualité de service sur le réseau. Le protocole **SAP** *(Session Announcement Protocol*) informe de l'ouverture d'une session multimédia en mode multicast ou non et le protocole **SDP** (*Session Description Protocol*) fournit la description des sessions multimédia.

Basé sur le modèle client serveur, SIP distingue 2 types d'agent : les clients et les serveurs. Les clients ou **UAC** (*User Agent Client*) sont les équipements à l'origine des appels SIP (téléphone IP) ou des passerelles voix. Les passerelles voix SIP ont les mêmes fonctionnalités que les passerelles H323.

Les agents serveurs (**UAS**, *User Agent Server*) sont des équipements classiques (Serveur NT...) qui regroupent les services offerts par SIP. Ce sont :

16.7.5 Le protocole MGCP

Un autre protocole entre en compétition **MGCP** (*Media Gateway Control Protocol*) encore plus simple, il centralise « l'intelligence » et peut donc être intégré à des terminaux peu intelligents (clients légers).

MGCP définit plusieurs entités. La passerelle de signalisation (**SG**, *Signalling Gateway*) assure la mise en relation de la signalisation du réseau téléphonique traditionnel, généralement SS7, avec la signalisation utilisée dans le réseau en mode paquets. La passerelle média (**MG**, *Media Gateway*) réalise la paquetisation des signaux voix. Enfin, le contrôleur de passerelle média (**MGC**, *Media Gateway Controller*), cœur du système, pilote les différentes passerelles. D'autres solutions proches ont été proposées. Ces différentes propositions ont conduit à l'élaboration d'un standard commun MEGACO (RFC 3015) pour l'IETF et H.248 pour l'UIT.

16.8 CONCLUSION

La convergence voix/données a donné naissance à une nouvelle génération de réseau dans laquelle la notion de qualité de service devient prépondérante. L'évolution de la téléphonie pour son intégration au réseau donnée est en plein développement. Si la téléphonie sur IP a fait naître l'espoir d'interopérabilité des systèmes, le développement de signalisations propriétaire sur IP, l'opposition H.323 et SIP font reculer cet espoir.

Cependant, le choix se fera autour de H.323 ou de SIP. H.323 bénéficie de son antériorité et d'un fonctionnement assuré. SIP a l'avantage de la simplicité et de l'évolutivité mais il doit encore faire ses preuves.

Preview from Notesale.co.uk
Page 617 of 837

© Dunod – La photocopie non autorisée est un délit

vegardes régulières, seule solution capable de protéger les données d'un effacement accidentel (erreur d'un utilisateur). Les sauvegardes peuvent être réalisées sur une autre machine du réseau dédiée à cet usage, sur des mémoires de masses distantes ou sur des bandes de sauvegardes conservées dans un autre local.

La mise en duplex d'équipement comme les serveurs représentent le niveau le plus élevé. Chaque serveur (figure 17.3) constitue un sous-système géré par le système d'exploitation. L'utilisateur est connecté à l'un des serveurs. Toutes les opérations effectuées sur l'un sont recopiées, via un canal à haut débit, sur l'autre. En cas de défaillance d'un serveur, la connexion de l'utilisateur est basculée sur l'autre. La panne est totalement transparente.

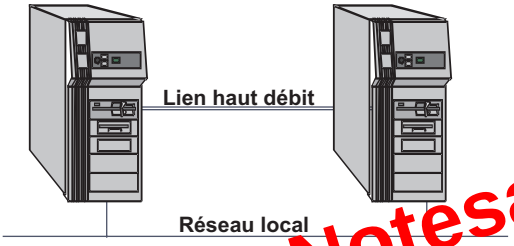


Figure 17.3 Duplexing de serveurs.

Preview from Notesale.co.uk
Page 623 of 837

La sécurité des moyens de transport est généralement réalisée par la redondance des liens obtenue par le maillage du réseau ou par le doublement des raccordements au réseau de l'opérateur. Dans ce dernier cas, il faut veiller à ce que le cheminement des liens, leur point de raccordement au réseau de l'opérateur et les pénétrations dans les locaux informatiques soient distincts. En fonctionnement normal le réseau peut utiliser les deux liens (équilibrage de charge), en cas de rupture d'un lien, le trafic sera intégralement écoulé sur le lien restant (fonctionnement dégradé). Compte tenu des coûts, de nombreuses entreprises préfèrent utiliser une connexion de secours établie à la demande. Dans ce cas, c'est le réseau téléphonique qui est utilisé comme lien de secours. Une communication est établie en agrégeant, selon le besoin, plusieurs canaux B (figure 17.4).

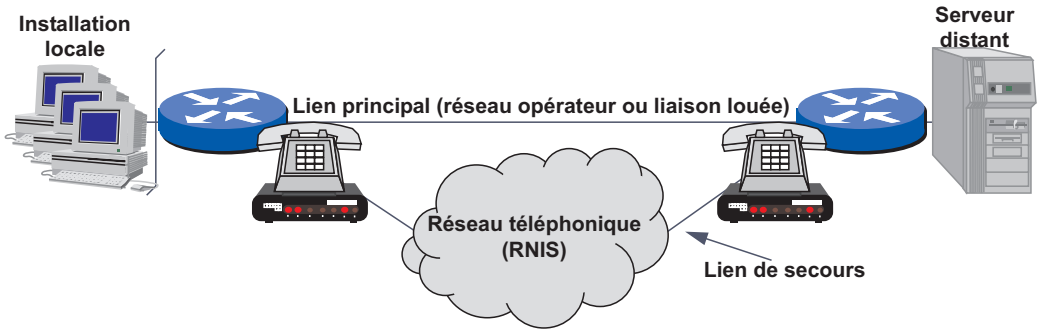


Figure 17.4 Duplication de la ligne de transmission.

17.2.3 La sûreté environnementale

L'indisponibilité des équipements peut résulter de leur défaillance interne mais aussi d'événements d'origine externe. Le réseau électrique est la principale source de perturbation (coupures, microcoupures, parasites, foudre...). Des équipements spécifiques peuvent prendre le

© Dunod – La photocopie non autorisée est un délit

Figure 17.14 Principe du PgP.

➤ Protocole d'échange de clés Diffie-Hellman

La cryptographie à clé publique nécessite une puissance de calcul importante. Le DES est entre 100 fois (implémentation logicielle) et 1 000 fois (implémentation *hardware*) plus rapide que le RSA. Le protocole d'échange de clés de Diffie-Hellman permet de construire une clé secrète (clef de session) sans que celle-ci circule sur le réseau. L'initiateur de l'échange transmet à son correspondant deux nombres grands et premiers (g, n). Les correspondants déterminent une clé privée, tenue secrète. Chacun, à partir de g, n et de sa clé secrète (nombres aléatoires A et B) génère une clé publique et la communique à l'autre. Puis, à partir de sa clé privée, de sa clé publique et de la clé publique de son correspondant, calcule la clé de session (figure 17.15).

Preview from Notesale.co.uk
Page 631 of 837

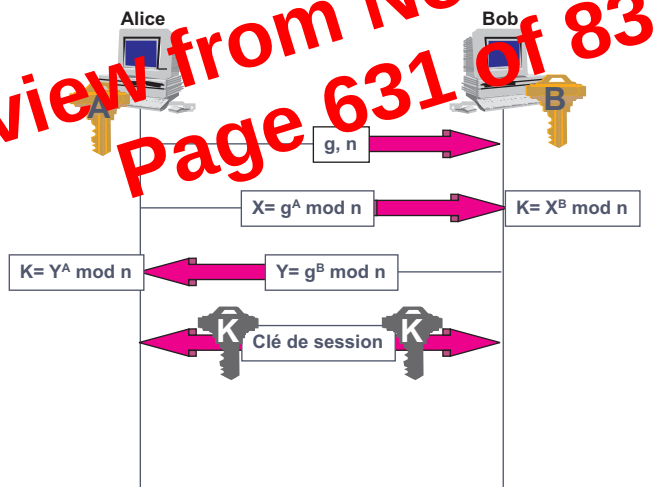


Figure 17.15 Principe de l'échange de Diffie-Hellman.

Le protocole de Diffie-Hellman permet de sécuriser l'échange de clé, cette technique est utilisée dans IPSec (*IP Secure*)

➤ Contrôle d'intégrité du message

Pour vérifier l'intégrité d'un message, on utilise une technique similaire à celle du CRC (*Cyclic Redundancy Check*). Une fonction dite de hachage (**hash**) est appliquée au contenu du message. Le résultat obtenu ou **digest** (résumé, sceau...) est joint au message à transmettre, il est recalculé par le destinataire. Si le résultat du calcul local est identique au digest reçu, le message n'a pas été altéré (figure 17.16).

La fonction de hachage doit garantir qu'il est impossible à partir du digest de retrouver le message initial (non retour arrière ou *one-way hash*) et qu'il doit être quasi impossible que

© Dunod – La photocopie non autorisée est un délit

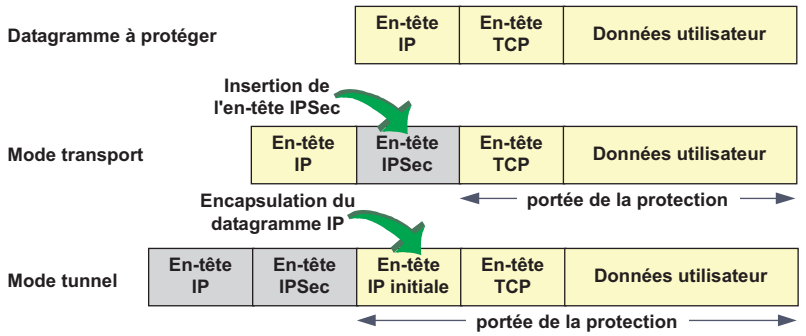


Figure 17.23 IPSec, mode transport et mode tunnel.

L'extension d'authentification (AH)

L'en-tête d'authentification (**AH**, *Authentification Header*) certifie au destinataire du paquet IP l'intégrité des données et l'identité de l'origine. Compte tenu de la modification par les éléments du réseau de certaines données d'en-tête IP (TTL, *Time to Live*...), le *digest* ne porte que sur les données non modifiées par le réseau. Lors du calcul, ces champs sont mis à zéro. L'en-tête AH comporte l'identificateur d'association de sécurité et, pour éviter le rejeu, un numéro de séquence unique. Les données de l'en-tête AH sont incluses dans le calcul.

Preview from Notesale.co.uk
Page 637 of 837

L'extension de confidentialité-authentification (ESP)

L'en-tête de confidentialité (**ESP**, *Encapsulating Sécurity Payload header*) garantit la confidentialité des datagrammes, l'intégrité des données et l'identité de la source, il se décompose en trois champs (figure 17.24) :

– à l'instar de l'en-tête AH, le sous-en-tête ESP comprend les données relatives à l'identification de l'association de sécurité et un numéro de séquence « anti-rejeu »,
– un *trailer* (en-queue) ESP précise la portée du chiffrement (mode transport ou mode tunnel),
– un *trailer* d'authentification ESP comporte les données d'authentification.

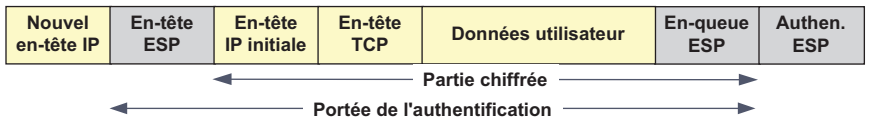


Figure 17.24 L'en-tête ESP en mode tunnel.

17.3.3 La protection du réseau

Les menaces

Les menaces contre les systèmes visent essentiellement à les rendre inaccessibles ou à en altérer profondément les performances. Par exemple, le protocole **ICMP** (*Internet Control Messages Protocol*) constitue l'une des failles (vulnérabilités) des environnements TCP/IP. En effet, il suffit, par exemple, d'adresser à un routeur d'interconnexion des paquets ICMP de

© Dunod – La photocopie non autorisée est un délit

Action	Protocole	Source	Destination	Commentaire
Accept	*	194.23.10.0/24	194.23.11.0/24	Trafic sortant vers établissement de Paris
Accept	*	194.23.11.0/24	194.23.10.0/24	Trafic entrant de l'établissement de Paris
Rejet	*	*	*	

Figure 17.26 Exemple de règles de filtrage.

trafics interdits. Dans notre exemple simple, l'écriture de la ligne 3 en tête de liste interdirait tout trafic ! Lorsque les filtres sont décrits très finement, il n'est pas rare que certaines lignes soient en contradiction.

➤ La translation d'adresses (RFC 1631)

La translation d'adresse[5] est un moyen de contourner la pénurie d'adresses Internet, mais aussi de masquer le plan d'adressage de l'entreprise (*IP masquerade*).

La traduction statique fait correspondre à une adresse interne du réseau une adresse externe, généralement une adresse publique. Ce mode de translation résout à la fois le problème de la pénurie d'adresse, du masquage du plan d'adressage local (mascarade) et sécurise le réseau en n'autorisant que certaines stations à accéder à l'Internet (figure 17.27).

Preview from Notesale.co.uk
Page 639 of 837

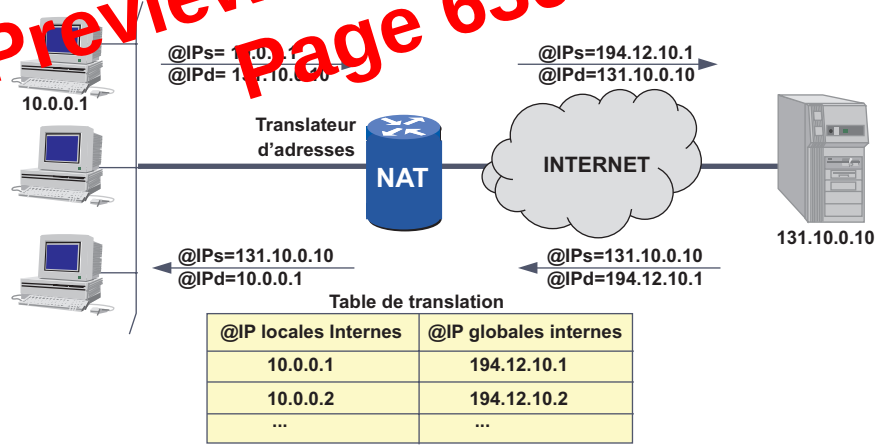


Figure 17.27 Traduction statique d'adresses.

La translation statique limite le nombre de machines ayant accès à l'extérieur au nombre d'adresses publiques attribuées. La traduction dynamique s'affranchit de cette limite. Lorsqu'une machine veut atteindre une machine extérieure, le NAT associe à l'adresse locale interne une adresse globale interne, ou adresse externe, choisie parmi un pool d'adresses mises à sa disposition. Le NAT introduit un protocole à état, indépendamment du fait qu'en cas de défaillance du NAT les relations sont perdues, l'état doit être détruit en fin de communication et l'adresse attribuée rendue disponible pour une autre connexion vers l'extérieur. Un tempori-

5. La notion de translation d'adresses a été introduite à la section 10.2.2.

© Dunod – La photocopie non autorisée est un délit

Lorsque le nombre de messages à traiter augmente, T_q devient prépondérant par rapport aux autres éléments, ces derniers pourront alors être négligés. Le problème consiste donc à calculer le temps de queue en fonction des caractéristiques du système (nombre d'items traités par unité de temps ou μ), de la longueur du message (L) et du débit de la ligne du système (D). Il est possible aussi, à partir de ces éléments, de déterminer les caractéristiques du système pour répondre aux contraintes temporelles des applications.

Notions de files d'attente

➤ Relation de base, formule de Little

Dans un système à file d'attente en équilibre (figure 19.20), c'est-à-dire que le nombre moyen d'entrées (λ) est égal au nombre moyen de sorties par unité de temps, le nombre moyen d'items (clients) dans le système N est donné par la relation :

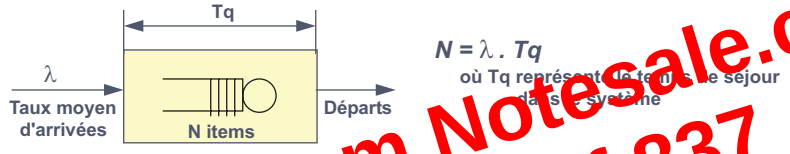


Figure 19.19 Formule de Little

Preview from Notesale.co.uk
Page 674 of 837

Si la condition d'équilibre est respectée, la relation de Little s'applique à tous les types de files d'attente.

➤ Les files d'attente M/M/1/∞

Le modèle M/M/1/∞ est le modèle plus simple retenu pour la modélisation des réseaux. Selon la notation de **Kendal** cette file est caractérisée par :

- **M**, processus Markovien en entrée (distribution exponentielle des arrivées),
- **M**, processus Markovien en sortie,
- **1**, il n'y a qu'un seul processeur (système mono-serveur),
- ∞, la file d'attente a une capacité infinie, aucun item entrant n'est perdu.

Dans ce type de processus, on considère les arrivées indépendantes les unes des autres, ce qui est généralement le cas des processus informatiques où les systèmes d'extrémité s'échangent des messages indépendamment les uns des autres.

Dans le système M/M/1/∞ (figure 19.11), on désigne par λ le taux d'arrivée des items dans la file, par *ta* le temps de séjour dans la file d'attente, par *ts* le temps de traitement par le système (son inverse 1/ts représente le nombre d'items traités par unité de temps ou taux de service et est désigné par μ) et *tq* le temps qui s'écoule entre l'entrée d'un item dans le système et sa sortie (temps de séjour). Le nombre d'items en attente de traitement *Na* et le nombre d'items en cours de traitement *Ns* sont une fonction directe du temps d'attente ou de traitement et du taux d'arrivée :

$$Na = \lambda ta \quad \text{et} \quad Ns = \lambda ts$$

Le nombre d'items N dans le système peut s'écrire (décomposition de la formule de Little) :

$$N = Na + Ns = \lambda(ta + ts) \quad \text{(relation 1)}$$

– compte tenu des caractéristiques des applications données par le tableau de la figure 19.18, déterminer le temps de réponse de l'application. Les différents éléments à prendre en compte pour ce calcul sont :
  – temps de traitement d'une transaction par le serveur central 0,2 s ;
  – les terminaux sont connectés à un concentrateur local par une ligne à 9 600 bit/s ;
  – le magasin est relié au site central par une liaison louée à 64 000 bit/s
  – on admettra que les bits de transparence et les données de service (ACK...) accroissent la taille des unités de 20 % ;
  – les grilles d'écran des terminaux points de vente sont organisées de telle manière que l'écran de consultation permette de saisir la vente du produit consulté ou la référence d'un autre produit à consulter (un seul échange pour la consultation suivie d'une vente) ;
  – les saisies s'effectuent sur une grille vierge ou en surcharge sur une grille de réponse. Seuls, les caractères saisis sont transmis ;
  – le temps de saisie n'est pas décompté dans le temps de réponse ;
  – le temps d'affichage des écrans sera considéré comme négligeable.

Terminal	Point de vente	Caisse	Point d'enlèvement	Comptable
Saisie	20c	100c	20c	200c
Réponse ou grille de saisie vierge	800c	800c	600c	800c

Figure 19.18 Caractéristiques des transactions.

Preview from Notesale.co.uk
Page 680 of 837

Exercice 19.3 Réalisation d'un réseau privé d'entreprise

Une entreprise désire réaliser un réseau privé à partir de liaisons louées (LL) à 64 kbit/s pour remplacer ses abonnements à un réseau public de transport de données dont le débit d'abonnement est actuellement de 19 200 bit/s. Le siège est à Paris. Les différentes implantations en province sont : Amiens, Lille, Metz, Nancy, Strasbourg, Rennes, Nantes, La Rochelle, Bordeaux, Toulouse, Clermont Ferrand, Dijon, Lyon, Marseille et Nice. On vous demande :

– De déterminer le réseau primaire (sans tenir compte d'aucune contrainte de débit), vous utiliserez l'algorithme de Kruskal ;
– D'intégrer une contrainte de débit, en garantissant un débit minimal de 19 200 bit/s à chaque site. C'est-à-dire qu'un nœud de concentration ne doit pas concentrer plus de deux sites. De plus, on souhaite que le nombre de bonds soit au maximum de deux pour chaque site ;
– De comparer les coûts des 2 solutions (l'unité sera le km).

Les distances intersites peuvent être obtenues sur le 36 14 code RLS.

Exercice 19.4 Caractéristique mémoire d'un routeur

Un réseau local est interconnecté à un autre réseau via un routeur par une ligne à 64 kbit/s. Plusieurs stations sont connectées sur le réseau local. L'analyse de trafic en arrivée montre que :

– 2 stations ont un trafic vers l'extérieur de 4 paquets/s ;
– 2 stations ont un trafic vers l'extérieur de 2 paquets/s ;

CHAPITRE 7

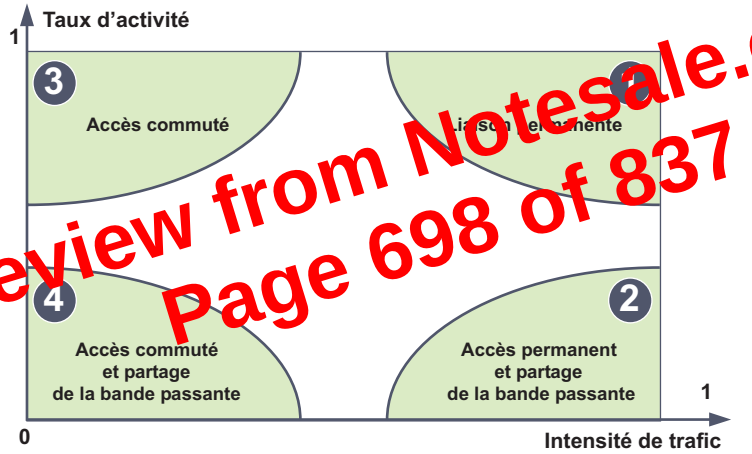
7.1 Intensité de trafic et taux d'activité

Lors de l'étude d'un système d'interconnexion de systèmes informatiques, deux critères essentiels, dépendant du type d'application, sont à prendre en compte :

– l'intensité de traffic qui caractérise la durée de la ou des sessions ;

– le taux d'activité, qui exprime la proportion de temps d'utilisation pendant le temps de connexion.

L'intensité de trafic (E) et le taux d'activité (θ) varient de 0 à 1. On peut représenter la relation entre ces valeurs par un rectangle et déterminer 4 aires spécifiques (figure 20.17).



Preview from Notesale.co.uk
Page 698 of 837

Figure 20.17 Les 4 aires définies par E et θ.

– L'aire 1 correspond à une occupation de la ligne importante et une utilisation conséquente, le partage des ressources n'est pas envisageable.

– L'aire 2 correspond aussi à une occupation de la ligne importante, mais à une utilisation faible. La bande passante de la ligne peut donc être partagée, le multiplexage est envisageable.

– L'aire 3 représente un secteur ou la ligne est peu occupée, mais le trafic est important. Le partage de la bande n'est pas envisageable, mais le partage dans le temps de son utilisation est possible. La ligne peut être commutée d'un utilisateur à un autre (réseaux à commutation de circuits).

– Dans la dernière aire, la ligne est peu occupée et faiblement utilisée, on peut imaginer un système de concentration de trafic auquel on accède via un réseau commuté, ce système servant d'interface avec un autre moyen où la bande pourra statiquement être partagée par plusieurs utilisateurs.

Le tableau de la figure 20.18 résume ces commentaires.

c) Temps en Commutation de Paquets

Avec N = 5, H = 28, le temps de transfert est :

– Pour CU 37 : $[(1\,480 + 40 \times 28)(8/64\,000)](1 + 5/40) = 0{,}325 \times 1{,}125 = 0{,}365$ s ;

– Pour CU 148 : $[(1\,480 + 10 \times 28)(8/64\,000)](1 + 5/10) = 0{,}22 \times 1{,}5 = 0{,}33$ s ;

– Pour CU de 296 : $[(1\,480 + 5 \times 28)(8/64\,000)](1 + 5/5) = 0{,}2025 \times 2 = 0{,}405$ s.

De manière générale, plus le paquet est de petite taille meilleur est le temps de transfert. Ce principe a déjà été vu lors de l'étude des multiplexeurs. Cependant en commutation de paquets (multiplexage par étiquette), on ajoute à chaque unité de données un en-tête, de ce fait il existe un rapport harmonieux entre la taille des unités de données et la taille de l'en-tête.

CHAPITRE 9

9.1 Fonctions et couches OSI

a) Le niveau physique réceptionne un flux de bits et le formate en trame pour remise à la couche liaison de données.

b) Le chemin à travers le réseau est déterminé par la couche réseau.

c) La synchronisation des échanges de données est gérée par la couche session.

Preview from Notesale.co.uk
Page 704 of 837

9.2 Adresse SAP d'une émission IAM

Le point d'accès à une entité réseau est la caractéristique qui identifie, sans confusion possible (adresse), un service. Une station d'émission d'un réseau de radio de diffusion est identifiée par sa fréquence d'émission. Le SAP d'une station est sa fréquence d'émission.

Il ne faut pas confondre la NSAP qui identifie le point d'accès à un service réseau avec la SNAP qui identifie le point d'accès au sous-réseau physique de transport, par exemple une adresse X.121.

9.3 Encapsulation

Dans le modèle OSI, ce sont les paquets qui encapsulent les TPDU (figure 20.24). Quand une TPDU arrive au niveau de la couche réseau, la totalité de l'en-tête et des données constituent le champ de données du paquet (N_SDU).

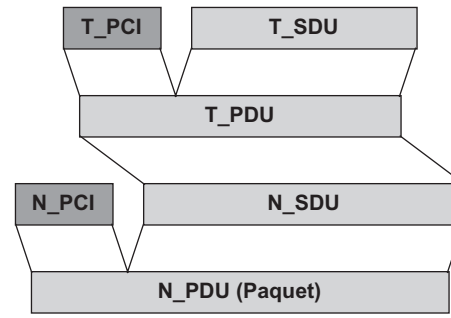


Figure 20.24 Encapuslation des messages de transport.

9.6 Contrôle de flux et transferts isochrones

Le mécanisme de contrôle de flux consiste à ralentir, voire arrêter l'émission, la conséquence directe est un asynchronisme dans la réception des données. Cet asynchronisme est incompatible avec une transmission de données dite isochrone comme le nécessite la voix et l'image animée.

9.7 Contrôle de flux et classe de transport 0

Les différentes classes de transport ont été définies pour pallier les insuffisances des sous-réseaux de transport utilisés. La couche transport rend transparent, aux services de session, le sous-réseau physique utilisé. Dans ces conditions, compte tenu que la classe 0 est faite pour s'appuyer sur un service réseau « parfait » elle implémente un minimum de mécanismes. Les TPDU ne comportent pas de champ numéro de TPDU, un service de fenêtrage n'est donc pas réalisable. Le contrôle de flux peut, éventuellement, être effectué par les couches inférieures.

Preview from Notesale.co.uk
Page 706 of 837

9.8 Référencement d'une connexion de transport

TP4 peut définir des connexions multiples entre toutes les paires de T_SAP. Dans ce cas, les connexions sont identifiées par les champs source référence et destination référence dans les T_PDU et non par l'adresse T_SAP. (Remarquons que dans le TPDU_CR le champ « référence destination » est toujours à zéro.)

9.9 Connexion de transport et connexion de session

Les principales similitudes sont :

– Service orienté connexion.
– Établissement et libération des connexions, avant et après utilisation.
– Primitives de transfert régulier de données.
– Délivrance de données fiables.

Les différences sont :

– La session : libération brutale ou négociée, transport : libération brutale uniquement.
– La connexion de transport n'autorise que des flux de données normales et exprès, la session comporte 4 types de flux de données (voir exercice suivant).
– Les connexions « session » ont un dialogue de gestion, les connexions « transport » un dialogue de transfert.
– Pas de notion de synchronisation, d'activité, ni de jeton dans les connexions transport.
– Une connexion session peut utiliser plusieurs connexions transport.

9.10 Les types de variables d'ASN-1

L'ASN–1 est un langage de description de données. Il définit des types simples ou structurés (comme tous les langages de haut niveau) ; l'ASN–1 est proche, en cela, du langage de programmation PASCAL.

Décodage trame MAC 1

1) En-tête MAC

Champ	Valeur hexa.	Commentaires
Adresse destination	00 A0 24 BD 75 BD	00 A0 24 Identification du fournisseur 3COM BD 75 BD N° séquentiel de fabrication de la carte
Adresse source	08 00 02 05 2D FE	08 00 02 Identification du fournisseur (ici 3 COM-Bridge)
Type de protocole	08 00	IP du DoD

2) En-tête IP

Champ	Valeur Hex.	Commentaires
Identification Version	4 -	Sur 4 bits, IP version 4
Longueur en-tête	- 5	IHL (*Internet Head Length*), sur 4 bits, en multiple de 4 octets la valeur normale est 5 soit 20 octets (plus si option).
Type de service	00	Champ de bits Priorité (Routine) – – – 0 0 0 Délai acheminement (Normal) – – – 0 – – – Débit (Normal) – – – 0 – – – – Fiabilité (Normale) – – 0 – – – – – Réservé 0 0 – – – – – –
Longueur totale	00 60	Exprime la longueur totale du datagramme (données utiles de la couche MAC). Ici, la valeur 60 soit 96 octets est supérieure à 48, il n'y a donc pas eu d'opération de bourrage.
Identification	3C EF	Identifie tous les fragments d'un même datagramme.
Drapeau	00	Sur les trois derniers bits – bit 7, non utilisé – bit 6, DF (*Don't Fragment*), à 0 : fragmentation possible – bit 5, MF (*More Fragment*), à 1 indique qu'un fragment suit. Les autres bits appartiennent au champ suivant.
Offset	00	Sur 13 bits, indique la position du fragment depuis le début.
Durée de vie	1C	*Time to Live*, durée de vie du fragment, initialement exprimé en seconde, représente aujourd'hui le nombre de bonds restants.
Protocole supérieur	06	Identifie TCP
Total de contrôle	A4 FE	
@ IP Source	80 00 64 01	@IP = 128.0.100.1, Adresse de classe B.
@ IP Destination	DO 80 08 29	@IP = 208.128.8.41, Adresse de classe C. En principe, les machines sur un même réseau appartiennent à un même espace d'adressage. Ce n'est pas le cas ici. On peut donc penser que la machine source n'est pas sur le même réseau physique que la station destinataire du message.

Preview from Notesale.co.uk
Page 712 of 837

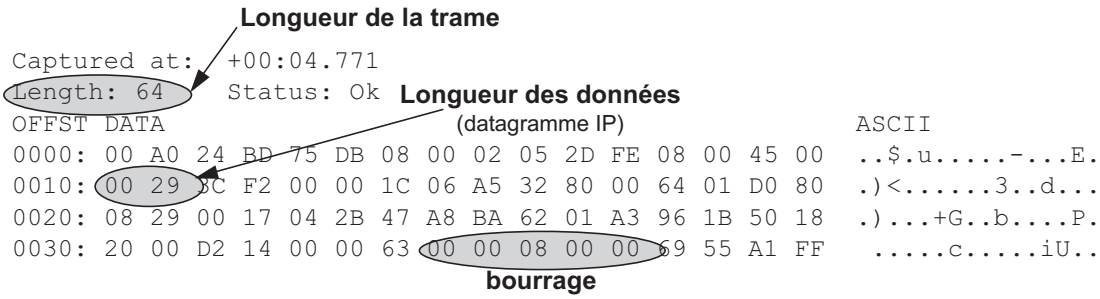


Figure 20.34 Trame MAC numéro 2.

CHAPITRE 11

11.1 SDH/PDH

Les principaux avantages s'expriment en termes de facilités d'exploitation, de fiabilisation des liaisons (autocicatrisation), de débit et de facilité à insérer ou à extraire un débit inférieur d'un lien.

Preview from Notesale.co.uk
Page 715 of 837

11.2 Reconstitution d'un paquet d'appel

Pour reconstituer le paquet d'appel il faut d'abord coder tous les éléments le constituant :

1) Codage de l'adresse

Au format X.121, l'adresse Transpac est codé : Type d'accès, Département, Commutateur de rattachement, Numéro de la liaison. L'accès se faisant sur une LS, le type d'accès identifié par la valeur 1. Avec un chiffre par quartet, l'adresse de l'appelé est

```
1 75 01 0089
```

L'adresse est codée en DCB, premier chiffre dans le quartet de poids fort du premier octet du champ adresse.

2) Codage des facilités

- Facturation à l'appelé : 01, 01 ;
- GFA valeur locale 3 : 03,03 ;
- Taille paquet : $64 = 2^6$, $128 = 2^7$ soit 42,06,07 ;
- Négociation taille fenêtre 2, 7 : 43,02,07 ;

Dans ces conditions, la longueur du champ facilité est 10 soit 0x0A.

Détermination du CV : pour un appel sortant, le NVL affecté à la voie logique est le NVL de plus grande valeur disponible. Ici, il s'agit de la première connexion soit 19 ou, en hexadécimal, 13.

© Dunod – La photocopie non autorisée est un délit

3) Format du paquet d'appel (figure 20.35)

Paquet	Binaire	Hexadécimal
GFI	0001 0000	10
NVL	0001 0011	13
Type paquet	0000 1011	0B
L. appelant / L. Appelé	0000 / 1001	09
Adresse appelé	0001 0111	17
	0101 0000	50
	0001 0000	10
	0000 1000	08
0000	1001 0000	90
Longueur champ facilités	0000 1010	0A
Facturation à l'appelé	0000 0001	01
Oui	0000 0001	01
GFA	0000 0011	03
3	0000 0011	03
Taille paquet	0100 0010	42
Émission	0000 0110	06
Réception	0000 0111	07
Taille fenêtre	0100 0011	43
Émission	0000 0010	02
Réception	0000 0111	07

Preview from Notesale.co.uk
Page 716 of 837

Figure 20.35 Codage d'un paquet d'appel.

11.3 Dialogue X.25

Rappels

La trace de niveau physique représente, codés en hexadécimal, tous les octets circulant sur la liaison. Avant d'entreprendre le décodage de ces valeurs, rappelons la structure générale de la trame LAP-B émise sur le niveau physique (figure 20.36) :

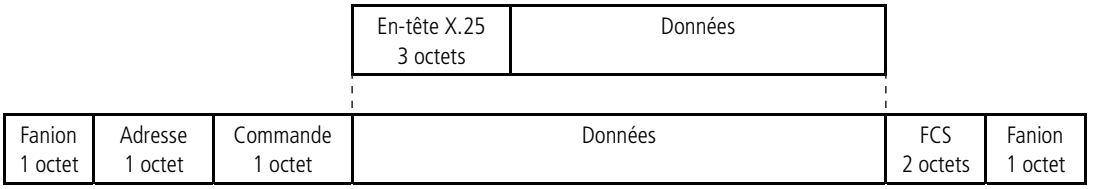


Figure 20.36 Trame LAP-B et paquet X.25

11.4 Définition d'un protocole

a) Valeur optimale de la taille de l'unité de données.

Cette valeur correspond au minimum de la fonction $T(p)$. Il convient donc de rechercher la valeur de p qui annule la dérivée première :

$$Tp = \frac{L + pH}{D}\left(1 + \frac{N}{p}\right) = \frac{L}{D} + \frac{LN}{Dp} + \frac{pH}{D} + \frac{HN}{D}$$

$$T'(p) = -\frac{LN}{D\,p^2} + \frac{H}{D}$$

La valeur qui annule cette fonction est :

$$p = \sqrt{\frac{LN}{H}}$$

soit

$$p = \sqrt{\frac{1\,500 \times 3{,}25}{5}} = 31{,}225 \text{ paquets (seule la solution positive est retenue !).}$$

L'étude des variations de la fonction ou du signe de la dérivée seconde montre qu'il s'agit bien d'un minimum. Ce qui correspond à une longueur de paquets de

$$Lp = \frac{1\,500}{31{,}225} = 48 \text{ octets.}$$

Preview from Notesale.co.uk
Page 720 of 837

b) Contrôle de flux

Pour déterminer l'efficacité de contrôle de flux, il convient de définir l'inertie du système. C'est-à-dire combien de paquets seront envoyés entre le paquet saturant et la réception par la source du message de demande d'arrêt.

Si on tient compte que du temps de transfert sur le réseau, cette valeur correspond au nombre de paquets (W) émis pendant le trajet aller et retour d'un message (Ta) soit $W = Ta/tb$ où tb correspond au temps d'émission d'un paquet

1) En interne au réseau

$Ta = 2 \cdot 10^5/2 \cdot 10^8 = 1$ ms

$tb = (53.8)/622 \cdot 10^6 = 0{,}68 \cdot 10^{-6}$ s

$W = 10^3/0{,}68 \cdot 10^{-6} = 1\,470$

Soit 1 470 paquets de 53 octets qui auront été émis inutilement. Ce mode de contrôle de flux est inefficace (temps de réaction) sans compter que ces paquets devront être mémorisés pour être retransmis !

2) À l'interface usager

$Ta = 4 \cdot 10^4/2 \cdot 10^8 = 2 \cdot 10^{-4}$

$tb = (53.8)/2{,}048 \cdot 10^6 = 0{,}207 \cdot 10^{-3}$

$W < 1$

Dans ce cas, le contrôle de flux peut être très efficace, l'émission est arrêtée immédiatement.

13.2 Données de la classe Isochrone

Traditionnellement, le transport de la voix nécessite de garantir la délivrance des échantillons (valeur) à un rythme précis, soit un échantillon toutes les 125 µs. Ceci nécessiterait dans FDDI-1 que le TTRT (*Target Token Rotation Time*) soit de 125 µs. Ce qui compte tenu du diamètre envisageable pour le réseau est inconcevable (100 km à $2 \cdot 10^8$ m/s correspond à un temps de 0,5 ms). C'est pour cette raison que les réseaux FDDI-2 et DQDB ont organisé le transfert de données à partir de trames dont la fréquence de récurrence est de 8 000 Hz (période de 125 µs).

Cependant, la technique du jeton temporisé est tout à fait à même d'assurer un transfert de la voix en mode paquets, les contraintes temporelles étant alors moins strictes. Un paquet voix de 20 octets requiert un TTRT de 2,5 ms (20 × 125 µs).

13.3 L'acquittement dans FDDI

Rappelons que dans FDDI le champ de statut de trame (**FS**) comporte les indications d'erreur, d'adresse reconnue et de trame recopiée. Il contient au moins trois symboles respectivement désignés E (erreur détectée), A (adresse reconnue) et C (trame recopiée). Chacun de ces symboles est mis au 0 logique par l'émetteur de la trame (symbole R) ; la station qui détecte une erreur positionne le champ E au 1 logique (symbole S). De même, chaque station qui reconnaît son adresse positionne le champ A à 1 logique (symbole S) et, si elle recopie correctement la trame, le champ C à 1 logique (symbole S) ; sinon ce champ reste à 0 logique (symbole R).

Preview from Notesale.co.uk
Page 731 of 837

	E	A	C	A	C	A	C
État	Reset	Set	Set	Set	Set	Set	Reset
Binaire	00111	11001	11001	11001	11001	11001	00111

Figure 20.47 Composition du champ FS.

Dans la figure 20.47, le champ FS indique qu'aucune station de l'anneau n'a détecté une erreur (Champ E = Reset), trois stations ont reconnu leur adresse (3 champs « A » à Set), mais seulement deux ont correctement recopié la trame (2 champs « C » à Set, un à Reset).

13.4 Rotation des données sur le réseau FDDI

La circulation des données est illustrée figure 20.48. Dans le schéma 1, la station A a acquis le jeton et émet sa trame, en 2, après l'émission de sa trame elle génère un jeton sur le réseau. En 3, C reconnaît son adresse, il recopie la trame. Pendant ce temps, en 4, B acquiert le jeton et émet ses données. À l'instar de A, à la fin de son émission, il insère un jeton. En 5, A reçoit les données qu'il a émises, il les retire de l'anneau. Il n'a pas besoin de régénérer un jeton puisqu'il l'a déjà fait après son émission de données (**ETR**, *Early Token Release*). En 6, D a reconnu son adresse, il recopie les données. Il n'y a plus que les données de B sur le réseau que ce dernier retirera lorsqu'elles lui arriveront.

© Dunod – La photocopie non autorisée est un délit

	Pont	Routeur
Configuration	Très simple (voire sans)	Complexe
Transparence aux protocoles	Oui	Non (Protocoles routables)
Sécurité (Filtre)	Sur adresse MAC	Sur adresse IP (Masque)
Extension du réseau	Aisée	Complexe si routage statique
Trafic de service	Sans, sauf Spanning Tree	Oui, pénalisant
Broacast	Transparent	Filtre, sauf broadcasts dirigés
Charge de travail (personnel)	Négligeable	Importante

Figure 20.58 Comparaison Pont/Routeur.

Preview from Notesale.co.uk
Page 738 of 837

14.7 Masque de sous-réseau

Les deux stations du réseau représenté figure 20.59 ne peuvent correspondre puisqu'elles sont, vis-à-vis du masque de sous-réseau sur le même réseau

Figure 20.59 Réseau défaillant.

Soit il s'agit d'une erreur de configuration d'une des stations qu'il suffit alors de corriger, soit d'une erreur dans la définition du masque de sous-réseau qui porté à 24 bits distinguerait alors deux sous-réseaux distincts.

14.8 Routage statique

Chaque entrée contient l'adresse réseau de la machine destination, la prochaine adresse distante de la route locale à prendre (adresse de l'extrémité distante de la liaison ou *Next Hop*) et les masques associés. Le routeur détermine le port de sortie à prendre par comparaison du Net_ID de la LS distante et du Net_ID de ses différents ports (adresses locales des LS).

Les tables d'extrémité sont les plus simples, les routeurs d'extrémité (Brest et Strasbourg) n'ont qu'à envoyer tout ce qu'ils reçoivent vers le centre de l'étoile (Paris). La table du nœud de Paris ne présente aucune difficulté particulière. La plus complexe est celle du nœud de Marseille qui doit tenir compte des deux sous-réseaux (figure 20.60).

DLCI signalisation

La signalisation est fournie par le PABX, quand des informations de signalisation sont émises, elles le sont au débit du lien PABX/VFRAD en conséquence seul un CIR est à déterminer. De même pour tenir compte des bits de transparence, on arrondira au kbit supérieur soit :

$$\text{CIR} = 10\,000 \text{ bit/s}$$

$$\text{EIR} = 0$$

En l'absence d'information de signalisation, toute la bande passante pourra être récupérée par l'EIR du DLCI données.

DLCI données

La donnée pourra utiliser toute la bande restante soit $128\,000 - 40\,000 - 10\,000 = 78\,000$ bit/s. Les caractéristiques du DLCI données seront fixées à :

$$\text{CIR} = 78 \text{ kbit/s}$$

$$\text{EIR} = 128 - 78 = 50 \text{ kbit/s}$$

Le débit réel de la donnée sera largement supérieur au CIR, le canal donnée pouvant profiter de la récupération des silences (50 à 60 % de la bande) et de l'absence d'information de signalisation.

Preview from Notesale.co.uk
Page 748 of 837

16.7 Comparaison H.323 et SIP

Critères	H.323	SIP
Normalisation	UIT H.323 V4	IETF RFC 2543
Transport de la signalisation	TCP	TCP/UDP
Transport des flux multimédia	UDP	TCP/UDP
Établissement de canaux logiques	Oui, un par sens	Non
Signalisation multicast	Non	Oui
Prioritisation des appels	Non	Oui
Codage des primitives	Binaire Interopérabilité facilitée	Texte Décodage simplifié
Evolutivité	Faible, beaucoup d'extensions propriétaires	Protocole ouvert
Détection des boucles	Non, pas dans la V1	Oui
Gestion des conférences	Centralisée (MCU)	Distribuée

Figure 20.67 Comparaison H.323 et SIP.

CHAPITRE 17

17.1 MTTR/MTBF

Calcul de la disponibilité

Étape 1 : Pour calculer la disponibilité et l'indisponibilité de l'ensemble, il faut déterminer la disponibilité et l'indisponibilité de chacun de ses composants.

Clair	N = Clair^C	Crypte = N mod n	N = Crypte^D	Clair = N mod n
11	1 331	11	194 87 171	11
12	1 728	12	35 831 808	12
13	2 197	19	893 871 739	13
14	2 744	5	78 125	14
15	3 375	9	4 782 969	15
16	4 096	4	16 384	16
17	4 913	29	17 249 876 309	17
18	5 832	24	4 586 471 424	18
19	6 859	28	13 492 928 512	19
20	8 000	14	105 413 504	20
21	9 261	21	180 108 8541	21
22	10 648	22	2 494 357 888	22
23	12 167	23	3 404 [illegible]	23
24	13 824	30	[illegible] 000 000	24
25	15 625	[illegible]	268 435 [illegible]	25
26	[illegible]	20	[illegible] 000 000	26
27	19 683	15	170 859 375	27
28	21 952	[illegible]	823 543	28
29	24 389	2	128	29
30	27 000	6	279 936	30
31	297 918	25	6 103 515 625	31

Preview from Notesale.co.uk
Page 756 of 837

Figure 20.83 Table de codage (C = 3, D = 7).

d) Crypte du mot « MODEM »

Clair	M		O			D			E			M	
Hex (8 bits)	4D		4F			44			45			4D	
Binaire 8 bits	01001	101	01	00111	1	0100	0100	0	10001	01		010	01101
Blocs de 5 bits	01001	101	01	00111	1	0100	0100	0	10001	01		010	01101
Clair Décimal	9	21		7	20		8		17		10		13
Crypte Décimal	3	21		23	14		17		27		10		19
Blocs de 5 bits	00011	10101		10111	01110		10001		11011		01010		10011
Binaire 8 bits	00011	101	01	10111	0	11110	1000	1	11011	01		010	10011
Décimal	29		110			232			237			83	
Hex (8 bits)	1D		6E			E8			ED			53	

Figure 20.84 Chiffrement du mot « MODEM ».

Soit le clair : 0x4D, 0x4F, 0x44, 0x45, 0x4D
et le cryptogramme : 0x1D, 0x6E, 0xE8, 0xED, 0x53.

Le temps de transport des données sera déterminé à partir de la transaction moyenne. Rappelons, qu'il a 100 transactions/heure point de vente, 60 transactions/heure caisse et enlèvement et 40 transactions/jour (soit 5 transactions/heure) pour les terminaux de comptabilité.

La transaction moyenne doit être définie dans le sens Host/Succursale (L_{HS}) et dans le sens Succursale/Host (L_{SH}), la longueur moyenne sera multipliée par 1,2 pour tenir compte des données de service :

$$L_{HS} = \frac{\Sigma \lambda L}{\Sigma L} = \frac{100 \cdot 800 + 60 \cdot 600 + 60 \cdot 500 + 5 \cdot 800}{100 + 60 + 60 + 5} \cdot 1{,}2 = 800 \text{ octets}$$

$$L_{SH} = \frac{\Sigma \lambda L}{\Sigma L} = \frac{100 \cdot 20 + 60 \cdot 100 + 60 \cdot 20 + 5 \cdot 200}{100 + 60 + 60 + 5} \cdot 1{,}2 = 54{,}4 \text{ octets}$$

Nombre de transactions ou taux d'arrivée :

$$\lambda = \sum \lambda = 100 + 60 + 60 + 5 = 225 \text{ transactions/heure} \quad \text{soit} \quad 0{,}0625 \text{ transaction/seconde}$$

Temps de réponse du concentrateur local (t_{rc}), considéré comme le temps de transfert des données du concentrateur aux terminaux (requête et réponse) :

$$t_{rc} = \frac{L_{HS}}{D_t - \lambda L_{HS}} + \frac{L_{SH}}{D_t - \lambda L_{SH}}$$

$$= \frac{800 \cdot 8}{9\,600 - 0{,}0625 \cdot 800 \cdot 8} + \frac{54{,}4 \cdot 8}{9\,600 - 0{,}0625 \cdot 54{,}4 \cdot 8} = 0{,}74 \text{ s}$$

Preview from Notesale.co.uk
Page 762 of 837

Temps de réponse de la liaison louée (t_{rt}) :

$$t_{rt} = \frac{L_{Hs}}{D_t - \lambda L_{HS}} + \frac{L_{SH}}{D_t - \lambda L_{SH}}$$

$$= \frac{800 \cdot 8}{64\,000 - 0{,}0625 \cdot 800 \cdot 8} + \frac{54{,}4 \cdot 8}{64\,000 - 0{,}0625 \cdot 54{,}4 \cdot 8} = 0{,}10 \text{ s}$$

Temps de réponse de la transaction :

$$Tr = t_{rc} + t_{rl} + \text{temps de traitement de la requête} = 0{,}74 + 0{,}1 + 0{,}2 = 1{,}04 \text{ s}$$

Nota : rappelons que lorsque le système est peu chargé, ce qui est fréquemment le cas dans les systèmes conversationnels, on peut admettre plus simplement :

$$Tr = \frac{L}{D}$$

19.3 Réalisation d'un réseau privé d'entreprise

a) Graphe du réseau sans contrainte

Matrice des coûts (Kruskal)

La première étape consiste à établir la matrice des coûts, les liens ayant tous un débit identique, cette matrice ne tiendra compte que des distances intersites (figure 20.91).

Coût du réseau sous contrainte :

Ordre	Lien	Distance
1	Metz Nancy	47
2	Amiens Lille	98
3	Rennes Nantes	100
4	Paris Amiens	115
5	Nancy Strasbourg	118
6	Nantes La Rochelle	122
8	Clermont Lyon	137
10	Marseille Nice	160
11	Dijon Lyon	174
14	Bordeaux Toulouse	213
23	Paris Nancy	282
36	Paris Nantes	344
45	Paris Lyon	393
70	Paris Bordeaux	500
98	Paris Marseille	662
Coût total (km)		**3 465**

Preview from Notesale.co.uk
Page 768 of 837

Figure 20.98 Coûts du réseau sous contrainte.

19.4 Caractéristique mémoire d'un routeur

Taux d'arrivée des paquets (λ)

Le taux d'arrivée des paquets se détermine en appliquant le principe de la superposition des flux, soit :

$$\lambda = 2 \times\ 4 + 2 \times\ 2 + 3 \times\ 6 + 5 \times\ 5 = 55 \text{ paquets/seconde}$$

Taux de service (μ)

Le taux de service représente le nombre de paquets traités par seconde. Il est donné par la relation :

$\mu = 1/\text{ts}$ où ts représente le temps de service soit,

$\text{ts} = (128 \times 8/64\,000) = 16$ ms

$\mu = 1/1610^{-3} = 62{,}5$ paquets/seconde

Charge du système (ρ)

La charge du système ou intensité de trafic est le rapport entre la charge soumise et la charge admissible :

$$\rho = 55/62{,}5 = 0{,}88$$

Notons que le système est stable ($\rho < 1$), mais proche de la saturation.

Nombre de paquets dans le routeur (N)

Le nombre de paquets dans le routeur est donné par la relation :

$$\mathrm{N} = \rho/(1-\rho) \quad \text{soit} \quad \mathrm{N} = \rho/(1-\rho) = 0{,}88/(1-0{,}88) = 7{,}3 \text{ paquets}$$

Temps moyen d'attente (ta)

Le temps moyen d'attente correspond au produit du nombre de paquets dans le routeur par le temps de traitement d'un paquet (temps de service) soit :

$$\mathrm{ta} = \mathrm{N} \times \mathrm{ts} = 7{,}3 \times [(128 \times 8)/64\,000] = 7{,}3 \times 0{,}016 = 0{,}1168 \text{ seconde}$$

Nombre de paquets dans la file d'attente (Paquets en attente Na)

$$\mathrm{Na} = \lambda \times \mathrm{ta} = 55 \times 0{,}1168 = 6{,}424 \text{ paquets}$$

Temps de réponse ou temps de queue (tq)

$$\mathrm{tq} = \mu/\lambda = 7{,}3/55 = 0{,}1327 \text{ s}$$

Taille du buffer (T)

$$\mathrm{T} = \text{Nombre d'items en attente} \times \text{taille d'un item} = 6{,}424 \times 128 = 822 \text{ octets}$$

On retiendra une taille buffer de 1 ko soit une contenance de 8 paquets, la file d'attente est donc du type M/M/1/8.

Probabilité de perte d'un item

Nombre moyen de paquets dans le système : 7,3 paquets.

si $\rho \neq 1$

$$p_n = \frac{\rho^n(1-\rho)}{1-\rho^{K+1}} = \frac{0{,}88^{7{,}3}(1-0{,}88)}{1-0{,}88^{8+1}} = 0{,}075$$

Notons que pour une charge de 50 %, la probabilité de perte serait encore de 2 %, c'est là que réside la difficulté du dimensionnement des mémoires tampons dans les éléments actifs.

19.5 Temps de transit dans un réseau

La méthode consiste à considérer le réseau comme une seule file d'attente et d'appliquer la relation de Little pour déterminer le temps de transit. Pour cela, il convient, à partir du trafic écoulé par chaque nœud, de déterminer le nombre de paquets en transit dans le réseau et d'appliquer ensuite la relation de Little.

© Dunod – La photocopie non autorisée est un délit

Preview from Notesale.co.uk
Page 769 of 837

Glossaire [1]

A

AAL (*ATM Adaptation Layer*) : Dans l'architecture ATM, la couche AAL est chargée de l'adaptation des unités de données des protocoles supérieurs en fonction des caractéristiques retenues pour le transfert (isochronisme...). Les services de la couche AAL se déclinent en AAL1 (Services à débit constant), AAL2 (Services sur connexion à débit variable), AAL3/4 (Services à débit variable pour le transfert de données) et AAL5 (Service sur connexion à débit variable). Voir *ATM*.

ABM (*Asynchronous Balanced Mode*) : Mode de communication supporté par HDLC (et par d'autres protocoles dérivés) concernant les communications point à point orientées poste à poste, dans lequel chaque station peut déclencher la transmission.

ABR (*Available Bit Rate*) : Classe de service dans ATM qui autorise une source à modifier son débit disponible en fonction d'information en provenance des commutateurs internes du réseau. Voir *CBR, UBR* et *VBR*.

Accès de base ou BRI *(Basic Rate Interface)* : Accès RNIS à 144 kbit/s, composé de deux canaux B à 64 kbit/s pour la transmission de la voix, de données et éventuellement d'images et d'un canal D à 16 kbit/s pour la transmission de la signalisation et de données (X.25). Voir aussi *RNIS et RNIS large bande.*

Accès Primaire ou PRI *(Primary Rate Interface)* : Accès RNIS composé de 30 canaux B à 64 kbit/s (voix, données, images) et d'un canal D à 64 kbit/s (signalisation). Voir aussi *RNIS* et *RNIS large bande*.

Accusé de réception de bout en bout : Méthode d'acquittement et de reprise sur erreur dans laquelle ce sont les organes d'extrémité qui assurent le contrôle et la reprise sur erreur. Cette méthode d'acquittement simplifie la réalisation du sous-réseau physique de transport. En environnement faiblement perturbé, l'accusé de réception de bout en bout améliore les performances du réseau (diminution de la charge de traitement des nœuds intermédiaires). Voir *Accusé de réception local*.

Accusé de réception local : Méthode d'acquittement et de reprise sur erreur utilisée entre deux nœuds adjacents d'un réseau. Ce mode d'acquittement permet la reprise sur erreur au plus vite, elle minimise les délais de transmission de bout en bout en environnement perturbé. Voir *Accusé de réception de bout en bout*.

ACD (*Automatic Call Distributor*) : Système de distribution des appels téléphoniques entrants ou sortants.

Preview from Notesale.co.uk
Page 785 of 837

1. Certains termes de ce glossaire sont extraits du dictionnaire CISCO des termes et acronymes réseaux, et reproduits ici avec l'aimable autorisation de la société CISCO System France.

passante minimale aux données des différentes stations (classe synchrone) mais ne garantit pas une récurrence temporelle entre les différentes émissions. De ce fait, FDDI-1 n'est pas susceptible d'assurer des transferts de données de type isochrone (voix, vidéo). FDDI-II superpose sur un même support, l'anneau FDDI, une voie asynchrone et synchrone (fonctionnement en mode paquets) et une voie isochrone (fonctionnement en mode circuits).

FDM (*Frequency Division Multiplexing*) : Voir *Multiplexage en fréquence*.

FECN (*Forward Explicit Congestion Notification*) : Les réseaux à relais de trames ne gèrent pas la congestion. Le contrôle de celle-ci est reporté aux organes d'extrémité. Lorsque le réseau est en état de congestion, il élimine purement et simplement les trames en excès et positionne un bit pour informer les organes d'extrémité de cet état. Les bits *FECN* (Notification de congestion en aval) et *BECN* (*Backward Explicit Congestion Notification*, notification de congestion en amont) sont utilisés pour signaler aux organes d'extrémité l'état de congestion du réseau.

Fédérateur : Voir *Réseau dorsal*.

Fenêtre d'anticipation : Technique de transmission dans laquelle les blocs de données sont émis sans attendre un accusé de réception. Le nombre de blocs pouvant être envoyés sans acquittement est désigné par fenêtre d'anticipation.

Fenêtre d'émission : Voir *Fenêtre d'anticipation*.

Fenêtre de réception : Nombre de blocs de données pouvant être reçus et éventuellement réordonnés par un système récepteur. Voir *Rejet sélectif, rejet simple*.

Fibre optique : Support de verre transportant les informations binaires en modulant un faisceau lumineux. La fibre optique autorise des débits élevés et permet de couvrir des distances importantes.

Fibre monomode : Fibre optique de diamètre relativement faible dans laquelle ne se propage qu'un seul faisceau de rayon lumineux. Ce type de fibre a une bande passante plus élevée que la fibre multimode, mais demande une source lumineuse ayant une plus faible largeur de spectre, par exemple LASER.

Fibre multimode : Fibre optique dans laquelle la propagation des informations s'effectue selon plusieurs chemins (modes).

FIFO (*First In, First Out*) : Mode de gestion des files d'attente selon lequel le premier message arrivé est le premier transmis.

File d'attente : Généralement, liste ordonnée d'éléments en attente de traitement. En routage, ensemble de paquets attendant d'être transmis sur une interface de routeur.

Firewall : Voir *Pare-feu.*

Flow control : Voir *Contrôle de flux.*

FM (*Frequency Modulation*) : Voir *Modulation de fréquence*.

Fondamental : Composante sinusoïdale de même fréquence que le signal périodique d'origine. Voir *Théorème de Fourier*.

Forwarding : Voir *Acheminement*.

Frame Interval (IFG, *Inter Frame Gap*) : Intervalle de temps minimal entre deux trames sur un réseau IEEE 802.3. Une station avant d'émettre doit détecter un silence d'au moins 9,6 μs (réseau à 10 Mbit/s). Ce temps minimal entre deux messages permet : d'une part, à l'électronique de bien discerner deux messages et, d'autre part, l'absorption d'éventuelles réflexions pour éviter la détection de collisions fantômes.

Frame Relay : Voir *Relais de trames*.

Frame Relay Forum : Consortium de constructeurs, d'opérateurs, de consultants et d'utilisateurs chargé de la définition et de la

© Dunod – La photocopie non autorisée est un délit

Preview from Notesale.co.uk
Page 801 of 837

promotion des techniques et solutions basées sur le Frame Relay. Voir *Relais de Trames*.

Freeware : Logiciels gratuits

Fréquence : Nombre de cycles d'un signal transmis pendant une unité de temps donnée. La fréquence se mesure en Hertz (Hz) ou cycles par seconde.

Fréquence vocale : Désigne généralement la bande de fréquence nécessaire à la transmission de la voix analogique (300 à 3 400 Hz).

FSK (*Frequency Shift Keying*) : Voir *Modulation de fréquence*.

FTP (*File Transfer Protocol*) : Protocole de manipulation de fichiers l'environnement TCP/IP. FTP permet la création, la suppression et le transfert de fichiers.

FTP (*Folied Twister Pair*) : Câble à paires torsadées écranté.

Full duplex : Mode de fonctionnement d'une liaison ou d'un équipement dans lequel les informations sont transmises simultanément dans les deux sens. Synonyme *bidirectionnel simultané.*

G

Gateway : Voir *Passerelle*.

GFI (*General Format Identifier* ou IGF, *Identificateur Général de Format*) : Champ d'un paquet X.25 qui permet de définir certains paramètres de l'échange.

GIF (*Graphic Interchange Format*) : Mode de compression d'images numérisées en 256 couleurs.

Gigue (*Jitter*) : Variation du temps de transmission d'un signal.

GPRS (*General Packet Radio Services*) : Norme de transmission de données en mode paquets s'appuyant sur un réseau GSM.

GPS (*Global Positioning System*) : Système militaire de localisation par satellite (USA).

Grappe : Ensemble de terminaux passifs raccordés derrière un concentrateur.

GSM (*Global System for Mobile* communication, adaptation anglo-saxonne de Groupe Spécial Mobile) : Norme de radiocommunication numérique avec les mobiles. France Télécom (Orange) et SFR utilisent cette norme.

H

H.323 : Norme UIT pour le transfert de flux multimédia sur réseau sans garantie de service (mode datagrammes), utilisé dans la voix sur IP.

Hachage : Technique de cryptographie garantissant l'intégrité des données.

Half-duplex : Mode de communication dans lequel les données ne circulent que dans un sens à la fois. Synonymes *Alternat* et *Semi-duplex*.

Hand Over ou **handoff** : Fonction d'un système de radiocommunication qui permet à une station de se déplacer sans interruption de la communication.

Harmonique : Composante sinusoïdale d'un signal périodique non sinusoïdal. Voir *Théorème de Fourier.*

HDBn (Haute Densité Binaire d'ordre *n*) : Codage de type bipolaire dans lequel on introduit des bits fictifs (bit de viol et bit de bourrage) pour éviter une suite de plus de *n* bits consécutifs à zéro.

HDLC (*High Level Data Link Control*) : Protocole ISO standard de Liaison de données orienté bit, dérivé de SDLC. Spécifie une méthode d'encapsulation sur des liaisons de données séries synchrones.

Header : Voir *En-tête*.

HEC (*Header Error Control*) : Octet de contrôle d'erreur sur l'entête d'une cellule ATM. Le calcul du HEC utilise les techniques du CRC. L'HEC sert aussi au cadrage des cellules ATM.

Hertz : Mesure de fréquence ou de largeur de bande. Synonyme cy*cles par seconde.* Abréviation : *Hz.*

Preview from Notesale.co.uk
Page 802 of 837

Liaison d'abonné : Liaison dédiée qui relie un abonné d'un réseau à un point d'accès de ce réseau.

Liaison de données (*data link*) : Liaison affectée à une transmission numérique. Cette expression désigne surtout la couche 2 du modèle OSI de l'ISO.

Ligne commutée : Circuit de communication établi par une connexion via un réseau à commutation de circuits utilisant l'infrastructure du réseau téléphonique.

Ligne multipoint : Ligne de communication reliant physiquement plusieurs équipements.

Link status (état de la ligne) : Signal particulier utilisé dans les réseaux 802.3 10 base T pour contrôler la continuité du lien entre le hub et la station.

Liste d'accès : Liste tenue à jour par les routeurs afin de contrôler l'accès à un certain nombre de services (par exemple pour empêcher les paquets ayant une certaine adresse IP de sortir sur une interface particulière du routeur).

Little-endian : Méthode de stockage ou de transmission des données dans laquelle le bit ou l'octet le moins significatif est présenté en premier. Voir aussi *Big-endian*.

LLC (*Logical Link Control*) : Voir *Contrôle de liaison logique*.

Logical link control : Voir *Sous-couche LLC*.

Loi-A : Norme CCITT (UIT-T) de compression-extension utilisée lors de la conversion de signaux analogiques/numériques sur les systèmes à modulation par impulsion et codage. Cette norme est surtout utilisée dans les réseaux téléphoniques européens. La loi-A est incompatible avec la loi-mu en vigueur en Amérique du Nord et au Japon.

Loi-mu : Norme nord-américaine de compression-extension utilisée lors de la conversion de signaux analogiques/numériques sur les systèmes à modulation par impulsion et codage.

Longueur d'IT : Exprime en bits le nombre de bits transporté durant un intervalle de temps dans un système de multiplexage temporel.

Longueur de mot : La longueur de mot exprime le nombre de bits qui code un symbole. Par exemple le code ASCII utilise des mots dont la longueur est de 7 bits.

Luminance : En télévision couleur, le signal de luminance représente l'image monochrome ou échelle des gris. Voir *Chrominance*.

MAC (*Medium Access Control*) : Dans les réseaux locaux, sous-couche de niveau liaison gérant l'accès au support. Voir *Contrôle d'accès au support.*

Mail Box : Voir *Boîtes à lettres (BAL)*.

Maillage : Définit la connectivité d'un nœud du réseau, le nœud pouvant être atteint par différents liens.

Mainframe : Voir *Ordinateur Central*.

MAN (*Metropolitan Area Network*) : Réseau de transmission couvrant généralement une ville et ses environs. Autorise l'interconnexion de plusieurs réseaux locaux.

Manchester : Voir *Codage Biphase*.

MAQ (*Modulation en Amplitude et à porteuse en Quadrature*) : Technique de modulation qui combine la modulation d'amplitude et de phase.

Masque de sous-réseau : Champ de bits qui permet d'étendre l'adresse réseau d'IP. Ce champ est utilisé pour spécifier des sous-réseaux du réseau principal.

MAU : **1)** *Medium Attachment Unit* : Équipement de raccordement dans un réseau Ethernet. Synonyme *Transceiver*. **2)** *Multiple Access Unit* : Hub dans les réseaux 802.5 (Token Ring).

Preview from Notesale.co.uk
Page 807 of 837

© Dunod – La photocopie non autorisée est un délit

définit par la RFC 1490 qui identifie le protocole transporté.

NNI (*Network Node Interface*) : Interface standard entre des commutateurs ATM. Également *Network-to-Network Interface* en relayage de trames. Dans un réseau SMDS, un NNI est appelé ISSI (*Inter-Switching System interface*).

Nœud : Terme générique utilisé pour faire référence à une entité pouvant accéder à un réseau. Synonyme de *station*. Système constituant un carrefour de lignes de communications dans un réseau : serveur, concentrateur, frontal.

Non-Répudiation : Mécanisme d'authentification dans lequel l'auteur d'un message ne peut nier l'avoir émis ou le destinataire l'avoir reçu.

Norme : Ensemble de règles ou de procédures consacrées par la pratique ou la décision d'un organisme officiel.

NSAP (*Network Service Access Point*) : Adresses réseau ISO, spécifiées par la norme ISO 8348/Ad. Point auquel les services réseaux OSI sont mis à la disposition d'une entité de transport.

Null modem : Voir *Éliminateur de modem*.

Numeris : Nom commercial du Réseau Numérique à Intégration de Services commercialisé par France Télécom. Voir *RNIS*.

Numérotation : Système de signalisation des adresses d'abonné (numéro d'abonné) dans un réseau téléphonique (plan de numérotation). Il existe deux types de numérotation : la numérotation décimale et la numérotation à fréquence vocale. Le plan de numérotation international est défini par la norme E.164.

Numérotation à fréquence vocale : Voir *Numérotation fréquentielle*.

Numérotation décimale ou analogique (33/66) : Numérotation téléphonique des postes téléphoniques à cadran. La numérotation est réalisée par ouverture de la liaison d'abonné. Les numéros sont envoyés au commutateur de rattachement sous forme d'impulsions de 66 ms suivi d'un repos de 33 ms, d'où le nom de système 33/66. Il est envoyé une impulsion pour le 1, deux pour le 2, etc.

Numérotation fréquentielle ou vocale : (multifréquentielle), Numérotation téléphonique normalisée (Q.23). Ce type de numéro est composé à partir du clavier à touche de téléphone. L'enfoncement d'une touche correspond à l'envoi de deux fréquences (la haute suivie de la basse) au central de rattachement (**DTMF**, *Dual-Tone MultiFrequency*). Les postes peuvent comporter 12 ou 16 touches. Certains postes téléphoniques fréquentiels ont la possibilité d'émettre une numérotation décimale. Transmise en transparence durant une conversation la numérotation à fréquence vocale autorise un dialogue homme machine.

Numérotation numérique ou binaire : Numérotation téléphonique des postes téléphoniques numériques. Ces postes émettent directement un signal binaire sur une voie dite de signalisation. La numérotation peut être propriétaire (poste numérique propriétaire) ou normalisée (RNIS).

NVL (*Numéro de Voie Logique*) : Étiquette d'identification d'une communication dans les réseaux X.25. Le NVL n'a qu'une valeur locale entre deux nœuds adjacents du réseau.

Nyquist (**Critère**) : Voir *Critère de Nyquist*.

O

Objet géré : En gestion de réseau, station qui peut être gérée par un protocole de gestion de réseau.

OCR (*Optical Character Recognition*) : Système de reconnaissance optique de caractères convertissant un document imprimé en un document texte.

Preview from Notesale.co.uk
Page 811 of 837

© Dunod – La photocopie non autorisée est un délit

Qualité de service : Mesure des performances d'un système qui reflète sa qualité de transmission et la disponibilité du service.

R

Radio Cellulaire : Technique d'organisation des transmissions radiofréquences dans laquelle on établit une correspondance entre une fréquence et une zone géographique (Cellule). Cette organisation autorise le réemploi des fréquences dans des cellules non contiguës.

RAID (*Redundant Array of Inexpensive Disk*) : Système de disques à tolérance de panne.

Rapidité de modulation : Voir *Baud*.

RARP (*Reverse Address Resolution Protocol*) : Inverse logique de ARP qui permet à une station d'obtenir une adresse IP.

RAS (*Remote Access Service*) : Système de contrôle des accès distants.

Réassemblage : Reconstitution d'une unité de données après sa fragmentation par la source ou à un nœud intermédiaire.

Récupération des silences (DSI, *Digital Speech Interpolation*) : Lors d'une communication téléphonique environ 60 % du temps est inutilisé par la communication (silence). La technique de récupération des silences récupère ces instants pour effectuer des transmissions de données. Pour éviter que le correspondant distant n'ait l'impression que la communication est interrompue le DSI réinjecte, localement, du souffle.

Redirection : Partie des protocoles ICMP et ES-IS qui permet à un routeur d'indiquer à un hôte que l'utilisation d'un autre routeur serait plus efficace.

Région : Ensemble logique de sous-réseaux interconnectés et constituant un domaine de routage autonome.

Reject sélectif : Technique dans laquelle le récepteur ne demande la retransmission que du seul bloc reçu erroné. L'utilisation du rejet sélectif implique que le récepteur ait la capacité de mémorisation des blocs reçus ultérieurement à celui erroné et que le récepteur soit capable d'assurer le réordonnancement des blocs avant de les délivrer à la couche supérieure. Le nombre de blocs en attente s'appelle la fenêtre de réception. Voir *Rejet simple*.

Rejet simple : Technique dans laquelle le récepteur demande à l'émetteur de reprendre la transmission à partir du bloc reçu erroné. Le récepteur n'a aucune capacité de stockage ni de réordonnancement, la fenêtre de réception est de 1. Voir *Rejet sélectif*, *Fenêtre de réception*.

Relais : Terminologie OSI décrivant une unité qui connecte plusieurs réseaux ou systèmes de réseaux. Un relais de Couche 2 est un pont, et un relais de Couche 3, un routeur.

Relais de trame (*Frame Relay*) : Protocole réseau issu d'HDLC LAP-B et présenté comme une simplification d'X.25.

Remise pour le mieux (*Best Effort*) : Se dit des réseaux datagrammes dans lesquels aucune garantie de remise au destinataire n'est donnée.

RENATER : Réseau NAtional de TElécommunications de la Recherche.

Répéteur : Équipement qui régénère le signal d'information et le signal d'horloge. Un répéteur permet d'augmenter la portée d'un système de transmission.

Réseau cellulaire : Réseau de télécommunication spécialement destiné aux équipements mobiles et qui permet la communication entre ces unités mobiles, ainsi qu'avec l'ensemble des abonnés au téléphone du monde entier. Le territoire couvert est divisé en cellules, et chaque cellule est équipée d'une station fixe à laquelle est attribué un certain nombre de fréquences radio-électriques.

Réseau d'entreprise : Réseau (généralement important et diversifié) connectant les principaux points d'une entreprise. À la dif-

Preview from Notesale.co.uk
Page 815 of 837

© Dunod – La photocopie non autorisée est un délit

Circuit virtuel 168, 312
Circuit Virtuel Commuté 169, 314
Circuit Virtuel Permanent 169, 314
Class of Service 343
Classes d'adressage 241
Classes de service 25, 346
Classical IP 448, 449
Clé publique 603
Clé secrète 603
Clés asymétriques 603
Clés symétriques 602
CLLM 330
CLP 340, 348, 349
CLS 447
CMIP 627
CMIS 627
Coaxial 54
Codage 68
Codage 4B5B 73
Codage à la source 9, 68
Codage des informations 10
Codage en ligne 68
Codage Manchester 70
Codage Manchester différentiel 70
Codage NRZ 70
Code *Delay Mode* 71
Code ASCII 12
Code autocorrecteur 107
Code Baudot 12
Code bipolaire 71
Code de Huffman 14
Codec 101
Codes autocorrecteurs 113
Codes cycliques 109
Codes HDBn 72
Coefficient de vélocité 51
Commerce électronique 620
Committed Information Rate 329
Common Channel Signalling 129
Commutation 141, 185, 409, 412
Commutation de cellules 166
Commutation de circuits 163, 164, 522
Commutation de messages 164
Commutation de paquets 165, 522
Commutation de segment 412
Commutation par port 412
Commutation spatiale 164
Commutation temporelle 164
Composante continue 46, 69
Compression 20
Concentrateur 144, 145
Concentration de trafic 142
Congestion 188, 330
Connection Admission Call 343, 348
Connexion de transport 267
CONS 169
Constant Bit Rate 344, 346
Constellation de satellites 63
Contrat de service 190
Contrôle d'admission 189, 190, 328, 343
Contrôle d'erreur 105, 270
Contrôle de congestion 172, 188
Contrôle de flux 123–125, 135, 189, 203, 215, 269, 339
Contrôle de flux dynamique 125
Contrôle de flux explicite 125, 269
Contrôle de flux implicite 124
Contrôle de la congestion 269
Convergence Sublayer 340
Corrélation 241
Correction d'erreur sur temporisation 114
CoS 343
Couche 196
Couche application 220
Couche homologue 196
Couche liaison de données 208
Couche physique 207
Couche présentation 218
Couche réseau 208
Couche session 217
Couche transport 212
Couches basses 201
Couches hautes 201
Couches homologues 197
CRC 109, 110, 338, 605
Crédit d'émission 119, 124
Critère de Nyquist 74, 75
CRTP 584
Cryptographie 601
CS 340
CSMA 528
CSMA/CA 420
CSMA/CD 385
CSS 568
CSTA 553
CT1 543

Preview from Notesale.co.uk
Page 829 of 837

© Dunod – La photocopie non autorisée est un délit

Modulation d'amplitude 79
Modulation de fréquence 79, 81
Modulation de phase 79, 81
Modulation en amplitude à porteuse en quadrature 82
MPLS 186, 356
MPOA 458, 459
MSS 238
MTBF 599
MTTR 599
MTU 187, 238, 401
Multicast 173, 242, 288, 290, 336
Multiplex 149, 150, 299, 300
Multiplexage 146
Multiplexage d'étiquette 151
Multiplexage de longueur d'onde 148
Multiplexage de position 151
Multiplexage des connexions 205
Multiplexage fréquentiel 147
Multiplexage par étiquette 165, 337
Multiplexage spatial 147
Multiplexage temporel 149
Multiplexeur 144–146, 304, 570
MultiProtocol Label Switching 356
Multisite 567

N

NAT 244, 283, 613
NBMA 485, 488
NCP 274
Net_ID 241, 242, 245, 283
NetBEUI 425
NetBIOS 424
Network Operating System 370
Next 52
NIC 378
NNI 339
Node 30
Nommage 171, 176
NOS 370
NRZ 69
NSAP 174, 209
NUA 174
Null modem 97
Numérisation 9, 15
Numéro de séquence initial 264
Nyquist 16

O

ODA 222
Off-net 561
On-line 307
On-net 561
Onduleur 598
Option 255
Organization Unit Identifier 378
OSFP 236
OSPF 185, 484
OUI 378, 384

P

PABX 523, 549, 550, 557, 560
PABX de transit 574, 578
PAD 145, 313, 320, 324
Paging 537
Paire torsadée 51
PAP 274, 609
Paquet 155
Paquétisation de la voix 192
Parabole 60
Paradiaphonie 52
Pare-feu 614
Passerelle 145
PAVI 145
PCI 199
PDH 153, 296, 300, 512
Piggybacking 133, 268
PIN 539
PING 257
PKI 607
Plesiochronous Digital Hierarchy 153
PNNI 351
Point d'accès au service 197
Point of Presence 355
Point to Point Protocol 137
Poison reverse 482
Polynôme générateur 109–112
Pont racine 471
Ponts 467
Ponts à routage par la source 468, 474
Ponts transparents 468, 469
PoP 355
Port 237, 265
Porteuse 78
POTS 360

Preview from Notesale.co.uk
Page 833 of 837

© Dunod – La photocopie non autorisée est un délit

VPN 617
VRC 108
VT 222
VTOA 579

W

WAN 158
WAP 545
WDM 148, 306, 354
Wide Area Network 158
Wireless Local Loop 358
WLAN 417
WLL 358
WMAN 417
WPAN 417
WWAN 417

X

X.121 174, 313
X.21 bis 99
X.25 307
X.500 222
XNS 422
XON, XOFF 124

Preview from Notesale.co.uk
Page 837 of 837

© Dunod – La photocopie non autorisée est un délit