Communication de données industrielles

Théorie et applications générales

Manuel Westermo

5.0

AUDIN - 8, avenue de la malle - 51370 Saint Brice Courcelles - Tel : 03.26.04.20.21 - Fax : 03.26.04.28.20 - Web : http: www.audin.fr - Email : info@audin.fr

Première édition décembre 1994 © Westermo, Suède 1994.
Deuxième édition 1996 © Westermo, Suède 1996.
Édition 2.1 1997 © Westermo, Suède 1996.
Édition 3.0 1998 © Westermo, Suède 1998.
Édition 4.0 2001 © Westermo, Suède 2001.
Édition 5.0 2004 © Westermo, Suède 2005.
Réalisation : Westermo Teleindustri AB, Suède.
Illustrations : Visual Information Sweden AB, Eskilstuna (Suède).
Photographie : bildN, Västerås, Suède.
Björn Fröberg, Jordnära bildform, Eskilstuna, Suède
futureimagebank.com
Contre-épreuve : Ågerups Repro AB, Eskilstuna, Suède
Impression : Eskilstuna Offset AB, Eskilstuna, Suède.

Cher Lecteur

Vous avez sous les yeux le manuel Westermo, .. dont la première édition remonte à 1994. En l'espace de 10 ans, il est devenu un outil indispensable pour les ingénieurs et les personnes intéressées par la communication de données.

Comme dans les éditions précédentes, ce manuel présente en détail la gamme des produits.

Westermo et décrit les aspects les plus courants de la communication de données. Chaque nouvelle mouture du manuel a été l'occasion d'augmenter les sections réservées à la théorie et aux applications générales ; cette 5e édition ne fait pas exception à la règle.

Toutefois, son principe diffère des versions précédentes dans le sens où, devant l'évolution considérable de notre assortiment, nous avons jugé opportun de diviser le manuel en différentes sections, plus pratiques à consulter.

Voici les différentes sections :

- Théorie et applications générales
- Accès à distance
- Ethernet industriel
- Communication locale de données

Nous espérons que, vous aussi, vous adopterez le Manuel Westermo dans l'exercice quotidien de vos activités et qu'il sera le complément idéal aux services fournis par nos collaborateurs dans le monde entier.

Table des matières

La communication de données – bien plus que des câbles et des connecteurs

Communication de données industrielles

La révolution de l'informatique industrielle

L'intégration de canaux d'information novateurs et efficaces dans les processus d'une entreprise peut générer des avantages par rapport à la concurrence. Réduction des délais de livraison, accélération du développement des produits, focalisation de la production sur le client et diminution des périodes de transition ; ce ne sont là que quelques-uns des concepts clés de l'informatique industrielle. Au même titre que l'accès rapide à l'information et le contrôle des processus. L'industrie développe des instruments informatiques qui requièrent une intégration accrue dans toutes les phases d'un processus, de l'achat au marketing en passant par la production. La qualité des flux et filières d'informations est devenue l'une des principales conditions pour l'accroissement de l'efficacité et de la compétitivité industrielles.

Différentes normes

Nous voyons émerger de nouvelles idées, de nouveaux systèmes et de nouvelles solutions visant la création de ces outils informatiques. Conséquence négative de cet élan dynamique et diversifié, l'industrie manque, depuis quelque temps, de normes communément acceptées malgré de nombreuses tentatives. Chaque développeur a créé sa propre solution. La pénurie de normes se manifeste lorsque les ordinateurs, les machines et l'équipement ont besoin de communiquer. Ce problème se pose à plusieurs niveaux, bien au-delà des seuls câbles et connecteurs. Il relève de la manière dont les données sont créées, enregistrées, compressées, adressées et envoyées, de la manière dont le support (un câble, par exemple) transporte, reçoit et décompresse les informations, et de la manière dont ces informations sont lues par le destinataire. Lorsque tous ces paramètres sont en harmonie, nous pouvons parler de communication de données, condition préalable au développement de l'informatique industrielle.

Communication de données industrielles

Les principales étapes de la normalisation relative à la communication de données ont été menées côté bureaux, dans le réseau intégré des ordinateurs personnels, mainframes, imprimantes, serveurs, modems télécom, etc. La communication locale de données au sein de l'industrie n'a pas vraiment bénéficié d'une attention soutenue, en raison du manque de normes. Cette diversité est en outre d'autant plus grande que la communication doit avoir lieu entre, par exemple, des ordinateurs, des tours, des équipements de mesure, des balances, des robots, des systèmes de transport et différents systèmes d'alarme. Les demandes sont plus importantes en termes de fiabilité opérationnelle et d'insensibilité aux interférences. L'objectif de ce manuel est de clarifier les divers concepts, d'expliquer leur fonctionnement et de fournir un guide pratique pour la résolution de problèmes liés à la communication de données industrielles. N'hésitez pas à contacter Westermo pour plus d'informations.

Que représente la communication de données industrielles à nos yeux ?

Pas de temps morts
Tous nos équipements sont conçus de manière à éliminer les interférences et les temps morts. Pour cela, nous utilisons des composants haute qualité tels que des condensateurs à longue durée de vie, et validons la conception des environnements exposés à des interférences.

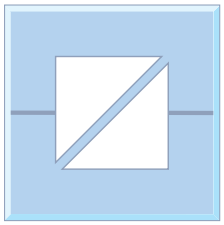
Aucune maintenance requise
Nos produits ont été conçus pour résister aux environnements les plus rigoureux sans la moindre maintenance. En plus de leur structure solide, ils ne comportent aucun élément à remplacer, tel que des batteries.

Environnements exigeants
Les équipements industriels sont généralement installés avec ou à proximité d'autres équipements générateurs d'interférences, comme les postes de soudage ou les machines lourdes. Nous possédons plus de 30 ans d'expérience dans la conception d'équipements de communication pour l'industrie, et ce savoir-faire est mis à profit lors de la conception d'équipements industriels.

Plage de températures étendue
Les applications industrielles requièrent fréquemment une plage de températures étendue. Nous garantissons la fonctionnalité de l'équipement via l'utilisation de composants haute qualité à plage de températures étendue. Ceci concerne notamment le matériel tel que les connecteurs.

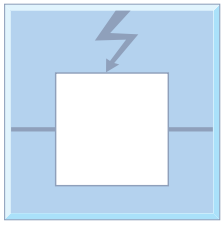
Rendement mécanique
Dans les applications industrielles, les unités sont souvent montées sur des machines exposées aux mouvements ou aux vibrations. Tous nos produits sont conçus pour résister à des contraintes mécaniques importantes. La méthode de montage est tout aussi importante que le rendement mécanique, si bien que notre gamme inclut des produits pour montage sur rack et rail DIN, ainsi que des modèles sur table ou des mini modems.

BACK



Isolation galvanique

Parmi les causes les plus fréquentes d'erreurs dans la communication de données figurent les différences de potentiel entre les unités connectées. L'isolation galvanique des interfaces permet d'éliminer ce problème ; elle est prévue en standard sur nos produits.



Suppression des parasites transitoires

Les équipements industriels sont souvent exposés aux interférences générées, par exemple, par des câbles à forte puissance, des charges réactives et différentes formes de parasites transitoires. Les produits de Westermo sont conçus pour résister à ce type d'interférence.

Alimentation

La fiabilité de l'alimentation électrique est importante pour les équipements industriels ; le courant continu est donc souvent secouru par des batteries afin d'éliminer les temps morts. Le chargement d'une batterie utilise une tension supérieure à la tension nominale de la batterie, de sorte que tous les équipements doivent être conçus en conséquence. Il peut également s'avérer important de prévoir une alimentation électrique redondante afin de doubler la fiabilité, ce qui est le cas pour bon nombre de nos produits.

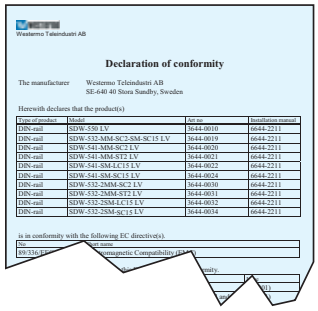
BACK

Déterminisme

Lorsque les équipements sont utilisés pour des applications en temps réel, il est impératif d'établir différents niveaux de priorité. Notre gamme de commutateurs Ethernet présente des fonctions et files d'attente intégrées garantissant le transfert des données prioritaires.

Agréments

Nos unités équipent un grand éventail d'applications dans le monde entier. Nos équipements sont conformes aux normes et critères internationaux en vigueur en matière de sécurité, d'immunité électrique, d'émissions et de contraintes mécaniques.



Westermo Teleindustri AB

Declaration of conformity

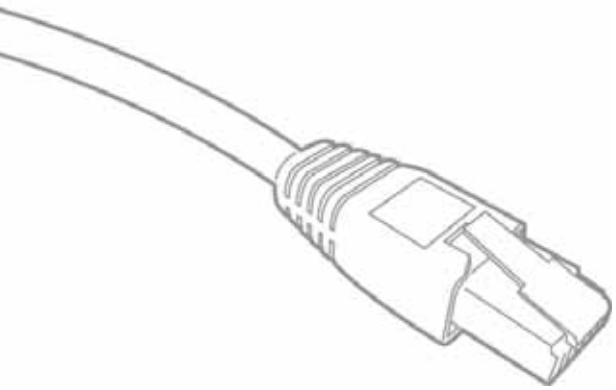
The manufacturer Westermo Teleindustri AB
SE-640 40 Stora Sandby, Sweden

Herewith declares that the product(s)

Type of product	Model	Art.no	Installation manual
DIN-rail	SDW-550 LV	3644-0010	6644-2211
DIN-rail	SDW-532-MM-SC2-SM-SC15 LV	3644-0019	6644-2211
DIN-rail	SDW-541-MM-SC2 LV	3644-0020	6644-2211
DIN-rail	SDW-541-MM-ST2 LV	3644-0021	6644-2211
DIN-rail	SDW-541-SM-LC15 LV	3644-0022	6644-2211
DIN-rail	SDW-541-SM-SC15 LV	3644-0024	6644-2211
DIN-rail	SDW-532-2MM-SC2 LV	3644-0030	6644-2211
DIN-rail	SDW-532-2MM-ST2 LV	3644-0031	6644-2211
DIN-rail	SDW-532-2SM-LC15 LV	3644-0032	6644-2211
DIN-rail	SDW-532-2SM-SC15 LV	3644-0034	6644-2211

is in conformity with the following EC directive(s).

No.	Act name
89/336/EEC	Electromagnetic Compatibility (EMC)



BACK

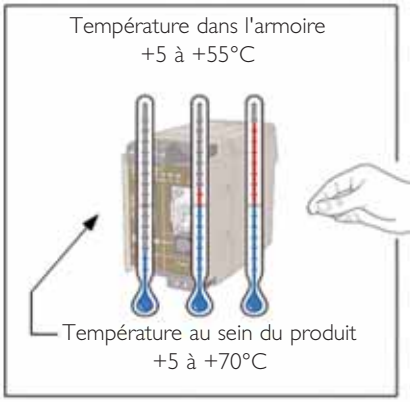
Caractéristiques techniques générales

Caractéristiques environnementales et mécaniques

	Exigences		
Facteur	**Niveau de risque**	**Norme**	**Remarques**
Température de service	+5 à +55° C –25 à +70° C**	IEC 721-3-3	
Température de stockage et de transport	–25 à +70° C	IEC 721-3-1/2	
Humidité relative de service	5 à 95%, sans condensation	IEC 721-3-3	Ne pas utiliser avant stabilisation de la température et de l'humidité
Humidité relative de stockage & transport	5 à 95% condensation autorisée à l'extérieur de l'emballage	IEC 721-3-1/2	Produit en emballage
Contaminants atmosphériques niveau de gravité	G2 (1000 Å=0,1 µm) modéré	ISA 71.04	Produit installé en boîtier IP 21 ou mieux, avec circulation d'air limitée (sans ventilateur)

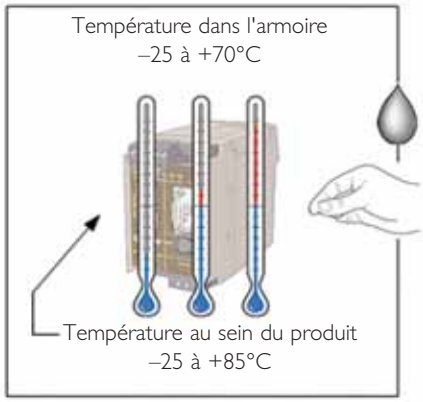
* Plage de températures étendue

Environnement industriel
Température d'exploitation admise +5 à +40°C



IP20
- Protection contre l'accès des doigts à des tensions dangereuses
- Protection contre la pénétration de corps étrangers solides ≥12,5 mm

Environnement extérieur
Température d'exploitation admise –25 à +55°C



IP21
- Protection contre l'accès des doigts à des tensions dangereuses
- Protection contre la pénétration de corps étrangers solides ≥12,5 mm
- Protection contre les dommages occasionnés par la pénétration de gouttes d'eau tombant verticalement.

Les spécifications relatives aux plages de température et à la classification IP se déclinent à différents niveaux, et diffèrent pour les environnements industriels et les installations intérieures. Les composants réalisés pour les diverses variantes doivent dès lors résister à la température ambiante ainsi qu'à la chaleur propre générée dans les coffrets et les armoires. D'une manière générale, chaque coffret est censé augmenter la température de 15°C. A titre d'exemple, nous devons sélectionner des composants résistant à +85°C pour garantir une température ambiante (à l'extérieur de l'armoire) de +55°C.

Caractéristiques électriques

	Exigences			
Facteur	**Niveau de risque**	**Norme**	**Remarques**	**Référence**
Émissions	EN 61000-6-3 Résidentiel	EN 55022 classe B		**Voir 1.1 et 1.2**
Immunité	EN 61000-6-2 Industriel	EN 61000-4-2 EN 61000-4-3 EN 61000-4-4 EN 61000-4-5 EN 61000-4-6 EN 61000-4-8 EN 61000-4-11		**Voir 1.1 et 1.2**
	Équipement informatique	EN 55024		**Voir 1.3**
Alimentation (LV) Plage de tensions nominales	12 à 48 VDC			**Voir 2.1**
Plage de tensions en fonctionnement	9,6 à 57,6 VDC			
Alimentation (HV) Plage de tensions nominales	95 – 240 VAC 110 – 250 VDC			**Voir 2.2**
Plage de tensions en fonctionnement	85,5–264 VAC 88 – 300 VDC			
Alimentation électrique plage de fréquences	48 – 62 Hz			
Protection inversion de polarités	Oui			
Protection court-circuit	Intégrée dans	l'installation du bâtiment		
TNV-3	Maximum 70,7 V crête / 120 VDC		RTC ou équivalent	**Voir 2.5**
TNV-1	Maximum 42,4 V crête / 60 VDC		RS-422/485, Ethernet ou équivalent	**Voir 2.4**
SELV	Maximum 42,4 V crête / 60 VDC		RS-232 ou équivalent	**Voir 2.3**

BACK

1.1 Emissions générales

EN 61000-6-3 EMC – Normes génériques – Norme d'émission pour les environnements résidentiels et commerciaux ainsi que l'industrie légère.

Immunité = Tolérance envers les effets de l'environnement.
Emission = Influence sur l'environnement (énergie émise).

Le niveau d'émission est environ 100 000 fois inférieur à ce que nos équipements peuvent supporter en termes d'immunité.

Niveaux maximum des interférences radio générées par l'équipement connecté au réseau public ou à une source d'alimentation DC. Les critères d'émission sont définis de telle sorte que les interférences générées par l'équipement durant son fonctionnement normal au sein des habitations, bureaux, magasins et environnements similaires n'atteignent pas une valeur néfaste au fonctionnement normal des autres installations (récepteurs radio, par exemple).

1.2 Emissions des équipements informatiques

EN 55022 Équipements informatiques (EI) – Caractéristiques des perturbations radioélectriques – Limites et méthodes de mesure.

- Méthodes de mesure et valeurs limites des interférences radio générées par les EI.
- Les EI de classe B sont destinés aux maisons, bureaux, magasins et environnements similaires. Ils n'offrent pas une protection garantie contre les effets de la réception radio et TV s'ils sont utilisés à moins de 10 m de l'antenne réceptrice.
- Les EI de classe A sont destinés à tous les autres environnements (industriels, par exemple). Ils n'offrent pas une protection garantie contre les effets de la réception radio et TV s'ils sont utilisés à moins de 30 m de l'antenne réceptrice.

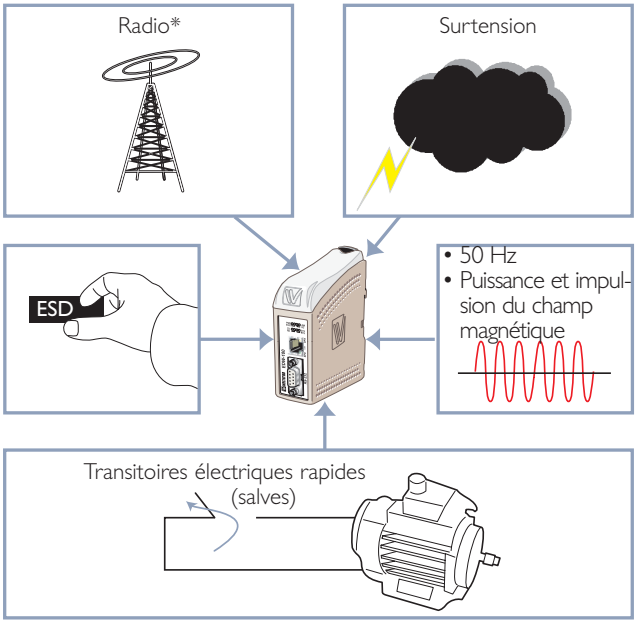
1.3 Immunité des équipements informatiques

EN 55024 Équipements informatiques (EI) – Caractéristiques en termes d'immunité – Limites et méthodes de mesure.

- Essai des équipements informatiques en matière d'immunité aux perturbations continues et transitoires, générées par conduction et rayonnement, y compris les décharges électrostatiques. Les critères d'immunité indiquent un niveau satisfaisant d'immunité intrinsèque, de sorte que l'équipement fonctionne comme prévu dans son environnement.

1.4 Immunité générale

EN 61000-6-2 Compatibilité électromagnétique (CEM). Normes génériques. Normes d'immunité pour les environnements industriels.



* Immunité aux rayonnements. Champs de radiofréquence transmis par conduction.

Essai des équipements connectés à des réseaux d'environnements industriels en matière d'immunité aux perturbations continues et transitoires, générées par conduction et rayonnement (y compris les décharges électrostatiques). Les critères d'immunité indiquent un niveau satisfaisant d'immunité pour les équipements placés dans des environnements industriels.

1.5 Méthodes d'essai de la CEM

EN 61000-4-2 Compatibilité électromagnétique (CEM). Techniques d'essai et de mesure. Test d'immunité aux décharges électrostatiques.

- Méthode appliquée pour tester l'immunité des équipements électriques aux décharges électrostatiques, directement par les opérateurs ou via des objets adjacents. Donne plusieurs niveaux de test renvoyant à différentes conditions d'environnement et d'installation.

Degré de gravité de la CEM dans différents environnements

Résidentiel
Environnements résidentiels et commerciaux, et industrie légère.

Industriel
Immunité pour les environnements industriels.

Chemin de fer
Applications ferroviaires – Équipements de signalement et de télécommunications.

Sous-station
Réseaux et systèmes de communication dans les sous-stations électriques.

Westermo
Une combinaison d'applications résidentielles, industrielles et ferroviaires, étayées par l'expérience d'autres installations Westermo.

Test	Port	Westermo	
		Niveau	Critère
Emission			
Rayonnement	Boîtier	30/37 dB (µV/m)	Classe B
Conduction	Alimentation AC	66-56/56/60 Qp dB (µV)	Classe B
	Alimentation DC	66-56/56/60 Qp dB (µV)	Classe B
Immunité			
TPT	Contact boît.	± 6 kV	B
	Air boît.	± 8 kV	B
Immunité aux rayonnements	Boîtier	20 V/m 1 kHz 80% AM 20 V/m 200 Hz impulsion	A A
Transitoire électrique rapide	Signal	± 2,0 kV	A
	Alimentation AC	± 2,0 kV	A
	Alimentation DC	± 2,0 kV	A
Surtension	Signal L-E Signal L-L	± 2,0 kV ± 2,0 kV	B B
	Alim. AC L-E Alim. AC L-L	± 2,0 kV ± 2,0 kV	B B
	Alim. DC L-E Alim. DC L-L	± 2,0 kV ± 2,0 kV	B B
Champ de radiofréquence transmis par conduction	Signal	10 V 1 kHz 80%AM	A
	Alimentation	10 V 1 kHz 80%AM	A
Alimentation champ magn.	Boîtier	100 A/m 50 Hz	A
Impulsion champ magnétique	Boîtier	300 A/m 6,4/16 µs	–
Alimentation AC*	Alimentation	30% 10/500 ms 60% 100/1000 ms Interruption 10/5 ms	B B B
Alimentation DC	Alimentation	30% 10 ms 60% 10 ms Interruption 10/100 ms 20% sup/inf tension nominale	B B
Vagues d'oscillation	Signal L-E Signal L-L	– –	 –
	Alimentation L-E Alimentation L-L	– –	– –
Perturbations 50 Hz**	Signal L-E Signal L-L	10/100 V 250 V	A A

* Chutes de tension, interruptions brèves et variations de tension.

** Mode différentiel et commun sous conduction.

Critères, classification des performances

Critères A : Performances normales dans les limites spécifiées (conformément aux spécifications du test).

Critères B : Perte temporaire de fonction ou de performances, qui cesse à l'issue de la perturbation. L'équipement testé retourne ensuite en mode de fonctionnement normal sans intervention de l'opérateur.

Critères C : Perte temporaire de fonction ou de performances, dont la résolution requiert une intervention de l'opérateur.

Test	Port	Résidentiel		Industriel		Chemin de fer		Sous-station	
		Niveau	Critère	Niveau	Critère	Niveau	Critère	Niveau	Critère
Emission									
Rayonnement	Boîtier	30/37 dB(µV/m)	Classe B	40/47 dB(µV/m)	Classe A	40/47 dB(µV/m)	Classe A	30/37 dB(µV/m)	Classe A&B
Conduction	Alimentation AC	66-56/56/60 Qp dB(µV)	Classe B	79/73 Qp dB(µV)	Classe A	79/73 Qp dB(µV)	Classe A	66-56/56/60 Qp dB(µV)	Classe A&B
	Alimentation DC	–	–	–	–	79/73 Qp dB(µV)	Classe A	–	–
Immunité									
TPT	Contact boît.	± 4 kV	B	± 4 kV	B	± 6 kV	B	± 6 kV	A***
	Air boît.	± 8 kV	B	± 8 kV	B	± 8 kV	B	± 8 kV	A***
Immunité aux rayonnements	Boîtier	3 V/m 1 kHz 80% AM	A	10 V/m 1 kHz 80% AM	A	20 V/m 1 kHz 80% AM	A	10 V/m 1 kHz 80% AM	A
						20 V/m 200 Hz impulsion	A		
Transitoire électrique rapide	Signal	± 0,5 kV	B	± 1,0 kV	B	± 2,0 kV	A	± 2,0 kV	A***
	Alimentation AC	± 1,0 kV	B	± 2,0 kV	B	± 2,0 kV	A	± 4,0 kV	A***
	Alimentation DC	± 0,5 kV	B	± 2,0 kV	B	± 2,0 kV	A	± 4,0 kV	A***
Surtension	Signal L-E Signal L-L	± 0,5 kV –	B	± 1,0 kV –	B –	± 2,0 kV ± 2,0 kV	B B	± 4,0 kV ± 4,0 kV	A*** A***
	Alim. AC L-E Alim. AC L-L	± 2,0 kV ± 1,0 kV	B B	± 2,0 kV ± 1,0 kV	B B	± 2,0 kV ± 2,0 kV	B B	± 4,0 kV ± 4,0 kV	A*** A***
	Alim. DC L-E Alim. DC L-L	± 0,5 kV ± 0,5 kV	B B	± 0,5 kV ± 0,5 kV	B B	± 2,0 kV ± 2,0 kV	B B	± 4,0 kV ± 4,0 kV	A*** A***
Champ de radiofréquence transmis par conduction	Signal	3 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A
	Alimentation	3 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A	10 V 1 kHz 80%AM	A
Alimentation champ magn.	Boîtier	3 A/m 50 Hz	A	30 A/m 50 Hz	A	100 A/m 50 Hz	A	100 A/m 50 Hz	A
Impulsion champ magn.	Boîtier	–	–	–	–	300 A/m 6,4/16 µs	B	–	–
Alimentation AC*	Alimentation	30% 0,5 s 60% 100 ms Interruption 5 s	B C C	30% 10 ms 60% 0,1/1 s Interruption 5 s	B C C	–	–		
Alimentation DC	Alimentation	–	–	–	–	–	–	Interruption 10 ms	A
								Interruption arbitraire	C
Vagues d'oscillation	Signal L-E Signal L-L	– –	– –	– –	– –	– –	– –	2.5 kV 1,0 kV	A*** A***
	Alimentation L-E Alimentation L-L	– –	– –	– –	– –	– –	– –	2.5 kV 1,0 kV	A*** A***
Perturbations 50 Hz**	Signal L-E Signal L-L	– –	– –	– –	– –	– –	– –	30 V cont. 300 V 1 s 250 V	A A

* chutes de tension, interruptions brèves et variations de tension.

** Mode différentiel et commun sous conduction.

*** Erreur acceptée durant la perturbation de la communication si elle n'entraîne pas de délais ni de pertes de données pour des fonctions cruciales. Les changements d'état des signaux électriques, mécaniques ou communicationnels ne sont pas admis, en ce compris les alarmes et indications du statut.

EN 61000-4-3 Compatibilité électromagnétique (CEM).
Techniques d'essai et de mesure. Test d'immunité au champ électromagnétique, aux radiofréquences et au rayonnement.

- Méthode appliquée pour tester l'immunité des équipements électriques au champ électromagnétique, aux radiofréquences et au rayonnement. Donne plusieurs niveaux et méthodes d'essai.

EN 61000-4-4 Compatibilité électromagnétique (CEM).
Techniques d'essai et de mesure. Test d'immunité aux transitoires électriques rapides/salves

- Méthode appliquée pour tester l'immunité des équipements électriques aux transitoires électriques rapides et aux salves. Donne plusieurs niveaux et méthodes d'essai.

EN 61000-4-5 Compatibilité électromagnétique (CEM).
Techniques d'essai et de mesure. Test d'immunité aux surtensions.

- Méthode appliquée pour tester l'immunité des équipements électriques aux surtensions générées par des éclairs ou la commutation de charges importantes. Donne plusieurs niveaux de test renvoyant à différentes conditions d'environnement et d'installation.

EN 61000-4-6 Compatibilité électromagnétique (CEM).
Techniques d'essai et de mesure. Immunité aux perturbations transmises par conduction, et induites par des champs de radiofréquence.

- Méthode appliquée pour tester l'immunité des équipements électriques aux perturbations transmises par conduction et générées par des champs de radiofréquence situés dans la plage 9 kHz – 80 MHz. Donne plusieurs niveaux et méthodes d'essai.

EN 61000-4-8 Compatibilité électromagnétique (CEM).
Techniques d'essai et de mesure. Test d'immunité aux champs magnétiques à fréquence industrielle.

- Méthode appliquée pour tester l'immunité des équipements électriques aux champs magnétiques à fréquence industrielle. Donne plusieurs niveaux de test renvoyant à différentes conditions d'environnement et d'installation.

EN 61000-4-11 Compatibilité électromagnétique (CEM).
Techniques d'essai et de mesure. Techniques d'essai et de mesure.
Test d'immunité aux chutes de tension, interruptions brèves et variations de tension.

- Méthode appliquée pour tester l'immunité des équipements électriques aux chutes de tension, interruptions brèves et variations de tension. Donne plusieurs niveaux et méthodes d'essai.

BACK

Conditions de sécurité

	Exigences			
Facteur	**Niveau de risque**	**Norme**	**Remarques**	**Référence**
Sécurité électrique	Équipement informatique	EN 60 950		**Voir 1.6**
Durée de vie	10 ans			
Branchement de l'alimentation	Connexion permanente			
Accessibilité	Zone à accès réglementé		Accessible par le personnel de maintenance, avec outillage	
Maintenance	Non			
Circuit d'isolation	Vers circuit(s)		Rigidité diélectrique	
Alimentation	Tout autre		≥1 kV AC	
Alimentation HT	Tout autre		3 kV AC	**Voir 2.3**
SELV	TNV-1, TNV-3		1 kV AC	
TNV-1	TNV-3		1 kV AC	
TNV-1	TNV-1		1 kV AC	**Voir 2.4**
TNV-3	TNV-3		1 kV AC	**Voir 2.5**

Conditions d'installation

Installation	**Cat. inst.**	**Type de câblage**	**Port**	**Remarques**
Alimentation	II		Alimentation	
Alimentation (HT)	II		Alimentation	
TNV-3 (<70,7 Vp 120 V DC)	I	Non blindé	Signal équilibré	RTC ou équivalent
TNV-1 (<42,4 Vp 60 V DC)	I	Paire torsadée Non blindé	Signal équilibré	RS-422/485, Ethernet ou équivalent
SELV (<42,4 Vp 60 V DC)	I	Non blindé	Signal	RS-232 ou équivalent

BACK

1.6 Sécurité électrique

EN 60950 Équipement informatique. Sécurité. Exigences générales.

- Norme de sécurité définissant les conditions requises pour réduire les risques d'incendie, d'électrocution ou de blessure de l'utilisateur et de toute personne entrant en contact avec l'équipement électrique, en ce compris le personnel de maintenance. Applicable aux EI branchés au secteur et alimentés par batterie, ainsi qu'aux EI directement connectés au réseau téléphonique, indépendamment de la source d'alimentation.

Boîtier

Facteur	Niveau de risque	Norme	Remarques	Référence
Dimension (L x H x P) mm	55 x 100 x 128 35 x 121 x 119		Rail DIN 2 cartes Rail DIN 1 carte	
Poids en kg	< 0,6 <			
Fixation	Rail DIN de 35 mm	EN 60715 (EN 50022)	Montage par encliquetage	
Classe de protection	IP 20	IEC 529		**Voir 1.7**
Refroidissement	Convection, écartement : 10 mm (gauche/droite) 25 mm (dessus/dessous)		Écartement (gauche/droite) recommandé pour la gamme complète de températures de fonctionnement	
Matériau boîtier	PC / ABS			
Classement au feu	Cat. d'inflammabilité V-0	UL 94		**Voir 1.8**

1.7 Niveau de protection

IEC 529 Niveaux de protection offerts par les boîtiers (code IP)

- Classification du niveau de protection offert par les boîtiers électriques.
  Type de protection :
- Protection des personnes contre les tensions dangereuses à l'intérieur des équipements
- Protection à l'intérieur des équipements, contre la pénétration de corps étrangers solides
- Protection à l'intérieur des équipements, contre les dommages dus à la pénétration d'eau.

Exemple, IP 21 :

- Protection contre l'accès des doigts à des tensions dangereuses
- Protection contre la pénétration de corps étrangers solides ≥12,5 mm
- Protection contre les dommages dus à la pénétration d'eau tombant à la verticale.

BACK

1.8 Inflammabilité

UL 94 Norme d'inflammabilité des matières plastiques entrant dans la composition d'appareils et de dispositifs

- Méthodes visant à mesurer et décrire les caractéristiques d'inflammabilité de matériaux lorsqu'ils sont exposés à la chaleur et à des flammes sous contrôle, au sein d'un laboratoire.

2 Définitions

2.1 Plage de tensions nominales

- Plage de tensions spécifiée par le fabricant.

2.2 Plage de tensions de service

- Plage de tensions dans laquelle le dispositif peut accomplir ses fonctions moyennant le respect des conditions spécifiées. Plage de tensions nominales et tolérances supérieure/inférieure.

2.3 SELV

- Circuit secondaire conçu et protégé de sorte que ses tensions ne dépassent pas une valeur sûre dans des circonstances normales, sous des conditions de type 'défaut unique'.

2.4 TNV-1

- Circuit secondaire dont les tensions de service normales ne dépassent pas les limites d'un circuit SELV dans des conditions d'exploitation ordinaires, et permettant les surtensions des réseaux de télécommunication.

2.5 TNV-3

- Circuit secondaire dont les tensions de service normales dépassent les limites d'un circuit SELV dans des conditions d'exploitation ordinaires, et permettant les surtensions des réseaux de télécommunication.

BACK

La communication des données...

...est extrêmement importante pour accroître la productivité

Les progrès de l'automatisation imposent également des exigences de fiabilité à la communication de données entre les unités et les systèmes de contrôle, de production et de mesure. La communication de données constitue, en effet, le système nerveux servant de base à l'accroissement de l'efficacité et de la compétitivité, qu'il s'agisse de fabrication, d'installation, de transport ou de soins de santé.

Interface

Il ne suffit pas de trouver un accord concernant le type de signaux et leur mode de conversion et de transmission. Il faut également un accord concernant le type de connecteur et les niveaux de tension qu'ils doivent pouvoir supporter – en d'autres termes, l'interface physique et électrique. A cela s'ajoute une interface logique, qui définit la pertinence du signal.
Un protocole contrôle la structure des signaux, la manière dont les communications sont amorcées ou achevées, l'ordre de transmission et d'émission, l'établissement d'un accusé de réception, etc. Il existe de nombreux protocoles : PROFIBUS, Comli, Modbus, etc.

L'interface physique	définit la manière dont l'équipement est connecté, ainsi que la structure du connecteur.
L'interface électrique	définit les niveaux électriques ainsi que leur valeur (uns ou zéros).
L'interface logique	désigne la signification des signaux.

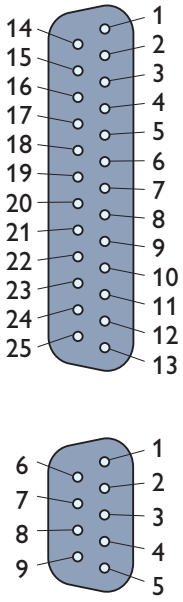
Interfaces les plus fréquentes

L'interface la plus fréquente pour la communication de données via le port série de l'équipement informatique est le RS-232/V.24, qui utilise généralement un connecteur sub D 9/25 pos. Conformément aux recommandations relatives au système RS-232/V.24, le câble reliant les unités connectées ne doit pas dépasser 15 mètres. Il est possible d'utiliser différents modems afin d'atteindre des distances de transmission plus élevées en fonction des supports de communication disponibles (fibre, cuivre, circuit de télécommunication, etc.). V.24 (norme CCITT européenne) et RS-232-C (norme ITU-T américaine) sont deux normes en principe identiques (voir le tableau de la page 25). V.24 décrit la norme physique tandis que V.28 correspond à la norme électrique. Voilà pourquoi l'interface est parfois décrite sous l'appellation V.24/V.28. L'interface décrit et définit les broches du connecteur, les signaux et les niveaux de tension supportés.

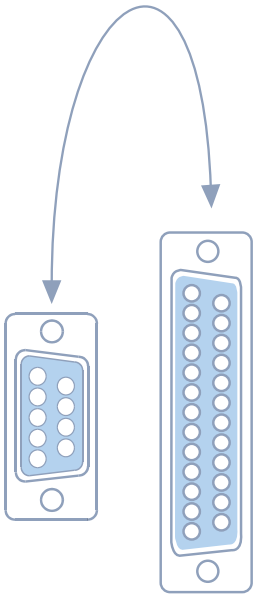
BACK

Signaux dans V.24/RS-232-C

Broche 9/25	Code V.24	Code RS-232	Signal	Nom du signal	Sens DCE
1	**101**	**AA**	**GND**	**Masse**	–
3 2	**103**	**BA**	**TD**	**Données transmises**	**I**
2 3	**104**	**BB**	**RD**	**Données reçues**	**O**
7 4	**105**	**AC**	**RTS**	**Demande d'envoi**	**I**
8 5	**106**	**CB**	**CTS**	**Prêt à l'envoi**	**O**
6 6	**107**	**DC**	**DSR**	**Set données prêt**	**O**
5 7	**102**	**AB**	**SG**	**Signal masse**	–
1 8	**109**	**CF**	**DCD**	**Détecteur de porteuse**	**O**
9	–	–		possibilité + 12 V	–
10	–	–		possibilité – 12 V	–
11	126	SCF	STF	Sélection de la fréquence d'émission	**I**
12	122	SCB		DCD secondaire	**O**
13	121	SBA		CTS secondaire	**O**
14	118	SBA		TD secondaire	**I**
15	**114**	**DB**	**TC**	**Horloge d'émission**	**O**
16	119	SBB		RD secondaire	**O**
17	**115**	**DD**	**RC**	**Horloge de réception**	**O**
18	–	–		–	–
19	120	SCA		RTS secondaire	**I**
4 20	**108/2**	**CD**	**DTR**	**Données bornier prêt**	**I**
21	110	CG	SQD	Détection de la qualité du signal	**O**
9 22	**125**	**CE**	**RI**	**Indicateur de sonnerie**	**O**
23	111	CH/CI		Sélecteur de débit binaire	**O**
24	**113**	**DA**	**EC**	**Horloge externe**	**I**
25	133	–	RFR	Prêt pour la réception	**I**



Les données en gras désignent les signaux les plus fréquents pour les communications locales utilisant des modems courte distance. Le paramètre **I/O** indique le sens de circulation des données vers/depuis le modem (DCE), **I** étant une entrée et **O** une sortie. Le signal TD (données de transmission) correspond dès lors à la sortie d'un DTE mais à l'entrée d'un DCE. La définition du DCE et du DTE compte parmi les sources d'erreurs les plus fréquentes lorsque ces dispositifs sont associés à un équipement RS-232. Voir page 26.



Configuration du câblage

La figure ci-dessous illustre la connexion entre les connecteurs sub D 9/25 pos. pour toutes les combinaisons d'unités DTE et DCE.

DTE vers DTE ou DCE vers DCE

9 Way D-sub	25 Way D-sub		25 Way D-sub	9 Way D-sub
	1		1	
3	2		2	3
2	3		3	2
7	4		4	7
8	5		5	8
6	6		6	6
5	7		7	5
1	8		8	1
4	20		20	4
9	22		22	9

DTE vers DCE

9 Way D-sub	25 Way D-sub		25 Way D-sub	9 Way D-sub
	1		1	
3	2		2	3
2	3		3	2
7	4		4	7
8	5		5	8
6	6		6	6
5	7		7	5
1	8		8	1
4	20		20	4
9	22		22	9

BACK

Eléments clés des principaux signaux

Description des principaux signaux

GND	**Masse**	La broche n° 1 est réservée à la masse entre les dispositifs.
SG	**Signal masse**	Le signal masse est une référence de signal et doit toujours être connecté à la broche 7 (25 broches) broche 5 (9 broches) dans V.24.
TD	**Données transmises**	Ce signal transmet les données d'un DTE vers un DCE.
RD	**Données reçues**	Ce signal correspond aux données transmises à un DTE par un modem ou un DCE.
RTS	**Demande d'envoi**	Ce signal correspond à une demande d'envoi de données à partir d'un DTE. L'appareil attend le signal de réponse du CTS.
CTS	**Prêt à l'envoi**	Signal de réponse du DCE, qui indique au DTE qu'il peut transmettre les données.
DSR	**Set données prêt**	Signal d'un DCE indiquant que l'appareil est sous tension, connecté et prêt.
DTR	**Données bornier prêt**	Même signal que le DSR, mais à partir d'un DTE.
DCD	**Détecteur de la porteuse de données**	Signal de sortie d'un DCE, indiquant qu'il y a une porteuse entre les DCE, et que la connexion est prête pour la communication.
EC	**Horloge externe**	Ce signal s'utilise dans le cas d'une transmission synchrone lorsqu'il faut minuter les données. Le signal correspond à l'entrée dans le DCE.
TC	**Horloge d'émission**	Transmet l'horloge du DCE dans les systèmes synchrones.
RC	**Horloge de réception**	Horloge reçue dans le DTE pour le décodage des données.
RI	**Indicateur de sonnerie**	Signal de sortie d'un modem indiquant qu'il a reçu un signal de sonnerie.

BACK

ASCII

ASCII est l'acronyme de « American Standard Code for Information Interchange » (code standard américain pour l'échange d'informations).
Le code ASCII est disponible en différentes versions pour différentes langues, ainsi que sous une forme « ASCII étendu » utilisant le 8ème bit de données.

BINARY				b_6	0	0	0	0	1	1	1	1
				b_5	0	0	1	1	0	0	1	1
				b_4	0	1	0	1	0	1	0	1
b_3	b_2	b_1	b_0	**HEX**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	0	0	**0**	NUL	DLE	SP	0	@ / É	P	` / é	p
0	0	0	1	**1**	SOH	DC_1	!	1	A	Q	a	q
0	0	1	0	**2**	STX	DC_2	"	2	B	R	b	r
0	0	1	1	**3**	ETX	DC_3	#	3	C	S	c	s
0	1	0	0	**4**	EOT	DC_4	$ / €	4	D	T	d	t
0	1	0	1	**5**	ENQ	NAK	%	5	E	U	e	u
0	1	1	0	**6**	ACK	SYN	&	6	F	V	f	v
0	1	1	1	**7**	BEL	ETB	'	7	G	W	g	w
1	0	0	0	**8**	BS	CAN	(	8	H	X	h	x
1	0	0	1	**9**	HT	EM	)	9	I	Y	i	y
1	0	1	0	**A**	LF	SUB	*	:	J	Z	j	z
1	0	1	1	**B**	VT	ESC	+	;	K	[/ Ä	k	{ / ä
1	1	0	0	**C**	FF	FS	,	<	L	\ / Ö	l	| / ö
1	1	0	1	**D**	CR	GS	-	=	M	] / Å	m	} / å
1	1	1	0	**E**	SO	RS	.	>	N	^ / Ü	n	~ / ü
1	1	1	1	**F**	SI	US	/	?	O	_	o	DEL

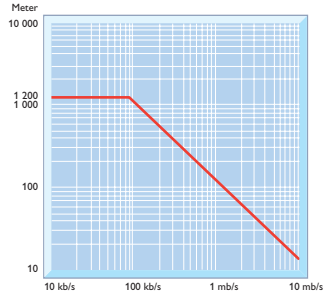
BACK

Interfaces industrielles

RS-422

L'interface RS-422 est idéale pour l'industrie, vu qu'elle est destinée à la réalisation de bus de données, généralement multipoints, entre des ordinateurs centraux et diverses sous-stations. Cette interface est équilibrée et relativement insensible aux interférences. Elle change de polarité sur la paire de fils selon que le transfert concerne un 'un' ou un 'zéro'. La spécification originale de RS-422 stipule que les communications peuvent s'effectuer d'un maître vers 10 esclaves, qui ne peuvent réagir qu'au trafic. Nous utilisons les circuits d'entraînement destinés à l'interface RS-485, dont l'émetteur peut communiquer avec 32 unités et être exploité en mode "à trois états". Nous pouvons dès lors concevoir des applications multipoints sur des connexions à 4 et 2 fils.

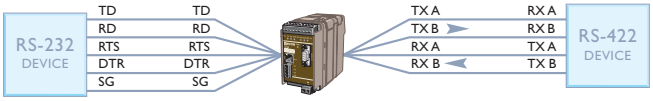
La distance maximale recommandée est de 1.200 m pour un débit de transmission de 100 kbit/s. Les circuits d'entraînement acceptent les débits de transmission jusqu'à 10 Mbits/s, mais la distance de transmission chute alors à 20 m. L'interface RS-422 peut être intégrée à RS-485, RS-232/V.24 par le biais d'un convertisseur.



Distance de communication RS-485

RS-422 sur une connexion à 4 fils

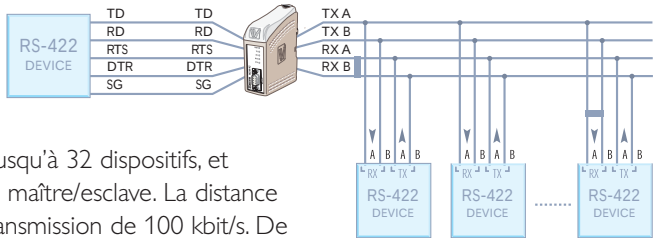
Dans un système RS-422 à 4 fils, l'émetteur maître peut toujours être actif/sous tension, selon l'activité des esclaves. La norme permet les communications simultanées en duplex.

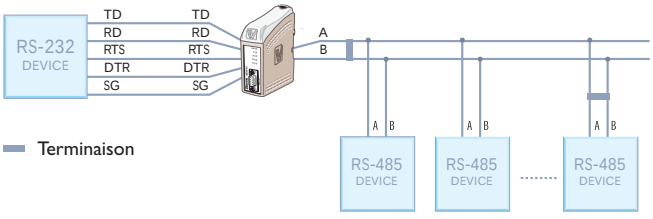


RS-485

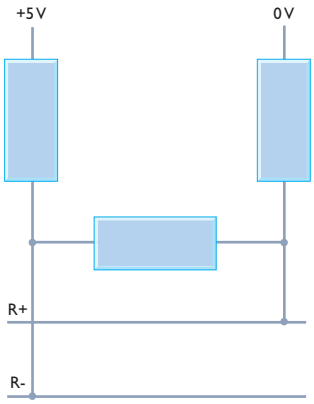
Version plus avancée de la RS-422, l'interface RS-485 est de plus en plus souvent installée par défaut sur différents équipements.

Son principal avantage est qu'elle supporte les communications à 2 fils, c'est-à-dire que l'émetteur et le récepteur de l'équipement peuvent commuter le sens de communication. Elle est conçue pour les bus de données supportant jusqu'à 32 dispositifs, et convient pour les réseaux multipoints appliquant une relation maître/esclave. La distance maximale recommandée est de 1.200 m avec un débit de transmission de 100 kbit/s. De nombreuses interfaces standard utilisent RS-485 en tant que support physique, par exemple, PROFIBUS, Interbus-S et Bitbus.





BACK

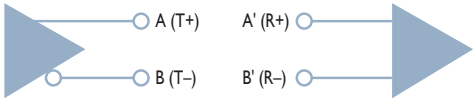


Terminaison et sécurité intégrée

La ligne doit se terminer par une résistance équivalant à l'impédance caractéristique de la ligne (environ 120 ohms). La terminaison doit être placée à chaque extrémité du bus, comme illustré aux schémas de la page 29. Elle permet d'éviter les réfléchissements à l'intérieur du câble. La "sécurité intégrée", quant à elle, est une résistance de chaque câble vers l'alimentation + d'un côté, et vers la source 0 V de l'autre. Cela signifie que la ligne est amenée à un niveau passif prédéterminé ; sinon elle présentera des fluctuations, et des perturbations pourront être interprétées comme étant des données.

Polarité

L'émetteur et le récepteur doivent être interconnectés avec la polarité mutuelle adéquate. Nous savons d'expérience que la connexion d'équipements de différents fournisseurs peut entraîner une interprétation différentes des normes. Une erreur de polarité par rapport à un autre équipement débouchera sur une interprétation incorrecte des données par cet équipement . D'après la norme, l'émetteur est désigné par A et B, lesquels sont connectés à A´ et B´. Nous avons choisi de clarifier ces désignations via l'utilisation de T+, T–, R+ et R– (émission/réception + et –).



Convertisseur RS-232/V.24 vers RS-422/485 – support RTS

Les systèmes dotés de convertisseurs RS-422/485 au sein d'un réseau multipoint ne permettent d'activer qu'un seul émetteur à la fois sur le bus. Les émetteurs d'autres dispositifs doivent être en mode "à trois états", c'est-à-dire passif. Pour ce faire, les équipements connectés doivent pouvoir être contrôlés par le biais d'un signal matériel, généralement un signal RTS ou DTR. Lorsqu'un dispositif cherche à émettre sur le bus, il doit d'abord activer son signal RTS ou DTR, de sorte que le convertisseur commute son émetteur. Il peut ensuite transmettre des données. Si aucun signal matériel n'est disponible, il est possible d'utiliser un convertisseur spécial, qui active son émetteur dès que les données ont été transmises via RS-232, et le coupe lorsque le flux de données s'interrompt.

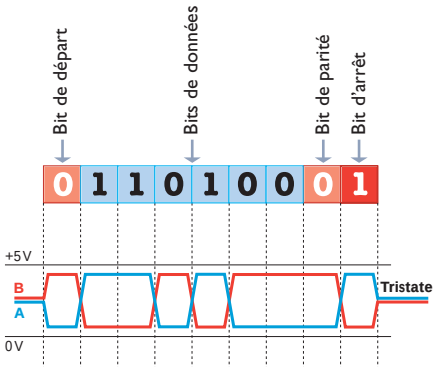
BACK

Installation des interfaces RS-422 et RS-485

Recommandations générales pour l'installation

- Il convient d'utiliser un câble à paire torsadée.
- Les réseaux en étoile ne sont pas autorisés et la distance entre le bus et le dispositif ne peut pas dépasser 30 cm.
- Les récepteurs situés à la fin du bus doivent se terminer par une résistance de 120 ohms.
- La connexion RS-232/V.24 ne peut pas dépasser 15 mètres de longueur.

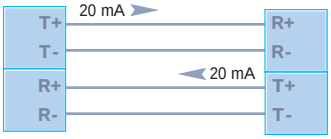
- L'interface RS-422/485 supporte les distances de transfert jusqu'à 1.200 m pour un débit de 100 kbit/s. Il est toutefois possible d'atteindre de plus grandes distances si le débit est moins élevé.



Modems longue et courte distances

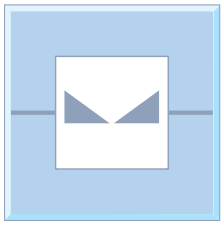
Comme signalé précédemment, il est conseillé de ne pas dépasser une longueur de câble de 15 m avec la norme RS-232/V.24. Les modems courte distance permettent d'allonger le réseau. Ils convertissent le RS-232/V.24 en signaux électriques ou optiques définis, qui sont transmis sur une distance de plusieurs kilomètres via une connexion 4 fils permanente ou une fibre, par exemple. Le modem courte distance du récepteur reconvertit ensuite le signal en RS-232/V.24. Le modem doit utiliser une norme commune ainsi qu'une interface identique pour permettre la communication via le câble.

Boucle de courant 20 mA (TTY)



La boucle de courant est la technique la plus ancienne. Les signaux RS-232/V.24 sont encodés sur une boucle de courant
de 20 mA, correspondant à l'absence ou à la présence de courant sur une paire de fils.
L'émetteur est connecté de manière active et le récepteur de manière passive, ou vice versa, afin d'alimenter chaque paire de fils en courant. La boucle de courant donne des communications fiables, mais est relativement sensible aux interférences, étant donné qu'elle n'est pas équilibrée (voir page 40). L'équipement peut en outre susciter des problèmes vu l'absence de norme reconnue pour la boucle de courant.

BACK



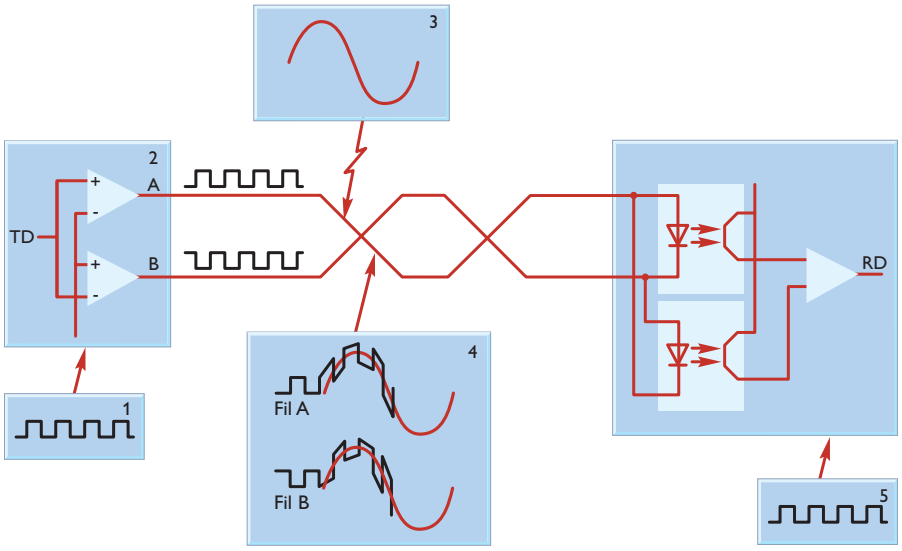
Boucle de courant équilibrée 10 mA (W1)

Westermo a développé sa propre technologie de transmission pour des modems courte distance garantissant des communications sur de grandes distances et dans des environnements soumis à des niveaux élevés d'interférences. Cette technologie est basée sur la conversion des signaux en boucle de courant équilibré de ±10 mA, le sens du courant étant modifié sur la paire de câbles selon qu'il s'agit d'un signal RS-232/V.24 fort ou faible. La ligne de l'émetteur est alimentée par un courant de ±10 mA et le récepteur est doté d'un photocoupleur afin de détecter les signaux. Les photocoupleurs assurent une isolation galvanique totale entre les modems. Le courant circule toujours dans un sens même si aucun équipement n'est connecté du côté RS-232/V.24, sauf lorsque l'émetteur est contrôlé/activé par le biais d'un signal de contrôle de flux. Cette technique, qui a prouvé sa grande fiabilité au fil des ans, est insensible aux interférences et supporte la transmission de données sur une distance maximale de 18 km.

La boucle de courant équilibrée de 10 mA est donc moins sensible aux sources d'interférences externes.

Par rapport à une boucle de courant non équilibrée, une boucle équilibrée est nettement moins sensible aux perturbations externes dues aux différences de potentiel restantes, même si des interférence se manifestent sur la ligne. Voir la figure ci-dessous.

1. Les données sont envoyées à l'émetteur.
2. Les données du fil A sont inversées par rapport aux données du fil B.
3. La ligne est exposée aux interférences.
4. Données de transmission superposées aux interférences.
5. Les données arrivant côté réception ne sont pas modifiées par rapport aux données transmises par l'émetteur (1).



Réseau

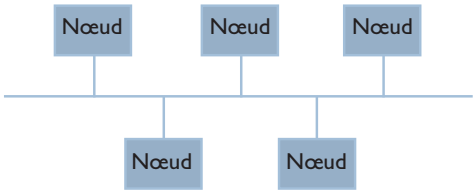
La percée du réseau local a eu lieu durant les années quatre-vingt, initialement via des mainframes centraux ou des mini-ordinateurs aux terminaux connectés en étoile. La mise sur pied de ces réseaux a également suscité le besoin de systèmes de communication de données sûrs et fiables.

La transmission requiert les éléments suivants : un émetteur, un récepteur, un support, des informations et un protocole. L'émetteur, le récepteur et le support ont besoin d'une spécification pour les dispositifs physiques (mode de connexion à un réseau, etc.), tandis que le protocole gère les modalités du transfert. Vous trouverez des explications plus détaillées dans une section ultérieure.

Un réseau local peut inclure la communication de données pour des bureaux, des industries, des hôpitaux, des exploitations minières ou la surveillance du trafic. Un réseau performant, associé à des communications fiables, constitue l'un des éléments clés pour que les entreprises ou organisations puissent se développer via :

- *Le partage des informations,* les bases de données communes peuvent être utilisées ; le partage des e-mails et des fichiers accroît encore l'efficacité du travail.
- *Le partage des ressources,* plusieurs utilisateurs partagent de précieuses ressources au sein du réseau, comme l'imprimante couleurs ou les logiciels communs sur un serveur.
- *La sécurité,* l'accès aux applications individuelles peut être contrôlé via l'octroi de privilèges d'accès au réseau à des utilisateurs individuels ou à des groupes d'utilisateurs, ce qui améliore l'efficacité administrative au niveau central.

Les nœuds sont un concept récurrent dans le domaine des réseaux. Un nœud est, par exemple, un ordinateur, une imprimante ou un équipement de communication. Comme il existe de nombreux types de nœuds présentant de multiples fonctions, il est extrêmement important de réglementer leur mode de communication.



Tout comme les humains ont besoin de parler la même langue pour se comprendre, les équipements du réseau doivent parler le même langage. Cette correspondance est régie par le biais d'un protocole qui détermine comment la communication doit être établie, ce qui peut être dit, par qui, quand et comment. Ces protocoles doivent être harmonisés de sorte que tous les fournisseurs observent les mêmes règles. Les normes peuvent être élaborées par des entreprises individuelles (normes de facto) ou par des instances officielles telles que ISO, ANSI ou IEEE.

La qualité d'un réseau dépend notamment des facteurs suivants :

- La vitesse, qui dépend à son tour du nombre d'utilisateurs simultanés, des médias, du matériel et des logiciels.
- La manière dont la transmission s'effectue, le fait qu'elle atteigne le destinataire adéquat et personne d'autre.
- La qualité des données, la minimisation des perturbations de la communication.
- La vitesse du réseau.
- La fiabilité, le niveau de protection du réseau contre les parasites transitoires, les courants telluriques et d'autres phénomènes susceptibles de perturber les communications.
- La sécurité – Niveau de protection du réseau contre les attaques et les virus.

La nécessité de pouvoir connecter différents réseaux locaux – afin de transférer des données entre entreprises ou à l'intérieur d'une entreprise, sur le plan national ou international – n'a cessé d'augmenter. Comment les systèmes informatiques et bases de données d'une entreprise communiquent-ils lorsqu'ils sont répartis à l'échelle mondiale ? Les options ne manquent pas :

- LAN ("**L**ocal **A**rea **N**etwork", réseau local)
  réseau rapide pour les communications locales, par exemple Ethernet.
- MAN ("**M**etropolitan **A**rea **N**etwork", réseau métropolitain)
  réseau rapide couvrant une zone géographique plus étendue.
- WAN ("**W**ide **A**rea **N**etwork", réseau étendu)
  réseau caractérisé par une très vaste distribution
  géographique. Il peut s'agir d'un pays, voire du monde entier.
- VAN ("**V**alue **A**dded **N**etwork", réseau à valeur ajoutée).
  Il s'agit d'un réseau offrant des services plus étoffés que la seule communication de données.
- GAN ("**G**lobal **A**rea **N**etwork", réseau global)
  réseau constitué de plusieurs réseaux locaux pouvant être interconnectés par MAN et WAN rapides.
- AAN ("**A**ll **A**rea **N**etwork", réseau toutes zones)
  réseau pouvant être utilisé dans les réseaux locaux et les réseaux plus étendus sur le plan géographique.

BACK

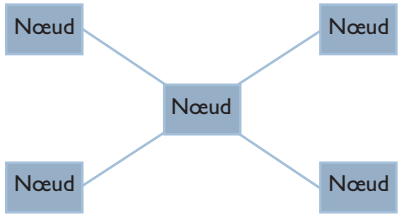
Topologie

Le terme 'topologie' désigne la structure d'un réseau, le placement physique ou logique des nœuds. Il existe cinq topologies de base : point à point, en anneau, en étoile, bus et combiné. Le choix de la topologie est important, car il s'agit d'une infrastructure à long terme, qui assurera la gestion et le transport de données importantes sans temps morts. Le réseau doit en outre pouvoir être adapté et étendu en cas de modification des conditions.

Réseau point à point en série

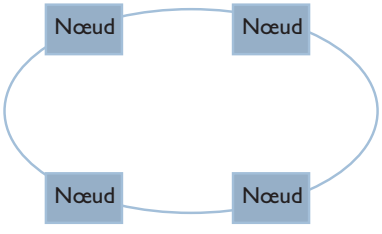
Les communications de données point à point, c'est-à-dire entre deux dispositifs de communication, sont l'une des applications les plus fréquentes. Elles s'utilisent dans des systèmes de base, comme la communication de l'ordinateur à l'imprimante, et des systèmes plus complexes, où l'on permet à chaque utilisateur de communiquer sur sa propre ligne pour des raisons de sécurité. L'interface standard RS-232/V.24 n'est pas recommandée pour les distances de transmission supérieures à 15 mètres.
On utilise dès lors un modem afin d'étendre la ligne et de supprimer les perturbations pour les communications jusqu'à 18 km.

Réseau en étoile



Un réseau regroupant de nombreux utilisateurs 'point à point' est appelé 'réseau en étoile'. Chaque dispositif communique avec l'unité centrale, au centre de sa propre ligne. Le réseau en étoile présente l'avantage d'une fiabilité élevée. Si une ligne tombe en panne, les autres n'en seront pas affectées. Un inconvénient réside dans le fait qu'il requiert plus de câble, d'où un coût plus élevé, et que toutes les communications doivent transiter par l'unité centrale.

Réseau en anneau

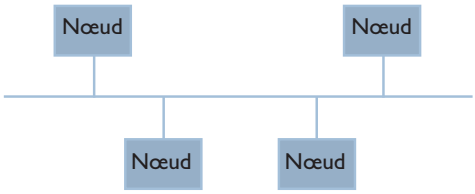


Un réseau en anneau permet d'interconnecter toutes les unités en série au sein d'une boucle fermée. Cela signifie que toutes les communications doivent passer "au travers" de chaque dispositif de l'anneau pour être transmises au récepteur. Un "créneau vide" est envoyé dans le réseau afin d'éviter les collisions. Le nœud de transmission vérifie s'il est vide, intègre son adresse et ajoute ses données. Le nœud suivant de l'anneau vérifie si le contenu du créneau lui est destiné, sinon, il passe le relais. Lorsque le récepteur reçoit son créneau, il le vide de son contenu, insère un reçu et le renvoie au réseau. L'émetteur s'assure que le message a été reçu et validé, puis transmet le créneau vide en vue d'un nouveau trafic. Token Ring est un exemple de réseau en anneau à partir d'un point de signal physiquement connecté en tant que réseau distribué en étoile. Les réseaux en anneau sont performants mais peuvent s'avérer plus difficiles à construire et à adapter qu'un réseau type bus.

BACK

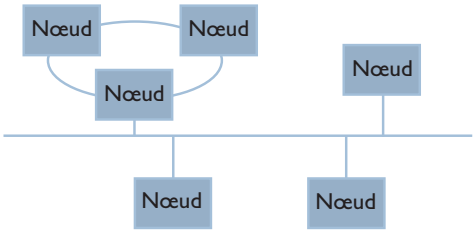
Réseau type bus

En principe, un réseau type bus se compose d'une ligne principale où toutes les unités sont connectées en tant que nœuds. L'ensemble du trafic de données est transmis au récepteur via le bus. Un réseau type bus doit avoir des règles concernant la manière dont un émetteur vérifie si la ligne est libre et dont il devrait réagir en cas de collision entre la transmission et un autre trafic de données, par exemple via une retransmission différée. Le réseau type bus est facile à installer, déployer et étendre ; Ethernet et AppleTalk en sont des exemples courants. Parmi leurs inconvénients figure la lenteur du trafic lorsque plusieurs dispositifs doivent communiquer sur le réseau. Le réseau type bus peut néanmoins être segmenté en plusieurs bus courts.



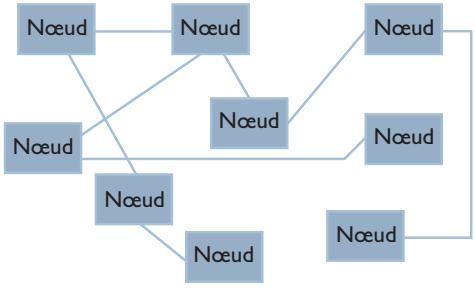
Réseau combiné

L'utilisation de différents produits de communication permet de créer un réseau personnalisé combinant les avantages (performances et fiabilité) des différentes topologies. A titre d'exemple, un réseau type bus avec une étoile distribuée, afin d'interconnecter plusieurs réseaux en étoile. Il ne faut pas oublier que chaque réseau doit disposer d'un système de règles (de trafic) parfaitement fonctionnel pour la communication de données.



Réseau maillé

Les réseaux interconnectés sans structure sont appelés 'réseaux maillés'. Dans un réseau mal documenté et dépourvu de structure, le risque d'erreurs de communication est considérable. Supposez que vous vous connectiez sur un autre nœud et que, ce faisant, vous créiez une boucle. Dans ce cas, une diffusion circulera au sein du réseau. D'autres diffusions accroîtront le trafic et vous finirez par avoir une tempête de diffusions dans votre réseau.

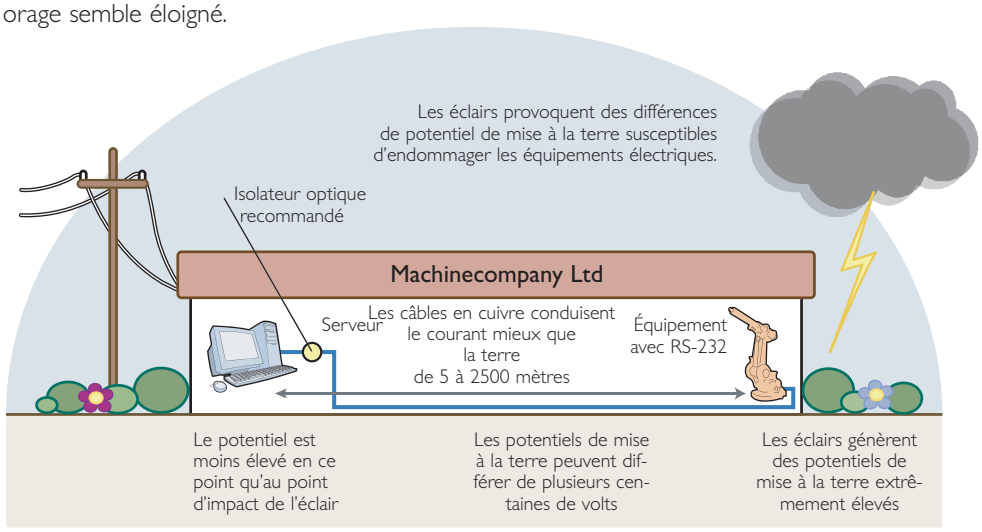


Le problème des interférences

Malheureusement, il ne suffit pas de trouver la bonne méthode de transmission et l'interface adéquate pour résoudre tous les problèmes. Il reste la principale source d'irritation des communications de données, à savoir les interférences : des perturbations externes entraînant une perte de données, des erreurs de transmission et, dans le pire des cas, un arrêt de l'équipement. L'évolution des ordinateurs a débouché sur la fabrication de circuits et composants plus petits, moins gourmands en énergie. C'est une solution idéale sur le plan de la consommation mais hélas, ils sont également devenus plus sensibles et plus vulnérables aux surtensions. Des recherches ont démontré que près de 70% des perturbations électroniques sont dues à une installation incorrecte ou à des interférences (environnement, équipement, machines ou câblages). Seules 20% de ces perturbations sont le fait de pannes matérielles ou logicielles. La majorité des coupables se trouvent dès lors entre nos murs ou à proximité. Les autres proviennent de l'extérieur et sont totalement inattendus. Il s'agit essentiellement de parasites transitoires, des impulsions de tension brèves mais intenses sur le réseau. Les équipements informatiques exposés à des transitoires, de 1.000 V à 10 kV pendant quelques millisecondes, mènent une vie dangereuse.

Eclairs, équipements et lampes fluorescentes

Nous savons qu'un contact direct de la foudre décharge une tension très élevée, qui se propage et endommage les câbles électriques ainsi que les lignes de communications. Dans le pire des cas, elle peut même provoquer un incendie. Vous pouvez, certes, échapper à un impact direct, mais vous risquez d'être affecté par des impulsions qui se propagent sur de grandes distances dans le réseau câblé, ou par des différences de potentiel de mise à la terre entre deux points. Voilà pourquoi une lampe peut scintiller même si un orage semble éloigné.



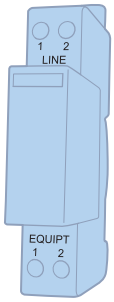
BACK

Les orages ne sont pas les seuls phénomènes à créer des transitoires externes. Vos lampes peuvent également clignoter lorsqu'une entreprise voisine démarre ou arrête ses machines. Ces activités génèrent elles aussi des transitoires et des pointes de tension sur le réseau.

En règle générale, la plupart des transitoires naissent dans vos propres locaux, car les machines, les équipements et les lampes fluorescentes suscitent des impulsions de tension sur le réseau. Une lampe fluorescente éteinte, par exemple, peut émettre de l'énergie stockée sous la forme d'une transitoire jusque 3.000 V. L'impact d'un éclair à proximité d'un câble électrique peut engendrer une transitoire de 6 à 10 kV ; or, la carte d'un circuit de communication standard au sein d'un ordinateur est conçue pour ±12 V. Les transitoires sont généralement à l'origine de l'arrêt inexpliqué d'un équipement informatique ou d'une perturbation temporaire des communications. Ce sont les causes de perturbations les plus fréquentes. Seules 10% des perturbations sont dues à un problème du secteur : surtension ou sous-tension à long terme, ou coupure de courant.

Protection contre la foudre et les surtensions

Comme les surtensions ou la foudre peuvent endommager l'équipement de communication, on nous demande souvent quelle est la protection la plus efficace.
Il est extrêmement difficile de contrôler pleinement les effets de la foudre ; de nombreux problèmes peuvent néanmoins être évités via l'installation de protections adéquates. La protection contre la foudre se décline en deux catégories : l'impact direct et les surtensions induites.
La protection contre les impacts directs requiert la possibilité de dévier plusieurs centaines de milliers d'ampères. Il est plus facile de vous protéger contre les tensions induites car leur période transitoire n'est pas aussi courte et le courant généré lors de la déviation est loin d'être aussi élevé. Comme leur nom l'indique, les tensions induites sont transférées par induction, et ne requièrent donc aucun contact avec la foudre. Ces surtensions sont les plus fréquentes, étant donné qu'elles surviennent à chaque éclair.



Exemples de protections contre les surtensions

Interface	Tension nominale
RS-232	12 V
RS-422/RS-485	12 V
W1	24 V
4-20 mA	24 V
Modem télécom par ligne louée	24 V
Modem télécom par commutation	170 V

BACK

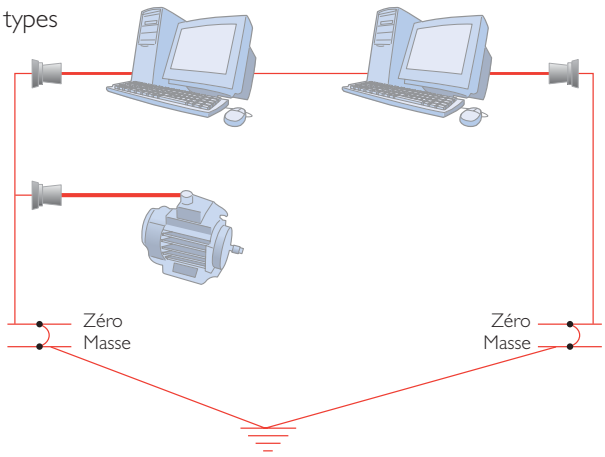
Le marché propose de nombreuses protections contre les surtensions pour les lignes de signalisation/télécommunication ainsi que pour les modems télécom, RS-232, 4–20 mA, RS-485 et d'autres signaux typiques. Cette protection consiste en une protection primaire et une protection secondaire, cette dernière étant adaptée à la méthode de communication. La protection ne requiert généralement aucune maintenance. Une fois le problème de transitoire résolu, la protection revient à son état initial. Sinon, cela signifie que la protection a perdu son efficacité pour l'une des raisons suivantes :

- L'énergie transitoire était trop élevée pour la protection (car la foudre a frappé tout près de l'installation).
- La protection a été endommagée par une surtension à long terme, par exemple à cause d'une connexion directe à l'alimentation 230 V.

Boucles de terre

Une autre cause fréquente d'erreurs de transmission de données réside dans les différences de potentiel de masse ou *boucles de terre*, surtout lorsque les éléments d'un réseau sont raccordés à plusieurs tableaux de distribution aux potentiels de masse différents. Tout courant de fuite peut suivre deux directions vers la terre : soit la direction correcte via une prise de terre dans le tableau de distribution, soit une direction incorrecte via la terre du port série et la terre de l'équipement. Les courants de fuite circulant dans le réseau peuvent susciter des perturbations et endommager les circuits d'alimentation de la ligne. Un réseau de communication est constitué de plusieurs mètres de câbles, fréquemment regroupés avec d'autres câbles destinés à l'électricité et aux télécommunications. Tous les câbles véhiculant du courant génèrent un champ électromagnétique affectant les câbles adjacents ou placés en intersection. Leur combinaison forme de grandes *antennes* qui peuvent capter différents types d'interférences. Il existe des recommandations spécifiant comment router différents types de câblages de manière à minimiser les interférences. La solution la plus simple pour résoudre les problèmes dus aux transitoires et différences de potentiel de masse consiste à utiliser un modem à *isolation galvanique*, qui procure une isolation électrique aux câbles et à l'équipement sans affecter les signaux. Les transitoires, la foudre et les courants de fuite ne peuvent dès lors plus atteindre l'équipement.

Dans l'exemple ci-dessous, les courants de fuite peuvent suivre un trajet incorrect et atteindre un tableau de fusibles via le signal masse du réseau informatique, causant dès lors des interférences.

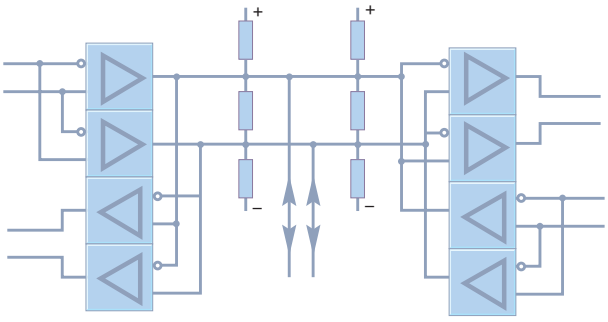


Réduction des interférences

Dans tout système, les signaux électroniques sont toujours sujets aux interférences. Les signaux analogiques tendent à y être plus sensibles car chacun de leurs points véhicule des informations (amplitude et fréquence). En cas de perturbation mineure du signal, le système de réception interprétera ce signal différemment du signal original, et réagira de manière incorrecte. Les signaux numériques sont moins sensibles aux interférences, étant donné qu'ils ne présentent que deux états de base : haut ou bas. Néanmoins, l'interaction de la capacité, de la résistance et de l'inductance des câbles utilisés pour transporter les signaux de données ainsi que les effets du bruit externe peuvent déformer les informations contenues dans le signal au point d'empêcher toute reconnaissance de celui-ci.

Signaux équilibrés

Les signaux équilibrés s'utilisent pour transférer les signaux d'impulsion sur de longues distances via des interfaces différentielles telles que RS-422/485 ou W1.
Lorsque des protocoles équilibrés sont utilisés sur un câble à paires torsadées, la diaphonie entre les paires est annulée efficacement par les champs à induction inverse générés par le flux de courant.
Ce phénomène ne se manifeste pas dans les systèmes déséquilibrés.



Communication rapide équilibrée

Isolation

Dans tous les systèmes de transmission de données, il est essentiel de prévoir une isolation galvanique mutuelle pour les équipements et réseaux, afin d'éviter la propagation de transitoires et d'autres formes d'interférences susceptibles de générer des erreurs de transmission ou d'endommager les équipements.

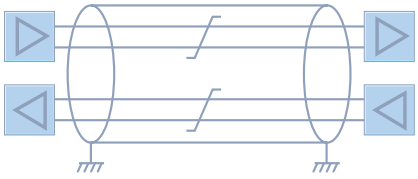
Il existe différents systèmes d'isolation : relais, transformateurs, amplificateurs d'isolation, photocoupleurs, etc. Les transitoires entrantes peuvent également être supprimées à l'aide de protections telles que des varistors, condensateurs, filtres RC et diodes Zener.

Westermo isole ses récepteurs par le biais de photocoupleurs, plus performants que les amplificateurs différentiels, par exemple. Les transformateurs assurent l'isolation de la source d'alimentation, tandis que les varistors et diodes Zener permettent de supprimer les transitoires.

BACK

Réseaux à la terre

D'une manière générale, la meilleure méthode pour minimiser les perturbations consiste à doter le système d'une structure équipotentielle. Cela signifie que les bâtiments, les systèmes électroniques, les bus de terrain et les dispositifs de terrain présentent tous le même potentiel de masse. Dans la pratique, ce résultat est très difficile à atteindre, mais vous pouvez obtenir un potentiel uniforme à l'aide de conducteurs de terre et de réseaux de fils de terre spéciaux. Il est important que le réseau de fils de terre et la masse soient interconnectés et aussi proches que possible l'un de l'autre.



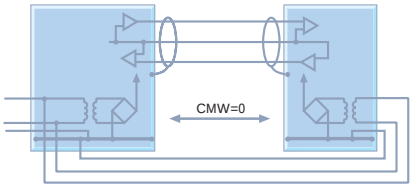
Transmission de données vers RS-422 pour 10 Mbits.

Blindage

La résistance aux interférences externes peut être accrue via l'utilisation de câbles à simple ou double blindage. Dans des circonstances ordinaires, il ne faut connecter qu'une seule extrémité du blindage à la terre.

Dans certaines circonstances extrêmes, où les fréquences élevées sont sources de problèmes, les deux extrémités du câble peuvent être connectées à la terre. Cette méthode suscite toutefois un problème qui peut s'avérer plus grave en cas de différence de potentiel entre les points : le courant circulera alors au travers du blindage et transportera tout bruit sur la masse.

A titre alternatif, il est parfois possible de connecter une extrémité du blindage à la masse et l'autre à la masse par le biais d'un condensateur à faible valeur et capacité élevée.



Transmission de données vers RS-232/V.24.

Liaisons courtes distances sans modem

La transmission directe de données à l'aide d'une interface RS232/V.24 sans modem ne fonctionnera que sur de très courtes distances. Les câbles doivent être routés séparément d'autres câbles, tout en restant aussi proches que possible du câble de masse. Le châssis du dispositif doit également être interconnecté à l'aide d'un fil de cuivre afin de réduire les problèmes de bruit CMV (**C**ommon **M**ode **V**oltages, tensions de mode commun). L'interface RS-232/V.24 donne des communications lentes sur des distances maximales de 15 m. Il convient d'utiliser un amplificateur de ligne ou un modem pour les distances plus élevées.

Le système RS-422 offre une meilleure protection, étant donné que l'émetteur et le récepteur sont équilibrés. Il est possible d'utiliser des câbles blindés à paires torsadées. S'ils sont distincts, les appareils devront présenter des châssis interconnectés et être alimentés de préférence par la même source.

BACK

Modems de télécommunications et interférences

Quand des modems de télécommunications sont utilisés à des fins industrielles, il ne faut pas oublier qu'ils sont particulièrement sensibles aux interférences, malgré l'isolation et les codes de signaux. Si le câble n'est pas protégé avec soin, les communications peuvent être perturbées et déboucher sur des défaillances de composants. Le câblage affecté aux télécommunications doit être séparé du câblage de traitement. Une protection combinée peut s'avérer plus efficace dans les environnements industriels rigoureux.

Câble en fibre optique

Dans ce contexte, le transfert de données par le biais d'un câble en fibre optique est totalement insensible aux interférences électriques. Il peut néanmoins être affecté par le type de câble et l'atténuation de l'épissure.

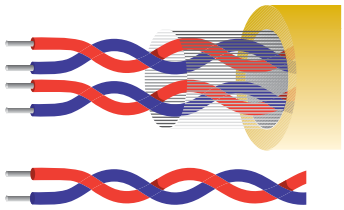
BACK

Types de câbles en cuivre

Le câble physique est souvent le chaînon faible des transmissions de données, car c'est lui qui véhicule le signal analogique sensible aux interférences. C'est le câble, par sa structure, son installation et sa longueur, en combinaison avec les effets électriques avoisinants, qui détermine le débit et la qualité des communications.

Câble à paire torsadée

Le câble à paire torsadée est le câble le plus simple, le moins cher et le plus courant, généralement constitué de 4 fils. Il s'agit d'un câble de cuivre standard sous une gaine protectrice en plastique, avec ou sans blindage métallique. Il existe différents types et marques de câbles, offrant différentes performances, qu'il convient de choisir selon les besoins de l'installation. De même, il existe différentes couches d'isolation correspondant à différents environnements d'installation. La qualité de transmission dépend de trois facteurs importants : la résistance, la capacité et l'atténuation.



Résistance désigne la résistance électrique du câble. Exprimée en ohm/km et variable selon le matériau et la section du câble, elle est mentionnée sur la fiche technique de chaque câble. Les câbles à conducteur solide ne peuvent pas avoir une section inférieure à 0,26 mm^2 et à 0,2 mm^2 pour les câbles multiconducteurs. Si le débit de transmission est peu élevé, c'est la résistance qui impose les limites.

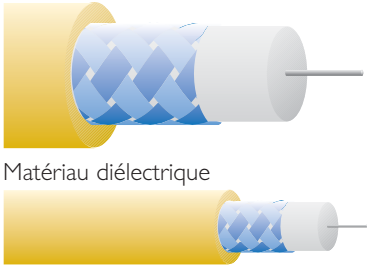
Capacité comme les conducteurs du câble sont isolés les uns des autres, ils génèrent un effet capacitif mutuel. La paire torsadée, le matériau du conducteur et l'éventuel blindage exerceront également un effet. La capacité atténue les signaux différemment à différentes fréquences, la valeur étant généralement de 800 Hz. La capacité se mesure en pF/m. Une valeur indicative pour un bon câble de données est d'environ 50–70 pF/m.
Si le débit de transmission est élevé, c'est la capacité qui impose les limites.

Atténuation indique l'atténuation globale du signal dans le câble, de l'émetteur vers le récepteur. L'atténuation du câble s'exprime en dB/km et s'accroît avec la fréquence. Une augmentation de 3 dB de l'atténuation représente une diminution de moitié de la sortie.

Atténuation (exemples)

150 kHz	8 dB/km
1 MHz	20 dB/km
4 MHz	40 dB/km
10 MHz	65 dB/km
16 MHz	82 dB/km
25 MHz	105 dB/km

BACK



Câble coaxial

Le câble coaxial consiste en un conducteur unique en cuivre, enveloppé dans un blindage. Pour maintenir la distance constante, l'intervalle est rempli d'une couche d'isolation diélectrique en plastique. Le blindage est utilisé en tant que protection ainsi que pour le signal de retour. Le câble coaxial présente d'intéressantes propriétés électriques et convient pour la communication à débit élevé. Au départ, Ethernet n'utilisait que des câbles coaxiaux et existait en deux variantes : la plus lourde (10Base5) et la plus légère (10Base2). Aujourd'hui, Ethernet recourt de plus en plus à un câble spécial à paire torsadée (10BaseT). Le câble coaxial offre l'avantage d'être à large bande, ce qui permet de transmettre plusieurs chaînes simultanément (comme la télévision par câble).

Distance et conception

Il n'est pas toujours aisé de construire des 'passerelles' pour les transmissions de données. Non seulement faut-il connecter différents points à l'aide d'un support de communications, mais il importe en outre de concevoir le support de sorte qu'il puisse prendre en charge le trafic présent et à venir. Il doit également pouvoir gérer efficacement certaines vitesses de transmission, se passer de maintenance et être capable de résister à l'environnement.

Comme la structure adéquate dépend des conditions spécifiques de l'application, il est impossible de formuler un concept général applicable dans tous les domaines. La meilleure approche consiste à envisager différentes alternatives avec un ou plusieurs experts afin d'aboutir à une solution optimale.

Distance de transmission avec différents types de câbles et débits

Le schéma ci-après indique la distance de transmission que l'on peut atteindre avec différents types de câbles et débits. Les lignes en noir, bleu et vert correspondent à un câble à paire torsadée, dont la section vaut 0,3 mm^2 et la capacité, 42 pF/m. Comme les câbles de télécommunications présentent des qualités et dimensions différentes, nous avons opté pour un câble couramment utilisé par le réseau téléphonique suédois, d'une section de 0,2 mm^2 et d'une atténuation d'environ 1,1 dB/km.

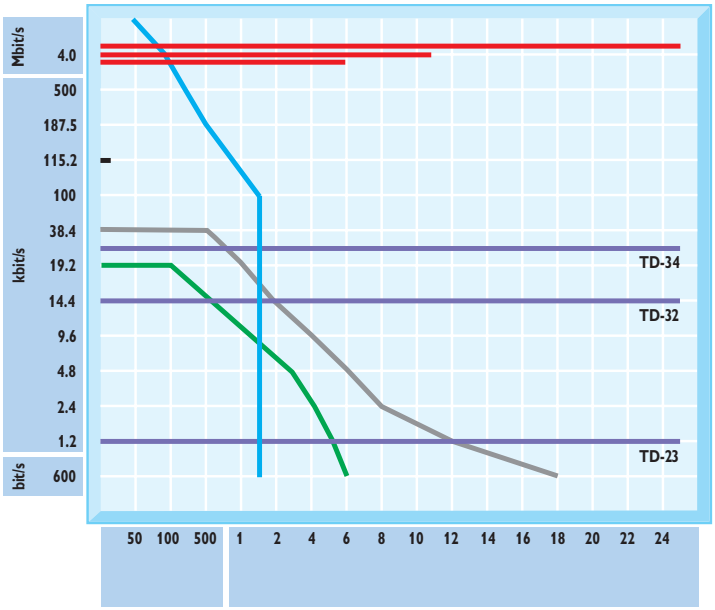
BACK

Calcul de la résistance

Si vous ne connaissez pas la résistance du câble, vous pouvez utiliser cette formule :
Q = R x A/l
Où Q = résistivité du matériau utilisé. Pour le cuivre, vous pouvez utiliser 0,017 μ Ωm, ou 0,017 x 10^{-6}. R = résistance du câble, A = section du câble et l = longueur.
Cette formule est facile à utiliser avec les conducteurs solides. Pour les câbles multi-conducteurs, il faut multiplier la section par le nombre de conducteurs.
Section = rayon x rayon x pi.

Deux symboles pour la capacité

Il existe deux symboles, nF/km ou pF/m, qui correspondent à deux variantes de la même unité de mesure. nF désigne le nanofarad, soit 10^{-9} farad par kilomètre (0,62 mi). pF, quant à lui, désigne le picofarad, soit 10^{-12} farad par mètre.



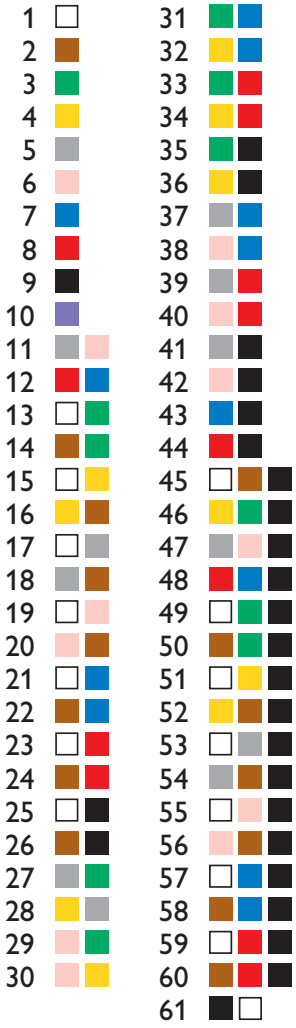
- Ligne téléphonique louée
- Boucle de courant équilibrée 10 mA (W1)
- Fibre optique
- RS-422/485
- Boucle de courant 20 mA
- RS-232/V.24

n.b. Toutes les vitesses et distances ont été calculées sur la base de câbles présentant des valeurs standard en matière de résistance et d'impédance.
Dans les installations sur site, la distance de transmission peut varier en fonction de la qualité du câble et des conditions locales.

BACK

Codes de couleurs

DIN 47100 pour les câbles de données LiYY et LiYCY.
N° et couleur de conducteur :



Codage des câbles

La norme suédoise de marquage des câbles est spécifiée dans SEN 241701. Une norme internationale commune a également été formulée par le comité CENELEC. Le câble est marqué de deux à cinq lettres présentant les significations suivantes :

Conducteur — E D C K P — *Autres*

Isolation — *Recouvrement* — *Propriétés*

1ère lettre
A *cuivre, unifilaire*
B *cuivre, multi-conducteurs*
K *tube coaxial*
M *cuivre, multi-torons*
R *cuivre, multi-torons suppl.*
S *cuivre, jauge fine*
T*cuivre, jauge extra-fine*

2ème lettre
D *caoutchouc, tube extérieur en caoutchouc*
E *caoutchouc éthylène-propylène*
F *caoutchouc fluorocarboné*
H *caoutchouc siliconé*
I *polyuréthane*
K *PVC*
L*plastique polyéthylène*
M *plastique polypropylène*
N *polyamide*
T *polytétrafluoroéthylène (PTFE)*
U *plastique polyéthylène cellulaire*
V *caoutchouc, sans recouvrement en caoutchouc*

2ème et 3ème lettres
O *caoutchouc résistant à l'huile et aux intempéries (caoutchouc chloroprène)*
S *polyéthylène chlorosulfoné*

3ème lettre
C *conducteur concentrique en cuivre*
H *toile gainée thermorésistante*
I *polyuréthane*
J *blindé à l'aide d'une bande d'acier*
K *gaine PVC à section arrondie*
L *plastique polyéthylène*
N *polyamide*
T *blindage en fil d'acier galvanisé*
U *sans recouvrement*
V *caoutchouc*
Y *recouvert d'une simple isolation et d'une gaine*

3ème et 4ème lettres
A *blindage au moyen d'une bande d'aluminium*
F *câble à blindage métallique*
P *blindage en fil d'acier galvanisé*

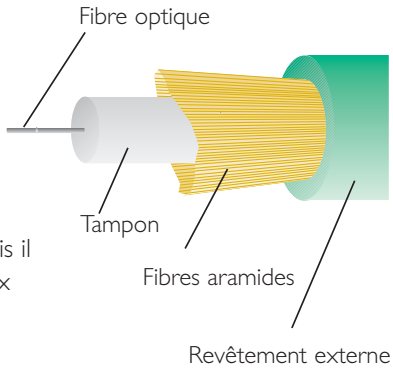
4ème lettre
B *connexion ou câble pour véhicules*
D *gaine avec renforts intégrés et conducteurs libres*
H *conducteurs isolés, câblage autour des renforts*
K *gaine PVC*
L *gaine PE*
N *gaine PA*
O*gaine caoutchouc résistante à l'huile et aux intempéries (caoutchouc chloroprène)*
T *ligne de connexion épaisse*
V *câble pour pose immergée*

5ème lettre
H *conducteurs à blindage séparé*
K *gaine PVC*
L *gaine PE*
N *gaine PA*
P *paires à gaines séparées*

4ème et 5ème lettres
C *câble avec renforts intégrés dans la gaine*
E *structure renforcée*
J *câble pouvant être posé dans le sol ou blindage à bande d'acier avec revêtement métallique*
R *câble de contrôle ou de signalement*
X *ligne RTC*
Y *ligne RTC résistante aux intempéries*

BACK

Communications par fibres optiques

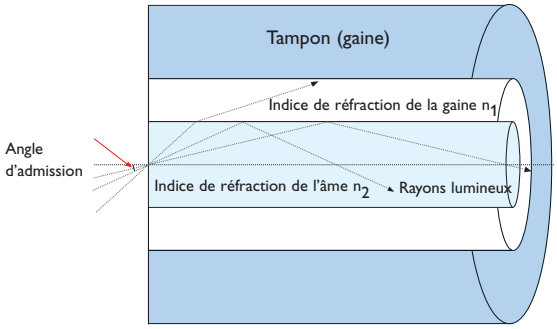


Le principal avantage de la fibre optique réside dans son insensibilité aux interférences électriques et magnétiques. Elle est donc parfaitement adaptée aux conditions rigoureuses des milieux industriels, où elle garantit la sécurité des transmissions à des débits très élevés. Les câbles en fibres optiques peuvent être utilisés sur des sections particulièrement sensibles des réseaux et combinés à l'aide d'un modem avec, par exemple, un câble à 4 fils dans un système. L'investissement requis pour installer un réseau à fibres optique demeure légèrement supérieur au prix de câbles en cuivre, mais il offre de nombreux avantages. Le marché est néanmoins en pleine expansion et les prix diminuent.

La gamme Westermo de produits en fibre optique convertit les signaux électriques en lumière, qui est ensuite transférée vers le câble par le biais d'un émetteur à fibre optique doté d'une diode électroluminescente ou d'un laser. L'utilisation d'un laser et de vitesses élevées permet d'allonger les distances de communication. Les diodes laser sont toutefois onéreuses, si bien qu'on utilise plus souvent des diodes électroluminescentes. Le récepteur abrite une photodiode, qui reconvertit les impulsions lumineuses en signaux électriques.

Câble en fibre optique

En principe, un câble en fibre optique est constitué de deux types de verre présentant des indices de réfraction différents. La partie centrale est appelée "âme" et la zone périphérique, "gaine".



Lorsqu'une impulsion lumineuse pénètre dans la fibre, elle est réfléchie dans le câble car la frontière entre deux couches agit comme un miroir, pour autant que l'angle d'incidence ne soit pas trop élevé.
L'âme et la gaine du câble en fibre optique sont entourées d'une enveloppe externe, dont la seule fonction est de protéger les fibres contre les influences extérieures.

La sélection d'un câble dépend de divers critères :

- Matériau
- Monomode ou multimode
- Saut ou gradient d'indice
- Longueur d'onde de l'émetteur

BACK

Matériau

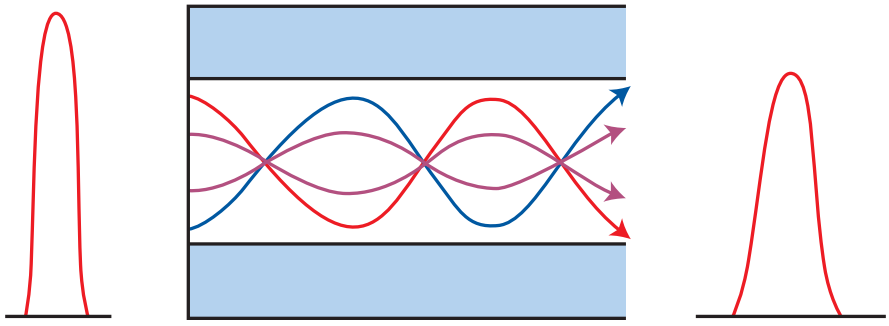
Le matériau utilisé pour l'âme et la gaine diffère selon le type de fibre. Le matériau le plus fréquent est le verre, un verre extrêmement pur, à savoir le dioxyde de silicium (silice). Les câbles peuvent aussi être constitués de silice à gaine de plastique (PCS, "Plastic-Clad Silica"), ou totalement réalisés en plastique (âme et gaine).
Les câbles en verre sont plus performants mais requièrent des terminaisons plus complexes. Les fibres en plastique, quant à elles, présentent des terminaisons plus simples mais sont moins performantes.

Atténuation dans les fibres multimode

Les différentes épaisseurs possibles pour le matériau de l'âme donnent différents types de câbles. Les deux types principaux à connaître sont les fibres multimode et monomode.

Les dimensions les plus courantes pour les câbles multimode sont 62,5 µm pour l'âme et 125 µm pour la gaine (62,5/125).

Les dimensions les plus courantes pour les câbles monomode sont 9 µm pour l'âme et 125 µm pour la gaine (9/125).



Impulsion lumineuse transmise

Traversées optiques dans les fibres multimode à gradient d'indice

Impulsion lumineuse reçue

Multimode

Les dimensions des fibres multimode offrent suffisamment d'espace pour intégrer plusieurs modes dans une seule âme. Les câbles multimode se déclinent en deux catégories, à savoir les fibres à gradient d'indice et à saut d'indice. Dans une fibre à saut d'indice, certains modes réfléchis dans le câble doivent se déplacer plus loin que d'autres, de sorte que l'impulsion lumineuse se propage. La fibre présente dès lors une bande moins large. La solution à ce problème réside dans le gradient d'indice. Dans les câbles à gradient d'indice, l'indice de réfraction diminue progressivement du centre de l'âme vers la gaine. Cela signifie qu'un faisceau lumineux circulant essentiellement au centre du câble est plus lent que ceux situés en périphérie. L'effet global maintient la cohérence de l'impulsion.

BACK

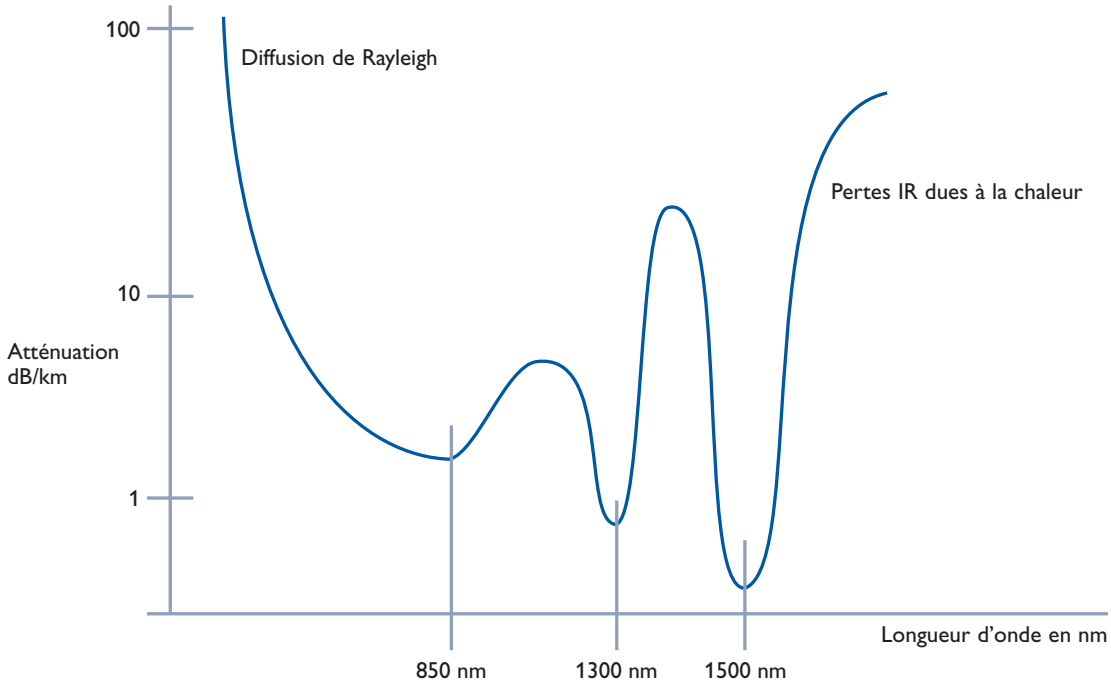
Atténuation dans les fibres monomode

Les fibres monomodes présentent une âme si fine qu'elles ne peuvent supporter qu'un seul mode, de sorte que l'impulsion lumineuse transmise ne subit aucune distorsion lors de son passage dans le câble.

Longueur d'onde

L'atténuation au sein d'un câble dépend également de la longueur d'onde de la lumière produite par l'émetteur. Les longueurs d'onde à faible atténuation sont 820 nm, 1300 nm et 1550 nm. Les fibres monomode n'offrent une propagation efficace que pour les fréquences plus élevées.

Atténuation de la lumière dans les fibres optiques pour différentes longueurs d'onde



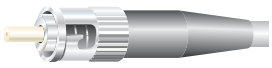
Récapitulatif des types de fibres

Matériau	Type	Ame/Gaine	Atténuation (dB/km)	Champ d'application
Plastique	Multimode Saut d'indice	200-600/450-1000 um	330-1000	Installation simple Distances courtes
Verre (silice) âme plastique	Multimode Saut d'indice	200-600/350-900 um	4-15	Coûts peu élevés, Distances courtes
Verre	Multimode Saut d'indice	50-400/125-440 um	4-15	Coûts peu élevés, Distances courtes
Verre	Multimode Gradient d'indice	30-100/100-140 um	2-10	Coûts moyens Distance moyenne
Verre	Monomode	3-10/50-125 um	0,4-5	Coûts élevés Longues distances

BACK

Terminaison

Les câbles en fibre optique peuvent être terminés de nombreuses manières. Avec les fibres de verre, c'est la terminaison des câbles multimode qui est la plus aisée. Une procédure simple, appelée "sertissage-clivage", consiste à sertir le connecteur sur la fibre à l'aide de pinces spéciales, puis à cliver la fibre avec soin. Une autre procédure, plus fiable, consiste à utiliser une résine époxyde afin de lier la fibre dans le connecteur (il existe des connecteurs déjà pourvus d'un adhésif). Le connecteur est alors chauffé à l'aide d'un four spécial pendant environ 1 minute, puis la fibre est insérée dans le connecteur, où on la laisse refroidir. Ces deux méthodes de terminaison requièrent un équipement permettant de préparer la fibre avant de monter le connecteur, et de polir la fibre une fois la terminaison effectuée. Les fibres reliées peuvent s'avérer bénéfiques aux systèmes dont les points de connexion sont fréquemment changés, vu qu'elles assurent une terminaison plus durable. Le marché propose de nombreux connecteurs de fibres, mais l'industrie en utilise essentiellement quatre :



ST connecteur simplex pour multimode 2 km

MTRJ connecteur duplex pour multimode 2 km ou monomode 15/40 km

SC connecteur simplex pour multimode 2 km ou monomode 15/40 km.

LC connecteur duplex pour monomode 15/40/85 km

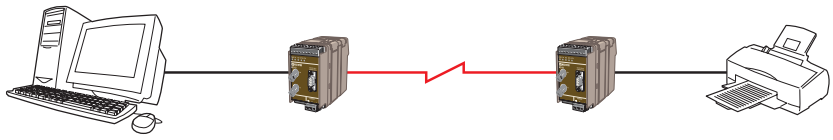
BACK

Calcul du budget des pertes

La distance de communication d'un système dépend de la puissance de sortie de l'émetteur, de la sensibilité du récepteur et de la perte inhérente aux terminaisons et aux épissures de câbles. Pour calculer cette distance, on établit un budget-fibre, qui correspond à la différence entre la puissance de sortie de l'émetteur et la sensibilité du récepteur. Ces deux facteurs présentent une valeur typique ainsi qu'un niveau minimal. Nous avons choisi de documenter ces deux valeurs pour la majorité de nos produits, car les spécifications des fabricants peuvent accuser d'importantes variations. Cela s'applique essentiellement aux fibres monomode.

Exemple

Nous interconnectons deux dispositifs à l'aide de deux MD-62. Devons-nous utiliser une fibre multimode ou monomode ? L'atténuation est de 3,2 dB/km à 820 nm pour le câble multimode, et de 0,5 dB/km à 1300 nm pour le monomode. La distance de notre exemple est de 6 km avec deux épissures dans le câble, qui donnent toutes deux une atténuation de 0,2 dB.



Option 1, câble multimode
3,2 dB/km x 6 + 2 x 0,2 dB = 19,6 dB

Option 2, câble monomode
0,5 dB/km x 6 + 2 x 0,2 dB = 3,4 dB

D'après le manuel du MD-62 les budgets-fibre minimum sont les suivants :
Câble multimode 62,5/125 d'une longueur d'onde de 820 nm 14,5 dB
Câble monomode 9/125 d'une longueur d'onde de 1300 nm 6,3 dB

Il serait donc préférable d'opter pour le monomode.
Cet exemple illustre l'utilisation du budget-fibre pour calculer la distance de transmission. Dans ce cas de figure, le budget-fibre est spécifié par le manuel du MD-62

BACK

Modèle OSI

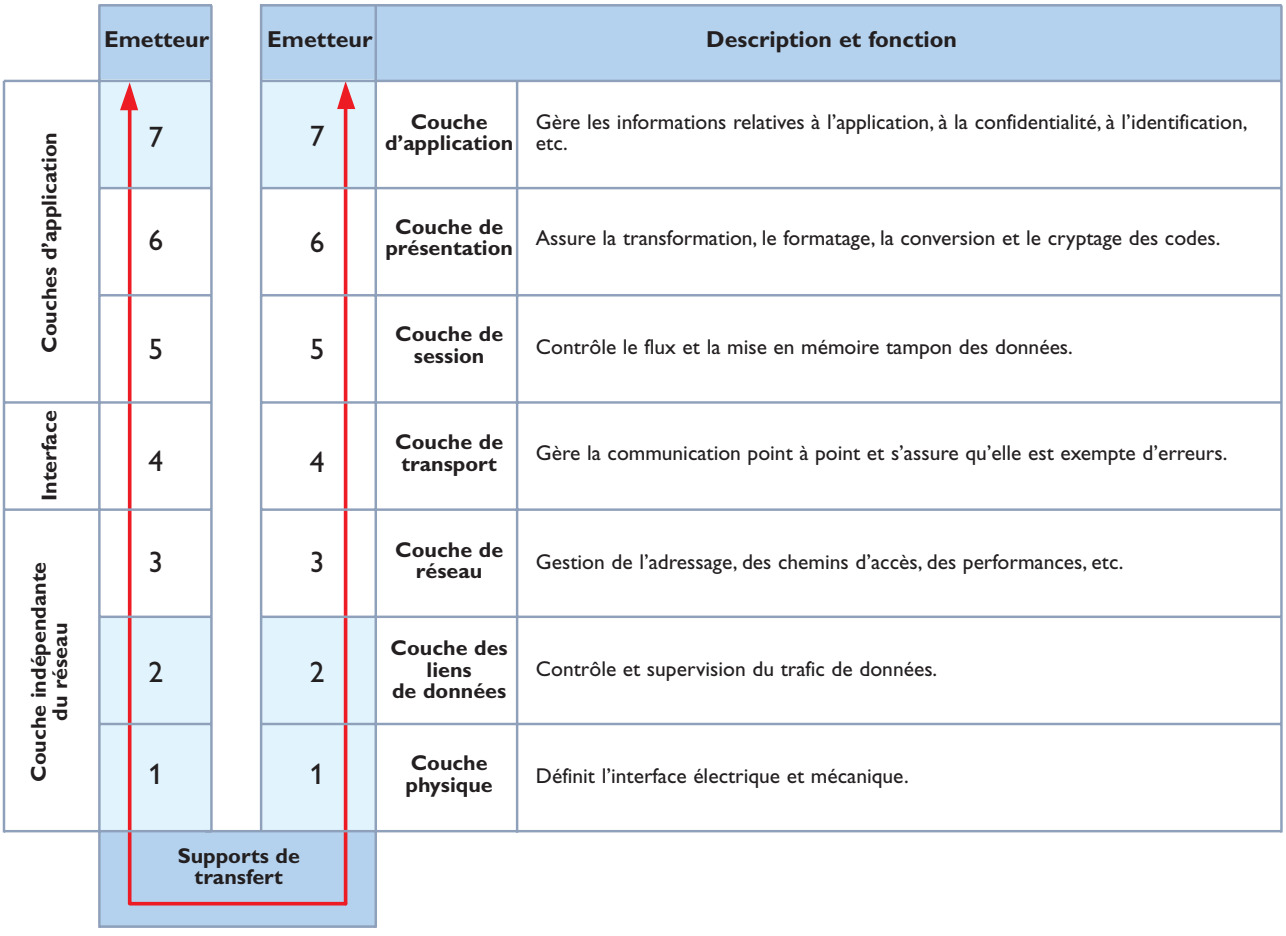
Pour que les systèmes puissent communiquer entre eux, il est nécessaire de créer un cadre structuré permettant d'interconnecter les solutions de fournisseurs individuels. C'est pour cette raison qu'a été créé le modèle OSI (**O**pen **S**ystem **I**nterconnection, interconnexion de systèmes ouverts). Le modèle OSI a été développé par ISO et décrit le fonctionnement de la communication entre deux systèmes. Comme son nom l'indique, son objectif consiste à rendre les systèmes ouverts et, par conséquent, indépendants des fournisseurs. Les systèmes spécifiques à une entreprise empêchent toute communication avec les équipements fabriqués par d'autres entreprises, mais l'utilisation d'un protocole normalisé supprime ces inconvénients. Notez qu'il s'agit d'un modèle et non d'un protocole. Son objectif consiste à concevoir et décrire des réseaux flexibles, robustes et surtout ouverts.

Structure du modèle OSI

En 1983, l'organisation ISO (**I**nternational **S**tandards **O**rganization, Organisation internationale de normalisation) a développé un modèle, OSI, (**O**pen **S**ystem **I**nterconnection Reference Model, modèle de référence pour l'interconnexion de systèmes ouverts) à cette seule fin. Ce modèle définit les pièces, structures et fonctions requises pour la communication et les répartit parmi 7 couches ou niveaux, dans un ordre dépendant des différentes phases du processus de communication.

En termes simplifiés, on peut dire que chaque couche (à l'exception de la couche d'application) fonctionne de manière à communiquer avec la couche adjacente. D'autres informations, à savoir un en-tête, sont ajoutées afin de permettre la communication entre les couches. Elles sont nécessaires pour que la couche sous-jacente puisse interpréter et gérer les données. Lorsque les données aboutissent au récepteur, chaque couche prélève les informations ajoutées (en-tête) dont elle a besoin. Ces informations sont alors transmises à la couche supérieure la plus proche. Quand les informations arrivent à la couche ultime, toutes les données supplémentaires ont été enlevées. Chaque couche communique dès lors avec la couche correspondante sur l'autre ordinateur.

A titre d'exemple, la norme européenne V.24 est une spécification logique dictée par la couche physique. Elle ne définit que la tâche des lignes : contrôle, données et débits de transmission possibles. Voilà pourquoi la norme V.24 est complétée d'une spécification électronique appelée V.28, qui est également un sous-ensemble de la couche physique. V.24 et V.28 ont leur équivalent dans la norme américaine RS-232, qui spécifie l'interface physique et électrique.



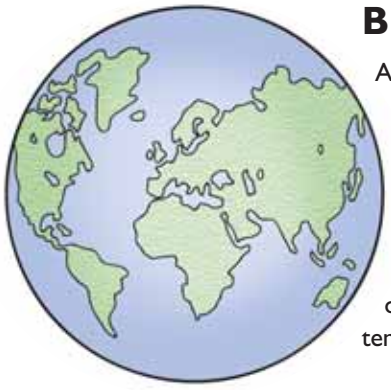
BACK

Comparaison

Pour clarifier l'image de l'OSI, nous pouvons établir une comparaison avec un appel téléphonique ordinaire.

- La couche physique réside dans le réseau téléphonique et dans les définitions des signaux transférés.
- Le contrôle de liaison logique (LLC) de la couche des liens de données correspond au haut-parleur et au microphone du téléphone. Le protocole d'accès au support (Media Access Control, MAC) de la couche des liens correspond aux composants du téléphone qui convertissent les signaux du microphone en signaux que le téléphone peut transmettre au réseau et inversement pour l'utilisateur.
- La couche du réseau correspond à la composition du numéro au clavier.
- La couche de transport peut être comparée à l'appel d'un autre abonné : vous composez son numéro de téléphone puis vous êtes connecté via la couche de transport, qui vous met en contact avec le destinataire.
- La couche de session correspond à l'appel proprement dit.
- La conversation trouve son équivalent dans la couche de présentation.
- La couche d'application correspond à l'ensemble de l'appel.

Communication locale



Bus de terrain

Aujourd'hui, les éléments des systèmes d'automatisation modernes doivent pouvoir communiquer et ce, via des chemins uniformes. Les exigences en termes de communication sont de plus en plus strictes, tant horizontalement, sur le terrain, que verticalement, dans une perspective hiérarchique. Les solutions de communication de données industrielles totalement intégrées impliquent généralement l'ensemble de ces éléments : signaux émis par des sondes, elles-mêmes connectées à des instruments, soupapes, moteurs, etc. Ces composants sous-jacents du système communiquent avec le système de contrôle principal ou des ordinateurs industriels qui exécutent une application.

Nous avons décrit la base du concept, mais en quoi consistent exactement les bus de terrain ?
En termes simples, on peut dire que les bus de terrain sont un peu comme Internet, mais pour l'industrie. Ils permettent essentiellement aux machines et autres équipements d'être mutuellement connectés au sein d'un réseau, de manière à pouvoir communiquer entre eux ainsi qu'avec d'autres systèmes. Lorsque survint l'idée de leur création, à la fin des années quatre-vingt, l'objectif principal était de raccourcir la période d'installation ainsi que le routage des câbles, donc de diminuer les coûts. Peu à peu, cet aspect a perdu de son importance et aujourd'hui, le facteur prépondérant réside davantage dans l'échange d'informations. On peut dire que le bus de terrain de demain sera de plus en plus semblable à Internet, et peut-être même fondé sur une technologie identique.

La normalisation internationale des systèmes à bus de terrain revêt une importance vitale pour leur mode d'acceptation et d'établissement. Intitulée "Digital Data communication for measurement and control. Fieldbus for use in industrial control systems" (Communication de données numériques à des fins de mesure et de contrôle. Bus de terrain destinés aux systèmes de contrôle industriels), la norme IEC 61158 décrit les bus de terrain et se décline en 6 parties.

Document IEC 61158	Sommaire	Couches OSI
61158-1	Introduction	
61158-2	Spécification et définition des services	Couche 1 Physique
61158-3	Définition du service	Couche 2 Lien de données
61158-4	Spécification du protocole	Couche 2 Lien de données
61158-5	Définition du service	Couche 7 Application
61158-6	Spécification du protocole	Couche 7 Application

BACK

Différents bus de terrain

Les communications industrielles utilisent différents supports, tels que les câbles en cuivre, la fibre optique, le transfert infrarouge ou la radiotechnologie. La technologie des bus de terrain a été développée dans le but de remplacer les systèmes précédents par des solutions normalisées. Vu les différents besoins, les divers champs d'application et les solutions propres de certains grands fabricants, le marché propose plusieurs systèmes de bus présentant différentes caractéristiques, et plus ou moins ouverts. Vous trouverez ci-dessous une comparaison exhaustive des bus de terrain les plus courants.

Bus de terrain	Développé par	Norme	Topologie	Supports	Dist. max.	Méthode de communication
PROFIBUS DP/PA	Siemens	EN 50170/ IEC 1158-2	Bus, étoile, anneau	Paire torsadée ou fibre optique	100 m à 12 Mbits/s	Maître/esclave D'égal à égal
INTERBUS-S	Phoenix Contact, Interbus club	DIN19258 EN 50254	Anneau	Paire torsadée ou fibre optique	400 m/ segment 128 km au total	Maître/esclave
DeviceNet	Allen-Bradley ODVA	ISO 11898 ISO 11519	Bus	Paire torsadée	500 m (dépend de la vitesse)	Maître/esclave Multimaître D'égal à égal
LonWorks®	Echelon Corp.		Bus, anneau, boucle, étoile	Paire torsadée ou fibre	2000 m @ 78 kbit/s	Maître/esclave D'égal à égal
CAN ouvert	CAN In. Automatisation	CiA	Bus	Paire torsadée	25 – 1000 m (dépend de la vitesse)	Maître/esclave D'égal à égal Multidiffusion Multimaître
Ethernet	DEC, Intel, Xerox	IEEE 802.3	Bus, étoile,	Paire torsadée ou fibre optique	10/100 Base T 100 mètres	D'égal à égal
Modbus Plus	Modicon		Bus	Paire torsadée	450 mètres par segment	D'égal à égal
Modbus RTU/ASCII	Modicon	EN 1434-3 ICE870-5	Bus	Paire torsadée	1000 mètres	Maître/esclave
Data Highway Plus (DH+)	Allen-Bradley		Bus	Paire torsadée	3000 m	Multimaître D'égal à égal

BACK

PROFIBUS

PROFIBUS est un système de communication numérique uniforme et ouvert, destiné à de nombreuses applications, surtout dans le domaine de l'ingénierie et de l'automatisation des processus. Il est idéal pour les applications rapides à durée critique, ainsi que pour les applications de communication complexes. Les communications PROFIBUS sont basées sur les normes internationales IEC 61158 et IEC 61784, et satisfont dès lors aux besoins des utilisateurs de bus de terrain souhaitant des systèmes ouverts et indépendants du fabricant. Les produits de différents fabricants peuvent en effet communiquer entre eux sans adaptation ni logiciel spécialisé.

Historique

L'historique du système PROFIBUS remonte à 1987, lorsqu'un groupe européen constitué d'entreprises et d'institutions a établi une stratégie visant la réalisation d'un bus de terrain. Ce groupe comptait 21 membres, entreprises, universités, autres institutions et différentes autorités. Leur objectif était de réaliser un bus de terrain série et d'obtenir sa reconnaissance générale ; et dans cette optique, une importante étape intermédiaire consistait à normaliser une interface pour les dispositifs de terrain. Les membres concernés de la ZVEI (Association centrale de l'industrie électrique) ont décidé de soutenir un concept technique commun en matière d'ingénierie et d'automatisation des processus, afin d'aboutir à une norme à grande échelle. La première phase fut la spécification du protocole de communication complexe appelé PROFIBUS FMS (**F**ieldbus **M**essage **S**pecification, spécification des messages du bus de terrain), établi afin de prendre en charge les applications de communication très exigeantes. Un jalon supplémentaire fut franchi en 1993, avec la première spécification du protocole Profibus DP, plus simple et donc beaucoup plus rapide. "DP" signifie **D**ecentralized **P**eripherals (périphériques décentralisés). Ce protocole n'a cessé d'évoluer et existe à présent en trois versions offrant divers degrés de fonctionnalité : DP-V0, DP-V1 et DP-V2. Au-dessus du système DP se trouve le système PROFIBUS PA (**P**rocess **A**utomation, automatisation des processus), spécialement créé pour répondre aux besoins de l'industrie des processus. Motion Control (commande de mouvement) est une version destinée aux équipements d'entraînement et PROFIsafe s'adresse aux applications de sécurité. Ce manuel ne décrira que les applications de type "DP".

Communication PROFIBUS

Le système Profibus repose sur RS-485, qui est probablement la technique de transmission industrielle la plus courante. Il utilise un câble blindé à paire torsadée et peut supporter des débits de transmission de l'ordre de 12 Mbits/s. La récente version RS-485-IS prévoit un support de transmission à 4 fils pour la classe de protection E, destinée aux environnements explosifs.

Débit de données (kbit/s)	Longueur de segment max. (m)
9,6	1200
19,2	1200
45,45	1200
93,75	1200
187,5	1000
500	400
1500	200
3000	100
6000	100
12000	100

Les valeurs renvoient à un **câble de type A** présentant les caractéristiques suivantes :

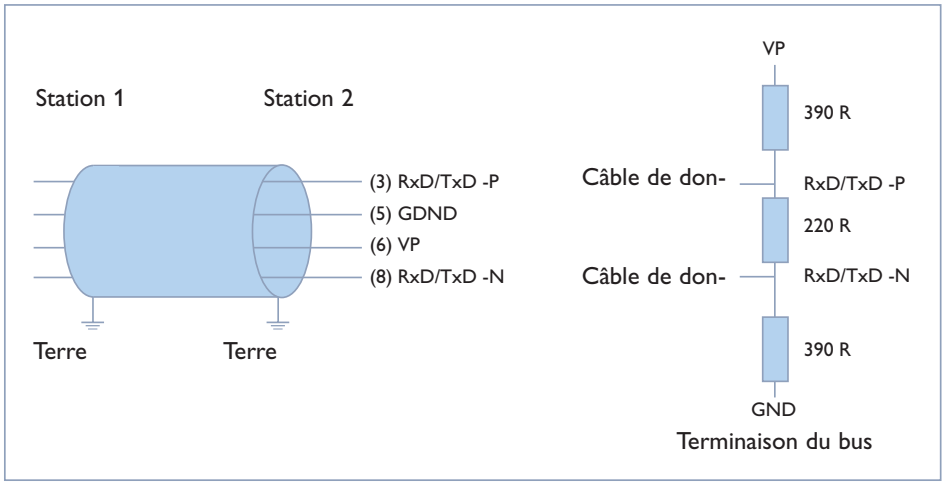
Surtension Impédance	135 – 165 Ω
Capacité	<30 pf/m
Résistance de boucle	110 Ω/km
Diamètre de l'âme	0,64 mm
Section du câble	>0,34 mm²

BACK

La technique de transmission MBP (**M**anchester coded, **B**us **P**owered, fondée sur le code Manchester) s'utilise pour les applications d'automatisation de processus requérant une alimentation via le bus pour les unités situées dans des zones de sécurité intrinsèques. Le transfert de données PROFIBUS par le biais d'un câble en fibre optique est recommandé pour les applications exposées à des interférences électromagnétiques, entre des sites d'installations présentant des potentiels de masse différents, ainsi que pour parcourir d'importantes distances.

Topologie de réseau PROFIBUS

Comme cette topologie utilise l'interface de base RS-485, les dispositifs doivent être connectés selon une structure de type bus. Il est possible de connecter 32 stations à un même segment. Les terminaisons de bus actives se connectent au début et à la fin de chaque segment, comme illustré dans la figure ci-dessous. Les deux terminaisons d'un bus doivent disposer d'une alimentation permanente afin de permettre une communication exempte d'erreurs. Elles sont généralement intégrées dans les connecteurs et activées par



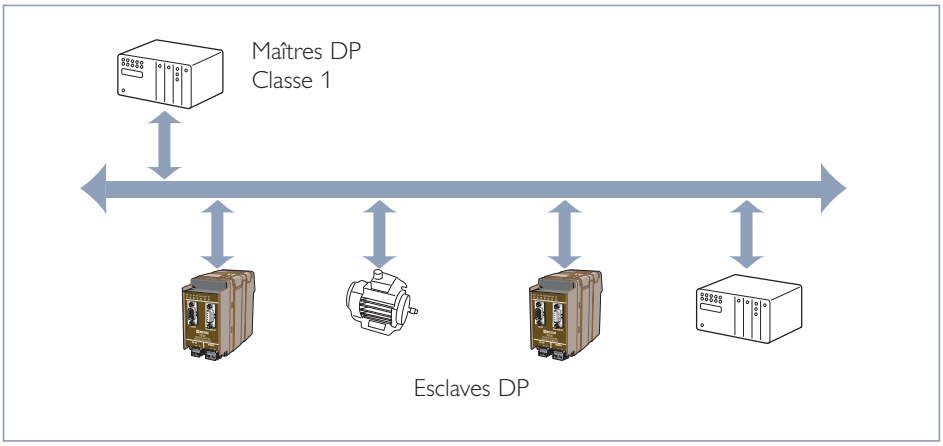
un commutateur. On utilise un répéteur s'il faut connecter plus de 32 stations au même réseau, ou si le réseau présente des distances de transmission supérieures à celles spécifiées au tableau de la page 51. N'oubliez pas qu'un répéteur soumet le réseau à une charge électrique, de sorte qu'un segment doté d'un répéteur ne peut avoir que 31 stations. L'utilisation de répéteurs à régénération permet d'interconnecter jusqu'à 10 segments consécutifs.

BACK

PROFIBUS DP

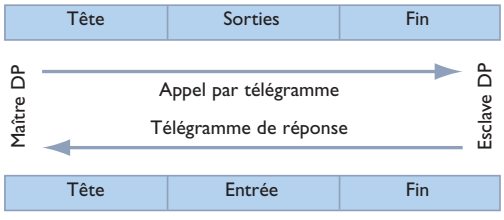
Représente un échange basique, rapide, cyclique et déterministe de données de calcul entre un maître bus et les esclaves qui lui sont affectés. La communication entre le maître et l'esclave est régulée et contrôlée par le maître. Celui-ci réside généralement dans le système de commande programmable central, comme un automate PLC ou un PC industriel.

Maître et esclave



Un esclave est un dispositif de terrain (terminal E/S, équipement d'entraînement, station HMI, soupape, émetteur, instrument d'analyse, etc.) qui lit les informations relatives au processus et/ou utilise les informations sortantes afin de contrôler le processus. Certaines unités se contentent de traiter les informations entrantes ou sortantes sans agir sur le processus. Sur le plan de la communication, les esclaves sont des acteurs passifs qui se bornent à répondre à une demande directe.

Communication des données cycliques entre le DPM1 et les esclaves



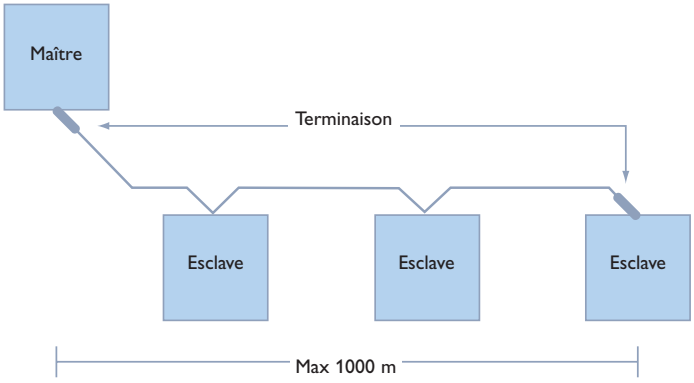
La communication de données entre le DPM1 (Maître DP de classe 1) et ses esclaves s'effectue automatiquement, selon un cycle prédéfini. L'utilisateur attribue les esclaves durant la configuration du système de bus, tout en spécifiant quels esclaves devront être inclus/exclus par rapport à la communication cyclique.

BACK

Modbus

Modbus ASCII et Modbus RTU

Les protocoles Modbus ASCII et Modbus RTU sont devenus la norme de facto dans de nombreuses applications. Réalisé par Modicon à la fin des années 1970, le protocole Modbus fonde la communication sur un réseau multipoint comprenant un maître et plusieurs esclaves. Il n'est pas uniquement destiné aux applications industrielles, mais s'utilise de manière universelle lorsqu'il faut contrôler un processus ou un flux d'informations.



Les dispositifs connectés au Modbus ASCII et au Modbus RTU communiquent en série via le RS-232 ou le RS-485. La principale différence entre les deux est que dans le RTU, chaque octet d'un message contient deux caractères hexadécimaux de 4 bits alors que dans l'ASCII, chaque octet d'un message est envoyé sous la forme de 2 caractères ASCII. Cela signifie que le RTU est plus efficace et peut transférer davantage de données, mais n'est pas tolérant vis-à-vis du paquet de données fragmenté lors de la transmission. Le Modbus ASCII, quant à lui, peut tolérer les lacunes de la transmission, ce qui en fait le protocole de prédilection pour les transmissions par modem.

Le débit de transfert maximal est normalement limité à 19,2 kbit/s. La communication est contrôlée par un maître et ne peut avoir lieu qu'en semi duplex. La communication entre esclaves n'est pas possible.

Le protocole Modbus de base entre un maître et un esclave se compose des éléments suivants :

Adresse	Code de fonction	Données	Correction des erreurs

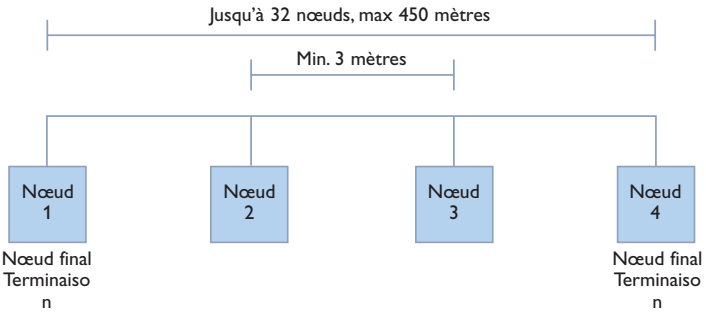
BACK

Modbus Plus

Modbus Plus est un réseau pour applications industrielles utilisant l'échange de jetons et la communication d'égal à égal (peer-to-peer). Ces deux caractéristiques impliquent une communication sur un circuit logique où tous les nœuds peuvent initier une communication. Un nœud ne peut toutefois pas transmettre de données tant qu'il n'a pas obtenu son jeton. Le débit de transfert est de 1 Mbits/s via un câble blindé à paire torsadée. Modbus Plus est un réseau ouvert destiné à l'échange d'informations entre des nœuds du réseau, créant ainsi la possibilité de contrôler et de superviser des processus industriels.

Le réseau est transparent, en ce sens qu'il permet d'atteindre tous les dispositifs du système via le point de connexion.

L'interface est basée sur le système RS-485 et se compose de sections pouvant accueillir 64 nœuds chacune. Il est possible de connecter 32 nœuds directement sur un segment de câble, la distance de transmission maximale d'un segment étant de 450 mètres. Un répéteur peut être installé si des distances plus importantes sont requises ou s'il faut connecter plus de 32 nœuds sur un segment. La longueur de section maximale est de 1.800 mètres ; vous pouvez utiliser un modem à fibres optiques pour les distances plus élevées.



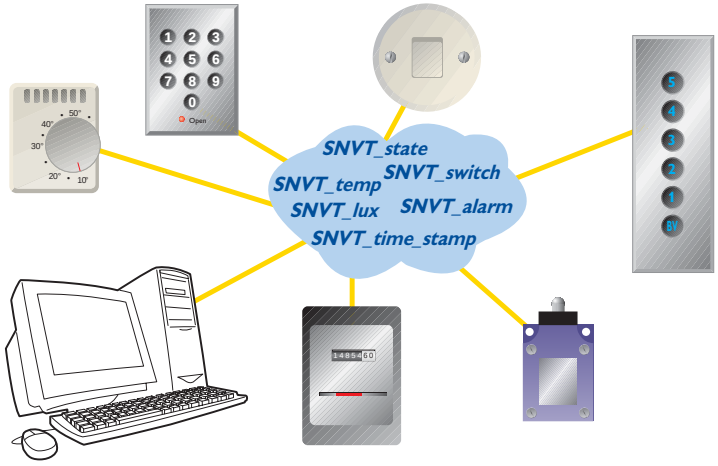
MODBUS/TCP

MODBUS/TCP est une variante de MODBUS, un protocole de communication direct et indépendant du fournisseur, destiné au contrôle et à la supervision des équipements d'automatisation. Ce protocole utilise les propriétés de MODBUS, le support de communication étant le protocole TCP/IP, qui peut transiter par les intranets ou Internet. Il est possible d'encapsuler un paquet Modbus ASCII ou Modbus RTU dans un paquet TCP ou UDP à l'aide d'un serveur série. Il n'en va pas de même pour le protocole Modbus/TCP : en Modbus/TCP, chaque nœud connaît son adresse IP et communique sur le port TCP 502.

BACK

LON®WORKS

L'introduction de la technologie LONWORKS® par la société Echelon® Corporation a fourni une plate-forme complète pour le développement de systèmes ouverts de contrôle distribué, basés sur une architecture de réseau intelligente. Un système LONWORKS® est généralement constitué d'une série d'équipements intelligents appelés nœuds, qui accomplissent chacun une tâche spécifique, par exemple la mesure de la température ou la régulation d'une vanne. Les nœuds échangent entre eux des informations essentielles via le réseau. Un réseau de contrôle basé sur cette intelligence distribuée est appelé 'architecture d'égal à égal' ('peer-to-peer'). Normalement, les nœuds ne s'envoient pas de commandes les uns aux autres mais échangent des paquets de données contenant des informations sur la



LONWORKS® – un réseau orienté-données

température, la pression, le statut, la date, l'heure, etc. Les nœuds peuvent ensuite utiliser les informations des paquets de diverses manières selon leur fonction spécifique. Au sein de LONWORKS®, ces paquets de données peuvent être considérés comme des variables globales disponibles sur le réseau ; c'est pourquoi on les appelle des variables de réseau. Lorsqu'un nœud met à jour une variable, l'information est automatiquement communiquée à l'ensemble du réseau pour que les autres nœuds soient informés. L'interopérabilité est un mot clé de la technologie LONWORKS®. L'une des conditions de l'interopérabilité est que les nœuds provenant de différents fabricants doivent pouvoir échanger et interpréter les données sans requérir d'adaptations particulières des logiciels ou du matériel. Pour se conformer à cette exigence, il ne suffit pas d'être sur le même réseau, d'avoir le même type d'émetteur ou de pouvoir envoyer des variables de réseau. Les nœuds doivent également comprendre le contenu des variables de réseau. A titre d'exemple, ils doivent savoir

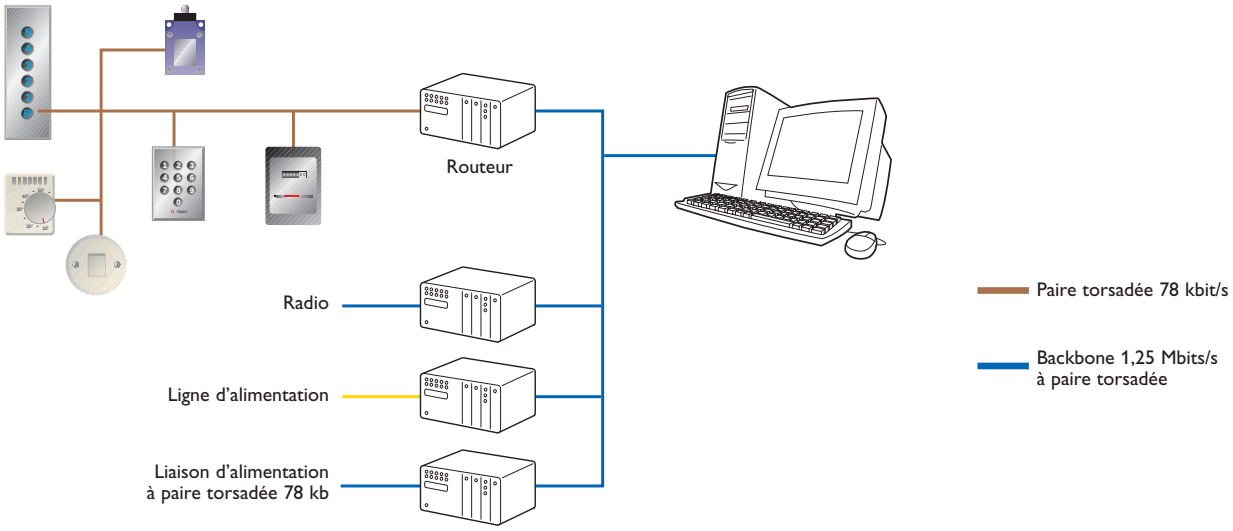
BACK

si une température est exprimée en degrés Fahrenheit ou Celsius, ou si un débit est exprimé en litres/seconde ou millilitres/seconde. Il importe donc de définir des normes spécifiant le mode d'interprétation du contenu de ces paquets de données. Au sein de LonWorks®, la normalisation est gérée par une organisation appelée l'Association LonMark®. Il s'agit d'une association indépendante constituée de fabricants de nœuds LonWorks®, d'intégrateurs de systèmes et d'utilisateurs finaux, qui ont établi une liste de types normalisés de variables de réseaux. Ces types sont désignés par l'acronyme 'SNVT' (à prononcer 'snivit'), qui signifie "**S**tandard **N**etwork **V**ariable **T**ypes" (types standard de variables de réseaux). Ces types contiennent des informations sur le dispositif, la résolution et les valeurs possibles pour le type. A titre d'exemple, si le type SNVT_speed est utilisé, tous les nœuds LonWorks® sauront que l'unité est le mètre/seconde, que la résolution est de 0,1 mètre/seconde et qu'il peut accepter les valeurs comprises entre 0 et 6553,5 mètres/seconde.

L'émetteur/récepteur le plus souvent utilisé est le FTT-10A à topologie libre, qui communique selon un débit de 78 kbit/s via un câble à paire torsadée. La topologie libre signifie qu'il peut être utilisé dans les réseaux en étoile, les réseaux à bus ou les combinaisons des deux. Echelon® propose également un émetteur/récepteur à topologie libre appelé LPT-10 LinkPower. Il est compatible avec le FTT-10A sur le plan du signal et peut être utilisé en combinaison avec lui. La particularité du LPT-10 réside dans le fait qu'il s'agit d'un "véritable système à 2 fils", dans ce sens que le fil transfère à la fois les données et l'alimentation. Comme ils permettent une libre combinaison des topologies, ces appareils sont extrêmement utiles dans les réseaux de contrôle actuels, où l'ajout de nouveaux dispositifs doit être aisé. Un autre avantage réside dans le fait qu'ils présentent une connexion insensible aux polarités, qui facilite l'installation et élimine les risques de connexions incorrectes. Parmi les autres émetteurs/récepteurs d'Echelon® figurent l'émetteur/récepteur à paire torsadée de 1.250 kbit/s pour la topologie en bus, ainsi qu'un émetteur/récepteur destiné à la communication avec les réseaux électriques. La possibilité d'alterner entre deux bandes de fréquences, le traitement avancé du signal et la correction des erreurs permettent à l'émetteur/récepteur du réseau électrique de gérer aisément les interférences de moteurs, variateurs, PC et télévisions, par exemple.

L'émetteur/récepteur PLT-22 peut être configuré de manière à communiquer via le réseau électrique sur la bande de fréquences publique Cenelec-C ou la bande de fréquences Cenelec-A, réservée aux compagnies électriques. La bande C est généralement utilisée pour les applications de logement intelligent et autres applications commerciales, tandis que la bande A est souvent affectée au relevé des compteurs électriques. Il existe également des émetteurs/récepteurs tiers pour les communications fibre optique, radio et IR. Il n'est pas rare qu'un réseau LonWorks® combine différents supports. Echelon® propose des routeurs pouvant transférer des données LonTalk® de différentes manières d'un support à un autre. Relativement fréquente, la connexion de canaux à support lent avec un

BACK



backbone doté d'un support plus rapide permet d'obtenir une segmentation logique et physique du réseau, afin d'améliorer les performances et la sécurité.

Considérations relatives aux réseaux LonTalk® étendus

L'augmentation de la distance de transmission entre deux ou plusieurs segments TP/FT via un câble à fibre optique entraîne un léger retard dans la communication entre les différents segments. Cela peut entraîner des collisions, qui débouchent à leur tour sur la retransmission du paquet de données, laquelle peut nuire aux performances du réseau. Nous recommandons dès lors de ne pas dépasser 25 km pour la longueur globale de la fibre. La norme EIA-709.3 autorise un délai maximum de 36 ms, ce qui correspond à une distance de transmission de 6,8 km. Nous recommandons l'utilisation de notre routeur LR-11 pour assurer la communication sur des distances plus élevées, plusieurs segments de réseau ou davantage de nœuds à 1.250 kbit/s. Quoi qu'il en soit, nous recommandons toujours d'analyser la communication sur le réseau par le biais d'un analyseur de protocole LonWorks®.

BACK

Connexions à distance

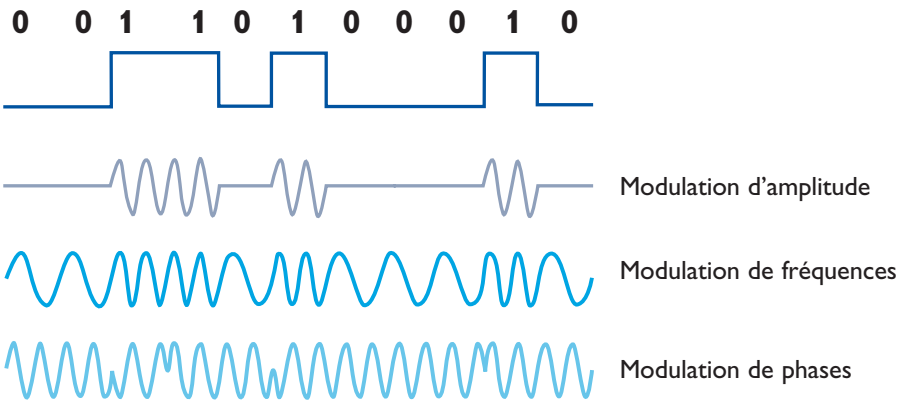
Lignes RTC

Transmission de données via le réseau téléphonique

La communication à distance offre un complément précieux à la transmission locale de données. Elle permet, en effet, de se connecter à des sources de données distantes afin de trouver des informations sur les marchés, les cotes de la bourse ou les registres publics, par exemple. Le nombre de sources de données s'est considérablement accru ; elles sont en outre souvent reliées par le biais de réseaux mondiaux. Ainsi, vous pouvez très bien vous connecter à une source de données dans un pays et vous retrouver dans une source internationale de données financières à New York. Il existe de nombreuses raisons pour effectuer des transmissions de données distantes, par exemple la nécessité de vous connecter à l'ordinateur de votre société via le réseau téléphonique pendant que vous travaillez sur site. Aujourd'hui, un ordinateur portable est souvent une combinaison d'ordinateur, de modem, de GSM et de fax.

Connexion par numérotation

Le principe de la transmission distante via le réseau téléphonique consiste à appeler le modem du destinataire, qui répond, puis les deux modems établissent une porteuse via la ligne téléphonique. Dès que les modems perçoivent leurs porteuses mutuelles, ils se verrouillent ou procèdent à une synchronisation. Les débits de transfert via le réseau téléphonique ont augmenté, et atteignent couramment 2.400 à 56.000 bits/s. Le débit n'est pas uniquement limité par le modem mais aussi par la ligne téléphonique, dont la qualité dépend en grande partie de la distance, du nombre de centraux et des relais. La plupart des modems à haute vitesse offrent une possibilité d'actualisation automatique afin de maintenir une transmission de bonne qualité. La communication par modem exige le respect de certaines normes, étant donné que l'émetteur et le récepteur proviennent souvent de fabricants différents. Le tableau de la page 69 présente les débits binaires associés à des normes spécifiques.



Modulation

Le terme "modem" est une abréviation des termes "modulation" (conversion du signal) et "démodulation" (régénération du signal d'origine). Les signaux de données doivent être convertis et adaptés pour être transférés via divers types de câbles. Les différents niveaux des signaux numériques (uns et zéros) sont convertis en transformations compréhensibles pour le câble choisi. Il existe trois types de modulations fondamentales. La modulation de fréquences utilise différentes fréquences pour représenter les uns et les zéros. La modulation de phases, quant à elle, utilise la variation de phases d'une porteuse pour représenter les uns et les zéros. Enfin, la modulation d'amplitude utilise le niveau du signal, ou les pics d'amplitude, afin de créer des uns et des zéros lisibles. La combinaison de ces types de base permet de réaliser des techniques de modulation plus complexes.

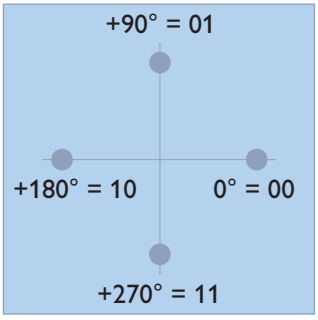
BACK

Le bit/s est-il l'équivalent du baud ?

Le débit de transfert d'un modem télécom s'exprime en bits/s (débit binaire) et en bauds (vitesse de transfert). Cette dualité a généré une certaine confusion, qui demande explication.

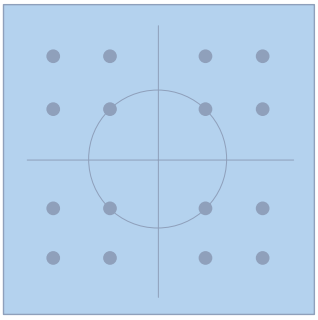
Débit binaire = Nombre de bits transmis via l'interface série par seconde ; exprimé en bits/s

Vitesse de transfert = Nombre de combinaisons de signaux transmises via l'interface de ligne par seconde; exprimé en bauds



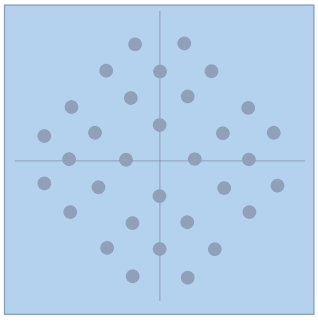
Pour accroître le débit de transfert sur un modem télécom, des bits supplémentaires sont modulés ensemble et transférés via le réseau téléphonique. L'exemple ci-contre illustre la technique de modulation de phases, pour laquelle deux bits sont décrits par la variation de phase du signal de ligne (V.22).

Dans l'exemple ci-contre, le débit binaire s'élève à 1.200 bits/s et la vitesse de transfert, à 600 bauds.



La modulation simultanée de signaux supplémentaires permet d'atteindre un débit de transfert plus élevé. Certaines normes, par exemple V.22bis, combinent la modulation d'amplitude et de phases (technique appelée QAM, "**Q**uadrature **A**mplitude **M**odulation", modulation d'amplitude en quadrature), ce qui débouche sur le transfert de 4 bits pour chaque modulation.

Dans l'exemple ci-contre, le débit binaire s'élève à 2.400 bits/s et la vitesse de transfert, à 600 bauds.



Les normes telles que V.32 fondent la modulation sur une technique appelée TCM (**T**rellis **C**ode **M**odulation, modulation par codage en treillis), qui correspond à QAM mais comprend un bit supplémentaire pour la correction des erreurs. Ce bit est nécessaire lorsque la frontière entre les combinaisons de bits transférés diminue, imposant des besoins plus prononcés en termes de correction des erreurs.

Dans l'exemple ci-contre, le débit binaire s'élève à 9.600 bits/s et la vitesse de transfert, à 2.400 bauds.

BACK

Exemples de normes

Norme	Débit binaire	Semi/ Intégral	Vitesse de transfert	Nb de bits	Modulation
V.21	300 bits/s	FDX	300 bauds	1 bit/baud	FSK
V.22	1200 bits/s	FDX	600 bauds	2 bits/baud	DPSK
V.22bis	2400 bits/s	FDX	600 bauds	4 bits/baud	QAM
V.23	1200 bits/s	FDX	1200 bauds	1 bit/baud	FSK
V.32	9600 bits/s	FDX	2400 bauds	4 bits/baud	TCM
V.32bis	14400 bits/s	FDX	2400 bauds	7 bits/baud	TCM
V.34	Jusqu'à 33600 bits/s	FDX	Jusqu'à 3429 bauds	*)	TCM
V.90	Jusqu'à 56000 bits/s	FDX FDX	Jusqu'à 8000 bauds	*)	PCM

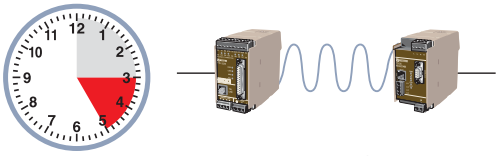
*) Le débit symbole est négocié durant le contrôle du flux (handshaking)

V.90

V.90 est une norme de modem intéressante, car elle offre des débits de transfert potentiellement élevés, via l'utilisation de la norme de communication partiellement numérique PCM (**P**ulse **C**ode **M**odulation, modulation par codage d'impulsions). Cette norme a été plus particulièrement réalisée afin de permettre aux utilisateurs de se connecter sur Internet, et n'offre dès lors pas un transfert symétrique. En effet, la vitesse ascendante vaut à peine 9600 bits/s, tandis que la vitesse descendante peut atteindre 56,0 kbit/s dans des circonstances favorables. L'autre complication réside dans le fait que les fournisseurs de services Internet doivent utiliser des modems spéciaux pour permettre la connexion d'un modem V.90. Cela signifie que deux modems V.90 standard interconnectés ne se connectent pas sous V.90, mais plus probablement sous V.34bis, assurant dès lors une liaison à 33,6 kbit/s dans les deux directions.

BACK

Connexion



Lorsqu'une connexion est établie par le biais d'un modem, la négociation est effectuée afin de déterminer le débit de transfert des données ainsi que le niveau de correction des erreurs. Les spécifications ci-dessous indiquent le délai de connexion entre deux modems pour différentes valeurs de protocoles. Cette mesure montre que le débit le plus rapide n'est pas toujours le plus efficace. Le délai de connexion est le facteur clé lorsqu'il faut appeler plusieurs appareils pour ne transférer qu'une faible quantité de données.

Protocole connexion	Délai de
V.32 bis correction d'erreur	16 s
V.32 bis	13 s
V.22 bis correction d'erreur	12 s
V.22 bis	7 s
V.23	6 s
V.21	7 s

Langage des modems télécom

Pour configurer une connexion, il faut un terminal ou un ordinateur doté d'un logiciel de communication utilisant le port série afin de communiquer avec le modem. Les commandes du modem télécom requièrent des instructions. Hayes Microcomputer Products a développé un jeu de commandes qui fait désormais office de norme, à savoir les "commandes Hayes®". Il s'agit d'un jeu de commandes pour modems télécom qui peuvent être transmises manuellement, à partir du clavier d'un ordinateur, ou automatiquement à partir d'un périphérique connecté offrant différentes configurations.

Correction d'erreurs et compression

La plupart des modems télécom communiquent entre eux de manière synchronisée, même si la communication entre l'ordinateur et le port série est asynchrone et n'assure donc qu'une simple compression des données. Pour vérifier la fiabilité, les données peuvent être scindées en plusieurs blocs associés chacun à une somme de contrôle ('checksum'). Si une perturbation survenue en cours de transfert modifie cette somme de contrôle, le récepteur demande à recevoir le bloc une nouvelle fois. C'est ce qu'on appelle l'ARQ (**A**utomatic **R**epeat re**Q**uest, demande de répétition automatique) et la méthode la plus courante pour ce faire réside, conformément à ITU-T, dans la correction d'erreur V.42, qui est prise en charge par le protocole MNP (**M**icrocom **N**etworking **P**rotocol, protocole de mise en réseau Microcom) et la procédure LAPM (**L**ink **A**ccess **P**rocedure for **M**odems, procédure d'accès à la liaison pour les modems).

ARQ et MNP

MNP Niveau 1 :
protocole asynchrone, semi-duplex

MNP Niveau 2 :
protocole asynchrone, duplex intégral. Données divisées en blocs. La vitesse de transmission effective est légèrement inférieure à la normale.

MNP Niveau 3 :
protocole synchrone, duplex intégral. Données en blocs. Vitesse supérieure de 10% avec transmissions sans erreurs.

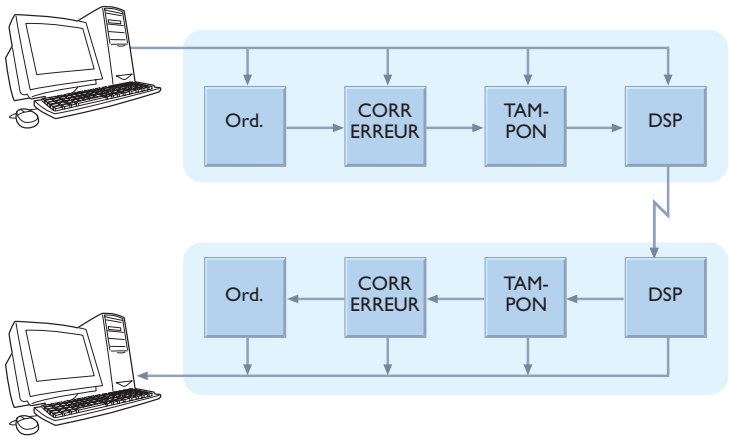
Recherche et transfert de fichiers

L'utilisation d'un modem télécom vous permet de vous connecter à d'autres ordinateurs, directement ou indirectement par le biais d'un réseau. Internet est très vite devenu le plus vaste réseau mondial, totalisant jusqu'à 250 millions d'utilisateurs. Basé sur le protocole Internet TCP/IP, il offre d'innombrables possibilités : courrier électronique, groupes de discussion, World Wide Web (bases de données, information et marketing), téléchargement et envoi de fichiers, téléphonie, vidéoconférence, 'chatting', etc. Les modems donnent toutefois accès à d'autres réseaux et services comme MEMO, Lotus Notes, Compuserve, etc. Les modems télécom favorisent également le télétravail et permettent de connecter les ordinateurs de l'entreprise par le biais de téléphones portables (GSM).

BACK

Les autoroutes de demain

Des travaux intensifs sont en cours afin de créer des normes internationales et de stimuler l'expansion de ce que l'on considère comme les futures autoroutes de la communication : les réseaux numériques à grande vitesse, comme ceux à large bande, qui peuvent transférer d'importantes quantités d'informations (données, audio, vidéo,...) par-delà les continents. La capacité élevée du réseau de télévision par câble peut également contribuer à l'accélération du trafic de données. Nous sommes convaincus que pour être efficaces, ces 'autoroutes' doivent démarrer entre nos quatre murs, en offrant des performances élevées pour la transmission de données locales. Cette infrastructure de base permettra ensuite de construire des routes d'accès vers les réseaux nationaux et mondiaux.



Lignes louées

Il s'agit d'un circuit connecté en permanence et fourni par une société de télécommunication, de manière à assurer les transmissions point à point ou multipoint (V.23) sur de longues distances. Contrairement à une liaison commutée, nous avons ici un circuit connecté en permanence entre deux points. Cette liaison peut passer par un central ou non (connexion câble directe). Bien entendu, les modems télécom dotés d'une fonction 'ligne louée' peuvent aussi utiliser des câblages de données standard. La communication en duplex intégral peut être réalisée via un câble à 2 ou 4 fils. Les modems de Westermo appliquent diverses normes jusqu'à V.90, qui supporte un débit maximal de 56,0 kbit/s. L'un des modems est configuré comme modem appelant et l'autre comme modem appelé. Les données peuvent être transférées en continu dès qu'une connexion a été établie.

La voie de communications la plus rapide passe toujours par ce qu'on appelle le mode direct. Chaque stade de compression, de correction d'erreur et de mise en mémoire tampon génère un délai.

MNP Niveau 4 :
données en blocs dont la taille dépend de la qualité de la ligne. Blocs plus petits que ceux du Niveau 3, d'où une transmission 20% plus rapide s'il n'y a pas d'interférences.

MNP Niveau 5 :
comme pour le Niveau 4, mais avec une compression de données pouvant doubler la vitesse.

MNP Niveau 10 :
amélioration de MNP 5, qui contrôle la ligne de manière dynamique et garantit une transmission sans erreurs.

BACK

V.23 sur une ligne louée

V.23 est une ancienne norme qui avait été initialement conçue pour les lignes louées. Ses débits de transfert sont normalisés à 600 et 1.200 bauds. Les modems conformes à la norme V.23 présentent généralement les fonctions suivantes minimum :

- Vitesses de modulation jusqu'à 600 ou 1200 bauds.
- Modulation de fréquences (FSK)

Ce système utilise deux modulations de fréquences différentes :

- Mode 1 : 600 bauds 1300 Hz–1700 Hz
- Mode 2 : 1200 bauds 1300 Hz–2100 Hz

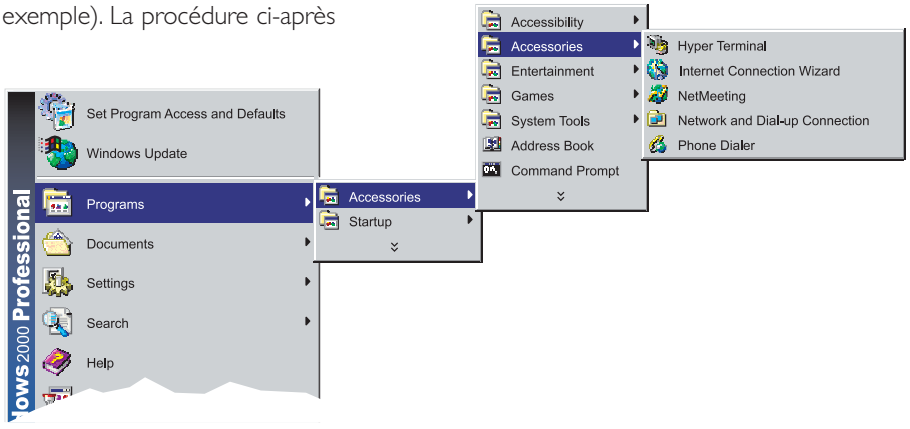
V.23 permet normalement d'établir des liaisons jusqu'à 6 points sur un câble à 2 fils. Le nombre maximal de modems sur une ligne dépend néanmoins de leur mode d'installation, car les problèmes d'impédance sont fréquents. L'impédance de la ligne pour V.23 devrait être de 600 ohms.

Modem Westermo V.23

Le modem Westermo V.23 (TD-23) prend en charge toutes les vitesses jusqu'à 1200 bauds. La ligne peut être terminée par une résistance de 600 ohms et tous les niveaux (onde porteuse, transmission, réception, etc.) sont ajustables.

Utilisation de HyperTerminal

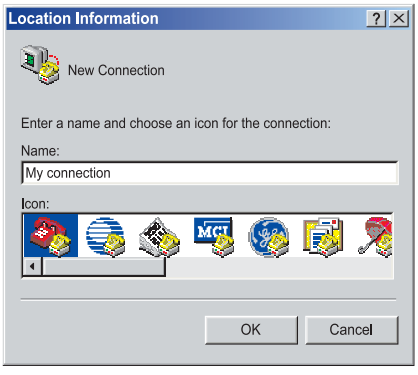
La configuration d'un modem requiert souvent un logiciel d'émulation série. L'une des applications les plus fréquemment utilisées est HyperTerminal de Windows (Windows XP dans notre exemple). La procédure ci-après vous explique comment utiliser HyperTerminal pour communiquer avec un modem :

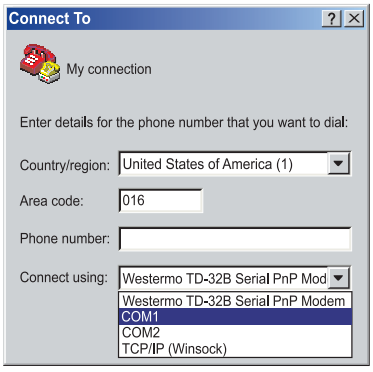


1. Connectez le modem au port série de l'ordinateur à l'aide d'un câble modem.
   Dans cet exemple, il s'agit du port Com 1. Nous utiliserons un câble droit complet à 9 pos., étant donné que l'ordinateur est un DTE et le modem, un DCE (voir page 26).

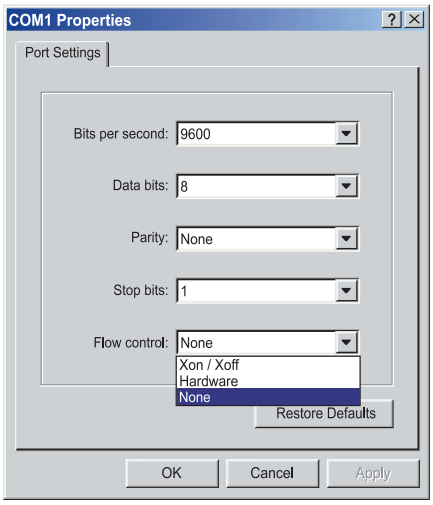
2. Démarrez HyperTerminal. Cette application se situe normalement sous Accessoires/Communications.

3. Nommez la connexion, par ex. Com 1 9600 8N1
   (pour Com 19,6 kbit/s, 8 bits de données, pas de parité (N) et 1 bit d'arrêt)





4. Dans la liste déroulante, sélectionnez le port de communication connecté au modem.
   - Dans cet exemple, il s'agit de COM1.
   - Une fois COM1 sélectionné, les champs du pays, de l'indicatif régional et du numéro de téléphone sont automatiquement désactivés (affichage grisé).
   - Cliquez sur OK.

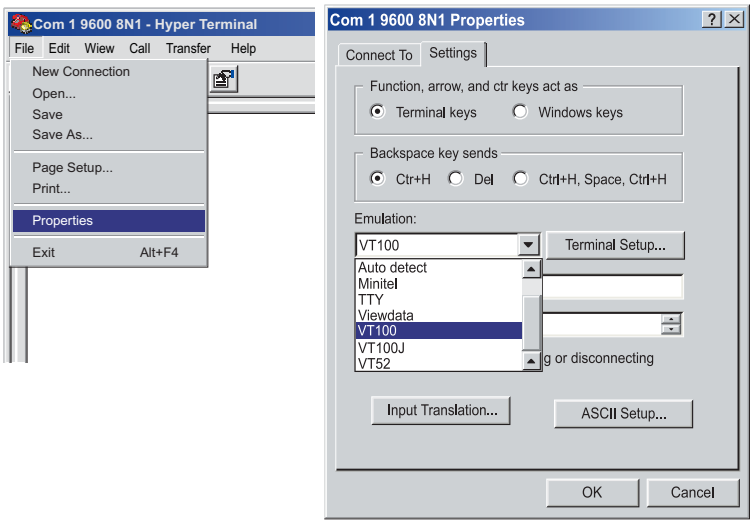


5. Spécifiez les paramètres du port de communication, à savoir la vitesse de communication, le nombre de bits de données, la parité, le nombre de bits d'arrêt et le contrôle de flux. Dans cet exemple, sélectionnez les valeurs suivantes :
   - Bits par seconde 9600
   - Bits de données 8
   - Parité Aucun (N)
   - Bit d'arrêt 1

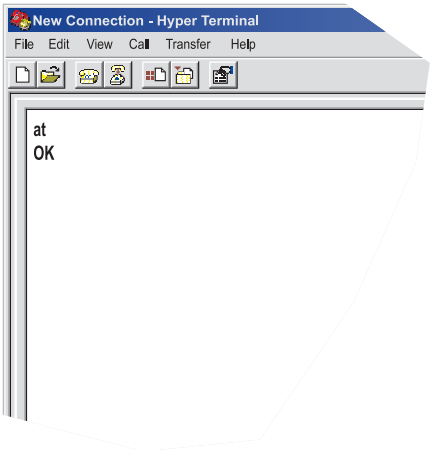
La valeur du contrôle de flux indique comment ce dernier est effectué entre le modem et le PC.
   - "Xon/Xoff" indique un contrôle par le logiciel.
   - "Matériel" désigne un signalement avec RTS/CTS.
   - "Aucun" signifie que le contrôle de flux est désactivé.

BACK

6. HyperTerminal est à présent configuré. Vous pouvez définir d'autres paramètres via l'option Propriétés du menu Fichier. La fenêtre qui s'affiche vous permet notamment d'émuler différents terminaux tels que VT100. Le bouton "Configuration ASCII", quant à lui, vous permet de spécifier les conditions relatives aux caractères, à la ligne entrante et à l'écho local.



7. HyperTerminal est prêt à l'emploi. Comme le modem télécom utilise des commandes AT pour la configuration, vous pouvez vérifier si le contact a été établi en tapant :
   - AT puis en appuyant sur <Retour>
   - Le modem devrait répondre "OK".



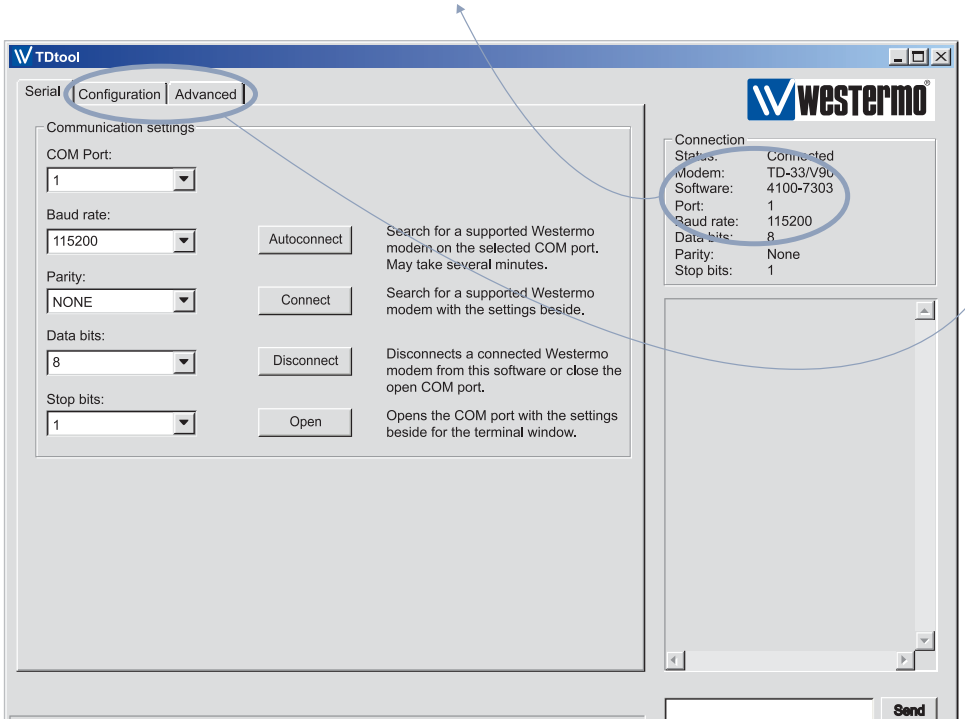
OK est le code de résultat utilisé par le modem pour indiquer que la commande a été exécutée ; la commande définit automatiquement la vitesse, le nombre de bits, la parité et le bit d'arrêt du modem.

La connexion est à présent établie entre HyperTerminal et le modem, et vous pouvez configurer le modem. N'oubliez pas de tenir compte des propriétés de communication utilisées par le modem dans l'application finale.

BACK

TDtool

L'une des options de configuration de nos modems réside dans l'utilitaire TDtool, une application qui détecte automatiquement le modem connecté et facilite sa configuration.



L'application lit les paramètres de configuration pour le modem connecté. Cette opération concerne les paramètres en cours ainsi que les éventuelles options de configuration. Vous les trouverez sous les onglets Configuration et Advanced.

TDtool peut être téléchargé depuis notre site Web.

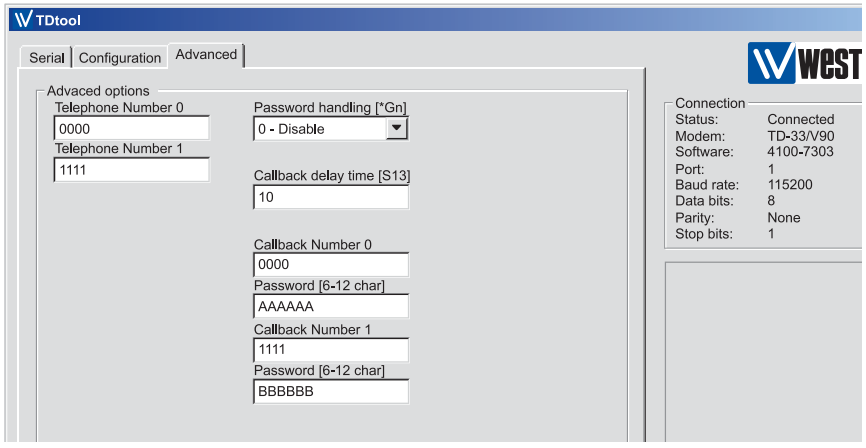
BACK

Dans nos exemples, nous avons connecté TDtool à deux types de modems. Les saisies d'écran montrent comment l'application s'adapte en fonction du modem connecté.

Option 1) A TD-33

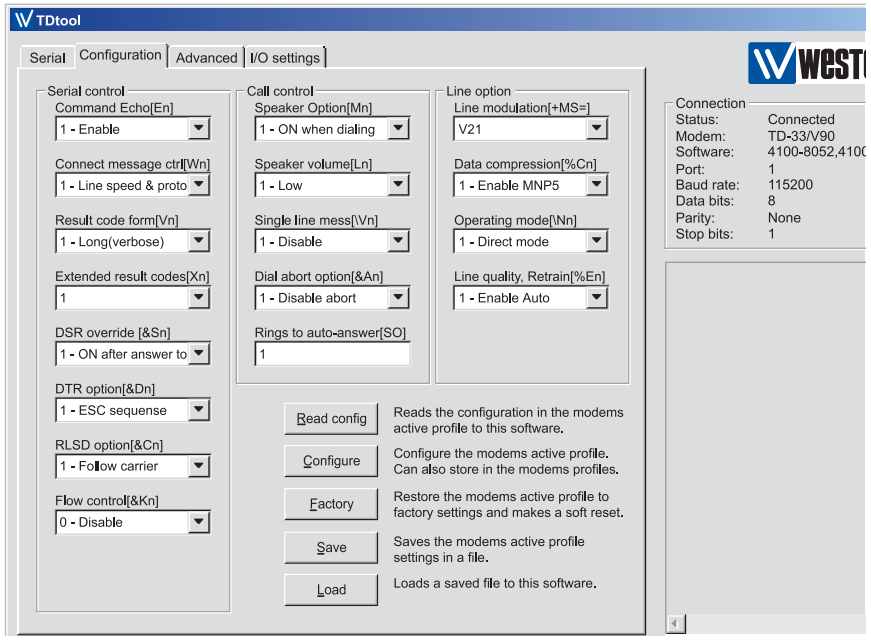
Option 2) A TD-34, modem pouvant notamment envoyer des messages SMS.

L'onglet Advanced de TD-33 vous permet d'introduire le numéro de téléphone pour les rappels ainsi que le mot de passe requis.



Option 1 TD-33

L'onglet Advanced de TD-34 présente d'autres options de configuration, notamment celle permettant de paramétrer les SMS.



Option 2 TD-34

TDtool est un excellent complément à des utilitaires tels que HyperTerminal, car il simplifie la configuration des modems télécom. Lorsque tous les paramètres ont été définis, ils sont téléchargés vers le modem ou enregistrés dans un fichier texte.

Commandes AT

Un modem télécom fonctionne sous deux modes :

- Le mode de commande.
- Le mode de communication.

Le mode de commande vous permet de configurer votre modem de sorte qu'il fonctionne avec votre application. Le mode de communication est le mode actif lorsque le modem est connecté à un autre modem et échange des données.

Comme expliqué précédemment, Hayes Microcomputer Products a développé un jeu de commandes qui fait désormais office de norme, à savoir les "commandes Hayes®". Ces commandes s'utilisent en partie pour configurer le modem et en partie pour établir une connexion.

Comme les commandes AT sont devenues une norme pour les modems télécom, leur mode d'utilisation présente d'importantes similitudes. Il convient toutefois de noter que le perfectionnement d'un modem par rapport à un autre peut entraîner des différences. Les paragraphes qui suivent décrivent certaines des commandes essentielles à nos modems. Pour des informations plus détaillées, veuillez consulter les manuels d'installation respectifs.

ATA – **A**nswer (réponse)

Induit un modem en mode de commande à répondre à un appel entrant. Le modem effectue la négociation afin d'établir une connexion. Une fois la connexion établie, les modems passent en mode de communication.

ATDn – **D**ial (numérotation)

Induit un modem en mode de commande à initier un appel. (n) correspond généralement au numéro de téléphone mais il existe divers autres codes, par exemple pour générer une pause durant la composition d'un numéro si le modem doit attendre une tonalité via un standard. Une fois la connexion établie, les modems passent en mode de communication.

ATH – **H**ang-Up (raccrocher)

Le modem termine la connexion et raccroche. Pour utiliser cette commande, il est nécessaire de faire passer le modem du mode de communication au mode de commande, généralement via le code +++.

AT&Fn – Restore **F**actory Configuration (rétablir la configuration d'usine)

Rétablit les paramètres d'usine du modem, ou le profil de configuration 0 ou 1.

ATQn – **Q**uiet Result Code Control (indication des codes retour)

Activation ou désactivation des codes de résultats envoyés par le modem. Certaines applications demandent que le modem soit configuré de manière à ne pas transmettre de caractères.

ATEn – Echo on/off (écho actif/inactif)

Active/désactive l'écho vers un terminal connecté. Cette fonction est nécessaire pour certaines applications et peut également générer une confusion lors de l'introduction de commandes.

AT&V – Display Current configuration and Stored Profiles (affichage de la configuration active et des profils enregistrés)

Cette commande affiche le contenu des profils et des registres-S enregistrés dans le modem, lesquels sont utilisés pour la configuration des fonctions. Voir l'exemple à la page 80.

AT&Wn – Store Current Configuration (enregistrer la configuration active)

Enregistre la configuration active dans le modem sous le profil 0 ou 1.

ATZn – Soft Reset and Restore Profile (profil de redémarrage et de restauration des logiciels)

Le modem fait l'objet d'un redémarrage logiciel, il est ramené au profil configuré.

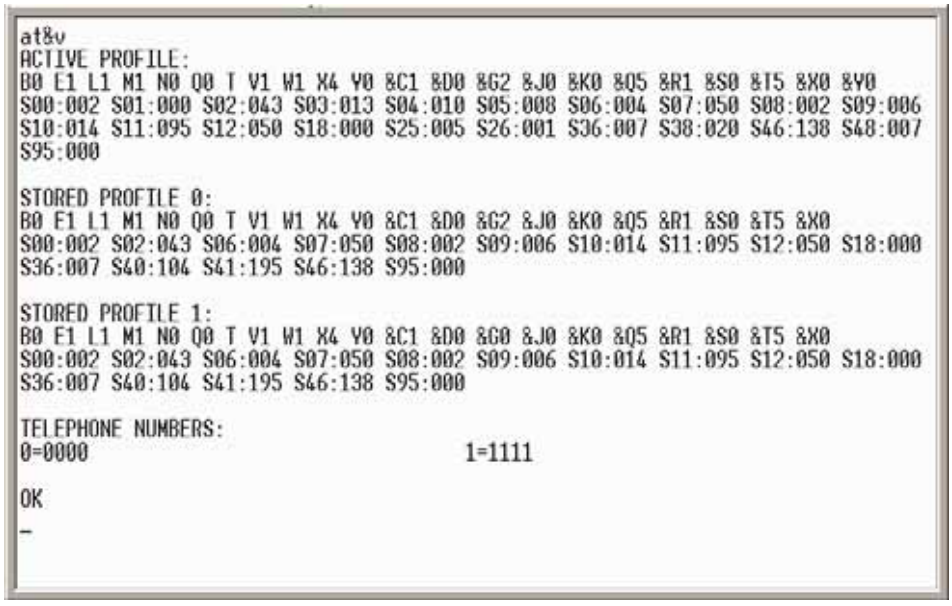
ATO – On Line Data Mode (mode de données en ligne)

Le modem passe au mode de données en ligne.

+++ Permet de passer du mode de données en ligne au mode de commande.

BACK

Saisie d'écran illustrant le contenu des registres du modem. Les spécifications complètes des registres figurent dans le manuel du modem. L'exemple ci-dessous décrit quelques fonctionnalités des registres-S



Registre	Fonctionnalité
S00	Le contenu du registre indique au modem après combien de sonneries il doit répondre. Dans cet exemple, le modem répondra après la deuxième sonnerie, étant donné que la valeur est réglée sur 002.
S01	Compte le nombre de sonneries entrantes.
S02	Indique le caractère à utiliser pour la séquence d'échappement.
S03	Indique le caractère à utiliser pour le retour chariot.
S04	Indique le caractère à utiliser pour le saut de ligne.
S05	Indique le caractère à utiliser pour le rappel arrière.
S07	Indique pendant combien de secondes le modem doit attendre la porteuse avant de raccrocher.
S10	Indique le délai d'attente observé par le modem avant de raccrocher en cas de perte de la porteuse.

Vitesses plus élevées

xDSL

xDSL est le nom collectif d'une famille de technologies utilisant des modems numériques sur une ligne téléphonique standard ou fixe. La lettre remplaçant le x correspond au type de système numérique transmis sur la ligne (exemples : ADSL, SDSL, SHDSL et VDSL). Ces technologies conviennent à différentes applications. Ainsi, le VDSL peut atteindre des débits de l'ordre de 52 Mbits/s mais uniquement sur une distance d'environ 300 m, tandis que le SHDSL supporte un maximum de 2,3 Mbits/s jusqu'à 3 km et de 192 kbit/s jusqu'à environ 6 km.

HDSL

HDSL, High speed Digital Subscriber Line (ligne d'abonné numérique à haut débit). Communication en duplex à 2,3 Mbits/s dans chaque direction.

ADSL

ADSL, Asymmetric Digital Subscriber Line (ligne d'abonné numérique asymétrique). Communication en duplex jusqu'à 8 Mbits/s vers l'abonné (débit descendant) et 640 kbit/s depuis l'abonné (débit ascendant). La communication utilise la même ligne en simultané pour le trafic téléphonique standard. L'utilisateur installe un filtre sur la première prise afin d'améliorer la qualité vocale de la ligne ; ce filtre est appelé 'splitter' (répartiteur) et est généralement fourni avec le produit ADSL. L'ADSL est une option populaire parmi les utilisateurs domestiques, car cette technologie offre un débit descendant supérieur au débit ascendant. L'utilisateur domestique accorde généralement plus d'importance aux délais de téléchargement, le débit ascendant étant normalement réservé aux e-mails.

VDSL

VDSL, Very high speed Digital Subscriber Line (ligne d'abonné numérique à très haut débit). Communication en duplex jusqu'à 52 Mbits/s vers l'abonné (débit descendant) et 6,4 Mbits/s depuis l'abonné (débit ascendant). La communication utilise 1 paire.

Le VDSL est la technologie la plus rapide actuellement disponible pour transférer des données via le réseau téléphonique ordinaire. Il offre une alternative à l'ADSL lorsque des débits très élevés s'avèrent nécessaires pour des applications telles que :

- Les séquences vidéo en continu.
- Les vidéoconférences.
- La combinaison de vidéos et de données sur une même connexion.
- Les besoins élevés en matière d'accès aux données.

BACK

SDSL

Le SDSL (Symmetric Digital Subscriber Loop, boucle d'abonné numérique symétrique) et le G.SHDSL sont des technologies xDSL symétriques.
Un de leurs traits distinctifs réside dans le fait qu'ils présentent les mêmes débits ascendants et descendants, raison pour laquelle ils sont dits 'symétriques'. Le SDSL permet à l'utilisateur d'atteindre un maximum de 2,3 Mbits/s dans les deux directions. Le SDSL peut être utilisé en mode "Back to Back" (dos à dos), lequel implique l'interconnexion de deux modems à l'aide d'un câble en cuivre. Il s'agit d'une technologie propriétaire essentiellement installée en Amérique du Nord. Les applications industrielles commencent à s'orienter vers la norme internationale SHDSL (voir ci-dessous).

SHDSL

"SHDSL" est l'acronyme de "Symmetric High-Bitrate Digital Subscriber Loop" (boucle d'abonné numérique symétrique à débit binaire élevé), qui constitue la première norme internationale pour le DSL symétrique multi-débits. Le SHDSL a été mis au point afin de permettre la communication sur une ou plusieurs paires torsadées. L'utilisation d'une seule paire de fils donne des débits de 192 kbit/s à 2,3 Mbits/s, alors que deux paires permettent d'atteindre de 384 kbit/s à 4,6 Mbits/s. Le SHDSL utilise un algorithme de codage sophistiqué, TC-PAM, qui permet d'améliorer le débit de transfert et/ou la distance de transmission par rapport à d'autres technologies DSL.

Indication des distances de transmission via le SHDSL

	Vitesse	Distance
Communication via une paire unique		
AWG 26	192 kbit/s	6 km
Communication via une paire unique		
AWG 26	2,3 Mbits/s	3 km
Communication via deux paires		
AWG 26	2,3 Mbits/s	5 km

Il est possible d'installer un répéteur entre les appareils pour atteindre des distances de transmission plus importantes.

Veuillez consulter les normes suivantes pour de plus amples informations :

- ANSI (T1E1.4/2001-174) pour l'Amérique du Nord.
- ETSI (TS 101524) pour l'Europe.
- ITU-T (G.991.2) dans le monde entier.

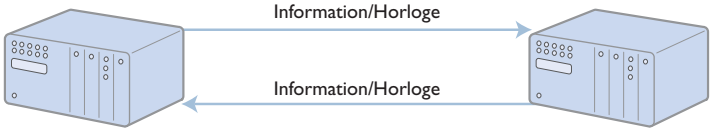
BACK

G.703

La norme ITU G.703 décrit les propriétés électriques et physiques ainsi qu'un certain nombre de débits de transfert.
Il existe trois types physiques de base pour l'interface : codirectionnelle, contradirectionnelle et centralisée.
La norme spécifie des vitesses de 64 kbit/s à 155 520 kbit/s. Elle a été initialement créée pour véhiculer la voix sur une liaison PCM (MIC).
Le support de transmission peut être une paire équilibrée à 120 ohms ou un câble coaxial non équilibré à 75 ohms.

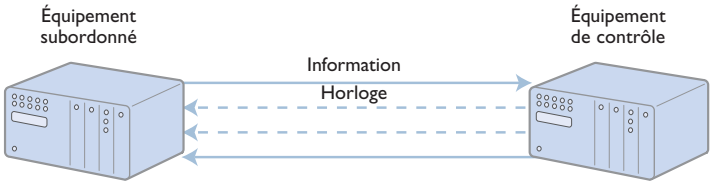
Interface codirectionnelle

La transmission s'effectue sur une paire de fils dans chaque direction. Les données et les informations relatives à l'horloge sont superposées et circulent dans le même sens, tandis que le récepteur se charge de leur synchronisation.



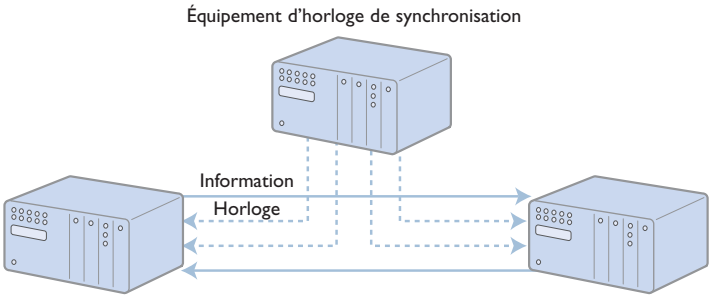
IInterface contradirectionnelle

Ce type de transfert utilise une paire à 4 fils. Les informations relatives à l'horloge sont fournies par le périphérique principal.



Interface avec horloge centralisée

Cette variante de l'interface utilise 3 ou 4 paires de câblage. Les informations relatives à l'horloge de synchronisation sont fournies par l'unité centrale. Dans l'exemple à 3 paires, l'horloge est commune à la transmission et à la réception. Dans l'exemple à 4 paires, la transmission et la réception font l'objet d'une horloge séparée.



BACK

GSM

GSM, GPRS, UMTS : que signifient ces acronymes et quelles possibilités offrent-ils pour la transmission de données ?

Les descriptions techniques comportent souvent des abréviations et des acronymes. Nous avons décidé d'utiliser les désignations et abréviations devenues des normes de l'industrie, bien qu'elles soient généralement libellées en anglais.

L'histoire du GSM

Au début des années quatre-vingt, l'Europe utilisait de nombreux systèmes analogiques de diverses qualités, mais il s'est rapidement avéré que la technologie analogique ne satisferait pas les futurs critères de communication. C'est alors qu'a été formé le **G**roupe **S**péciale **M**obile (GSM).
Ce groupe (né à Vienne en 1982) a été chargé de créer un système mobile capable d'offrir une excellente qualité audio à faible prix.

En 1989, l'ETSI (**E**uropean **T**elecommunication **S**tandards **I**nstitute, Institut européen des normes de télécommunication) s'est vu confier la poursuite du développement du GSM. L'acronyme GSM a alors adopté une nouvelle signification : **G**lobal **S**ystem for **M**obile communications, système mondial de communications mobiles.

La norme GSM permet la transmission sans fil de données de divers types (voix/texte/images) entre différents types d'équipements, mais uniquement si ces derniers se trouvent dans la zone de couverture des émetteurs d'un opérateur. Après la normalisation, le nombre d'utilisateurs d'équipements GSM a augmenté de manière explosive, tout d'abord dans le secteur de la téléphonie vocale. Au début de 1994, il y avait 1,3 million d'abonnés ; aujourd'hui, ils sont 1.024 millions à l'échelle mondiale (février 2004).

On constate à présent une forte augmentation de l'usage dans le cadre des applications M2M (**M**achine **à M**achine). Il peut s'agir de transmission de données ou de signaux d'alarme d'équipements esclaves vers un système de contrôle, ou encore de transmission de données depuis ou entre des parcmètres. Ce domaine d'application est pratiquement illimité et de nombreux types de matériel GSM vont voir le jour en fonction des besoins à venir.

BACK

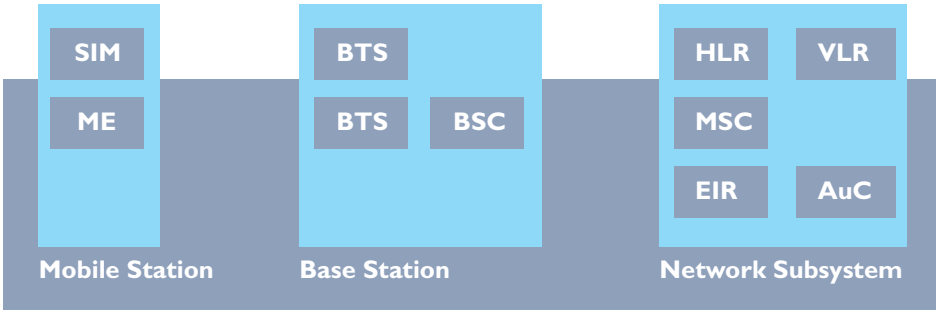
Dans le cadre des réseaux mobiles, la transmission numérique présente de nombreux avantages par rapport à la technologie analogique :

- Connexion téléphonique de meilleure qualité.
- Débits de transmission plus élevés.
- Meilleure utilisation de la bande passante, d'où une augmentation du nombre d'abonnés sur le réseau.
- Possibilité d'offrir de nouveaux services et de nouvelles fonctions (données, textes, fax, etc.).
- Possibilité de crypter les données pour une sécurité accrue.
- Diminution de la consommation électrique, ce qui permet d'augmenter l'autonomie et les temps de transmission sur les appareils alimentés par batterie.

Architecture

Un réseau GSM peut être scindé en trois composantes majeures :

- **M**obile **S**tation (MS, station mobile)
- **B**ase **S**tation **S**ystem (BSS, système de station de base).
- **N**etwork **S**ubsystem (sous-système de réseau), avec des connexions vers des réseaux externes, comme les réseaux RNIS ou RTC.



BACK

Composantes du réseau

ME **M**obile **E**quipment (équipement mobile). Il s'agit de l'équipement adapté au réseau GSM. Chaque unité ME possède un numéro d'identification unique (le numéro IMEI, International Mobile Equipment Identity, identité internationale de l'équipement mobile), qui permet à l'opérateur du réseau de bloquer un appareil volé, par exemple.

SIM Acronyme de **S**ubscriber **I**dentity **M**odule (module d'identification d'abonné). Carte utilisée en combinaison avec l'unité ME. La carte SIM est fournie par l'opérateur du réseau et contient des données telles que le numéro de téléphone, le code PIN, le répertoire, etc. La carte SIM peut être placée dans différentes unités ME.

BTS Acronyme de **B**ase **T**ransceiver **S**tation (station d'émission et de réception). Il s'agit d'une station radio de base, c'est-à-dire un émetteur/récepteur permettant de communiquer avec certains ME.

BSC Acronyme de **B**ase **S**tation **C**ontroller (contrôleur de station de base). Il s'agit d'une sous-station communiquant avec la station radio de base. La sous-station peut communiquer avec un certain nombre de stations de base.

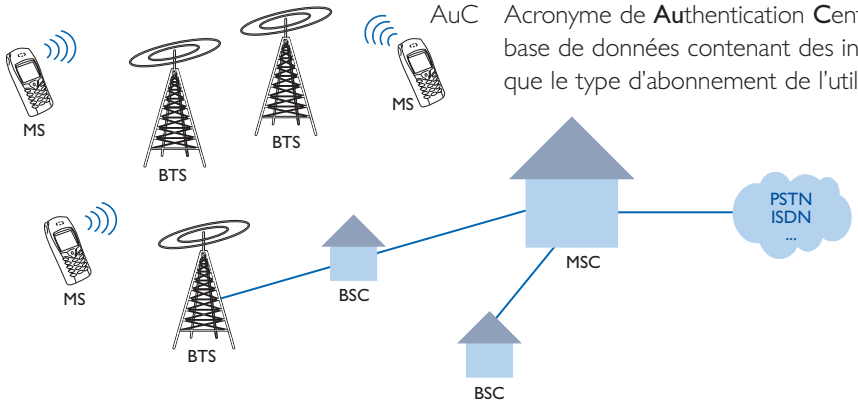
MSC Acronyme de **M**obile **S**witching **C**entre (centre de communication mobile) qui permet le transfert vers un réseau analogique, PSTN (**P**ublic **S**witched **T**elephone **N**etwork, réseau téléphonique commuté, RTC), ou numérique, ISDN (**I**ntegrated **S**ervices **D**igital **N**etwork, réseau numérique à intégration de services, RNIS/NUMERIS).

HLR Acronyme de **H**ome **L**ocation **R**egister (enregistreur de localisation nominal). Il s'agit d'une base de données contenant entre autres des informations de base sur l'utilisateur, comme le type d'abonnement.

VLR Acronyme de **V**isitor **L**ocation **R**egister (enregistreur de localisation de visiteurs). Il s'agit d'une base de données contenant des informations sur un ME situé dans une cellule non contrôlée par un HLR.

EIR Acronyme de **E**quipment. **I**dentity **R**egister (enregistreur d'identité d'équipement), qui enregistre tous les utilisateurs du réseau. L'identifications s'effectue via le numéro IMEI de l'unité ME.

AuC Acronyme de **Au**thentication **C**entre (centre d'authentification). Il s'agit d'une base de données contenant des informations sur l'opérateur du réseau ainsi que le type d'abonnement de l'utilisateur.

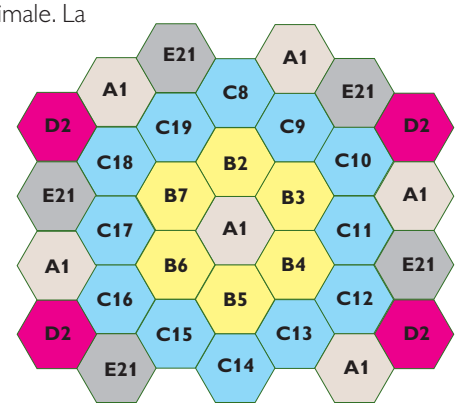


Structures cellulaires

Les stations de base sont positionnées de manière à assurer une couverture optimale. La zone couverte par une station de base est appelée "cellule".

L'ensemble du réseau GSM est constitué de cellules de divers formats. Une cellule peut couvrir un rayon de 200 mètres à ~30 km, selon l'emplacement et l'environnement de la station de base.

Parmi les autres facteurs affectant l'installation figurent la puissance de sortie et le fait que la station de base soit située ou non dans un environnement néfaste au trafic radio. La structure cellulaire se traduit par la réutilisation des fréquences dans les stations de base. Dans la figure ci-contre, la fréquence A1 peut être réutilisée dans la troisième couche sans risque de diaphonie entres les cellules de même fréquence.



Si vous vous déplacez au sein d'une zone, il est nécessaire de passer d'une cellule à une autre. C'est ce que l'on appelle le transfert intercellulaire.

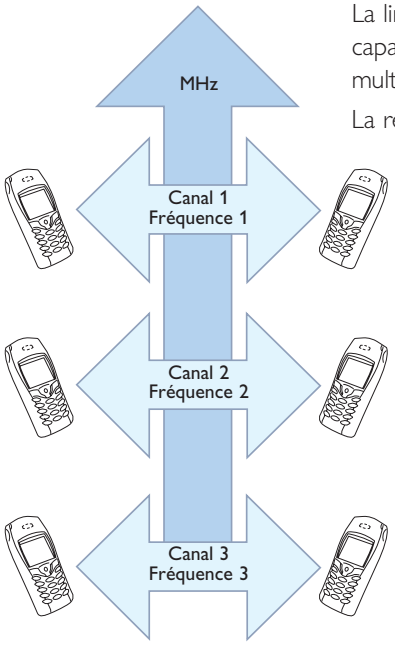
Transmissions radio entre les systèmes MS et BSS

Dans les années quatre-vingt, lors de l'établissement de la spécification GSM, l'ITU (International Telecommunication Union, Union internationale des télécommunications) a réservé deux bandes de fréquences de 25 MHz pour les transmissions radio par GSM :

- 880–915 MHz pour le transfert "ascendant" de MS vers BSS.
- 925–960 MHz pour le transfert "descendant" de BSS vers MS.

L'essor des communications mobiles a rendu nécessaire le recours à de multiples fréquences. Aujourd'hui, il existe cinq fréquences standard : 400, 850, 900, 1800 et 1900 MHz. Cette dernière est généralement utilisée aux Etats-Unis et dans certaines régions d'Asie, tandis que 900 et 1800 MHz sont davantage utilisées à l'échelle mondiale.

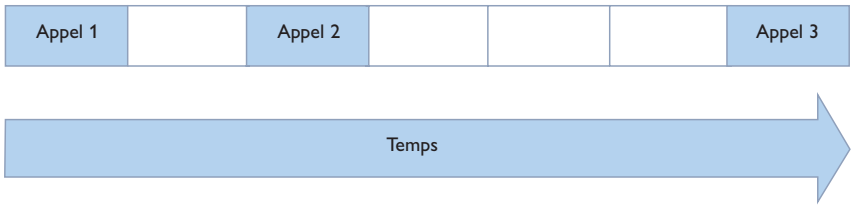
BACK



Répartition fréquentielle

La limitation de la bande passante a débouché sur l'utilisation de diverses techniques capables de supporter un maximum d'utilisateurs simultanés, grâce à la combinaison du multiplexage TDM (*Multiplexage temporel*) et FDM (*Multiplexage fréquentiel*).

La répartition fréquentielle (FDM) implique une division de la bande de 25 MHz disponible en bandes de 200 KHz. Dans la description, ci-dessus, l'utilisation des fréquences entre les cellules, A1, B2, B3, etc. sont des exemples de répartition fréquentielle.



Multiplexage temporel

En multiplexage temporel (TDM), tous les émetteurs utilisent la même fréquence, mais à des moments différents. Les équipements doivent être synchronisés pour empêcher les émetteurs de s'interrompre les uns les autres.

Compilation

Fréquence pour la transmission du système ME à la station de base	880-915	MHz
Fréquence pour la transmission depuis la station de base	925-960	MHz
Bande passante	35+35	MHz
Méthode d'accès	TDMA/FDMA	
Fréquence par canal radio	200	KHz
Ecart fréquentiel entre le transfert descendant et ascendant	45	MHz
Rayon maximal pour une cellule	30	km
Rayon minimal pour une cellule (microcellule)	30	m
Puissance de sortie maximale à partir du terminal mobile	2	W @ 900 MHz

Services fournis sur le réseau GSM

Le GSM permet de proposer divers services tels que :

- La téléphonie
- Le CSD (**C**ircuit **S**witched **D**ata, transfert de données).
- Les SMS (**S**hort **M**essage **S**ervice, messages courts).
- Les MMS (**M**ultimedia **M**essage **S**ervice, messages multimédias).
- La télécopie.
- Le GPRS (**G**eneral **P**acket **R**adio **S**ervice, service général de radiocommunication en mode paquet).

Téléphonie

Le service GSM le plus courant, qui a contribué à sa mondialisation. Les algorithmes de codage et de décodage du trafic n'ont cessé d'évoluer, ce qui a entraîné une minimisation continue de la bande passante affectée à la téléphonie sans préjudice pour la qualité de la transmission.

CSD, transmission de données à commutation de circuits

Transfert de données, à des vitesses de 2.400 bits/s à 14,4 kbit/s. Le tableau ci-contre reprend les vitesses et protocoles disponibles.

La transmission de données peut être configurée pour un transfert transparent ou non transparent. Le protocole RLP (**R**adio **L**ink **P**rotocol, protocole de liaison radio) est utilisé pour les transferts non transparent; il s'agit d'un protocole de correction d'erreur GSM. Ce protocole accroît la fiabilité des transferts mais génère également des délais. L'utilisation de cette fonction requiert la prise en charge du service et des dispositifs connectés.

Vitesse	Protocole
2400 bits/s	V.22 bis
4800 bits/s	V.32
9600 bits/s	V.32
14400 bits/s	V.32 bis
2400 bits/s	V.110
4800 bits/s	V.110
9600 bits/s	V.110
14400 bits/s	V.110

BACK

SMS

Le service le plus utilisé après la téléphonie. Un message SMS utilise le canal de signalement pour transférer les messages textes. Les SMS sont devenus populaires sur le plan privé comme professionnel en raison de leur simplicité. En résumé, ce service présente les caractéristiques suivantes :

- Un message peut compter jusqu'à 160 caractères.
- Le transfert ne peut pas être garanti car le récepteur peut être éteint ou situé en dehors de la zone de couverture. Le message peut être envoyé avec différents paramètres :
- Durée de conservation du message sur le réseau avant effacement s'il ne parvient pas au destinataire (jusqu'à une semaine).
- Accusé de réception (l'expéditeur reçoit une confirmation de l'arrivée du message).
- Réception d'un accusé d'envoi du message.
- Possibilité d'envoyer et de recevoir des messages durant un appel.
- Possibilité d'effectuer des transmissions vers des destinataires individuels ou groupés.

MMS

MMS est l'acronyme de **M**ultimedia **M**essaging **S**ervice (service de messages multimédia). Ce système fonctionne de la même manière que les SMS mais offre des options supplémentaires :

- Envoi d'images et d'animations.
- Envoi de musique.
- Enregistrement et envoi de vos propres messages.
- Introduction de longs messages textes.
- Un MMS peut contenir des milliers de caractères selon le modèle de téléphone utilisé.

Télécopie

Convient pour la télécopie de classe 1 et de classe 2

BACK

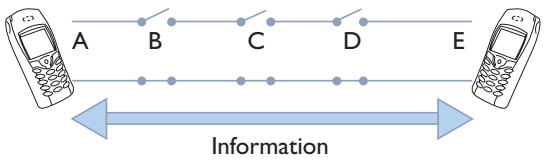
GPRS

Extension du réseau GSM, la norme GPRS prend en charge les données circulant par paquets commutés. Ce système diffère du trafic de données à commutation de circuits pris en charge par la norme GSM. Avec le GPRS, chaque canal non affecté à la transmission vocale peut servir au transfert de paquets de données commutés. Les paquets en provenance de différents usagers peuvent emprunter le même canal, ce qui optimise le partage des ressources réseau.

Le GPRS permet des débits encore plus élevés car il utilise plusieurs créneaux de temps pour le transfert. En théorie, des débits maximum de 115,2 kbit/s sont possibles mais en pratique, le débit se situe plutôt entre 20 et 50 kbit/s (contrairement à la norme HSCSD [*High Speed Circuit Switched Data*, données de circuits commutés à haute vitesse], qui correspond à des débits allant de 9,6 à 43,2 kbit/s et que certains opérateurs proposent également en communication GSM par commutation de circuits). Quoi qu'il en soit, le débit est fonction de divers facteurs : opérateur, terminal, nombre d'usagers dans une même cellule, distance par rapport à la station de base (renvoi), équipement fixe ou en mouvement (le débit est inférieur en cas de prises en charge successives par plusieurs stations de base), etc.

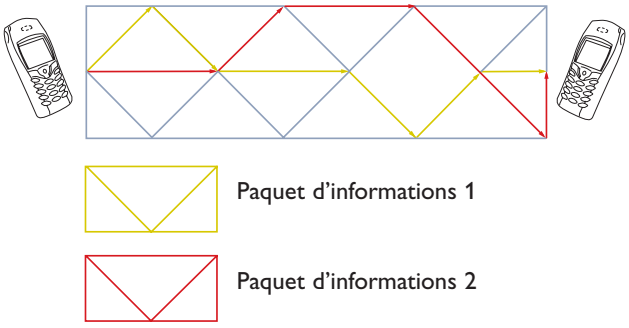
Le débit dépend également du nombre de créneaux de temps utilisés ainsi que du schéma de codage utilisé par la liaison de communication. La norme GPRS comprend 4 CS (**C**oding **S**chemes, schémas de codage) : CS1 est le plus sûr et le plus fiable, mais également le plus lent (9,05 kbit/s) tandis que CS4 n'applique pas des critères aussi draconiens pour la correction des erreurs et les retransmissions, et atteint donc des vitesses de 21,4 kbit/s. Les vitesses spécifiées ci-dessus dépendent du nombre de créneaux de temps et du CS, ce qui signifie par exemple que 4 créneaux de temps en CS4 donnent 4 x 21,4 = 85,6 kbit/s. Il convient également de préciser que la norme GSM spécifie 4 CS mais que seuls les deux premiers, CS1 et CS2 (13,4 kbit/s/créneau de temps), sont actuellement implémentés sur les réseaux GPRS actifs.

La différence entre la commutation de circuits et la commutation de paquets peut être brièvement décrite comme suit :



Dans un réseau à **commutation de circuits**, la connexion s'effectue via une liaison physique entre les deux parties. Cette liaison est constamment ouverte et ne se ferme que lorsqu'une des parties l'a décidé, comme dans le cas d'un appel téléphonique. Ce système présente des avantages et des inconvénients. Les unités en communication conservent un lien mutuel constant ; elles détectent la capacité disponible et savent qu'elle ne sera pas utilisée par une autre unité. D'un autre côté, cela revient à un gaspillage de ressources lorsque les parties n'échangent pas de données, car la ligne est occupée et personne d'autre ne peut l'utiliser. Les parties doivent donc interrompre la connexion lorsqu'elles n'en ont plus besoin.

BACK



Un **réseau à commutation de paquets** est un réseau dont le trafic est scindé en petits paquets. Cela signifie que d'autres peuvent l'utiliser simultanément. Si l'on compare le réseau à commutation de circuits à un appel téléphonique, on peut comparer le réseau à commutation de paquets à une entreprise de transport ou à un bureau de poste. Plusieurs personnes peuvent envoyer de nombreux paquets en même temps. Le bureau de poste ou l'entreprise de transport achemineront tous les paquets chez le destinataire, et les paquets partageront les camions ainsi que les infrastructures routières.

En février 2004, 172 opérateurs dans de nombreux pays proposaient le GPRS. Le nombre de téléphones mobiles compatibles GPRS devrait passer de 10 millions en 2001 à 280 millions en 2005.

Sécurité du réseau

GSM

Les principaux mécanismes de sécurité du réseau GSM sont les suivants :

- Authentification forte des utilisateurs (le réseau authentifie la carte SIM, la carte SIM authentifie l'utilisateur via le code PIN).
- Protection contre l'interception clandestine des données sur l'interface radio.
- Protection contre l'interception clandestine du signal sur l'interface radio.
- Vérification de l'identité de l'appareil. Possibilité de blocage en cas de vol.

Cryptage des données transitant par la connexion radio, c'est-à-dire entre l'unité et la station de base. La clé de cryptage secrète de chaque utilisateur est enregistrée sur sa carte SIM, centrale d'authentification de l'opérateur domestique.

GPRS

Les communications GPRS utilisent essentiellement les mêmes mécanismes de sécurité que le GSM. L'authentification s'effectue de la même manière, éventuellement via la même technologie et la même carte SIM. La clé cryptographique générée est toutefois toujours différente pour le GSM et le GPRS. Le GPRS utilise en effet des algorithmes cryptographiques spéciaux, fondés sur des clés à 64 bits.

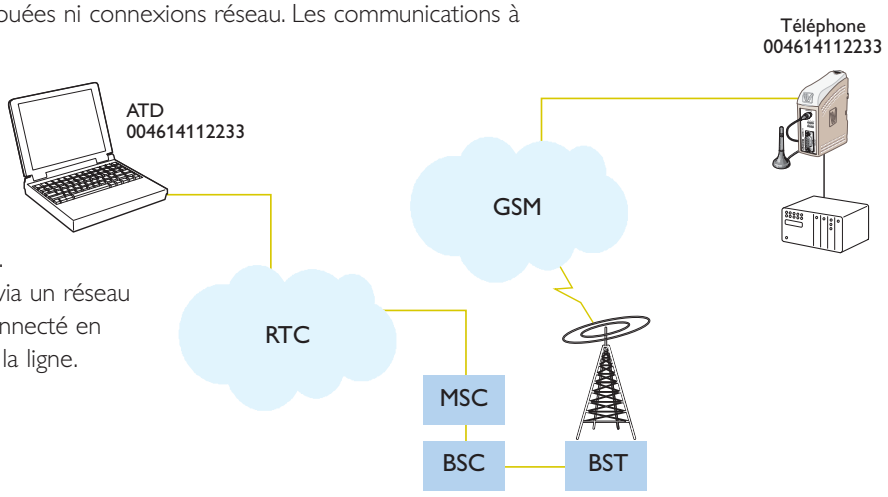
Différences entre les systèmes GSM et GPRS

CSD Circuit Switched Data TDM Time Division Multiplexing	GPRS General Packet Radio Service TDM Time Division Multiplexing
1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
Utilisation d'un créneau de temps, ce qui donne un débit maximal de 14,4 kbit/s. Les coûts d'utilisation reposent sur la longueur de la connexion, indépendamment de la quantité de données transmises.	L'utilisation de quatre créneaux de temps et du schéma de codage 4 donne un débit maximal de 85,6 kbit/s. Les coûts d'utilisation reposent sur la quantité de données transmises (nombre de paquets), indépendamment du temps de connexion.

Applications basées sur les systèmes GSM et GPRS

L'utilisation de systèmes GSM et GPRS pour la transmission de données offre une alternative à la radiocommunication. Les applications sans fil sont essentiellement utiles pour les communications effectuées sans lignes louées ni connexions réseau. Les communications à l'aide d'un modem GSM ou GPRS imposent néanmoins certaines conditions de base.

Le modem GSM se connecte au réseau GSM. Une connexion est établie via le MSC et le BSC, et aboutit à l'ordinateur par le biais d'une ligne RTC. Comme la connexion GSM est établie via un réseau à commutation de circuits, vous êtes connecté en permanence jusqu'à la déconnexion de la ligne.

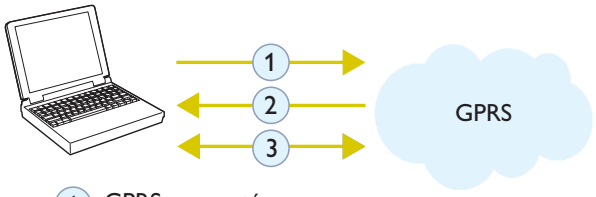


BACK

La communication par GPRS applique une autre procédure. Le GPRS est fondé sur la communication IP, et l'unité connectée doit fournir une adresse IP avant qu'une connexion puisse être établie.

Cette opération s'effectue comme suit :

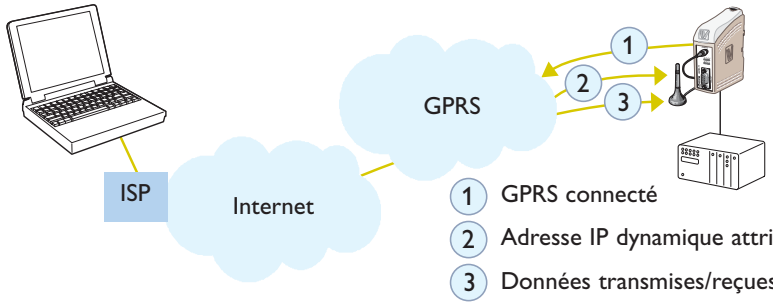
- Connexion au réseau GPRS.
- Attribution d'une adresse dynamique.
- L'échange de données peut s'effectuer.



1. GPRS connecté
2. Adresse IP dynamique attribuée
3. Données transmises/reçues

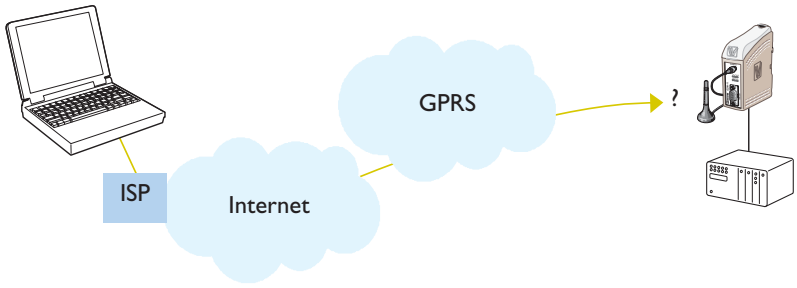
Tous les opérateurs ne sont pas encore en mesure de proposer des abonnements avec attribution d'une adresse statique. Or, une attribution dynamique ne permet pas de savoir, d'un cas à l'autre, quelle adresse a été attribuée à l'équipement opposé.

Ce n'est pas un problème si le modem GPRS est connecté au maître, car ce dernier prend l'initiative de la connexion et le modem se voit attribuer une adresse IP. Cela signifie qu'une connexion peut être établie avec un équipement disposant d'une adresse IP fixe, par exemple un ordinateur.

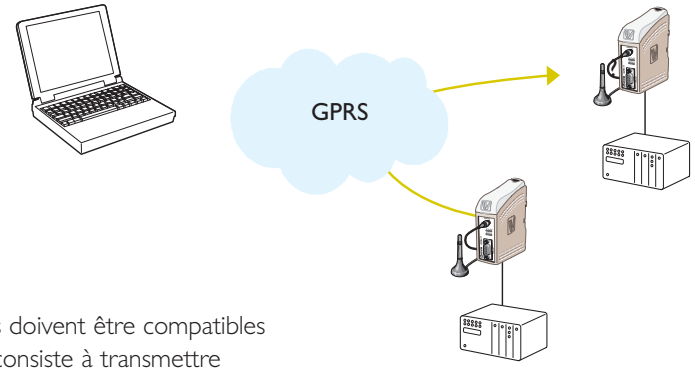


1. GPRS connecté
2. Adresse IP dynamique attribuée
3. Données transmises/reçues

Ce problème survient lorsqu'un appareil, par exemple un ordinateur, veut communiquer avec des périphériques et que c'est l'ordinateur qui génère la connexion. Personne ne sait à quelle adresse IP l'ordinateur doit se connecter, car ces adresses sont attribuées dynamiquement.

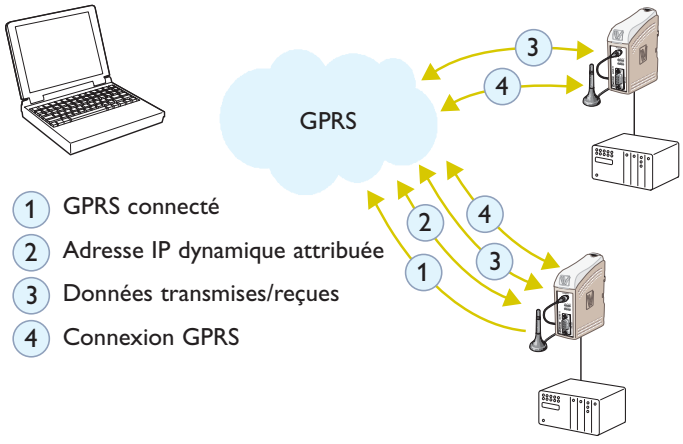


Une autre application présentant le même type de problèmes réside dans la communication entre deux dispositifs lorsque aucun n'agit en tant que maître. Le modem ne peut initier la communication IP car il ne sait pas quelle adresse sera attribuée.



Il existe des solutions à ce problème, mais elles doivent être compatibles avec les applications connectées. Un exemple consiste à transmettre l'adresse IP à l'autre partie par le biais d'un SMS.

Si l'un des dispositifs connectés tombe en panne, la procédure devra être réitérée comme s'il avait perdu son adresse IP.



Classes GPRS

Il existe trois catégories d'équipement GPRS, appelées Classe A, B et C.

Classe A	Compatible avec les opérations GSM et GPRS simultanées
Classe B	Compatible avec les opérations GSM et GPRS, mais pas simultanément.
Classe C	La connexion ne prend en charge que les données GPRS ou GSM. Si une commutation est nécessaire entre le GPRS et le GSM, vous devrez redémarrer la connexion.

Classes multicréneaux intégrant de 1 à 4 créneaux de temps.

	Nombre maximal de créneaux		
Classe GPRS multicréneaux	RX "transfert descendant"	TX "transfert ascendant"	Max
Classe 1	1	1	2
Classe 2	2	1	3
Classe 4	3	1	4
Classe 6	3	2	4
Classe 8	4	1	5
Classe 10	4	2	5
Classe 11	4	3	5
Classe 12	4	4	5

RX : Nombre maximal de créneaux de temps que le MS peut recevoir par plage TDMA GSM.
TX : Nombre maximal de créneaux de temps que le MS peut envoyer par plage TDMA GSM.
Max : Nombre total de créneaux de temps, sur la liaison ascendante et descendante, qui peuvent être utilisés simultanément par le MS dans la plage TDMA.

UMTS (3G)

3G est la dénomination usuelle d'une norme appelée 'UMTS' (**U**niversal **M**obile **T**elecommunications **S**ystem, système universel de télécommunications mobiles) dans de nombreux pays. Elle décrit la technologie de base de la troisième génération de systèmes téléphoniques, mais peut englober d'autres normes correspondantes dans certains pays. L'expression '3G' vient du fait qu'il s'agit de la troisième génération de téléphonie mobile : la première était analogique et fut suivie par le GSM, qui est la plus courante à l'heure actuelle. Le système 3G vient désormais d'être lancé.

La principale différence entre le 3G et le GSM réside dans la capacité de transfert, c'est-à-dire la vitesse à laquelle les données peuvent être envoyées et reçues par le téléphone. Plus la capacité de transfert est élevée, plus le réseau mobile offre de possibilités. La vitesse est environ 40 fois supérieure avec le 3G, ce qui signifie que vous pouvez recourir à des services sophistiqués tels que l'envoi et la réception d'images, le transfert de séquences vidéo et l'utilisation de services basés sur la position de l'utilisateur. Voilà pourquoi bon nombre de personnes qualifient le 3G de large bande mobile.

BACK

RNIS

Qu'est-ce que le RNIS/NUMERIS ?

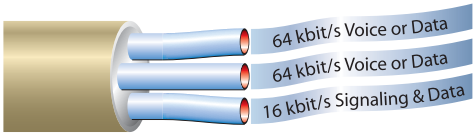
Le RNIS (de l'anglais ISDN [**I**ntegrated **S**ervice **D**igital **N**etwork, réseau numérique à intégration de services]) est l'équivalent numérique du réseau téléphonique analogique classique PSTN (**P**ublic **S**witched **T**elephone **N**etwork, réseau téléphonique commuté ou RTC). La technologie RNIS est normalisée conformément aux recommandations de l'ITU (**I**nternational **T**elecommunications **U**nion, Union internationale des télécommunications).

Signalisation

Au lieu que la compagnie du téléphone active la sonnerie de votre téléphone ("signal intra-bande"), un paquet numérique est transmis sur un canal distinct ("signal hors bande"). Le signal hors bande n'interrompt pas l'appel en cours et présente un temps de connexion très court. Il contient des informations sur l'identité de l'appelant, le type d'appel (voix/données) et le numéro appelant. L'équipement RNIS connecté se charge ensuite de la gestion de l'appel.

Connexions

Une liaison RNIS se compose de canaux B (transfert de données) et D (principalement signaux de commande). Le débit de transfert sur un canal B est de 64 kbit/s, mais il est possible d'interconnecter plusieurs canaux afin d'accroître la vitesse. Les clients se voient généralement proposer la connexion RNIS sous la forme de deux possibilités d'abonnement. La première possibilité est l'accès de base, constitué de deux canaux B et d'un canal D à 16 kbit/s (2B+D). Cela donne un débit maximal de 128 kbit/s (2 x 64 kbit/s), suffisant pour des utilisateurs désirant bénéficier d'un débit supérieur, combiner téléphone, télécopie et transfert de données, ou disposer d'un réseau local restreint. Il est possible de connecter jusqu'à 8 dispositifs RNIS sur la même ligne, ce qui s'avère très avantageux lorsqu'une connexion RNIS comprend différents types d'appareils.



Les appareils sont associés à des numéros individuels comme s'ils avaient leur propre connexion au réseau. La seconde possibilité est l'accès primaire, composé de 30 canaux B et d'un canal D à 64 kbit/s (30B+D). La capacité maximale s'élèvera alors à 2 Mbits/s si les 30 canaux sont interconnectés. L'accès RNIS primaire convient pour la connexion d'ordinateurs requérant un débit élevé (à des fins de vidéoconférence, par exemple), pour les grands réseaux locaux, les centraux numériques et les passerelles entre de vastes réseaux régionaux.

Les principaux avantages du RNIS résident dans le débit de transfert (64 à 128 kbit/s), le temps de connexion inférieur à 2 secondes, la stabilité accrue des connexions et leur sensibilité réduite aux interférences, ainsi que dans la possibilité de connecter plusieurs appareils à la même ligne (téléphone, fax ou ordinateur, par exemple).

BACK

Composants/interface RNIS

Les composants RNIS incluent les terminaux, les adaptateurs de terminaux (TA), les dispositifs de terminaison de réseau (NT), les équipements de terminaison de ligne (LT), et les équipements de terminaison de centraux (CLA). Le système RNIS utilise deux types de terminaux : les terminaux RNIS spécialisés, dotés d'une interface RNIS et appelés équipements de terminaux de type 1 (TE1), et les terminaux dotés d'une interface non-RNIS, les unités à interface V.24, qualifiés d'équipements de terminaux de type 2 (TE2). Les TE1 se connectent au système RNIS par le biais d'une liaison numérique d'interface à "paire torsadée" 4 fils, tandis que les TE2 se connectent au réseau RNIS par le biais d'un adaptateur de terminal. Celui-ci peut être un dispositif autonome ou une carte d'interface intégrée dans le dispositif TE2. Si le TE2 et le TA sont des unités autonomes, on utilise généralement une interface normalisée telle que RS-232/V.24 ou V11/RS-485.

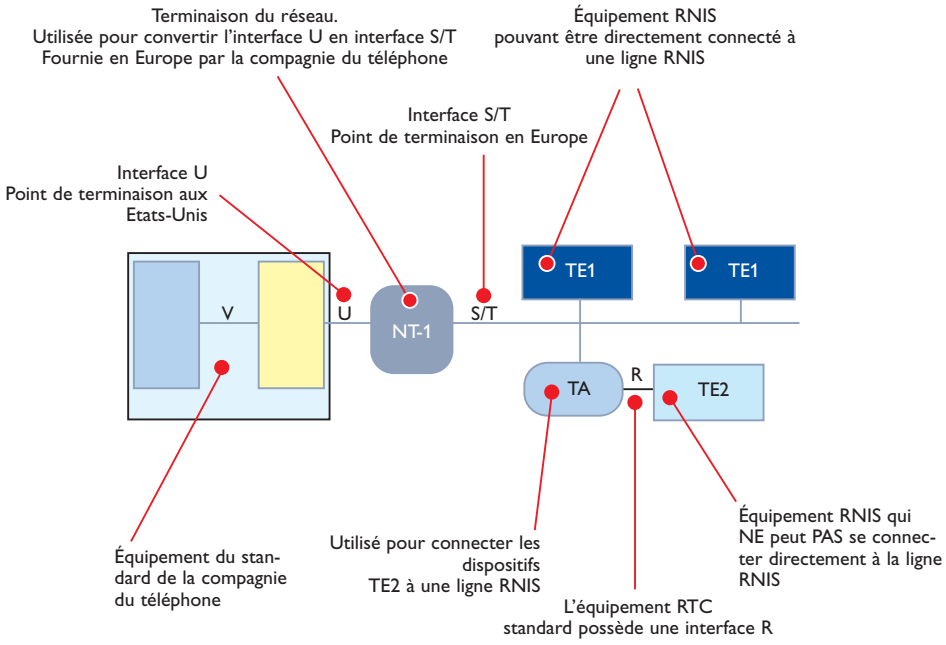
La prochaine interface en amont est le terminal de réseau, qui forme l'interface entre l'interface à 4 fils de l'installation du client et les câbles en cuivre traditionnels à 2 fils de l'opérateur télécom.

Les terminaux de réseau se déclinent également en deux types, NT1 et NT2, où NT2 est un dispositif plus complexe. On obtient alors les couches 2 et 3, ainsi que des fonctions protocolaires et une concentration. Les NT2 se retrouvent, par exemple, dans les centraux de bureaux. Dans la plupart des pays, les terminaux de réseaux appartiennent à l'opérateur télécom.

Le modèle de référence du système RNIS inclut un certain nombre de points de référence constituant l'interface entre les périphériques/terminaux du modèle de référence d'après les critères suivants :

- R --- Point de référence constituant l'interface entre les dispositifs non-RNIS et les adaptateurs de terminaux TA, norme RS-232/V.24.
- S --- Point de référence constituant l'interface entre TE/TA et NT1.
- T --- Point de référence constituant l'interface entre les dispositifs NT1 et NT2.
- U --- Point de référence constituant l'interface entre NT et le terminal de ligne LT.

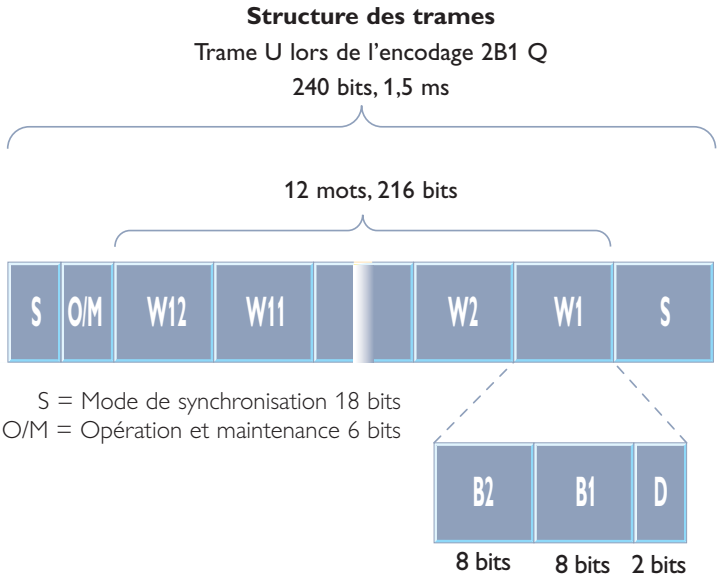
BACK



Couche physique

La signalisation entre le terminal de ligne (LT) du central de télécommunications et le terminal de réseau (NT) de l'utilisateur s'effectue via l'interface U tandis que la signalisation dans les locaux de l'utilisateur, entre le NT et l'adaptateur de terminal TA, s'effectue via l'interface S. L'interface U utilise des trames de 240 bits de longueur, transférées à 160 kbit/s. Les trames de l'interface U sont structurées comme illustré dans la figure ci-dessous.

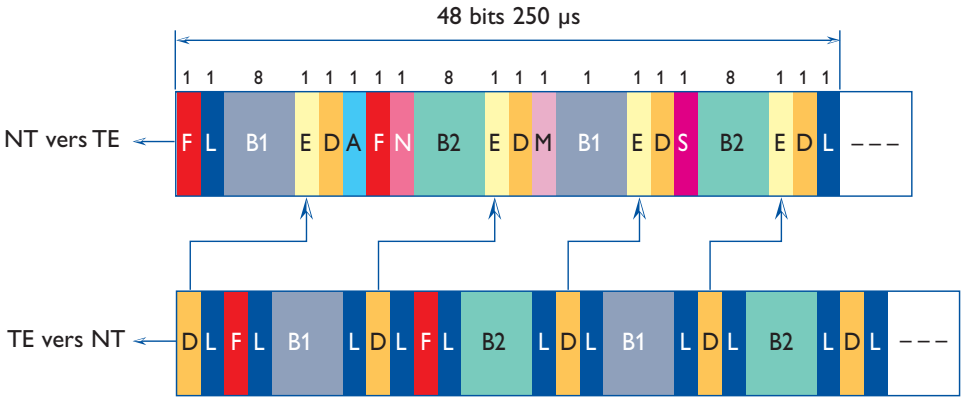
BACK



Format des trames de l'interface S

Les trames de l'interface S utilisent 48 bits, dont 36 sont affectés au transfert de données ; le débit binaire de l'interface S est de 192 kbit/s. La structure interne des trames diffère légèrement selon le sens d'envoi des trames. La figure ci-dessous illustre l'utilisation des différents bits.

A = Bit d'activation
B1 = Canal B1 (2 x 8 bits / trame)
B2 = Canal B2 (2 x 8 bits / trame)
D = Canal D (4 x 1 bit / trame)
E = Echo du bit D précédent
F = Bit d'encadrement
L = Equilibrage DC
S = Canal S
N = F inversé de NT vers TE
M = Bit de multitramage



BACK

Couche 2 – Couche de lien de données

La couche de lien de données pour le système RNIS est spécifiée par les normes ITU Q.920 à Q.923. La signalisation du canal D est définie sous Q.921. LAP-D (Link Access Procedure – D channel, procédure d'accès au lien – canal D) est le protocole utilisé dans la couche de lien de données. Le protocole LAP-D est quasi identique à X.25 LAP-B, et tous deux sont basés sur HDLC. La figure ci-dessous illustre la structure des trames utilisées par LAP-D :

Indicateur	Adresse	Contrôle	Information	CRC	Indicateur

Indicateur (1 octet)
L'indicateur initial est toujours 7E16 (0111 11102).

Adresse (2 octets)

8	7	6	5	4	3	2	1
SAPI (6 bits)						C/R	EA0
TEI (7 bits)							EA1

SAPI (**S**ervice **A**ccess **P**oint **I**dentifier, identificateur de point d'accès au service), 6 bits.
C/R (**C**ommand/**R**esponse, commande/réponse), bit indiquant si la trame correspond à une commande ou à une réponse.
EA0 (**A**ddress **E**xtension, extension d'adresse), bit indiquant le dernier octet d'une adresse.
TEI (**T**erminal **E**ndpoint **I**dentifier, identificateur de point d'extrémité du terminal), identificateur de périphérique à 7 bits (voir la page 102).
EA1 (Address Extension, extension d'adresse) bit présentant la même fonctionnalité que EA0.

Contrôle (2 octets)
Le champ de contrôle permet d'indiquer le type de trame et de commande. Il existe trois types de trames : les trames d'information, les trames de contrôle/surveillance et les trames non numérotées, les deux premières contenant également les numéros de séquence (N[r] et N[s]).

Information
Informations destinées à la couche de réseau sus-jacente et aux données de l'utilisateur.

CRC(2 octets)
Cyclic Redundancy, redondance cyclique : somme de contrôle de 16 bits permettant de détecter les erreurs de bits lors du transfert.

Indicateur(1 octet)
L'indicateur final est toujours 7E16 (0111 11102).

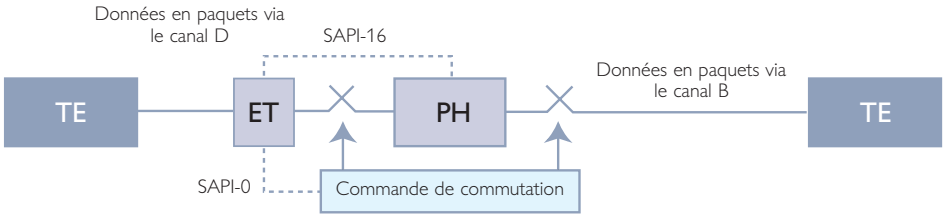
BACK

SAPI

Le SAPI (identificateur de point d'accès au service) est un champ de 6 bits permettant de spécifier jusqu'à 64 fonctions de service fournies à la couche 3 par la couche 2.

Valeur SAPI	Couche 3 apparentée ou entité de gestion
0	Procédures de contrôle des appels
1–11	Réservé pour une future normalisation
12	Communication / téléaction
13–15	Réservé pour une future normalisation
16	Communication en paquets conformément aux procédures X.25 de niveau 3
17–31	Réservé pour une future normalisation
63	Procédures de gestion de la couche 2
Tous les autres	Non disponible pour les procédures Q.921

La figure ci-dessus illustre l'utilisation du champ SAPI, SAPI = 0 étant utilisé pour la commande de commutation et SAPI = 16 étant utilisé pour le routage des paquets en cas d'utilisation de X.31 et X.25 via le canal D.



TEI

Le TEI (Terminal Endpoint Identifier, identificateur du point d'extrémité du terminal) est une ID unique attribuée à chaque TA/TE sur le bus RNIS S/T. L'identificateur peut être attribué dynamiquement si le dispositif est activé, ou statiquement lors de l'installation.

Valeur TEI	Type d'utilisateur
0–63	Attribution non automatique du TEI à l'équipement de l'utilisateur
64–126	Attribution automatique du TEI à l'équipement de l'utilisateur
127	Diffusion vers tous les dispositifs

Couche 3 – Couche de réseau

La couche de réseau réservée au système RNIS est spécifiée par ITU dans Q.930 à Q.939. La couche 3 possède des fonctions permettant d'établir, de maintenir et d'interrompre une connexion logique entre deux dispositifs. La structure du champ d'information sur la couche 3 présente une longueur variable, et les différents champs sont spécifiés par Q.931 :

Champ d'informations							
8	7	6	5	4	3	2	1
Discriminateur de protocole							
0	0	0	0	Longueur de la CRV			
Call Reference Value (valeur de référence de l'appel, 1 ou 2 octets)							
0	Type de message						
Eléments d'informations obligatoires et optionnels (variables)							

L'en-tête du message du champ d'information se présente comme suit :

Protocol Discriminator (discriminateur de protocole)(1 octet)

Ce champ identifie le type de protocole utilisé pour gérer les messages de la couche 3. En cas d'utilisation de Q.931, ce champ correspond à 0816.

Length (longueur)(1 octet)

Longueur du champ en aval.

Call Reference Value (CRV, valeur de référence de l'appel) (1 ou 2 octets)

Ce champ permet d'identifier l'appel/la connexion dont le message de signalisation fait partie. Sa valeur sera utilisée tout au long de la signalisation tant que l'appel sera en cours.

Message Type (type de message) (1 octet)

Ce champ indique le type de message envoyé. Il existe quatre groupes de messages : les messages de connexion, d'information, de déconnexion et autres. 'SETUP' (configuration) et 'CONNECT' (connexion) font partie du premier groupe. Eléments d'information (longueur variable).

Ce champ comprend différents éléments d'information. Le type d'élément d'information envoyé dépend du champ précédent, qui indique le type de message. Les éléments relatifs aux informations du nombre B, aux services supplémentaires, aux besoins de transmission sur le réseau, etc. figurent ici.

CAPI

La norme CAPI (COMMON-ISDN-API) offre une interface normalisée permettant de concevoir des logiciels basés sur le système RNIS. Le recours à la norme CAPI donne des applications capables de communiquer via le réseau RNIS sans devoir envisager des implémentations RNIS spécifiques au fabricant.

Cette norme n'est quasiment plus utilisée et la plupart des opérateurs téléphoniques fournissent le RNIS sur la base de la norme Q931/**ETSI 300 102**, version 2.0 de CAPI développée pour prendre en charge le protocole fondé sur Q 931. La norme CAPI a été mise sur pied afin de constituer la base de nombreuses piles de protocole différentes pour les réseaux, la téléphonie et le transfert de fichiers.

CAPI a été englobée dans la norme européenne ETS 300 838 "**I**ntegrated **S**ervice **D**igital **N**etwork (réseau numérique à intégration de service ou RNIS); HPCI (Harmonized Programmable Communication Interface, interface de communication programmable harmonisée) pour le système RNIS".

BACK

Radio

Communication radio

La transmission de données sans fil par le biais d'un modem radio permet de communiquer avec :

- des unités distantes.
- des stations de mesure.
- des bâtiments externes et des installations sans personnel.
- des sites temporaires ou mobiles.

Les objectifs peuvent être divers : rassemblement de résultats de tests, contrôle ou réglage de l'équipement ou enregistrement de différents types d'alarmes.

La technologie de radiocommunication ainsi que le mode de planification, de dimensionnement et de gestion des bruits et interférences diffèrent fortement des communications locales dans un réseau de données.

Fonctionnement

L'équipement de communication inclut un modem radio, qui convertit le signal de données en ondes radio pour un canal spécifique correspondant à une bande passante précise. Il peut s'avérer nécessaire de traiter ou filtrer le signal de données avant de pouvoir le transmettre via le canal radio. Le signal est en outre modulé (par un modem) vers une fréquence porteuse adéquate afin de pouvoir être transmis au récepteur par le biais d'une liaison radio. La transmission est presque toujours analogique, que la source soit analogique ou numérique. L'équipement du récepteur décode puis reconstruit le signal original.

La plage de fréquences disponible pour la communication radio est limitée et réglementée par un accord international (ITU).

Les ondes radio se propagent dans l'atmosphère au niveau de la couche située entre l'ionosphère et la surface de la terre. Les conditions de communication peuvent présenter d'importantes variations selon la bande de fréquences, des ondes les plus longues (jusqu'à 1 000 mètres) dans la bande ELF aux plus courtes (10 mm) dans la bande EHF. Les modems radio fonctionnent dans la bande UHF à environ 440 mhz. La bande UHF située entre 300 et 3 000 mHz inclut les radars, la radio, la TV, la téléphonie mobile NMT, la radio mobile, les communications satellite, la radio amateur, le GSM et les téléphones sans fil.

Bande de fréquences

ELF	300–3000 Hz
VLF	3–30 kHz
LF	30–300 kHz
MF	300–3000 kHz
HF	3–30 MHz
VHF	30–300 MHz
UHF	300–3000 MHz
SHF	3–30 GHz
EHF	30–300 GHz

BACK

Atténuation et bruit

La propagation d'une onde radio est affectée par les couches de sol et d'air qu'elle traverse. Les bandes de fréquences des modems radio, qui incluent des longueurs d'ondes d'environ 1 mètre, peuvent rencontrer de nombreux obstacles, tels que les collines et bâtiments, susceptibles de générer une zone d'ombre radio (cf. téléphonie mobile), en plus des interférences intermittentes d'autres équipements. Ces interférences suscitées par des objets (évanouissements dus aux zones d'ombres ou aux interférences) entraînent une atténuation ou une distorsion du signal.

Le signal aboutissant au récepteur est souvent très faible par rapport au signal émis, mais cela n'implique pas nécessairement une perte de qualité de la communication. La source du problème réside dans les interférences échappant à notre contrôle, dans le bruit ajouté au signal. Ces perturbations ne sont pas l'apanage de l'équipement de réception : elles se manifestent aussi sous la forme de bruit thermique (agitation thermique de particules), de bruit atmosphérique (phénomènes électriques tels que les éclairs), de bruit cosmique (rayonnement naissant à fréquence radioélectrique du soleil ou 'bruit galactique') et de bruit généré localement (équipement électrique dans le voisinage du récepteur).

BACK

Antennes

Terminologie

Le domaine des communications radios et des antennes demande la compréhension de quelques termes et expressions de base. La première formule fondamentale à connaître met la fréquence (f) en corrélation avec la longueur d'onde (l) via l'équation suivante : l [m] = 300 / f [MHz].

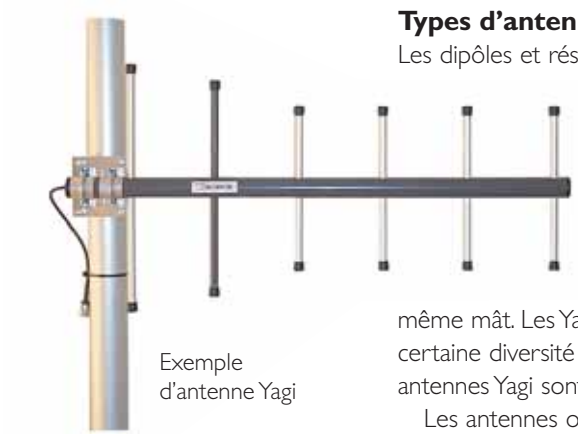
Le diagramme de rayonnement englobe les caractéristiques de rayonnement tridimensionnelles d'une antenne dans 2 plans : le champ électrique (E) et le champ magnétique (H). Le gain de l'antenne correspond à sa capacité de forcer le rayonnement dans une direction spécifique, aux dépens d'autres directions. Il s'exprime en dB par rapport à une référence : à titre d'exemple, 'dBi' et 'dBd' désignent respectivement le gain par rapport à une antenne isotrope et à une antenne dipôle. La polarisation se définit comme étant le plan du champ électrique E de l'antenne, et peut être verticale, horizontale, inclinée ou circulaire. L'orientation physique de l'antenne est généralement équivalente à sa polarisation. Les polarisations orthogonales présentent une perte de 21 dB. Dans la pratique, toutes les antennes d'un système devraient présenter la même polarisation.

L'impédance d'une antenne correspond à sa résistance AC et à sa réactance dans la même bande d'activité. La valeur par défaut de l'impédance nominale est de 50 ohms. La bande passante correspond à la plage de fréquences dans laquelle les caractéristiques de l'antenne – impédance, gain et diagramme de rayonnement, par exemple – demeurent conformes aux spécifications. Le terme 'atténuation', couramment utilisé, concerne essentiellement les systèmes d'alimentation et la propagation radio. Son unité est également le dB.

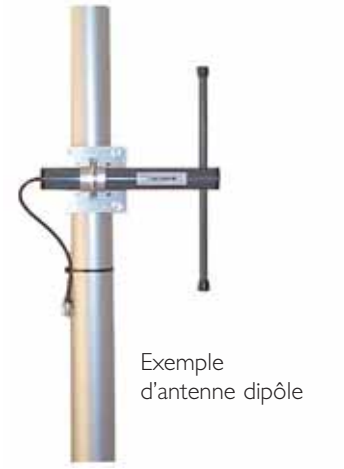
L'antenne et ses composants

Une antenne est un dispositif électromécanique dont le rôle consiste à diffuser la puissance de l'émetteur le plus efficacement possible et d'une manière spécifique. Un diviseur de puissance harmonise et combine des charges ou sources multiples, et répartit la puissance entre elles de manière équitable, sans perturber l'impédance caractéristique du système. On utilise des diviseurs dans des réseaux d'antennes, afin de combiner plusieurs antennes, ou dans des faisceaux de distribution RF. Une ligne d'alimentation est un câble d'interconnexion entre un équipement radio et une antenne. Les systèmes d'alimentation tendent à subir des pertes, de sorte qu'il faut choisir leur type avec soin selon la distance et la fréquence d'exploitation requises. Il est possible de placer des parafoudres entre l'équipement radio et le système d'alimentation afin de protéger la radio contre les éclairs. Les parafoudres sont généralement des stubs quart d'onde court-circuités en DC. Lors de l'interconnexion de composants de circuits d'antenne, il convient de maintenir l'équilibre des impédances afin de fournir un débit de puissance idéal sans pertes supplémentaires dues aux réflexions. L'équilibre des impédances est habituellement mesuré en tant que VSWR (**V**oltage **S**tanding **W**ave **R**atio, rapport d'ondes stationnaires). Un VSWR de 1:1 est idéal mais dans la pratique, un rapport de 1:1,5 est plus réaliste.

BACK



Exemple d'antenne Yagi



Exemple d'antenne dipôle

Types d'antennes

Les dipôles et réseaux de dipôles sont constitués d'une ou plusieurs antennes dipôles, ainsi que de diviseurs de puissance combinant ces antennes. Il s'agit généralement d'antennes omnidirectionnelles ou d'antennes à source décalée. Les Yagi et réseaux de Yagi sont constitués d'une ou plusieurs antennes Yagi, ainsi que de diviseurs de puissance combinant ces antennes. Il s'agit toujours d'antennes directionnelles. Les Yagi à polarisation croisée sont une combinaison de deux antennes Yagi à alimentation indépendante, polarisation orthogonale et phase physique en quart d'onde sur le même mât. Les Yagi à polarisation croisée s'utilisent dans des applications requérant une certaine diversité de polarisation ou en mode de polarisation circulaire, lorsque deux antennes Yagi sont combinées avec un diviseur de puissance.

Les antennes omnidirectionnelles peuvent être des antennes demi-onde alimentées en extrémité, des antennes colinéaires ou des antennes à plan géométrique. Ces antennes rayonnent de manière égale dans toutes les directions.

Les antennes portables sont généralement des antennes quart d'onde flexibles appliquant des méthodes d'alimentation spécifiques, afin d'assurer un équilibre des impédances adéquat avec les équipements radio portables de petit format.

Propagation du signal

Les ondes radio se propagent essentiellement en ligne droite mais subissent également des courbures, des réflexions et des diffractions. D'habitude, elles se propagent simultanément selon différents modes et trajets. Cette propagation par trajets multiples entraîne une certaine instabilité du signal en fonction du temps, étant donné l'addition de plusieurs signaux présentant des phases différentes. Cela explique également pourquoi un déplacement physique mineur de l'antenne peut exercer une influence sur la puissance de signal indiquée.

L'horizon radio est environ 15 % plus lointain que l'horizon optique, en raison de la tendance des ondes radio à se courber.

BACK

Réseau radio

Il convient de calculer le budget de la liaison radio afin de savoir si la propagation laisse suffisamment de puissance et de marge à l'extrémité récepteur de cette liaison. Dans les calculs des liaisons radio, toutes les valeurs sont exprimées en dB, positifs ou négatifs, et additionnées. Les paramètres de calcul sont la distance, la fréquence, le terrain, la hauteur d'antenne, la puissance de l'émetteur, la sensibilité du récepteur, la perte du système d'alimentation, le gain de l'antenne et la perte de propagation. Le calcul du budget de liaison radio donne le même résultat dans les deux directions.

La couverture du réseau radio peut être améliorée par le biais de répéteurs installés à des emplacements adéquats et disposés en chaîne afin d'étendre la zone de couverture.

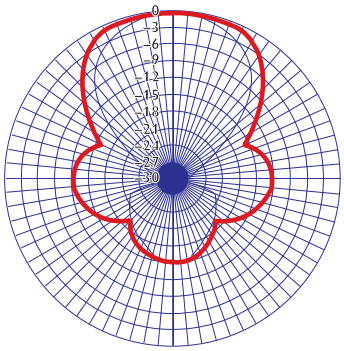


Diagramme de rayonnement Yagi

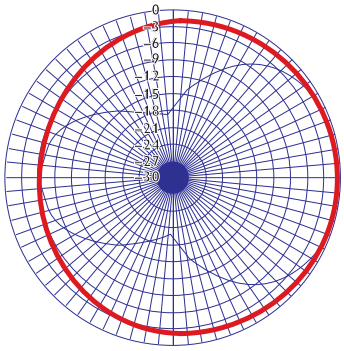


Diagramme de rayonnement dipôle

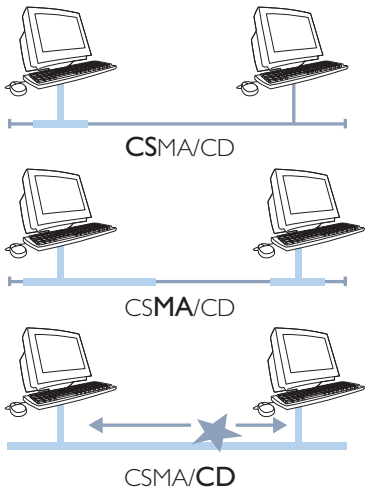
Ethernet industriel

Standard des communications depuis de nombreuses années, Ethernet constitue la base de la plupart des réseaux dans le monde. Bien que d'aucuns affirment depuis longtemps qu'il est en passe de se faire supplanter, Ethernet poursuit son évolution en offrant aux utilisateurs des fonctions répondant à leurs attentes. Récemment, Ethernet a également suscité l'agrément du marché industriel.

IEEE 802.3 Ethernet

Méthodes d'accès

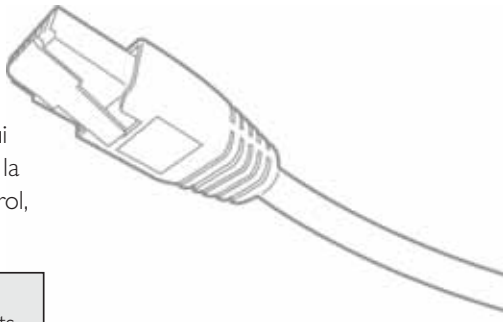
La communication entre deux ou plusieurs parties requiert un ensemble de règles. Cette vérité s'applique à toute situation, et particulièrement à la communication de données. Le mode de transmission des données sur une ligne est appelé "méthode d'accès". La méthode originale utilisée par Ethernet était le CSMA/CD, ce qui signifie : **C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etect (accès multiple par détection de porteuse et détection de collision). Il est important de préciser qu'Ethernet utilise deux méthodes d'accès, à savoir l'accès constant ou le CSMA/CD. Le CSMA/CD est régulièrement mentionné dans la documentation mais n'est pas si couramment utilisé de nos jours. Il s'inscrit dans un contexte historique, raison pour laquelle nous allons décrire brièvement ses divers composants :



- **C**arrier **S**ense (détection de porteuse) signifie qu'avant d'émettre, une unité doit vérifier si quelqu'un utilise le réseau. Si tel est le cas, elle devra attendre avant d'effectuer la transmission.
- **M**ultiple **A**ccess (accès multiple) signifie que tout le monde peut utiliser le réseau mais pas simultanément.
- **C**ollision **D**etect (détection de collision) signifie que le système doit pouvoir détecter deux ou plusieurs unités effectuant une transmission en même temps. Si une collision est détectée, un signal de collision sera transmis et toutes les unités concernées cesseront d'émettre. Elles observeront un délai aléatoire avant d'effectuer de nouvelles tentatives, de manière à minimiser le risque de transmission simultanée. Naturellement, les collisions ralentissent le trafic du système. Un réseau saturé entraîne de nombreuses collisions, qui génèrent davantage de trafic sur le réseau, ce qui provoque de nouvelles collisions, etc. Certains équipements sont pourvus de diodes indiquant les collisions, de sorte que vous puissiez vérifier aisément la charge du réseau. L'avantage d'un réseau CSMA/CD réside dans le fait que tous les équipements peuvent transmettre des données à n'importe quel moment, contrairement aux systèmes à interrogation ou aux réseaux Token Ring, où la transmission fait l'objet d'un contrôle strict.

BACK

Adresses et paquets Ethernet



Tous les équipements Ethernet disposent d'une adresse identifiant chaque nœud du réseau. Cette adresse est programmée par le fabricant dans le dispositif, par exemple une carte réseau. Elle ne peut pas être modifiée par l'utilisateur ni par un logiciel, ce qui signifie qu'il n'y a pas (qu'il ne devrait pas y avoir) deux cartes réseau correspondant à la même adresse. Cette adresse est souvent appelée l'adresse MAC **M**edia **A**ccess **C**ontrol, contrôle d'accès au support.

Préambule 8 octets	Adresse de destination 6 octets	Adresse de la source 6 octets	Type 2 octets	Données 46 – 1.500 octets	CRC 4 octets

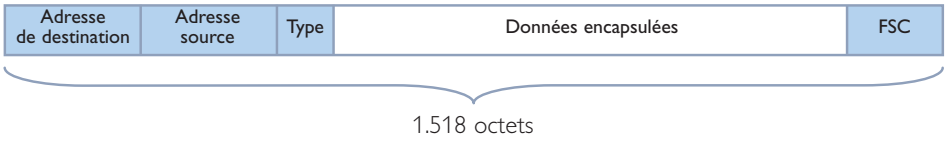
Le paquet Ethernet contient les informations suivantes :

- **Préambule.** Le préambule est un champ de 64 bits (8 octets) contenant un système de synchronisation constitué de uns et de zéros en alternance, terminés par deux uns consécutifs. Une fois la synchronisation établie, le préambule est utilisé afin de localiser le premier bit du paquet. Ce préambule est généré par la carte d'interface LAN.
- **Adresse de destination.** Le champ d'adresse de destination est un champ de 48 bits (6 octets) spécifiant la ou les stations auxquelles le paquet doit être envoyé. Chaque station examine ce champ afin de déterminer si elle doit accepter le paquet.
- **Adresse source.** Le champ d'adresse source est un champ de 48 bits (6 octets) contenant l'adresse unique de la station qui transmet le paquet.
- **Champ type.** Le champ type est un champ de 16 bits (2 octets) identifiant le protocole de haut niveau associé au paquet. Il est interprété au niveau des liens de données.
- **Champ de données.** Le champ de données se compose de 46 à 1.500 octets (champ de 8 bits) contenant chacun une séquence arbitraire de valeurs. Le champ de données correspond aux informations transmises par la Couche 3 (Couche Réseau). Les informations – ou le paquet – transmises par la Couche 3 sont scindées en trames d'informations de 46 à 1.500 octets par la Couche 2.
- **Champ CRC.** Le champ CRC (Cyclic Redundancy Check, contrôle de redondance cyclique) est un champ de 32 bits destiné à vérifier les erreurs. Le contrôle CRC est généré en fonction des champs d'adresse de destination, de type et de données.

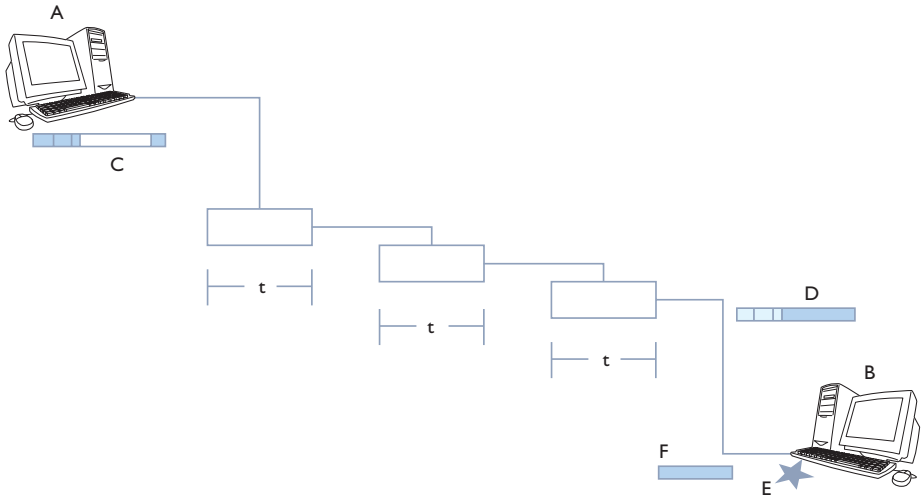
BACK

Domaine de collision

Un domaine de collision est un segment de réseau où l'équipement doit pouvoir détecter et gérer les collisions (dues aux envois simultanés de plusieurs dispositifs). Les données entrant en collision ne disparaissent pas automatiquement : le système CSMA/CD assure leur retransmission correcte en temps opportun. Le nombre de tentatives de retransmission peut être limité à 16, et les données ne pourront être perdues qu'à partir de ce moment. D'un autre côté, ce phénomène est habituel étant donné le grand nombre de tentatives de retransmission sur un réseau Ethernet fortement surchargé.

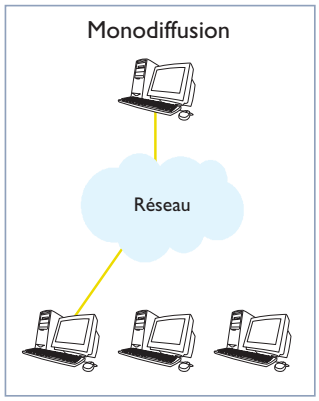


A la base, un paquet Ethernet est constitué de 1.518 octets. 4 octets seront ajoutés si vous utilisez un VLAN, ce qui donne un total de 1.522 octets. Cette règle, avec la vitesse du réseau, donne les conditions requises pour connaître la vitesse à laquelle un message atteindra les dispositifs les plus distants du réseau. Il ne faut, en aucune circonstance, réaliser un domaine de collision empêchant le dispositif d'envoi d'identifier une collision avant d'être sûr que le paquet est parvenu au récepteur. Le réseau et l'équipement installé déterminent la propagation maximale sur un domaine de collision, étant donné que tous les équipements ajoutent un délai, également appelé 'latence'.



BACK

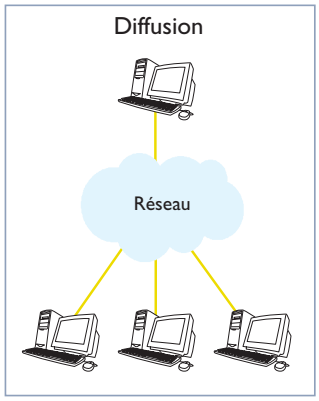
- Supposons que **A** souhaite envoyer un paquet à **B**.
- Le réseau comprend divers équipements associés à un délai interne (**t**).
- **A** vide son tampon d'envoi en continu si aucune collision n'est détectée.
- Une collision survient sur le nœud placé à l'extrémité du réseau (**E**).
- Les données (**D**) ne sont pas toutes reçues, ce qui empêche (**B**) de les interpréter.
- Le signal de collision (**F**) est renvoyé à l'émetteur (**A**).
- Si le domaine est trop vaste, le signal de collision ne parvient pas à (**A**) avant que le tampon d'émission soit vide. Il devient donc impossible de retransmettre le paquet.



Réseaux IP

Protocole Internet

Le Protocole Internet – IP – a été conçu pour les connexions effectuées au sein d'un réseau ou entre plusieurs réseaux. Ses spécifications ont été établies compte tenu du développement continu de nouvelles technologies et de nouvelles méthodes de transfert, ce qui a débouché sur une norme ouverte et essentiellement indépendante du réseau et du support sous-jacents. TCP/IP est une famille de protocoles déployée entre différentes couches du modèle OSI.

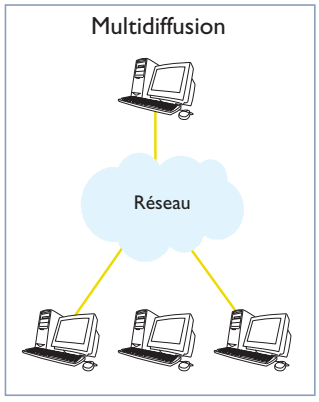


Méthodes d'adressage

Une grande partie des informations d'un réseau transite d'un émetteur unique vers un récepteur unique. Cette situation est tout à fait naturelle dans la plupart des cas, par exemple la communication entre un automate programmable et un dispositif E/S. Ce type de transfert est généralement appelé « monodiffusion » (Unicast).

Le contraire d'une monodiffusion est une « diffusion » (Broadcast), qui correspond au mode de transmission appliqué par la radio et la télévision : un émetteur et plusieurs récepteurs. La diffusion réside dans l'envoi de l'information à tout le monde. Cette technique s'utilise dans certains réseaux informatiques fermés, mais une diffusion globale sur Internet est impossible car elle surchargerait le réseau.

La « multidiffusion » (Multicast) est une technique située entre la monodiffusion et la diffusion. L'information n'est pas envoyée à tout le monde comme dans la diffusion, mais une même information peut avoir plusieurs destinataires, contrairement à la monodiffusion. Le recours à la multidiffusion permet de réaliser des réseaux de distribution convenant à la surveillance vidéo ou aux transmissions télévisuelles via Internet (information ayant un émetteur et plusieurs récepteurs). La multidiffusion ouvrira de nouvelles perspectives pour Internet et l'empêchera de s'effondrer à cause d'une surcharge.



Octet	1	2	3	4
	192.	168.	3.	23

Adressage dans un réseau

Avant de décrire la structure d'une adresse IP, il convient d'expliquer certains concepts :

- Une adresse IP est constituée de quatre octets.
- Un octet se compose de 8 bits de données, par exemple, 11000000, ce qui correspond à la valeur décimale 192 (voir l'octet 1 dans l'exemple ci-contre).
- A leur tour, les adresses sont réparties en différentes classes (A, B, C, D et E) qui décrivent un intervalle d'adresses. Il existe actuellement cinq classes d'adresses, dont les trois premières (A-C) sont utilisées pour différents types de réseaux, l'adresse IP étant scindée en deux segments (réseau et ordinateur). A cela s'ajoutent les groupes D et E. Une adresse D est une adresse de multidiffusion, tandis que les adresses E sont réservées à une utilisation ultérieure.
- Les adresses IP dans les réseaux de classe A, B et C sont scindées en deux parties : une partie réseau et une partie ordinateur.

Classe	Premier octet	Intervalle d'adresses
A	0xxx xxxx	**0**.0.0.0 à **127**.255.255.255
B	10xx xxxx	**128**.0.0.0 à **191**.255.255.255
C	110x xxxx	**192**.0.0.0 à **223**.255.255.255
D	1110 xxxx	**224**.0.0.0 à **239**.255.255.255
E	1111 xxxx	**240**.0.0.0 à **247**.255.255.255

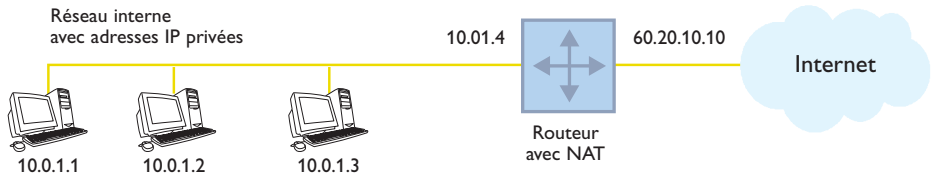
Les réseaux A, B et C diffèrent par le nombre de bits utilisés pour identifier le réseau et les dispositifs :
L'identité du réseau de classe A comprend 8 bits (1 octet), celle de la classe B 16 bits et celle de la classe C 24 bits. Cela permet d'adresser un nombre différent de dispositifs dans les réseaux respectifs. Voir également la répartition en sous-réseaux ci-après.

Classe					Valeur décimale dans l'octet 1	Nombre max. de dispositifs dans le réseau
A	Réseau	Ordinateur	Ordinateur	Ordinateur	0 à 127	16 777 215
B	Réseau	Réseau	Ordinateur	Ordinateur	128 à 191	65 535
C	Réseau	Réseau	Réseau	Ordinateur	192 à 223	255

BACK

Adresses privées et publiques

Il se peut que vous ne puissiez ou vouliez pas utiliser d'adresses IP publiques sur votre réseau interne. Dans ce cas, vous pouvez utiliser des adresses IP privées (RFC1918), mais elles ne fonctionneront pas sur une connexion Internet. La solution réside alors dans l'utilisation d'une NAT (**N**etwork **A**ddress **T**ranslation, translation d'adresse réseau).



Un routeur ou "pare-feu" compatible avec la NAT traduit les adresses privées en adresses publiques :
Si un ordinateur dont l'adresse est 10.0.1.2 a besoin d'accéder à Internet, l'élément adressé sera 10.0.1.4, c'est-à-dire le "portail par défaut" ou la "sortie". Lorsque les données de l'adresse 10.0.1.2 franchiront le routeur, la NAT traduira l'adresse IP interne 10.0.1.2 en 60.20.10.10, c'est-à-dire l'adresse IP à l'"extérieur". Cette procédure permet à une adresse IP interne de communiquer avec d'autres ordinateurs sur Internet. Peu importe si une autre adresse IP interne communique en même temps, car le routeur gère l'adéquation entre les différentes sessions et les adresses IP internes, et s'assure que le trafic transite par l'ordinateur adéquat sur le réseau interne.

L'IANA (**I**nternet **A**ssigned **N**umbers **A**uthority, autorité d'affectation des numéros Internet) a réservé les trois blocs d'adresses suivants pour les adresses IP dans les réseaux privés :
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

BACK

Ipv4 et Ipv6

IPv6 est la version 6 du protocole Internet. Cette nouvelle version a été conçue à la fin des années 1990 afin de remplacer l'actuelle, IPv4 (version 4), transition essentiellement due au fait que les adresses IP commencent à toucher à leur fin. La principale différence entre IPv6 et IPv4 réside dans l'allongement de l'adresse de 32 bits à 128 bits. Cela signifie que le nombre d'adresses possibles est passé de 4 milliards à un nombre véritablement astronomique.

En-tête Ipv6

<table>
<tr><td colspan="3">Adresse source à 128 bits</td></tr>
<tr><td>Capacité utile</td><td>En-tête suivant</td><td>Limite de saut</td></tr>
<tr><td colspan="3">Adresse source à 128 bits</td></tr>
<tr><td colspan="3">Adresse de destination à 128 bits</td></tr>
</table>

Division en sous-réseaux

Il est rare que des réseaux locaux totalisent plus de quelques centaines de dispositifs. L'association de ce type de réseau à sa propre classe A ou B (plus de 16 millions de réseaux avec 65.000 dispositifs possibles sur chacun) constitue donc un immense gaspillage d'adresses disponibles. Voilà pourquoi la plupart de ces classes sont scindées en **sous-réseaux**, utilisant une partie de l'identité du dispositif en tant que type d'adresse réseau. Ainsi, la "frontière" entre l'adresse réseau et l'identité du dispositif est "déplacée" de manière à augmenter le nombre d'identités réseau disponibles, tandis que le nombre de dispositifs dans le sous-réseau diminue. Pour ce faire, on utilise un **masque réseau** où les bits associés au réseau sont réglés sur un (et les bits de l'ordinateurs sur zéro).

Les réseaux plus petits sont plus faciles à administrer : le trafic de données dans le sous-réseau est moins intense, le réseau physique devient plus facile à configurer et à entretenir (vous pouvez, par exemple, utiliser différents sous-réseaux à différents étages d'un bâtiment), etc.

BACK

Les masques réseau standard (c.-à-d. sans sous-réseau) ci-après s'appliquent aux classes d'adresses A, B et C :

Classe d'adresse	Masque réseau	Valeur binaire Octet 1	Valeur binaire Octet 2	Valeur binaire Octet 3	Valeur binaire Octet 4
A	255.0.0.0	11111111	00000000	00000000	00000000
B	255.255.0.0	11111111	11111111	00000000	00000000
C	255.255.255.0	11111111	11111111	11111111	00000000

Comme expliqué précédemment, une adresse IP de classe B consiste en deux éléments de tailles égales, comptant 2 octets chacun pour l'identité du réseau et du dispositif. Ces éléments peuvent s'écrire sous la forme "N.N.D.D", où N représente l'octet associé à l'identité du réseau (Network) et D, l'octet associé à l'identité du dispositif. Le masque réseau devient dès lors 255.255.0.0.

Si le 3ème octet est utilisé dans son intégralité pour définir le sous-réseau au lieu d'une identité de dispositif, l'adresse pourra être interprétée sous la forme N.N.N.E. Le masque de réseau deviendra donc 255.255.255.0. Cela signifie que nous disposons de 254 réseaux de type C comptant chacun 254 ordinateurs (la première et la dernière adresse du réseau ainsi que les sections des ordinateurs sont réservées).

En principe, tout bit d'un octet peut être utilisé pour définir un sous-réseau. On réserve ordinairement les bits les plus élevés à cet effet, car cela simplifie considérablement la gestion. Si, par exemple, les trois premiers bits d'une adresse C sont affectés à des adresses de sous-réseaux, le réseau C sera divisé en 6 sous-réseaux (voir les combinaisons de réseaux possibles ci-dessous). Deux séquences binaires de l'identité du dispositif (11111 et 00000) sont réservées à la diffusion et à l'identité du réseau, raison pour laquelle 30 adresses seront disponibles sur chacun de ces réseaux.

Masque	Masque réseau de type C	3 premiers bits dans le masque de type C	Autres bits dans le masque de type C	Travail sous-réseau	Nombre d'identités de dispositifs
255.255.32.0	32	001	00000	1	30
255.255.64.0	64	010	00000	2	30
255.255.96.0	96	011	00000	3	30
255.255.128.0	128	100	00000	4	30
255.255.160.0	160	101	00000	5	30
255.255.192.0	192	110	00000	6	30

BACK

Ports

Une application reçoit des données sur un numéro de port spécial, qui identifie la communication avec cette application.

A titre d'exemple, un ordinateur peut être à la fois un serveur Web, un serveur d'e-mails et un serveur DNS actifs en même temps. Pour empêcher une collision du trafic vers les différentes applications, il faut le scinder via une préaffectation du port à l'application. Les numéros de ports compris entre 1 et 1024 sont des numéros connus et ne doivent pas être utilisés pour des applications autres que celles spécifiées.

Exemples de numéros de ports connus :

21	ftp	Transfert de fichiers
23	Telnet	Telnet
25	smtp	Courrier, Transfert de courrier simple
80	http	www

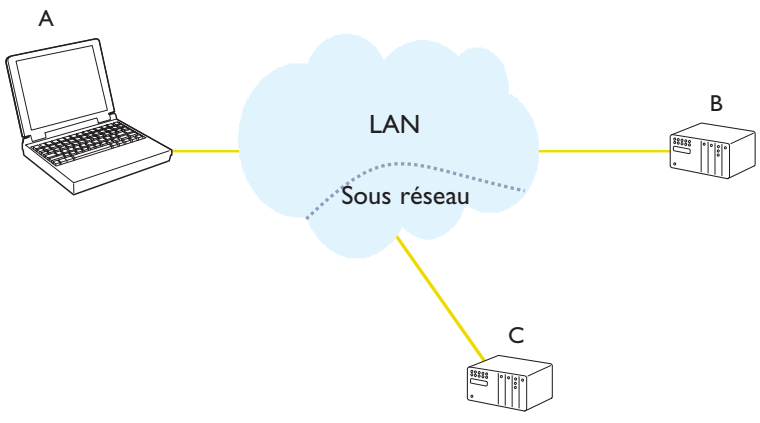
Vous trouverez une liste complète sur le site www.iana.org/assignments/port-numbers

Adresse MAC

Abréviation d'adresse Media Access Control, une adresse matérielle qui identifie de manière unique chaque nœud d'un réseau Ethernet. Cette adresse est programmée par le fabricant dans le dispositif, par exemple une carte réseau. Elle ne peut pas être modifiée par l'utilisateur ni par un logiciel, ce qui signifie qu'il n'y a pas (qu'il ne devrait pas y avoir) deux cartes réseau correspondant à la même adresse MAC.

ARP

Les ordinateurs, ou autres équipements informatiques, connectés à un réseau TCP/IP disposent tous au moins d'une adresse IP. L'adresse IP est également considérée comme l'adresse logique car elle est généralement implémentée dans les logiciels et peut être



modifiée selon l'emplacement physique du matériel dans le réseau. Les dispositifs possèdent également une adresse physique, appelée "adresse MAC" dans les réseaux Ethernet. Elle est unique pour chaque composante du matériel connecté.

Lorsque deux dispositifs (A) et (B) utilisent le protocole TCP/IP pour communiquer sur un réseau Ethernet, ils doivent conserver leurs adresses MAC mutuelles, étant donné que toutes les communications transitant par Ethernet concernent des adresses MAC.
Voilà pourquoi les dispositifs A et B disposent de leur propre table ARP d'adresses IP et d'adresses MAC associées.
Le protocole ARP (**A**ddress **R**esolution **P**rotocol, protocole de résolution d'adresse) régit la mise à jour dynamique des tables ARP, de sorte que l'association entre les adresses IP et MAC soit toujours connue.

- Supposons que l'ordinateur A souhaite communiquer avec l'automate programmable B. L'ordinateur A connaît d'ores et déjà l'adresse IP de B (configuration manuelle par un opérateur, par exemple) mais ignore l'adresse MAC de B. La communication ne peut pas démarrer tant que A ne connaît pas l'adresse MAC de B.
- A découvre que B se trouve sur le même réseau en comparant l'adresse IP de la destination et le masque réseau.
- A émet une requête ARP sous la forme d'un message de diffusion. La requête contient l'adresse IP et MAC de A ainsi que l'adresse IP de B.
- Toutes les unités du réseau comprennent le message, mais seul B reconnaît son adresse IP et envoie une réponse ARP contenant l'adresse MAC de B.
- La table ARP de A peut alors être mise à jour de manière à intégrer l'adresse MAC de B.

Point à Point (PPP)

Il se peut également que vous deviez communiquer à l'aide du protocole TCP/IP via une connexion série. Cette situation concerne l'accès Internet par le biais d'un modem ou la connexion à un réseau local. Le mode de communication varie d'une application à l'autre et utilise PPP (**P**oint to **P**oint **P**rotocol, protocole point à point), qui est sans doute le protocole de liaison le plus utilisé pour les ordinateurs connectés à distance à un réseau. Exemples de communications série : modem télécom, modem connecté à sa propre ligne louée, RNIS, GSM, radio ou modems courte distance.

Sécurité (CHAP et PAP)

Le protocole PPP est souvent utilisé pour les connexions distantes point à point, qu'il s'agisse d'une ligne commutée, RNIS ou louée. Une certaine forme de sécurité est généralement requise entre les parties communicantes. Le protocole PPP supporte deux méthodes de vérification de l'utilisateur : PAP (**P**assword **A**uthentication **P**rotocol, protocole d'identification de mot de passe) et CHAP (**C**hallenge **H**andshake **A**uthentication **P**rotocol, protocole d'authentification par défi-réponse). L'authentification, la vérification de messages, n'est pas obligatoire sous PPP, de sorte que les parties sont libres de communi-

quer sans s'identifier ou négocier le protocole requis. La principale règle est d'opter en premier lieu pour le protocole CHAP. PAP n'est généralement choisi que si l'une des parties n'est pas compatible avec CHAP.

Le protocole PAP fonctionne d'une manière similaire à la connexion par le biais d'un terminal : vous devez introduire votre nom d'utilisateur et un mot de passe. L'authentification n'a lieu qu'une fois la connexion établie, et jamais en cours de communication.

- La procédure PAP démarre lorsqu'une des parties envoie une requête d'authentification, contenant son nom et son mot de passe. Ce paquet est répété jusqu'à ce que l'autre partie réponde.
- Une fois le nom et le mot de passe acceptés, le destinataire répond par le biais d'un 'Ack' (accusé de réception) d'authentification. Sinon, il envoie un 'Nak' (AR négatif), et coupe la connexion.

L'utilisation du protocole PAP est une méthode d'authentification relativement vulnérable car le nom et le mot de passe sont transmis en texte clair sur le lien. Le mot de passe peut-être intercepté aisément par des utilisateurs clandestins, et aucune protection n'est prévue contre les attaques répétées de type 'essais et erreurs'.

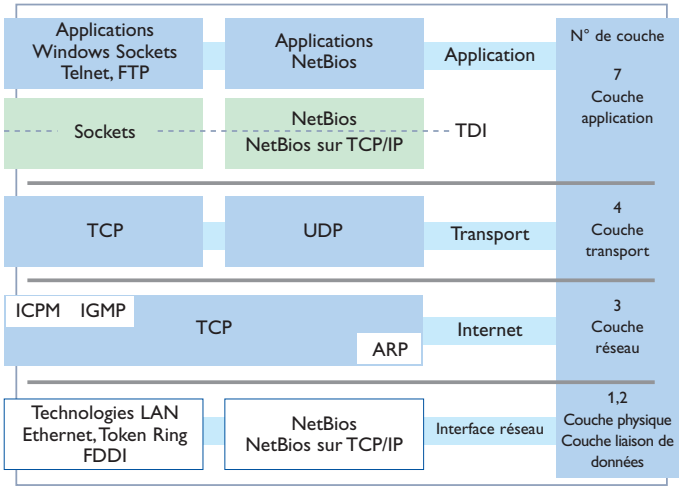
Le protocole CHAP est beaucoup plus sûr que PAP.

CHAP utilise un mot de passe crypté dans le cadre d'une procédure à trois étapes. De plus, l'authentification est partiellement effectuée durant l'établissement de la liaison, et peut être répétée à tout moment. L'objectif de la répétition périodique est de limiter le temps d'ouverture du système, et donc son exposition à une attaque. C'est toujours l'authentificateur (destinataire) qui détermine la fréquence des authentifications. Les trois étapes de l'authentification sont les suivantes :

- Lorsque la liaison est établie, l'une des parties (authentificateur) envoie un défi à son correspondant.
- Celui-ci calcule une valeur cryptée basée sur le défi et son mot de passe. La valeur cryptée est ensuite renvoyée à l'authentificateur.
- L'authentificateur fait un calcul équivalent (le défi et le mot de passe du correspondant sont connus) puis compare la valeur escomptée avec celle du correspondant. Si la valeur est identique, l'authentification est confirmée, sinon la connexion est interrompue.

TCP/IP et UDP/IP

Dans le modèle OSI, chaque couche est responsable des données qui la traversent. La couche de transport assume la responsabilité du transfert de données, pour lequel deux protocoles sont disponibles : TCP et UDP.



UDP

UDP (**U**ser **D**atagram **P**rotocol, protocole de datagramme utilisateur) est généralement classé parmi les protocoles sans connexion. Cela signifie que les données peuvent être envoyées indépendamment de l'existence ou non du destinataire. De même, le destinataire ne signalera pas à l'émetteur s'il a reçu ou non les données. Comme les données sont transmises sans établissement d'une connexion, le transfert est plus efficace et généralement plus rapide. UDP est par conséquent utilisé dans des applications nécessitant une utilisation efficace de la bande passante et permettant la retransmission des données perdues si nécessaire.

UDP peut être comparé à l'envoi d'une lettre par la poste, les données étant placées dans une enveloppe adressée. Une fois la lettre postée, vous vous attendez à ce que la poste la distribue correctement. Une autre fonction importante d'UDP réside dans la possibilité de "diffusion" et de "multidiffusion", c'est-à-dire l'envoi d'un message à plusieurs destinataires. C'est la principale raison d'opter pour UDP.

TCP

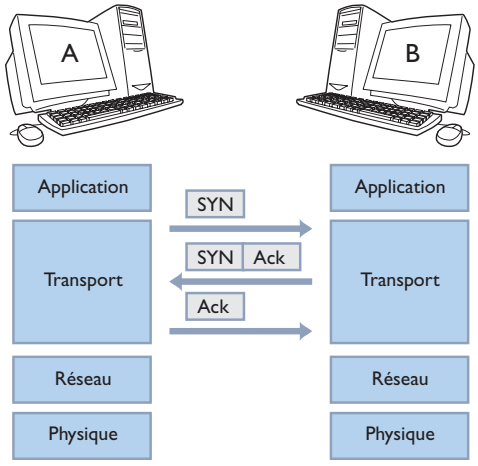
TCP (**T**ransmission **C**ontrol **P**rotocol, protocole de contrôle de transmission) est un protocole orienté sur la connexion, ce qui signifie qu'une session doit être préalablement ouverte pour permettre l'échange des données. TCP assume une plus grande responsabilité envers le transfert de données qu'UDP, car les données transmises sont validées par le destinataire. Ce dernier doit renvoyer un accusé de réception (ACK) pour chaque paquet de données envoyé. Si aucun ACK n'est reçu, le paquet sera retransmis, ce qui garantit l'arrivée des données à destination.

Une autre fonction du protocole TCP est qu'il maintient le contrôle de la séquence et du flux lors du transfert de grandes quantités de données. Plusieurs paquets TCP peuvent parvenir au destinataire dans un ordre différent de celui de leur envoi. Le protocole TCP garantit que les paquets seront regroupés dans la séquence adéquate, car ils sont associés à un numéro de séquence. Vu la nécessité d'établir préalablement une session et d'accuser réception des transferts, la transmission de données par TCP est plus lente et exige un débit plus élevé qu'avec UDP.

BACK

Etablissement d'une connexion TCP

Une connexion s'établit par le biais d'une procédure de contrôle de flux en trois étapes :



- Le client A envoie une requête de connexion avec le bit SYN actif. Cela permet au client de synchroniser un numéro de séquence avec le serveur (B).
- Le serveur (B) envoie un accusé de réception (ACK) au client ayant activé son bit SYN, ce qui a également permis au serveur de synchroniser son numéro de séquence avec le client.
- Enfin, le client envoie un accusé de réception (ACK).

Le transfert s'effectue avec un ou plusieurs octets, qui sont numérotés et font l'objet d'un accusé de réception.

Une connexion est terminée lorsque le client (A) vérifie le paquet TCP local et que toutes les informations ont été transférées et réceptionnées. Un paquet TCP au bit FIN activé est ensuite envoyé. Le serveur (B) envoie un accusé de réception mais continue à transmettre des données si l'application le demande. Une fois cette opération terminée, le serveur (B) envoie un paquet TCP dont le bit FIN est activé.

Construction d'un réseau

Les dispositifs d'un réseau

Répéteurs

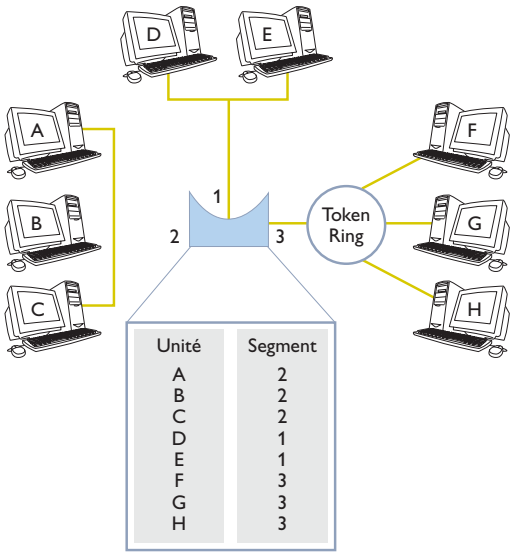
Un répéteur peut être comparé à un amplificateur : il n'a aucune intelligence et se contente de reproduire des signaux. Les signaux sont atténués en fonction de leur fréquence et de la longueur du support, ce qui limite la portée du réseau. L'utilisation d'un répéteur permet d'allonger un support en reproduisant le signal, qui conserve donc son état initial en termes de puissance et d'aspect. Un répéteur agit dans le même domaine de collision (HDPX CSMA/CD), et il n'est pas possible d'installer un nombre illimité de répéteurs au sein d'un segment vu le surcroît de latence dans chaque répéteur.

Pont (Bridge)

Un pont permet de séparer deux ou plusieurs domaines de collision et peut être utilisé pour connecter différentes topologies. Les ponts détectent et consignent les adresses associées aux différents segments, et apprennent dès lors à quel segment les dispositifs sont connectés.

Un pont s'utilise, par exemple, pour combiner Ethernet avec Token Ring. Les ponts fonctionnent généralement de manière sélective, c'est-à-dire qu'ils filtrent les adresses de sorte que les données n'atteignent que les adresses de destination (les dispositifs A et B ne communiqueront que sur le segment 2, par exemple). Le réseau est dès lors scindé et le trafic interne ne charge pas d'autres segments.

Un pont ne fonctionne que sur le trafic de routage de la couche MAC basée sur son adresse physique, tandis qu'un routeur prend ses décisions d'après les adresses de la couche 3

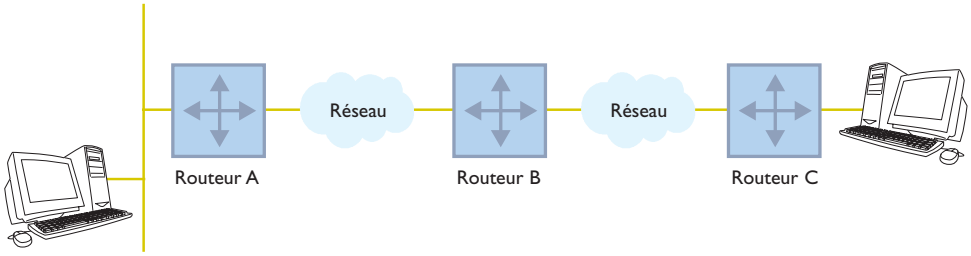


Unité	Segment
A	2
B	2
C	2
D	1
E	1
F	3
G	3
H	3

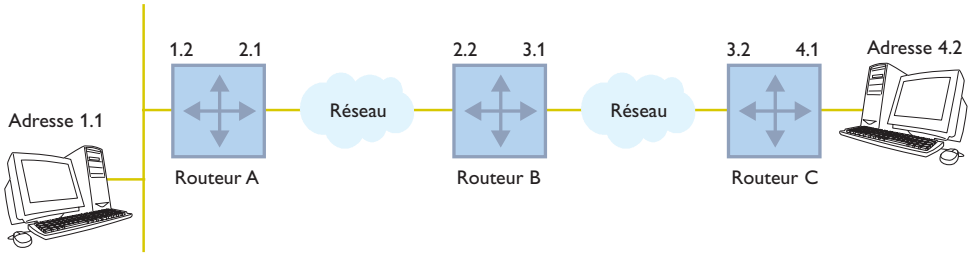
BACK

Routeur

Le terme 'router' signifie sélectionner ou trouver le trajet adéquat. Le routeur est un appareil ou – dans certains cas – un logiciel qui détermine le point vers lequel un paquet doit être envoyé pour atteindre sa destination finale (dans le cas d'un LAN, le routeur correspond à la destination finale). Il s'agit donc d'un dispositif de réseau reliant deux ou plusieurs réseaux séparés logiquement. Il ne connecte pas des réseaux à l'aveuglette, mais agit davantage en tant que commutateur de paquets pour l'interconnexion de réseaux locaux sur de courtes ou longues distances. En plus de l'équipement installé dans des réseaux distincts, le réseau peut également utiliser différentes normes et topologies.



Comme tous les dispositifs possèdent une adresse unique, l'équipement émetteur peut toujours effectuer un envoi à l'adresse d'un destinataire spécial dans le même ou un autre réseau. Si l'adresse d'un destinataire figure dans un autre réseau, les données seront acheminées de manière adéquate via une connexion logique entre les réseaux. Ces informations sont regroupées au sein d'une table de routage, qui définit les options de routage ainsi que les autres possibilités de connexion.



L'exemple ci-contre applique une technique d'adressage simplifiée. Les adresses des réseaux sont 1, 2, 3 ou 4. Quant aux dispositifs de ces réseaux, ils possèdent l'adresse 1.1, 1.2, etc.

Supposons que l'ordinateur associé à l'adresse 1.1 souhaite communiquer avec l'ordinateur 4.2. Le routeur A reçoit un paquet adressé à 4.2 et détecte que cette adresse fait partie d'un autre réseau, si bien que le paquet est routé plus avant, en l'occurrence vers 2.1 puis 2.2. La même procédure est appliquée entre les routeurs B et C. Enfin, le paquet arrive au routeur C et est transféré vers le réseau 4, à destination de l'ordinateur correspondant à l'adresse 4.2.

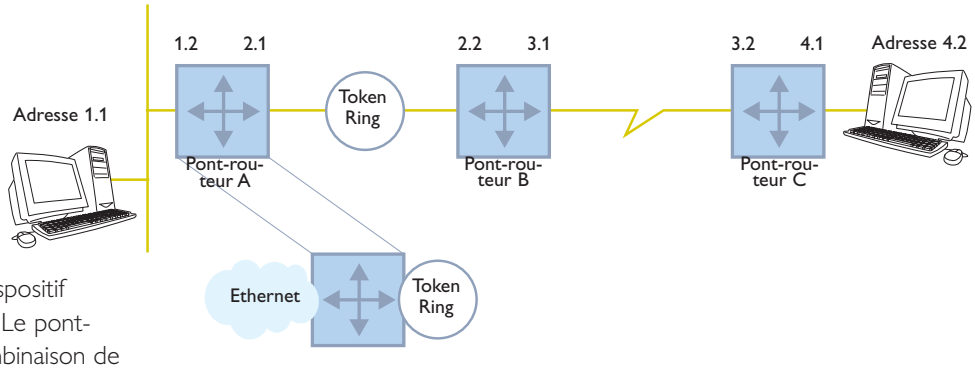
Outre le routage, le trafic peut généralement faire l'objet d'un contrôle et d'une filtration. Une table de routage indique les emplacements des différents équipements et réseaux. Elle peut être dynamique ou statique. Une table de routage dynamique est mise à jour automatiquement d'après la structure de l'environnement.

Le mode de routage du trafic est régi par un protocole de routage, par exemple RIP (**R**outing **I**nformation **P**rotocol, protocole de routage des informations) ou OSPF (**O**pen **S**hortest **P**ath **F**irst, le plus court chemin en premier).

Pont-routeur (Brouter)

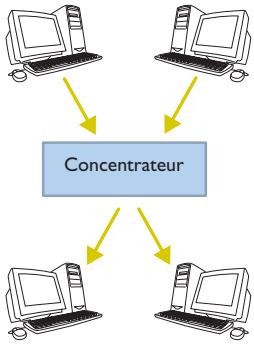
Le marché compte de nombreuses normes, dont les plus courantes sont Ethernet, Token Ring et FDDI. Elles utilisent toutes différents formats et techniques de communication, mais le mode d'adressage est commun et normalisé par le standard IEEE.

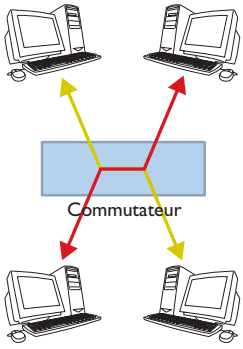
Un pont-routeur est une combinaison d'un pont et d'un routeur au sein du même dispositif. En fait, de nombreux routeurs sont des ponts-routeurs. Lorsque le dispositif doit transférer le même protocole au sein d'un LAN ou vers un autre LAN, c'est la fonction de pont qui s'en charge. D'un autre côté, lorsqu'un PC est connecté à un WAN (**W**ide **A**rea **N**etwork, réseau étendu), il faut davantage d'informations sur les connexions alternatives, de sorte que le dispositif requiert une table de routage. Le pont-routeur devient donc une combinaison de routeur et de pont.



Concentrateur (Hub)

Comme son nom l'indique, ce dispositif sert de connexion centrale au sein d'un réseau. Un concentrateur fonctionne comme un coupleur en étoile. Les données arrivant sur un port sont envoyées à tous les autres indépendamment du destinataire. Le concentrateur est le dispositif réseau qui a fait le succès de 10baseT. Il a ouvert de nouvelles perspectives pour la construction de réseaux, avec un équipement centralisé et des points de connexion sur chaque poste de travail. Il existe deux types de concentrateurs, les actifs et les passifs. Un concentrateur passif rassemble des segments de réseau sans amplifier le signal, tandis qu'un concentrateur actif agit de la même manière mais amplifie également le signal.





Commutateur (Switch)

Un commutateur est similaire à un concentrateur, en ce sens qu'il constitue le point de connexion central du réseau. La différence réside dans le fait que le commutateur consigne les dispositifs connectés à ses ports respectifs. Lorsque des données sont transmises à un dispositif du réseau, l'adresse du destinataire est vérifiée par le commutateur et les données ne sont envoyées qu'au port de connexion du dispositif concerné (réseau commuté). Cette procédure évite de surcharger le réseau d'un trafic inutile. Un autre avantage tient au renforcement de la sécurité, vu qu'il est plus difficile d'accéder aux informations non destinées à l'ordinateur en question.

Un commutateur de couche 2 est du type 'pont'.

Un commutateur de couche 3 est du type 'routeur'.

Les termes 'commutateur', 'pont' et 'routeur' sont donc synonymes dans certains contextes.

On parle aussi couramment de commutateurs administrés et non administrés. La différence réside dans le fait que l'on peut communiquer avec un commutateur administré (contrôlable), ce qui s'effectue généralement via SNMP. Voir les pages 138 à 143.

Passerelle (Gateway)

Une passerelle connecte des réseaux entre eux, mais sa tâche principale consiste à convertir les données entre différents protocoles, par exemple AppleTalk et TCP/IP. En plus de convertir des protocoles, une passerelle supporte aussi différents formats, codes de caractères, adresses, etc.

Pare-feu (Firewall)

Un pare-feu est un équipement ou logiciel spécial qui ne laisse passer des données que si des critères spécifiques ont été satisfaits. Tout autre trafic est refusé. Les utilisateurs d'un réseau peuvent donc être préservés d'un trafic interdit. On établit généralement un pare-feu entre un réseau local et Internet. Vous pouvez également avoir des pare-feu sur des réseaux internes ou combinés à des équipements permettant d'accéder à un réseau. Le trafic autorisé par le pare-feu est déterminé par des règles de complexité variable. Le moment, le lieu et le mode d'utilisation d'un pare-feu sont régis par les critères de sécurité du réseau. Le marché donne le choix entre de nombreux produits, d'une combinaison de matériel et logiciels aux pare-feux téléchargeables gratuitement sur votre propre ordinateur.

BACK

Concentrateur ou commutateur

Pourquoi un commutateur est-il nettement plus intéressant qu'un concentrateur, et quelle est la différence entre ces deux appareils ? Nous avons déjà expliqué que c'est le concentrateur qui a permis l'installation de réseaux couplés en étoile, et popularisé les systèmes à câbles structurés en combinaison avec Ethernet. Il repose néanmoins sur un concept simple : toutes les données transmises vers un port sont transférées vers les autres ports. Cela signifie que chaque périphérique capte tous les envois et que tous les périphériques se situent dans le même domaine de collision.

Le commutateur fonctionne plus intelligemment – soit par le biais de processeurs, soit par le biais de circuits intégrés spécifiques permettant de contrôler et de traiter les données reçues sur un port. Le commutateur identifie les équipements connectés à tel ou tel port et enregistre cette information dans sa mémoire d'adresses MAC. Il existe deux types de commutateurs : les commutateurs pseudo-transit (Cut-through) et les commutateurs à stockage et retransmission (Store and Forward). Les commutateurs pseudo-transit examinent l'adresse de destination et envoient les données au port destinataire, ce qui entraîne une collision si le port est utilisé par d'autres trafics où le dernier paquet se perd. Ces commutateurs sont très rapides. Les commutateurs à stockage et retransmission, quant à eux, copient le paquet reçu et le placent dans la mémoire tampon avant de localiser le port destinataire. La transmission n'a lieu qu'une fois le port libéré. Le paquet n'est donc pas perdu. Les données peuvent également être hiérarchisées, le réseau peut être scindé en LAN virtuels, etc.

La liste ci-dessous énumère quelques différences entre un concentrateur et un commutateur.

Concentrateur	Commutateur
Communication en semi-duplex.	Semi-duplex ou duplex intégral (HDX/FDX).
Etend le domaine de collision.	Segmente le réseau.
Bande passante partagée par l'ensemble du réseau.	Bande passante adaptée à la demande (système à auto-apprentissage).
Faible utilisation de la bande passante en raison du système CSMA/CD.	Stockage et retransmission (contrôle du paquet avant son transfert).
Plus rapide qu'un commutateur (moins de latence).	Détection des adresses MAC (quel périphérique est connecté à quel emplacement ?).
	Suppression des anciennes adresses (Délai de temporisation dépassé dans le buffer d'adresses MAC).
	Contrôle du flux pour FDX et HDX.
	Tampon de paquets au niveau du port.
	QoS, hiérarchisation des données (les données prioritaires sont placées en tête du tampon de paquets).
	Réseau virtuel, VLAN (permet d'interconnecter virtuellement des ports spécifiques).
	Commutateurs Gbit (commutateurs puissants à haute capacité).

Le principal avantage d'un commutateur réside dans le fait qu'il segmente le réseau (Ethernet commuté), et permet donc d'éliminer les collisions.

Les différents types de commutateurs

Il existe différents commutateurs selon l'application et les critères d'installation. Pour commencer, les interfaces peuvent être de type TX (cuivre) et FX (fibre). Les commutateurs peuvent également être administrés ou non administrés, ce qui signifie que vous pouvez avoir ou non la possibilité de communiquer avec le commutateur ou de le contrôler via SNMP. Enfin, on établit une distinction entre les commutateurs pour anneaux et les commutateurs synchronisés, utilisés pour construire un réseau en anneau avec redondance ou un réseau axé sur la synchronisation.

FRNT et Spanning Tree

Les réseaux complexes requérant une certaine redondance doivent pouvoir être reconfigurés en cas d'erreur de réseau.

La reconfiguration est gérée par le commutateur : c'est lui qui doit détecter l'éventuelle erreur de lien. Cette opération peut être effectuée de différentes manières. Parmi les solutions standard figurent les protocoles STP (**S**panning **T**ree **P**rotocol, protocole de l'arbre maximal) ou RSTP (**R**apid **S**panning **T**ree **P**rotocol, protocole de l'arbre maximal rapide) d'IEEE. Le protocole STP crée une connexion via le réseau en éliminant les boucles non désirées. Pour générer la redondance, il maintient la structure arborescente du réseau et bloque certaines connexions (mode d'attente). Si un segment ne peut être atteint, le réseau est reconfiguré via l'algorithme Spanning Tree (arbre maximal), de manière à réactiver les connexions en mode d'attente. La reconfiguration d'un réseau STP peut prendre 30 secondes, vu la nécessité de calculer les nouvelles conditions et d'actualiser les commutateurs. Ce calcul est complexe car le réseau ne présente pas d'architecture particulière. RSTP est une version de STP permettant une reconfiguration plus rapide, à savoir 5 secondes.

Il existe également des solutions spécifiques, par exemple FRNT (**F**ast **R**ecovery **N**etwork **T**opology, topologie réseau à reconfiguration rapide), utilisé dans notre commutateur d'anneau R200 et notre commutateur synchronisé T200. FRNT est une solution brevetée qui reconfigure le réseau très rapidement, en <30 ms à peine, grâce au fait que les commutateurs connaissent la configuration du réseau (topologie en anneau). La reconfiguration est en outre contrôlée en fonction des événements : le "trafic inactif" est transmis entre tous les dispositifs de l'anneau afin de vérifier si le lien est opérationnel. Si une erreur est détectée, l'information est automatiquement envoyée au point focal de l'anneau (maître de l'anneau), qui veille à la reconfiguration du réseau.

BACK

RingSwitch

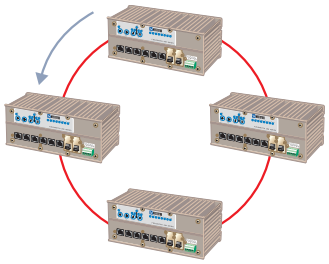
Nos RingSwitches existent en deux variantes, les réseaux en anneau simple et l'autre pour les réseaux en anneau pontés. . Les protocoles de reconfiguration sont FRNT0 et FRNT1.

FRNT0

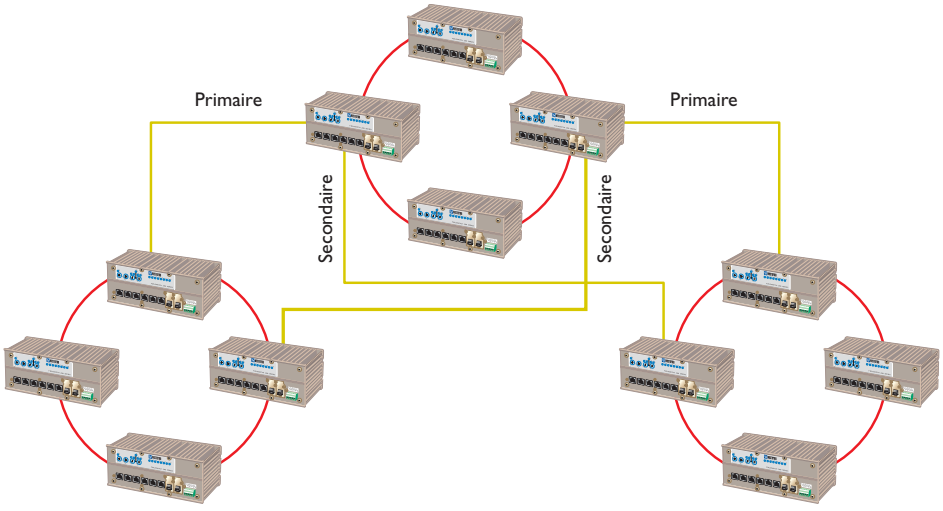
Le trafic d'un réseau peut toujours s'effectuer dans deux directions : vers la droite ou vers la gauche. Les RingSwitches en tirent parti et éliminent donc les erreurs de réseau. En cas d'erreur, le commutateur configuré en tant que « focal point » sera averti et reconfigurera le réseau de manière à rétablir toutes les communications.

FRNT1

Certains commutateurs ont la possibilité d'interconnecter plusieurs anneaux, pour une fiabilité accrue. Ces anneaux sont pontés vers d'autres anneaux du réseau par le biais d'un lien primaire et secondaire. Si une erreur survient au niveau du lien primaire, le « focal point » en sera averti, puis reconfigurera le réseau et connectera le lien secondaire à l'anneau sous-jacent. Le dysfonctionnement d'un câble doit être rectifié, mais une redondance empêchera la détection de cette erreur, sauf si une alarme est générée en même temps.



FRNT0



FRNT1

Commutateurs synchronisés

Ethernet ne repose pas sur un concept déterministe, c'est-à-dire que vous ne pouvez pas garantir le délai de transfert d'un paquet de données d'un cas à un autre. Ces limitations empêchaient jadis l'utilisation d'Ethernet pour les applications en temps réel, comme la supervision de stations de distribution électrique ou le contrôle d'équipements complexes, mais elles ne sont plus qu'un souvenir. Dans un système en temps réel, toutes les liaisons doivent communiquer en duplex intégral, et le contrôle du flux (au niveau d'Ethernet) doit être désactivé. Il doit en outre être possible de hiérarchiser les données. Toutes les données à priorité élevée seront donc placées en tête de la file d'attente et transmises en priorité au destinataire. Combinée avec la synchronisation temporelle, cette structure permet de concevoir des applications en temps réel basées sur Ethernet. Voir également les pages 136 à 137.

Quelles peuvent être les sources de problèmes pour les applications en temps réel dans un réseau commuté ?

Un réseau commuté peut subir des retards en raison de l'encombrement du réseau, de la vitesse de la liaison, de la taille des paquets, de l'architecture du commutateur et du nombre de commutateurs entre le serveur et le client. Ces retards peuvent varier de dix µs à plusieurs ms. La plupart des commutateurs sont fondés sur la technologie "stockage et retransmission", qui réceptionne et vérifie l'intégralité du paquet avant de le retransmettre. Supposons que le commutateur ait une vitesse de liaison de 10 Mbits/s (port de réception sur le commutateur) et que la taille du paquet soit de 1.522 octets. Nous obtenons un retard maximal de 1,2 ms dû au stockage et à la retransmission. Mais si la vitesse est de 100 Mbits/s, le retard maximal sera de 1,2 µs. Le choix de la technologie adéquate en combinaison avec la synchronisation constitue la condition préalable à l'utilisation d'Ethernet dans les applications en temps réel.

BACK

Fonctions des commutateurs

Hiérarchisation (QoS, Quality of Service, Qualité de Service)

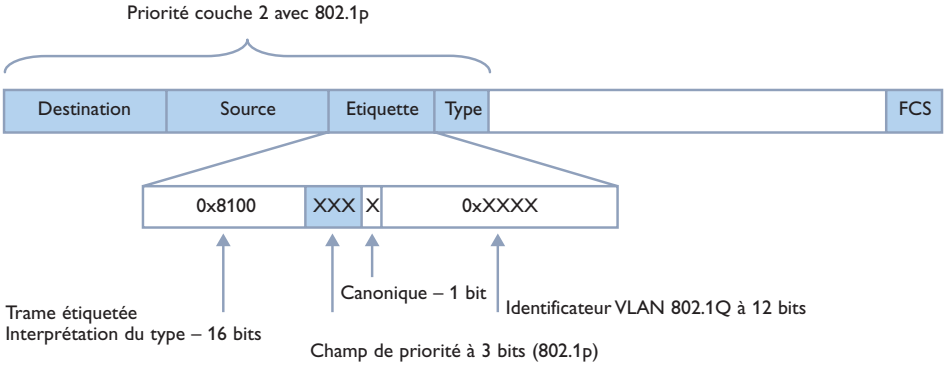
Les commutateurs supportant la hiérarchisation présentent des ports associés à plusieurs files d'attente en vue du traitement des données (QoS). La hiérarchisation peut s'effectuer à différents niveaux via diverses techniques.

Ainsi, le commutateur peut envoyer un nombre prédéterminé de paquets à partir d'une file à haute priorité avant de transmettre un paquet de faible priorité ('tour de rôle'). Il peut également appliquer une hiérarchisation stricte, accordant la préférence à l'ensemble du trafic prioritaire par rapport au trafic de faible priorité.

Priorité couche 2

Un commutateur couche 2 peut hiérarchiser les données au niveau MAC sur la base des éléments suivants :

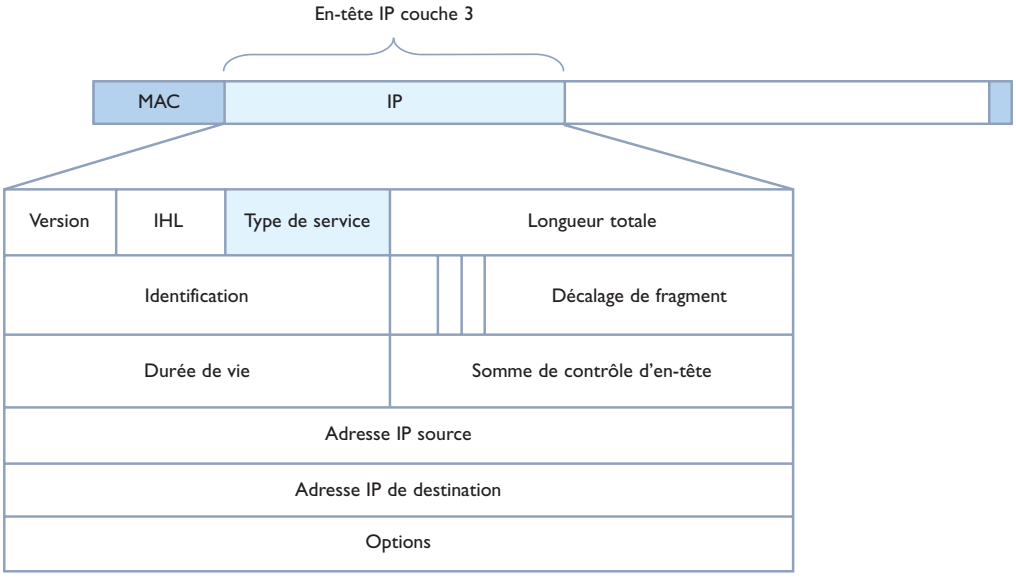
- **Adresse MAC** Les données peuvent être hiérarchisées via l'adresse de destination et l'adresse de la source. Pour ce faire, le commutateur doit être administré de manière à permettre la définition des priorités sur les adresses MAC.
- **Port Ethernet (couche 1)** Il est possible de configurer un ou plusieurs ports pour les données à haute priorité. L'ensemble du trafic à destination de ces ports sera traité en priorité.
- **Définition de la priorité par le biais d'étiquettes** Dans IEEE 802.1 p (et 802.1Q), le paquet Ethernet est complété d'un champ libellé 'Tag Control Info' (TCI, étiquette d'information de contrôle). Ce champ se situe entre l'adresse source et le champ de type, et permet d'allonger le paquet de 1.518 octets à 1.522 octets. L'"étiquette d'information" utilise 3 bits afin de définir la priorité, ce qu'elle peut donc faire à 8 niveaux.



BACK

Priorité couche 3

L'utilisation d'un commutateur couche 3 permet de hiérarchiser partiellement les données au niveau MAC (couche 2) comme ci-dessus, ou en conjonction avec un « niveau d'en-tête » IP, c'est-à-dire un routeur. Chaque paquet est associé à une priorité d'après le contenu du champ Type of Service (ToS, type de service).

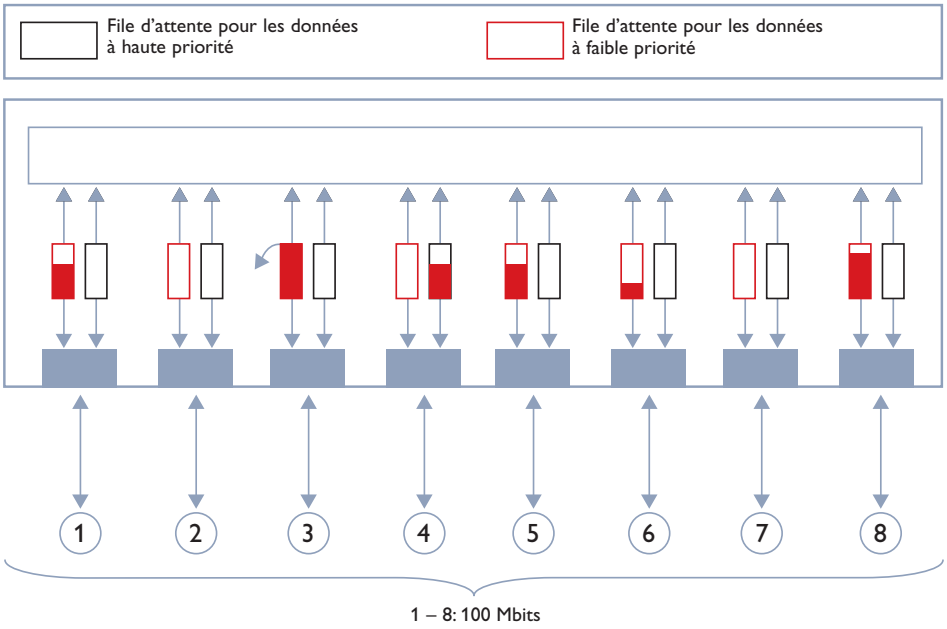


Prévention du blocage en tête de file

Les données entrantes et sortantes sont placées dans la mémoire tampon d'un commutateur (gestion de la file d'attente), généralement sur la base d'un système FIFO ("first in-first out", premier entré, premier sorti). Si les données reçues doivent être envoyées à plusieurs ports et que l'un d'eux est surchargé, il faudra attendre que le tampon surchargé puisse à nouveau recevoir des données. Cette fonction est appelée « Head of Line blocking (HoL), blocage en tête de file ».

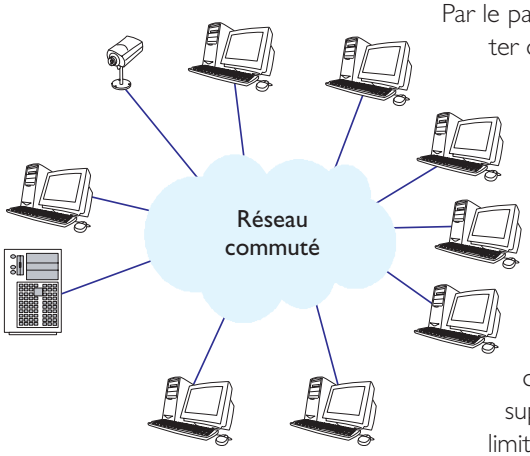
Si un commutateur présente plusieurs files d'attente pour des données à haute et basse priorité, un paquet à haute priorité pourra être retardé en vertu du HoL.

La prévention du blocage en tête de file peut gérer cette situation en vérifiant si le paquet a été associé à une priorité. Si tel est le cas, le paquet sera placé dans une file distincte. En revanche, les données peu prioritaires pourront être supprimées (port 3 dans la figure ci-contre). Cette dernière opération est possible car les applications ou le protocole TCP consignent le degré de nécessité d'une retransmission.



VLAN

Le VLAN ou LAN virtuel est une technique permettant de regrouper des équipements au sein d'un réseau commun. Il se présente sous diverses formes, au niveau d'un port ou d'une adresse MAC. Les différents fournisseurs offrent en outre des solutions spécifiques.

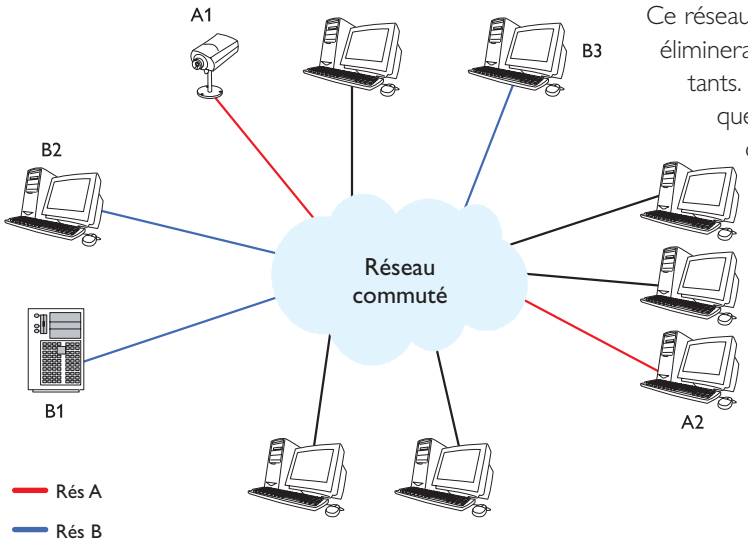


Par le passé, les entreprises et organisations utilisaient des routeurs pour segmenter de vastes réseaux, une scission qui peut également s'effectuer par le biais de VLAN.

Le réseau et ses équipements forment un domaine de "diffusion" commun pour l'ensemble des dispositifs connectés. L'expansion du réseau implique généralement sa segmentation, en partie pour des raisons de vitesse mais aussi pour optimiser l'administration. Cette opération s'effectue normalement à l'aide d'un ou plusieurs routeurs.

Dans un réseau, chaque connexion constitue un domaine de collision distinct, alors que tous les équipements font partie du même domaine de diffusion. Toutes les diffusions seront donc transférées vers l'ensemble des dispositifs. Une expansion du réseau risque de générer des diffusions supplémentaires dues à la connexion de nouveaux équipements, d'où une limitation des performances. Certains équipements peuvent aussi recourir à la multidiffusion et transmettre des données à un certain nombre de destinataires. Il peut s'avérer nécessaire de limiter tout ce trafic, ce qui peut être effectué par le biais de routeurs ou d'un VLAN (**V**irtual **LAN, LAN virtuel**).

Le principe consiste à utiliser un commutateur compatible VLAN afin de spécifier les dispositifs devant être associés à un réseau virtuel commun. Ce réseau créera alors un domaine de diffusion distinct, qui éliminera le trafic non désiré à destination des dispositifs restants. Dans l'exemple ci-contre, B1, B2 et B3 communiquent mutuellement au sein d'un réseau virtuel. La caméra vidéo A1 envoie constamment des informations, mais uniquement vers A2. Les autres dispositifs communiquent conformément à la norme relative aux réseaux commutés.



IGMP et snooping IGMP

IGMP (**I**nternet **G**roup **M**anagement **P**rotocol, protocole de gestion des groupes sur Internet) est un protocole utilisé par les hôtes IP afin de signaler leur appartenance à des groupes de multidiffusion aux routeurs de multidiffusion les plus proches. Les routeurs de multidiffusion envoient périodiquement un message d'interrogation ("Host Membership Query message") afin de rester informé de la composition des groupes au sein du réseau local. Les hôtes du réseau local répondent alors par le biais d'un datagramme-rapport, mais uniquement aux requêtes concernant les groupes dont ils font partie. Si aucun rapport n'est transmis pour un groupe spécifique après un certain nombre de demandes, le routeur présuppose qu'il ne reste plus aucun membre de groupe sur le réseau local. Il ne transférera donc plus aucun datagramme relatif à ce groupe d'autres réseaux vers le réseau local.

Les commutateurs couche 2 supportent généralement le trafic IP multidiffusion de la même manière qu'une diffusion, c'est-à-dire en distribuant les données à l'ensemble des ports. Cette procédure peut entraîner un encombrement important et réduire les performances du réseau. L'utilisation du snooping IGMP permet à un commutateur de filtrer le trafic et, par conséquent, de réduire le trafic non sollicité. Pour ce faire, le commutateur 'écoute' la conversation IGMP entre l'hôte et le routeur. Il peut alors déterminer si un hôte devient membre d'un groupe ou met fin à sa qualité de membre, afin de savoir quels dispositifs sont inclus dans un groupe multidiffusion. A l'heure actuelle, trois niveaux d'IGMP ont été définis :

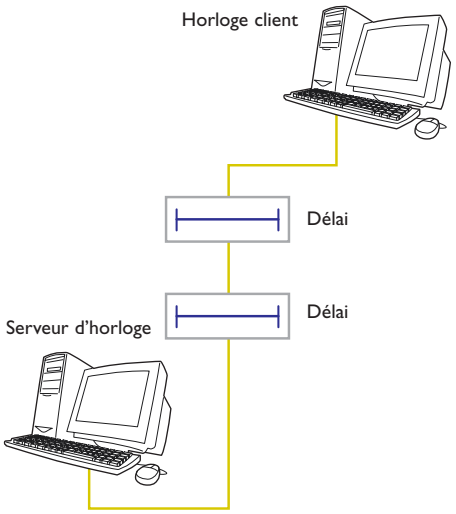
- IGMPv1 (REF 1112) : version originale d'IGMP, spécifiant comment un hôte demande à adhérer à un groupe. D'un autre côté, v1 ne stipule aucune méthode pour quitter un groupe, de sorte que les routeurs doivent utiliser une minuterie pour ce faire.
- IGMPv2 (REF2236) : cette version inclut les modalités de sortie d'un groupe.
- IGMPv3 (REF3376) : révision générale d'IGMP.

Réseaux synchronisés

Jusqu'à présent, les systèmes distribués en temps réel étaient généralement fondés sur des bus de terrain, mais ils peuvent désormais s'appuyer sur une infrastructure Ethernet commutée. Cette intégration est en partie imputable à ses caractéristiques : bande passante, possibilité de hiérarchisation, spécification industrielle de l'équipement réseau. Elle s'explique aussi par la diminution du prix des équipements Ethernet.

Le concept de délais variables (latence) au sein d'un réseau commuté signifie que les données de nœuds peuvent être affectées par différents retards, notamment en raison de l'encombrement du réseau. La précision du transfert synchronisé dépend essentiellement des facteurs suivants :

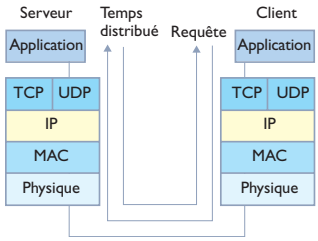
1. La latence dépend de l'encombrement du réseau, de la vitesse de la liaison, de la taille des paquets et de l'architecture du commutateur.
2. Le protocole de prédilection ne revêt qu'une importance mineure compte tenu des conditions ci-dessus. Nous recommandons néanmoins les normes SNTP/NTP, peu limitées.
3. L'horodatage des paquets de données entrants et sortants est effectué le plus près possible du matériel, c'est-à-dire sur les couches les plus basses du modèle OSI.



SNTP/NTP

RFC 2030 **S**imple **N**etwork **T**ime **P**rotocol (SNTP, protocole de temps de réseau simple), RFC 1305 **N**etwork **T**ime **P**rotocol (NTP, protocole de temps de réseau) et P1588 sont des protocoles reconnus pour le trafic IP à synchronisation temporelle. SNTP est un sous-ensemble de NTP. Le serveur SNTP/NTP gère l'horloge système, qui peut à son tour être basée sur le GPS ou l'horloge interne. Les informations horaires sont ensuite distribuées par le biais d'une monodiffusion ou d'une multidiffusion.

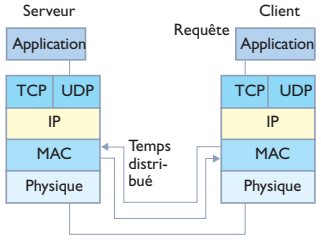
1. Mise à jour par monodiffusion : la mise à jour est initiée par le client puis le serveur renvoie une réponse. La référence temporelle est ajoutée à toutes les communications entre le client et le serveur, afin de permettre une précision de calcul maximale.
2. Mise à jour par multidiffusion : l'heure est envoyée du serveur au groupe de clients (groupe de multidiffusion) à intervalles définis. Les clients n'ont pas la possibilité de calculer le retard dans le réseau.



Horodatage
par le biais d'applications

Horodatage via les applications

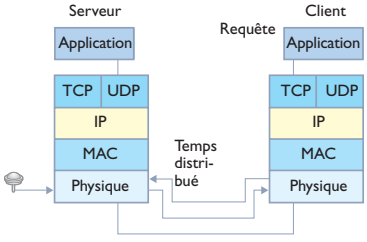
La plupart des applications SNTP/NTP génèrent l'horodatage des données sur la couche d'application, de sorte que la précision dépend du retard/des fluctuations dans l'ensemble de la pile IP. En général, cette technique présente une précision de l'ordre d'une ou deux millisecondes.



Horodatage
par le biais de pilotes Ethernet

Horodatage par le biais de pilotes Ethernet

La précision peut être nettement accrue en effectuant l'horodatage via le programme de traitement des interruptions d'Ethernet. L'horodatage est alors appliqué lors de l'envoi des données entre le serveur et le client. La requête est générée par le client ; et dans ce cas, la précision dépend des fluctuations dans la gestion des interruptions au niveau du serveur et du client. La précision de cette application varie d'environ 10 µs à environ 100 µs.



Horodatage
sur la couche physique

Horodatage sur la couche physique

Le délai de passage par la pile IP peut être éliminé si l'horodatage est effectué sur la couche physique, c'est-à-dire par le biais d'un matériel informatique. Dans ce cas, la synchronisation peut être extrêmement précise (moins de 1 µs). Une telle précision requiert une connexion directe entre le serveur et le client, étant donné qu'un surcroît d'équipement allongerait le délai. Voilà pourquoi le serveur temporel est intégré dans le commutateur. Il est également possible de synchroniser le commutateur à partir de l'horloge de référence via GPS ou à partir de l'oscillateur interne.

BACK

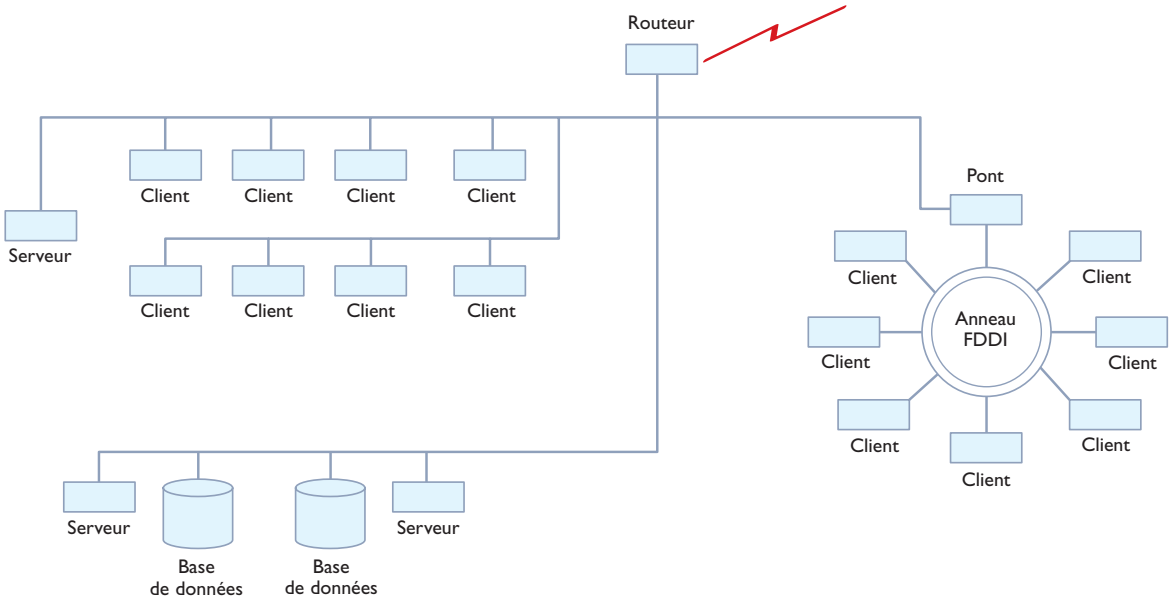
SNMP

SNMP est l'acronyme de **S**imple **N**etwork **M**anagement **P**rotocol (protocole de gestion de réseau simple). Le protocole SNMP permet de gérer les dispositifs d'un réseau. Un dispositif que l'on peut contrôler est appelé "agent".

Un système maître envoie une requête aux agents afin d'obtenir des données. Cette opération peut être effectuée par le biais d'applications spéciales ou à l'aide de Telnet.

L'utilisation de SNMP permet de :

- Surveiller les tendances.
- Surveiller les événements en vue d'une analyse.
- Surveiller les dispositifs du réseau ainsi que leur statut.
- Surveiller une connexion particulièrement importante.
- Vérifier le trafic sur un ou plusieurs dispositifs du réseau à des fins de prévention.
- Configurer des dispositifs.

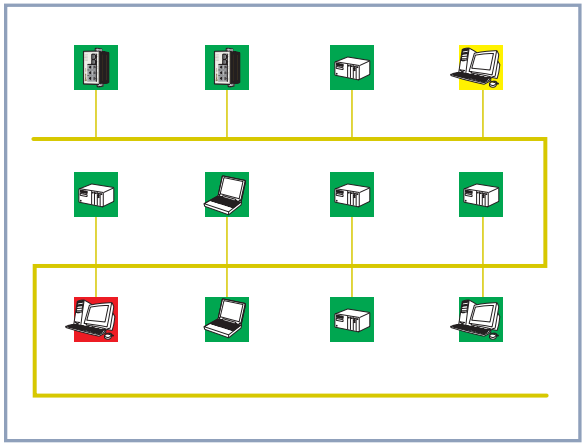


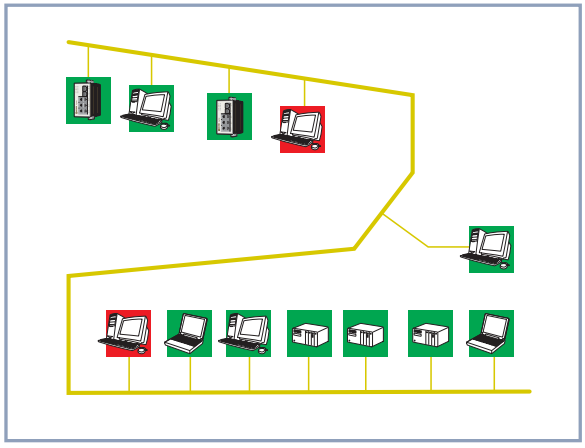
Logiciels SNMP

Les logiciels utilisés pour communiquer avec l'agent sont appelés **N**etwork **M**anagement **S**olution (NMS, solution de gestion de réseau). L'échange de données avec les agents s'apparente à la communication entre un maître et ses esclaves, en ce sens que la communication avec les dispositifs sous-jacents s'effectue par interrogation. L'administrateur peut demander une information à l'agent ou le soumettre à une action, en réponse aux requêtes ou aux actions demandées. Une autre option pour l'agent consiste à tendre un 'piège', c'est-à-dire une fonction contrôlée par un événement et activée par une condition prédéfinie. L'agent renvoie alors des données à l'administrateur.

Prenons un exemple :

Dans un vaste réseau, un équipement critique utilise UPS pour son alimentation d'appoint. En cas de panne électrique, les unités UPS sont automatiquement connectées et les dispositifs continuent à fonctionner. Cette erreur doit être signalée d'une manière ou d'une autre à l'administrateur du réseau, opération réalisable par le biais d'un 'piège' détectant la connexion de l'unité UPS. Les informations en question sont transférées à un système SCADA (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition, acquisition et contrôle des données), où l'administrateur du réseau reçoit une alarme par le biais d'une icône clignotante (activée par le piège SNMP) sur l'unité UPS.





BACK

SNMP, SNMPv2 et SNMPv3

Il existe trois versions de SNMP. La version originale, SNMPv1, possède un mécanisme de sécurité multiple constitué par un mot de passe. Elle ne permet toutefois pas d'identifier l'expéditeur d'un message en toute certitude et reste donc ouverte, de sorte que les dispositifs peuvent être reconfigurés au sein du réseau. Par conséquent, de nombreux fabricants d'équipements ont décidé de ne pas implémenter toutes ses fonctions. Ces limitations ont été identifiées à partir du décalage et une version nettement améliorée, SNMPv2, a été mise sur pied. Elle utilise un algorithme de cryptage pour l'authentification des transferts entre les serveurs SNMP et les agents. Cette norme peut également crypter le transfert. SNMPv2, qui devait remplacer la version précédente, n'a jamais été acceptée, notamment à cause de l'impossibilité d'aboutir à un accord sur les modalités de sécurité. Elle constitue néanmoins un chaînon important du développement de la version suivante, SNMPv3.

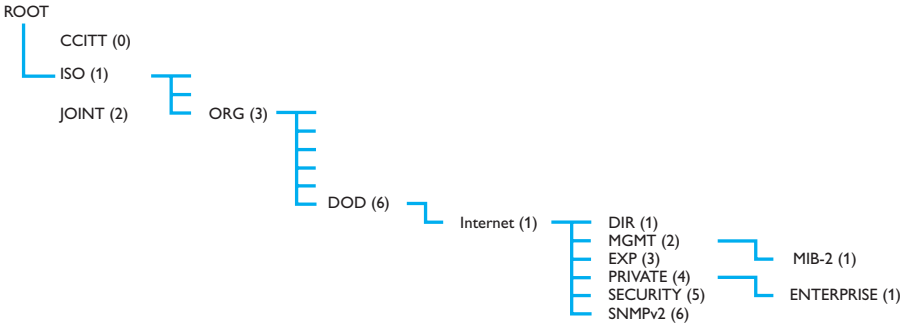
Le groupe de travail SNMPv3 a été formé en mars 1997 afin d'examiner les propositions soumises en matière de sécurité et d'administration et, sur cette base, de trouver une solution commune au problème. Son principal objectif était de compléter autant que possible les propositions existantes et de ne pas avancer de nouvelles idées. La proposition relative à SNMPv3 a été clôturée en 1998. Elle était basée sur la version 2, ainsi que sur un concept de sécurité et d'administration centré sur différents modules pouvant être alternés selon le niveau de sécurité requis.

SNMPv3, la norme actuelle, offre de nombreuses autres possibilités pour sécuriser les dispositifs de réseaux, mais son introduction est lente. La plupart des dispositifs installés appliquent toujours SNMPv1.

MIB

Chaque agent du réseau possède un jeu de MIB (**M**anagement **I**nformation **B**ase, base d'informations de gestion). Une MIB est un objet pouvant être activé par un administrateur. Elle peut contenir des informations standard comme le statut ou l'état du port, ou des données spécifiques à l'entreprise (privées), par exemple la température au sein du dispositif.

Les MIB sont des tables structurées constituées des différents objets pouvant être consultés. Leur structure est comparable à celle d'un arbre, avec une racine et des répertoires sous-jacents. Le niveau le plus bas inclut les répertoires de la MIB standard et des MIB privées.



OPC

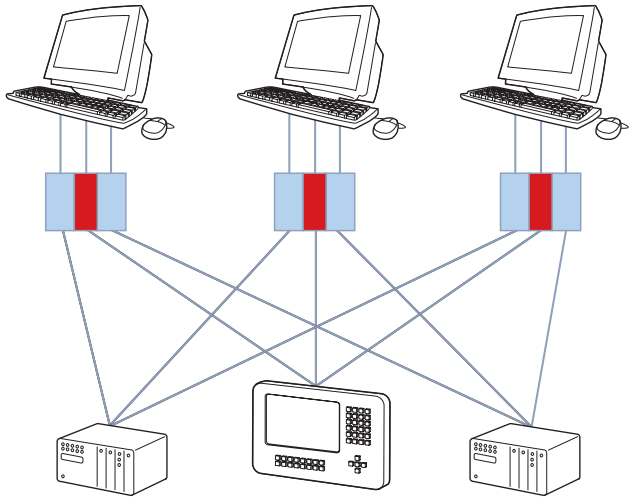
Une alternative à SNMP est OPC, acronyme de 'OLE for Process Control' (OLE pour contrôle de processus). Il s'agit d'une série de normes convenant à l'échange d'informations dans le domaine de l'automatisation industrielle. L'un de leurs objectifs est d'améliorer l'efficacité et de minimiser la nécessité de pilotes spécifiques au fabricant. L'utilisation de nombreux pilotes différents débouche généralement sur une implémentation complexe, étant donné que plusieurs applications doivent interagir et échanger des informations.

Les spécifications OPC incluent des fonctions pour :

- **OPC D**ata **A**ccess or (OPC DA, accès aux données OPC), accès de données entre des applications, échange d'informations entre des systèmes en temps réel.
- **OPC H**istorical **D**ata **A**ccess (OPC HAD, accès à l'historique OPC), utilisé pour traiter l'historique et analyser les tendances.
- **OPC A**larm and **E**vents (OPC A&E, alarmes et événements OPC). Contrôle des alarmes et événements.
- **OPC D**ata e**X**change (OPC DX, échange de données OPC) indique comment l'échange de données doit s'effectuer entre différents serveurs OPC.

BACK

- **OPC** e**X**tensible **M**arkup **L**anguage (communément appelé OPC XML, langage de balisage extensible OPC). Langage HTML pour l'échange d'informations entre des applications.



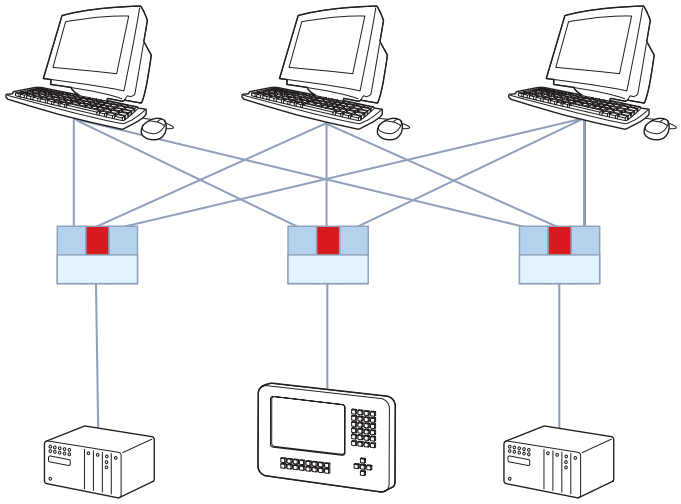
Pour illustrer les problèmes, supposons que trois applications doivent échanger des informations entre deux API et un terminal opérateur (IHM).

Chaque fournisseur possède sa propre application spécifique avec ses pilotes. Ces derniers doivent télécharger des données depuis leurs API et IHM respectifs, ce qui donne neuf points d'intégration.

BACK

OPC simplifie cette procédure en utilisant des outils standard. L'évolution d'OPC est le résultat d'une collaboration entre Microsoft et d'éminents fournisseurs en automatisation. Sur le plan technique, les modèles COM (**C**omponent **O**bject **M**odel, modèle d'objet composant) et DCOM (**D**istributed **C**omponent **O**bject **M**odel, modèle d'objet composant distribué) de Microsoft sont utilisés pour la communication entre applications. Par conséquent, dans cet exemple, chaque API et IHM n'a qu'un seul point de connexion, ce qui permet d'accroître la simplicité et la rentabilité du système dans son ensemble.

Ces avantages et possibilités ont poussé les fournisseurs de systèmes composants à intégrer une prise en charge directe d'OPC dans leurs équipements.



BACK

Ethernet sur le câble

Ethernet 10 Mbits/s

Les signaux transmis par le biais de supports à 10 Mbits/s recourent au codage Manchester. Ce codage combine les données et l'horloge en symboles binaires, générant une transition d'horloge au milieu de chaque bit. Un zéro logique (0) est défini en tant que signal élevé pour la première moitié de la période binaire et faible pour la seconde moitié (transition de signal négative). Un 1 logique est défini en tant que transition de signal positive au milieu de la période binaire.

La transition de signal facilite la synchronisation d'un récepteur avec le signal entrant, ainsi que l'extraction des données qu'il contient. Un inconvénient réside dans le fait que la vitesse de transmission la moins favorable vaut le double du débit de données. Un signal d'essai de liaison est émis lorsqu'il n'y a pas de données à envoyer.

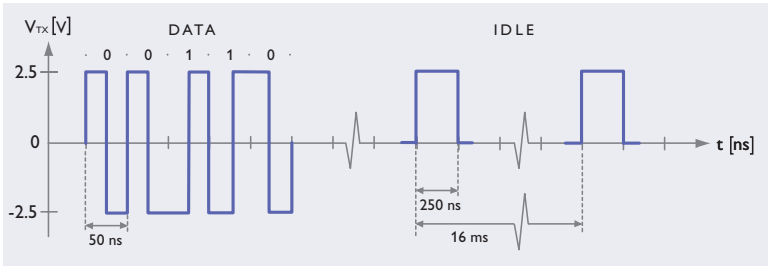
Ethernet rapide

Les systèmes 100Base-T utilisent un codage par blocs 4B/5B, qui transpose des blocs de données à 4 bits en symboles de codes à 5 bits pour la transmission via les supports de média. Le codage à 5 bits permet la transmission de 32 symboles de 5 bits comprenant 16 symboles véhiculant les données sur 4 bits et 16 symboles utilisés pour le contrôle. Le symbole de contrôle IDLE est transmis en continu en l'absence d'autres données. Voilà pourquoi le réseau Ethernet rapide est continuellement actif, envoyant des symboles IDLE 5 bits à 125 Mbits/s s'il n'y a pas d'autres données à transmettre. Tout système à 100 Mbits/s (Ethernet rapide) utilise une signalisation différente pour le support.
100Base-TX applique une signalisation à chiffrement et codage MLT-3 ('Multilevel Threshold-3', à 3 niveaux). Le signal parcourant le câble peut avoir trois niveaux différents. Le passage d'un niveau au suivant correspond à un 'un' logique (1), tandis que le maintien d'un niveau constant désigne un 'zéro' logique.
Pour réduire (disperser) l'émission électromagnétique, on applique un processus de chiffrement avant la modulation du signal en MLT-3. Le crypteur génère une séquence binaire non répétitive des bits à transmettre.
Les systèmes à support fibre 100Base-FX recourent à l'encodage NRZI. Ce système n'apporte aucun changement au niveau du signal lors de l'envoi d'un zéro logique, mais inverse le niveau pour les uns logiques.

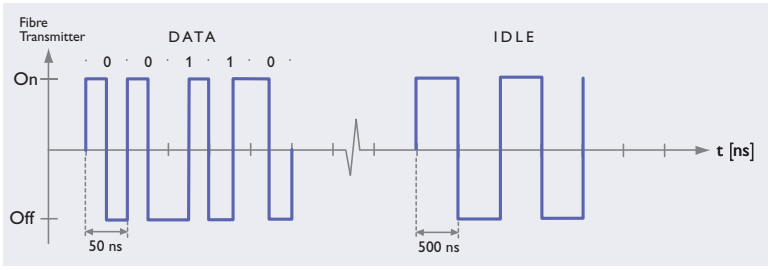
Gigabit Ethernet

1000Base-T (cuivre) utilise le codage 4D-PAM5. Le système transmet et reçoit des données simultanément sur des paires à quatre fils (4D), en appliquant cinq niveaux de tension (PAM5) à chaque paire torsadée.
1000Base-SX/LX (fibre) utilise le codage 8B/10B. Les données et symboles de contrôle sont transmis à 1.250 Mbits/s. La vitesse de signalisation élevée demande l'utilisation d'émetteurs/récepteurs laser.

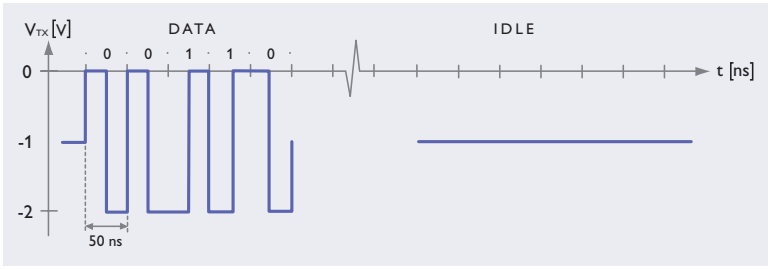
BACK



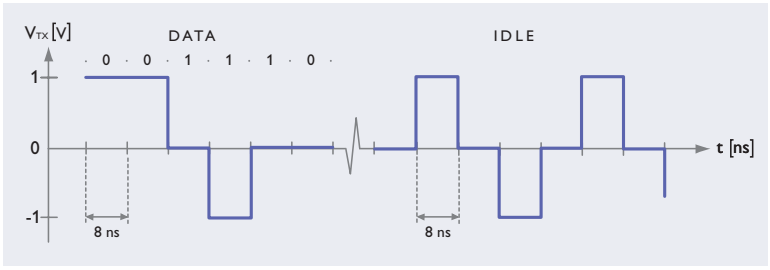
10Base-T



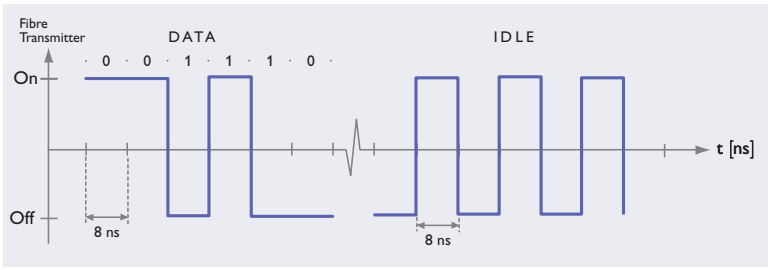
10Base-FL



10Base2



100Base-TX



100Base-FX

BACK

Glossaire

10Base2 Standard de câblage Ethernet utilisant un câble coaxial de faible section. Permet de réaliser des segments de réseau d'un maximum de 185 mètres de long. Les périphériques se connectent directement au LAN par connexion en série.

10Base5 Standard de câblage Ethernet utilisant un câble coaxial de section importante, à double blindage. Permet de réaliser des segments de réseau d'un maximum de 500 mètres de long. Une MAU est insérée dans le câble pour permettre aux équipements de communiquer via un port AUI situé sur le périphérique Ethernet.

10BaseFL Standard de câblage Ethernet utilisant un câble en fibre optique. 10BaseFL atteint un débit de 10 Mbits/s.

10BaseT Standard de câblage Ethernet utilisant deux paires de conducteurs cuivre torsadées. La distance maximale entre périphériques, nœuds de réseau ou commutateurs est de 100 mètres. Un connecteur type RJ-45 établit la connexion sur les périphériques Ethernet. 10BaseT atteint un débit de 10 Mbits/s et 100BaseT, de 100 Mbits/s.

4 fils Câble à paire torsadée de 4 fils.

Adresse IP L'adresse IP est un numéro à 32 octets qui identifie un périphérique réseau. L'adresse IP se compose de deux parties. D'abord, l'identifiant d'un réseau spécifique, et ensuite, celui du périphérique spécifique connecté sur ce réseau. Étant donné le nombre limité de combinaisons possibles avec 32 octets, une nouvelle méthode d'adressage IPv6 est à présent utilisée.

Adresse MAC L'adresse MAC (**M**edia **A**ccess **C**ontrol address, contrôle d'accès au support) est le numéro de matériel unique attribué à un périphérique Ethernet lors de sa fabrication. En principe, l'adresse MAC ne peut être modifiée.

ARP Le protocole ARP (**A**ddress **R**esolution **P**rotocol, protocole de résolution d'adresse) s'utilise pour mapper les adresses IP en adresses MAC. Cet outil TCP/IP permet d'ajouter ou de supprimer des informations d'adressage MAC ou IP.

ARQ **A**utomatic **R**epeat re**Q**uest, demande de répétition automatique.

ASCII Système définissant 128 codes binaires reposant sur diverses combinaisons de uns et de zéros ASCII = **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange, code standard américain pour l'échange d'informations

Asynchrone Transmission de données un caractère après l'autre, séparés par des bits de départ et d'arrêt. Près de 90 à 95% des transmissions de données en série sont du type asynchrone.

BACK

Atténuation	Affaiblissement du signal provoqué par la longueur du câble et le nombre d'épissures (fibre optique).
AUI	Port AUI, **A**ttachment **U**nit **I**nterface (interface de raccordement). Câble Ethernet 15 broches type D standard utilisé pour connecter un périphérique et une MAU.
Autodétection (autosense)	Faculté d'un périphérique Ethernet 10/100 d'interpréter la vitesse et le mode duplex du périphérique connecté. Se paramètre automatiquement pour correspondre à la configuration requise.
Autonégociation	Le standard IEEE802.3u détermine une sous-couche MAC pour l'identification de la vitesse et du mode duplex des connexions prises en charge par un périphérique. En option.
Baud	Définit la vitesse de transmission – nombre de " paquets " de données à la seconde. En transmission de données locale, " baud " = " bit/s ". Dans le secteur des télécommunications, chaque paquet peut receler un nombre supérieur de bits.
Binaire	Système numérique dans lequel les chiffres ne peuvent avoir que l'un des deux valeurs suivantes : un et zéro, représentés par les deux états possibles du semi-conducteur du processeur de l'ordinateur (absence/présence de courant électrique).
Bit	Un bit de données est un chiffre numérique, soit un un ou un zéro.
Bit d'arrêt	Un ou plusieurs bits d'arrêt indiquent la fin d'un caractère.
Bit de départ	Indique le début du transfert de données. En transfert asynchrone, chaque caractère est précédé d'un bit de départ.
Bit de parité	Bit de contrôle calculé par l'équipement émetteur à des fins de contrôle de parité et de détection d'erreurs de transmission.
Bit/s	Unité de mesure du débit de données : nombre de bits de données par seconde.
Bits de données	Voir bit.
Boucle de courant	Mode de transmission en série reposant sur l'absence et la présence d'une tension au niveau d'une paire de fils.
BOOTP	Le protocole BOOTP permet aux périphériques du réseau d'interroger un serveur BOOTP pour obtenir les informations de configuration.
BRI	**B**asic **R**ate **I**nterface (interface à débit primaire), service RNIS donnant accès à deux canaux B et à un canal D à 16 kbit/s.
Broche	L'un des contacts d'un connecteur (D-sub, etc.) ou de circuits conçus pour l'enfichage ou le soudage.

BACK

BSC — **B**ase **S**tation **C**ontroller (contrôleur des stations de base). Station de commutation au sein d'un réseau GSM, assurant la liaison entre les stations de base et le réseau d'infrastructure.

BTS — **B**ase **T**ransceiver **S**tation (station de base). Station radio de base du réseau GSM assurant la liaison entre les équipements mobiles et une station de contrôle (BSC = Base Controller Station).

Bus de données — Plusieurs câbles parallèles servant au transfert interne des données dans les équipements.

Bus de terrain — Norme pour réseaux de données industriels (PROFIBUS, etc.).

CA/AC — **C**ourant **A**lternatif

Câble coaxial — Câble à gaine blindée et conducteur protégé assurant des transmissions rapides et non parasitées.

Capacité — Capacité d'absorption d'une charge électrique.
Mesurée en microfarads $= 10^{-6}$ F = 1 µF
nanofarad $= 10^{-9}$ F = 1 µF
picofarad $= 10^{-12}$ F = 1 pF

CAT5 — Câble cuivre à paire torsadée prenant en charge une bande passante de 100 MHz ou 1.000 MHz lorsque les quatre paires sont utilisées. Débits habituels de 100 Mbits/s ou 1.000 Mbits/s.

CAT5e — Le standard enhanced Cat 5 garantit une immunité de bruit. La plupart des nouvelles installations en sont dotées.

CC/DC — **C**ourant **C**ontinu.

CEM — **C**ompatibilité **E**lectro-**M**agnétique, se rapporte à des produits conçus de manière à ne pas provoquer des interférences au niveau d'autres équipements électroniques.

CHAP — Le protocole CHAP (**C**hallenge **H**andshake **A**uthentication **P**rotocol, protocole d'authentification par défi-réponse) est bien plus sûr que PAP. Au-delà du mot de passe requis lors de l'identification, des mots de passe sont également requis en mode challenge. Lorsque le caractère ou mot de passe adéquat n'est pas fourni, la connexion est interrompue.

Checksum (somme de contrôle) — Résultat d'une fonction mathématique contrôlant le bon déroulement de la transmission.

CMV — **C**ommon **M**ode **V**oltage, tension en mode commun généralement produite par induction.

Collision — C'est ce qui se produit lorsque deux ou plusieurs périphériques tentent d'envoyer des données au même moment sur le même réseau. Lorsqu'une collision se produit, les données sont inutilisables.

BACK

Commandes Hayes	Ensemble de commandes servant à la communication avec les modems RTC.
Communication à distance	Possibilité de se connecter à des équipements distants par le biais de divers moyens de communication (liaisons GSM, RNIS, RTC).
Commutateur	Dispositif matériel ou logiciel redirigeant le flux de données.
Concentrateur	Élément simple permettant de connecter des segments de réseau. Lorsqu'un paquet parvient à un port, il est envoyé à tous les ports du concentrateur.
Convertisseur d'interface	Modem assurant la conversion des signaux entre deux interfaces différentes, par exemple entre les protocoles RS-232 et RS-422/485.
Courants de terre	Courants circulant dans les conducteurs de terre entre deux systèmes dont le potentiel de terre est différent.
CSD	**C**ircuit **S**witched **D**ata, transmission de données à commutation de circuits. Mode de transmission le plus courant via le réseau GSM.
CSMA/CD	**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etect, détection de porteuse avec accès multiples et détection de collision. Méthode d'accès Ethernet qui régit la façon dont les périphériques se partagent l'accès au réseau pour transmettre des données. Lorsqu'un appareil détecte le signal d'un autre périphérique alors qu'il tente d'envoyer des données, la transmission est interrompue ; un nouvel essai est effectué après un délai d'attente.
Datagramme	Séquence autonome de données contenant suffisamment d'informations pour pouvoir être routées de la source vers le point de destination sans autre forme d'interaction ni interaction préalable entre ces deux périphériques. C'est ce que l'on appelle souvent la communication en mode sans connexion.
DCE	**D**ata **C**ommunication **E**quipment, équipement de transmission de données.
DDS1	Norme européenne de liaisons RNIS.
DEL / LED	**L**ight **E**mitting **D**iode, diode électroluminescente. Semi-conducteur émettant de la lumière sous l'action d'un courant électrique.
DHCP	Le protocole DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol, protocole de configuration dynamique d'hôte permet aux périphériques de demander et de se voir attribuer des adresses IP par un serveur DHCP du LAN. En l'absence de serveur DHCP, les adresses IP doivent être fixées de manière statique dans la configuration du périphérique Ethernet.

BACK

Dispositif de surveillance (" Chien de garde ")	Circuit de surveillance et de réinitialisation automatique des modems.
DTE	**D**ata **T**erminal **E**quipment, équipement terminal de données.
Duplex	Duplex intégral : communication simultanée dans les deux sens. Semi-duplex : communication alternée dans un sens, puis dans l'autre.
Duplex intégral	Communications bidirectionnelles permettant le transfert simultané de signaux dans les deux sens.
Écran LCD	**L**iquid **C**rystal **D**isplay, écran à cristaux liquides.
EMI	**E**lectro **M**agnetic **I**nterference, interférence électro-magnétique.
Esclave	Périphérique recevant les commandes du maître.
Ethernet	L'une des principales normes de communication pour réseau bureautique local – par câble coaxial ou câble 4 fils spécial.
Étiquettes de priorité	Un périphérique de réseau Ethernet a la possibilité de marquer d'un indicateur les paquets Ethernet afin qu'ils soient traités de manière prioritaire par rapport aux autres paquets circulant sur le même réseau.
Euro-RNIS	RNIS aux normes européennes.
Évanouissement	Affaiblissement du signal du fait de la distance de transmission (câble, air, etc.)
FAI	**F**ournisseur **d'A**ccès **I**nternet. Société commerciale fournissant un accès Internet aux sociétés et aux particuliers.
FDDI	**F**ibre **D**istributed **D**ata **I**nterface, interface de données distribuées par fibre optique : Norme relative aux réseaux à fibre optique.
Fibre optique	Fibre de verre ou de plastique très mince dans laquelle est diffusé un faisceau lumineux (compris entre 800 et 1300 nm, nanomètres) produit et modulé par des diodes électroluminescentes ou par des diodes laser. Les câbles à fibres optiques permettent d'acheminer de gros volumes d'information.
Fibre optique monomode	Technologie de transmission par fibre optique. Concerne généralement la transmission laser via des fibres au cœur très mince.
FP	Un **P**ort Ethernet Fibre **O**ptique.
Fréquence modulation	Technologie permettant de transférer des informations via la variation de la fréquence de de l'onde porteuse.

BACK

FRNT	**F**ast **R**e-Configuration **N**etwork **T**opology, topologie réseau à reconfiguration rapide. Les commutateurs Ethernet sont disposés en anneaux redondants multiples. La redondance accrue est assurée en connectant des anneaux séparés par des chemins d'accès sauvegardés.
FTP	**F**ile **T**ransfer **P**rotocol, protocole de transfert de fichiers.L'un des moyens les plus simples de transférer des fichiers par Internet. Utilise les protocoles TCP/IP pour permettre le transfert de fichiers.
GPRS	**G**eneral **P**acket **R**adio **S**ervice, service général de radiocommunication en mode paquet. Service GSM prenant en charge la commutation par paquets.
GPRS Attach	Signal émis par un équipement GSM en vue de se brancher sur un réseau GPRS.
GPS	**G**lobal **P**osition **S**ystem (système mondial de localisation).Système de navigation utilisant 24 satellites en orbite autour du globe. Chaque satellite possède une horloge atomique qui assure une précision au milliardième de seconde.
GSM	**G**lobal **S**ystem for **Mobile,**système mondial de communication téléphonique mobile. Norme de communication numérique sans fil.
Horloge	Fréquence régulière émise par une source telle qu'un générateur d'impulsions ; sert par exemple à réguler les débits en transmissions en série.
IEEE802.1d	Standard STP (Spanning Tree Protocol). Méthode élémentaire assurant la redondance du réseau.
IEEE802.1p	Standard de définition des niveaux de priorité des paquets. Permet d'attribuer des étiquettes de priorité aux paquets ; les paquets à priorité élevée sont traités plus rapidement.
IEEE802.3	Spécification standard d'Ethernet
IEEE802.3x	Standard de régulation de flux d'Ethernet. Méthode permettant de modérer le débit d'un commutateur lorsque le tampon est proche de la saturation. Un paquet est envoyé pour demander au commutateur expéditeur de suspendre temporairement l'envoi des paquets.
Interface	Norme relative aux signaux, aux niveaux électriques et aux interconnexions.
IP	Le protocole IP (**I**nternet **P**rotocol, protocole Internet) déplace les paquets de données d'un nœud à l'autre sans se soucier de leur contenu. Le protocole IP transfère chaque paquet en fonction d'une adresse de destination de quatre octets (l'adresse IP).

BACK

ISDN (RNIS)	**I**ntegrated **S**ervices **D**igital **N**etwork, réseau numérique à intégration de services. Norme de télécommunication sur réseaux numériques (données, télécopie, vidéo et vidéophonie).
Isolateur	Assure l'isolation galvanique entre deux équipements en communication.
Isolation galvanique	Isolation électrique (aucun contact électrique).
LAPM	**L**ink **A**ccess **P**rocedure for **M**odems, protocole de connexion des modems. Mode de correction d'erreurs en transmission via modems RTC.
Large bande	Système permettant la transmission simultanée de données texte, audio et vidéo sur différentes fréquences.
Liaison multipoint	L'une des architectures les plus courantes en matière de réseaux industriels.
Ligne louée	Ligne 2 ou 4 fils louée à une compagnie des téléphones. Une ligne louée assure une liaison du type point à point ou multipoint.
Ligne privée	Câble de communication en propriété privée.
M2M	**(M**achine-**toM**achine). Abréviation de "communication de machine à machine".
Maître	Appareil principal qui dirige les esclaves.
MAN	**M**etropolitan **A**rea **N**etworks, réseau métropolitain. Type de réseau utilisé conjointement par diverses parties, généralement dans une zone bien circonscrite.
Manchester encodage	Mode de modulation combinant signaux de données et signaux d'
MDI	**M**edium **D**ependent **I**nterface (interface dépendant du support). Port Ethernet permettant la connexion à d'autres équipements de communication de données (commutateurs, concentrateurs, etc.) sans câble coaxial croisé. On les appelle également ports ascendants.
MDI/MDI-X auto	Port Ethernet qui détecte si le port final est un périphérique MDI ou MDI-X et effectue automatiquement la configuration appropriée.
MDI-X	**M**edium **D**ependent **I**nterface – **C**rossover (interface dépendante du support – croisement). Port Ethernet permettant la connexion à d'autres terminaux informatiques (PC, API, etc.).
MIB	**M**anagement **I**nformation **B**ase (base d'informations de gestion).Base de données d'objets pouvant être sondés ou interrogés par un système de gestion SNMP.

BACK

MNP	**M**icrocom **N**etworking **P**rotocol (protocole de mise en réseau Microcom), méthodes de correction d'erreurs et de compression de données pour les modems RTC.
Modem	Mot composé de **mo**dulateur et **dém**odulateur. Module qui convertit le signal en provenance d'un ordinateur en un signal électrique à des fins de transmission (modulation). Le modem récepteur procède à l'opération inverse (démodulation).
Modem courte distance	Module le signal et l'adapte aux différents câbles et interfaces, tout en assurant une transmission correct sur de longues distances. Utilisé dans le domaine des transmissions locales.
Modem fax	Modem pouvant envoyer et recevoir des données (texte, images) au format télécopie.
Modem local	Voir modem courte distance
Modem Rack	Modem pour montage sur rack 19".
Modem RTC	Modem pour transmissions via le réseau téléphonique classique.
Modulation d'amplitude	Transfert d'informations via la variation de la force du signal – amplitude – de l'onde porteuse.
Modulation de phase	Modification de la position du signal dans le temps (angle de phase) à des fins d'encodage de bits de données. La modulation de phase est une technique surtout répandue en transmission numérique.
Module de partage de ligne	Divise une ligne de transmission de données en plusieurs lignes, par exemple lorsque plusieurs ordinateurs doivent exploiter les mêmes périphériques.
MSC	**M**obile **S**witching **C**enter, centre de commutation mobile. Poste de commutation d'un réseau GSM en communication avec d'autres réseaux tels que RNIS ou RTC
Multimode	Système de transmission par fibre optique dont le cœur est nettement plus grand que la longueur d'onde.
Multiplexeur	Remplace plusieurs lignes louées et modems (établissement de canaux indépendants).
NMT	**N**ordic **M**obile **T**elephony, l'un des premiers réseaux de téléphonie mobile analogique.
Non intelligent	Équipement ne pouvant mémoriser des données le concernant (son adresse réseau, etc.). Il s'agit d'équipements tels que des dispositifs E/S, des transducteurs, des capteurs, des instruments de mesure, etc.

BACK

NTP	**N**etwork **T**ime **P**rotocol, protocole de temps de réseau.Standard Internet qui assure une synchronisation à la milliseconde des horloges des périphériques Ethernet. Protocole fondé sur TCP/IP.
Octet	Caractère composé de chiffres binaires (" bits "), par exemple caractère ASCII, composé de 7–8 bits correspondant à un caractère alphanumérique.
OPC	**O**pen **P**rocess **C**ontrol, contrôle de processus ouvert(anciennement OLE Process Control). Standard ouvert qui permet aux périphériques de communiquer ouvertement entre eux, quel que soit leur fabricant.
OSI	**O**pen **S**ystem **I**nterconnection (interconnexion de systèmes ouverts), modèle de référence pour la définition du traitement des données en cours de transfert, selon les couches de communication.
PAP	**P**assword **A**uthentication **P**rocedure (procédure d'authentification par mot de passe). Un mot de passe en clair est envoyé au serveur pour permettre la comparaison.
Paquet	Unité de données transmise entre un périphérique source et cible via Internet. Lorsque des données sont demandées à un périphérique, la couche TCP de TCP/IP " saucissonne " le fichier. Le protocole TCP/IP attribue un numéro à chacun de ces paquets et, malgré les itinéraires différents qu'ils empruntent, permet de les réassembler correctement au niveau du périphérique destinataire. La taille des paquets varie de 48 à 1.518 octets (1.522 octets lorsque l'étiquetage de priorité est utilisé).
Pare-feu (firewall)	Routeur utilisé pour scanner les adresses IP.
PDP Context (contexte PDP)	**P**acket **D**ata **P**rotocol (protocole de paquets de données). PDP Context est une information définissant une connexion GPRS entre une MS (**M**obile **S**tation, station mobile) et un réseau GPRS. Contexte = divers aspects tels que l'acheminement, la qualité du service, la sécurité, les tarifs, etc.
PDS	**P**remises **D**istributed **S**ystem, système distribué sur site. Concerne différents niveaux d'intégration systèmes pour la transmission de données, les télécommunications, le chauffage, la ventilation, la surveillance, etc.
Photocoupleur	Assure une transmission par le biais de la lumière (LED, phototransistors, etc.). Ne conduit pas le courant électrique et assure donc une isolation galvanique.
Photoplexeur	Multiplexeur pour fibre optique. Voir " Multiplexeur ".

BACK

SPLC/API	**P**rogrammable **L**ogic **C**ontroller, API Automate Programmable Industriel.
Polling (interrogation)	Invitation à émettre. L'ordinateur principal " demande " aux équipements connectés s'ils ont des informations à transmettre.
POTS	**P**lain **O**ld **T**elephone **S**ystem (service téléphonique traditionnel), identique au RTC
PPP	**P**oint to **P**oint **P**rotocol (protocole point à point). Protocole de communication permettant à un PC de se connecter et de communiquer avec une connexion Ethernet supplémentaire via un lien en série.
PRI	**P**rimary **R**ate **I**nterface (interface à débit primaire), service RNIS donnant accès à un canal D à 64 kbit/s et à 30 canaux B (en Europe).
PROFIBUS	Norme de réseau industriel.
Protocole	Régule la transmission de données, les rapports entre signaux, les mode d'émission, de réception et d'interruption, le traitement des files d'attente, etc.
PSTN	**P**ublic **S**witched **T**elephone **N**etwork (réseau téléphonique commuté ou RTC), le réseau téléphonique public classique.
QoS/QdS	**Q**ualité **d**e **S**ervice. Niveau spécifique de qualité des services réseau (écho, bruit, taux d'erreur sur les bits, temps de connexion, etc.).
Rail DIN	**D**eutsche **I**ndustri **N**orme. Rail servant au montage des équipements en armoire, conforme à la norme allemande DIN.
Répéteur	Amplificateur de signal permettant d'augmenter la distance de transmission du réseau.
Réseau	Ensemble des liaisons de communication entre plusieurs équipements.
Réseau commuté	Autre nom du réseau téléphonique commuté (RTC).
Réseau en anneau	Réseau dont tous les composants sont connectés en série et forment un anneau fermé, les transmissions atteignant chacun d'entre eux.
Réseau en étoile	Réseau constitué autour d'un poste central relié directement à un certain nombre de postes périphériques.
Réseau étendu (WAN)	Un WAN (**W**ide **A**rea**N**etwork, réseau étendu)est un réseau de communication dispersé géographiquement.

BACK

Réseau local (LAN)	Un réseau LAN (Local Area Network) est un groupe d'ordinateurs ou périphériques Ethernet qui partagent une structure de communication commune. La taille d'un réseau local est très variable, de quelques périphériques à plusieurs centaines.
Résistance	Résistance électrique d'un câble par kilomètre.
RJ-45	Connecteur modulaire 8 broches conforme à la norme ISO 8877.
RLP	**R**adio **L**ink **P**rotocol, protocole de liaison radio. Protocole de correction d'erreur en transmissions GSM.
RMON	**R**emote **Mon**itoring (contrôle à distance).Standard MIB fournissant des données de diagnostic relatives aux réseaux.
Roaming	Possibilité d'utiliser des équipements GSM sur les réseaux d'opérateurs différents.
Routeur	Un routeur est un périphérique (généralement un PC) connecté à un minimum de deux réseaux et qui détermine le point suivant du réseau vers lequel un paquet doit être envoyé. En général, un paquet peut transiter par plusieurs routeurs avant de parvenir à sa destination finale. Les routeurs plus élaborés disposent de tables de référence qui leur permettent de déterminer les itinéraires les plus courts et les plus rentables pour envoyer un paquet.
RS-232	Norme américaine, communication série.
Segment	Portion donnée d'un réseau.
Semi-duplex	Communication à deux sens.
Serveur client	Solution de réseau local – le traitement des données et les logiciels sont partagés entre des ordinateurs personnels (clients) et un serveur.
Signal d'état	Indique l'état du matériel connecté (sous tension, prêt à recevoir, prêt à émettre, etc.).
Signaux de contrôle de flux (handshaking)	Envoi de signaux de confirmation et d'état entre des équipements en communication à des fins de contrôle du flux de données.
Simplex	Transmission à sens unique.
SMS	**S**hort **M**essage **S**ervice (service de messages courts), courts messages texte passant par le réseau GSM.
Synchrone	Transmission se caractérisant par l'émission et la réception de caractères en séquence unique à un débit constant régulé par les signaux d'horloge.
Tampon	Mémoire de stockage temporaire des données, servant entre autres lors de l'attente du signal d'envoi par le récepteur.

BACK

TCP	**T**ransmission**C**ontrol **P**rotocol, protocole de contrôle de transmission.Assure la remise et la vérification des données d'un périphérique à l'autre. Il détecte les erreurs et les pertes de données ; il peut également déclencher une nouvelle transmission jusqu'à ce que la réception des données soit correcte et complète.
TCP/IP	(**T**ransmission and **C**ontrol **P**rotocol/**I**nternet **P**protocol (protocole de contrôle de transmission/protocole Internet). Protocole Internet permettant l'interconnexion de plusieurs réseaux locaux en un réseau étendu de manière à assurer l'échange de données quelle qu'en soit la source, notamment sur la base d'un protocole d'acheminement. Le protocole TCP/IP, issu de l'environnement UNIX, est en passe de s'imposer en tant que protocole réseau dans divers autres environnements.
TDM	**T**ime **D**ivision **M**ultiplexing (multiplexage temporel). Multiplexage par répartition dans le temps, le canal étant divisé en tranches temporelles auxquelles sont affectés des sous-canaux différents. Voir " Multiplexeur ".
Terminal	Poste de travail sans capacité de traitement qui lui soit propre, raccordé à un ordinateur central. Un ordinateur personnel (PC, etc.) peut également tenir lieu de terminal dans certains contextes.
TFTP	**T**rivial **F**ile **T**ransfer **P**rotocol (protocole de transfert de fichiers secondaires).Un autre protocole simple permettant de transférer des fichiers, basé sur le protocole UDP/IP.
Topologie	Architecture d'un réseau.
TP	Port de type 'Copper **T**wisted **P**air' (cuivre à paire torsadée).
Trame (frame)	Une **trame**correspond aux informations transmises entre deux périphériques Ethernet, constituant une unité complète avec adressage et informations de contrôle du protocole. Les informations sont transmises en série bit par bit.
Transfert intercellulaire (handover)	Passage d'une station de base à une autre en communication sur réseau GSM.
Transitoires	Importantes surintensités et perturbations réseau.
Transmission en série	Transmission des caractères un à la fois, contrairement à une transmission parallèle.

BACK

Transmission parallèle	Transmission simultanée de bits de données sur chaque ligne. Un caractère de 8 bits (octet) nécessite 8 lignes parallèles. En communication 32 bits, il y a transmission simultanée de 4 octets sur 32 lignes parallèles. La transmission parallèle concerne principalement les communications à l'intérieur des équipements ainsi qu'entre eux sur de très courtes distances.
UDP	**U**ser **D**atagram **P**rotocol (protocole de datagramme utilisateur)permet la remise de données d'un périphérique à l'autre. L'UDP utilise généralement le protocole IP pour transférer les données mais, contrairement au TCP, ne permet pas la fragmentation des paquets. L'application utilisant le protocole UDP doit donc être capable de détecter si le message ou les données ont été réceptionnés correctement. Toutefois, l'UDP présente l'avantage d'une vitesse supérieure et d'un coût réduit par rapport au TCP. L'UDP est idéal pour les applications requérant le transfert rapide de petites quantités de données.
Unité MAU	**M**edia **A**ttachment **U**nit, unité de branchement de support. Permet à un périphérique de s'insérer dans un réseau LAN. En général, ce type d'interface est utilisé avec un câble coaxial appelé " Thicknet " ou " Thinnet ".
Unix	Système d'exploitation multi-utilisateurs pour gros ordinateurs et mini-ordinateurs conçu pour la gestion simultanée de nombreux processus.
V.24	Norme américaine, communication série.
VN4	Norme française de liaisons RNIS.

BACK