

Licence Professionnelle EGC-ITEB

Energie - Génie Climatique:

Intelligence Technique et Energétique du Bâtiment

Module EC2b_2

Réseau de Communication et Télégestion

par Pr. **Eddy BAJIC**

IUT Nancy Brabois - Génie Electrique & Informatique Industrielle
Université de Lorraine

SOMMAIRE

Introduction	p3
Fonctionnement d'un réseau par l'exemple	p4
Architecture des réseaux	p8
Transmission de Données	p15
Connectique et Câblage des Réseaux	p23
Méthodes de Gestion d'Accès à la Voie	p36
Détection des Erreurs en Transmission	p42
Le Modèle OSI	p49
Le Réseau MODBUS	p57
Le Réseau ETHERNET	p75
Impact de Ethernet et Internet dans les automatismes	p88
Module Wago sur Ethernet	p93
Internet	p96
Adressage IP	p105
Protocole DHCP/BOOTP	p109
Routage d'un paquet IP	p112
Protocole ARP	p115
Serveur DNS	p118
Le Protocole IP	p125
Le Protocole TCP	p132
Le Protocole UDP	p135
Ethernet Industriel MODBUS-TCP	p138

Un **Réseau de Communication Industriel / Bâtiment** est un système de communication numérique entre des équipements d'un Automatismes Industriel / Bâtiment.

☞ Automates Programmables, Contrôleurs, Régulateur, Micro-Ordinateur PC, IHM Pupitre Opérateur, Centrale intelligente, ...

☞ dans le but de réaliser :

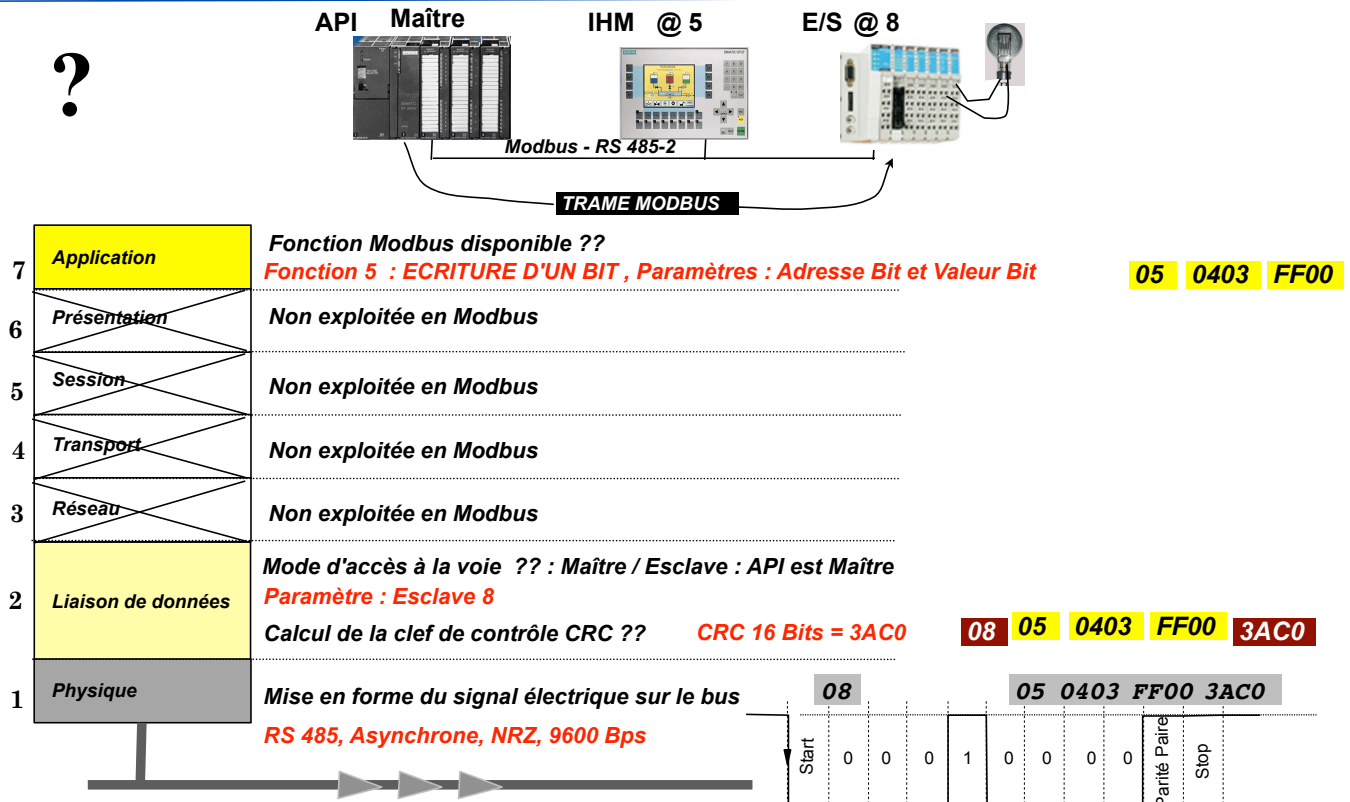
-
-
-
-

Les Besoins Industriels sont :

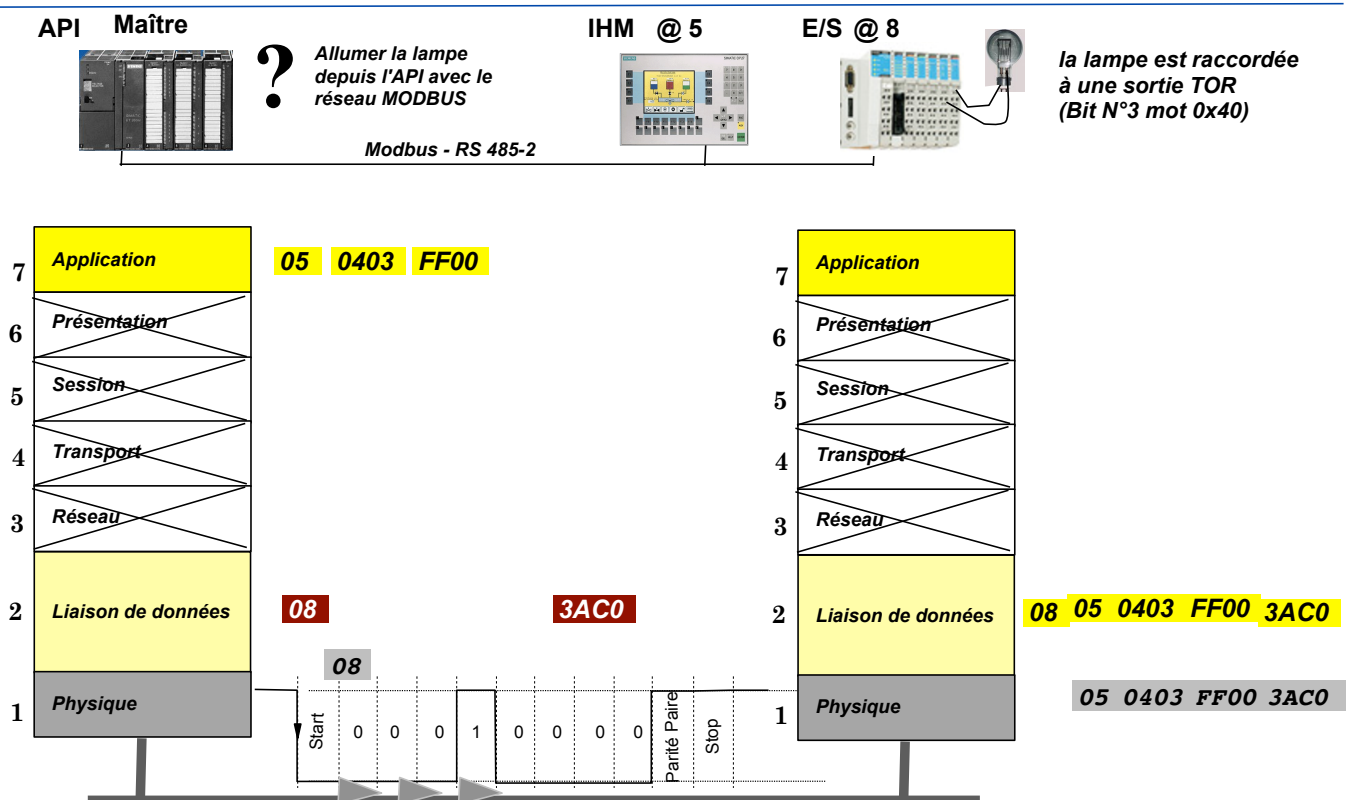
- Faire **Coopérer** des systèmes industriels de contrôle / commande
- Rendre **Accessibles** les *informations du processus en tout point* du Bâtiment, de la ville, du Monde ...
- Disposer d'une **Structure Evolutive** de communication
- **Localisation géographique** limitée mais **Extensible**

Fonctionnement d'un réseau par l'exemple

Analogie du Modèle OSI pour Modbus



Analogie du Modèle OSI pour Modbus



Un réseau se définit par :

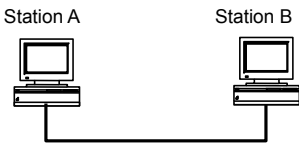
- Ses **limites physiques** (longueur, débit, nombre "d'abonnés"...).
-
-
- Les **modes de transmissions** (synchrone/asynchrone, codage NRZ/Manchester...)
-
- Son **analogie par rapport au Modèle OSI**

Architecture des réseaux

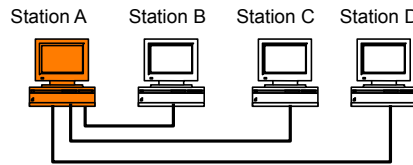
L'architecture d'un réseau représente :

1. la forme
2. la répartition

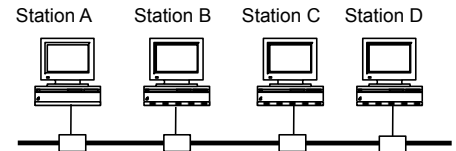
Liaison Point à Point



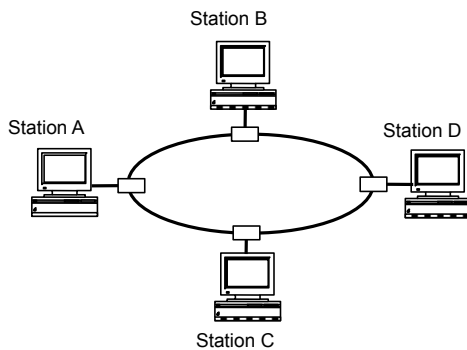
Réseau en Etoile



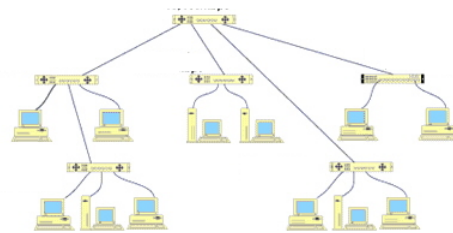
Réseau en Bus



Réseau en Anneau

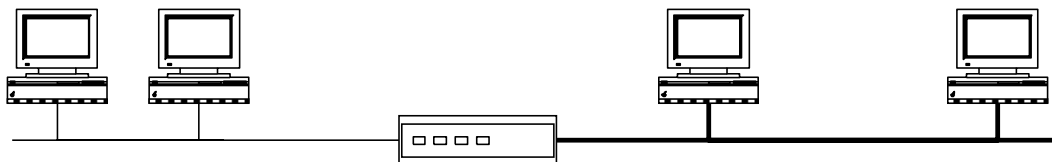


Réseau Arborescent



Répéteur

Utilisé pour les topologies en Bus, il assure la régénération et l'amplification du signal physique. Il connecte ensemble plusieurs segments du même réseau.



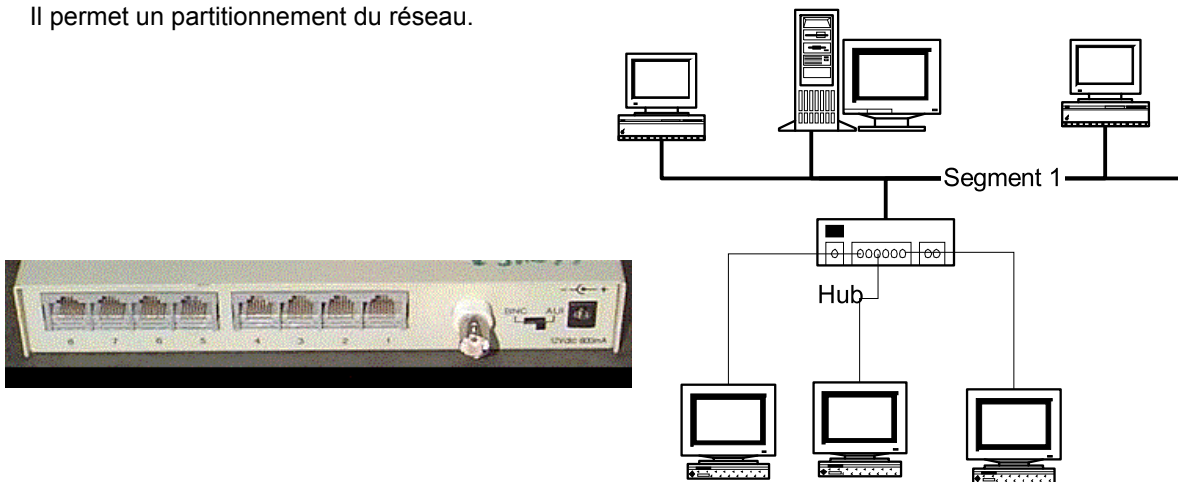
Un répéteur permet d'étendre la distance du réseau :

- ↳ **Equipement PASSIF** : Ne concerne que le signal électrique
- ↳ **Extension du Réseau** par Interconnexion de deux segments A et B
- ↳ **Changement de Médium** : Câble coaxial, Paire Torsadée, Fibre Optique

Utilisé pour les topologies en Bus et en Anneau, il assure la fonction de convertisseur de Média et de *concentrateur* d'accès.

- Appelé **HUB** ou **Concentrateur**
- **Équipement ACTIF** : Une trame reçue sur une des voies est diffusée sur toutes les autres voies
- **Structure apparente en Etoile mais Structure réelle en Bus**

Il permet un partitionnement du réseau.



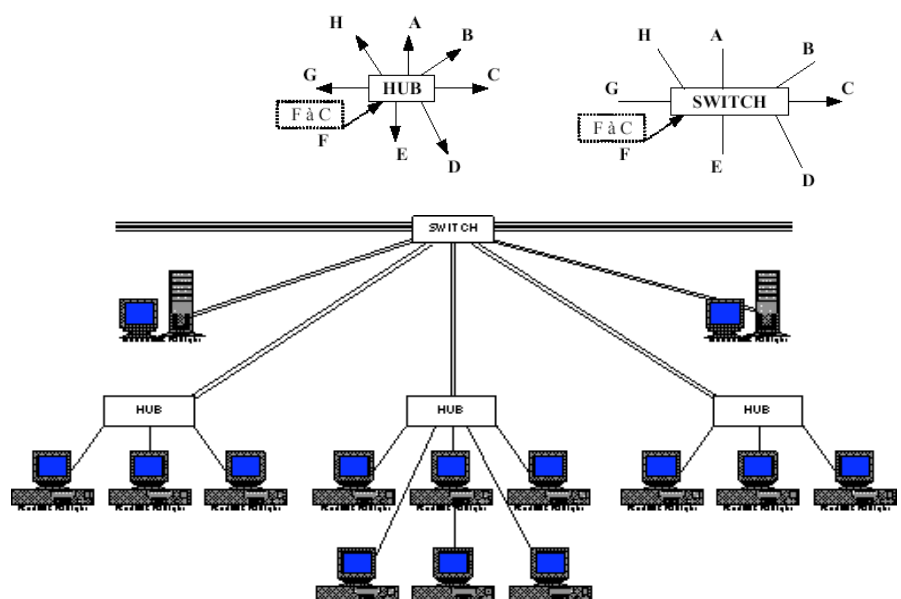
Contrairement au Hub avec qui toute la bande passante est utilisée dès qu'une station émet, Le switch gère individuellement chaque station en lui offrant toute la bande passante.

Commutateur à la volée (on the fly, ou Cut and through)

Très rapide,
Commence l'émission de la trame sur le port de destination avant de l'avoir reçue complètement sur le port de réception.
Les trames erronées sont propagées sur le réseau

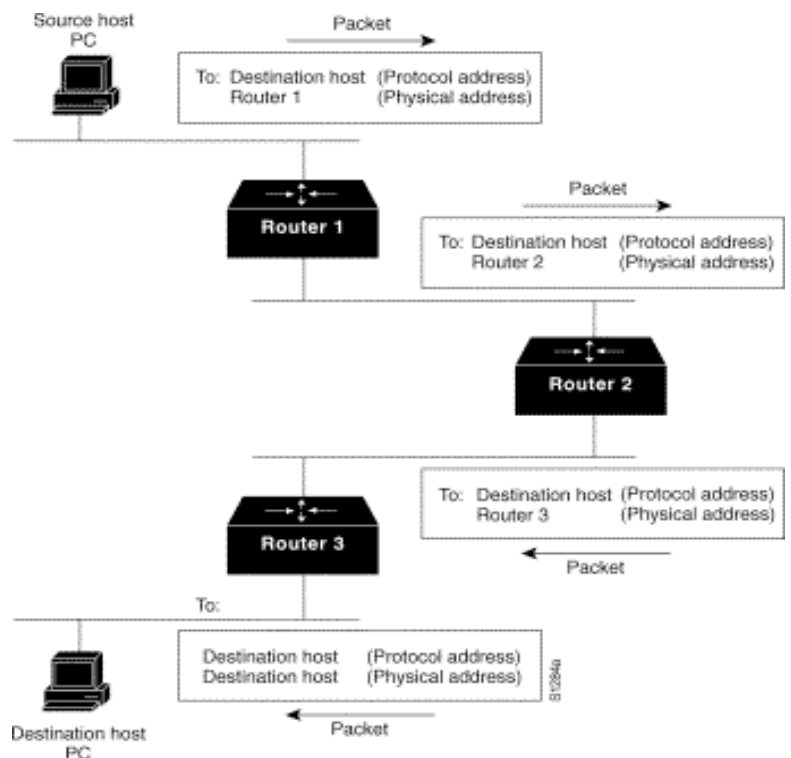
Commutateurs « store and forward »

La trame est reçue sur le port, contrôlée puis émise sur le port de destination.
Moins rapides que le précédent, mais offrent l'avantage de vérifier la validité des trames avant de les réémettre.



Routeur

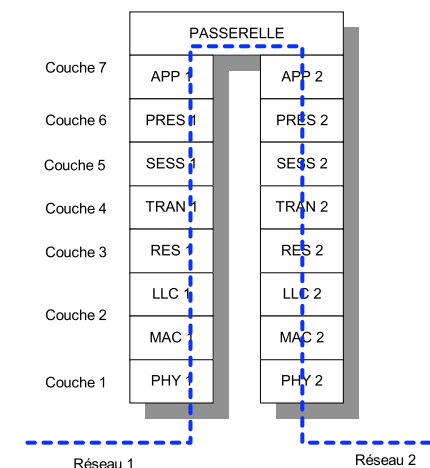
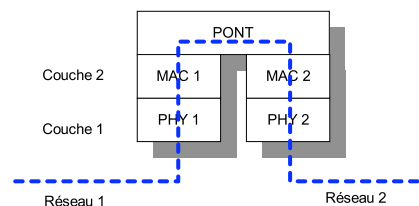
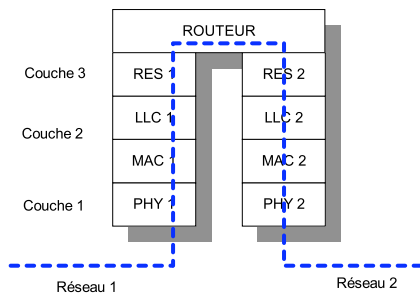
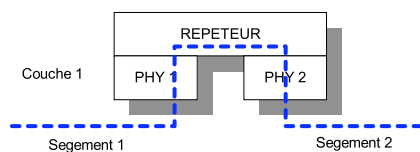
Equipement destiné à acheminer des trames d'une station d'un réseau vers une autre station d'un autre réseau distant. A l'inverse du pont il interconnecte deux réseaux différents.



→ Agit comme un Pont

→ Filtre les trames selon les adresses
Emetteur / Destinataire

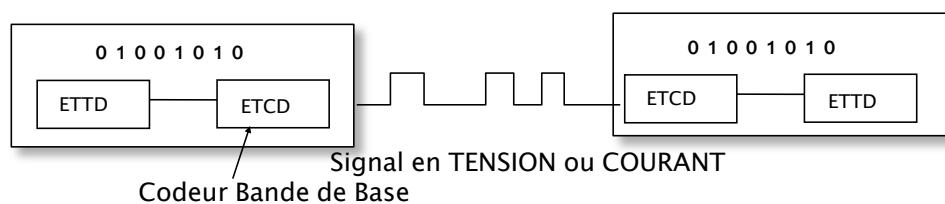
Equipements d'Interconnexion et Modèle OSI



Transmission de Données

Transmission Numérique en Bande de Base

Les informations numériques sont transmises directement sur le support par des changements d'états discrets du signal (0 ou 1).



Tension Absolue	$\pm 12\text{ V}$	: Standard RS 232 - V24
Tension Différentielle	$\pm 3\text{ V}$	: Standard RS 422 / RS 485
Transmission en courant	$0 - 20\text{ mA}$	: Standard RS 232 Boucle de Courant



La transmission directe des suites de symboles binaires n'est pas toujours souhaitable :

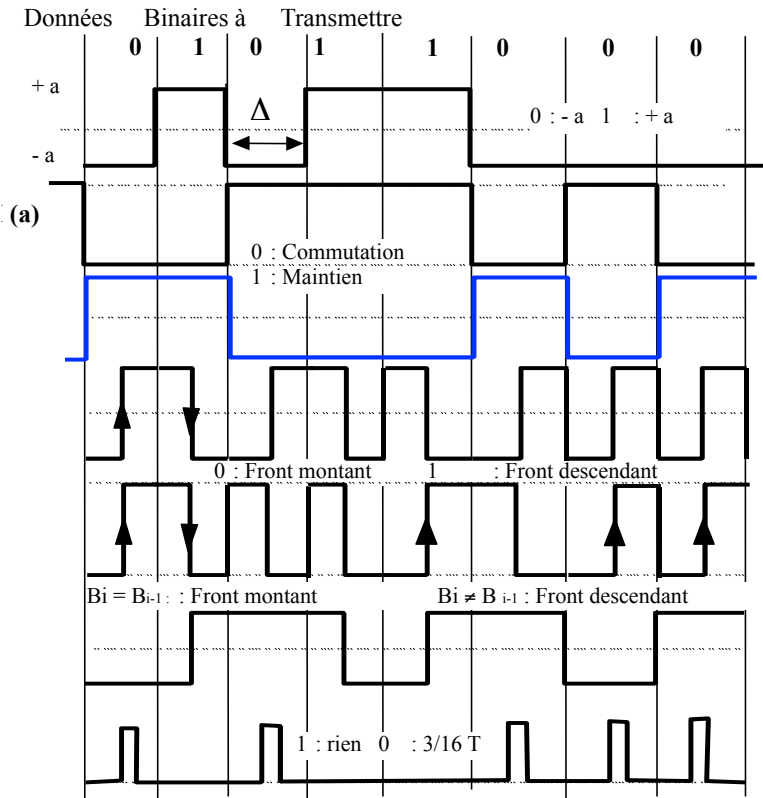
- ⇒ Les Bandes Passantes des supports sont limitées vers le bas comme vers le haut
- ⇒ La synchronisation du récepteur par transmission du signal d'horloge doit être possible
- ⇒ Les déformations des signaux sont d'autant plus importants que la bande de fréquence utilisée est large.



Il est donc nécessaire d'**Adapter le signal** pour qu'il exploite au mieux les caractéristiques de la ligne par des **Techniques de Codage en Bande de Base**.



Tension :
+a ou -a

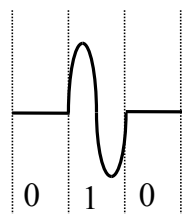


La modulation de signal transforme le message à transmettre en un signal adapté à la transmission sur un support passe bande. Un **MODEM** (**MOD**ulateur/ **DEM**odulateur) remplit cette fonction. Il permet :

- ⇒ une **transposition** du signal dans un domaine de fréquence correspondant au support ;
- ⇒ une **protection** du signal contre les bruits ;
- ⇒ de transmettre simultanément **plusieurs signaux** dans des bandes de fréquences adjacentes.

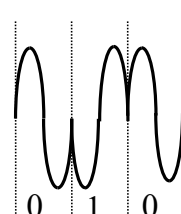
↪ Une **Onde Porteuse** $p(t)$ est modulée par le signal numérique à transmettre

$$p(t) = A \cos(2 \Pi f t + \phi)$$



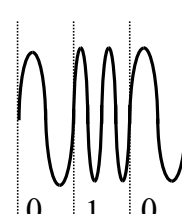
A.M. / A.S.K.
Amplitude Shift Keying

$$s(t) = \begin{cases} A_c \cos(2\pi f_c t) & \text{Binary 1} \\ 0 & \text{Binary 0} \end{cases}$$



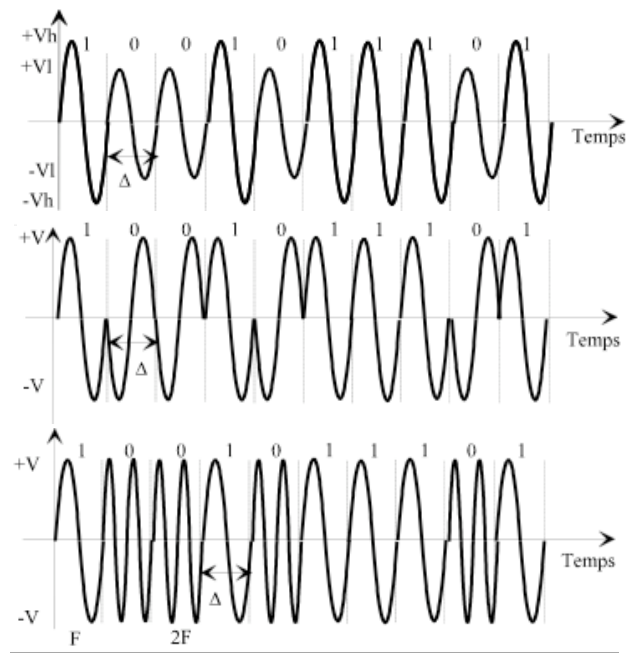
P.S.K.
Phase Shift Keying

$$s(t) = \begin{cases} A_c \cos(2\pi f_c t) & \text{Binary 1} \\ A_c \cos(2\pi f_c t + \pi) & \text{Binary 0} \end{cases}$$



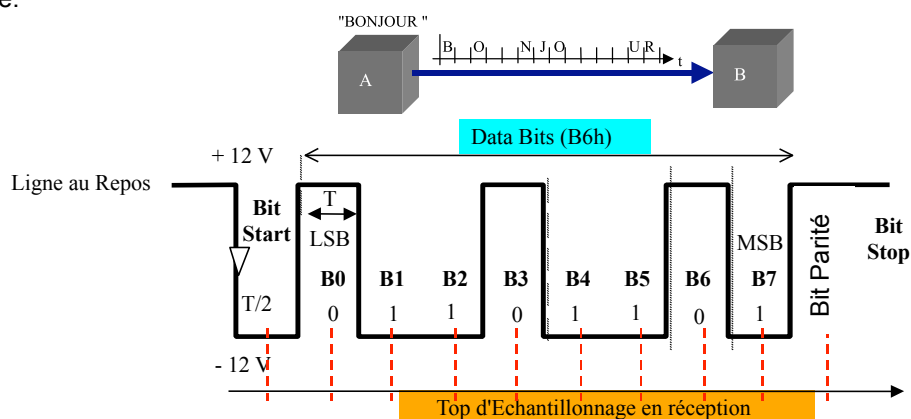
F.S.K.
Frequency Shift Keying

$$s(t) = \begin{cases} A_c \cos(2\pi f_1 t) & \text{Binary 1} \\ A_c \cos(2\pi f_2 t) & \text{Binary 0} \end{cases}$$



Les **messages** sont transmis sous forme de **mots ou caractères émis un par un**, et séparés par des temps aléatoires.

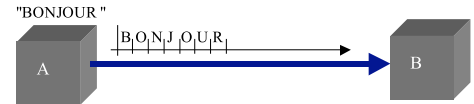
Les **caractères sont transmis de façon asynchrone**, il faut donc **synchroniser le récepteur** en début de chaque caractère.



Chaque caractère à transmettre est encadré par un bit de début (Start : -12V) et un ou des bits de fin (Stop : +12V). C'est le mode de transmission utilisé en standard RS 232 appelé aussi V24.

Cette mise en forme est assurée par une interface série (**UART** : Universal Asynchronous Receiver Transmitter)

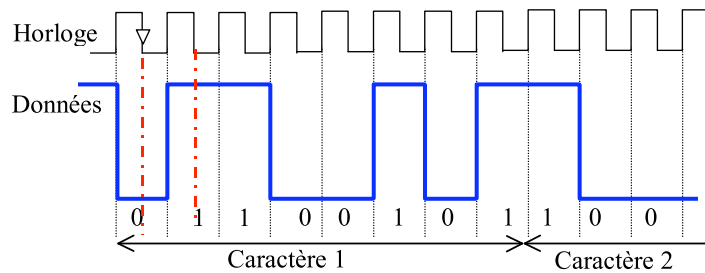
Les **messages** est constitué de caractères émis en bloc continu.



Mode de Synchronisation du récepteur

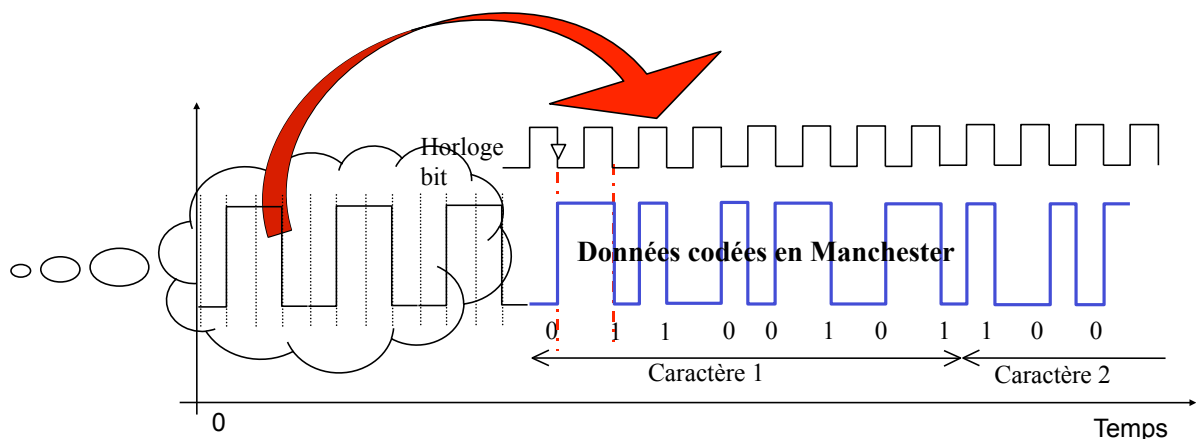
-> par horloge transmise en parallèle

-> par signal de données Auto-Synchrone



Les données sont émises en paquets de caractères consécutifs sans intervalles.

Le message transmis contient les données PLUS une mécanique d'auto-synchronisation de l'horloge de réception



Le préambule est une suite de bits alternants 0 et 1 permettant de synchroniser l'horloge de réception
 ⇒ **Préambule Ethernet = 7 Octets 0xAA Plus 1 Octet 0xAB**

Les données sont émises en paquets de caractères consécutifs sans intervalles.

Connectique et Câblage des Réseaux

Les Câbles Métalliques

Les paires torsadées se classent en deux catégories selon qu'elles sont entourées d'une enveloppe métallique dite de blindage garantissant une meilleure immunité aux parasites grâce à un effet "cage de Faraday" :

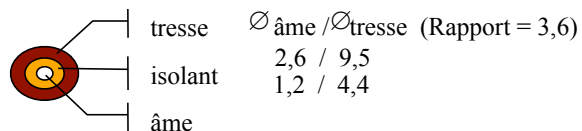
- UTP Unshielded Twisted Pair



- STP Shielded Twisted Pair



- coaxial RG-58 (1,2/4,4mm) impédance caractéristique de 50 Ω.



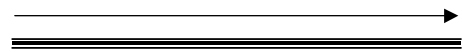
Le débit de transmission sur un câble coaxial peut aller jusqu'à de 100 MBps pour une distance de 1 Km. Une régénération du signal est nécessaire au delà de cette distance.

- Fibre Optique
- Câble Electrique 1,5mm2

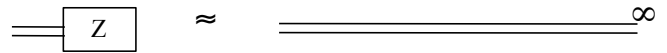
ATTENUATION : dB $A = 10 \log (P1/P2)$
Dépend de la Fréquence et de la longueur



VITESSE DE TRANSMISSION : ns / m
Par rapport à la vitesse de la lumière C



IMPEDANCE CARACTERISTIQUE : OHM
Comportement câble infini



BANDE PASSANTE : Hz
Gamme de fréquences acceptées avec 3db d'atténuation



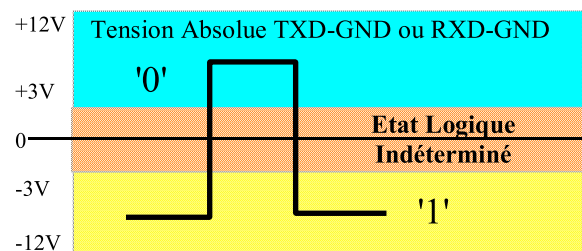
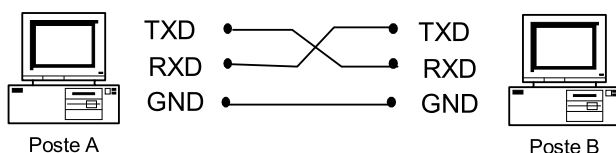
DIAPHONIE : dB
Interférence d'une ligne sur une ligne voisine

CATEGORIES DE CABLES

Catégorie 3	Jusqu'à 16 MHz, Débit 10 à 50 Mbps, Précâblage 10 Base T
Catégorie 4	Jusqu'à 20 MHz, Débit 50 Mbps, Utilisé pour Token Ring 16 MHz
Catégorie 5	Jusqu'à 100 MHz, Débit 100 Mbps et plus
Catégorie 6	Jusqu'à 1GHz, Débit > 100 Mbps

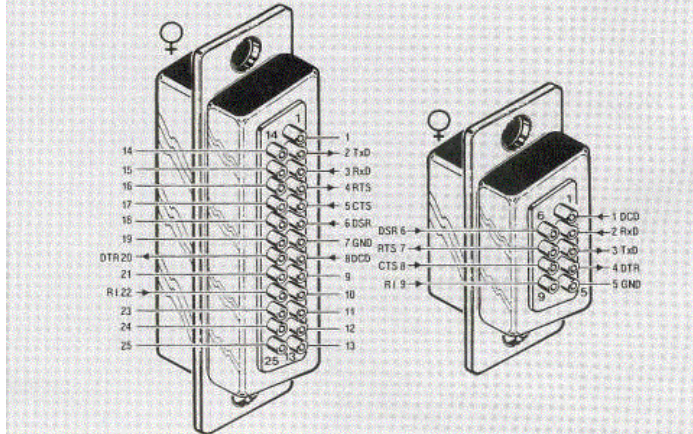
Aussi appelée **liaison V24** (CCITT : Comité Consultatif International du Télégraphe téléphone) ou **ISO 2110**.

Caractérisée par une communication half ou full duplex, établie sur 3 Fils : TXD (Transmission), RXD (Réception), GND (Masse).

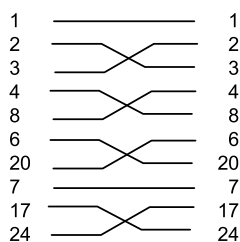


Le signal est transmis selon une **tension absolue** par rapport à une référence de tension commune **GND**. Les niveaux de tension correspondant au niveau logique.

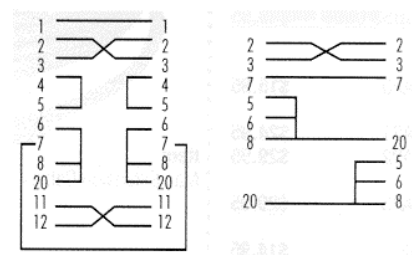
Broche DB 25	Broche Db 9	Entrée/Sortie	Dénomination	Fonction
2	3	Sortie	TxD (Transmit Data)	Émission de données
3	2	Entrée	RxD (Receive Data)	Réception de données
4	7	Sortie	RTS (Request To Send)	Activation émission
5	8	Entrée	CTS (Clear To Send)	Prêt à émettre
6	6	Entrée	DSR (Data Set Ready)	Prêt à émettre
7	5	GND	(Ground)	Masse
8	1	Entrée	DCD (Data Carrier Detect)	Niveau du signal de réception
20	4	Sortie	DTR (Data Terminal Ready)	Terminal prêt
22	9	Entrée	RI (Ring Indicator)	Appel entrant



Câblage RS232 entre deux équipements exploitant tous les signaux de contrôle, afin de permettre une synchronisation totale des équipements.



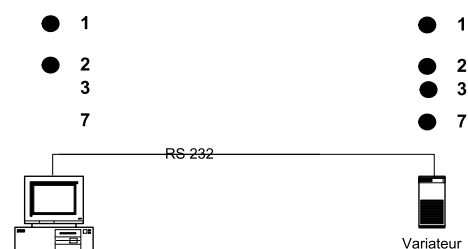
Câblage RS 232 dit "**Null Modem**" garantissant très souvent un fonctionnement correct de la liaison avec tous les types d'équipements.

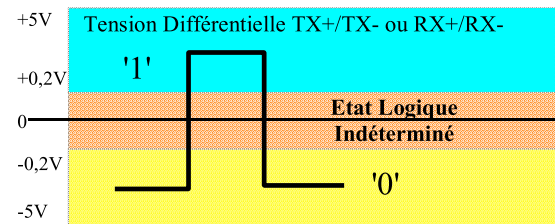


EXEMPLE :

2 équipements dotés d'une prise DB25 supportant une liaison RS232 dont le brochage est identique.

Tracer le câblage nécessaire entre les 2 équipements pour dialoguer sur le bus point à point en Null Modem.

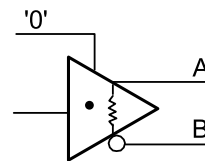
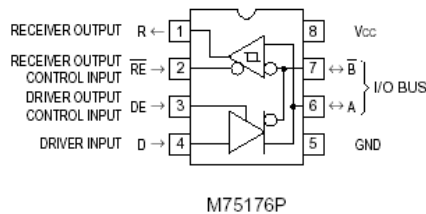




Caractérisée par une communication half ou full duplex :

- sur 4 Fils : **TX+, TX-, RX+, RX-**
- sur 2 fils : **TX-/RX- (A)** et **TX+/RX+ (B)**

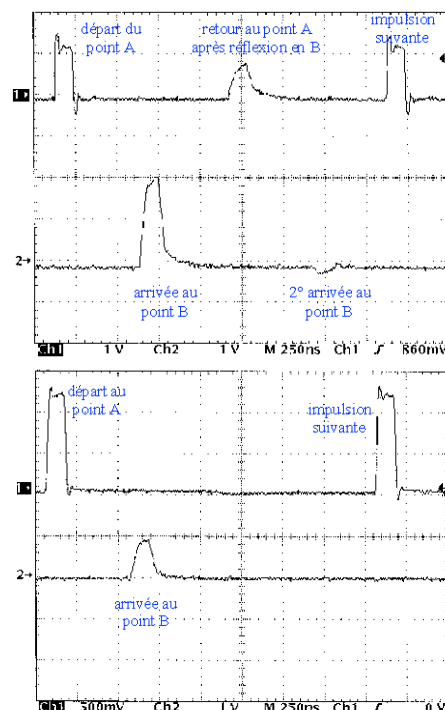
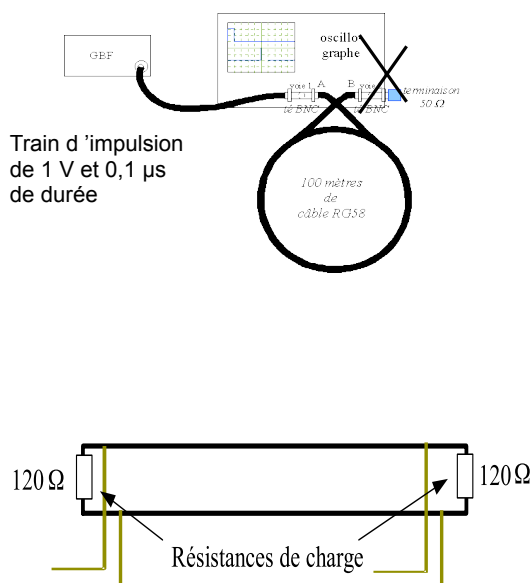
Les signaux sont gérés par des circuits "**Drivers RS485**" à 3 états : SN 75176 / DS 3695



Emetteur différentiel RS485 à 3 états : une entrée de commande 'Enable' permet de positionner le circuit en état **Haute Impédance**, permettant de ne pas charger en tension la ligne.

L'entrée **Enable** est toujours connectée au signal **RTS** de l'émetteur.

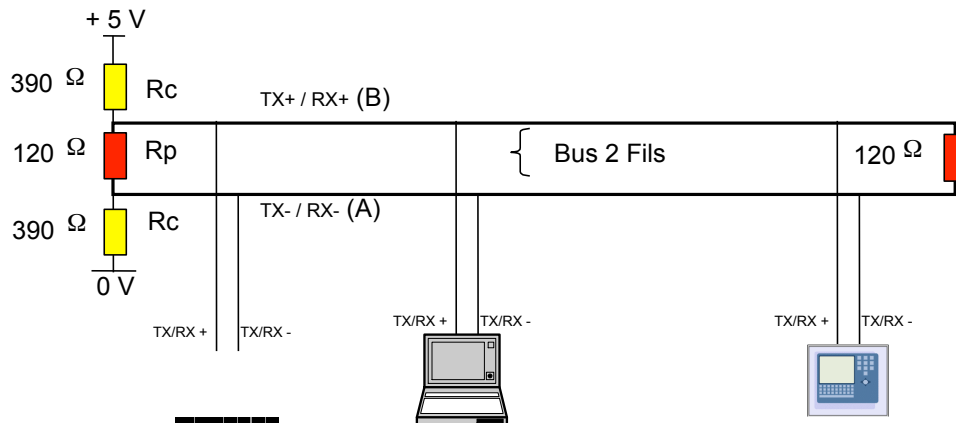
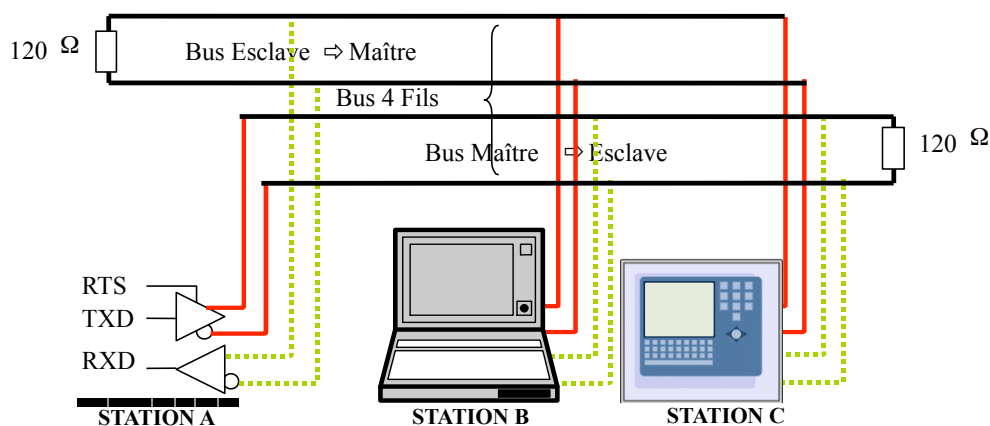
Quand un signal circule sur un câble et rencontre une discontinuité en fin de ligne, il se produit une **réflexion de signal**. Une signal réfléchi circule en sens opposé, se superpose et produit une perturbation, un bruit qui provoque une distorsion de la ligne.

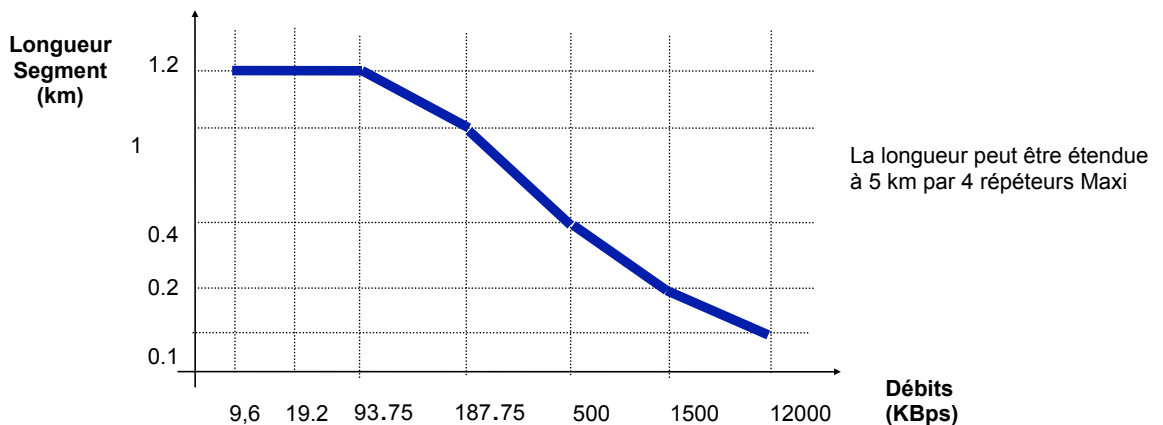


⇒

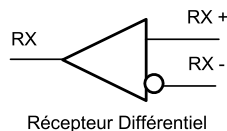
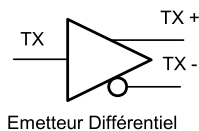
⇒ Transmission

⇒ Emetteur / Récepteur différentiel intégrés 3 états (SN 75175 / 75176 et DS 3695 / 3696.)

⇒ **Résistance Terminale** Obligatoire ($R_c = 120 \Omega$) à chaque extrémité du bus⇒ **Résistance de Polarisation du Bus** ($R_p = 390 \Omega$ Facultative mais Recommandée)⇒ Branchement identique pour toutes les stations, **2 fils** (+ 1 Masse Commune conseillé)⇒ Bus **Multi-Points** jusqu'à 32 stations⇒ Transmission **FULL DUPLEX**⇒ Branchement différent 4 fils **Maître / Esclave figé par câblage** : Station A Maître, B et C Esclaves⇒ **Résistance Terminale** Obligatoire ($R_c = 120 \Omega$) à chaque extrémité du bus⇒ **Résistance de Polarisation du Bus** ($R_p = 390 \Omega$ Facultative mais Recommandée)⇒ $R = 120 \Omega$ **Résistance Terminale de Charge** (Obligatoire + Masse Commune)



Liaison RS 422 est Identique à RS485-4 MAIS en liaison Point à Point (Driver ne sont pas 3 états)

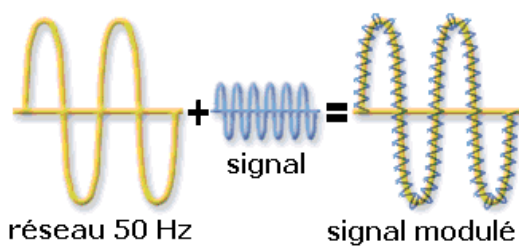


Amplificateurs différentiels RS422

Caractérisée par une communication half ou full duplex sur 4 Fils : **TX+,TX-, RX+, RX-**

La technologie CPL (Courants Porteurs en Ligne)

permet de faire transiter des informations numériques sur la ligne électrique existante



Le signal résultant transporte

-
-

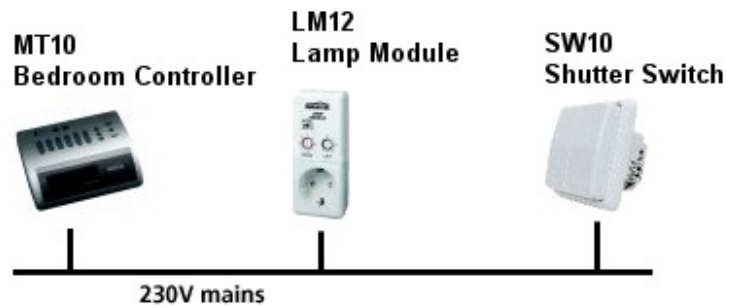
Le signal numérique se propage dans l'installation électrique et peut être récupéré en un autre point de la ligne

Les signaux CPL sont arrêtés par le disjoncteur d'une installation ce qui évite d'émettre ou de recevoir des instructions de ou vers les appartements voisins.

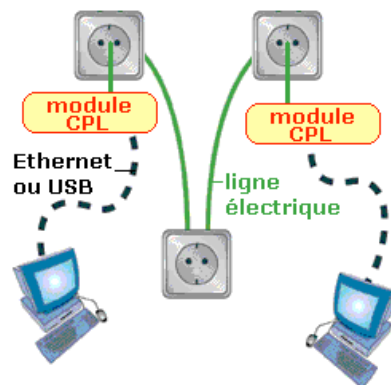
Par sécurité, on peut insérer un module de filtrage en tête de l'installation.

www.cpl-france.org

Transmission Domotique par CPL



Transmission Réseau Informatique à Domicile par CPL (Ethernet)



Modules CPL (Ethernet)



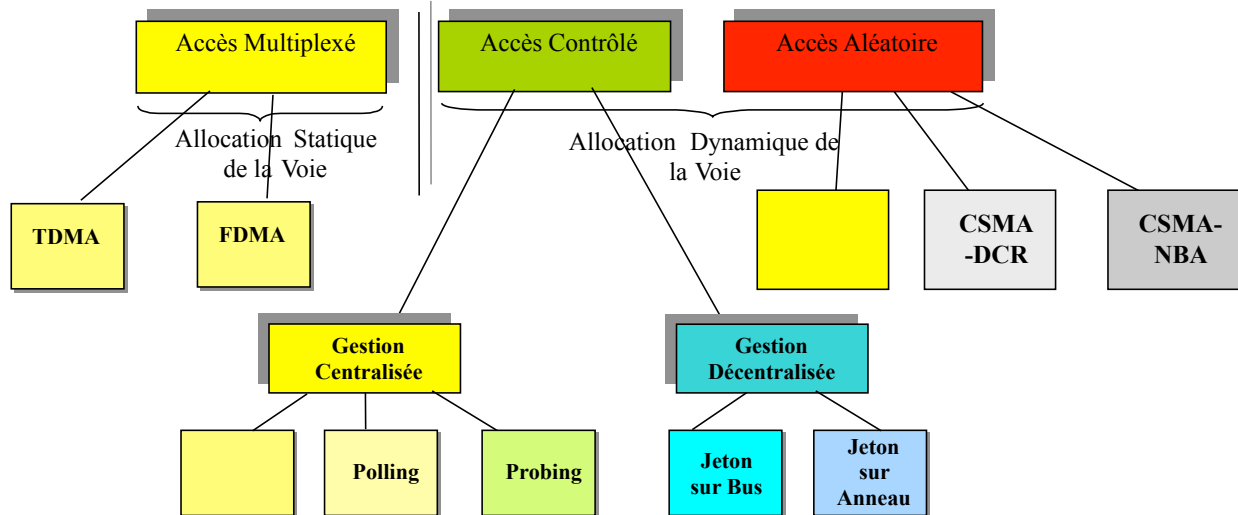
Méthodes de Gestion d'Accès à la Voie

Un réseau local permet à plusieurs stations de partager le même support (**Médium**)

Nombreuses méthodes de partage ou politiques d'accès au médium.

Les critères de choix seront :

- ↗ Le **Volume d'Information** à échanger
- ↗ Le **Nombre de Stations**
- ↗ Le Fonctionnement **Temps Réel**

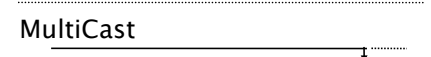
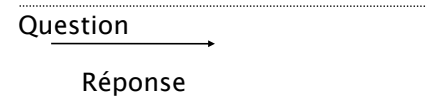
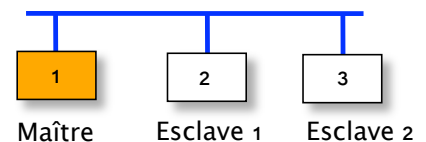


La méthode la plus élémentaire mais le plus répandue

Une station est Maître de la voie.

C'est elle qui décide des échanges.

Les Esclaves ne peuvent que répondre à une requête générée par le Maître.



Mécanisme de

Le maître émet une question destinée à **un** esclave, qui lui répond.

Mécanisme de)

Le maître émet une commande destinée à tous les esclaves, personne ne répond.

Mécanisme de

Le maître émet une commande destinée à certains esclaves, personne ne répond

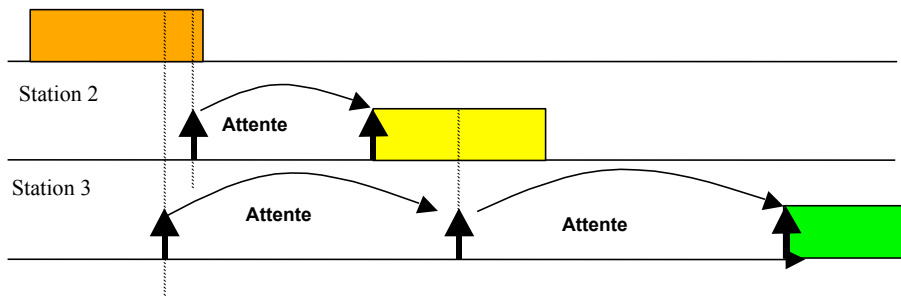


Si il y a déjà une activité, elle diffère son émission à une date ultérieure, sinon elle **émet** son message

Pendant l'émission, la station compare le signal émis (TXD) avec celui circulant sur le médium.

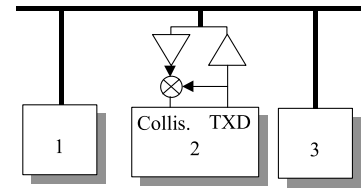
S'ils sont différents $\Rightarrow$ **COLLISION.** :

Station 1

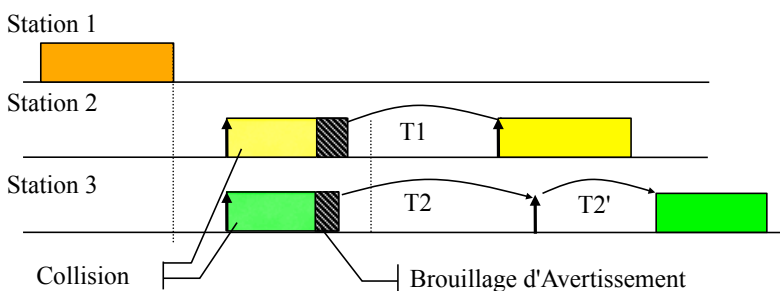


Le **temps d'attente** est fonction des n° stations différent

$\Rightarrow$ Réduit les risques de collisions, mais



Lorsqu'une collision est détectée par une station, elle émet un signal de brouillage pour assurer que la collision soit détectée par toutes les stations :



Signal de Brouillage (JAM)
(entre 32 à 48 Temps Bits)

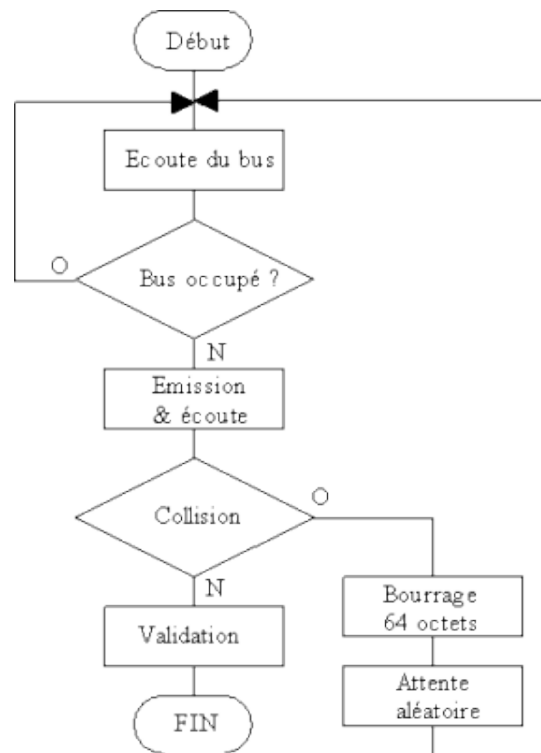
Le temps d'attente avant retransmission est tiré aléatoirement par chaque station selon son numéro de station.

Plus la temporisation est courte, plus le risque de collision est important.

Solution : La temporisation d'attente (T) est fonction du nombre de collisions déjà subies par une trame.

Soit Bt une base de temps, n le nombre de collisions

$$T = X * 51,2 \mu s \quad \text{avec } X \text{ tiré aléatoirement dans } [0, 2^n]$$

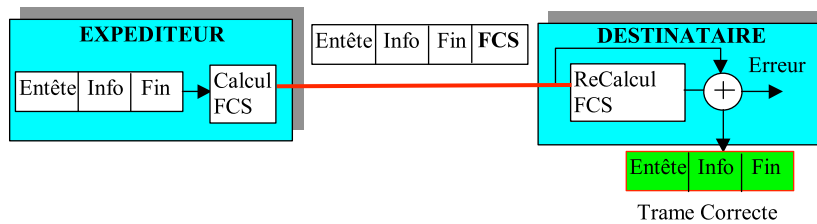


Détection des Erreurs en Transmission

On introduit une redondance dans le message transmis au moyen d'une clef de contrôle.

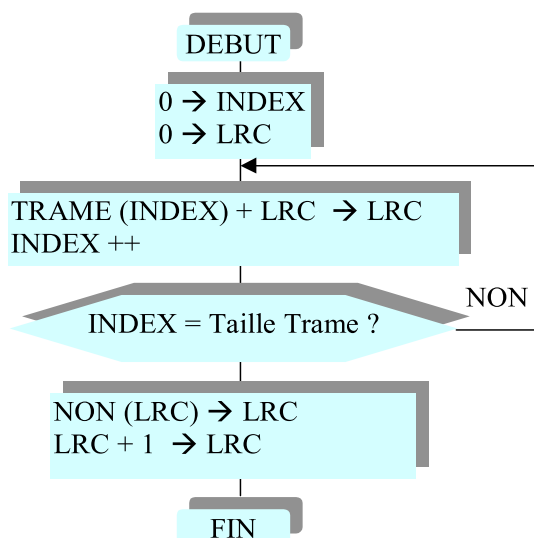


Cette clef est élaborée à partir des octets de la trame, elle est une image unique de la trame originale.



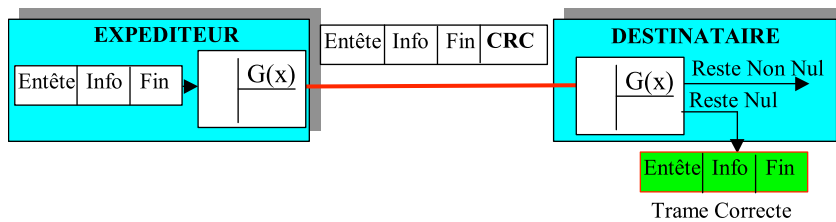
2 Mécanismes principaux :

-
-



Quelquefois la somme est transmise complémentée à 2, si bien que le récepteur n'a plus qu'à tout sommer et vérifier si le résultat est 0; dans ce cas, le FCS est bon.

↳ pas très efficace, efficacité estimée à 50%, cette méthode ne permet pas de détecter les erreurs doubles (deux bits de même rang changeant en même temps).



Chaque station calcule le CRC avec le même
Plusieurs polynômes sont normalisés

CRC 16 **Avis V41 (UIT)** ⇒

Ce polynôme permet la détection de :

- toutes les erreurs simples, doubles ou triples;
- toutes les salves d'erreur de nombre impair de bits, ou de moins de 17 bits;
- de 99,998 % des salves d'erreurs de plus de 16 bits.

⇒ Le taux d'erreur non détecté sur un circuit où le taux d'erreur est de 10^{-6} , atteint 10^{-10}

Une trame est une suite de bits, dont on fera l'analogie avec un polynôme $P(x)$ dont les coefficients a_i sont les bits de la trame.

Soit la trame : 0 1 1 0 0 1 0 1 0 1 1 1 1 0 1 1 0 1 1 1

Que l'on associe à un polynôme : $P(x) = a_0 + a_1 x^1 + a_2 x^2 + a_3 x^3 + \dots + a_n x^n$

Soit un autre polynôme $G(x)$ de degré d : $G(x) = b_0 + b_1 x^1 + b_2 x^2 + \dots + b_d x^d$

Pour $P(x)$ et $G(x)$ donnés : $R(x)$ est unique

$R(x)$: Clef de Contrôle **CRC** (Cyclical Redundancy Check)

Soit $x^d P(x) + R(x) = Q(x) \cdot G(x)$ (Etant en binaire (modulo 2), soustraction = addition)
= $T(x)$

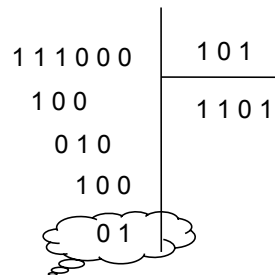
$T(x)$ constitue alors la suite de bit initiale de la trame $P(x)$ à laquelle est ajoutée la suite des d bits de $R(x)$: CRC

Soit le message à transmettre : **1 1 1 0**

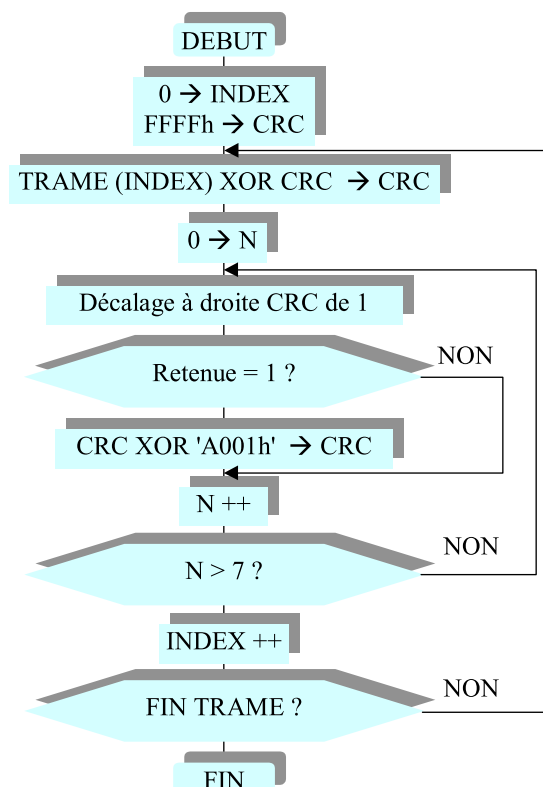
Que l'on associe à un polynôme : $P(x) = x + x^2 + x^3$

Soit le polynôme générateur $G(x) = 1 + x^2$ (suite binaire 1 0 1)

$x^2 \cdot P(x) \rightarrow 1 1 1 0 0 0$



Reste de degré < 2

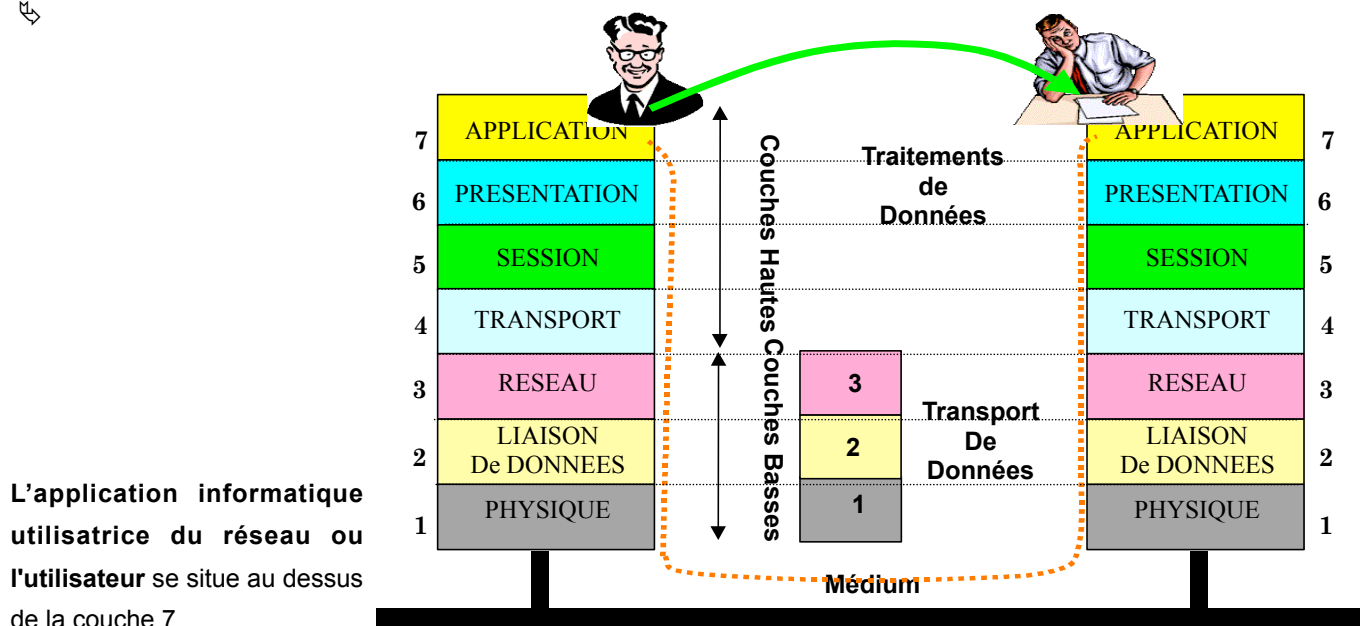


Le Modèle OSI

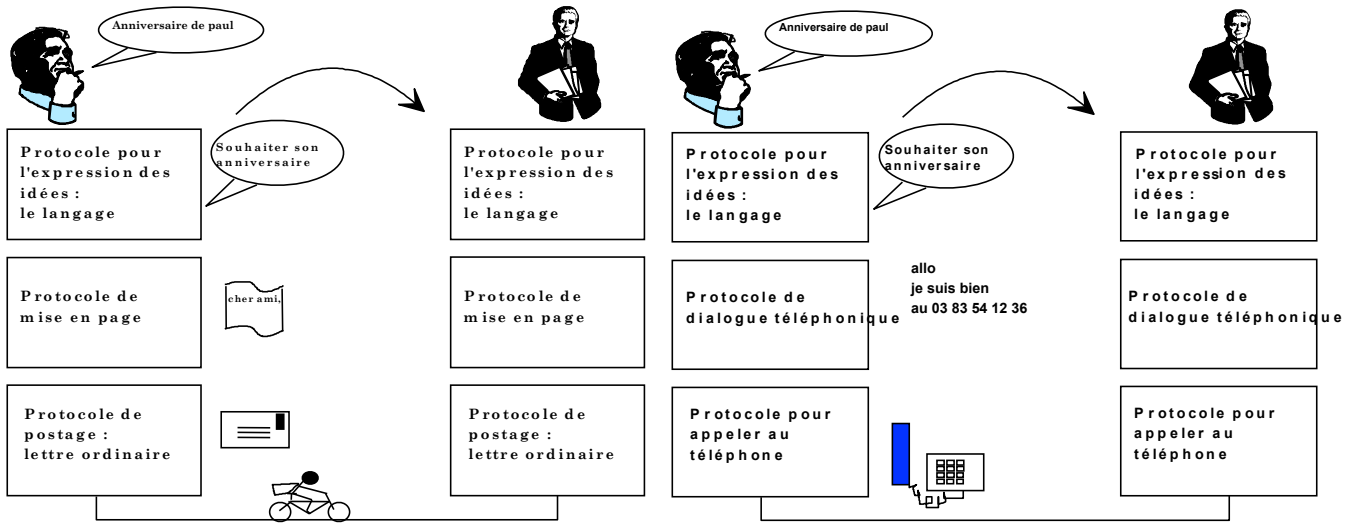
Open System Interconnection

Le Modèle OSI

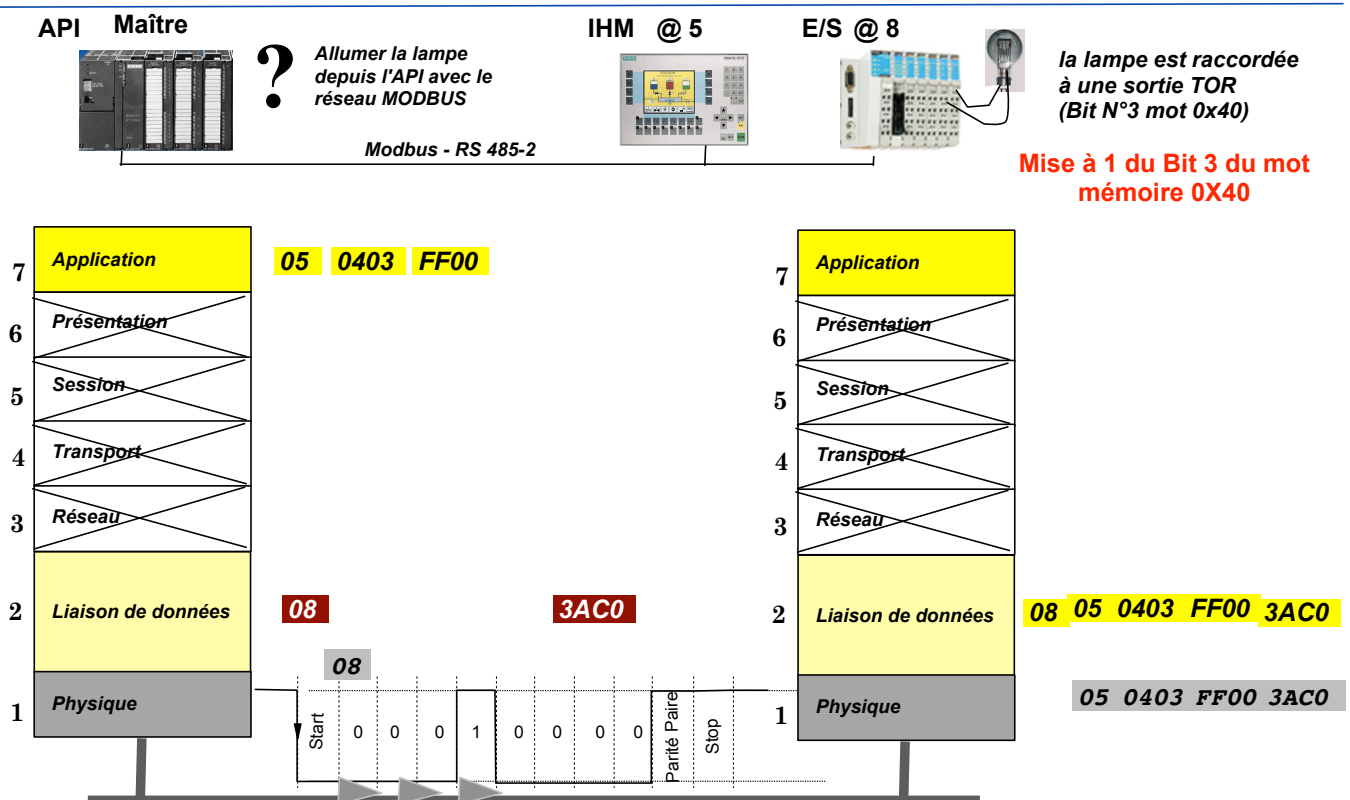
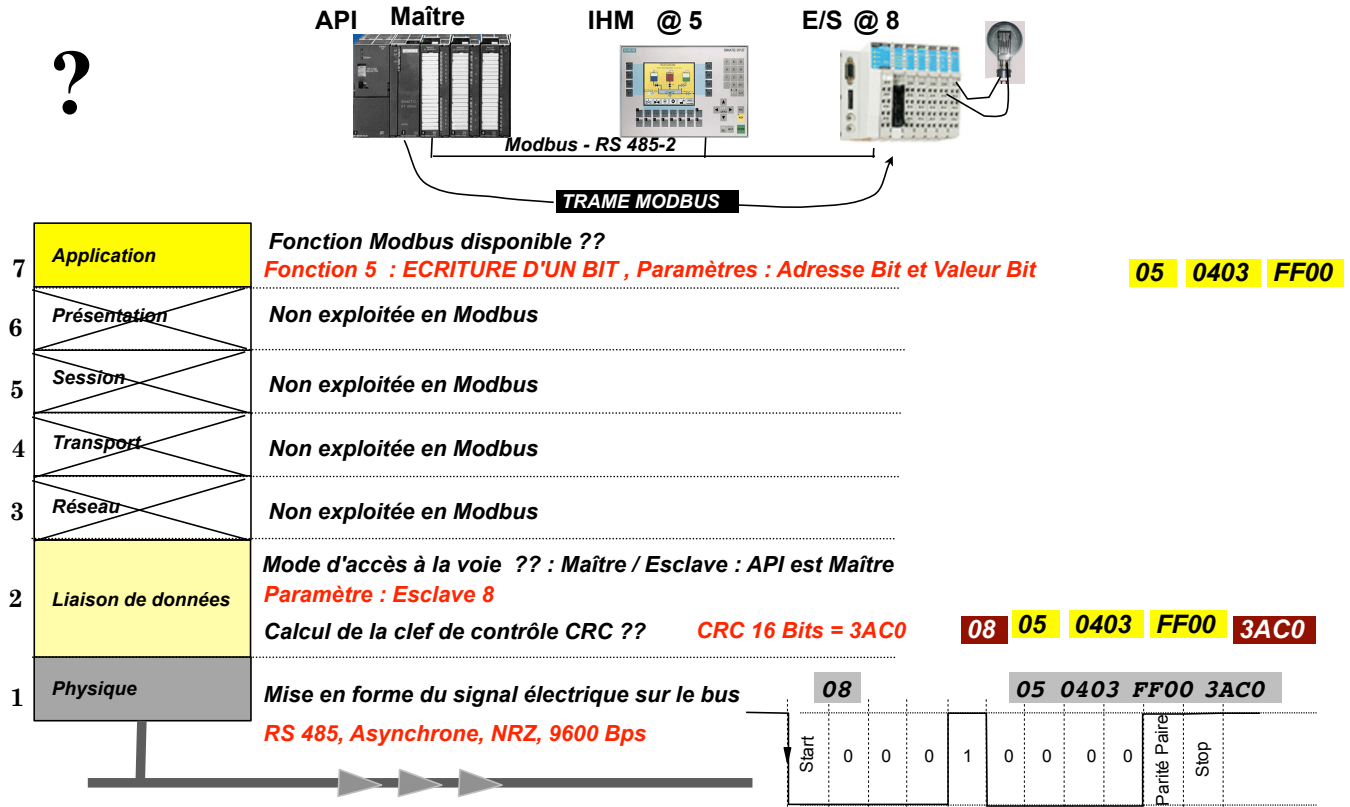
Le modèle **OSI** (Open System Interconnection) développé en 1979 par l' **ISO** (International Standard Organisation) a pour objectif de déterminer un standard pour la description, la spécification et le développement des systèmes de communication ouverts.



Tout être humain est station d'un réseau mondial car il peut communiquer avec tout le monde. Voyons comment



APPLICATION	7	Fournit à l'utilisateur les fonctions qui lui permettent d'exploiter le réseau (transfert de fichier, télécommande, gestion mode de marche, messagerie, accès aux variables mots et bits, etc ...) selon la spécialisation du réseau
PRESENTATION	6	S'occupe de la représentation des données : cryptage, compression de données, sécurité.
SESSION	5	Elle établit une communication formelle et synchronise le dialogue avec la station destination. Ouverture d'une session, transfert de données, puis fermeture de la session.
TRANSPORT	4	Assure la fiabilité du transfert d'information sur le réseau, contrôle le transport des données de bout en bout. Découpe et ré-assemble les messages volumineux en paquets et vice-versa.
RESEAU	3	Choisit le chemin optimum pour acheminer les informations vers le destinataire sur un autre réseau : techniques de ROUTAGE.
LIAISON De DONNEES	2	S'occupe de la transmission des trames en point à point entre deux équipements sur un même réseau. Prend en charge la méthode d'accès à la voie et les mécanismes de détections d'erreurs (CRC, LRC) et de contrôle de flux, retransmission.
PHYSIQUE	1	Gère tout ce qui concerne la connexion physique des équipements sur le réseau, ainsi que la réalisation des signaux de transmission sur le Médium. Assure la transmission des bits .

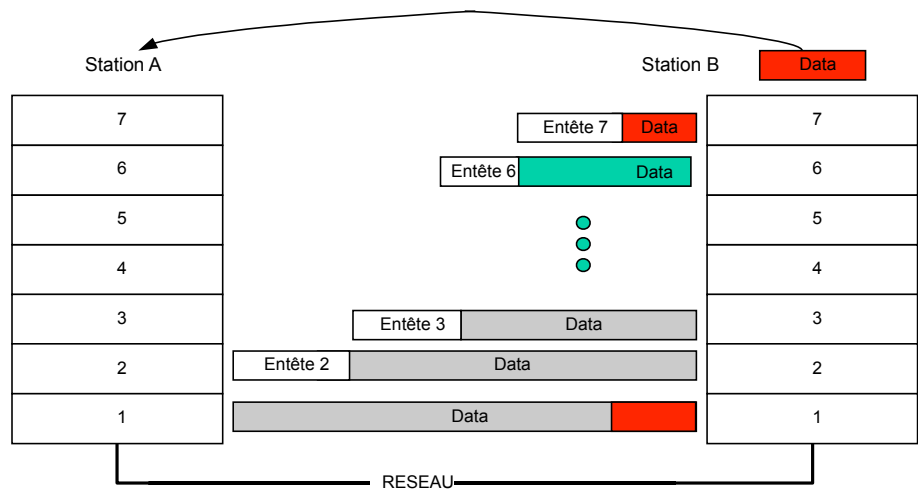


L'empilement des couches entraîne pour chaque couche, l'ajout ou la modification de données à celles qui lui sont fournies par la couche supérieure.

⇒ Ces informations sont ajoutées suivant un mécanisme dit .

Les données traitées par la couche 2 sont constituées des données de la couche 3 qui ont été encapsulées par la couche 4.

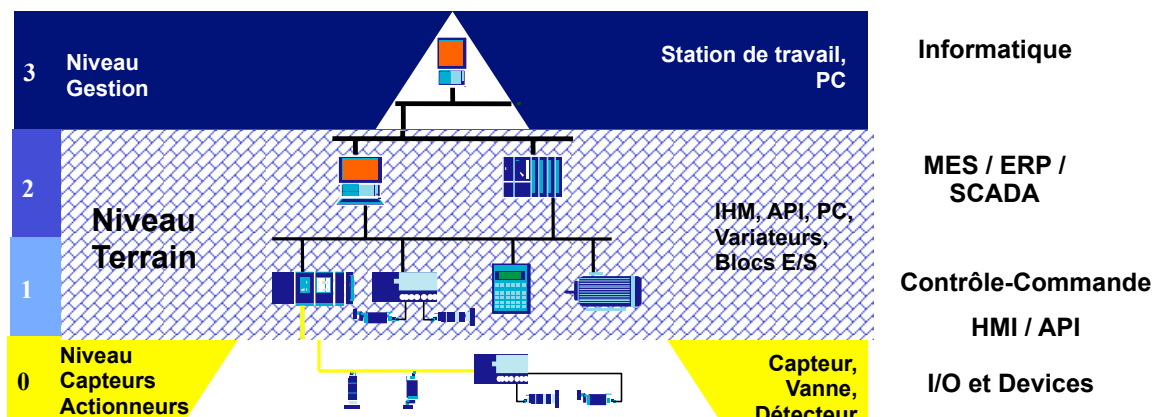
La couche 2 prendra l'ensemble comme des données sans se soucier de leur contenu déjà traité par la couche3.



Modèle d'architecture de communication dans une entreprise datant des années 1980, basé sur Plusieurs niveaux fonctionnels hiérarchisés

Chaque niveau dispose de fonctions et de besoins d'échanges d'information distincts selon sa **hiérarchie** dans la pyramide appelée aussi **Pyramide CIM** (Computer Integrated Manufacturing).

Les réseaux de communication seront aussi classifiés selon ces Niveaux.



Le Réseau Modbus

Spécifications 1979 **Gould Modicon**

Standard de fait : adopté par tous les constructeurs, permet de **faire communiquer des systèmes d'origines et de constructeurs différents**.

MODBUS est avant tout un Protocole de communication, donc un ensemble de règles d'échange et de dialogue entre des équipements, et non pas réellement un réseau.

Mais par abus de langage, un système de communication mettant en œuvre le protocole Modbus est couramment appelé "réseau Modbus".

www.modbus.org

Table ASCII

American Standard Code for Information Interchange (norme iso-646)

Un ensemble de caractères très utilisés pour la communication entre équipement informatique est codé sur 7 bits pour former un caractère ASCII

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	NUL	SOH	STH	ETH	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1	DLE	DC1	CD2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2	spc	!	"	#	\$	%	&	'	(	)	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	DEL

Pour bien lire le tableau, il faut construire le code hexadécimal en prenant d'abord le digit de la ligne, puis le digit de la colonne.

Par exemple, le Caractère "n" a pour code ASCII hexadécimal **6E**

Les "caractères" sur fond bleu sont les caractères non imprimables.



Allumer la lampe depuis l'API avec le réseau MODBUS

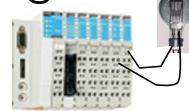
API Maître



IHM @ 5



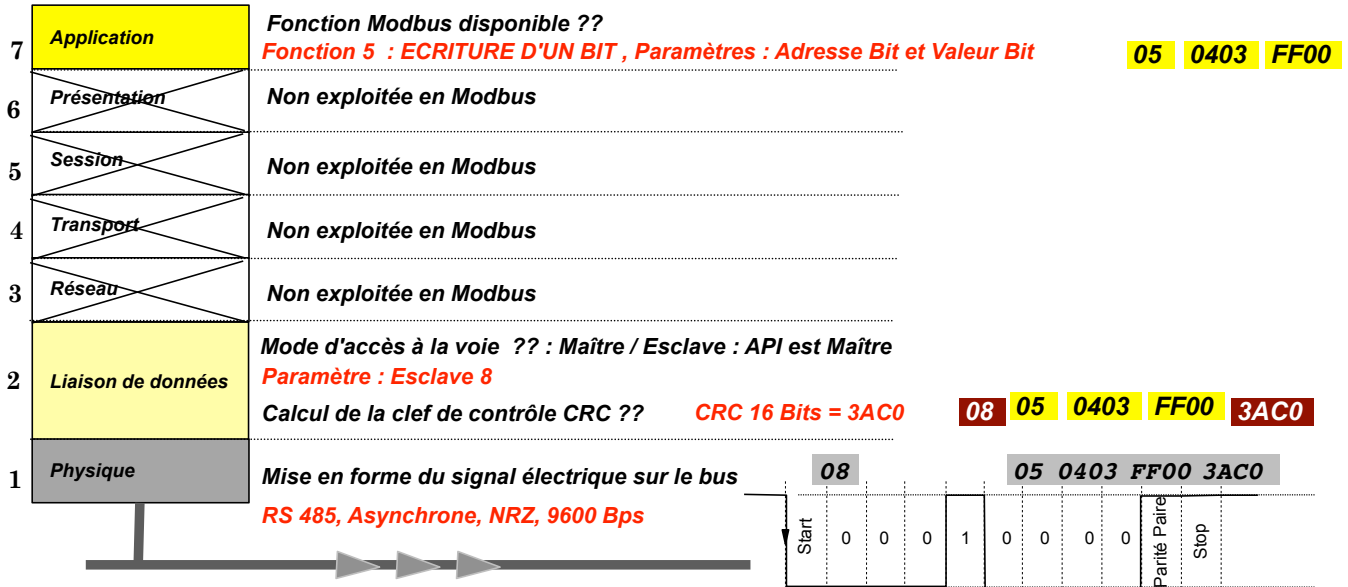
E/S @ 8



la lampe est raccordée à une sortie TOR (Bit N°3 mot 0x40)

Modbus - RS 485-2

TRAME MODBUS



API Maître

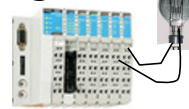


Allumer la lampe depuis l'API avec le réseau MODBUS

IHM @ 5



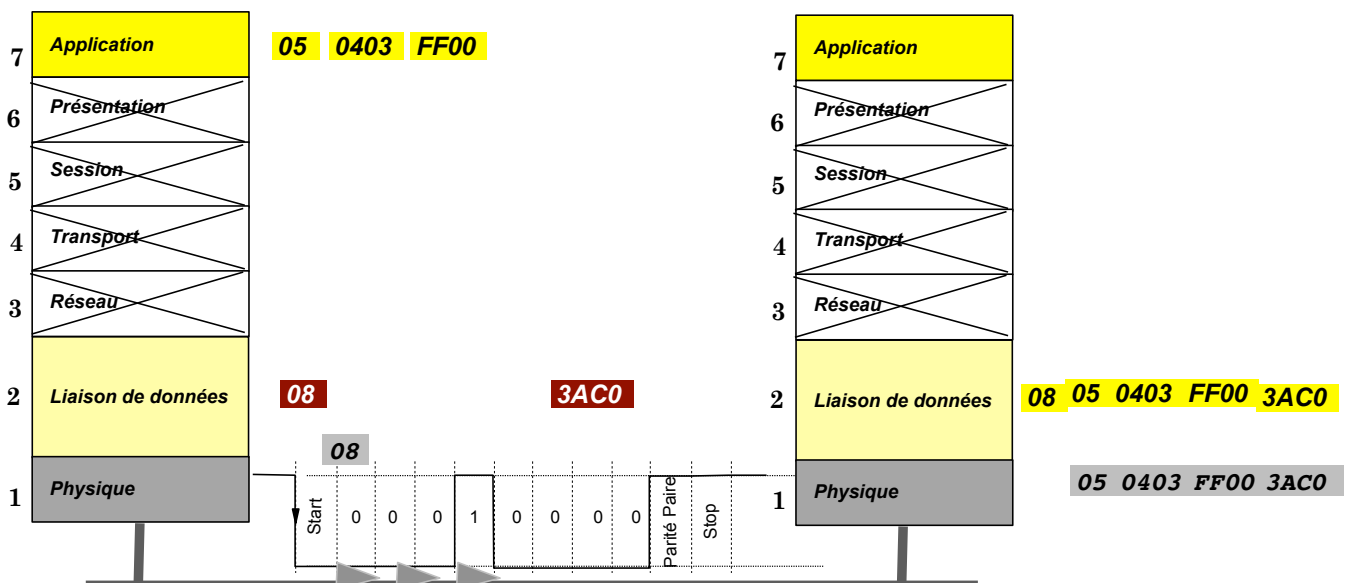
E/S @ 8



la lampe est raccordée à une sortie TOR (Bit N°3 mot 0x40)

Modbus - RS 485-2

Mise à 1 du Bit 3 du mot mémoire 0x40



Type :

Topologie :

Transmission : Les spécifications modbus ne stipulent pas de médium, ni de mode de transmission particulier, mais de façon générale, on observe en pratique les caractéristiques suivantes :

- Transmission asynchrone Half-Duplex
- Bande de base de 50 à 19200 Bits/Seconde
- RS 232- V24, RS422 ou RS485

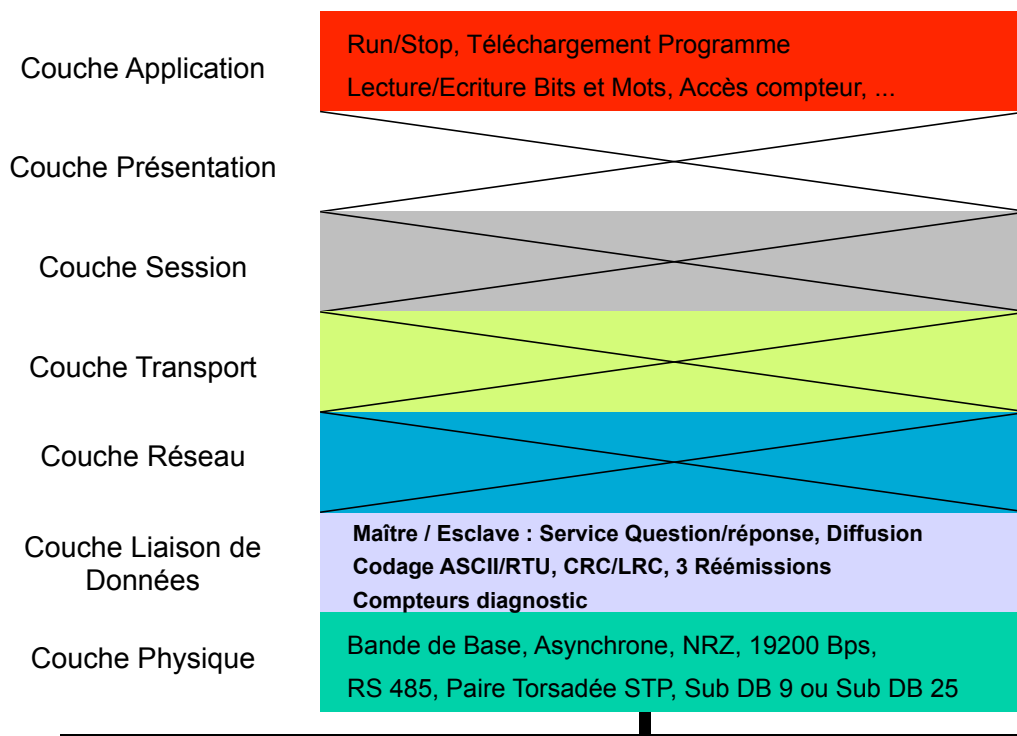
Protocole d'accès :

- Question/Réponse entre le maître et un esclave
- Diffusion du maître vers tous les esclaves

Fonctions :

- Ecriture/Lecture de Mots de 16 bits
- Ecriture/Lecture de Bits
- Lecture Rapide d'un Octet Particulier de l'esclave
- * Téléchargement de programme
- * Run/Stop Automate

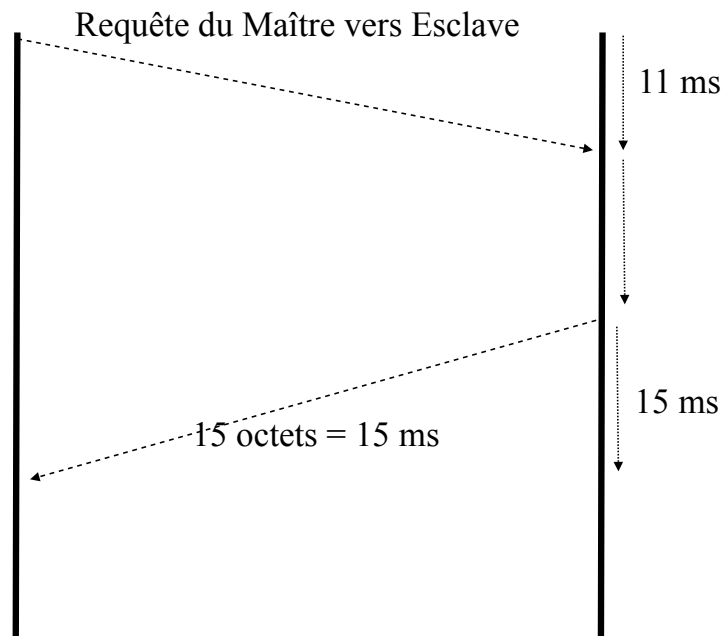
Surveillance : Chaque esclave gère de façon interne des compteurs de diagnostic accessible par le maître, et permettant de surveiller l'état de fonctionnement des coupleurs des esclaves.



9600 Bps

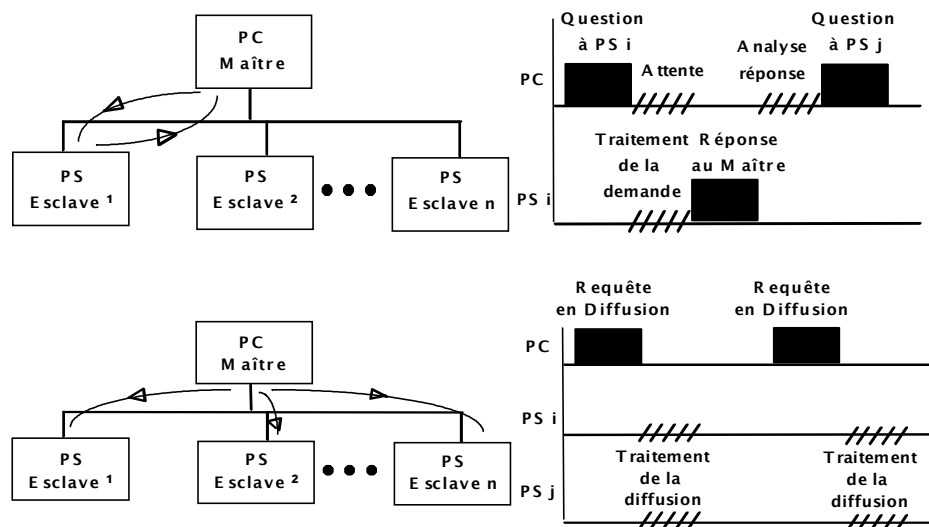
1 octet est transmis sur 11 bits

1 Octet $\approx$ 1 ms



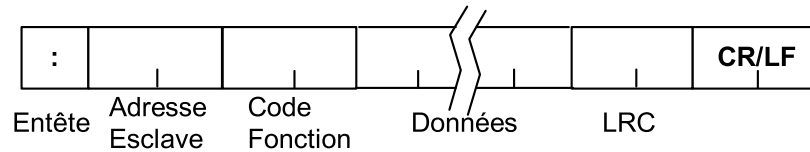
Type **Maître/esclave**, tel qu'il n'existe pas en permanence d'activité sur la ligne.

Seul le Poste Maître a la possibilité de lancer un échange. Un Esclave est toujours passif, il ne fait qu'attendre les requêtes en provenance du Poste Maître.



Toute communication horizontale, d'esclave vers esclave, ne peut exister que si le logiciel application du poste maître a été conçu pour recevoir des données et les renvoyer d'un esclave à l'autre.

Une **trame ASCII** d'une longueur maximale de **525 octets**, est composée de six champs distincts



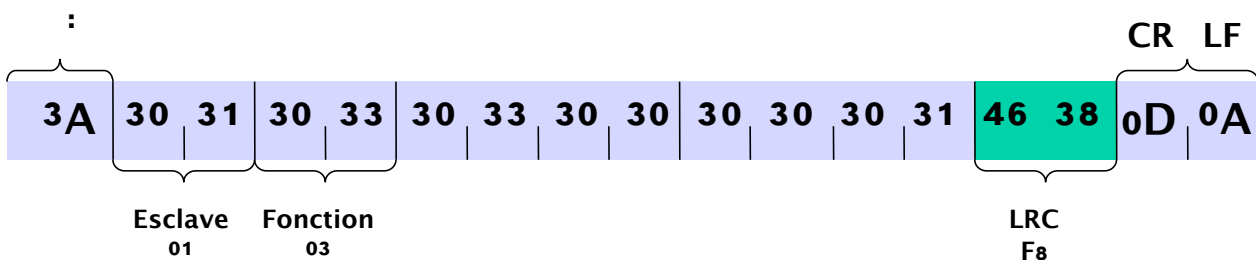
Entête	:Caractère ":" (3Ah) indiquant le début de la trame
Adresse	:Adresse sur deux octets en hexadécimal de l'esclave destinataire
Code Fonction	:Code représentant la fonction demandée à l'esclave
Données	:Paramètres et valeurs associés à la fonction demandée
LRC	:Clef de contrôle de la trame (Longitudinal Redundancy Check sur 8 bits)
Fin	:Caractères "CR" (0Dh) et "LF" (0Ah) délimitant la fin de la trame

Chaque octet est codé sur deux caractères ASCII, chacun contenant quatre bits d'information :

- le premier caractère émis contient le quartet de poids fort,
- le second caractère émis contient le quartet de poids faible

Ainsi, pour coder l'esclave d'adresse 01H, le champ adresse de la trame ASCII comprendra les deux octets 30H (caractère '0') et 31H (caractère '1').

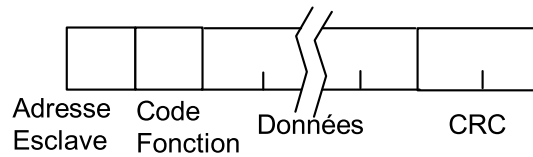
Trame ASCII



Le LRC est calculé sur les valeurs hexadécimal avant conversion en ASCII, en excluant l'entête et les délimiteurs de fin : Somme Modulo 256 de tous les octets de la trame sauf les délimiteurs, puis complémentée à 2.

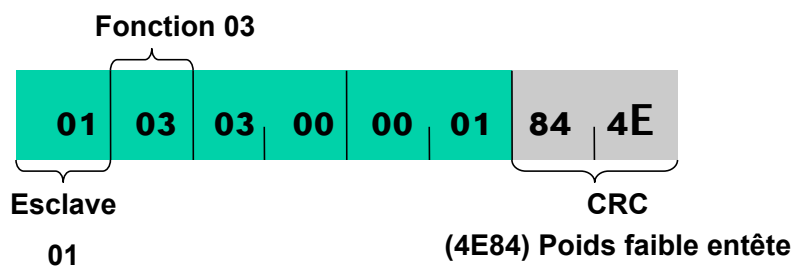
$$\text{LRC} = (01 + 03 + 03 + 00 + 00 + 01) + 1 = \text{F8h} = (46,38)\text{ASCII}$$

Une **trame RTU** d'une longueur maximale de **261 octets**, est composée de quatre champs distincts.



Adresse : Adresse sur un octet en hexadécimal de l'esclave destinataire
Code Fonction : Code sur un octet représentant la fonction demandée à l'esclave
Données : Paramètres et valeurs sur n octets associés à la fonction demandée
CRC16 : Clef de contrôle de la trame sur deux octets (Cyclic Redundancy Check 16 bits)

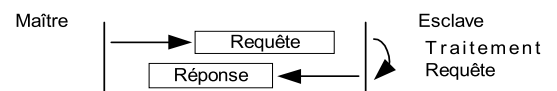
Chaque octet d'information est codé sur un caractère (valeur 00H à FFH).



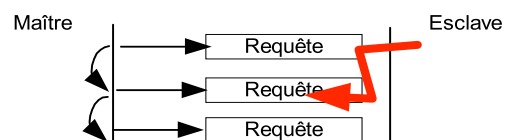
Une trame circulant sur le médium peut être parasitée par différentes sources ou être interrompue par une coupure de ligne.

Dans ces cas, le protocole MODBUS définit les modes de recouvrement d'erreurs suivants :

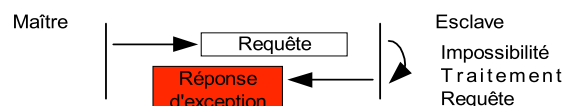
Echange Normal : L'esclave reçoit une demande correcte du maître. Après avoir réaliser la fonction demandée, l'esclave répond par une trame de réponse.



Trame erronée : dû à des parasitages ou coupures de ligne ou défaut coupleur, ... L'esclave ou le maître ne traite pas la trame



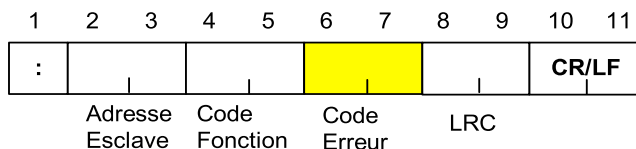
Pas de réponse Esclave : Le maître ne reçoit pas de réponse d'un esclave interrogé : Le maître attend une durée paramétrable (**Time-Out**), puis ré-émet la question maxi. trois fois.



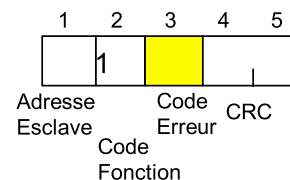
Requête impossible : dû à un fonction demandée non supportée par l'esclave, ... L'esclave répond par une **trame d'exception** signalant le type d'erreur.

Trames de réponse d'exception MODBUS

ASCII



RTU



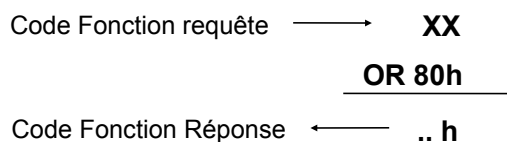
Code erreur

Code erreur	Signification
1	Code Fonction erroné
2	Adresse Incorrecte
3	Données Incorrectes
4	Automate Non Prêt

Signification

Fonction non supportée par l'esclave
Adresse non autorisée sur l'esclave
Données non autorisées à l'adresse indiquée
Impossibilité d'échange coupleur avec CPU de l'esclave

L'esclave retourne le **code fonction** émis par le maître en positionnant le bit de poids fort à 1, pour signifier une réponse d'exception.



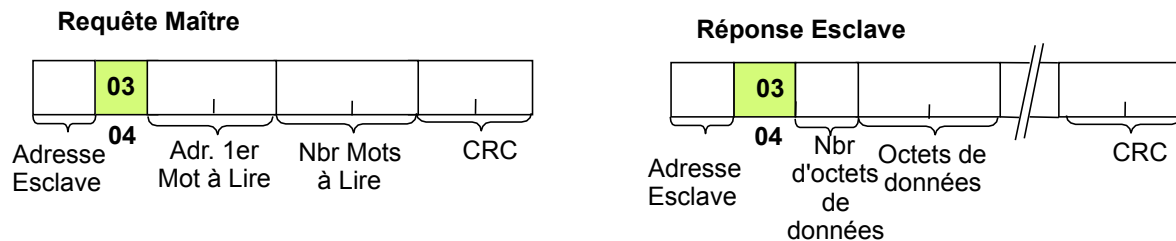
Fonctions du Protocole MODBUS

Fonction	Sous Fonction	Données	Fonction demandée
00	00 00	00 00	STOP automate
	00 01	00 00	RUN automate
	00 02	00 00	RUN automate avec initialisation
	00 03	00 XX	Télélecture de programme : XX est le N° de séquence
	00 04	YY XX	Téléchargement de programme dans l'esclave
01			Lecture de N Bits d'Entrée
02			Lecture de N Bits de Sortie
03			Lecture de N Mots d'Entrée
04			Lecture de N Mots de Sortie
05			Ecriture de 1 Bit
06			Ecriture de 1 Mot
07			Lecture Rapide d'un Octet
08	00		Echo : Vérification de la ligne de transmission
	03		Modif du Délimiteur de fin de trame : 0x0A par défaut
	0A		RAZ des compteurs de diagnostic
	0B		Lect du compt 1 Nb trames sans erreur CRC
	0C		Lect du compt 2 Nb trames avec erreur CRC
	0D		Lect du compt 3 Nb trames avec réponse d'exception
	0E		Lect du compt 4 Nb trames adressées à l'esclave
	0F		Lect du compt 5 Nb trames de non réponse
(diffusion)	12		Lect du compt 7 Nb de caractères reçus et non traités
0B			Lecture du compteur d'échange 8
0F			Ecriture de N Bits de sortie
10			Ecriture de N Mots de sortie

Demande de lecture de n mots

Le code fonction 03 correspond à une demande de lecture de N Mots, qui nécessite de spécifier le nombre de mots à lire codé sur 2 octets.

La réponse fournie par l'esclave, comprend quant à elle, un champ stipulant le nombre d'octets de données dans la trame lequel est codé sur un seul octet, puis les mots lus.



Le nombre de mots à lire en une seule requête est limité selon l'esclave (de 5 à 32 mots)



Anachronisme Modbus :

Le champ « Nombre d'octets de données » de la réponse est plus petit que le champ « Nombre de mots à lire » de la question

Un maître API connecté à un esclave d'adresse 10h

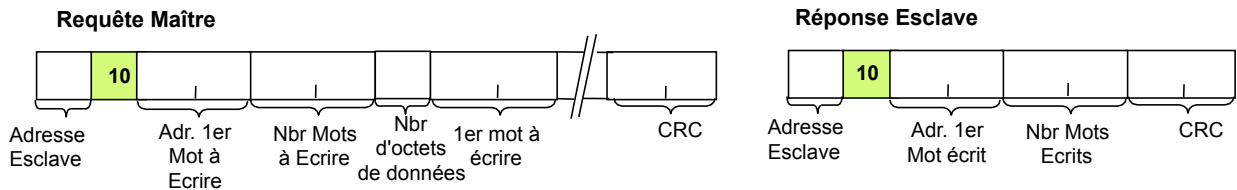
On veut lire les mots de 0x100 à 0x105 et 0x1F0 à 0x200

- Donner le diagramme de séquence des échanges réseau
- Donner le contenu des trames échangées

Demande d'écriture de n mots

Le code fonction 10 correspond à une demande d'écriture de N Mots, qui nécessite de spécifier le nombre de mots à écrire codé sur 2 octets, ainsi que le nombre d'octets de données (nombre de mots * 2), puis les mots à écrire sont rangés à la suite dans la trame poids fort en tête.

La réponse fournie par l'esclave, reprend l'adresse du 1^{er} mots écrit et le nombre de mots écrits.



Le nombre de mots à écrire en une seule requête est limité selon l'esclave (de 5 à 32 mots)

Réponse d'Exception

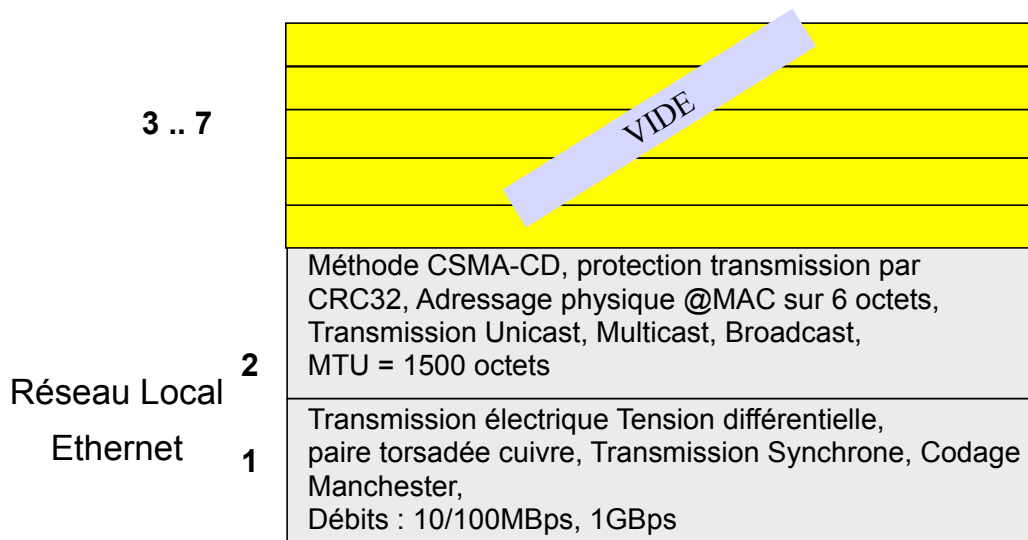
On remarquera le code fonction renvoyé par l'esclave est celui émis par le maître auquel le bit de poids fort est forcé à 1 : 0x00 or 0x80 = 0x80



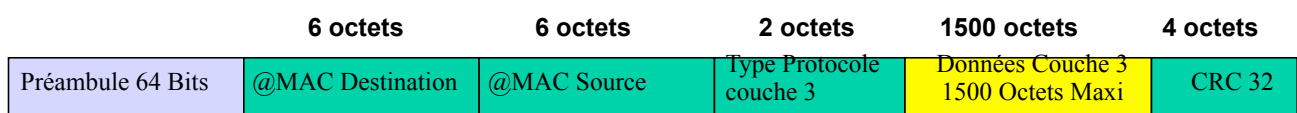
Code erreur		Signification
1	Code Fonction erroné	Fonction non supportée par l'esclave
2	Adresse Incorrecte	Adresse non autorisée sur l'esclave
3	Données Incorrectes	Données non autorisées à l'adresse indiquée
4	Automate Non Prêt	Impossibilité d'échange coupleur avec CPU l'esclave

Le Réseau Ethernet

Ethernet et le Modèle OSI



Format Trame Ethernet



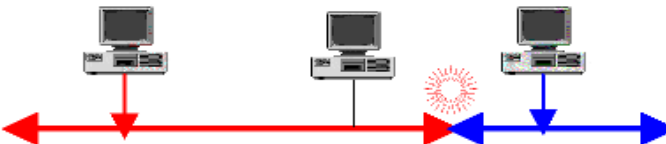
Standard **IEEE 802.3** : Carrier Sense and Multiple Access with Collision Detection**CARRIER SENSE**

Avant d'émettre, toute station "écoute" la voie pour savoir si elle est libre :

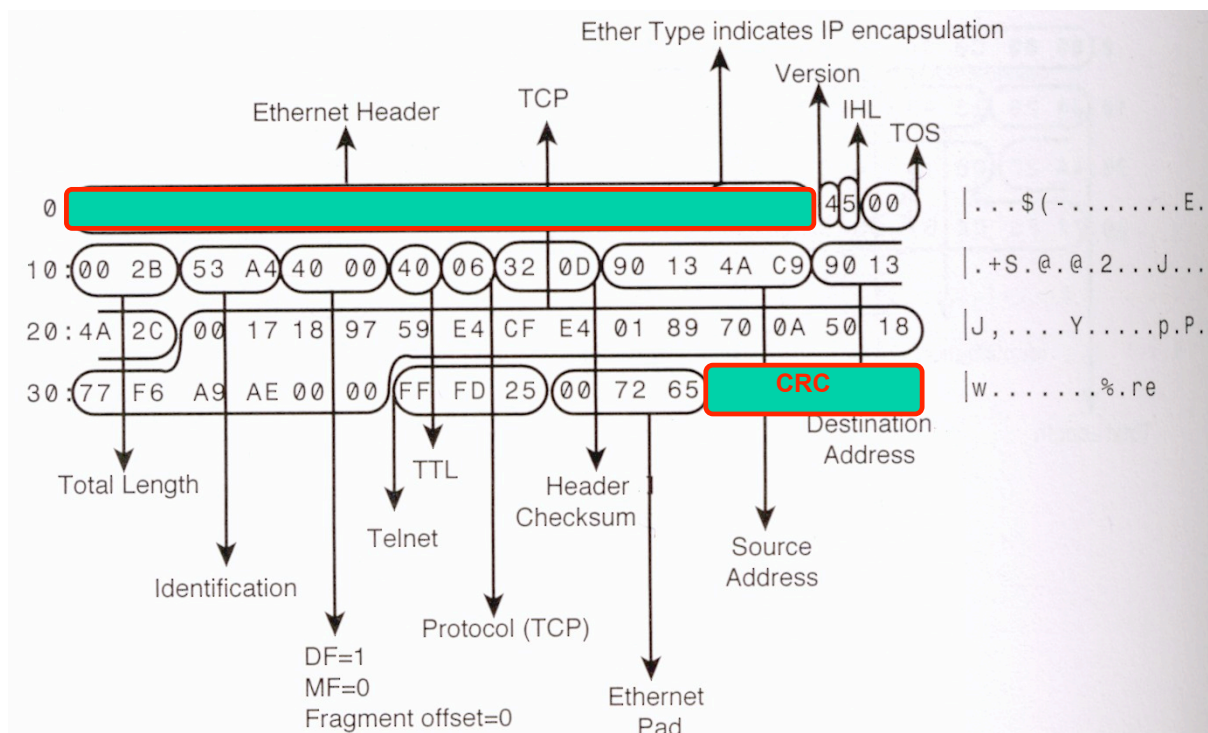
- 1) Si LIBRE, elle émet sa trame
- 2) Si OCCUPÉE, elle attend un temps tiré au hasard

MULTIPLE ACCESS

Topologie apparente est un bus
Chaque station a les mêmes droits,

COLLISION DETECTION**CSMA/CD**

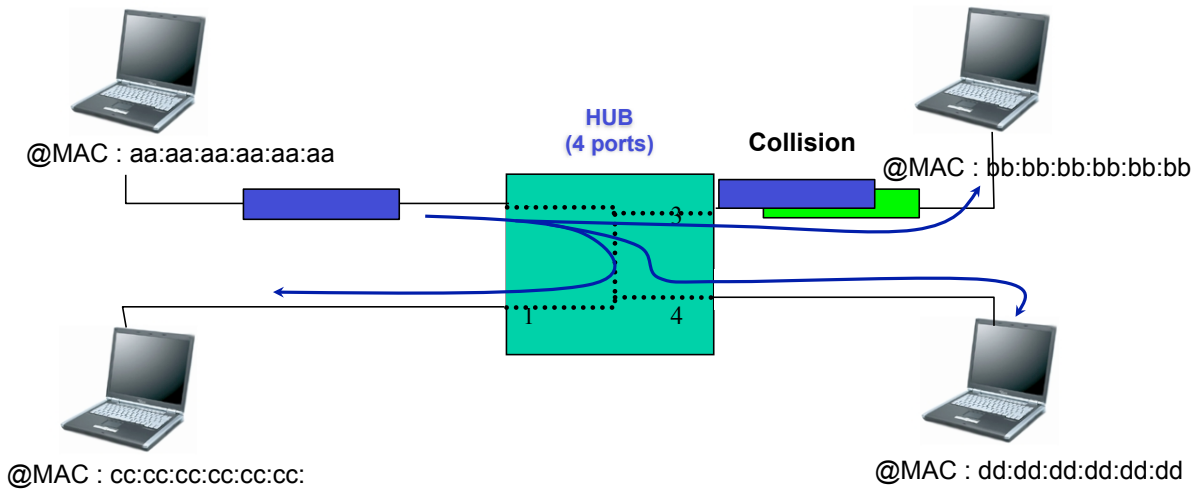
Détail d'une trame Ethernet



Ethernet Partagé en Bus

Hub ou Concentrateur :

Equipement d'interconnexion de stations, agit en **diffusion de trames** sur tous ses ports (répéteur non intelligent : inondation des ports)



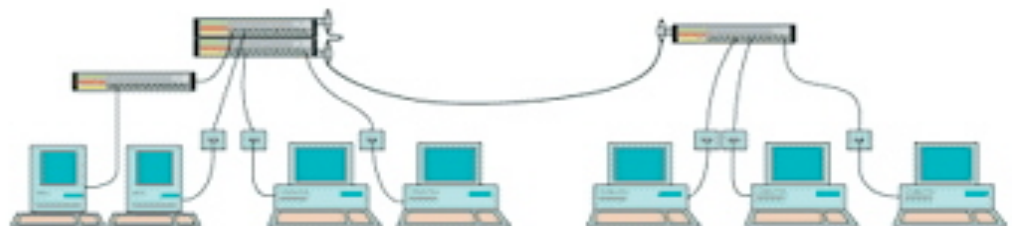
Hub Ethernet 8 voies



ETHERNET 10/100 Base T

ETHERNET 10/100 Base T sur Paires Torsadées

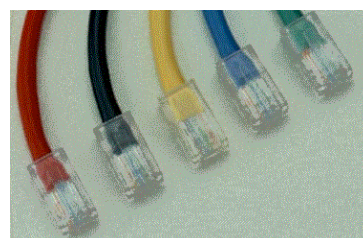
RESEAU 10baseT



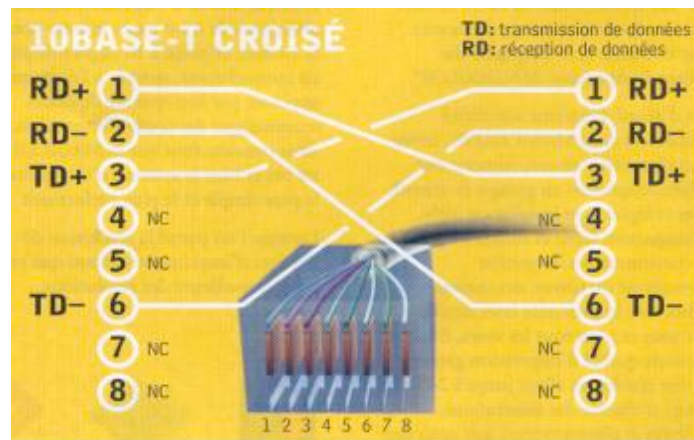
Caractéristiques :

- Segment 100 m maxi STP, 40 m UTP
- Une seule Station par segment
- Segments dérivés depuis un Hub (4, 8, 16, 24 Voies)
- Connexion par connecteurs RJ45
- Câble UTP AWG 22, 24 ou 26

Connecteur RJ 45



Câble Croisé entre 2 stations

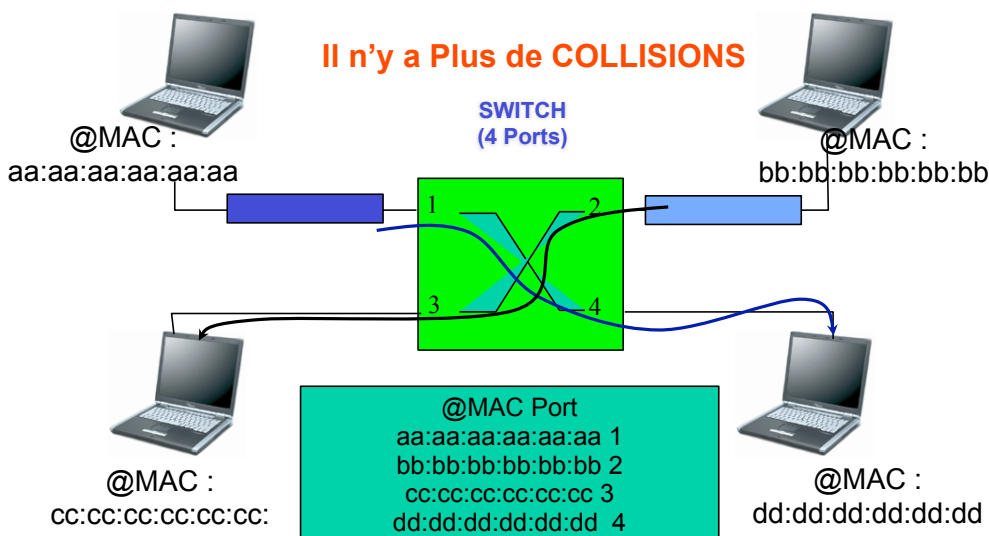


<http://www.youtube.com/watch?v=0S6cjJS5y1I>

Ethernet commuté

Switch ou Commutateur :

Équipement d'interconnexion de stations, agit en **roulage de trames** sur chaque port (équipé d'un processeur RISC qui gère le roulage des trames entre les ports)

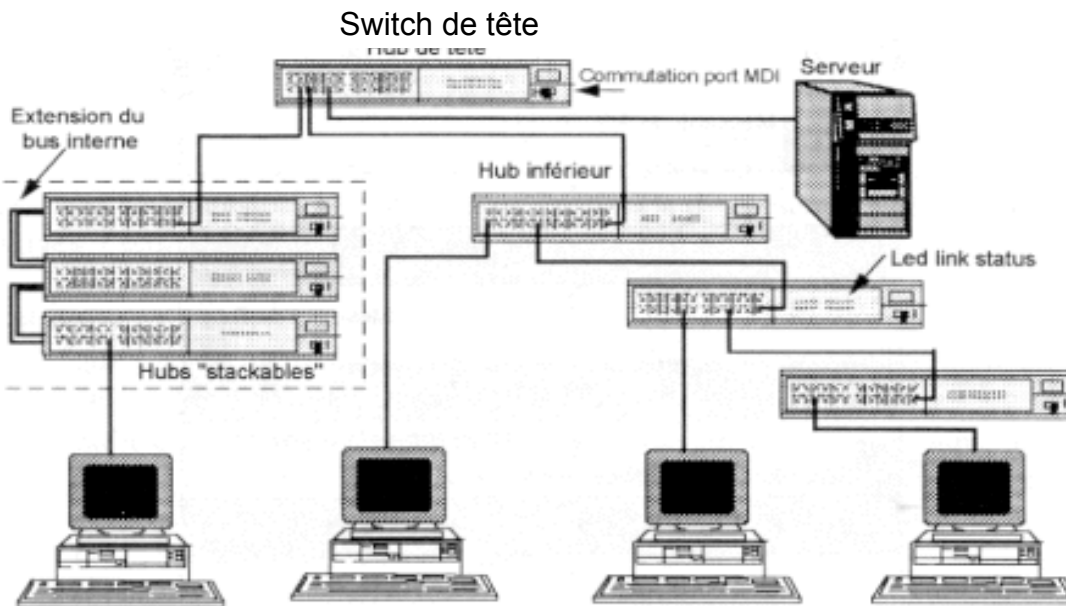


2 méthodes de gestion de flux de trames:

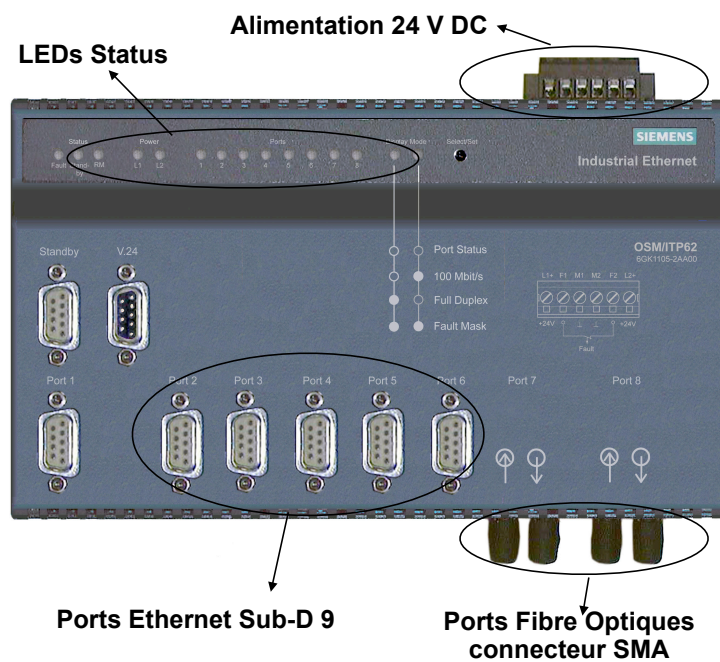
- **Cut Through** : flux tiré par l'adresse dest de la trame entrante, pas de contrôle d'erreur
- **Store and Forward** : trame bufferisée, analysée puis routée vers le port dest

Auto-Apprentissage des adresses MAC connectées aux différents ports

Architecture Capillaire Ethernet

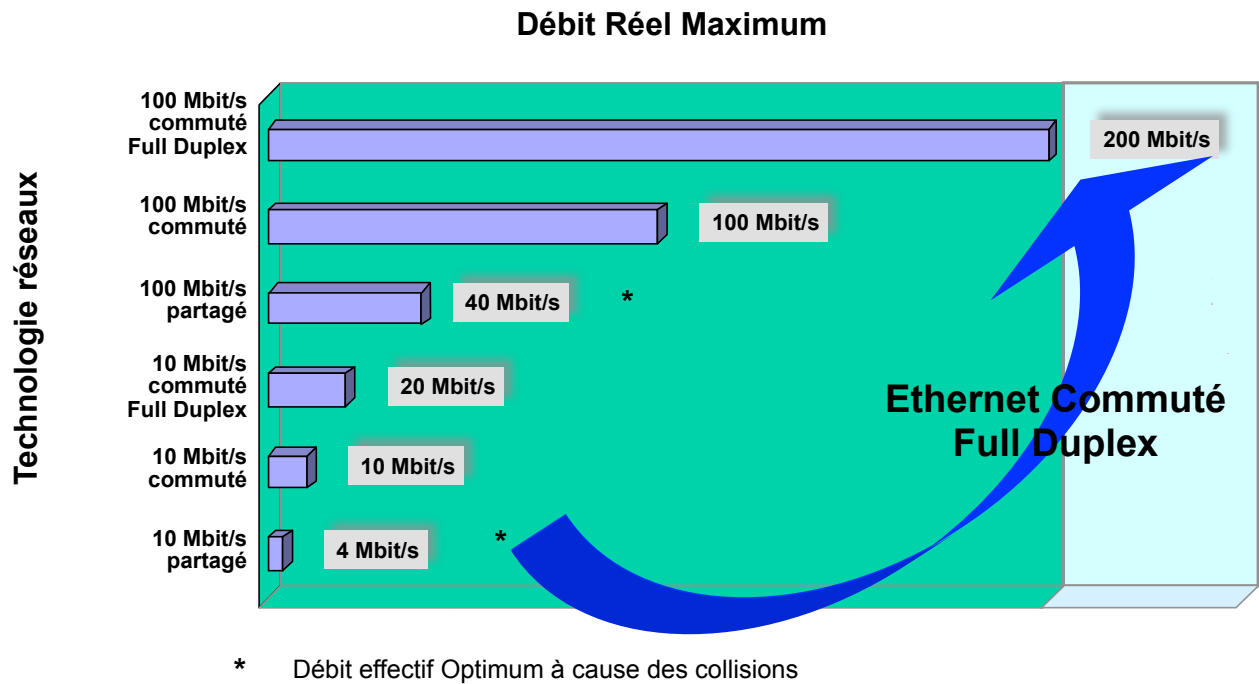


Switch Industrial Ethernet 100 Mbit/s



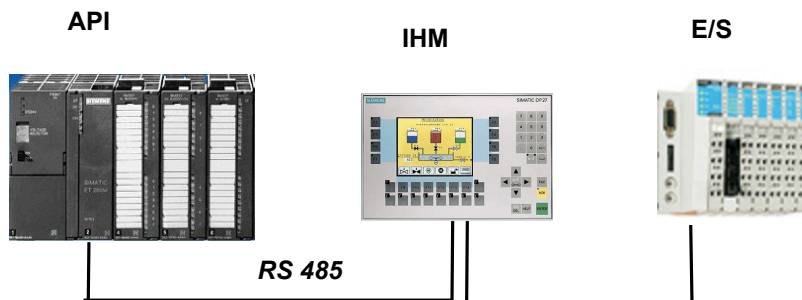
Caractéristiques

- Industrial Twisted Pair
- OSM : Optical Switch Module
6 ports ITP/TP
2 ports FO
- ESM : Electrical Switching Module
8 ports ITP/TP
- Gestion de Redondance
- Manageable SNMP
Simple Network Management Protocole



Impact de Ethernet et Internet dans les automatismes

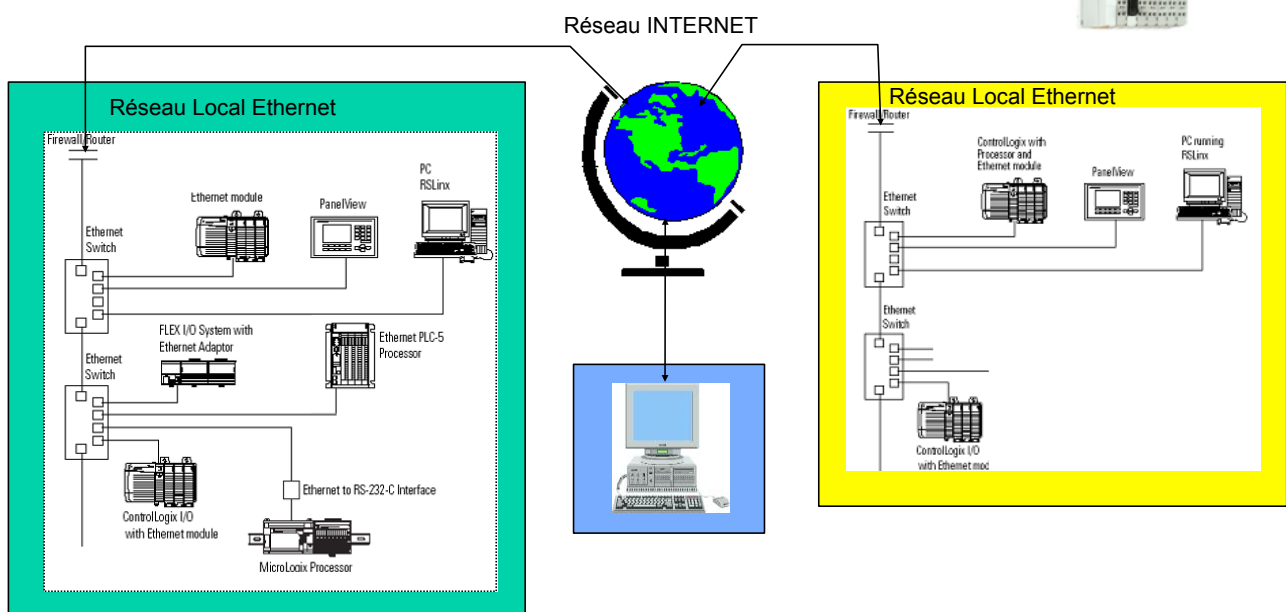
Depuis un Un réseau d'Automatisme “Isolé”



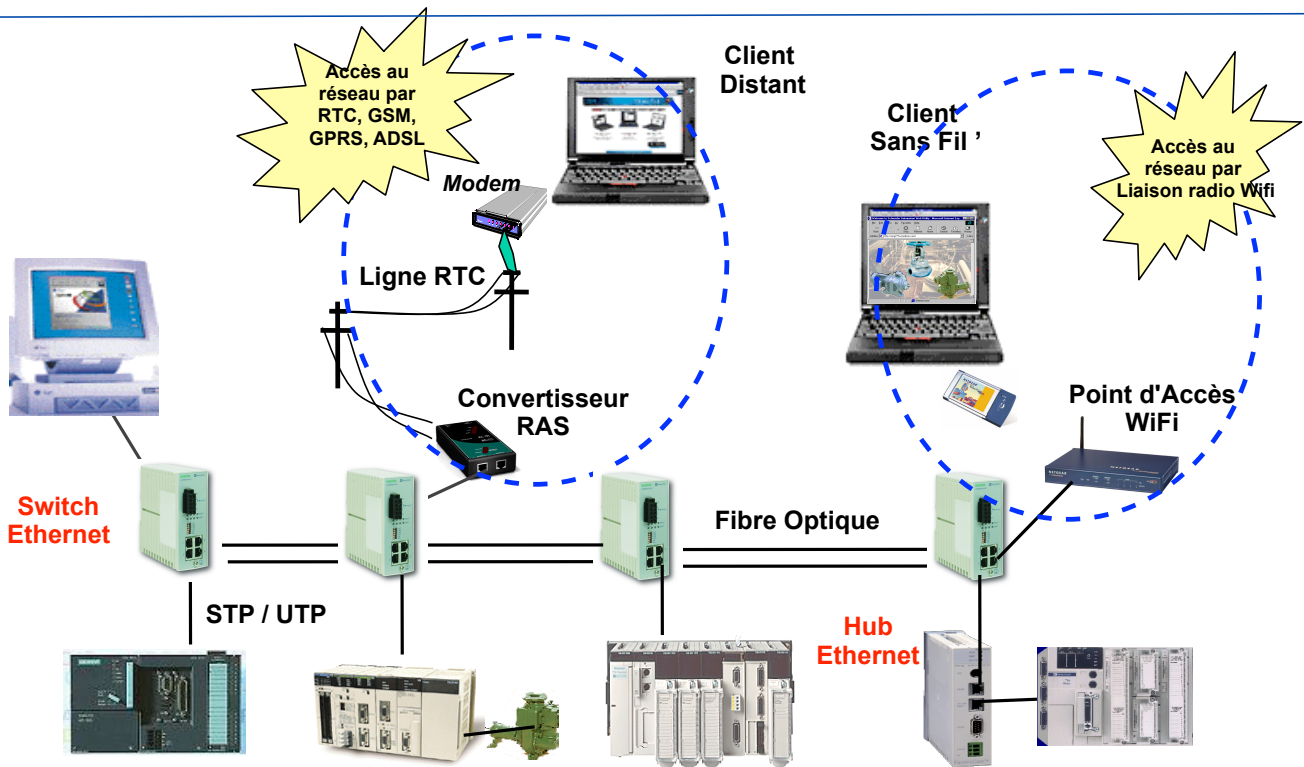
- Lire / Ecrire des informations sur BITS, MOTS vers des cibles industrielles PROCHES
- RESEAU LOCAL INDUSTRIEL , Câblage en guirlande
- Architecture traditionnelle (ancienne ?)

Vers des Automatismes sur INTERNET

Disposer des équipements industriels (E/S, API,) sur Ethernet dans l'entreprise / atelier
Accéder aux équipements industriels à distance par Internet



Architecture Réseau Industriel Ethernet



QuickTime™ et un
décompresseur
sont requis pour visionner cette image.

Module Wago Ethernet

Module E/S WAGO sur Modbus TCP



Wago 750

WAGO-I/O-System - Microsoft Internet Explorer

WAGO-Ethernet TCP/IP FBC

Coupler details

Order number 750-342
Firmware revision 02.00.00(06)

Network details

Hardware address 0030DE000578
IP address 193.49.35.63
Gateway address 193.49.35.254
Subnet mask 255.255.255.0
Number of sent packets 828
Number of received packets 1107

Coupler status

Error code: 0
Error argument: 0
Error description: FBC running OK

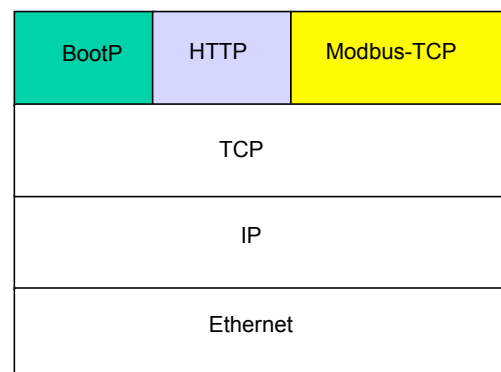
[Terminal status](#)

Terminal status - Microsoft Internet Explorer

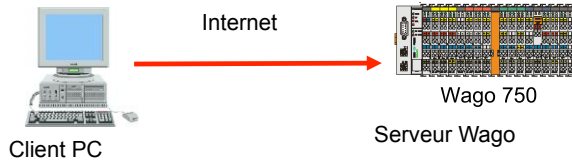
Terminals info	Process image
1.Digital input	Digital outputs 1 0
2.Digital output	Digital inputs 0 0 1 0
3.Complex 468	Analog outputs 0x0000
4.Complex 550	Analog inputs 0x10E9
	0x0000
	0x3613
	0x3FCB

Terminé Internet

Stack TCP-IP du module WAGO 750 -342



Adresse E/S Wago



Gestion connexion TCP-IP encapsulant MODBUS-TCP

Client Local		Etat de la Connexion	Serveur Distant	
@ IP Client	Port TCP		@ IP Serveur	Port TCP
192.168.2.106	3238	Ouverte	193.49.35.63	502
lussac			Wago1Geii.iutnb.uhp-nancy.fr	

APDU Modbus TCP Emission

000000000000601060202ABCD

APDU Modbus TCP Réception

00 00 00 00 00 06 01 06 02 02 AB CD

Envoi APDU

E. BAJIC 2003

Internet

☒ Ces réseaux sont administrés, exploités et financés dans tous pays par des d'organisations privées et publiques différentes.

☒ La coordination de l'ensemble est assurée par l' **IAB** (Internet Architecture Board), groupe de chercheurs et industriels qui coordonne et spécifie des règles de fonctionnement d'Internet.

☒ Documents de standardisation Internet sont appelés Request For Comments (RFC) :

RFC xxxx (Request For Comment N° xxxx) (<http://ds.internic.net>)

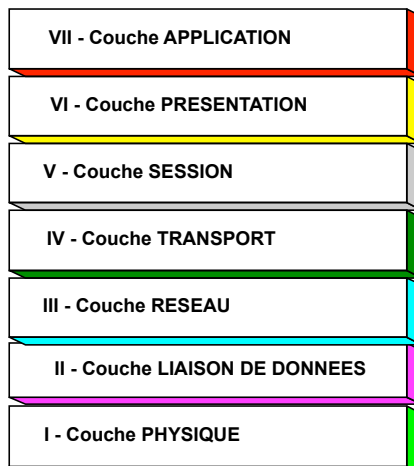
Le protocole TCP a été défini en 1981 dans la RFC 792.

Site Web de référence sur TCP - IP <http://www.frameip.com/accueil/>

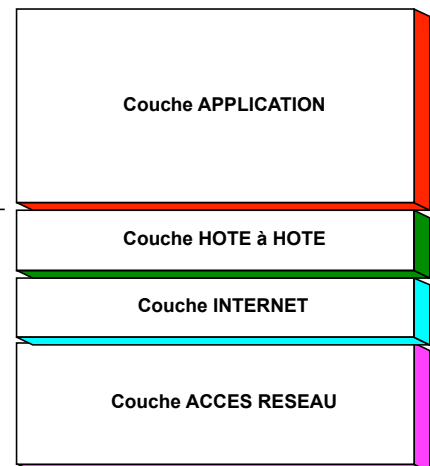
Le modèle DOD (**Department Of Defense of USA**), simplification du modèle OSI.

⇒ adapté aux réseaux basés sur les protocoles TCP/ IP.

Modèle OSI

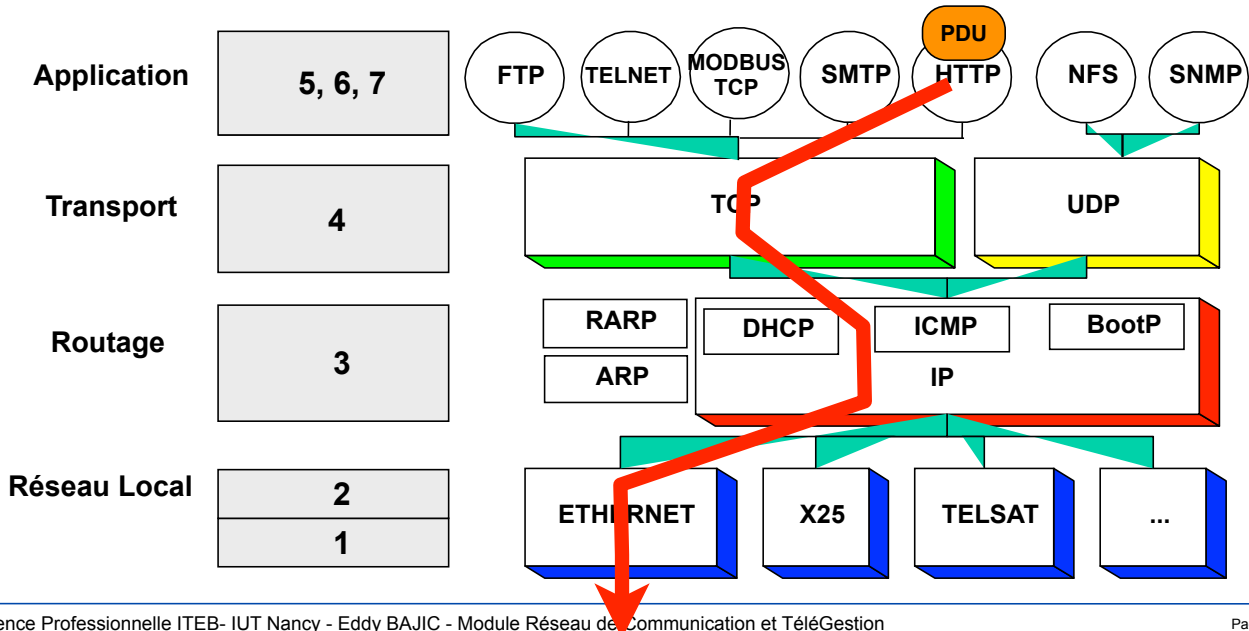


Modèle DOD / TCP-IP



Le terme **TCP-IP** englobe un ensemble de protocoles réseaux assurant les mécanismes d'échanges d'information sur Internet (Le terme n'est pas réservé aux seuls protocoles TCP et IP)

⇒



HTTP (Hyper Text Transfer Protocol) : Envoi de pages hypertexte à un ordinateur équipé d'un navigateur (browser) pouvant lire des documents graphiques, audio et vidéo.
Les pages web sont codées dans un langage HTML (Hyper text Markup Language).

SMTP (Simple Mail Transfer Protocol) : Envoi de messages (E-Mail) depuis un client SMTP vers un serveur SMTP. Le compte destinataire du message sur le serveur est identifié par son adresse électronique.

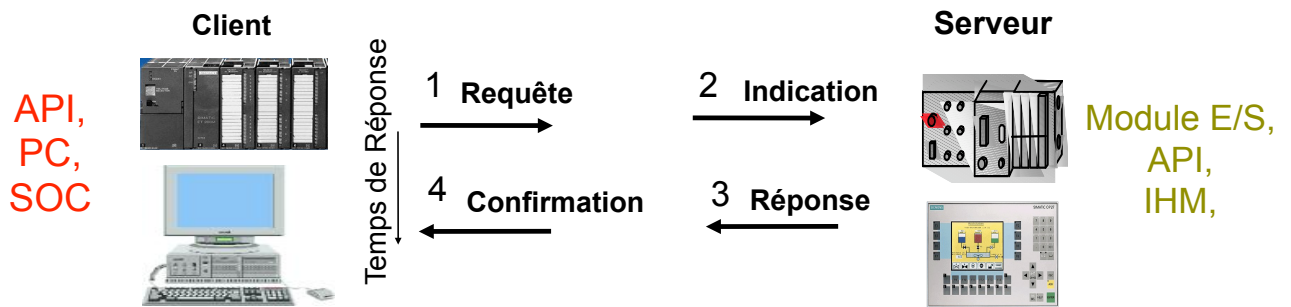
FTP (File Transfer Protocol) : Transfert de fichiers entre deux machines. L'utilisateur (client FTP) se connecte à un serveur FTP et peut visualiser et transférer les fichiers et répertoires de l'hôte.

SNMP (Simple Network Management Protocol) Gestion à distance des équipements d'interconnexion réseau tels que routeur, hub, switch
Un programme (agent SNMP) doit être installé sur ces périphériques.

NFS (Network File System) : Equivalent à FTP pour des systèmes Unix.

TELNET : Connexion à distance à une station. Permet de travailler comme en connexion locale avec l'hôte (clavier/écran déportée par le réseau)

L'architecture Internet est basée sur un modèle de communication Client-Serveur

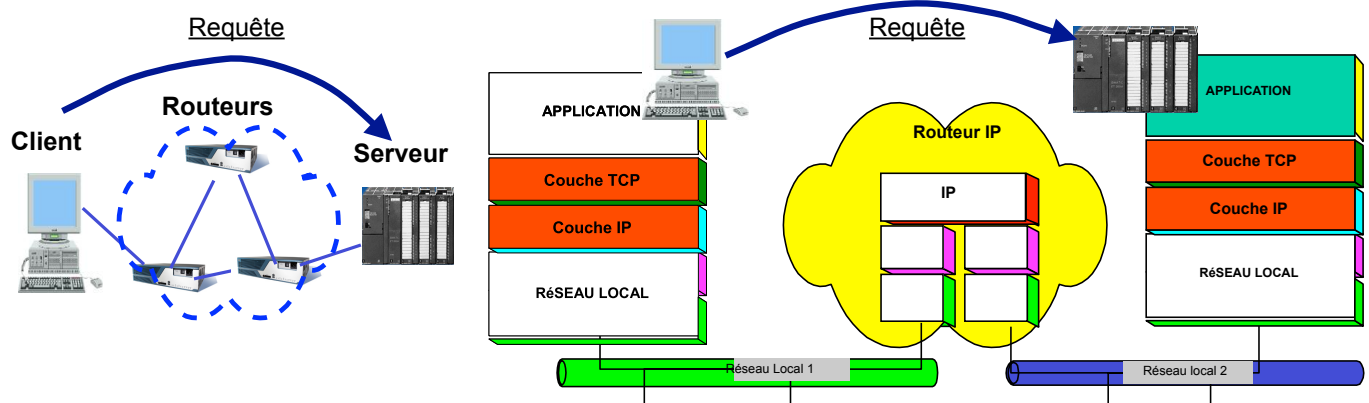


Client :

Serveur :

- Est à l'écoute des clients qui le sollicitent (écoute sur N° de port TCP/UDP donné)
- Ne répond qu'aux requêtes des clients

Temps de Réponse :



4 Mécanismes de base nécessaires aux réseaux TCP-IP

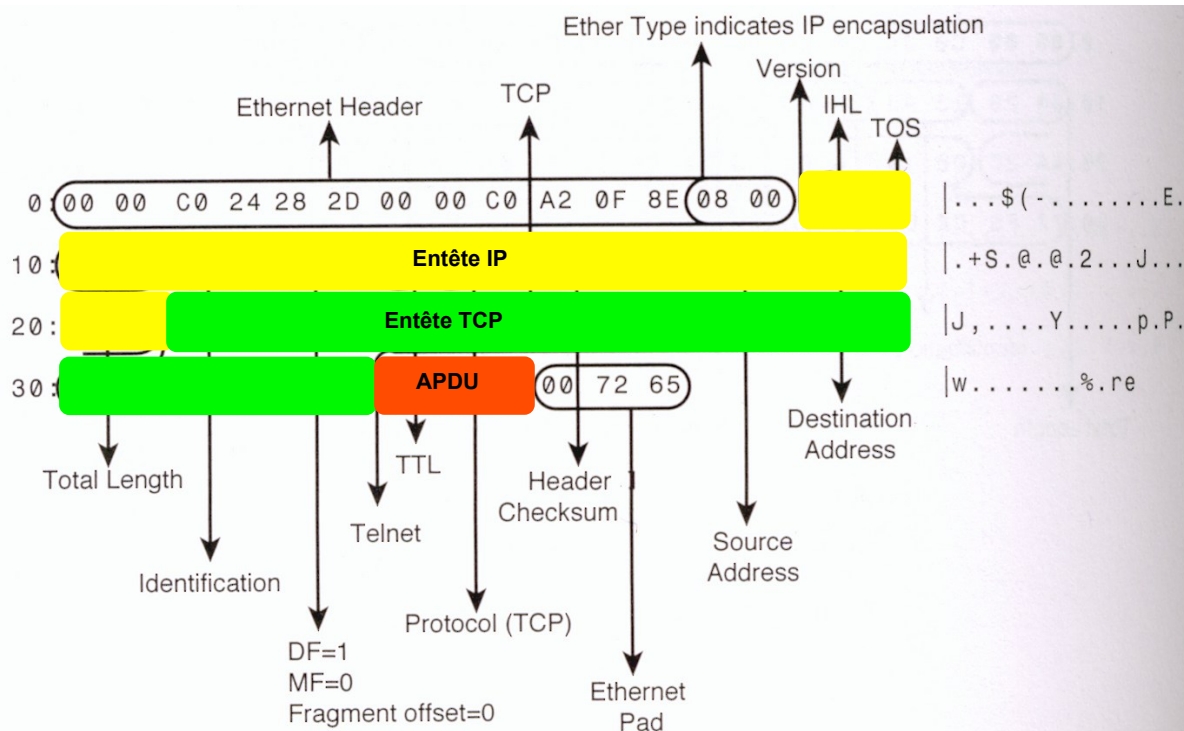
⇒

⇒

⇒ **CONTRÔLE DE FLUX** des paquets pour garantir leur acheminement au destinataire (Acquittement / Réémission)

⇒ **FRAGMENTATION / ASSEMBLAGE** des paquets dans les réseaux traversés pour correspondre aux tailles maximales des trames autorisées

Encapsulation d'une Trame Ethernet



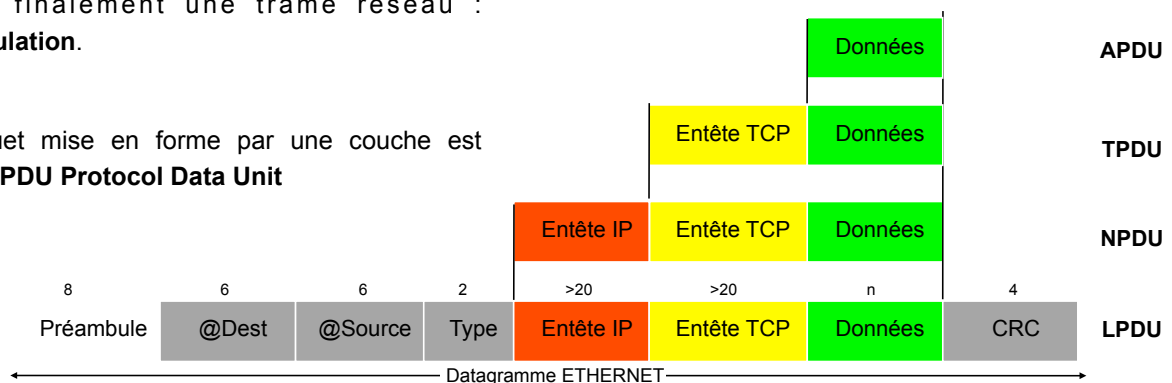
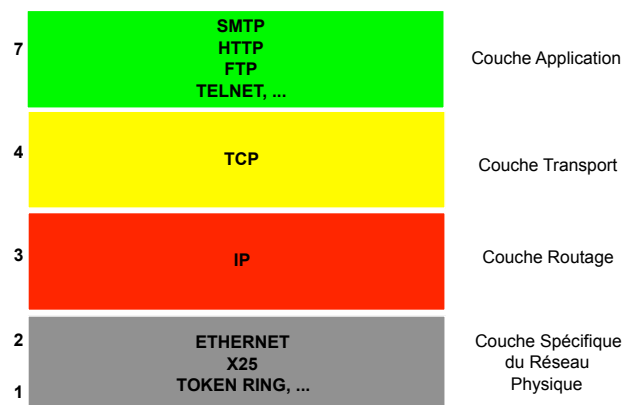
Mécanisme d'encapsulation

L'empilement des protocoles selon les couches du modèle OSI (ou DOD) permet d'installer l'ensemble des services nécessaires à l'utilisateur d'un réseau.

☒ Cet empilement est appelé la **pile de protocoles OSI** ou le **Stack OSI**.

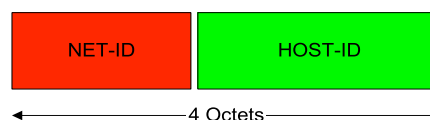
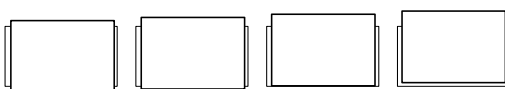
Chaque couche de la pile fournit des données qui sont encapsulées par la couche inférieure pour former finalement une trame réseau : **Encapsulation**.

Le paquet mis en forme par une couche est appelé : **PDU Protocol Data Unit**

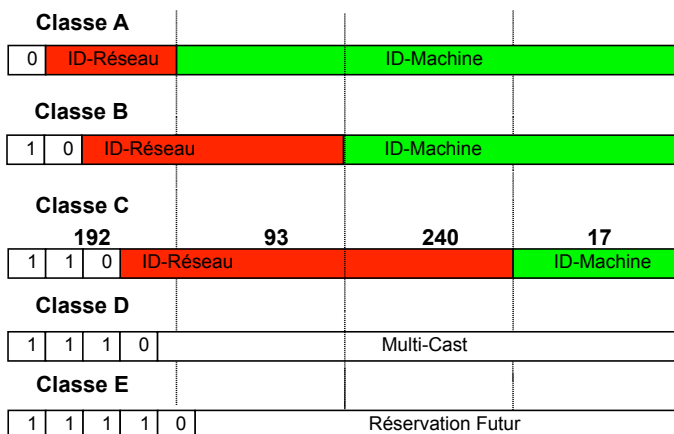


Adressage IP

Adressage IP et Classes de Réseau Internet



3 classes de réseaux Internet basés sur la taille maximale du réseau (nb maxi de stations adressables)



Classe	Plage d'Adressage	Nbre de Réseaux	Nbre de Stations
A	0.xxx.xxx.xxx à 127.xxx.xxx.xxx	127	16 777 214
B	128.0.xxx.xxx à 191.255.xxx.xxx	16 383	65 534
C	192.0.0.xxx à 223.255.255.xxx	2 097 151	254

Adressage IPv4 (32 bits)
permet de définir **2,1 Millions de réseaux pour un total de 3,72 Milliards d'hôtes.**

Adressage IPv6 (128 bits)
permet d'adresser au minimum **1 Milliard de réseaux**

Masque de Sous - Réseau IP

Une station peut déterminer à quel réseau IP elle appartient ainsi que son numéro de station grâce à son masque de sous – réseau

Station A : IP : **192 . 44 . 01 . 48** Masque de sous réseau : **255 . 255 . 255 . 0**

1) Déterminer le réseau IP auquel appartient la Station A : (Net ID)

@IP	192 . 044 . 001 . 48	
MASQUE	<u>255 . 255 . 255 . 000</u>	ET LOGIQUE

2) Déterminer le numéro de la Station A sur son réseau : (Host ID)

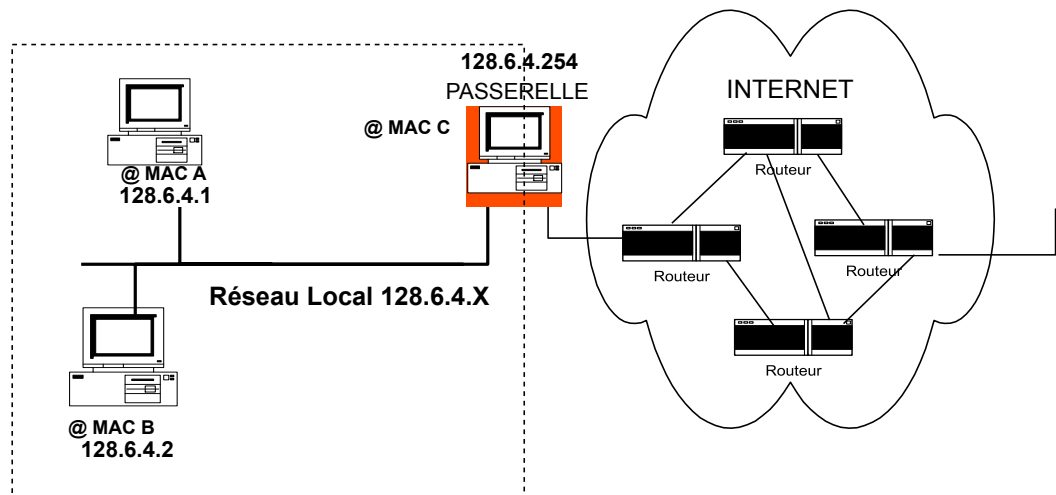
@IP	192 . 044 . 001 . 48	
NOT MASQUE	<u>000 . 000 . 000 . 255</u>	ET LOGIQUE



Paramètres d'une Machine Connectée à Internet

Une machine (PC, API) connectée à INTERNET est d'abord connectée à un réseau LOCAL ETHERNET :

4 paramètres sont nécessaires pour communiquer sur Internet



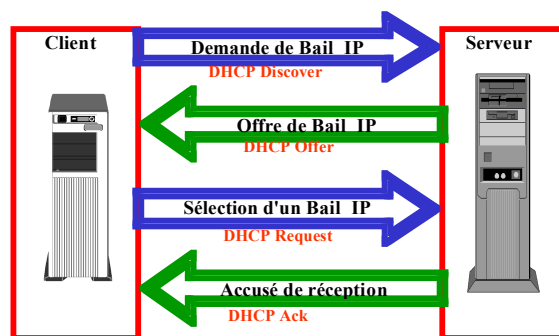
Protocoles DHCP / BootP

Serveur DHCP (Dynamic Host Configuration Protocol)

C'est un logiciel installé sur une machine qui permet d'attribuer des adresses IP dynamiques à chaque poste de travail, et ainsi éviter de configurer manuellement les adresses IP.

DHCP est une extension du protocole BOOTP qui permet à un client sans disque dur (terminal X, imprimante, etc.) de démarrer et de configurer automatiquement TCP/IP.

L'objectif du protocole DHCP est de permettre à un client d'obtenir une adresse IP (et d'autres paramètres éventuellement) auprès d'un serveur DHCP.



En Résumé

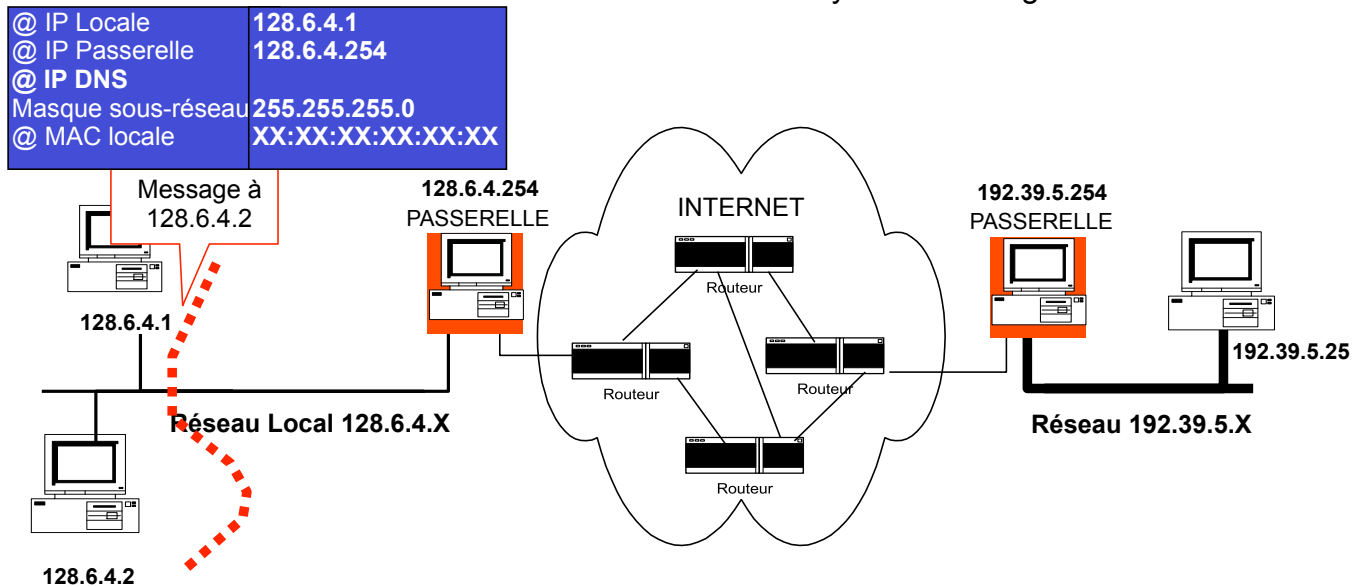
En-têtes de trames.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x6719436e
2	0.001182	192.168.0.253	192.168.0.9	ICMP	Echo (ping) request
3	0.342454	192.168.0.253	192.168.0.9	DHCP	DHCP Offer - Transaction ID 0x6719436e
4	0.344405	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x6719436e
5	0.348264	192.168.0.253	192.168.0.9	DHCP	DHCP ACK - Transaction ID 0x6719436e
6	0.353014	CIS_b9:49:37	Broadcast	ARP	Who has 192.168.0.9? Tell 192.168.0.9
7	0.571241	CIS_b9:49:37	Broadcast	ARP	Who has 192.168.0.9? Tell 192.168.0.9
8	1.571441	CIS_b9:49:37	Broadcast	ARP	Who has 192.168.0.9? Tell 192.168.0.9

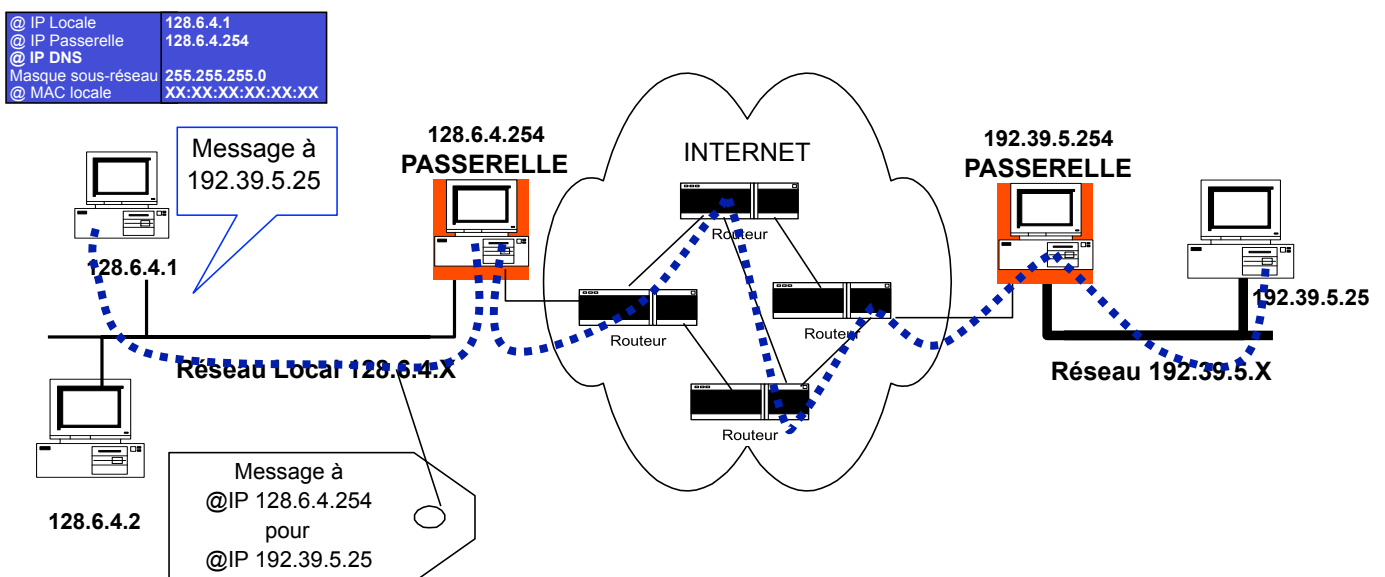
1. Le client DHCP démarre, il n'a pas d'IP et utilise 0.0.0.0 pour faire un "broadcast général (255.255.255.255)". C'est le DHCP Discover.
2. Notre serveur DHCP, qui a l'intention d'offrir à ce client l'IP 192.168.0.9, fait un ping sur cette adresse, histoire de voir si elle est réellement disponible sur le réseau.
3. Comme il ne reçoit pas de réponse à son ping, il offre cette adresse au client.
4. Le client fait alors un DHCP Request
5. Le serveur accepte
6. Le client fait un broadcast ARP pour vérifier de son côté que l'IP 192.168.0.9 n'est pas dupliquée sur le réseau.
7. idem
8. idem

"Routage" d'un Paquet IP

Les machines source et destination sont sur le même réseau local
⇒ 128.6.4.1 veut envoyer un message à 128.6.4.2



Les machines source et destination ne sont pas sur le même réseau
⇒ 128.6.4.1 veut envoyer un message à 192.39.5.25



Protocole ARP

Mécanisme de Résolution d'Adresse ARP

La station A veut envoyer un message à la station B
Mais A ne connaît que l'adresse IP de la station B (@IP 192.39.5.25)

http://192.39.5.25

@ IP A : 192.39.5.27

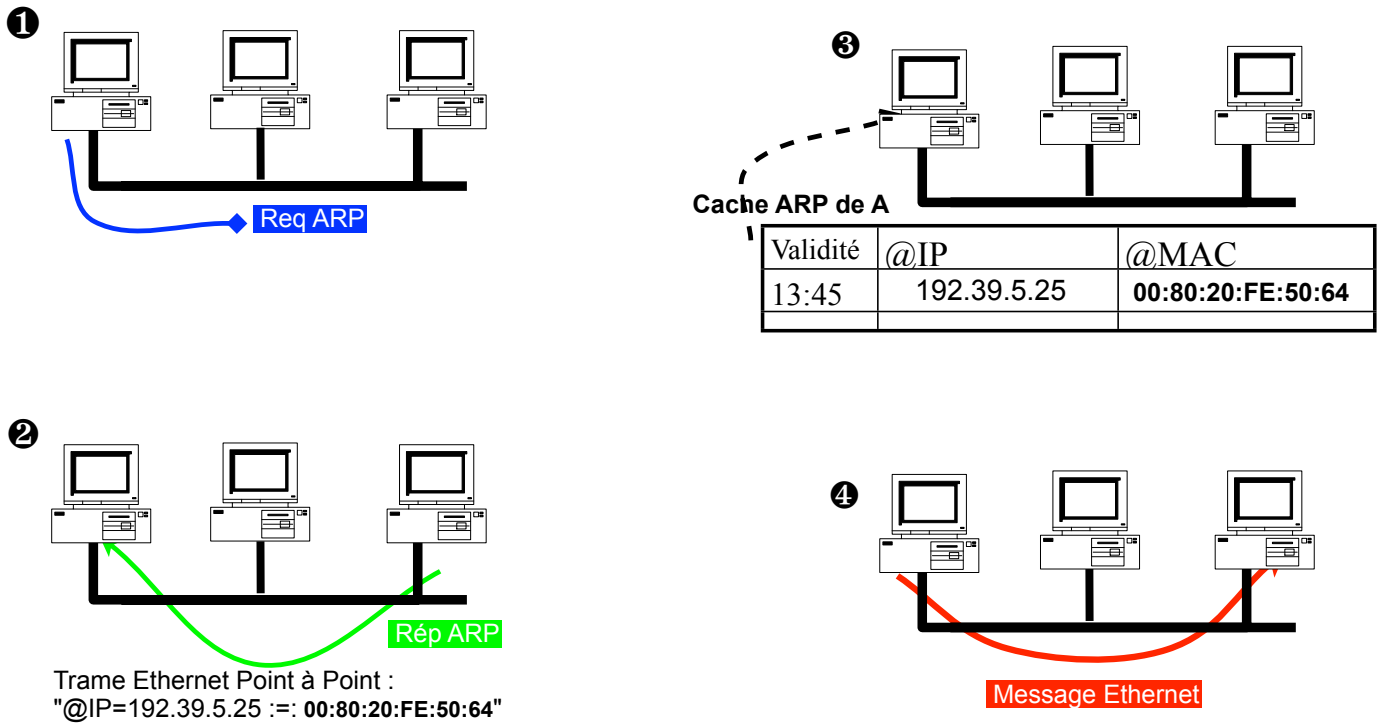
@ MAC A : 00:80:20:FE:10:15



@ IP B : 192.39.5.25

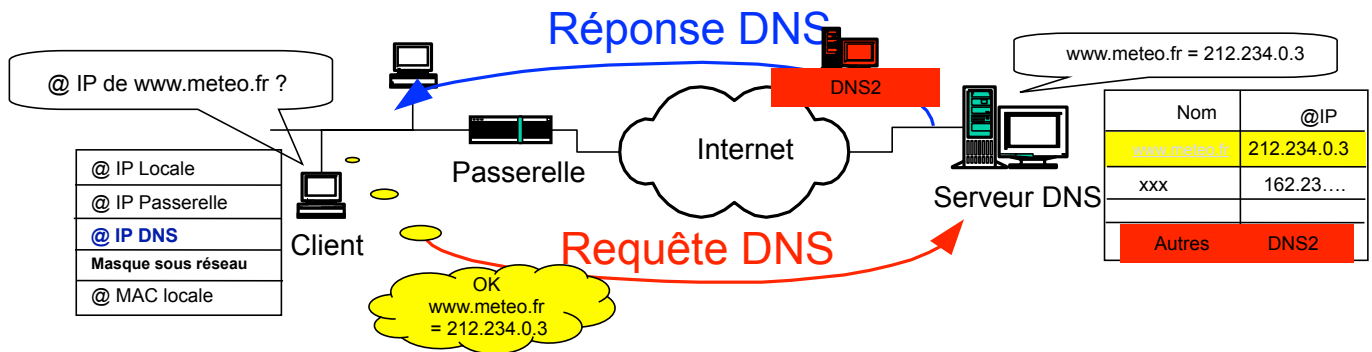
Or Ethernet a besoin de l'adresse MAC du destinataire pour lui envoyer une trame





Serveur DNS

👉 Trouver l'adresse IP d'une machine à partir de son symbolique



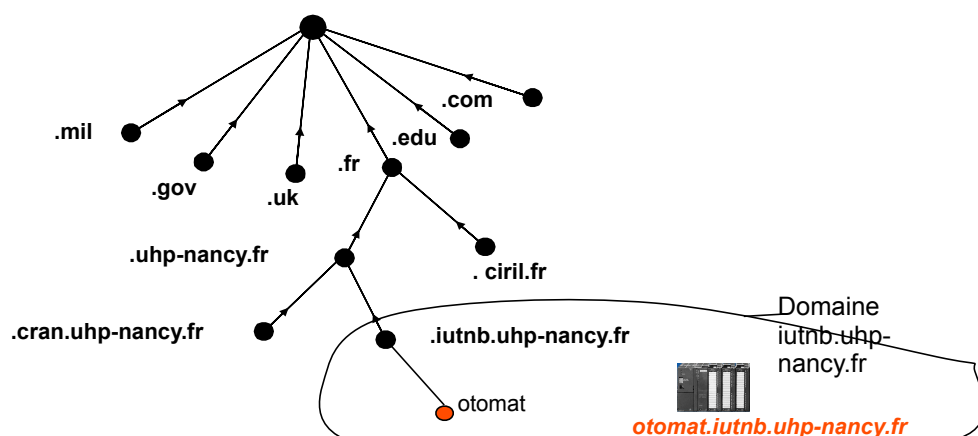
❶ la **résolution de nom** : Le client interroge son serveur DNS pour avoir l'@IP du nom symbolique : *www.meteo.fr*

❷ le **serveur DNS interroge d'autres DNS** jusqu'à trouver l'association nom de domaine ⇔ @IP

❸ un **serveur DNS retourne l'adresse IP** du nom demandé : 212.234.0.3

❹ le **client peut maintenant contacter le destinataire** par son adresse IP : 212.234.0.3

Le nom d'une machine est : **Machine . Sous-Domaine . Domaine**



Lorsqu'un client a besoin d'un nom ou d'une adresse (Nom ⇔ Adresse IP), il s'adresse au serveur DNS qui gère son sous-domaine.

Chaque sous domaine (noeud du graphe) est géré par un ou plusieurs serveurs DNS

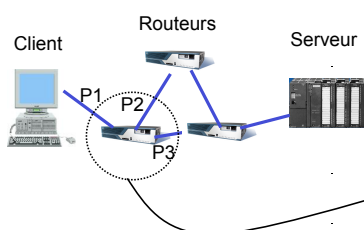
Le serveur DNS relaie la demande au niveau supérieur s'il ne connaît pas le nom recherché (arborescence)

Le Protocole IP

Internetwork Protocol RFC 791

Principe de Routage IP

- Le routage est le processus permettant à une **Trame** d'être acheminé vers son destinataire quand celui-ci n'est pas sur le même réseau physique que l'émetteur.
- Le chemin parcouru par une trame est le résultat du **processus de routage** qui effectue les choix nécessaires afin d'acheminer le datagramme.
-
-
- Chaque routeur dispose d'une **table de routage IP**, indiquant la manière d'atteindre les destinations



Destination	Prochain Routeur	Interface
183.27.0.0	Connexion directe	P1
172.9.0.0	Connexion directe	P2
137.5.0.0	183.27.2.5	P1
140.4.0.0	172.9.1.2	P3
0.0.0.0	183.27.2.5	P1 (par défaut)

Le protocole **IP** (RFC 792) a été conçu pour s'adapter à des types de réseaux différents.
La taille maxi. des données admissibles par un réseau (MTU) varie selon la nature du réseau

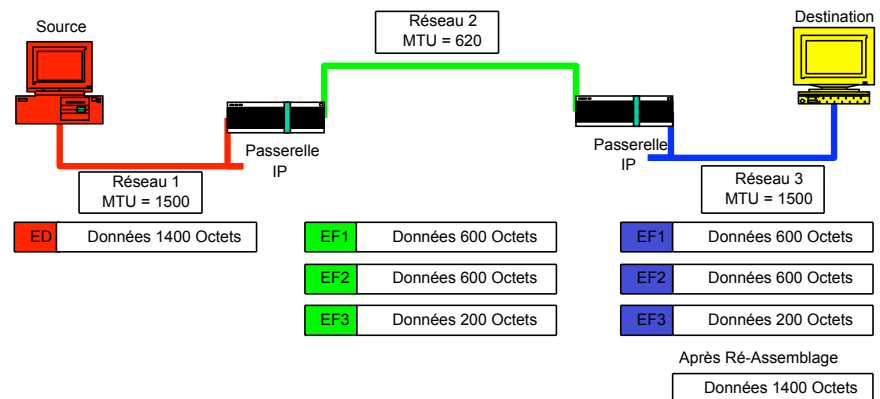
☒ IP s'adapte par un mécanisme de **fragmentation** de paquets.

Maximum Transfert Unit (MTU) : Taille maximale d'un datagramme sur une machine IP, passerelle ou routeur.

Ethernet : MTU = 1500 octets
jeton) **ATM** : MTU = 32

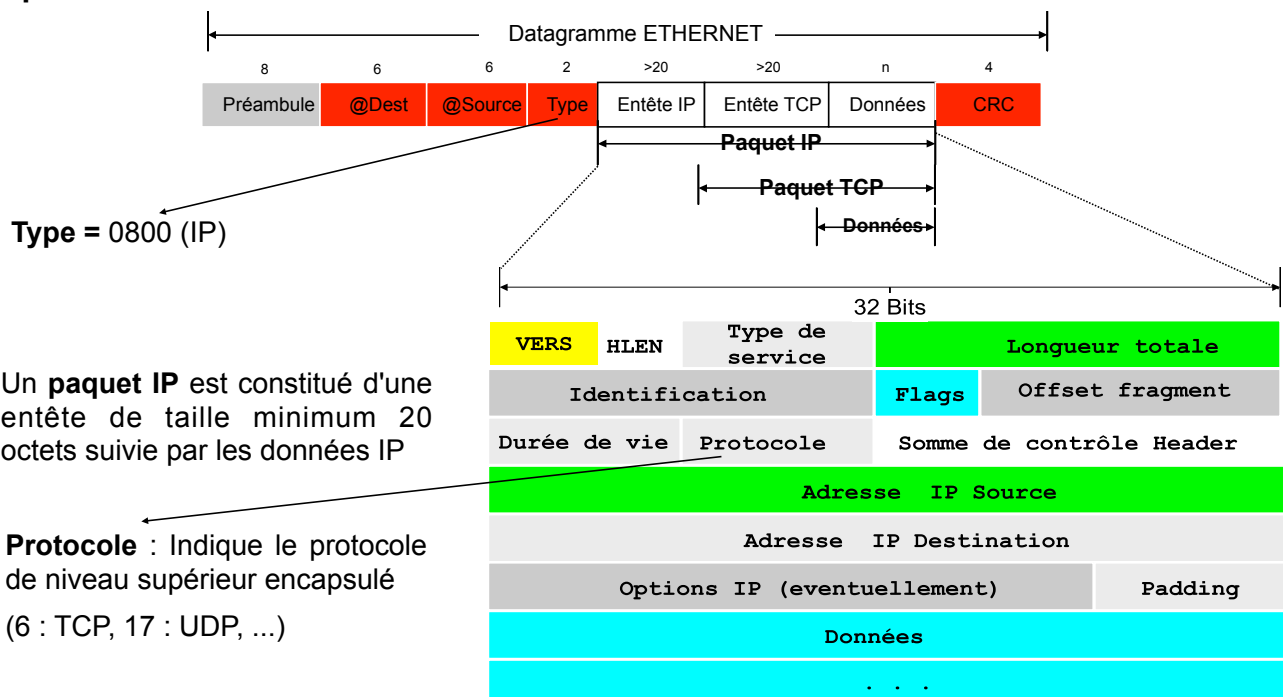
X25 : MTU = 1007 octets **Token Ring** : MTU = 4440 à 17940 octets f(temps conservation

IP adapte la taille des paquets de données aux MTU des différents réseaux traversés, en découpant le paquet en paquets plus petits : c'est un rôle majeur des routeurs sur Internet appelé **fragmentation**



Le **ré-assemblage** est effectué par la couche IP du destinataire **jamais par les routeurs**.

Le protocole IP encapsule les données générées par les couches 7 à 4 pour former un **paquet IP**.



VERS : Version IP (4 : IPV4, 6 : IPV6 IPng)

HLEN : Longueur de l'entête IP en mots de 32 bits

Longueur Totale : Long. de l'entête et des données IP en octets.

Identification : Numéro du datagramme IP.

Flags : DF = 1 : (Do not Fragment) Le Datagramme ne doit pas être fragmenté

MF = 1 : (More Fragments) Le destinataire est informé que d'autres fragments vont arriver

Offset Fragment : Offset sur 13 bits des données contenues dans le datagramme IP depuis le 1er fragment

Durée de Vie : Compteur de sauts (**hops**) décrémenté à la traversée de chaque routeur. Si =0 le routeur stoppe le paquet et renvoi un message ICMP. Limite la durée de vie des datagrammes sur Internet.

Protocole : Indique le protocole de couche supérieure (6 : TCP, 17 : UDP, 1 : ICMP,...)

Somme de contrôle header : Checksum sur 16 bits de l'entête sans les données IP. Recalculé à chaque routeur car TTL change.

Adresses IP Source et Destination

Options : Indique le niveau de sécurité, information de routage, d'horodatage : rarement utilisées.

Padding : Sert à compléter l'entête IP en nombre de mots de 32 pleins.

Données : Données encapsulées à destination du protocole de niveau supérieur.

Type de Service : TOS : Qualité de service demandée

Bits 0-2	1	1	1	1	1
Préséance	Délai	Débit	Fiabilité	Coût	MBZ
000 Routine	0	0	0	0	
001 Priority	Normal	Normal	Normal	Normal	
010 Immediate	1 Faible	1 Elevé	1 Elevé	1 Faible	
011 Flash					
101 Critical					
110 Internetwork					
Control					
11 Network					
Control					

C'est une commande interne au protocole IP implémentée dans le système d'exploitation de la machine

- Envoi des paquets (32 octets de données ASCII 'a' à 'z' ...) vers l'@ cible
: Commande ECHO du protocole **ICMP** (Internet Control Message Protocol)
- Attente des réponses, jusqu'à 1 seconde pour chaque paquet.
- Vérification des paquets reçus (32 octets de données ASCII 'a' à 'z' ...) , et mesure du temps d'attente.

```
Sélectionner - Commandes MS-DOS
C:\WINDOWS>ping www.ciril.fr

Envoi d'une requête 'ping' sur arcturus.ciril.fr [193.50.27.66] avec 32 octets de données :

Réponse de 193.50.27.66 : octets=32 temps=169 ms TTL=252
Réponse de 193.50.27.66 : octets=32 temps=168 ms TTL=252
Réponse de 193.50.27.66 : octets=32 temps=148 ms TTL=252
Réponse de 193.50.27.66 : octets=32 temps=145 ms TTL=252

Statistiques Ping pour 193.50.27.66:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en milli-secondes :
        minimum = 145ms, maximum = 169ms, moyenne = 157ms

C:\WINDOWS>
```

- Exécute un ping vers une station distante avec un paramètre interprété par chaque routeur traversé lui signifiant de répondre par son adresse.
- Attente des réponses et mesure du temps d'attente.

```
C:\WINDOWS>tracert www.ciril.fr

Détermination de l'itinéraire vers arcturus.ciril.fr [193.50.27.66]
avec un maximum de 30 sauts :

 1  159 ms   140 ms   135 ms  viete.cran.uhp-nancy.fr [193.50.39.44]
 2  140 ms   148 ms   139 ms  gw1.sciences.stannet.ciril.fr [193.50.39.254]
 3  176 ms   150 ms   150 ms  gw1.ciril.stannet.net [193.50.80.34]
 4  167 ms   150 ms   140 ms  arcturus.ciril.fr [193.50.27.66]

Itinéraire déterminé.

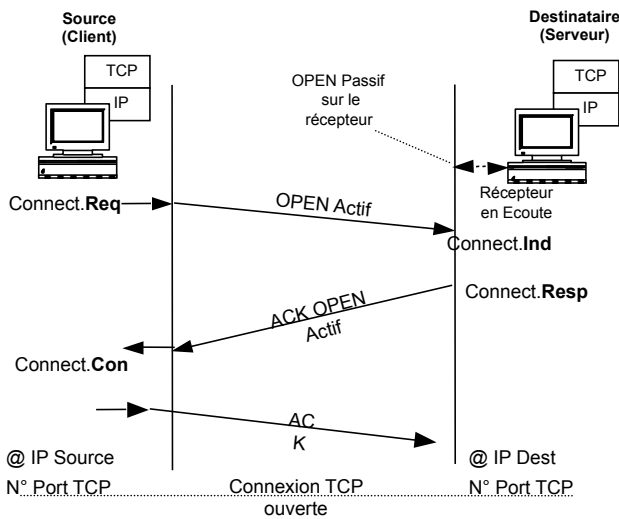
C:\WINDOWS>
```

Le Protocole TCP

Transmission Control Protocol RFC 792

Ouverture d'une connexion TCP

Une connexion TCP est établie en 3 temps de manière à assurer la synchronisation entre Client et Serveur



Le serveur se met en écoute : OPEN passif.
La couche TCP serveur se met en attente de connexions.

Un client fait une demande de connexion : OPEN actif.

La couche TCP cliente spécifie les **sockets** source et destination liées à cette connexion.
Le Serveur Accepte ou Refuse la connexion (Nb limité)

Une connexion est établie entre l'émetteur et le destinataire caractérisés chacun par un couple
(@ IP, N° port TCP), appelé une **SOCKET**

Emetteur	Destinataire
(@ IP, port TCP) (124.32.12.1 , 1512)	(@ IP, port TCP) (19.24.67.2 , 1538)

Gestion d'une connexion TCP

L'envoi de trame réseau Internet est réalisé après **ouverture préalable d'une connexion** entre l'émetteur et le destinataire.

Les services fournis par la couche TCP sont :

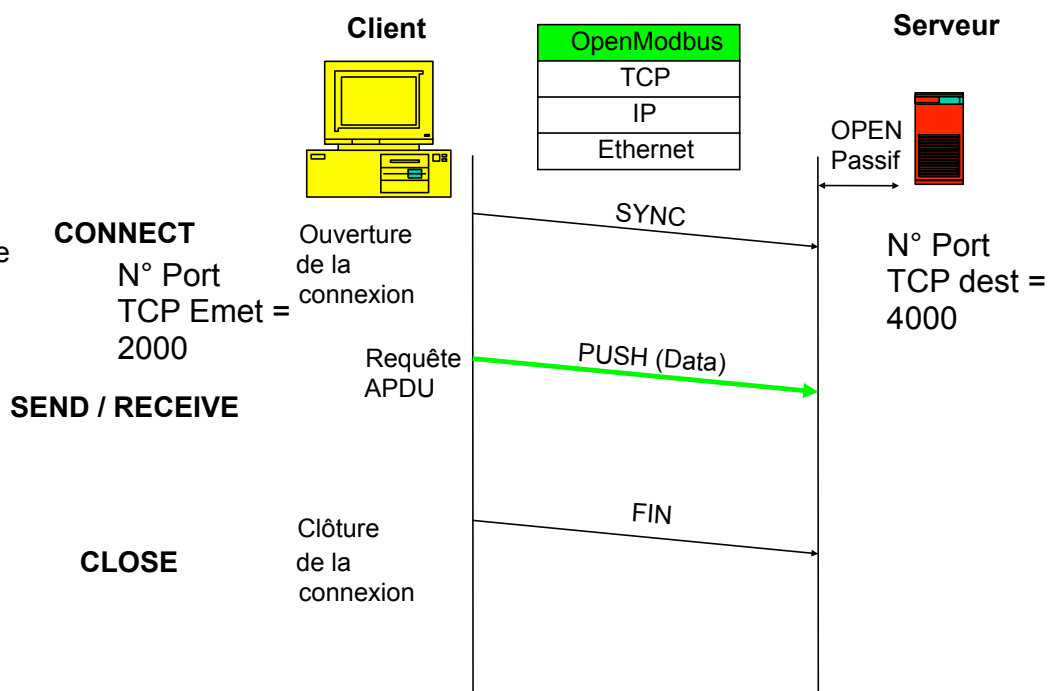
CONNECT ouverture d'une connexion

CLOSE : fermeture d'une connexion

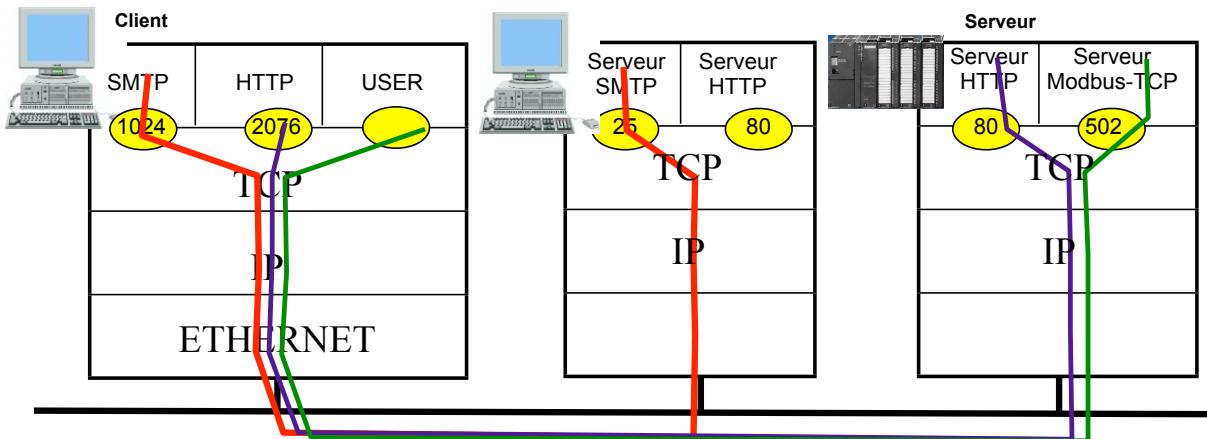
SEND : envoyer les données sur une connexion ouverte

RCV : recevoir les données sur une connexion ouverte

STATUS : fournir des renseignements sur une connexion ouverte

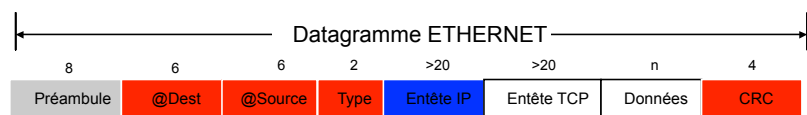


- ☞ TCP peut servir plusieurs applications en même temps sur la même machine source :
⇒ Principe de multiplexage.
- ☞ TCP associe un numéro de port à chaque application qui utilise ses services.



Port TCP réservés : 20, 21 : FTP, 23 : TELNET, 25 : SMTP, 80 : HTTP, 110 : POP3, 512 : MODBUS-TCP...
N° Port libres utilisateur > 1023

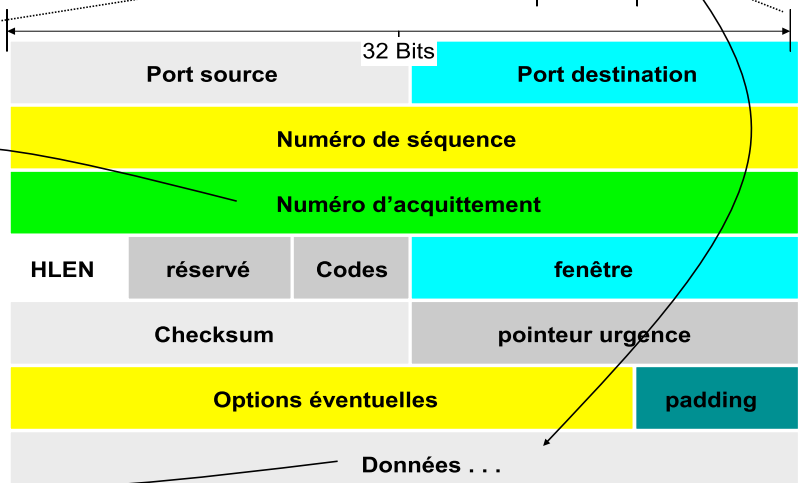
Le protocole TCP encapsule les données générées par les couches 7 à 5 pour former **un paquet TCP**



Un paquet TCP est constituée d'une entête de 20 octets minimum suivie par des données TCP

Chaque paquet TCP sera acquitté assurant un transport fiable de bout en bout

Les Données TCP sont constituées de l'APDU de la couche supérieure



L'entête TCP à une longueur minimale de 20 Octets, qui peut augmenter avec les options.

Port Source, Port Destination : ports en connexion des applications origine et destination.

Numéro de séquence : Le numéro du premier octet est le numéro de séquence.

Numéro d'acquittement : prochain numéro de séquence attendu par l'émetteur de cet acquittement.
Acquitte implicitement les datagrammes reçus avec les octets précédents.

HLEN : Code sur 4 bits la longueur de l'entête TCP en mots de 32 bits

Codes : 6 bits de drapeau
d'acquittement

URG : Indique l'envoi des données en urgence sans attente

ACK	: Indique que le champ "Numéro d'acquittement est valide"
PSH	: Indique la remise immédiate des données à la couche supérieure
RST	: Demande de ré-initialisation de la connexion
SYN	: Indique l'ouverture d'une connexion de circuit virtuel
FIN	: Indique la fermeture de la connexion

Fenêtre : Taille de la fenêtre d'anticipation.

Checksum : Somme complémentée à 1 des compléments à 1 de tous les mots de 16 bits du paquet TCP

Pointeur d'urgence

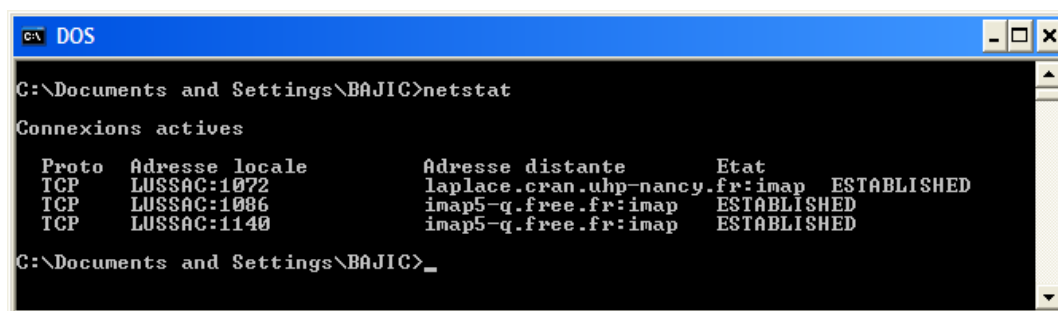
Options : Permet de négocier la taille maximale des segments échangés. TCP calcule une taille maximale de segment de manière à ce que le datagramme IP résultant corresponde au MTU du réseau. La recommandation est de 536 octets.

Padding : Sert à compléter en nombre de mots de 32 pleins l'entête TCP.

Données : Données encapsulées à destination du protocole de niveau supérieur.

Ports TCP ouverts

La commande NETSTAT.EXE permet de connaître les connexions ouvertes et les ports utilisés par la couche TCP



```
C:\Documents and Settings\BAJIC>netstat

Connexions actives

Proto  Adresse locale      Adresse distante     Etat
TCP    LUSSAC:1072         laplace.cran.uhp-nancy.fr:imap ESTABLISHED
TCP    LUSSAC:1086         imap5-q.free.fr:imap ESTABLISHED
TCP    LUSSAC:1140         imap5-q.free.fr:imap ESTABLISHED

C:\Documents and Settings\BAJIC>
```

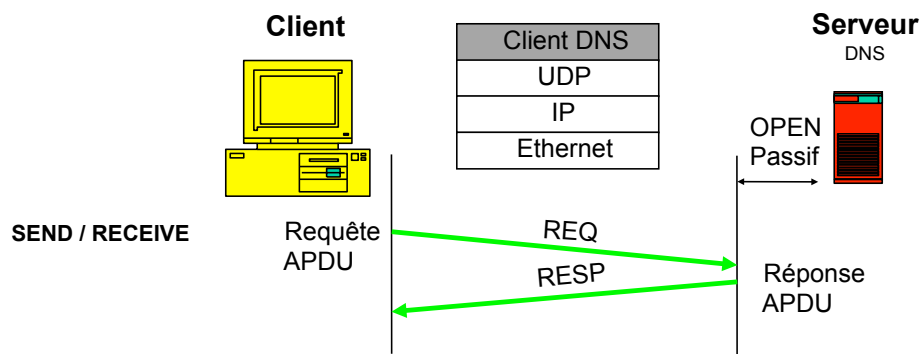
Protocole UDP

User Datagram Protocol RFC 768

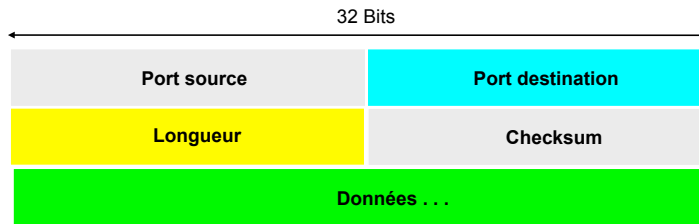
Requête APDU en Mode non connecté UDP

L'échange avec UDP est de type Question/Réponse sans connexion préalable.

- ⇒ Le transport de bout en bout n'est pas fiable car la réception d'une trame n'est jamais acquittée.
- ⇒ Seule la réponse transmise permet de savoir si la requête est bien arrivée (Time Out)



L'entête UDP, très simple, est de taille fixe de 8 octets



Port Source, Port Destination : Indiquent les N° port des applications émetteur et destinataire sur 16 bits .

Longueur : Longueur totale du paquet UDP, comprenant l'entête de huit octets plus les données UDP.

Checksum : Somme complémentée à 1 des compléments à 1 de tous les mots de 16 bits du paquet UDP, avec un remplissage de zéros pour obtenir une longueur multiple de deux octets, auquel est ajoutée une pseudo-entête telle que ci-dessous

Ethernet Industriel

Modbus-TCP

Selon Spécification Schneider Mars 1999
(www.modbus.org)

Pr. Eddy BAJIC
IUT Nancy Brabois
Nancy Université

Mais Pourquoi Utiliser Ethernet en Automatisation Industrielle ?

Avantages *Standard Mondial, Banalisé,
Peu coûteux, Multi-usages
Rapide,
Protocoles TCP-IP et au dessus : HTTP (Web), SMTP (Mail), FTP (Fichiers) ...*

Inconvénients

Besoin de Solutions "Ethernet Industriel" Adaptée aux Contextes Industriels

*Fin des Domaines de Collision : **Commutation, Full Duplex** (Switch, ASIC switch)*

*Des Protocoles d'application dédiés pour l'Industrie : **Bataille pour un standard***

*La quête du déterminisme : **Temps réel, Isochronisme***

Sites Internet Intéressants :

<http://ethernet.industrial-networking.com>

www.iona.org

Assoc promotion Ethernet dans l'automatisation



⇒ Enjeux : Optimiser la gestion de l'éclairage public ⇒ Principes

- ✓ Importance du budget de maintenance
- ✓ Temps d'indisponibilité des installations
- ✓ Gestion du bon fonctionnement des centaines, milliers de lampes
- ✓ Économies d'énergie
- ✓ Futures chartes de l'environnement,

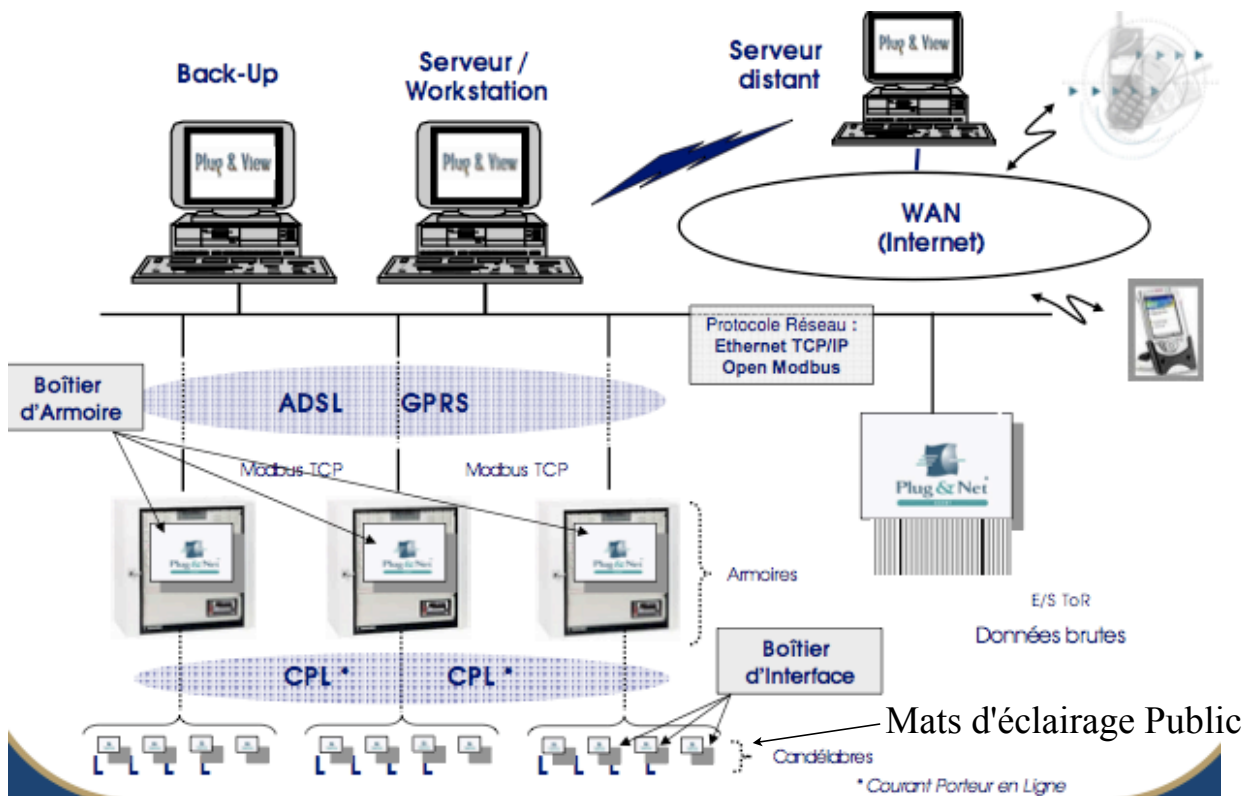
- ✓ Un logiciel de supervision avec aéo localisation sur un PC serveur : **Plug & View**
- ✓ Un concentrateur CPL dans l'armoire de distribution
- ✓ Un équipement d'interface CPL par mât
- ✓ Une valise de paramétrage

⇒ Infrastructures à gérer

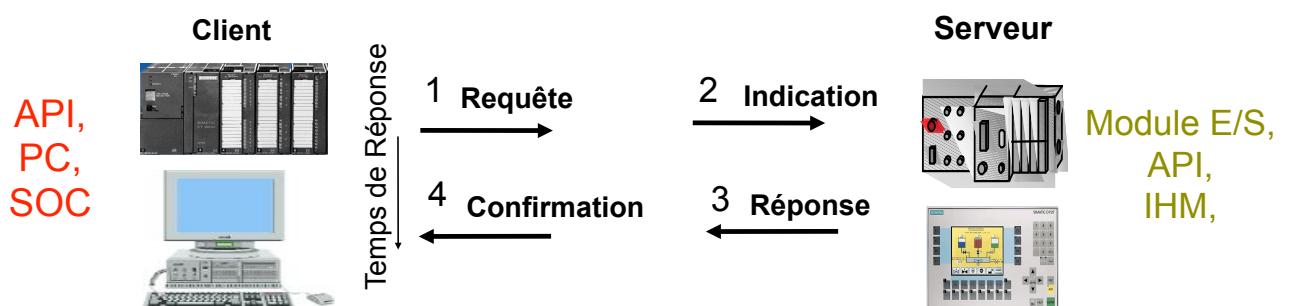
- ✓ Lampes à décharge sur réseau électrique :
 - Sodium Haute Pression
 - Iodure métallique
 - Ballon fluo
 - ...
- ✓ Ballast et condensateur

⇒ Avantages

- ✓ Performance
- ✓ Modularité
- ✓ Bas coûts
- ✓ Simplicité d'installation
- ✓ Facilité à utiliser



L'architecture Internet est basée sur un modèle de communication Client-Serveur



Client : Sollicite un service du Serveur par une Requête

Serveur :

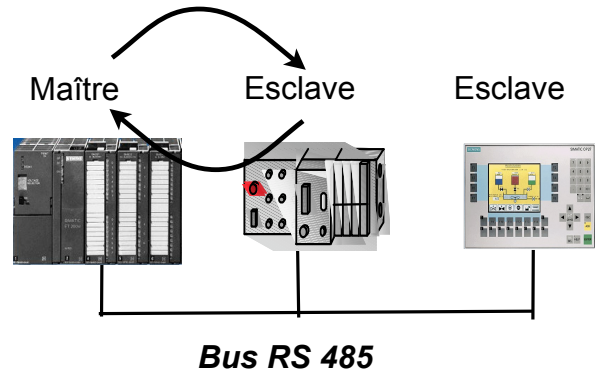
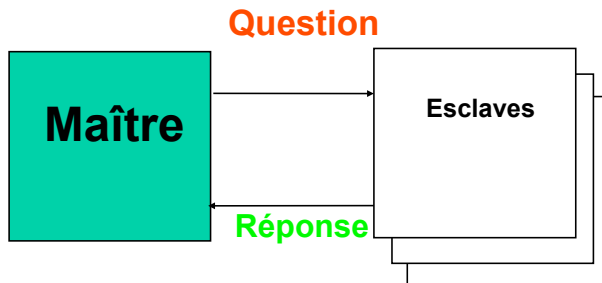
- Est à l'écoute des clients qui le sollicitent (écoute sur N° de port TCP/UDP donné)
- Ne répond qu'aux requêtes des clients

Temps de Réponse : Non garanti, indéterminé, il dépend de l'architecture réseau traversée

Modèle Maître / Esclave Vs Client / Serveur

Modèle Maître / Esclave (MODBUS-RTU)

Principe de Communication par Question/Réponse

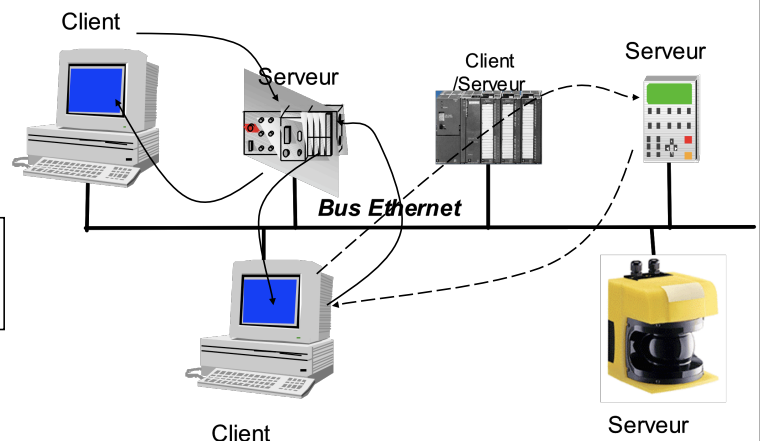
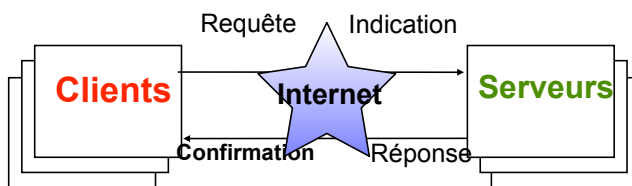


- 1 Maître unique
- Plusieurs Esclaves (@1 à @63)
- Transactions séquentielles

Modèle Maître / Esclave Vs Client / Serveur

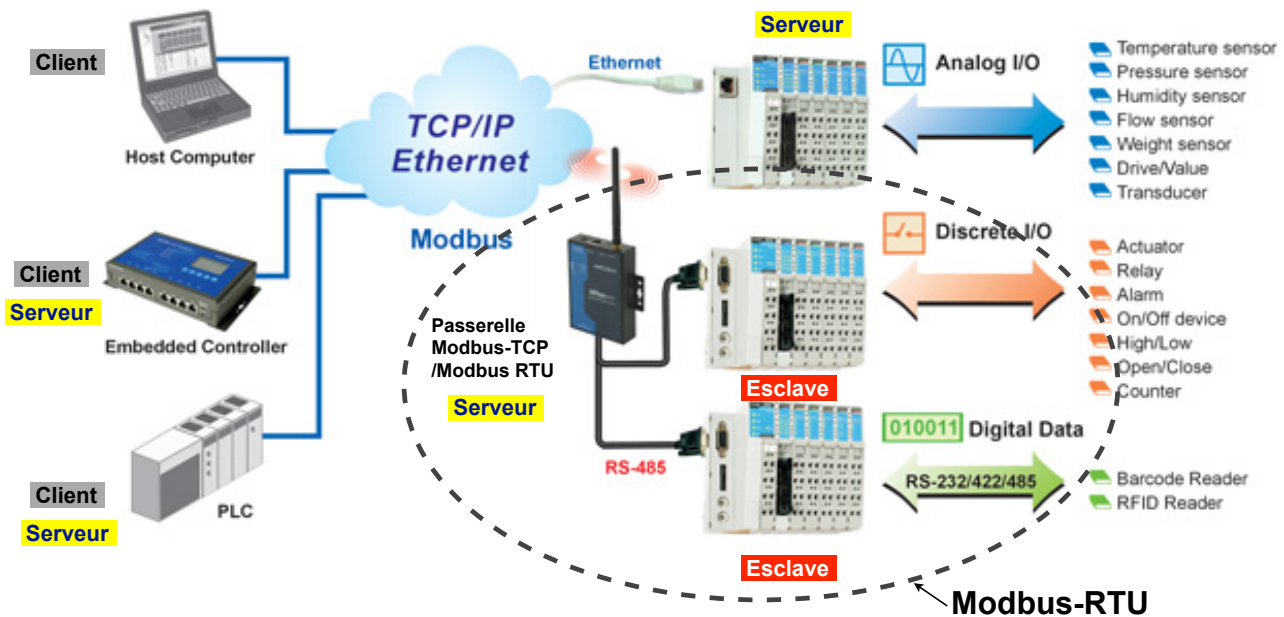
Modèle Client / Serveur (MODBUS-TCP)

Principe de Communication par Requêtes Multiples



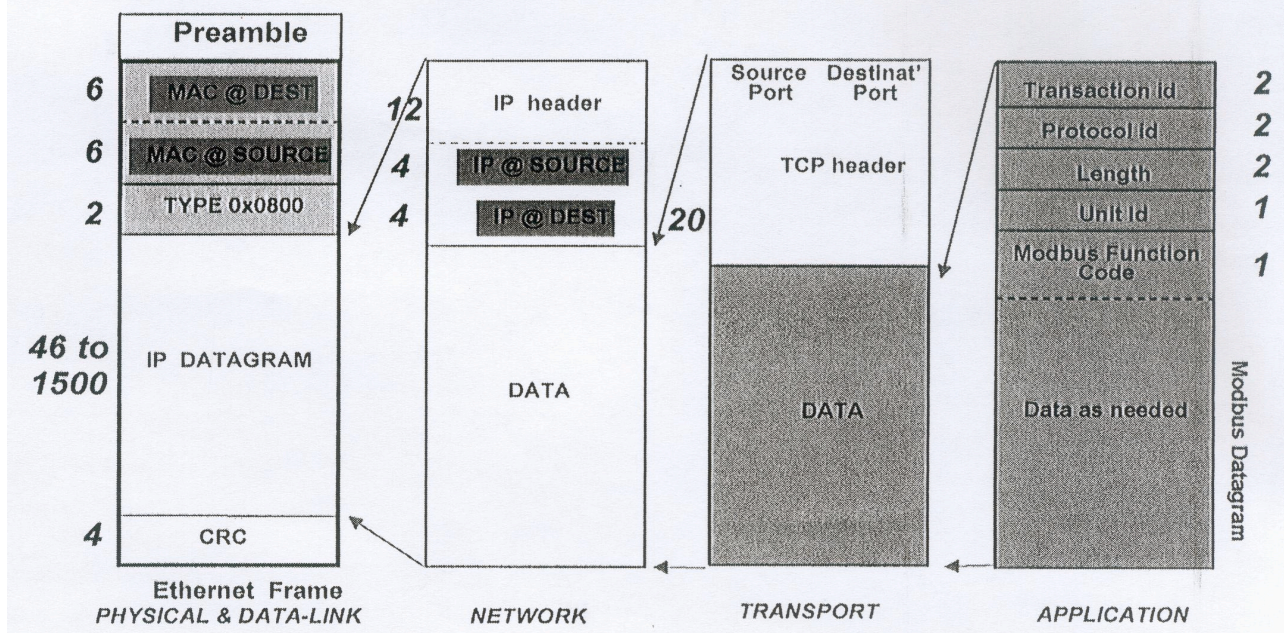
- Clients Multiples (@IP clients)
- Serveurs Multiples (@IP serveurs)
- Transactions Simultanées

Accéder aux E/S d'un processus à Distance en Mode Client / Serveur



<http://www.moxa.com/product/iologik-4000.htm#top>

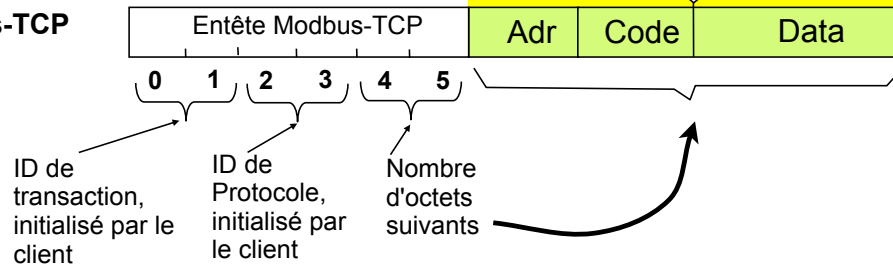
Ethernet carries IP carries TCP carries Modbus



Trame Modbus RTU



APDU Modbus-TCP



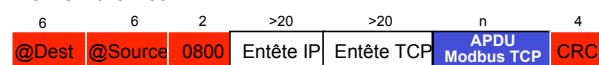
ID de transaction : Valeur positionnée par le client afin de repérer les réponses retournées par le serveur qui recopie la valeur

ID de Protocole : Valeur positionnée par le client (Modbus = 0)

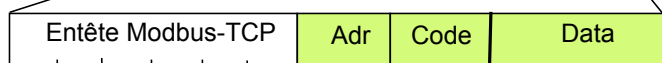
Scénario d'une requête MODBUS-TCP routée sur Internet

1

Trame Ethernet



La passerelle (Serveur) Modbus-TCP extrait l'APDU

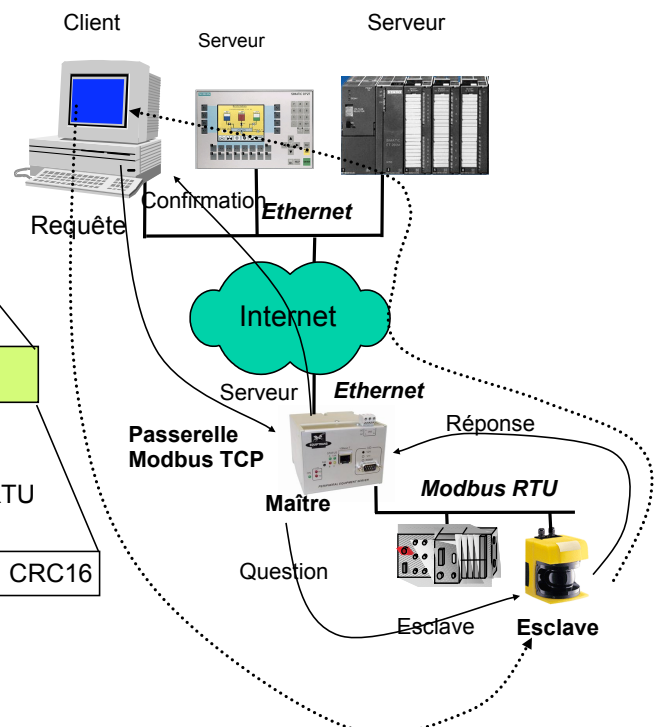


2 La passerelle Modbus-TCP génère une question Modbus-RTU à l'esclave adressé.



3

4



Une Connexion et requête Modbus TCP

Logiciel ETHEREAL (www.ethereal.com)

capture échange Modbus TCP WAgp.eth - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.106	193.49.35.63	TCP	3186 > 502 [SYN] Seq=0 Ack=0 win=25200 Len=0 MSS=1460
2	0.062895	193.49.35.63	192.168.2.106	TCP	502 > 3186 [SYN, ACK] Seq=0 Ack=1 win=1500 Len=0 MSS=512
3	0.062938	192.168.2.106	193.49.35.63	TCP	3186 > 502 [ACK] Seq=1 Ack=1 win=25200 Len=0
4	2.452694	192.168.2.106	193.49.35.63	Modbus	query [1 pkt(s)]: trans: 0; unit: 1, func: 6: write single register.
5	2.515688	193.49.35.63	192.168.2.106	Modbus	response [1 pkt(s)]: trans: 0; unit: 1, func: 6: write single register.
6	2.667830	192.168.2.106	193.49.35.63	TCP	3186 > 502 [ACK] Seq=13 Ack=13 win=25188 Len=0
7	84.415068	192.168.2.106	193.49.35.63	Modbus	query [1 pkt(s)]: trans: 0; unit: 1, func: 3: Read multiple registers.
8	84.478560	193.49.35.63	192.168.2.106	Modbus	response [1 pkt(s)]: trans: 0; unit: 1, func: 3: Read multiple registers.
9	84.585667	192.168.2.106	193.49.35.63	TCP	3186 > 502 [ACK] Seq=25 Ack=30 win=25171 Len=0
10	94.749318	192.168.2.106	193.49.35.63	Modbus	query [1 pkt(s)]: trans: 0; unit: 1, func: 3: Read multiple registers.
11	94.813640	193.49.35.63	192.168.2.106	Modbus	response [1 pkt(s)]: trans: 0; unit: 1, func: 3: Read multiple registers.
12	95.000656	192.168.2.106	193.49.35.63	TCP	3186 > 502 [ACK] Seq=37 Ack=289 win=24912 Len=0
13	102.58838	192.168.2.106	193.49.35.63	TCP	3186 > 502 [FIN, ACK] Seq=37 Ack=289 win=24912 Len=0
14	102.64770	193.49.35.63	192.168.2.106	TCP	502 > 3186 [ACK] Seq=289 Ack=38 win=1500 Len=0
15	102.64887	193.49.35.63	192.168.2.106	TCP	502 > 3186 [FIN, ACK] Seq=289 Ack=38 win=1500 Len=0
16	102.64890	192.168.2.106	193.49.35.63	TCP	3186 > 502 [ACK] Seq=38 Ack=290 win=24912 Len=0

Frame 7 (66 bytes on wire, 66 bytes captured)

Ethernet II, Src: 00:80:c8:02:27:5e, Dst: 00:04:e2:7c:6f:e8

Internet Protocol, Src Addr: 192.168.2.106 (192.168.2.106), Dst Addr: 193.49.35.63 (193.49.35.63)

Transmission Control Protocol, Src Port: 3186 (3186), Dst Port: 502 (502), Seq: 13, Ack: 13, Len: 12

Modbus/TCP

0000 00 04 e2 7c 6f e8 00 80 c8 02 27 5e 08 00 45 00 ...|o... ..A..E..

0010 00 34 73 6b 40 00 06 df d5 c0 a8 02 6a c1 31 .4sk@.....j..1

0020 23 3f 0c 72 01 f6 83 82 28 b6 bd 95 fe 0e 50 18 #?.r.....(.....P.

0030 62 64 2c 87 00 00 00 00 00 00 06 01 03 02 00 bd.....

0040 00 04 ..

File: capture P: 16 D: 16 M: 0

Passerelle ModBus série RTU / Modbus Ethernet TCP, alimentation interne

- Compatible Ethernet 10Base-T (802.3)
- Fonction serveur TCP/IP (HTTP, TFTP, SMTP, SNMP, etc...)
- Supporte les protocoles Modbus RTU-ASCII
- E/S série V24, V11 ou RS485 avec isolation optique
- Logiciel re-routage port COM vers Ethernet en option



Le serveur de périphériques SP1xxxRMB ou passerelle Modbus/TCP permet la gestion de périphériques asynchrones Modbus, via un réseau Ethernet, à partir du protocole TCP/IP.

Le logiciel applicatif pilotant l'équipement asynchrone peut utiliser soit un port COM traditionnel avec un logiciel de re-routage soit un port Ethernet 10Base-T (Modbus/TCP).

Le protocole de communication Modbus, basé sur le principe Maître - Esclaves, est supporté de différentes façons par le serveur de périphérique SP1xxxRMB:

- Connexion d'équipements Modbus esclaves vers un poste maître Modbus/TCP
- Connexion d'un poste maître Modbus-RTU vers des équipements esclaves Modbus/TCP
- Connexion traditionnelle Modbus maître / esclaves via un support Ethernet TCP/IP

Le serveur de périphérique ou passerelle Modbus SP1xxxRMB supporte ces différentes configurations, qui permettent la migration progressive vers Modbus/TCP. Différents paramètres doivent être sélectionnés lors de la phase de configuration :

- Adresse "slave" unique ou multiple (pour une adresse IP)
- Time-out de réception caractères
- Time-out de réception réponse de l'esclave

Le serveur de périphériques ou passerelle Modbus SP1xxxRMB comporte une E/S série asynchrone de type V24, V11 ou RS485 avec isolation optique et un débit maximal de 115,2 Kbps avec/sans gestion de flux.

L'accès Ethernet 10 Mbps (IEEE802.3) de type 10Base-T (RJ45) permet le raccordement sur le réseau local Ethernet via un port de hub Ethernet ou par l'intermédiaire d'un convertisseur de média cuivre / fibre optique.

Le serveur de périphériques SP1 est proposé sous forme de boîtier plastique autonome ou de boîtier compact pour fixation sur rail Din.

De nombreuses applications sont envisageables grâce au serveur de périphériques, de la simple gestion de capteurs à des processus industriels, en passant par des applications de télécontrôle et de téléalarme, etc...

Le serveur de périphériques peut également supporter localement des applicatifs spécifiques sur demande.

La passerelle Modbus/TCP induit de nombreux protocoles en plus de TCP/IP, UDP, Telnet, DHCP, SNMP, TFTP, HTTP, etc...

Les applications autorisées par ces différents services sont à prendre en compte par l'utilisateur.

GMI-DATABOX propose plusieurs types de prestations de service, du transfert de compétences à la réalisation complète de vos applications spécifiques.

De nombreux autres modèles sont disponibles pour des environnements Modbus et industriels avec :

- entrées et/ou sorties numériques (T.O.R)
- entrées et sorties analogiques, etc...

Contactez notre service commercial.

CARACTERISTIQUES

• Fonction : Convertisseur Modbus / Ethernet TCP-IP

E/S série : V24, V11 ou RS485

Mode de transmission : Asynchrone

Code de transmission : transparent

Protocole de transmission : Modbus RTU ou ASCII

Débit : jusqu'à 115,2 Kbps

Gestion de flux : XON/XOFF, CTS/DTR ou sans.

Isolation : par coupleurs optiques

Accès Ethernet :

Conforme IEEE 802.3 (CSMA/CD)

Interface : RJ45 (10 Base-T)

Adresse IP : programmable

Protocoles : TCP, IP, ICMP, ARP

Services TCP : SNMP, DHCP, TFTP, HTTP, SMTP, etc...

Dimensions :

- Boîtier plastique : 110 x 50 x 170 mm (l x h x p)

- Boîtier rail Din : 75 x 100 x 110 mm

Connecteurs :

- LAN : RJ45

- E/S de contrôle : DB9 femelle

- E/S utilisateur : DB9 mâle

Voyants :

- Lan : Activité, TD, RD et Collision

- E/S : TD, RD, ON

Alimentation : 230 VAC 50/60 Hz

Option alimentation : 24 ou 48VDC

Environnement :

- Température d'utilisation : 0° à 50°C

- Température de stockage : -10° à +70°C

- Humidité : 10 % à 90 % sans condensation.

Normes : CEM 89/336

EN60950

Fabrication : France