NTCIP : les protocoles de communications pour les applications trafic : analyse de NTCIP

Samy Branci, Sylvie Chambon

RAPPORT D'ETUDE

Organisme auteur :

CERTU : Centre d'études sur les réseaux,
les transports,
l'urbanisme et les constructions publiques

Rédacteur et coordonateur :
Samy BRANCI (Département Technologies)
Sylvie CHAMBON (Département Technologies)

NTCIP : LES PROTOCOLES DE COMMUNICATIONS POUR LES APPLICATIONS TRAFIC

Analyse de NTCIP

Novembre 1997

NOTICE ANALYTIQUE

<table>
<tr><td colspan="4">Organisme commanditaire :

CERTU : Centre d'études sur les réseaux, les transports, l'urbanisme et les constructions publiques
9, rue Juliette Récamier 69456 Lyon Cedex 06 - Tél. : 04 72 74 58 00 - Fax : 04 72 74 59 00</td></tr>
<tr><td colspan="4">Titre :
NTCIP : Les protocoles de communications pour les applications trafic</td></tr>
<tr><td colspan="3">Sous-titre :
Analyse de NTCIP</td><td>Langue : Français</td></tr>
<tr><td>Organisme auteur :

CERTU : Centre d'études sur les réseaux, les transports, l'urbanisme et les constructions publiques</td><td colspan="2">Rédacteur et coordonateur :

Samy BRANCI
(Département Technologies)
Sylvie CHAMBON
(Département Technologies)</td><td>Date d'achèvement :

Novembre 1997</td></tr>
<tr><td colspan="4">Remarques préliminaires :

Ce document présente la famille de protocoles NTCIP – National Transportation Communications for ITS Protocol - en cours de développement aux Etats Unis.
Ce document est destiné à tous les acteurs concernés par le déploiement des systèmes techniques pour l'exploitation de la route.</td></tr>
<tr><td colspan="4">Résumé :

Face au déploiement tous azimuts des systèmes de gestion de la route dans chaque état des Etats Unis, et de façon non coordonnée, la FHWA – Federal HighWay Administration - a souhaité dés 1993, la construction d'un standard de communication pour les systèmes de gestion de la route. En effet, à l'heure actuelle, chaque état possède un système de gestion de la route de type propriétaire, avec pour conséquence un coût élevé, une non interopérabilité entre systèmes adjacents, et surtout une incompatibilité entre des équipements de terrain de fournisseurs différents. En étroite coopération avec les industriels regroupés au sein de l'organisme NEMA – National Electrical Manufacturers Association- des groupes de travail ont été constitués afin de réfléchir et de promouvoir un standard de communication. Ce futur standard outre atlantique devrait permettre de répondre aux besoins des gestionnaires, et assurer une meilleure pérennité des systèmes de gestion de la route.</td></tr>
<tr><td colspan="2">Mots clés :
NTCIP, Protocoles, Réseaux de télécommunications routiers, recueil et échanges de données routières</td><td colspan="2">Diffusion :
DSCR, SETRA, INRETS, CERTU, LCPC</td></tr>
<tr><td>Nombre de pages :
51 pages</td><td>Prix : 50 FF</td><td>Confidentialité :
Non</td><td>Bibliographie :
Oui</td></tr>
</table>

AVERTISSEMENT

Ce document est une synthèse des études menées aux Etats Unis sur les protocoles NTCIP. Ces études décrivent les protocoles en cours de construction et portent sur des recommandations. Il se peut, comme tout protocole naissant, que des modifications puissent être apportées dans les mois qui suivent la sortie de ce document.

Nous nous proposons de définir dans ce document le contexte dans lequel NTCIP a vu le jour, et de décrire les protocoles de communications développés par le comité de pilotage NTCIP.

Ce document s'appuie sur des ouvrages référencés au chapitre bibliographie. Les références seront signalées dans ce document par des nombres entre parenthèses. A la fin de ce document, nous proposons un glossaire répertoriant tous les termes techniques utilisés dans la rédaction de ce document ainsi que les études techniques NTCIP disponibles ou en cours de développement.

SOMMAIRE

1 INTRODUCTION

1.1 LES SYSTEMES INFORMATIQUES DE GESTION DE LA ROUTE

1.1.1 Naissance des systèmes informatiques de gestion de la route

La mobilité des personnes et des marchandises a depuis les années 1950 considérablement augmenté dans les pays industrialisés du fait de la banalisation de l'usage de l'automobile. La croissance des déplacements est essentiellement supportée par la route. Pour répondre à cet essor, les autorités ont massivement construit des autoroutes, des voies express et amélioré le réseau routier existant. Néanmoins, les phénomènes de congestion sont aujourd'hui devenus endémiques dans les grandes agglomérations, aux heures de pointe ou sur les grands axes lors des départs et retours de vacances. De plus, la construction de tels ouvrages coûte cher et ne peut perdurer indéfiniment. Une solution proposée dans le courant des années 80 fut d'améliorer l'utilisation du réseau routier. La connaissance en temps réel du trafic routier et des incidents qui s'y produisent devraient permettre d'optimiser l'utilisation de ce réseau en organisant les flux de circulation (affectation de voies, mise en place d'itinéraires de délestage ou de déviation, fermeture de voies, etc.), en maintenant ou en rétablissant des conditions normales de circulation, et en apportant une aide aux voyageurs (1).

1.1.2 Construction d'un réseau de gestion du trafic

La mise en place d'un système informatique de gestion de la route consiste à recueillir des informations provenant de plusieurs sources (boucles de comptage, capteurs, patrouilleurs, RAU - Réseau d'Appel d'Urgence- etc.), de détecter et de traiter les situations particulières, afin de mettre en œuvre des actions permettant une certaine fluidité du trafic routier. Les informations recueillies par les capteurs sont de natures diverses car regroupent des données de trafic proprement dites c'est à dire : taux d'occupation, vitesse, débit, distances intervéhicules, silhouette, poids du véhicule ; des données météorologiques, par exemple présence de neige, verglas, vent ; ou relatives à des événements perturbateurs tels que : chantiers, accidents, manifestations (4). S'ajoutent à ces dernières, la surveillance vidéo de points particuliers ainsi que la gestion d'installations plus complexes comme la ventilation de grands ouvrages comme les tunnels.

Ces divers équipements : capteurs, PMV - Panneau à Message Variable -, PAU –Poste d'Appel d'Urgence - etc., sont reliés par des liaisons duplex, semi-duplex ou simple à différents postes d'exploitation, les centres d'exploitation autoroutiers, d'entretien et de gendarmerie. L'ensemble des éléments permettant la transmission de données entre le centre d'exploitation, le PC Central, et les équipements dynamiques constitue le réseau de transmission (3).

1.1.3 Les protocoles de communications

Pour permettre l'échange de données entre les différents équipements électroniques et les centres d'exploitation, il convient d'utiliser un protocole de communication qui est un jeu de règles pour la transmission de messages codés entre deux équipements électroniques (2). Le protocole de communication peut être «spécifique » et en dehors de tout standard, on le qualifie de «propriétaire » ou bien il peut s'appuyer sur des standards de l'ISO – International Standard Organisation - reconnus à plus ou moins grande échelle.

1.2 CREATION DES PROTOCOLES STANDARDS DE COMMUNICATIONS AMERICAINS

1.2.1 Les problèmes rencontrés

Aux Etats-Unis, la surveillance et la gestion du réseau routier sont partagées entre plusieurs gestionnaires (le terme employé aux Etats Unis est agence). Chaque constructeur vend aux agences ses équipements électroniques routiers et logiciels avec ses propres spécifications, et utilise un protocole de communication propriétaire pour les échanges de données. Il est ainsi difficile de rajouter de nouveaux équipements, développés par un autre constructeur, ayant un autre protocole de communication, sur un système existant. **L'incompatibilité** technique et fonctionnelle des équipements risque de conduire à des monopoles industriels freinant l'ouverture des marchés. Pour les agences, les conséquences majeures sont un coût plus élevé et la **non interopérabilité** des systèmes informatiques de gestion de la route entre agences adjacentes !

1.2.2 Solution proposée

Afin d'y remédier, the FHWA – the Federal HighWay Administration - a encouragé et financé la concertation (qui a eu lieu en mai 1993) entre les différents gestionnaires et NEMA - the National Electrical Manufacturers Association - dans le but de recenser les problèmes rencontrés pour le bon déploiement d'ITS, the Intelligent Transport System. Dés 1992, NEMA avait commencé des études sur ce sujet. Il apparaît au cours de cette concertation, que la priorité des priorités devait être mise sur la création d'un protocole de communication standard, calqué sur le modèle OSI, sur lequel les industriels puissent se baser. D'autre part, ce protocole devrait être capable de prendre en compte, à terme, la totalité des divers équipements électroniques routiers : capteurs de chaussées, feux de circulation, caméras, dispositifs de contrôle d'accès, etc. (2).

1.2.3 Objectifs à atteindre

Des groupes de travail ont été créés ayant pour objectif d'élaborer ce standard de communication, appelé NTCIP, The National Transportation Communication for ITS Protocol. Le but de NEMA étant de faire des réseaux privés routiers des systèmes ouverts permettant :

- La compatibilité de tout équipement électronique routier respectant ce standard ;
- L'interopérabilité entre les différentes architectures de réseaux des agences ;
- La flexibilité, c'est à dire l'intégration des technologies futures avec un impact minimum sur les systèmes actuels ;

- La possibilité d'être fonctionnel sur des architectures de réseaux déjà existantes.

En fait, l'objectif est bien plus ambitieux. Les concepteurs de NTCIP s'attachent à définir l'ensemble du système de gestion à travers des documents globaux décrivant le cadre dans lequel NTCIP est développé, et des documents spécifiques traitant chaque type d'équipement électronique routier existant, c'est à dire les contrôleurs de feux et de caméra, les boucles de comptage, les Panneaux à Message Variable etc. S'ajoutent à ces derniers les recommandations pour les diffusions radio, pour les messages diffusés entre centres d'administration ainsi que dans les transports en commun. Les documents globaux servent à définir comment utiliser, maintenir ou changer les protocoles standards de communications, de gestion, et qui en a la responsabilité. La deuxième série de documents appelés documents spécifiques, sont des recommandations afin que chaque équipement routier puisse répondre aux besoins et aux attentes des gestionnaires.

1.2.4 Les premiers résultats

La préoccupation initiale du comité de pilotage NTCIP fut de définir le standard pour le contrôle des feux de circulation. En décembre 1995, le premier protocole de communication NTCIP élaboré pour la gestion des feux de circulation voit le jour. Ce premier protocole, *Class B protocol*, ne prend en compte que les équipements électroniques traitant les données des feux de circulation spécifiques à la réglementation américaine.

Les groupes de travail s'attachent actuellement, attendu fin 1997 et courant 1998 (voir annexe), à définir toutes les informations utiles, c'est à dire celles qui permettraient de contrôler les caméras, les dispositifs de contrôle d'accès, les PMV, celles provenant des capteurs pour le diagnostic des conditions routières, ainsi que les types de messages pour les radios, entre centres d'administration et dans les transports publics. En parallèle de nouveaux protocoles sont en cours de développement destinés à couvrir tous les types de communication pour la gestion de la route:

Class A protocol : Similaire au *Class B protocol* mais prend en compte le routage.
Class C protocol : Similaire au *Class A protocol* mais en mode connecté avec la possibilité de transfert de fichier.
Class D protocol : Pour les communications de type «dial up » sécurisé.
Class E protocol : Pour réaliser des transferts de données entre centres.

Ces développements sont récents, seul le *Class B protocol* est en démonstration - aucun des protocoles NTCIP ne fonctionnent sur le terrain - mais FHWA et NEMA effectuent à l'heure actuelle un forcing afin que ces protocoles de communications soient reconnus par toutes les agences américaines. Un effort est effectué en direction de la communauté internationale et de l'OSI afin qu'il s'impose comme un standard dans les systèmes de gestion de la route. Actuellement, les cahiers des charges de certaines agences américaines spécifient que les systèmes de gestion de la route doivent pouvoir supporter les protocoles NTCIP. Cet ouvrage se propose d'expliquer les différents protocoles issus de NTCIP, d'analyser l'implémentation de ces protocoles dans les systèmes de gestion de la route existants.

2 FAMILLE DE PROTOCOLES NTCIP

2.1 PRELIMINAIRE

Pour répondre à la diversité des architectures réseaux et aux besoins des gestionnaires, le comité de pilotage NTCIP a défini plusieurs stacks qui sont des ensembles de protocoles réunis constituant un profil portant sur plusieurs couches du modèle OSI. Ces profils appartiennent au groupe des protocoles de communications de NTCIP. Ils sont au nombre de quatre, classes A, B, C et E, et fournissent un ensemble d'outils permettant d'offrir un éventail de services comme la scrutation : *polling*, l'envoi de commandes et le transfert de fichiers. Si des besoins nouveaux apparaissent, d'autres profils y répondant, pourraient voir le jour. Notamment, un autre profil est en cours développement (il n'existe pas à l'heure actuelle de document traitant de ce profil), le profil de classe D, 'D'ial-up communications. Il aura la charge de faciliter les communications de type «dial up » sécurisé.

2.2 LES DIFFERENTS PROFILS

Ces profils sont établis à partir du modèle OSI, de la façon suivante :

	PROFILS			
	CLASSE A	***CLASSE B***	***CLASSE C***	***CLASSE E***
APPLICATION	STMP	STMP	SNMP Telnet, FTP	SNMP Telnet, FTP
PRESENTATION	Pas de couche présentation			
SESSION	Pas de couche session			
TRANSPORT	UDP	Pas de couche transport	TCP	TCP
RESEAU	IP	Pas de couche réseau	IP	IP
LIAISON	PMPP	PMPP	PMPP	PPP
PHYSIQUE	EIA 232 E FSK	EIA 232 E FSK	EIA 232 E FSK	EIA 232 E

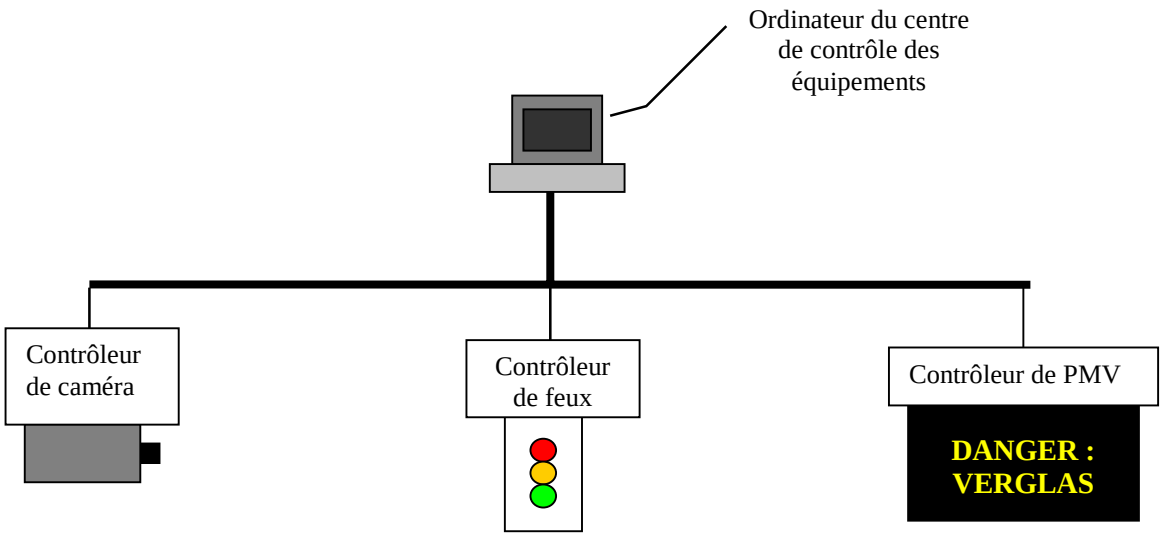
1. Tableau: Les différents profils.

Avant de développer en détail les protocoles utilisés, nous allons décrire les fonctionnalités de chacun, et le contexte dans lequel nous pourrions les utiliser.

2.2.1 le profil de Classe B –'B'asic Field Communications-

Le profil Classe B a été le premier développé par le groupe de pilotage NTCIP en décembre 1995. Il s'applique à des communications entre équipements routiers et stations de supervision. Initialement, ce profil était destiné au contrôle des feux de circulation, quatre commandes de feux sur une liaison semi-duplex à 1200 bauds par canal ou huit commandes de feux sur une liaison duplex. Depuis son champ d'action s'est étendu, et il peut prendre en compte tous les contrôleurs d'équipements électroniques routiers sur des liens bas débits. C'est un protocole de communication directe entre le «maître », le P.C., et les équipements électroniques **connectés sur le même lien physique ou canal**, à faible débit : 1200 bauds (pouvant aller jusqu'à 4800 bauds). Il ne prend pas en compte la fonction de routage. Ce profil a été conçu pour effectuer de la scrutation, *polling*, c'est à dire envoi de messages de type questions réponses avec comme priorité **un délai de transmission rapide**. NTCIP spécifie que 62 équipements de terrain au plus peuvent être «adressables » sur un même canal de communication. Dans la pratique un cycle de scrutation sur 62 équipements se révèle suffisant.

Pour atteindre cet objectif, le profil classe B est un protocole de communication basé seulement sur trois couches du modèle OSI, couches physique, liaison et application, permettant ainsi de réduire considérablement la charge protocolaire de chaque message et donc augmenter la vitesse. La liaison est non fiable car il n'y a pas d'acquittement de la part du destinataire des messages reçus. La trame défectueuse est détruite, sa retransmission doit être gérée par l'application. Ce protocole convient pour les types d'architecture de réseau dont les équipements électroniques routiers nécessitent une faible puissance de traitement ou bien, une capacité de communication à faible vitesse.

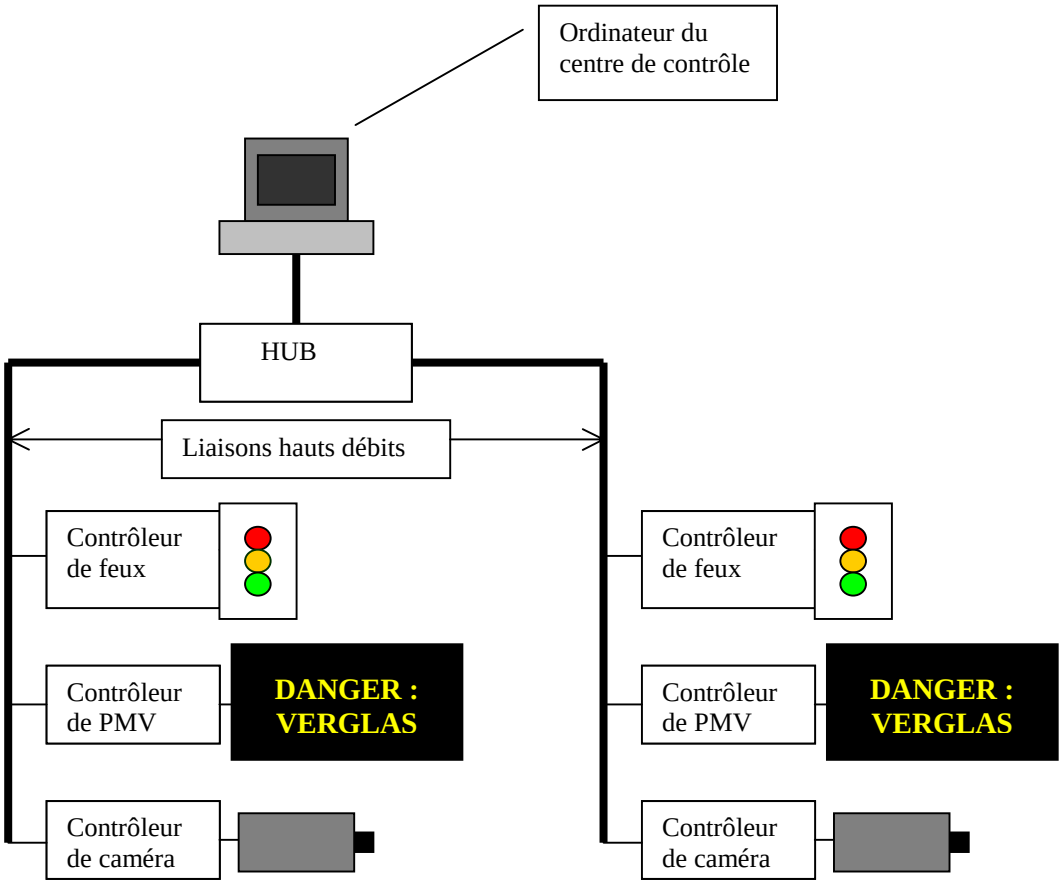


2. Le profil de classe B

2.2.2 Le profil de Classe A –'A'dvanced Field Communications-

Le profil de Classe A remplit les mêmes fonctions que le profil de Classe B, mais en y adjoignant **la notion de routage**, les équipements de terrain peuvent être sur le même lien physique ou sur des liens physiques différents. Il convient donc à tout type d'architecture réseau grâce à cette notion de routage. La liaison, entre les stations de contrôle et les équipements électroniques routiers via des contrôleurs intermédiaires, comme par exemple des concentrateurs ou routeurs, est établie en mode non connecté. Son premier usage est donc le transfert de données quand le routage s'avère nécessaire, et pour des transferts de données à haut débit.

Ce profil est constitué de cinq des sept couches du modèle OSI, à savoir les couches physique, liaison, réseau, transport et application. Une particularité de ce profil est qu'il repose sur le protocole UDP pour la couche transport. Ceci signifie que les données ne sont pas assurées d'arriver à bon port et exemptes d'erreurs. Le contrôle d'erreur ainsi que la récupération des données devront être des services gérés par la couche application. Le PMPP - Point to Multi Point Protocol- est le protocole de la couche liaison (comme pour les classes B et C) donc un message peut être envoyé en même temps à plusieurs destinataires.



3. Le profil de classe A

2.2.3 Le profil de Classe C –'C'onnection Oriented Communications -

Le profil de Classe C a pour rôle principal de fournir des services orientés connexion sur des lignes hauts débits. Avant d'échanger des données l'équipement source établit une connexion (circuit virtuel) avec l'équipement destinataire. L'avantage majeur d'un tel service est la garantie de remise des données au destinataire voulu. En effet, la couche transport utilise le protocole TCP, service orienté connexion avec garantie de remise. Elle a la responsabilité de l'intégrité des données, libérant ainsi la couche application de cette fonction. En contrepartie, la ligne étant monopolisée, le rendement s'en trouve affecté. Il est utilisé pour les communications entre les stations de contrôle et les équipements routiers qui échangent des données relativement importantes comme les PMV ou les messages radios. Il peut aussi être employé pour des communications entre centres. Il s'appuie sur le protocole de transfert de fichier FTP - File Transfert Protocol- qui est bien adapté à ce type de service.

Ce profil est constitué de cinq des sept couches du modèle OSI, à savoir les couches physique, liaison, réseau, transport et application. Les protocoles supportés par la couche application sont : FTP, Telnet et SNMP - Simple Network Management Protocol -.

2.2.4 Le profil de Classe E –Center to Center 'E'xchange -

Le profil de Classe E est équivalent en terme de services au profil de Classe C. Il supporte aussi les applications FTP et SNMP. La différence réside au niveau de la couche 2 du modèle OSI car le profil de Classe E utilise le protocole PPP - Point to Point Protocol -. Il a été conçu pour répondre aux demandes de connexions large bande entre deux sites distants sur une liaison point à point. Ce profil est issu en totalité des standards de la communauté Internet.

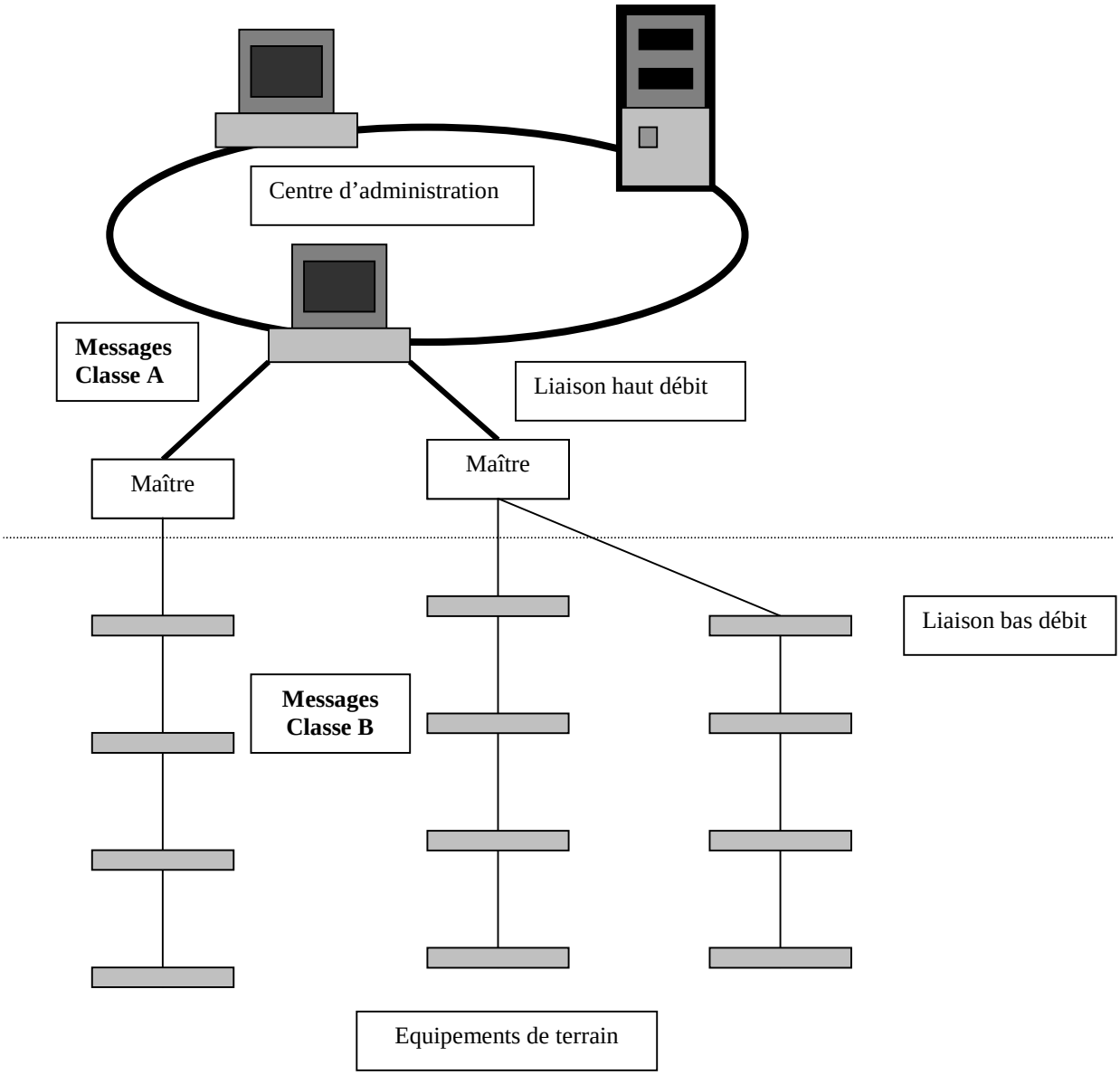
2.3 EXEMPLES D'ARCHITECTURES RESEAUX POSSIBLES BASEES SUR LES PROTOCOLES DE COMMUNICATIONS NTCIP

La diversité de la famille des protocoles de NTCIP offre un éventail de communication entre équipements allant du mode connecté à non connecté, et de bas débit à haut débit. Une propriété intéressante des réseaux dont profitent les architectures réseaux NTCIP, demeure **la possibilité de faire coexister les multiples profils, définis précédemment, sur le même lien physique**. L'unité logique de l'équipement se conformera à chacun des profils qu'elle rencontrera. De plus, certains équipements comme un ordinateur maître, connecté à deux brins supportant des profils différents, a la faculté de renvoyer l'information reçue sur le brin suivant dans le format approprié. Tous les scénarios d'architectures réseaux peuvent dés lors être envisagés.

Nous allons représenter quelques exemples d'architectures réseaux rencontrés aux Etats Unis en considérant NTCIP comme le protocole de communications.

2.3.1 Le système en boucle fermée

C’est le système le plus traditionnel avec une machine maître contrôlant plusieurs équipements de terrain. Sur le schéma suivant, un centre d’administration envoie ces requêtes aux équipements de terrain (contrôleur PMV, caméra et feux tricolores etc.) via des ordinateurs maîtres. Ces derniers recueillent les données provenant des équipements de terrain et les dirigent vers le centre d’administration.

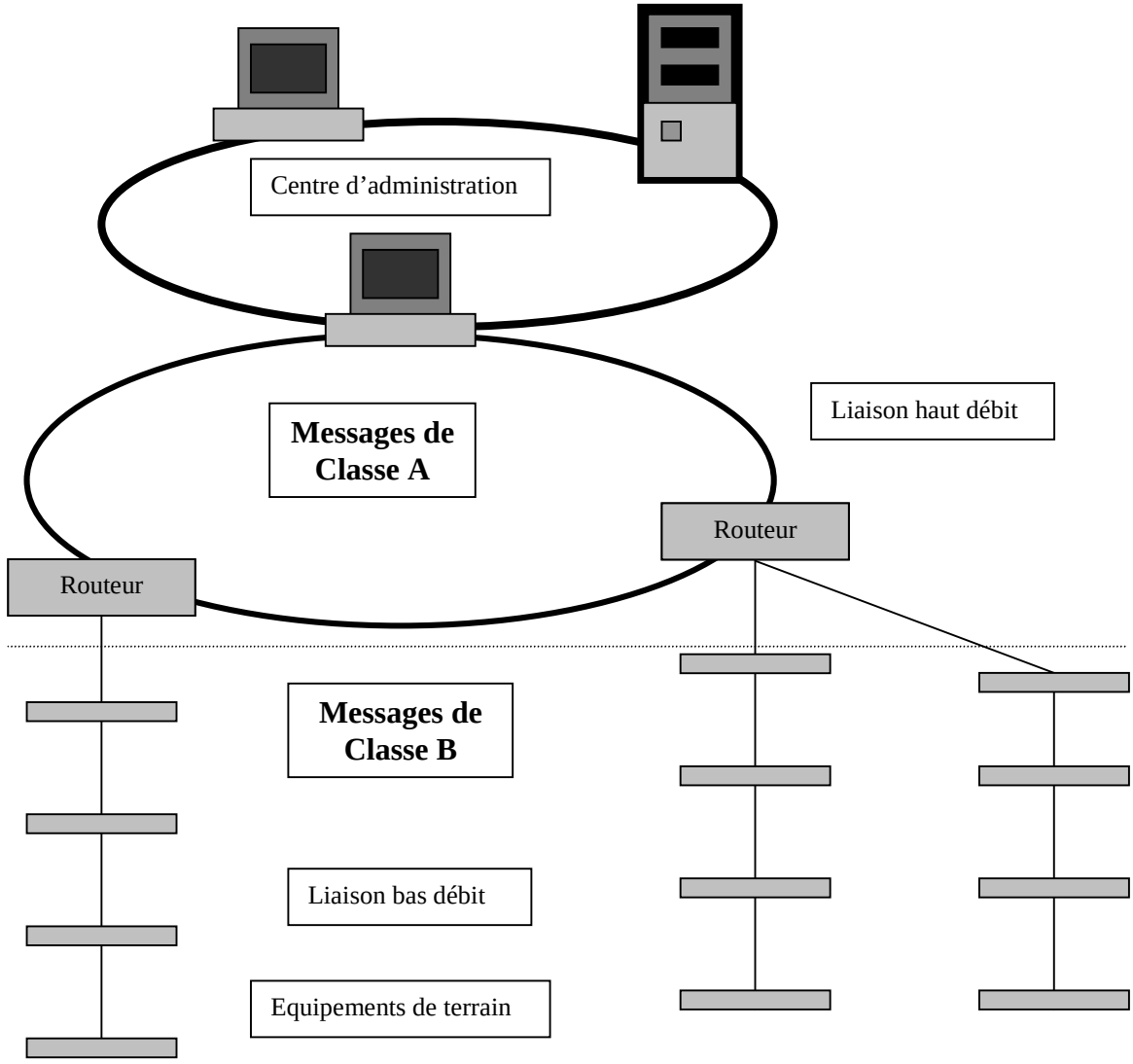


4. Le système en boucle fermée

2.3.2 Système distribué avec infrastructure bas débit

Cette configuration permet de distribuer les messages provenant du centre d'administration vers un routeur, connecté d'égal à égal (peer to peer) sur le deuxième anneau, qui se charge de les transmettre aux équipements locaux concernés.

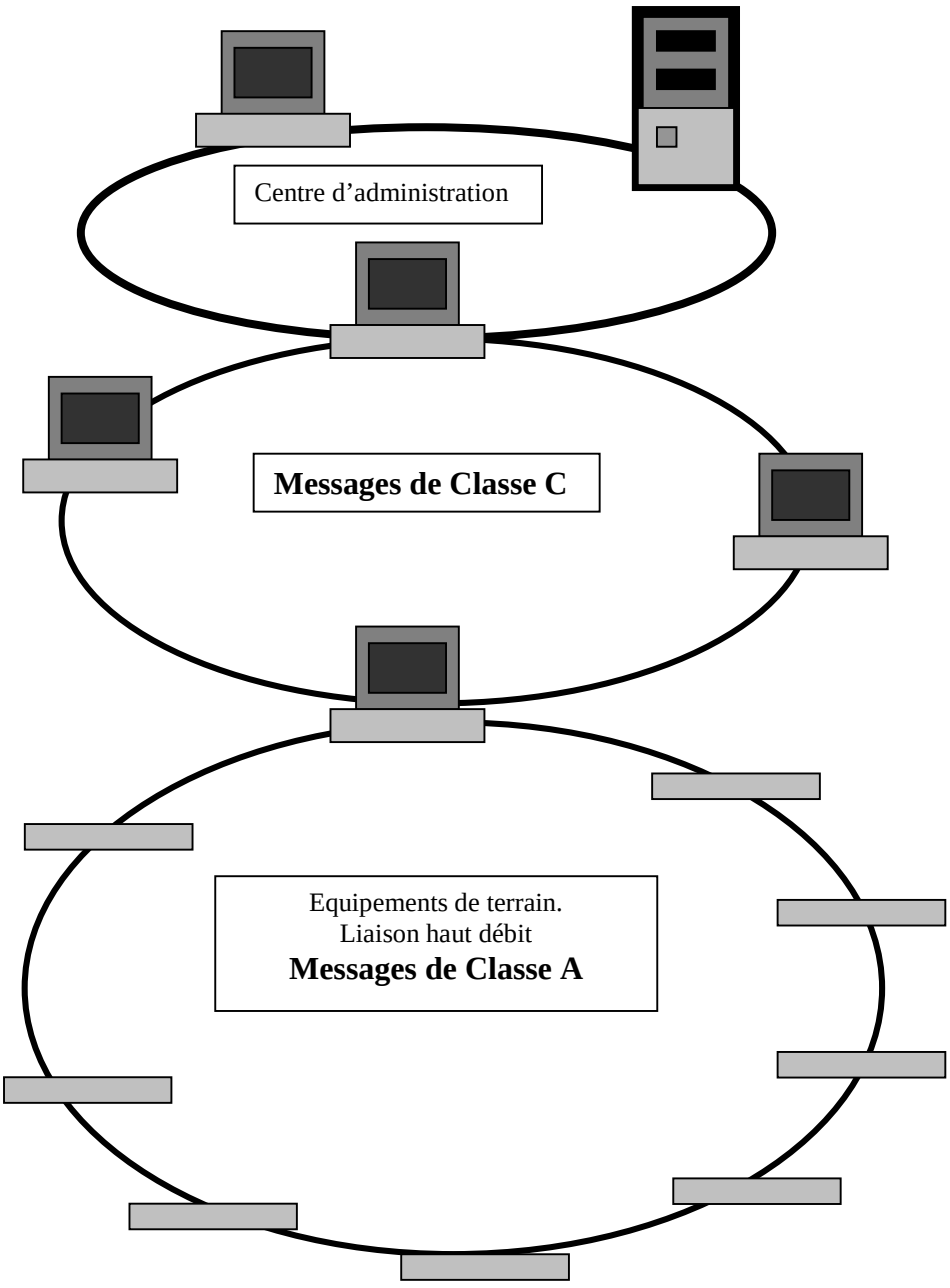
Cette architecture demeure cependant une solution intermédiaire appelée à évoluer vers un système plus performant où les équipements de terrain seraient directement connectés sur des liaisons hauts débits.



5. Système distribué avec infrastructure bas débit

2.3.3 Système distribué avec infrastructure haut débit

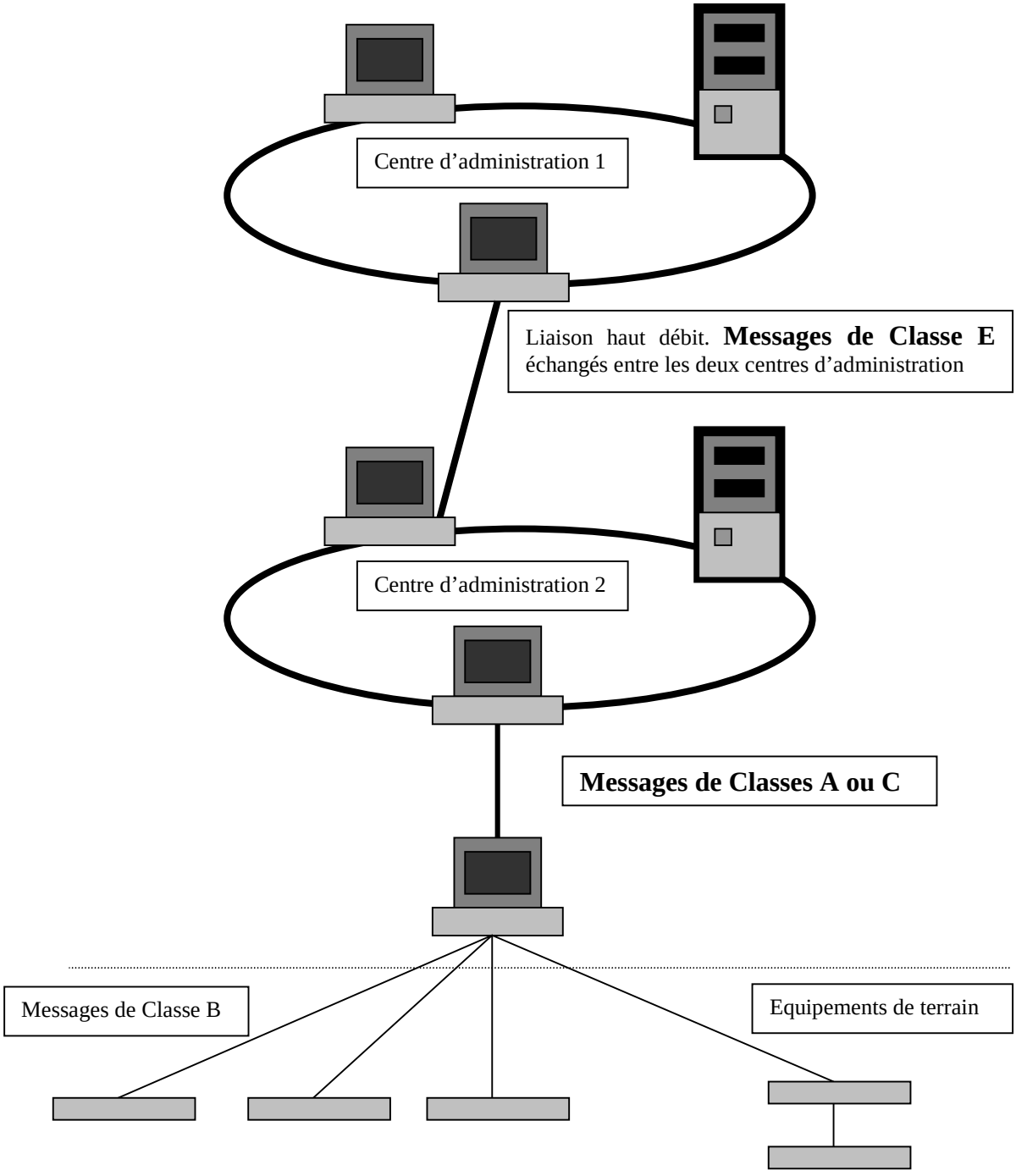
Il s'agit d'une architecture réseau identique à la précédente mais supportant des liaisons hauts débits, tous les équipements reçoivent des messages de classe A. Le centre d'administration communique avec chaque équipement maître d'un sous réseau par des messages de classe C. Cet équipement maître contrôle tout un sous réseau d'équipements de terrain.



6. Système distribué avec infrastructure haut débit

2.3.4 Système à architecture centralisée traditionnelle

Ces systèmes conviennent pour l'interconnexion entre différents gestionnaires. Deux centres d'administration peuvent cogérer un groupe d'équipements locaux. Dans l'exemple qui suit, le centre d'administration 1 est connecté au centre d'administration 2 par une liaison à haut débit reposant sur le protocole PPP. Grâce aux protocoles de sa couche application – en particulier FTP – les échanges de données sont permis et s'effectuent de façon fiable (protocole de transport : TCP). Pour des raisons de coûts, les liens physiques entre la station maître et les équipements de terrain supporteraient uniquement le profil de Classe B donc des liaisons bas débits.

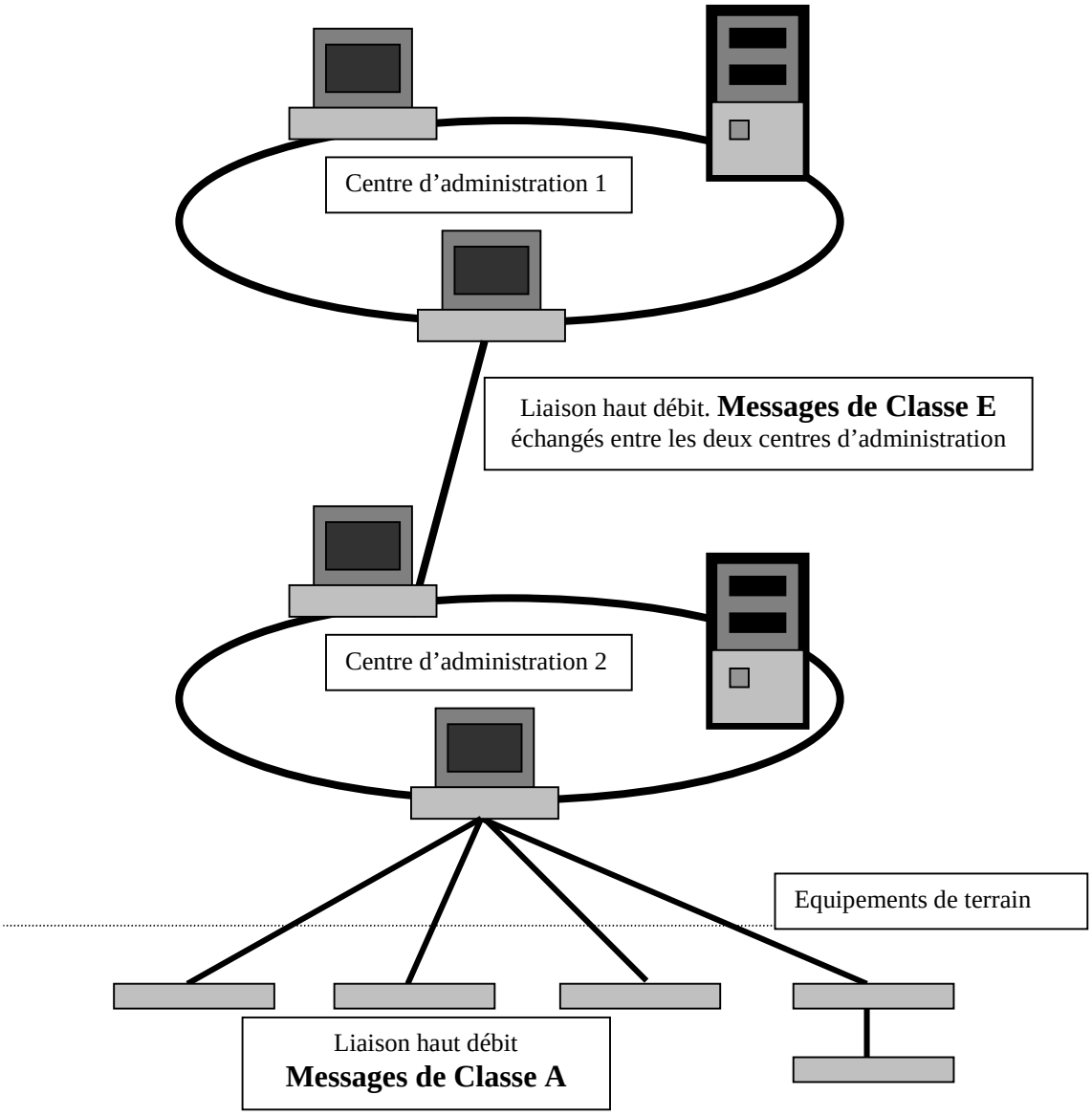


7. Système à architecture centralisée traditionnelle

L'avantage d'un tel système, puisque chaque station de centre d'administration a une adresse Internet, est la possibilité de construire un réseau dans lequel toutes les agences seraient connectées entre elles à la manière du réseau Internet. Bien que cela ne soit pas dit dans les spécifications de NTCIP, le raccordement des centres d'administration via Internet est facilement réalisable.

2.3.5 Système à architecture centralisée avancée.

C'est le même type de système que le précédent, mais les liens physiques entre la station maître et les équipements de terrain supportent le profil de Classe A. L'ordinateur maître est relié directement aux équipements de terrain par des lignes dédiées.



8. Système à architecture centralisée avancée

2.4 CONCLUSION

Au niveau des couches basses des réseaux, NTCIP utilise des protocoles issus des standards de l'Internet. Plusieurs types d'architectures basés sur ces protocoles peuvent être envisageables. Nous allons nous intéresser, au chapitre suivant, à l'administration de ces réseaux. NTCIP s'appuie pour la gestion des équipements de terrain sur un protocole standard dans l'administration des réseaux LAN ou WAN.

3 L'APPROCHE OBJET DE NTCIP

3.1 LE PROTOCOLE SNMP

La famille des protocoles de communications NTCIP utilise pour la gestion et le contrôle des équipements de terrain le protocole du niveau application SNMP – Simple Network Management Protocol –, et STMP –Simple Transportation Management Protocol-.

Dans ce chapitre nous nous intéresserons au concept du protocole SNMP qui est un standard pour l'administration des réseaux. Nous essaierons de détailler les grandes lignes de l'administration de réseaux par l'intermédiaire du protocole SNMP.

3.1.1 Un peu d'histoire …

En mars 1987, la communauté Internet constate que la fameuse toile d'araignée s'étend, entraînant une croissance exponentielle des nœuds de la toile qui sont eux-mêmes gérés par des équipements hétérogènes. Afin de ne pas se laisser déborder dans la gestion du réseau, cette communauté décide de renforcer son contrôle dans la supervision des nœuds de la toile. Il convient d'établir un standard de supervision auquel les constructeurs d'équipements devront se soumettre. Dès le mois de mai de la même année les différents organismes IAB - Internet Architecture Board- et ISO élaborent ce standard nommé SNMP/CMOT. Deux ans plus tard, des divergences apparaissent entre ces deux organismes. Le pragmatisme SNMP de l'IAB s'oppose au formalisme CMIP de l'ISO. Chacun travaille donc sur son propre protocole, l'IAB sort dès la fin 1989 ses premiers produits SNMP qui deviennent un véritable standard du marché l'année suivante.

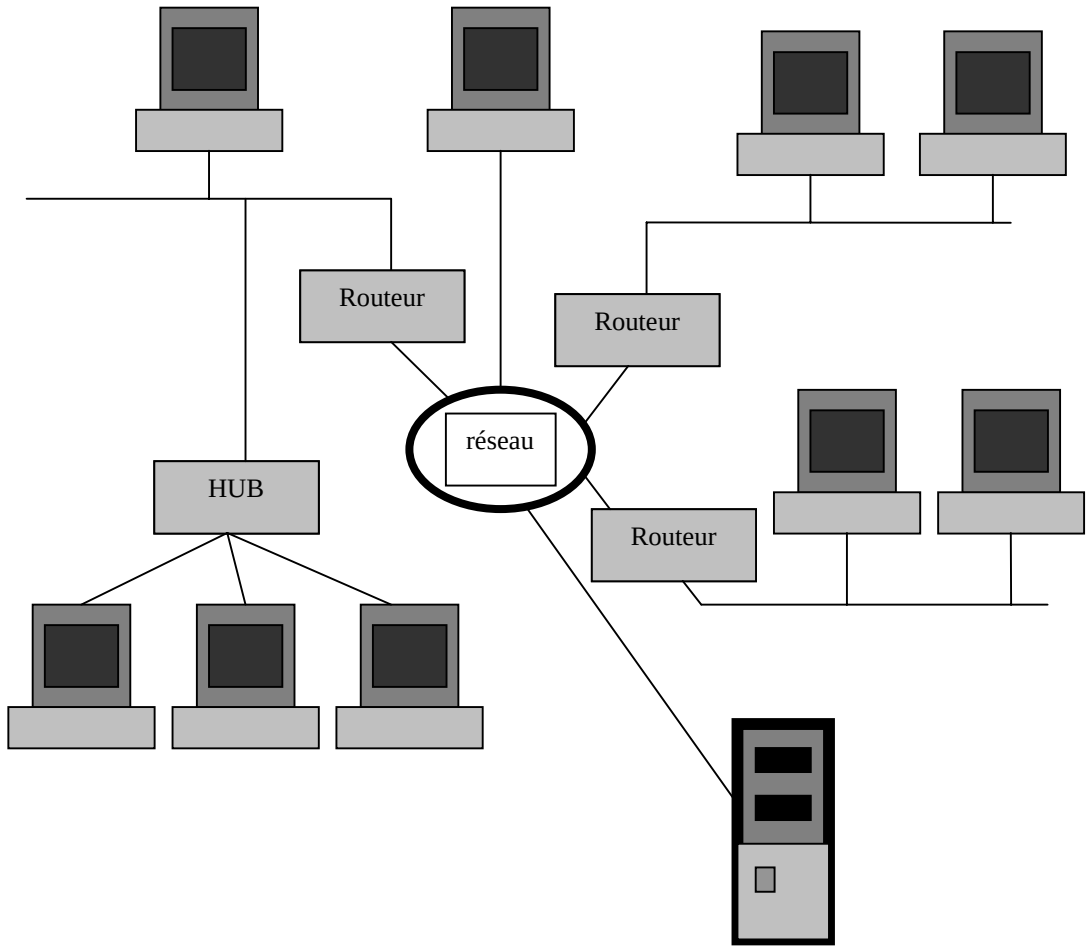
L'ISO quant à elle, sort ses protocoles CMIS/CMIP, CMOT qui n'ont cependant pas le même succès auprès des usagers que SNMP. **SNMP est un protocole définissant un ensemble de règles pour l'administration d'un réseau hétérogène. Il permet donc de superviser toutes les gammes de matériels de tout constructeur et ainsi améliore l'administration du réseau**.

Administrer un réseau consiste à maintenir le fonctionnement du réseau de façon continue conformément à la qualité de service définie, c'est à dire :

- le gérer ;
- l'optimiser ;
- le configurer ;
- le sécuriser ;
- l'observer ;
- et enfin le corriger.

3.1.2 Mise en place de SNMP

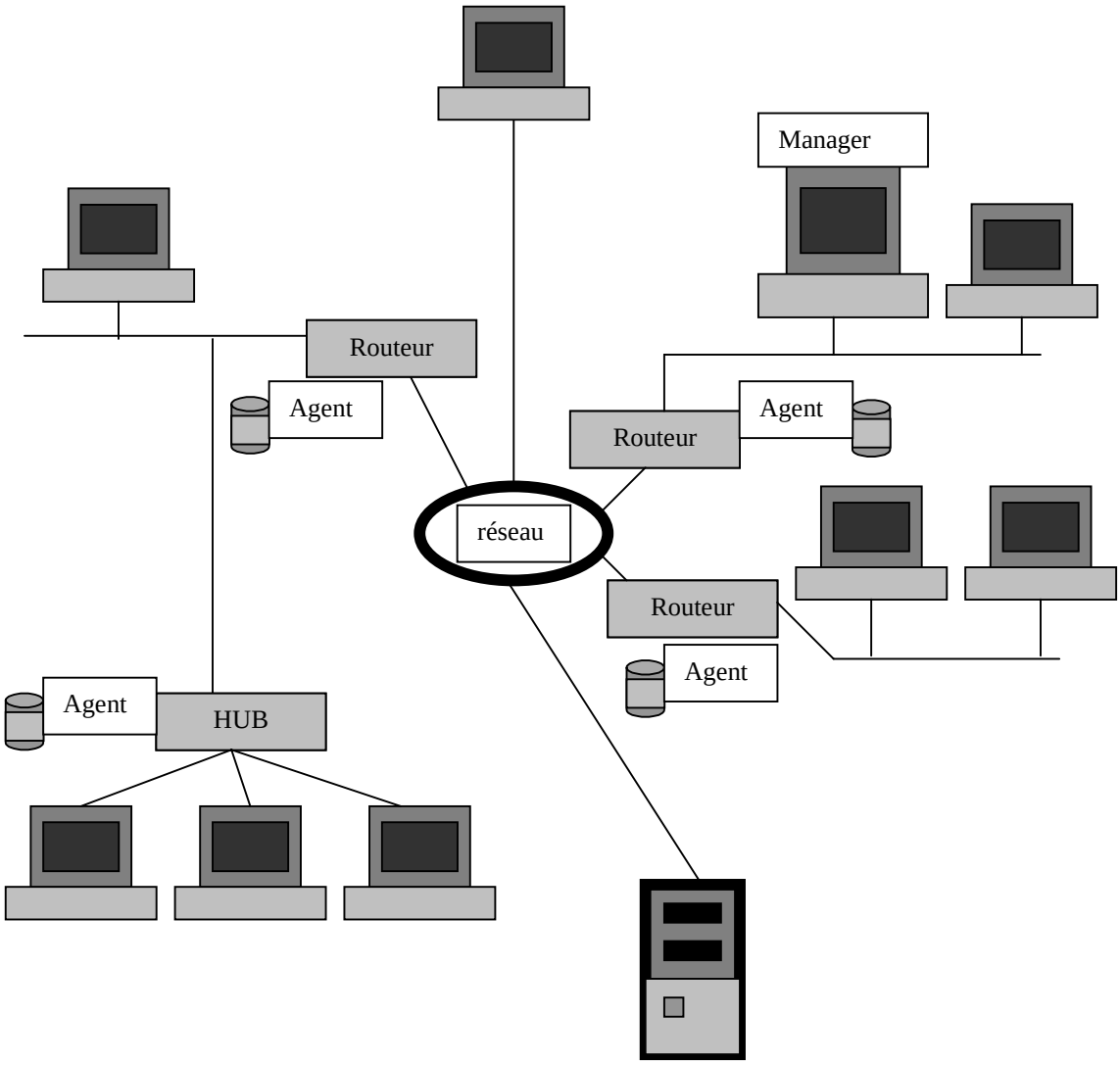
Le protocole SNMP s'avère indispensable face aux architectures réseaux des années 90 plus complexes et hétérogènes comme représenté ci-dessous :



9. Architectures réseaux des années 90

Les réseaux des années 90 reposent sur le concept Client - Serveur. Le client n'est autre qu'un poste de travail, les applications étant en général sur les serveurs. L'idée de SNMP fut d'installer des «agents » sur les points stratégiques -les routeurs- du réseau. Le rôle des agents est de superviser le bon fonctionnement de ces nœuds névralgiques et d'informer l'administrateur lorsqu'un événement de nature critique s'y produit. D'autre part, ces derniers relèvent les statistiques réseaux du nœud dont ils ont la charge. Lorsqu'une panne réseau survient, la tâche de l'administrateur se trouve facilitée grâce aux informations recueillies par les agents.

En adjoignant le protocole SNMP sur l'architecture du réseau de l'exemple ci-dessus, nous obtenons la configuration suivante :



10. Contrôle par SNMP des architectures réseaux des années 90

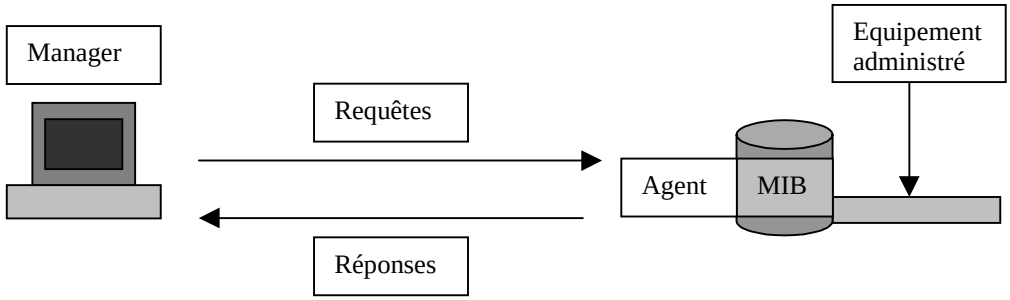
Des informations sont échangées entre la station de supervision – manager – et les entités gérées par les agents SNMP sur le réseau.
Agent SNMP : logiciel implémenté sur l'équipement administré.
Manager SNMP : station d'administration.
MIB – Management Information Base - : Ensemble des objets nécessaires pour l'administration d'un équipement réseau. Base d'information administrative. ***Elle est maintenue par l'agent, et consultée et mise à jour par l'administrateur***.

3.2 FONCTIONNEMENT DE SNMP

Toute entité administrée (routeur, pont, etc.) doit tenir à jour des informations d'état accessibles pour la station de supervision qui a en charge l'administration du réseau. Ces informations peuvent être de natures diverses, un routeur par exemple fournira des statistiques

relatives à l'état de ses interfaces, aux messages d'erreurs émis, au trafic entrant et sortant et aux datagrammes détruits. La station de supervision «interroge les agents installés sur les entités administrées » par des commandes - les requêtes - afin de relever les informations et de détecter les dysfonctionnements des branches de ce réseau.

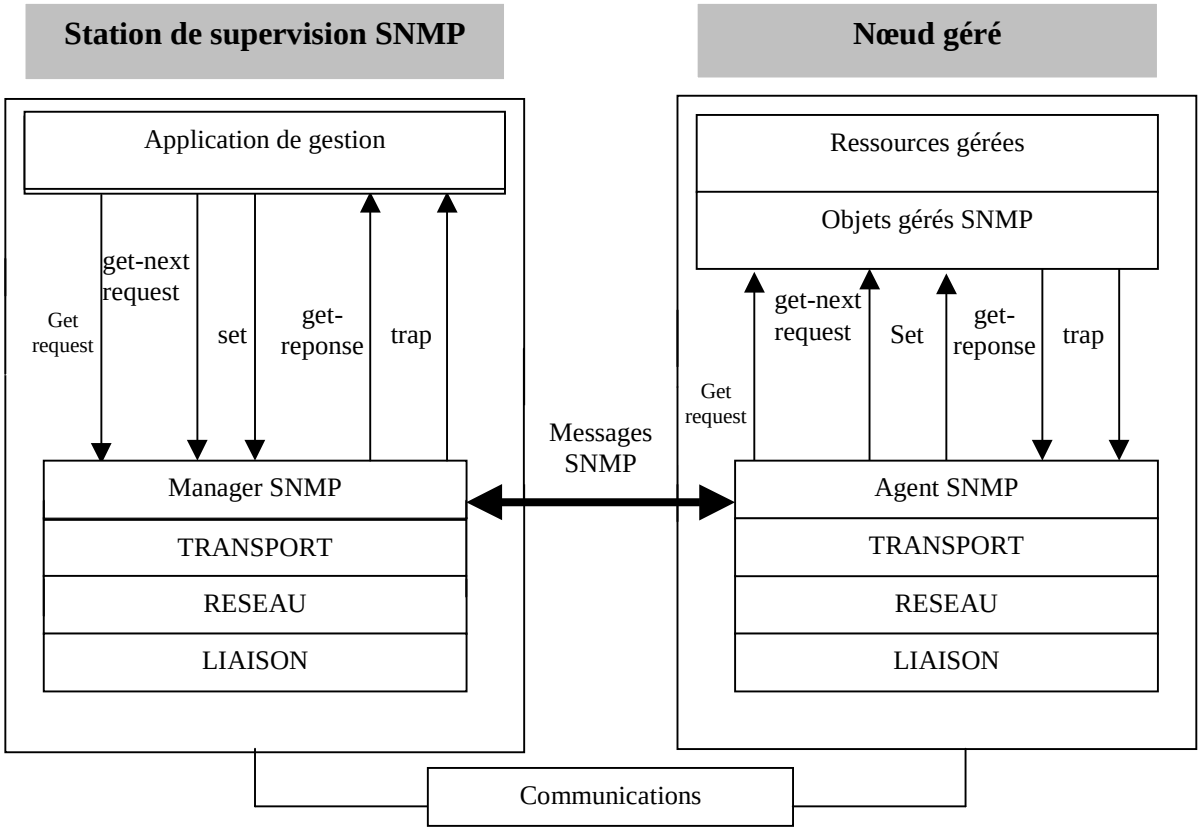
Le protocole SNMP repose sur ce principe :



11. Fonctionnement de SNMP

3.2.1 Les commandes SNMP

SNMP permet à la station de supervision d'accéder aux statistiques des entités administrées par l'intermédiaire de cinq commandes appelées – primitives – du protocole SNMP :

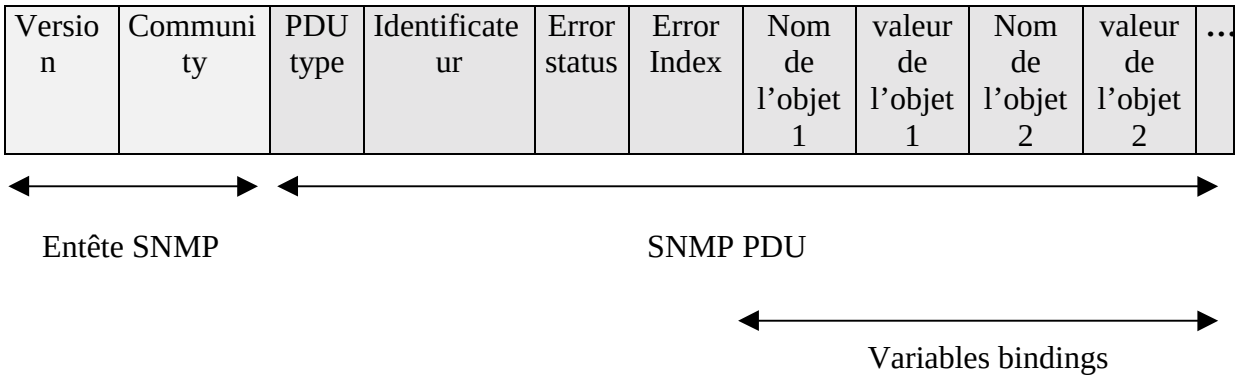


12. Les commandes SNMP

Les commandes, *get request* et *get reponse*, permettent de rechercher une valeur particulière et d'obtenir la valeur de cette variable. La commande *set* est réservée pour la modification de la valeur d'une variable de la MIB. La commande *get nest request* permet de rechercher la valeur d'une variable sans connaître son nom exact. La commande *trap* est une commande d'alerte générée par l'occurrence d'un événement (par exemple, un problème rencontré au niveau du nœud géré).

3.2.2 Le PDU –Protocol Data Unit- de SNMP

Il existe actuellement deux versions de SNMP. La structure du message SNMP est représentée ci-dessous et correspond à la version 1 de SNMP :



Variables bindings : paire de valeurs (identifiant de l'objet, valeur pour cet objet).
Version : Version de SNMP.
Community : Relation entre un agent SNMP et les managers (private ou public).
PDU type : Indique le type de PDU encapsulé dans le message SNMP. Le tableau ci-dessous indique les valeurs prises par ce champ suivant les requêtes envoyées :

Type PDU	NOM
0	get-request
1	get-next-request
2	set-request
3	get-response
4	Trap

Les quatre premiers types de PDU définis dans le tableau ci-dessus partagent la même structure. Le type PDU Trap a une structure légèrement modifiée.

Identificateur ou Request ID : Permet de distinguer les requêtes en attente.
Error status : Spécifie un code d'erreur du message.
Error Index : Une valeur non nulle indique que l'objet référencé dans «variables bindings » est la cause de l'erreur.

3.3 LA MIB

3.3.1 Quelques définitions

Les MIBs jouent un rôle essentiel dans le protocole SNMP. Ce sont des tables de données qui définissent toutes les informations spécifiques à l'administration de réseaux ainsi que leur signification.

Ces variables (informations spécifiques) sont regroupées dans huit catégories standards définies comme suit (5) :

Catégories	Comprend les informations sur :
System	Le système d'exploitation de la machine ou du routeur
Interfaces	Chaque interface réseau
Addr. Trans.	La traduction d'adresse (correspondance ARP, Address Resolution Protocol)
IP	Le logiciel IP
ICMP	Le logiciel ICMP
TCP	Le logiciel TCP
UDP	Le logiciel UDP
EGP	Le logiciel EGP

13. Les différentes catégories d'objets

Le choix des catégories est important car les identificateurs utilisés pour définir les éléments incluent un code de catégorie. Exemples de variables MIB et de leur catégorie :

Variables	Signification	Catégorie
SysUpTime	Temps écoulé depuis le dernier démarrage	System
IfNumber	Nombre d'interfaces réseaux	Interfaces
AtTable	Table de correspondance adresse MAC-IP	addr. Trans.
IpRoutingTable	Table de routage IP	IP
IpReasmOKs	Nombre de paquets réassemblés correctement	IP
TcpMaxConn	Nombre maximum de connexions TCP permises	TCP
UdpInDatagrams	Nombre de datagrammes UDP reçus	UDP
EgpInMsgs	Nombre de messages EGP reçus	EGP
IcmpInEchos	Nombre de demandes d'écho ICMP reçues	ICMP

14. Exemples de variables

Les objets de la MIB sont de deux types :

- *Objet de type variable simple* : attribut représentant un paramètre de fonctionnement, pour un équipement donné. Cette variable est unique, exemple : IcmpInEchos.
- *Objet de type table* : regroupement de plusieurs variables caractérisant une même ressource ou regroupement de plusieurs ressources de même type sur un équipement donné, exemple : IpRoutingTable.

Ces variables, quel que soit l'équipement administré ou le constructeur, demeurent les mêmes. Il se peut que la MIB d'un constructeur ne contienne pas toutes ces variables, et dans ce cas, lors d'un envoi d'une demande de la part de la station de supervision sur une variable manquante, il y aura renvoi d'un message d'erreur indiquant que cette variable n'est pas disponible. L'IAB a conçu une MIB I dans laquelle tous les objets utiles – 114 au total - sont recensés dans 8 catégories. La MIB II est plus récente, c'est un sur ensemble compatible de la MIB I, 171 objets y sont définis avec l'ajout de trois nouvelles catégories de variables.

Une variable est caractérisée par la manière dont elle est définie, codée, et par son emplacement au sein de l'arborescence ISO. Il y a distinction entre le logiciel d'administration qui est basé sur le paradigme aller chercher - enregistrer et les données (variables) prises en compte. Chacun repose sur un standard distinct, le premier –SNMP- définit le format et la signification des messages échangés ainsi que les destinataires de ces messages, le second spécifie l'ensemble des règles utilisées pour définir et identifier les variables contenues dans la MIB. Dans la suite de ce chapitre, nous allons expliciter ce second standard.

3.3.2 SMI, *Structure of Management Information*.

SMI est un ensemble de règles utilisées pour définir les variables des MIBs et spécifier la structure de l'arbre d'enregistrement de ces dernières. Les objets gérés sont par exemples des ponts, des routeurs, des stations, etc. Ces travaux sont à la disposition du public (RFC 1155) sur le réseau Internet.

3.3.2.1 Représentation des noms d'objets MIBs

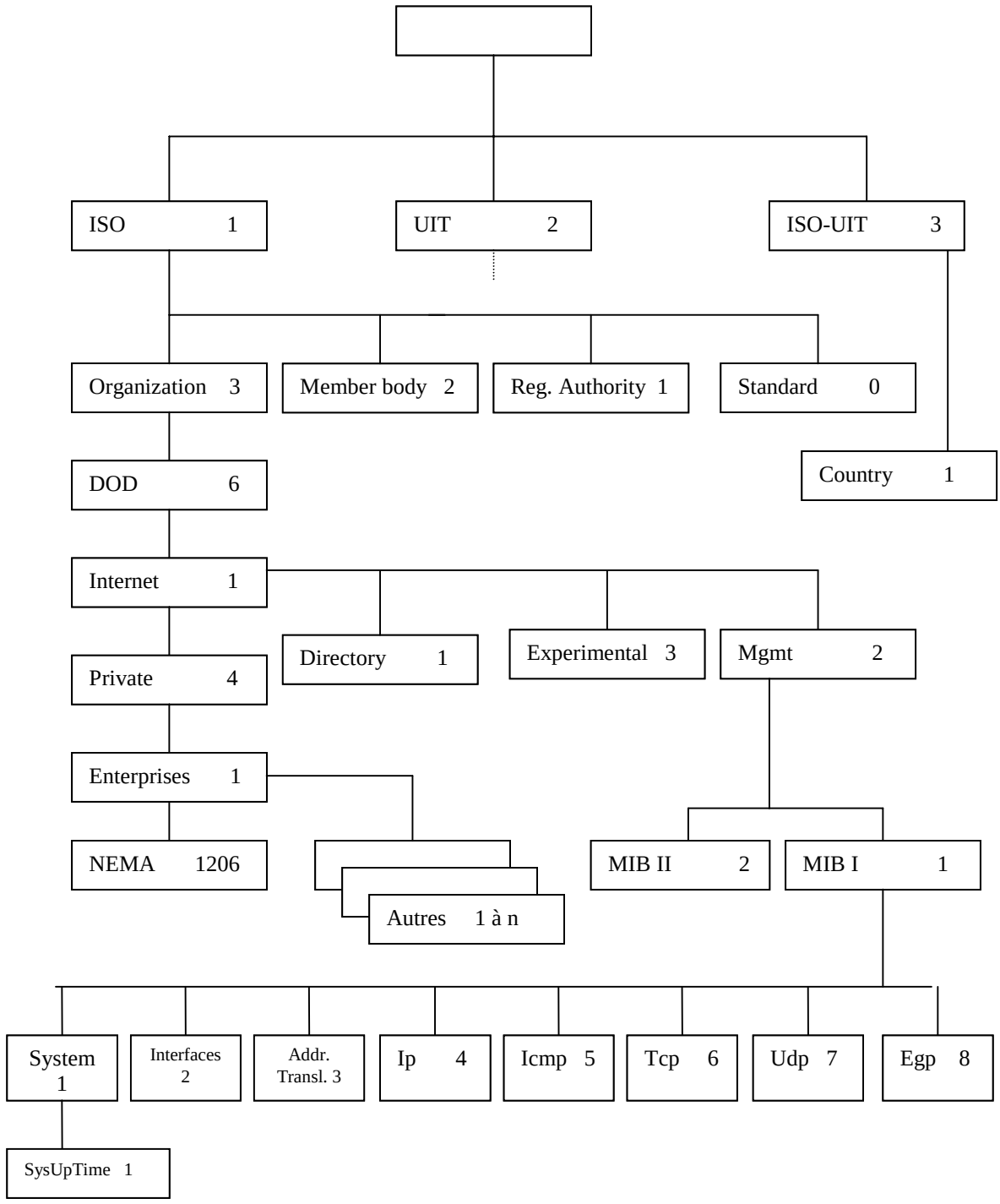
Les noms des variables MIB sont extraits d'un espace de noms d'identificateurs d'objets géré par l'ISO et l'UIT. Le but de cette démarche est de fournir un espace de noms dans lequel tous les objets possibles puissent être nommés. Cet espace de noms d'identificateurs d'objets est structuré de façon à ce que les objets définis demeurent uniques. Cet espace de noms d'identificateurs d'objets est organisé hiérarchiquement, la responsabilité des règles de nommage est décomposée, à chaque niveau, en domaines, ce qui permet à chaque groupe d'avoir la responsabilité du choix de certains noms sans avoir à consulter l'autorité supérieure pour chaque décision (5). Deux possibilités pour identifier les objets sont permises :

- Soit par une chaîne de caractères plus accessible à la personne humaine ;
- Soit par une suite d'entiers, adaptée aux ordinateurs.

Chaque grand organisme – ISO, UIT et ISO/UIT- se sont vus confier une branche de l'espace des noms d'identificateurs d'objets. La racine n'a pas de nom. Pour ce qui nous

concerne, c'est le DOD –Department of Defense- qui a alloué une sous branche à l'IAB afin que ce dernier puisse ranger ses objets.

L'arborescence est définie comme suit :



15. Arborescence OSI

Chaque objet de l'arborescence SMI est identifié par son chemin pour y accéder depuis la racine. Par exemple le chemin d'accès au nœud *management* dans lequel se trouve

les MIB I et II standards est : 1.3.6.1.2 soit littéralement iso.org.dod.internet.management. La variable *system* est donc sur la branche 1.3.6.1.2.1.1. Le chemin pour accéder à la variable *SysUpTime* est : 1.3.6.1.2.1.1.1

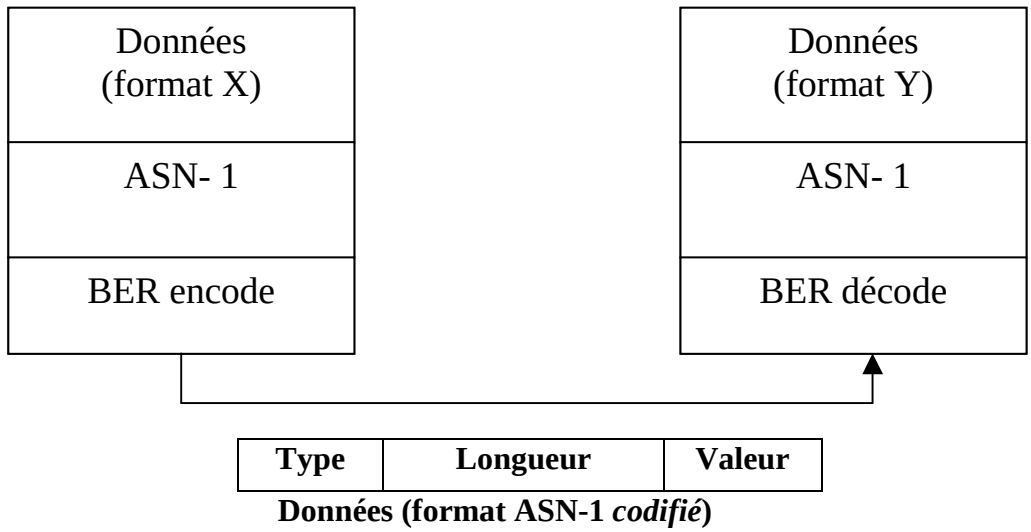
La branche 1.3.6.1.4.1 conduit au nœud *entreprises* ou chaque industriel peut se voir réserver un nœud dans lequel il entrepose ses MIBs.

3.3.2.2 Définition et identification des variables

la MIB ainsi que les objets sont décrits dans un langage macro ASN-1 – Abstract Syntax Notation One – (normes ISO 8824 et ISO 8825, recommandation X208 de l'UIT) qui a la propriété de pouvoir être lu par un utilisateur (texte ASCII) et compilé par un ordinateur. La forme lisible par l'homme peut être directement et automatiquement traduite dans la forme codée utilisée dans les messages. Ce langage procure une méthode standard pour définir un objet, son organisation et son identification. Il définit comment coder le nom et la valeur entière de la variable dans un message SNMP, ainsi que la forme exacte et le domaine des valeurs prises par cet entier. Ce langage, ASN-1, correspond à la couche présentation du modèle OSI. Il est également utilisé, à titre d'exemple, dans la messagerie normalisée X400 ou bien l'annuaire normalisé X500.

3.3.2.3 Codage des variables

Pour faciliter la transmission de données (description de l'objet défini en ASN-1) on utilise un jeu de règles standards, BER – Basic Encoding Rules -, qui code ces données en binaire. Elles sont ensuite décodées au niveau du récepteur puis récupérées sous forme ASN-1, comme représenté ci-dessous :



16. Codage, décodage ASN-1

4 LE PROTOCOLE STMP : SIMPLE TRANSPORTATION MANAGEMENT PROTOCOL

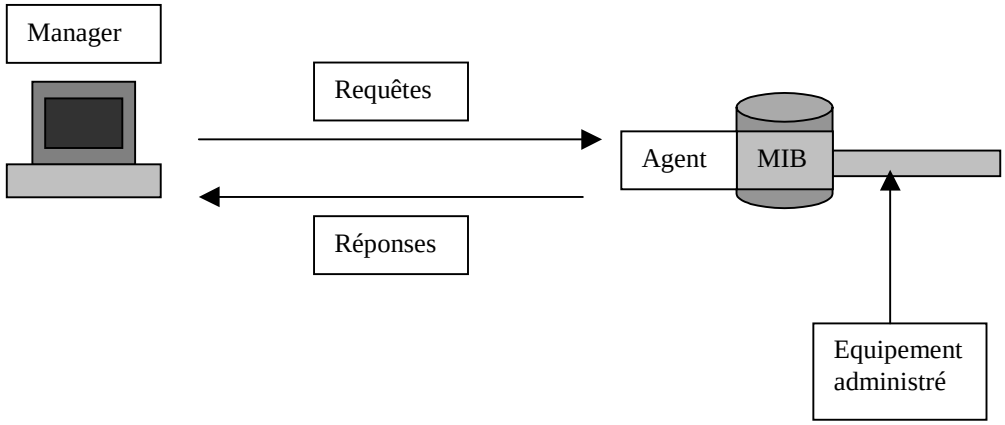
Le comité de pilotage NTCIP a développé autour d'un modèle de management, dérivé de SNMP, toute une série de bases de données, les MIBs, se rapportant au contrôle des feux tricolores, des messages variables, des conseils radios, etc. ainsi que les structures communes et la nomenclature utilisée pour référencer les objets définis.

Ces travaux sont décrits dans un document spécifique STMF – Simple Transportation Management Framework- (6).

4.1 LES ECHANGES DE MESSAGES ENTRE LE MANAGER ET L'AGENT

4.1.1 Principe de STMP

Comme SNMP, STMP établit un dialogue entre le manager et l'équipement administré de la façon suivante :



17. STMP

4.1.2 Les commandes de STMP

STMP repose sur le principe «requêtes – réponses ». Il reprend donc les mêmes commandes que SNMP mais rajoute quatre autres commandes nécessaires pour la gestion des équipements routiers en toute sécurité. Les quatre dernières commandes en italiques du tableau suivant ont été créées pour STMP.

Commandes	Description
Get-request	Lire la valeur d'une variable.
Set request	Affectation d'une valeur à une variable.
Trap	Réponse déclenchée par l'agent suite à l'occurrence d'un événement.
Get-response	Réponse de l'agent suite à une demande de type Get-request du manager.
Set-not reply	Affectation d'une valeur à une variable sans demande de réponse de l'agent.
Set- response	Réponse de l'agent suite à une demande de type Set request du manager.
Set-error-response	Réponse de l'agent indiquant qu'il y a une erreur dans un *Set-request.*
Get –error – response	Réponse de l'agent indiquant qu'il y a une erreur dans un *Get-request.*

18. Commandes STMP.

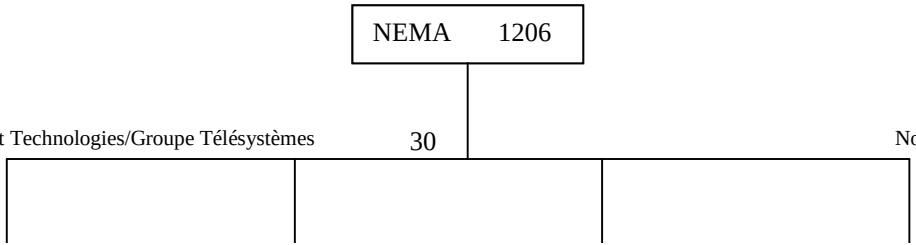
4.2 LES MIBS DANS LE CONTEXTE ROUTIER

L'idée du groupe de pilotage de NTCIP fut d'adapter le mécanisme de gestion des réseaux développé par l'IAB à la gestion des équipements routiers. Il convenait de définir le cadre dans lequel les MIBs allaient s'intégrer et d'élaborer les protocoles du niveau application. Le groupe de pilotage de NTCIP a conservé le protocole SNMP et défini un autre protocole STMP plus adapté à la scrutation.

Chaque équipement routier à une fonction à remplir bien définie. Par exemple, une station de comptage rend compte de la densité du trafic, le contrôleur de feux les cycles des feux tricolores, la station météo la vitesse du vent etc. Ces informations appelées *variables* sont collectées, stockées, consultées et modifiées par les opérateurs à l'aide des protocoles SNMP et STMP. Toutes ces variables peuvent être recensées, c'est à dire, pour une station de comptage par exemple, on définit plusieurs variables standards comme : la vitesse moyenne des véhicules, le débit, la distance inter véhicules, etc. Ces variables sont rangées selon un ordre défini dans la MIB, au niveau de l'équipement routier, et peuvent dés lors être consultées par une commande appropriée à partir de la station de supervision. Dans chaque équipement routier, un programme appelé agent SNMP se charge de maintenir et de tenir à jour ces variables.

4.2.1 Emplacement de l'objet au niveau de la branche NEMA.

La figure suivante représente l'arborescence à partir du nœud NEMA. Sous ce nœud, tous les objets décrivant des variables routières devront être définis. Ces objets sont sous la responsabilité de NEMA.



19. Branche NEMA

4.2.2 Création d'un objet

Une MIB contient un ensemble d'objets écrits en ASN-1 ayant chacun une fonctionnalité particulière. Elle correspond à une suite de définitions d'objets et elle décrit les chemins pour accéder à ces objets dans l'arborescence ISO.

Considérons l'exemple ci dessous, nous allons définir un objet en ASN-1 et son emplacement dans l'arborescence ISO :

essAirTemperature OBJECT-TYPE
SYNTAX INTEGER (-127..128)
ACCESS read-only
STATUS mandatory
DESCRIPTION "The air temperature in degrees Celsius."
::= {essTemperature 1}

Dans cet exemple nous avons défini l'objet *essAirTemperature* – Il indique la températuer en degré Celsius de l'air, et sous quelle forme la valeur de la variable est décrite, ici un entier signé. Les termes ASN-1 couramment utilisés pour définir un objet sont :

Termes ASN-1	***Description***	***Options***
Object type	Chaîne de caractères nommant l'objet. Nom de l'objet.	
Syntax	Type d'objet : Integer ; Sequence of ; Null ; Counter32 ; Gauge ; Opaque ; TimeTicks ; IpAddress … Sequence of est utilisé pour la définition de tables.	Byte (-127 , 127) Ubyte (0 , 255) Short (-32782 , 32782) Ushort (0 , 65535) Long (+/- 2147483647) Ulong (0 , 4294967295) Octet string : chaîne de caractères sur 8 bits.
Access	Détermine si la variable peut être lue ou écrite.	*Read* : Objet peut être lu. *Write* : On peut changer la variable de l'objet. *No access* : On ne peut accéder à la valeur de cet objet.
Status	Détermine l'importance de l'objet, c'est à dire s'il doit ou pas être implémenté.	*Mandatory* : Toutes les MIBs de ce type doivent inclure cet objet. *Obsolete* : Cet objet a été remplacé ou détruit ; il n'est pas requis de l'implémenter. *Optional* : optionnel. *Deprecated* : Cet objet est déprécié, tend à être obsolète.
Description	Que représente l'objet et comment doit-on l'interpréter ?	

20. Définitions des termes employés par ASN-1

Dans notre exemple, l'objet défini est obligatoire, et la variable ne peut être que lue. A la dernière ligne de notre exemple, l'entier 1 est affecté à cet objet. Nous allons expliquer à quoi sert cet entier. Après avoir défini l'objet, nous devons indiquer son chemin dans l'arborescence ISO. Considérons l'arborescence ISO représentée page 27 pour accéder au nœud NEMA, puis aidons-nous de la branche NEMA décrite page 32 pour accéder à notre objet. Il existe deux façons d'indiquer ce chemin (comme pour SNMP) soit :
- de manière littérale :
iso.org.dod.private.enterprises.nema.transportation.devices.ess.essTemperature.*essAirTemperature*
- sous forme d'une chaîne d'entiers :
1.3.6.1.4.1.1206.4.2.6.7.1.1

4.2.3 Codage de l'objet pour la transmission.

L'information contenue dans un message STMP est codée selon les règles standards ISO, comme le BER (se reporter au chapitre 3 pour plus d'explications). NTCIP codifie aussi les messages STMP selon des règles définies par NEMA nommées PER – Packets Encoding Rules -, qui sont un «sous-ensemble » de BER. ***PER est uniquement utilisé pour des objets dynamiques –spécifique à STMP-*** que nous expliquerons plus loin.

4.3 MESSAGE STMP

Lorsque le manager désire connaître la valeur de la variable, il spécifie l'emplacement de l'objet dans l'arborescence ISO. Considérons notre objet défini précédemment. Les quatre paramètres suivants doivent être codés:

OBJECT IDENTIFIER	1.3.6.1.4.1.1206.4.2.7.1.1
TYPE	Byte
LENGTH	1
VALUE	25 (température en°C)

OBJECT IDENTIFIER spécifie l'emplacement de l'objet dans l'arborescence ISO ; TYPE décrit le type de la variable ; LENGTH la longueur de cette variable ; VALUE sa valeur.

Lors de la transmission, le message comportera deux entités : {object ID} et {Object Value}. Deux possibilités d'encodage sont offertes : soit nous codons en partant du nœud racine de l'arborescence ISO, et nous utilisons SNMP ; soit en prenant pour référence le nœud NEMA, et dans ce cas, nous emploierons STMP. La méthode utilisée est spécifiée dans le message (au niveau du premier octet).

4.3.1 Codage de {object ID}

Nous obtenons la séquence d'octets suivante en considérant le nœud racine comme référence (pour SNMP) :
NOTE : [xx] représente un nombre codé en hexadécimal.

[06][0C] [2B][06][01][04][01][89][36][04][02][07][01][01]

Le premier octet indique le type de OBJECT IDENTIFIER, ici [06].
Le second octet indique la longueur de la chaîne d'octets identifiant l'emplacement de l'objet recherché (le chemin ISO), ici 12, soit codé en hexadécimal 0x0C.
Du troisième octet au quatorzième c'est le chemin ISO, codé en hexadécimal, pour atteindre cet objet :
[2B] correspond à iso.organisation.
[06] : DOD.
[01] : Internet.
[04] : private.
[01] : enterprise.
[89][36] : NEMA.
[04] : transportation.
[02] : devices.
[07] : ess.
[01] : essTemperature.
[01] : *essAirTemperature*, notre objet.

Nous obtenons la séquence d'octets suivante en considérant le nœud NEMA comme référence (pour STMP) :

[06][05] [04][02][07][01][01]

Nous avons supprimé les 7 premiers octets de OBJECT IDENTIFIER et remplacé le second octet par la nouvelle valeur de la longueur de la chaîne, qui est égale à 5, soit [05].

4.3.2 Codage de {Object Value}

La valeur de la variable étant 25 soit [19] en héxadécimal, BER la considère comme un entier [02] de longueur 1 soit [01]. {Object Value} sera codifié de la manière suivante :

[02][01][19]

La séquence combinant {object ID} et {Object Value} utilisant SNMP est:

{[06][0C] [2B][06][01][04] [01][89][36][04][02][07][01][01]} {[02][01][19]}

Si nous prenons pour référence le nœud NEMA, la séquence devient :

[06][05] [04][02][07][01][01] [02][01][19]

4.3.3 Entête du PDU de STMP

Structure du 1er octet du message STMP:

Format PDU - 1 bit -	Type de message - 3 bits -	Identifiant de l'objet - 4 bits - (OBJECT-ID)

7 0

L'information contenue dans cet octet correspond à :

Bits	Valeur	Description
Bits 0 à 3	**ID objet**	
	0000	Le nœud NEMA est prit comme référence
	0001 - 1101	ID des objets dynamiques
	1110	Le nœud racine est prit comme référence
	1111	Réservé
Bits 4 à 6	**Type du message**	
	000	Get-request
	001	Set-request
	010	Set-request-no-reply
	011	Trap
	100	Get-response
	101	Set-response
	110	Get-error-response
	111	Set-error-response
Bit 7	**PDU format**	**Format STMP**
	0	Format réservé (non STMP)
	1	Format standard STMP

21. Descriptif du premier octet du message STMP

Note : Il est possible que le positionnement des bits soit modifié par le comité de pilotage de NTCIP. Néanmoins, nous respecterons cet ordre dans la suite du document.

Exemple d'envoi d'un message SNMP :

Nous souhaitons obtenir la valeur de notre objet, dans ce cas nous adressons à notre agent un message STMP avec pour type de message un get-request. En binaire, en respectant l'ordre, nous obtenons la séquence suivante : 1 000 0000 (1 pour STMP, 000 pour get-request, 0000 pour prendre comme référence le nœud NEMA). Nous obtenons en convertissant cet octet en hexadécimal la valeur 0x80. Notre PDU STMP ainsi constitué est de la forme suivante :

STMP	OBJECT IDENTIFIER	OBJECT VALUE
[80]	[06][06] [04][02][07][01][01][00]	[02][01]

L'agent enverra pour sa part un get-response suivant :
Le premier octet correspond à la séquence en binaire suivante : 1 100 0000 (1 pour STMP, 100 pour get-response, 0000 pour prendre comme référence le nœud NEMA). Nous obtenons en convertissant cet octet en hexadécimal la valeur 0xC0. Notre PDU STMP ainsi constitué est de la forme suivante :

STMP	OBJECT IDENTIFIER	OBJECT VALUE
[C0]	[06][06] [04][02][07][01][01][00]	[02][01][19]

Note : L'utilisation des protocoles SNMP et STMP nécessite l'ajout d'un octet de valeur nulle à la fin de la suite d'octets définissant object identifier.

4.3.4 Les objets dynamiques

Les objets dynamiques sont une particularité de STMP. Un objet dynamique n'est qu'un ensemble d'objets de type simple ou de type table. Afin d'obtenir des demandes et des réponses plus rapides, il convenait de réduire la charge protocolaire des messages STMP. Nous avons vu précédemment que sur les quatre bits de poids les plus faibles - correspondant à la partie ID de l'objet -, 13 combinaisons possibles étaient réservées aux objets dynamiques (de 0001 à 1101). Le principe est d'identifier à partir d'une de ces combinaisons l'emplacement d'un objet dynamique. Dans ce cas nous n'avons plus à spécifier dans le PDU STMP, l'identificateur d'objet soit OBJECT IDENTIFIER. De plus le type et la longueur sont connus et n'ont pas à être codés. De même pour OBJECT VALUE le type et la longueur sont aussi connus et donc non codés. Ceci est possible car le manager et l'agent choisissent les objets définis dans l'objet dynamique. Le gain est donc conséquent, le PDU STMP se résume donc à :

STMP	OBJECT IDENTIFIER	OBJECT VALUE
[XX]		[XX]

Afin de clarifier le propos, considérons l'exemple suivant :
(NOTE : Cet exemple est fictif tant pour la définition des objets que pour leur identificateur ; OBJECT IDENTIFIER est une chaîne d'entiers courte dans le but de simplifier l'écriture et ne correspond pas à la réalité).

Soit l'objet dynamique suivant :

Dyn Obj 1 :

- Durée du feu rouge (OBJECT IDENTIFIER 1.1.0)
- Durée du cycle (OBJECT IDENTIFIER 1.2.0)
- Etat de l'alarme (OBJECT IDENTIFIER 1.6.0)

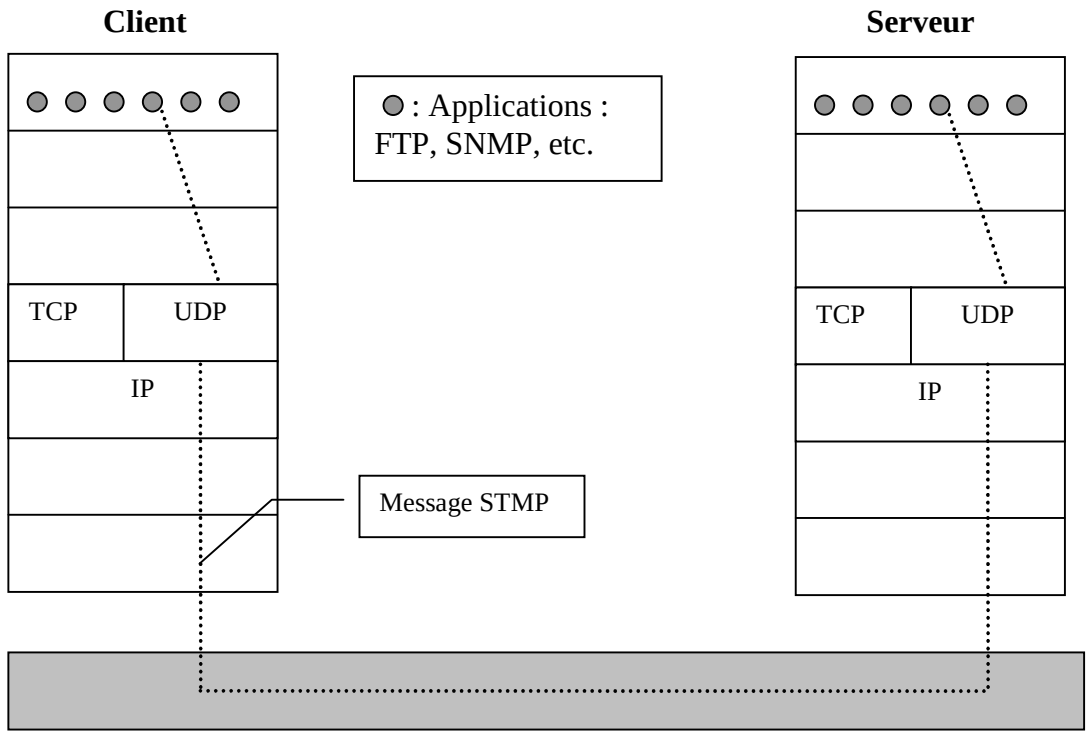
Une demande – get-request- du manager sur l'objet dynamique 1 est transmise de la manière suivante :
Le premier octet du message STMP est constitué de la suite de bits suivante : 1 (STMP) 000 (get-request) 0001 (Dyn Obj 1) soit en hexadécimal 0x81.

L'agent répond par un get-response suivant :
Le premier octet du message STMP est donc constitué de la suite de bits suivante : 1 (STMP) 100 (get-response) 0001 (Dyn Obj 1) soit en hexadécimal 0xC1, suivi des valeurs des objets définis dans Dyn Obj 1.

Il existe des procédures pour créer des objets dynamiques, voir le document NEMA TS 3.2 en vente sur le site WEB nema.org.

4.4 COEXISTENCE DE PROFILS DIFFERENTS SUR UN MEME CANAL.

Il est possible de faire coexister différents profils sur un même canal de communication physique. De plus, plusieurs applications peuvent cohabiter au niveau de la couche application. Les profils de classes A, C et E supportent le concept de port. Un port est un «passage logique » - identifié comme un entier - entre la couche transport et la couche application. Il permet de «cibler » l'application habilitée à recevoir le message. Le schéma ci-dessous illustre le concept de port :



22. Notion de port

Il existe des numéros de ports standards comme :

Application	FTP data	FTP control	SNMP	SNMP trap	STMP et STMP trap
Numéro de ports	20	21	161	162	Non définis

Ce numéro de port est codifié dans le datagramme (cas UDP) ou dans le segment (cas TCP) de la couche transport.

5 COUCHE LIAISON : LA TRAME HDLC

La coexistence de différents profils sur le même canal de communication nécessite qu'au niveau de la couche de liaison, l'information soit orientée vers les couches supérieures adéquates. NTCIP, pour les profils de classes A, B et C, utilise le protocole HDLC –High level Data Link Control – modifié (car un champ IPI est ajouté à la trame), au niveau de la couche liaison, pour encapsuler les messages STMP. La transmission, dans le cadre NTCIP, s'effectue en ***mode asynchrone***.

La structure d'une trame HDLC est représentée ci-dessous :

FLAG	**ADDRESS**	**CONTROL**	**IPI**	**INFORMATION**	**FCS**	**FLAG**
1 octet						dernier octet

FLAG : Fanion annonçant le début de la trame. Sa valeur codée en hexadécimal est 0x7F, et reste constante. Sa longueur est d'un octet.
ADRESS : Adresse du destinataire de cette trame. Sa longueur est d'un octet ou deux. Deux octets sont nécessaires lorsqu'il existe des adresses étendues. Nous pouvons définir des adresses de groupe, faire du broadcast ou bien envoyer un message à un destinataire unique.
CONTROL : Identifie le type de trame, soit commande/reponse, information non numérotée ou poll non numérotée. Ce champ est codé sur un octet.
IPI : Initial Protocol Identifier, codé sur un octet. Permet d'identifier à quelle couche s'adresse l'information contenue dans la trame. Selon sa valeur l'information est transmise au protocole IP ou au protocole STMP :

	Valeur de IPI en hexadécimal	Profils concernés
IP	0x21	Classes A et C
SNMP	0xC1	Classe B

FCS : Frame Check Sequence Field. Codé sur deux octets. Effectue le contrôle d'erreur sur les bits de la trame.

6 CONCLUSION

NTCIP est principalement un document de spécifications, identifiant toutes les fonctions de gestion de la route souhaitées par les exploitants. Il offre un large éventail de protocoles de communications couvrant l'essentiel des besoins des utilisateurs. L'objectif de NTCIP est de créer un système ouvert, afin de pouvoir intégrer les technologies du futur sans remise en question des protocoles définis, et de s'insérer dans un existant. Pour qu'un système puisse être «ouvert », les applications doivent être distinctement séparées des supports de communications, ce qui est le cas pour NTCIP proposant des applications standards supportées par les protocoles de l'Internet TCP/IP.

De plus, le comité de pilotage de NTCIP a eu une approche originale en intégrant le protocole standard SNMP, et un dérivé STMP élaboré par les groupes de travail de NTCIP, sur la couche application. SNMP est un protocole souvent utilisé dans la gestion des réseaux LAN et WAN ce qui lui octroie une certaine notoriété. A l'aide du paradigme aller chercher-enregistrer, les autres opérations ne sont que des effets secondaires des deux précédentes, il est possible de gérer un ensemble d'équipements hétérogènes. Cet avantage confère à SNMP une certaine stabilité, souplesse et simplicité, à la différence des protocoles d'administration conçus à partir de commandes qui requièrent que toutes les fonctions d'administration doivent être définies par avance. SNMP est stable car sa définition est figée, même si de nouveaux éléments sont ajoutés à la base de données. Il est simple à mettre en œuvre et à utiliser car il évite la complexité liée à la gestion de commandes particulières. Il est de plus souple, car il prend en compte des commandes quelconques de façon élégante. Les avantages de SNMP sont dus en partie à l'indépendance de la MIB par rapport au protocole d'administration (5). Chaque constructeur implémentant dans son équipement un agent SNMP, lorsque la MIB est définie, est certain de son bon fonctionnement. L'administrateur peut gérer tout type d'équipement ayant des MIBs différentes, même si certaines variables ne sont pas prises en compte par certains équipements. Il n'y aura pas de réponse, un message d'erreur est alors émis. Toute nouvelle fonction s'insère sans bouleversement de l'existant, au contraire d'un langage de commandes qui nécessite de définir une nouvelle commande qui va s'ajouter à la pile de commandes précédemment définies, rendant ce protocole plus complexe à gérer.

Certes, la famille des protocoles NTCIP n'est pas à ce jour opérationnelle, mais les efforts consentis par les groupes de travail NTCIP devraient aboutir rapidement à un standard de fait dans les systèmes de gestion de la route américains. L'intérêt de ce standard dépasse les frontières américaines, d'autres pays y sont fortement intéressés. Le comité de pilotage de NTCIP a soumis ses travaux auprès de l'ISO afin d'obtenir la normalisation de ces protocoles. Les industriels américains (les industriels français aussi) se préparent déjà à investir ce marché qui pourrait aller en s'accroissant. La concurrence risque d'être rude entre industriels car les choix des fonctions sont laissés à leur initiative (en accord avec les gestionnaires de la route), la conséquence majeure pour les gestionnaires est une baisse des coûts des équipements de terrain et du système de gestion.

7 GLOSSAIRE

AGENT : En gestion de réseau, logiciel serveur qui s'exécute sur la machine hôte ou l'équipement à gérer.
ARP : *Address Resolution Protocol*. Protocole TCP/IP utilisé pour faire le lien entre une adresse IP et une adresse MAC.
ASN-1 : *Abstract Syntax Notation 1*. Protocole normalisé du niveau présentation, et utilisé sous forme simplifiée, par SNMP ou STMP pour codifier les messages.
BAUD : Unité de rapidité de modulation. Tend a disparaître au profit de bit par seconde.
BER : *Basic Encoding Rules*. Règles permettant de coder des données en binaire.
CLASS A PROTOCOL : Similaire au *Class B protocol* mais prend en compte le routage.
CLASS B PROTOCOL : Protocole dédié à la scrutation, pas de notion de routage.
CLASS C PROTOCOL : Similaire au *Class A protocol* mais en mode connecté avec possibilité de transfert de fichier.
CLASS D PROTOCOL : Pour les communications de type « dial up » sécurisé.
CLASS E PROTOCOL : Pour réaliser des transferts de données entre centres.
DATAGRAMME : Bloc de données émis sur un réseau à commutation par paquets en mode non connecté.
DUPLEX : Mode de transmission permettant le transfert d'informations dans les deux sens sur un même canal.
EIA : *Electronic Industries Association*. Association américaine regroupant les industriels en électronique.
FSK : Frequency Shift Key. Principe de modulation en fréquence. Le modem FSK type Bell 202 est utilisé pour des communications semi-duplex sur 2 fils ou duplex sur 4 fils de qualité téléphonique. C'est une modulation en fréquence à 1200 bits/s en mode asynchrone.
FTP : *File Transfert Protocol*. Protocole de transfert des fichiers fonctionnant sur des protocoles TCP/IP. FTP permet le transfert bidirectionnel de fichier en mode ASCII ou en mode binaire. Il offre également la possibilité de gérer des fichiers sur le système distant (création, destruction, nommage etc.). RFC 959.
HDLC : *High Level Data Link Control*. Famille de protocoles, du niveau liaison, orientés bits (pas de notion de caractères) fonctionnant en mode synchrone bidirectionnel utilisant une procédure de sécurité de type code cyclique et une anticipation des échanges (envoi de trames sans attendre l'acquittement) permettant ainsi d'optimiser les lignes. Il est cependant possible de le modifier afin qu'il puisse fonctionner en mode asynchrone. Il est très utilisé dans les réseaux utilisant X25 ou Rnis.
IAB : *Internet Architecture Board*. Groupe de quelques personnes qui définissent les conditions générales du développement d'Internet et des protocoles TCP/IP.
INTERNET : Ensemble de réseaux reliés par des routeurs, sur lesquels circulent des blocs de données et que les protocoles TCP/IP permettent de voir comme un unique et grand réseau virtuel.
IP : *Internet Protocol*. Protocole du niveau de la couche réseau. IP est un protocole orienté datagramme. Il offre des services d'acheminement des données de transport, de routage, de fragmentation/réassemblage et d'adressage. Il constitue la base du service de remise de paquets non fiable en mode non connecté. Il est indépendant des réseaux physiques utilisés pour la circulation des datagrammes. RFC 791.

ISO : *International Standards Organisation*. Organisation internationale de normalisation. Les projets de normes sont discutés au sein de cet organisme (autour de comités techniques ou sous comités, eux mêmes subdivisés en groupe de travail), et passent par trois stades différents (Draft Proposal (document de travail), Draft International Standard (proposition de normes), et enfin International Standard) avant d'être adoptés définitivement.
ITS : *Intelligent Transport System*.
LAN : *Local Area Network*. Signifie réseau local ou réseau local d'entreprise.
MIB : *Management Information Base*. Base de données contenant toutes les informations de gestion des différents objets d'un réseau. La dernière version, la MIB-2, est décrite dans la RFC 1213.
MODEM : Raccourci de modulateur – démodulateur. Appareil d'adaptation servant à transformer des signaux numériques pour les transmettre sur un canal de communication analogique et inversement. Il existe trois types de modulation : en amplitude (AM), en fréquence (FM) et en phase (PM).
NEMA : *National Electrical Manufacturers Agency*. Agence regroupant les industriels en électricité chargée de proposer et établir des normes dans son domaine d'application.
NTCIP : *National Transportation Communications for ITS Protocol*. Famille de protocoles amenés à « devenir des standards de communications » dans le domaine des réseaux routiers. Ils sont actuellement développés aux Etats Unis.
OSI : *Open System Interconnection*. Modèle de référence en sept couches des réseaux, destiné à fournir un cadre conceptuel et normatif aux échanges de données entre systèmes hétérogènes. Il a été normalisé par l'ISO. Chaque couche assure une fonction, communique avec la couche homologue du système interconnecté et fournit des services à la couche supérieure à travers une interface. Les sept couches du modèle OSI étant :

7	Application
6	Présentation
5	Session
4	Transport
3	Réseau
2	Liaison
1	Physique

PAQUET : Un paquet est un bloc de données, fréquemment utilisé pour exprimer un conteneur d'information sans référence à une couche particulière. Néanmoins son usage devrait se limiter lorsque le réseau est en mode connecté.
PAU : Poste d'Appel d'Urgence.
PMPP : *Point to Point Protocol*. A la différence d'une liaison point à point, une liaison multipoint permet à un émetteur de transmettre vers plusieurs récepteurs au même instant. PMPP est équivalent à HDLC avec un champ additionnel d'information rajouté dans la portion de la trame HDLC. Ce champ, IPI –Initial Protocol Identifier - est utilisé pour déterminer à quel niveau se situe le protocole qui envoie ou doit recevoir les données. Cette propriété permet aux dispositifs utilisant une application de classe B de coexister avec des applications de classe A ou de classe C sur le même canal physique de communication. Le

dispositif d'extrémité lit l'octet IPI et peut déterminer à quelle couche suivante il doit s'adresser. S'il ne reconnaît pas ce IPI les trames sont refusées.

PMV : Panneau à Message Variable.

POLLING : Terme anglo-saxon signifiant scrutation. Désigne une méthode de transmission de données dans laquelle un équipement contrôle un certain nombre d'équipement par des invitations à émettre et des invitations à recevoir.

PPP : *Point to Point Protocol*. Protocole du niveau liaison. Une transmission de données point à point ne met en relation à un moment donné qu'un seul émetteur à un seul récepteur.

Les fonctionnalités de base sont :

- Configuration de la liaison et négociation des options de liaisons,
- Reconnaissance du protocole encapsulé,
- Tests de la qualité des liens et détection des erreurs,
- Authentification,
- Compression d'en-tête.

Il est décrit par plusieurs RFC, et plus particulièrement la RFC 1661 : « The Point to Point Protocol (PPP) ».

PROTOCOLE : Description formelle des règles et de la structure de messages que les ordinateurs doivent respecter pour pouvoir communiquer.

RAU : Réseau d'Appel d'Urgence.

RFC : *Request For Comment*. Série de documents qui contiennent tout à la fois des commentaires, des exposés généraux, des idées, des remarques, des observations, des techniques ou encore des standards découlant de TCP/IP. Ils sont accessibles sur différents serveurs WEB comme inria.fr.

ROUTAGE : Fonction d'acheminement d'une communication à travers un ou plusieurs intermédiaires.

ROUTEUR : Ordinateur spécialisé qui relie deux réseaux, permettant ainsi de faire passer, en fonction de l'adresse IP du destinataire, des paquets de l'un à l'autre. Le terme de passerelle IP est parfois employé pour signifier un routeur.

RS–232 : C'est une des interfaces normalisées les plus répandues entre un équipement terminal informatique et un équipement d'adaptation. L'interface RS-232 définit des caractéristiques physiques suivantes : prise à 25 broches, longueur et dimension du câble, vitesse maximale de 19200 bauds. C'est une interface du niveau physique.

SEGMENT : Terme employé pour les unités de données utilisant le protocole TCP.

SMI : *Structure of Management Information*. Spécifie la structure de l'arbre d'enregistrement. RFC 1155.

SNMP : *Simple Network Management Protocol*. Protocole standard du niveau application. Il est utilisé pour la gestion des hôtes, des routeurs et des réseaux auxquels ils sont connectés. Il existe deux versions actuellement, la nouvelle version étant SNMPv2. RFC 1157 pour la version 1. RFC 2011, 2012, 2013 pour SNMPv2.

STACK : *Pile de protocoles*. Ensemble de protocoles réunis constituant une norme portant sur plusieurs couches du modèle OSI.

STMP : *Simple Transportation Management Protocol*. Protocole dérivé du protocole standard SNMP utilisé pour la gestion des équipements de terrain routiers.

TCP : *Transport Control Protocol*. Protocole standard du niveau transport. Il permet un transport fiable (car il y a acquittement de la part du destinataire des segments reçus) en duplex intégral et de bout en bout, sur lequel de nombreuses applications, comme FTP ou SNMP, s'appuient. Il est largement utilisé dans les connexions entre réseaux hétérogènes. Il est orienté connexion, c'est à dire qu'un accord entre les deux extrémités doit être établi avant qu'un processus s'exécutant sur une machine puisse envoyer un flux de données, transitant

sur des segments TCP eux-mêmes encapsulés dans des datagrammes IP, à un processus s'exécutant sur une autre machine. Le mode de commutation est la commutation de paquets. Le contrôle d'erreurs s'effectue à ce niveau. RFC 1180.

TELNET : Telnet repose sur les protocoles TCP/IP pour la connexion à distance. Telnet est basé sur le concept NVT (Network Virtual Terminal) de terminal virtuel. NVT définit un périphérique virtuel composé d'un affichage (display ou printer) et d'un clavier (keyboard). Il permet donc à un utilisateur de communiquer avec le système en temps partagé d'une machine distante comme s'il disposait d'un clavier/écran directement attaché à cette machine. RFC 854.

TRAME : Terme employé pour les unités de données du niveau liaison.

UDP : User Datagram Protocol. Protocole standard du niveau transport. C'est un protocole standard de la famille TCP/IP qui permet à un programme d'application d'une machine d'envoyer à un autre programme d'application un datagramme ou d'en recevoir un. UDP s'appuie sur le protocole standard IP. D'un point de vue pratique, c'est un protocole de transport sans connexion. La liaison est non fiable car sans acquittement des datagrammes reçus. Néanmoins il comporte un contrôle des données émises qui est optionnel. RFC 768.

UIT-T : Union Internationale des Télécommunications – Secteur de la standardisation des télécommunications. Organisation internationale regroupant les Etats membres de l'ONU et qui propose des avis relatifs aux services de télécommunication et de radiocommunication. Ex-CCITT (Comité Consultatif International pour le Télégraphe et le Téléphone).

X-400 : Norme de l'UIT-T pour le courrier électronique.

8 BIBLIOGRAPHIE

(1) : Télématique routière et normalisation. Exploiter des voies nouvelles. SETRA 1996.
(2) : National Transportation Communications for ITS Protocol, Guide, NTCIP Joint Standards commîtes, march 3, 1997.
(3) : 503 mots de l'exploitation de la route. Glossaire. SETRA, décembre 1996.
(4) : Réseaux de télétransmission des autoroutes de liaison non concédées. Guide technique. SETRA, mai 1993.
(5) : TCP/IP Architecture, protocoles, applications, Troisième édition, interEditions, Douglas Comer.
(6) : Simple Transportation Management Framework, Prliminary Draft, Michael Mc Crary, Intersection Development Corporation.

9 ANNEXE: STANDARDS DISPONIBLES OU EN COURS DE DEVELOPPEMENT

9.1 STANDARDS NTCIP DISPONIBLES

TS 3.1-1996 National Transportation Communications For ITS Protocol —Overview :

This publication provides an overview of the concepts and protocols that are planned for the NTCIP series of standards, which can be used to implement a working NTCIP-basedb transportation control system. This standard encompasses roadside device control, data collection, data routing, and file transfer services using various communication system topologies.

TS 3.2-1996 National Transportation Communications For ITS Protocol—Simple Transportation Management Framework :

The STMF describes the simple transportation management framework used for managing and communicating information between management stations and transportation devices. It covers integrated management of transportation networks, networking devices and transportation specific equipment attached to NTCIP based networks.

TS 3.3-1996 National Transportation Communications For ITS Protocol — Class B Profile :

This communications protocol standard can be used for interconnecting transportation and traffic control equipment over low bandwidth channels. It establishes a common method of interconnecting ITS field equipment such as traffic controllers and dynamic message signs (DMS), defines the protocol and procedures for establishing communications between those components, and references common data sets to be used by all such equipment.

TS 3.5-1996 National Transportation Communications for ITS Protocol – Actuated Traffic Signal Controller Units :

This publication defines objects which are specific to actuated signal controllers. It also defines standardized object groups which can be used for conformance statements.

TS 3.4-1996 National Transportation Communications for ITS Protocol — Global Object Definitions :

The messaging between Transportation Management and field devices is accomplished by using the NTCIP Application Layer services to convey requests to access or modify values stored in a given device; these values are referred to as objects. The purpose of this publication is to identify and define these objects definitions that may be supported by multiple device types (e.g., actuated signal controllers and variable message signs). The grouping of objects for a given device type is performed in the device-type-specific object definition standard.

9.2 STANDARDS NTCIP EN COURS DE DEVELOPPEMENT

9.2.1.1 TS 3.6-199X National Transportation Communications For ITS Protocol - ObjectDefinitions for Dynamic Message Signs (DMS) :

Contains object definitions to support the functionality of DMSs used for transportation applications. A dynamic message sign is any sign that can change the message presented to the viewer, such as a variable message sign, changeable message sign, or blank-out sign. Also includes conformance group requirements and conformance statements to support comliance with the standard.
Expected approval date: 3rd Quarter CY 1997

TS 3.ESS National Transportation Communications For ITS Protocol – Object Definitions for Environmental Sensor Stations (ESS) :

Contains object definitions for ESS, which traditionally have been called road/weather information systems (RWIS). The ESS consists of a Remote Processing Unit (RPU) and a suite of sensors to monitor weather, atmosperhic conditions, the roadway surface, air quality, and other parameters. The information is used by transportation operators to improve roadway maintenance and traffic operations. Also includes conformance group requirements and conformance statements to support compliance with the standard.
Expected approval date: 4th Quarter CY 1997

TS 3.HAR National Transportation Communications For ITS Protocol – Object Definitions for Highway Advisory Radio (HAR) :

Stations Contains object definitions for HAR stations, which are low-power AM broadcast radio stations used to provide traveler information in local geographic areas. The objects define HAR configuration, management, message status, and program messages. Also includes conformance group requirements and conformance statements to support compliance with the standard.
Expected approval date: CY 1998

TS 3.CLE National Transportation Communications for ITS Protocol - Class E Profile for Center-to-Center Communications :

This communications protocol profile is established to connect a transportation management center (TMC) to other TMCs and information service providers. The profile will include a data transmission standard and a message set standard.
Expected approval date: CY 1998

TS 3.RMC National Transportation Communications for ITS Protocol – Object Definitions for Ramp Meter Control (RMC) :

Contains object definitions for RMC units to support the functionality used within transportation applications. Ramp metering is used on entrance ramps to main line traffic on freeways. Ramp metering plans may be selected manually, by a central computer, by time of day, or by main line traffic conditions. Also includes conformance group requirements and conformance statements to support compliance with the standard.
Expected approval date: CY 1998

TS 3.SEN National Transportation Communications for ITS Protocol – Object Definitions for Advanced Sensor Objects :

Contains object definitions for advanced sensor systems to detect vehicles and traffic flow. Also includes conformance group requirements and conformance statements to support compliance with the standard.
Expected approval date: CY 1998

TS 3.DCM National Transportation Communications for ITS Protocol – Object Definitions for Data Collection and Monitoring Devices :

Contains object definitions for data collection and monitoring device systems to detect vehicle presence, speed, occupancy, weight, and other parameters. Also includes conformance group requirements and conformance statements to support compliance with the standard.
Expected approval date: CY 1998

TS 3.CLC National Transportation Communications for ITS Protocol - Class C Profile :

This communications protocol profile is established to connect transportation and traffic control field equipment, containing sufficient processing power and communications bandwidth, to support reliable data transfer and routing between network nodes. The Class C Profile includes the file transfer protocol (FTP) and the transmission control protocol (TCP).
Expected approval date: CY 1998

TS 3.CLA National Transportation Communications for ITS Protocol - Class A Profile :

This communications protocol profile is established to connect transportation and traffic control field equipment, containing sufficient processing power and communications bandwidth, to support reliable data transfer and routing between network nodes. The Class C Profile includes the file transfer protocol (FTP) and the transmission control protocol (TCP).
Expected approval date: CY 1998

TS 3.TCIP Transit Communications Interface Protocols (TCIP) :

Contains data dictionary and information transfer requirements, message sets and object definitions, and physical and data link protocol standards, to be used among public transportation vehicles and the TMC, other transit facilities, and other intelligent transportation system centers.
Expected approval date: CY 1998

TS 3.CLD National Transportation Communications for ITS Protocol - Class D Profile :

This communications protocol profile is established to connect transportation and traffic control field equipment over dial up telephone lines.
Expected approval date: CY 1999

TS 3.VCCNational Transportation Communications for ITS Protocol – Object Definitions for Video Camera Control :

Contains object definitions for control of closed circuit television video surveillance cameras.
Expected approval date: CY 1999