

Administration de réseaux IP

Roland Dirlewanger

CNRS - Délégation Aquitaine et Poitou Charentes

rd@dr15.cnrs.fr

(1)

- [RFC 826] "An Ethernet Address Resolution Protocol", 1982.
- [RFC 903] "A Reverse Address Resolution Protocol", 1984.
- [RFC 951] "Bootstrap Protocol (BOOTP)", 1985.
- [RFC 1531] "Dynamic Host Configuration Protocol", 1993.
- [RFC 1533] "DHCP Options and BOOTP Vendor Extensions", 1993.

- [RFC 1156] "Management Information Base for network management of TCP/IP-based internets", 1990.
- [RFC 1157] "Simple Network Management Protocol (SNMP)", 1990.
- [RFC 1902] "Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)", 1996.
- [RFC 1905] "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", 1996

(1)

- une adresse IP est codée sur quatre octets. On représente une adresse IP par la valeur de ces quatre octets (base 10) séparés par des points
- les octets de poids forts représentent le numéro du réseau IP, les octets de poids faible, le numéro de l'équipement dans ce réseau.

(2)

- l'espace d'adresses IP est divisé en classes
- soit $x.y.z.t$ une adresse IP

		réseaux	machines
classe A	$1 < x < 128$	x	$y.z.t$
classe B	$128 \leq x < 192$	$x.y$	$z.t$
classe C	$192 \leq x < 223$	$x.y.z$	t

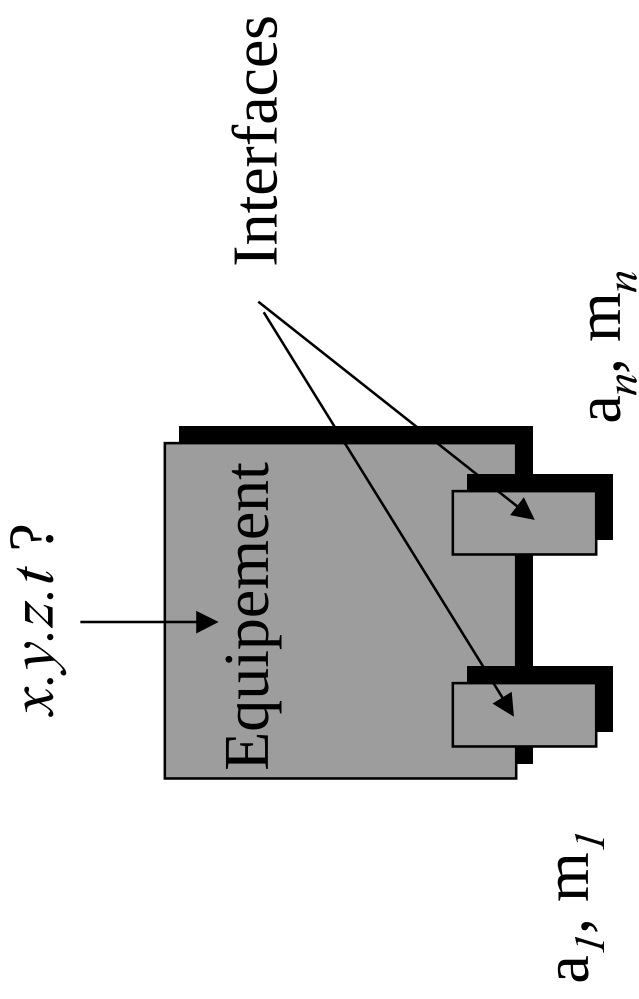
Les sous-réseaux

- pour subdiviser (*subnetting*) la partie droite de l'adresse en sous-réseaux + machines, on introduit la notion de masque :
 - *numéro réseau = adresse IP & masque*
 - *numéro machine = adresse IP & ~masque*
- la même notion de masque est utilisée pour définir des sur-réseaux (*supernetting*, *CIDR*)

Administrer un réseau IP

- un réseau IP c'est un ensemble d'équipements
 - possédant chacun une ou plusieurs interface
 - reliés entre eux par des supports physiques divers
- administrer un réseau IP
 - définir un plan d'adressage cohérent
 - affecter une adresse IP à chaque interface
 - mettre en œuvre le routage entre ces divers éléments

Acheminer un paquet IP (1)



$x.y.z.t$ destination du paquet IP
 a_i les adresses des interfaces
 m_i les masques

Acheminer un paquet IP (2)

- on recherche parmi toutes les interfaces s'il en existe une telle que

$$x.y.z.t \ \& \ m_i = a_i \ \& \ m_i$$

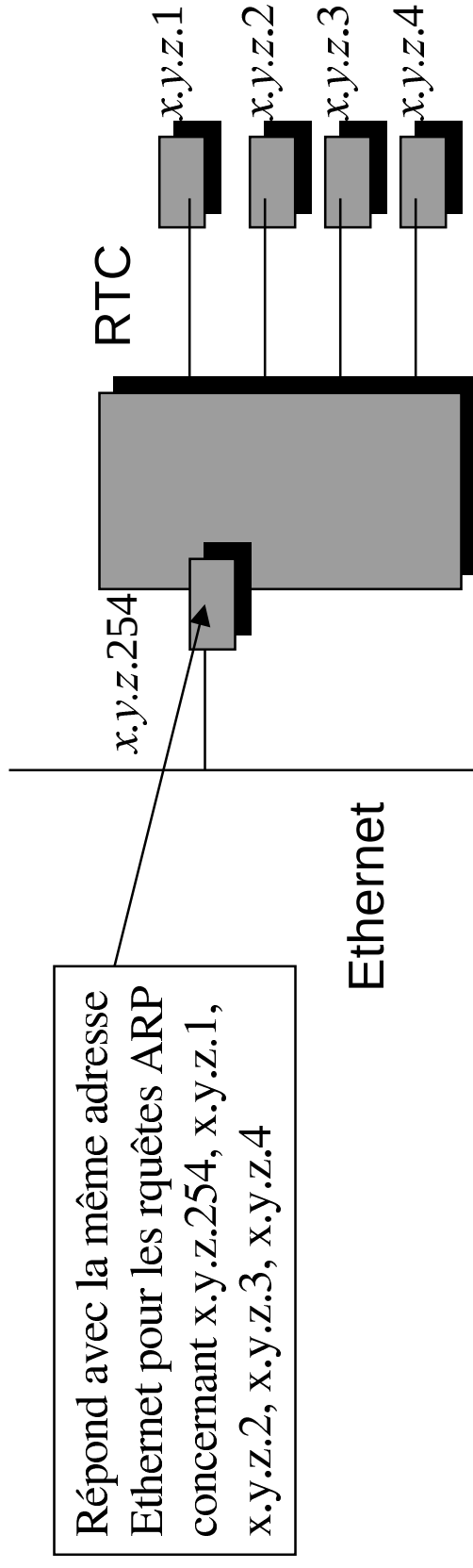
- s'il en existe une, $x.y.z.t$ est donc directement accessible via la couche 2 de cette interface.
- il faut trouver un voisin, i.e. un équipement directement accessible, par lequel faire transiter le paquet : c'est le **routage**.

(1)

- utilisé pour trouver la correspondance entre une adresse réseau (niveau 3) et une adresse physique (niveau 2)
 - émission : diffusion d'une requête contenant le type d'adresse physiques (Ethernet = 1), le type d'adresses réseau (IP = 2048), les longueurs de ces adresses, les adresses physique et réseau de l'émetteur, l'adresse réseau de la destination.
 - réception : le même paquet complété avec l'adresse physique de la destination.

Le protocole ARP (2)

- dans le cas d'IP/Ethernet
 - chaque station gère un cache pour éviter la multiplication des requêtes ARP. L'accès à ce cache se fait par la commande "arp" (Unix, Windows NT)
 - un équipement peut attirer vers lui le trafic vers un groupe d'adresses (proxy-ARP). Exemple d'une passerelle RTC :



Acquisition de l'adresse IP

- L'acquisition de l'adresse IP d'une interface peut se faire
 - par configuration statique
 - en fonction d'une donnée propre à l'interface, par exemple l'adresse Ethernet (RARP, BOOTP)
 - interrogation d'un serveur d'adresses (DHCP)

Le protocole RARP

- Le protocole RARP (Reverse Address Resolution Protocol) permet à un équipement connaissant son adresse physique d'obtenir son adresse réseau
 - nécessite des tables de correspondance adresse physique -> adresse réseau sur un ou plusieurs serveurs
 - émission, réception : symétrique de ARP
- Limites
 - protocole de niveau 2 (diffusion uniquement, pas de routage)
 - seule information : adresse réseau

- | | |
|--|---|
| | <ul style="list-style-type: none">• démarrage de stations Sun sans disque<ul style="list-style-type: none">– le client émet une requête RARP– il récupère son adresse IP et l'adresse d'un serveur– il transfère par TFTP un fichier de paramètres de boot contenant<ul style="list-style-type: none">• le chemin d'accès de la partition racine (serveur:/client/root)• le chemin d'accès du fichier de swap (serveur:/client/swap) |
|--|---|

Le protocole Bootp (1)

- basé sur UDP/IP : ports 67 vers le serveur et vers le client 68.
- caractéristiques
 - un seul paquet pour la requête et la réponse
 - un serveur BOOTP peut jouer le rôle de passerelle
 - gère les chemins d'accès des fichiers de boot
 - possibilité de désigner un serveur
 - extensible par le biais d'options (vendor options)

Le protocole Bootp (2)

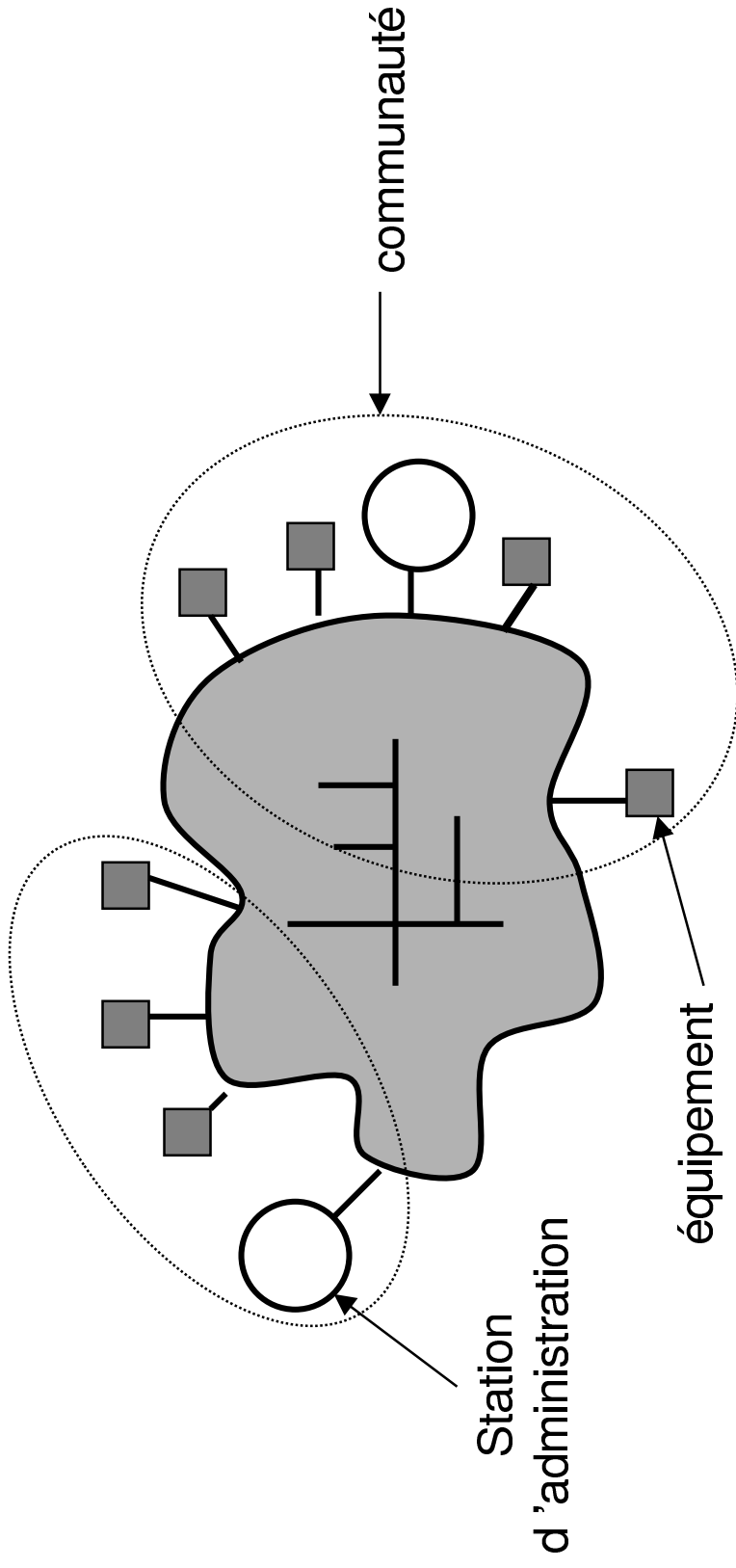
op	h type	hlen	hops	identification requête				secondes	adresse IP du client				adresse IP proposée	adresse IP du serveur				adresse IP du relais	adresse physique du client (16 octets)				nom du serveur (64 octets)				nom du fichier de boot (128 octets)				options (64 octets)			
----	--------	------	------	------------------------	--	--	--	----------	----------------------	--	--	--	---------------------	-----------------------	--	--	--	----------------------	---	--	--	--	-------------------------------	--	--	--	--	--	--	--	------------------------	--	--	--

Le protocole DHCP (1)

- extension de BOOTP pour gérer l'allocation dynamique d'adresses IP
- l'adresse IP est allouée selon les critères suivant
 - ne pas être déjà allouée à une autre station
 - la même station reçoit toujours la même adresse
 - cette adresse est allouée pendant une période déterminée
 - le client vérifie la validité de l'adresse (ARP)

Le protocole SNMP

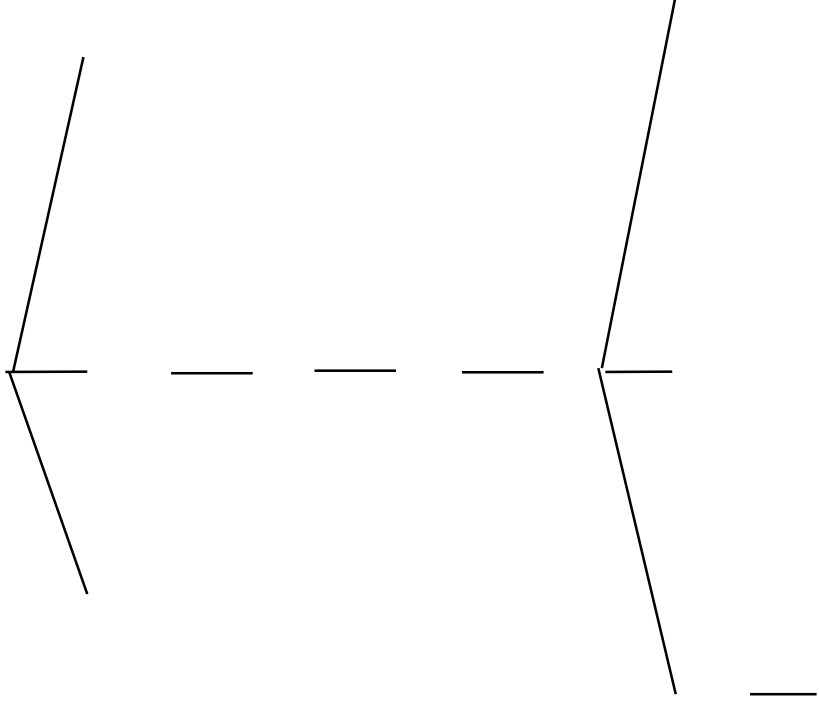
- SNMP (*Simple Network Management Protocol*)
- Architecture d'un réseau administré par SNMP :



SNMP : définitions

- Station d'administration : émet des requêtes vers les équipements
- Agent SNMP : composant logiciel sur ces équipements permettant de répondre aux requêtes SNMP
- Communauté :
 - association entre agents et stations d'administration
 - politique d'accès
- Management Information Base (MIB)
 - hiérarchie « normalisée » d'objets(i.e. éléments d'information dans un système)
 - objets d'écrits par les Basic Encoding Rules d'ASN.1

SNMP : les MIB



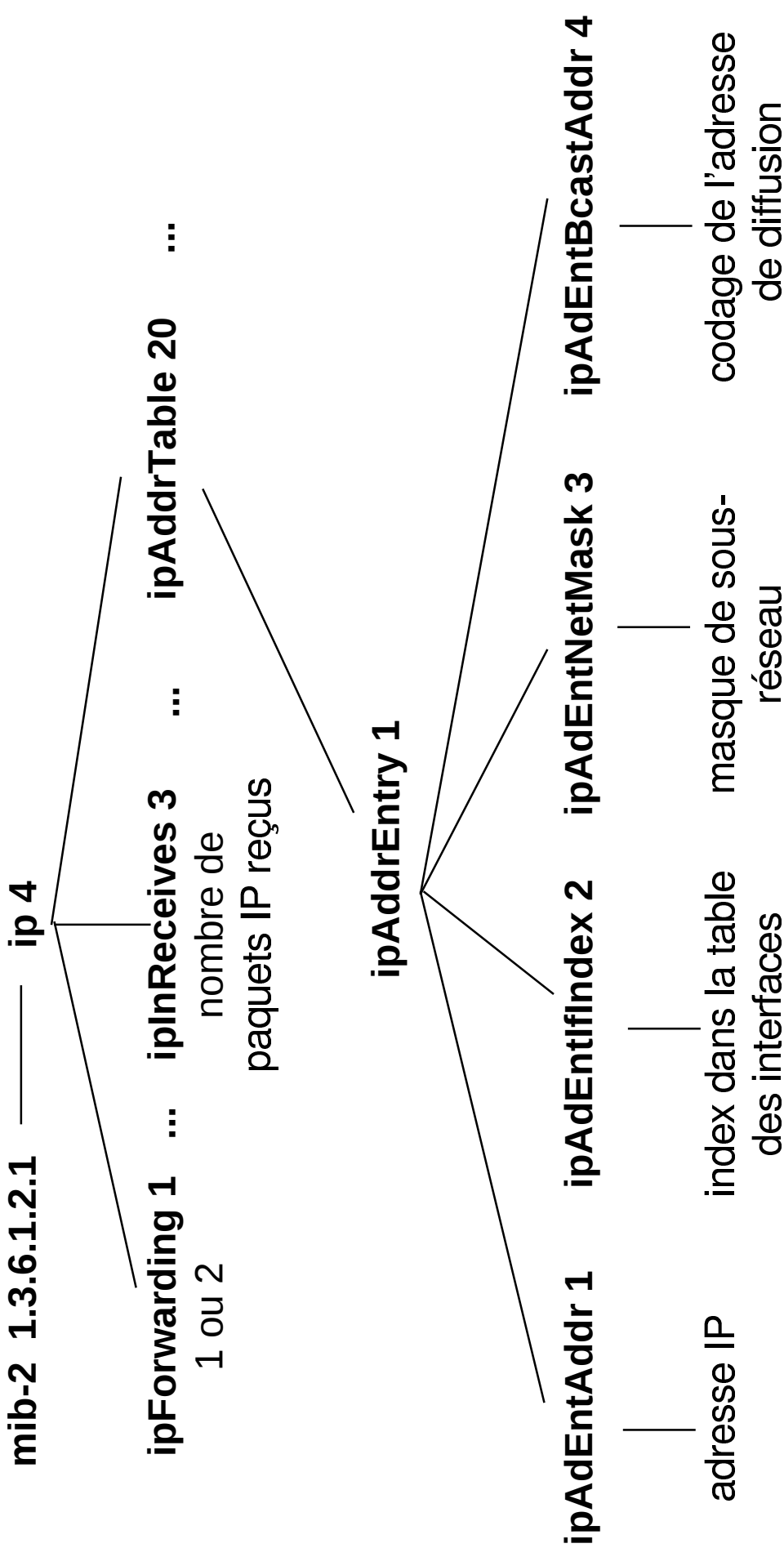
mib-2 : 1.3.6.1.2.1

SNMP : la MIB II

- RFC 1156, puis 1902 définissent plusieurs groupes d'objets dans MIB-2 (1.3.6.1.2.1)

– System	1
– Interfaces	2
– Address Translation	3
– IP	4
– ICMP	5
– TCP	6
– UDP	7
– EGP	8
- chaque groupe d'objet a sa propre hiérarchie « normalisée »

SNMP : exemple d'un groupe d'objets



SNMP : instantiation des objets

- objets simples (chaînes de caractères, compteurs, constantes) : l'instance d'un objet = « *nom de l'objet dans la MIB* » .0
- objets complexes : les règles d'instanciation font partie de la définition des objets
- exemples :
 - nombre de paquets IP reçus : **1.3.6.1.2.1.4.3.1**  ipInreceives
 - masque de sous-réseau pour l'adresse 147.210.72.254 : **1.3.6.1.2.1.4.20.1.3.147.210.72.254**  ipAdEntNetMask

SNMP : les requêtes

- requêtes et réponses tiennent dans un paquet UDP
- chaque paquet contient
 - numéro de version de SNMP (1 ou 2)
 - nom de la communauté
 - données (Protocol Data Unit - PDU)
 - type d'opération (getRequest, getNextRequest, getResponse, setRequest, Trap, getBulkRequest, InformRequest)
 - données spécifiques à l'opération. Exemple pour getRequest, getResponse :
 - identification de la requête
 - code d'erreur
 - index de la variable ayant causé l'erreur
 - liste de couples variables / valeurs