Les autoroutes de l'information

2ème partie

Protocoles réseaux : TCP/IP

IDEC

Sommaire

Sommaire 2
Introduction 4
Problématique de la communication réseau 4
Origine de TCP/IP 4
Utilisations de TCP/IP 5
Principe de base, en résumé 5
L'adressage IP 6
Notations binaire et décimale pointée 6
Les classes d'adresses 7
Adressage public ou privé 7
Le masque de sous-réseau 8
La mise en œuvre de sous-réseaux 8
L'exploration 9
La résolution de noms 10
Résolution de noms en adresses IP 10
Noms DNS 10
Noms NetBIOS 11
Résolution d'adresses IP en adresses MAC 13
Le cache ARP 13
Le routage 14
Tous les chemins mènent chez vous : le maillage 14
Etablir un itinéraire : principe du routage 16
Types de routeurs 16
Routage statique (tables) 17
Routage dynamique (protocoles) 18
Contrôle du routage 19
Connexions Intranet - Internet 20
Avec adresses IP publiques 20
Sans adresses IP publiques 20
Solutions mixtes 21
Au cœur de TCP/IP 22
TCP/IP dans le modèle OSI 22
Rôles des protocoles de transport 23
TCP 24
UDP 24
Contrôle des connexions 24
Rôle des protocoles Internet 25
IP 25
Protocoles de maintenance 25
IGMP 26
Rôles des protocoles d'application 26
Sockets 26
FTP et TFTP 26
Telnet 27
IPP 27
HTTP 27
SMTP, IMAP, POP 27
SNMP 28
Structure des paquets 29
Paquet IP 29
Paquet TCP 30
Paquet UDP 30
DNS 31

Organisation des données 32
Serveurs 32
Zones 32
Types d'enregistrements 33
Types de recherches 34
DNS sous Windows 35
Intégration avec Active Directory 35
DDNS 36
WINS 37
DHCP 38
Serveurs, étendues et baux 38
Procédure d'attribution 38
Expiration et renouvellement 39
Options d'étendues 39
Agents de relais DHCP 40
Evolutions de TCP/IP 41
IPSec 41
La multidiffusion 42
La voix sur IP 42
IPv6 43
TCP/IP et les autres protocoles 44
Utilisation de plusieurs protocoles 44
Encapsulation 44
Utilisation en parallèle 44
Autres protocoles LAN 45
NetBEUI 45
IPX/SPX 45
AppleTalk 45
Autres protocoles WAN 46
X. 25 46
Frame Relay 46
ATM 47
Fiche méthode: configurer un serveur DHCP 48
Fiche méthode : configurer un serveur DNS 50
Fiche méthode : configurer un serveur DDNS 51
Récapitulatif des principales commandes 52
Récapitulatif des principaux chiffres 53
Aide au diagnostic 54
Liste des principaux ports 55
Lexique 58

Introduction

Problématique de la communication réseau

La communication logique entre différents hôtes reliés par un réseau physique suppose que différents problèmes soient résolus :

- identification unique d'un hôte
- résolution de noms en adresses
- routage sur les réseaux maillés (interréseaux)
- communication normalisée entre tous les systèmes d'exploitation et logiciels impliqués

Pour chacune de ces fonctions, des protocoles ont été développés.
Il y a donc des protocoles de transport, mais aussi des protocoles de routage, des protocoles d'application, etc.

Lorsque l'on dispose d'au moins un protocole pour remplir chaque tâche, la communication en réseau devient possible. Autrement dit, il est indispensable d'associer plusieurs protocoles pour obtenir la connectivité réseau. On appelle souvent cette association de protocoles une suite ou une pile.

La pile de protocole la plus utilisée est TCP/IP.

Origine de TCP/IP

Comme son nom l'indique, le développement de TCP/IP[1] est indissociable d'Internet, et réciproquement.
D'origine militaire, le réseau ARPANET fut sans doute le premier à poser les problèmes de connectivité évoqués ci-dessus, rendant impératif la mise en œuvre de protocoles fiables et efficaces, adaptés aux réseaux maillés.

L'ancêtre de TCP/IP se nommait NCP[2] et a été utilisé sur ARPANET de 1970 à 1983, année où TCP/IP, après 11 ans de développement, l'a remplacé. Le système DNS, quant à lui, a été mis en place sur Internet l'année suivante.

Les spécifications des protocoles TCP/IP sont élaborées par un groupe de volontaires nommé IETF[3] et publiées sous forme de RFC[4] numérotées.
Les RFC peuvent être obligatoires, recommandées ou facultatives.

[1] Transport Control Protocol / Internet Protocol
[2] Network Control Protocol
[3] Internet Engineering Task Force
[4] Request For Comments

Utilisations de TCP/IP

Les problèmes de connectivité en interréseau n'étant pas l'apanage d'Internet, les entreprises n'ont pas tardé à mettre en œuvre TCP/IP sur leurs réseaux locaux.

On peut actuellement distinguer 3 types d'utilisation de ces protocoles :

- **Internet** : il s'agit d'un réseau « public », dont on peut faire partie à condition d'obtenir une adresse IP et un nom de domaine uniques au monde et de participer au routage de toutes les informations.
- **Intranet** : ce type de réseau fonctionne sur les principes d'Internet mais à l'échelle privée, et donc avec moins de contraintes. Un Intranet peut être ou ne pas être relié à Internet.
- **Extranet** : cette dénomination se rapporte à l'ouverture d'un Intranet à un sous-ensemble restreint et connu d'utilisateurs d'Internet.

Principe de base, en résumé

Toutes les opérations allant de l'envoi de messages par une application sur un hôte du réseau jusqu'à la réception par une autre application sur un autre hôte d'un autre réseau sont prises en charge par TCP/IP.

Cette communication suppose différentes étapes de mise en forme et d'adressage ; chacune de ces étapes étant assumée par l'un des protocoles de la pile TCP/IP.

Par exemple, TCP est chargé de découper les informations en paquets numérotés et de contrôler que tous les paquets sont bien arrivés à destination.
Chaque paquet est ensuite transmis à IP, qui est chargé de les adresser et de les router.

Chaque paquet peut prendre une route différente des autres paquets composant le message de l'application. Les paquets n'arrivent donc pas nécessairement dans l'ordre.
De plus, le système d'adressage employé est rigoureusement identique, quels que soient la distance et le nombre d'intermédiaires qui séparent le destinataire de l'expéditeur.

Le routage est donc une opération complexe.

Cependant, la complexité des opérations de découpage, contrôle, adressage, routage est masquée car entièrement prise en charge de manière transparente par TCP/IP.
Pour bénéficier des vastes fonctionnalités de TCP/IP, il suffit que chaque intervenant (destinataire, expéditeur et équipements intermédiaires) possède une configuration IP correcte, à savoir simplement :

- une adresse IP ,
- un masque de sous-réseau,
- l'adresse de la passerelle par défaut.

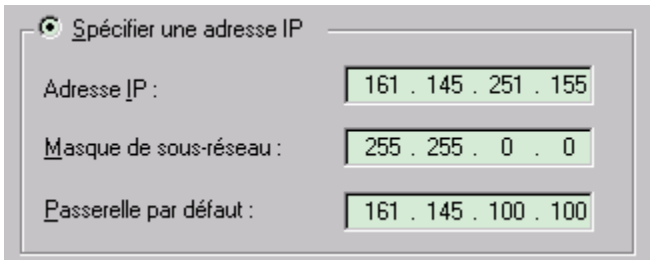
L'adressage IP

Tous les hôtes doivent posséder une adresse IP unique sur leur réseau accompagnée du masque de sous-réseau correspondant ainsi que l'adresse d'une passerelle.
Ces données peuvent être attribuées manuellement ou automatiquement, par un serveur DHCP.

Il faut distinguer ici le réseau physique du réseau logique. En effet, indépendamment de la segmentation physique, TCP/IP établit sa propre segmentation logique.
Chaque segment logique porte le nom de réseau et possède un identificateur unique : l'adresse du réseau, constituée d'une partie de l'adresse IP.

La communication entre hôtes appartenant à des réseaux IP différents est impossible sans l'intervention d'un hôte intermédiaire chargé du routage interréseau. On appelle cet hôte passerelle, routeur ou encore *gateway.*

Pour qu'un ordinateur puisse communiquer par TCP/IP, il faut installer une implémentation de TCP/IP compatible avec son système d'exploitation, et lui attribuer une adresse, un masque de sous-réseau et – le plus souvent –, une passerelle par défaut.



Notations binaire et décimale pointée

L'adresse IP est représentée sur 4 octets soit 32 bits.

Bien que les ordinateurs se servent exclusivement de la notation binaire, nous utilisons une notation plus parlante consistante à calculer la valeur décimale représentée par chaque octet. Ainsi, ces deux adresses sont identiques :

197	.	75	.	200	.	22
11000101		01001011		11001000		00010110

On parle de notation pointée car les valeurs décimales sont séparées par des points.

Sachant que la valeur la plus élevée (ou le nombre de valeurs différentes) que l'on peut représenter sur un octet est 255, aucune adresse IP ne peut comporter de valeur décimale supérieure.

Les classes d'adresses

Contrairement à d'autres protocoles, TCP/IP utilise une seule valeur pour identifier à la fois le réseau et l'hôte. La partie gauche de l'adresse IP identifie le réseau, tandis que la partie droite constitue l'identificateur de l'hôte.

Afin que la répartition des octets entre partie réseau et partie hôte corresponde aussi bien aux besoins de vastes réseaux qu'à ceux de petits, trois classes d'adresses ont été créées.

Classe	Plage de valeurs	Masque de sous-réseau	Nombre de réseaux	Nom d'hôtes
A	1 – 126	255.0.0.0	126	16 777 214
B	128 – 191	255.255.0.0	16 384	65 534
C	192 – 223	255.255.255.0	2 097 151	254

L'identificateur de réseau 127 n'est pas une adresse valide car réservé au test de bouclage et à la communication interprocessus de l'ordinateur.

Les identificateurs d'hôte 0 et 255 ne peuvent pas non plus être attribués ; 0 représentant l'adresse du réseau et 255 l''adresse de diffusion.

La classe D, allant de 224 à 231, est réservée aux adresses de multidiffusion.
La classe E existe également mais il s'agit d'une classe réservée à l'expérimentation.

Adressage public ou privé

Si vous souhaitez installer un hôte sur le réseau Internet, vous devez obtenir une adresse IP disponible, c'est-à-dire qui ne soit pas déjà allouée à un autre hôte.
Plusieurs organismes ont reçu des concessions internationales pour allouer les adresses IP ainsi que les noms de domaine. Eux seuls sont habilités à délivrer des adresses publiques.

En revanche, si les hôtes de votre réseau ne sont pas directement reliés à Internet, vous pouvez théoriquement choisir n'importe quelle adresse.
Néanmoins, les plages d'adresses suivantes ont été réservées pour l'adressage privé :

Classe	Plage d'adresses privées		
A	10.0.0.0	-	10.255.255.255
B	172.16.0.0	-	172.31.255.255
C	192.168.0.0	-	192.168.255.255

Aucune adresse comprise dans ces plages n'est attribuée sur Internet.

Le masque de sous-réseau

Indissociable de l'adresse IP, le masque de sous-réseau (ou *netmask*) est utilisé à la façon d'un cache par l'hôte qui cherche à envoyer un message. Il permet de masquer la partie identificateur d'hôte pour ne voir que l'identificateur du réseau, ou l'inverse.

L'examen successif de ces deux parties est indispensable avant d'envoyer quoi que ce soit sur le réseau, car il faut d'abord déterminer si le destinataire appartient au même réseau que l'expéditeur ou non.
En effet, le procédé de routage n'est pas le même selon le cas.

Si le destinataire se trouve sur le même réseau IP que l'expéditeur, ce dernier va se charger directement des opérations d'identification et d'acheminement.
Par contre, si le destinataire se trouve sur un sous-réseau différent, l'expéditeur ne peut pas lui envoyer directement ses paquets. Il les envoie donc à sa passerelle par défaut, qui mettra ensuite en œuvre les opérations de routage nécessaires.

La mise en œuvre de sous-réseaux

Créer des sous-réseaux au sein d'un réseau IP consiste à ajouter un niveau de segmentation supplémentaire.
Pour ce faire, on utilise une partie de l'adresse de l'hôte.
Un masque de sous-réseau comportant des valeurs autres que 0 et 255 indique que des sous-réseaux ont été mis en œuvre.