

Administration Système et Réseaux, Sécurité

Rappels TCP/IP

Philippe Harrand

¹ Département Informatique
Pôle Sciences et Technologie
² Direction Territoriale Sud Ouest
France Télécom

24 septembre 2007

Rappels TCP/IP

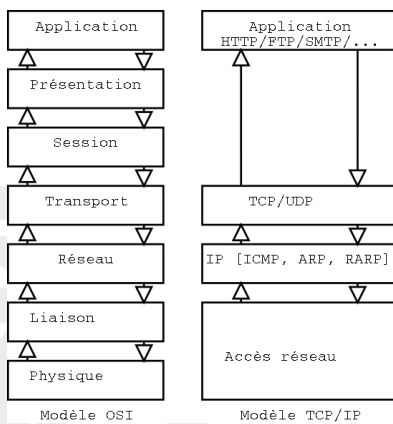
Modèle TCP / IP

Adressage IP

DHCP

Rappels TCP / UDP

Modèle TCP / IP



Généralités

- ▶ Une adresse IP compte 4 octets généralement représentés sous forme dite « décimale pointée ».
- ▶ Une adresse IP désigne une machine unique (sauf adresses privées) et une machine peut avoir plusieurs adresses IP.
- ▶ Une machine dotée d'une adresse IP fait généralement partie d'un réseau (sinon à quoi ça sert ?).

Notion de masque

- ▶ L'adresse IP comprend 2 parties, la partie réseau et la partie hôte (ou noeud ou machine).
- ▶ Un réseau est défini par une adresse réseau et un masque
- ▶ Le masque permet de déterminer quels sont les bits correspondants à la partie réseau. Les bits à 1 du masque sont nécessairement contigus

Masque

Pour calculer si une machine fait partie d'un réseau donné, on fait un & bit à bit entre l'adresse IP de la machine et le masque du réseau considéré. Exemple :

```

192.168.236.025
&
255.255.255.000
-----
192.168.236.000

```

Conventions

- ▶ Une adresse dont tous les bits **hôte** sont à **0** est l'adresse d'un réseau
- ▶ Une adresse dont tous les bits **hôte** sont à **1** est une adresse de **broadcast**
- ▶ On assigne aux routeurs les adresses les plus élevées du réseau
- ▶ Si la partie **hôte** d'un réseau comporte **n** bits, on peut assigner $2^n - 2$ adresses

Classes

Classe	Début	Fin	Masque
A	1.0.0.0	126.0.0.0	255.0.0.0
B	128.0.0.0	191.255.0.0	255.255.0.0
C	192.0.0.0	223.255.255.0	255.255.255.0
D	224.0.0.0	239.255.255.255	Multicast
E	240.0.0.0	254.255.255.255	Réservé

Classes Réservées

Classe	Début	Fin	Usage
A	10.0.0.0	10.0.0.0	Adressage privé
A	127.0.0.0	127.0.0.0	Adresse locale
B	172.16.0.0	172.32.0.0	Adressage privé
C	192.168.0.0	192.168.255.0	Adressage privé

RFC 1918

Sous-réseaux

- ▶ Pourquoi
 - ▶ Diviser une classe d'adresses louées
 - ▶ Filtrer les communications
- ▶ Comment
 - ▶ Utiliser un masque personnalisé
 - ▶ Relier les sous-réseaux par des routeurs

Sous-réseaux

- ▶ "Prendre" n bits à la partie hôte du masque
- ▶ Divise le réseau en $2^n - 2$ sous-réseaux
- ▶ Les sous-réseaux "tout à 0" et "tout à 1" sont inutilisables
- ▶ Les parties hôtes "tout à 0" et "tout à 1" sont inutilisables

Sous-réseaux

Exemple			
Hôte	192.168.236.153		192.168.236.217
	192.168.236.10011001		192.168.236.11011001
	&		&
Masque	255.255.255.11000000		255.255.255.11000000
Réseau	192.168.236.128		192.168.236.192

VLAN

- ▶ **Virtual Local Area Network**
- ▶ Extension du protocole *Ethernet*
- ▶ La trame Ethernet est *taggée* avec le numéro de VLAN
- ▶ Les switch délivrent les trames selon une table Port | MAC
⇔ VLAN

Attribution des adresses IP

L'administrateur établit un plan d'adressage puis attribue les adresses de manière :

- ▶ Statique
 - ▶ Manuelle
 - ▶ Automatique
- ▶ Dynamique
- ▶ Mélange des deux méthodes

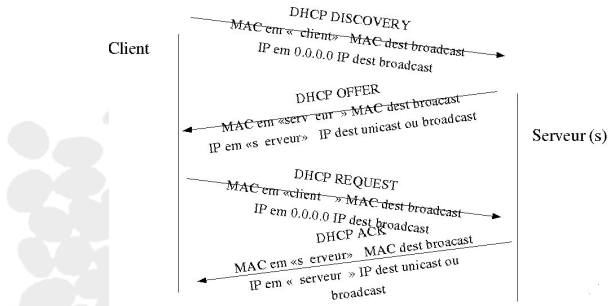
BootP

- ▶ RFC951 (Bootstrap Protocol) et RFC1542 (Clarifications and Extensions for Bootp)
- ▶ Le client émet une requête en broadcast (UDP) en indiquant son adresse MAC
- ▶ Si un serveur BootP trouve cette adresse dans sa table, il envoie alors une réponse Bootp, contenant les paramètres de configuration IP du client (adresse IP, masque de réseau, routeur par défaut, serveur DNS, etc)
- ▶ Le client configure sa pile IP
- ▶ Si le serveur a envoyé l'adresse d'un serveur et un nom de fichier, le client le charge en TFTP et l'exécute...

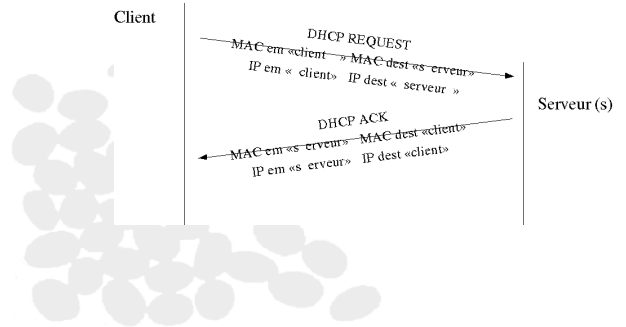
DHCP

- ▶ RFC2131 Dynamic Host Configuration Protocol
- ▶ Extension de BootP
- ▶ Attribution dynamique des adresses dans une plage
- ▶ Notion de bail
- ▶ Mise à jour des DNS (expérimental)

Demande de bail



Renouvellement de bail



fichiers

- ▶ Le serveur conserve les baux dans `/var/lib/dhcp/`
- ▶ les 2 principaux clients
 - ▶ dhclient (du paquetage dhcp) stocke les baux dans `/var/lib/dhcp/hclient-<interface>.leases`
Noter que dhclient commence la négociation par *DHCP REQUEST* à l'adresse du dernier serveur connu
 - ▶ dhcpd stocke les baux dans `/etc/dhcp/dhcpd-<interface>.cache`

DHCP Relay

- ▶ Les datagrammes en broadcast ne sont pas routés
- ▶ Le "relais" retransmet les trames vers un autre réseau en broadcast ou vers un serveur DHCP en unicast
- ▶ Le serveur destinataire sait qu'il a affaire à un relay car le champ "giaddr" est renseigné avec l'adresse du relay

TCP / UDP

- ▶ Protocoles de couche 4 (Transport)
- ▶ UDP
 - ▶ Mode non connecté
 - ▶ Non fiable
 - ▶ Utilisé pour des messages brefs
- ▶ TCP
 - ▶ Mode connecté
 - ▶ Fiable
 - ▶ Utilisé pour des transfert de données

TCP

- ▶ TCP remet en ordre les datagrammes IP
- ▶ TCP gère le flux de données
- ▶ TCP formate les données en segments et les "remet" à IP
- ▶ TCP multiplexe les données
- ▶ TCP transporte les données de façon sûre indépendamment du protocole de réseau

Remise fiable

- ▶ Chaque extrémité maintien un compteur d'octets envoyés
- ▶ Chaque extrémité envoie des accusés de réception contenant le numéro de l'octet attendu
- ▶ Les compteurs sont initialisés lors du processus de connexion

Gestion du Flux

- ▶ Chaque extrémité dispose d'une fenêtre : nombre d'octet pouvant être envoyés sans accusé de réception
- ▶ A tout instant une extrémité peut modifier la taille de la fenêtre
- ▶ Si la taille de la fenêtre vaut 0, la transmission est interrompue et reprend quand la taille de fenêtre augmente
- ▶ Les tailles de fenêtres sont initialisées lors de la connexion