

# Points essentiels à retenir pour le partiel d'ING

## Introduction à l'Internet

- Problèmes liés à la croissance (facteur d'échelle, pénurie d'adresses, explosion du nombre de routes, explosion du nombre de flots, ...)
- Diversité des besoins et des contraintes des applications (tolérance aux pertes, sensibilité temporelle, besoins en bande passante, ...)
- Structure hiérarchique de l'Internet : hiérarchie d'ISP, interconnexion d'AS
- Principes « fondateurs » de l'Internet (réseau à commutation de paquets, pas d'intelligence au cœur du réseau, service non fiable, ...)
- Rôle des différentes couches (physique, liaison, réseau, transport et application)
- Principe de l'encapsulation

## Sécurité

- Notion de confidentialité, intégrité, authentification
- Peut-on avoir l'une sans les autres ?
- Principes cryptographie à clé symétrique / publique (nombre de clés, fonctionnement)
- Quels sont les avantages et inconvénients de chacune des méthodes ?
- Qu'est-ce qu'une autorité de confiance ? Quelles sont les autorités de confiance pour chaque système ? (KDC pour clé symétrique, CA pour clé publique). Principe de fonctionnement
- A quelle catégorie appartient l'algorithme DES ?
- A quelle catégorie appartient l'algorithme RSA ?
- Quelle clé (publique ou privée) utilise-t-on pour chiffrer un message en vue de garantir la confidentialité ?
- Quelle clé (publique ou privée) utilise-t-on pour chiffrer un message en vue de garantir l'intégrité et l'authentification ?
- Qu'est-ce qu'une signature numérique ? Quelle(s) garantie(s) fournit-elle ?
- Qu'est-ce qu'un message digest ? Dans quel contexte et de quelle manière s'en sert-on ?
- Qu'est-ce qu'une fonction de hachage ? Quelles sont les propriétés d'une « bonne » fonction de hachage ?
- Qu'est-ce qu'une attaque par déni de service ? Exemples ?
- Filtrage (niveau réseau, niveau applicatif)
- Sécurité à différents niveaux protocolaires (PGP, SSL, IPSec, WEP)

## Multicast

- Définition et intérêt du multicast IP
- Exemple d'applications
- Différences entre le multicast réseau et l'émulation multicast avec plusieurs unicasts (au niveau du réseau, des sources, des récepteurs...)
- Adresses multicast IP (adresses de classe D, structure des adresses,...)
- Modèle de service orienté récepteur (pourquoi ce choix, quelles conséquences...)

- Notion de groupe et caractéristiques (pas de contrainte de localisation ni de nombre de membres, appartenance dynamique, possibilité d'appartenir simultanément à plusieurs groupes, possibilité d'être source sans être membre du groupe, groupes permanents / temporaires, ...)
- 2 solutions pour le multicast au niveau 2 (sur un LAN), différences, conséquences...
- But du protocole IGMP et différence par rapport aux protocoles de routage multicast
- Machines concernées par IGMP
- Fonctionnement d'IGMP (messages, entités impliquées, temporisation...)
- Différences selon les 3 versions d'IGMP, conséquences...
- Notion d'état mou / dur (soft / hard state)
- Quel état pour IGMP et pour les protocoles de routage multicast ?
- Rôle des protocoles de routage multicast (arbre par source, arbre par groupe, inondation, élagage, greffe, approches centrées avec point de rendez-vous ou cœur, arbre de coût minimum...)
- A quelle(s) catégorie(s) appartiennent les protocoles étudiés (DVMRP, MOSPF, RPF/RPB, Truncated RPB, RPM, PIM-DM, PIM-SM, CBT) ?
- Différence mode dense / mode épars (sparse)
- Avantages et inconvénients de chaque catégorie
- Qu'est-ce que le MBONE ?
- Comment fait-on lorsque l'on doit traverser des routeurs non multicast ? (notion de tunnel, encapsulation IP dans IP, fonctionnement, conséquences...)
- Quels sont les inconvénients de l'implémentation du multicast au niveau réseau (par rapport au niveau transport ou application) ? Et inversement ?

## QoS

- Définition et objectifs de la QoS
- Quelles applications ont besoin de QoS ?
- Composants de la QoS
- Notion de marquage de paquets, d'isolation des classes, d'admission d'appel
- Paramètres de QoS
- Différence délai de bout-en-bout en gigue
- Max-Min Fair share
- Gestion de files d'attente (passive / active)
- Qu'est-ce que le Drop Tail ?
- Problèmes du DropTail
- Disciplines d'attente
- RED
- Problèmes restant avec RED
- Description des flots
- Contrôle de trafic : fonctionnement et rôle d'un token/leaky bucket
- Paramètres des buckets
- Buckets en cascade (MBS, MBD...)