

Administration réseau

Introduction

A. Guermouche

1. Introduction

- Organisation
- Contenu

2. Quelques Rappels : Internet et le modèle TCP/IP

- Visage de l'Internet
- Le modèle TCP/IP

Plan

1. Introduction

- Organisation
- Contenu

2. Quelques Rappels : Internet et le modèle TCP/IP

- Visage de l'Internet
- Le modèle TCP/IP

Objectifs

Objectif du module : former des administrateurs réseaux

- ★ connaître le modèle Client/Serveur (90% des applications de l'Internet)
- ★ avoir des notions de conception d'applications Client/Serveur
- ★ connaître les protocoles applicatifs de l'Internet et savoir mettre en place les services associés sous Linux et sous Windows

⇒ Manipulation des notions/outils nécessaire à un administrateur réseaux.

Organisation du module

26h de cours + 28h de travaux pratiques

TP par groupe :

1. en salle avec droits d'administration
 - ▶ accès restreint à l'extérieur
 - ▶ possibilité de câblage
2. en salle standard en utilisant des machines virtuelles
User-mode Linux.

Dans les deux cas root sur les machines (réelles pour 1 et virtuelles pour 2) 😊

Contrôle continu : un ou plusieurs TPs notés + partiel sur machine.

Examen final : examen de 1h30 concernant le cours.

Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

Administration réseau

Le rôle d'un administrateur réseau consiste (entre autre) à :

- ★ Mettre en place et maintenir l'infrastructure du réseau (organisation, ...).
- ★ Installer et maintenir les services nécessaires au fonctionnement du réseau.
- ★ Assurer la sécurité des données internes au réseau (particulièrement face aux attaques extérieures).
- ★ S'assurer que les utilisateurs "n'outrepassent" pas leurs droits.
- ★ Gérer les "*logins*" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, ...).
- ★ Gérer les systèmes de fichiers partagés et les maintenir.

L'administrateur réseau est responsable de ce qui peut se passer à partir du réseau administré.

Contenu

- ★ Routage et passerelle :
 - ▶ Configuration d'une passerelle.
 - ▶ Configuration d'un réseau privé : NAT (**N**etwork **A**ddress **T**ranslation), IP masquerading ...
- ★ Sécurité dans les réseaux:
 - ▶ Configuration de pare-feu (*firewall*):
 - Manipulation des tables *iptables*.
 - Règles de filtrage.
 - ...
 - ▶ Outils de diagnostic :
 - *nmap*
 - ...
- ★ Configuration et manipulation de services spécifiques :
 - ▶ Gestion d'utilisateurs distants (NIS)
 - ▶ Un annuaire fédérateur (LDAP)
 - ▶ Transfert de fichiers et autres (FTP, TFTP, NFS, SMB)
 - ▶ Connexions à distance (telnet, rlogin, ssh, X11, ...)
 - ▶ Les serveurs de noms (DNS)

Plan

1. Introduction

- Organisation
- Contenu

2. Quelques Rappels : Internet et le modèle TCP/IP

- Visage de l'Internet
- Le modèle TCP/IP

Le visage de l'Internet (1)

- ★ Un réseau de réseaux
- ★ Un ensemble de logiciels et de protocoles
- ★ Basé sur l'architecture TCP/IP
- ★ Fonctionne en mode Client/Serveur
- ★ Offre un ensemble de services (e-mail, transfert de fichiers, connexion à distance, WWW, ...)
- ★ Une somme « d'inventions » qui s'accumulent
 - ▶ mécanismes réseau de base (TCP/IP)
 - ▶ gestion des noms et des adresses
 - ▶ des outils et des protocoles spécialisés
 - ▶ le langage HTML

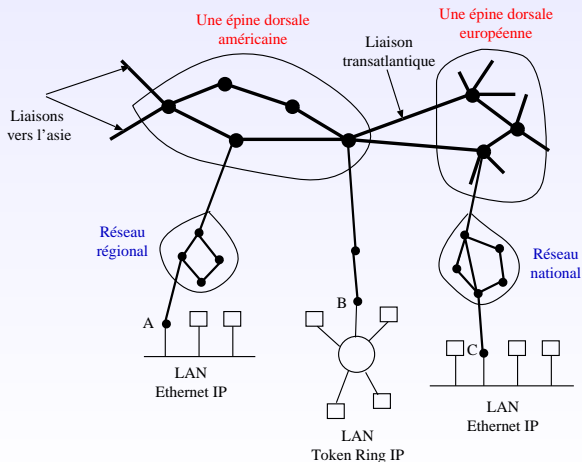
Le visage de l'Internet (2)

- ★ Une construction à partir du « bas »
 - ▶ réseau local (laboratoire, département)
 - ▶ réseau local (campus, entreprise)
 - ▶ réseau régional
 - ▶ réseau national
 - ▶ réseau mondial

- ★ 3 niveaux d'interconnexion
 - ▶ postes de travail (ordinateur, terminal...)
 - ▶ liaisons physiques (câble, fibre, RTC...)
 - ▶ routeurs (équipement spécialisé, ordinateur...)

Le visage de l'Internet (3)

Un ensemble de sous-réseaux indépendants (Autonomous System) et hétérogènes qui sont interconnectés (organisation hiérarchique)



L'architecture de TCP/ IP (1)

Une version simplifiée du modèle OSI

Application FTP, WWW, telnet, SMTP, ...

Transport TCP, UDP (entre 2 processus aux extrémités)

- ★ TCP : transfert fiable de données en mode connecté
- ★ UDP : transfert non garanti de données en mode non connecté

Réseau IP (routage)

Physique transmission entre 2 sites

TCP → **T**ransport **C**ontrol **P**rotocol

UDP → **U**ser **D**atagram **P**rotocol

IP → **I**nternet **P**rotocol

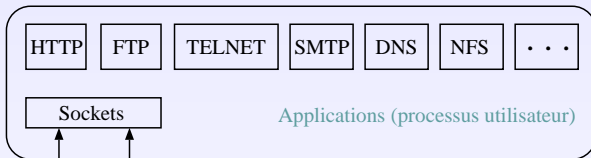
L'architecture de TCP/ IP (2)

OSI

7

6

5



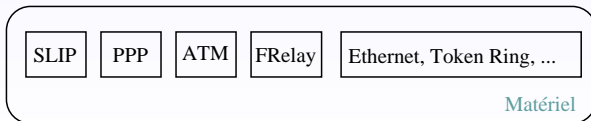
4

3



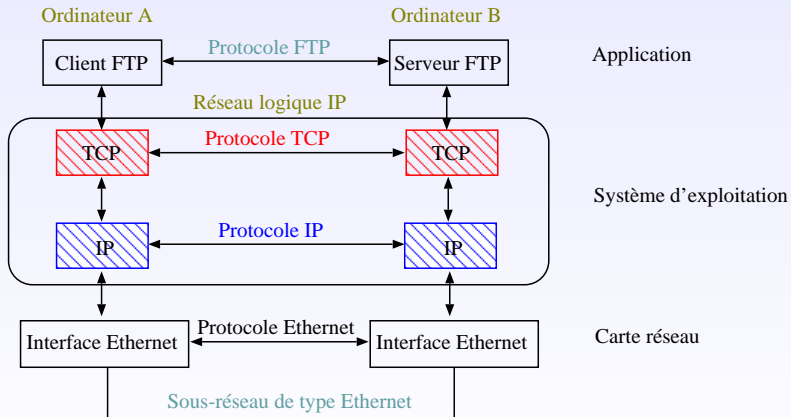
2

1



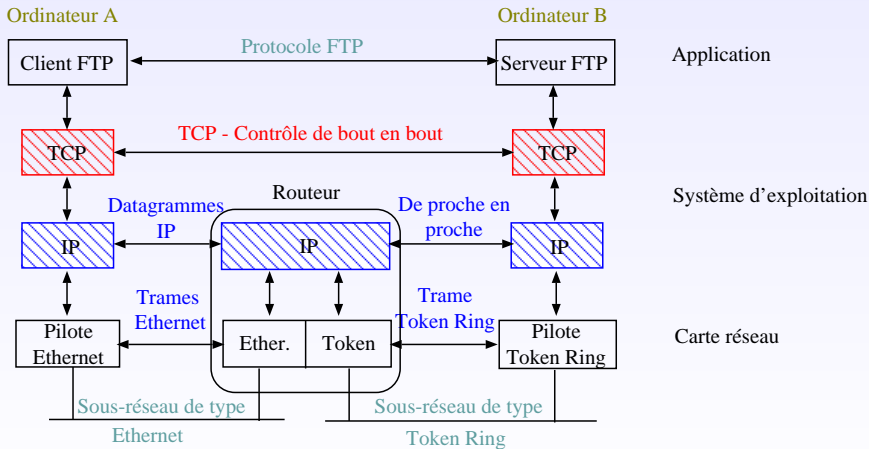
L'architecture de TCP/ IP (3)

Deux machines sur un même sous-réseau IP



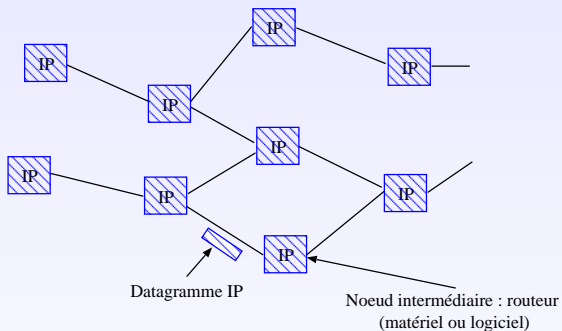
L'architecture de TCP/ IP (4)

Prise en compte de l'hétérogénéité



L'architecture de TCP/IP (5)

Couche réseau : communications entre machines

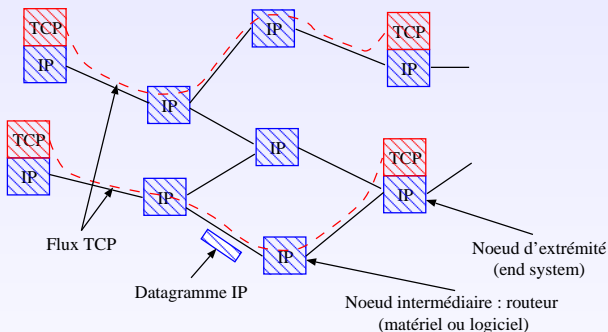


IP - protocole d'interconnexion, best-effort

- ★ acheminement de **datagrammes** (mode **non connecté**)
- ★ peu de fonctionnalités,
- ★ pas de garanties simple mais robuste (défaillance d'un noeud intermédiaire)

L'architecture de TCP/IP (6)

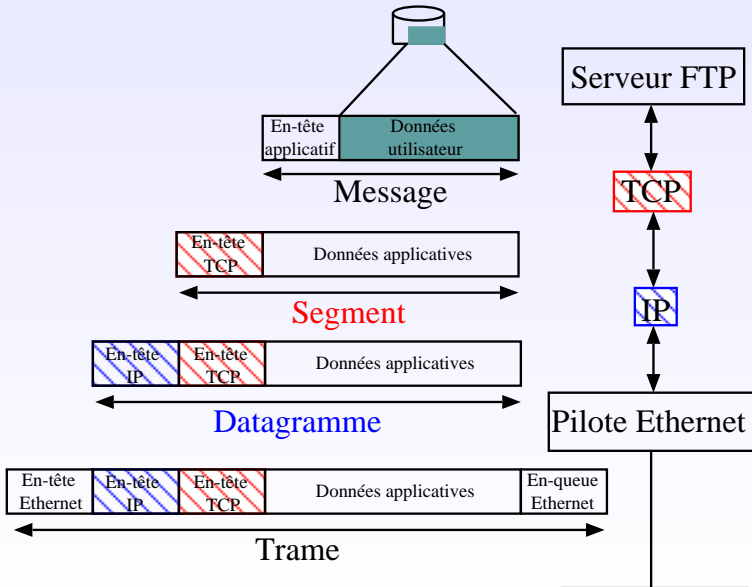
Couche transport : communications entre applications



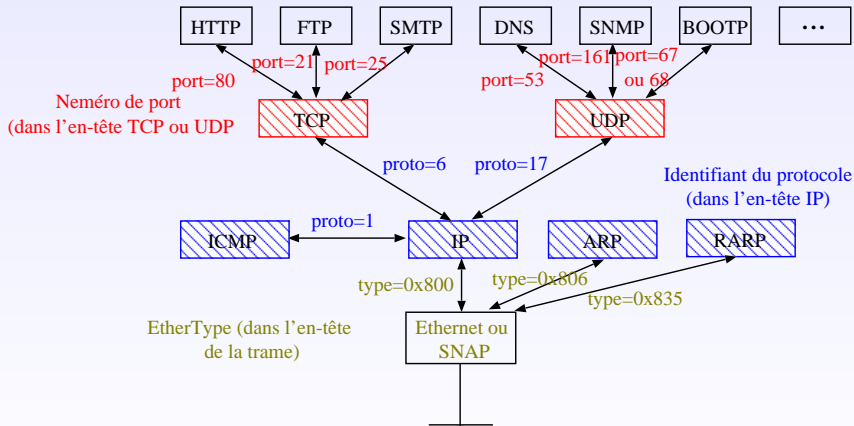
TCP - protocole de transport **de bout en bout**

- ★ uniquement présent aux **extrémités**
- ★ transport **fiable** de **segments** (mode **connecté**)
- ★ protocole complexe (retransmission, gestion des erreurs, séquençement, ...)

L'architecture de TCP/IP (7)



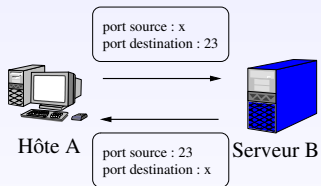
Identification des protocoles (1)



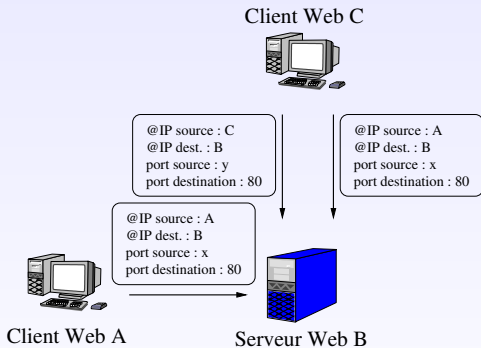
Identification des protocoles (2)

- ★ Une adresse de transport = une adresse IP + un numéro de port (16 bits) → adresse de socket
- ★ Une connexion s'établit entre une socket source et une socket destinataire → une connexion = un quintuplé (proto, src, port src, dest, port dest)
- ★ Deux connexions peuvent aboutir à la même socket
- ★ Les ports permettent un multiplexage ou démultiplexage de connexions au niveau transport
- ★ Les ports inférieurs à 1024 sont appelés **ports réservés**

Identification des protocoles (3)



Telnet Simple



Serveur Web

Le protocole UDP

UDP (RFC 768) - User Datagram Protocol

- ★ protocole de transport le plus simple
- ★ service de type best-effort (comme IP)
 - ▶ les segments UDP peuvent être perdus
 - ▶ les segments UDP peuvent arriver dans le désordre
- ★ mode non connecté : chaque segment UDP est traité indépendamment des autres

Pourquoi un service non fiable sans connexion ?

- ★ simple donc rapide (pas de délai de connexion, pas d'état entre émetteur/récepteur)
- ★ petit en-tête donc économie de bande passante
- ★ sans contrôle de congestion donc UDP peut émettre aussi rapidement qu'il le souhaite

Les utilisations d'UDP

- ★ Performance sans garantie de délivrance
- ★ Souvent utilisé pour les applications multimédias
 - ▶ tolérantes aux pertes
 - ▶ sensibles au débit
- ★ Autres utilisations d'UDP
 - ▶ applications qui envoient peu de données et qui ne nécessitent pas un service fiable
 - ▶ exemples : DNS, SNMP, BOOTP/DHCP

Transfert fiable sur UDP

- ▶ ajouter des mécanismes de compensation de pertes (reprise sur erreur) au niveau applicatif
- ▶ mécanismes adaptés à l'application

Le protocole TCP

Transport Control Protocol (RFC 793, 1122, 1323, 2018, 2581)

Attention: les RFCs ne spécifient pas tout - beaucoup de choses dépendent de l'implémentation

Transport fiable en mode connecté

- ★ point à point, bidirectionnel : entre deux adresses de transport (@IP src, port src) → (@IP dest, port dest)
- ★ transporte un flot d'octets (ou flux)
 - ▶ l'application lit/écrit des octets dans un tampon
- ★ assure la délivrance des données en séquence
- ★ contrôle la validité des données reçues
- ★ organise les reprises sur erreur ou sur temporisation
- ★ réalise le contrôle de flux et le contrôle de congestion (à l'aide d'une fenêtre d'émission)

Exemples de protocole applicatif

HTTP - HyperText Transport Protocol

- ★ protocole du web
- ★ échange de requête/réponse entre un client et un serveur web

FTP - File Transfer Protocol

- ★ protocole de manipulation de fichiers distants
- ★ transfert, suppression, création, ...

TELNET - TELetypewriter Network Protocol

- ★ système de terminal virtuel
- ★ permet l'ouverture d'une session distante

DNS - Domain Name System

- ★ assure la correspondance entre un nom symbolique et une adresse Internet (adresse IP)
- ★ bases de données réparties sur le globe