Architectures et Systèmes Communicants (ASC2)

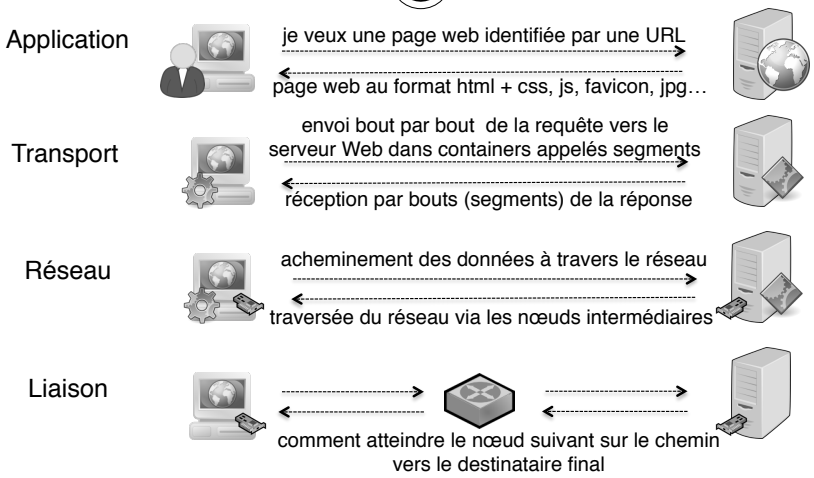
Lien avec le programme national (PN) BUT Info

- **RESSOURCES**
  - R2.04 : Communication et fonctionnement bas niveau
    - Comprendre le fonctionnement des couches systèmes et réseaux bas niveau
  - R2.05 : Introduction aux services réseaux
    - Comprendre les notions de service et d'architecture client-serveur et savoir installer un service simple dans un réseau informatique
- **SAÉ**
  - S2.03 : Installation de services réseau
    - À partir d'un besoin exprimé d'un client, il faut installer et configurer des services réseau permettant de développer ou de déployer des applications informatiques communicates

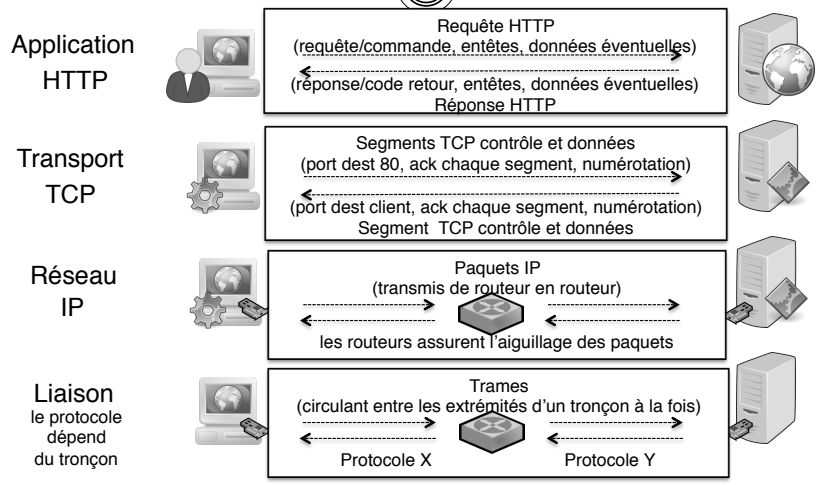
Organisation des enseignements

- **MODULE ASC2 DÉCOMPOSÉ EN 2 PARTIES**
  - Partie réseaux informatiques : ASR2.1 (fin janvier à mi-avril)
    - contenu issu d'une partie de R2.04, de tout R2.05 et tout de la SAÉ S2.03
    - cours Moodle : BUT-INFO-S2-R2.05 - Introduction aux services réseaux
    - intervenants : MRa (mourad.rabah@univ-lr.fr - bureau D106), ECa, PCo, JmBo, AmBo, HTA
  - Partie architecture et programmation bas niveau : ASR2.2 (mi-avril à fin mai)
    - contenu issu d'une partie de R2.04
    - cours Moodle : BUT-INFO-S2-R2.04 - Communication et fonctionnement bas niveau
    - intervenants : PCo, JmBo, CeLA

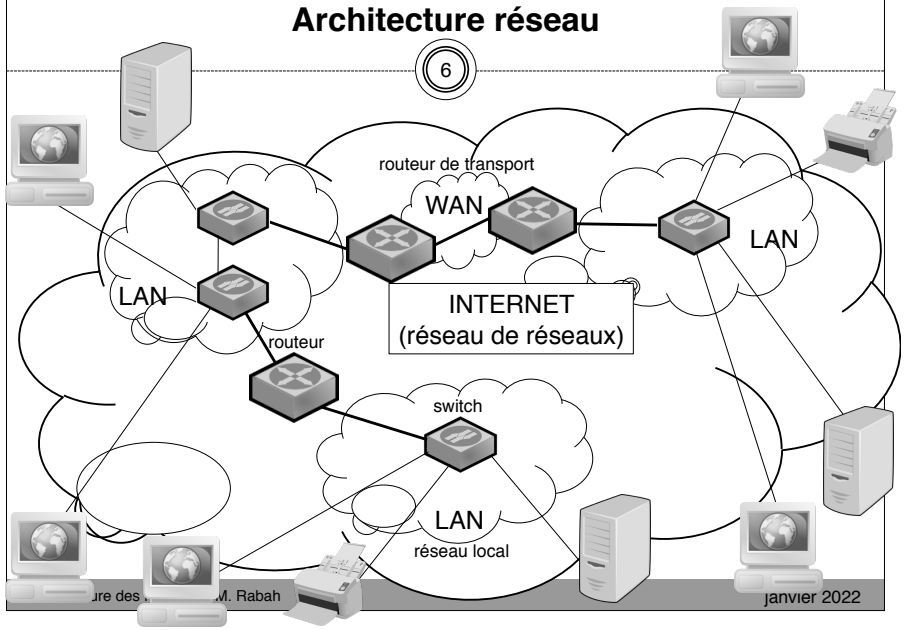
Exemple introductif : Récupération page web
Les échanges



Exemple introductif : Récupération page web
Les protocoles



Architecture réseau



Plan des chapitres ASR2.1

1. Généralités et terminologie
2. Modèles en couches
3. Réseaux locaux
4. Interconnexion des réseaux
5. Services réseau courants
6. Compléments sur la couche transport
7. Compléments sur la couche liaison de données

Cours et TD

- 2 Cours (2 x 1h) sem 4
  - Généralités, modèles en couches, services réseaux et protocoles courants
- 6 TD (6 x 2h) sem 5, sem 9 à 11, sem 13 et 14
  1. Généralités
  2. Encapsulation et décodage de trames
  3. Réseaux locaux et Ethernet
  4. Interconnexion des réseaux et configuration IP
  5. Interconnexion des réseaux et routage IP
  6. Couche transport et mécanismes protocolaires

TP et SAÉ

- 7 TP (7 x 2h) sem 4 et 5, sem 9 à 11, sem 13 et 14
  1. découverte des commandes réseau courantes
  2. architecture client-serveur et connexion à distance dans un LAN
  3. étude de protocoles avec l'analyseur Wireshark (2 séances)
  4. configuration des réseaux IP et interconnexion de LAN (3 séances)
- SAÉ sem 5 à 12
  1. thème : installation et configuration d'un serveur Web
  2. séances en autonomie (6 x 2h) : sem 5 et 6, sem 9 à 12
  3. séances encadrées : 1TD (2h) et TP (2h) sem 6
  4. restitution / démo : sem 12

Modalités d'évaluation

- Notes
  - Devoir de Synthèse sem 14 ou 15 (1h30)
  - QCM moodle à la fin de certaines séances de TP (en général, 10mn à la fin de la dernière séance d'un sujet)
  - prérapports pour certains TP
  - remises de rapport ou de relevés de TP pour certains TP
- Absences (en plus des pénalités du livret étudiant)
  - si absence non justifiée, note 0 pour l'activité notée
  - si absence justifiée au CC : non noté
  - si absence justifiée au DS : rattrapage à la demande de l'étudiant·e

Références bibliographiques

- Réseaux, A. Tanenbaum, Pearson Education
- Les réseaux, G. Pujolle, Eyrolles
- Réseaux Informatiques, J. Dordoigne, eni Editions
- Technologie des ordinateurs et des réseaux, P.-A. Goupille, Dunod
- Architecture des réseaux, D. Dromard et D. Seret, Pearson Education
- Réseaux et télécoms, C. Servin, Dunod
- ressources sur Internet : www.guill.net, www.frameip.com, www.commentcamarche.net, fr.wikipedia.org…

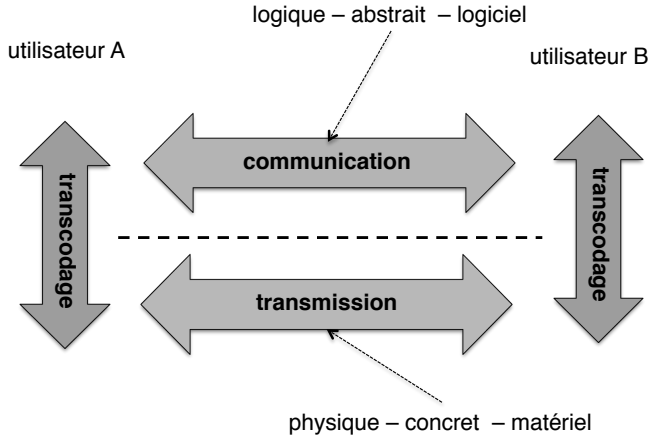
Généralités et terminologie
Introduction

- Réseau
  - ensemble d'entités interconnectée physiquement ou logiquement et communicant entre elles
- Réseau matériel
  - ensemble d'équipements reliés entre eux et échangeant des informations sous forme de signaux
- Réseau informatique
  - réseau entre ordinateurs incluant les équipement d'interconnexion, les services accessibles et les utilisateurs qui les utilisent
  - par la suite : « réseau » désignera « réseau informatique »
- Objectifs
  - partage de ressources et de données
  - échange d'informations
  - réduction des coûts
  - rapprocher les utilisateurs et/ou les services

Généralités et terminologie
Système de communication

- Système de communication
  - ensemble de moyens matériels et logiciels permettant le dialogue entre les utilisateurs et assurant
    - la transmission : représentation du signal, caractéristiques du support, parcours de la distance physique entre utilisateurs…
    - la communication : nommage, adressage, fiabilité, règles du dialogue (protocole), représentation de l'information…
    - le transcodage : relation entre informations, signaux et supports adaptation des signaux aux supports, partage et accès au support…
- Utilisateur : entité utilisant le réseau
  - opérateur humain, ordinateur (matériel), application (logiciel)…

Généralités et terminologie
Système de communication



Généralités et terminologie
Plus concrètement

- Réseau informatique = interconnexion de réseaux
- Utilisateurs connectés directement sur des réseaux locaux via des équipements spécifiques (concentrateurs/hubs ou commutateurs/switchs)
  - maillage (topologie physique) régulier
  - directement accessible
- Réseaux locaux interconnectés par des réseaux fédérateurs ou réseaux de transports via des équipement de routage (routeurs ou passerelles)
  - maillage irrégulier
  - nécessite configuration particulière
- Inter-réseaux = tout ce qui est au delà du réseau local

Généralités et terminologie
Contraintes

- Hétérogénéité
  - diversité des matériels, des logiciels et de systèmes
- Interopérabilité
  - nécessité de communiquer quels que soit les outils utilisés
- Évolution
  - modification, amélioration et perfectionnement des outils et des usages
- Sécurité
  - nécessité de contrôler et de protéger services et données
- Normes
  - respect des standards et des lois
- Coût
  - limitation des budgets accordés

Généralités et terminologie
Éléments d'un réseau

- hôtes : ordinateurs connectés au réseau
  - serveurs : hôtes qui fournissent des ressources partagées ou des services aux utilisateurs
  - clients : hôtes qui accèdent aux ressources partagées et aux services disponibles
- supports de connexion
  - liens physiques entre les équipements pas forcement filaires
- données partagées
  - informations communes accessibles à aux utilisateurs
- périphériques partagés
  - imprimantes, scanners, disques…
- équipements d'interconnexion
  - répéteurs, concentrateurs (hubs), commutateurs (switchs), routeurs, passerelles…

Généralités et terminologie
Identifiants dans les réseaux

- @ symbolique
  - nom textuel de machine complètement ou non complètement qualifié facilitant l'identification des hôtes sur le réseau pour les humains
  - moodle, www.iut-larochelle.com, serverRX.univ-lr.fr
  - organisation hiérarchique par domaine
- @ logicielle ou @IP
  - identifiant de la machine sur 4 octets (IPv4) ou 16 octets (IPv6)
  - exprimée en décimal pour IPv4 : 10.192.50.253
  - permet de rattacher une machine à un réseau logique
- @ matérielle ou @MAC
  - identifie la carte réseau d'une manière unique sur 6 octets
  - exprimée en hexadécimal : 00:0b:5d:db:73:1e
- n° de port
  - identifiant de service pour les applications et l'OS
  - normalisé pour les services standards : 80 (HTTP→Web), 25 (SMTP→Mail), 20-21 (FTP→transfert de fichiers)…

Généralités et terminologie
Équipements d'interconnexion

- répéteurs et concentrateurs/hubs
  - régénèrent et resynchronisent les signaux entre 2 (répéteur) ou plusieurs (concentrateur) segments du réseau
  - ce qui est reçu sur un port est retransmis sur tous les ports
- ponts et commutateurs/switchs
  - connectent 2 (pont) ou plusieurs (commutateur) segments d'un même réseau en séparant les machines au niveau physique
  - ce qui est reçu sur un port n'est retransmis que sur le port du destinataire
- routeurs
  - connectent des réseaux logiques distincts d'un même espace d'adressage
- passerelles
  - solution logicielle aux problèmes d'interconnexion, espaces d'adressages ou protocoles applicatifs différents

Généralité et terminologie
Concepts de base

- débit : D = Data / t
  - quantité d'information (Data) transmise par unité de temps
- délai ou temps de propagation : $t_p = d / V$
  - temps nécessaire à l'information pour parcourir une distance (d) donnée à la vitesse de propagation (V) des signaux
- unités d'information : exprimant la quantité des données
  - bit, octet (8 bits) ou mot de données (2^n octets)
  - unité binaires : kibi (Ki) = 2^{10}, mébi (Mi) = 2^{20}, gibi (Gi) = 2^{30}… (norme)
  - unité décimale : kilo (k) = 10^3, méga (M) = 10^6, giga (G) = 10^9… (usage)
- efficacité = utile / total
  - utile : en général les données utiles (données à transférer)
  - total : en général toutes les données (incluant les surcharges protocolaires tels que les entêtes et/ou les acquittements)

Généralité et terminologie
Concepts de base (suite)

- adressage/nommage
  - attribution aux machines d'un identifiant/nom unique permettant de déterminer le chemin pour les atteindre ou d'avoir un nom pour les désigner
  - nécessité d'un plan d'adressage/nommage cohérent
- acheminement
  - façon dont on convoie les informations jusqu'au destinataire
  - mise en forme des informations pour le transport
  - mécanismes de contrôle logique et/ou physique

Généralité et terminologie
Concepts de base (suite)

- commutation (niveau physique)
  - sélection du bon port de sortie dans un équipement en fonction du destinataire
- routage (niveau logique)
  - détermination du chemin à prendre et des routeurs à traverser pour atteindre le destinataire
- connexion
  - établissement d'un lien physique ou logique entre une source et un destinataire
  - mode connecté
    - 3 phases : ouverture, échange fermeture
    - permet de configurer les paramètres de l'échange et de contrôler ce dernier
  - mode non connecté
    - une seule phase (échange) sans garantie de remise

Généralité et terminologie
Concepts de base (suite)

- Topologie
  - Arrangement physique ou logique des éléments du réseau → bus, étoile, anneau…
    - topologie physique : interconnexion réelle (tel que c'est connecté)
    - topologie logique : simulation par logiciel ou via des équipements particuliers (tel que ça fonctionne)
  - Bus (réseau à diffusion) : tout ce qu'on envoie arrive à tout le monde
  - Étoile : tout passe par un point central (en général un équipement d'interconnexion)
  - Anneau : on est connecté au précédent et au suivant

Généralité et terminologie
Concepts de base (suite)

- type d'architecture : type de lien entre les hôtes
  - client – serveur : les hôtes clients contactent les hôtes serveurs fournissant un ou plusieurs services
    - avantages : ressources centralisées, meilleure sécurité, administration plus simple, évolutif, traitements sur le serveur
    - inconvénients : coût élevé, goulot d'étranglement, point critique
  - poste à poste (peer to peer ou égal à égal) : chaque hôte est un peu client un peu serveur
    - avantages : coût réduit, simplicité
    - inconvénients : difficile à administrer, peu sûr, peu fiable, baisse des performances

Généralité et terminologie
Concepts de base (suite)

25

- catégorie d'un réseau
  - classification des réseaux selon un critère donné, critères possibles = envergure, utilisation
- selon la distance
  - PAN (quelques mètres), LAN (jusqu'à 1km), MAN (campus, ville), WAN (pays, continent)
- selon l'utilisation
  - Internet : gigantesque ensemble de « tuyaux » capables de transférer tout type d'information numérique couvrant tout le globe
    - messagerie électronique, forums de discussion, Web...
  - Intranet : un ensemble de services Internet interne à un réseau local et système d'information interne d'une entreprise
    - clients, serveurs d'applications, serveurs de bases de données...
  - Extranet : extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau
    - problème : sécurité

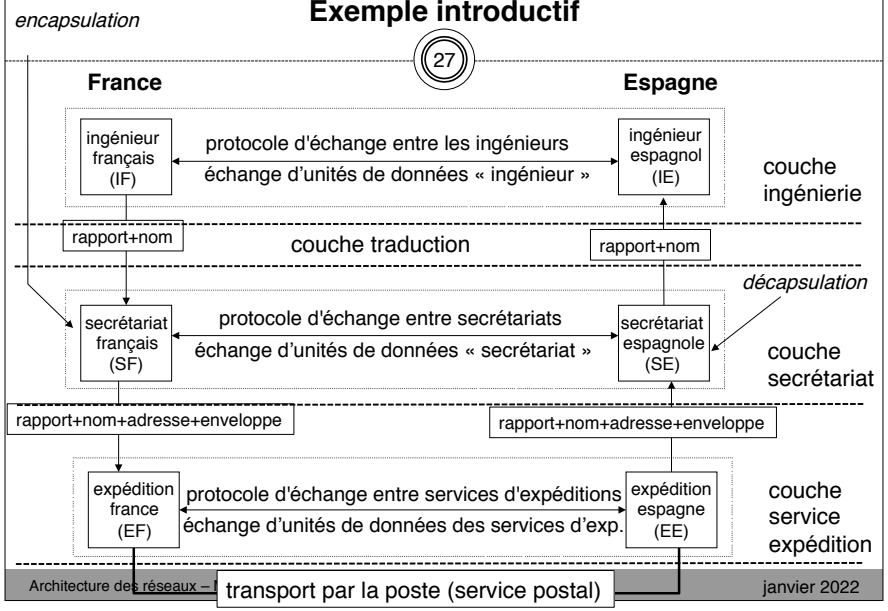
Modèles en couches
Introduction

26

- Idée :
  - transformer un problème complexe de grande taille en un ensemble de problèmes maîtrisables en hiérarchisant
- Objectifs :
  - réduire la complexité
  - faciliter la conception modulaire
  - uniformiser les interfaces
  - assurer l'interopérabilité
  - dégager les fonctions principales des réseaux
- Exemple illustratif :
  - 2 ingénieurs d'Alstom, l'un en France l'autre en Espagne travaillent en commun en échangeant des rapports ← protocole de travail

Modèles en couches
Exemple introductif

27



Modèles en couches
Principes

28

- Hétérogénéité → nécessité de normes internationales
- Solution : modèle d'interconnexion des systèmes ouverts
  - systèmes ouverts = systèmes destinés à communiquer
  - modèle de référence définissant les grandes fonctions d'un système de communication et les relations entre ces fonctions
  - OSI (Open System Interconnection) de ISO (International Standard Organisation) : norme ISO 7498
  - OSI n'est pas un produit mais un ensemble de définitions et de spécifications qu'il faut respecter pour interconnecter des architectures différentes
- Principe : découpage des fonctions du système en ensembles appelés *couches*, il y en a 7
  - chaque couche se pose 3 questions :
    - quoi ? → données ; comment ? → service ; à qui ? → destinataire

Modèles en couches
Principes (suite)

- Une couche offre un ensemble de services en masquant les détails d'implémentation
- Chaque couche est bâtie sur la couche directement inférieure
- Principe d'élaboration des couches :
  - une couche = un niveau d'abstraction
  - chaque couche exerce des fonctions bien définies permettant la définition de protocoles normalisés
  - une couche peut fournir ses service de plusieurs façons différentes
  - l'interface doit minimiser le flux d'information entre couches
  - nombre de couche suffisant
  - si couche absente, service assuré par couche supérieure

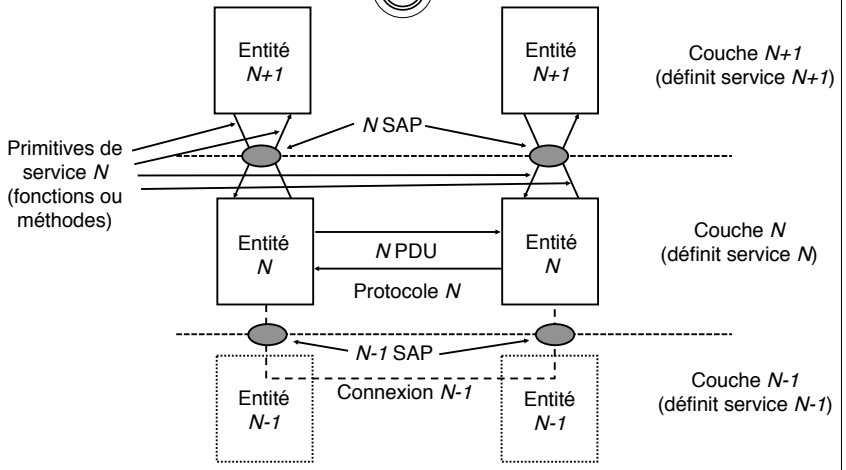
Modèles en couches
Les couches OSI

- Application : sémantique des données et des traitements
- Présentation : syntaxe des données présentées
- Session : gestion du dialogue – synchronisation, début, fin
- Transport : transport transparent de bout en bout avec qualité de service (organisation des données à transférer)
- Réseau : relais et acheminement des données dans le réseau (identification des correspondants et des chemins)
- Liaison de données : transfert sur un tronçon
  - sous-couche LLC : contrôle d'établissement du lien logique
  - sous-couche MAC : contrôle d'accès au support
- Physique : accès physique au support, acheminement de bits et représentation physique de ces derniers

Modèles en couches
Définitions

- entité : élément actif d'une couche (logiciel, OS, pilote, matériel…)
  - il peut y en avoir plusieurs pour une même couche
  - entités homologues : extrémités d'une liaison bout en bout ou tronçon (vertical)
  - entités adjacentes : entités voisines pour demande/exécution de service (horizontal)
- service : capacité de la couche N fournie aux entités N+1
- protocole : ensemble de règles et de formats régissant les données et les traitements entre des entités homologues
  - normalisés et connus d'avance (exemple : HTTP – requête/réponse)
- unité de données de protocoles (PDU) : informations échangées entre deux entités homologues distantes
  - PDU (structure complète) = PCI (entête) + SDU (charge utile)
- point d'accès au service (SAP) : point d'interaction ou interface d'accès entre deux entités adjacentes
- connexion : canal d'échange entre 2 entités homologues
- primitive de service : interactions entre couches adjacentes
  - classées par type et par catégorie

Modèles en couches
Définitions



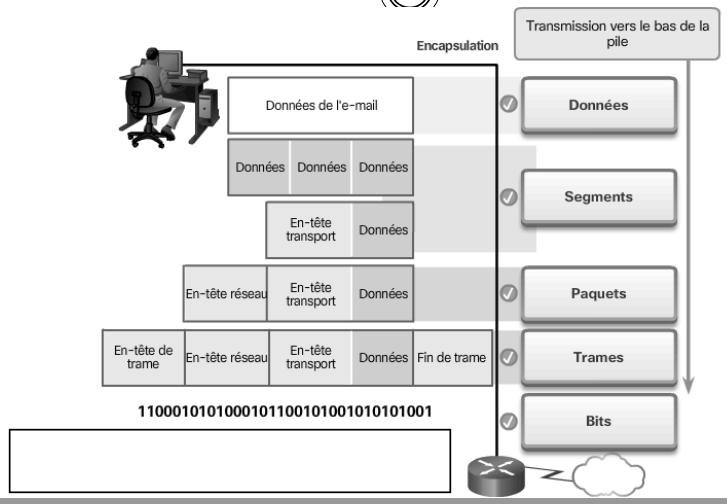
Modèles en couches
Flux de données et encapsulation

33

- Encapsulation des données
  - chaque couche N reçoit des données de la couche N+1
  - l'incorpore dans sa propre structure de données
  - demande à la couche N-1 de traiter/envoyer/transmettre à son tour cette nouvelle unité de données de la couche N
- Ordre d'encapsulation
  - Données applicatives – Messages (couches 5 à 7 : A, P, S)
  - Segments (couche 4 : T)
  - Paquets (couche 3 : R)
  - Trames (couche 2 : L)
  - Bits (couche 1 : ϕ)
- Exemple : envoie d'un courrier électronique

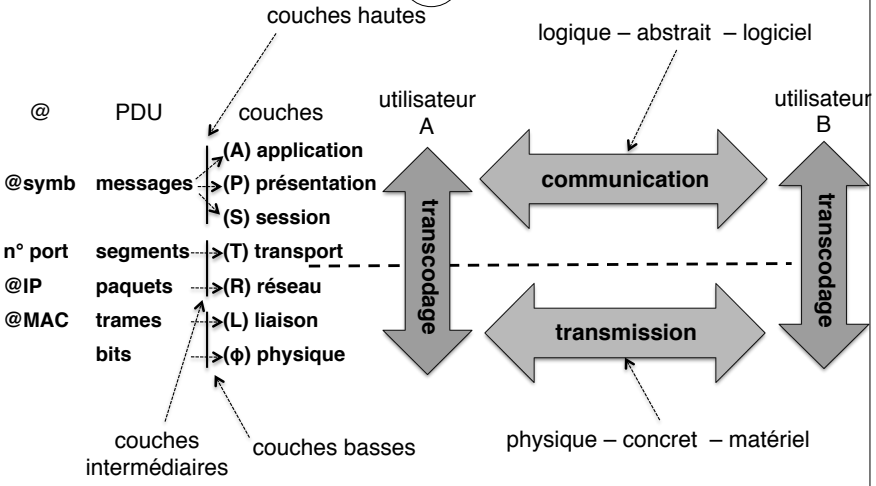
Modèles en couches
Encapsulation dans le modèle TCP/IP

34

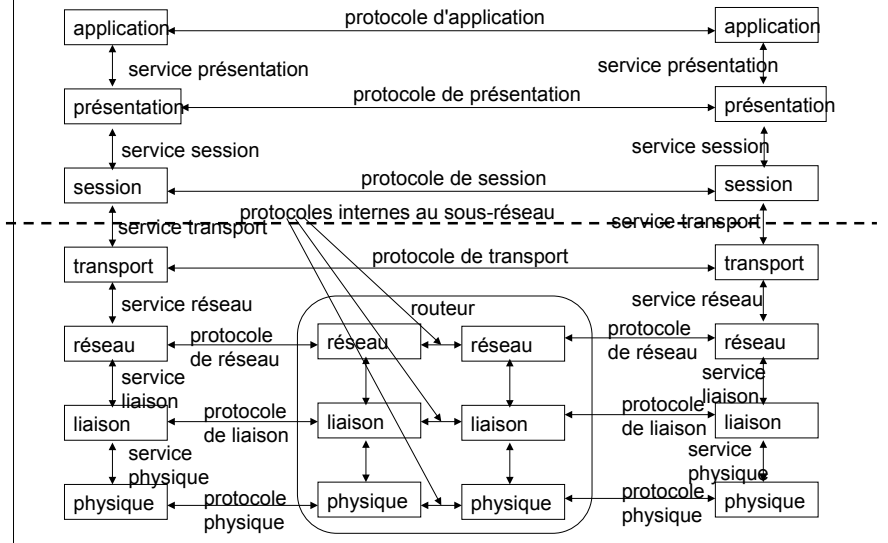


Généralités et terminologie
Système de communication

35



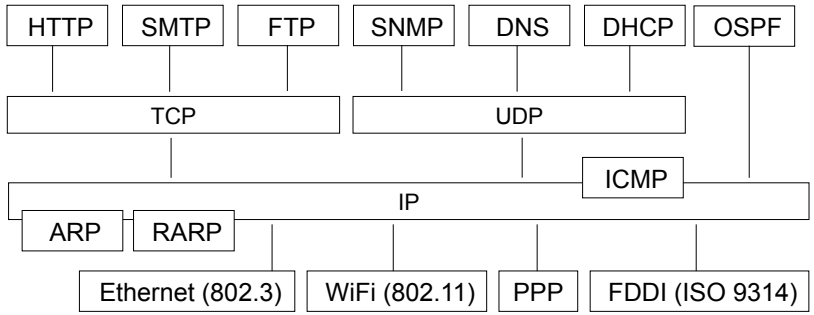
Modèles en couches
Encapsulation intermédiaire



Modèles en couches
Modèle TCP/IP

- Modèle de l'Internet (mais également des réseaux locaux)
  - Application : sémantique et syntaxe des données, traitement des données, gestion des dialogues
    - protocoles : HTTP, FTP, DNS, SMTP, DHCP…
  - Transport : gestion du transport de bout en bout
    - protocoles : TCP (mode connecté avec acquittements), UDP (mode non connecté)
  - Réseau : relais et acheminement de bout en bout
    - protocoles : IP, ICMP, ARP, RARP
  - Liaison MAC (Medium Access Control) : contrôle d'accès au support et transfert sur un tronçon du chemin
    - protocoles : Ethernet (LAN), WiFi (LAN), FDDI (MAN), PPP (WAN), ATM (WAN)…

Modèles en couches
Exemple de piles de protocoles TCP/IP



Modèle en couches
Adressage dans le modèle TCP/IP

- Identification d'un hôte dans le réseau ou d'un service
  - Application : @ symboliques (pour les hôtes) ou URL (pour les ressources telles que les fichiers)
  - Transport : numéro de port (pour les services)
  - Réseau : @ IP ou @ logiques (pour tout équipement adressable)
  - Liaison MAC : @ MAC ou @ physiques ou @ matérielles (pour toute carte pouvant accéder au réseau)
- Nécessité de protocoles et de services de correspondance
  - ARP = associer @ MAC à une @ IP
  - DNS = correspondance @ symbolique - @ IP

Réseaux locaux
L'accès au réseau

- LAN = partage d'un support de transmission unique
  - souvent un seul tronçon du réseau
  - nécessité de la répartition de l'accès au support entre les utilisateurs
    - règles d'accès au support et de résolution de conflits d'accès
    - rôle de la sous-couche MAC (Media Access Control)
    - méthode de contrôle d'accès mise en œuvre par le protocole de la sous-couche MAC de la couche Liaison de données
- Méthode d'accès
  - a des répercussions sur les caractéristiques du niveau physique
  - dépend plus ou moins de la topologie choisie/utilisée
    - la topologie choisie impose des composants d'accès et va +/- bien s'adapter à une méthode d'accès donnée
- Trois grandes familles de méthodes
  - accès statique (très ancien et pas flexible), accès déterministe (garantit un temps maximum pour l'accès), accès aléatoire (le plus répondu)

Réseaux locaux
Ethernet DIX, CSMA/CD et IEEE 802.3

41

- Ethernet = un des premiers types de LAN
  - protocole de la couche Liaison de données (fonctionnalités MAC)
  - standard DIX défini en 1978 (Digital/Intel/Xerox)
  - normalisé par IEEE (norme IEEE 802.3), reprise ensuite par ISO (norme ISO/IEC 8802-3)
- CSMA/CD = méthode d'accès utilisée par Ethernet
  - Carrier Sense Multiple Access / Collision Detection (accès multiple par écoute de porteuse avec détection des collisions)
  - méthode décentralisée à compétition
  - chaque machine décide en fonction de ce qu'elle voit
- Actuellement le protocole le plus répondu dans les réseaux locaux filaires

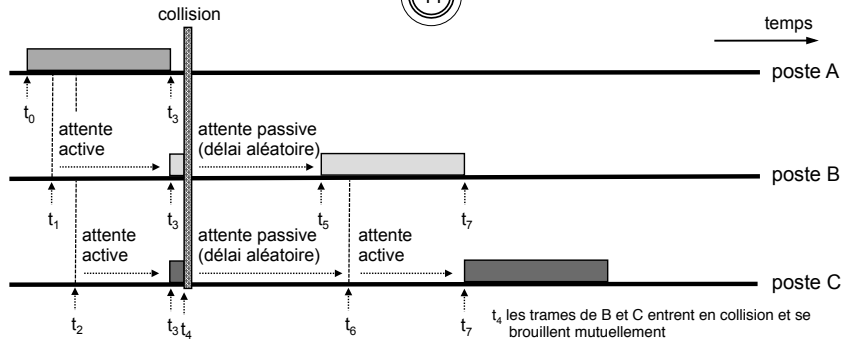
Réseaux locaux
Principe de Ethernet, CSMA/CD et 802.3

42

- Diffusion des messages à tous les hôtes du réseau
  - topologie logique = bus
  - problème = collisions de trames lors d'envois simultanés
- Principe de fonctionnement
  - on écoute le bus avant d'émettre (afin d'éviter les collisions avec des émissions en cours) :
    - pas de porteuse ? (canal libre) ⇒ on émet
    - porteuse ? (canal occupé) ⇒ on attend jusqu'à la libération du support (attente active)
  - la collision est détectée par écoute permanente du bus, si ce qu'on entend diffère de ce qu'on émet :
    - collision en cours
    - arrêt de l'émission
    - réémission plus tard (exécution du BEB pour déterminer le temps d'attente et attente passive jusqu'à expiration de ce temps)

Réseaux locaux
Accès au média avec CSMA/CD

44



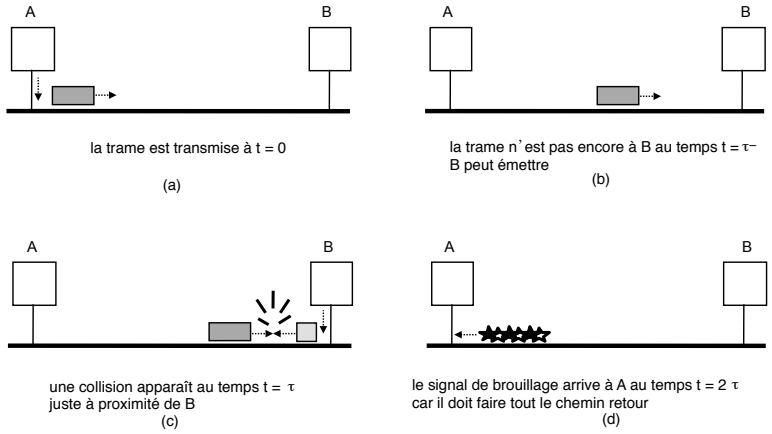
t_0 A veut émettre une trame, écoute le support (via sa carte réseau), le support est libre à la sortie de A, A émet
t_1 B veut émettre une trame, écoute le support (via sa carte réseau), le support est déjà occupé (trame de A), B se met en attente active
t_2 C veut émettre une trame, écoute le support (via sa carte réseau), le support est déjà occupé (trame de A), C se met en attente active
t_3 A a fini d'émettre et libère le support
t_3 B constate la libération du support, à la fin de la propagation de la trame de A, et émet
t_3 C constate la libération du support, à la fin de la propagation de la trame de A, et émet
t_4 les trames de B et C entrent en collision et se brouillent mutuellement
B et C exécutent le BEB pour déterminer le délai d'attente et se mettent en attente passive
t_5 B a fini d'attendre, le support est libre, B émet
t_6 C a fini d'attendre, le support est occupé par B, C se met en attente active
t_7 B a fini d'émettre et libère le support, C émet

Réseaux locaux
Le protocole Ethernet

45

- Fenêtre de collision (ou slot ou tranche canal)
  - temps aller/retour entre les deux hôtes les plus éloignés du LAN
  - conditionne la taille minimale des trames (PDU Ethernet)
  - à l'origine avec D=10 Mbit/s, V=10^5 km/s et d = 2,5 km la norme a fixé taille minimale de la trame Ethernet à 64 octets
- Domaine de collision (Ethernet commuté)
  - ensemble d'hôtes observant les mêmes collisions
  - hôtes situés sur le même port d'un switch
    - 1 port de switch= 1 domaine de collision
- BEB (Binary Exponential Backoff)
  - algorithme exécuté localement permettant de calculer le temps aléatoire d'attente passive après une collision
  - taille de l'intervalle du tirage augmente exponentiellement à chaque nouvelle collision de la même trame

Réseaux locaux
Fenêtre de collision



Réseaux locaux
La trame Ethernet

Format de la trame

Préambule	@destination	@source	type/longueur	données + bourrage (PAD)	FCS
8 octets	6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

longueur minimale ⇒ 64 octets — longueur maximale ⇒ 1518 octets

- Préambule : permet la synchronisation du récepteur
  - champ géré par la couche physique
  - représente une séquence alternée de 1 et 0
  - le dernier 1 est doublé pour indiquer que la trame commence
  - le début du préambule peut être perdu par la couche physique

Réseaux locaux
La trame Ethernet (suite)

- Adresses destination et source
  - @MAC (uniques) des cartes réseaux du destinataire et du récepteur
  - taille = 6 octets : 3 octets constructeur et 3 octets identifiant (exemple 08 00 20 = SUN, 00 AA 00 = Intel, 00 06 5B = DELL)
  - il est possible d'émettre à plusieurs stations en même temps
    - BROADCAST : envoi à toutes les stations @MAC_dest = FF FF FF FF FF FF
    - MULTICAST : envoi à un groupe de stations 1er bit du 1er octet est à 1
    - MULTICAST constructeur : envoi à toutes les machines d'un même constructeur
  - ne sont pas réservées à Ethernet

Réseaux locaux
La trame Ethernet (suite)

- Type/Longueur : différence fondamentale entre la norme Ethernet et la norme IEEE 802.3
  - avec Ethernet : le champ est « type »
    - type du protocole de niveau 3 (couche réseau) utilisé
    - sert d'aiguillage vers le protocole du niveau supérieur (exemple 0800 = IP, 0805 = X25, 0806 = ARP)
    - utilisé principalement lorsqu'il n'y a pas de sous couche LLC
  - avec 802.3 : le champ est « longueur »
    - longueur des données utiles (hors bourrage)
    - le type est alors défini dans le protocole de la sous-couche LLC
  - pour les distinguer on regarde la valeur du champ
    - si > 1500 (0x5DC) ⇒ Ethernet, sinon 802.3

Réseaux locaux
La trame Ethernet (suite)

- Données + bourrage : ce qui est transporté par la trame
  - champ données = paquet niveau 3 (ou PDU d'un protocole supérieur, LLC par exemple)
  - bourrage = caractères non significatifs pour arriver à des trames de 64 octets
- FCS (Frame Check Sequence) : champ de contrôle de la trame sur 4 octets
  - code CRC (Cyclic Redundancy Code) de degré 32 qui englobe tout sauf le préambule
- Temps Inter Trame (IFG) : d'une durée de 96 bits pour un débit à 10Mbit/s
  - permet un repos aux circuits électroniques après une émission
  - donne l'occasion à d'autres stations de prendre la main

Réseaux locaux
Trames Ethernet incorrectes

- Les incidents sur le réseau peuvent générer des trames particulières parfois incompréhensibles (éliminées par la sous-couche MAC)
  - Runt : trame de moins de 64 octets
  - Jabber : trame trop longue (plus de 1518 octets)
  - trame désalignée (nombre de bits pas divisible par 8)
  - Bad CRC : CRC calculé différent du CRC reçu
  - Jam : trame de 32bits signalant une collision

Réseaux locaux
Interconnexion dans les réseaux locaux

- Étendre la portée géographique
- Respecter les particularités des services
  - administration, ingénierie, production, recherche, étudiants…
- Structurer le réseau de l'établissement ou de l'entreprise en fonction de l'organisation permet de
  - limiter le rayon d'action de certains serveurs
  - circonscrire la circulation des informations secrètes
  - limiter les accès à ou depuis certaines machines
  - diminuer la vulnérabilité du réseau
    - limiter les effets des défaillances
    - limiter la portée des actions malveillantes

Réseaux locaux
Moyens d'interconnexion dans les LAN

- Plusieurs moyens d'interconnexion existent (éventuellement en passant pas un FAI)
  - par un appareil dédié (équipement d'interconnexion ou relais)
  - par un réseau intermédiaire dit de transport
  - par une ligne spécialisée
- Il existe 3 techniques d'interconnexion pour les relais
  - conversion de service : protocoles différents mais compatibles
    - exemple : adaptation de média ou de débit comme passer de FastEthernet (100Mbit/s) au Gigabit Ethernet (1000Mbit/s) ou communiquer entre WiFi 802.11g, 802.11n et 802.11ac
  - conversion de protocole : protocole changé en cours de route
    - exemple : passage de Ethernet à WiFi
  - encapsulation : les PDU du protocole A transportés par les PDU de B
    - exemple : paquets NetBios transportés par des paquets IP
- Les principes énoncés sont généraux, ils ne sont pas réservés à Ethernet et peuvent s'appliquer à d'autres réseaux

Réseaux locaux
Différents types de relais

- Répéteurs (niveau 1 - connectivité physique)
  - régénère le signal et étend la portée d'un tronçon réseau
  - convertisseurs de média et/ou de débit
  - concentrateurs (hubs) = répéteurs multiport
  - de plus en plus rares dans les réseaux locaux au profit des switchs
- Ponts (niveau 2 - filtrage et commutation MAC, VLAN)
  - ne retransmet sur un port que si le destinataire (@MAC) s'y trouve
  - commutateurs (switchs) = pont multiport
  - domaine de collision par port de switch
- Routeurs (niveau 3 - filtrage et commutation IP)
  - interconnexion de réseaux (architecture de l'Internet notamment)
  - espace d'adressage homogène
- Passerelles (niveau 3 et au delà)
  - interconnexion applicative : solution logicielle pour l'interconnexion
  - espace d'adressage éventuellement hétérogène

Interconnexion des réseaux
Généralités sur la couche Réseau

- La couche réseau définit un espace d'adressage homogène pour pouvoir interconnecter des LAN
  - permet de mettre en place des WAN
- Pour pouvoir communiquer dans un WAN il est important de
  - pouvoir identifier la machine qu'on veut atteindre
  - véhiculer correctement les paquets jusqu'au destinataire final
- Ces deux points représentent les deux notions de base mises en œuvre par la couche réseau
  - adressage : attribution des adresses logiques
  - routage : aiguillage des paquets et leur propagation depuis une extrémité du réseau jusqu'à l'autre
- Le protocole choisi doit impérativement les mettre en œuvre
  - protocole le plus répondu est IP : Internet Protocol
    - basé sur la commutation de paquets dans des réseaux irréguliers et fortement maillés
    - 2 versions co-existent : IPv4 (rfc 791) et IPv6 (rfc 2460)

Interconnexion des réseaux
Adressage IPv4

- Adresses de 4 octets (32 bits) exprimés en décimal et séparés par des '.'
  - en IPv6 c'est 16 octets (128 bits) exprimés en hexa
- Schéma d'adressage hiérarchique
  - une partie identifie le réseau auquel est rattaché la machine :
    - id_réseau (identifiant réseau ou partie réseau)
    - dans un même réseau, toutes les machines ont le même identifiant réseau mais des identifiants machines différents
  - l'autre partie identifie la machine dans le réseau concerné :
    - id_machine (identifiant machine ou partie machine)
  - la limite entre id_réseau et id_machine est variable et définie par le masque réseau (ou masque de sous-réseaux)
    - est le même pour toutes les machines d'un même LAN

Interconnexion des réseaux
Adresse machine, adresse réseau, masque

@IP :
- utilisation décimale
- traitement binaire

@IP d'une machine ⟶ 140.179.220.200

@IP binaire 10001100.10110011.11011100.11001000

id_réseau && id_machine

masque 11111111.11111111.00000000.00000000

255 . 255 . 0 . 0

=

10001100.10110011.00000000.00000000

@réseau 140.179.0.0

Interconnexion des réseaux
Adresse machine, adresse réseau, masque (suite)

masque (toujours exprimé en décimal comme les @IP) :
- bits 1 à gauche et bits 0 à droite
- limite entre 1 et 0 peut être n'importe où (selon plan d'adressage)

@IP d'une machine ⟶ 140.179.220.200

@IP binaire 10001100.10110011.11011100.11001000

id_réseau && id_machine

masque 11111111.11111111.11111000.00000000

255 . 255 . 248 . 0

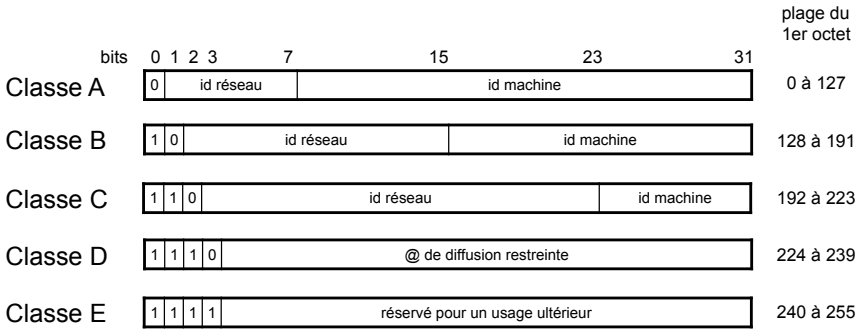
=

10001100.10110011.11011000.00000000

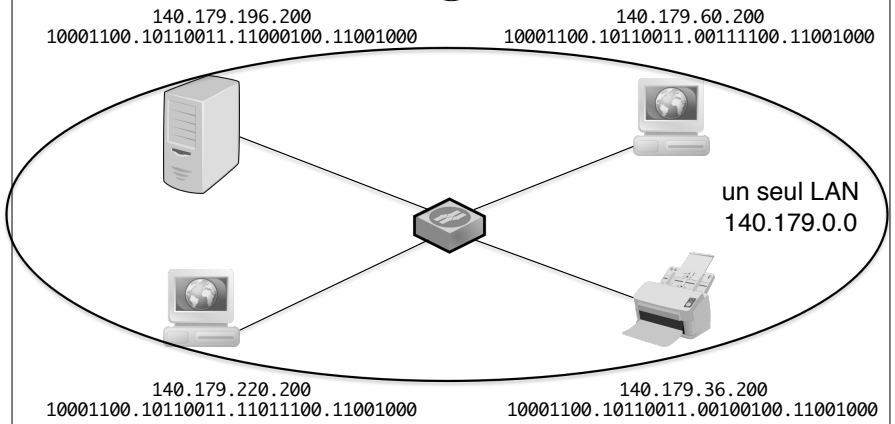
@réseau 140.179.216.0

Interconnexion des réseaux
Classes d'adresses

- 5 classes sont définies par la norme IP
  - les 4 premiers bits de l'@ définissent sa classe
  - chaque classe a un masque par défaut (mais qu'on peut adapter)

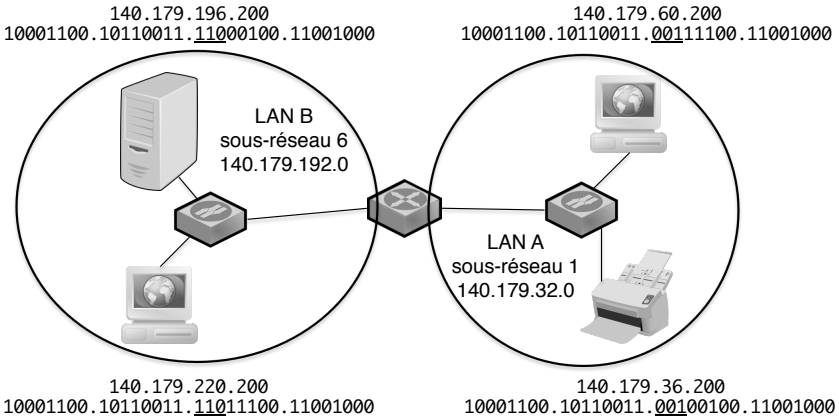


Interconnexion des réseaux
Découpage en sous-réseaux



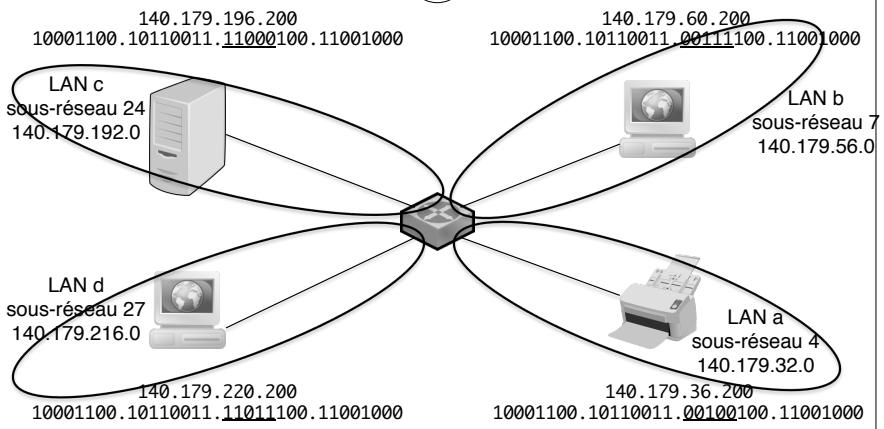
masque par défaut 255.255.0.0 : 11111111.11111111.00000000.00000000

Interconnexion des réseaux
Découpage en sous-réseaux



masque sur 19 bits, 255.255.224.0 : 11111111.11111111.**111**00000.00000000

Interconnexion des réseaux
Découpage en sous-réseaux



Interconnexion des réseaux
Adresses particulières

- 0.0.0.0 : n'importe quelle @
  - @IP par défaut si pas de configuration IP, utilisée notamment avec durant la phase d'initialisation avec DHCP
- @ dont le premier octet = 127 : boucle locale
  - 127.0.0.1 : @ de la machine locale (localhost)
- id_machine particuliers (tout à 0 ou tout à 1)
  - id_réseau.0 : identifie le réseau concerné
  - id_réseau.255 : @ de diffusion sur le réseau concerné
- adresses pour les réseaux privés (non routables tels quels sur les réseaux publics dont Internet)
  - 10.0.0.0 à 10.255.255.255 (1 réseau classe A)
  - 172.16.0.0 à 172.31.255.255 (16 réseaux classe B)
  - 192.168.0.0 à 192.168.255.255 (256 réseaux classes C)
- APIPA (Automatic Private Internet Protocol Addressing)
  - 169.254.0.0/16

Interconnexion des réseaux
Remarques sur l'adressage IPv4

- les paquets destinés à des @ particulières ne sont pas réémis vers d'autres réseaux
  - ne traversent pas les routeurs (sont arrêtés par ces derniers)
- un organisme international (ICANN – Internet Corporation for Assigned Names and Numbers) est chargé d'attribuer les adresses
- il est possible de personnaliser une plage d'@ en la divisant en plusieurs sous-réseaux → subnetworking
  - on utilise une partie de l'id_machine pour désigner un sous-réseau au sein du réseau identifié par id_réseau
  - masque couvre alors id_réseau + id_sous_réseau
- le masque peut s'exprimer avec un `/nb_de_bits_à_1` collé à une adresse IP
  - 140.179.220.200/18 → masque = 255.255.192.0 (18 bits à 1)

Interconnexion des réseaux
Routage IP

- Acheminer un paquet d'un endroit du réseau à un autre
  - le paquet IP passe de routeur en routeur jusqu'au LAN destinataire
  - chaque routeur (sauf le dernier) transmet le paquet reçu vers le prochain routeur sur le chemin vers le destinataire
  - le dernier routeur envoie le paquet vers le destinataire du paquet
- Le routeur fait de la commutation de paquet
  - les ports d'un routeur s'appellent « interfaces » et ont une @IP (ce sont des cartes réseaux)
    - l'@IP d'une interface a la même partie id_réseau que le réseau qu'elle relie
  - le routeur sélectionne l'interface de sortie qui se trouve sur le réseau à traverser vers le prochain routeur jusqu'au destinataire
  - chaque routeur tient à jour une table de routage permettant de déterminer où il faut renvoyer les paquets reçus

Interconnexion des réseaux
Table de routage

66

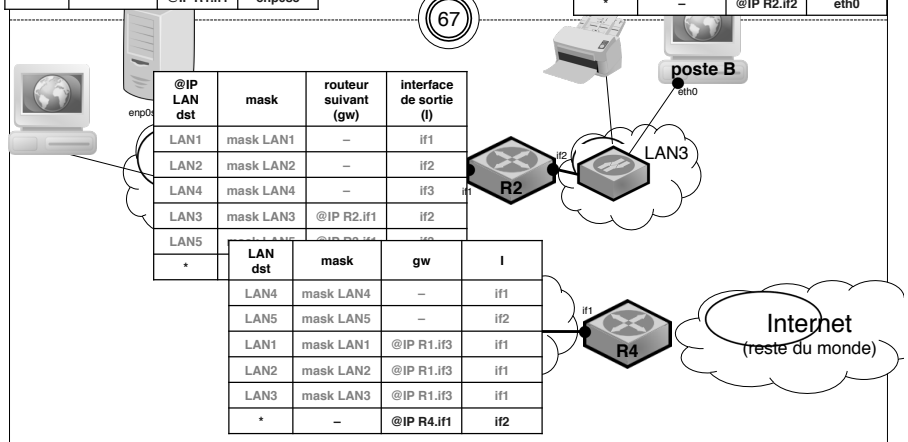
- Le routage se fait en fonction de la partie id_réseau des @IP et donc des @réseau
  - il est indépendant de la source
- Les entrées (routes) d'une table de routage peuvent être :
  - des entrées générales : <@, [mask], gw, I> ⇒ **routes explicites**
    - le LAN destinataire « @ » avec le masque « mask » est accessible via l'interface « I » du routeur et le prochain nœud (routeur) du chemin est « gw »
    - « I » et « gw » sont forcement sur le même réseau
  - des routes <@, [mask], –, I> désignant les LAN directement accessibles sans passer par un autre routeur ⇒ **routes locales**
    - « @ » se trouve forcement sur le réseau de l'interface « I »
  - une entrée particulière <*, [–], gw ,I> définissant la **route par défaut**
    - « * » signifie que toutes les autres adresses sont accessibles via l'interface « I » en passant par « gw »

@IP LAN dst	mask	routeur suivant (gw)	interface de sortie (I)
LAN1	mask LAN1	–	enp0s3
*	–	@IP R1.if1	enp0s3

connexion des rés
ple de tables de ro

67

@IP LAN dst	mask	routeur suivant (gw)	interface de sortie (I)
LAN3	mask LAN3	–	eth0
*	–	@IP R2.if2	eth0



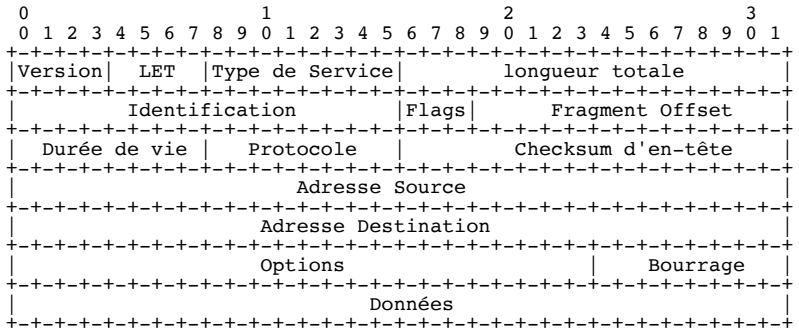
@IP LAN dst	mask	routeur suivant (gw)	interface de sortie (I)
LAN1	mask LAN1	–	if1
LAN2	mask LAN2	–	if2
LAN4	mask LAN4	–	if3
LAN3	mask LAN3	@IP R2.if1	if2
LAN5			
*			

LAN dst	mask	gw	I
LAN4	mask LAN4	–	if1
LAN5	mask LAN5	–	if2
LAN1	mask LAN1	@IP R1.if3	if1
LAN2	mask LAN2	@IP R1.if3	if1
LAN3	mask LAN3	@IP R1.if3	if1
*	–	@IP R4.if1	if2

Interconnexion des réseaux
PDU IP

68

- Structure du paquet IP



Interconnexion des réseaux
Filtrage et NAT/PAT

69

- Les routeurs peuvent jouer un rôle de filtre, on parle alors de « pare-feu » ou de « firewall » ou de « garde-barrière »
  - fonction désormais indispensable pour la protection des réseaux
  - le filtrage peut porter sur n'importe quel champ de l'entête IP et éventuellement TCP/UDP
    - filtres courants = blocage de ports, d'adresses ou de protocoles
- La translation consiste à substituer certaines @IP (NAT) ou n° de port (PAT) par d'autres lors de la traversée du routeur
  - mascarading = substituer @IP sources (souvent privées) des paquets sortants par l'@IP extérieure du routeur (publique)
    - seulement le routeur est visible en dehors du LAN
    - l'opération inverse est effectuée à la réception de la réponse
  - PAT = substituer un n° port dst par un autre dans un paquet entrant
    - permet de garder secret le port réel d'écoute d'un serveur

Couche Réseau
Filtrage IP – exemple de NetFilter

- NetFilter est le pare-feu intégré aux systèmes Linux accessible avec la commande `iptables`
- Il est possible de le configurer pour effectuer un filtrage et traitement des paquets IP :
  - sécuriser le réseau en contrôlant ce qui entre, sort ou traverse une machine
  - limiter le trafic
  - translation d'adresses (NAT) ou de ports (PAT)
  - marquage de paquets
- Les chaînes ou hooks (ou encore points d'accrochage) définissent les points sur lesquels des modules de traitement des paquets vont se greffer
  - PREROUTING, INPUT, FORWARD, POSTROUTING, OUTPUT

Couche Réseau
Filtrage IP – exemple de NetFilter (2)

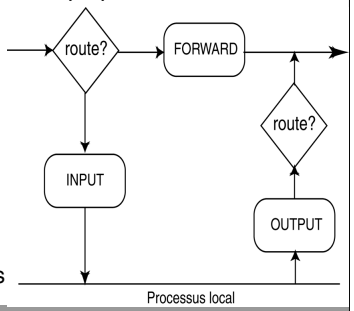
- Les 5 chaînes correspondant aux différents points d'ancrages (hooks) sont réparties dans des tables de traitement et regroupent les règles identifiant les paquets selon des critères définis et les envoyant sur une cible choisie
  - chaîne INPUT
    - décide du sort des paquets entrant localement sur l'hôte (destinés explicitement au routeur)
  - chaîne OUTPUT
    - décide du sort des paquets émis localement par l'hôte (émis explicitement par le routeur)
  - chaîne FORWARD
    - décide du sort des paquets qui traversent l'hôte (ni l'émetteur ni le récepteur du paquet n'est le routeur lui-même)
  - chaîne PREROUTING
    - décide du sort des paquets qui arrivent sur l'hôte avant même la décision du routage
  - chaîne POSTROUTING
    - décide du sort des paquets qui sortent de hôte après tous les autres traitement et notamment la décision de routage

Couche Réseau
Filtrage IP – exemple de NetFilter (3)

- À travers ces points d'insertion, Netfilter va pouvoir
  - effectuer le filtrage de paquets – table *filter* (défaut)
  - effectuer des opérations de NAT ou PAT – table *nat*
  - effectuer des opérations de marquage des paquets, pour leur appliquer un traitement spécial – table *mangle*
- Il y a dans Netfilter trois tables
  - « filter » : filtrage des paquets (table par défaut)
  - « NAT » : translation d'adresses (masquerading)
  - « mangle » : marquage des paquets (en modifiant leur qualité de service)
- Chaque table agit sur des chaînes bien définies et offre des cibles possibles aux règles
  - par exemple : la table filter agit sur les chaînes INPUT, OUTPUT et FORWARD, et propose les cibles : ACCEPT, DROP, LOG, REJECT…

Couche Réseau
Filtrage IP – exemple de NetFilter (4)

- Processus de filtrage – table *filter*
  - un paquet entrant, passe d'abord par la fonction de décision de routage
    - si le paquet est destiné au hôte local, il traverse la chaîne INPUT et, s'il n'est pas refusé, est transmis au processus local impliqué.
    - si le paquet est destiné à un hôte d'un autre réseau, il traverse la chaîne FORWARD et s'il n'est pas refusé, il poursuit alors sa route
  - un paquet envoyé par notre machine, traverse la chaîne OUTPUT et, s'il n'est pas rejeté, va vers la sortie
  - chaque chaine contient
    - des critères de sélection des paquets
    - une cible pour les paquets correspondants



Couche Réseau
Filtrage IP – exemple de NetFilter (5)

- Les règles spécifient les critères recherchés dans l'entête du paquet (@IP, protocole intérmédiaire, port…) et la cible en cas de test positif
- Les cibles sont des sortes d'aiguillage qui dirigent les paquets satisfaisant aux critères. Les cibles préconstruites sont :
  - ACCEPT
    - les paquets qui satisfont aux critères sont acceptés, ils continuent leur chemin dans la pile
  - DROP
    - les paquets qui satisfont aux critères sont rejetés, on les oublie, on n'envoie même pas de message ICMP
  - LOG
    - c'est une cible particulière qui permet de tracer au moyen de syslog les paquets qui satisfont aux critères
  - D'autres cibles deviennent accessibles suivant le contexte : REJECT, RETURN, REDIRECT…

Couche Réseau
Filtrage IP – utilisation de `iptables`

- iptables [-t *table*] -[AD] *chaîne règle* [*options*]
- iptables [-t *table*] -I *chaîne* [*numéro-de-règle*] *règle* [*options*]
- iptables [-t *table*] -R *chaîne numéro-de-règle règle* [*options*]
- iptables [-t *table*] -D *chaîne numéro-de-règle* [*options*]
- iptables [-t *table*] -[LFZ] [*chaîne*] [*options*]
- iptables [-t *table*] -N *chaîne*
- iptables [-t *table*] -X [*chaîne*]
- iptables [-t *table*] -P *chaîne cible* [*options*]
- iptables [-t *table*] -E *ancien-nom-de-chaîne nouveau-nom-de-chaîne*

Couche Réseau
Filtrage IP – utilisation de `iptables` (2)

- utilisation d'une table : `iptables –t table`
  - *table* = filter, nat ou mangle (par défaut c'est « filter »)
- affichage de la table : `iptables –t table –L`
- ajout d'une règle : `iptables –t table –A` suivi des critères de sélection et de la cible
- @source du paquet : -s ou --source *adresse/mask*
  - pour l'@dest du paquet : -d ou --destination
- interface d'entrée : -i ou --in-interface
- interface de sortie : -o ou --out-interface
- spécifier un protocole intermédiaire : -p ou --protocol
  - protocoles acceptés : icmp, tcp et udp
- spécifier un port avec TCP/UDP : --sport ou –dport
  - permet de spécifier le protocole applicatif (80 ou http pour HTTP)

Couche Réseau
Filtrage IP – utilisation de `iptables` (3)

- ajout d'un filtre du trafic TCP entrant sur le port 22 (protocole applicatif SSH) avec rejet silencieux
  - iptables -A INPUT -p tcp --dport 22 -j DROP
  - iptables -A INPUT -p tcp –dport ssh -j DROP
- insertion en 2e position d'un filtre du trafic traversant issu de @IP A.B.C.D et arrivant sur interface eth0 avec rejet verbeux
  - iptables -I FORWARD 2 -i eth0 -s A.B.C.D -j REJECT
- changement des @source en 1.2.3.4
  - iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4
- masquerading de tout ce qui sort par interface ppp0
  - iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE

Services réseau courants
Introduction et principes

- On distingue 2 types de services « réseau »
  - les services « utilisateur »
    - destinées à rendre un service précis directement à l'utilisateur
    - principalement (voire exclusivement) couche Application
    - consultation de page web, échange de fichiers, messagerie électronique, jeux…
  - les services auxiliaires
    - permettent/facilitent l'accès au réseau et l'utilisation des services « utilisateur »
    - se situent n'importe où dans la pile OSI selon besoin
    - résolution identifiants/adresses, configuration dynamique…

Services réseau courants
ARP - *Address Resolution Protocol* (rfc 826)

- Protocole de la couche Réseau directement au dessus de la couche Liaison (n'utilise pas IP)
- Permet de trouver la correspondance entre une @IP et @MAC dans un réseau local
  - associe à @IP recherchée (connue), l'@MAC de la carte réseau correspondante (inconnue) dans un LAN
  - protocole décentralisé (pas de serveur dédié)
    - diffusion de la demande dans tout le LAN « Qui a @IP ? »
    - uniquement la carte concernée répond « C'est moi ! »
    - ne traverse pas les routeurs
- Résolution inverse faite par RARP (Reverse ARP)
  - moins utilisé que ARP, centralisé (dans routeurs), rfc 903

Services réseau courants
ICMP - *Internet Control Message Protocol* (rfc 792)

- Protocole de la couche Réseau au dessus de IP
- Est utilisé pour véhiculer des messages d'information, de contrôle et d'erreur au niveau IP
  - compense les lacunes de IP en définissant un ensemble de messages de gestion (principalement signalisation d'erreur)
  - peut être vu comme le « mécanisme d'acquittement » de IP
  - en général transparent pour l'utilisateur
    - à l'exception de `echo request` et `echo reply` (ping) est géré automatiquement par les modules IP
- Par exemple, il permet de :
  - signaler que la destination est non accessible
  - signaler qu'il y a eu une redirection par un routeur
  - vérifier si un hôte est présent dans le réseau
  - …

Services réseau courants
DNS - *Domain Name System* (rfc 1034 et rfc 1035)

- Protocole couche Application (au dessus de UDP, port 53)
- Annuaire de correspondances @symboliques - @IP
  - service centralisé offert par un serveur
  - système des @symboliques (noms de domaines)=arborescence
    - nœud = domaine géré par au moins un serveur DNS
    - feuille = machine
    - chemin dans l'arborescence = FQDN de la machine
- Principe
  - le client envoie sa demande de résolution à son serveur
  - le serveur se charge de trouver la réponse
    - soit il la connaît soit il interroge d'autres serveurs selon le domaine du destinataire
  - il est possible de garder certaines correspondances fréquentes en local (fichier /etc/hosts sous Linux ou cache DNS)

Services réseau courants
DHCP - *Dynamic Host Configuration Protocol* (rfc 2131)

- Protocole couche Application (au dessus de UDP, ports 67 et 68)
- Mécanisme client-serveur d'attribution dynamique d'@IP et des paramètres réseaux courants
- Le serveur DHCP gère des plages d'@IP et les attribue à la demande
  - au démarrage un hôte n'a ni @IP, ni l'@IP du serveur DHCP
  - il contacte (par diffusion IP) les serveurs accessibles pour avoir une @IP et des paramètres réseaux valides
  - chaque serveur DHCP accessible renvoie une offre d'@IP
    - le serveur DHCP peut être sur un autre LAN
  - le client choisit parmi les réponses reçues et diffuse son choix
  - les serveurs non sélectionnées invalident leur proposition
  - le serveur choisi confirme son offre

Services réseau courants
NTP - *Network Time Protocol* (rfc. 1305)

- Protocole couche Application (au dessus de UDP port 123)
- Synchronisation de l'horloge locale des ordinateurs sur une heure de référence
  - heure de référence fournie en UTC (nb sec depuis minuit 1/1/1900)
  - architecture hiérarchique où
    - chaque niveau est appelé « strate »
    - strate 0 = récepteurs récupérant l'heure de référence par radios, câbles, satellites ou directement depuis une horloge atomique
    - strates intermédiaires = serveurs de temps récupérant l'heure auprès des récepteurs ou auprès d'autres serveurs de temps
    - dernière strate = clients récupérant l'heure auprès des serveurs de temps
  - plusieurs modes de diffusion (client/serveur, égal à égal, diffusion)

Services réseau courants
HTTP – *HyperText Transfer Protocol* (rfc. 1945)

- Protocole couche Application (au dessus de TCP port 80)
- Protocole de transfert de fichiers
  - très simple (peu de commandes), efficace et très populaire dans Internet
    - base du WWW (World Wide Web)
    - échange sous forme requête-réponse
  - principalement destiné à transférer des fichiers au format HTML mais fonctionne avec n'importe quel fichier
    - fichiers contenant le formatage spécifié entre balises
    - le contenu HTML peut être généré dynamiquement
  - les fichiers (ou ressources) sont identifiées par une URL (Uniform Ressource Locator) qui spécifie :
    - le protocole, le serveur, l'arborescence des répertoires et le nom du fichier de la ressource (et éventuellement n° port, login, mot de passe et paramètres complémentaires)
- Nécessite un navigateur coté client

Services réseau courants
FTP – *File Transfer Protocol* (rfc. 959)

- Protocole couche Application (au dessus de TCP ports 20-21)
- Protocole de transfert de fichiers
  - permet d'accéder à un système de fichiers distant
    - dépôt et récupération des fichiers
    - possibilité de manipuler les fichiers distants (effacer, renommer...)
  - pour accéder à un site FTP, il est nécessaire de s'identifier
    - il faut y être déclaré et avoir les bon droits
    - les serveurs publics acceptent souvent des accès anonymes
  - problème de sécurité : transport en clair de toutes les données
- Les messages FTP sont transportés par TCP
  - le port 21 est le port « commande » du serveur
  - le port 20 est le port « données » du serveur en mode actif
  - un port quelconque est le port « données » du serveur en mode passif
  - le client a toujours un port quelconque (1024 à 65635)
- Variantes
  - TFTP version réduite de FTP (UDP au niveau Transport)
  - SFTP version sécurisé de FTP (TCP au niveau Transport et TLS au niveau Session)

Services réseau courants
SMTP – *Simple Mail Transfer Protocol* (rfc 2821)

- Protocole de la couche Application (au dessus de TCP port 25)
- Protocole de transfert du courrier électronique
  - courrier électronique = texte du message accompagné éventuellement de fichiers inclus en pièces jointes (l'ensemble, avec les entêtes protocolaires, représente le message transmis : PDU SMTP)
- On distingue :
  - le serveur de transfert de courrier (MTA) : centre de tri
  - le serveur de distribution (MDA) : facteur + boîtes aux lettres
    - souvent sur la même machine que le MTA
  - le client de consultation des courriers (MUA) : logiciel de mail
- Les adresses ont un format spécifique
  - partie_locale@domaine ou partie_locale@machine
    - partie_locale (utilisateur ou service) gérée par le serveur lui-même
    - domaine ou machine géré par le service DNS (mais @IP possible)
- Protocoles et codages affiliés : POP, IMAP, MIME

Compléments sur la couche Transport
Introduction

- Assure l'interface entre couches hautes, orientées « traitement », et les basses, orientées « réseau »
- Se charge du transport des messages de bout en bout éventuellement à travers plusieurs réseaux
  - est transparente pour l'utilisateur
  - peut rendre divers services de bout en bout
    - transport fiable : acquittement de chaque donnée envoyée
    - gestion de flux : éviter de submerger le récepteur
    - segmentation/réassemblage : découper/reconstituer les PDU de la couche application (message)
- PDU appelé « segment »
- TCP, UDP, SPX (Novell), NetBEUI (Microsoft)

Compléments sur la couche Transport
Dans le modèle TCP/IP

- Le modèle TCP/IP définit deux protocoles de transport :
  - TCP (rfc 793) → mode connecté avec acquittements, numérotation des segments et gestion des flux
  - UDP (rfc 768) → non connecté et sans garantie (meilleur effort)
- Les extrémités sont identifiées par des numéros de port
  - numéro identifiant le service et/ou l'application qui communique
  - numéros de 0 à 1023 réservés aux applications et services connus nécessitant des droits administrateurs pour être lancés
  - numéros de 1024 à 65635 réservés aux application clientes
    - depuis peu il est suggéré de ne pas utiliser la plage 1024-49151 réservée aux services enregistrées mais avec droits ordinaires
  - le rfc 1700 donne les numéros déjà attribués et /etc/services contient les services reconnus par une machine sous Unix
- Association entre deux applications est définie d'une manière unique par : @IP src, @IP dst, port src, port dst, type protocole de transport

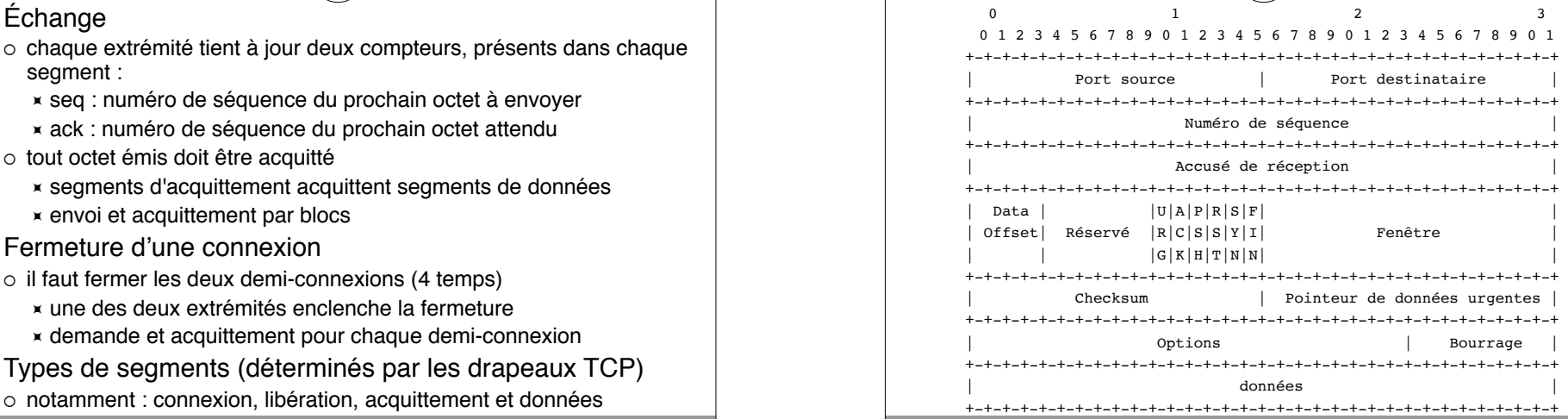
Compléments sur la couche Transport
TCP

- Transport fiable en mode connecté avec acquittements et gestion de flux
  - trois phases : ouverture, échange et fermeture
  - plusieurs types de segments mais toujours même structure de l'entête (même PDU)
- Ouverture d'une connexion
  - connexion = 2 demi-connexions : src-dst et dst-src
  - ouverture de connexion en trois temps (appelée « poignée de mains en trois temps ») :
    - → demande d'ouverture de la demi-connexion src-dst
    - → acquittement de cette demande et demande d'ouverture de la demi-connexion dst-src
    - → acquittement de cette demande
  - lors de l'ouverture les extrémités échangent leurs numéros de séquence initiaux et leurs tailles de fenêtres de réception

Compléments sur la couche Transport
TCP (suite)

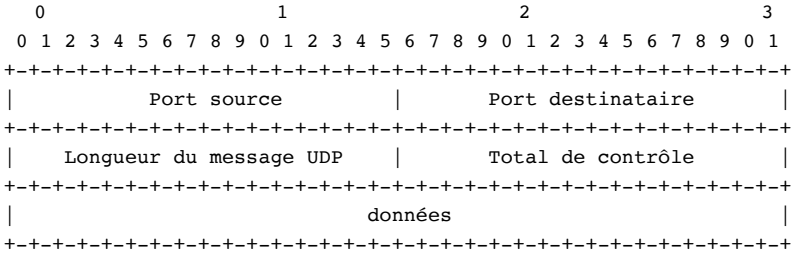
- Échange
  - chaque extrémité tient à jour deux compteurs, présents dans chaque segment :
    - seq : numéro de séquence du prochain octet à envoyer
    - ack : numéro de séquence du prochain octet attendu
  - tout octet émis doit être acquitté
    - segments d'acquittement acquittent segments de données
    - envoi et acquittement par blocs
- Fermeture d'une connexion
  - il faut fermer les deux demi-connexions (4 temps)
    - une des deux extrémités enclenche la fermeture
    - demande et acquittement pour chaque demi-connexion
- Types de segments (déterminés par les drapeaux TCP)
  - notamment : connexion, libération, acquittement et données

Compléments sur la couche Transport
PDU TCP



Compléments sur la couche Transport
PDU UDP

- Service transport sans garantie : sans connexion, sans acquittements, sans contrôle de flux…
  - fournit juste
    - mécanisme de gestion des ports
    - interface au dessus de IP



Compléments sur la couche Transport
Mécanismes protocolaires

- Mécanismes permettant de contrôler les échanges
  - acquittements, time-out, fenêtres d'anticipation, numérotation des données, séquence ou somme de contrôle, piggybacking
- Plusieurs types de contrôle
  - contrôle de flux : éviter de submerger le récepteur
  - contrôle de séquencement : vérifier le bon ordre des PDU
  - contrôle d'erreur : détection et traitement de l'erreur
- Deux familles de protocoles
  - non orientés connexion : directement phase d'échange
  - orientés connexion : ouverture, échange, fermeture
    - à l'ouverture de connexion, l'émetteur et le récepteur se mettent d'accord sur les paramètres du transfert de données
- Peuvent être rencontrés dans d'autres couches notamment la couche liaison sous-couche LLC

Compléments sur la couche Transport
Mécanismes protocolaires (2)

- Acquittements
  - PDU particulier informant l'émetteur de la bonne réception d'un PDU de données
  - positif (ACK, c'est bon) ou négatif (NAK, faut réémettre)
  - sélectif (porte sur un PDU)
    - PDU de données et d'acquittement sont numérotés
  - collectif (porte sur un groupe de PDU)
- Time-out (expiration de temporisateur)
  - évite à l'émetteur l'attente indéfinie d'un acquittement
  - réémission automatique à l'expiration du temporisateur
    - nécessité de conserver les PDU non acquittés
- Numérotation des données
  - on peut numéroter les octets de données ou bien les PDU

Compléments sur la couche Transport
Mécanismes protocolaires (3)

- Fenêtres d'anticipation
  - chez l'émetteur : ensemble de PDU émis et non encore positivement acquittés (fenêtre d'émission)
  - chez le récepteur : ensemble de PDU qu'il peut recevoir sans saturer ses tampons (fenêtre de réception)
    - pour deux sites très éloignés, l'attente de l'acquittement après l'envoi d'un PDU implique sous-utilisation du médium
    - on autorise l'envoi de plusieurs PDU de données avant la réception des acquittements → utilisation de fenêtres d'anticipation
    - une fenêtre d'anticipation est un ensemble de PDU qui se suivent

Compléments sur la couche Transport
Mécanismes protocolaires (4)

- Fenêtres d'anticipation (suite)
  - Lorsqu'un acquittement arrive chez l'émetteur :
    - numéro du PDU acquitté = borne inférieure → décalage fenêtre
    - numéro du PDU acquitté ≠ borne inférieure → numéro conservé, fenêtre décalée après acquittement des PDU qui précédent (le décalage porte sur la séquence acquittée)
  - Lorsqu'un PDU de données arrive au récepteur :
    - numéro du PDU reçu ∉ fenêtre de réception → rejet du PDU
    - numéro du PDU reçu = borne inférieure → décalage fenêtre
    - numéro du PDU reçu ∈ fenêtre de réception (mais ≠ borne inférieure) → décalage reporté

Compléments sur la couche Transport
Mécanismes protocolaires (5)

- Séquence ou somme de contrôle
  - champs particulier permettant de détecter l'altération d'un ou de plusieurs bits
- Piggybacking
  - si les deux entités communiquent dans les deux sens (elles sont à la fois émetteur et récepteur) :
    - transfert des PDU de données et de supervision dans les deux sens
    - utilisation des PDU de données pour transmettre les acquittements (dans des champs particuliers)
  - minimise échanges inutiles : PDU de supervision (ACK)remplacés par quelques bits dans PDU de données
  - l'émetteur attend l'acquittement plus longtemps (récepteur attend d'avoir quelque chose à envoyer)

Compléments sur la couche Liaison
Notion de trame

- La couche liaison
  - découpe le train de bits (PDU) en provenance de la couche réseau
  - étiquette ces bits et forme ses propres PDU appelés « trames »
  - applique des techniques de comptage de caractères, de détection et de correction d'erreur sur ces trames
  - assure leur transport en utilisant le service de la couche physique
- Une trame peut contenir plusieurs champs (en plus du PDU de la couche supérieure dans la partie données)
  - @destinataire
  - numéro de séquence
  - taille de la trame
  - type des données transportées
  - type de la trame
- Pour un protocole donné, la structure est connue d'avance

Compléments sur la couche Liaison
Découpage en trame

- Le découpage permet au récepteur de bien délimiter chaque trame
- Plusieurs techniques peuvent être utilisées et combinées (certaines au niveau de la couche physique)
  - comptage de caractères : un champ donne la taille de la trame
  - utilisation de champs délimiteurs de trame
    - Exemple : fanions et bits de transparence
      → trame délimitée par des suites 01111110 (fanions) et afin d'éviter l'apparition de ces suites dans les données on introduit des bits de transparence (un 0 après toute suite de cinq 1)
  - violation codage physique : codes interdits délimitent les trames

Compléments sur la couche Liaison
Altération des trames

- Problème : les supports de transmission ne sont pas fiables
  ⇒ erreurs de transmission
  - nombre de bits inférieur ou supérieur à l'arrivée qu'au départ
  - un ou plusieurs bits sont erronés (valeur fausse, inversée)
- Comment garantir l'intégrité des trames ?
  - champs de contrôle d'erreur pour détecter voire corriger les erreurs
- Quel traitement en cas d'erreur ?
  - mécanismes protocolaires adéquats assurant la réémission des trames

Compléments sur la couche Liaison
Détection/correction d'erreurs

- Pour détecter (voire corriger) les erreurs, il faut ajouter aux informations transmises (I) des informations de redondance (R)
  - on augmente ainsi la distance entre les mots à transmettre
  - la distance est le nombre minimal de bits qu'il faut changer pour passer d'un mot valide à un autre mot valide
  - plus la distance est grande plus il est possible de détecter et de corriger d'erreurs
- Les couples (I,R) forment les mots de code (C) à transmettre
- À la réception, on vérifie si le mot de code C reçu est valide et on extrait I

Compléments sur la couche Liaison
Détection/correction d'erreurs (suite)

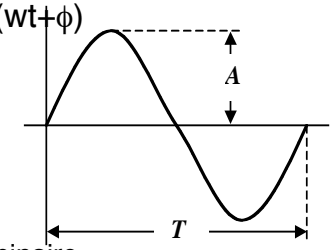
- Les bits de R sont obtenus à partir des bits de I
- Plusieurs méthodes existent pour déterminer R à partir de I
  - parité paire (ou impaire)
    - on rajoute un bit pour rendre le nombre total de 1 paire (ou impaire)
  - code cyclique (CRC)
    - on considère I comme un polynôme et on définit R comme le reste de division de I par un autre polynôme dit générateur tel que $x^{16}+x^{12}+x^5+1$
  - code linéaire tel que celui de Hamming
    - on rajoute des bits de parité portants sur certains bits de I aux positions multiples de 2
  - somme de contrôle (ou checksum)
    - on découpe I en blocs identiques et on fait la somme de ces blocs (en complément à 1 par exemple)

Compléments sur la couche Physique
Rôles de la couche physique

- assure la transmission brute des bits sur le support
- détermine propriétés physiques du support de transmission :
  - niveaux électriques, fréquences ou longueurs d'onde représentant les éléments binaires
  - interface avec la couche liaison
- caractérisée par :
  - nature des signaux
  - stratégie d'acheminement
  - mode de la transmission
  - type de support
  - type de la transmission
  - sens de la transmission
  - modulation des signaux
  - technique de multiplexage
  - technique de codage

Compléments sur la couche Physique
Notion de signal

- fonction périodique : $a(t) = A \sin(wt+\phi)$
  - a(t) : amplitude à l'instant t
  - A : amplitude maximale
  - w : pulsation = $2\pi f$ où f = fréquence
  - ϕ : phase



- A, f et ϕ = caractéristiques fondamentales
  - varient pour transporter l'information binaire
    - modifications des caractéristiques se fait par rapport à une onde porteuse
  - laps de temps significatif minimal = moment élémentaire (nécessité d' une horloge)
    - nb moments élémentaires/seconde = rapidité de modulation
    - nb bits/seconde = débit binaire

Compléments sur la couche Physique
Supports de transmission

- Le câble le plus courant dans les LAN est un câble de paires torsadées avec connecteurs RJ45
  - 8 fils torsadés par 2
  - simple, générique, bon marché
  - plusieurs types de blindage
    - UTP (non blindé), FTP (blindage global), STP (blindage individuel)
  - plusieurs catégories de câble en fonction de l'utilisation
    - classement de 1 à 8 par bande passante et débit
  - les caractéristiques du câble sont souvent écrites dessus
- Contraintes
  - de distance entre équipements
  - de proximité avec les câbles de courant fort (électricité)