Les Réseaux Informatiques*

Sidi Mohammed SENOUCI
Orange Labs, Lannion

* Ces transparents ont été en grande partie réalisés grâce au support de cours de Nadjib ACHIR (Univ. Paris-Nord) et fortement inspiré des tutoriaux d'Olivier BONAVENTURE (UCL)

Introduction - PLAN

- ✓ Qu'est-ce qu'un réseau ?
- ✓ Classifications des réseaux
- ✓ Normes et standards
- ✓ Architecture en couches

Qu'est-ce qu'un réseau ?

- Définitions générales
  - Un **réseau** est un ensemble d'objets interconnectés les uns aux autres qui permet de faire circuler des éléments entre ces objets selon des règles bien définies
  - Un **réseau d'ordinateurs** est un ensemble de calculateurs autonomes capables d'échanger des informations
    - Objets → calculateur autonome = unité de traitement propre + mémoire non partagé
    - Elément → information (elle est échangée au travers d'un support de communication)

Qu'est-ce qu'un réseau ?

- Le domaine des réseaux consiste en l'étude de l'ensemble des techniques permettant la communication entre calculateurs autonomes
- Objectif
  - Fournir les moyens matériels et logiciels pour faire communiquer et permettre l'échange d'informations entre plusieurs équipements ou machines informatiques de manière souple et fiable

Introduction - Plan

1. Qu'est-ce qu'un réseau ?
2. **Classifications des réseaux**
   - ✓ **par type de transmission**
   - ✓ **par taille**
   - ✓ **par topologie**
   - ✓ **les techniques de commutations**
3. Normes et standards
4. Architecture en couches

Classification des réseaux

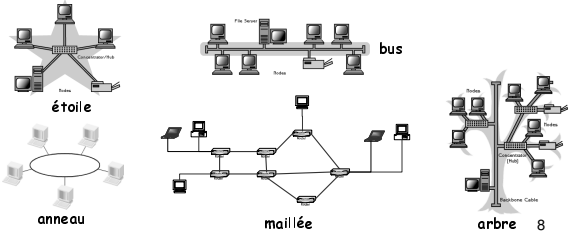
- **Classification des réseaux :**
  - **Analyse par le type de transmission (diffusion ou point-à-point)**
  - **Analyse par topologie**
  - **Analyse par la taille (LAN, MAN, WAN) …**
- **Mais également :**
  - **Analyse par la propriété (privé ou public)**
  - **Analyse par la nature de l'info transportée**
    - Données, images, voix, son ...
  - **Analyse par type d'application**
    - Application temps réel (Audiovisuelle)
    - Application temps différés (Bureautique)

Classification par type de transmission

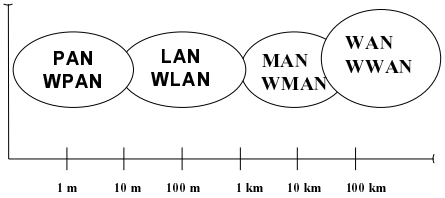
- La **diffusion**
  - Un seul canal de transmission partagé par toutes les machines du réseau
  - Les données émises sont reçues par tous, mais seul(s) le(s) destinataire(s) les prend (prennent) en compte
  - Ex : Ethernet, satellite, TV
  - Diffusion restreinte (*multicast*)
- Le **point à point**
  - Le réseau repose sur des connexions entre des machines prises 2 à 2
  - Les données peuvent transiter par plusieurs machines intermédiaires avant d'arriver à leur destination
  - Ex : Internet

Classification par topologie

- la **topologie physique** décrit la façon selon laquelle les machines sont reliées *physiquement* entre elles (configuration spatiale du réseau)



Classification par taille



PAN - Personal Area Network
LAN – Local Area Network
MAN – Metropolitan Area Network
WAN – Wide Area Network
W??? – Wireless ???

Caractéristiques des PAN

- Tous petits réseaux permettant d'interconnecter des machines personnelles (PC portable, téléphone mobile, PDA, etc.)
- Réseaux sans fil
- Technologies émergentes : Bluetooth, ZigBee, …
- Débits : qq centaines à qq Méga bits/s (~700kbs pour bluetooth)
- Étendue : quelques équipements connectés

Caractéristiques des LAN

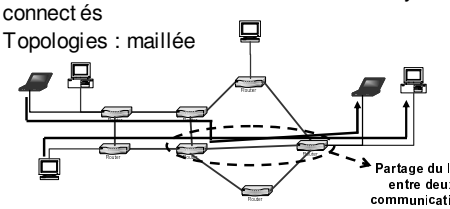
- Réseaux adaptés à la taille d'un site d'entreprise dont la taille ne dépasse pas qq km
- Réseaux privés
- Utilisés pour relier les PC ou les stations de travail à des ressources partagées
- Étendue : quelques centaines d'ordinateurs
- Débits : ~10 ~100 Mbit/s (voir 1Gbits/s)
- Reposent sur un support *partagé*
  - Nécessitent un mécanisme d'arbitrage pour résoudre les conflits d'accès
- Topologies : bus (Ethernet), anneau (Token Ring), canal radio (WiFi)

Caractéristiques des MAN

- Réseaux atteignant la taille d'une métropole
- Réseaux publics ou privés
- Débits : 100 Mbits/s
- Utilisent un support de transmission auquel sont reliés tous les ordinateurs
- Peuvent servir à interconnecter des LAN
- Étendue : quelques centaines, quelques milliers d'ordinateurs
- Topologie : double bus (DQDB), anneau (FDDI), canal radio (WiMax)

Caractéristiques des WAN

- Réseaux étendus sur plusieurs centaines voire milliers de km (un pays, un continent, ..)
- Réseaux publics ou privés
- Composés de commutateurs et de liaisons entre eux
- Des milliers voire millions d'ordinateurs y sont connectés
- Topologies : maillée



13

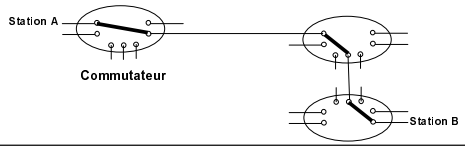
Les techniques de commutations

- Commutation :
  - Définition :
    - Etablissement d'une communication / connexion entre deux points distants du réseau
  - Principe de base :
    - Tirer profit d'une infrastructure commune (un réseau) pour faire transiter plusieurs connexions possibles
  - Supposition de base :
    - Il est peu probable que tous les utilisateurs soient connectés en même temps

14

Les techniques de commutations

- Commutation de circuits :
  - Méthode de communication dans laquelle un trajet spécifique est défini pour le transite de toutes les données entre l'émetteur et le récepteur
  - Ce trajet implique l'établissement d'une continuité électrique entre les deux extrémités
  - Inconvénient : pas d'optimisation des ressources au niveau des commutateurs



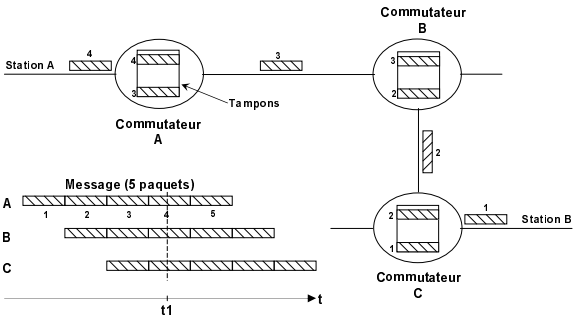
15

Les techniques de commutations

- Commutation de paquets :
  - Technique de commutation dans laquelle on transmet des paquets de données (un ensemble de bits)
  - Quand on veut faire passer un gros fichier, on peut le découper en petits paquets
  - La taille d'un paquet peut être variable
  - C'est le principe du protocole IP de l'Internet
  - Optimisation 1 : Plus faciles à manipuler et permet de faire passer en même temps plusieurs fichiers dans un même canal (lien)
  - **Optimisation 2 : permettre une politique de routage (choix des chemin suivant la charge du réseau)**
  - Inconvénient : non adapté au transmission temps réels

16

Les techniques de commutations



17

Les techniques de commutations

- Commutation de cellules :
  - Dans laquelle on transmet des cellules de données
  - Une cellule est généralement plus petite qu'un paquet (53 octets pour ATM)
  - Pas de mémorisation, redirection immédiate
  - Adaptée aux transmissions de données temps réel (voix et vidéo)
  - Création de chemin ou circuits virtuels basés sur la commutation de cellules
  - Inconvénients :
    - Limitation au niveau de la vitesse de commutation (< 2Gbits/s)
    - Adapté au "temps réels"

18

Les techniques de commutations

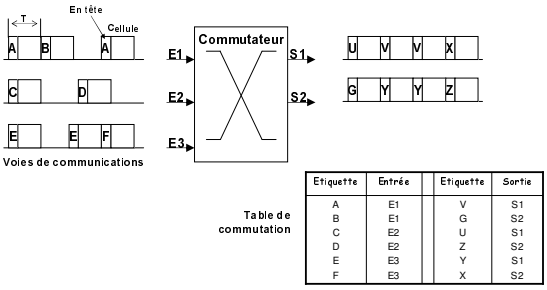


Table de commutation

Etiquette	Entrée		Etiquette	Sortie
A	E1		V	S1
B	E1		G	S2
C	E2		U	S1
D	E2		Z	S2
E	E3		Y	S1
F	E3		X	S2

Les acteurs et leurs approches

1. Industriels des télécommunications
   - But : mettre à la disposition de l'utilisateur un réseau pour interconnecter les équipements terminaux
   - Applications synchrones à contraintes temporelles (voix)
   - Solution : commutation de circuits ou de cellules
2. Industriels de l'informatique
   - But : relier des machines informatiques entre elles, en local ou à distance
   - Applications asynchrones à temps de réponse variable (transfert de fichiers, transactions, etc.)
   - Solution : commutation de paquets

Les acteurs et leurs approches

3. Câblo-opérateurs
   - But : déployer des réseaux câblés de télévision
   - Applications à très hauts débits en numérique
   - Solution : diffusion, multiplexage en fréquence et modulation large bande
     - multiplexage en fréquence: partition de la bande passante en sous bandes et chaque sous-bande transporte un canal TV. En plus de canaux pour la téléphonie et un canal pour l'Internet.
     - Pousser l'ensemble des programmes TV vers l'utilisateur
   - **Intégration**: retirer les canaux de TV et de téléphonie et tout intégrer sur le canal Internet
     - N'envoyer que le flot réclamé par l'utilisateur

Introduction – Plan

1. Qu'est-ce qu'un réseau ?
2. Classification des réseaux
3. **Normes et standards**
   - ✓ **le besoin**
   - ✓ **l'UIT**
   - ✓ **l'ISO**
   - ✓ **l'IETF**
   - ✓ **l'IEEE**
4. Architecture en couches

Normes et standards : le besoin

- Bénéfices
  - Faire converger les différents équipementiers, opérateurs, etc..
  - Permettre à des équipements hétérogènes de communiquer (ex. téléphonie GSM ->sol: "U"MTS)
  - Accroître le marché des produits adhérant aux standards
- Standards
  - ***de facto*** : lorsqu'un consensus s'établit autour d'une proposition industrielle, sans démarche formelle (ex. Unix, windows, TCP, etc.)
  - ***de jure*** (norme): document formel, adopté par une instance reconnue (X.25, etc.)
- Organisations
  - Les organismes créés à la suite d'accord gouvernementaux (IUT, etc.)
  - Les organisations non gouvernementales (IETF, IEEE, etc.)

L'UIT et ses recommandations

- Union Internationale des Télécommunications
- Organisation Intergouvernementale
- Rôle :
  - émettre des recommandations techniques sur les interfaces pour le télégraphe, le téléphone, la communication de données
- 1865 : création de l'Union Télégraphique Internationale
- 3 secteurs de normalisation
  - UIT-R (Radiocommunications)
  - UIT-D (Développement de l'accès aux Télécoms)
  - UIT-T (Télécommunications) : ex-CCITT (1956-1993)

L'ISO et ses normes

- International Organization for Standardization
- Rôle
  - favoriser le développement de la normalisation et des activités connexes dans le monde, en vue de faciliter entre les nations les échanges de biens et de services et de développer la coopération dans les domaines intellectuel, scientifique, technique et économique
- Organisation non gouvernementale, créée en 1947

25

L'ISO

- Fédération mondiale d'organismes nationaux de normalisation (140 pays), à raison d'un membre par pays
  - Comité membre : plein droit de vote
    - AFNOR (France), ANSI (US), DIN (Allemagne), BSI (GB), JISC (Japon), …
  - Membre correspondant : pays dont l'activité de normalisation n'est pas totalement développée
  - Membre abonné : pays à économie très limitée
- Fonctionnement : 2850 comités techniques / sous-comités / WG

26

L'IETF et ses RFC

- Internet Engineering Task Force
- Rôle
  - Développement et ingénierie des protocoles de l'Internet (ex. TCP/IP: RFC 1122)
- Créé formellement en 1986
- Communauté internationale ouverte (concepteur, opérateurs, équipementiers, chercheurs)
- Fonctionne sur le principe du consensus
- RFC (**Request For Comments**)
- Organisation : domaines / groupes de travail
- Fonctionnement (mailing lists, meetings - 3 fois/an)

27

L'IEEE et ses standards

- Institute of Electrical and Electronics Engineers
- Fusion en 1963
  - AIEE (American Institue of Electrical Engineers)
  - IRE (Institute of Radio Engineers)
- Organisation professionnelle à but non lucratif
  - 377 000 membres individuels, répartis dans 150 pays
- Rôle
  - Edition scientifique et technique
  - Organisation de conférences
  - Activités de standardisation
- A l'origine des standards IEEE 802.XX (LAN/MAN)

28

Introduction - Plan

1. Qu'est-ce qu'un réseau ?
2. Classifications des réseaux
3. Normes et standards
4. **Architecture en couches**
   - ✓ **le besoin**
   - ✓ **les principes**
   - ✓ **le modèle OSI**

29

Pourquoi une architecture ?

transfert de fichier de A à B via un réseau

- transformer des bits en signaux
- transporter des paquets
- gérer les échanges d'applications
- etc.

- altérations de données
- pertes de données
- congestions du réseau
- pannes matérielles
- etc.

⇘ il faut décomposer le problème !

30

Comment décomposer ?

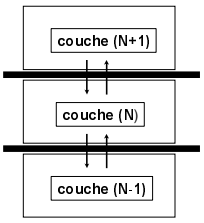
Principe : structuration en couches (niveaux)

- Chaque couche est construite sur les acquis de la précédente
- Dans tous les réseaux, le rôle de chaque couche est d'offrir des services à la couche supérieure
  - Fiabilité
  - Sécurité
  - …
- Le nombre, le nom, le contenu et les fonctions des couches diffèrent d'un réseau à l'autre
  - ↳ 2 aspects : vertical et horizontal

Pourquoi une architecture en couches ?

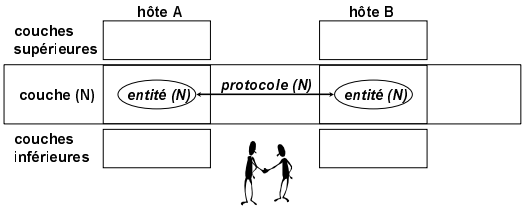
- Transformer un problème **complexe** en une suite de problèmes **simples** et **résolvables**
- Chaque couche est responsable de la gestion **d'une partie** du problème
- A chaque couche, l'information est mise en forme pour être traitée **de manière adaptée**:
  1. Par les couches sous jacente
  2. Par la couche distante de même niveau
- A chaque couche correspond un groupe **homogène** de fonctions de communication
- Chaque couche exécute les **fonctions afférentes** à son niveau au moyen d'un protocole de communication

Aspect vertical



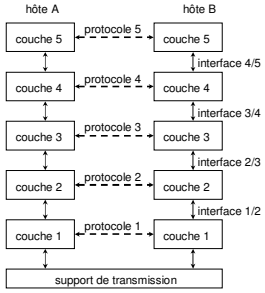
- la couche (N+1) voit la couche (N) uniquement par le ***service*** offert
- la couche (N+1) n'a aucune vue sur la couche (N-1)
- la couche (N) est séparée de la couche (N-1) et de la couche (N+1) par une ***interface de service*** **bien définie**

Aspect horizontal



- le ***protocole*** (N) définit les règles de communication à l'intérieur de la couche (N): contrôle et envoi des données entre entités
- les ***entités*** (N) représentent les éléments actifs de la couche (N)

Communication virtuelle VS communication réelle



- communication ***virtuelle***

  aucune donnée n'est passée directement de la couche (N) de A à la couche (N) de B
- communication ***réelle***

  la couche (N) passe les données à la couche (N-1)

..un protocole, un service, une interface de service par couche

- **Protocole**
  - Règles et conventions utilisées pour gérer la conversation entre deux entités (distantes et de même niveau)
  - Formats des informations échangées et séquences des opérations à effectuer pour réaliser une fonction précise
- **Service**
  - Ensemble de fonctions offertes par un niveau donné à un niveau supérieur
  - Une couche offre des services à la couche supérieure au travers d'une interface de service
  - Une couche utilise les services de la couche inférieure
- **Interface de service**
  - Sert à la couche supérieure pour accéder aux services offerts par la couche inférieure
  - Utilisée par un protocole pour rendre un service plus complet
  - Un protocole ajoute une valeur au service qu'il utilise

Le modèle de référence OSI

- Open Systems Interconnection
- Travaux entrepris à l'ISO en 1978
- Adopté également par le CCITT
- Norme parue en 1980 : IS 7498
- Pourquoi faire ?
  - Régler les problèmes de l'interconnexion de systèmes hétérogènes (logiciel et matériel) appelés aussi systèmes ouverts
- Portée du modèle ?
  - Il ne concerne que l'interconnexion et n'est utilisé que pour décrire les communications entre systèmes
    - Modèle abstrait
    - Modèle indépendant des logiciels et technologies

37

La normalisation ISO : Objectifs

- Préciser les concepts et la terminologie
- Hiérarchiser les fonctions à réaliser
- Mettre en œuvre des mécanismes connus aux deux extrémités
- Réutilisation des blocs entre applications ayant des objectifs commun vis à vis du réseau
- L'ISO a donc mis en œuvre une architecture cohérente comprenant :
  - Les fonctions que doit remplir un système
  - La définition des protocoles à mettre en œuvre entre ces systèmes

38

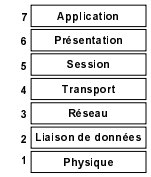
Les 7 couches OSI

7	application
6	présentation
5	session
4	transport
3	réseau
2	liaison de données
1	physique

- **Couches hautes**
  - Rendent un service d'accès
  - Comportent les fonctions de traitement sur les données transportées
- **Couches basses**
  - Rendent un service de transport
  - Comportent les fonctions de transmission de données

39

La couche application



- But : fournir aux utilisateurs des applications et des services applicatifs réseaux
- Exemples : partage de fichiers, transfert de fichiers, HTTP...
- Question : comment ces messages ou fichiers sont ils codées ?
  - Quel format ?

40

La couche présentation

- But : affranchir les applications des contraintes syntaxiques
- Représentation des données transférées entre entités d'application
  - Encodage dans une norme agrée permettant à des équipements ASCII et EBCDIC par exemple de communiquer.
  - Compression des données, chiffrement.
- Exemple : la syntaxe abstraite ASN.1 (ISO 8824, UIT X208) normalisée par l'ISO.
  - Utilisée dans la messagerie X400 et les annuaires X500.
- Question : comment établir la connexion entre les 2 applications ?

41

La couche session

- But : gérer le dialogue entre deux entités distantes
- Fiabilité assurée par les couches inférieurs
- Gestion du dialogue :
  - Établissement de la session (dialogue)
  - Dialogue unidirectionnel ou bidirectionnel
  - Gestion du tour de parole
  - Synchronisation entre entités distantes
  - Association entre noms et adresses
  - Mécanisme de points de reprise en cas d'interruption dans le transfert d'information
  - ...
- Question : et si une erreur de transmission se produit ?

42

La couche transport

- But :
  - Offrir aux couches supérieurs un canal de transport de données de **bout en bout** fiable quel que soit la nature du réseau sous jacent
- Canal fiable
  - Détection et contrôle d'erreur
  - Qualité de service de bout en bout
  - Autoriser ou non les dé-séquencements
  - Autoriser ou non les pertes de paquets
  - Contrôle de flux de bout en bout
- Question : On sais à qui on doit envoyer et on a mis en place une session fiable, mais comment les messages vont arriver à destination ?

7 Application
6 Présentation
5 Session
4 Transport
3 Réseau
2 Liaison de données
1 Physique

La couche réseau

- But :
  - **Assure le Routage**
    - Acheminer les données du système source au système destination
    - Réalise le transfert de données quelques soit la topologie du réseau
  - Gestion de l'adressage dans l'interconnexion de réseaux hétérogènes
  - Mode connecté / non connecté (datagramme)
  - Unité de transfert : paquets
- Question : comment les nœuds de la route communiquent entre eux et arrivent à échanger les paquets ?

7 Application
6 Présentation
5 Session
4 Transport
3 Réseau
2 Liaison de données
1 Physique

La couche liaison de données

- But :
  - Transformer un moyen brut de transmission en une liaison de données plus fiable
- Gestion de la liaison de données
  - Données de l'émetteur en *trame de données*,
  - Transmission des trames en séquences,
  - Gestion des trames d'acquittement,
  - Reconnaissance des frontières de trames envoyées par la couche physique.
  - Contrôle d'erreur
    - régulation du trafic
    - gestion des erreurs
- Questions : comment l'information est elle transmise sur le lien ?

7 Application
6 Présentation
5 Session
4 Transport
3 Réseau
2 Liaison de données
1 Physique

La couche physique

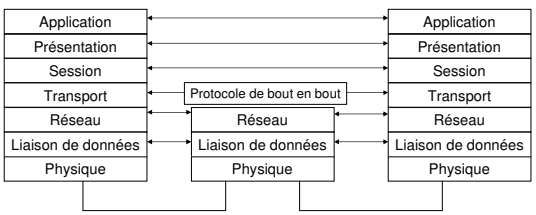
- Gère la transmission des bits de façon brute sur un lien physique
- Transmet un flot de bits sans en connaître la signification ou la structure :
  - Règles de codages : 7 Bits / 8 Bits
  - Transmission : Série / Parallèle
  - Mode : Synchrone / Asynchrone,
  - Transmission Bande de Base / Modulation,
  - Multiplexage : Temporelle / Fréquentielle
- Conception de la couche physique → domaine de l'électronicien.

7 Application
6 Présentation
5 Session
4 Transport
3 Réseau
2 Liaison de données
1 Physique

Vue simplifiée du modèle OSI

- Pour un utilisateur non averti il est possible de ne voir que 3 niveaux seulement :
  - Niveau applicatif :
    - Couches 7, 6 : (exemple transfert de fichier, Messagerie, ...)
  - Niveau transport :
    - Couches 5, 4, 3 : (exemples NetBEUI, TCP/IP, ...)
  - Niveaux transmission :
    - Couches 2, 1, 0 : (exemples cartes Ethernet, drivers PPP + modem, ...)

Le modèle de Référence OSI



En résumé…

- Architecture : ens. de couches et de protocoles
- Décomposition en couches
  - Chaque couche est responsable de la gestion d'une partie du problème
  - A chaque niveau d'abstraction donné correspond un groupe homogène de fonctions de communication
- ↳ Distinguer
  - Protocoles et services (interfaces)
  - Communications virtuelles et communications réelles
- ☺ Avantages
  - Faciliter la compréhension globale
  - Simplifier la mise en œuvre
  - Eviter les interactions non désirées

Le monde Internet

Le réseau Internet : historique

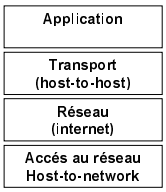
- Lancé en 1969 par la DARPA
- ARPANET : réseau expérimental
- 1978 : passage à un stade opérationnel
- Internet : INTERconnexion of NETworks : réseau de réseaux
- 1983 : standardisation de TCP/IP
- Résultat
  - Plus grand réseau au monde en terme de médiatisation …et sans doute en terme de trafic

Le monde Internet - Plan

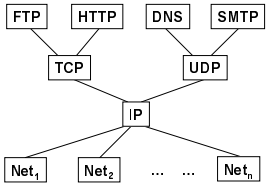
- **Services et modes de transfert dans l'Internet**
  - ✓ **Architecture TCP/IP**
  - ✓ **Mode de transmission**
  - ✓ **Utilité de la couche réseau**
  - ✓ **La couche réseaux de l'Internet**
- Le routage dans l'Internet
- La qualité de service dans l'Internet

L'architecture Internet (TCP/IP)

- Autre architecture : l'architecture TCP/IP

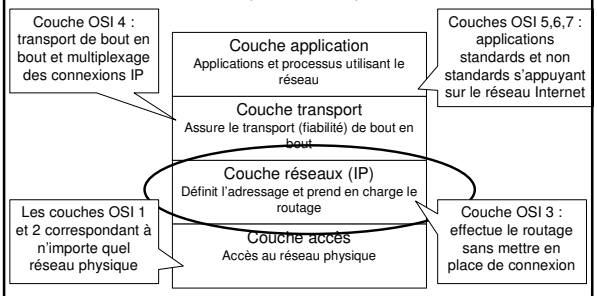


architecture
à 4 niveaux



graphe (simplifié)
des protocoles TCP/IP

L'architecture (TCP/IP)



Protocoles de l'architecture TCP/IP

- Technologie de base de l'Internet
  - Protocole IP, UDP et TCP
- Service Unicast
  - Service fournis par IP
    - Service non fiable (perte, erreurs, dé séquencement : possibles) en mode sans connexion
    - Rarement utilisé directement par les applications
    - Sert de base aux services fournis par UDP et TCP
  - Service fourni par UDP
    - Service non fiable(perte, dé séquencement possibles, détection erreurs sans corrections) en mode sans connexion
    - Applications; échange d'infos très rapides, téléphonie TCP/IP, jeux, petits réseaux locaux avec peu de problèmes
  - Service fourni par TCP
    - Service fiable orienté connexion
    - Applications: web mail, news, etc.
- Service Multicast (ou la communication de groupe)
  - Service IP
  - Service UDP

55

Protocoles de l'architecture TCP/IP

- Service sans connexion
  - un message peut etre transmis directement de S-D.
  - Utile pour envoyer les petits messages
  - Exemple service postale
  - Il ya une demande d'envoi (S) et une indication d'envoi (D)
- Service orienté connexion
  - Envoi d'un message
    - Ouverture de la connexion S-D
    - Envoi du message
    - ..;
    - Fermeture du message
  - Utile pour envoyer plusieurs messages
  - Fiable, pas de pertes, pas d'erreurs
  - Exemple : service téléphonique

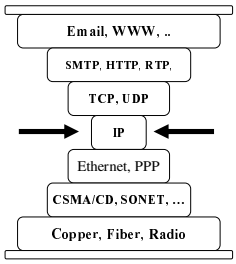
56

Mode de transmission

- Unicast
  - Un émetteur, un récepteur
  - Point à point
  - Exemple : téléphonie
- Broadcast
  - Un émetteur, tout le monde reçoit
  - Restreinte au réseaux locaux (ne passe pas les routeurs)
  - Exemple : diffusion
- Multicast
  - Un ou plusieurs émetteur(s), plusieurs récepteurs
  - Point à multipoint ou multipoint à multipoint
  - Exemple : vidéoconférence

57

Contexte de notre étude



58

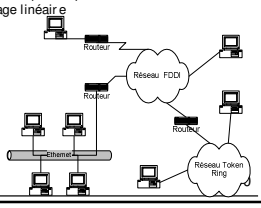
La couche réseau - PLAN

- ✓ Utilité de la couche réseau
- ✓ La couche réseaux de l'Internet
  - ✓ Adressage
  - ✓ Format de paquets
  - ✓ Les protocoles associés
  - ✓ Fonctionnement des stations et routeurs IP

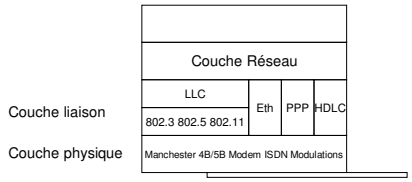
59

Limitations de la couche liaison de données

- Couche liaison de données permet de nous affranchir de la couche Physique
- Couches liaison de données classique
  - HDLC, PPP (surtout réseaux longue distance)
  - En général, connexion uniquement entre deux machines à travers un même fil"
- Couche liaison de données, réseau locaux
  - Ethernet, Token Ring, FDDI
  - Limitation de la taille géographique du réseau
  - Limitation sur le nombre de machines que l'on peut connecter
  - Utilisation d'un système d'adressage linéaire
- Hétérogénéité des réseaux

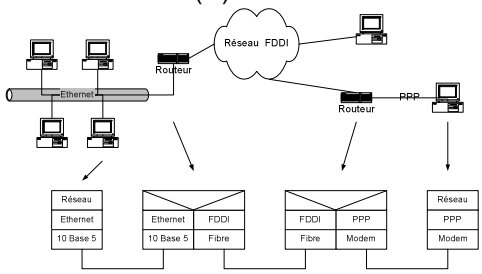


Couche réseau



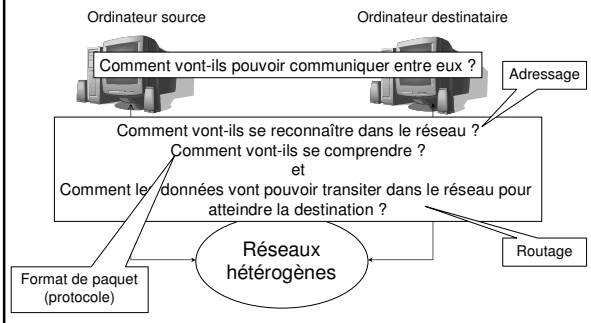
- Objectifs
  - Couche réseau permet de nous affranchir de la couche liaison de données
  - Service de transmission de données de bout en bout à travers un ensemble de réseaux hétérogènes
  - Service indépendant du type de couche liaison de données utilisée

Couche réseau (2)



- Routeur
  - Relais fonctionnant dans la couche réseau
- Unité de transfert dans la couche réseau
  - Paquet

Notion d'adressage et de routage



Couche réseau : principes de base

- Chaque station/routeur connecté au réseau doit être identifié par une adresse réseau qui est indépendante du type de la couche liaison de données sous-jacente
- Le service fourni doit être complètement indépendant du type de la couche liaison de données sous-jacente
- Les différentes couches liaison sous-jacentes doivent être complètement invisible par rapport à l'utilisateur
- La couche réseau achemine les paquets depuis une source vers une destination via plusieurs routeurs intermédiaires

Couche réseau : principes de base (2)

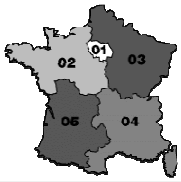
- Définir une couche réseau particulière consiste à définir :
  - Un système d'adressage
  - Un protocole pour la mise en place des routes (protocole de routage)
    - Construit une table de routage
  - Une technique d'acheminement des paquets (Type de commutation utilisé)
    - Utilise la table de routage construite par le protocole de routage
  - Un format de paquets et son interprétation (protocole de niveau Réseau)
    - Le format de paquets dépend du système d'adressage et de la technique d'acheminement

Couche réseau : système d'adressage

- Quelle structure doivent avoir les adresses de niveau réseau ?
- Les adresses de niveau liaison de données sont dites linéaires
  - Exemples d'adresses 802.XX (dites aussi adresses MAC)
    - 00-OD-56-6E-D7-D4, 00-20-ED-B1-BC-0C, …
  - Adresses correspondante au numéro de série des cartes réseaux correspondante
- Est il possible de faire du routage en se basant sur ces adresses ?
  - Non, car la taille des tables de routages risque de devenir ingérables …problème de mise au facteur d'échelle
- Quelle est la solution ? => Utiliser un système d'adressage hiérarchique …

Adressage hiérarchique : Exemple

- Le réseau téléphonique : le plan de numérotation français
  - 0 Z A B PQ M C D U
  - Z = zone géographique (vue macroscopique)
  - ZAB => région (un sous ensemble adjacents de départements au sein de la zone géographique)
  - ZABPQ = Zone de Numérotation Elémentaire (ZNE)
  - MCDU = permet d'identifier l'usager à l'intérieur de la ZNE



La couche réseau - PLAN

- ✓ Utilité de la couche réseau
- ✓ La couche réseaux de l'Internet
  - ✓ Adressage
  - ✓ Format de paquets
  - ✓ Les protocoles associés
  - ✓ Fonctionnement des stations et routeurs IP

Le routage et l'adressage IP

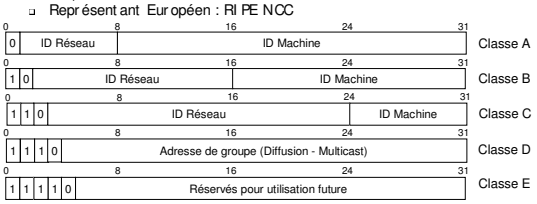
- L'adressage IP => Identifier une station/routeur supportant IP
  - En pratique, une adresse IP identifie une interface sur une station ou un routeur
    - L'interface est le point d'accès de la station/routeur à la couche liaison de données
    - En générale une station possède une interface
    - En générale un routeur possède plusieurs interfaces
- Le routage IP au sens large du terme
  - C'est l'acheminement des paquets vers la bonne destination
  - Chaque routeur contient une table dite de routage qui fera la correspondance entre des @IP et une interface de sortie
  - Une interface de sortie permet d'atteindre un autre routeur
  - Le protocole de routage est celui qui permet de mettre à jour continuellement cette table

Adressage IP

- Comment attribuer les adresses IP ?
  - Par construction, comme Ethernet
    - La table de routage doit alors contenir l'ensemble des @IP possibles
    - @IPv4 ⇔ 4 octets ⇔ 2^{32} ⇔ 4 milliards d'adresses ⇔ problème de mise à jour des tables de routage
  - Solution : regroupement d'adresses suivant le réseau auxquelles elles appartiennent (2 niveaux de hiérarchie)
    - Première hiérarchie : attribution des ensembles d'adresses IP à des « zones » du réseau
      - Routeurs doivent seulement connaître ces « zones »
    - Deuxième hiérarchie : attribution d'un identificateur à chaque station

Adresses IPv4 (1)

- Comment attribuer une plage d'adresses à une zone (réseau) ?
  - Suivant sa taille (Le nombre de bit pour spécifier le sous réseau dépend du nombre de machines)
- Adresse unique de réseau délivrée par la NIC (Network Information Center)
  - Représentant Européen : RIPE NCC

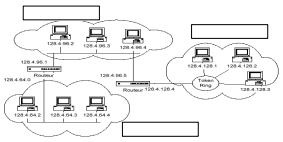


Adresses IPv4 (2)

Classe d'@	Nombre de réseaux	Nombre d'hôtes	Type de réseaux
Classe A	$2^{(8-1)}-2$ = 126	$2^{24}-2$ = 16777214	Réseaux de grands opérateurs
Classe B	$2^{(16-2)}$ = 16384	$2^{16}-2$ = 65534	Réseaux d'opérateurs moyens et de grandes entreprises
Classe C	$2^{(24-3)}$ = 2097152	$2^{8}-2$ = 254	Réseaux de petites entreprises
Classe D	x	X	Adresses de diffusion
Classe E	x	x	Réservés pour un usage ultérieur

Grandes organisations

- Grande organisation
  - Intranet d'une grande entreprise possédant plusieurs sites
    - Réseaux réparties sur plusieurs sites
- Quels type d'adresses donnée à ces organisations ?
  - Adresses de classe A ou B vs. plusieurs adresses de classes C ?



73

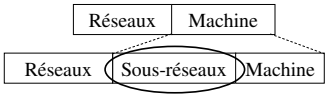
Réseaux de classe A et B

- Problème :
  - Les réseaux des organisations nécessitent un routage en interne (réseaux de classe A et B)
  - 12 octets minimum par entrée dans la table de routage
  - Temps de rafraîchissement pour chaque adresse
- Solution
  - Limiter le nombre de nœuds à adresser dans le réseau
  - Structurer l'organisation interne des réseaux (hiérarchisation en définissant des sous réseau)
- Conséquence
  - Diminue les entrées dans les tables de routage
  - Facilite la gestion des adresses et le dépannage du réseau
  - Limite l'encombrement par re-direction du trafic

74

Masque de sous-réseau

- Technique permettant de définir des sous-réseaux
- Permet de définir un nouveau champ dans l'adresse IP (adresse de sous réseau)



- Toutes les stations faisant partie d'un sous réseau peuvent directement s'échanger des trames par l'intermédiaires de la couche liaison de données
- La démarcation entre les 1 et 0 dans le masque permet d'établir quels seront les bits du champ de numéro du sous-réseau (SubNet ID) et ceux de la machine (host ID) dans le sous réseau

75

Exemple de masque

- Adresse de réseau de classe B: 130.50.0.0
- On veut créer 8 sous réseaux.
  - Le champ sous-réseau devrait être de 3 bits (2^3=8)
- Le masque sera de la forme
  - En binaire : 11111111.11111111.11100000.00000000
  - En décimal :255.255.224.0
- Notation des adresses de sous réseaux
  - 130.50.0.0/19 ou 130.50.0.0 255.255.224.0
- Sous-réseaux
  - 130.50.0.0/19, 130.50.32.0/19, 130.50.64.0/19, ...
  - On peut avoir jusqu'à 2046 (2^{13}-2) hôtes par sites ou sous réseau

76

Allocation des adresses IP

- Comment allouer les adresses IP ?
  - Première solution
    - Objectif : assurer l'unicité des adresses IP
    - Règles : toute organisation peut obtenir un réseau IP unique pour ses ordinateurs parmi les adresses non encore allouées
    - 1er arrivée, premier servi.
    - En pratique : trois types de réseaux
      - Classe A : sous-réseau avec masque de 8 bits (ex. MIT)
      - Classe B : sous-réseau avec masque de 16 bits
      - Classe C : sous-réseau avec masque de 24 bits
  - Inconvénients
    - Taille des différentes classes d'adresses trop rigide
      - **Gaspillage d'adresses**
    - Deux entreprises se connectant à l'Internet par le même fournisseur peuvent avoir des adresses compétemment différentes → **agrégation impossible**

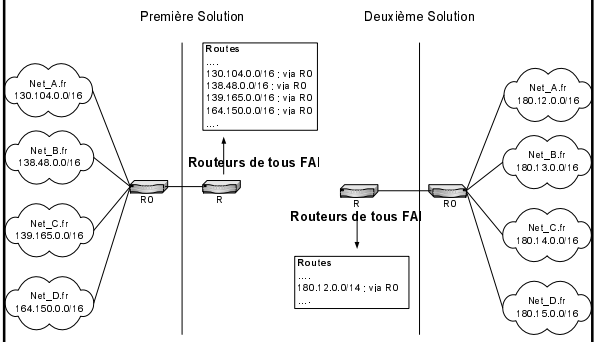
77

Allocation des adresses IP (2)

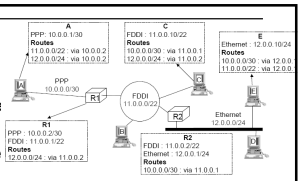
- Deuxième solution
  - Objectif : assurer l'unicité des adresses en permettant une meilleure agrégation des routes
  - Règles :
    - Seuls les fournisseurs d'accès Internet peuvent recevoir des blocs d'adresses IP
      - La taille du bloc attribué dépend du nombre d'utilisateurs
    - Une organisation qui veut se connecter à Internet doit obtenir ses adresses IP de son fournisseur d'accès
- Avantages
  - Meilleure agrégation des adresses
- Inconvénients
  - Une organisation qui change de fournisseur d'accès devra changer les adresses IP de ses machines

78

Allocation des adresses IP (3)



Sous-réseau et routage



- Le routeur utilise un ET logique entre l'adresse du paquet et l'adresse masque pour identifie le sous-réseau destinataire
- Comment se fait le routage au niveau de l'hôte source
  - Si les 2 machines sont dans le même sous-réseau, pas de routage
  - Sinon on envoi les paquets vers un des routeurs connecté au sous-réseau qui se chargera de trouver leur chemin
    - Lorsque plus qu'un routeur est connecté au sous-réseau, nécessité parfois des redirections (Voir messages ICMP correspondants)
- Le routeur sait comment atteindre les autres sous-réseaux, de même que les stations appartenant à son sous-réseau

Adresses IP Spéciales

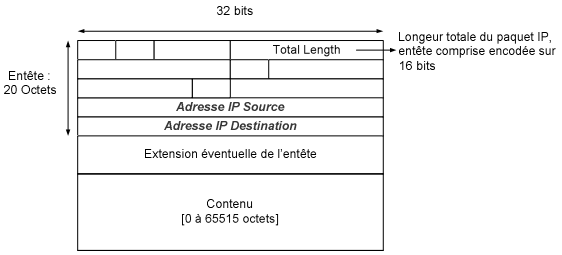
- Adresses IP particulières
  - 127.0.0.1 (localhost ou loopback)
    - Adresse virtuelle accessible sur chaque machine
    - Permet de contacter un serveur sur la machine locale
  - 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16
    - Réservé pour les réseau privés (non connecté à Internet !)
  - 255.255.255.255
    - Broadcast « général » (pas en pratique)
  - Si tous les numéros machine à 1 => diffusion
    - Adresse = 128.4.10.255 correspond à toutes les machines du sous réseau 128.4.10.0/24
    - Adresse = 128.4.255.255 correspond à toutes les machines du réseau de classe B 128.4.0.0/16
  - Reste
    - Adresses IP de stations connectées à l'Internet global

La couche réseau - PLAN

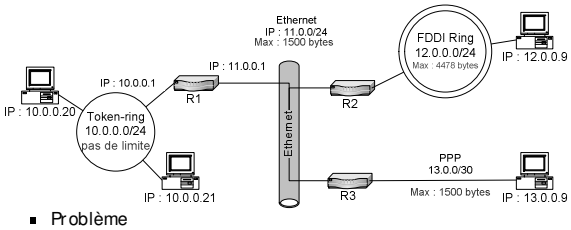
- ✓ Utilité de la couche réseau
- ✓ La couche réseaux de l'Internet
  - ✓ Adressage
  - ✓ Format de paquets
  - ✓ Les protocoles associés
  - ✓ Fonctionnement des stations et routeurs IP

Paquet IPv4

- Format des paquets IPv4

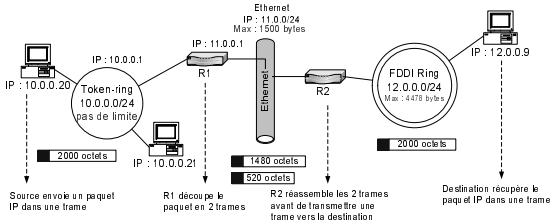


Couche liaison de données : Limitations



- Problème
  - La taille des paquets IPv4 peut atteindre 64 kbytes au total
  - IP doit s'appuyer sur la couche liaison de données pour la transmission des paquets
  - La plupart des protocoles du niveau liaison de données ne supportent pas des trames aussi longues

Transmission de longs paquets IP

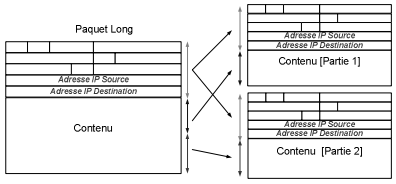


- Idée
  - Permettre le découpage des longs paquets sur chaque couche liaison de données si nécessaire
  - Exemple
    - Envoie de paquets IP contenant 2000 octets utiles

Transmission de longs paquets IP (2)

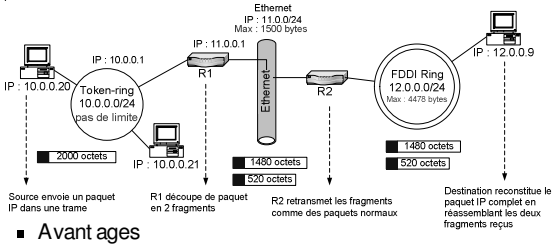
- Avantage
  - Bonne utilisation de chaque réseau intermédiaire
- Inconvénients
  - Chaque station/routeur doit pouvoir fragmenter un paquet en N trames
  - Chaque station/routeur doit pouvoir réassembler N trames dans un paquet
    - Ce réassemblage consomme du CPU et de la mémoire
    - Ce réassemblage peut induire un délai important
  - Un paquet peut devoir être fragmenté plusieurs fois avant d'arriver à la destination

Transmission de longs paquets IP (3)



- Amélioration
  - Éviter de réassembler dans les routeurs
- Principes
  - Toute station/routeur est capable de ***fragmenter*** un paquet IP
    - Chaque fragment est un paquet IP contenant l'@ IP source et l'@ IP destination
  - La destination effectue le réassemblage des fragments

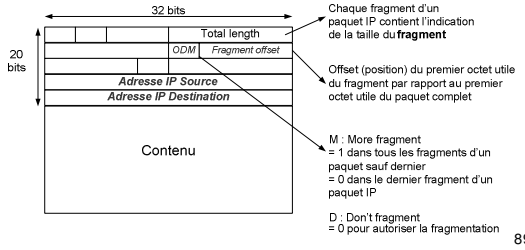
Transmission de longs paquets IP (4)



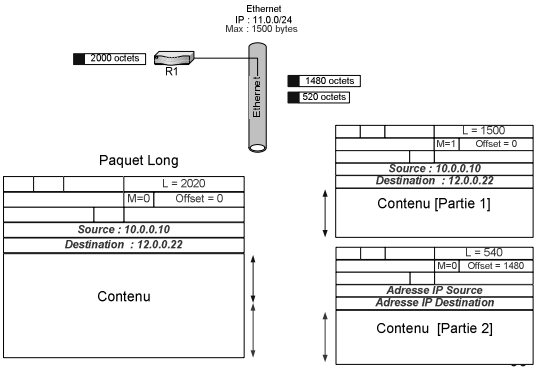
- Avantages
  - Les routeurs n'effectuent plus le réassemblage
- Inconvénients
  - Utilisation non optimale des réseau intermédiaires

Fragmentation

- Principe
  - Découper la partie contenu du paquet IP
  - Numéroter les fragments pour contrecarrer le problème de déséquencement



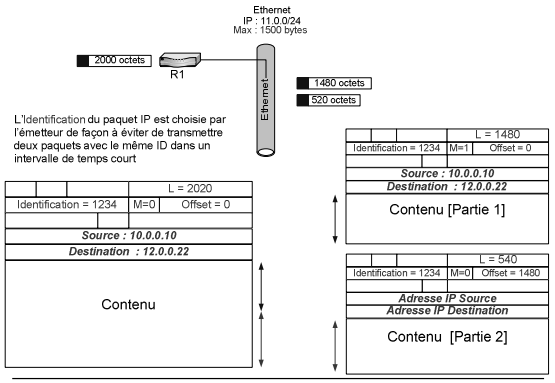
Fragment : Exemple



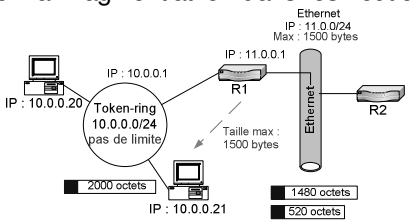
Réassemblage

- Problème à résoudre
  - Quant à t'on reçu tous les fragments ?
    - Dernier paquets contenant le bit *M* a 0
  - Que faire en cas de perte d'un fragment
    - Le paquet complet ne peut être réassembler correctement par la destination =>destruction
  - Que faire en cas de dé-séquencement
    - Utiliser le champ Offset pour réordonner les fragments d'un même paquet IP
    - Comment faire face au dé-séquencement de plusieurs fragments provenant de paquets différents ?
      - Chaque fragment doit contenir une identification du paquet duquel il provient

Identification des paquets et fragments



Éviter la fragmentation dans les routeurs



- **Problème**
  - Comment connaître la taille maximale des paquets à utiliser pour joindre une destination
- **Solution**
  - Plutôt que de fragmenter la paquet envoyé par la source, le routeur jette le paquet et informe la source de la taille maximale à utiliser
  - Connaissant la taille maximale, la source peut adapter les paquets IP qu'elle envoie
- Solution optimale mais complexe à mettre en œuvre …

IP : Problème des boucles

- Problème
  - Dans un réseau, des boucles peuvent se produire
    - Exemple
      - Mauvaise configuration des tables de routage
      - Pendant que le protocole de routage distribue une nouvelle route les tables de routage peuvent être incohérentes
  - Si un paquet boucle entre quelques routeurs, il consomme inutilement de la bande passante
- Comment résoudre ce problème ?
  - Ethernet / Spanning tree
    - Arbre de recouvrement minimum
      - Certaines lignes du réseau sont inutilisées, gênant dans les gros réseau
      - Inutilisable dans un réseau IP

Détection des boucles

- Principe
  - Chaque paquet contient un champ Time-to-Live (TTL) indiquant le nombre maximum de routeurs intermédiaires qu'un paquet IP peut traverser
    - Exemple de valeur pour les nouveaux paquets (valeur initiale) : 64
  - Chaque routeur vérifie le TTL des paquets reçus
    - Si le TTL == 1, supprimer le paquet en informant la source
    - Si le TTL > 1, traiter le paquet et le transmettre vers la destination en décrémentant d'au moins une unité le TTL
  - L'utilisation du TTL permet de limiter le temps de survie d'un paquet IP dans le réseau

IP et les erreurs de transmission

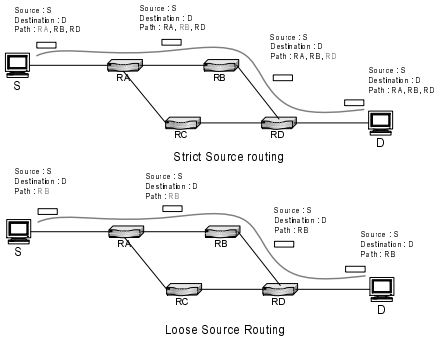
- Réaction face aux erreurs de transmission ?
  - Erreur de transmission dans le contenu du paquet
    - Impact dépendra de l'application qui utilise ce paquet
    - IP : aucune détection pour erreur sur le contenu
  - Erreur de transmission à l'intérieur de l'entête IP
    - Potentiellement plus gênant
      - L'erreur peut modifier l'adresse source ou l'adresse destination
    - IP protège l'entête des paquets avec un CHECKSUM
      - Somme de contrôle sur 16 bits calculé sur l'entête IP
      - Tout routeur vérifie le CHECKSUM des paquets reçus et supprime tout paquet reçu avec un CHECKSUM erroné dans l'entête
      - Le CHECKSUM est recalculé à chaque routeur car la valeur de l'entête change (décrémentation du TTL)

Option IP

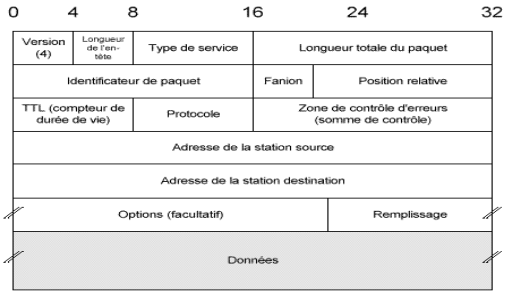
- Extensions possibles de l'entête IP
  - Strict source route option
    - Permet à la source de spécifier la liste de tous les routeurs à utiliser pour atteindre la destination
  - Loose source route option
    - Permet à la source de spécifier la liste de certains routeurs intermédiaires à utiliser pour atteindre la destination
  - Record route option
    - Permet de demander à chaque routeur traversé par un paquet d'insérer son adresse dans les options
  - Router alert
    - Permet d'indiquer aux routeurs intermédiaires qu'ils doivent faire attention en traitant ce paquet

Contraintes : maximum 60 octets pour entête + option

IP Source Routing



Format du paquet IPv4 (IP version 4)



La couche réseau - PLAN

- ✓ Utilité de la couche réseau
- ✓ La couche réseaux de l'Internet
  - ✓ Adressage
  - ✓ Format de paquets
  - ✓ Les protocoles associés
    - ✓ Protocole des messages de contrôle de l'Internet (ICMP)
    - ✓ Protocoles de résolution d'adresses : ARP et RARP
  - ✓ Fonctionnement des stations et routeurs IP

Les protocoles associés à la couche IP

- Plusieurs protocoles sont associés au fonctionnement de la couche IP
  - Routage
    - IGP : IGRP, RIP, OSPF, IS-IS, …
    - EGP : BGP, …
  - Résolution d'adresses
    - ARP et RARP
  - Contrôle (messages de diagnostic)
    - ICMP
- Le champs '**Protocole**' de l'en-tête d'un paquet IP permet
  - à un paquet complet (après son réassemblage éventuel) d'être transmis au protocole de niveau transport ou de niveau …réseau concerné
    - **ICMP** : **1** → protocole Internet de message de contrôle (de niveau réseau)
    - TCP : 6 → protocole de contrôle du transport (de niveau transport)
    - UDP : 17→ protocole des datagrammes utilisateurs (de niveau transport)
    - **OSPF** : **89** → protocoles de routage intra-domaine (de niveau réseau)
    - …
- Remarque :
  - Tous les protocoles associées à la couche IP n'utilisent pas le protocole IP directement :
    - Exemple : ARP et RARP, RIP, …

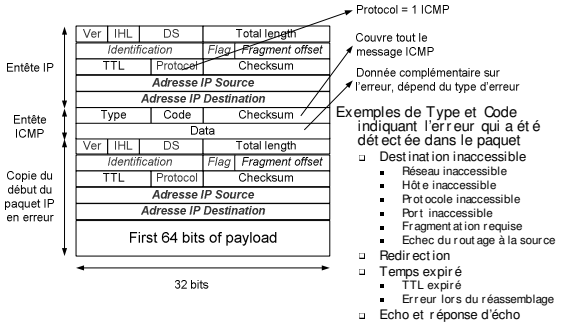
La couche réseau - PLAN

- ✓ Utilité de la couche réseau
- ✓ La couche réseaux de l'Internet
  - ✓ Adressage
  - ✓ Format de paquets
  - ✓ Les protocoles associés
    - ✓ Protocole des messages de contrôle de l'Internet (ICMP)
    - ✓ Protocoles de résolution d'adresses : ARP et RARP
  - ✓ Fonctionnement des stations et routeurs IP

ICMP Internet Control Message Protocol

- Principe
  - Lorsqu'un routeur ne peut retransmettre un paquet vers sa destination, il doit informer la source du problème qu'il a rencontré
    - Aussi utilisable par une station
  - Problème détectables par un routeur
    - Le routeur ne connaît pas de route vers la destination
    - Le format du paquet IP est incorrect
    - La source aurait du utiliser un autre routeur intermédiaire pour joindre la destination
    - Le paquet reçu a un TTL = 1
    - Le paquet reçu devrait être fragmenté, mais il contient le flag « Don't fragment »

ICMP : Format des messages



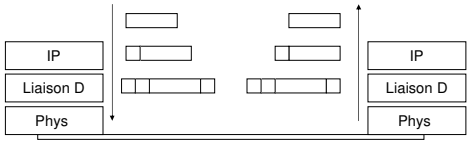
Utilisation d'ICMP : Exemples

- Exemples d'utilisation des messages ICMP
  - Destination inaccessible
    - Le routeur ou la station qui envoie ce message n'a pas de route permettant de joindre la destination du paquet 'erroné'
  - Temps expiré
    - Le TTL du paquet 'erroné' est arrivé à 0
    - Utilisé par traceroute
  - Redirection
    - Pour atteindre la destination, il faut passer par un autre routeur dont l'adresse est donnée dans le msg ICMP
  - Echo et réponse d'écho
    - Utilisé par le ping
  - Fragmentation requise
    - Le paquet aurait dû être fragmenté par le routeur mais sont bit « Don't fragment » aurait la valeur « vrais »

La couche réseau - PLAN

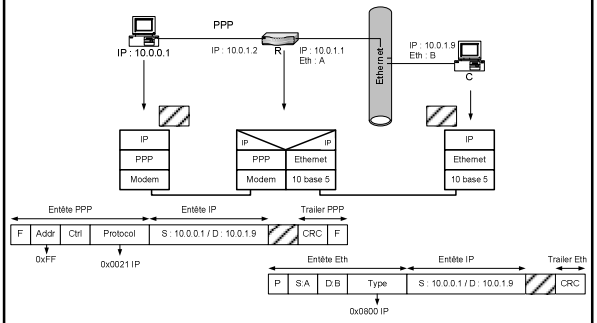
- ✓ Utilité de la couche réseau
- ✓ La couche réseaux de l'Internet
  - ✓ Adressage
  - ✓ Format de paquets
  - ✓ Les protocoles associés
    - ✓ Protocole des messages de contrôle de l'Internet (ICMP)
    - ✓ Protocoles de résolution d'adresses : ARP et RARP
  - ✓ Fonctionnement des stations et routeurs IP

Transmission des paquets IP



- Problème
  - Comment la couche liaison de données de la destination peut-elle savoir que la trame contient un paquet IP et non un paquet IPX, Appletalk, …
    - Sol: Champ de contrôle dans la trame indiquant le type de contenu

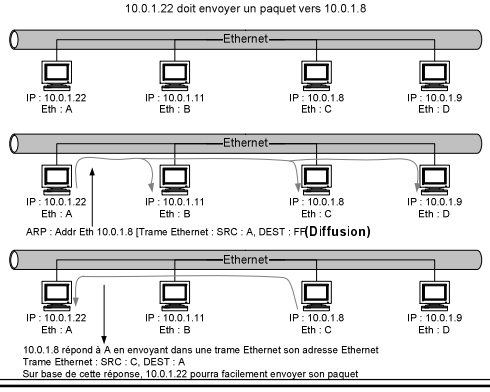
IP sur PPP et sur Ethernet



IP et les réseaux locaux

- Dans un réseau local, comment trouver l'adresse MAC qui permet de joindre une adresse IP
  - LAN supportant l'envoi de trames en diffusion (Ethernet, FDDI, Token Ring)
    - Envoyer une trame en diffusion nécessite de demander à quelle adresse de couche 2 une adresse IP correspond
    - La station ayant cette adresse IP devra répondre
      - Solution utilisé pour IP sur Ethernet (*Protocol ARP*)
  - LAN ne supportant pas l'envoi de trames en diffusion
    - Placer sur un serveur les couples @IP:@MAC
    - Contacter le serveur pour connaître une adresse MAC
      - Solution utilisé dans les réseaux ATM

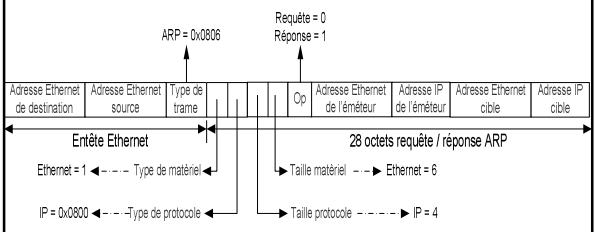
IP sur Ethernet : Protocole ARP



Optimisations

- Faut-il envoyer une requête ARP pour chaque paquet IP ?
  - Non, chaque station conserve une table ARP reprenant la correspondance entre adresse IP et adresse Ethernet
    - ARP est utilisé lorsque l'info n'est pas dans la table
- Comment faire si une station change de réseau ?
  - Temporisateur associé à chaque entrée de la table ARP
    - Temporisateur expire : entrée supprimée (15 min)
    - Validation d'une ligne de la table via une requête ARP : temporisateur réinitialisé

ARP : Format du message ARP



RARP : Reverse ARP

- Permet à un hôte (station de travail) sans disque de récupérer son adresse IP à partir d'une adresse MAC
  - Hôte sans disque => pas de fichier de configuration (IP)
    - Adresse IP récupérée au boot de la machine grâce à RARP et qu'il gardera en mémoire
    - Récupérer ensuite les fichiers de configuration
      - Masque de sous réseau récupéré grâce à ICMP (Type 17 et 18)
      - Adresse du routeur local récupérée grâce à ICMP (Type 10 et 9)
- RARP est statique et nécessite l'existence d'un Serveur RARP
  - Table de correspondance entre @ Physique et @ IP des machines sans disque
- RARP fonctionne selon le même principe que ARP
  - Les messages requêtes sont envoyés en Broadcast
  - Les requêtes RARP sont récupérées par le serveur RARP
  - Les réponses sont envoyées en unicast
  - Utilise le même format de message
    - Frame Type => 0x8035 (au lieu de 0x0806 pour ARP)
    - Op => 2 pour la requête et 3 pour la réponse (au lieu de 0 et 1 pour ARP)

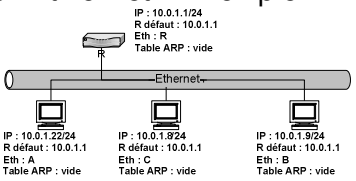
La couche réseau - PLAN

- ✓ Utilité de la couche réseau
- ✓ La couche réseaux de l'Internet
  - ✓ Adressage
  - ✓ Format de paquets
  - ✓ Les protocoles associés
    - ✓ Protocole des messages de contrôle de l'Internet (ICMP)
    - ✓ Protocoles de résolution d'adresses : ARP et RARP
  - ✓ Fonctionnement des stations et routeurs IP

Fonctionnement d'une station IP

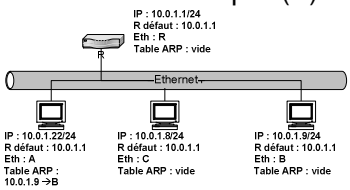
- *Informations nécessaire à une station IP*
  - Adresses MAC des interfaces de la station
  - Adresses IP des interfaces de la station
    - Pour chaque adresse IP, le masque de sous-réseau permet de connaître les adresse IP joignables via le réseau local LAN
  - Table de routage
    - Réseau(x) directement(s) connecté(s)
    - Réseaux connus de la station
      - Par configuration ou grâce à la réception d'ICMP redirects
    - Routeur par défaut
      - Route vers le réseau 0.0.0.0/0

IP sur Ethernet : Exemple



- Envoie d'un paquet IP de 10.0.1.22 vers 10.0.1.9
  - Vérifier si l'adresse destination se trouve dans le sous réseau 10.0.1.0/24 auquel la station est directement connectée
  - Oui => il faut transmettre le paquet directement sur l'Ethernet
  - Consulter la table ARP pour obtenir l'adresse Eth pour 10.0.1.9
  - Adresse Eth pas dans la table → envoi trame ARP en broadcast
  - Trame ARP de réponse venant de Eth:B (10.0.1.9 <=> Eth : B)
  - Mise à jour de la table ARP
  - Envoie du paquet IP (S:10.0.1.22, D:10.0.1.9) dans Eth
    - Source : Eth:A, Destination : Eth:B

IP sur Ethernet : Exemple (2)



- Envoie d'un paquet IP de 10.0.1.22 vers 10.0.2.9
  - Vérifier si l'adresse destination se trouve dans le sous réseau 10.0.1.0/24 auquel la station est directement connectée
  - Non => il faut transmettre le paquet au routeur par défaut
  - Routeur par défaut (10.0.1.1) est connecté à Ethernet local
  - Consulter la table ARP pour obtenir l'adresse Eth 10.0.1.1
  - Adresse Eth pas dans la table → envoi trame ARP en broadcast
  - Trame ARP de réponse venant de Eth:R (10.0.1.1 <=> Eth:R)
  - Mise à jour de la table ARP
  - Envoie du paquet IP (S:10.0.1.22, D:10.0.2.9) dans trame Eth
    - Source Eth : A , Destination Eth : R

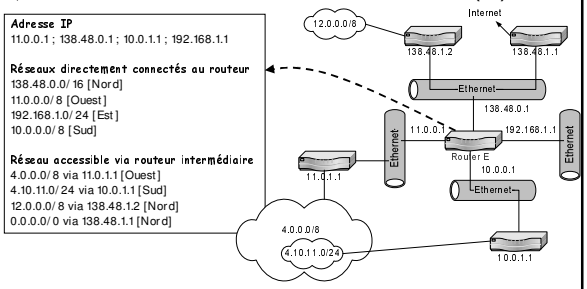
Fonctionnement d'un routeur IP

- *Que doit connaître un routeur IP ?*
  - Adresses MAC des interfaces du routeur
  - Adresses IP des interfaces du routeur
    - Pour chaque adresse IP, le masque de sous-réseau permet de connaître les adresses IP joignables via le/les LANs
  - Table de routage
    - Réseau(x) directement(s) connecté(s)
    - Réseaux connus du routeur
      - Comment joindre tous les réseaux
        - Par configuration
        - Grâce aux **protocoles de routage**
    - Éventuellement routeur par défaut
      - Route vers le réseau 0.0.0.0/0

Fonctionnement d'un routeur IP (2)

- Arrivée d'un paquet IP
  1. Vérifier si la destination du paquet est une des adresse IP du routeur
     - Si oui, le paquet est arrivé à destination
  2. Vérifier si le paquet est destiné à un des réseaux auxquels le routeur est directement connecté
     - Comparer les M premiers bits de l'adresse destination du paquet avec les M premier bits de chaque réseau directement connecté au routeur (M étant la taille du masque)
     - Transmettre le paquet sur ce réseau
  3. Rechercher dans la table de routage la route la plus spécifique
     - Comparer les M premiers bits de l'adresse destination avec les M premiers bits des réseaux connus par le routeur pour trouver la correspondance la plus longue (spécifique)
     - Transmettre le paquet en suivant cette route
  4. Si aucune route vers la destination n'est trouvée
     - Eliminer le paquet
     - Informer la source via un message ICMP

Fonctionnement d'un routeur IP (3)



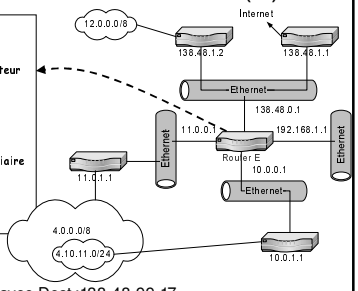
- Arrivé en E d'un paquet avec Dest :192.168.1.1
  - Dest == @ du routeur
    - Oui, paquet arrivé à sa destination

Fonctionnement d'un routeur IP (4)

Adresse IP
11.0.0.1 ; 138.48.0.1 ; 10.0.1.1 ; 192.168.1.1

Réseaux directement connectés au routeur
138.48.0.0/16 [Nord]
11.0.0.0/8 [Ouest]
192.168.1.0/24 [Est]
10.0.0.0/8 [Sud]

Réseau accessible via routeur intermédiaire
4.0.0.0/8 via 11.0.1.1 [Ouest]
4.10.11.0/24 via 10.0.1.1 [Sud]
12.0.0.0/8 via 138.48.1.2 [Nord]
0.0.0.0/0 via 138.48.1.1 [Nord]



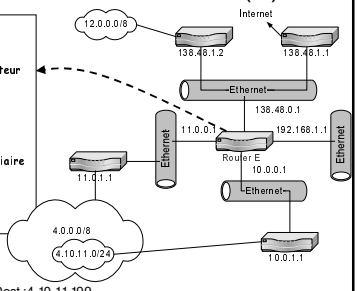
- Arrivé en E d'un paquet avec Dest :138.48.99.17
  - Dest == @ du routeur
    - Non
  - Destination dans réseau directement connecté ?
    - Oui, envoyer le paquet sur Ethernet Nord

Fonctionnement d'un routeur IP (5)

Adresse IP
11.0.0.1 ; 138.48.0.1 ; 10.0.1.1 ; 192.168.1.1

Réseaux directement connectés au routeur
138.48.0.0/16 [Nord]
11.0.0.0/8 [Ouest]
192.168.1.0/24 [Est]
10.0.0.0/8 [Sud]

Réseau accessible via routeur intermédiaire
4.0.0.0/8 via 11.0.1.1 [Ouest]
4.10.11.0/24 via 10.0.1.1 [Sud]
12.0.0.0/8 via 138.48.1.2 [Nord]
0.0.0.0/0 via 138.48.1.1 [Nord]



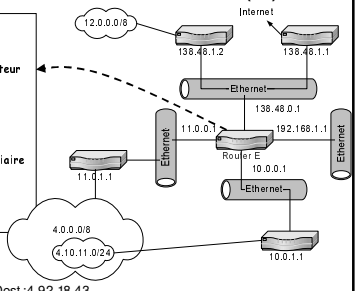
- Arrivé en E d'un paquet avec Dest :4.10.11.199
  - Dest == @ du routeur (Non)
  - Dest dans réseau directement connecté ? (Non)
  - Trouver dans table de routage la route la plus spécifique
    - Route vers 4.10.11.0/24 via 10.0.0.1 [Sud]
    - Envoyer le paquet sur le port Sud

Fonctionnement d'un routeur IP (6)

Adresse IP
11.0.0.1 ; 138.48.0.1 ; 10.0.1.1 ; 192.168.1.1

Réseaux directement connectés au routeur
138.48.0.0/16 [Nord]
11.0.0.0/8 [Ouest]
192.168.1.0/24 [Est]
10.0.0.0/8 [Sud]

Réseau accessible via routeur intermédiaire
4.0.0.0/8 via 11.0.1.1 [Ouest]
4.10.11.0/24 via 10.0.1.1 [Sud]
12.0.0.0/8 via 138.48.1.2 [Nord]
0.0.0.0/0 via 138.48.1.1 [Nord]



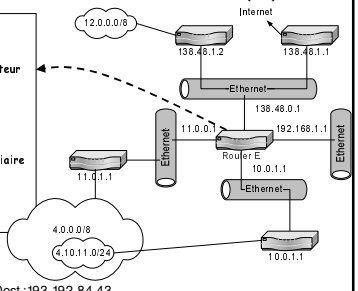
- Arrivé en E d'un paquet avec Dest :4.92.18.43
  - Dest == @ du routeur (Non)
  - Dest dans réseau directement connecté ? (Non)
  - Trouver dans table de routage la route la plus spécifique
    - Route vers 4.0.0.0/8 via 11.0.1.1 [Ouest]
    - Envoyer le paquet sur le port Ouest

Fonctionnement d'un routeur IP (6)

Adresse IP
11.0.0.1 ; 138.48.0.1 ; 10.0.1.1 ; 192.168.1.1

Réseaux directement connectés au routeur
138.48.0.0/16 [Nord]
11.0.0.0/8 [Ouest]
192.168.1.0/24 [Est]
10.0.0.0/8 [Sud]

Réseau accessible via routeur intermédiaire
4.0.0.0/8 via 11.0.1.1 [Ouest]
4.10.11.0/24 via 10.0.1.1 [Sud]
12.0.0.0/8 via 138.48.1.2 [Nord]



- Arrivé en E d'un paquet avec Dest :193.192.84.43
  - Dest == @ du routeur (Non)
  - Dest dans réseau directement connecté ? (Non)
  - Trouver dans table de routage la route la plus spécifique (Non)
  - =>éliminer le paquet et générer un message ICMP (Type 3 – destination inaccessible, Code 0 – réseau inaccessible)

Annexe

- ✓ Protocole des messages de contrôle de l'Internet (ICMP)

ICMP : Internet Control Message Protocol

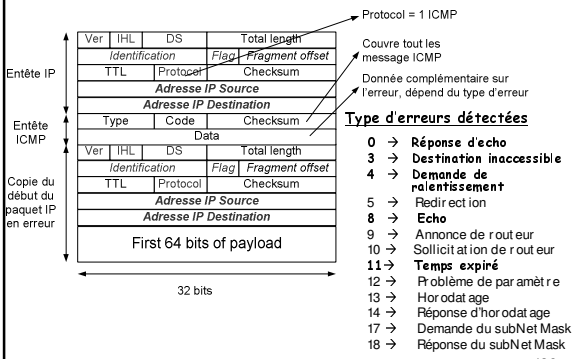
- Principe
  - Permet à un routeur ou à un hôte de fournir des informations de diagnostic à la source ou à un autre routeur
    - But : fournir un retour d'information en cas de problème réseau
      - Pas de fiabilisation du service datagramme (IP)
  - Problèmes détectables par un routeur
    - Le routeur ne connaît pas de route vers la destination
    - Le format du paquet IP est incorrect
    - La source aurait dû utiliser un autre routeur intermédiaire pour joindre la destination
    - Le paquet reçu a un TTL = 1
    - Le paquet reçu doit être fragmenté, mais il contient le flag « Don't fragment »

=> Le paquet IP est éliminé => Un message d'erreur ICMP est généré

ICMP : Internet Control Message Protocol

- Remarque :
  - Un message d'erreur ICMP ne peut être généré suite à la perte d'un autre message d'erreur ICMP
  - ICMP contient également des messages de requête (/ réponse)
  - Un message ICMP est lui-même un datagramme IP

ICMP : format des messages



Type d'erreurs détectées

- **0 → Réponse d'echo**
- **3 → Destination inaccessible**
- **4 → Demande de ralentissement**
- 5 → Redirection
- **8 → Echo**
- 9 → Annonce de routeur
- 10 → Sollicitation de routeur
- **11→ Temps expiré**
- 12 → Problème de paramètre
- 13 → Horodatage
- 14 → Réponse d'horodatage
- 17 → Demande du subNet Mask
- 18 → Réponse du subNet Mask

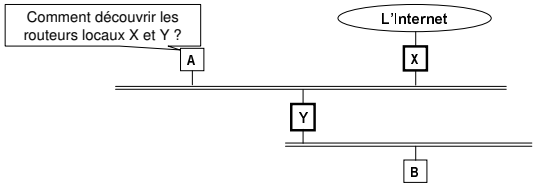
ICMP : problème de destruction de paquet

- Destination inaccessible (Type = 3)
  - Le routeur a un problème pour joindre la destination pour ce paquet
  - Codes associés (à ce type d'erreurs)
    - 0 → Réseau inaccessible (le routeur ne connaît pas de chemin vers celui-ci)
    - 1 → Hôte inaccessible (la passerelle ne connaît pas de chemin vers celui-ci)
    - 2 → Protocole inaccessible (le module du protocole spécifié n'est pas présent dans cet hôte)
    - 3 → Port inaccessible (aucun processus n'écoute sur le port spécifié)
    - 4 → Fragmentation requise mais DF = 1
    - 5 → Echec de routage source (dans IP on peut spécifier une route à la source)
  - Le champs « DATA » est inutilisé
- Problème de paramètre (Type = 12)
  - Signifie qu'une erreur de codage a été détectée dans le paquet
  - Le champs « DATA » contient un pointeur vers l'octet erroné

ICMP : problème de destruction de paquet

- Temps expiré (Type = 11)
  - Un paramètre temporel associé au paquet est arrivé à 0
  - Codes associés (à ce type d'erreurs)
    - 0 → Erreur lors de l'acheminement (TTL = 0)
    - 1 → Erreur lors du réassemblage (tous les fragments ne sont pas arrivés à temps)
  - Le champs « DATA » est inutilisé
  - Utilisé par l'outil de déboguage Traceroute
    - Génération successives de paquet IP en incrémentant leur TTL
    - Permet de tracer la route (routeurs traversés) vers une destination donnée
- Demande de ralentissement ou "source quench" (Type = 4)
  - A chaque fois qu'un routeur ou un terminal perd un paquet par débordement du buffer, il envoi ce message
    - Demande à la source de diminuer son débit d'émission
  - Pas de codes associés à ce type d'erreurs (mis à 0)
  - Le champs « DATA » est inutilisé

Comment trouver les routeurs locaux



1. Un fichier de configuration lu au démarrage du système → Non
   - Maintenance et mise à jours lourdes
     - Ajout / retrait de routeurs, changement des priorités locales ou machines sans disque
2. Ecoute des messages des protocoles de routage → Non
   - Procédure complexe
     - Diversité des protocole de routage et leurs différences
3. Découverte dynamique par utilisation des messages ICMP → Oui
   - Permet la sélection d'un routeur par défaut (ce n'est pas un protocole de routage)

ICMP : information de routage aux hôtes

- Annonce de routeur (Type = 10)
  - Permet à un routeur d'annoncer toutes ces adresses (interfaces)
  - Diffusée en utilisant l'adresse 240.0.0.1 ou 255.255.255.255
  - Diffusion à intervalle régulier
  - Le champs « CODE » est toujours à 0
  - Le champs « DATA » contient :
    - Le nombre d'adresses du routeur (en nombre de mots de 32 bits)
    - La durée de validité de l'annonce (>>intervalle pour la diffusion)
    - La liste des adresses et le niveau de préférence associé
  - Valeurs choisies en général
    - Validité = 30 minutes et intervalle = 7 minutes
    - Permet d'éviter la surcharge du réseau par la répétition de ces messages
    - Pb. : un hôte qui vient de s'initialiser peut attendre longtemps avant de pouvoir accéder au réseau

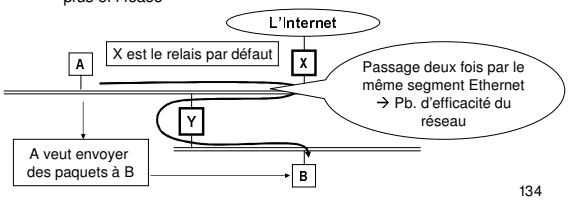
ICMP : information de routage aux hôtes

- Sollicitation de routeur (Type = 9)
  - Permet à un hôte de solliciter l'envoi du message annonce de routeur
  - Diffusée en utilisant l'adresse 240.0.0.2 ou 255.255.255.255
  - Réponse envoyée soit directement à l'hôte demandeur soit en diffusion
  - Seul le champs type est utilisé

133

ICMP : information de routage aux hôtes

- A la réception du message « Annonce de routeur »
  1. Les hôtes sélectionnent les adresses qui appartiennent au même sous-réseau
  2. La valeur « prochain relais par défaut » correspondra à l'@ du routeur ayant la plus grande valeur de préférence
- Une route par défaut Permet d'établir la connectivité
  - Inconvénient : cette route par défaut n'est pas forcement la plus efficace



134

ICMP : information de routage aux hôtes

- Redirection (Type = 5)
  - Permet d'éviter l'anomalie précédente
  - Message généré à la suite de la réception d'un paquet qui ne devrait pas passer par ce routeur
  - Signifie qu'il faut passer par un autre routeur pour atteindre la destination
    - Le champs « DATA » contient :
      - L'adresse du routeur alternatif
    - Le champs « CODE » contient :
      - 0 et 1 : rediriger les paquets pour tous les services
      - 2 et 3 : rediriger les paquets pour ce type de service
  - L'en-tête du paquet étant retransmise dans le message ICMP => reconnaître le service concerné par la redirection

135

ICMP : l'outil de déboguage PING

- Echo (Type = 8) et réponse d'echo (Type = 0)
  - Réponse d'echo est générée après réception d'un message echo
    - Inversion des adresses IP sources et destination
    - Changer le TYPE du message ICMP (8 → 0)
    - Recalculer les sommes de contrôles (paquets IP et message ICMP)
    - Garder le champs « DATA » inchangé
    - Le champs « DATA » contient des informations permettant l'édition de statistiques : un identifiant, un numéro de séquence ainsi que des données de bourrage
  - Le champs « CODE » est inutilisé (0) ds les 2 types de msg
- Demande d'information (15) et réponse d'information (16)
  - Permet le test de connectivité uniquement sans statistiques
  - Dans la spécification initiale de ICMP [RFC 792] → obsolète à présent
  - L'absence du champs données de bourrage
- L'outil de déboguage PING
  - Utilise les messages echo et réponse d'echo
  - Permet le test de la connectivité entre deux hôtes distants
  - Permet l'édition de statistiques sur l'état de la connexion

136

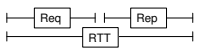
ICMP : la gestion du temps

- Horodatage (Type = 13) et réponse d'horodatage (Type = 14)
  - Permettent la synchronisation des horloges réseau (hôtes et routeurs)
  - Horodatage : format du message
    - Le champ « DATA » contient :
      - Un identifiant et un numéro de séquence (pour identifier les réponses du destinataire)
      - Les trois paramètres d'horloge (seul le premier est renseigné)
    - Le champs « CODE » est inutilisé (0)
  - Réponse d'horodatage est générée après réception d'un message horodatage
    - Inversion des adresses IP sources et destination
    - Changer la valeur du champs « TYPE » du message ICMP (13 → 14)
    - Renseigner les deux champs paramètres liés à l'horodatage au niveau de la destination
    - L'identifiant et le numéro de séquence restent inchangés
    - Recalculer les sommes de contrôle (paquets IP et message ICMP)

137

ICMP : la gestion du temps

- Messages d'horodatage
  - But : très utiles pour la supervision et l'administration du réseau
  - Exemple : reconstituer la chronologie d'une panne par un superviseur
  - Idée :
    - Envoyer l'horloge de la source (originateur) à une destination (horodatage)
    - Renvoi par le destinataire à l'originateur de 3 valeurs de l'horloge (réponse d'horodatage)
      - La valeur de l'horloge transmise par l'originateur
      - La valeur de l'horloge de la destination au moment de la réception du message d'horodatage
      - La valeur de l'horloge de la destination au moment de la transmission de la réponse d'horodatage



    - Mesurer l'écart entre les deux horloges

138

ICMP : la gestion du temps

- Les valeurs d'horloges sont en nombre de millisecondes depuis minuit UTC le jour même
  - UTC (*Coordinated Universal Time*) => référence temporelle commune
- Remarque : difficile de faire une bonne mesure de l'écart entre horloge
  - Routeurs ou hôtes qui n'utilisent pas le référentiel UTC (le bit de poids fort à 1)
  - Précision de l'horloge non en millisecondes (les bits de poids faible toujours à 0)

139

ICMP : demande du masque de sous réseau

- Procédure effectuée par les machines sans disque pour connaître leur masque d'adresse
- Requête (Type = 17)
  - Le message est envoyé à l'adresse de broadcast
  - Le champs « DATA » contient :
    - L'identification de la requête : identifiant + numéro de séquence
    - Un champs masque de sous réseau (non renseigner)
- Réponse du subNet Mask (Type = 18) est générée après réception d'un message requête
  - Remplacer l'adresse IP destination par l'adresse IP source
  - Renseigner l'adresse IP source par son adresse
  - Changer le champs « TYPE » du message ICMP (17 → 18)
  - Renseigner le champs masque de sous réseau du champs « DATA »
  - L'identifiant et le numéro de séquence restent inchangés
  - Recalculer les sommes de contrôle (paquets IP et message ICMP)
- Le champs « CODE » est inutilisé (0) dans les deux types de messages

140