CHAPITRE 5

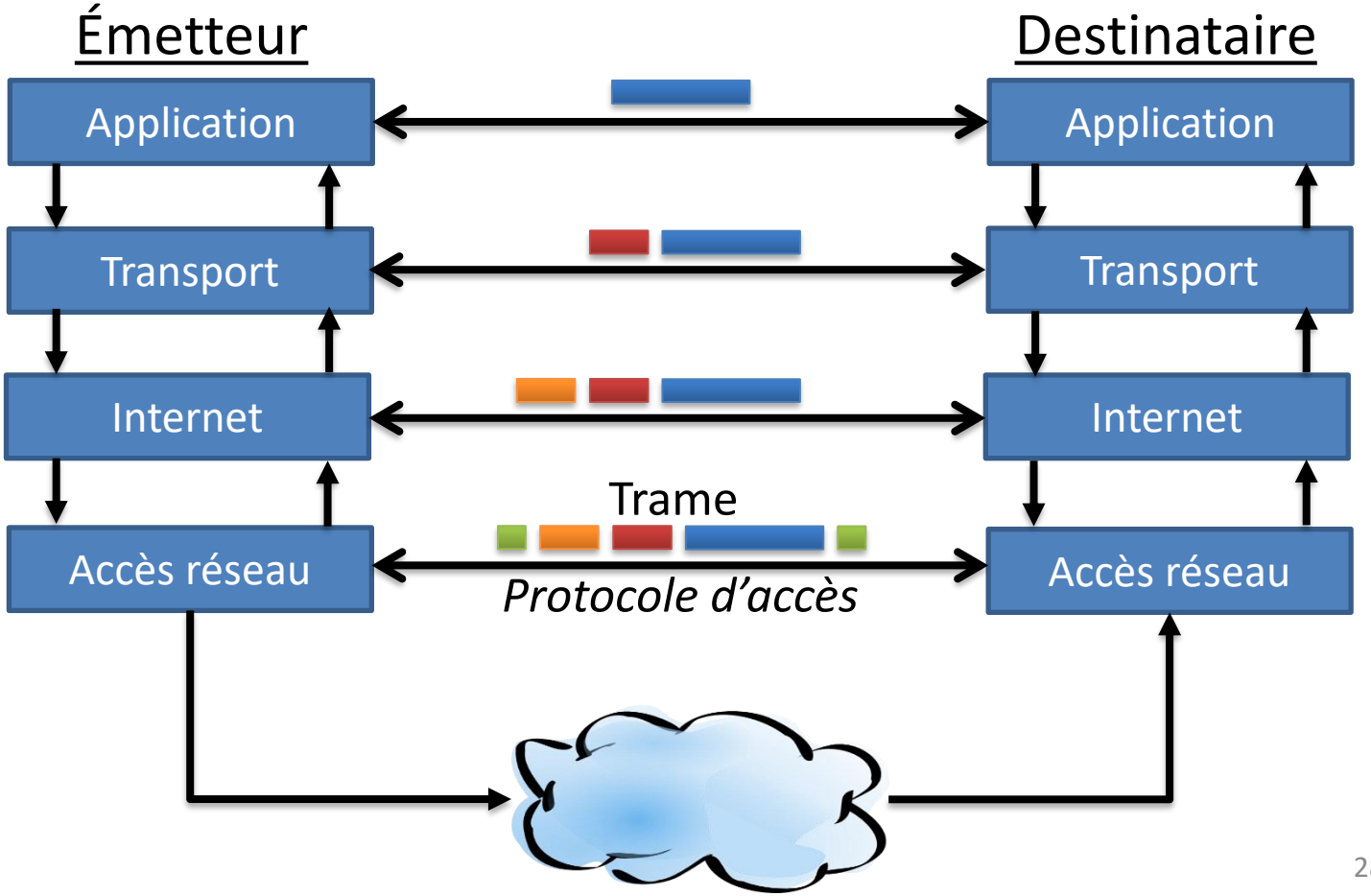
LA COUCHE ACCÈS RÉSEAU

Introduction (1)

Plan :

- **Intro**
- Délimitat. & erreurs
- Accès

- Illustration



SWILABUS

Introduction (2)

- Services fournis
  - Entre 2 couches « accès réseaux », des *trames* sont échangées
    - Les trames sont dépendantes de la technologie utilisée
      - Trame ethernet
      - Trame PPP
  - Cette couche concerne l'échange d'information **entre 2 machines directement connectées**
    - Uniquement pour des hôtes dans le même (sous-) réseau !

Plan :

- **Intro**
- Délimitat. & erreurs
- Accès

Introduction (3)

Plan :
- **Intro**
- Délimitat. & erreurs
- Accès

– Service de base
  - Propagation des informations sur la ligne
  - Le format de l'information dépend de la technologie sous-jacente

– Services possibles (pas tous disponibles)
  - *Framing :* Encapsulation des paquets à l'intérieur d'une trame (ie. *frame* en anglais)
    – *Délimitation de l'information*
    – *Identification de la source et de la destination* ***(indépendant des couches supérieures)***
  - *Link Access:* Le protocole MAC (*Medium Access Control*) contrôle l'accès au réseau (Qui ? Quand ?)

SWILABUS

Introduction (4)

- *Reliable delivery* : transfert fiable des données (avec acquits, …). Peut être utile pour des médias où le taux de perte est important
- *Flow control:* Contrôle de flux pour éviter de dépasser les capacités de traitement d'un nœud
- *Error detection* : Permet la détection (et parfois la correction) d'erreurs
- *Half / Full duplex :* Possibilité d'un dialogue bidirectionnel (envoi et réception d'information en même temps).

Plan :

- **Intro**
- Délimitat. & erreurs
- Accès

Introduction (5)

– Comparaison avec la couche transport
  - Similitudes
    –
    –
  - Différences
    –

Plan :
- **Intro**
- Délimitat. & erreurs
- Accès

Délimitation et erreurs (1)

- Délimitation de l'information
  - Une fonction importante de cette couche est de délimiter l'information
    - Connaître la taille des informations transmises
    - Pouvoir déterminer où commence une trame et où elle se termine
  - Délimitation
    - Comment délimiter la trame ?
      - En utilisant un champ longueur qui indique la taille (en octets par exemple) de l'information transmise.

Plan :

- Intro
- **Délimitat. & erreurs**
- Accès

Délimitation et erreurs (2)

Plan :

- Intro
- **Délimitat. & erreurs**
- Accès

– Exemple

– Si erreur de transmission

– En cas d'erreur

»

»

»

– Quelle solution ?

»

»

»

Délimitation et erreurs (3)

Plan :
- Intro
- **Délimitat. & erreurs**
- Accès

- Character stuffing
  - Utilisation d'une séquence de caractères de contrôles, déterminée pour signaler le début/fin de la trame
    - »
    - –

- Bit stuffing
  - Utilisation d'un marqueur binaire (séquence de bits) au début et à la fin de la trame :
    - »
    - »

Délimitation et erreurs (4)

- Illustration

Plan :

- Intro
- **Délimitat. & erreurs**
- Accès

Données à transmettre :

`01100111111111100111111101110001111111000111110`

Données adaptées :

Information transmise :

Le destinataire:

`01100111111111100111111101110001111111000111110`

Délimitation et erreurs (5)

- Détection des erreurs
  - En plus de l'information à transmettre, une donnée supplémentaire est ajoutée pour permettre de déterminer si l'information n'a pas été modifiée
    - D + EDC
  - Sur base de l'information reçue, le destinataire sait si elle est correcte :
    - D' + EDC'
  - La qualité de la détection d'erreur dépend de la méthode utilisée.

Plan :
- Intro
- **Délimitat. & erreurs**
- Accès

Délimitation et erreurs (6)

Plan :
- Intro
- **Délimitat. & erreurs**
- Accès

– Principes

- La *distance de Hamming* est le numbre de bits qui diffère entre 2 séquences (de bits) valides:
  – Soit *m* bits dans le message initial
  – Soit *r* bits ajoutés pour réaliser la détection. *m+r* bits sont transmis
  – Seul 2^m séquences de bits sont valides sur 2^{m+r} séquences de bits possibles
- Pour **détecter** *d* erreurs simples, le code doit avoir une distance de Hamming de *d+1*
- Pour **corriger** *d* erreurs simples, le code doit avoir une distance de Hamming de *2d+1*

Délimitation et erreurs (7)

Plan :
- Intro
- **Délimitat. & erreurs**
- Accès

– La parité (1 bit)
  - A chaque bloc de donnée transmis, **un bit** de parité est ajouté
    – Suivant que l'on travaille en parité *paire* ou *impaire*, le bit ajouté est positionné à 0 ou à 1 pour que le bloc contiennent un nombre pair ou impair de bits à 1.
  - Que se passe-t-il s'il y a plus d'une erreur ?
    – Les erreurs pourraient ne pas être détectées.
    – Il arrive très souvent que les erreurs se produisent en rafale. Le mécanisme de la parité est peu adapté à la vérification des informations envoyées.

Délimitation et erreurs (8)

- Que peut détecter la parité ?
  - Revenons à la distance de Hamming.
  - 8 bits de données + 1 bit de parité
  - m = 8 ; r = 1
  - 256 (2^8) combinaisons valides sur 512 (2^{8+1}) combinaisons possibles
  - Distance minimale entre 2 combinaisons valides: 2 (le bit dans la donnée + le bit de parité)
  - Suivant la relation précédente, d + 1 (avec d = 1)
    - » Donc, ce mécanisme permet **de détecter 1 erreur simple**

Délimitation et erreurs (9)

Plan :

- Intro
- **Délimitat. & erreurs**
- Accès

– La parité (2 dimensions)

- Détection et correction d'erreurs

$d_{1,1}$	...	$d_{1,j}$	$d_{1,j+1}$
$d_{2,1}$	...	$d_{2,j}$	$d_{2,j+1}$
...	...	...	...
$d_{i,1}$	...	$d_{i,j}$	$d_{i,j+1}$
$d_{i+1,1}$	...	$d_{i+1,j}$	$d_{i+1,j+1}$

0	1	0	0	1	0
1	0	1	1	1	0
0	0	1	1	1	1
1	0	1	0	0	0
0	1	1	0	1	1

0	1	0	0	1	0
1	0	1	1	1	0
0	0	**0**	1	1	1
1	0	1	0	0	0
0	1	1	0	1	1

Exemple: © Addisson Wesley, 2002

Délimitation et erreurs (10)

- Que peut détecter la parité à 2 dimensions ?
  - Revenons à la distance de Hamming
  - 8 bits de données + 2 bits de parité
  - m = 8 ; r = 2
  - 256 (2^8) combinaisons valides sur 1024 (2^{8+2}) combinaisons possibles
  - Distance minimale entre 2 combinaisons valides : 3 (le bit dans la donnée, la parité de la ligne et la parité de la colonne)
  - Suivant la relation précédente, d + 1 (avec d = 2)
    - » Peut **détecter 2 erreurs simples**
  - Suivant la relation précédente, 2d + 1 (avec d = 1)
    - » Peut **corriger 1 erreur simple**

Délimitation et erreurs (11)

Plan :
- Intro
- **Délimitat. & erreurs**
- Accès

– Le CRC (Cyclic Redudancy Check)
  - Code polynomial
  - Il faut transformer une séquence de bits en polynômes
    – 1001110 → $1*x^6 + 0*x^5 + 0*x^4 + 1*x^3 + 1*x^2 + 1*x + 0*x^0$
  - Toutes les opérations sont effectuées en arithmétique *modulo-2 sans report*
    – *Addition* et *soustraction* sont alors équivalentes à une opération XOR bit à bit
    – Ex:
      » 1001 + 1010 = 1001 XOR 1010 = 0011
      » 1001 – 1010 = 1001 XOR 1010 = 0011

Délimitation et erreurs (12)

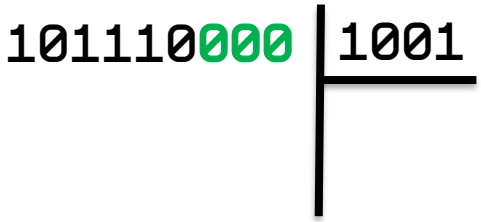
Plan :
- Intro
- **Délimitat. & erreurs**
- Accès

- Fonctionnement
  - L'émetteur et le destinataire se mettent d'accord sur un polynôme, **le polynôme générateur G(x)**
  - La donnée à une taille de *m* bits ➔ polynôme M(x)
  - Idée:
    - » On colle à M(x) une valeur de sorte que M(x) *modifié* soit exactement divisible par G(x)
    - » Le reste de la division de M(x) *modifié* par G(x) vaut alors 0.
  - Le destinataire vérifie facilement si l'information est reçue correctement en effectuant l'opération de division par le polynôme générateur
    - » Si le reste de la division vaut 0, c'est que la donnée a été transmise correctement.

Délimitation et erreurs (13)

Plan :
- Intro
- **Délimitat. & erreurs**
- Accès

- Algorithme
  - Soit *r* le degré du polynôme générateur G(x)
    - » $x^6 + x^3 + x^2 + x + 1$ est de degré 6
  - On décale M(x) de r bits vers la gauche
    - » Cela revient à ajouter *r* 0 après M(x)
    - » Cela donne M(x) modifié, noté : x^r M(x)
  - Division modulo-2 sans report de x^r M(x) par G(x)
  - Calcul de la donnée à transmettre : T(x)
    - » T(x) = x^r M(x) – reste trouvé
  - Ex: G(x) = x^3 + 1 avec la donnée: M(x) =$x^5 + x^3 + x^2 + x$



Délimitation et erreurs (14)

Plan :

- Intro
- **Délimitat. & erreurs**
- Accès

Exemple: © Addisson Wesley, 2002

```
101110000 | 1001
1001      |------
----      | 101011
00101
 0000
 ----
  1010
  1001
  ----
  00110
   0000
   ----
    1100
    1001
    ----
     1010
     1001
     ----
Reste : 0011
```

A transmettre (XOR) :

```
  101110000
-     0011
-----------
T(x) : 101110011
```


Exercice: $M(x) = x^7+x^5+x^4+x^3+ x + 1$ et $G(x) = x^3 + 1$

Délimitation et erreurs (15)

Plan :
- Intro
- **Délimitat. & erreurs**
- Accès

- Si G(x) est bien choisi, on peut
  - Détecter toutes les erreurs simples, doubles
  - Détecter toutes les erreurs en rafale de longueur <=r
- Des polynômes générateurs standardisés:
  - CCITT-CRC : $x^{16} + x^{12} + x^5 + 1$
  - IEEE CRC-32: 10000010011000001000111011011011 1
- Les CRC sont utilisés également ailleurs:
  - Disques durs, programmes de compression, …
- Un CRC peut être vu comme **une fonction de hachage à sens unique**
  - Pourquoi ?

Accès au média (1)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- Introduction
  - L'élément physique qui interconnecte les hôtes peut être
    - *Partagé:* tous les hôtes partagent le *même média*. Il convient alors d'établir des règles précises pour **accéder à ce média**
      - Ex: réseau sans-fil, réseau en bus (câble coaxial)
    - *Dédié:* Chaque hôte est relié séparément au réseau
      - Ex: réseau en étoile (câble RJ-45)

Accès au média (2)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

– On distingue généralement 2 types de liaison:
  - Lignes point-à-point
    – Il y a 2 entités : l'émetteur et le destinataire
    – Technologie: PPP (ou variante de celle-ci), …
    – Exemple: xDSL, VPN, communication série, …
  - Lignes broadcast
    – Il y a plusieurs émetteurs / destinataires
    – Chaque entité connectée reçoit (ou peut recevoir) tout le trafic réseau
    – Utilisé dans les réseaux locaux

Accès au média (3)

- 3 familles pour l'accès au média
  - Les protocoles de partitionnement du canal
    - Chaque nœud reçoit exactement une part équitable
    -
  - Les protocoles à accès aléatoire
    - Possibilité d'envoyer de l'information n'importe quand
    - Possibilité de collisions entre deux hôtes qui émettent en même temps
    -
  - Les protocoles *taking-turns*
    - Chaque hôte peut émettre à un moment déterminé et pendant un temps déterminé
    - Un système de permission est mis en place
    -

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**

Accès au média (4)

- Quel serait le protocole idéal ?
  - Soit un débit de *R* bit/s (bps)
  - Lorsqu'1 seul nœud souhaite transmettre
    -
  - Lorsque *M* nœuds souhaitent transmettre
    -
  - Protocole décentralisé
    -
  - Protocole simple et performant

Accès au média (5)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- Protocoles de partitionnement du canal
  - 2 techniques:
    - TDM (Time Division Multiplexing)
    - FDM (Frequency Division Multiplexing)
  - Si *N* nœuds et un débit de *R* bps
    - TDM
      - Division en périodes de temps. Pendant ce temps, le nœud considéré dispose de *R* bps
      - Une fois le temps écoule, le nœud suivant **peut** transmettre
      - En moyenne, chaque nœud reçoit *R/N* bps

Accès au média (6)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- FDM
  - Le canal de *R* bps est divisé en fréquences, une fréquence particulière pour chaque nœud
  - Chaque nœud utilise continuellement le canal avec un débit de *R/N* bps

– Avantages et inconvénients ?
  - Partage équitable du média (TDM et FDM)
  - Il n'y a pas de collisions
  - Si un nœud n'a rien à transmettre, sa bande passante est perdue
  - Dans tous les cas, un nœud transmet avec un débit moyen de *R/N* bps (même s'il est seul à transmettre).

Accès au média (7)

- Protocoles à accès aléatoire
  - Comment gérer l'accès au média ?
    - Supposons une ligne broadcast
    - Comment gérer l'accès ?
      - **Faire comme les humains: <u>apprendre la politesse</u>**
        - » *Donner à chacun l'occasion de parler*
        - » *Ne pas parler sans y être invité*
        - » *Ne pas monopoliser la conversation*
        - » *Demander avant d'agir*
        - » *Ne pas interrompre quelqu'un qui parle*
    - Si des nœuds parlent en même temps, on dit qu'il y a collision. En cas de collision, l'information est perdue.

<u>Plan :</u>
- Intro
- Délimitat. & erreurs
- **Accès**

SWILABUS

Accès au média (8)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- ALOHA
  - Hawaï est un ensemble d'îles. L'idée est de permettre à chaque île de dialoguer avec l'île principale
  - Pour ce faire, un satellite géostationnaire est utilisé
    - » Ce satellite peut recevoir des informations des îles et les transmettre à l'île principale
    - » Il retransmet tout ce qu'il reçoit : si 2 îles émettent en même temps ➔ superposition des signaux
    - » Avec cette technologie, pas moyen de savoir si une autre île transmet
  - Résultats:
    - » Beaucoup de collisions
    - » Si un bit d'une trame est mélangé avec un bit d'une autre ➔ collision et perte d'information
    - » Performance mauvaise: utilisation < 20 %

Accès au média (9)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- Slotted-ALOHA
  - Le temps est découpé en période: le slot. Durant cette période, il est permis de transmettre.
  - La satellite transmet un signal informant le début d'un slot de temps
  - Les trames ont une taille maximale déterminée
  - Un slot peut être : vide, contenir 1 trame, ou être en collision
  - On réduit ainsi la possibilité d'avoir des collution car toute la trame est en collision ou il n'y a pas de collisions !
  - Résultats
    - » 37% des slots sont vides
    - » 37% des slots contiennent 1 trame
    - » 26% des slots sont « en collision »

Accès au média (10)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
  - Dans d'autres technologies, il est possible de savoir si une entité est en train d'émettre ou non
  - Amélioration ?
    - » *Ecouter avant de transmettre.* Si un nœud transmet une information, attendre que celui-ci ait terminé
    - » *Si quelqu'un d'autre commence à transmettre en même temps, arrêter.* Si la réaction est rapide, la retransmission reprendra plus vite
  - Qui peut détecter une collision ?
    - » Le nœud qui transmet une information écoute le média pour s'assurer que ce qu'il entend est identique à ce qu'il transmet (➔ pas de collision).

Accès au média (11)

- Protocoles *taking-turns*
  - Un nœud est désigné comme nœud maître
  - Ce nœud offre à chacun la possibilité de dialoguer (sur base d'un tourniquet)
  - Si un nœud n'a rien à transmettre, on passe au suivant
  - Si un nœud souhaite émettre, il dispose de toute la bande passante (*R* bps)
  - Il n'y a pas de collisions (**pourquoi ?**)
  - Il faut tenir compte du temps nécessaire pour interroger les machines

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

SWILABUS

Accès au média (12)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

– Implémentation alternative: le jeton
  - La permission de transmettre est associée à la détention d'une trame spéciale: le jeton
  - Les nœuds se passent le jeton : s'il souhaite transmettre, il envoie l'information et puis le jeton
  - Si un nœud n'a rien à transmettre, il propage le jeton
  - Problème
    – Il faut veiller à ne pas perdre le jeton (en cas de problème, il pourrait ne pas être retransmis)
      » Le nœud *maître* est responsable de cela
    – Un nœud maître *backup* est nécessaire en cas de défaillance du nœud maître principal.

Accès au média (13)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- Technologies
  - Les réseaux locaux (**L**ocal **A**rea **N**etwork)
    - Un réseau local interconnecte tous les équipements d'un campus, d'une entreprise, ...
    - Certains réseaux comportent 1 ou plusieurs routeurs et sont connectés à Internet
    - Les vitesses de transmission sont très variables:
      - 10, 100, 1000, 10000 Mbps pour Ethernet RJ-45
      - 11, 54, 125, 300, 900, 1500 Mbps en Wi-Fi
      - 1000, 10000 Mbps en fibre optique

Accès au média (14)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

– Standards et normes
  - IEEE 802.3 → Ethernet
  - IEEE 802.5 → Tokenring (jeton, anneau)
  - IEEE 802.11a/b/g/n/ac → réseau Wifi
– Ethernet est la technologie la plus répandue dans les réseaux locaux
– Adresse physique (ou adresse MAC)
  - Adresse liée au matériel et se trouvant à l'intérieur d'une trame Ethernet
  - Une trame Ethernet reçue est lue par toutes les machines du même segment réseau

Accès au média (15)

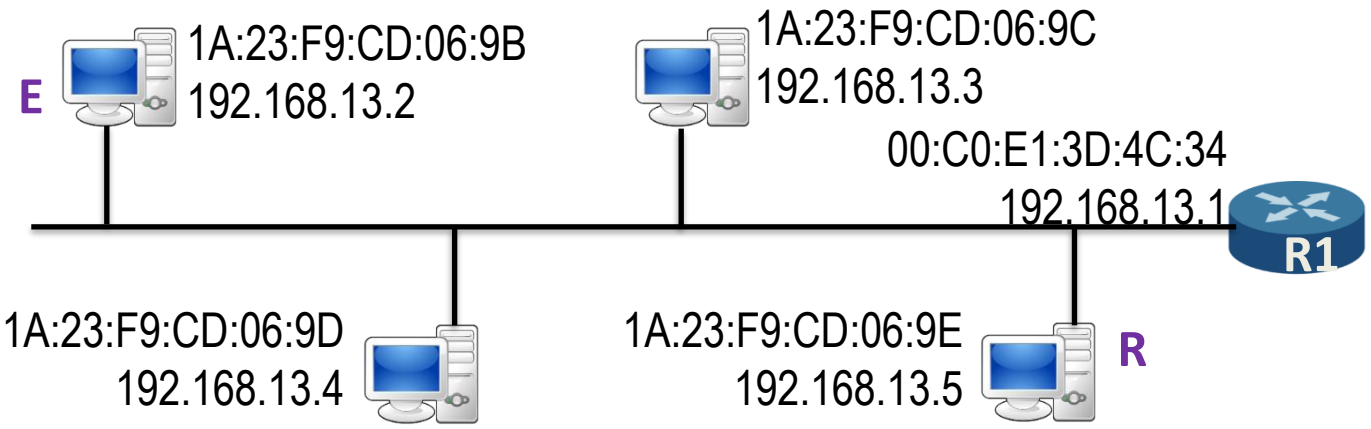
Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- L'adresse physique destinataire permet de savoir qui doit recevoir l'information
- Fonctionnement
  - Lorsqu'un nœud reçoit une information, il vérifie si l'adresse physique dans la trame correspond à son adresse à lui
    - » Si l'adresse correspond, l'information est transmise à la couche réseau
    - » Sinon, l'information est ignorée
  - L'adresse MAC est codée sur 48 bits **et est unique**
    - » IEEE alloue les 24 premiers bits suivant le vendeur
    - » Le vendeur fixe les 24 derniers bits

Accès au média (16)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- Exemple
  - 58:82:A8:BC:8D:3A (linux) 58-82-A8-BC-8D-3A (win)
- Adresse multi-diffusion (ou broadcast): FF:FF:FF:FF:FF:FF
- L'adresse est codée dans le matériel
- Fonctionnement



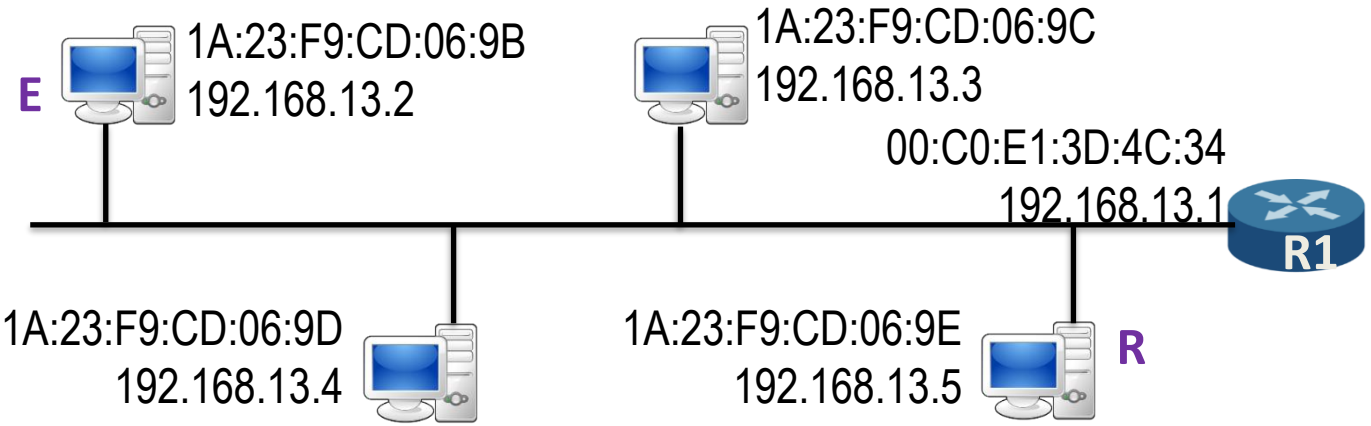
Comment connaître l'adresse physique destinataire ?

SWILABUS

Accès au média (17)

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**



Comment connaître l'adresse physique destinataire ?

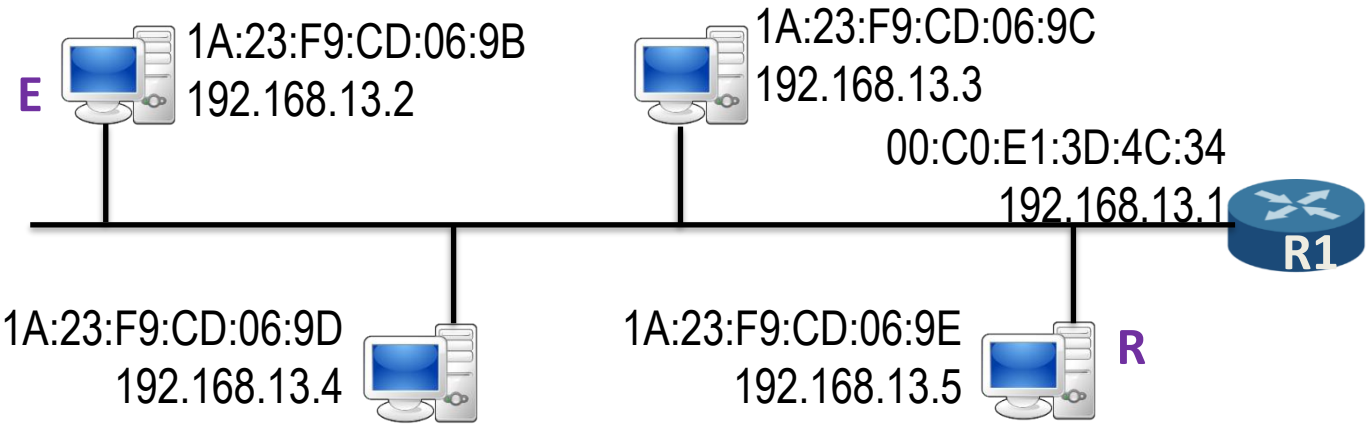
- Etape 1:
  - _
  - _
- Etape 2:
  - _

SWILABUS

Accès au média (18)

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**



Comment connaître l'adresse physique destinataire ?

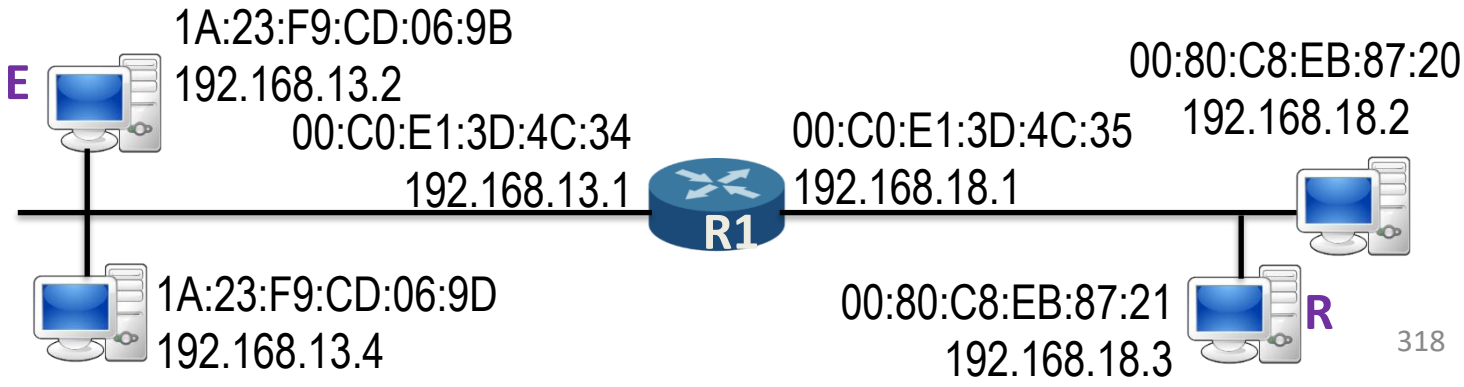
- Etape 3:
  - _
  - _
- Etape 4:
  - _
  - _

SWILABUS

Accès au média (19)

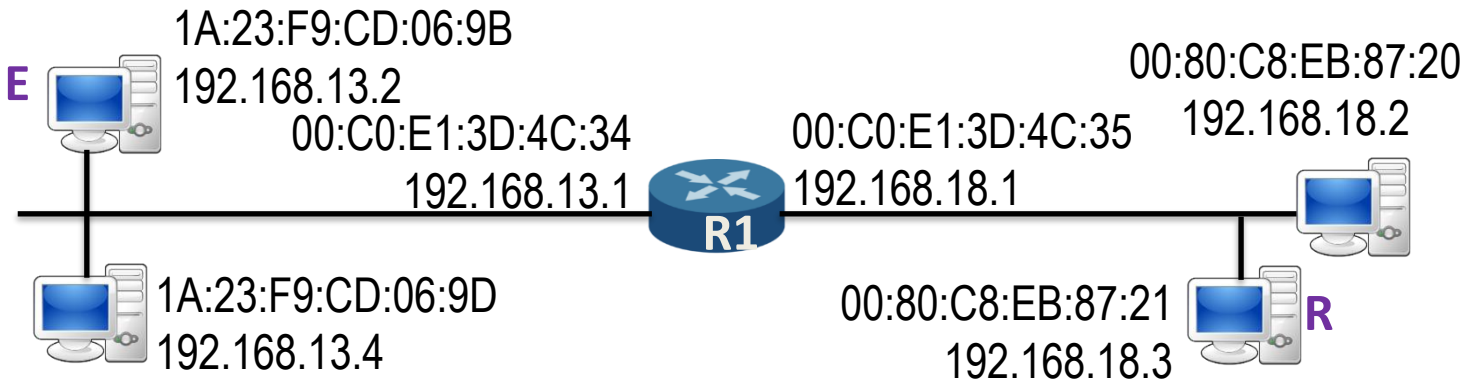
Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- Observations
  - Ce système s'appelle ARP (Address Resolution Protocol)
  - Il est utilisé **exclusivement au sein d'un sous-réseau**
  - Pour des raisons de performances, chaque nœud maintient **une table ARP** de correspondance
    - » arp -a (sous Windows / Linux) affiche la table
  - Pour des raisons de sécurité, il est possible d'imposer une correspondance MAC ⇔ IP (contre l'IP spoofing)
- Fonctionnement entre 2 réseaux :



SWILABUS

Accès au média (20)



Plan :

- Intro
- Délimitat. & erreurs
- **Accès**

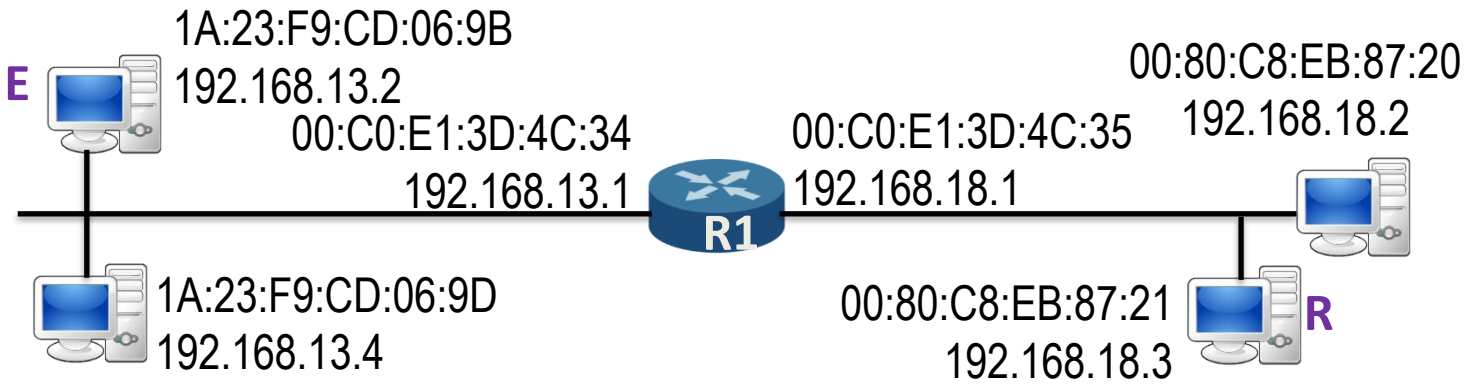
- Etape 1:
  - –
  - –
- Etape 2:
  - –
  - –
  - –

SWILABUS

Accès au média (21)

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**



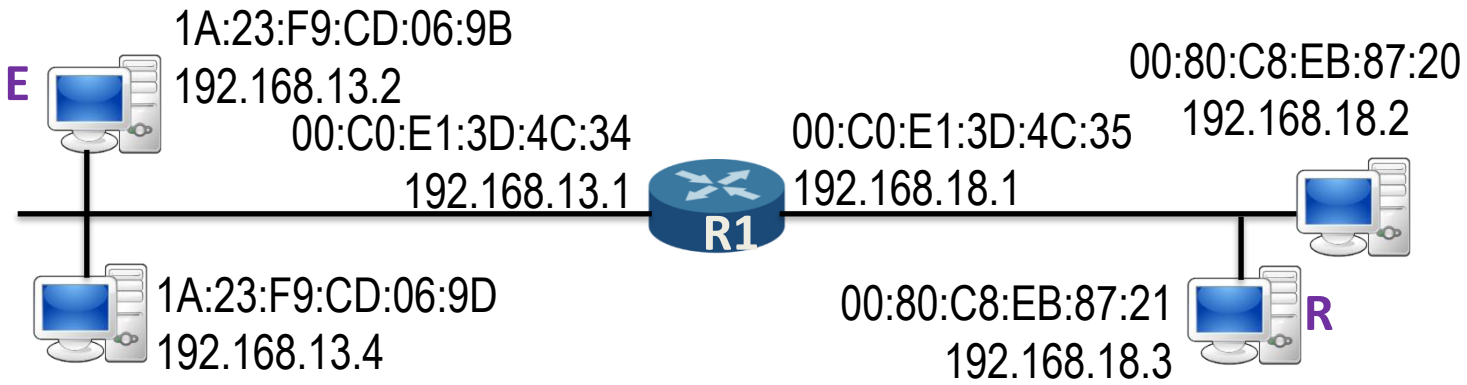
- Etape 3:
  - –
  - –
- Etape 4:
  - –
  - –
  - –

SWILABUS

Accès au média (22)

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**



- Etape 5:
  -
  -
  -

- **Pour une définition d'ARP, voir RFC 826**

SWILABUS

Accès au média (23)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

– Adresse physique en IPv6
  - En IPv6, une autre solution a été imaginée
    – Eviter les messages broadcast, très consommateur
    – Envoyer la demande à un groupe particulier contenant la machine cible (en multicast)
    – Avantage: plus efficace et moins intrusif
    – Comment identifier le groupe:
      » L'adresse multicast : ff02::1:ff00:0/104
      » Les 24 derniers bits sont copiés de l'adresse IPv6
      » Ex: Si on veut trouver l'adresse physique de la machine 2002:d970:bed2:fffa:20c:29ff:fef9:2973, on envoie un message à l'adresse multicast ff02::1:fff9:2973 qui est écoutée par la machine.
      » Elle répond en fournissant son adresse MAC

Accès au média (24)

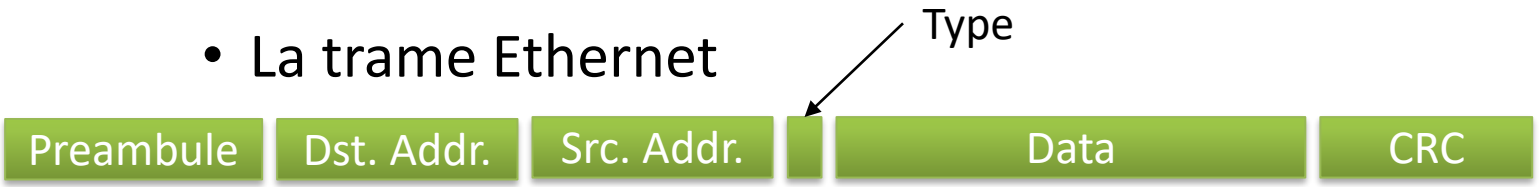
Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

– Description d'Ethernet (IEEE 802.3)
  - Très courant car:
    – Technologie éprouvée (milieu 1970) et simple
    – Evolutive (s'adapte à toutes les vitesses)
    – Matériel bon marché
  - Connectique
    – En étoile (avec un relai: switch)
      » Utilise 2 paires torsadées (et connecteur RJ45)
      » Câble UTP (Unshield Twisted Pair)
      » Vitesse: 100 Mbps – 1 Gbps – 10 Gbps

Accès au média (25)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- La trame Ethernet



  - Préambule (8 o): permet la synchronisation
  - Dest. Addr. (6 o): adresse MAC destination
  - Src. Addr. (6 o): adresse MAC source
  - Type (2 o): couche destinataire des données (IP, AppleTalk, IPX, …)
  - Data (46 – 1500 o): données en provenance des couches supérieures. Une taille minimale est imposée pour assurer la détection des erreurs
  - CRC (4 o): permet de détecter les erreurs à l'intérieur de la trame (ne porte pas sur le préambule)
- Service: orienté sans-connexion, et non fiable

SWILABUS

Accès au média (26)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

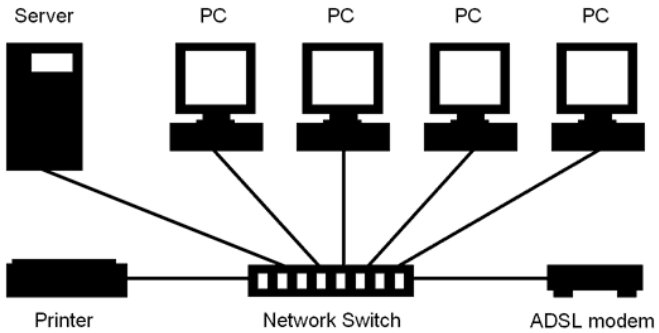
- CSMA/CD
  - Ethernet utilise une ligne broadcast (tout élément envoyé est reçu par toutes les machines connectées sur le même média)
  - CSMA/CD est utilisé pour contrôler l'accès
  - Principes
    - » Avant de transmettre une information, écoute du canal
      - Si une transmission est en cours, attente
      - Sinon, début de la transmission de la trame **avec écoute du canal** pour détecter les collisions
      - Si une collision survient, signal de collision émis et **exponential back-off** (l'attente avant la retransmission dépend du nombre de collisions)

Accès au média (27)

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**

- Topologie
  - Paires torsadées et relai
  - Connexion point à point entre le relai et les hôtes



  - Connecteurs RJ-45, 100 m entre 2 points
  - Vitesses: 10 Mbps – 100 Mbps (fast ethernet) – 1000 Mbps (1 GbE) – 10000 Mbps (10 GbE)
  - Le relai
    - » Dispose de 4,8, 16, 24, 32 ou 48 ports
    - » Le switch permet de monitorer le réseau
    - » Il peut être « intelligent », c'est-à-dire *manageable*
    - » Il peut être compatible SDN (Software Defined Network)

Image: © yourownlinux.com, 2013

SWILABUS

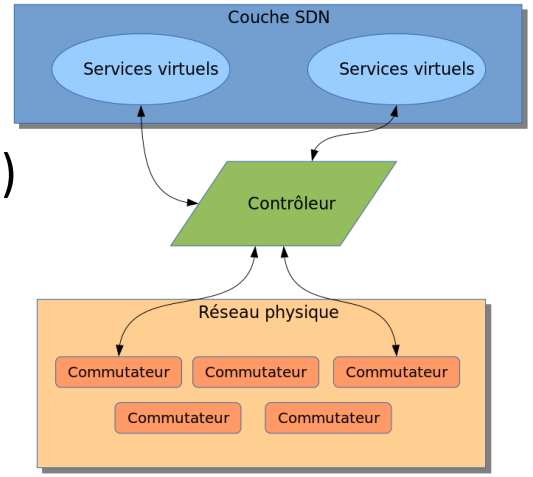
Accès au média (28)

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**

Source: Wikipédia

- SDN (Software Defined Network)
  - Découplage entre l'équipement (les switchs) et la configuration
  - L'équipement (Switch & routeur) est connecté au contrôleur SDN qui « gère » et optimise l'utilisation du réseau
    - » Equilibrage de charge,
    - » Optimisation
    - » Qualité de service
    - » Routage intelligent
  - Indépendance par rapport au fabricant
  - Exemple de protocole utilisé: OpenFlow



SWILABUS

Accès au média (29)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- Multicast Ethernet avec IPv4
  - Adresse IP multicast: entre 224.0.0.0 et 239.255.255.255
  - Construction d'une adresse MAC multicast
    - » Les 23 derniers bits de l'adresse IP sont copiés
    - » Un identificateur (fixe) est placé dans les 24 premiers bits
    - » Le bit restant est fixé à 0
  - Problème ?
    - » Une adresse MAC multicast correspond à plusieurs adresses IP multicast
    - » 5 bits de l'adresse IP sont perdus
      - Une adresse MAC multicast correspond à 2^5 adresses IP multicast, soit 32 adresses.

Accès au média (30)

– Exemple: 224.43.1.162 (adresse IP multicast)

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**

IP en binaire: `11100000 00101011 00000001 10100010`

Adresse MAC multicast

Accès au média (31)

– Exercices

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**

226.235.15.125  11100010 11101011 00001111 01111101

00000001 00000000 01011110 (0)1101011 0001111 01111101

01 : 00 : 5E : 6B : 0F : 7D

Adresses IP ? 2xx.107.15.125 et 2xx.235.15.125 (xx = 24 => 39)

01:00:5E:3D:E5:18 **Adresses IP ?**

0011 1101 1110 0101 0001 1000

61 229 24

224.61.229.24
jusque
239.61.229.24

224.189.229.24
jusque
239.189.229.24

SWILABUS

Accès au média (32)

2002:d970:bed2:fffa:20c:29ff:fffp:2973

- Multicast Ethernet avec IPv6
  - Mécanisme semblable à IPv4
  - L'adresse multicast IPv6 est construite comme suit:

128 bits

Adr. IPv6: ff02:0:0:0:1:fff9:2973 (ff00::/8)

La machine intéressée par ce trafic multicast doit écouter sur cette adresse physique également

Les 32 derniers bits sont recopiés

Adr. ethernet: 33-33-ff-f9-29-73

48 bits

Accès au média (33)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

– Interconnexion: les switchs
  - Hub = relai au niveau physique (**rare !**)
    – Reproduit sur tous ses ports un signal reçu sans vérification ➔ collisions possibles
  - Switch = relai au niveau accès internet
    – Le switch voit et peut analyser une trame
    – Lorsqu'une trame est reçue, elle est propagée sur **le** port connecté à la destination
      » Il maintient, par port, une table listant les hôtes (adresses MAC) accessibles par ce port
    – Il implémente CSMA/CD, contre les collisions
    – Il peut interconnecter des technologies différentes
    – La table de forwarding se remplit automatiquement
    – Manageable (peut être configuré)

Comment fait-il ?

SWILABUS

Accès au média (34)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

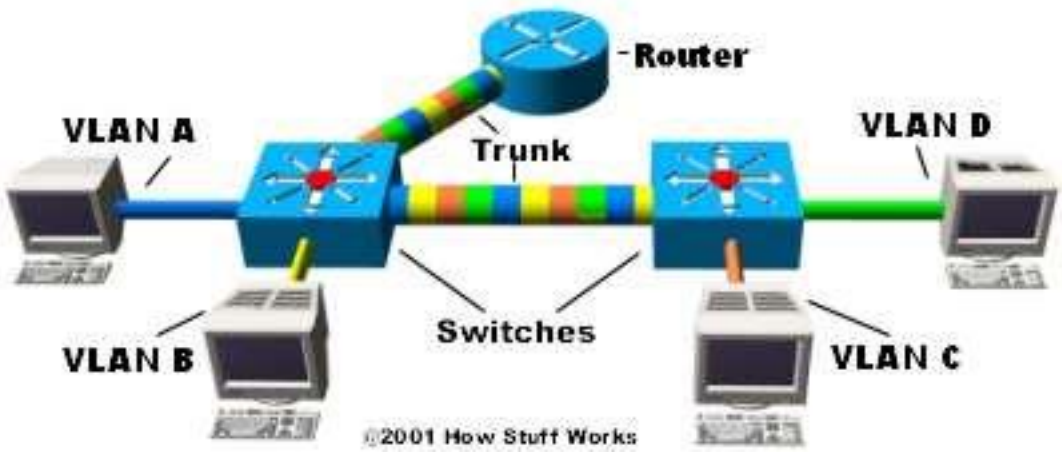
– Les VLANs
  - » Les switchs manageables peuvent permettre la création de VLANs
  - » Il s'agit de « découper » le switch pour créer des réseaux différents
  - » Ainsi, on peut choisir d'allouer 5 ports à un réseau donné et 3 ports à un autre.
    - 5 ports pour le réseau pédagogique
    - 3 ports pour le réseau administratif
    - Chaque VLAN est identifié par un numéro, le VLAN ID
  - » Plus économe que de déployer 2 switchs
  - » Plus simple à maintenir aussi

Accès au média (35)

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**

– Les VLANs et le « trunking »
  - » Un port peut appartenir à plusieurs VLANs
  - » Possible en « étiquetant » les trames
  - » Un même lien peut alors transporter plusieurs « sous-réseaux » ou plusieurs VLANs

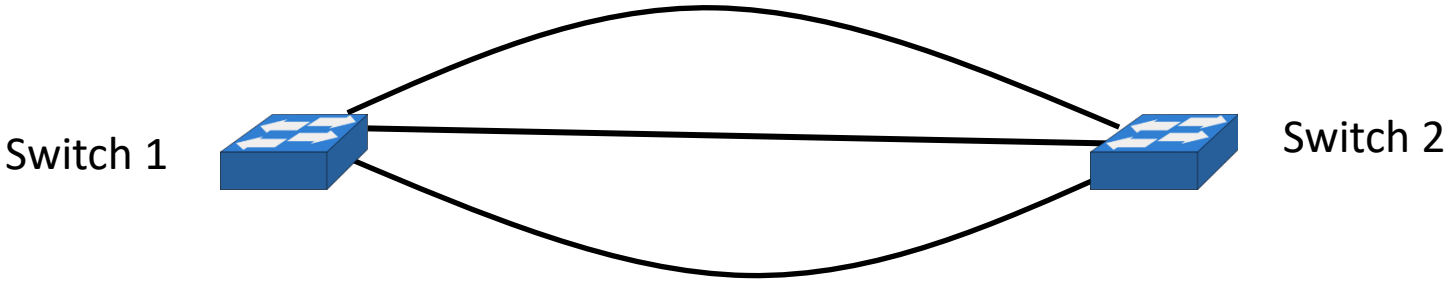


SWILABUS

Accès au média (36)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- Problème



  - Pour des raisons de sécurité, les switchs peuvent disposer de plusieurs connexions redondantes entre-eux
    - » Qui empruntent des chemins différents
    - » Qui assurent qu'en cas de rupture, les deux switchs restent interconnectés
  - **Comment éviter qu'une trame ne boucle entre ces deux switchs ?**

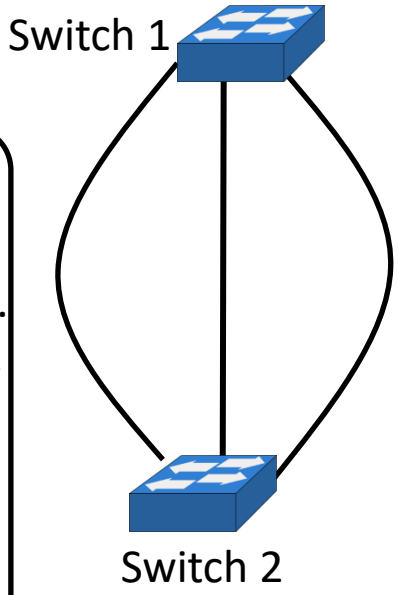
SWILABUS

Accès au média (37)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- Idée: Construire *un arbre de recouvrement minimum*
  - » Intégrant tous les nœuds du réseau
  - » « Supprimant » les boucles
- Principe: **désactiver** certains ports des switchs pour éviter qu'une trame boucle
- **Algorithme: spanning tree protocol (STP)**
  - » Norme : **802.1d**
  - » Messages échangés: appelé BPDU (Bridge Protocol Data Unit) ou message 802.1d
    - Identification de la racine (R)
    - Coût pour atteindre la racine (C)
    - Identification de l'émetteur (T)
  - » Cet algorithme est réparti dans les switchs
    - Uniquement *Manageable*

Accès au média (38)



Plan :

- Intro
- Délimitat. & erreurs
- **Accès**

» Si M1 et M2 sont 2 BPDU, on dira que M1 est *meilleur* que M2 si:

- R1 < R2 ou
- R1 = R2 **et** C1 < C2 ou
- R1 = R2 **et** C1 = C2 **et** T1 < T2

» Fonctionnement

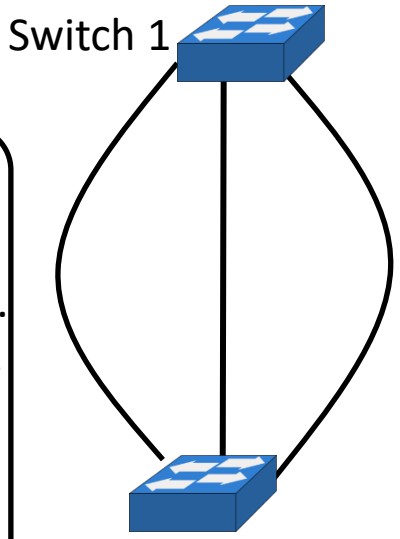
- Au démarrage, le switch se considère comme la racine. Message avec un coût de 0
- Le switch sauvegarde, **pour chaque port**, le meilleur message BPDU qu'il reçoit
- Si sur un port, le switch reçoit un meilleur message que le sien, il adapte son message
- Le protocole est stabilisé lorsqu'il n'y a plus qu'un seul émetteur de BPDU
- Le **switch racine** est le switch avec le plus petit ID (valeur T, dia précédente)

Source: © O. Bonaventure, 2019 [3]

SWILABUS

Accès au média (39)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**



Le coût est très souvent lié à la rapidité de la liaison: afin de privilégier les liaisons rapides

» Sur chaque switch, il y a:

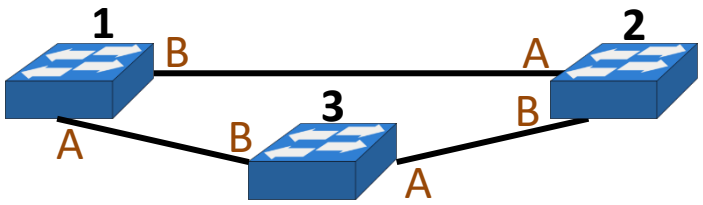
- **Un port racine** qui est le port par lequel les BPDU sont reçus. Exactement 1 port racine sur les switchs, **sauf sur le switch racine**
  - Le coût sera, ici, considéré comme étant 1+distance pour atteindre la racine ou 0 s'il s'agit du switch racine
- **Des ports désignés** si le meilleur message reçu sur ce port est moins bon que la message émis par le switch
  - Utilisé pour propager l'information
- **Des ports bloqués** si le meilleur message reçu sur ce port est meilleur que le message émis par le switch
  - Information ignorée (port désactivé)

SWILABUS

Accès au média (40)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

– Exemple simple



Switch 2, 1 puis 3

» Etape 1
- S2 démarre en pensant être la racine
  - BPDU S2: 2,0,2 (R,C,T)
- Aucun autre switch n'est actif

» Etape 2: démarrage switch 1
- S1 démarre en pensant être la racine
  - BPDU S1: 1,0,1 (R,C,T)

S2	2 0 2
A	
B	

S1	1 0 1
A	
B	

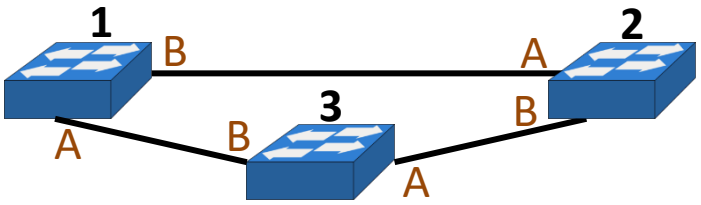
S2	2 0 2
A	
B	

SWILABUS

Accès au média (41)

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**



Switch 2, 1 puis 3

» Etape 3 : Démarrage de S3

- S3 démarre en pensant être la racine

S1	1 0 1
A	3 0 3
B	1 1 2

S2	1 1 2
A	1 0 1
B	3 0 3

S3	3 0 3
A	1 1 2
B	1 0 1

» Résultat

S1	1 0 1
A	1 1 3
B	1 1 2

S2	1 1 2
A	1 0 1
B	1 1 3

S3	1 1 3
A	1 1 2
B	1 0 1

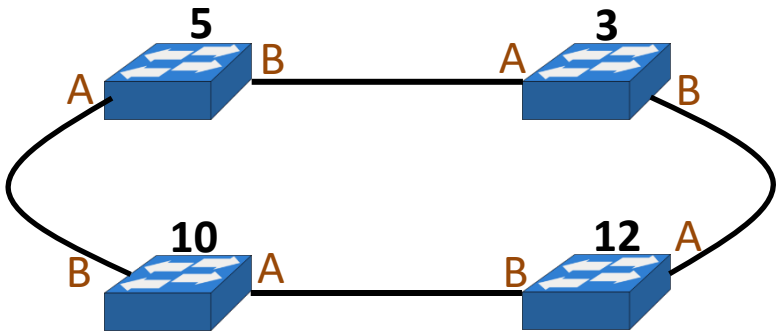
SWILABUS

Accès au média (42)

Plan :

- Intro
- Délimitat. & erreurs
- **Accès**

– Exercice



Ordre de mise sous-tension des switchs: 12, 5, 10 puis 3

Accès au média (43)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- Le protocole Point-à-point (PPP)
  - Utilisé entre **un** émetteur et **un** destinataire
    Permet la connexion au réseau internet via un modem (téléphonique ou xDSL)
    - xDSL ➔ comme PPPoE ou PPPoA
    - VPN ➔ comme PPTP
  - Décrit dans le **RFC 1661**
  - Fonctions de PPP
    - *Encapsulation*: Pour transporter des paquets IP, IPX, AppleTalk, …
    - *General:* Indépendant des technologies utilisées

Accès au média (44)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- *Détection d'erreur:* PPP doit être capable de détecter les erreurs de transmission
- *Activité d'une ligne:* PPP doit pouvoir détecter si une ligne n'est plus active
- *Négociation:* PPP doit permettre la négociation de paramètres réseaux

– Contenu d'une trame PPP

- *Flag*: permet la délimitation de la trame PPP (bit stuffing)
- *Addr* et *Control* ont des valeurs fixées: *11111111* pour l'adresse et *00000011* pour control

SWILABUS

Accès au média (45)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

- *Protocol:* Indique le type de données présentes dans les informations
  - Ex: IP (21h), AppleTalk (29h), PPCP (C021h), IPCP (8021h), …
  - Standardisé ➔ RFC 1700 & 3232
- *Information:* Information transmise dans la trame
- *Checksum:* CRC pour détecter les erreurs

– 3 sous-protocoles:
- LCP (Link-Control Protocol)
  - Etablissement de la liaison et négociation des options
  - Authentification des utilisateurs (si requis)
  - Maintient de l'activité sur la ligne
  - Fermeture de la connexion PPP

Accès au média (46)

Plan :
- Intro
- Délimitat. & erreurs
- **Accès**

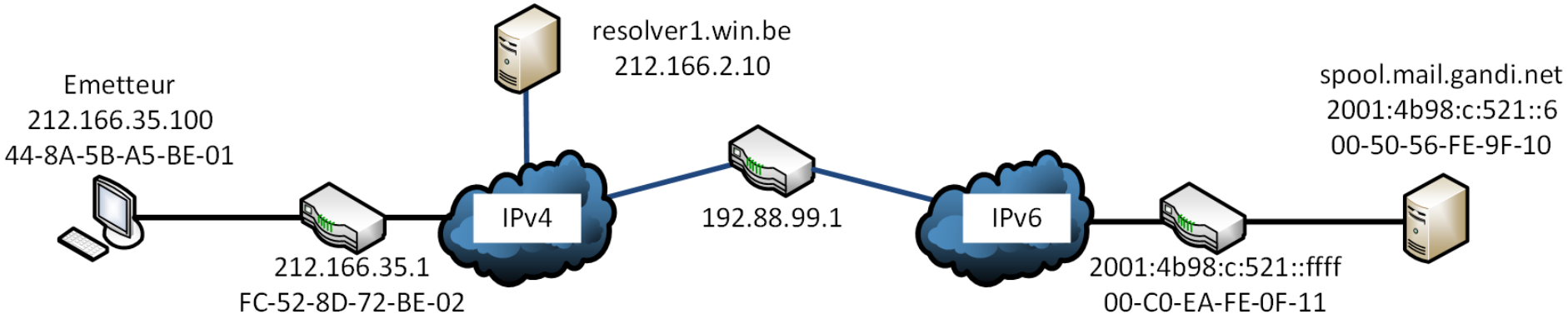
- NCP (Network Control Protocol)
  - Familles de protocoles permettant de configurer les couches réseaux supérieures
    - » IP Configuration Protocol (IPCP) permet d'obtenir des paramètres IP, DNS, …
- PPP
  - Gère la transmission des informations à la destination

– Authentification
- Devenue importante si liaison VPN
  - Ex: PAP (dépassé), CHAP (sur base d'un secret partagé)
  - MS-CHAPv1 (dépassé) ou MS-CHAPv2

EXERCICE D'INTEGRATION

Intégration (1)

- Problème
  - L'émetteur souhaite envoyer un mail en utilisant son prestataire *Gandi*



Intégration (2)

- Il faut peut-être savoir que :
  - L'émetteur est connecté au **Win** en IPv4 avec l'adresse publique 212.166.35.100 (/24). Le routeur dispose de l'adresse 212.166.35.1
  - La requête DNS **est déjà faite** et a fourni l'adresse IPv6 de Gandi => 2001:4b98:c:521::6
  - L'émetteur utilise 6to4 pour se connecter en IPv6 et le routeur relai 192.88.99.1
  - Le protocole SMTP utilise TCP, sur le port 25
  - Les adresses MAC sont précisées sur le schéma du coté de l'émetteur et du destinataire

Intégration (3)

– On vous demande de:

- Détailler ce qu'il se passe **de bout en bout** au niveau des couches **transport** et **internet**
- Détailler ce qu'il se passe **localement** au niveau des couches **accès réseau** de l'émetteur et du destinataire
- Supposer qu'aucune erreur de transmission de vient empêcher l'établissement de la connexion
- Détailler tous les mécanismes utilisés
- Préciser des valeurs si des données sont manquantes.