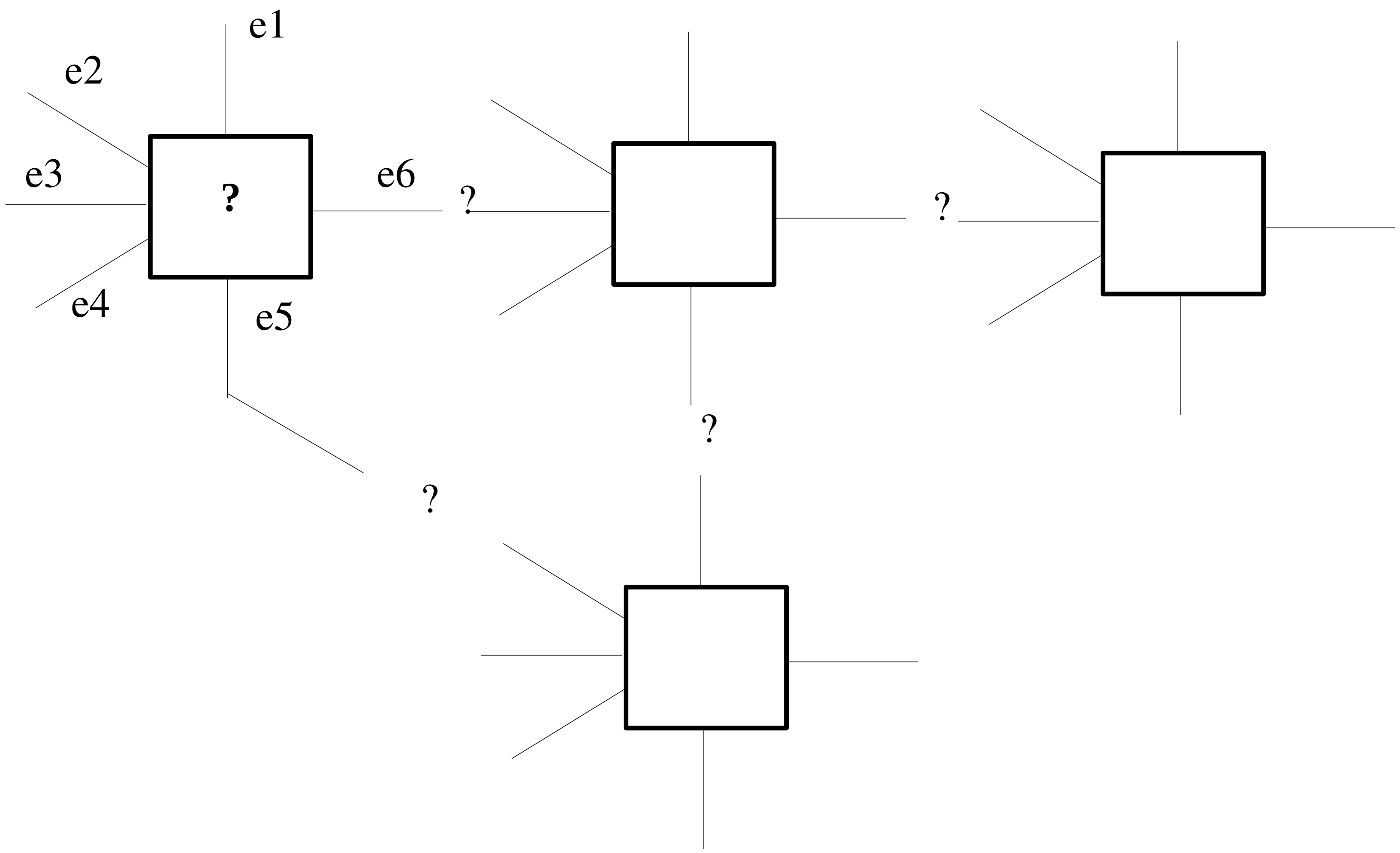
Répéteurs, ponts, routeurs

Hubs, bridges, switchs, commutateurs

Spanning tree   VLAN

environnement: interconnexion de réseaux ethernet multiprotocoles

Quels types d'équipements de raccordement ? Comment les interconnecter ?



principes généraux:

Transmission numérique: suite de bits

Espace/temps occupé par 1 bit:

à 10 Mb/s et 200 000 km/s : 1 bit = 100 ns = 20 m

à 1 Gb/s 1 bit = 1 ns = 20 cm

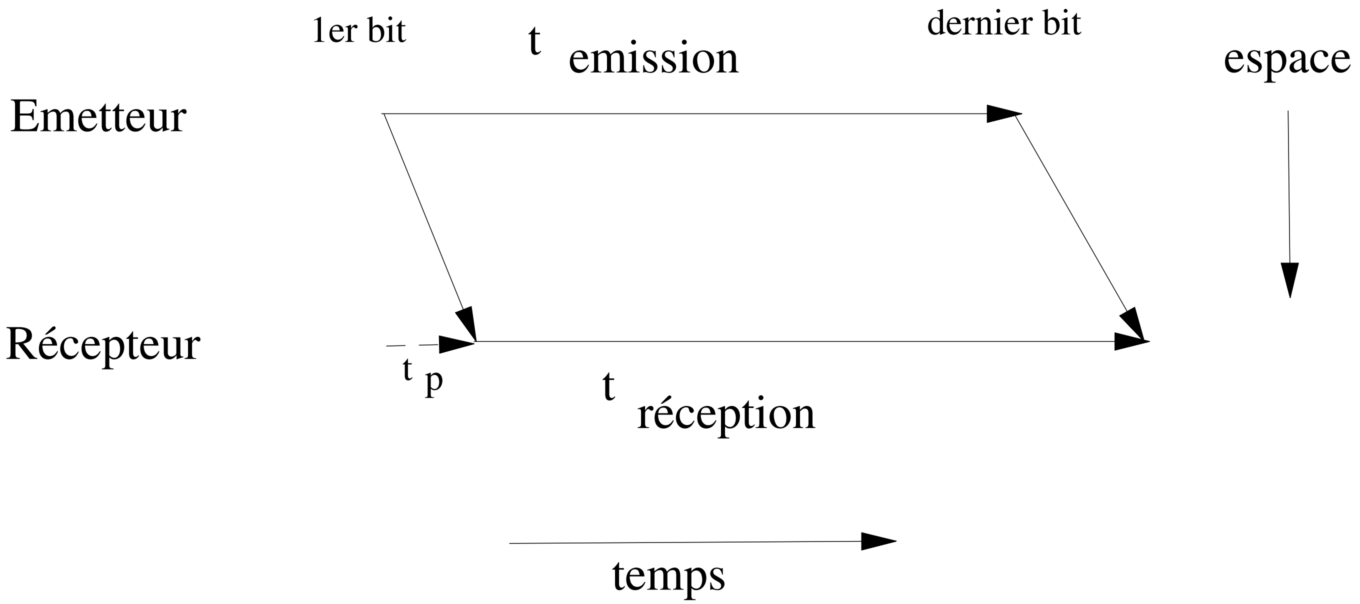
Réseau à commutation de paquets (ou de trames, de cellules)

découpage en paquets de taille limitée

partage des liens entre plusieurs communications plus souple

protection de chaque paquet contre les erreurs

Temps de transfert d'un paquet



temps de propagation= t_p = distance/vitesse

exemple: 500m à 200 000 km/s = 2,5 microsec

temps émission = temps réception = longueur paquet / débit

exemple: 10 000 bits à 10 Mb/s = 1 ms

53 octets à 155 Mb/s = 2,74 microsec

nécessité d’avoir des équipements intermédiaires

- amplification
  - affaiblissement (ex Ethernet: 100 m sur PT, 500 m coax, 2 km FO)
- partage
  - interconnexion de câbles

notions de couches (physique, liaison-MAC, réseau)

- modèle OSI

	FONCTIONS
couche réseau (ex IP)	adressage routage
couche MAC (ex ethernet)	contrôle d’accès au réseau adressage MAC (identification)
couche physique	codage adaptation au support

Trame ethernet contenant un paquet IP

entête ethernet adresses MAC destination et source

entête IP adresses IP source et destinantion

préambule	entête ether	entête IP	entête TCP ....

ethernet

principe de CSMA/CD

MA Multiple Access: réseau à accès multiple (partagé)

CS Carrier Sense: Détection du signal (ne parler que si le support est libre)

CD Collision Detect: Détection des collisions (émissions simultanées)

Détection faite par les émetteurs:

comparaison signal émis / signal reçu

En cas de détection de collision, l'émission est stoppée

puis recommencée après un temps aléatoire

influence du délai aller-retour sur la détection de collision

répéteurs / hubs

amplification (distances supérieures)

interconnexion de câbles (plus grande couverture)

- répéteurs multiports = hub
- possibilité de changer de support (optique, PT, coax)

autres fonctions

- régénération du préambule (synchronisation)
- partitionnement des segments défectueux

avantages et limitations des répéteurs

délais de traversée: de l'ordre de 0,8 µs (2,1 µs total)

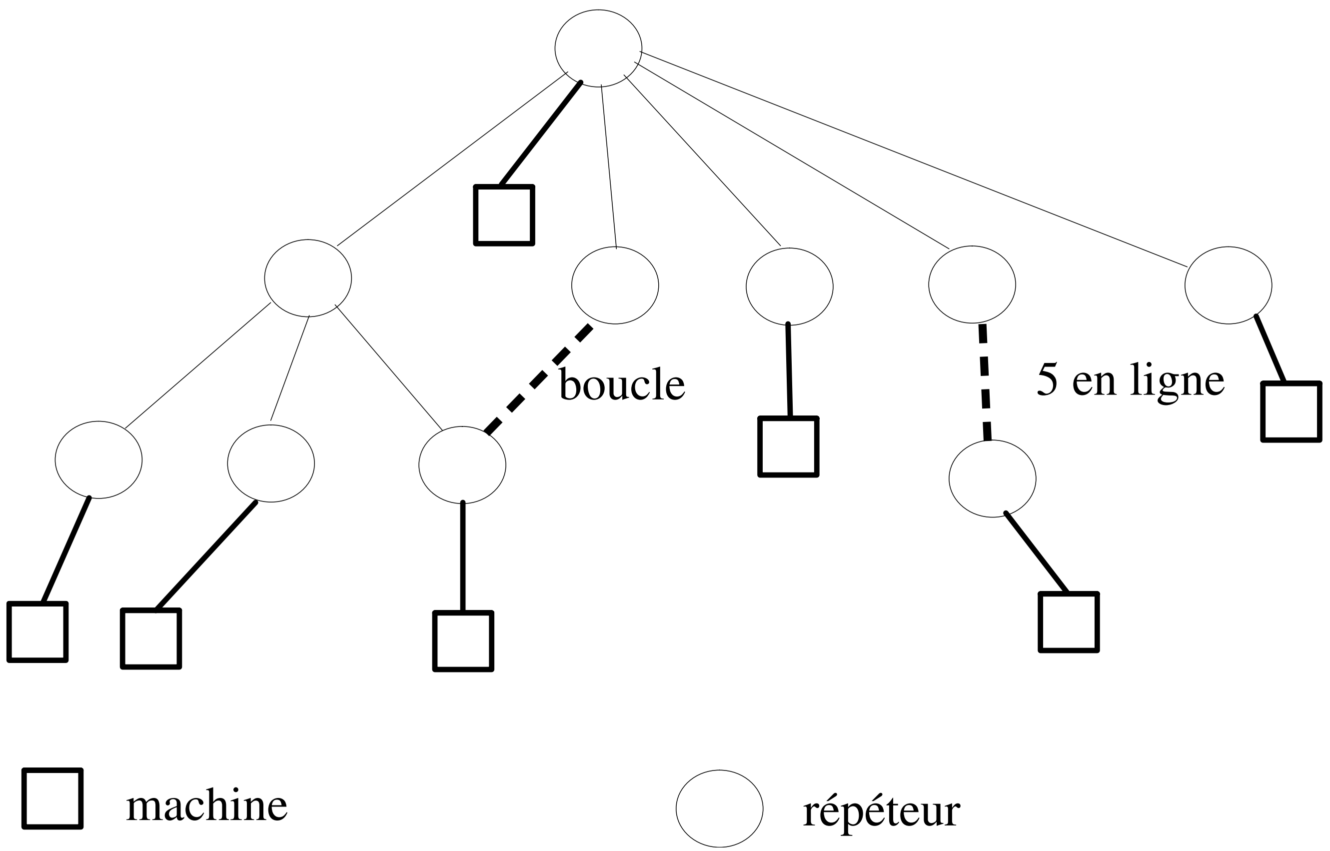
limites de configuration

pas de boucle (arbre)

pas plus de 4 en ligne (délai aller-retour)

=> limite en distance totale

CONFIGURATIONS de RÉPÉTEURS



trafic

- aucun filtrage, tout le trafic y compris les trames fausses
- traverse tous les répéteurs
- => limite en nombre de machines (saturation)

sécurité

- aucune, le trafic étant diffusé

les ponts (bridge)

pourquoi

- distances
  - augmenter les distances au delà des 2,5 km
- trafic
  - filtrer le trafic pour qu'il ne se propage pas partout
- redondance
  - permettre la redondance en cas de défaillances

- comment ça marche
  - mode store and forward
    - chaque trame arrivant par un port est stockée
    - puis réémise vers 0, 1 ou plusieurs ports
    - en fonction de l’adresse MAC destination
  - apprentissage
    - construction automatique d’une table adresse MAC => port de sortie
    - calculée à partir des adresses sources trames entrantes
    - adresses inconnues et multicast => envoyées sur tous les ports
    - entrées validées périodiquement

crc-cisco>sho bri

Total of 300 station blocks, 162 free

Codes: P - permanent, S - self

Bridge Group 1:

Address	Action	Interface	Age	RX count	TX count
00a0.2463.8b8b	forward	Fddi0	1	138	0
aa00.0400.d4d4	forward	Ethernet8	0	16290	10981
0100.8100.0101	discard	-	P	0	0
0100.8100.0100	discard	-	P	0	0
0207.010e.edef	forward	Ethernet2	0	25	0
aa00.0400.dcd4	forward	Ethernet8	0	160657	0
0207.010e.060d	forward	Fddi0	0	1	0
0020.aff2.a8a4	forward	Fddi0	1	2	0

spanning-tree

but: permettre une configuration redondante

chemins multiples en cas de défaillance

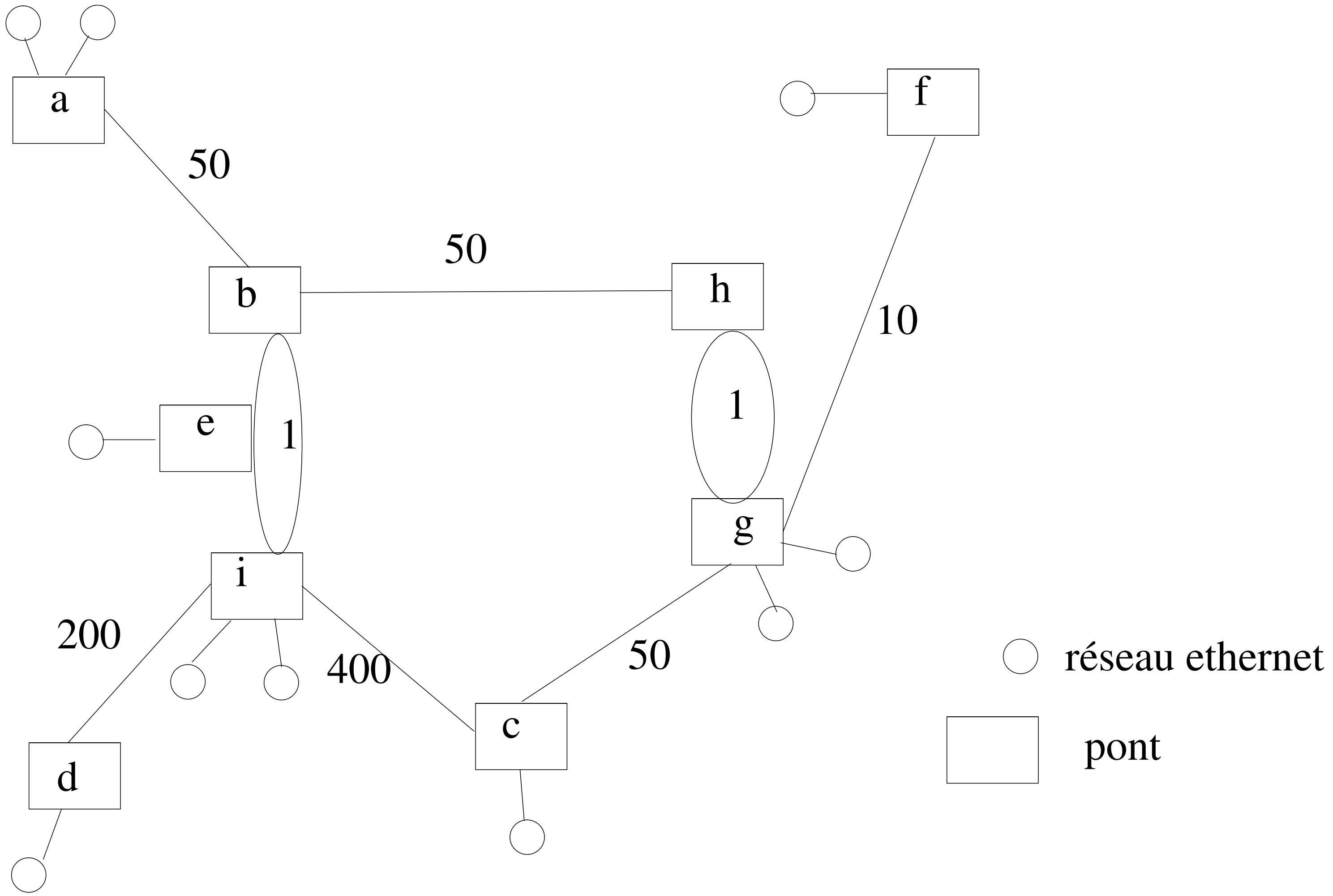
éviter que les trames tournent en rond

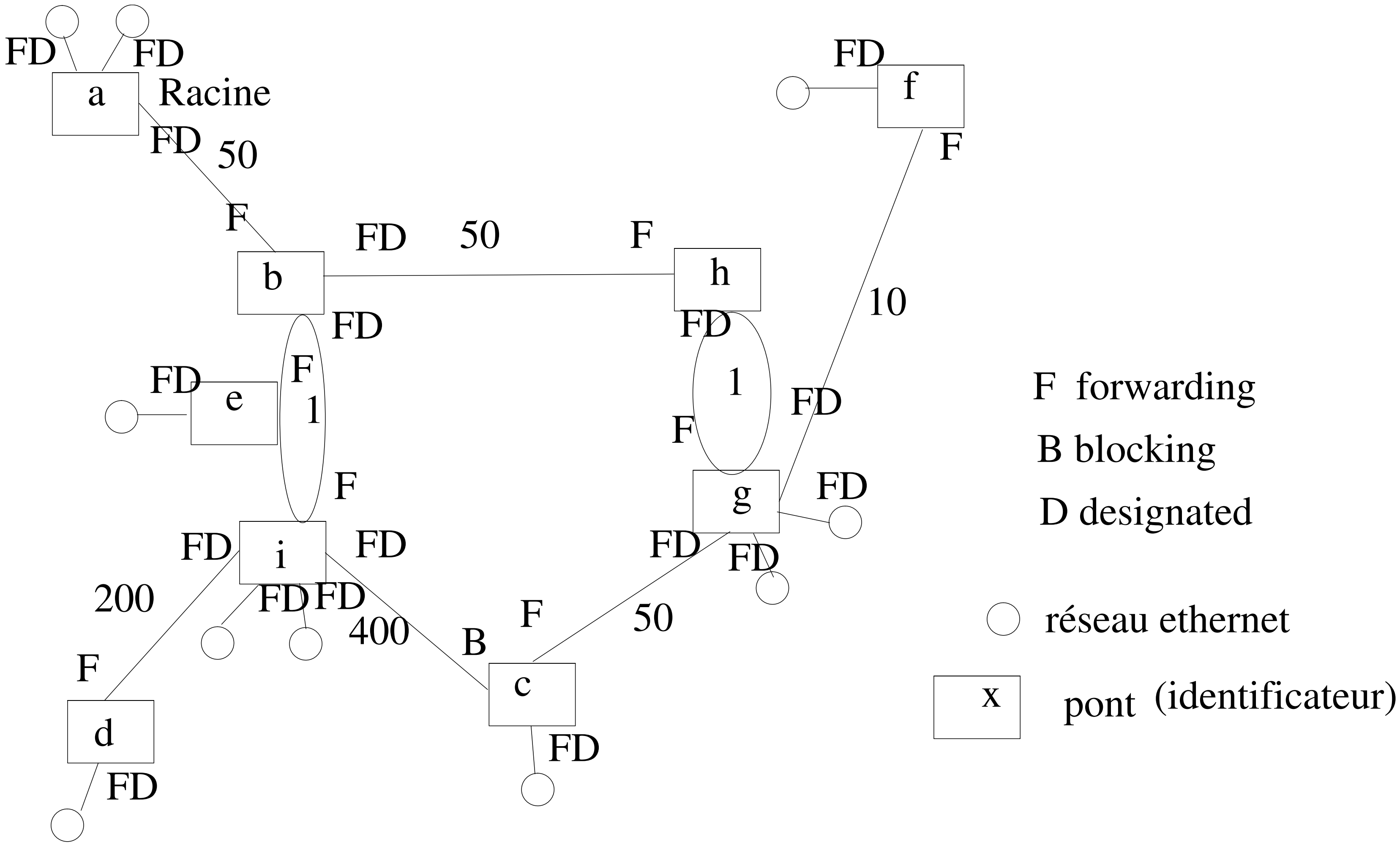
configuration automatique.

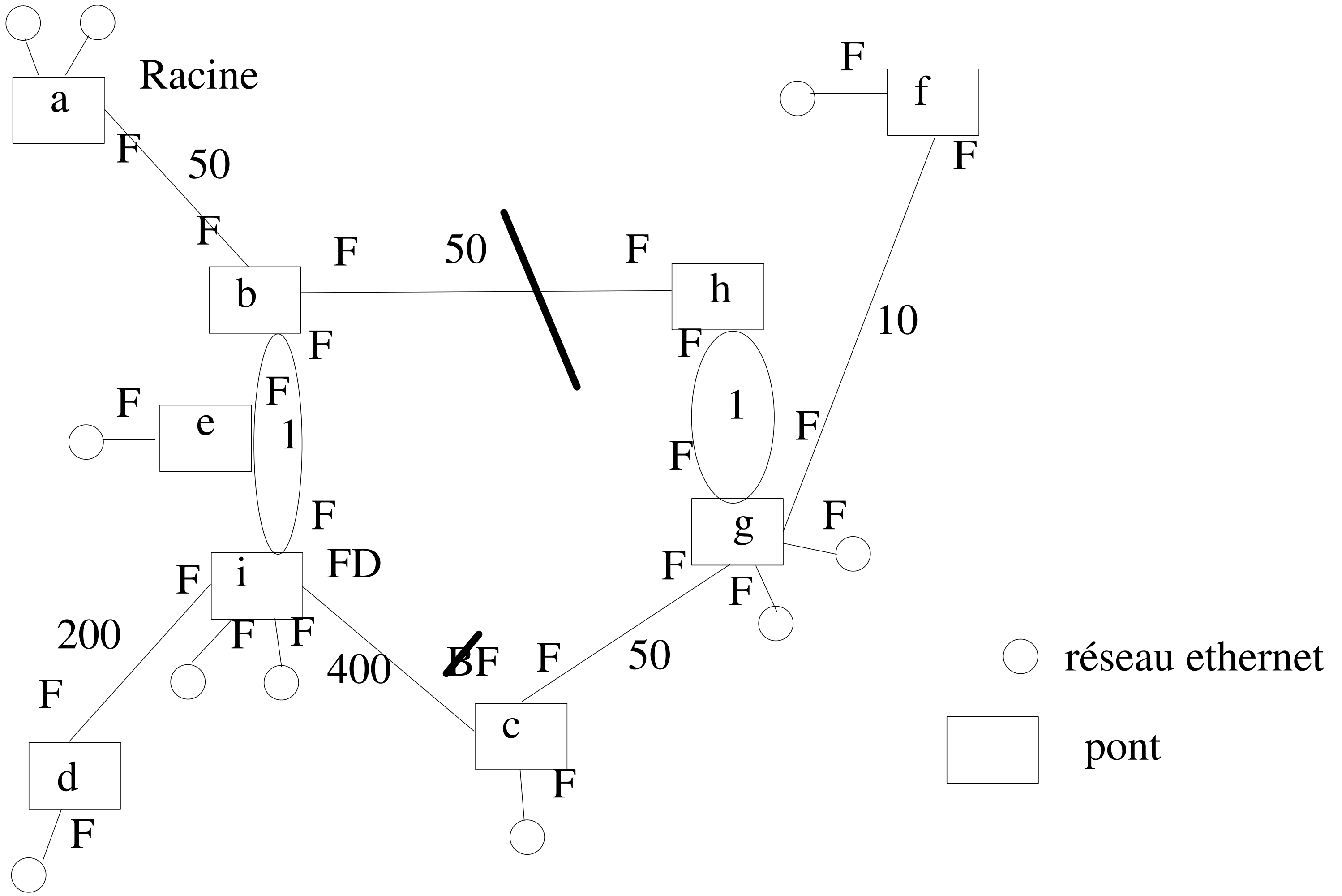
Principe: construire un arbre (tree) permettant de mettre

en "backup" (veilleuse) les liens redondants

Norme IEEE 802.1b, protocole DEC


a
50
b
50
h
10
f
e
1
1
g
i
200
400
50
c
d
réseau ethernet
pont


FD
FD
a
Racine
FD
50
F
b
FD
50
F
h
FD
FD
f
F
10
FD
F
1
e
FD
1
F
FD
1
F
FD
g
FD
FD
FD
i
FD
200
FD
FD
400
B
F
50
FD
F
d
FD
c
FD
F forwarding
B blocking
D designated
réseau ethernet
x
pont (identificateur)



Coupure de la liaison b-h

algorithme

élection d’une racine (plus petite adresse MAC par défaut)

envoi d’un message HELLO périodique par la racine (1 seconde)

désactivation des liens qui ne sont pas sur les + courts chemins vers la racine

reconstruire l’arbre si non réception de messages HELLO

absence HELLO

élire nouvelle racine

et/ou calculer nouveau chemin vers la racine

```
crc-cisco>sho span

Bridge Group 1 is executing the DEC compatible Spanning Tree protocol
  Bridge Identifier has priority 128, address 0000.0c1a.0276
  Configured hello time 1, max age 15, forward delay 30
  Current root has priority 128, address 0000.0c03.833c
  Root port is 26 (Fddi0), cost of root path is 1
  Topology change flag not set, detected flag not set
  Times:  hold 1, topology change 30, notification 30
          hello 1, max age 15, forward delay 30, aging 300
  Timers: hello 0, topology change 0, notification 0
```

Port 6 (Ethernet2) of bridge group 1 is forwarding

Port path cost 10, Port priority 128

Designated root has priority 128, address 0000.0c03.833c

Designated bridge has priority 128, address 0000.0c1a.0276

Designated port is 6, path cost 1

Timers: message age 0, forward delay 0, hold 0

Port 17 (Ethernet7) of bridge group 1 is forwarding

Port path cost 10, Port priority 128

Designated root has priority 128, address 0000.0c03.833c

Designated bridge has priority 128, address 0000.0c1a.0276

Designated port is 17, path cost 1

Timers: message age 0, forward delay 0, hold 0

```
lebel_cisco>sho span

Bridge Group 1 is executing the DEC compatible Spanning Tree protocol
  Bridge Identifier has priority 128, address 0000.0c03.833c
  Configured hello time 1, max age 15, forward delay 30
  We are the root of the spanning tree
  Topology change flag not set, detected flag not set
  Times:  hold 1, topology change 30, notification 30
          hello 1, max age 15, forward delay 30, aging 300

  Timers: hello 1, topology change 0, notification 0
```

limitations

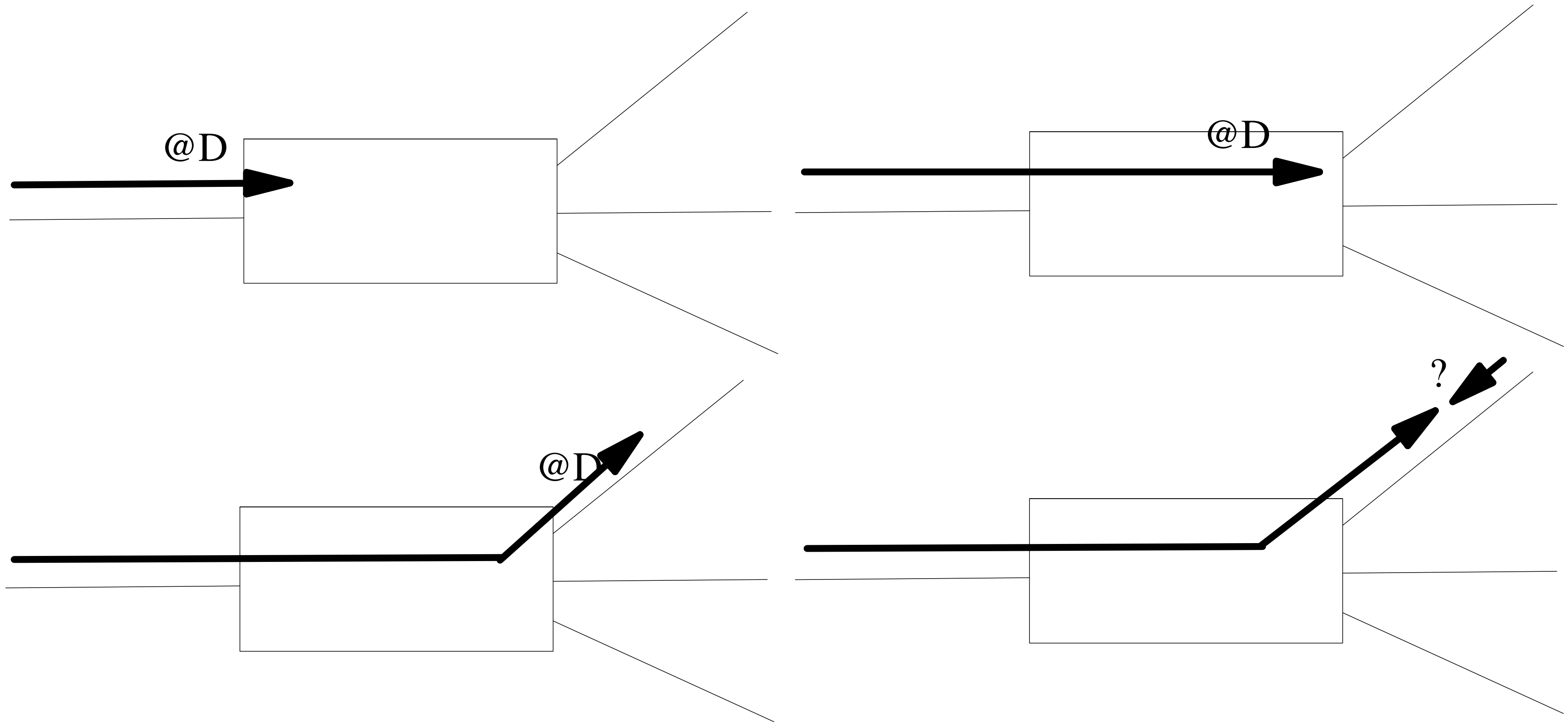
- trafic broadcast/multicast
  - trames broadcast/multicast ou a un destinataire inconnu
  - inondent le réseau risque de Broadcast Storm
- concentration du trafic
  - en cas de liens redondants, un seul est utilisé à un moment donné
  - pas de partage de charge
- sécurité
  - pas de contrôle sur la localisation des machines
  - filtrage sur les adresses MAC possible mais difficile à gérer

les commutateurs (de trames) (switch)

ponts multi-ports rapides (commutation hard, ASIC)

modes store and forward / cut-through

- mode cut-through :
  - une trame commence à être réémise sur un/des port de sortie
  - avant d'être reçue: décision sur une partie d'entête
    - adresse MAC destination: préambule + 6 octets


@D
@D
@D
?

avantages

- rapidité de commutation ou latence (15 à 60 µs)
- store and forward: dépend de la longueur de la trame
  - de 51,2 µs (64 octets) à 1,21 ms (1518 octets) + temps commutation

inconvénients

- propagation de trames fausses et collisions
- ports de même débit
- gestion des collisions plus complexe
- le gain en rapidité n’existe que quand le port de sortie est libre

Vers la micro-segmentation

Un port commuté par machine

Différent de 10 Mb/s par machine !

dépend de la répartition des flux

nécessité de backbone à plus haut débit (FDDI, fast ethernet, ATM)

Ethernet 100 Mb/s (100 base Tx, 100 base FX)

10 fois + rapide => délai aller retour doit être 10 fois moindre (5,12 µs)

100 base Tx: 100 m sur 2 paires (catégorie 5)

100 base Fx: 400 m (point à point half duplex), 2 km (full duplex)

moins s'il y a des répéteurs (100 m PT + 185 m FO)

2 types de répéteurs:

classe I: temps de traversée 1,68 µs 1 seul répéteur autorisé

classe II: temps de traversée < 0,92 µs   2 répéteurs autorisés

Conclusion: plus le réseau est rapide,

plus on a besoin de remplacer les répéteurs par des switchs

les routeurs

pourquoi router

- mieux contrôler qui communique
  - par où il communique
- système extensible à très grande échelle (Internet)

adressage / table de routage

- adresse donne une indication sur le lieu (au sens réseau)
- table de routage: adresse => direction (port) à prendre

protocole de routage

- permet d'échanger automatiquement des informations de routage avantages

- partage de charge
  - toutes les routes ne prennent pas les même liens
  - possibilité de répartition de charge entre plusieurs routes
- limitation des multicasts
- limitation des tables (notions de réseau)
  - les adresses sont regroupées
    - machine => sous-réseau => réseau => "super"-réseau

inconvénients

- temps de latence
  - store and forward + traitement complexe par soft
  - apparition de routeurs hard
- dépendance adresse/localisation
  - l'adresse dépend de la localisation dans le réseau
  - => changement de lieu ou de réseau => changement d'adresse
- dépendance des protocoles de niveau réseau
  - le routage est différent pour chaque protocole réseau
  - IP, IPX, AT, Decnet, ISO, ...

configuration

nécessite une configuration des machines et des routeurs

adresse, netmask, routeur par défaut, ...

les VLAN (Virtual LAN)

principe général

Dans un réseau comportant un ou plusieurs commutateurs

Répartir les trames dans plusieurs "ensembles" (VLAN)

Ces trames ne sont propagées que vers les ports des commutateurs

associés à ce VLAN.

Dans un VLAN distribué sur plusieurs commutateurs

- les commutateurs jouent le rôle de pont
- possibilité d'un spanning tree différent par VLAN

Les VLAN ne communiquent pas directement entre eux

nécessite des routeurs inter VLAN

Association d'une trame à un VLAN

pas de méthode normalisée actuellement

VLAN par port

méthode la plus courante: VLAN = ensemble de ports distribués

on définit une sorte de commutateur distribué

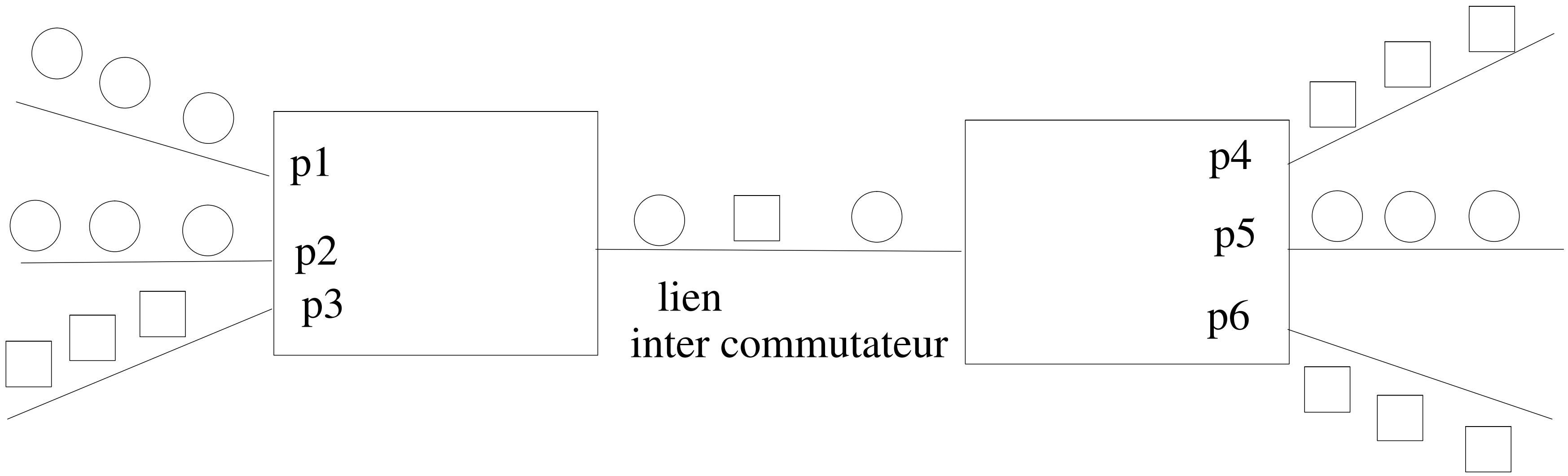
inconvénient: on doit repérer l'appartenance de la trame

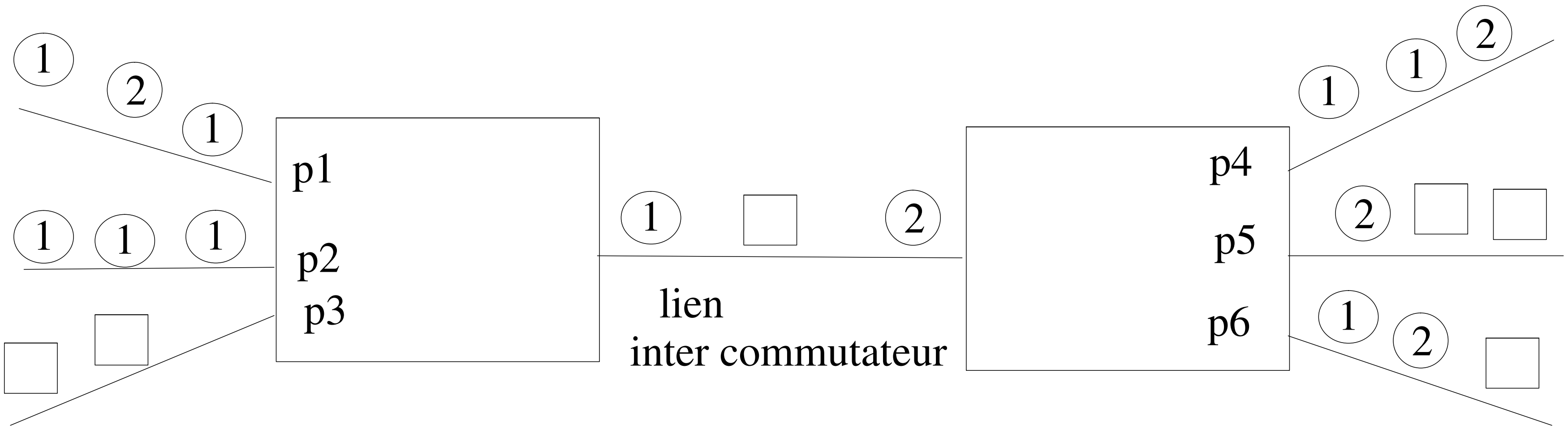
à son VLAN en ajoutant de l'information (tag, ...)

difficile à interopérer

VLAN défini par le contenu de la trame

- adresse MAC source (permet la mobilité, sécurité)
- protocole (IP, IPX, ..., code protocole de la trame)
- adresse réseau (subnet IP: permet la mobilité, mais spoofing)
- tout champs fixe de la trame


p1
p2
p3
lien
inter commutateur
p4
p5
p6


1
2
1
1
1
1
p1
p2
p3
1
2
lien
inter commutateur
p4
p5
p6
1
1
2
2
1
2

- intérêts
  - indépendance physique/logique
    - les utilisateurs d'une communauté peuvent être dispersés
  - séparation de trafic
  - rapidité de la commutation
- inconvénients
  - normalisation?
    - pas de méthode normalisée pour relier des commutateurs
      - marquer les trames par Numéro de VLAN (tagging 802.1q)
      - connexions par VLAN (ELAN ATM)

distribution automatique de règles décrivant chaque VLAN

administration

difficile suivant type de VLAN (MAC address)

difficultés de diagnostic de connectivité

TABLE RÉCAPITULATIVE

Critère	Répéteur	Pont/Commutateur	Routeur (IP)
limite cascade	oui (4 à 10Mb/s)	pas vraiment	non (TTL 255)
topologie boucle	non	oui	oui
redondance automatique	non	oui	oui
Partage charge	non	non	oui
latence	0,8 μs	qq μs à 1 ms	qq ms
propagation broadcast/multicast	oui	oui	non
filtrage trafic	non	oui	oui

multiprotocole (IP, IPX, ...)	oui	oui	ça dépend
MAC différents	non	parfois	oui
débits différents	non	oui (sauf cut-through)	oui
media différents	oui (parfois)	oui	oui
Nombre ports	centaines	quelques uns (ponts) dizaines (commutateurs)	peu (ou cher)