13

Le routage des flux multimédias

Qui dit multimédia dit également diffusion d'un flux audio ou vidéo à plusieurs destinataires, dans le cadre d'une conférence, par exemple. Un même film vidéo peut ainsi être dupliqué en autant de flux qu'il y a de destinataires.

Afin de limiter la charge induite sur le réseau, il est bien plus judicieux de dupliquer ce flux au plus près des destinataires. Pour ce faire, trois mécanismes doivent être mis en place sur notre réseau IP :

- un adressage permettant de désigner des groupes de machines plutôt qu'une seule ;
- un mécanisme permettant d'identifier les groupes actifs au sein du réseau ;
- un mécanisme permettant de router les paquets en les dupliquant le moins possible.

Sans cela, notre réseau IP serait vite engorgé, surtout sur les liaisons WAN pour lesquelles le débit est compté.

Dans ce chapitre, vous apprendrez ainsi :

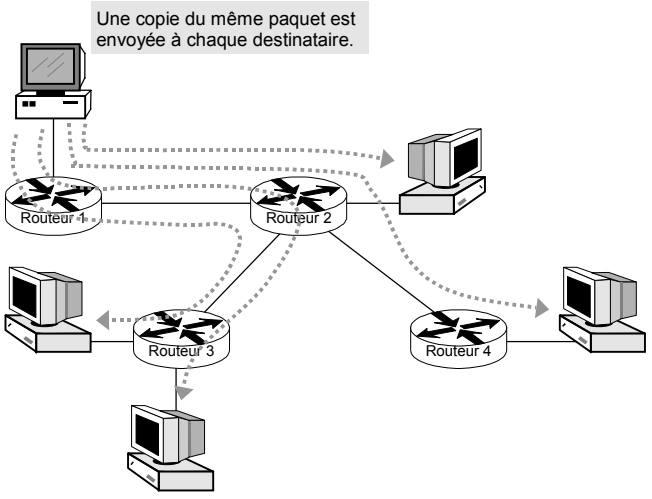
- à utiliser l'adressage multicast ;
- à gérer les groupes de diffusion ;
- à configurer les algorithmes de routage multicast DVMRP, MOSFP et PIM ;
- à choisir l'un de ces algorithmes en fonction de vos besoins.

La diffusion sur un réseau IP

Un participant à une audioconférence parle à tous les autres participants : sa voix est numérisée, puis découpée en paquets IP qui sont ensuite envoyés sur le réseau.

Au premier abord, il est possible de transmettre ces paquets sur un réseau IP classique : une copie de ce paquet est alors transmise à chaque destinataire. Chacun d'eux est, en effet, identifié par une adresse IP unique qui est insérée dans le champ destination du paquet. Les routeurs se servent de cette adresse pour acheminer le paquet jusqu'au destinataire.

Figure 13-1.
Diffusion des paquets unicast.



Cet exemple montre que ce type de fonctionnement n'est pas adapté à une diffusion : le réseau est inondé par des paquets dupliqués dès la source d'émission. Les adresses utilisées (classes A, B ou C) sont, en effet, de type **unicast**, car à une adresse est associé une machine cible. Par extension, les paquets sont dits unicast.

L'adressage IP propose une autre classe d'adresses, la classes D. Ces adresses sont dites **multicast**, car elles désignent un groupe de machines. Il ne s'agit pas d'une adresse de broadcast, car seules les machines qui sont configurées pour accepter une adresse multicast prendront en compte le paquet.

La plage réservée pour la classe D s'étend de 224.0.0.0 à 239.255.255.255. L'adresse 224.0.0.0 n'est attribuée à aucun groupe ; l'adresse 224.0.0.1 permet d'adresser toutes les machines sur un réseau (le réseau local sur lequel est émis le paquet). L'adresse 224.0.0.2 permet d'adresser, plus spécifiquement, tous les routeurs sur un réseau.

Des adresses de groupes permanents sont attribuées officiellement par l'IANA (*Internet Assigned Number Authority* — www.iana.org — RFC 1700).

Groupe concerné	Exemple d'adresse attribuée
Toutes les machines sur le réseau local	224.0.0.1
Tous les routeurs sur le réseau local	224.0.0.2
Tous les routeurs DVMRP	224.0.0.4
Tous les routeurs OSPF	224.0.0.5
Tous les routeurs OSPF désignés	224.0.0.6
Tous les routeurs RIP	224.0.0.9
Tous les routeurs PIM	224.0.0.13
Messages RSVP encapsulés dans UDP	224.0.0.14
NTP (*Network Time Protocol*)	224.0.1.1
Artificial Horizons — Aviator	224.0.1.5
Music-Service	224.0.1.16
IETF-2-Video	224.0.1.15
Microsoft-ds	224.0.1.24

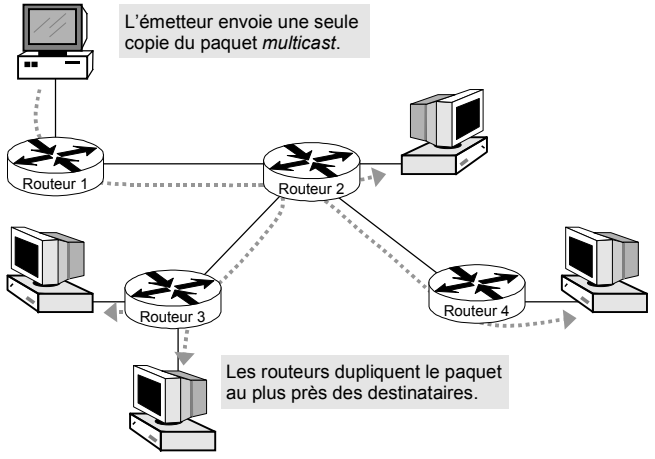


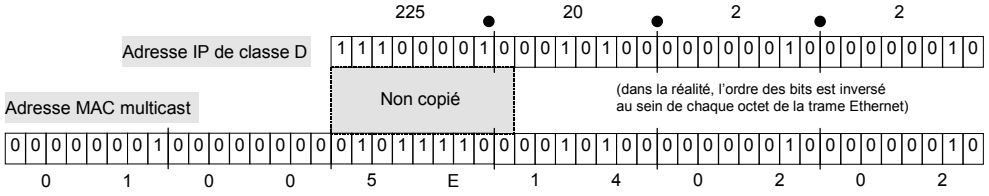
Figure 13-2.
Diffusion d'un paquet multicast.

Sans les mécanismes du multicast, le serveur devrait, tout d'abord, déterminer les destinataires (leur adresse IP ou leur nom), puis envoyer autant d'exemplaires du paquet qu'il y a de destinataires.

L'adresse IP source est toujours celle de la station qui envoie le paquet (une adresse unicast). Aucun paquet n'est émis avec une adresse source multicast. Une adresse de classe D identifie toujours un groupe de destinataires.

Sur les réseaux qui prennent en charge ce type d'adressage, le multicast IP utilise les fonctions de multicast du niveau 2, c'est-à-dire des trames multicast. Sur un réseau Ethernet, les paquets multicast IP sont envoyés dans des trames multicast dont l'adresse MAC de destination commence par " 01-00-5E ". Les 23 derniers bits de cette adresse correspondent aux 23 derniers bits de l'adresse IP.

Figure 13-3.
Correspondance entre les adresses multicast IP et Ethernet.



Un PC envoie donc tous ses paquets multicast IP dans une trame multicast Ethernet. Le mécanisme de routage par défaut (voir chapitre 11) ne s'applique, en effet, qu'aux paquets unicast.

Sur les réseaux ne disposant pas de la fonction multicast de niveau 2 (X.25, Frame Relay, ATM, par exemple), les paquets multicast sont transportés dans les trames unicast de niveau 2.

La gestion des groupes de diffusion

Un groupe de diffusion (groupe *multicast*) est dynamique : ses membres peuvent adhérer au groupe ou le quitter à tout moment, être dispersés à travers le monde, adhérer à plusieurs groupes en même temps. Aucune restriction quant au nombre de participants n'est également appliquée. Le groupe peut être permanent ou non. Un participant peut être actif ou non (la machine est éteinte).

La première tâche pour un participant (une machine connectée sur le réseau) est donc de se faire connaître. Pour cela, il dispose du protocole **IGMP** (*Internet Group Membership Protocol*) défini par la RFC 1112, datée de 1989, et mis à jour en 1997 par la RFC 2236 (IGMP v2).

En principe, toutes les piles TCP/IP, et en particulier celle de Windows, supportent IGMP. Aucune configuration spécifique n'est nécessaire, car la gestion des groupes n'est pas réalisée manuellement mais directement par les applications *via* des API (*Application Programming Interface*).

Par exemple, l'interface Winsock offre les primitives permettant d'entrer et de sortir d'un groupe :

- *JoinHostGroup* (adresse IP du groupe, numéro de l'interface réseau) ;
- *LeaveHostGroup* (adresse IP du groupe, numéro de l'interface réseau).

Ces fonctions permettent à la pile TCP/IP d'accepter d'une part les paquets dont l'adresse IP de destination lui correspond et, d'autre part, les paquets dont l'adresse IP de destination est celle du ou des groupes multicast auxquels l'interface réseau est non jointe . La pile TCP/IP maintient ainsi une liste d'appartenance pour chaque interface réseau de la machine.

Ainsi, plusieurs logiciels utilisent déjà le multicast à votre insu :

- les serveurs WINS de Windows NT, qui se placent d'office dans le groupe 224.0.1.24 qui est utilisé pour dialoguer avec des partenaires de réplication ;
- le logiciel de visioconférence Netmeeting ;
- le logiciel de diffusion audio et vidéo RealG2 Player.

La plupart des routeurs prennent également en charge ce protocole. La configuration d'un routeur Cisco consiste simplement à activer la fonction multicast d'IP :

```
int e 0
ip multicast-routing
```

Si le routeur dispose de plusieurs interfaces sur le même réseau local, une seule doit être configurée avec IGMP.

On peut indiquer au routeur de devenir membre d'un groupe. Cela permet aux exploitants de savoir si un groupe est joignable en utilisant la commande *ping*. Si personne n'est actif sur ce groupe, le routeur pourra au moins répondre au *ping* :

```
ip igmp join-group 224.10.1.1
```

Considérons l'exemple suivant : chacun des deux routeurs est élu Demandeur pour un réseau en fonction de son adresse IP.

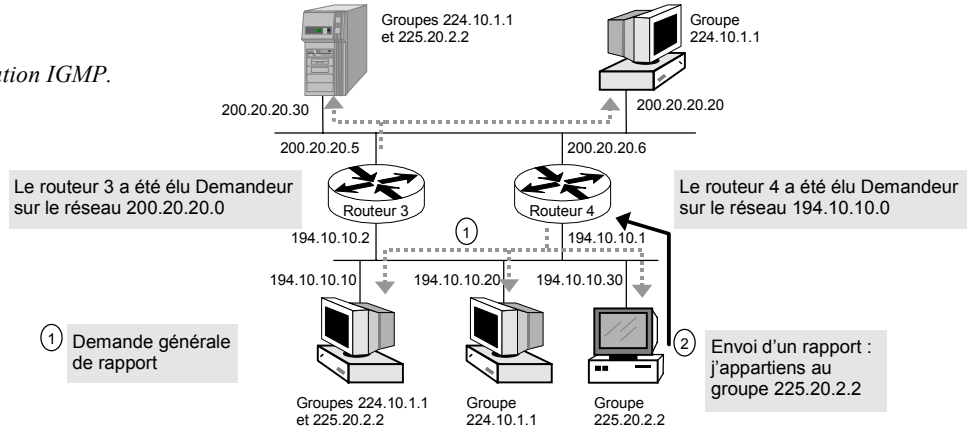


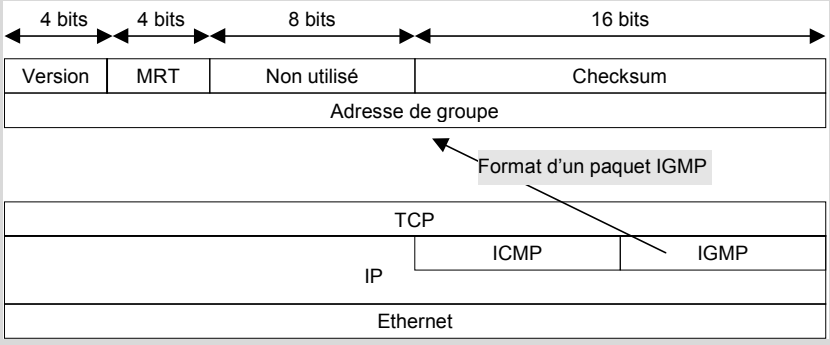
Figure 13-4.
Exemple de configuration IGMP.

LE POINT SUR IGMP (RFC 1112 ET 2236)

IGMP (*Internet Group Membership Protocol*) est un protocole qui fonctionne conjointement avec IP, au même titre qu'ICMP. Il permet aux membres d'un groupe de signaler leur présence au routeur le plus proche, celui connecté au réseau local. Si plusieurs routeurs sont connectés à un même réseau local, celui qui a la plus petite adresse IP est élu Demandeur.

Le routeur Demandeur émet périodiquement une **demande générale de rapport** (adresse de destination 224.0.0.1). Les membres de tous les groupes actifs sur ce réseau local lui répondent en envoyant un r**apport** pour chaque groupe auquel ils appartiennent.

Le routeur maintient à jour une liste des groupes dont au moins un membre est actif. Les routeurs non demandeurs n'émettent pas de demande de rapport, mais lisent les rapports et mettent à jour leur table.
Il existe trois types de paquets IGMP : demande de rapport, sortie d'un groupe (demandée par un membre) et rapport d'activité. Un quatrième type, le rapport IGMP version 1, est supporté à des fins de compatibilité.



Le champ MRT (*Max Response Time*) est utilisé dans les paquets de demande de rapport pour indiquer, en dixièmes de secondes, le délai maximal autorisé pour envoyer un rapport d'activité. Au-delà de ce délai, le destinataire est considéré comme n'étant pas actif dans le groupe.

Un membre peut également demander à sortir du groupe (message à destination de 224.0.0.2). Le routeur Demandeur émet alors une **demande spécifique de rapport** (adresse de destination identique à celle du groupe) pour s'assurer qu'un membre au moins est encore actif.

Les routeurs sont à l'écoute de tout message multicast, et prennent donc en compte tous les rapports. La commande suivante montre le résultat obtenu sur un routeur Cisco :

```
Routeur3# show ip igmp interface
Ethernet0 is up, line protocol is up
```

```
  Internet address is 194.10.10.2, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  IGMP query interval is 120 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 194.10.10.1
  Multicast groups joined: 224.10.1.1 225.20.2.2
Ethernet1 is up, line protocol is up
  Internet address is 200.20.20.5, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  IGMP query interval is 120 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 200.20.20.5
  Multicast groups joined: 224.10.1.1 225.20.2.2
```

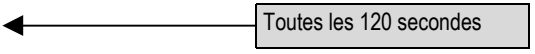
Le routeur 3 n'est pas Demandeur pour le réseau 194.10.10.0 ; il n'envoie donc pas de requête. En revanche, il prend en compte tous les rapports qu'il voit passer :

```
Routeur4# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface       Uptime    Expires   Last Reporter
224.10.1.1       Ethernet0       17:15:15  0:02:05   194.10.10.20
224.10.1.2       Ethernet1        1:01:01  0:01:05   220.20.20.30
224.10.1.1       Ethernet1       17:15:40  0:01:40   220.20.10.30
225.20.2.2       Ethernet0        1:00:45  0:01:50   194.10.10.10
```

De même, le routeur 4 n'est pas Demandeur pour le réseau 220.20.20.0 ; il n'envoie donc pas de requête. En revanche, il prend également en compte tous les rapports qu'il voit passer.

La périodicité d'envoi des demandes générales de rapports peut être paramétrée comme suit :

```
ip igmp query-interval 120
```



La version 3 d'IGMP, en cours d'étude, permettra aux machines d'indiquer au routeur l'adresse IP source pour laquelle elle accepte de recevoir des paquets multicast ; ainsi, la diffusion du paquet prendra en compte l'adresse de l'émetteur en plus du groupe destination.

Le routage des flux multicast

Le protocole IGMP permet aux routeurs de détecter les groupes situés sur leurs réseaux locaux (les réseaux auxquels une interface est connectée).

Mais les routeurs ne savent pas où sont situés les autres membres du groupe, puisque IGMP n'a qu'une portée locale. Pour cela, il faut utiliser des protocoles de routage spécifiques au multicast. Trois standards sont disponibles :

- DVMRP (*Distance Vector Multicast Routing Protocol*), analogue au protocole RIP adapté au multicast ;
- MOSPF (*Multicast Open Shortest Path First*), une extension d'OSPF ;
- PIM (*Protocol Independent Multicast*), spécialement dédié au multicast.

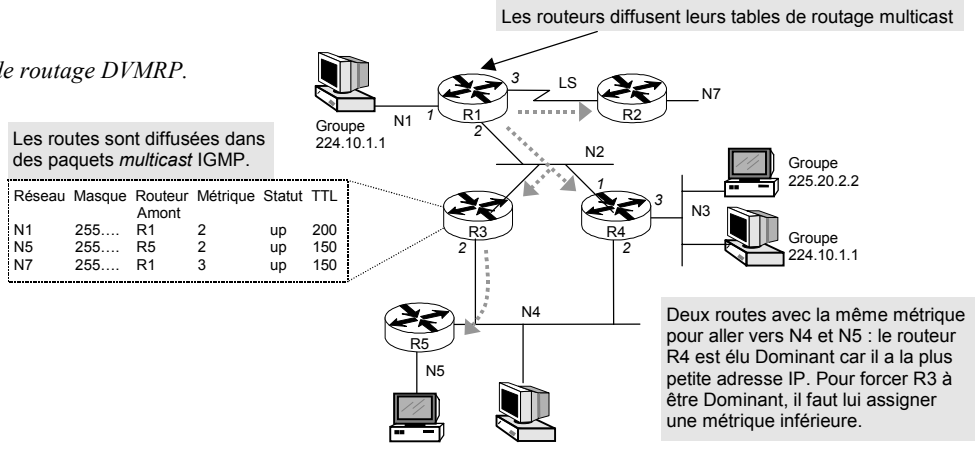
Le choix de l'un de ces protocoles dépend de nombreux paramètres. Les paragraphes suivants décrivent donc leurs principes de fonctionnement, afin de mieux cerner leurs conséquences sur l'architecture de notre réseau.

Le routage à l'aide de DVMRP

Le premier protocole de routage multicast a été DVMRP (*Distance Vector Multicast Routing Protocol*). Comme son nom l'indique, il repose sur un algorithme de calcul du plus court chemin, basé sur le plus petit nombre de routeurs à traverser pour atteindre une destination (nombre de sauts, appelé métrique).

Le principe est en cela identique à RIP (*Routing Information Protocol*) : les routeurs s'échangent l'intégralité de leurs tables de routage. DVMRP doit donc être utilisé en supplément d'un protocole de routage unicast (RIP, OSPF, etc.).

Figure 13-5.
Diffusion des tables de routage DVMRP.



La commande suivante permet d'activer DVMRP sur notre routeur R1, qui est un Netbuilder de marque 3com. Elle doit être utilisée pour chaque interface gérant le trafic *multicast*. La commande MIP permet d'activer le protocole IGMP :

```
setdefault -MIP control = enable
setdefault !1 -DVMRP control = enable
setdefault !2 -DVMRP control = enable
setdefault !3 -DVMRP control = enable
```

Lorsque plusieurs routeurs coexistent sur le même réseau local, seul l'un d'eux a la charge de diffuser les paquets multicast, afin d'éviter la duplication des paquets. Comme pour RIP, la route choisie repose sur le plus petit nombre de sauts (la métrique). En cas d'égalité de métrique, le routeur dominant élu est celui qui possède la plus petite adresse IP.

Pour forcer R3 à être le routeur dominant sur le réseau N4, il faut lui attribuer une métrique inférieure à celle de R4 :

```
#Routeur R3
setdefault !2 -DVMRP metric = 5
#Routeur R4
setdefault !2 -DVMRP metric = 10
```

La commande suivante permet de visualiser la table de routage du routeur R4 :

```
show -dvmrp routetable long

SourceSubnet SubnetMask    FromGateway Metric Status TTL InPort OutPorts
200.10.10.0  255.255.255.0 200.20.20.1 2      Up     200 1      2 3*
200.30.30.0  255.255.255.0             1      Up     150 3      1 2
...
```

La colonne " FromGateway " indique le routeur le plus proche qui mène à la source (un champ vide indique que le réseau est directement connecté au routeur R4).

La colonne " InPort " (*Incoming Port*) indique l'interface par laquelle arrivent les paquets multicast émis par la source précisée dans la colonne " SourceSubnet ".

La colonne " OutPorts " (*Outgoing Ports*) donne la liste des ports vers lesquels seront diffusés par défaut les paquets multicast issus de la source indiquée dans la colonne " SourceSubnet ". Un astérisque indique que le port conduit à une feuille de l'arbre, c'est-à-dire qu'aucun routeur ne se trouve en dessous.

En plus de la table de routage, le routeur gère une table de diffusion construite lorsque les premiers paquets *multicast* transitent par le routeur. Elle permet d'enregistrer les groupes identifiés pour chaque réseau source.

La commande suivante affiche la table de diffusion pour le routeur R4 :

```
show -dvmrp forwardtable

SourceSubnet MulticastGroup TTL InPort OutPorts
200.10.10.0  224.10.1.1     200 1      1 2p
200.30.30.0  224.10.1.1     150 3      2p 3
             225.20.2.2     200 3      2p 3
...
```

La colonne " MulticastGroup " indique la liste des groupes de diffusion des paquets en provenance de la source indiquée dans la colonne " SourceSubnet ". Les autres colonnes ont la même signification que celles de la table de routage. L'indicateur " p " (*prune*) indique qu'un message de non-appartenance a été reçu ; par conséquent, aucun paquet multicast ne sera envoyé vers cette interface. Dans notre cas, cela indique que R3 est dominant.

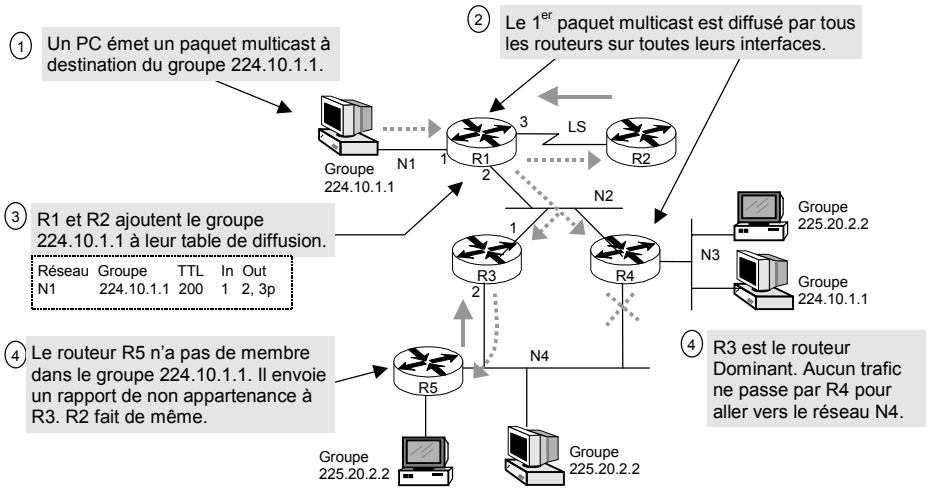


Figure 13-6. *Routage d'un paquet multicast.*

Dans notre réseau, le routeur R1 a diffusé le paquet multicast vers les interfaces 2 et 3. Il met alors à jour sa table de diffusion. L'interface 3 a par la suite été marquée *p* (*pruned*) car le routeur R2 lui a renvoyé un rapport de non-appartenance. En effet, ce dernier n'a détecté (*via* IGMP) aucun membre actif pour le groupe 224.10.1.1.

De même, le routeur R5 renvoie un message de non-appartenance au routeur R3, qui ne lui transmettra alors plus aucun paquet pour le groupe 224.10.1.1. Le routeur R3 fait ensuite de même vis-à-vis de R1 et R4.

LE POINT SUR DVMRP (RFC 1075)

DVMRP (*Distance Vector Multicast Routing Protocol*) utilise son propre protocole de routage de paquets multicast, qui est analogue à celui de RIP : les routeurs s'échangent l'intégralité de leurs tables de routage et calculent les routes sur la base d'une **métrique** (nombre de sauts en termes de routeurs).

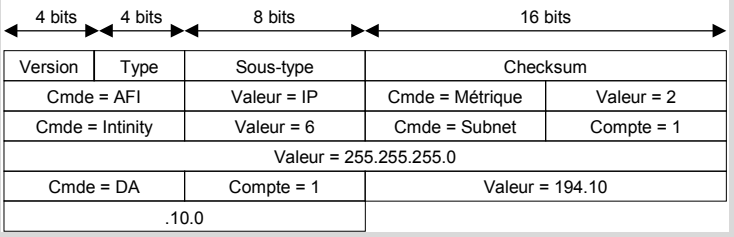
Il existe plusieurs implémentations de DVMRP qui diffèrent par l'algorithme utilisé pour construire la table de diffusion : **TRPB** (*Truncated Reverse Path Broadcasting)* ou **RPM** (*Reverse Path Multicasting*), ce dernier étant le plus répandu car plus performant. Les routeurs 3com et le démon Unix *mrouted* (à partir de la version 3.8) utilisent RPM.

Le principe du TRPB est le suivant : un routeur recevant un paquet multicast le transmet sur toutes les autres interfaces. Les routeurs situés en aval reçoivent donc le paquet. S'ils ne disposent d'aucun membre déclaré ni d'aucun autre routeur en aval, ils renvoient un rapport de non-appartenance au routeur situé en amont. Ce dernier ne leur transmettra alors plus de paquets multicast.

Si un nouveau membre s'enregistre sur un des routeurs situés en aval, celui-ci enverra au routeur situé en amont un message d'annulation, pour recevoir à nouveau les paquets *multicast* destinés au groupe en question.

Le principe du RPM reprend celui du TRPB, mais pousse plus loin la remontée d'information : un routeur qui ne dispose pas de membre ni de routeur en aval ayant de membre envoie un rapport de non-appartenance aux routeurs situés en amont, de sorte que lui-même ne reçoive pas de paquets multicast. Le rapport peut ainsi remonter jusqu'à la source si nécessaire.

Un paquet DVMRP est composé d'un en-tête IGMP auquel sont jointes des données de longueur variable (512 octets au maximum) formatées sur le mode : " Commande, Valeur " ou " Commande, nombre de valeurs, valeur 1, valeur 2, etc. ". L'exemple suivant montre un paquet d'annonce de la route 194.10.10.0.



Le champ Cmde contient le code d'une commande qui détermine la taille et la signification du champ Valeur. Plusieurs commandes se suivent dans un paquet. Le champ Sous-type détermine le type de message : requête, réponse, rapport de non-appartenance ou annulation d'un rapport de non-appartenance.

La commande AFI est toujours présente : elle indique simplement que la famille d'adresses est IP (seul supporté). La commande DA indique une adresse destination.

L'inconvénient de DVMRP est que les paquets multicast doivent périodiquement être envoyés aux routeurs situés en aval pour tenir compte d'éventuels changements de topologie ou d'appartenance à un groupe (pour un groupe donné, les messages d'annulation ne remontent que si un multicast a été précédemment reçu et un message de non-appartenance émis). Il en résulte une nouvelle cascade de rapports de non-appartenance ou d'annulation remontant vers les routeurs situés en amont.

Sur un réseau, tous les routeurs ne sont pas DVMRP. La mise en place du routage multicast est, en effet, progressive. En outre, le fait de ne pas installer de routeurs DVMRP partout permet de définir des domaines dans le but de circonscrire la diffusion des paquets multicast.

Pour assurer néanmoins la diffusion des paquets multicast, il est possible de créer un tunnel entre deux routeurs DVMRP séparés par des routeurs qui ne savent pas router les paquets multicast.

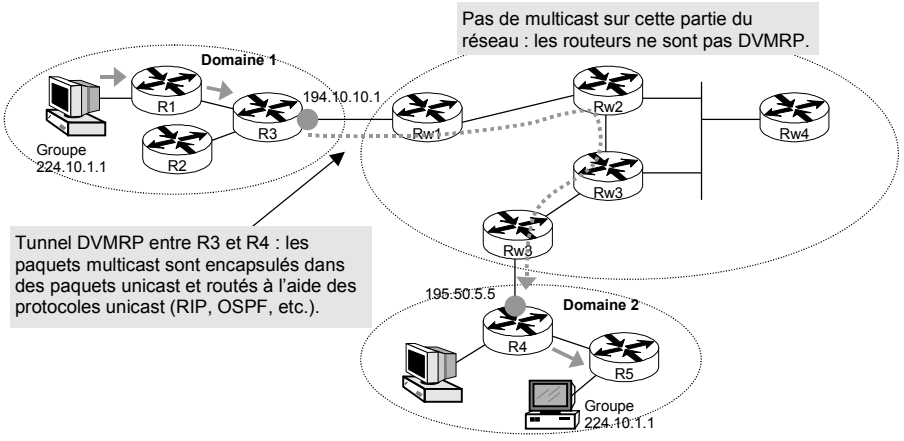


Figure 13-7. *Principe du tunneling DVMRP.*

Sur nos routeurs 3com, la création du tunnel IP est réalisée simplement en indiquant les adresses des deux routeurs :

```
#Sur le routeur R3
setdefault !1 -DVMRP mon_tunnel = 194.10.10.1 195.50.5.5

#Sur le routeur R4
setdefault !2 -DVMRP mon_tunnel = 195.50.5.5 194.10.10.1

#Activation de DVMRP sur le tunnel
setdefault mon_tunnel -DVMRP control = enable
```

Afin d'atténuer les effets d'un trafic multicast important sur un réseau non dimensionné pour cela, il est possible d'en limiter le débit à 64 Kbit/s, par exemple :

```
# Sur les routeurs R3 et R4
setdefault mon_tunnel -dvmrp ratelimit = 64
```

De même, il est possible d'augmenter la périodicité d'échange des tables de routage entre les deux routeurs (60 secondes par défaut) :

```
setdefault -dvmrp updatetime = 120
```

Enfin, la durée de validité des entrées dans la table de diffusion peut également être allongée (dans notre cas, 3 600 secondes) :

```
setdefault -dvmrp cachetime = 3600
```

Le routage à l'aide de MOSPF

Le protocole MOSPF (*Multicast Open Shortest Path First*) est une extension d'OSPF permettant de router les paquets IP *multicast*. La détection des membres actifs d'un groupe est, comme toujours, assurée par IGMP, mais MOSPF permet aux routeurs de diffuser les groupes auxquels ils appartiennent (c'est-à-dire pour lesquels au moins un membre est actif).

Reprenons l'exemple de notre réseau : chaque routeur est configuré avec IGMP et MOSPF. Localement, chaque routeur établit une liste de tous les groupes pour lesquels il existe un membre actif sur son (ou ses) interface LAN.

En même temps, les routeurs s'échangent des messages d'annonce d'état des liens, suivant en cela le fonctionnement classique d'OSPF (voir chapitre 11). Cela leur permet de connaître la topologie du réseau.

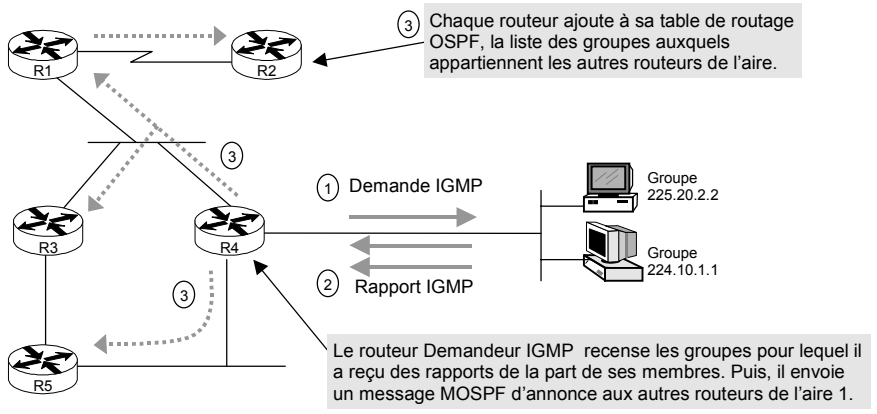


Figure 13-8. *Diffusion d'un paquet multicast par MOSPF.*

Dès le premier enregistrement d'un membre de groupe *via* IGMP, les routeurs sont considérés par OSPF comme étant membres du groupe. Ces routeurs s'échangent alors des messages d'annonce d'appartenance à un groupe. Tous les routeurs savent désormais quel routeur appartient à quel groupe.

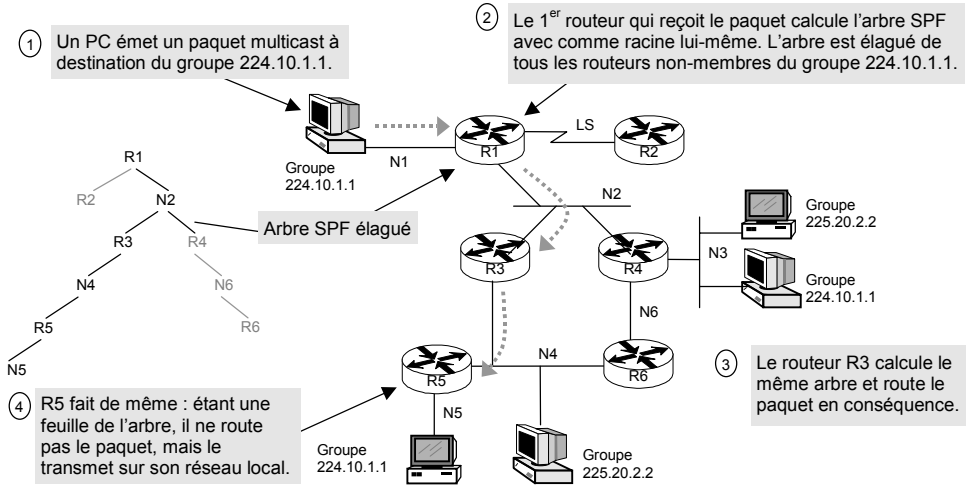
Sur nos routeurs 3com, l'activation de MOSPF est effectuée grâce à la commande suivante :

```
#Activation d'igmp
setdefault -mip control = enable

#Activation de mospf sur chaque interface
setdefault !1 -mospf control = enable
setdefault !2 -mospf control = enable
```

Le routage des paquets *multicast* au sein d'une aire est réalisé en fonction de la source (adresse IP *unicast* de la machine), de la destination (adresse IP *multicast* du groupe) et du TOS (*Type of Service*). Le routeur construit pour cela un arbre SPF (*Shortest Path First*) dont tous les routeurs non-membres du groupe indiqué dans le paquet ont été supprimés. Cet arbre est calculé à la demande lorsqu'un paquet *multicast* arrive sur le routeur.

Figure 13-9.
Calcul de l'arbre SPF élagué.



Dans cet exemple, il est à noter que le routeur Demandeur IGMP doit être un routeur MOSPF, seul capable d'envoyer des messages d'annonce d'appartenance à un groupe. Il faut donc affecter une priorité supérieure aux routeurs MOSPF pour qu'ils soient élus routeurs désignés (au sens OSPF).

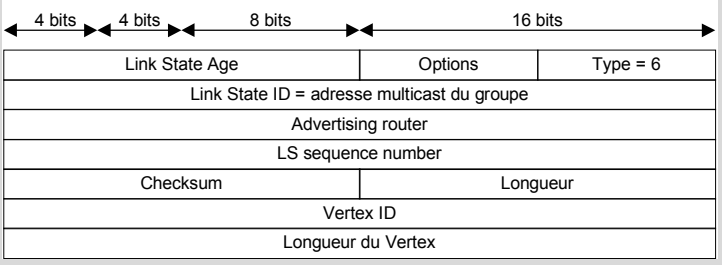
LE POINT SUR MOSPF (RFC 1584)

Au sein d'une aire (voir encadré " Le point sur OSPF "), les routeurs s'échangent des **messages d'annonce d'appartenance à un groupe**, permettant à chacun d'eux de disposer d'une visibilité complète de la topologie du réseau.

Chaque routeur calcule un **arbre SPF** pour chaque triplet adresse source unicast/adresse destination *multicast*/TOS (*Type of Service*). Ce calcul est effectué à la demande, c'est-à-dire lorsque le premier paquet multicast arrive. L'arbre ainsi calculé est conservé dans une mémoire cache, puis détruit au bout d'un certain temps lorsqu'aucun autre paquet de ce type n'a été reçu.

L'arbre est **élagué** : tous les routeurs qui ne sont pas membres du groupe indiqué dans le paquet sont supprimés. Les réseaux terminaux (*stub*) n'ont pas besoin d'être pris en compte : la diffusion locale au routeur est, en effet, assurée par IGMP.

Un chemin *multicast* est donc calculé en construisant un arbre élagué du plus court chemin dont la racine est l'émetteur du paquet (la RFC emploie l'expression : " *pruned shortest-path tree rooted at the packet's IP source* "). Pour la diffusion des appartenances à un groupe, un nouveau paquet d'annonce a été ajouté : *group-membership-LSA*.



Par ailleurs, les modifications suivantes ont été apportées à OSPF :

- Le champ " Option " des paquets Hello, Description de la base et Annonce d'état de lien contient un nouvel indicateur, le bit MC, qui indique si le routeur prend en charge l'extension multicast d'OSPF (MOSPF).
- Le champ " Rtype " des paquets d'annonce d'état de liens contient un nouvel indicateur, le bit W, qui indique si le routeur accepte ou non les multicast provenant de n'importe quelle source.

Un routeur calcule autant d'arbres qu'il y a de participants à une conférence, et calcule autant de variantes de cet arbre qu'il y a de groupes destinataires. La prise en compte du TOS augmente encore le nombre de combinaisons.

Le nombre d'arbres peut donc être très important. C'est pour cela qu'ils sont calculés à la demande et que le résultat est conservé en mémoire cache. Cela implique également que, plus le nombre de machines et de groupes est élevé, plus la CPU des routeurs est sollicitée pour calculer les arbres.

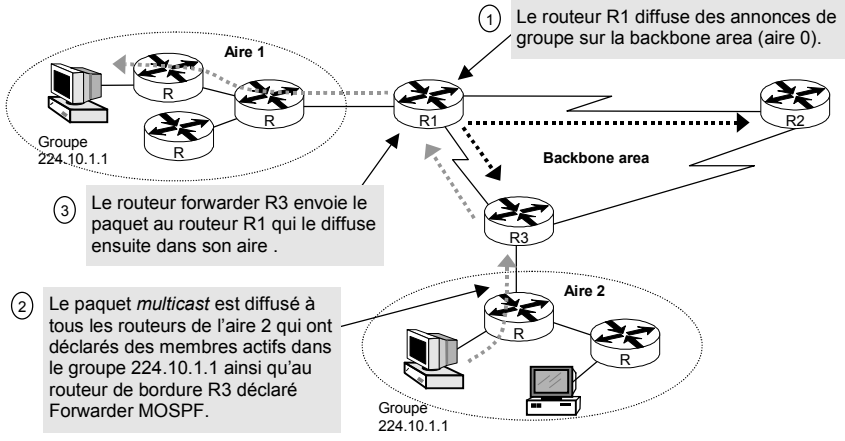
Le résultat du calcul d'un arbre est conservé aussi longtemps qu'un trafic entre le couple d'adresses IP *unicast* source/*multicast* destination existe, et jusqu'à ce qu'un changement de topologie intervienne. La taille mémoire requise est donc plus importante par rapport à un routeur OSPF classique (14 à 20 octets par triplet adresses source/groupe/TOS).

Le dimensionnement mémoire/CPU dépend du constructeur du routeur (architecture et puissance), de l'importance du réseau (nombre de machines *multicast* et nombre de groupes) ainsi que des performances visées (utilisation intensive ou non des téléconférences, utilisation du réseau à d'autres fins que le multimédia, etc.).

Il est également recommandé de limiter le nombre de TOS, voire de ne pas activer cette fonctionnalité, afin de limiter le nombre de combinaisons d'arbres SPF.

La diffusion des paquets multicast entre aires et systèmes autonomes utilise le principe appelé Multicast Forwader : les routeurs de bordure et les routeurs inter-AS déclarés comme tels ne sont jamais supprimés des arbres SPF. En conséquence, tous les paquets multicast leur seront envoyés. De leur côté, ces routeurs calculent un arbre SPF pour chaque aire (ou AS) à laquelle ils sont rattachés.

Figure 13-10.
Routage des paquets multicast entre aires.



Les annonces d'appartenance à un groupe sont diffusées au sein de l'aire 0 (*backbone area*) par tous les routeurs de bordure. Tous les routeurs participant à la backbone area connaissent donc tous les groupes présents au sein du système autonome. Les informations provenant de la backbone area ne sont cependant pas transmises aux autres aires. Seuls les Forwarders conservent ces informations.

L'architecture et le dimensionnement des réseaux constituant la *backbone area* sont donc très importants. Il faut tenir compte du nombre de postes de travail et de leur répartition entre les aires. L'aire backbone concentre, en effet, la somme des flux circulant dans chacune des aires où les groupes sont actifs. Si cela est possible, il est donc conseillé de limiter le nombre d'aires ou bien de répartir des groupes entre plusieurs aires.

La configuration pour déclarer Forwarder un routeur de bordure 3com est la suivante :

```
SETDefault -MOSPF MABR = Enable
```

Le mot clé MABR signifie *Multicast Area Border Router*.

Le principe est identique pour le routage entre systèmes autonomes : un routeur frontière est désigné Forwarder de système autonome, et reçoit tous les paquets *multicast* circulant au sein du système autonome (et non plus seulement au sein d'une aire). La différence est importante, car la concentration de trafic est encore plus prononcée et les routeurs de ce type sont encore plus sollicités que les autres. Il est donc conseillé de dédier un routeur frontière de système autonome à cette seule tâche et de le relier à un réseau à haut débit.

Comme il a été mentionné au chapitre 11, OSPF ne permet pas de router les paquets entre AS. Il faut lui adjoindre un protocole de routage extérieur, tel que BGP4. Dans le cadre d'un réseau multicast, c'est DVMRP qui se charge de cette tâche au niveau des routeurs frontières.

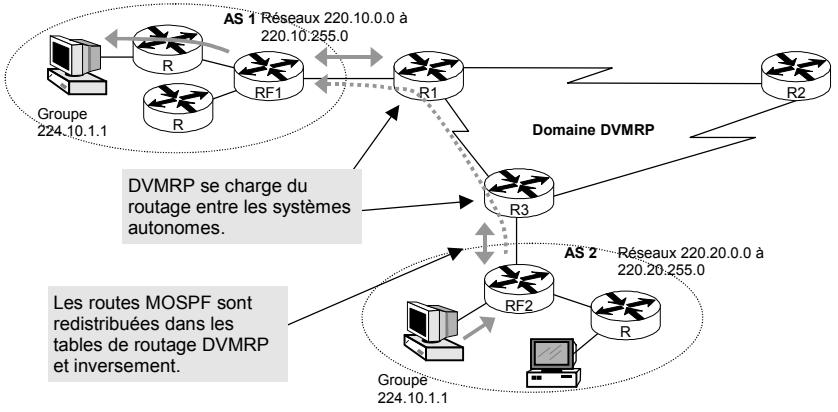


Figure 13-11.
Routage DVMRP entre systèmes autonomes.

La configuration suivante doit donc être effectuée sur nos routeurs frontières RF1 et RF3 (ici, l'exemple concerne RF1) :

```
#Active la diffusion des routes MOSPF dans DVMRP
add -dvmrp mospf 220.10.0.0/16 aggregate 1
#Active le routage d'ospf vers dvmrp
setdefault -dvmrp policycontrol = mospf

#Active la diffusion des routes DVMRP dans ospf
add -mospf dvmrp 220.20.0.0/16 aggregate 5
#Active le routage de dvmrp vers ospf
setdefault -mospf policycontrol = dvmrp
```

L'option " Aggregate " permet de diffuser une seule route pour les routes comprises entre 220.10.0.0 et 220.10.255.0 au lieu de diffuser 256 routes.

Le système permet de mêler des routeurs OSPF et MOSPF. Cependant, aucune machine située dernière un routeur OSPF ne recevra les messages multicast. Il doit donc y avoir continuité des routeurs MOSPF tout au long des routes menant vers les machines multicast. À l'inverse de DVMRP, le tunneling n'est, en effet, pas supporté.

De plus, il faut toujours que le routeur désigné sur un réseau local soit un routeur MOSPF, sinon les requêtes IGMP n'alimenteront pas le protocole de routage multicast. Pour cela, il faut assigner une priorité supérieure aux routeurs OSPF également configurés en MOSPF.

Le routage à l'aide de PIM

Comme cela a été montré aux paragraphes précédents, le protocole MOSPF — et encore moins DVMRP — n'est pas adapté pour de grands réseaux, et notamment l'Internet (plusieurs dizaines de milliers d'aires et de systèmes autonomes).

Pour résoudre ce problème, l'IETF a défini le protocole PIM (*Protocol Independent Multicast*) qui, comme son nom le laisse penser, est indépendant du protocole de routage *unicast* utilisé. PIM fonctionne, en effet, avec RIP, OSPF, BGP, et même DVMRP.

PIM utilise deux modes de fonctionnement :

- *dense* (densité élevée), qui est adapté à des réseaux à haut débit et à des situations où les membres de groupes sont géographiquement proches ;
- *sparse* (clairsemé), qui correspond aux cas de figures où les réseaux ont de plus faibles débits et où les membres de groupes sont très dispersés.

Un routeur PIM bascule d'un mode à l'autre indépendamment de chaque groupe.

Le mode dense (PIM-DM) fonctionne de manière identique à DVMRP (algorithme *reverse path flooding*) sans toutefois utiliser un protocole de routage multicast dédié ; il utilise les protocoles de routage unicast en place (RIP, OSPF, etc.), d'ou le nom de " *Protocol Independant* ". PIM-DM ne fait pas encore l'objet d'une RFC.

Le mode *sparse* (PIM-SM) nécessite de convenir d'un routeur qui tienne lieu de point de rendez-vous pour chaque groupe. Un routeur peut être le point de rendez-vous pour plusieurs groupes. Il peut exister plusieurs points de rendez-vous pour un groupe, mais un seul doit être actif à un moment donné.

Principe de PIM-SM

Pour un couple réseau source/groupe multicast, un routeur PIM-SM bascule entre deux algorithmes de routage : un dont le chemin passe par le point de rendez-vous, et un second qui bénéficie d'un chemin direct entre la source et la destination. Pour le premier, le calcul de la route s'établit à partir d'un arbre partagé dont la racine est le point de rendez-vous (*Rendez-vous Point shared tree*). Pour le second, ce calcul se fonde sur un arbre du plus court chemin dont la racine est la source d'émission du paquet multicast (*source shortest path tree*).

Si plusieurs routeurs sont connectés au même réseau local, celui dont l'adresse IP est la plus élevée sera élu routeur désigné et aura à charge d'envoyer et de recevoir les messages Join/Prune. Pour découvrir ses voisins, un routeur émet périodiquement un message Hello dont la périodicité par défaut est de 30 secondes :

```
ip pim query-interval 30
```

Tous les routeurs désignés dont les membres actifs appartiennent à un même groupe s'enregistrent auprès du même routeur, appelé point de rendez-vous (RP). Les routeurs intermédiaires enregistrent également cette information et font de même auprès du RP. Ce dernier peut donc calculer un arbre de routage pour un couple adresse réseau source/adresse multicast de groupe. En définitive, le RP connaît tous les réseaux sources susceptibles d'émettre et de recevoir des paquets multicast au sein d'un groupe donné.

Pour terminer cette introduction, plusieurs routeurs peuvent être candidats à l'élection du point de rendez-vous. L'un d'eux est élu routeur bootstrap ; il est chargé de désigner le RP actif pour chaque groupe. Il en résulte de nouveaux messages d'annonce entre les RP.

Principe du calcul des routes

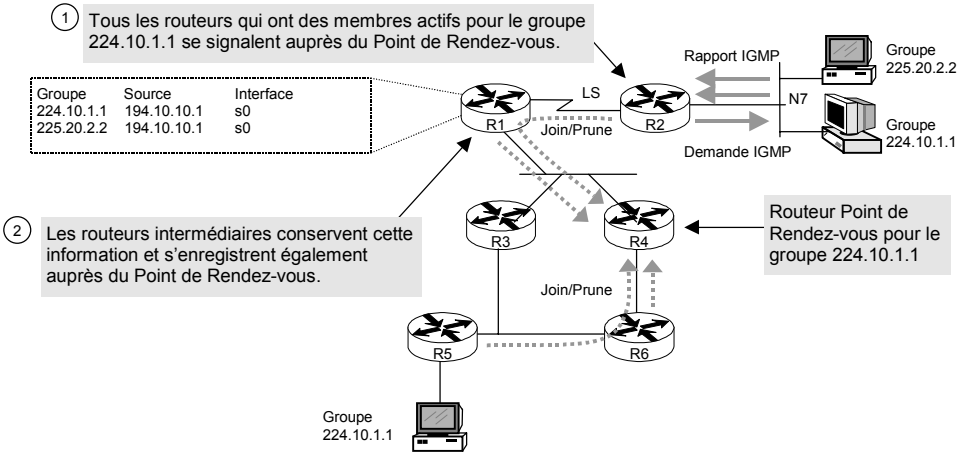
Un routeur PIM-SM ayant enregistré (*via* IGMP) des membres d'un ou plusieurs groupes envoie périodiquement un message Join/Prune (joindre/élaguer) au point de rendez-vous RP. Chaque routeur chargé de transporter ce message se trouvant sur le chemin enregistre les mêmes informations : le groupe, la source (l'adresse du réseau sur lequel ont été identifiés les membres du groupe) et l'interface d'entrée du message Join/Prune.

Un message Join/Prune contient, pour chaque adresse de groupe (multicast), la liste des adresses sources incluses dans l'arbre de routage (*joined*, qui ont rejoint l'arbre) et de celles qui ne le sont pas (*pruned*, élaguées de l'arbre).

Un routeur émet un message Join/Prune vers un routeur situé en amont (en direction de la racine de l'arbre). Il indique par là qu'il fait partie de l'arbre de routage pour les paquets *multicast* du groupe G émis par la source S.

En retour, un routeur diffuse les paquets multicast uniquement vers les interfaces à partir desquelles des messages *Join/Prune* ont été reçus (et qui correspondent à un couple adresse source unicast/groupe multicast).

Figure 13-12.
Calcul des routes par le routeur point de rendez-vous.



Les commandes suivantes permettent d'activer PIM sur nos routeurs Cisco :

```
ip multicast-routing
interface ethernet 0
ip pim sparse-dense-mode
```

Aucune autre configuration n'est requise pour les routeurs intermédiaires et le routeur point de rendez-vous.

En revanche, tous les routeurs susceptibles d'enregistrer des membres de groupe doivent pointer vers le routeur point de rendez-vous :

```
access-list 1 permit 224.10.1.1
access-list 1 permit 224.20.2.2
ip pim rp-address 220.20.20.6 1
```

L'access-list 1 précise la liste des groupes pour lesquels le routeur 220.20.20.6 sera élu point de rendez-vous.

Principe du routage

Le premier paquet multicast émis par un PC est envoyé dans un paquet multicast IP qui est pris en charge par le routeur PIM-SM désigné. Celui-ci encapsule ce paquet dans un paquet unicast à destination du RP. Le RP décapsule ce paquet et l'envoie tel quel (donc sous forme multicast) aux membres du groupe (les routeurs qui se sont déclarés).

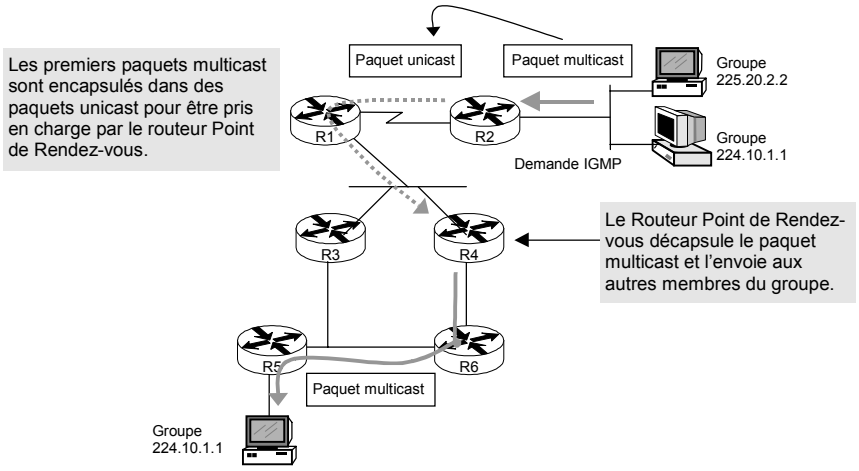


Figure 13-13. *Principe du routage PIM-SM.*

Tous les messages passent donc par le RP, ce qui n'est pas forcément une route optimale.

Si le trafic multicast persiste, un routeur (la source, la destination ou le RP) peut alors décider que le flux emprunte un chemin direct entre la source et la destination. Les routeurs concernés basculent alors d'un arbre de routage dont la racine est le RP vers un arbre du plus court chemin dont la racine est la source.

Dans notre réseau, le routeur R1 crée la table de routage suivante :

```
Router4# show ip pim interface
Address       Interface    Mode    Neighbor  Query   DR
                                   Count     Interval
220.20.20.6   Ethernet0    sparse   2         30     220.20.20.6
197.10.10.0   serial0      sparse   1         10     0.0.0.0
```

La colonne *Address* indique l'adresse du routeur vers lequel envoyer les paquets à router *via* l'interface spécifiée dans la colonne *Interface*.

La colonne *Neighbor count* indique le nombre de voisins découverts sur cette interface.

La colonne *DR* indique l'adresse du routeur désigné.

Routage sur les liaisons WAN

Sur Ethernet, le paquet IP multicast est envoyé dans une trame Ethernet multicast. Mais, sur les réseaux qui n'offrent par cette fonction (X.25, Frame Relay, ATM, etc.), seules des trames unicast peuvent être envoyées.

LE POINT SUR PIM-SM (RFC 2362)

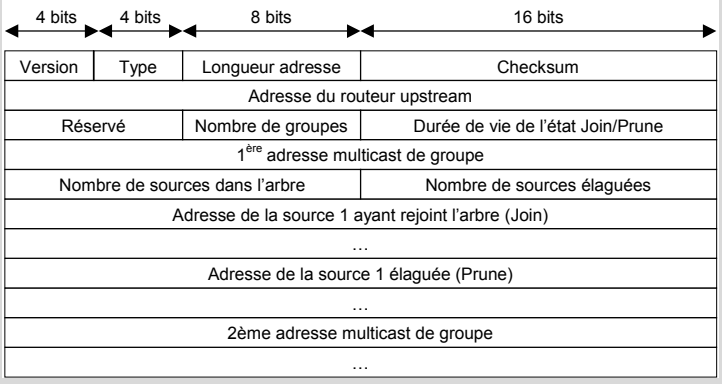
Un routeur source qui reçoit des rapports IGMP indiquant que des membres du groupe G sont actifs ajoute une route (*, G) vers le routeur **point de rendez-vous** pour le groupe ; il lui envoie alors périodiquement un message **Join/Prune** (joindre/élaguer). Tous les routeurs situés sur le chemin qui relie ces deux routeurs ajoutent la même route (*,G) en notant l'adresse du réseau source et l'interface d'entrée, puis envoient un message Join/Prune au routeur point de rendez-vous. Ce dernier connaît donc le chemin le reliant au routeur source qui déclare que des membres du groupe G sont actifs. Les routeurs ont donc rejoint un **arbre partagé** qui a comme racine le routeur point de rendez-vous (*RP shared tree*).

Un routeur source ayant pris en charge un paquet *multicast* l'encapsule dans un paquet *unicast*, puis l'envoie au routeur point de rendez-vous, qui le décapsule et le renvoie vers tous les routeurs sources déclarés (qui sont ici des routeurs destinations) et ayant rejoint l'arbre partagé.

Au bout d'un moment, un routeur (source, destination ou point de rendez-vous) peut décider de quitter l'arbre partagé afin que les paquets *multicast* soient échangés directement sans passer par le routeur point de rendez-vous. Il envoie alors un message Join/Prune au point de rendez-vous pour quitter l'arbre partagé, et un autre à la source pour rejoindre l'**arbre du plus court chemin** (SPT, *Shortest Path Tree* — dont la racine est la source) pour le couple routeur source S/groupe G. Tous les routeurs situés sur le chemin routeur source-routeur destination ajoutent la route (S,G) dans leur table de routage.

Le basculement vers le SPT s'opère lorsque le flux multicast est suffisamment important et de longue durée (en fait, au bout de quelques secondes).

Les messages Join/Prune contiennent, pour chaque groupe, la liste des sources (routeurs ou réseau) appartenant à l'arbre et celles qui en sont élaguées.



Le champ " Nombre de groupes " indique le nombre de groupes décrits dans le message (notés 1, 2, etc.).

Le champ " Adresse de la source " indique que le routeur transmettra (ou non, s'il est dans l'état Prune) un paquet multicast issu de cette source s'il provient de l'interface par laquelle il envoie ce message Join/Prune. Une adresse source peut être celle d'un routeur, d'un réseau ou d'un agrégat de réseaux.

Les routeurs diffusent les paquets multicast uniquement vers les interfaces par lesquelles sont entrés des messages Join/Prune. Par ce biais, chaque routeur connaît la topologie du réseau et calcule un arbre de routage (soit partagé, soit du plus court chemin) pour chaque couple Source/Groupe. Les routeurs s'échangent, par ailleurs, des messages Hello pour découvrir leurs voisins.

Les messages PIM sont envoyés dans des paquets *unicast* (*Register* et Register-*stop*) et *multicast* 224.0.0.13 (Hello, etc.) en utilisant le protocole n° 103 au-dessus d'IP.

L'activation du mode NBMA (*NonBroadcast MultiAccess*) permet au routeur de garder une trace des adresses IP qui émettent les messages PIM *Join* arrivant par l'intermédiaire de l'interface WAN. Les paquets multicast devant ainsi être diffusés vers cette interface seront dupliqués en autant de paquets encapsulés dans des trames unicast.

Cela est notamment le cas sur les interfaces série de nos routeurs R1 et R2 :

```
int s 0
ip pim nbma-mode
```

Il est à noter que le mode NBMA consomme de la mémoire puisqu'il garde trace de toutes les adresses IP sources arrivant par l'intermédiaire de l'interface WAN.

De même, le mode *source shortest path tree* requiert davantage de mémoire que le mode *RP shared tree*. En revanche, il réduit la charge réseau et optimise le chemin (il n'est plus besoin de passer par le RP).

Les routeurs Cisco basculent du mode *shared* vers le mode *shortest path* dès le premier paquet émis. Cependant, il est possible de n'activer le basculement qu'à partir d'un certain débit constaté, en d'autres termes, lorsque cela en vaut la peine.

```
ip pim spt-threshold 64 group-list 1
```

La commande précédente indique que le basculement s'opérera lorsque le flux multicast aura atteint 64 Kbit/s pour les groupes figurant dans l'access-list 1.

Quel protocole choisir ?

Pour l'enregistrement des membres d'un groupe auprès d'un routeur, IGMP est incontournable. Les informations collectées sont ensuite utilisées par les protocoles de routage multicast.

Trois protocoles de routage multicast sont proposés : trois solutions, trois approches différentes.

Critère	DVMRP	MOSPF	PIM
Mise à jour des tables de routage	Diffusion périodique de l'intégralité des tables	Diffusion des modifications par messages d'annonce	Centralisée au niveau du point de rendez-vous (PR)
Diffusion du premier paquet	Inondation du premier paquet	Routé directement vers les membres du groupe	Encapsulé dans un paquet unicast vers le PR, puis rediffusé par le PR
Calcul du meilleur chemin (arbre SPT) pour le couple Source/Groupe	Par élagage des routeurs ne désirant pas recevoir le paquet	À la demande, par tous les routeurs recevant le premier paquet	Par remontée de messages Join/Prune de proche en proche jusqu'à la source
Protocole de routage	DVMRP	MOSPF s 'appuie sur OSPF	S'appuie sur les protocoles existants (RIP, OSPF, etc.)
Tunneling entre routeurs non multicast	Oui	Non : les routeurs MOSPF doivent être contigus	Oui

DVMRP est le protocole le plus ancien et le moins performant (il présente les mêmes défauts que RIP). L'inondation régulière des paquets multicast ainsi que la diffusion périodique des tables de routage ne font pas de DVMRP un protocole adapté aux grands réseaux.

MOSPF est le protocole le plus performant au sein d'une aire ; il est relativement performant entre aires. Entre systèmes autonomes, l'usage de DVMRP est requis pour le multicast (en plus de BGP pour l'unicast), ce qui peut présenter quelques inconvénients.

PIM est adapté aux grands réseaux et notamment l'Internet, là où les membres d'un même groupe sont très dispersés. Dans un petit réseau, cet avantage se transforme en inconvénient, car le routeur de point de rendez-vous n'est pas obligatoirement situé sur le meilleur chemin (à moins que le réseau soit très centralisé).

D'autres considérations, non techniques, entrent en jeu :

- Les RFC de DVMRP (datée de 1988) et de PIM (datée de 1998) n'en sont qu'au stade expérimental, alors que celle de MOSPF (datée de 1994) en est à l'état de proposition de standard.
- Cependant, Cisco, le principal fournisseur de routeurs sur l'Internet, ne prend en charge que PIM, et pour cause : les ingénieurs de la société ont participé à son élaboration mais pas à celle de MOSPF.
- En outre, DVMRP est le plus répandu au sein de MBONE (*Multicast Backbone*, une portion de l'Internet expérimentant le multicast). Son utilisation est donc requise, au moins sur le routeur de frontière utilisé en interconnexion avec ce réseau.

En conclusion :

- Si vos routeurs sont de marque Cisco, PIM est le seul choix possible.
- Si votre réseau fonctionne avec OSPF et ne comprend pas de routeurs Cisco, le choix de MOSPF va de soi.
- Utilisez DVMRP entre les systèmes autonomes et pour vous raccorder à MBONE.

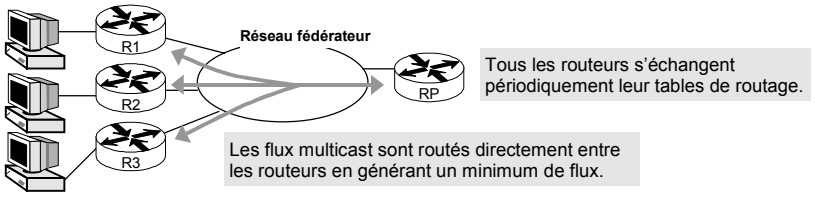
L'étape suivante consiste à définir l'architecture la mieux adaptée au protocole choisi, afin de limiter le trafic généré par les routeurs.

Si plusieurs routeurs sont présents sur le même réseau local, il faut déterminer quel est le meilleur candidat à l'élection du demandeur. Le processus d'élection dépend du protocole de routage activé. Pour les routeurs DVMRP, le routeur demandeur IGMP est celui qui a la plus petite adresse IP ou celui dont la métrique est la plus faible. Pour les routeurs MOSPF, il s'agit du routeur désigné OSPF (celui dont la priorité est la plus basse), tandis que pour PIM, il s'agit de celui dont l'adresse IP est la plus haute.

Architecture adaptée au protocole DVMRP

Il existe peu de solutions pour optimiser les flux DVMRP, si ce n'est l'emploi d'un réseau centralisé autour d'un réseau fédérateur.

Figure 13-14.
Optimisation des flux DVMRP.

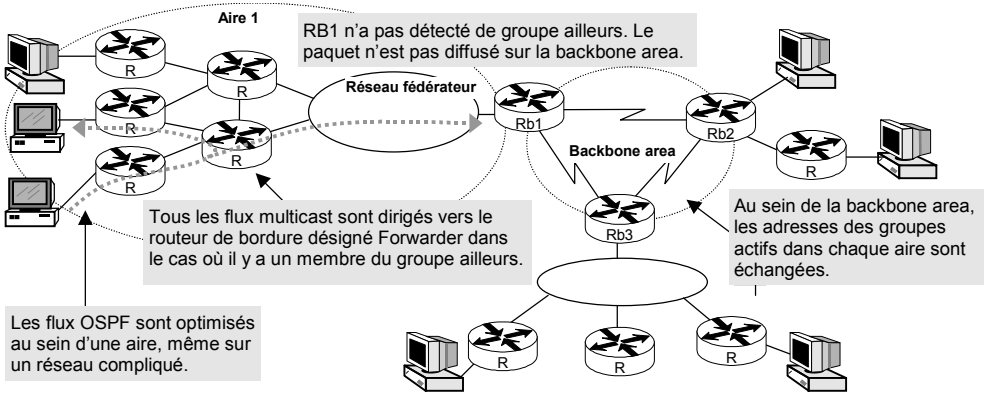


On le voit, DVMRP est adapté à un réseau localisé sur un site ou un campus avec un réseau fédérateur à haut débit.

Architecture adaptée au protocole MOSPF

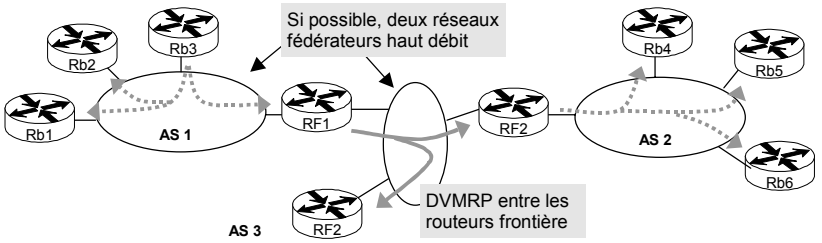
Le routage au sein des aires est bien contrôlé par MOSPF. Entre les aires, le routeur de bordure désigné forwarder reçoit tous les flux multicast ; il doit donc être positionné sur un réseau fédérateur à haut débit.

Figure 13-15.
Optimisation des flux MOSPF.



MOSPF est adapté aux grands réseaux mais limité à un seul système autonome. En effet, la concentration des flux entre AS est encore augmentée, à l'image de la concentration sur la backbone area.

Figure 13-16.
Optimisation des flux entre systèmes autonomes.



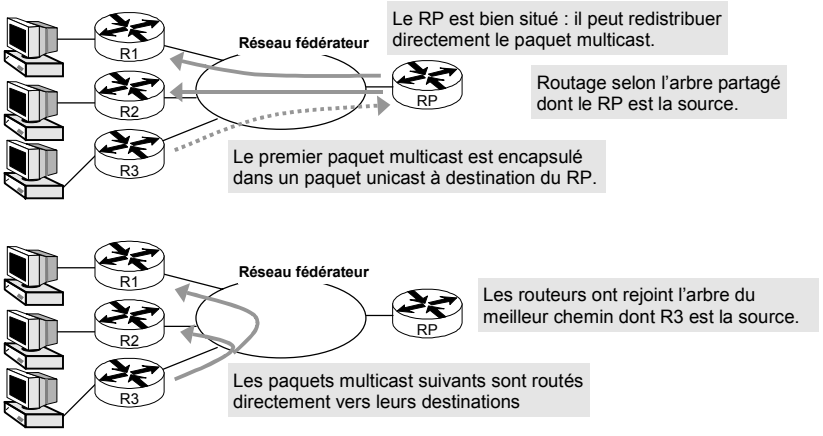
Entre systèmes autonomes, DVMRP doit être configuré en point à point, ou en multipoint sur un réseau fédérateur à haut débit, et ce afin d'optimiser le flux multicast.

Afin de limiter la taille des tables de routage, les routes redistribuées entre DVMRP et MOSPF doivent être agrégées. Cela implique que les adresses réseau soient contiguës au sein d'un système autonome (voir chapitre 11).

Architecture adaptée au protocole PIM

Le routeur point de rendez-vous de PIM doit être situé au centre du réseau, afin d'optimiser la route des premiers paquets multicast.

Figure 13-17.
Optimisation des flux PIM.



Si les membres d'un groupe sont répartis entre plusieurs sites, la meilleure position du RP se situe sur un routeur WAN.

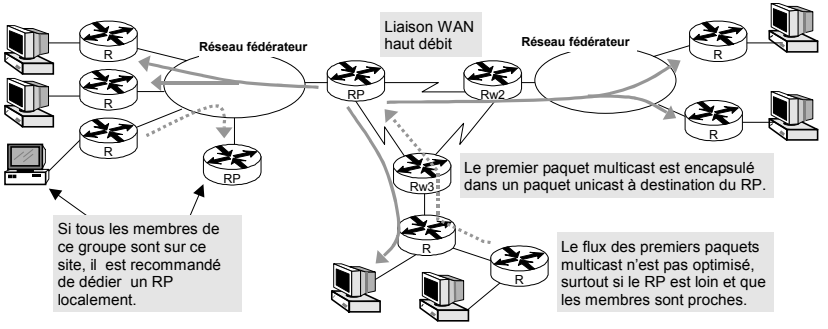


Figure 13-18.
Flux PIM sur un réseau intersite.

Il est conseillé de paramétrer les routeurs PIM pour basculer rapidement vers l'arbre du meilleur chemin, afin de ne plus passer inutilement par le RP. Les routeurs Cisco basculent dès le premier paquet : la commande *ip pim spt-threshold* ne doit donc pas être utilisée. Le revers de la médaille est un basculement inutile si le flux multicast est sporadique, ce qui entraîne une plus grande consommation de bande passante réseau (pour les messages Join/Prune) et de ressources CPU sur tous les routeurs qui calculent le nouvel arbre du meilleur chemin. En outre, ce dernier utilise beaucoup de ressources mémoire, d'autant plus qu'un arbre par couple adresse source/adresse de groupe est nécessaire.

Par ailleurs, des messages Bootstrap circulent entre les routeurs point de rendez-vous, ajoutant encore des flux de gestion propres à PIM.

Tout est donc affaire de dosage en fonction du nombre d'utilisateurs et du type de trafic. Du fait de la complexité du protocole PIM, la conception de l'architecture réseau n'en est que plus difficile.

Contrôler la diffusion sur son réseau

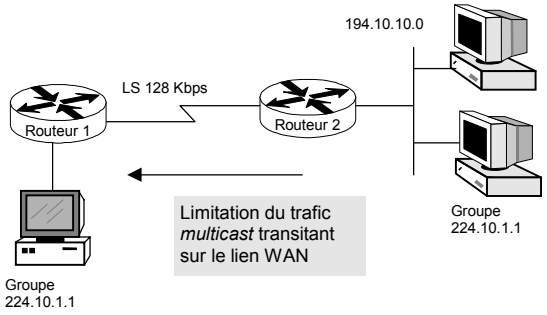
Les flux *multicast*, tels que la vidéo, peuvent générer un volume de données important. Afin de contrôler ces flux, il est possible de filtrer les groupes multicast sur chaque interface. Cela évite également de voir fleurir des groupes un peu partout sans que l'administrateur n'en soit tenu informé.

```
access-list 90 225.20.2.2 0.0.0.0
access-list 90 224.10.1.1 0.0.0.0
interface ethernet 0
ip igmp access-group 90
```

L'access-list 90 contient la liste des adresses de groupe qui seront autorisées à être diffusées sur l'interface Ethernet 0.

Il est également intéressant de contrôler le débit généré par les membres d'un groupe, pour ne pas pénaliser les autres applications et, également, ne pas inonder votre réseau.

Figure 13-19.
Contrôle du trafic multicast.



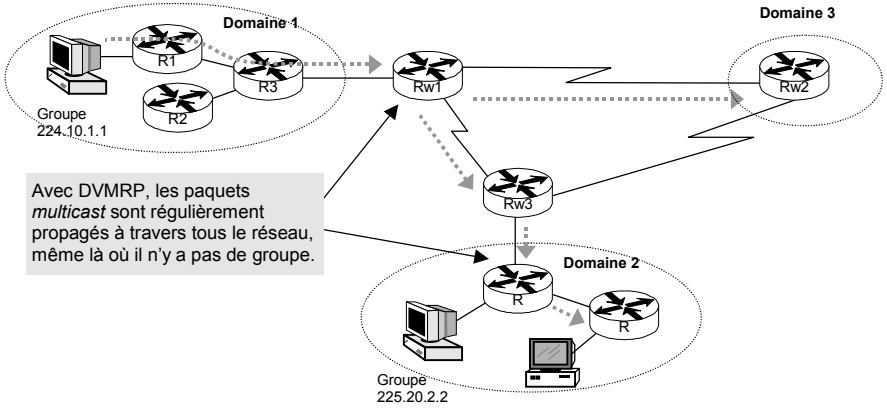
Dans cet exemple, les membres indiqués dans l'access-list 90 et qui émettent au sein des groupes précisés dans l'access-list 80 sont limités à un débit de 64 Kbit/s sur la liaison WAN. Cette limite peut être positionnée en entrée (*in*) ou en sortie (*out*) de l'interface.

```
interface serial 1
ip multicast rate-limit out group-list 80 source-list 90 64
access-list 80 permit 0.0.0.0 255.255.255.255
access-list 90 permit 194.10.10.0 0.255.255.255
ip multicast rate-limit in group-list 80 source-list 90 64
```

Dans l'exemple précédent, tous les multicast issus du réseau 194.10.10.0 seront limités à 64 Kbit/s, laissant une bande passante de 64 Kbit/s disponible pour les autres applications.

Reprenons l'exemple de notre réseau intersite.

Figure 13-20.
Contrôler la diffusion.

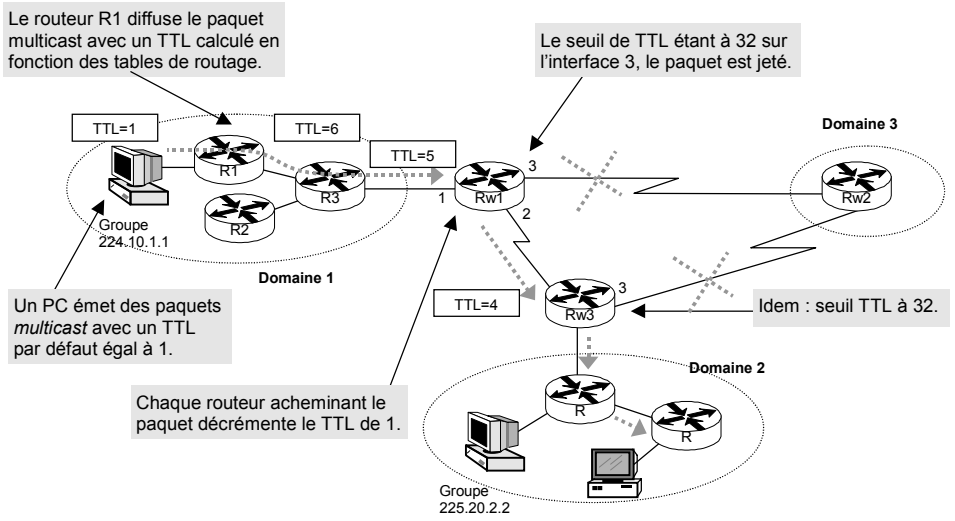


Si DVMRP est utilisé, tous les premiers paquets multicast émis par une source pour un groupe donné sont diffusés à travers l'ensemble du réseau (tant qu'il y a des routeurs DVMRP). Comme on l'a vu, DVMRP est obligé de répéter cette procédure régulièrement afin de tenir compte des changements de topologie et d'appartenance à un groupe.

Cela est également le cas de MOSPF, dans la *backbone area*, et de PIM, au niveau des réseaux auxquels est connecté le routeur point de rendez-vous.

Les routeurs permettent de limiter la propagation de ces paquets en contrôlant leur TTL (*Time To Live*). Ce mécanisme impose qu'un paquet IP ne soit pas routé lorsque son TTL est égal à 1. Le mécanisme proposé permet de définir un seuil supérieur en dessous duquel le paquet ne sera pas routé.

Figure 13-21.
Limitation de la diffusion des paquets.



Seuls les paquets dont le TTL est supérieur au seuil de 32 seront routés par les routeurs Rw1 et Rw3 sur leur interface série 3. La commande Cisco est la suivante :

```
int s3
ip multicast ttl-threshold 32
```

La valeur par défaut est 0

En positionnant différents seuils à certains points stratégiques du réseau, il est possible de définir des domaines de diffusion. On peut ainsi limiter la portée du point de rendez-vous PIM ou la propagation des paquets *via* des routeurs DVMRP.

Par exemple, MBONE utilise la convention suivante :

TTL	Périmètre
0	Restreint à la machine (paquet boucle en local)
1	Restreint au même réseau local
32	Site
64	Région
128	Continent
255	Pas de restriction de diffusion

Des mécanismes propres à IGMP sont également prévus pour limiter le trafic local :

- Les rapports sont envoyés avec un TTL = 1, ce qui permet de supprimer le paquet rapidement : le rapport est censé être adressé uniquement au routeur du réseau local.
- Les rapports sont envoyés un à un pour chaque groupe d'appartenance, avec un intervalle de temps aléatoire.
- Au niveau du routeur, les temporisateurs *(timers)* sont armés indépendamment pour chaque groupe identifié.

Les groupes de paquets compris entre 224.0.0.0. et 224.0.0.255 ne sont jamais routés : de tels paquets transitent d'une machine vers un routeur, d'un routeur vers un autre routeur, et ce quelle que soit la valeur du TTL (en principe égale à 1).