

Comunicare tra molti nelle reti IP: l'instradamento IP multicast

FRANCESCO IUSO
LORIS MARCHETTI

Immaginiamo che una sorgente debba inviare la medesima informazione a un gruppo di ricevitori: ci aspetteremmo che la sorgente "immetta" in rete una distinta istanza dell'informazione per ogni ricevitore interessato, in modo da recapitarla secondo le consuete modalità unicast.

Le caratteristiche di instradamento multicast permettono in questo caso di trasportare le informazioni in modo più efficiente, consentendo alla sorgente di trasmettere una sola istanza dell'informazione e lasciando ai nodi della rete l'onere di replicarla solo quando necessario, in modo da recapitarla ai ricevitori che hanno manifestato interesse a riceverla.

Riprendendo il caso della consegna dei telegrammi, portato spesso come esempio per descrivere la consegna dei pacchetti IP, il mittente, invece di imbucare n copie del medesimo telegramma destinato a un gruppo di destinatari, ne imbuca una sola copia indicando come destinatario l'identificativo del gruppo di interesse. È poi cura del servizio postale fotocopiare il telegramma, quando necessario, in modo da consegnarlo ai destinatari che hanno manifestato interesse a ricevere le informazioni destinate al gruppo di interesse.

La tecnologia IP prevede un insieme di protocolli che consente di realizzare le funzioni di instradamento multicast. I servizi introdotti impiegando queste funzioni sono sia di tipo distributivo (ad esempio il broadcasting di informazioni multimediali) sia interattivo (ad esempio la multivideoconferenza, dove ogni partecipante è allo stesso tempo sorgente e ricevitore di flussi multicast).

In questo articolo, dopo aver descritto i protocolli necessari per introdurre le soluzioni IP multicast standard, sono analizzate soluzioni alternative – di tipo proprietario – che consentono di realizzare soluzioni di servizio di tipo distributivo multimediale.

1. Cos'è il multicast IP

Il trasporto in multicast è un sistema efficiente - consentito dalle caratteristiche tecnologiche della rete - per trasmettere, come mostrato in figura 1, la stessa informazione a numerosi ricevitori.

Dalla figura si osserva che la sorgente, invece di trasmettere l'informazione un numero di volte pari a quello dei destinatari interessati, si limita a immettere in rete una sola istanza dell'informazione. È poi la rete che, mediante le funzioni di instradamento multicast, provvede a replicarla nei nodi di rete (cioè nei router) solo quando necessario, in modo da recapitarla a tutti i destinatari interessati.

Questa modalità di funzionamento mette in luce due vantaggi: è ridotto anzitutto il numero di flussi immessi dalla sorgente in rete ed è perciò ottimizzata

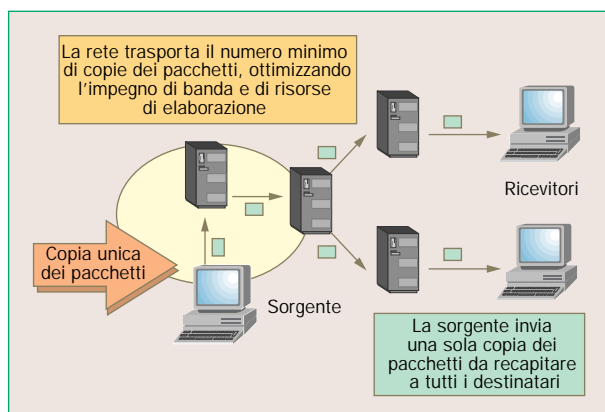


Figura 1

La trasmissione multicast.

la capacità con la quale la sorgente deve essere connessa alla rete. Risulta poi essere contenuto il numero di pacchetti da trasportare ed è quindi reso ottimo il trasporto delle informazioni in rete.

Per questi vantaggi il multicast è considerato una componente importante per le soluzioni di servizio che prevedono di distribuire contenuti multimediali a un gran numero di ricevitori.

I servizi previsti dallo standard IP multicast sono sia quelli di tipo "da uno a molti" sia quelli di tipo "da molti a molti".

La tecnologia IP multicast consente poi ai ricevitori di richiedere dinamicamente di entrare a far parte di un gruppo di interesse – il gruppo multicast – identificato da un indirizzo IP di tipo multicast. Il multicast IP è *receiver based*: i ricevitori, per ricevere traffico multicast destinato a un particolare gruppo multicast, devono infatti aderire a questo gruppo. La sorgente viceversa non deve essere iscritta necessariamente al gruppo verso il quale trasmette.

L'iscrizione o l'abbandono del gruppo multicast sono regolati da un protocollo specifico tra il ricevitore e il router con il quale esso può comunicare direttamente. L'appartenenza al gruppo multicast può infatti essere modificata in ogni momento e ciascun ricevitore può far parte di diversi gruppi multicast.

Il gruppo multicast è identificato da un indirizzo di classe D [1], analizzato di seguito nell'articolo.

Il traffico emesso dalla sorgente, inviato a un indirizzo multicast, è trasportato in rete in modo efficiente secondo quanto previsto dal protocollo di instradamento multicast utilizzato che interessa i router della rete.

Da questa descrizione sintetica del funzionamento del multicast nelle reti IP possono essere delineati gli elementi che compongono l'architettura, rappresentati nella figura 2:

- gli indirizzi multicast, necessari per identificare i singoli gruppi multicast;
- il trasporto, a livello fisico, del traffico IP multicast nonché la modalità per tradurre gli indirizzi IP multicast in quelli di livello MAC (*Media Access Control*);
- il protocollo per gestire l'appartenenza al gruppo, utilizzato dai ricevitori per informare il router della rete, con il quale essi comunicano direttamente, circa la volontà di ciascuno di essi di aderire o di lasciare uno specifico gruppo multicast, identificato da un indirizzo di classe D;
- il protocollo di instradamento multicast, utilizzato dai singoli router presenti in rete per instradare il traffico multicast emesso dalla sorgente multicast e indirizzato a un gruppo multicast.

Qui di seguito sono esaminate le singole componenti sopra elencate.

1.1 Indirizzi IP multicast

Gli indirizzi multicast differiscono da quelli unicast in quanto non identificano una sola interfaccia IP, ma un insieme di ricevitori, cioè un gruppo di "host", la cui numerosità può variare nel tempo in base alla richiesta di ciascuno di essi di aderire al gruppo.

La rete Internet attuale (IPv4) ha uno spazio per

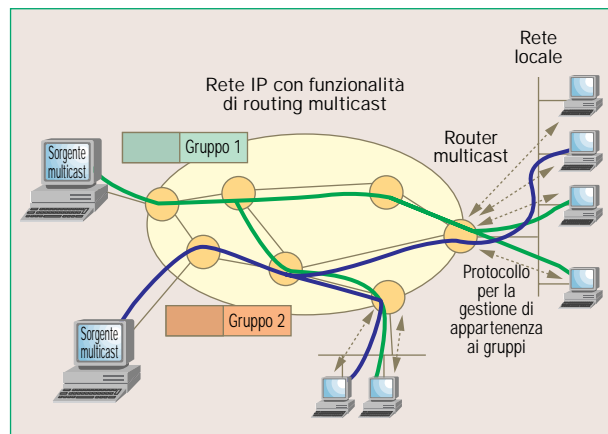


Figura 2 Architettura multicast.

l'indirizzamento che impiega 32 bit. Questo spazio è diviso in cinque classi (*blocchi*) denominate rispettivamente indirizzi di classe A, B, C, D ed E [1].

Gli indirizzi multicast appartengono alla classe D. Tutti gli indirizzi appartenenti a questa classe sono identificati dal prefisso "1110" (figura 3). I rimanenti 28 bit identificano il particolare gruppo multicast.

Il sottoinsieme di indirizzi multicast è compreso nell'intervallo da 224.0.0.0 a 239.255.255.255. Il corrispondente decimale del primo byte può infatti variare da 224 (cioè "11100000") a 239 (cioè "11101111").

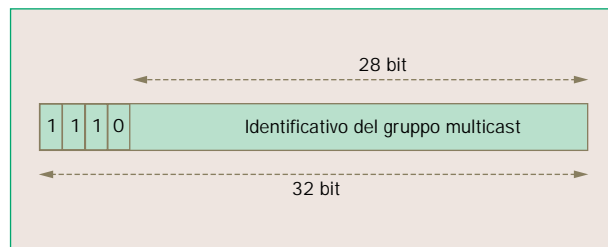


Figura 3 Formato degli indirizzi di classe D.

In particolare, gli indirizzi multicast sono utilizzati solo come *indirizzi di destinazione* per identificare il gruppo di unità ricevente il traffico IP multicast, e non sono quindi impiegati come *indirizzo sorgente*, che rimane unicast: un pacchetto IP multicast ha come indirizzo sorgente *SA* (*Source Address*) l'indirizzo unicast della sorgente e come indirizzo di destinazione quello *DA* (*Destination Address*), che è l'indirizzo multicast che identifica il gruppo multicast.

Non tutti gli indirizzi di classe D possono essere utilizzati per indirizzare il traffico multicast. Alcuni sono difatti riservati per scopi particolari: così, ad esempio, l'indirizzo multicast 224.0.0.1 è assegnato permanentemente a un gruppo particolare di cui fanno parte tutti gli apparati impiegati nella rete locale (router, workstation, PC, ...); l'indirizzo 224.0.0.2 identifica invece tutti i router presenti nella rete locale.

Indirizzi multicast riservati

- Gli indirizzi compresi tra 224.0.0.0 e 224.0.0.255 sono chiamati *Reserved Link Local* e sono impiegati per lo scambio di messaggi per il controllo dei protocolli impiegati all'interno di una LAN. I router che ricevono pacchetti con questi indirizzi di destinazione non devono inoltrarli verso altre reti.
- Gli indirizzi compresi tra 224.0.1.0 e 238.255.255.255 sono indicati come *Globally Scoped* e sono stati assegnati da IANA a particolari applicazioni. I pacchetti multicast con questi indirizzi di destinazione non hanno limiti nella propagazione verso altre reti.
- Gli indirizzi compresi tra 239.0.0.0 e 239.255.255.255 sono chiamati *Limited Scope o Administratively Scoped*. La RFC 2365 [4] li definisce come indirizzi multicast utilizzabili all'interno di una rete corporate o comunque di un dominio. I router di bordo sono in genere configurati per riuscire a individuare e filtrare in ingresso e in uscita flussi multicast indirizzati a questi gruppi.
- Lo spazio di indirizzi da 233.0.0.0 a 233.255.255.255 è chiamato GLOP ed è riservato alle Organizzazioni che dispongono di un sistema autonomo, AS (*Autonomous System*). Come descritto nella RFC 2770 [5], è stata definita una modalità per cui il secondo e terzo otteetto identificano in maniera univoca il sistema autonomo mentre il quarto può essere utilizzato per individuare i diversi flussi multicast del sistema autonomo. Il limite massimo di 256 indirizzi multicast può d'altra parte non coprire le esigenze del sistema autonomo di una certa dimensione.

Nota: La lista aggiornata degli indirizzi multicast è disponibile nel sito <http://www.isi.edu/in-notes/iana/assignments/multicast-addresses>

Altri indirizzi multicast sono riservati per lo scambio di traffico di segnalazione relativo ai protocolli di instradamento: gli indirizzi 224.0.0.5 e 224.0.0.6 sono infatti utilizzati dal protocollo *OSPF (Open Shortest Path First)* [2]; l'indirizzo 224.0.0.4 identifica tutti i router *DVMRP (Distance Vector Multicast Routing Protocol)* [3] sulla rete locale ed è impiegato dal protocollo di routing di instradamento multicast *DVMRP*.

Lo spazio di indirizzamento multicast è stato classificato dall'Autorità internazionale preposta all'assegnazione degli indirizzi Internet, cioè *IANA (Internet Assigned Numbers Authority)*. Nel riquadro riportato in questa stessa pagina sono elencate le più importanti categorie di indirizzi multicast "riservati".

1.2 Corrispondenza tra multicast a livello IP e a livello MAC (*Media Access Control*)

Nella *RFC (Request For Comments)* 1112 [6] è descritto come il traffico multicast IP è trasportato fisicamente sulla rete locale. Lo standard non comprende tutte le tecnologie di sistemi impiegati nella rete locale; esso definisce però le modalità di trasporto del traffico multicast previste per la tecnologia Ethernet, in quanto essa è oggi quella maggiormente diffusa a livello di rete locale.

Per trasmettere il traffico IP multicast è necessario che esso sia imbustato in trame Ethernet con un indi-

irizzo multicast Ethernet (MAC IEEE 802.3), ricavato a partire dall'indirizzo IP multicast, in analogia con quanto previsto per il trasferimento del traffico unicast che utilizza il protocollo *ARP (Address Resolution Protocol)* per tradurre l'indirizzo IP in quello MAC [1].

La regola stabilita per ricavare l'indirizzo multicast Ethernet, a partire dall'indirizzo IP multicast, è relativamente semplice: gli ultimi 23 bit dell'indirizzo IP multicast di classe D diventano quelli meno significativi dell'indirizzo Ethernet multicast 01-00-5E-00-00-00 Hex [6]. Non è, d'altra parte, necessario usare ARP in quanto la trasformazione è automatica.

Nella figura 4 è mostrato come, ad esempio, l'indirizzo multicast IP 224.10.8.5 (in esadecimale E0-0A-08-05) è tradotto nel corrispondente indirizzo multicast Ethernet.

La figura 4 mostra che la corrispondenza non è univoca e che a blocchi di 32 indirizzi IP multicast corrisponde uno stesso indirizzo MAC Ethernet: ad esempio all'indirizzo IP multicast 224.138.8.5 (in esadecimale E0-8A-08-05) e a quello 225.10.8.5 (in esadecimale E1-0A-08-05) corrisponde l'indirizzo multicast Ethernet 01-00-5E-0A-08-05 (Hex).

Questo schema di corrispondenza rappresenta un compromesso curato da IANA in quanto, altrimenti, avrebbe dovuto acquistare da IEEE 16 prefissi consecutivi da 24 bit, con una spesa di 16 mila US \$ e con la violazione delle regole di IEEE, che

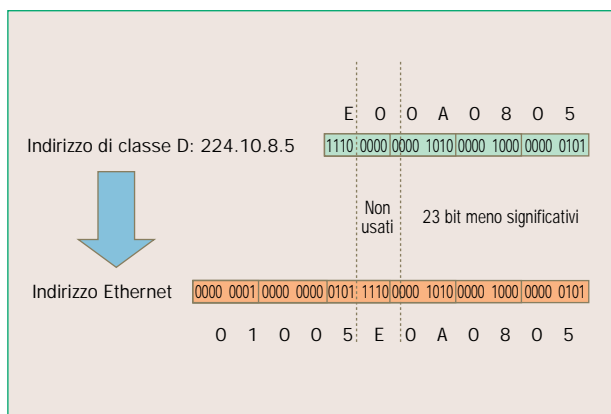


Figura 4 Corrispondenza tra l'indirizzo multicast IP e quello Ethernet.

vietano di assegnare ai costruttori blocchi di indirizzi consecutivi da 24 bit.

Si scelse di tollerare la probabilità, peraltro bassa, che in una rete locale avrebbe potuto presentarsi la sovrapposizione di indirizzi. Si procedette perciò all'acquisto di un unico blocco di indirizzi: quello con prefisso 01-00-5E Hex; si decise poi di utilizzare solo metà dello spazio di indirizzamento acquisito, quello con il ventiquattresimo bit posto a 0, riservando la seconda metà del blocco per scopi da definire (si utilizzano solo gli ultimi 23 bit). Nella costituzione dell'indirizzo Ethernet multicast il bit dopo il prefisso 01-00-5E Hex è posto a 0 e ad esso seguono i ventitré bit ricavati dall'indirizzo IP multicast.

1.3 L'adesione ai gruppi: il protocollo IGMP (Internet Group Management Protocol)

Steve Deering in [6] ha specificato nel 1989 che gli host, per poter scambiare traffico multicast in una rete locale, devono utilizzare l'architettura per i protocolli mostrata in figura 5.

La figura mostra che IGMP, come pure ICMP, è compreso in IP.

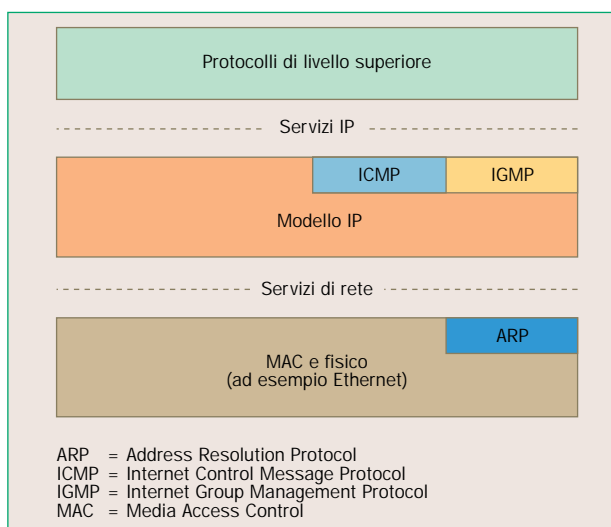


Figura 5 Architettura dei protocolli impiegati negli host.

L'architettura dei protocolli impiegati rappresenta un'estensione di quella IP. Si differenzia da essa per l'aggiunta delle funzioni necessarie per inviare e per ricevere traffico multicast, secondo quanto chiarito nel §1.2 precedente, e per il protocollo *IGMP* (*Internet Group Management Protocol*), che definisce le modalità di scambio di informazioni di appartenenza ai gruppi tra gli host e il router multicast presenti nella rete locale.

Il meccanismo di funzionamento del protocollo IGMP, di seguito descritto, è valido per le reti di tipo *broadcast*, come ad esempio le reti Ethernet. Per altri tipi di reti, quali quelle ATM, che non sono per loro natura *broadcast*, sono state sviluppate soluzioni che fanno ricorso a configurazioni e, anche, all'aggiunta di server esterni che riproducono il meccanismo che prevede lo scambio periodico di informazioni tra router multicast e host sulla rete. Nel riquadro di pagina 66 sono descritte le soluzioni previste per le reti locali realizzate in tecnica ATM.

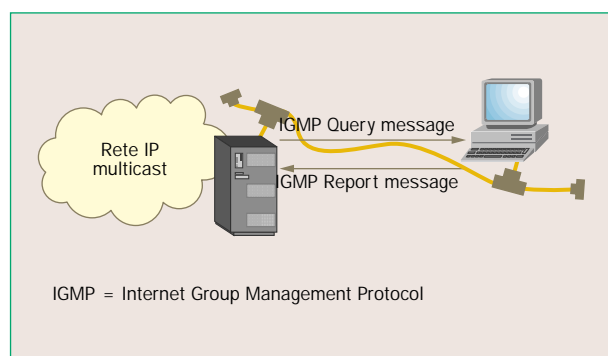


Figura 6 Scambio del protocollo IGMP (Internet Group Management Protocol) tra router e terminali sulla LAN.

Gli host presenti nella rete locale, con i meccanismi previsti da IGMP [6] [7], possono comunicare al router multicast l'intenzione di aderire a un gruppo multicast (identificato da uno specifico indirizzo IP multicast) in modo che il router provveda a rilanciare il traffico relativo a quel gruppo sulla rete locale.

Lo scambio di informazioni previsto dal protocollo IGMP è schematizzato in figura 6: il router multicast impiegato nella rete locale emette periodiche interrogazioni (*IGMP Query message*) per verificare la presenza sulla rete di membri di gruppi multicast; gli host presenti in rete rispondono alle interrogazioni per confermare l'appartenenza al gruppo multicast. Quando un host aderisce a un nuovo gruppo trasmette un messaggio di risposta (*IGMP Report message*) senza aspettare la richiesta periodica del router.

Se sulla rete locale sono presenti più router multicast, allora solo uno di essi effettuerà le interrogazioni periodiche per la gestione dei gruppi.

Con cadenza periodica, in genere ogni 60 s, il router multicast invia richieste IGMP con *Time To Live* uguale a 1 (TTL=1) in modo che il traffico rimanga confinato nella rete locale (l'impiego del TTL è chiarito nel riquadro di pagina 67).

Le richieste (IGMP Query message) sono inviate all'indirizzo multicast 224.0.0.1, che identi-

fica il gruppo di cui fanno parte tutti gli host presenti nella rete locale.

La cadenza periodica con la quale il router multicast genera le richieste IGMP può essere modificata. Essa infatti costituisce il risultato di un compromesso: da un lato deve rispondere all'esigenza di limitare il traffico di segnalazione IGMP, che porta a configurare l'intervallo quanto più possibile esteso; d'altro canto essa deve garantire un'adeguata "interattività", e quindi configurare l'intervallo quanto più possibile breve.

Alle richieste emesse dal router multicast - il cui formato è mostrato nella figura 7 - gli host rispondono con il messaggio IGMP Report di formato analogo all'IGMP Query.

Il pacchetto di risposta IGMP contiene l'indirizzo del gruppo multicast a cui l'host intende aderire o confermare l'adesione. Ogni host prevede l'emissione di un IGMP Report per ciascun gruppo a cui esso aderisce.

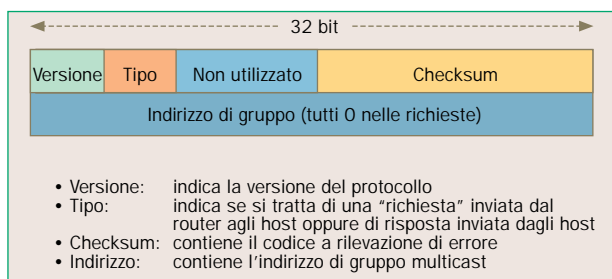


Figura 7 Formato del messaggio IGMP.

In base alle informazioni scambiate con il protocollo IGMP, il router multicast può costruire una lista in cui tiene traccia dei gruppi multicast di cui fanno parte gli host presenti nella rete locale. È importante osservare che l'informazione di cui ha bisogno il router riguarda solo il fatto che un dato gruppo multicast (identificato da un indirizzo di classe D) sia attivo nella rete locale (e cioè che almeno un host ne faccia parte). Non ha rilevanza quindi quale particolare host faccia parte del gruppo.

Per il protocollo IGMP è stata prevista una serie di accorgimenti che consentono di evitare che il traffico di segnalazione possa causare uno stato di congestione.

I pacchetti di risposta sono inviati con TTL (il cui impiego come si è già detto è chiarito nel riquadro di pagina 67) posto a 1 all'indirizzo multicast riportato all'interno del messaggio IGMP di figura 7. In questo modo la risposta può essere sentita dagli altri membri del gruppo in rete, in modo che essi evitino l'invio di ulteriori messaggi IGMP per confermare la propria adesione a quel gruppo.

Gli host non rispondono immediatamente a una interrogazione IGMP, ma attendono un tempo la cui durata è casuale: in questo modo da un lato si evita che il router riceva tutte le risposte contemporaneamente e si impedisce dall'altro canto che un host che aderisce ad un gruppo G invii una propria risposta se nel frattempo ne è stata già trasmessa un'altra sempre relativa al gruppo G. Al router perviene così un solo IGMP Report per ciascun gruppo, anche se

sulla rete locale sono presenti più host interessati a questo stesso gruppo.

Per rendere minimo il traffico, il protocollo IGMP prevede anche che la cancellazione da un gruppo multicast avvenga in modo silenzioso: se l'host infatti non intende più far parte del gruppo multicast si limita solo a non rispondere alle richieste periodiche emesse dal router multicast.

Se il router multicast non riceve alcuna risposta che interessi uno specifico gruppo multicast, allora deduce che sulla rete locale non sono più presenti membri di tale gruppo e procede quindi a rimuovere dalla propria lista l'identificativo del gruppo (cioè l'indirizzo multicast del gruppo) e a interrompere il rilancio del relativo traffico multicast sulla rete locale.

Con la versione 2 del protocollo IGMP [7] è stato modificato l'algoritmo per l'elezione del router multicast delegato a inviare periodicamente le richieste e, allo stesso tempo, sono state introdotte alcune funzioni aggiuntive:

- il router con l'indirizzo IP più basso è delegato a effettuare le interrogazioni periodiche e a mantenere la lista dei gruppi qualora sulla rete locale sono presenti più router multicast;
- un nuovo messaggio (*messaggio group-specific query*) provvede a indirizzare le richieste IGMP solo ai membri di uno specifico gruppo;
- gli host in maniera autonoma (senza attendere l'interrogazione periodica operata dal router multicast sulla rete locale) possono inviare un messaggio (*messaggio leave group*) che chiede di lasciare il gruppo multicast. Il messaggio è indirizzato al gruppo 224.0.0.2, cioè a tutti i router presenti nella rete locale.

In risposta a un messaggio di tipo *leave group*, il router trasmette un'interrogazione del tipo *group-specific query* per verificare la presenza di altri membri del gruppo da cui un host si è appena dissociato. Se non riceve risposta elimina l'identificativo del gruppo dalla sua lista e interrompe il rilancio del flusso di traffico multicast verso quel gruppo.

Con la versione 3 del protocollo [8], oggi ancora in fase di definizione, gli host potranno anche scegliere da quali sorgenti del gruppo ricevere informazioni.

1.4 Instradamento dei pacchetti multicast in rete

Per il trasporto del traffico multicast dalla sorgente alle destinazioni occorre che nei nodi della rete geografica (cioè nei router della rete IP) siano attivate le funzioni necessarie per l'instradamento multicast.

Queste funzioni servono per realizzare un albero di consegna che ha come *radice* la sorgente delle informazioni e come *foglie* i membri del gruppo multicast; si evitano così percorsi chiusi (*routing loop*) e l'inondazione della rete per effetto di repliche a valanga.

I *nodi dell'albero* rappresentano i router della rete geografica IP e permettono di replicare il traffico in modo da ottimizzarne il trasporto in rete.

Gli algoritmi per l'instradamento multicast, a differenza di quelli per l'instradamento unicast [1], permettono di replicare i pacchetti e computano il loro instradamento in base all'analisi dell'indirizzo relativo alla sorgente e al gruppo multicast a cui i pacchetti sono destinati.

IP MULTICAST SU ATM

In ambito IETF sono state definite due tecniche per effettuare il multicasting di pacchetti IP in reti ATM commutate. *L'approccio a maglia* di circuiti virtuali VC *mesh* utilizza una magliatura di connessioni ATM punto-multipunto tra ciascuna sorgente e i membri del gruppo multicast. *L'approccio MCS (MultiCast Server)* impiega invece un server centralizzato che consente di ricevere i dati dalla sorgente, di replicarli e di inviarli a tutti gli host appartenenti al gruppo multicast, sfruttando le connessioni virtuali ATM di tipo punto-multipunto. Nella figura A sono mostrate le due diverse alternative.

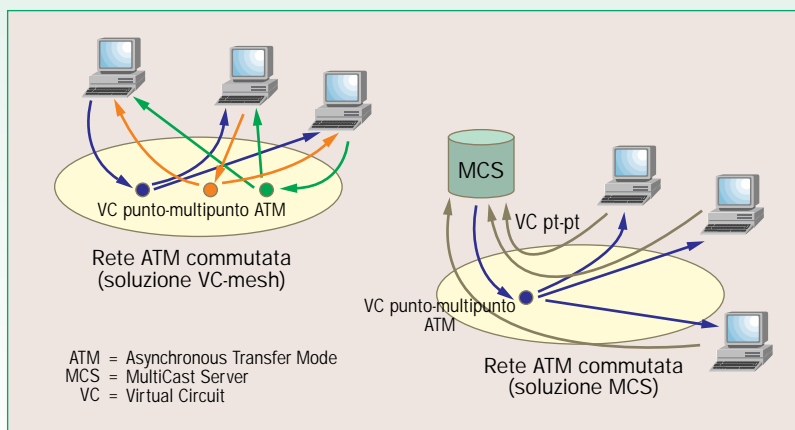


Figura A Tecniche per effettuare il multicasting IP in reti ATM.

Entrambi gli approcci richiedono l'impiego di un server centralizzato denominato *MARS (Multicast Address Resolution Server)*, che garantisce lo scambio dei messaggi IGMP tra il router e gli host in rete. Il server, in base ai messaggi IGMP scambiati, fornisce le informazioni necessarie per l'aggiornamento delle connessioni ATM punto-multipunto impiegate nei due approcci per il trasferimento delle informazioni multicast (cioè ai terminali della soluzione VC mesh oppure ai multicast server).

Ciascun MARS server gestisce un cluster di terminazioni (*end-points*) ATM (figura B). Un cluster corrisponde in genere a una *LIS (Logical IP Subnet)*. Ogni host che desidera

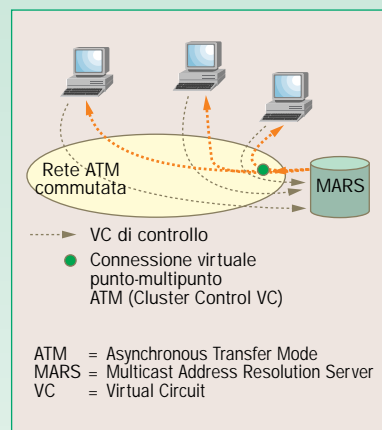


Figura B Rete ATM commutata.

essere iscritto a un gruppo multicast, registra l'indirizzo multicast che identifica il gruppo e il proprio indirizzo ATM presso il MARS (l'indirizzo ATM del MARS è fornito nel corso della configurazione).

Il MARS ridistribuisce i messaggi di *join* e di *leave* verso gli altri membri del gruppo multicast attraverso una connessione punto-multipunto nota come *Cluster Control VC*.

Nella soluzione *VC mesh*, ad esempio, gli host o il router presenti nella rete locale, che desiderano trasmettere traffico verso un gruppo multicast, possono ottenere le informazioni necessarie (ovvero gli indirizzi ATM dei membri) interrogando il server MARS.

Da ciò si deduce una prima importante differenza con l'instradamento unicast: l'instradamento unicast si basa infatti solo sull'analisi della destinazione dei pacchetti e per questo è chiamato *destination-based*; l'instradamento multicast si basa invece sull'analisi dell'origine dei pacchetti ed è perciò denominato *source-based*.

Per l'instradamento multicast sono stati sviluppati diversi algoritmi, che si differenziano sia per le strategie impiegate nell'ottimizzazione dell'albero di consegna sia per le informazioni utilizzate.

Anche da questo punto di vista il multicast differisce dall'unicast: per l'instradamento unicast è stato infatti definito un solo algoritmo che serve per determinare il nodo successivo verso il quale inoltrare il pacchetto in base all'analisi dell'indirizzo di destinazione e alle informazioni contenute nella tabella di instradamento unicast [1].

2. Algoritmi di instradamento multicast

Come chiarito nel paragrafo 1.3, IGMP realizza solo l'ultimo passo nella consegna dei pacchetti multicast: dal router ai membri di un gruppo sulle LAN a essa direttamente interconnesse. Nel più vasto ambiente *internetwork* l'instradamento corretto dei pacchetti è possibile grazie ai protocolli di instradamento multicast. Essi provvedono alla costruzione degli alberi di consegna multicast e all'inoltro (*forwarding*) dei pacchetti. Sono stati studiati diversi algoritmi di inoltro multicast da cui poi sono stati specificati i protocolli per l'instradamento multicast [9].

Di seguito si riporta una descrizione sintetica dei principali algoritmi oggi impiegati.

2.1 Flooding

L'algoritmo di *flooding* (letteralmente inondazione) è estremamente semplice nel suo enunciato:

Controllo della propagazione basato sul Time To Live

In alternativa alle regole basate sugli indirizzi, è stato messo a punto un meccanismo per il controllo della propagazione (*scoping*) di pacchetti multicast fondato sul concetto del *TTL (Time To Live)*. Ogni pacchetto IP ha un campo TTL che fissa il limite del numero massimo di *hop*, e cioè del numero di ritrasmissioni in cascata da un router al successivo, che il pacchetto può attraversare. Accanto al concetto di TTL associato alla sorgente, è stato messo a punto quello di soglia (*threshold*) associato al multicast router: in questo caso il valore del TTL relativo al pacchetto entrante è confrontato con quello di soglia e, se esso è superiore, è inoltrato dopo essere stato ridotto di un'unità, altrimenti esso è scartato.

«se il pacchetto è ricevuto per la prima volta, allora il router provvede a replicare il pacchetto ricevuto e a ritrasmetterlo attraverso tutte le proprie interfacce, ad eccezione di quella dalla quale il pacchetto è pervenuto».

In realtà la difficoltà riscontrata nella messa a punto dell'algoritmo consiste proprio nel determinare se il pacchetto è stato effettivamente ricevuto per la prima volta.

Una soluzione potrebbe essere quella di tenere traccia di tutti i pacchetti pervenuti al router, ma essa richiederebbe di predisporre una memoria di grande capacità e comporterebbe soprattutto un elevato consumo di risorse di elaborazione.

L'algoritmo non richiede per il funzionamento informazioni sull'instradamento, e non comporta perciò la predisposizione di alcuna tabella di instradamento multicast.

Questo algoritmo è utilizzato nei protocolli di instradamento unicast, come ad esempio *OSPF (Open Shortest Path First)* [2], per scambiare le informazioni di instradamento tra i nodi della rete.

2.2 Spanning Tree

L'algoritmo *spanning tree* (letteralmente albero ricoprente) è una soluzione più efficiente del *flooding*, ed è utilizzata ad esempio dai bridge per interconnettere diverse LAN in modo da evitare percorsi chiusi (*loop*).

L'algoritmo agisce in una prima fase per individuare i rami che costituiscono l'albero ricoprente. Su questa base si identificano le interfacce dei router agli estremi dei rami dell'albero ricoprente.

L'algoritmo consente poi che ciascun router replichi i pacchetti multicast sulle sole interfacce appartenenti all'albero ricoprente, con l'eccezione dell'interfaccia da cui il pacchetto è arrivato.

In questo modo, senza disporre di informazioni di instradamento aggiuntive né di grandi quantità di memoria, è possibile garantire che nella trasmissione in multicast il pacchetto non segua percorsi chiusi (*loop*).

Questo algoritmo non consente tuttavia di tenere traccia dell'appartenenza ai gruppi multicast e concentra il traffico su un sottoinsieme di collegamenti della rete.

2.3 Reverse Path Forwarding

Il funzionamento legato all'algoritmo *RFP (Reverse Path Forwarding)* può essere così sintetizzato:

- alla ricezione di un pacchetto multicast si analizza l'indirizzo della sorgente "S" e quello dell'interfaccia "I" attraverso la quale è arrivato il singolo pacchetto;
- se "I" si trova sul percorso più breve verso "S", allora il pacchetto è replicato ed è inoltrato verso tutte le interfacce ad eccezione di "I";
- nel caso non si sia verificata la condizione precedente, il pacchetto è scartato.

L'algoritmo richiede per il proprio funzionamento la predisposizione di una tabella all'interno di ogni nodo che indichi, per ciascuna sorgente, l'interfaccia del nodo sul percorso più breve verso la sorgente e, a questo scopo, potrebbe essere utilizzata la tabella di instradamento unicast.

Alcuni protocolli realizzano invece una *tabella ad hoc*, in quanto il traffico in Internet non è simmetrico: per il funzionamento dell'algoritmo RFP è necessario riconoscere da quale interfaccia proviene il traffico di una data sorgente. Nella tabella di instradamento unicast è indicato al contrario il nodo successivo sulla strada più breve verso una data destinazione.

2.4 RPF con "potatura" (RPF and prunes)

Questa variante dell'algoritmo RPF prevede che l'albero multicast sia *potato* di tutti i rami a cui non è attestato alcun fruitore interessato alle trasmissioni del gruppo multicast.

Nel caso, ad esempio, di una trasmissione multicast, generata da una sorgente "S" e destinata a un gruppo multicast "G", i nodi foglia senza membri del gruppo "G" possono inviare uno speciale messaggio di potatura (*prune*) al router multicast a monte. Quando questo messaggio è ricevuto attraverso l'interfaccia "I", il router a monte è informato che non deve inoltrare ulteriore traffico multicast generato da S e destinato a G attraverso l'interfaccia I, perché a valle non sono presenti fruitori interessati a questo traffico. In figura 8 è schematizzato il meccanismo del *pruning*.

Con questo meccanismo, partendo dalle foglie e ripercorrendo l'albero verso la radice, sono potati i rami sui quali è inutile inoltrare traffico.

L'algoritmo RPF introduce così il concetto di appartenenza ai gruppi e richiede che i router tengano traccia dello stato dell'albero per gruppo e per sorgente.

Per il corretto funzionamento del sistema deve essere aggiornato periodicamente lo stato dell'albero, per mantenerlo coerente con i gruppi multi-

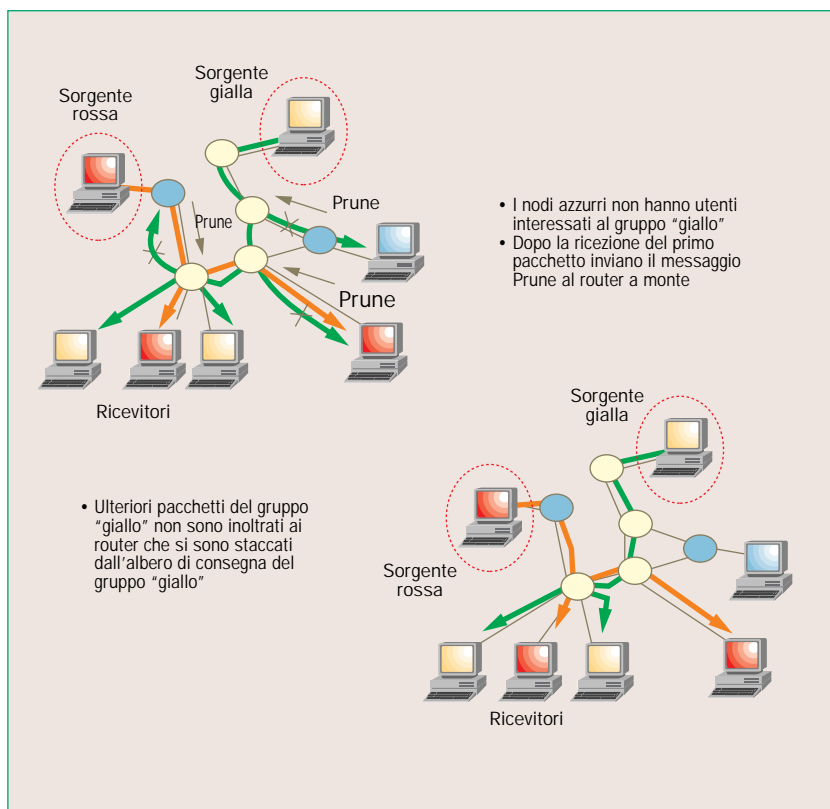


Figura 8 Schema del meccanismo di Pruning.

cast in rete.

Questo algoritmo prevede infatti che con una frequenza determinata un pacchetto multicast di G sia inoltrato sull'intera rete, fino alle foglie dell'albero, in modo da ripetere periodicamente l'operazione di "potatura dell'albero".

Nelle reti geografiche di grandi dimensioni, con un numero limitato di potenziali ricevitori multicast rispetto al numero totale di utenti collegati, il meccanismo delle inondazioni e delle potature periodiche e la necessità di mantenere traccia dello stato nei router della rete potrebbe introdurre una condizione di inutile sovraccarico sia nei nodi della rete sia nei collegamenti: infatti, anche in assenza di ricevitori interessati a trasmissioni multicast, la rete è periodicamente interessata dal traffico dati e da quello di segnalazione di tutti i gruppi multicast attivi.

2.5 Shortest Path Tree

L'algoritmo *Shortest Path Tree* individua il cammino più breve tra la sorgente (*radice dell'albero*) e ognuno dei ricevitori (*le foglie dell'albero*) senza ottimizzare il costo totale dell'albero, in termini di impiego di collegamenti. I due più noti algoritmi utilizzati sono quello di Bellman-Ford¹ e quello di Dijkstra².

2.6 Steiner Tree

L'albero di Steiner [10] è quello che rende minimo il numero di collegamenti utilizzati per connettere i membri di un gruppo all'interno di un grafo. Questo approccio comporta un degrado delle presta-

zioni nella consegna dei dati, in quanto i cammini prescelti, realizzando la massima condivisione delle connessioni, non sono quelli ottimi in termini di distanza dalla sorgente ai ricevitori.

3. Protocolli di instradamento multicast nelle reti IP

Con il termine *protocollo di instradamento multicast* si indica sia l'*algoritmo di instradamento* sia il *protocollo* impiegato per mantenere aggiornate le informazioni che l'algoritmo richiede per un suo corretto funzionamento.

Le tecniche più importanti su cui si basano i protocolli di routing multicast per la costruzione degli alberi di distribuzione del traffico multicast sono catalogabili in due classi:

- la *tecnica SBT (Source-Based Tree)* ha come obiettivo la costruzione di alberi di distribuzione da ogni sorgente verso l'insieme completo dei ricevitori di un gruppo multicast. La tecnica determina la realizzazione di tanti alberi quante sono le sor-

genti di traffico multicast. La costruzione di ogni albero avviene seguendo la strada più breve tra sorgente e destinazioni del traffico. La critica mossa a queste tecniche è la loro scarsa scalabilità; diventano infatti assai poco efficaci quando è presente un numero elevato di sorgenti e soprattutto quando i ricevitori risultano dispersi su molte reti diverse. *DVMRP (Distance Vector Multicast Routing Protocol)* [3] e *PIM-DM (Protocol Independent Multicast - Dense Mode)* [11] sono due esempi di protocolli multicast che appartengono a questa categoria.

- la *tecnica Shared-Tree* è stata sviluppata con l'obiettivo di superare le limitazioni della tecnica *Source-Based Tree*. Essa è anche chiamata *core-based* in quanto prevede la costruzione di un unico albero di distribuzione multicast intorno a un router (o a più di uno) chiamato *core* o *RP (Rendez-vous Point)*. Per ogni gruppo multicast viene individuato un *core router* che opera come punto di raccolta dei flussi multicast generati dai diversi trasmettitori e come radice dell'albero di distribuzione verso tutti

⁽¹⁾ L'algoritmo Bellman-Ford è utilizzato dai protocolli di tipo "distance-vector" ed è definito in R. E. Bellman "Dynamic Programming", Princeton University Press, Princeton N. J., 1957.

⁽²⁾ L'algoritmo Shortest Path First è utilizzato dai protocolli di tipo "link state" ed è definito da E. W. Dijkstra nel suo lavoro "A Note on Two Problems in Connection with Graphs", pubblicato in *Numerische Matematica*, vol. 1, pp. 269-271, 1959.

i ricevitori. Questa tecnica risulta sicuramente più scalabile ma presenta alcune limitazioni, che si manifestano in particolare per la concentrazione del traffico verso il *core router* (con evidenti rischi di congestione) e per la possibilità di costituire percorsi di instradamento non ottimizzati. *CBT (Core Based Trees)* e *PIM-SM (Protocol Independent Multicast - Sparse Mode)* [12] sono due esempi di protocolli multicast appartenenti a questa categoria.

Accanto a questa classificazione di tipo generale, i protocolli di *routing multicast* possono ulteriormente essere distinti in protocolli intra e interdominio, in analogia a quelli unicast [1] e in protocolli che operano con modalità *dense* e protocolli che operano con modalità *sparse*.

I *protocolli dense-mode* impiegano strategie basate su inondazioni e potature periodiche. Questi protocolli non sono consigliabili per le reti geografiche, per l'elevato carico del traffico "di segnalazione" introdotto, ma sono adatti a contesti caratterizzati da un'alta concentrazione di utenti multicast. DVMRP e PIM-DM sono due esempi di protocolli multicast che operano in modalità *dense*.

I *protocolli sparse-mode* si basano viceversa su strategie di adesione esplicita, e rendono così minimo il traffico "di segnalazione". Risultano perciò indicati per le reti geografiche e più in generale per quei contesti in cui la densità di utenza multicast è bassa. CBT e PIM-SM sono due esempi di protocolli multicast che operano in modalità *sparse*.

Occorre infine segnalare che i protocolli di routing multicast utilizzano informazioni di routing unicast per costruire gli alberi di distribuzione del traffico multicast. A tal proposito i diversi protocolli di routing multicast si differenziano tra quelli che utilizzano le informazioni di instradamento unicast generate da altri protocolli (OSPF, RIP, routing statico) - come ad esempio PIM-DM e PIM-SM - e quelli che costruiscono le proprie tabelle di instradamento unicast, disaccoppiate da quelle realmente utilizzate per instradare il traffico unicast, come DVMRP.

Di seguito sono descritti sinteticamente i principali protocolli utilizzati in Internet, rimandando agli standard di riferimento citati per ulteriori approfondimenti.

3.1 Protocolli per l'instradamento multicast intra-dominio

- *Distance Vector Multicast Routing Protocol*

Il DVMRP (*Distance Vector Multicast Routing Protocol*) [3] è un protocollo di routing multicast che utilizza l'algoritmo RPF con potatura descritto nel paragrafo precedente ed è stato utilizzato nella rete sperimentale MBONE, il primo backbone multicast di Internet descritto nel paragrafo 4.1.

Per il corretto funzionamento dell'algoritmo, il protocollo prevede la costruzione e l'aggiornamento di una tabella di instradamento multicast, contenente per ciascuna rete sorgente l'interfaccia di ingresso del traffico.

Il protocollo prevede che i nodi adiacenti della rete si scambino periodicamente l'intero contenuto delle tabelle di instradamento, in modo da aggiornarle in base alle differenze riscontrate (*modalità distance vector*). Insieme alle informazioni di instradamento, i nodi della rete si scambiano anche informazioni sui gruppi.

Lo scambio delle informazioni tra i router avviene utilizzando il protocollo IGMP: i pacchetti scambiati sono costituiti da un'intestazione IGMP (primi 32 bit del pacchetto mostrato in figura 7), in cui il valore del campo *tipo* è posto a 4, e da una sequenza di dati strutturati. Questi ultimi dati sono chiamati comandi e sono costituiti da un identificatore del tipo di comando e da un campo informativo. Per maggiori particolari si rimanda alla bibliografia [3].

L'algoritmo utilizzato da DVMRP definisce un albero di consegna diverso per ciascuna coppia S, G (Sorgente-Gruppo). Ogni router multicast DVMRP determina la propria posizione all'interno di ciascun albero, in modo da stabilire su quali delle sue interfacce deve inoltrare i traffici multicast.

Il *processo di potatura* avviene in seguito allo scambio di informazioni tra i router a partire dai nodi più periferici dell'albero. Il protocollo prevede che periodicamente sia verificata la presenza dei membri dei gruppi multicast, in modo da eliminare i rami superflui e da ottenere per ciascun gruppo multicast il corrispondente albero minimo: periodicamente le interfacce escluse sono nuovamente inserite nell'albero multicast, al fine di verificare l'esistenza di nuovi membri e per aggiornare quindi l'albero. Se non si sono presentate variazioni nel gruppo, si procede a una nuova fase di potatura (inondazioni e potature periodiche).

Per consentire l'introduzione di soluzioni di rete multicast anche su piattaforme di rete che non utilizzano il multicast nei nodi, il DVMRP prevede l'impiego della tecnica di tunneling: con questa tecnica i router multicast possono scambiare traffico dati e di segnalazione multicast, incapsulandolo nel traffico IP unicast (secondo la tecnica del *tunneling* descritta in figura 10: i pacchetti IP multicast, cioè il traffico incapsulato, sono il carico utile, il *payload*, di pacchetti IP unicast, cioè il traffico incapsulante).

Gli aspetti critici di questo protocollo sono quelli tipici dei protocolli *distance-vector*, e cioè il carico di elaborazione e di traffico conseguente al traffico di segnalazione (sia per lo scambio periodico delle tabelle di instradamento sia per le inondazioni e potature periodiche), che ne sconsiglia l'impiego nelle reti geografiche di grandi dimensioni.

- *Protocol Independent Multicast*

Il PIM (*Protocol Independent Multicast*) [11] [12], a differenza del DVMRP, ipotizza che i percorsi tra sorgente e destinazione siano simmetrici e utilizza perciò le informazioni contenute nella tabella di instradamento unicast per consentire il funzionamento dell'algoritmo di instradamento multicast.

Il PIM può operare in due diversi modi: *DM (Dense Mode)* e *SM (Sparse Mode)*. Il primo approccio ricalca quanto si è già visto per il DVMRP.

Il secondo schema è particolarmente indicato nei casi in cui la concentrazione di utenti multicast è bassa.

Dense Mode

Il PIM-DM (*Protocol Independent Multicast-Dense Mode*) [11] utilizza l'algoritmo RPM (*Reverse Path Multicasting*) quale tecnica per la costruzione di alberi. Nel RPM un datagramma multicast è inoltrato solo se

proviene dall'interfaccia abitualmente utilizzata dal nodo per raggiungere la sorgente dei dati.

Quando un multicast router riceve il primo datagramma multicast da una determinata sorgente, ipotizza che tutti i nodi a valle siano interessati a ricevere quei dati e inoltra i datagrammi su tutti i propri link, ad eccezione di quello d'arrivo (*default to send*). In aree della rete in cui non sono presenti membri del gruppo, si ricorre al pruning per eliminare rami inutili dell'albero multicast. Nel caso opposto i datagrammi successivi sono ancora inoltrati sull'interfaccia non in *pruning state*. Ogni router deve conoscere la propria posizione all'interno dell'albero: infatti i nodi foglia devono monitorare mediante messaggi IGMP la presenza di membri per ogni gruppo, in modo da gestire il pruning delle interfacce; le informazioni di pruning sono poi propagate a monte.

Si può notare come l'approccio seguito sia assolutamente indipendente dal protocollo di routing unicast, il che porta inevitabilmente ad alcune inefficienze. Ad esempio, il PIM-DM accetta l'eventuale duplicazione di datagrammi pur di non legarsi a un particolare protocollo di routing e di non gestire la base di dati riguardante la relazione tra padre e figlio nell'albero (come in DVMRP).

Altre caratteristiche di PIM-DM riguardano l'introduzione di particolari tecniche di pruning per evitare la duplicazione di pacchetti in *LAN multi-accesso*, di schemi che permettono di diminuire il tempo di ritardo per l'inclusione nell'albero multicast di link che avevano precedentemente subito il *pruning* ed infine di un meccanismo di monitoraggio dei nodi foglia al fine di accelerare il *pruning*.

Sparse Mode

L'introduzione del PIM-SM (*Protocol Independent Multicast- Sparse Mode*) [12] è stata indirizzata a permettere una distribuzione dei dati multicast che coinvolga il minor numero possibile di router. Per ottenere questo risultato è necessario che i router che servono membri facenti parte di un gruppo dichiarino esplicitamente l'adesione al multicast. L'approccio quindi è opposto a quello degli schemi *dense mode*, in cui l'inoltro dei datagrammi multicast avveniva per *default* su tutte le interfacce e i router dovevano utilizzare il *pruning* delle connessioni non interessate al multicast.

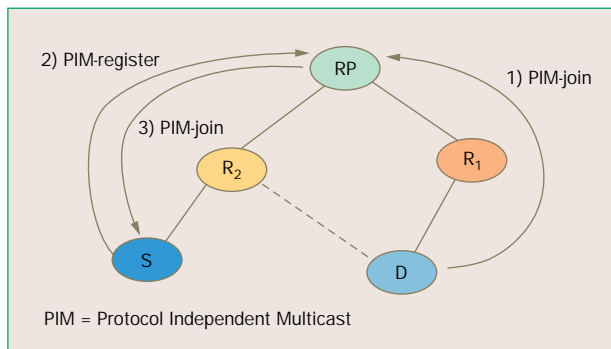


Figura 9 Esempio di funzionamento di PIM-SM.

Il PIM-SM provvede ad associare ogni gruppo a un RP (*Rendezvous Point*), cioè a un router che risulta essere il punto d'incontro tra sorgenti e destinatari. Le sorgenti devono, infatti, notificare al RP la propria presenza in modo che le destinazioni possano esserne messe a conoscenza.

A differenza del DVMRP, PIM-SM non richiede di inondare periodicamente la rete.

In figura 9 è mostrato un esempio di funzionamento di PIM-SM: quando un host vuole unirsi a un gruppo multicast (G) invia al multicast router la richiesta. Il router PIM più vicino (D) riceve la richiesta e trasmette al RP relativo al gruppo, un messaggio *PIM-join*. Il messaggio è elaborato dai nodi intermedi (ad esempio R1) che costruiscono così il percorso da RP al nuovo destinatario. Nelle tabelle di routing multicast dei router lungo il percorso da RP al nodo destinatario compare l'informazione di stato (*,G).

Quando una sorgente comincia a trasmettere dati al gruppo, il PIM-router designato (S) trasmette un messaggio *PIM-register* (unicast) a RP e incapsula il datagramma multicast. RP risponde con un messaggio *PIM-join* che, intercettato dai router intermedi (R2), serve a instaurare una connessione dalla sorgente verso RP. Nelle tabelle di routing multicast dei router lungo il *path* da RP al nodo sorgente compare l'informazione di stato (S,G).

Nel momento in cui a RP arriva il primo pacchetto multicast nativo (non incapsulato) proveniente dalla sorgente, RP invia un messaggio di *PIM-register-stop* al router S.

Nel caso in cui il ricevitore richieda l'instradamento *source-based tree* (del tipo *shortest path*), il router D, a questo punto, dovrebbe trasmettere un secondo messaggio *PIM-join* verso la sorgente: quando il primo datagramma multicast viene ricevuto dal nuovo percorso (S-R2-D), il router D deve inviare un messaggio *PIM-prune* a RP, in modo da eliminare dall'albero (*shared*) i collegamenti inutili e da evitare la ricezione di datagrammi duplicati.

Può presentarsi l'eventualità che datagrammi multicast arrivino a un router che non ne conosce l'RP oppure che non ha nessuna *entry* per quel gruppo: in questo caso i dati sono trasmessi dal router con modalità *dense mode*. Se invece il *multicast group* è sparso su una wide area ed è noto l'RP associato, sia i messaggi di controllo di PIM che i dati viaggiano sulla connessione in *sparse mode*.

Caratteristiche generali

Un importante obiettivo perseguito dal PIM è la robustezza del protocollo nei confronti della perdita di messaggi di controllo e dei potenziali *point-of-failure*.

- *robustezza del protocollo*: la perdita di un messaggio *PIM-register* non provoca alcun danno, in quanto i datagrammi multicast continuano a essere incapsulati nei messaggi successivi finché non viene ricevuto il *PIM-join*. In caso di mancata ricezione del *PIM-join*, il router continua a trasmettere dati sul vecchio percorso, finché, scattato un *time-out*, il messaggio è ritrasmesso e quindi è ricevuto correttamente.

- **affidabilità:** per evitare la perdita di messaggi dovuta alla presenza di singoli *point-of-failure*, gli RP sono duplicati in ogni gruppo. È però necessario che ogni sorgente notifichi la propria attività a tutti gli RP del gruppo, anche se le destinazioni restano comunque associate all'RP più vicino. I ricevitori controllano la raggiungibilità degli RP restando in ascolto dei messaggi *RP-reachability* che gli RP inviano periodicamente. Allo scadere di un *time-out*, durante il quale non è stato ricevuto alcun messaggio di raggiungibilità, il router cerca un RP del gruppo alternativo e, una volta trovato, gli invia il messaggio *PIM-join* e quindi si unisce all'albero di instradamento associato al nuovo RP.
- **interoperabilità con reti non-PIM:** l'interoperabilità con reti non-PIM è piuttosto complessa nel caso di modalità di invio *sparse mode*. Contrariamente a tutti gli altri protocolli multicast, nel PIM-SM le destinazioni richiedono esplicitamente una connessione all'albero di instradamento. È quindi necessario predisporre un router di confine in grado di gestire la transizione tra le due diverse modalità di funzionamento. Nel caso, infatti, in cui sorgenti o destinazioni di dati multicast siano nella rete non-PIM, il router di confine deve effettuare correttamente la trasmissione e la ricezione dei messaggi *PIM-join* e *PIM-register* da e verso RP.

3.2 Protocolli per l'instradamento multicast inter-dominio

In questo paragrafo sono approfonditi i problemi e l'applicabilità dei protocolli di routing multicast in una rete come Internet, organizzata secondo la gerarchia dei *sistemi autonomi* e gestita da diversi *ISP (Internet Service Provider) competitor*.

Per *dominio* si intende, generalmente, un insieme di router sui quali è attivo lo stesso protocollo di instradamento (politica di indirizzamento e di instradamento). Accanto al concetto di dominio in Internet si è quindi sviluppato il concetto di *sistema autonomo* con il quale si indica l'insieme di uno o più domini appartenenti a un singolo controllo amministrativo. La rete Internet è, ad esempio, un insieme di sistemi autonomi. I router all'interno di ciascun sistema autonomo interagiscono tra loro con *protocolli di routing definiti intra-dominio*. Router appartenenti a sistemi autonomi separati interagiscono mediante *protocolli di routing inter-dominio*.

I protocolli di instradamento multicast analizzati nei paragrafi precedenti quali DVMRP, PIM e CBT sono applicabili solo in un contesto intra-dominio. DVMRP, con il suo meccanismo di *flooding and pruning*, non è certamente adatto a una rete IP multicast estesa su un'area geografica e con molti gruppi multicast i cui membri possono essere poco numerosi e molto distanti (in termini di *hop*) tra loro. PIM-DM presenta caratteristiche simili a DVMRP. I protocolli del tipo *core-based* quali PIM-SM e CBT hanno problemi nell'ubicazione ottimale del RP (o *core router*).

Vari gruppi dell'*IETF (Internet Engineering Task Force)* si sono quindi dedicati alla ricerca di una nuova soluzione. Di seguito si presentano le due "architet-

ture" principali così individuate per realizzare IP multicast nativo su Internet secondo il modello tradizionale (molti a molti).

La prima soluzione si fonda sui protocolli *MBGP (Multiprotocol Border Gateway Protocol)* [13], *MSDP (Multicast Source Discovery Protocol)* [14] e *PIM-SM*. Questa soluzione è oggi adottata dai gestori delle principali reti di ricerca internazionali e da alcuni ISP.

La seconda soluzione - assai più complessa da realizzare - si fonda sui protocolli *BGMP (Border Gateway Multicast Protocol)* [15] e *MASC (Multicast Address-Set Claim)* [16] ed è ancora oggetto di studio in ambito IETF. Queste soluzioni non sono ancora disponibili in commercio.

Di seguito è riportata la descrizione dell'architettura MBGP/MSDP/PIM-SM (per la descrizione delle soluzioni BGMP e MASC si rimanda al riquadro di approfondimento riportato a pagina 72).

Architettura MBGP/MSDP/PIM-SM

L'architettura si basa su un insieme di protocolli che svolgono funzioni distinte:

- PIM-SM il *multicast forwarding* e la costruzione degli alberi di distribuzione multicast inter-dominio;
- MSDP il *discovery* di sorgenti appartenenti a domini o *autonomous system* disgiunti;
- MBGP il protocollo di *routing inter-domain* per sorgenti multicast.

Si ipotizza che nei diversi domini il protocollo di *routing multicast intra-domain* sia quello PIM-SM. In ciascun dominio si definiscono uno (nel caso in cui si opti per la soluzione di RP statico) o più RP (quando si scelga anycast RP [17] o meccanismi di RP dinamico).

Si assume che ciascun dominio PIM-SM usi i propri RP e che non dipenda quindi da RP localizzati in altri domini. Una sorgente cioè che faccia parte di un dato dominio trasmette a un gruppo multicast il cui RP appartiene allo stesso dominio.

MSDP è il protocollo mediante il quale gli RP appartenenti a domini PIM-SM disgiunti si scambiano informazioni relative all'esistenza di sorgenti attive. Il principio di funzionamento è riportato nel riquadro di pagina 73.

MBGP (o BGP4+) è un'estensione del ben noto protocollo di *routing unicast inter-domain* BGP4 [18]: grazie a questa estensione, sulla medesima sessione BGP4 transitano le informazioni di routing valide sia per il traffico unicast che per quello multicast. Perché un protocollo multicast come PIM operi correttamente, esso deve infatti disporre dell'informazione che gli consenta di raggiungere - via unicast - la sorgente multicast. PIM esegue infatti il controllo *RPF (Reverse Path Forwarding)*: accetta come valido un pacchetto multicast che riceve su una certa interfaccia quando è disponibile una rotta unicast verso la sorgente multicast attraverso la suddetta interfaccia. Se il controllo RPF dà esito positivo il pacchetto è distribuito (replicato), altrimenti esso è scartato.

Il protocollo MBGP permette tra l'altro di usare

Architettura con i protocolli BGMP e MASC

BGMP (*Border Gateway Multicast Protocol*) è il protocollo di *multicast routing* e *multicast forwarding*; **MASC** (*Multicast Address Set Claim*) è il protocollo di allocazione dinamica degli indirizzi multicast.

Le caratteristiche su cui è basato BGMP sono stati tratti da protocolli esistenti quali **CBT** (*Core Based Trees*) e **PIM-SM**. La principale innovazione riguarda gli alberi di distribuzione in BGMP che sono alberi di domini più che di router. Il protocollo BGMP richiede poi che ciascun gruppo multicast globale sia associato a un unico *root domain*. BGMP, come PIM-SM, costruisce due tipi di alberi: *condivisi* (bidirezionali) e *source-based* (mono-direzionali).

A ogni dominio è assegnata una lista di indirizzi di gruppo globali. Ciascun dominio deve essere *root domain* per tutti gli alberi condivisi, relativi ai gruppi in esso allocati. Il meccanismo di assegnazione degli indirizzi a ciascun dominio è realizzato dal protocollo MASC.

Ciascun router BGMP di un dominio inoltra a quelli corrispondenti (*peer BGMP*) di domini adiacenti, i prefissi degli indirizzi di gruppo assegnati. Quando un ricevitore di un certo dominio si iscrive a un gruppo il router BGMP del dominio invia una richiesta di *join* verso il router BGMP del *root domain* per quel gruppo.

BGMP si basa su un protocollo **EGP** (*Exterior Gateway Protocol*) capace di trasportare anche prefissi multicast (ad esempio MBGP). Un router BGMP deve infatti consentire di inoltrare pacchetti dati e di controllo al *next hop router* sia verso la sorgente sia verso l'indirizzo di gruppo (che, come si è già accennato in precedenza, è associato a un *root domain*).

BGMP interopera con tutti i protocolli di routing IP multicast intra-dominio.

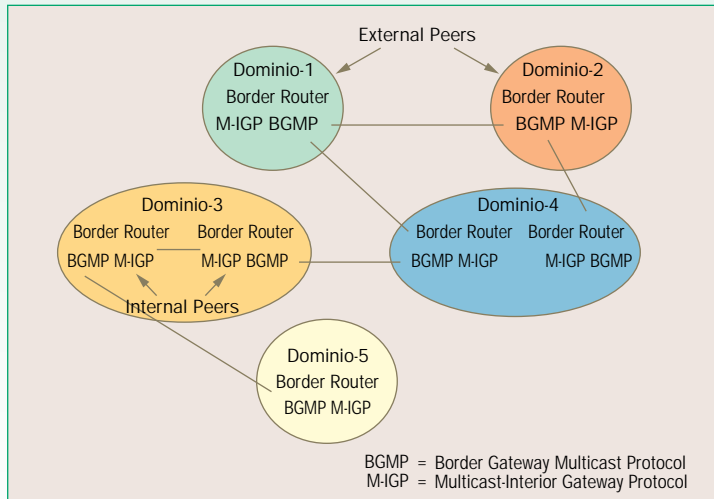


Figura A Architettura del protocollo BGMP (*Border Gateway Multicast Protocol*).

Nella figura A sono riportati gli elementi principali della architettura BGMP. In particolare sono indicati i domini o sistemi autonomi disgiunti e i router di frontiera (i *border router*) con due componenti: 1) BGMP e 2) **M-IGP** (*Multicast Interior Gateway Protocol*), che può essere uno qualunque fra DVMRP, PIM-DM, PIM-SM o CBT.

Due router di frontiera adiacenti sono detti corrispondenti esterni (*external peer*) se appartengono a due domini disgiunti, corrispondenti interni (*internal peer*) se operano nello stesso dominio.

topologie e politiche di instradamento distinte per il traffico unicast e multicast (come richiesto da molti gestori). Costruire infatti rotte distinte per il traffico può costituire un ausilio per ottimizzare le risorse di rete e ancor più per non immettere flussi multicast sulle rotte di traffico normalmente destinate alle applicazioni unicast tradizionali.

I vantaggi di questa architettura per un ISP sono evidenti: con MBGP si utilizza di fatto un protocollo di routing che già gli ISP conoscono e

che impiegano per il routing unicast. MSDP permette a ogni ISP di avere i propri RP e di non dover utilizzare, per le sorgenti attive nel proprio dominio, RP di competitor.

Questa soluzione, anche se considerata temporanea - perché non dà garanzie in termini di modularità - è ormai assai diffusa perché funzionale e relativamente semplice. A dicembre dello scorso anno, 321 sistemi autonomi annunciavano anche rotte relative a sorgenti multicast.

Principio di funzionamento del protocollo MSDP (Multicast Source Discovery Protocol)

Il meccanismo base di funzionamento di MSDP è mostrato nella figura A:

- 1) Un RP di un dominio PIM-SM stabilisce una sessione di corrispondenza diretta (*peering MSDP*) con gli RP dei domini PIM-SM adiacenti.
- 2) Quando una nuova sorgente IP multicast diventa attiva, essa si registra presso l'RP esistente nel proprio dominio. Quest'operazione prevede che il PIM Designated Router, cui è connessa la sorgente, invii i pacchetti multicast incapsulati in messaggi di tipo PIM register all'RP.
- 3) L'RP, che svolge funzioni di MSDP peer all'interno del dominio della sorgente, costruisce un messaggio *source active* e lo inoltra a tutti i *peer MSDP* connessi direttamente. Il messaggio SA contiene i seguenti campi:
 - indirizzo IP della sorgente;
 - gruppo cui la sorgente indirizza il traffico multicast;
 - indirizzo IP dell'RP.
- 4) Ciascun *MSDP peer*, che riceve un messaggio SA, esegue un *peer-RPF check*: verifica infatti se il messaggio *source active* è ricevuto sull'interfaccia corretta, cioè su quella utilizzata per raggiungere in *unicast* (sulla base della tabella di *routing BGP*) il peer MSDP che ha generato *source active*. I controlli RPF sono necessari per evitare eventuali situazioni di funzionamento in loop.
- 5) Se il messaggio *source active* è ricevuto sull'interfaccia corretta, il messaggio è inoltrato a tutti i *peer MSDP*, a eccezione di quello che ha ricevuto il messaggio (*peer RPF flooding*).
- 6) Ciascun *MSDP peer*, che, come è stato già detto, svolge anche funzioni di RP, verifica la presenza di qualche ricevitore per quel gruppo all'interno del suo dominio. In caso affermativo l'RP invia un messaggio di tipo PIM *join* verso l'indirizzo della sorgente, noto mediante il messaggio SA.

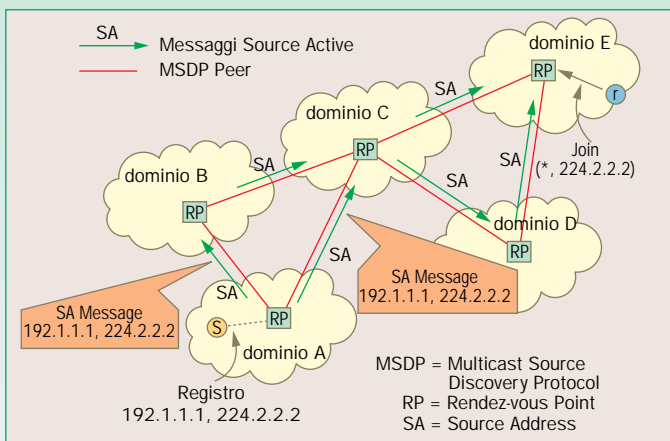


Figura A Il protocollo MSDP (Multicast Source Discovery Protocol).

4. Offerta di servizi

4.1 L'esperienza MBONE (Multicast backBONE)

Per anni IP multicast su Internet è coinciso con la rete MBONE: era costituito, come è mostrato in figura 10, da un backbone IP multicast sovrapposto a Internet basato su un insieme di domini DVMRP interconnessi attraverso dei tunnel (tunnel DVMRP definiti tra multicast router su cui è attivo il software che implementa il protocollo di router multicast, chiamato demone *mrouted*).

Su questa piattaforma sperimentale sono state provate le prime applicazioni multicast di audio-video conferenza basate sui protocolli di trasporto per traffico in tempo reale (ad esempio RTP [19], RTCP [20]). Tra queste applicazioni, note ancora oggi come applicazioni MBONE, possono essere ricordate quelle *VIC* (*Video Conferencing tool*), *VAT* (*Visual Audio Tool*), *SDR* (*Session Directory*): nate su piattaforma UNIX, queste applicazioni sono oggi disponibili per qualsiasi sistema operativo (<http://www-nrg.ee.lbl.gov/>).

Gli utilizzatori di MBONE erano per lo più ricercatori e l'interesse era rivolto quasi esclusivamente allo sviluppo di applicazioni e protocolli; IP multicast su MBONE non era visto come un servizio.

Nel momento in cui il numero dei siti connessi è

cresciuto, e con esso è aumentato il numero delle sorgenti, l'infrastruttura di MBONE si è rivelata inadeguata. L'interesse sempre crescente verso applicazioni audio e video e la convinzione che IP multicast è una tecnologia indispensabile come supporto di queste applicazioni, ha spinto la comunità scientifica internazionale (e non solo) verso nuove soluzioni sia per i protocolli sia anche per le applicazioni.

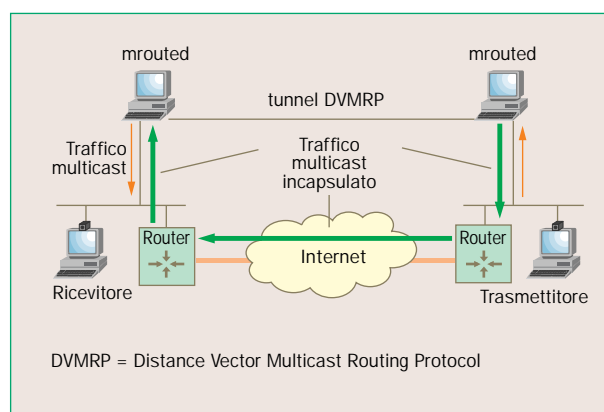


Figura 10 L'impiego dei tunnel in MBONE.

Quella che era la MBONE originaria è oggi un *sistema autonomo* (con numero di AS 10888) della rete IP multicast su Internet (che molti chiamano ancora MBONE) basato sull'architettura MBGP; MSDP; PIM-SM. IP multicast su Internet, da un punto di vista dei protocolli di routing, si è quindi evoluta da rete virtuale sovrapposta a Internet a rete di tipo gerarchica su cui IP multicast è abilitato con una modalità nativa.

A dicembre dello scorso anno, come è stato già accennato, erano 321 i sistemi autonomi in servizio con capacità di instradamento multicast.

Quasi tutti i più noti sistemi applicativi commerciali di audio e di video conferenza; e di audio e video streaming (ad esempio Cisco IP/TV, Microsoft Windows Media Services, Real Audio/Real Video, QuickTime) sono in grado oggi di gestire IP multicast.

4.2 La gestione degli indirizzi multicast

Nella definizione del servizio multicast, e in particolare lato sorgente, un aspetto non marginale riguarda l'assegnazione degli indirizzi IP multicast, ossia degli identificativi dei gruppi multicast.

Allo stato dell'arte sono ipotizzabili due alternative: l'assegnazione dinamica o quella statica. Per chiarire le differenza tra i due tipi di assegnazione

possono essere presentati due esempi tipici.

Nel caso in cui su MBONE è prevista l'*assegnazione dinamica* degli indirizzi IP multicast, ogni sorgente, prima di avviare l'invio del traffico, individua le trasmissioni già attive e quindi si appropria di un indirizzo IP multicast non ancora utilizzato. Per queste funzioni è stato sviluppato uno specifico protocollo *SDP (Session Description Protocol)* [21].

La soluzione funziona se ciascuna sorgente è in grado di rilevare tutti gli indirizzi impegnati e non si impossessa, né per errore né in modo fraudolento, di indirizzi già utilizzati: trasmissioni differenti che impiegano lo stesso indirizzo multicast possono infatti essere distruttive. Questo aspetto ha un impatto diretto sulla sicurezza e sull'integrità delle informazioni. Nel riquadro sotto riportato è descritto un ulteriore meccanismo per l'allocazione dinamica degli indirizzi multicast.

In alternativa, gli indirizzi multicast possono essere *assegnati staticamente*, come ad esempio avviene per il servizio UUCAST offerto da UUNET. In questo caso all'atto della stipula del contratto il cliente indica a UUNET il numero di flussi che saranno trasmessi in rete e di conseguenza sono assegnati altrettanti indirizzi IP multicast.

Soluzioni statiche sono in genere utilizzate dai provider che *non intendono* integrare la propria rete

MALLOC

Un ulteriore meccanismo per l'allocazione dinamica degli indirizzi multicast è quello proposto dal Gruppo di Lavoro IETF *MALLOC* (*Multicast Address aLLOcation*) [22] mostrato nella figura A. L'architettura proposta dal gruppo MALLOC è realizzata su più livelli e propone un protocollo distinto per ciascuno strato:

- *Protocollo di allocazione di indirizzi IP Multicast Host-Server: MADCAP (Multicast Address Dynamic Client Allocation Protocol)* [23]. È impiegato da un host per chiedere un indirizzo multicast a un *allocation server* (MAAS) locale.
- *Protocollo di allocazione di indirizzi IP Multicast intra-domain: AAP (Address Allocation Protocol)* [24]. È utilizzato dagli *allocation server* (MAAS) di un dominio per evitare conflitti di indirizzi all'interno dello stesso dominio. I MAAS allocano un indirizzo multicast per i propri utilizzatori (*client*) e comuni-

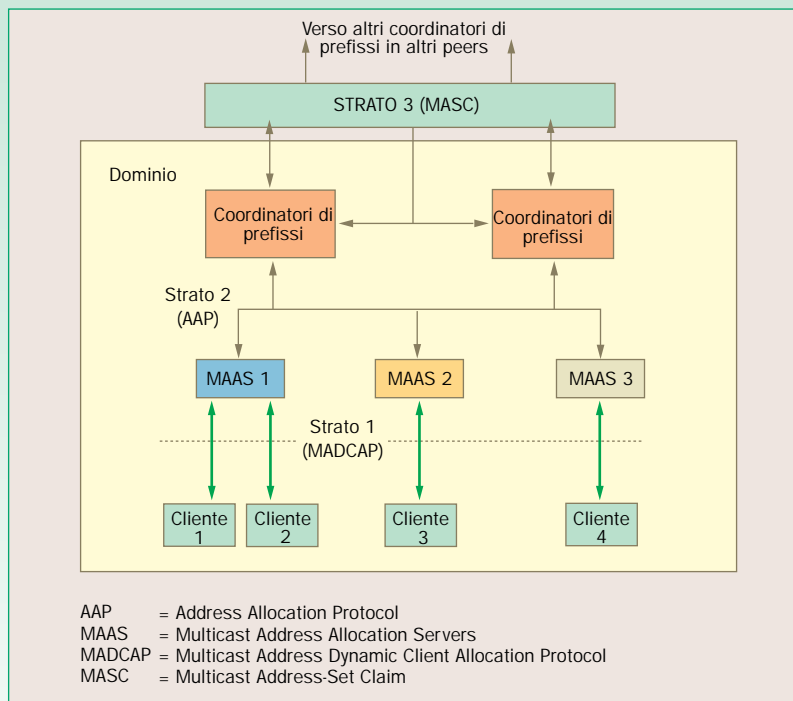


Figura A Architettura Multicast Allocation.

cano agli altri MAAS l'indirizzo perché non venga riutilizzato.

- *Protocollo di allocazione di indirizzi IP Multicast inter-domain: MASC (Multicast Address-Set*

Claim) [28]. Consente ai domini di richiedere blocchi di indirizzi da assegnare ai MAAS. È un protocollo tra router di tipo gerarchico e generalmente lo si accoppia a BGMP.

multicast con MBONE e che vogliono offrire soluzioni di servizio orientate alla clientela affari. MBONE è stata infatti finora prevalentemente indirizzata al mondo accademico.

La soluzione statica è semplice e sicura: con filtri di traffico sull'interfaccia di accesso della sorgente si possono infatti evitare interferenze per errore o fraudolente con altre trasmissioni multicast.

4.3 Accounting e conditional access

Non sono previste per il momento specifiche funzioni di rete a supporto della tassazione (*accounting*) delle trasmissioni multicast o in grado di limitare la fruizione delle trasmissioni multicast da parte dei clienti finali.

Per limitare l'adesione ai gruppi e per contabilizzare (*accounting*) la fruizione delle trasmissioni multicast si ricorre in genere a soluzioni applicative, che prevedono l'accesso a server in cui è immagazzinato il palinsesto e in cui è presente l'accesso condizionato su base *username* e *password* (ad esempio quello IP-TV di Cisco).

Nell'architettura standard non sono impiegati strumenti di rete efficaci che consentano di limitare la fruizione delle informazioni (ad esempio *conditional access*). Per l'offerta dei servizi bisogna quindi far leva su soluzioni a livello applicativo.

4.4 Soluzioni e modelli alternativi

Il modello IP multicast tradizionale è assai complesso da realizzare e presenta una serie di problemi da esaminare e risolvere che ne hanno rallentato la diffusione come base tecnologica per la commercializzazione di nuovi servizi. In particolare gli ISP [25] temono che l'abilitazione del servizio IP multicast possa provocare parecchie criticità in una rete sin qui pensata, dimensionata e modellata per il servizio unicast.

L'incremento del traffico sui collegamenti, l'impatto del servizio IP multicast sulle risorse di memoria ed elaborative degli apparati di accesso e di backbone, l'impatto dei protocolli di routing multicast sui protocolli unicast, l'aggiornamento di meccanismi di controllo e di tariffazione sono solo alcune possibili criticità che un ISP deve considerare.

Sono quindi apparse sul mercato nuove soluzioni e alcune proposte di semplificazione che rispondono alle numerose richieste, in particolare di applicazioni di audio e video diffusivo (broadcasting) o di media-streaming.

In particolare si assiste all'incontro (o forse allo scontro) di due diversi orientamenti: soluzioni di rete (livello 3 della pila OSI) e soluzioni applicative (livelli 4-7).

Si sottolinea tuttavia che un'eventuale soluzione applicativa non è necessariamente un'alternativa a una soluzione di rete; anzi, se opportunamente integrata con un progetto di rete, un'applicazione con "architettura gerarchica" può ottimizzare le risorse di rete e può così consentire di fornire un servizio migliore ai clienti.

Soluzione di rete: Source Specific Multicast

La SSM (*Source Specific Multicast*) [26] rappresenta un nuovo modello di IP multicast adatto ad

applicazioni da uno ovvero da pochi a molti, quali il servizio video diffusivo. Rispetto al modello tradizionale multi-a-molti questo paradigma presenta alcune semplificazioni poiché non richiede meccanismi di allocazione dinamica degli indirizzi e protocolli di *source discovery*.

Un ricevitore oltre all'indirizzo di gruppo deve specificare l'indirizzo delle sorgenti. IGMPv3 [27] è l'evoluzione del protocollo multicast host-router definito in IETF per realizzare queste funzionalità.

Il protocollo IGMPv3, rispetto alla versione precedente, dispone di funzioni di *source filtering* che permettono ai ricevitori e a specifiche applicazioni di abilitare la ricezione di flussi multicast provenienti solo da determinate sorgenti. Non esistono ancora sviluppi standard di questo protocollo. È stata invece realizzata una soluzione temporanea proprietaria (Cisco), nota come URD (*URL Rendez vous Directory*) che permette già oggi di utilizzare SSM senza alcuna modifica ai sistemi operativi e alle applicazioni multicast esistenti (<ftp://ftpeng.cisco.com/lipmulticast/ssm/index.html#Stacks>).

Il ricevitore deve possedere, come unico requisito, la capacità di attivare l'applicazione attraverso un browser web. Essa si basa sulla capacità, che presenta il *last-hop router* nei riguardi del ricevitore, di intercettare alcune ben definite richieste URL: in pratica non appena il router intercetta, come generati dal ricevitore, l'iscrizione al canale, identificato dalla coppia (S,G), codificata in una richiesta URL e un messaggio IGMPv2 verso il gruppo G, il router stesso inoltra una *join* verso il router cui è attestata la sorgente S.

È già disponibile una versione commerciale del protocollo SSM realizzata da Cisco. Si tratta sostanzialmente di una versione aggiornata e adattata della realizzazione del protocollo PIM-SM. La rapidità con cui è stata sviluppata e "messa in campo" la soluzione SSM è spiegabile con l'interesse manifestato da importanti operatori e istituzioni quali Sprint e Internet 2³.

La prima sessione multicast basata su SSM è stata trasmessa dall'Università dell'Oregon durante il meeting Internet 2 che si è tenuto a Toronto nell'agosto 2000. La trasmissione è stata effettuata sul backbone Abilene di Internet 2.

Una successiva dimostrazione è stata realizzata nel settembre del 2000 durante il 37esimo meeting RIPE tenuto ad Amsterdam. In questo caso oltre al backbone IP multicast nativo della rete Abilene il flusso attraversava il backbone IP multicast della rete di ricerca pan-europea TEN-155. Queste sperimentazioni oltre a consolidare la soluzione SSM hanno permesso di verificare la perfetta integrazione del modello e dei relativi sviluppi con la piattaforma IP multicast esistente basata su MBGP/MSDP/PIM-SM. Per differenziare il traffico multicast SSM da quello tradizionale è stato definito da IANA un intervallo di indirizzi IP multicast (da 232.0.0.0 a 232.255.255.255) dedicato a sorgenti SSM.

(3) Oggi il sito web ufficiale cui si può accedere sperimentalmente a sorgenti audio e video è quello SSM: <http://videolab.uoregon.edu/cgi-bin/urd.cgi>

In questo articolo è stato messo in evidenza che accanto alle soluzioni IP multicast standard, sono state sviluppate soluzioni proprietarie, che sfruttano la piattaforma di rete IP unicast, che utilizzano soluzioni multicast sovrapposte. Queste soluzioni, pur non essendo completamente ottimizzate per il trasporto del traffico in rete, introducono efficacemente quelle funzioni necessarie per l'offerta dei servizi (cioè sicurezza, accessi condizionati, tariffazione, ...).

Real Network è il primo esempio di soluzione tecnologica multicast sovrapposta alla rete IP unicast.

Nel testo è stata anche mostrata la soluzione di servizio oggi emergente, denominata *CDN (Content Delivery Network)*. L'importanza di questa nuova realizzazione non consiste tanto nella soluzione tecnologica, quanto piuttosto nell'impiego che essa permette per attuare nuovi modelli di business basati sul pagamento per la fruizione dei contenuti. Gli ISP possono così incrementare la loro catena del valore individuando nuove fonti di guadagno. Nuovi attori, quali ad esempio gli *Application Service Provider*, possono trovare spazi per offrire nuovi servizi basati sulle informazioni prelevate dai fornitori di contenuti e offerte ai fruitori finali che ne facciano richiesta con livelli di qualità adeguati.

Il multicast, in conclusione, sembra poter rappresentare la chiave per lo sviluppo futuro dei servizi multimediali con soluzioni di tipo standard o, forse anche, almeno in un periodo transitorio, con soluzioni non normalizzate.

Bibliografia

- [1] Baiocchi, A.; Iuso, F.; Liffredo, L.: *Come funziona l'instradamento dei pacchetti IP*. «Notiziario Tecnico Telecom Italia», Anno 9, n. 1, aprile 2000, pp. 14-24.
- [2] Moy, J.: *OSPF Version 2*. IETF RFC 1583, marzo 1994.
- [3] Waitzman, D.; Partridge, C.: *Distance Vector Multicast Routing Protocol*. IETF RFC 1075, novembre 1988.
- [4] Meyer, D.: *Administratively Scoped IP Multicast*. IETF RFC 2365, luglio 1998.
- [5] Meyer, D.; Lothberg, P.: *GLOP Addressing in 233/8*. IETF RFC 2770, febbraio 2000.
- [6] Deering, S.: *Host Extensions for IP Multicasting*. IETF RFC 1112, agosto 1989.
- [7] Fenner, W.: *Internet Group Management Protocol, Version 2*. IETF RFC 2236, novembre 1997.
- [8] Cain, B.; Deering, S.; Fenner, W.; Kouvelas, I.; Thyagarajan, A.: *Internet Group Management Protocol, Version 3*. IETF Internet-Draft, gennaio 2001.
- [9] Laxman H. Sahasrabudhe; Biswanath Mukherjee: *Multicast Routing Algorithms and Protocols: A Tutorial*. «IEEE Network», gennaio/febbraio 2000.
- [10] Winter, P.: *Steiner problem in networks: a survey*. «Networks», Vol. 17, 1987, pp. 129-167.
- [11] Estrin, et al.: *Protocol Independent Multicast-Dense Mode (PIM-DM): Protocol Specification*. Internet Draft draft-ietf-idmr-pim-dm-spec-05.txt, maggio 1997.
- [12] Estrin, et al.: *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*. Internet RFC 2362, giugno 1998.
- [13] Bates, T.; Chandra, R.; Katz, D.; Rekhter, Y.: *Multiprotocol Extensions for BGP-4*. IETF RFC 2283, febbraio 1998.
- [14] Farinacci, et al.: *Multicast Source Discovery Protocol*. IETF Internet Draft draft-ietf-msdp-spec-06.txt, luglio 2000.
- [15] Thaler, D.; Estrin, D.; Meyer, D.: *Border Gateway Multicast Protocol (BGMP): Protocol Specification*. IETF Internet Draft draft-ietf-bgmp-spec-02.txt, novembre 2000.
- [16] Radoslavov, P.; Estrin, D.; Govindan, R.; Handley, M.; Kumar, S.; Thaler, D.: *The Multicast Address-Set Claim (MASC) Protocol*. IETF RFC 2909, settembre 2000.
- [17] Dorian Kim; Meyer, D. et al.: *Anycast RP mechanism using PIM and MSDP*. IETF Internet Draft draft-ietf-mboned-anycast-rp-06.txt, aprile 2000.
- [18] Rekhter, Y.; Li, T.: *A Border Gateway Protocol 4 (BGP-4)*. IETF RFC 1771, marzo 1995.
- [19] Schulzrinne, H.; Casner, S.; Frederick, R.; Jacobson, V.: *RTP: A Transport Protocol for Real-Time Applications*. IETF RFC 1889, gennaio 1996.
- [20] Schulzrinne, H.: *RTP Profile for Audio and Video Conferences with Minimal Control*. IETF RFC 1890, gennaio 1996.
- [21] Handley, M.; Jacobson, V.: *SDP: session description protocol*. IETF RFC 2327, aprile 1998.
- [22] Thaler, D.; Handley, M.; Estrin, D.: *The Internet Multicast Address Allocation Architecture*. IETF RFC 2908, settembre 2000.
- [23] Hanna, S.; Patel, B.; Shah, M.: *Multicast Address Dynamic Client Allocation Protocol (MADCAP)*. IETF RFC 2730, dicembre 1999.
- [24] Handley, M.; Hanna, S.: *Multicast Address Allocation Protocol (AAP)*. Work in Progress.
- [25] Diot, C.; Levine, B.; Lyles, B.; Kassem, H.; Balensiefen, D.: *Deployment Issues for the IP Multicast Service and Architecture*. «IEEE Networks Magazine's Special Issue on Multicast», gennaio 2000.
- [26] Hobbrook, H.; Cain, B.: *Source-Specific Multicast for IP*. IETF Internet Draft draft-holbrook-ssm-arch-01.txt, novembre 2000.
- [27] Cain, B.; Deering, S.; Fenner, B.; Kouvelas, I.; Thyagarajan, A.: *Internet Group Management Protocol, Version 3*. Internet Draft draft-ietf-idmr-igmp-v3-06.txt, gennaio 2001.
- [28] Estrin, D.; Govindan, R.; Handley, M.; Kumar, S.; Radoslavov, P.; Thaler, D.: *The Multicast Address-Set Claim (MASC) Protocol*. Internet Draft draft-ietf-malloc-masc-06.txt, luglio 2000.

Abbreviazioni

AAP	Address Allocation Protocol
ARP	Address Resolution Protocol
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BGMP	Border Gateway Multicast Protocol
BGP4	Border Gateway Protocol version 4
BGP4+	Border Gateway Protocol version 4 +
CBT	Core Based Trees
CDN	Content Delivery Network
DA	Destination Address
DVMRP	Distance Vector Multicast Routing Protocol
EGP	Exterior Gateway Protocol
Hex	Esadecimale
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LIS	Logical IP Subnet
MAAS	Multicast Address Allocation Servers
MAC	Media Access Control
MADCAP	Multicast Address Dynamic Client Allocation Protocol
MALLOC	Multicast address ALLOCation
MARS	Multicast Address Resolution Server
MASC	Multicast Address-Set Claim
MBGP	Multiprotocol Border Gateway Protocol
MCS	MultiCast Server
M-IGP	Multicast-Interior Gateway Protocol
MSDP	Multicast Source Discovery Protocol
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast - Dense Mode
PIM-SM	Protocol Independent Multicast - Sparse Mode
RFC	Request For Comments
RIP	Routing Information Protocol
RIPE	Réseaux IP Européens
RP	Rendez-vous Point
RPF	Reverse Path Forwarding
RPM	Reverse Path Multicasting
RTCP	Real-Time Control Protocol
RTP	Real-time Transport Protocol
SA	Source Address
SBT	Source-Based Tree
SDP	Session Description Protocol
SDR	Session DiRectory
SPT	Shortest Path Tree
SSM	Source Specific Multicast
TEN-155	Trans-European Network interconnect at 155 Mbps

TTL	Time To Live
URD	URL Rendez vous Directory
VAT	Visual Audio Tool
VC	Virtual Circuit
VIC	Video Conferencing tool



Francesco Iuso ha conseguito la laurea con lode in Ingegneria Elettronica presso l'Università degli studi "La Sapienza" di Roma nell'anno accademico 1989/90, discutendo la tesi sul riconoscimento della voce. Nel corso del 1991 ha prestato attività di consulenza presso l'Alenia Spazio di Roma sulla tematica "prodotti di intermodulazione nelle trasmissioni via satellite", dovendo ancora concludere gli obblighi di leva. Nel 1992 è stato assunto in SIP (oggi Telecom Italia) e per conto della società ha frequentato e superato con lode il master in Tecnologie dell'Informazione presso il centro "CEFRIEL", analizzando le problematiche di internetworking e di integrazione delle reti locali nell'architettura di rete integrata nei servizi a larga banda in tecnica ATM. Dal 1993 si è occupato di reti e servizi dati ad alta velocità nella Ricerca e sviluppo di SIP. Nel 1994 è stato nominato chairman del gruppo ESIG (European SMDS Interest Group) e ha ricoperto la carica per un anno. Ha partecipato alle attività di definizione dell'interlavoro Frame Relay-ATM in ITU-T. Dal 1994 al 1999 ha partecipato alle attività del gruppo IETF (Internet Engineering Task Force) e si è occupato di problematiche di internetworking, materia sulla quale è stato coautore di diversi articoli. Ha partecipato al progetto SIRIUS e alle sperimentazioni di Telecom Italia per lo sviluppo di servizi multimediali interattivi e ha curato la realizzazione delle soluzioni innovative di rete per i clienti della rete SIRIUS. Si è occupato di protocolli e politiche di instradamento IP, con riferimento alle problematiche di interconnessione di reti IP. Si è occupato della ingegneria della rete dial-up Tin.it. Nell'ambito della Ingegneria dei Servizi della Funzione Rete di Telecom Italia si è occupato di soluzioni di rete privata virtuale dial-up. Da febbraio 2001 opera in TIM.



Loris Marchetti si è laureato in Scienze dell'Informazione presso l'Università degli Studi di Pisa nel luglio 1988. Dal novembre dello stesso anno lavora in Telecom Italia Lab - TILAB (già CSELT) dove ha svolto attività di ricerca nel campo delle tecnologie e dei servizi di networking. Inizialmente è stato coinvolto in attività di standardizzazione e sperimentazione di protocolli per reti metropolitane. In particolare ha partecipato alla definizione del protocollo "Distributed Queue Dual Bus" (DQDB) ed alle relative sperimentazioni condotte nell'ambito di diversi progetti ESPRIT II quali MAX "Metropolitan Area Communication System" (1991-1992) e MAXI "Metropolitan Area Communication System Integration" (1992-1993). Dal 1993 ha partecipato alle prime sperimentazioni geografiche a livello europeo di reti in tecnologia ATM (Asynchronous Transfer Mode) condotte in progetti finanziati dalla Comunità Europea (il progetto ACTS NICE, "National Host Interconnection Experiments") e in collaborazioni bilaterali come quella tra TILAB e CNET, il centro di ricerca di France Télécom. Successivamente ha svolto attività di definizione, progettazione e verifica sperimentale di servizi innovativi basati su IP multicast in laboratorio, in reti corporate e su rete geografica. Nell'ambito di questa attività ha dato supporto tecnico a società del gruppo Telecom Italia interessate ad introdurre detto servizio sulle loro reti ed ha partecipato come responsabile TILAB ai Progetti Eurescom P911 "IP Multicast" e P1010 "Real Time Services with IP multicast (RealCast)". Attualmente oltre ad occuparsi della tematica IP multicast è impegnato in un progetto ("Soluzioni Wireless LAN per ISP ed aziende") che si pone come obiettivo l'offerta di servizi IP wireless in area metropolitana ed in ambiti indoor pubblici e privati.