(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-208302
(P2004-208302A)
(43)公開日　平成16年7月22日(2004.7.22)

(51)Int.Cl.[7]	F I	テーマコード（参考）
H04L 12/56	H04L 12/56 260A	5K030

審査請求 未請求　請求項の数 15　ＯＬ　外国語出願　（全 38 頁）

(21)出願番号　特願2003-419296(P2003-419296)
(22)出願日　平成15年12月17日(2003.12.17)
(31)優先権主張番号　323633
(32)優先日　平成14年12月20日(2002.12.20)
(33)優先権主張国　米国(US)

(71)出願人　501279833
アルカテル・カナダ・インコーポレイテッド
カナダ国、オンタリオ・ケー・２・ケー・２・イー・６、カナタ、マーチ・ロード・６００
(74)代理人　100062007
弁理士　川口　義雄
(74)代理人　100113332
弁理士　一入　章夫
(74)代理人　100114188
弁理士　小野　誠
(74)代理人　100103920
弁理士　大崎　勝真

最終頁に続く

(54)【発明の名称】通信ネットワークにおける異なるマルチキャストプロトコル間で要求を変換するシステムおよび方法

(57)【要約】
【課題】あるプロトコルでの要求を別のプロトコルで作らた別の要求から生成し、評価するシステムおよび方法を提供する。
【解決手段】その要求は、グループへのメンバシップの変更に関連し、グループは、サービスを通信ネットワークにおけるそのサービスのホストに関連付ける。特にこの方法は、別の要求を受信することと、別の要求からターゲットグループを識別することと、ターゲットグループに関連するホストを識別することと、ターゲットグループおよび関連するホストへの参照を含む要求を別のプロトコルとは異なるプロトコルで生成することとを含む。要求は、グループを識別するものであって、かつ関連するホストを一意に識別するものではない。本発明は、認識されたグループに属していない場合、要求がさらに進むのを阻止する能力を提供する。
【選択図】　図１

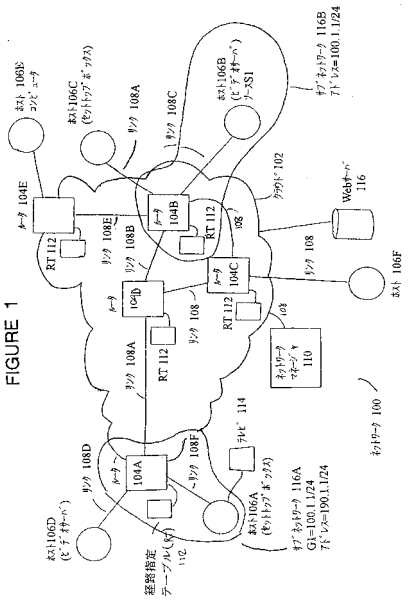
FIGURE 1

【特許請求の範囲】
【請求項１】
あるプロトコルでの要求を別のプロトコルで作られた別の要求から生成する方法であって、該要求が、サービスを通信ネットワークの前記サービスのホストに関連付けるグループに対する、メンバシップの変更に関し、前記方法が、
前記別の要求を受信することと、
前記別の要求からターゲットグループを識別することと、
前記ターゲットグループに関連するホストを識別することと、
前記ターゲットグループおよび前記関連するホストへの参照を含む要求を前記別のプロトコルとは異なるプロトコルで生成することとを含み、
前記別の要求が、前記グループを識別するものであって、かつ前記関連するホストを一意に識別するものではない、前記方法。
【請求項２】
前記サービスが、前記ネットワーク内でのマルチキャスト伝送である、請求項１に記載のあるプロトコルでの要求を別のプロトコルで作られた別の要求から生成する方法。
【請求項３】
前記ホストが、すべてのホストを前記ネットワークで構成されているすべてのグループに関連付けるデータにアクセスすることによって識別される、請求項２に記載のあるプロトコルでの要求を別のプロトコルで作られた別の要求から生成する方法。
【請求項４】
前記データが、前記ネットワークの各ルータからアクセス可能である、請求項３に記載のあるプロトコルでの要求を別のプロトコルで作られた別の要求から生成する方法。
【請求項５】
前記データのインスタンスが、前記各ルータでローカルに格納される、請求項４に記載のあるプロトコルでの要求を別のプロトコルで作られた別の要求から生成する方法。
【請求項６】
前記データの前記インスタンスが、前記ネットワークに関連付けられているネットワークマネージャコンピュータによって更新される、請求項５に記載のあるプロトコルでの要求を別のプロトコルで作られた別の要求から生成する方法。
【請求項７】
前記別のプロトコルが、ＩＧＭＰバージョン２構成に従い、前記要求が、ＩＧＭＰバージョン３構成に従う、請求項６に記載のあるプロトコルでの要求を別のプロトコルで作られた別の要求から生成する方法。
【請求項８】
前記別の要求が、前記ネットワークの要求側ホストで生成され、かつ前記要求側ホストに接続されているルータで受信される、請求項７に記載のあるプロトコルでの要求を別のプロトコルで作られた別の要求から生成する方法。
【請求項９】
前記要求を反映する更新が、前記グループに関連付けられている転送テーブルに対して行われる、請求項８に記載のあるプロトコルでの要求を別のプロトコルで作られた別の要求から生成する方法。
【請求項１０】
あるプロトコルでの要求を別のプロトコルで作られた別の要求から管理しかつ変換するシステムであって、前記要求が、サービスを通信ネットワークのホストに関連付けるグループに対する、メンバシップの変更に関し、前記システムが、
前記別の要求を受信するモジュールと、
すべてのホストを、前記ネットワークで構成されているすべてのグループに関連付けるデータと、
前記データを使用するターゲットグループに関連するホストを識別する識別モジュールと、

前記ターゲットグループおよび前記関連するホストへの参照を含む前記要求を選択的に生成する生成モジュールとを備え、
前記別の要求が、前記グループを識別するものであって、かつ前記関連するホストを一意に識別するものではない、前記システム。
【請求項１１】
前記データが、前記ネットワークの各ルータによってアクセス可能である、請求項１０に記載のあるプロトコルでの要求を別のプロトコルで作られた別の要求から管理しかつ変換するシステム。
【請求項１２】
前記データのインスタンスが、前記各ルータでローカルに格納され、
前記データの前記各インスタンスが、前記ネットワークに関連付けられているネットワークマネージャコンピュータによって更新され、
前記別のプロトコルが、ＩＧＭＰバージョン２構成に従い、
前記要求が、ＩＧＭＰバージョン３構成に従う、
請求項１１に記載のあるプロトコルでの要求を別のプロトコルで作られた別の要求から管理しかつ変換するシステム。
【請求項１３】
前記ホストおよび前記ターゲットグループに関連付けられているメンバシップ情報を使用して、前記ターゲットグループへの前記別の要求のアクセス権を評価する評価モジュールと、
前記別の要求がアクセス不可のアクセス権を有している場合、前記生成モジュールが前記要求を生成するのを選択的に阻止するブロッキングモジュールとをさらに備える、請求項１２に記載のあるプロトコルでの要求を別のプロトコルで作られた別の要求から管理しかつ変換するシステム。
【請求項１４】
あるプロトコルで受信された要求を評価しかつ変換する方法であって、前記要求が、通信ネットワークのホストによって提供されるサービスに関連するグループへの参加に関し、前記方法が、
前記要求を受信することと、
前記要求からターゲットグループを識別することと、
前記ターゲットグループに関連するホストを識別することと、
前記ホストおよび前記ターゲットグループに関連付けられているメンバシップ情報を使用して、前記ターゲットグループへの前記要求のアクセス権を評価することと、
前記要求が、前記ターゲットグループへのアクセス可能なアクセス権を有していない場合、前記ホストを前記ターゲットグループから阻止することと、
前記アクセス権がアクセス可能な場合、前記ターゲットグループおよび前記関連するホストへの参照を含む他の要求を生成することとを含み、
前記要求が、前記グループを識別するものであって、かつ前記関連するホストを一意に識別するものではない、前記方法。
【請求項１５】
あるプロトコルで受信された要求を評価しかつ変換する方法であって、前記要求が、グループにファイルを配信するものであり、
サービスが、ネットワークへのマルチキャスト伝送であり、
別のプロトコルが、ＩＧＭＰバージョン２構成に従い、
前記要求が、ＩＧＭＰバージョン３構成に従う、前記方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般にデータ通信に関し、より詳細にはインターネットグループ管理プロトコルが動作するルータとホストとの間のインターフェースをとるためのシステムおよび方

法に関する。
【背景技術】
【０００２】
デジタル媒体サービスは、テレビ番組、映画、音声番組、テキストベースの情報ストリームなど、ダウンロード可能なビデオ情報へのアクセスを加入者に提供する。一般に加入者は、通信ネットワークへの接続を介してこうしたサービスに選択的にアクセスする。ネットワークにおいて、サービスは、１つまたは複数の情報ソースから提供される。ネットワークにおけるルータは、ソースおよび加入者の両方に結合され、ルータは、リンクインターフェースを提供して、ソースがサービスをネットワーク内の目的の加入者に送信できるようにする。
【０００３】
一般に、サービスが、ネットワーク内の特定リストの加入者に提供されるとき、マルチキャスト伝送が使用される。マルチキャスト伝送では、１つのルータがメッセージを複数の宛先に送信する。マルチキャスト伝送では、ルータは、指定されたマルチキャスト伝送を受信する予定のグループのメンバを識別するグループ情報が必要である。インターネットプロトコル（ＩＰ）ｖ４ネットワークでは、Ｉｎｔｅｒｎｅｔ Ｇｒｏｕｐ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ（ＩＧＭＰ）コマンドが、ネットワークにおいてホストからルータに送信されて、ＩＰマルチキャスト伝送を管理する。ＩＧＭＰは、進化するプロトコルである。その標準が進化するため、インターネット特別技術調査委員会（ＩＥＴＦ）は、「Ｈｏｓｔ Ｅｘｔｅｎｓｉｏｎｓ ｆｏｒ ＩＰ Ｍｕｌｔｉｃａｓｔｉｎｇ」という名称のＲＦＣ１１１２、「Ｉｎｔｅｒｎｅｔ Ｇｒｏｕｐ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ，Ｖｅｒｓｉｏｎ２」という名称のＲＦＣ２２３６、および「Ｉｎｔｅｒｎｅｔ Ｇｒｏｕｐ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ，Ｖｅｒｓｉｏｎ３」という名称のＲＦＣ３３７６など、ＩＧＭＰの仕様を多数発行している。こうしたすべての仕様は、参照により本明細書に組み込まれる。ＩＧＭＰバージョン２は、Ｐｒｏｔｏｃｏｌ Ｉｎｄｅｐｅｎｄｅｎｔ Ｍｕｌｔｉｃａｓｔ－Ｓｐａｒｓｅ Ｍｏｄｅ（ＰＩＭ－ＳＭ）マルチキャスティングと相互運用可能なように構成されている。ＩＧＭＰバージョン３は、Ｐｒｏｔｏｃｏｌ Ｉｎｄｅｐｅｎｄｅｎｔ Ｍｕｌｔｉｃａｓｔ－Ｓｉｎｇｌｅ Ｓｏｕｒｃｅ Ｍｕｌｔｉｃａｓｔ（ＰＩＭ－ＳＳＭ）マルチキャスティングの能力を追加している。ＰＩＭ－ＳＳＭは、ＰＩＭ－ＳＭよりもデータプレーンおよび制御プレーンの両方で簡略化された処理を提供する。残念ながら、ＩＧＭＰｖ３の一部のマッピング構成は、ＩＧＭＰｖ２との互換性がない。このことは、ＩＧＭＰバージョン２のプロトコルコマンドのみを認識するレガシーホストが、ＰＩＭ－ＳＳＭを使用するネットワークに接続されているときに問題である。
【０００４】
【非特許文献１】「Ｈｏｓｔ Ｅｘｔｅｎｓｉｏｎｓ ｆｏｒ ｉＰ Ｍｕｌｔｉｃａｓｔｉｎｇ」という名称のＲＦＣ１１１２
【非特許文献２】「Ｉｎｔｅｒｎｅｔ Ｇｒｏｕｐ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ，Ｖｅｒｓｉｏｎ２」という名称のＲＦＣ２２３６
【非特許文献３】「Ｉｎｔｅｒｎｅｔ Ｇｒｏｕｐ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ，Ｖｅｒｓｉｏｎ３」という名称のＲＦＣ３３７６
【発明の開示】
【発明が解決しようとする課題】
【０００５】
したがって、レガシープロトコルに、ＰＩＭ－ＳＳＭ互換性を提供するマルチキャストグループ伝送をサポートする方法および装置が必要である。
【課題を解決するための手段】
【０００６】
第１の態様において、あるプロトコルでの要求を別のプロトコルで作られた別の要求から生成する方法が提供される。その要求は、あるグループへのメンバシップの変更に関連

し、グループは、通信ネットワークのホストによって提供されるサービスに関連する。この方法は、別の要求を受信することと、別の要求からターゲットグループを識別することと、ターゲットグループに関連するホストを識別することと、ターゲットグループおよび関連するホストへの参照を含む要求を別のプロトコルとは異なるプロトコルで生成することとを含む。この方法では、別の要求は、グループを識別するものであって、かつ関連するホストを一意に識別するものではない。

【０００７】

この方法でのサービスは、ネットワークにおけるマルチキャスト伝送に関連し得る。

【０００８】

この方法によって、すべてのホストをネットワークで構成されたグループのすべてに関連付けるデータにアクセスすることによって、ホストが識別され得る。

【０００９】

この方法によって、データがネットワークの各ルータからアクセス可能になり得る。

【００１０】

この方法では、データのインスタンスを、各ルータにローカルに格納することができる。

【００１１】

この方法では、データの各インスタンスを、ネットワークに関連付けられているネットワークマネージャコンピュータによって更新することができる。

【００１２】

この方法では、別のプロトコルはＩＧＭＰバージョン２構成に従い、要求はＩＧＭＰバージョン３構成に従うことができる。

【００１３】

この方法によって、別の要求がネットワークの要求側ホストで生成され、要求側ホストに接続されているルータで受信され得る。

【００１４】

この方法では、グループに関連付けられている転送テーブルを更新させて要求を反映することができる。

【００１５】

第２の態様では、あるプロトコルでの要求を別のプロトコルで作られた別の要求から管理しかつ変換するシステムが提供される。そのシステムでは、要求は、あるグループへのメンバシップの変更に関連し、グループは、通信ネットワークのホストによって提供されるサービスに関連する。このシステムは、別の要求を受信するモジュールと、すべてのホストをネットワークで構成されたグループのすべてに関連付けるデータと、そのデータを使用してターゲットグループに関連するホストを識別する識別モジュールと、ターゲットグループおよび関連するホストへの参照を含む要求を選択的に生成する生成モジュールとを備える。このシステムでは、別の要求は、グループを識別するものであって、かつ関連するホストを一意に識別するものではない。

【００１６】

このシステムによって、データがネットワークの各ルータからアクセス可能になり得る。

【００１７】

このシステムでは、データのインスタンスを各ルータにローカルに格納することができる。データの各インスタンスを、ネットワークに関連付けられているネットワークマネージャコンピュータによって更新することができる。別のプロトコルは、ＩＧＭＰバージョン２構成に従うことができ、要求は、ＩＧＭＰバージョン３構成に従うことができる。

【００１８】

このシステムは、評価モジュールおよびブロッキングモジュールをさらに備えることができる。評価モジュールは、ホストおよびターゲットグループに関連付けられているメンバシップ情報を使用して、別の要求のターゲットグループへのアクセス権を評価する。ブ

ロッキングモジュールは、別の要求がアクセス不可のアクセス権を有している場合、生成モジュールが要求を生成するのを選択的に阻止する。

【００１９】

第３の態様では、あるプロトコルで受信された要求を評価しかつ変換する方法が提供される。その方法では、要求は、グループに参加することに関連し、グループは、通信ネットワークのホストによって提供されるサービスに関連する。この方法は、要求を受信することと、要求からターゲットグループを識別することと、ターゲットグループに関連するホストを識別することと、ホストおよびターゲットグループに関連するメンバシップ情報を使用することによって、要求のターゲットグループへのアクセス権を評価することと、要求がターゲットグループへのアクセス可能なアクセス権を有していない場合は要求を阻止し、アクセス権がアクセス可能な場合は、ターゲットグループおよび関連するホストへの参照を含む他の要求を生成することを含む。この方法では、要求は、グループを識別するものであって、関連するホストを一意に識別するものではない。

【００２０】

この方法は、ネットワークにおけるマルチキャスト伝送に関連する要求を有することができる。別のプロトコルは、ＩＧＭＰバージョン２構成に従うことができ、要求は、ＩＧＭＰバージョン３構成に従うことができる。

【００２１】

本発明の別の態様では、上記の態様の様々な組合せおよび一部が提供される。

【００２２】

本発明の上記および他の態様は、その特定の実施形態の以下の説明、および本発明の原理を単に例として示した添付の図面からより明らかになる。図中、同様の要素は同様の参照符号で示しており、同様の要素の特定の例示を識別するために、参照符号に一意の英字の接尾文字を付加しているものもある。

【００２３】

以下の説明およびその実施形態は、本発明の原理の特定の実施形態の例を示す目的で示している。これらの例は、そうした原理を限定するものではなく、例示の目的で示している。以下の説明では、同様の要素には、明細書および図面を通じて同じ参照符号を付している。

【発明を実施するための最良の形態】

【００２４】

従来技術のシステム

図１を参照すると、ネットワーク１００が示されている。従来技術のシステムおよび本発明の実施形態を示すために、ネットワーク１００の態様が示されている。

【００２５】

従来技術のシステムでは、ネットワーク１００によって、ネットワーク要素が、クラウド１０２を介して別のネットワーク要素に接続されている。特に、ネットワーククラウドは、通信リンク１０８によって接続される一連のルータ１０４を備える。図に示すように、クラウド１０２は、ルータ１０４Ａ、１０４Ｂ、１０４Ｃ、１０４Ｄ、および１０４Ｅを備える。データトラフィックが、ネットワーククラウド１０２を介してソース装置から宛先装置に送信されるとき、様々なルータ１０４を通過する通信パスが画定されなければならない。

【００２６】

ネットワーク１０２のアーキテクチャはＩＰであることが好ましい。したがって、データトラフィックのアドレス構成およびパス生成構成は、ＩＰ構成に従う。したがって、パスを確立するときは、宛先装置に向かう通信パスのセグメントにおける隣接するルータに、データトラフィックを送信できるルータを連続的に見つけることによって、パスは、ソース装置から複数のセグメントで宛先装置に延長される。各ルータは、各ルータが受信したデータトラフィックの経路指定パスの次のセグメントを識別するのを助けるために、ネットワーククラウド１０２のトポロジのマップを提供する経路指定テーブル１１２を有す

る。ネットワークマネージャ１１０は、クラウド１０２に接続され、各ルータ１０４の経路指定テーブル１１２を維持し、かつ更新するよう働く。ネットワークマネージャ１１０は、通信リンク１０８を介してクラウド１０２内の各ルータ１０４に接続される。

【００２７】

ホスト１０６は、コンピューティング装置であり、各ホストはＩＰアドレスを有している。各ホスト１０６は、ネットワーク１００へのホスト１０６の接続ポイントを提供するルータ１０４に接続される。例えば、ホスト１０６Ａおよび１０６Ｄは、ルータ１０４Ａを介してネットワーク１００に接続され、ホスト１０６Ｂおよび１０６Ｃは、ルータ１０４Ｂを介してネットワーク１００に接続され、ホスト１０６Ｅは、ルータ１０４Ｅに接続され、ホスト１０６Ｆは、ルータ１０４Ｃに接続される。接続は、接続リンク１０８を介して確立される。他の実施形態では、ホストとその接続ルータとの間の通信リンクは、非対称デジタル加入者回線、Ｅｔｈｅｒｎｅｔ（登録商標）接続、ローカルマルチポイントデータサービス（ＬＭＤＳ）、または非同期転送モード（ＡＴＭ）パッシブ光ネットワーク（ＡＰＯＮ）などの広帯域通信リンクでよい。

【００２８】

一部のホストは、サービスの記憶サイトとして使用することができ（ホスト１０６Ｂおよび１０６Ｄなど）、あるホストは、コンピュータ（ホスト１０６Ｅおよび１０６Ｆ）またはセットトップボックス（ホスト１０６Ａおよびホスト１０６Ｃ）でよい。セットトップボックスを使用して、他のホストにマルチキャストグループ伝送などのサービスを要求する。マルチキャスト伝送を受信するように構成された場合、セットトップボックスは、１つまたは複数の要求をルータに発行し、ルータは、セットトップボックスをネットワーク１００に接続して、ユーザによって選択されたプログラミング情報に対応するマルチキャスト伝送を受信する。こうした構成では、テレビを観ているユーザがチャンネルを変えると、セットトップボックスは、チャンネル変更に関する情報を接続ルータに中継する。本質的に、セットトップボックスは、以前表示されていたチャンネルはもはや要求されておらず、ユーザが選択したチャンネルに対応する新しいマルチキャストデータストリームが要求されていることを、接続ルータに知らせる。また、パーソナルコンピュータをホストとして構成して、セットトップボックスと同じようにマルチキャストグループを要求することもできる。ホストのそれぞれを様々な時点で作動または非作動にし、またホストのそれぞれが、作動時に１つまたは複数のマルチキャストグループを要求することができる。

【００２９】

従来技術では、ネットワーク１００を使用して、デジタルビデオ配信サービスへのある程度のアクセスを提供する。テレビ１１４のユーザは、ネットワーク１００にアクセスして、遠隔ホスト１０６に、サービスによって提供される特定のビデオ番組のダウンロードを要求する。ユーザは、表示装置（テレビなど）およびネットワーク１００に接続されているセットトップボックス１０６Ａを有する。セットトップボックス１０６Ａは、ホストであり、ユーザによって開始されるビデオ番組のネットワーク要求を生成し、かつ送信する。ユーザは、ビデオ番組をダウンロードしたいとき、メニュー（一般にテレビ１１４に表示される）にアクセスし、そのメニューから所望のビデオ番組を選択する。次いでセットトップボックス１０６Ａは、ビデオ番組の受信要求をネットワークに発行する。セットトップボックス１０６Ａによって送信される要求を、ネットワーク１００への接続ポイントであるルータ１０４Ａが受信する。ルータ１０４Ａは、要求をビデオ番組のソースに向かってネットワーク１００に転送する必要がある。ネットワーク１００において、ビデオ番組を提供するホストは、ホスト１０６Ｂである。

【００３０】

ネットワーク１００において、ホスト１０６Ｂおよび１０６Ｄは、ＩＰマルチキャスティングプロトコルを使用して、ネットワーク１００に、そのプログラムを要求側セットトップボックスまたはコンピュータに対して配信させる。マルチキャスティングは、ネットワーク１００における帯域幅の使用を保護する利点を提供する。マルチキャスティングで

は、ホストは、同じデータをそのルータに繰り返し送信し、次いでそのルータにデータを各加入側サービスに対して送信させるのではなく、マルチキャストされたデータの１つのコピーをそのサーバに一度送信することができる。

【００３１】

ＩＰマルチキャストセッションは、保持されたマルチキャストＩＰアドレスにパケットを送信することによって規定される。マルチキャストＩＰアドレスは、ＩＰｖ４では、２２４．０．０．０から２３９．２５５．２５５．２５５のアドレスを含む、クラスＤ範囲内のアドレスを備える。したがって、パケットのＩＰヘッダからのソースおよび宛先のＩＰアドレスを調べることによって、ルータは、どのリンク１０８を介してパケットがマルチキャストされるかを決定することができる。マルチキャストアドレスは、特定の物理的宛先ホストではなく特定の伝送セッションを識別する。これによってホストは、確実に進行中のマルチキャストセッションに参加できるようになる。

【００３２】

従来技術では、マルチキャストプロトコルを動作させるホストおよびルータの対話を管理する３つのプロトコルがある。

１．標準化されたレガシープロトコルであるＰＩＭ－ＳＭネットワークと相互運用するＩＧＭＰｖ２

２．最近標準化されたプロトコルであるＰＩＭ－ＳＭネットワークと相互運用するＩＧＭＰｖ３

３．最近標準化された別のソリューションであるＰＩＭ－ＳＳＭネットワークと相互運用するＩＧＭＰｖ３。

【００３３】

次の例では、ＩＧＭＰｖ３要求がＰＩＭ－ＳＳＭ要求に変換される、プロトコル＃３の動作態様を示している。ビデオ番組のマルチキャストの実施を助けるために、各ルータは、各ビデオ番組に関連付けられているホストのマルチキャスト転送テーブル（ＭＦＴ）を維持する。テーブルの各エントリは、２つの構成要素を有する。第１の構成要素は、そのグループのＩＰアドレスおよび番組のソースホストを含む、マルチキャストされる番組の情報を提供する。第２の構成要素は、番組に関連付けられている発信リンク（１０８）のリストである。テーブルＡは、ネットワーク１００におけるルータ１０４Ｂの代表的なマルチキャスト転送テーブルである。

【表１】

テーブルA

MFTグループ	マルチキャスト受信側リンク
ソースS=ホスト106B(10.1.2.3) グループG=ABC(239.0.0.1)	リンク108Aからセットトップボックス106C リンク108Cからルータ104C
ソースS=ホスト106D(10.2.3.4) グループG=NBC(239.0.0.9)	リンク108Eからルータ104E
ソースS=ホスト106B(10.1.2.3) グループG=HBO(239.0.0.5)	リンク108Aからセットトップボックス106C

ＭＦＴを、経路指定テーブル１１２の一部として含めていてもよい。マルチキャストの宛先が追加され、またグループから削除されると、ＭＦＴを更新する必要がある。マルチキャストの経路指定の際に、ルータは、互いに通信して、マルチキャストグループメンバシップ情報に関する情報を隣接するルータと交換する。

【００３４】

ＩＧＭＰｖ３を使用して、ホスト１０６Ａは、ルータ１０４ＡへのＪＲ（Ｓ，Ｇ）を生成する。ここでは、Ｓはホスト１０６ＢのＩＰアドレス、ＧはＡＢＣのグループＩＰアドレスである。ルータ１０４Ａは、アドレスＳに関してユニキャストルーティングテーブル内を照会して、ソースへの予備パスが、ルータ１０４Ｄへのリンク１０８Ａから出て行く

ことを決定する。ＰＩＭ－ＳＳＭを使用して、ＳＴＢルータ１０４Ａは、構文ＪＲ（Ｓ，Ｇ）を有する参加要求コマンドを生成する。ルータ１０４Ｄの作動は、説明される作動を除いて、ルータ１０４Ａに類似している。テーブルＢに、結果として得られるルータ１０４Ｂでのマルチキャスト転送テーブルを、変更を強調表示して示している。

【表２】

テーブルB

MFTグループ	マルチキャスト受信側リンク
ソースS=ホスト106B(10.1.2.3) グループG=ABC(239.0.0.1)	リンク108Aからセットトップボックス106C リンク108Cからルータ104C ***リンク108Bからルータ104D(およびホスト106Aへ)***
ソースS=ホスト106D(10.2.3.4) グループG=NBC(239.0.0.9)	リンク108Eからルータ104E
ソースS=ホスト106B(10.1.2.3) グループG=HBO(239.0.0.5)	リンク108Aからセットトップボックス106C

【００３５】

以下で詳しく説明するように、ＰＩＭ－ＳＳＭネットワークによるＩＧＭＰｖ２を組み込む別のシステムを提供する一実施形態を提供する。

【００３６】

一実施形態の詳細

一般に、本発明は、マルチキャスト配信グループのマルチキャストグループ加入を処理するシステムおよび方法を提供する。ルータがマルチキャストグループへの参加要求を受信したが、グループのソースの識別が提供されていないとき、ルータは、応答してグループソーステーブルから情報を取得してグループのソースを識別する。次にルータは、配信グループへの参加要求を作成し、要求をソース情報とともにグループに関連付けられているルータに送信する。

【００３７】

再度図１を参照すると、以下の例は、実施形態の動作態様を示している。残念ながら、セットトップボックス１０６Ａなどのレガシーセットトップボックスは、ＩＧＭＰｖ２プロトコルコマンドを生成できるだけにすぎず、したがって、ＩＧＭＰｖ３参加要求コマンドを実施することはできない。実施形態では、レガシーシステムが、ＩＧＭＰｖ２プロトコルを使用してＰＩＭ－ＳＳＭを使用するネットワークとインターフェースをとることができるようにする、インターフェース機構を提供する。実施形態では、レガシーセットトップボックス１０６Ａが、ＩＧＭＰｖ２　ＪＲ（＊，Ｇ）要求を生成したとき、その要求が、ＳＴＢルータ１０４Ａに送信され、ルータ１０４Ａは、次いで対応するＰＩＭ－ＳＳＭ　ＪＲ（Ｓ，Ｇ）要求を生成する。したがって、ＳＴＢルータ１０４Ａは、ＪＲ（＊，Ｇ）要求を受信すると、グループＧのソースＳを識別する必要がある。ソースが識別された後、参加要求ＪＲ（Ｓ，Ｇ）は、標準のＰＩＭ－ＳＳＭ手順に従ってソースホスト１０６に送信される。一般に、ＰＩＭ－ＳＳＭ動作は、単方向ツリーに基づいており、ツリーの根はソースであり、ツリーの葉は受信機である。ソース特定マルチキャスト（ＳＳＭ）は、ＳＳＭ宛先アドレスＧのソースＳからの、（Ｓ，Ｇ）の対で識別された「チャンネル」を定義する。グループをモデル化するツリーは、ソース専用ツリー、または最短パスツリー（ＳＰＴ）と呼ばれている。

【００３８】

実施形態による（Ｓ１，Ｇ１）の場合のＳＰＴの構成および使用の一例を示す。ネットワーク１００は、（１９０．１．１／２４とアドレス指定されている）サブネットワーク１１６Ａに受信機／ホスト１０６Ａを有する。ソースＳ１は、サブネットワーク１１６Ｂに関連付けられており、アドレスＳ１＝１００．１．１／２４，Ｇ１＝２３２．１．１．

１を有する。マルチキャスト受信機１０６Ａが、ソースＳ１からグループＧ１のトラフィックを受信したいとき、通知をサブネットワーク１１６Ｂに送信する必要がある。受信機１０６Ａは、この通知を実施するために、ＩＧＭＰｖ２またはＩＧＭＰｖ３メッセージをルータ１０４Ａに送信することができる。この例では、ルータ１０４Ａは、サブネットワーク１１６Ａ内の指定されたルータである。ルータ１０４Ａは、ツリー情報ベース（ＴＩＢ）におけるサブネットワーク１１６Ａ内の受信機１０６によってアクセスされるグループを追跡する。ルータ１０４Ａが、受信機１０６ＡからＩＧＭＰメッセージを受信したとき、ルータ１０４Ａは、そのＴＩＢで（Ｓ１，Ｇｌ）エントリを作成し、次いでＥｔｈｅｒｎｅｔ（登録商標）インターフェースＥ０をその発信インターフェースリストに配置する。このリストは、グループに参加しているインターフェースのリストである。

【００３９】

ルータ１０４Ａは、新しい（Ｓ１，Ｇ１）状態を作成しなければならないので、ソースＳ１に向かう上流側のルータ１０４に参加要求（Ｓ１，Ｇ１）コマンドを送信しなければならない。ルータ１０４Ａは、マルチキャストトポロジテーブルに問い合わせて、メッセージを送信する場所を決定する。この例では、ルータ１０４Ａは、参加要求（Ｓ１，Ｇ１）メッセージをルータ１０４Ｄに送信する。このように、参加要求（Ｓ１，Ｇ１）メッセージは、ホップごとにグループＧ１のＳ１に向かって移動し、それが通過する各ルータ１０４で、（Ｓ１，Ｇ１）状態がインスタンス化される。最後には、参加要求（Ｓ１，Ｇ１）メッセージは、Ｓ１、または（Ｓ１，Ｇ１）参加状態をすでに有するルータ１０４に到達する。

【００４０】

同様に、受信機１０４は、グループを離れることを要求することができる。サブネットワーク２０２のすべての受信機１０４が、グループを離れる場合、指定されたルータであるルータ１０４は、マルチキャストグループＧ１のソースＳ１に対してプルーン（Ｓ１，Ｇ１）メッセージを送信する。

【００４１】

実施形態において、すべてのソースおよびグループ情報が、各ルータ１０４に格納される。ソースおよびグループ情報の管理は、ネットワーク１００のコンピュータであるネットワークマネージャ１１０によって行われる。ソースおよびグループ情報は、テーブルで構成されていることが好ましい。ネットワークマネージャ１１０は、テーブルの内容を維持し、テーブルの情報が、確実にネットワーク１００のすべてのルータ１０４に配信されるようにする。実施形態では、ネットワークマネージャ１１０は、知られている任意の方法を使用して、リンク１０８を介してテーブルを配信することができる。

【００４２】

テーブルＣは、ネットワークのソースおよびグループ情報のテーブルの一例である。テーブルＣに対する任意の変更（追加および除去）は、すべてのルータ１０６に配信する必要がある。例えば、新しいチャンネル（ＦＯＸなど）が、ビデオサーバから送信を開始した場合、ネットワーク管理オペレータは、テーブルＣを、新しいチャンネルのグループおよびソースアドレスを含むように修正し、次いで更新されたテーブルを各ルータに配信する必要がある。

【表３】

テーブルC

チャンネル(グループG)	ソースホストS
ABC(239.0.0.1)	ホスト106B(10.1.2.3)
HBO(239.0.0.5)	ホスト106B(10.1.2.3)
NBC(239.0.0.9)	ホスト106D(10.2.3.4)
CBS(239.0.0.12)	ホスト106D(10.2.3.4)

【００４３】

ソースおよびグループ情報を使用して、実施形態では、次のように、生成を実行する代表的な通信装置としてルータ１０４Ａを使用して、ＪＲ（＊，Ｇ）ＩＧＭＰｖ２コマンドからＪＲ（Ｓ，Ｇ）ＰＩＭ－ＳＳＭコマンドを生成する。ルータ１０４Ａは、コマンドを生成する内部ハードウェアおよびソフトウェアモジュールを有している。特に、モジュールの態様は、状態マシンで実施される。

【００４４】

最初に、ルータ１０４Ａは、ホスト１０６ＡからＩＧＭＰｖ２　ＪＲ（＊，Ｇ）メッセージを受信する。ルータ１０４Ａは、プログラムのホストのアドレス指定情報を決定する必要がある。このためには、ルータ１０４Ａは、ソースおよびグループ情報テーブルにアクセスする。ＳＴＢルータは、グループＧの識別を知っているため、相互に関係のあるソースＳは、ソースおよびグループ情報テーブルから識別することができる。ソースＳ情報で、ＳＴＢルータ１０４Ａは、テーブルＢから「Ｓ」ＩＰアドレスと決定されたように、ＰＩＭ－ＳＳＭ　ＪＲ（Ｓ，Ｇ）にソースアドレスを配置するＰＩＭ－ＳＳＭ参加要求を構築する。ＰＩＭ－ＳＳＭは、ユニキャスト経路指定テーブルのアドレスＳの照会によって決定されたリンクに送信される。これは、ルータ１０４Ｄに向かうリンク１０８である。

【００４５】

グループ間の区別を容易にするために、一意のマルチキャストアドレスがマルチキャストグループ内の各グループに提供されて、ＩＧＭＰｖ１／ｖ２参加要求を可能にすることが好ましい。

【００４６】

実施形態では、ＰＩＭ－ＳＭ標準およびＰＩＭ－ＳＳＭ標準で規定されているように、ソースおよびグループ情報を「逆方向パス転送」（ＲＰＦ）参照とともに使用する。ＰＩＭ－ＳＭ標準によれば、（＊，Ｇ）参加の受信によって、ランデブーポイント（ＲＰ）と呼ばれるネットワークにおける特別なルータに基づく特別なＲＰＦチェックがもたらされる。上述したように、このステップは、実施形態では実行する必要がないので、実行しなくてもよい。実施形態では、ソースおよびグループ情報を調べてソースアドレス（Ｓ）を決定した後、ソースアドレス（Ｓ）情報を使用してＲＰＦ照会を行い、アドレスＳへの到達に使用する発信インターフェースを決定する。この例では、アドレスＳ（１０．１．２．３）に到達するための発信インターフェースは、リンク１０８Ａであり、これはルータ１０４Ｄにつながるリンクである。実施形態では、リンク１０８Ａ上の受信された（Ｓ，Ｇ）パケットが、ホスト１０６Ａに向かって送出されるようなデータパスを構成する。次いで実施形態は、ＰＩＭ－ＳＳＭ参加要求（Ｓ，Ｇ）をリンク１０８Ａを介してルータ１０４Ｄに送信する。

【００４７】

ルータ１０４Ｄは、ＰＩＭ－ＳＳＭ参加要求（Ｓ，Ｇ）を受信し、その要求を、ソースアドレスＳ１に関する別のＲＰＦ照会を行うその状態マシンに渡す。状態マシンは、アドレスＳに到達するための発信インターフェースが、ルータ１０４Ｂにつながるリンク１０８Ｂであることを決定する。実施形態は、リンク１０８Ｂを介して受信した（Ｓ，Ｇ）パケットをリンク１０８Ａに送信するようなデータパスを構成する。

【００４８】

次に、実施形態は、ＰＩＭ－ＳＳＭ参加要求（Ｓ，Ｇ）をリンク１０８Ｂを介してルータ１０４Ｂに送信する。ルータ１０４Ｂは、要求を受信し、ソースアドレスＳに対して第３のＲＰＦ照会を行うその状態マシンに要求を渡す。これは、アドレスＳに到達するための発信インターフェースが、ホスト１０６Ｂに向かうリンク１０８Ｃであることを決定する。実施形態は、リンク１０８Ｃを介して受信した（Ｓ，Ｇ）パケットを、リンク１０８Ｂに送出するようなデータパスを構成する。ここで、ホスト１０６Ｂからの（Ｓ，Ｇ）トラフィックは、ネットワーク１００を横断し、ホスト１０６Ａに到達する。

【００４９】

切断要求の場合、同様のプロトコルに従う。切断要求は、参加要求用と同じマルチキャ

ストツリートポロジに従う必要がある。

【００５０】

図２Ａを参照すると、ルータ１０４Ａの動作態様に関してさらに詳しく示している。ルータ１０４Ａは、他のルータ１０４およびホスト１０６などの外部装置に、インターフェースポイントを提供するラインカード２０２Ａ、２０２Ｂ、および２０２Ｃを有する。特に、ラインカード２０２Ａは、（ｉ）通信リンク１０８Ｆを介したホスト１０６Ａへの接続、および（ｉｉ）通信リンク１０８Ａを介したルータ１０４Ｄへの接続を提供する。ラインカード２０２Ｂは、リンク１０８Ｄを介したホスト１０６Ｄへの接続を提供する。図１に示したリンクおよびホストに加えて、図２Ａには、ラインカード２０２Ｃは、リンク１０８Ｇを介した追加のホスト１０６Ｇへの追加接続、およびリンク１０８Ｈを介した追加ホスト１０６Ｈへの追加接続を有するものとして示されている。また、ルータ１０４Ａは、転送情報の処理を提供する制御モジュール２０４を有する。外部装置は、ルータ１０４Ａによって管理されるグループに、ホスト１０６Ｂ、ルータ１０４Ｄ、ホスト１０６Ｇ、およびホスト１０６Ｈの順序で参加する。最後に、ホスト１０６Ｄは、ＩＰパケットをグループアドレスＧ１に送信する。ホスト１０６Ｄは、グループに参加したとき、ＩＧＭＰ参加メッセージを送信してグループＧ１に参加する。次いでラインカード２０２Ｂは、参加メッセージを検出し、ラインカード２０２Ａに提供する。ラインカードを使用しない実施形態の場合に、他のルータを提供できることは理解されよう。

【００５１】

図１を参照すると、別の実施形態は、マルチキャストトラフィックに関するサービス攻撃に対してネットワークを保護するための、選択的に実行可能なマルチキャストを提供する。別の装置は、ビデオサーバに加えて、異なるソースアドレスではあるが、同じグループアドレス（Ｓ’，Ｇ）によってマルチキャストトラフィックを送信することができる。セットトップボックスがグループ（＊，Ｇ）に参加することにより、ビデオサーバからの（Ｓ，Ｇ）トラフィックへの接続の要望を示すと、この特徴は、セットトップボックスによって受信されたトラフィックを、（Ｓ，Ｇ）トラフィックに制限する。（Ｓ’，Ｇ）または他の任意の（＊，Ｇ）トラフィックは、セットトップボックスに送信されない。

【００５２】

例えば、ＡＢＣチャンネルは、グループアドレス２３９．０．０．１でマルチキャストトラフィックの許可されたキャリアであるソースアドレス１０．１．２．３を使用して、ソースホスト１０６Ｂによって運ばれるグループアドレス２３９．０．０．１で運ばれる。ネットワークにおける別のホスト１０６Ｄは、不正または悪意でグループアドレス２３９．０．０．１上を伝送している。ホスト１０６Ｄは、これをそのソースアドレス１０．２．３．４で行わなければならない。この不正なチャンネルへの加入者はいないため、トラフィックは終了され、ルータ１０４Ａによって転送されない。各ルータでグループアドレス２３９．０．０．１が、ソースアドレス１０．１．２．３にマップされるため、他のホストは、この不正なチャンネルへの参加を試みることはできない。ソースアドレス１０．２．３．４を有するグループアドレス２３９．０．０．１に対して要求は生成されない。

【００５３】

具体的には、図２Ｂを参照すると、一実施形態では、許可されていないマルチキャスト伝送を阻止する伝送セキュリティの特徴も提供している。このセキュリティの特徴は、ＩＧＭＰｖ２参加要求（＊，Ｇ）をＩＧＭＰｖ３参加要求（Ｓ，Ｇ）に変換する変換プロセスを使用して、知られていない悪意のあるソースを評価して、所与のマルチキャストグループでの伝送から排除する。マルチキャストソースアドレスは、ＣＬＩを介して構成することができる。この特徴を使用して、マルチキャストトラフィックをサポートするネットワークソースに対するサービス拒否（ＤＯＳ）攻撃を防ぐことができる。

【００５４】

上述したように、ルータ１０４は、ルータ１０４と接続されているそれぞれのホスト１０６およびルータ１０４との間に接続ポイントを提供するラインカード２０２を有する。

各ラインカード２０２内には、機器構成の構成に応じて、ルータ１０４によって選択的に作動または非作動にできるインターフェース２０４が提供される。代替実施形態では、インターフェース２０４は、遠隔に制御されることができる。インターフェース２０４を非作動にすると、そのインターフェース２０４を介して受信されたデータトラフィックは、ルータ１０４によってネットワーク内の任意の他のポイントに転送されない。こうしたデータトラフィックは、単にルータ１０４によって破棄されるだけである。

【００５５】

図１および２Ｂを参照して、以下に、マルチキャストソース（ホスト１０６または他のルータ１０４）から受信されたときに、破棄されるパケットの例を示す。

【００５６】

・ルータ１０４Ａに関連付けられているマルチキャストグループ、例えばグループＧ１が空の場合、それに関連付けられているインターフェースはない。ホスト１０６Ｄが、そのインターフェース２０４を介してＩＰパケットをルータ１０４Ａに送信するとき、グループＧ１は空なので、インターフェースは実行不可になり、パケットは、ホスト１０６Ｄによって、インターフェース２０４Ａを介して受信されるルータ１０４Ａに送信される。インターフェース２０４Ｂは、マルチキャストソースとして実行不可になる。したがって、ホスト１０６Ｄから受信されたマルチキャストパケットは、ルータ１０４Ａによって破棄される。

【００５７】

・インターフェース２０４Ａが実行不可になり、ホスト１０６ＦがＩＧＭＰ参加要求（ホスト１０６Ａ，Ｇ１）を開始すると、ルータ１０６Ｃは、ＰＩＭ－ＳＳＭ参加要求（１０４Ａ，Ｇ１）をルータ１０４Ａに向かって送信し、インターフェース２０４Ａがマルチキャストソースとして実行不可になるので、マルチキャスト転送ツリーは作成されない。したがって、ホスト１０６Ｃから受信されたマルチキャストパケットは、ルータ１０４Ａによって破棄される。

【００５８】

・グループＧ２は、ルータ１０４Ａに構成されているが、それに関連付けられている受信機がなく、ホスト１０６Ｅが、ＩＰパケットをマルチキャストグループアドレスＧ２に送信する場合、ルータ１０４Ｅは、パケットをインターフェース２０４Ａを介してルータ１０４Ａに転送する。しかし、ここでは、ルータ１０４Ａ上のグループＧ２にはメンバがない。したがって、受信機がないため、ルータ１０４Ａはパケットを破棄する。

【００５９】

・ホスト１０６Ｄは、ＩＧＭＰｖ２を使用してＩＧＭＰ参加要求（Ｇ２）を送信する。しかし、グループ（ホスト１０６Ｄ，Ｇ２）は、ルータ１０４Ａでは構成されない。Ｇ２のソースはわからないため、マルチキャスト転送ツリーは作成されないので、パケットは、ルータ１０４Ａによって破棄される。

【００６０】

ＤＯＳ攻撃を防ぐために、ルータ１０４Ａの他の構成も提供できることを理解されたい。

【００６１】

上記の実施形態は、説明の目的で、ある程度の特定性で説明してきた。様々な変形および変更を、本発明の範囲から逸脱することなく、本明細書に開示した実施形態に加えることができることを当分野の技術者であれば理解されよう。

【図面の簡単な説明】

【００６２】

【図１】本発明の一実施形態によって動作するホストおよびルータを含む通信ネットワークのブロック図である。

【図２Ａ】図１の実施形態の動作上の態様を示す図１の通信ネットワークのルータのブロック図である。

【図２Ｂ】図１の実施形態の他の動作上の態様を示す図２Ａのルータのブロック図である

。

【符号の説明】

【００６３】

１００　ネットワーク
１０２　ネットワーククラウド
１０４Ａ、１０４Ｂ、１０４Ｃ、１０４Ｄ、１０４Ｅ　ルータ
１０６Ａ、１０６Ｂ、１０６Ｃ、１０６Ｄ、１０６Ｅ、１０６Ｆ、１０６Ｇ　ホスト
１０８　通信リンク
１１０　ネットワークマネージャ
１１２　経路指定テーブル
１１４　テレビ
１１６Ａ、１１６Ｂ、２０２　サブネットワーク
２０２Ａ、２０２Ｂ、２０２Ｃ　ラインカード
２０４　制御モジュール
２０４　インターフェース

【図１】

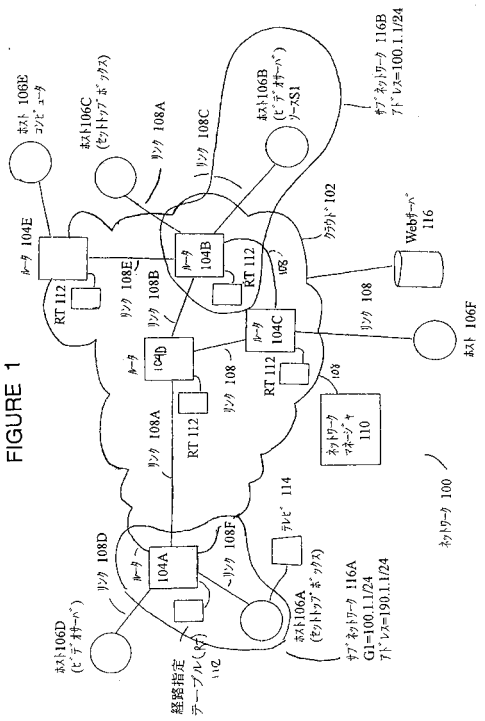

FIGURE 1

【図２Ａ】

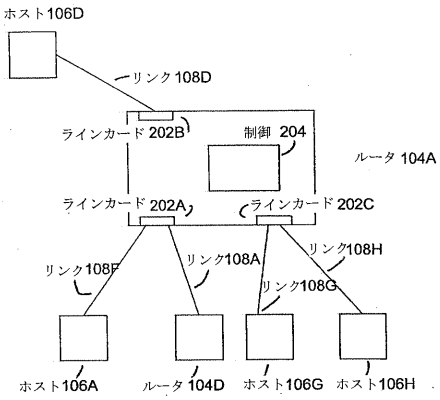

FIGURE 2A

【図２Ｂ】

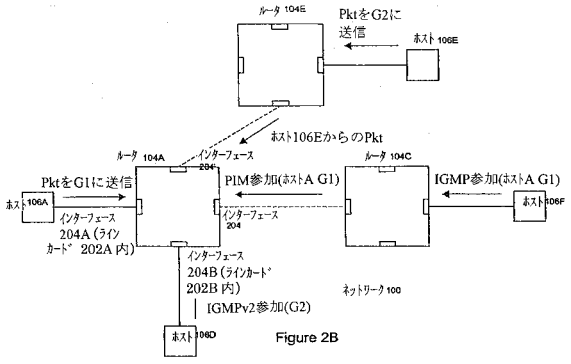

Figure 2B

フロントページの続き

(74)代理人 100124855
弁理士 坪倉 道明
(72)発明者 デイビツト・アンドリユウ・ワトキンソン
カナダ国、オンタリオ・ケー・２・ケー・２・アール・５、カナタ、イプスウイツチ・テラス・３１

Ｆターム(参考) 5K030 HB14 HB18 HD03 LB05 LD06

【外国語明細書】

Specification

Title of Invention

SYSTEM AND METHOD FOR CONVERTING REQUESTS BETWEEN DIFFERENT MULTICAST PROTOCOLS IN A COMMUNICATION NETWORK

FIELD OF THE INVENTION

The invention relates generally to data communications, in particular to a system and method for interfacing between routers and hosts running internet group management protocols.

BACKGROUND OF THE INVENTION

Digital media services provide subscribers with access to downloadable video information, such as television programs, movies, audio programs and text-based information streams. Typically, subscribers selectively access such services via a connection to a communication network. In the network, the services are provided from one or more information sources. Routers in the network are coupled to both the sources and the subscribers; the routers provide linking interfaces to enable the sources to transmit their services to the intended subscribers in the network.

Generally, when services are provided to a specific list of subscribers in a network, a multicast transmission is used. Therein, one router transmits messages to multiple destinations. For multicast transmissions, a router requires group information identifying members of a group which are to receive a specified multicast transmission. In an Internet Protocol (IP) v4 network, Internet Group Management Protocol (IGMP) commands are sent from hosts to routers in the network to manage IP multicast transmissions. IGMP is an evolving protocol. The Internet

Engineering Task Force (IETF) has published numerous specifications for IGMP, as its standards evolve, including: RFC 1112, entitled "Host Extensions for IP Multicasting"; RFC 2236, entitled "Internet Group Management Protocol, Version 2"; and RFC 3376 entitled "Internet Group Management Protocol, Version 3". All three specifications are incorporated herein by reference. IGMP, version 2 is designed to be interoperable with Protocol Independent Multicast - Sparse Mode (PIM-SM) multicasting. IGMP, version 3 adds the capability for Protocol Independent Multicast - Single Source Multicast (PIM-SSM) multicasting. PIM-SSM provides simplified processing in both the data plane and the control plane over PIM-SM. Unfortunately, some mapping constructs of IGMP v3 are not compatible with IGMP v2. This is problematic when a legacy host, which recognizes only IGMP version 2 protocol commands, is connected to a network which utilizes PIM-SSM.

Therefore, a need exists for a method and apparatus for supporting multicast group transmissions that provides PIM-SSM compatibility with legacy protocols.

SUMMARY OF THE INVENTION

In a first aspect, a method of generating a request in a protocol from another request formed in another protocol is provided. The request is related to a membership change to a group and the group is related a service provided by a host in a communication network. The method comprises receiving the request, identifying a target group from the request, identifying an associated host to the target group and generating in another protocol, another request containing a reference to the target group and the associated host. For the method, the request identifies the group and does not uniquely identify the associated host.

The service in the method may relate to a multicast transmission in the network.

The method may have the host identified by accessing data relating all hosts to all of their groups which are configured in the network.

The method may have the data being accessible by each router in the network.

For the method, an instance of the data may be stored locally at each router.

For the method, each instance of the data may be updated by a network manager computer associated with the network.

For the method, the another protocol may follow IGMP version 2 constructs and the request may follow IGMP version 3 constructs.

The method may have the another request generated at a requesting host in the network, which is received at a router connected to the requesting host.

The method may update a forwarding table associated with the group to reflect the request.

In a second aspect, a system for managing and converting a request in a protocol from another request formed in another protocol is provided. Therein, the request relates to changing a membership to a group and the group relates to a service provided by a host in a communication network. The system comprises a module for receiving the another request, data relating all hosts to all of their groups which are configured in the network, an identification module for identifying an associated host to the target group utilizing the data and a generation module for selectively generating the request containing a reference to the target group and the associated host. In the system, the another request identifies the group and does not uniquely identify the associated host.

The system may have the data accessible by each router in the network.

The system may store an instance of the data locally at each router; each instance of the data may be updated by a network manager computer associated with the network; the another protocol may follow IGMP version 2 constructs; and request may follow IGMP version 3 constructs.

The system further may comprise an evaluation module and a blocking module. The evaluation module evaluates access rights of the another request to the target group by utilizing membership information associated with the host and the target group; the blocking module selectively blocks the generation module from generating the request if the another request has access rights which are not acceptable.

In a third aspect, a method of evaluating and converting a request received in a protocol is provided. Therein, the request relates to joining a group and the group relates a service provided by a host in a communication network. The method comprises receiving the request, identifying a target group from the request, identifying an associated host to the target group, evaluating access rights of the request to the target group by utilizing membership information associated with the host and the target group, blocking the request if the request does not have acceptable access rights to the target group and generating another request containing a reference to the target group and the associated host if the access rights are acceptable. In the method, the request identifies the group and does not uniquely identify the associated host.

The method may have the request relating to a multicast transmission in the network; the another protocol may follow IGMP version 2 constructs; and the request may follow IGMP version 3 constructs.

In other aspects of the invention, various combinations and subsets of the above aspects are provided.

The foregoing and other aspects of the invention will become more apparent from the following description of specific embodiments thereof and the accompanying drawings which illustrate, by way of example only, the principles of the invention. In the drawings, where like elements feature like reference numerals which may bear unique alphabetical suffixes in order to identify specific instantiations of like elements.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

The description which follows, and the embodiments therein, are provided by way of illustrating an example, or examples, of particular embodiments of principles of the present invention. These examples are provided for the purpose of explanation, and not limitations, of those principles. In the description, which follows, like elements are marked throughout the specification and the drawings with the same respective reference numerals.

Prior Art Systems

Referring to Fig. 1, network 100 is shown. Aspects of network 100 are shown to illustrate prior art systems and an embodiment of the invention.

For a prior art system, network 100 enables network elements to be connected through cloud 102 to other network elements. In particular, network cloud comprises a series of routers 104 connected by communication links 108. As shown, cloud 102 comprises routers 104A, 104B, 104C, 104D and 104E. When data traffic is sent from a source device to a destination device in through network cloud 102, a communication path through various routers 104 must be defined.

The architecture of network 102 is preferably IP. Accordingly, address constructs for data traffic and path generation constructs follow IP constructs. As such, when establishing a path, it is extended from the source device to the destination device in segments by sequentially finding a router which can send the data traffic to an adjacent router which is in a segment of a communication path towards the destination device. Each router has a routing table 112 providing a map of the topology of network cloud 102 to assist each router in identifying a next segment for a routing path for received data traffic. Network manager 110 is connected to cloud 102 and is responsible for maintaining and updating routing tables 112 of each router 104. Network manager 110 is connected to each router 104 in cloud 102 via a communication link 108.

Hosts 106 are computing devices and each host has an IP address. Each host 106 is connected to a router 104 which provides the point of connection for host 106 to network 100. For example, hosts 106A and 106D are connected to network 100 via router 104A; hosts 106B and 106C are connected to network 100 via router 104B; host 106E is connected to router 104E

and host 106F is connected to router 104C. Connections are made via communication links 108. In other embodiments, the communication link between the hosts and their connecting router may be a broadband communication link such as an assymetric digital subscriber line, Ethernet connection, local multipoint data service (LMDS), or an asynchronous transfer mode (ATM) passive optical network (APON).

Some hosts may be used as storage sites for services (for example hosts 106B and 106D); a host may be a computer (host 106E and 106F) or set-top box (hosts 106A and 106C). A set-top box is used to request services from other hosts, such as multicast group transmissions. When configured to receive multicast transmissions, a set top box issues one or more requests to the router which connects it to network 100 to receive a multicast transmission corresponding to programming information selected by the user. In such an arrangement, when a user watching television changes channels, the set top box relays information concerning the channel change to the connecting router. Essentially, the set top box indicates to the connecting router that the previously viewed channel is no longer required and that a new multicast data stream corresponding to the channel to which the user has selected is required. Also, a personal computer may be configured as a host to request multicast groups in a similar manner as a set top box. Each of the hosts may be active or inactive at various points in time, and each of the hosts may request one or more multicast groups when active.

Therein, network 100 is used to provide, in part, access to digital video distribution services. A user of television 114 access network 100 to request downloads of specific video programs offered by the services from remote hosts 106. The user has a set-top box 106A connected to his display device (e.g. his television) and network 100; the set-top box 106A is a host and generates and transmits network requests for video programs initiated by the user. When the user wishes to download a video program, he accesses a menu (typically displayed on

television 114) and selects the desired video program from the menu. The set-top box 106A then issues a request to network 100 to receive the video program. The request sent by the set-top box 106A is received by router 104A, as the point of connection to network 100; in turn, router 104A must forward the request towards the source of the video program to network 100. In network 100, the host which provides the video program is host 106B.

In network 100, hosts 106B and 106D utilize IP multicasting protocols to have network 100 distribute their programs to requesting set-top boxes or computers. Multicasting provides the benefit of conserving bandwidth usage in network 100. With multicasting, a host can send one copy of the multicasted data once to its server rather than repeatedly sending the same data to its router, then having its router send the data to each subscribing service.

An IP multicast session is defined by sending a packet to a reserved multicast IP address, which in IPv4, comprise addresses in the Class D range, encompassing addresses from 224.0.0.0 to 239.255.255.255. Accordingly, by examining the source and destination IP addresses from the IP header of a packet, a router can determine over which links 108 the packet is to be multicasted. A multicast address identifies a particular transmission session rather than a specific physical destination host. This ensures that a host is able to join an ongoing multicast session.

In the prior art, there are three protocols governing the interaction of hosts and routers operating multicast protocols.

1. IGMPv2 interoperating with PIM-SM network, which is a standardized legacy protocol;
2. IGMPv3 interoperating with PIM-SM network, which is a recently standardized protocol; and

3. IGMPv3 interoperating with PIM-SSM network, which is another recently standardized solution.

The following example illustrates operating aspects of the protocol #3 where IGMPv3 requests are translated into PIM-SSM requests. To assist implementation a multicast of the video program, each router maintains a multicast forwarding table (MFT) of hosts associated with each video program. Each entry in the table has two components: the first component provides information on the multicasted program, including its Group's IP address and the source host of the program; the second component is a list of outgoing links (108) associated with the program. Table A is a representative multicast forwarding table for router 104B in network 100.

Table A

MFT Group	Multicast Receiving Links
Source S = host 106B (10.1.2.3) Group G = ABC (239.0.0.1)	Link 108A to Set-top box 106C, Link 108C to Router 104C
Source S = host 106D (10.2.3.4) Group G = NBC (239.0.0.9)	Link 108E to Router 104E
Source S = host 106B (10.1.2.3) Group G = HBO (239.0.0.5)	Link 108A to Set-top box 106C

The MFT may be included as a part of routing table 112. The MFT needs to be updated as multicast destinations are added and dropped from a group. In multicast routing, routers communicate with each other to exchange information about multicast group membership information to neighboring routers.

Using IGMPv3, a host 106A generates a JR (S, G) to router 104A, where S is the IP address of host 106B and G is the group IP address of ABC. Router 104A does a lookup in the unicast routing table on address S to determine that the reverse path towards the source egresses

out link 108A towards router 104D. Using PIM-SSM, STB router 104A will generate a join request command which has the syntax: JR (S, G). The behaviour of router 104D is similar to 104A and outside the scope of the behaviour being described. The resulting Multicast Forwarding Table at Router 104B is shown in Table B with the change highlighted.

Table B

MFT Group	Multicast Receiving Links
Source S = host 106B (10.1.2.3) Group G = ABC (239.0.0.1)	Link 108A to Set-top box 106C, Link 108C to Router 104C, **Link 108B to Router 104D (and on towards Host 106A)**
Source S = host 106D (10.2.3.4) Group G = NBC (239.0.0.9)	Link 108E to Router 104E
Source S = host 106B (10.1.2.3) Group G = HBO (239.0.0.5)	Link 108A to Set-top box 106C

As is discussed in detail below, an embodiment provides another system incorporating IGMPv2 with PIM-SSM network is provided.

Details of an Embodiment

Generally, the present invention provides a system and method for processing multicast group subscriptions for a multicast distribution group. When a router has received a request to join a multicast group, but has not been provided the identity of the source of the group, the router responsively obtains information from a group source table to identify the source for the group. Next, the router creates a request to join the distribution group and sends the request with the source information to the router associated with the group.

Again, referring to Fig. 1, the following example illustrates operating aspects of the embodiment. Unfortunately, legacy set-top boxes, such as set-top box 106A, can only generated IGMP v2 protocol commands and accordingly, cannot implement an IGMP v3 join request

command. The embodiment provides an interface mechanism allowing legacy systems to use IGMPv2 protocols to interface with a network which uses PIM-SSM. Therein, when a legacy set-top box 106A generates an IGMPv2 JR (*, G) request, it is sent to STB router 104A, which then generates a corresponding PIM-SSM JR (S, G) request. Accordingly, when a JR (*, G) request is received by STB router 104A, it needs to identify a source S for the group G. After the source is identified, the join request JR (S, G) is sent towards the source host 106 according to standard PIM-SSM procedures. Generally, PIM-SSM operation is based on a unidirectional tree whose root is the Source and whose leaves are the receivers. A Source Specific Multicast (SSM) defines a "channel" identified by an (S, G) pair, from source S for SSM destination address G. The tree which models the group is called source-specific tree, or shortest-path tree (SPT).

An example of construction and use of a SPT for (S1, G1) by the embodiment is provided. Network 100 has receiver/host 106A on subnetwork 116A (addressed as 190.1.1/24). Source S1 is associated with subnetwork 116B and has address S1=100.1.1/24, G1=232.1.1.1. When multicast receiver 106A wishes to receive traffic for group G1 from source S1, it must send a notification to subnetwork 116B. Receiver 106A may send an IGMPv2 or IGMPv3 message to implement this notification to router 104A which, in the example, is the designated router in subnetwork 116A. Router 104A tracks groups which are being accessed by receivers 106 in its subnetwork 116A in a tree information base (TIB). When router 104A receives the IGMP message from receiver 106A, router 104A creates an (S1, G1) entry in its TIB and then places the Ethernet interface E0 in its outgoing interface list which is a list of interfaces that have joined the group.

Since router 104A had to create a new (S1, G1) state, router 104A must send a Join Request (S1, G1) command to the upstream router 104 towards source S1. Router 104A consults a multicast topology table to decide where to send the message. In the example, router 104A

send a Join Request (S1,G1) message to router 104D. In this manner, the Join Request (S1,G1) message travels hop-by-hop towards S1 for the group G1 and, in each router 104 it passes through, a (S1,G1) state is instantiated. Eventually the Join Request (S1,G1) message either reaches S1, or reaches a router 104 that already has the (S1,G1) Join state.

Similarly, receivers 104 can request to leave a group. If all receivers 104 in subnetwork 202 leave a group, router 104, as the designated router, sends a Prune (S1,G1) message towards source S1 for multicast group G1.

In the embodiment, all of the source and group information is stored at each router 104. Management of the source and group information is performed by network manager 110 is a computer in network 100. The source and group information is preferably organized in a table. Network manager 110 maintains the contents of the table and ensures that information in the table is distributed to all routers 104 in network 100. For the embodiment, network manager 110 may use any known method to distribute the table over the links 108.

Table C is an exemplary table of the source and group information for a network. Any changes (additions and subtractions) to Table C need to be distributed to all routers 106. For example, if a new channel (e.g. FOX) starts transmitting from a video server, Table C needs to be modified to include the group and source address of the new channel by a network management operator and then the updated table needs to be distributed to each of the routers.

Table C

Channel (Group G)	Source Host S
ABC (239.0.0.1)	Host 106B (10.1.2.3)
HBO (239.0.0.5)	Host 106B (10.1.2.3)
NBC (239.0.0.9)	Host 106D (10.2.3.4)
CBS (239.0.0.12)	Host 106D (10.2.3.4)

Using the source and group information, the embodiment generates a JR (S, G) PIM-SSM command from a JR (*, G) IGMPv2 command as follows, using router 104A as a representative communication device to perform the generation. Router 104A has internal hardware and software modules to generate the command. In particular aspects of the modules are implemented in a state machine.

Initially, router 104A receives the IGMPv2 JR (*, G) message from host 106A. Router 104A needs to determine addressing information of the host of the program. To do this, router 104A accesses a source and group information table. As the STB router knows the identity of group G, the correlating source S can be identified from the source and group information table. With the source S information, STB router 104A builds a PIM-SSM join request placing the source address as determined from Table B as the "S" IP address in the PIM-SSM JR (S, G). The PIM-SSM is sent on a link as determined by a lookup of address S in the unicast routing table. This will be link 108 towards router 104D.

In order to facilitate distinguishing amongst groups, it is preferable that unique multicast addresses are provided to each group within the multicast groups in order to allow IGMP v1/v2 join requests.

In the embodiment, source and group information is used in conjunction with the "Reverse Path Forwarding" (RPF) lookup as defined in the PIM-SM and PIM-SSM standards. According to the PIM-SM standard, the reception of a (*, G) join results in a special RPF check based on a special router in the network named the Rendezvous Point (RP). As explained above, this step may not be performed by the embodiment, as it is not needed. In the embodiment, after the source and group information is examined to determine the source address (S), the source address (S) information is used to perform an RPF lookup to determine the outgoing interface

used to reach address S. In the present example, the outgoing interface to reach address S (10.1.2.3) is link 108A, which is the link leading towards router 104D. The embodiment configures the datapath such that received (S, G) packets on link 108A are sent out towards host 106A. The embodiment then sends a PIM-SSM Join Request (S, G) on link 108A towards router 104D.

Router 104D receives the PIM-SSM Join Request (S, G) and passes the request to its state machine which performs another RPF lookup on the source address S1. The state machine determines that the outgoing interface to reach address S is link 108B leading towards router 104B. The embodiment configures the datapath such that received (S, G) packets on link 108B are sent out towards link 108A.

Next, the embodiment sends a PIM-SSM Join Request (S, G) on link 108B towards router 104B. Router 104B receives the request and passes the request to its state machine which performs a third RPF lookup on the source address S. This determines that the outgoing interface to reach address S is link 108C towards host 106B. The embodiment configures the datapath such that received (S, G) packets on link 108C are sent out towards link 108B. Now (S, G) traffic from host 106B traverses network 100 and reaches host 106A.

For a disconnect request, a similar protocol is followed. The disconnect requests must follow the same multicast tree topology as they were for the join requests.

Referring to Fig. 2A, further detail is provided on operating aspects of router 104A. Router 104A has line cards 202A, 202B and 202C providing interface points to external devices, such as other routers 104 and hosts 106. In particular, line card 202A provides (i) a connection via communication link 108F to host 106A; and (ii) a connection via communication link 108A to router 104D. Line card 202B provides a connection via link 108D to host 106D. In addition

to links and hosts shown in Fig. 1, in Fig. 2A, line card 202C is shown as having an additional connection via link 108G to an additional host 106G and an additional connection via link 108H to an additional host 106H. Router 104A also has control module 204 which provides processing of the forwarding information. External devices join the group managed by router 104A in the following order: host 106B, router 104D, host 106G, and host 106H. Finally, host 106D transmits IP packets to group address G1. When host 106D joins the group, host 106D sends an IGMP join message to join group G1. Then, line card 202B detects join message and provides it line card 202A. It will be appreciated that other routers may be provided for the embodiment which do not use line cards.

Referring to Fig. 1, another embodiment provides for selectively enabled multicast to secure a network against denial of service attacks involving multicast traffic. Another device, besides the video server, would be able to send multicast traffic with a different source address but the same group address (S', G). When the set-top box joins group (*, G) implying the desire to connect to the (S, G) traffic from the video server, this feature restricts the traffic received by the set-top box to the (S, G) traffic. The (S', G) or any other (*, G) traffic is not sent to the set-top box.

For example, the ABC channel is carried on group address 239.0.0.1 which is carried by source host 106B using source address 10.1.2.3 is the authorized carrier of multicast traffic on group address 239.0.0.1. Another host 106D in the network is improperly or maliciously transmitting on group address 239.0.0.1. The host 106D must do this with its source address 10.2.3.4. The traffic is terminated and not forwarded by Router 104A as there are no subscribers to this improper channel. No other host can attempt to join this improper channel as on each router the group address 239.0.0.1 is mapped to the source address 10.1.2.3. There will be no requests generated for group address 239.0.0.1 with the source address 10.2.3.4.

Specifically, referring to Fig. 2B, an embodiment also provides a transmission security feature which blocks unauthorized multicast transmissions. This security feature utilizes the conversion process of converting IGMPv2 join requests (*, G) to IGMPv3 join requests (S, G) to evaluate and exclude unknown malicious sources from transmitting on a given multi-cast group. The multicast source addresses can be configured through CLI. This feature may be used to prevent denial of service (DOS) attacks on a network source which supports multicast traffic.

As noted above, router 104 has line cards 202 which provide connection points between it and each connected host 106 and router 104. Within each line card 202, an interface 204 is provided, which may be selectively activated or deactivated by its router 104, depending on configuration constructs. In alternative embodiments, an interface 204 may be remotely controlled. When an interface 204 is deactivated, no data traffic received through its interface 204 will be forwarded by the router 104 to any other point in the network. Such data traffic may simply be discarded by the router 104.

Referring to Figs. 1 and 2B, following are instances of packets being discarded when received from a multicast source (either from a host 106 or another router 104):

- If a multicast group associated with router 104A, for example, group G1, is empty, there is no interface associated with it. When host 106D transmits IP packets to router 104A via its interface 204, as Group G1 is empty, the interface is disabled and packets sent by host 106D to router 104A which is received through interface 204A, interface 204B is disabled as a multicast source. As such, multicast packets received from host 106D are discarded by router 104A.
- If interface 204A is disabled and if host 106F initiates a IGMP Join Request (host 106A, G1), router 106C sends a PIM-SSM Join request (104A, G1) towards router 104A, no multicast

forwarding tree is created since interface 204A is disabled as a multicast source. As such, multicast packets received from host 106C are discarded by router 104A.

- If Group G2 is configured on router 104A, but has no receiver associated with it, then if host 106E transmits IP packets to multicast group address G2, router 104E forwards the packets to router 104A through interface 204A. However, here, there is no member in group G2 on router 104A; as such, router 104A discards packets since there is no receivers.
- Host 106D sends an IGMP Join Request (G2) using IGMPv2. However, the group (host 106D, G2) is not configured on router 104A. As a multicast forwarding tree is not created since source of G2 is unknown, packets are discarded by router 104A.

It will be appreciated that other configurations for router 104A may also be provided to prevent DOS attacks.

The foregoing embodiment has been described with a certain degree of particularity for the purposes of description. Those skilled in the art will understand that numerous variations and modifications may be made to the embodiments disclosed herein without departing from the scope of the invention.

Brief Description of Drawings

Fig. 1 is a block diagram of a communication network including a host and a router which operate in accordance with an embodiment of the present invention.

Fig. 2A is a block diagram of a router in the communication network of Fig. 1 illustrating operational aspects of the embodiment of Fig. 1.

Fig. 2B is another block diagram of the router of Fig. 2A illustrating additional operational aspects of the embodiment of Fig. 1.

Claims

1. A method of generating a request in a protocol from another request formed in another protocol, said request relating to a change of membership to a group, said group relating a service to a host of said service in a communication network, said method comprising:

receiving said request;

identifying a target group from said request;

identifying an associated host to said target group; and

generating in another protocol another request containing a reference to said target group and said associated host,

wherein said request identifies said group and does not uniquely identify said associated host.

2. The method of generating a request in a protocol from another request formed in another protocol as claimed in claim 1, wherein said service is a multicast transmission within in said network.

3. The method of generating a request in a protocol from another request formed in another protocol as claimed in claim 2, wherein said host is identified by accessing data relating all hosts to all of their groups which are configured in said network.

4. The method of generating a request in a protocol from another request formed in another protocol as claimed in claim 3, wherein said data is accessible by each router in said network.

5. The method of generating a request in a protocol from another request formed in another protocol as claimed in claim 4, wherein an instance of said data is stored locally at said each router.

6. The method of generating a request in a protocol from another request formed in another protocol as claimed in claim 5, wherein each said instance of said data is updated by a network manager computer associated with said network.

7. The method of generating a request in a protocol from another request formed in another protocol as claimed in claim 6 wherein said another protocol follows IGMP version 2 constructs and said request follows IGMP version 3 constructs.

8. The method of generating a request in a protocol from another request formed in another protocol as claimed in claim 7 wherein said another request is generated at a requesting host in said network and is received at a router connected to said requesting host.

9. The method of generating a request in a protocol from another request formed in another protocol as claimed in claim 8 wherein an update reflecting said request is performed to a forwarding table associated with said group.

10. A system for managing and converting a request in a protocol from another request formed in another protocol, said request relating to a membership change to a group, said group relating a service to a host in a communication network, said system comprising:

a module for receiving said another request;

data relating all hosts to all of their groups which are configured in said network;

an identification module for identifying an associated host to said target group utilizing said data; and

a generation module for selectively generating said request containing a reference to said target group and said associated host,

wherein said another request identifies said group and does not uniquely identify said associated host.

11. The system for managing and converting a request in a protocol from another request formed in another protocol, as claimed in claim 10, wherein said data is accessible by each router in said network.

12. The system for managing and converting a request in a protocol from another request formed in another protocol, as claimed in claim 11, wherein

an instance of said data is stored locally at said each router;

each said instance of said data is updated by a network manager computer associated with said network;

said another protocol follows IGMP version 2 constructs; and

said request follows IGMP version 3 constructs.

13. The system for managing and converting a request in a protocol from another request formed in another protocol, as claimed in claim 12, wherein said system further comprises

an evaluating module to evaluate access rights of said another request to said target group by utilizing membership information associated with said host and said target group; and

a blocking module to selectively block said generation module from generating said request if said another request does not said access rights are not acceptable.

14. A method of evaluating and converting a request received in a protocol, said request relating to joining a group, said group being relating a service provided by a host in a communication network, said method comprising:

receiving said request;

identifying a target group from said request;

identifying an associated host to said target group;

evaluating access rights of said request to said target group by utilizing membership information associated with said host and said target group; and

blocking said host from said target group if said request does not have acceptable access rights to said target group; and

generating another request containing a reference to said target group and said associated host if said access rights are acceptable,

wherein said request identifies said group and does not uniquely identify said associated host.

15. The method of evaluating and converting a request received in a protocol, said request being to distribute a file to a group 14, wherein

said service is a multicast transmission to said network;

said another protocol follows IGMP version 2 constructs; and

said request follows IGMP version 3 constructs.

1. Abstract

The invention provides a system and method for generating and evaluating a request in a protocol from another request formed in another protocol. Therein, the request relates to a change of membership to a group and the group relates a service to a host of the service in a communication network. In particular, the method comprises receiving said request, identifying a target group from said request, identifying an associated host to said target group and generating in another protocol another request containing a reference to said target group and said associated host. The request identifies said group and does not uniquely identify said associated host. The invention provides the ability to block a request from proceeding further if it does not belong to a recognized group.

2. Representative Drawing

Fig. 1

Fig. 1

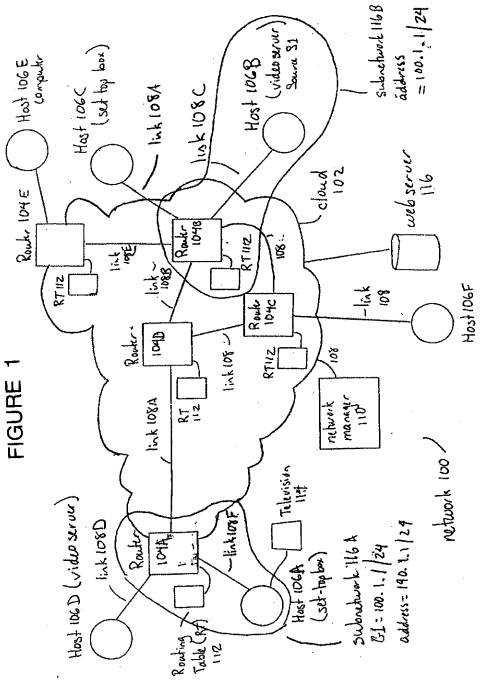

FIGURE 1

Fig. 2 A

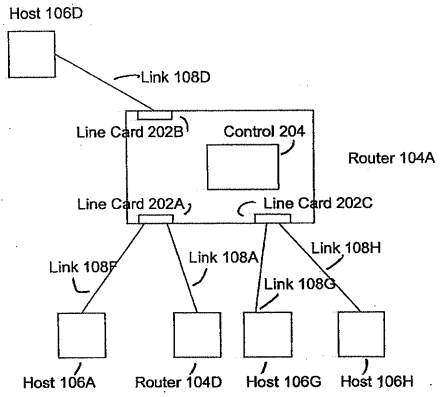

FIGURE 2A

Fig. 2 B

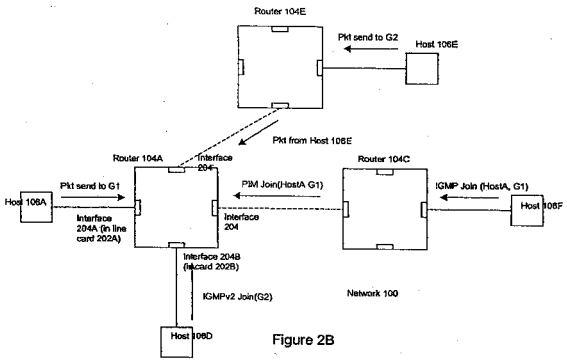

Figure 2B