(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2014 年 7 月 24 日(24.07.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/112616 A1

(51) 国際特許分類:
H04L 12/717 (2013.01) *H04L 12/66* (2006.01)

(21) 国際出願番号: PCT/JP2014/050923

(22) 国際出願日: 2014 年 1 月 20 日(20.01.2014)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2013-008835 2013 年 1 月 21 日(21.01.2013) JP

(71) 出願人: 日本電気株式会社(NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者: 千葉　靖伸(CHIBA, Yasunobu); 〒1088001 東京都港区芝五丁目７番１号　日本電気株式会社内 Tokyo (JP). 須堯　一志(SUGYOU, Kazushi); 〒1088001 東京都港区芝五丁目７番１号　日本電気株式会社内 Tokyo (JP).

(74) 代理人: 加藤　朝道(KATO, Asamichi); 〒2220033 神奈川県横浜市港北区新横浜３丁目２０番１２号加藤内外特許事務所内 Kanagawa (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) **Title**: CONTROL APPARATUS, COMMUNICATION APPARATUS, COMMUNICATION SYSTEM, SWITCH CONTROL METHOD AND PROGRAM

(54) 発明の名称 : 制御装置、通信装置、通信システム、スイッチの制御方法及びプログラム

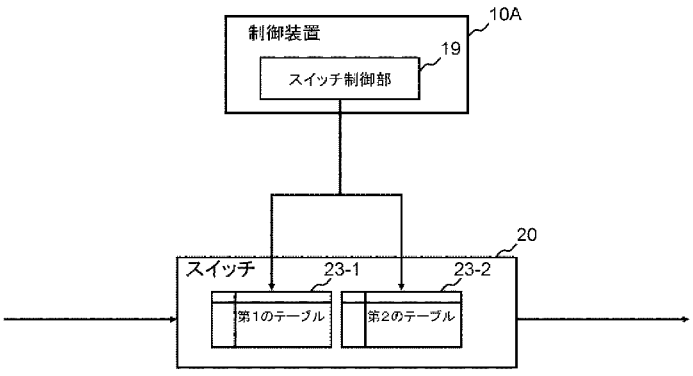


FIG. 1:
10A Control apparatus
19 Switch control unit
20 Switch
23-1 First table
23-2 Second table

(57) **Abstract**: The objective of the invention is to reduce the load of managing flow entries that are set in a switch in a centralized control type network. A control apparatus sets, in a first table included in a switch, a first entry used to filter packets received by the switch, and also sets, in a second table include in the switch, a second entry including a rule for processing one of the received packets that is selected by use of the first entry.

(57) 要約:　集中制御型のネットワークにおけるスイッチに設定するフローエントリの管理負担を軽減する。制御装置は、スイッチが備える第１のテーブルに、前記スイッチの受信パケットをフィルタリングするための第１のエントリを設定し、前記スイッチが備える第２のテーブルに、前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを設定する。

WO 2014/112616 A1

明　細　書

発明の名称 ：

制御装置、通信装置、通信システム、スイッチの制御方法及びプログラム

技術分野

[0001] ［関連出願についての記載］

本発明は、日本国特許出願：特願２０１３－００８８３５号（２０１３年１月２１日出願）に基づくものであり、同出願の全記載内容は引用をもって本書に組み込み記載されているものとする。

本発明は、制御装置、通信装置、通信システム、スイッチの制御方法及びプログラムに関し、特に、ネットワークに配置されたスイッチを集中制御する制御装置、通信システム、スイッチの制御方法及びプログラムに関する。

背景技術

[0002] 近年、オープンフロー（ＯｐｅｎＦｌｏｗ）という技術が提案されている（非特許文献１、２参照）。オープンフローは、通信をエンドツーエンドのフローとして捉え、フロー単位で経路制御、障害回復、負荷分散、最適化を行うものである。非特許文献２に仕様化されているオープンフロースイッチは、オープンフローコントローラとの通信用のセキュアチャネルを備え、オープンフローコントローラから適宜追加または書き換え指示されるフローテーブルに従って動作する。フローテーブルには、フロー毎に、パケットヘッダと照合するマッチ条件（Ｍａｔｃｈ　Ｆｉｅｌｄｓ）と、フロー統計情報（Ｃｏｕｎｔｅｒｓ）と、処理内容を定義したインストラクション（Ｉｎｓｔｒｕｃｔｉｏｎｓ）と、の組が定義される（非特許文献２の「４．１　Ｆｌｏｗ　Ｔａｂｌｅ」の項参照）。

[0003] 例えば、オープンフロースイッチは、パケットを受信すると、フローテーブルから、受信パケットのヘッダ情報に適合するマッチ条件（非特許文献２の「４．３　Ｍａｔｃｈ　Ｆｉｅｌｄｓ」参照）を持つエントリを検索する。検索の結果、受信パケットに適合するエントリが見つかった場合、オープ

ンフロースイッチは、フロー統計情報（カウンタ）を更新するとともに、受信パケットに対して、当該エントリのインストラクションフィールドに記述された処理内容（指定ポートからのパケット送信、フラッディング、廃棄等）を実施する。一方、検索の結果、受信パケットに適合するエントリが見つからなかった場合、オープンフロースイッチは、セキュアチャネルを介して、オープンフローコントローラに対してエントリ設定の要求、即ち、受信パケットの処理内容の決定の要求（Ｐａｃｋｅｔ－ＩｎメッセージＩ）を送信する。オープンフロースイッチは、処理内容が定められたフローエントリを受け取ってフローテーブルを更新する。このように、オープンフロースイッチは、フローテーブルに格納されたエントリを処理規則として用いてパケット転送を行う。

[0004] 非特許文献２のＯｐｅｎＦｌｏｗ Ｓｗｉｔｃｈ Ｓｐｅｃｉｆｉｃａｔｉｏｎ Ｖｅｒｓｉｏｎ １．１．０では、さらに、処理内容（Ｉｎｓｔｒｕｃｔｉｏｎ）として、他のフローテーブルへの遷移を指示する命令（Ｇｏ－ｔｏ Ｔａｂｌｅ）を設定することにより、複数のフローテーブルを使って複数の処理内容を実行するパイプライン処理を実施することもできる（非特許文献２の「４．１．１ Ｐｉｐｅｌｉｎｅ Ｐｒｏｃｅｓｓｉｎｇ」参照）。

先行技術文献

非特許文献

[0005] 非特許文献1：Ｎｉｃｋ ＭｃＫｅｏｗｎほか７名、“ＯｐｅｎＦｌｏｗ：Ｅｎａｂｌｉｎｇ Ｉｎｎｏｖａｔｉｏｎ ｉｎ Ｃａｍｐｕｓ Ｎｅｔｗｏｒｋｓ”、［ｏｎｌｉｎｅ］、［平成２４（２０１２）年１１月２２日検索］、インターネット〈URL:http://www.openflow.org/documents/openflow-wp-latest.pdf〉

非特許文献2：“ＯｐｅｎＦｌｏｗ Ｓｗｉｔｃｈ Ｓｐｅｃｉｆｉｃａｔｉｏｎ” Ｖｅｒｓｉｏｎ １．１．０ Ｉｍｐｌｅｍｅｎｔｅｄ （Ｗｉｒｅ Ｐｒｏｔｏｃｏｌ ０ｘ０２）、［ｏｎｌｉｎｅ］、［平成２４（２０

１２）年１１月２２日検索］、インターネット〈URL:http://www.openflow.org/documents/openflow-spec-v1.1.0.pdf〉

発明の概要

発明が解決しようとする課題

[0006] 以下の分析は、本発明によって与えられたものである。非特許文献２には、上述の通り、複数のフローテーブルを用いてパケットの処理を行うことが記載されている。しかしながら、上述したように、パイプライン処理を用いて、あるフローテーブルのエントリでパケットのヘッダを書き換えた後、次のフローテーブルでは前記書き換え後のヘッダにて該当するエントリを検索するといった用法が記載されるに止まっており、複数のフローテーブルの具体的用法については記載されていない。

[0007] 非特許文献１には、上述の通り、オープンフロースイッチに関する記載が開示されているが、スイッチがフローテーブルを複数有することに関しては記載されていない。

[0008] 本発明は、集中制御型のネットワークのスイッチに設定するエントリの管理負担の軽減に貢献できる制御装置、通信装置、通信システム、スイッチの制御方法及びプログラムを提供することを目的とする。

課題を解決するための手段

[0009] 第１の視点によればパケットを処理するための規則を含むエントリをスイッチに設定する制御装置であって、前記スイッチが備える第１のテーブルに、前記スイッチの受信パケットをフィルタリングするための第１のエントリを設定し、前記スイッチが備える第２のテーブルに、前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを設定する制御装置が提供される。

[0010] 第２の視点によれば、パケットを処理するための規則を含むエントリを制御装置から受信し、当該エントリに従って前記パケットを処理する通信装置であって、前記通信装置の受信パケットをフィルタリングするための第１のエントリを格納するための第１のテーブルと、前記受信パケットのうち、前

記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを格納するための第２のテーブルと、を備える通信装置が提供される。

[0011] 第３の視点によれば、受信パケットをフィルタリングするための第１のエントリを格納するための第１のテーブルと、前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを格納するための第２のテーブルと、を備え、前記第１、第２のテーブルに格納するエントリを制御装置から受信し、当該エントリに従って前記パケットを処理する通信装置と、前記スイッチが備える第１のテーブルに、前記スイッチの受信パケットをフィルタリングするための第１のエントリを設定し、前記スイッチが備える第２のテーブルに、前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを設定する制御装置と、を含む通信システムが提供される。

[0012] 第４の視点によれば、パケットを処理するための規則を含むエントリをスイッチに設定する制御装置が、前記スイッチが備える第１のテーブルに、前記スイッチの受信パケットをフィルタリングするための第１のエントリを設定するステップと、前記スイッチが備える第２のテーブルに、前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを設定するステップと、を含むスイッチの制御方法が提供される。本方法は、スイッチを制御する制御装置という、特定の機械に結びつけられている。

[0013] 第５の視点によれば、パケットを処理するための規則を含むエントリをスイッチに設定するコンピュータに、前記スイッチが備える第１のテーブルに、前記スイッチの受信パケットをフィルタリングするための第１のエントリを設定する処理と、前記スイッチが備える第２のテーブルに、前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを設定する処理と、を実行させるプログラムが

提供される。なお、このプログラムは、コンピュータが読み取り可能な（非トランジエントな）記憶媒体に記録することができる。即ち、本発明は、コンピュータプログラム製品として具現することも可能である。

発明の効果

[0014] 本発明によれば、複数のテーブルを用いて、スイッチが受信するパケットに対するフィルタリングを行うことが可能となる。

図面の簡単な説明

[0015] [図1]本発明の第１の実施形態の構成を示す図である。

[図2]本発明の第１の実施形態の動作を説明するための図である。

[図3]本発明の第１の実施形態の通信システムの構成を示す図である。

[図4]本発明の第１の実施形態のスイッチの構成を表した図である。

[図5]本発明の第１の実施形態のテーブルの例を示した図である。

[図6]本発明の第１の実施形態の制御装置の構成を表した図である。

[図7]本発明の第１の実施形態の制御装置の変形構成を表した図である。

[図8]本発明の第１の実施形態のテーブルの別の例を示した図である。

[図9]本発明の第１の実施形態の通信システムの構成を示す図である。

[図10]本発明の第１の実施形態のスイッチにおいて、テーブルを１つ用いる場合のエントリの設定例を示した図である。

[図11]本発明の第１の実施形態のテーブルの例を示した図である。

[図12]本発明の第２の実施形態の通信システムの構成を表した図である。

[図13]本発明の第２の実施形態のスイッチの詳細構成を示す図である。

[図14]本発明の第２の実施形態の制御装置の詳細構成を示す機能ブロック図である。

[図15]本発明の第２の実施形態の制御装置の仮想ネットワーク構成管理部に保持される仮想ネットワーク構成情報の一例である。

[図16]本発明の第２の実施形態の制御装置によってスイッチに設定される第１のテーブルのエントリの例である。

[図17]本発明の第２の実施形態の制御装置によってスイッチに設定される第

２のテーブルのエントリの例である。

[図18]本発明の第２の実施形態の制御装置によってスイッチに設定される第３のテーブルのエントリの例である。

[図19]本発明の第２の実施形態の制御装置のアクセスポリシ管理部に保持されるアクセスポリシの一例である。

[図20]図１９のアクセスポリシによる第２のテーブルの操作内容を説明するための図である。

[図21]図１２のスイッチ２００Ｂの接続により更新された仮想ネットワーク構成情報の一例である。

[図22]図１２のスイッチ２００Ｂの接続による第１のテーブルの操作内容を説明するための図である。

[図23]図１２のスイッチ２００Ｂの接続による第３のテーブルの操作内容を説明するための図である。

[図24]本発明の第１の実施形態のスイッチの動作を説明するための図である。

[図25]図２２、図２３のテーブルに設定されたエントリにより実現されるパケット転送経路を示す図である。

[図26]本発明の第３の実施形態の制御装置によってスイッチに設定される第１のテーブルのエントリの例である。

[図27]本発明の第３の実施形態の制御装置によってスイッチに設定される第２のテーブルのエントリの例である。

[図28]本発明の第３の実施形態の制御装置によってスイッチに設定される第３のテーブルのエントリの例である。

[図29]図１２のスイッチ２００Ｂの接続による第１のテーブルの操作内容を説明するための図である。

[図30]図１２のスイッチ２００Ｂの接続による第２のテーブルの操作内容を説明するための図である。

[図31]図１２のスイッチ２００Ｂの接続による第３のテーブルの操作内容を

説明するための図である。

[図32]本発明の第３の実施形態のスイッチの動作を説明するための図である。

発明を実施するための形態

[0016] ［第１の実施形態］

はじめに本発明の第１の実施形態について図面を参照して説明する。なお、以下の実施形態に付記した図面参照符号は、理解を助けるための一例として各要素に便宜上付記したものであり、本発明を図示の態様に限定することを意図するものではない。

[0017] 第１の実施形態は、図１に示すように、複数のテーブルを参照して受信パケットを処理するスイッチ２０に、受信パケットをフィルタリングする第１のテーブル２３－１と、第１のテーブル２３－１によって選別されたパケットを処理する第２のテーブル２３－２と、を保持させるスイッチ制御部を備える制御装置を有する通信システムに適用できる。スイッチ２０は、それぞれ物理的なスイッチでもよいが、サーバ等の装置上で動作する仮想スイッチであってもよい。また、スイッチ２０は、携帯電話やスマートフォン等の端末上で仮想的に動作する仮想スイッチであってもよい。

[0018] 例えば、第１のテーブル２３－１には、フィルタリング対象のパケットを特定するためのマッチ条件と、廃棄等の処理内容とを対応付けたエントリと、その他のパケットを特定するマッチ条件と、第２のテーブル２３－２を参照して処理するよう指示する処理内容とを対応付けたエントリとが設定される。上記構成によれば、図２に示すように、スイッチ２０は、第１のテーブル２３－１を参照して、例えば、第２のテーブル２３－２を参照した処理決定の対象となるパケットと、それ以外のパケットとを選別する動作を行う。そして、スイッチ２０は、第２のテーブル２３－２を参照して、前記選別されたパケットについて適用する処理を求め、転送処理等を実行する。なお、第１のテーブル２３－１を用いて行われるフィルタリングの例としては、例えば、ループを発生させるパケットや異常パケット等を廃棄することや、あ

る特定のホスト間の通信や特定のパケット等に対するアクセス制御を行うこと等が挙げられる。また、これらのパケットに適用する処理としては、廃棄のほか、所定の宛先へのリダイレクトなどを行ってもよい。また、図２の例では、第１のテーブル２３－１が一つである例を示しているが、第１のテーブル２３－１に相当するテーブルを複数用意し、それぞれのテーブルを用いて、異なる観点でフィルタリングを行うようにしてもよい。

[0019] 図３は、第１の実施形態の通信システムの構成を示す図である。本発明は、第１の実施形態において、複数のスイッチ２０Ａ、２０Ｂを制御して端末とサーバ間の通信を実現する制御装置にて実現できる。

[0020] 図４は、スイッチ２０Ａ、２０Ｂ（以下、スイッチ２０Ａ、２０Ｂを特に区別しない場合「スイッチ２０」と記す。）の詳細構成を示す図である。図４を参照すると、制御メッセージ送受信部２１と、パケット処理部２２と、テーブル２３とを備えた構成が示されている。なお、以下では、第１のテーブルと第２のテーブルとを区別しない場合「テーブル２３」とも記す。

[0021] 制御メッセージ送受信部２１は、制御装置１００からテーブルの操作に関する制御メッセージを受信し、テーブルの更新を行う。また、制御メッセージ送受信部２１は、制御装置１００に対するテーブル２３に登録するエントリの送信要求や、制御装置１００からのパケット出力指示に応じた動作を実行する。

[0022] パケット処理部２２は、パケットを受信すると、テーブル２３を参照し、受信パケットに適合するマッチ条件を持つエントリを検索し、該当するエントリに定められた動作を実行する。

[0023] テーブル２３は、上述の通り、第１のテーブルと、第２のテーブルとを含む。

[0024] 図５は、テーブル２３の構成例を示している。図５の例では、マッチ条件が「Ａ」というパケットに対しては通信を許容し、マッチ条件が「Ｂ」というパケットに対しては、フィルタリングを行うというポリシを適用している。

[0025] 第１のテーブルの１番目のエントリには、「Ａ」というマッチ条件のパケットに対しては、第２のテーブルを参照させるという処理が設定されている。また、第１のテーブルの２番目のエントリには、「Ｂ」というマッチ条件のパケットに対して、そのパケットを廃棄するという処理が設定されている。

[0026] また、第２のテーブルの１番目のエントリには、マッチ条件「Ａ」というパケットに対して、そのパケットをポート＃２から転送させるという処理が設定されている。

[0027] 図６は、第１の実施形態の制御装置１００Ｃの構成を表した図である。制御装置１００Ｃは、フィルタリングポリシ管理部１１１と、処理決定部１１３と、２つのテーブル操作部１１４、１１５と、スイッチ通信部１０７とを備えて、スイッチ２０を制御する構成が示されている。なお、図６の例では、テーブル操作部は２つ設けられているが、複数ではなく、制御装置１００Ｃ内に１つ設けられていてもよい。

[0028] より具体的には、フィルタリングポリシ管理部１１１は、スイッチが受信するパケットをフィルタリングするためのポリシを管理する。前記ポリシ（フィルタリングポリシ）の例としては、ホストからのループパケット等、異常なパケットを廃棄するためのポリシや、ある特定のホストからのパケットを廃棄するようなアクセス制御のためのポリシ等が挙げられる。

[0029] そして、テーブル操作部１１４は、フィルタリングポリシ管理部１１１に管理されているポリシを参照して、スイッチ２０の第１のテーブル２３－１に設定するエントリを作成し、スイッチ通信部１０７経由でスイッチ２０に送信する。

[0030] 処理決定部１１３は、前記テーブル操作部１１４が生成するフィルタリング用のエントリによって選別されたパケットについて適用する処理を決定する。

[0031] そして、もう一方のテーブル操作部１１５は、スイッチ２０に、処理決定部１１３にて決定された処理を実行させるための第２のテーブル２３－２の

エントリを作成し、スイッチ通信部１０７経由でスイッチ２０に送信する。

[0032] 図６のスイッチ２０は、図４に示した構成を有し、制御装置１００からテーブルの操作に関する制御メッセージを受信し、テーブル２３－１、２３－２の更新を行う。また、スイッチ２０は、制御装置１００に対するテーブル２３－１、２３－２に登録するエントリの送信要求や、制御装置１００からのパケット出力指示に応じた動作を実行する。そして、スイッチ２０は、パケットを受信すると、テーブル２３－１、２３－２を参照し、受信パケットに適合するマッチ条件を持つエントリを検索し、該当するエントリに定められた動作を実行する。例えば、スイッチ２０は、「Ａ」というマッチ条件に適合するパケットを受信した場合、第２のテーブルを参照し、処理を決定する。また例えば、スイッチ２０は、「Ｂ」というマッチ条件に適合するパケットを受信した場合、そのパケットを廃棄する動作を行う。

[0033] また、スイッチ２０に、フィルタリングを行うためのテーブルを複数設けて、それぞれのテーブルを用いて、異なる観点でフィルタリングを行うようにすることもできる。この場合の構成について、以下説明する。図７は、制御装置１００Ｄの構成を表した図である。制御装置１００Ｄは、第１のフィルタリングポリシ管理部１２１と、第２のフィルタリングポリシ管理部１２２と、処理決定部１１３と、３つのテーブル操作部１２４、１２５、１２６と、スイッチ通信部１０７とを備えて、スイッチ２０を制御する構成が示されている。また、スイッチ２０は、第１のテーブル２３－１、第２のテーブル２３－２、第３のテーブル２３－３の３つのテーブルを備える。

[0034] 図６に示した構成との相違点は、スイッチ２０が、フィルタリングを行うためのテーブルを複数有する点にある。図６の例では、第１のテーブル２３－１を、受信パケットをフィルタリングするために用いていたが、フィルタリングを行うためのテーブルを複数設けることができる。例えば、第１のテーブル２３－１と、第２のテーブル２３－２を、それぞれ異なる観点でフィルタリングを行うためのテーブルとして用いる。図７の例では、例えば、第１のテーブル２３－１には、第１フィルタリングポリシ管理部１２１によっ

て定められるフィルタリングポリシを設定する。また、第２のテーブル２３－２には、第２フィルタリングポリシ管理部１２２によって定められる第２のフィルタリングポリシを設定する。ここで、第１のフィルタリングポリシと、第２のフィルタリングポリシは、異なる観点によるフィルタリングポリシであってもよい。

[0035] 図８を用いて、第１のテーブル、第２のテーブル、第３のテーブルの設定方法について説明する。第１のテーブルには、マッチ条件が「Ｃ」のパケットを廃棄するためのポリシが設定されている。また、マッチ条件が「Ａ」と「Ｂ」のパケットに対しては、第２のテーブルを参照させるという処理内容が対応づけられたエントリが設定されている。同様に、第２のテーブルには、マッチ条件が「Ｂ」となるパケットを廃棄するためのポリシが設定されている。第３のテーブルには、第１のテーブルおよび第２のテーブルにおいて廃棄されなかったマッチ条件が「Ａ」のパケットについて、ポート＃２から転送させるという処理内容を対応付けたエントリが設定されている。

[0036] 以下、制御装置１００Ｄの構成について、図７を用いて説明する。図６に示した構成と比較して、図６のフィルタリングポリシ管理部１１１に対応する第１のフィルタリングポリシ管理部１２１と、第２のフィルタリングポリシ管理部１２２との２つを備える。第１のフィルタリングポリシ管理部１２１は、例えば、スイッチ２０の第１のテーブル２３－１に設定するエントリを作成するためのフィルタリングポリシを管理する。第２のフィルタリングポリシ管理部１２２は、例えば、スイッチ２０の第２のテーブル２３－２に設定するエントリを作成するためのフィルタリングポリシを管理する。上述の通り、第１のテーブル２３－１に設定されるフィルタリングポリシと、第２のテーブル２３－２に設定されるフィルタリングポリシとは、異なる観点によるものであっても良い。なお、処理決定部１１３は、図６と同様に、前記テーブル操作部１１４、１１５が生成するフィルタリング用のエントリによって選別されたパケットについて適用する処理を決定する。また、図６のテーブル操作部１１４、１１５と同様に、図７の制御装置１００Ｄが有する

テーブル操作部は、３つでなくても良い。

[0037] 以上のように、本実施形態によれば、スイッチに、受信パケットのフィルタリングを行うためのテーブルと、フィルタリングを行った後にパケットの処理を行うためのテーブルとを設けている。したがって、複数のテーブルを用いて、スイッチが受信するパケットに対するフィルタリングを行うことが可能となる。

[0038] さらに、本実施形態によれば、１つのテーブルで、受信パケットのフィルタリングと、受信パケットに対する処理との双方を行う場合に比べて、スイッチに設定するエントリ数を削減することができる。

[0039] 以下、図９に示すシステムを例に挙げて説明する。図９のシステムは、スイッチ２０Ａに、端末＃１－１、端末＃１－２、端末＃１－３が接続している構成を示している。ここで、端末＃１－１、＃１－２、＃１－３は、端末グループ「Ａ」に属するものとする。端末グループＡは、例えば、各端末のＩＰアドレスの一部が共通であるとする。また、端末＃１－１はスイッチ２０Ａのポート＃１に、端末＃１－２はポート＃２に、端末＃１－３はポート＃３に、それぞれ接続している。

[0040] 以下では、スイッチ２０Ａにおいて、端末＃１－１および端末＃１－３からの通信だけを許容し、端末＃１－２からの通信は制限する（拒否する）というフィルタリングポリシを適用する場合を例に挙げて説明する。

[0041] 図１０は、上述のフィルタリングポリシを、１つのテーブルで適用する場合の、テーブルの構成例を示している。例えば、端末＃１－１に関しては、２番目、３番目のエントリのように、候補となる宛先＃１－２、＃１－３に対して、それぞれ対応するポートからパケットを転送するような処理内容が対応づけられている。また、例えば、１番目のエントリのように、送信元と宛先が一致する場合には、ループが発生してしまうため、パケットを廃棄する処理内容が設定されている。

[0042] また、通信を制限する端末＃１－２を送信元とするパケットに対しては、宛先がどこであっても廃棄するという処理内容が対応づけられている。なお

、図中の「＊」はワイルドカードを示している。例えば、図１０の４番目のエントリのマッチ条件であれば、端末＃１－２を送信元とするアドレスがマッチ条件となり、宛先アドレスに特定の値は指定されない。つまり、受信パケットの送信元のアドレスが端末＃１－２のアドレスであれば、宛先がいかなる値であっても、受信パケットは当該エントリにマッチする。

[0043] 一方、図１１は、上述のフィルタリングポリシを、２つのテーブルを用いて適用する場合の、各テーブルの構成例を示している。まず、第１のテーブルの１番目と２番目のエントリは、上述したようなループを発生させるパケットを廃棄するためのエントリである。また、３番目と４番目のエントリでは、通信を許容する端末＃１－１および＃１－３を送信元とするパケットに対して、第２のテーブルを参照させるという処理内容が対応付けられている。また、第１のテーブルの５番目のエントリは、端末＃１－１～＃１－３を含むグループＡのいずれかを送信元とするパケットを廃棄するという処理内容が記載されている。なお、このエントリのマッチ条件は、通信を許容する端末＃１－１と＃１－３を含むが、送信元アドレスが＃１－１、＃１－３に対応するパケットは、第１のテーブルの１番目から４番目のいずれかのエントリのマッチ条件に適合し、処理される。よって、端末＃１－１、＃１－３を送信元とするパケットは、５番目のエントリで廃棄されることはない。

[0044] また、図１１の第２のテーブルには、宛先アドレスに応じて、それぞれ対応するポートからパケットを転送するという処理内容が記載されている。第２のテーブルの各々のエントリには、送信元がいずれであるかに拘らず、パケットの宛先アドレスに応じたポートからパケットを転送させるという処理が設定されている。

[0045] ここで、図１１のように、第１のテーブルでフィルタリングを行うようにすることで、第２のテーブルでは、送信元に依存せず、宛先のみを考慮して処理内容を設定することができる。

[0046] まず、第１のテーブルでは、特定の端末を送信元とするパケットに対して、フィルタリングを行っており、各々のパケットの宛先がどこであるかにつ

いては考慮していない。つまり、マッチ条件のうち、宛先アドレスのフィールドは、ワイルドカードで設定される。第１のテーブルでフィルタリングを行うため、第２のテーブルで処理されるパケットは、既にフィルタリングされた後のパケットである。上述の例でいえば、アクセスを拒否したい端末＃１－２からのパケットは、第２のテーブルで処理されない。

[0047] 第１のテーブルにおいて、特定の端末を送信元とするパケットに対するフィルタリングが実行されているので、第２のテーブルでは、送信元を考慮する必要がなくなる。したがって、第２のテーブルでは、送信元アドレスを特定せずに、宛先アドレスのみをマッチ条件として、処理内容を記載することができる。具体的には、図１１の例のように、送信元アドレスを「＊」に設定でき、例えば宛先アドレスが同一で送信元アドレスが異なる場合に、送信元アドレスの数だけ設定されていたエントリを１つのエントリに圧縮できる。例えば、図１０では、２番目と６番目のエントリのマッチ条件は、いずれも宛先アドレスが＃１－２であるが、送信元アドレスは異なる。これらのエントリは、図１１の第２のテーブルでは、２番目のエントリ１つに圧縮することができる。よって、本発明のように複数のテーブルでフィルタリングを行うことで、エントリ数を削減することが可能となる。

[0048] 以上のことから、本実施形態におけるテーブルに設定すべきエントリ数は、１つのテーブルを用いた場合と比較して削減される。また、端末数が増えるほど、送信元と宛先との組み合わせが増加するため、本実施形態によるエントリ数削減の効果はより顕著になる。

[0049] さらに、本実施形態によれば、制御装置からスイッチのテーブルに対して設定するエントリ数を削減することができるので、制御装置からスイッチに対してエントリを設定するための通信量も削減することが可能となる。従って、本実施形態によれば、制御装置の負荷を削減することも可能となる。

[0050] ［第２の実施形態］

続いて、本発明の第２の実施形態について図面を参照して詳細に説明する。図１２は、本発明の第２の実施形態の通信システムの構成を示す図である

。図１２を参照すると、ネットワーク（ＮＷ）及びスイッチ２００Ａ、２００Ｂを制御する制御装置１００と、スイッチ２００Ａ、２００Ｂを介して通信する仮想マシン（以下、「ＶＭ」と記す。）＃１－１、＃１－２、＃２－１と、ネットワーク（ＮＷ）に構成された仮想トンネルのエンドポイント（以下、「ＴＥＰ」と記す。）４００とが示されている。なお、仮想トンネルとは、ネットワーク上において仮想的、あるいは論理的に構築されたパスである。

[0051] 図１２の例では、スイッチ２００Ａは、＃１～＃３の３つのポートを持ち、ポート＃１には、ＶＭ＃１－１が接続され、ポート＃２には、ＶＭ＃１－２が接続されている。また、スイッチ２００Ａのポート＃３はＴＥＰ４００と接続され、ＶＭ＃１－１、ＶＭ＃１－２から受信したパケットを、仮想トンネルを介してスイッチ２００Ｂに送信可能となっている。スイッチ２００Ｂは、＃１、＃２の２つのポートを持ち、ポート＃１には、ＶＭ＃２－１が接続され、ポート＃２には、ＴＥＰ４００が接続されている。また、スイッチ２００Ａ、２００Ｂは、それぞれ物理的なスイッチでもよいが、ＶＭ＃１－１、＃１－２、＃２－１が動作する仮想化サーバ上で動作する仮想スイッチであってもよい。また、スイッチ２００Ａ、２００Ｂは、携帯電話やスマートフォン等の端末上で仮想的に動作する仮想スイッチであってもよい。

[0052] 図１３は、スイッチ２００Ａ、２００Ｂ（以下、スイッチ２００Ａ、２００Ｂを特に区別しない場合「スイッチ２００」と記す。）の詳細構成を示す図である。図１３を参照すると、制御メッセージ送受信部２１と、パケット処理部２２と、テーブル２３とを備えた構成が示されている。

[0053] 制御メッセージ送受信部２１は、制御装置１００からテーブル２３の操作に関する制御メッセージを受信し、テーブル２３の更新を行う。また、制御メッセージ送受信部２１は、制御装置１００に対するテーブル２３に登録するエントリの送信要求や、制御装置１００からのパケット出力指示に応じた動作を実行する。

[0054] パケット処理部２２は、パケットを受信すると、テーブル２３を参照し、

受信パケットに適合するマッチ条件を持つエントリを検索し、該当するエントリに定められた動作（アクション）を実行する。

[0055] テーブル２３は、参照順序として機能する＃０～＃Ｎまでの番号が付与されたＮ個のテーブルによって構成されている。以下、本実施形態では、スイッチ２００は、＃０～＃２の３つのテーブルを持つものとして説明するが、テーブル数に制約はない。例えば、後記する第１～第３テーブルがそれぞれ複数枚設けられている構成も採用可能である。

[0056] 例えば、パケット処理部２２は、パケットを受信すると、テーブル＃０から順番に受信パケットに適合するマッチ条件を持つエントリを検索する。検索の結果、すべてのテーブルに受信パケットに適合するマッチ条件を持つエントリがない場合、パケット処理部２２は、制御メッセージ送受信部２１に対し、制御装置１００へのエントリ送信要求の送信を依頼する。なお、テーブル２３に、制御装置１００への問い合わせを規定した動作（アクション）を有するエントリを設定することも可能である。一方、いずれかのテーブル＃０に、受信パケットに適合するマッチ条件を持つエントリがある場合、パケット処理部２２は、該当するエントリに定められた動作（アクション）を実行する。個々のエントリの動作（アクション）として、例えば、指定した番号のテーブルへの参照を指示することも可能となっている（但し、ループを避けるため、現在参照しているテーブルよりも若い番号のテーブルを指定することはできない。）。このようなスイッチは、例えば、非特許文献２の仕様に準拠したオープンフロースイッチにて実現できる。

[0057] ＴＥＰ４００は、所定のトンネルプロトコルに従い、送受信するパケットのカプセル化、デカプセル化を実行する機器である。例えば、制御装置１００から制御可能なスイッチによりＴＥＰ４００を構成することもできる。なお、所定のトンネルプロトコルとしては、例えば、ＧＲＥ（Ｇｅｎｅｒｉｃ Ｒｏｕｔｉｎｇ Ｅｎｃａｐｓｕｌａｔｉｏｎ）や、ＮＶＧＲＥ（Ｎｅｔｗｏｒｋ Ｖｉｒｔｕａｌｉｚａｔｉｏｎ ｕｓｉｎｇ ＧＲＥ）、ＩＰｓｅｃ（Ｓｅｃｕｒｉｔｙ Ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ Ｉｎｔｅｒ

ｎｅｔ　Ｐｒｏｔｏｃｏｌ）が挙げられる。

[0058] 図１４は、制御装置１００の詳細構成を示す図である。図１４を参照すると、仮想ネットワークの構成を保持する仮想ネットワーク構成管理部１０１と、アクセス制御を実施する通信の特徴と通信可否とを対応付けたアクセスポリシを保持するアクセスポリシ管理部１０２と、スイッチ２００Ａ、２００Ｂに実行させる処理を決定する処理決定部１０３と、第１～第３テーブル操作部１０４～１０６とを備えた構成が示されている。なお、図１４の破線で示した部分１０９が、図１のスイッチ制御部１９に相当する。

[0059] 図１５は、制御装置１００の仮想ネットワーク構成管理部１０１に保持される仮想ネットワーク構成情報の一例である。図１５を参照すると、それぞれの仮想ネットワークにおいて、スイッチと、そのポート番号と、各ポートに付与されたＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスとを対応付けたエントリが示されている。なお、図１５の２つのエントリは、図１２において、スイッチ２００Ａのポート＃１、＃２が仮想ネットワークＩＤ＝１の仮想ネットワークに属していることを示している。なお、図１５においては、図１２のスイッチ２００Ｂのポート情報は登録されていない。これについては、後に図２１を用いて説明する。なお、仮想ネットワーク構成管理部１０１には、図１５に示した内容に限らず、その他の情報を格納してもよい。

[0060] 第１テーブル操作部１０４は、仮想ネットワーク構成管理部１０１に保持される仮想ネットワーク構成情報から、スイッチ２００の第２のテーブル（テーブル＃１）以降のテーブルを参照した処理決定の対象となるパケットを選別するエントリを生成する。例えば、第１テーブル操作部１０４は、仮想ネットワークに含まれる特定のホストから、同じホストを宛先とするループを発生させるパケットを廃棄するためのエントリを生成する。より具体的には、ポート＃１又は＃２から、そのポートのＭＡＣアドレスを宛先とするパケット（すなわち、自身のアドレスを宛先とする異常パケット）を受信した場合に、当該パケットを廃棄（Ｄｒｏｐ）することを指示するエントリを生

成する。その後、第１テーブル操作部１０４は、スイッチ２００に対して、スイッチ２００の第１のテーブル（テーブル＃０）に格納することを指示する制御メッセージとともに送信する。

[0061] 図１６は、第１テーブル操作部１０４によって図１５に示す仮想ネットワーク構成情報から生成されて、図１２のスイッチ２００Ａの第１のテーブル（テーブル＃０）に設定されるエントリの例である。図１６の上から１、２番目のエントリは、ポート＃１又は＃２から、そのポートのＭＡＣアドレスを宛先とするパケット（すなわち、自身のアドレスを宛先とする異常パケット）を受信した場合に、当該パケットを廃棄（Ｄｒｏｐ）することを指示するエントリである。図１６の上から３番目のエントリは、上記１、２番目のエントリ以外のパケットを受信した場合に、ヒットと判定し、テーブル＃１へのジャンプ（Ｇｏ　ｔｏ）を指示するエントリである（なお、以下、テーブル中の記号「＊」は、ワイルドカードを示す。）。なお、図１６の優先度フィールドは、各エントリの優先度を示し、例えば、あるパケットに複数のエントリのマッチ条件に適合する場合に、適用するエントリを選択する際に参照される。また、図１６の例では、マッチ条件に入力ポートと宛先ＭＡＣアドレスを用いているが、その他のヘッダ情報を用いてもよい。なお、図１６に示したエントリは、あくまで一例であり、例えば、パケットヘッダの情報が明らかに異常な値を示しているパケットや、ＤｏＳ（Ｄｅｎｙ　ｏｆ　Ｓｅｒｖｉｃｅ）攻撃に使用されている可能性があるパケットなどを捕捉して破棄するエントリを設定してもよい。

[0062] 第２テーブル操作部１０５は、アクセスポリシ管理部１０２に保持されるアクセスポリシに基づいて、仮想ネットワークを流れるパケットについてフィルタリングを実施するエントリを生成する。そして、第２テーブル操作部１０５は、スイッチ２００に対して、前記生成したエントリを、スイッチ２００の第２のテーブル（テーブル＃１）に格納することを指示する制御メッセージとともに送信する。

[0063] 図１７は、初期状態において、第２テーブル操作部１０５によって図１２

のスイッチ２００Ａの第２のテーブル（テーブル＃１）に設定されるエントリの例である。図１７の上から１番目のエントリは、ポート＃１からの送信元ＭＡＣアドレスが００：００：００：０１：００：０１からの宛先ＭＡＣアドレスがＡＡ：ＡＡ：ＡＡ：ＡＡ：ＡＡ：ＡＡを宛先とするパケットを受信した場合に、当該パケットを廃棄（Ｄｒｏｐ）することを指示するエントリである。このようなエントリは、ＭＡＣアドレスが００：００：００：０１：００：０１であるＶＭからＭＡＣアドレスがＡＡ：ＡＡ：ＡＡ：ＡＡ：ＡＡ：ＡＡであるＶＭへのアクセスを禁止するといったアクセスポリシに基づいて生成される。図１７の上から２番目のエントリは、マッチ条件中のすべてのフィールドにワイルドカード「＊」が設定されている。このため、先の第１のテーブルの３番目又は４番目のエントリにヒットした場合、第２のテーブル（テーブル＃１）においてもヒットと判定されて、テーブル＃２にジャンプ（Ｇｏ　ｔｏ）することになる。

[0064] 処理決定部１０３は、スイッチ２００Ａ、２００Ｂを含む仮想ネットワークのトポロジに基づいたエンドツーエンドの経路を計算する。また、処理決定部１０３は、必要に応じて、ヘッダの書き換え等のスイッチ２００Ａ、２００Ｂに実行させるべき処理を決定する。

[0065] 第３テーブル操作部１０６は、処理決定部１０３から得られた経路情報に基づいて、スイッチ２００に、受信パケットの転送やヘッダ変換を実行させるエントリを生成し、スイッチ２００に対して、スイッチ２００の第３のテーブル（テーブル＃２）に格納することを指示する制御メッセージとともに送信する。

[0066] 図１８は、第３テーブル操作部１０６によって図１２のスイッチ２００Ａの第３のテーブル（テーブル＃２）に設定されるエントリの例である。図１８の上から１番目のエントリは、宛先アドレスとしてＶＭ＃１－２が接続されているポート＃２のＭＡＣアドレスが設定されているパケットを、ポート＃２から出力することを指示している。同様に、図１８の上から２番目のエントリは、宛先ＭＡＣアドレスとしてＶＭ＃１－１に接続されたポート＃１

のＭＡＣアドレスが設定されているパケットをポート＃１から出力することを指示している。以上、２つのエントリにより、スイッチ２００Ａを介したＶＭ＃１－１、＃１－２間の通信が可能となる。図１８の上から３番目、４番目のエントリは、上記第１のテーブルにて第２のテーブル（テーブル＃１）以降のテーブルを参照した処理決定の対象となると判定されたパケットであるが、上記２つのエントリに適合しないパケットを、該当仮想ネットワークの受信ポート以外のポートから送信するフラッディングを実施することを指示するエントリである。

[0067] なお、図１４の例では説明のため、第１テーブル操作部１０４～第３テーブル操作部１０６をそれぞれ独立した処理ユニットとして記載しているが、フィルタリング用のテーブル（上記第１のテーブル（テーブル＃０）、第２のテーブル（テーブル＃１）に相当）と、パケットに適用する処理を決定するためのテーブル（上記第３のテーブル（テーブル＃２）に相当）とをそれぞれ更新可能な構成であればよく、第１テーブル操作部１０４～第３テーブル操作部１０６は適宜統合することが可能である。例えば、第１テーブル操作部１０４～第３テーブル操作部１０６に変えて、第１テーブル操作部１０４～第３テーブル操作部１０６のすべての処理を実行する単体のテーブル操作部を設けてもよい。

[0068] なお、図１４に示した制御装置の各部（処理手段）は、制御装置を構成するコンピュータに搭載された記憶手段と、そのハードウェアを用いて上記した各処理を実行させるコンピュータプログラムとにより実現することもできる。

[0069] 続いて、制御装置１００の動作について図面を参照して説明する。はじめに、アクセスポリシ管理部１０２に、アクセスポリシが追加された場合の動作について説明する。

[0070] 図１９は、制御装置１００のアクセスポリシ管理部１０２に追加されたアクセスポリシの一例である。図１９の例では、接続ポートのＭＡＣアドレスにて指定されたＶＭ＃１－１からＶＭ＃１－２へのＩＰｖ６（タイプ＝０ｘ

８６ｄｄ）による通信を遮断するというアクセスポリシが設定されている。なお、図１９の例は、あくまで一例であり、例えば、特定のＶＭから特定のＶＭ宛のパケットだけを通過させるアクセスポリシや特定のサービスに関するパケットのみ通過させるアクセスポリシ等を設定することができる。

[0071] 第２テーブル操作部１０５は、上記アクセスポリシに基づき、仮想ネットワークを流れるパケットについてフィルタリングを実施するエントリを生成し、スイッチ２００に対して、スイッチ２００の第２のテーブル（テーブル＃１）に格納することを指示する制御メッセージとともに送信する。

[0072] 図２０は、第２テーブル操作部１０５によって図１９に示すアクセスポリシから生成されて、図１２のスイッチ２００Ａの第２のテーブル（テーブル＃１）に追加されるエントリの例である。図２０の例では、上記第１のテーブルにてスイッチ２００の第２のテーブル（テーブル＃１）以降のテーブルを参照した処理決定の対象となると判定されたパケットのうち、ポート＃１から、ＶＭ＃１－１の接続ポートを送信元ＭＡＣアドレスとし、ＶＭ＃１－２の接続ポートを宛先ＭＡＣアドレスとし、かつ、上位プロトコルがＩＰｖ６であるパケットを受信した場合に、当該パケットを廃棄（Ｄｒｏｐ）することを指示するエントリが追加されている。なお、図２０の例では、アクションとして廃棄（Ｄｒｏｐ）を指定しているが、アクセスポリシに応じて、例えば、ヘッダの書き換えを行ったり、特定の宛先へのリダイレクトを指示するエントリを設定してもよい。

[0073] 続いて、仮想ネットワーク構成情報の更新が行われた場合の制御装置の動作について説明する。以下、図１２のＶＭ＃２－１が立ち上げられて、スイッチ２００Ｂを介して、ＶＭ＃１－１、＃１－２と同一の仮想ネットワークに接続した場合の動作を例に説明する。

[0074] 図２１は、スイッチ２００Ｂのポート＃１が追加された後の仮想ネットワーク構成情報を示している。図２１を参照すると、３番目のエントリとして、スイッチ２００ＢのＩＤと、ＶＭ＃２－１が接続されているポート番号＃１と、そのポートに付与されたＭＡＣアドレスとを対応付けたエントリが追

加されている。

[0075] 上記仮想ネットワーク構成情報の変化を検出すると、第１テーブル操作部１０４は、変更後の仮想ネットワーク構成情報に基づいて、スイッチ２００の第１のテーブル（テーブル＃０）の操作を開始する。

[0076] 図２２は、図２１に示す仮想ネットワーク構成情報に基づき、第１テーブル操作部１０４によって操作されるスイッチ２００Ａの第１のテーブル（テーブル＃０）の内容を示す図である。図２２の例では、スイッチ２００Ａのポート番号＃３について、そのポートのＭＡＣアドレスを宛先とするパケット（すなわち、自身のアドレスを宛先とする異常パケット）を受信した場合に、当該パケットを廃棄（Ｄｒｏｐ）することを指示するエントリが追加されている（図２２の上から３番目のエントリ参照）。

[0077] 図２３は、図２１に示す仮想ネットワーク構成情報に基づき、第３テーブル操作部１０６によって操作されるスイッチ２００Ａの第３のテーブル（テーブル＃２）の内容を示す図である。図２３の例では、上記第１、第２のテーブルにてスイッチ２００の第３のテーブル（テーブル＃２）以降のテーブルを参照した処理決定の対象となると判定されたパケットのうち、宛先アドレスとしてスイッチ２００ＢのＶＭ＃２－１が接続されているポート＃１のＭＡＣアドレスが設定されているパケットをポート＃３から出力することを指示するエントリが追加されている（図２３の上から３番目のエントリ参照）。以上により、ＶＭ＃１－１、＃１－２からＶＭ＃２－１へのパケット送信が可能となる。また、図２３の例では、上記３つのエントリに適合しないパケットを受信ポート以外のポートから送信するフラッディングを実施することを指示するエントリが追加されている（図２３の上から６番目のエントリ参照）。

[0078] なお、スイッチ２００Ｂにも、同様にして異常パケット等をフィルタリングした上で、その宛先ＭＡＣアドレスに応じスイッチ２００Ａ側にパケットを転送するエントリが設定される。

[0079] 以上の結果、スイッチ２００には、図２４に示すように、第１のテーブル

（Ｔａｂｌｅ＃０）～第３のテーブル（Ｔａｂｌｅ＃２）が設定されることになる。スイッチ２００は、適正なパケットを受信すると、スイッチ２００は、第１のテーブル（Ｔａｂｌｅ＃０）２３０－０の次に、第２のテーブル（Ｔａｂｌｅ＃１）２３０－１を検索する。第２のテーブル（Ｔａｂｌｅ＃１）２３０－１の検索の結果、所定のアクセスポリシを具現したエントリにヒットした場合、スイッチ２００は、その内容に応じたアクセス制御（ヒットならＤｒｏｐ等）を行う。さらに、スイッチ２００は、第３のテーブル（Ｔａｂｌｅ＃２）２３０－２を検索して、最終的に、当該パケットを該当仮想ネットワークに接続されたポートから出力する（図２５参照）。

[0080] スイッチ２００の基本動作として、受信パケットに適合するマッチ条件を持つエントリを保持していない場合、制御装置１００に対して、当該受信パケットに対応するエントリの送信を要求する場合がある。また、スイッチ２００には、制御装置１００に対するエントリの送信要求を実行させるエントリが低優先度で設定されている場合もあり得る。この場合、スイッチ２００は、受信パケットのうち、異常パケットについては第１のテーブル（Ｔａｂｌｅ＃０）の優先度が上位のエントリに従い廃棄を行ない、残る受信パケットのうち、第２のテーブル（Ｔａｂｌｅ＃１）、第３のテーブル（Ｔａｂｌｅ＃２）のエントリのいずれにもヒットしなかったパケットのみ制御装置１００にエントリの送信要求を送信することになる。よって、スイッチ２００が異常パケットを処理するためのエントリの送信要求を送信し、制御装置１００がこれに応じる必要が無くなる。このため、スイッチ２００からのエントリ送信要求や、要求に対する制御装置１００からの応答等、スイッチ２００と制御装置１００との間で行われる通信量が削減されるので、制御装置１００及びスイッチ２００の負荷が軽減される。

[0081] 以上のように、本実施形態によれば、スイッチに、受信パケットのフィルタリングを行うためのテーブルと、フィルタリングを行った後にパケットの処理を行うためのテーブルとを設けている。したがって、第１の実施形態と同様に、複数のテーブルを用いて、スイッチが受信するパケットに対するフ

ィルタリングを行うことが可能となる。

[0082] さらに、本実施形態によれば、第１の実施形態と同様に、１つのテーブルで、受信パケットのフィルタリングと、受信パケットに対する処理との双方を行う場合に比べて、スイッチに設定するエントリ数を削減することができる。

[0083] なお、本実施形態では、スイッチ２００側の第１のテーブル（Ｔａｂｌｅ＃０）２３０－０～第３のテーブル（Ｔａｂｌｅ＃２）２３０－２の３つのテーブルを用い、そのうちの２つのテーブル（第１のテーブル（Ｔａｂｌｅ＃０）２３０－０、第２のテーブル（Ｔａｂｌｅ＃１）２３０－１）でフィルタリングを行うものとして説明したが、テーブル数は複数であれば制限は無い。例えば、第１テーブル操作部１０４及び第２テーブル操作部１０５がスイッチ２００側の一のテーブル（フィルタリング用）のテーブルを操作し、第３テーブル操作部１０６がスイッチ２００側の別のテーブル（処理決定用）を操作する構成とすることができる。同様に、例えば、第１テーブル操作部１０４～第３テーブル操作部１０６が、スイッチ２００の複数のテーブルをそれぞれ操作する構成とすることもできる。

[0084] ［第３の実施形態］

続いて、第３の実施形態について説明する。第３の実施形態では、複数のテーブルのうち、前段のテーブルにおいて、受信パケットのフィルタリングに加えて、特定のホスト（ＶＭ）に行わせたい処理を設定することが可能である。例えば、ＶＭ＃１－１に対して仮想ネットワークＩＤ「１」を付与したい場合、前段のテーブルにおいて、ＶＭ＃１－１に対して次段のテーブルを参照させる処理とともに、仮想ネットワークＩＤ「１」を付与する処理を設定することができる。以下では、前段のテーブルにて、仮想ネットワークへの属否を判定し、その情報をマッチングに用いるようにした例について説明する。なお、本発明の第３の実施形態は、上記本発明の第２の実施形態と、略同一の構成にて実施可能であるため、第２の実施形態との相違点を中心に説明する。

[0085] 図２６は、本発明の第３の実施形態の第１テーブル操作部１０４によって図１５に示す仮想ネットワーク構成情報から生成されて、図１２のスイッチ２００Ａの第１のテーブル（テーブル＃０）に設定されるエントリの例である。第１の実施形態および第２の実施形態と異なる点は、第１のテーブル（テーブル＃０）において、受信したパケットが属する仮想ネットワークのＩＤを設定した上で、次のテーブル＃１を参照させることを指示する処理内容が設定されている点である。例えば、図２６の上から１、２番目のエントリには、入力ポートが＃１又は＃２であるパケットを受信した場合に、仮想ネットワークＩＤの記憶領域として用いるメタ情報格納レジスタ（ｒｅｇ０）に、仮想ネットワークＩＤ“１”をセットした上で、テーブル＃１にジャンプ（Ｇｏ　ｔｏ）することを指示するアクションが設定されている。図２６の上から３番目のエントリはそれ以外のパケット（すなわち、いずれの仮想ネットワークにも属さないパケット）を受信した場合に、当該パケットを廃棄（Ｄｒｏｐ）することを指示するエントリである。パケット処理部２２が、各テーブルを参照してパケットを処理する際、メタ情報格納レジスタの内容を参照すれば、処理中のパケットが属する仮想ネットワークＩＤを認識することができる。

[0086] 図２７は、本発明の第３の実施形態の第２テーブル操作部１０５によって図１２のスイッチ２００Ａの第２のテーブル（テーブル＃１）に設定されるエントリの例である。図１７に示したエントリと相違するのは、マッチ条件中に上記メタ情報格納レジスタ（ｒｅｇ０）が設定可能となっている点である。

[0087] 図２８は、本発明の第３の実施形態の第３テーブル操作部１０６によって図１２のスイッチ２００Ａの第３のテーブル（テーブル＃２）に設定されるエントリの例である。図１８に示したエントリと相違するのは、上記メタ情報格納レジスタ（ｒｅｇ０）がマッチ条件に使用されている点である。具体的には、図２８の上から１番目のエントリは、上記第１のテーブルにて仮想ネットワークＩＤ＝“１”に属すると判断されたパケット（ｒｅｇ０＝１）

のうち、宛先アドレスとしてＶＭ＃１－２が接続されているポート＃２のＭＡＣアドレスが設定されているパケットを、ポート＃２から出力することを指示している。同様に、図２８の上から２番目のエントリは、上記第１のテーブルにて仮想ネットワークＩＤ＝“１”に属すると判定されたパケット（ｒｅｇ０＝１）のうち、宛先ＭＡＣアドレスとしてＶＭ＃１－１に接続されたポート＃１のＭＡＣアドレスが設定されているパケットをポート＃１から出力することを指示している。以上、２つのエントリにより、スイッチ２００Ａを介したＶＭ＃１－１、＃１－２間の通信が可能となる。図２８の上から３番目、４番目のエントリは、上記第１のテーブルにて仮想ネットワークＩＤ＝“１”に属すると判定されたパケット（ｒｅｇ０＝１）であるが、上記２つのエントリに適合しないパケットを、該当仮想ネットワークの受信ポート以外のポートから送信するフラッディングを実施することを指示するエントリである。

[0088] 図２９は、図２１に示す仮想ネットワーク構成情報に基づき、第１テーブル操作部１０４によって操作されるスイッチ２００Ａの第１のテーブル（テーブル＃０）の内容を示す図である。図２９の例では、入力ポートが＃３であるパケットを受信した場合に、メタ情報格納レジスタ（ｒｅｇ０）に、仮想ネットワークＩＤ“１”をセットした上で、テーブル＃１にジャンプ（Ｇｏ　ｔｏ）することを指示するアクションを設定したエントリが追加されている（図２９の上から３番目のエントリ参照）。

[0089] 図３０は、図１９に示すアクセスポリシから生成されて、図１２のスイッチ２００Ａの第２のテーブル（テーブル＃１）に追加されるエントリの例である。図１１に示したエントリと相違するのは、マッチ条件中に上記メタ情報格納レジスタ（ｒｅｇ０＝１）が設定されている点である。

[0090] 図３１は、図２１に示す仮想ネットワーク構成情報に基づき、第３テーブル操作部１０６によって操作されるスイッチ２００Ａの第３のテーブル（テーブル＃２）の内容を示す図である。図２３に示したエントリと相違するのは、マッチ条件中に上記メタ情報格納レジスタ（ｒｅｇ０＝１）が設定され

ている点である。

[0091] 以上の結果、スイッチ２００には、図３２に示すように、第１のテーブル（Ｔａｂｌｅ＃０）～第３のテーブル（Ｔａｂｌｅ＃２）が設定されることになる。スイッチ２００は、適正な仮想ネットワークに属するパケットを受信すると、第１のテーブル（Ｔａｂｌｅ＃０）２３０－０の該当エントリに従い、メタデータ（ｒｅｇ０）に仮想ネットワークのＩＤをセットして、第２のテーブル（Ｔａｂｌｅ＃１）２３０－１、第３のテーブル（Ｔａｂｌｅ＃２）２３０－２と検索する。最終的に、スイッチ２００は、第２の実施形態と同様に、当該パケットを該当仮想ネットワークに接続されたポートから出力する（図３２参照）。

[0092] 以上のように、本実施形態によれば、スイッチに、受信パケットのフィルタリングを行うためのテーブルと、フィルタリングを行った後にパケットの処理を行うためのテーブルとを設けている。したがって、第１の実施形態、第２の実施形態と同様に、複数のテーブルを用いて、スイッチが受信するパケットに対するフィルタリングを行うことが可能となる。

[0093] さらに、本実施形態によれば、第１の実施形態、第２の実施形態と同様に、１つのテーブルで、受信パケットのフィルタリングと、受信パケットに対する処理との双方を行う場合に比べて、スイッチに設定するエントリ数を削減することができる。

[0094] 加えて、第３の実施形態では、複数のテーブルのうち、前段のテーブルにおいて、受信パケットのフィルタリングに加えて、特定のホスト（ＶＭ）に行わせたい処理を設定することが可能である。

[0095] また、本実施形態では、第１のテーブル（Ｔａｂｌｅ＃０）で仮想ネットワークへの属否を判定した際に、仮想ネットワークＩＤ“１”を割り当てる例を挙げて説明したが、他の仮想ネットワークに属する通信には、他の仮想ネットワークＩＤ（例えば、メタ情報格納レジスタ（ｒｅｇ０＝２）を割り当てることができる。そして、第２のテーブル（Ｔａｂｌｅ＃１）、第３のテーブル（Ｔａｂｌｅ＃２）で、この仮想ネットワークＩＤをマッチ条件と

して用いて、仮想ネットワーク毎に異なる処理を適用することができる。例えば、第２のテーブル（Ｔａｂｌｅ＃１）を用いて、仮想ネットワークＩＤ毎に、異なるアクセスポリシを適用したり、さらなるフィルタリングをかけることも可能である。同様に、第３のテーブル（Ｔａｂｌｅ＃２）を用いて、仮想ネットワークＩＤの構成に応じた経路でパケットを転送させることが可能となる。

[0096] 以上、本発明の実施形態を説明したが、本発明は、上記した実施形態に限定されるものではなく、本発明の基本的技術的思想を逸脱しない範囲で、更なる変形・置換・調整を加えることができる。例えば、上記した実施形態で用いたネットワーク構成や、要素の数に制約は無い。

[0097] また例えば、図６、図７、図１４の例では、制御装置１００、１００Ｃ、１００Ｄが処理決定部１０３を備えているが、処理決定部１０３は他の装置に備えられていても良い。また、処理決定部１０３に代えて、予め計算した経路情報やスイッチに設定するエントリを記憶する記憶部を設けた構成でもよい。

[0098] また、上記した第３の実施形態では、マッチ条件に適合するパケットが属する仮想ネットワークを識別するための情報（仮想ネットワークＩＤ）を記録する領域として、非特許文献２のメタデータ（ｒｅｇ０）を用いるものとして説明したが、パケットヘッダの所定の領域（例えば、ＶＬＡＮ　ＩＤ）に、前記判定した仮想ネットワークＩＤを書き込む構成も採用可能である。

[0099] また、上記した実施形態では、処理決定部１０３は、トポロジ情報に基づいてエンドツーエンドの経路を計算するとのみ説明したが、処理決定部１０３が、仮想ネットワーク構成情報やアクセスポリシを考慮した経路計算を行ってもよい。

[0100] 最後に、本発明の好ましい形態を要約する。

［第１の形態］

（上記第１の視点による制御装置参照）

［第２の形態］

第１の形態において、

前記受信パケットと比較するための条件を含む前記第１および前記第２のエントリの少なくとも１つを前記スイッチに設定し、

前記第１および第２のエントリの少なくとも１つは、複数の受信パケットをグループとして比較するための条件を含む制御装置。

［第３の形態］

第１又は第２の形態において、

前記受信パケットと比較するための条件を含む前記第１および前記第２のエントリの少なくとも１つを前記スイッチに設定し、

前記第１および第２のエントリの少なくとも１つは、ワイルドカードとして設定された条件を含む制御装置。

［第４の形態］

第１から第３いずれか一の形態において、

前記第２のエントリは、前記受信パケットの送信元アドレスに対応する情報がワイルドカードとして設定された条件を含む制御装置。

［第５の形態］

第１から第４いずれか一の形態において、

前記第１のテーブルに、第２のテーブルを参照した処理決定の対象となるパケットと、前記第２のテーブルを参照した処理決定の対象外となるパケットと、を選別するエントリを設定する第１のテーブル操作部と、

前記第２のテーブルに、前記第１のテーブルによって選別されたパケットに基づいて、前記選別されたパケットについて適用する処理を定めたエントリを設定する第２のテーブル操作部と、を備えた制御装置。

［第６の形態］

第５の形態において、

前記第１のテーブル操作部は、前記第１のテーブルに、前記スイッチを含んで構成される仮想ネットワークの構成情報に基づいて、前記仮想ネットワークに属するパケットを選別するエントリを設定し、

前記第２のテーブル操作部は、前記第２のテーブルに、前記仮想ネットワークに属するパケットについて適用する処理を定めたエントリを設定する制御装置。

［第７の形態］

第５又は第６の形態において、

前記第１のテーブル操作部は、前記スイッチの前記第１のテーブルに、仮想ネットワークへの属否を判定するためのマッチ条件と、パケットヘッダ又は前記第２のテーブルのマッチ条件として使用可能なメタデータに、前記マッチ条件に適合するパケットが属する仮想ネットワークを識別するための情報を記録する処理内容とを設定したエントリを設定する制御装置。

［第８の形態］

第５から第７いずれか一の形態において、

前記第２のテーブル操作部は、前記第２のテーブルに、前記仮想ネットワークを識別するための情報をマッチ条件とするエントリを設定する制御装置。

［第９の形態］

第５から第８いずれか一の形態において、

前記第１のテーブル操作部は、前記スイッチの前記第１のテーブルに、前記第２のテーブルを参照した処理決定の対象外となるパケットについて、破棄又は所定の宛先へのリダイレクトを実行させるエントリを設定する制御装置。

［第１０の形態］

第５から第９いずれか一の形態において、

さらに、第３のテーブルに、前記第１のテーブルによって選別されたパケットが所定のアクセスポリシに適合するか否かを確認するエントリを設定する第３のテーブル操作部を備え、

前記第１のテーブル操作部は、前記第１のテーブルのエントリに、前記第３のテーブルを参照させるアクションを設定する制御装置。

［第１１の形態］

第５から第１０いずれか一の形態において、

仮想ネットワークに属する仮想マシン間の通信に用いる仮想トンネルの終端ポイントとして機能するトンネルエンドポイント又は仮想マシンとトンネルエンドポイントの間に配置されたスイッチを対象に、前記第１、第２のテーブルのエントリを設定する制御装置。

［第１２の形態］

（上記第２の視点による通信装置参照）

［第１３の形態］

（上記第３の視点による通信システム参照）

［第１４の形態］

（上記第４の視点によるスイッチの制御方法参照）

［第１５の形態］

（上記第５の視点によるプログラム参照）

なお、上記第１２～第１５の形態は、第１の形態と同様に、第２～第１１の形態に展開することが可能である。

[0101] なお、上記の非特許文献の各開示を、本書に引用をもって繰り込むものとする。本発明の全開示（請求の範囲を含む）の枠内において、さらにその基本的技術思想に基づいて、実施形態ないし実施例の変更・調整が可能である。また、本発明の請求の範囲の枠内において種々の開示要素（各請求項の各要素、各実施形態ないし実施例の各要素、各図面の各要素等を含む）の多様な組み合わせ、ないし選択が可能である。すなわち、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし得るであろう各種変形、修正を含むことは勿論である。特に、本書に記載した数値範囲については、当該範囲内に含まれる任意の数値ないし小範囲が、別段の記載のない場合でも具体的に記載されているものと解釈されるべきである。

符号の説明

[0102] １０Ａ、１００、１００Ｃ、１００Ｄ 制御装置

１９、１０９　スイッチ制御部

２０、２０Ａ、２０Ｂ、２００、２００Ａ、２００Ｂ　スイッチ

２１　制御メッセージ送受信部

２２　パケット処理部

２３、２３－１、２３－２、２３－３、２３０－０～２３０－２　テーブル

３０、３１　ホスト

１０１　仮想ネットワーク構成管理部

１０２　アクセスポリシ管理部

１０３、１１３　処理決定部

１０４、１２４　第１テーブル操作部

１０５、１２５　第２テーブル操作部

１０６、１２６　第３テーブル操作部

１０７　スイッチ通信部

１１１　フィルタリングポリシ管理部

１１４、１１５　テーブル操作部

１２１　第１フィルタリングポリシ管理部

１２２　第２フィルタリングポリシ管理部

３１１、３２１　ＶＭ（仮想マシン）

４００　トンネルエンドポイント（ＴＥＰ）

請求の範囲

[請求項1] パケットを処理するための規則を含むエントリをスイッチに設定する制御装置であって、

前記スイッチが備える第１のテーブルに、前記スイッチの受信パケットをフィルタリングするための第１のエントリを設定し、

前記スイッチが備える第２のテーブルに、前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを設定する

ことを特徴とする制御装置。

[請求項2] 前記制御装置は、

前記受信パケットと比較するための条件を含む前記第１および前記第２のエントリの少なくとも１つを前記スイッチに設定し、

前記第１および第２のエントリの少なくとも１つは、複数の受信パケットをグループとして比較するための条件を含む

ことを特徴とする請求項１の制御装置。

[請求項3] 前記制御装置は、

前記受信パケットと比較するための条件を含む前記第１および前記第２のエントリの少なくとも１つを前記スイッチに設定し、

前記第１および第２のエントリの少なくとも１つは、ワイルドカードとして設定された条件を含む

ことを特徴とする請求項１又は２の制御装置。

[請求項4] 前記第２のエントリは、前記受信パケットの送信元アドレスに対応する情報がワイルドカードとして設定された条件を含む

ことを特徴とする請求項１から３いずれか一の制御装置。

[請求項5] 前記第１のテーブルに、第２のテーブルを参照した処理決定の対象となるパケットと、前記第２のテーブルを参照した処理決定の対象外となるパケットと、を選別するエントリを設定する第１のテーブル操作部と、

前記第２のテーブルに、前記第１のテーブルによって選別されたパケットに基づいて、前記選別されたパケットについて適用する処理を定めたエントリを設定する第２のテーブル操作部と、を備えた請求項１から４いずれか一の制御装置。

[請求項6] 前記第１のテーブル操作部は、前記第１のテーブルに、前記スイッチを含んで構成される仮想ネットワークの構成情報に基づいて、前記仮想ネットワークに属するパケットを選別するエントリを設定し、

前記第２のテーブル操作部は、前記第２のテーブルに、前記仮想ネットワークに属するパケットについて適用する処理を定めたエントリを設定する請求項５の制御装置。

[請求項7] 前記第１のテーブル操作部は、前記スイッチの前記第１のテーブルに、仮想ネットワークへの属否を判定するためのマッチ条件と、パケットヘッダ又は前記第２のテーブルのマッチ条件として使用可能なメタデータに、前記マッチ条件に適合するパケットが属する仮想ネットワークを識別するための情報を記録する処理内容とを設定したエントリを設定する請求項５又は６の制御装置。

[請求項8] 前記第２のテーブル操作部は、前記第２のテーブルに、前記仮想ネットワークを識別するための情報をマッチ条件とするエントリを設定する請求項５から７いずれか一の制御装置。

[請求項9] 前記第１のテーブル操作部は、前記スイッチの前記第１のテーブルに、前記第２のテーブルを参照した処理決定の対象外となるパケットについて、破棄又は所定の宛先へのリダイレクトを実行させるエントリを設定する請求項５から８いずれか一の制御装置。

[請求項10] さらに、第３のテーブルに、前記第１のテーブルによって選別されたパケットが所定のアクセスポリシに適合するか否かを確認するエントリを設定する第３のテーブル操作部を備え、

前記第１のテーブル操作部は、前記第１のテーブルのエントリに、前記第３のテーブルを参照させるアクションを設定する請求項５から

９いずれか一の制御装置。

[請求項11] 仮想ネットワークに属する仮想マシン間の通信に用いる仮想トンネルの終端ポイントとして機能するトンネルエンドポイント又は仮想マシンとトンネルエンドポイントの間に配置されたスイッチを対象に、前記第１、第２のテーブルのエントリを設定する請求項５から１０いずれか一の制御装置。

[請求項12] パケットを処理するための規則を含むエントリを制御装置から受信し、当該エントリに従って前記パケットを処理する通信装置であって、

前記通信装置の受信パケットをフィルタリングするための第１のエントリを格納するための第１のテーブルと、

前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを格納するための第２のテーブルと、

を備えることを特徴とする通信装置。

[請求項13] 前記通信装置は、

前記受信パケットと比較するための条件を含む前記第１および前記第２のエントリの少なくとも１つを前記制御装置から受信し、

前記第１および第２のエントリの少なくとも１つは、複数の受信パケットをグループとして比較するための条件を含む

ことを特徴とする請求項１２の通信装置。

[請求項14] 前記通信装置は、

前記受信パケットと比較するための条件を含む前記第１および前記第２のエントリの少なくとも１つを前記制御装置から受信し、

前記第１および第２のエントリの少なくとも１つは、ワイルドカードとして設定された条件を含む

ことを特徴とする請求項１２又は１３の通信装置。

[請求項15] 前記第２のエントリは、前記受信パケットの送信元アドレスに対応

する情報がワイルドカードとして設定された条件を含む

ことを特徴とする請求項１２から１４いずれか一の通信装置。

[請求項16] 受信パケットをフィルタリングするための第１のエントリを格納するための第１のテーブルと、

前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを格納するための第２のテーブルと、

を備え、

前記第１、第２のテーブルに格納するエントリを制御装置から受信し、当該エントリに従って前記パケットを処理する通信装置と、

前記スイッチが備える第１のテーブルに、前記スイッチの受信パケットをフィルタリングするための第１のエントリを設定し、

前記スイッチが備える第２のテーブルに、前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを設定する制御装置と、

を含む通信システム。

[請求項17] 前記制御装置は、

前記受信パケットと比較するための条件を含む前記第１および前記第２のエントリの少なくとも１つを前記スイッチに設定し、

前記第１および第２のエントリの少なくとも１つは、複数の受信パケットをグループとして比較するための条件を含む

ことを特徴とする請求項１６の通信システム。

[請求項18] 前記制御装置は、

前記受信パケットと比較するための条件を含む前記第１および前記第２のエントリの少なくとも１つを前記スイッチに設定し、

前記第１および第２のエントリの少なくとも１つは、ワイルドカードとして設定された条件を含む

ことを特徴とする請求項１６又は１７の通信システム。

[請求項19] 前記第２のエントリは、前記受信パケットの送信元アドレスに対応する情報がワイルドカードとして設定された条件を含む

ことを特徴とする請求項１６から１８いずれか一の通信システム。

[請求項20] 前記制御装置は、

前記第１のテーブルに、第２のテーブルを参照した処理決定の対象となるパケットと、前記第２のテーブルを参照した処理決定の対象外となるパケットと、を選別するエントリを設定する第１のテーブル操作部と、

前記第２のテーブルに、前記第１のテーブルによって選別されたパケットに基づいて、前記選別されたパケットについて適用する処理を定めたエントリを設定する第２のテーブル操作部と、を備える請求項１６から１９いずれか一の通信システム。

[請求項21] 前記スイッチの第１のテーブル操作部は、前記第１のテーブルに、前記スイッチを含んで構成される仮想ネットワークの構成情報に基づいて、前記仮想ネットワークに属するパケットを選別するエントリを設定し、

前記第２のテーブル操作部は、前記第２のテーブルに、前記仮想ネットワークに属するパケットについて適用する処理を定めたエントリを設定する請求項２０の通信システム。

[請求項22] パケットを処理するための規則を含むエントリをスイッチに設定する制御装置が、

前記スイッチが備える第１のテーブルに、前記スイッチの受信パケットをフィルタリングするための第１のエントリを設定するステップと、

前記スイッチが備える第２のテーブルに、前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを設定するステップと、

を含むスイッチの制御方法。

[請求項23] 前記制御装置は、

前記受信パケットと比較するための条件を含む前記第１および前記第２のエントリの少なくとも１つを前記スイッチに設定し、

前記第１および第２のエントリの少なくとも１つは、複数の受信パケットをグループとして比較するための条件を含む

を含む請求項２２のスイッチの制御方法。

[請求項24] 前記制御装置は、

前記受信パケットと比較するための条件を含む前記第１および前記第２のエントリの少なくとも１つを前記スイッチに設定し、

前記第１および第２のエントリの少なくとも１つは、ワイルドカードとして設定された条件を含む

ことを特徴とする請求項２２又は２３のスイッチの制御方法。

[請求項25] 前記第２のエントリは、前記受信パケットの送信元アドレスに対応する情報がワイルドカードとして設定された条件を含む

ことを特徴とする請求項２２から２４いずれか一のスイッチの制御方法。

[請求項26] 前記第１のテーブルに、第２のテーブルを参照した処理決定の対象となるパケットと、前記第２のテーブルを参照した処理決定の対象外となるパケットと、を選別するエントリを設定し、

前記第２のテーブルに、前記第１のテーブルによって選別されたパケットに基づいて、前記選別されたパケットについて適用する処理を定めたエントリを設定する請求項２２から２５いずれか一のスイッチの制御方法。

[請求項27] 前記第１のテーブルに設定するエントリは、前記スイッチを含んで構成される仮想ネットワークの構成情報に基づいて、前記仮想ネットワークに属するパケットを選別するエントリであり、

前記第２のテーブルに設定するエントリは、前記仮想ネットワークに属するパケットについて適用する処理を定めたエントリである請求

項２６のスイッチの制御方法。

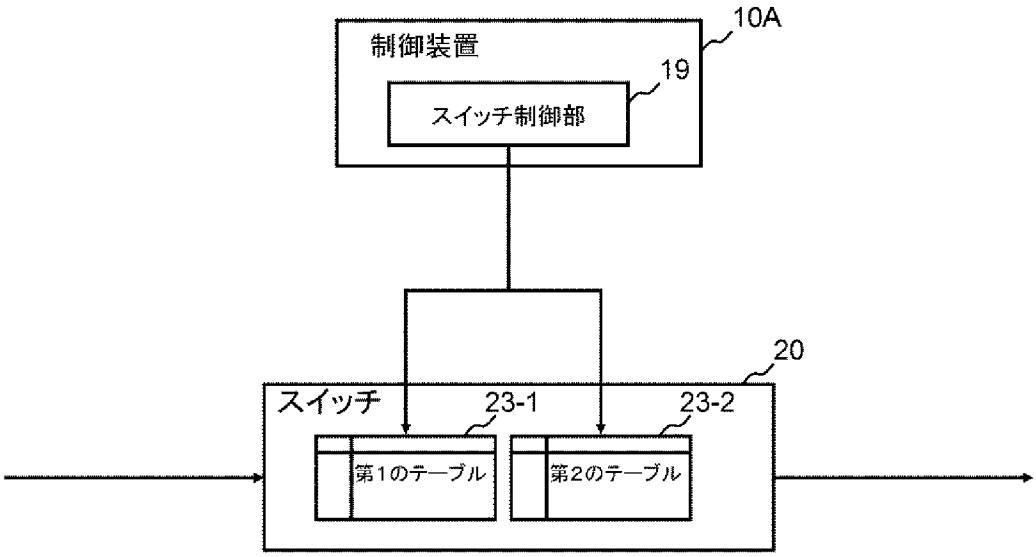
[請求項28] パケットを処理するための規則を含むエントリをスイッチに設定するコンピュータに、

前記スイッチが備える第１のテーブルに、前記スイッチの受信パケットをフィルタリングするための第１のエントリを設定する処理と、

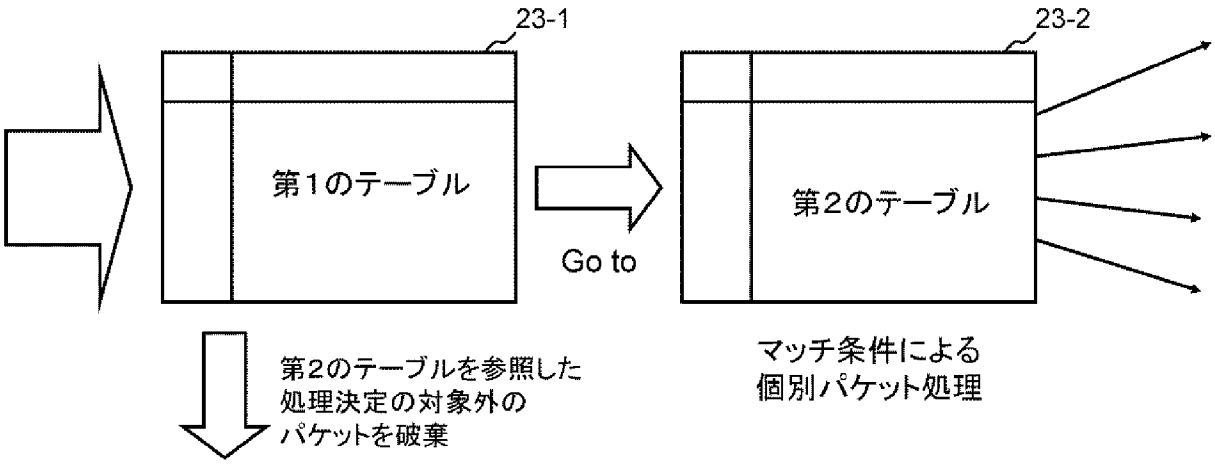
前記スイッチが備える第２のテーブルに、前記受信パケットのうち、前記第１のエントリにより選別されたパケットを処理するための規則を含む第２のエントリを設定する処理と、

を実行させるプログラム。

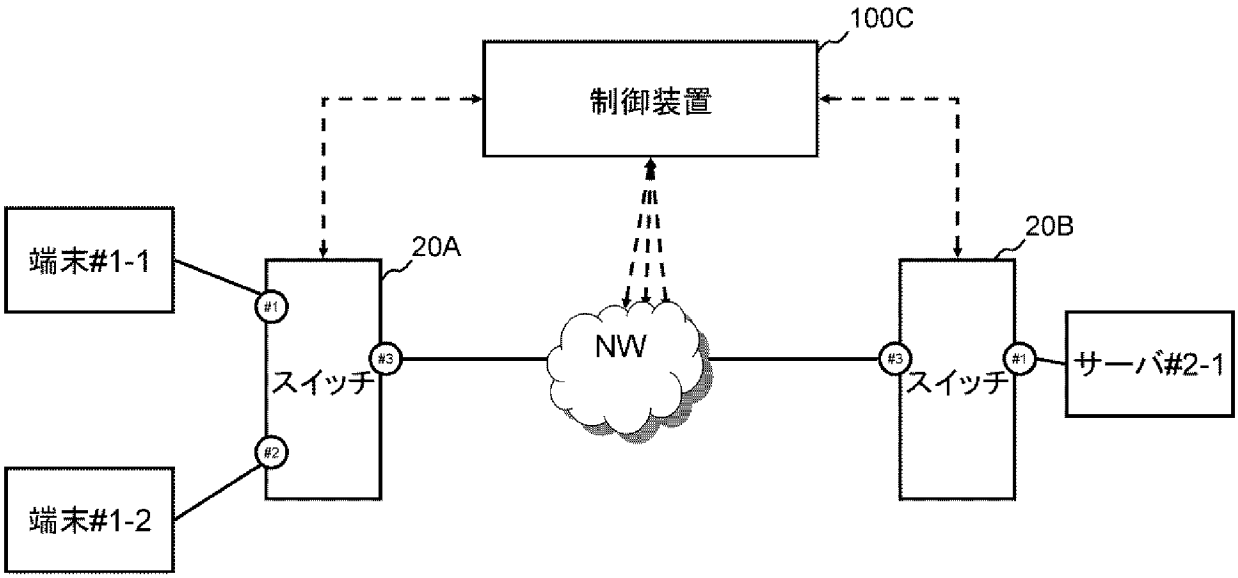
[図1]


制御装置
10A
19
スイッチ制御部
20
スイッチ
23-1
23-2
第1のテーブル
第2のテーブル

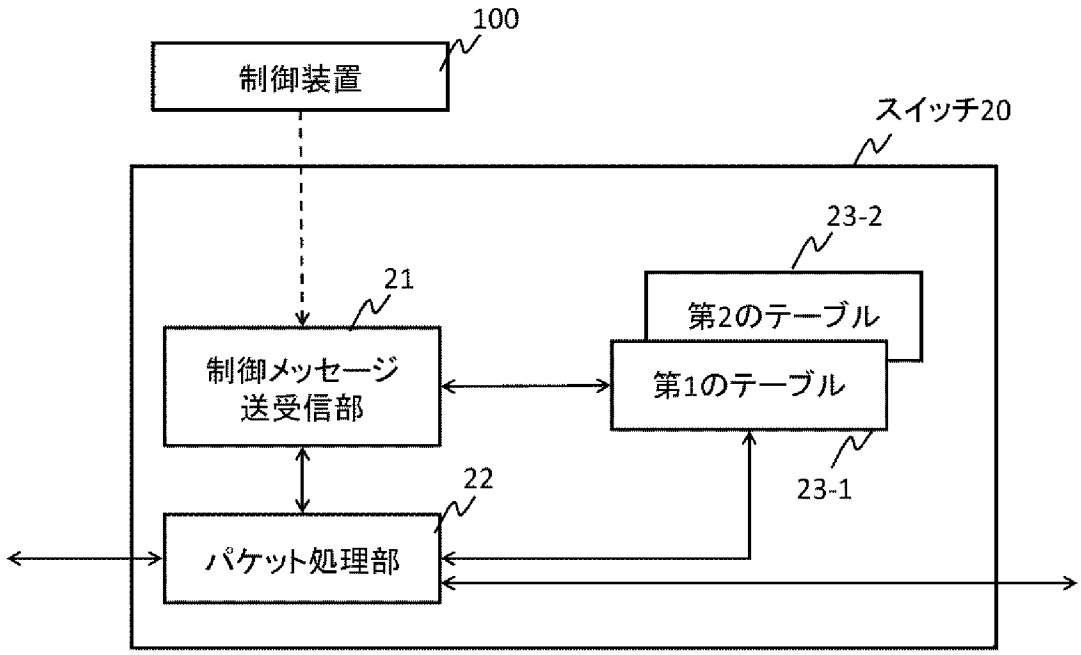
[図2]


23-1
23-2
第1のテーブル
第2のテーブル
Go to
第2のテーブルを参照した
処理決定の対象外の
パケットを破棄
マッチ条件による
個別パケット処理

[図3]


100C
制御装置
端末#1-1
端末#1-2
20A
スイッチ
#1
#2
#3
NW
20B
スイッチ
#3
#1
サーバ#2-1

[図4]


100
制御装置
スイッチ20
23-2
第2のテーブル
21
制御メッセージ
送受信部
第1のテーブル
23-1
22
パケット処理部

[図5]

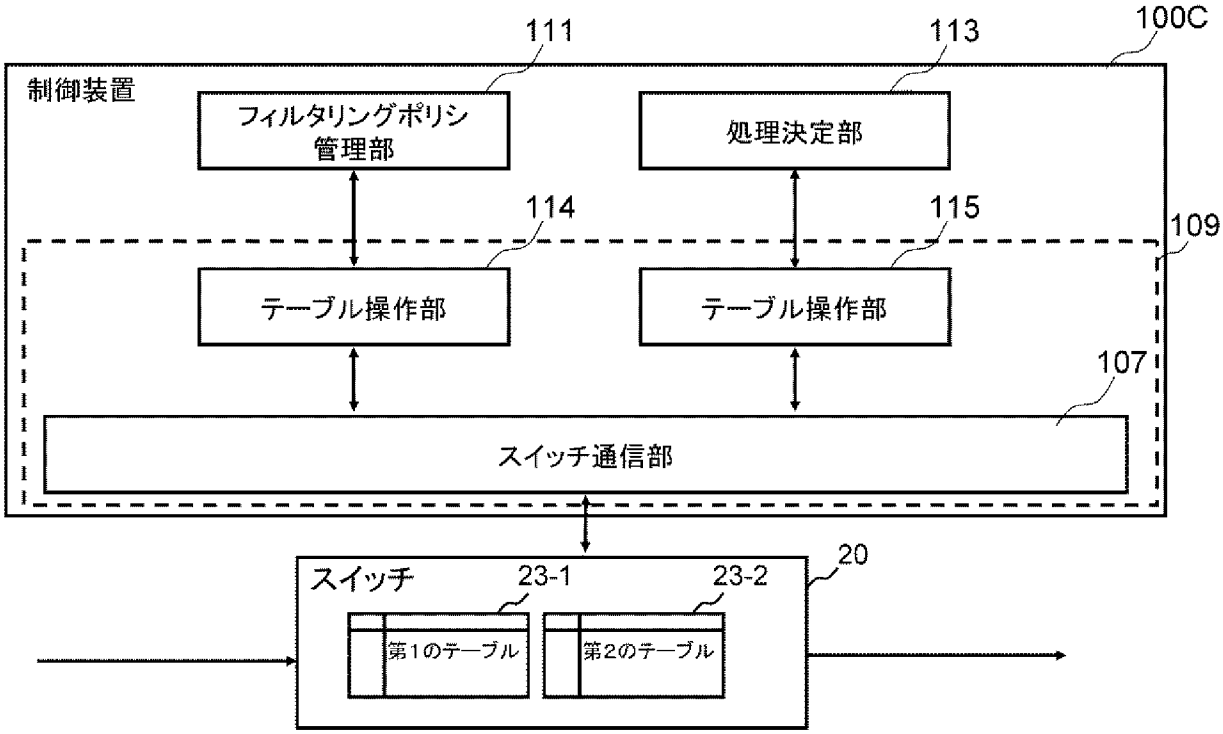
第1のテーブル

マッチ条件	処理内容
A	第2のテーブルを参照
B	廃棄
・・・	・・・

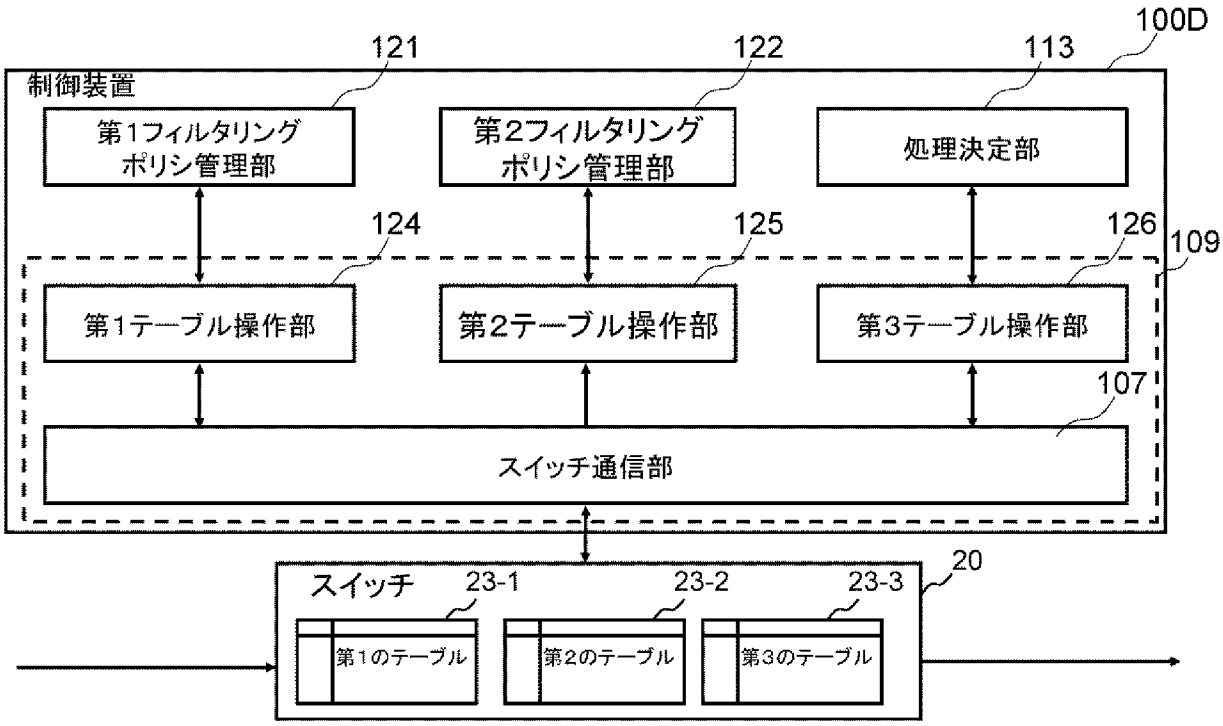
第2のテーブル

マッチ条件	処理内容
A	ポート#2から転送
・・・	・・・
・・・	・・・

[図6]



[図7]



[図8]

第1のテーブル

マッチ条件	処理内容
A	第2のテーブルを参照
B	第2のテーブルを参照
C	廃棄
・・・	・・・

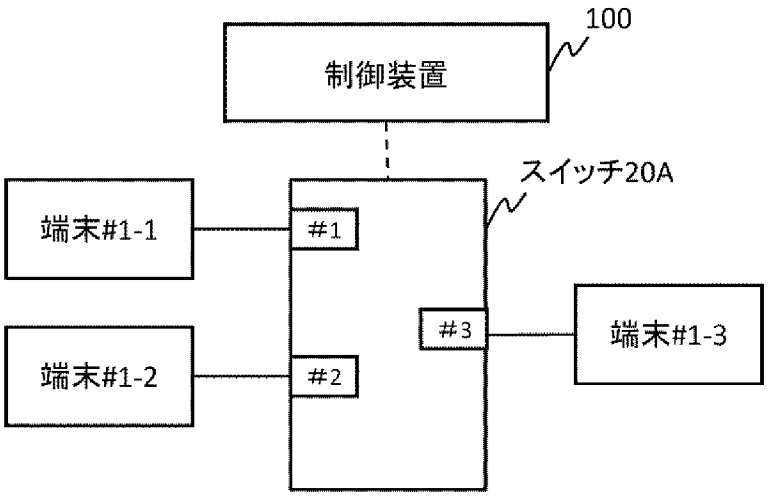
第2のテーブル

マッチ条件	処理内容
A	第3のテーブルを参照
B	廃棄
・・・	・・・
・・・	・・・

第3のテーブル

マッチ条件	処理内容
A	ポート#2から転送
・・・	・・・
・・・	・・・
・・・	・・・

[図9]



[図10]

テーブル

マッチ条件		処理内容
送信元アドレス	宛先アドレス	
#1-1	#1-1	廃棄
#1-1	#1-2	ポート#2から転送
#1-1	#1-3	ポート#3から転送
#1-2	*	廃棄
#1-3	#1-1	ポート#1から転送
#1-3	#1-2	ポート#2から転送
#1-3	#1-3	廃棄

[図11]

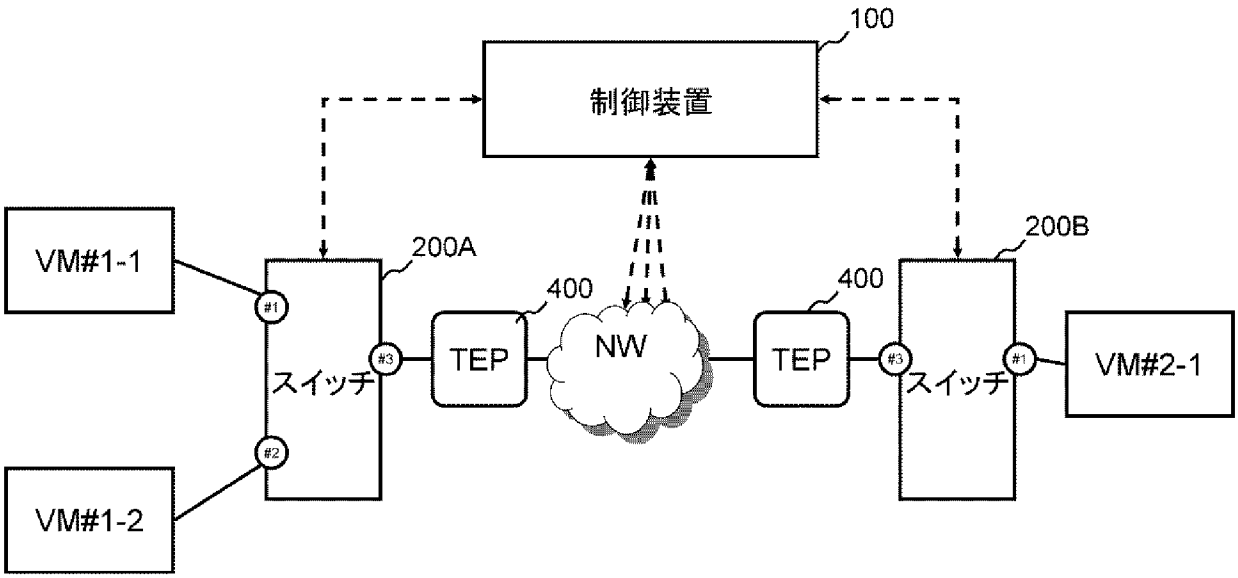
第1のテーブル

マッチ条件		処理内容
送信元アドレス	宛先アドレス	
#1-1	#1-1	廃棄
#1-3	#1-3	廃棄
#1-1	*	第2のテーブルを参照
#1-3	*	第2のテーブルを参照
A	*	廃棄

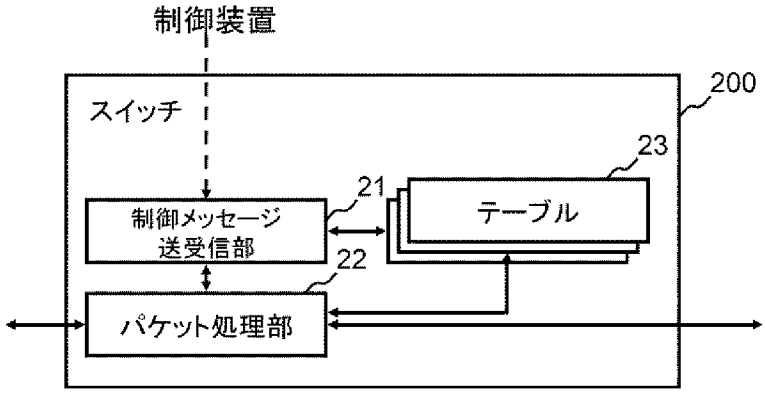
第2のテーブル

マッチ条件		処理内容
送信元アドレス	宛先アドレス	
*	#1-1	ポート#1から転送
*	#1-2	ポート#2から転送
*	#1-3	ポート#3から転送

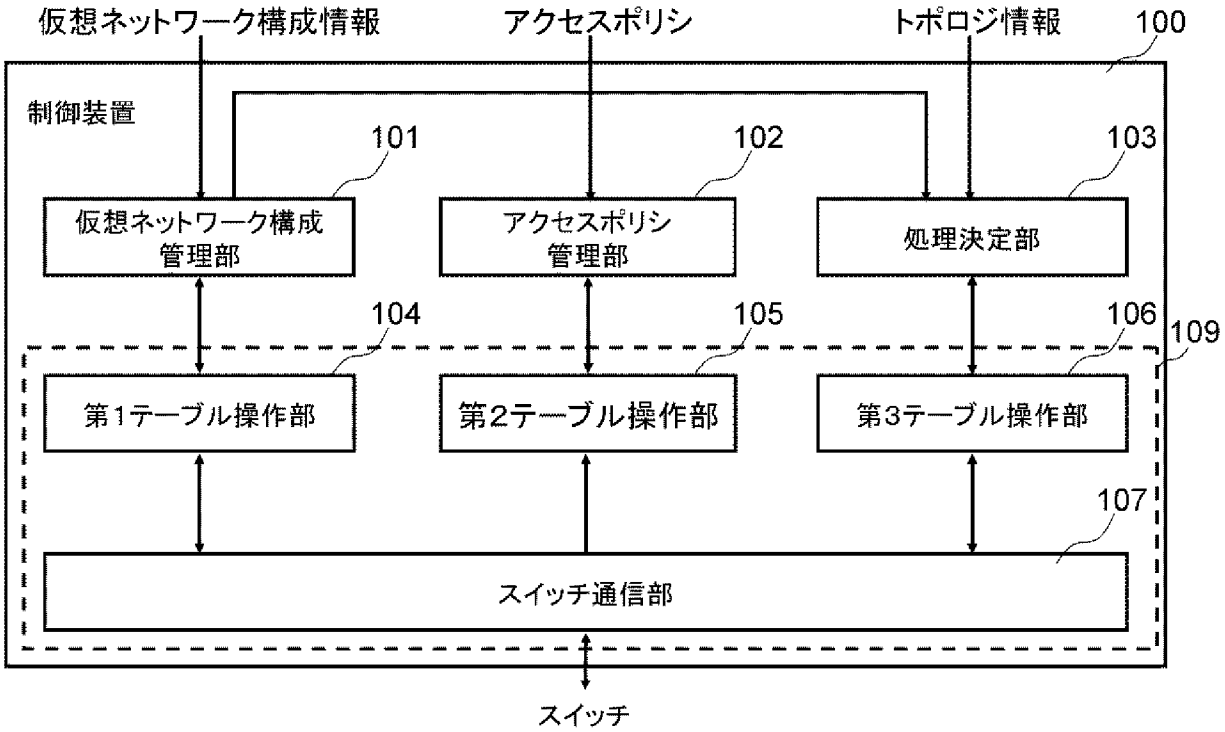
[図12]



[図13]


制御装置
スイッチ
200
23
21
テーブル
制御メッセージ
送受信部
22
パケット処理部

[図14]


仮想ネットワーク構成情報
アクセスポリシ
トポロジ情報
100
制御装置
101
102
103
仮想ネットワーク構成
管理部
アクセスポリシ
管理部
処理決定部
104
105
106
109
第1テーブル操作部
第2テーブル操作部
第3テーブル操作部
107
スイッチ通信部
スイッチ

[図15]

仮想ネットワークID	スイッチID	ポート番号	MACアドレス
1	200A	1	00:00:00:01:00:01
1	200A	2	00:00:00:01:00:02

[図16]

table#0

優先度	マッチ条件		インストラクション
	入力ポート	宛先MACアドレス	
255	1	00:00:00:01:00:01	Drop
255	2	00:00:00:01:00:02	Drop
127	*	*	Go to table #1

[図17]

table#1

優先度	マッチ条件					インストラクション
	入力ポート	送信元MACアドレス	宛先MACアドレス	タイプ（上位プロトコル）	・・・	
255	1	00:00:00:01:00:01	AA:AA:AA:AA:AA:AA	*	・・・	Drop
127	*	*	*	*	・・・	Go to table #2

[図18]

table#2

優先度	マッチ条件			インストラクション
	入力ポート	宛先MACアドレス	・・・	
255	*	00:00:00:01:00:02	・・・	Output to port #2
255	*	00:00:00:01:00:01	・・・	Output to port #1
127	1	*	・・・	Output to port #2 and #3
127	2	*	・・・	Output to port #1 and #3

[図19]

送信元 MACアドレス	宛先 MACアドレス	タイプ （上位プロトコル）	・・・	アクセス可否
00:00:00:01:00:01	00:00:00:01:00:02	0x86dd	・・・	deny

[図20]

table#1

優先度	マッチ条件					インストラクション
	入力ポート	送信元MAC アドレス	宛先MAC アドレス	タイプ （上位プロトコル）	・・・	
32768	1	00:00:00: 01:00:01	00:00:00:0 1:00:02	0x86dd	・・・	Drop
255	1	00:00:00: 01:00:01	AA:AA:AA: AA:AA:AA	*	・・・	Drop
127	*	*	*	*	・・・	Go to table #2

ADD

[図21]

仮想ネットワークID	スイッチID	ポート番号	MACアドレス
1	200A	1	00:00:00:01:00:01
1	200A	2	00:00:00:01:00:02
1	200B	1	00:00:00:02:00:01

ADD

[図22]

table#0

優先度	マッチ条件		インストラクション
	入力ポート	宛先MACアドレス	
255	1	00:00:00:01:00:01	Drop
255	2	00:00:00:01:00:02	Drop
255	3	00:00:00:02:00:01	Drop
127	*	*	Go to table #1

ADD

[図23]

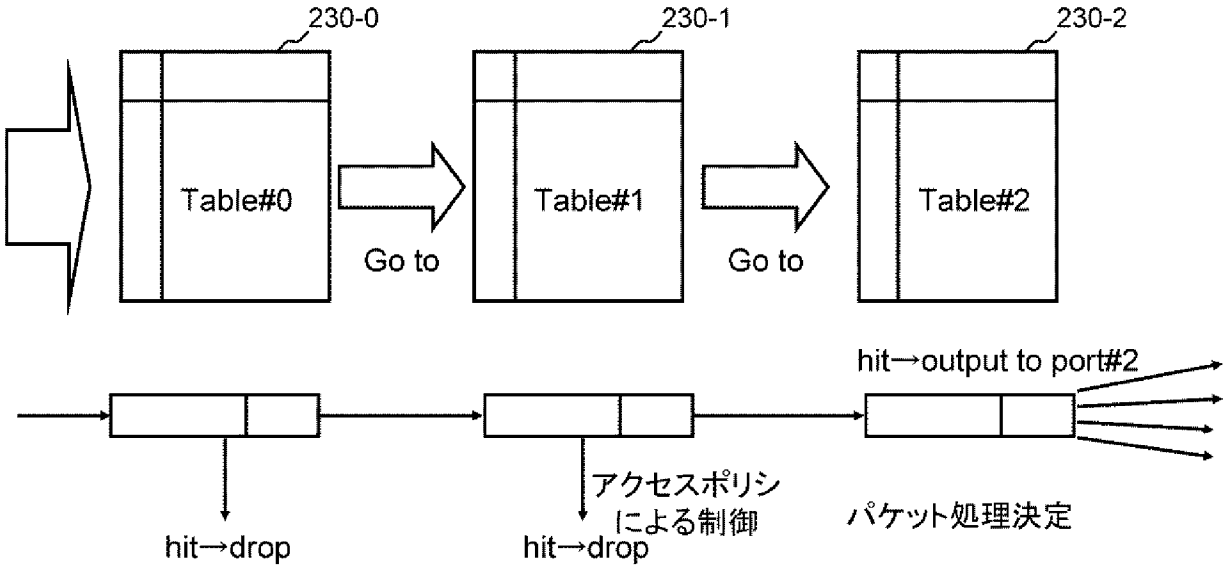
table#2

優先度	マッチ条件			インストラクション
	入力ポート	宛先MACアドレス	・・・	
255	*	00:00:00:01:00:02	・・・	Output to port #2
255	*	00:00:00:01:00:01	・・・	Output to port #1
255	*	00:00:00:02:00:01	・・・	Output to port #3
127	1	*	・・・	Output to port #2 and #3
127	2	*	・・・	Output to port #1 and #3
127	3	*	・・・	Output to port #1 and #2

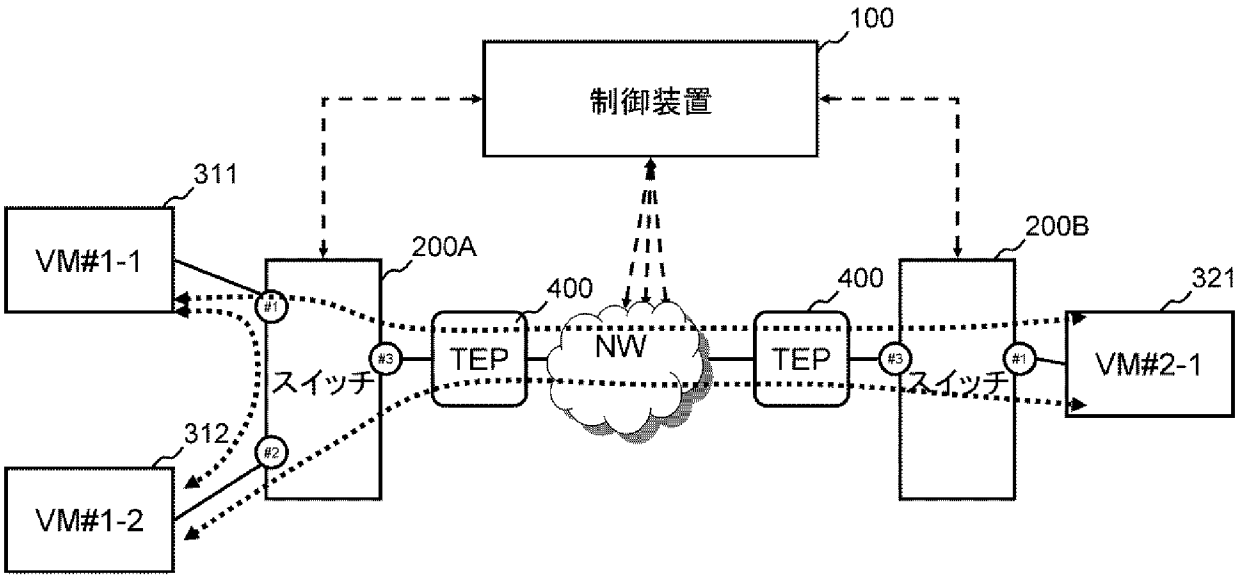
ADD

ADD

[図24]



[図25]



[図26]

table#0

優先度	マッチ条件		インストラクション
	入力ポート	宛先MACアドレス	
255	1	*	Set reg0 to 1, Go to table #1
255	2	*	Set reg0 to 1, Go to table #1
127	*	*	Drop

[図27]

table#1

優先度	マッチ条件					インストラクション
	メタデータ格納レジスタ(reg0)	入力ポート	送信元MACアドレス	宛先MACアドレス	タイプ(上位プロトコル)	
127	*	*	*	*	*	Go to table #2

[図28]

table#2

優先度	マッチ条件			インストラクション
	メタデータ格納レジスタ(reg0)	入力ポート	宛先MACアドレス	
255	1	*	00:00:00:01:00:02	Output to port #2
255	1	*	00:00:00:01:00:01	Output to port #1
127	1	1	*	Output to port #2 and #3
127	1	2	*	Output to port #1 and #3

[図29]

table#0

優先度	マッチ条件		インストラクション
	入力ポート	宛先MACアドレス	
255	1	*	Set reg0 to 1, Go to table #1
255	2	*	Set reg0 to 1, Go to table #1
255	3	*	Set reg0 to 1, Go to table #1
127	*	*	Drop

[図30]

table#1

優先度	マッチ条件					インストラクション
	メタデータ格納レジスタ(reg0)	入力ポート	送信元MACアドレス	宛先MACアドレス	タイプ(上位プロトコル)	
32768	1	1	00:00:00:01:00:01	00:00:00:01:00:02	0x86dd	Drop
127	*	*	*	*	*	Go to table #2

[図31]

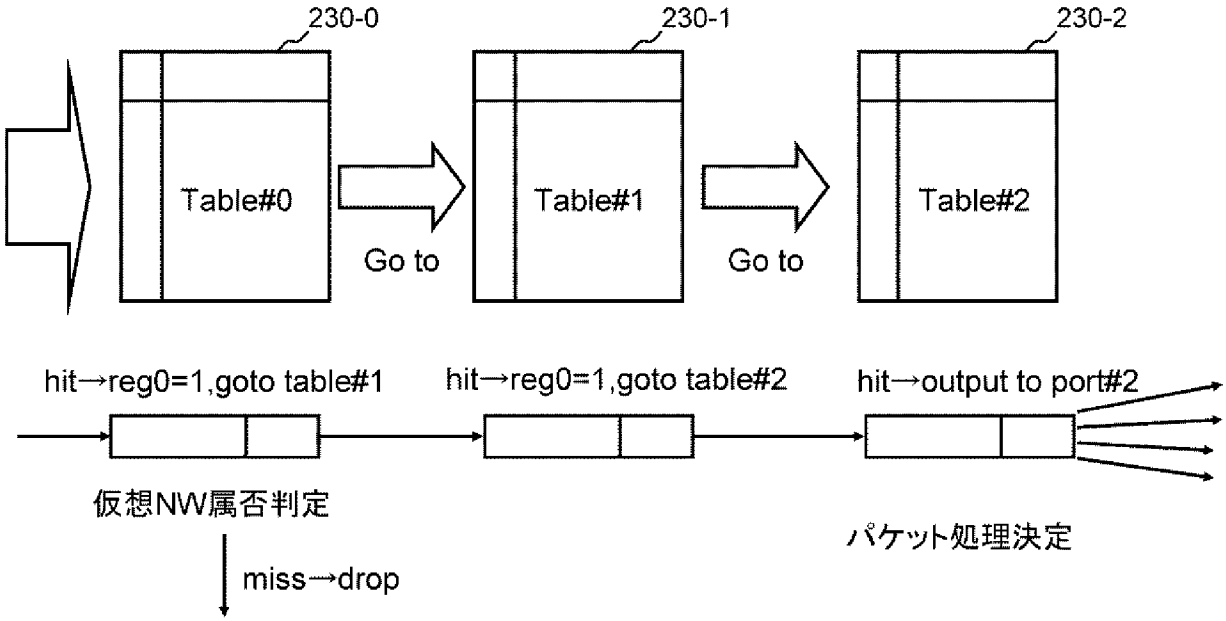
table#2

優先度	マッチ条件			インストラクション
	メタデータ格納レジスタ(reg0)	入力ポート	宛先MACアドレス	
255	1	*	00:00:00:01:00:02	Output to port #2
255	1	*	00:00:00:01:00:01	Output to port #1
255	1	*	00:00:00:02:00:01	Output to port #3
127	1	1	*	Output to port #2 and #3
127	1	2	*	Output to port #1 and #3
127	1	3	*	Output to port #1 and #2

ADD

ADD

[図32]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/050923

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/717(2013.01)i, *H04L12/66*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L12/717, H04L12/66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Shigeaki MAEDA, OpenFlow ver1.1 Oyobi ver1.2 no Tsuika Kino to Katsuyorei, Rensai: OpenFlow -Ima made no Gainen o Kutsugaesu Atarashii Network no Jitsugen-, ThinkIT, IMPRESS BUSINESS MEDIA CORP., 23 February 2012 (23.02.2012)	1-28
Y	WO 2011/43379 A1 (NEC Corp.), 14 April 2011 (14.04.2011), paragraphs [0002], [0042], [0193] & US 2011/0261723 A1	1-28

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 March, 2014 (05.03.14)	25 March, 2014 (25.03.14)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１４／０５０９２３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/717(2013.01)i, H04L12/66(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/717, H04L12/66

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１４年
日本国実用新案登録公報	１９９６－２０１４年
日本国登録実用新案公報	１９９４－２０１４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	前田繁章, OpenFlow ver1.1およびver1.2の追加機能と活用例, 連載：OpenFlow～今までの概念を覆す新しいネットワークの実現～, ThinkIT, IMPRESS BUSINESS MEDIA CORPORATION, 2012.02.23	1-28
Y	WO 2011/43379 A1（日本電気株式会社）2011.04.14, 段落［０００２］、［００４２］、［０１９３］ & US 2011/0261723 A1	1-28

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０５．０３．２０１４	２５．０３．２０１４

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｘ　４４４９
上田　翔太
電話番号　０３－３５８１－１１０１　内線　３５９６