(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2019-201364
(P2019-201364A)
(43)公開日　令和1年11月21日(2019.11.21)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/28	(2006.01)	H04L	12/28	200A	5K033

審査請求 未請求　請求項の数 6　ＯＬ　（全 18 頁）

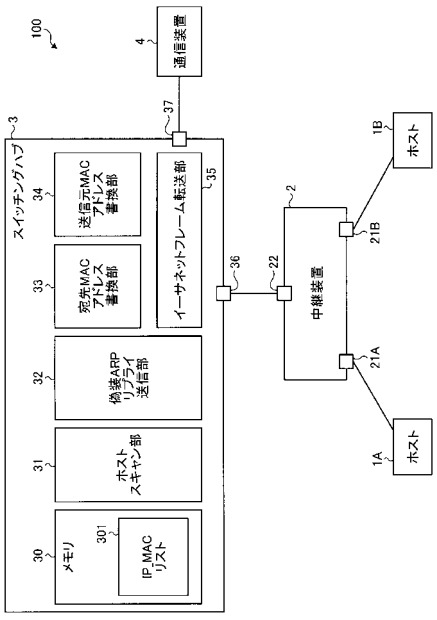
(21)出願番号　特願2018-95731(P2018-95731)
(22)出願日　平成30年5月17日(2018.5.17)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　五十嵐　弓将
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

Ｆターム(参考)　5K033 BA11　DB20　EC04

(54)【発明の名称】通信装置及び通信方法

(57)【要約】
【課題】ポートミラー機能を持たないスイッチングハブ、或いは、無線ＬＡＮのＡＰを中継点として折り返すホスト間の通信経路に対し、ホスト間の通信トラフィックをミラー可能にする。
【解決手段】ポートミラー機能を持たないスイッチングハブ或いは無線ＬＡＮのＡＰである中継装置２に接続するスイッチングハブ３は、ＡＲＰのＡＲＰリプライ部分を用いて、ホスト１Ａ，１Ｂの通信先のＰアドレスに対応するＭＡＣアドレスを、偽装ＭＡＣアドレスに書き換え、中継装置２から、偽装ＭＡＣアドレスを宛先ＭＡＣアドレスとしたイーサネットフレームを受け取ると、該イーサネットフレームの宛先ＭＡＣアドレスを本来のＭＡＣアドレスに書き換えてミラー送信し、本来のＭＡＣアドレスに書き換えられたイーサネットフレームの送信元ＭＡＣアドレスを偽装ＭＡＣアドレスに書き換えて中継装置２に送信する。
【選択図】図１



【特許請求の範囲】
【請求項１】
複数のホストを収容するとともにポートミラー機能を持たないスイッチングハブ或いは無線ＬＡＮ（Local Area Network）のアクセスポイントである中継装置に接続する通信装置であって、
前記中継装置が収容するホストのＩＰ（Internet Protocol）アドレスとＭＡＣ（Media Access Control）アドレスとを対応付けたリストを記憶するメモリと、
前記ホストの通信先のＩＰアドレスに対応するＭＡＣアドレスを、当該通信装置のＭＡＣアドレスである偽装ＭＡＣアドレスに書き換える偽装部と、
前記中継装置から送信された、偽装ＭＡＣアドレスを宛先ＭＡＣアドレスとしたイーサネットフレームに対し、前記リストを検索して、宛先ＭＡＣアドレスを、該イーサネットフレームのＩＰアドレスに対応する本来のＭＡＣアドレスに書き換える第１の書換部と、
前記第１の書換部において宛先ＭＡＣアドレスを本来のＭＡＣアドレスに書き換えられたイーサネットフレームの送信元ＭＡＣアドレスを、前記偽装ＭＡＣアドレスに書き換える第２の書換部と、
前記第１の書換部において宛先ＭＡＣアドレスを本来のＭＡＣアドレスに書き換えられたイーサネットフレームを、ミラートラフィック受信用装置に送信するとともに、前記第２の書換部において送信元ＭＡＣアドレスを前記偽装ＭＡＣアドレスに書き換えられたイーサネットフレームを、前記中継装置に送信する送信部と、
を有することを特徴とする通信装置。
【請求項２】
前記中継装置が収容するホストのＩＰアドレスとＭＡＣアドレスとをスキャンし、ＩＰアドレスとＭＡＣアドレスとを対応付けたリストを前記メモリに格納するスキャン部をさらに有することを特徴とする請求項１に記載の通信装置。
【請求項３】
前記スキャン部は、予め与えられる、前記ホストが属するＩＰサブネットのネットワークアドレスと、サブネットマスクとの２つの情報から、前記中継装置に接続されるホストが持つＩＰアドレスの値の範囲を計算し、ＡＲＰ（Address Resolution Protocol）を用いて、前記ホストが持つ可能性のあるＩＰアドレスの値の範囲の全てのＭＡＣアドレスをスキャンすることを特徴とする請求項２に記載の通信装置。
【請求項４】
前記偽装部は、ＡＲＰのＡＲＰリプライ部分を用いて、前記ホストのＡＲＰキャッシュを書き換えて、前記ホストの通信先のＩＰアドレスに対応するＭＡＣアドレスを、当該通信装置のＭＡＣアドレスである偽装ＭＡＣアドレスに書き換えることを特徴とする請求項３に記載の通信装置。
【請求項５】
前記通信装置は、スイッチングハブであることを特徴とする請求項１～４のいずれか一つに記載の通信装置。
【請求項６】
複数のホストを収容するとともにポートミラー機能を持たないスイッチングハブ或いは無線ＬＡＮのアクセスポイントである中継装置に接続する通信装置が実行する通信方法であって、
前記通信装置は、前記中継装置が収容するホストのＩＰアドレスとＭＡＣアドレスとを対応付けたリストを記憶するメモリを有し、
前記ホストの通信先のＩＰアドレスに対応するＭＡＣアドレスを、当該通信装置のＭＡＣアドレスである偽装ＭＡＣアドレスに書き換える偽装工程と、
前記中継装置から送信された、偽装ＭＡＣアドレスを宛先ＭＡＣアドレスとしたイーサネットフレームに対し、前記リストを検索して、宛先ＭＡＣアドレスを、該イーサネットフレームのＩＰアドレスに対応する本来のＭＡＣアドレスに書き換える第１の書換工程と、

前記第１の書換工程において宛先ＭＡＣアドレスを本来のＭＡＣアドレスに書き換えられたイーサネットフレームの送信元ＭＡＣアドレスを、前記偽装ＭＡＣアドレスに書き換える第２の書換工程と、
前記第１の書換工程において宛先ＭＡＣアドレスを本来のＭＡＣアドレスに書き換えられたイーサネットフレームを、ミラートラフィック受信用装置に送信する第１の送信工程と、
前記第２の書換工程において送信元ＭＡＣアドレスを前記偽装ＭＡＣアドレスに書き換えられたイーサネットフレームを、前記中継装置に送信する第２の送信工程と、
を含んだことを特徴とする通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信装置及び通信方法に関する。
【背景技術】
【０００２】
リピータハブを利用する通信方法がある。リピータハブとは、ＯＳＩ（Open Systems Interconnection）参照モデルの物理層（レイヤ１）で動作し、複数のホストの間の通信を中継する機器のことをいう。ここで、ＯＳＩ参照モデルとは、国際標準化機構（International Organization for Standardization：ＩＳＯ）により策定されたコンピュータなどの通信機器の通信機能を階層構造に分割した国際標準のモデルであり、第１層から第７層まで７つの層が定義されている。
【０００３】
リピータハブは、スター型と呼ばれるネットワークトポロジー（形態）で端末などのホストと接続される。すなわち、リピータハブは、複数のホストと接続して、複数のホストの間の通信を中継する中心的な役割を果たすネットワーク機器である。
【０００４】
次に、リピータハブの動作を説明する。まず、リピータハブは、ホストが送信した電気信号を、ホストを収容する物理的なポートで受信する。この物理的なポートは、１本の電気信号を伝送するケーブルによってホストと接続されている。次に、リピータハブは、受信した電気信号の波形の増幅と整形後に、リピータハブの持つ他の全てのポートに受信した電気信号を送信する。
【０００５】
このような機能を持つリピータハブを利用すると、以下のようにしてコンピュータネットワークにおける通信トラフィックをミラーすることが可能である。まず、ミラー対象となる通信を行うホストをリピータハブに接続する。この場合、３つ以上の複数のホストを接続してもよい。次に、リピータハブの空きポートに通信トラフィックを取得する機器などを接続する。リピータハブは、自身のあるポートに受信した電気信号を他の全てのポートに送信するため、リピータハブのある１つのポートには、リピータハブを通過する全ての通信がミラーされることになる。
【０００６】
このように、リピータハブを利用すると、リピータハブを通過する全ての通信をミラーすることが可能である。しかしながら、リピータハブを利用する場合には、ある１つのホストから受信した電気信号が常に全ての他のポートに送信されるため、無駄なトラフィックや通信の衝突が発生するという問題がある。
【０００７】
無駄なトラフィックとは、例えば、リピータハブに接続されるある２つのホストの間で通信が行われる場合、リピータハブの全てのポートに、２つのホスト間の通信が送信されることによる。すなわち、実際には、２つのホストが接続されるポートにだけ電気信号を中継すれば２つのホスト間の通信は成立するが、リピータハブは、それ以外のポートにも不要な電気信号を送信してしまうため、無駄な通信のトラフィックが発生する。

【０００８】
　また、通信の衝突とは、ある同時刻にリピータハブに接続した２つ以上のホストが電気信号を送信した場合に、リピータハブにおいてそれらの電気信号を全て同時に他のポートに送信することは不可能であるために発生する。
【０００９】
　このような通信の衝突の発生を減らすために、コリジョン（衝突）ドメインの分割と呼ばれる電気信号の到達範囲を分割する方法や、電気信号の送信可否をホストが確認した後で送信を行う方式などが利用されている。
【００１０】
　例えば、近年では、ネットワークの伝送速度が上がるに伴い、スイッチングハブと呼ばれる、コリジョン（衝突）ドメインをできるだけ小さくするネットワーク機器が主に利用されている。
【００１１】
　スイッチングハブとは、ＯＳＩ参照モデルのデータリンク層（レイヤ２）で動作する機器であり、リピータハブの複数のホストの間の通信を中継する機能に加えて、データリンク層のイーサネット（登録商標）フレームのヘッダを解読する機能を持つネットワーク機器である。
【００１２】
　スイッチングハブは、自身のあるポートにホストからのイーサネットフレームを受信すると、イーサネットフレームヘッダに含まれる宛先ＭＡＣ（Media Access Control）アドレス（フレームの宛先を示すアドレス）を参照し、宛先アドレスに該当するホストが接続されているポートにのみフレームを転送する。このような機能によって、スイッチングハブは、リピータハブの無駄なトラフィックや通信の衝突が発生するという問題を解決している。
【００１３】
　しかしながら、スイッチングハブではリピータハブと同様の方式で通信トラフィックをミラーすることはできない。これは、リピータハブは自身のあるポートに受信した電気信号を他の全てのポートに送信したが、スイッチングハブは宛先ＭＡＣアドレスに該当するホストが接続されているポートにしかフレームを送信しないためである。したがって、スイッチングハブにおいては、トラフィックのミラーを実現する方式としてポートミラー方式が利用されている（非特許文献１参照）。
【００１４】
　ポートミラー方式とは、スイッチングハブのポート単位でトラフィックをミラーするか否かを設定し、ミラーする設定を行ったポートが送信または受信、或いは、送受信するイーサネットフレームを、ミラー先となる通信トラフィックの取り出し専用に割り当てた別のポートに全て複製する方式である。このようなポートミラー方式を用いれば、スイッチングハブでも通信トラフィックのミラーは可能である。
【先行技術文献】
【非特許文献】
【００１５】
【非特許文献１】ネットワーク機器講座｜スイッチ編、［online］、［平成３０年５月１０日検索］、インターネット＜ＵＲＬ：https://www.allied-telesis.co.jp/library/nw_guide/device/switch.html#003＞
【発明の概要】
【発明が解決しようとする課題】
【００１６】
　しかしながら、ポートミラー方式には、以下の２つの問題がある。
【００１７】
　第一に、ポートミラー機能を有するスイッチングハブ以外では、ミラーできないという問題がある。ポートミラー機能は、付加的機能であるため、このポートミラー機能を持た

ないスイッチングハブ製品も多い。そして、ポートミラー機能を有する製品は、高機能なスイッチングハブとして高価になる場合がある。特に、ポートミラー機能を持たないスイッチングハブでは、そのスイッチングハブに接続されるある２つのホスト間の通信は、２つのホストが接続されるスイッチングハブのポートの間でのみ中継される。このため、この場合には、スイッチングハブを中継点として折り返すホスト間の通信をミラーして取得することができない。スイッチングハブの通信トラフィックをミラーするためには、ポートミラー機能を有するスイッチングハブを別途用意して、ホスト間の通信経路の途中に挿入する必要がある。

【００１８】

第二に、無線通信のコンピュータネットワークである無線ＬＡＮ（Local Area Network）には、ポートミラー方式を適用することができないという問題がある。有線通信では通信を行うホストとそれを収容するスイッチングハブとの間は、物理的な１本のケーブルによって接続されるため、ポート単位のミラーが可能である。しかしながら、無線通信では、通信を行うホストとそれを収容するアクセスポイント（ＡＰ）と呼ばれる機器との間は、無線で接続されるため、電気信号の伝送路は電磁波であり、スイッチングハブに相当する機能は、ＡＰの内部に隠蔽されている。そのため、無線ＬＡＮでは、ポートミラー機能を有する有線のスイッチングハブを無線通信経路の途中に挿入することができない。

【００１９】

このように、コンピュータネットワークにおける従来の通信トラフィックのミラー方式には、第一の問題として、ポートミラー機能を有するスイッチングハブを別途用意してホスト間の通信経路の途中に挿入しない限り、通信トラフィックをミラーできないという問題がある。また、第二の問題として、無線通信を行う無線ＬＡＮでは、無線によるホスト間の通信経路にポートミラー機能を有するスイッチングハブを挿入することは不可能であるため、通信トラフィックをミラーできないという問題点がある。

【００２０】

本発明は、上記に鑑みてなされたものであって、ポートミラー機能を持たないスイッチングハブ、或いは、無線ＬＡＮのＡＰを中継点として折り返すホスト間の通信経路に対し、ホスト間の通信トラフィックをミラー可能にする通信装置及び通信方法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】

【００２１】

本発明の通信システムは、複数のホストを収容するとともにポートミラー機能を持たないスイッチングハブ或いは無線ＬＡＮのアクセスポイントである中継装置に接続する通信装置であって、中継装置が収容するホストのＩＰ（Internet Protocol）アドレスとＭＡＣアドレスとを対応付けたリストを記憶するメモリと、ホストの通信先のＩＰアドレスに対応するＭＡＣアドレスを、当該通信装置のＭＡＣアドレスである偽装ＭＡＣアドレスに書き換える偽装部と、中継装置から送信された、偽装ＭＡＣアドレスを宛先ＭＡＣアドレスとしたイーサネットフレームに対し、リストを検索して、宛先ＭＡＣアドレスを、該イーサネットフレームのＩＰアドレスに対応する本来のＭＡＣアドレスに書き換える第１の書換部と、第１の書換部において宛先ＭＡＣアドレスを本来のＭＡＣアドレスに書き換えられたイーサネットフレームの送信元ＭＡＣアドレスを、偽装ＭＡＣアドレスに書き換える第２の書換部と、第１の書換部において宛先ＭＡＣアドレスを本来のＭＡＣアドレスに書き換えられたイーサネットフレームを、ミラートラフィック受信用装置に送信するとともに、第２の書換部において送信元ＭＡＣアドレスを偽装ＭＡＣアドレスに書き換えられたイーサネットフレームを、中継装置に送信する送信部と、を有することを特徴とする。

【発明の効果】

【００２２】

本発明によれば、ポートミラー機能を持たないスイッチングハブ、或いは、無線ＬＡＮのＡＰを中継点として折り返すホスト間の通信経路に対し、ホスト間の通信トラフィックをミラー可能にする。

【図面の簡単な説明】
【００２３】
【図１】図１は、実施の形態に係る通信システムの構成を説明する図である。
【図２】図２は、図１に示すＩＰ－ＭＡＣリストのデータ構成の一例を示す図である。
【図３】図３は、実施の形態に係る通信システムの通信トラフィックのミラー処理の流れを説明する図である。
【図４】図４は、実施の形態に係る通信システムの通信トラフィックのミラー処理の流れを説明する図である。
【図５】図５は、実施の形態に係る通信システムの通信トラフィックのミラー処理の流れを説明する図である。
【図６】図６は、実施の形態に係る通信システムの通信トラフィックのミラー処理の流れを説明する図である。
【図７】図７は、実施の形態に係る通信システムの通信トラフィックのミラー処理の流れを説明する図である。
【図８】図８は、実施の形態に係る通信システムの通信トラフィックのミラー処理の流れを説明する図である。
【図９】図９は、実施の形態に係る通信システムのホストスキャン処理の処理手順を示すシーケンス図である。
【図１０】図１０は、実施の形態に係る通信システムのミラー処理の処理手順を示すシーケンス図である。
【発明を実施するための形態】
【００２４】
以下、図面を参照して、本発明の一実施形態を詳細に説明する。なお、この実施の形態により本発明が限定されるものではない。また、図面の記載において、同一部分には同一の符号を付して示している。
【００２５】
［実施の形態］
本実施の形態では、ホストを収容する中継装置とは別に、中継装置に接続する他の通信装置（後述のスイッチングハブ３）を用いて、ホスト間の通信トラフィックをミラーする通信システムを例に説明する。
【００２６】
［通信システムの構成］
図１は、実施の形態に係る通信システムの構成を説明する図である。図１に示すように、例えば、実施の形態に係る通信システム１００では、２つのホスト１Ａ、１Ｂと、中継装置２と、スイッチングハブ３とを有する。この中継装置２は、ポートミラー機能を持たない、或いは、無線ＬＡＮのＡＰである。そして、スイッチングハブ３は、中継装置２の１つのポートに、有線で接続する。なお、ホストの台数は、一例である。また、ホスト１Ａ，１Ｂを区別することなく説明する場合には、ホスト１とする。
【００２７】
ホスト１Ａ、１Ｂは、中継装置２を中継点として折り返す通信を行う。ホスト１Ａは、ＩＰアドレスが「IP_A」であり、ＭＡＣアドレスが「MAC_A」である。ホスト１Ｂは、ＩＰアドレスが「IP_B」であり、ＭＡＣアドレスが「MAC_B」である。
【００２８】
中継装置２は、ポートミラー機能を持たないスイッチングハブ或いは無線ＬＡＮのＡＰである。中継装置２は、一般的なスイッチングハブの機能を有し、受信したイーサネットフレームヘッダに含まれる宛先ＭＡＣアドレスにしたがって、宛先アドレスに該当するホストが接続されているポートにイーサネットフレームを転送する。図１の例では、ホスト１Ａからホスト１Ｂへの経路は、ホスト１Ａ、中継装置２、ホスト１Ｂとなる。なお、ポート２１Ａは、ホスト１Ａとの接続用ポートであり、ポート２１Ｂは、ホスト１Ｂとの接続用ポートであり、ポート２２は、スイッチングハブ３との接続用ポートである。

【００２９】
スイッチングハブ３は、中継装置２がポートミラー機能を持たないスイッチングハブの場合には、送受信のポート３６を介して、中継装置２であるスイッチングハブの１つのポート（例えば、ポート２２）に、他のホスト１と同様に有線で接続する。また、スイッチングハブ３は、中継装置２が無線ＬＡＮのＡＰである場合には、中継装置２であるＡＰが持つ無線ＬＡＮと同じＩＰサブネットに属する有線インターフェース（ポート）に有線で接続する。
【００３０】
また、スイッチングハブ３は、ポート３７を介して、通信装置４と接続する。通信装置４は、ポート３７を介して、スイッチングハブ３によってミラーされた通信トラフィックをキャプチャする。
【００３１】
この通信システム１００では、ポートミラー機能を持たないスイッチングハブ、或いは、無線ＬＡＮのＡＰである中継装置２を中継点として折り返すホスト１Ａ、１Ｂ間の通信経路を、外部のスイッチングハブ３を用いて操作し、ホスト１Ａ、１Ｂ間の通信トラフィックをミラー可能にする。
【００３２】
［スイッチングハブの構成］
そこで、次に、スイッチングハブ３の構成について説明する。図１に示すように、スイッチングハブ３は、メモリ３０、ホストスキャン部３１（スキャン部）、偽装ＡＲＰ（Address Resolution Protocol：アドレス解決プロトコル）リプライ送信部３２（偽装部）、宛先ＭＡＣアドレス書換部３３（第１の書換部）、送信元ＭＡＣアドレス書換部３４（第２の書換部）、イーサネットフレーム転送部３５（送信部）、ポート３６，３７を有する。
【００３３】
ホストスキャン部３１、偽装ＡＲＰリプライ送信部３２、宛先ＭＡＣアドレス書換部３３、送信元ＭＡＣアドレス書換部３４及びイーサネットフレーム転送部３５の機能は、基板上に形成される。ポート３６は、中継装置２接続用のポートである。ポート３７は、ミラートラフィック取り出し用に用意されたポートである。ポート３７には、例えば、ミラーされたパケットをキャプチャする通信装置４が有線で接続する。
【００３４】
メモリ３０は、基板上に形成されたＲＡＭ（Random Access Memory）、フラッシュメモリ（Flash Memory）等の半導体メモリ素子で実現される。メモリ３０は、スイッチングハブ３の動作処理に関するデータを記憶する。具体的には、メモリ３０は、ＩＰ－ＭＡＣリスト３０１を記憶する。ＩＰ－ＭＡＣリスト３０１は、中継装置２が収容するミラー対象のホスト１Ａ、１ＢのＩＰアドレスとＭＡＣアドレスとを対応付けたデータである。
【００３５】
図２は、図１に示すＩＰ－ＭＡＣリスト３０１のデータ構成の一例を示す図である。図２に示すように、ＩＰ－ＭＡＣリスト３０１は、ホストのＩＰアドレスと、ＭＡＣアドレスとを項目として有する。例えば、ＩＰ－ＭＡＣリスト３０１には、ＩＰアドレス「IP_A」にＭＡＣアドレスが「MAC_A」が対応付けられており、ＩＰアドレス「IP_B」にＭＡＣアドレス「MAC_B」が対応付けられている。
【００３６】
ホストスキャン部３１は、中継装置２に接続しているホスト１Ａ、１ＢのＩＰアドレスとＭＡＣアドレスとの組をスキャンし、ＩＰアドレスとＭＡＣアドレスとを対応付けたＩＰ－ＭＡＣリスト３０１をメモリ３０に格納する。
【００３７】
具体的には、ホストスキャン部３１は、予め与えられる、ホスト１Ａ、１Ｂが属するＩＰサブネットのネットワークアドレスと、サブネットマスクとの２つの情報から、中継装置２に接続されているホストが持つＩＰアドレスの値の範囲を計算する。例えば、ネット

ワークアドレスが「192.168.1.0」でサブネットマスクが「255.255.255.0」であった場合について説明する。この場合には、中継装置２に接続されているＩＰサブネットのホスト部は、サブネットマスクでマスクされていないアドレス部分、すなわち「192.168.1.X」の第四オクテット部分である「0」～「255」となる。したがって、このＩＰサブネットに接続するホストは、ＩＰアドレスとして「192.168.1.0」～「192.168.1.255」までの値を取る可能性があることが計算により分かる。

【００３８】

そして、ホストスキャン部３１は、ＡＲＰ（例えば、［online］、［平成３０年５月１０日検索］、インターネット＜ＵＲＬ：http://www.infraexpert.com/study/tcpip2.html＞、及び、［online］、［平成３０年５月１０日検索］、インターネット＜ＵＲＬ：http://www.infraexpert.com/study/dhcpz6.html＞参照）と呼ばれる、あるＩＰアドレスに対応するＭＡＣアドレスを取得する通信プロトコルを用いて、ホストが持つ可能性のあるＩＰアドレスの値の範囲の全てのＭＡＣアドレスをスキャンする。

【００３９】

例えば、ホストスキャン部３１が、ＩＰアドレス「192.168.1.1」に対応するＭＡＣアドレスを調査する場合には、問い合わせ元のホストスキャン部３１自身のＭＡＣアドレス「MAC_D」を送信元ＭＡＣアドレスとして、ＩＰアドレス「192.168.1.1」を持つホストのＭＡＣアドレスを応答するように要求するイーサネットフレーム（ＡＲＰリクエストと呼ぶ）を中継装置２に接続している全ホスト１Ａ、１Ｂに対して一斉同報（ブロードキャスト）する。

【００４０】

ＡＲＰリクエストを受信した全ホスト１Ａ、１Ｂは、自身のＩＰアドレスがＡＲＰリクエストで問い合わせを受けているＩＰアドレスと一致するか比較し、一致する場合には自身のＭＡＣアドレスをＡＲＰリプライとして問い合わせ元に応答するイーサネットフレームを送信する。ＡＲＰリプライは中継装置２で受信され、宛先ＭＡＣアドレス（問い合わせ元）「MAC_D」の接続しているポートに送信される。

【００４１】

このようにして、ホストスキャン部３１は、ＡＲＰによるスキャンを繰り返しＩＰサブネットの全てのＩＰアドレスに対して用いることで、中継装置２に接続している全てのホスト１Ａ、１ＢのＩＰアドレスとＭＡＣアドレスとの組を取得することができる。

【００４２】

ホストスキャン部３１は、上記の手順で取得した中継装置２に接続しているホストのＩＰアドレスとＭＡＣアドレスとの組のリストであるＩＰ－ＭＡＣリスト３０１を、メモリ３０に格納する。

【００４３】

なお、ホストスキャン部３１は、上記で述べたように中継装置２に接続しているホストのＩＰアドレスとＭＡＣアドレスとの組をアクティブにスキャンするだけでなく、ホスト１Ａ、１Ｂがブロードキャストするａｒｐリクエストをパッシブに受信して、ＡＲＰリクエストの送信元ホストのＩＰアドレスとＭＡＣアドレスとを、スイッチングハブ３内部のメモリ３０に保持することもできる。ただし、この場合には、中継装置２に接続しているホスト全てのＩＰアドレスとＭＡＣアドレスとの組を取得できるとは限らない。

【００４４】

次に、偽装ＡＲＰリプライ送信部３２について説明する。偽装ＡＲＰリプライ送信部３２は、ホストの通信先のＩＰアドレスに対応するＭＡＣアドレスを、別のＭＡＣアドレス（ここでは偽装ＭＡＣアドレスと呼ぶ）に書き換える。偽装ＡＲＰリプライ送信部３２は、偽装アドレスとして、当該通信装置のＭＡＣアドレスを用いる。偽装ＡＲＰリプライ送信部３２は、ＡＲＰのＡＲＰリプライ部分のみを利用して、あるホストのＩＰアドレスに対応するＭＡＣアドレスを偽装アドレスに書き換える。この機能は、一般には「ＡＲＰキャッシュポイズニング」と呼ばれる、ホストが保持しているＩＰアドレスとＭＡＣアドレスとの一時記憶情報（ＡＲＰキャッシュと呼ぶ）を強制的に書き換えて不正な通信を行う

、コンピュータネットワーク通信に対する攻撃の一種である。

【００４５】

ホストスキャン部３１で説明したように、通常ＡＲＰ機能は、ＡＲＰリクエストとそれに応答するＡＲＰリプライによって動作している。しかし、ＡＲＰリクエストがない場合でも、ＡＲＰリプライのみをホストに送信することにより、標的となるホストのＡＲＰキャッシュの内容を書き換えることが可能である。

【００４６】

例えば、図１において、あるホスト（ＭＡＣアドレスが「MAC_B」とする）がＡＲＰキャッシュ内にホスト１のＩＰアドレス「IP_A」とそれに対応するＭＡＣアドレス「MAC_A」とを保持していたとする。正常通信では、ホスト「MAC_B」は、ホスト「IP_A」と通信しようとした場合、宛先ＭＡＣアドレス「MAC_A」を自身のＡＲＰキャッシュから検索、抽出した後、宛先ＭＡＣアドレスを「MAC_A」としてイーサネットフレームを中継装置２に送信している。

【００４７】

この正常状態に対し、偽装ＡＲＰリプライ送信部３２は、ホスト「IP_A」に対応するＭＡＣアドレスを、自身の偽装ＭＡＣアドレス「MAC_D」であるとするＡＲＰリプライを標的となるホスト「MAC_B」に周期的に送信する。この偽装ＭＡＣアドレスを含むＡＲＰリプライを標的となるホスト１に送信する時間周期は、ＡＲＰキャッシュの一時記憶が消失しないで維持されるために十分短い時間とする。このように偽装ＭＡＣアドレスのＡＲＰリプライを周期的に送りつけることにより、偽装ＡＲＰリプライ送信部３２は、強制的に標的となるホスト１のＡＲＰキャッシュを書き換えることが可能である。

【００４８】

偽装ＭＡＣアドレスを受信した標的となるホストは、あるホストのＩＰアドレスに対応するＭＡＣアドレスを偽装されたＭＡＣアドレスとして記憶するので、当該ＩＰアドレス宛のイーサフレームの宛先ＭＡＣアドレスは偽装ＭＡＣアドレスとなって送信される。

【００４９】

以上の手順を、偽装ＡＲＰリプライ送信部３２は、ホストスキャン部３１で取得した中継装置２に接続しているホスト１のＩＰアドレスとＭＡＣアドレスとの組に対して実施すると、中継装置２に接続しているホスト１が保持するＡＲＰキャッシュの宛先ＭＡＣアドレスを偽装ＭＡＣアドレスに書き換えることが可能である。なお、この偽装ＡＲＰリプライ送信部３２によるＡＲＰキャッシュの書き換えは、ホストスキャン部３１で取得した中継装置２に接続しているホスト全てに対して実施してもよいし、その一部のホストに対してのみ実施してもよい。スイッチングハブ３では、ＡＲＰキャッシュの書き換えを行った宛先ＭＡＣアドレスの通信のみ、そのトラフィックをミラーすることが可能である。

【００５０】

また、ＡＲＰキャッシュの書き換えを中継装置２に接続しているホスト全てに対して実施する場合には、以下のように行う。まず、偽装ＡＲＰリプライ送信部３２は、ホストスキャン部３１で取得した中継装置２に接続しているホストのＩＰ－ＭＡＣリスト３０１全体を取り出す。次に、偽装ＡＲＰリプライ送信部３２は、ホスト１のＩＰアドレスとＭＡＣアドレスとの組を一つ選び、各ＩＰアドレスについてＡＲＰキャッシュを書き換える操作を、そのＩＰアドレス以外の全てのホストに対して実施する。偽装ＡＲＰリプライ送信部３２は、この操作をＩＰ－ＭＡＣリスト３０１にある全てのＩＰアドレスに対して実施することにより、全てのＩＰアドレスに対応するＭＡＣアドレスを偽装ＭＡＣアドレスに書き換える。これにより、中継装置２に接続しているホスト１全てが通信を行う際に偽装ＭＡＣアドレスに向けてイーサネットフレームを送信するようになる。

【００５１】

宛先ＭＡＣアドレス書換部３３は、中継装置２から送信された、偽装ＭＡＣアドレスを宛先ＭＡＣアドレスとしたイーサネットフレームに対し、宛先ＭＡＣアドレスを、該イーサネットフレームのＩＰアドレスに対応する本来のＭＡＣアドレスに書き換える。宛先ＭＡＣアドレス書換部３３は、書き換えの際に、ＩＰ－ＭＡＣリスト３０１を検索して、イ

ーサネットフレームのＩＰアドレスに対応する本来のＭＡＣアドレスを取得する。
【００５２】
宛先ＭＡＣアドレス書換部３３は、受け取ったイーサネットフレームに含まれるＩＰパケットの宛先ＩＰアドレスを参照し、その値を基に、ＩＰ－ＭＡＣリスト３０１から、宛先ＩＰアドレスに対応するホスト１のＭＡＣアドレスを検索する。この検索によって得られる宛先のＩＰアドレスとＭＡＣアドレスとの組は、本来の正常な通信が行われる場合に用いられる値である。
【００５３】
宛先ＭＡＣアドレス書換部３３は、受け取ったイーサネットフレームの偽装ＭＡＣアドレスとなっている宛先ＭＡＣアドレスを、この本来の正常な通信が行われる場合に用いられる宛先ＭＡＣアドレスに書き換える。例えば、図１において、ホスト「MAC_B」がホスト「IP_A」と通信しようとして、偽装ＡＲＰリプライ送信部３２によって書き換えられたホスト「MAC_B」内部のＡＲＰキャッシュを参照し、宛先ＭＡＣアドレスを偽装ＭＡＣアドレスである「MAC_D」としてイーサネットフレームを送信する。この場合、そのイーサネットフレームは、中継装置２を経由してスイッチングハブ３に届く。このスイッチングハブ３に届いたイーサネットフレームの送信元ＭＡＣアドレスは、「MAC_B」である。
【００５４】
宛先ＭＡＣアドレス書換部３３は、そのイーサネットフレームを受け取り、その宛先ＭＡＣアドレスをホスト「IP_A」の本来のＭＡＣアドレスである「MAC_A」に書き換える。宛先ＭＡＣアドレス書換部３３は、宛先ＭＡＣアドレスを書き換えたイーサネットフレームをイーサネットフレーム転送部３５に送る。
【００５５】
イーサネットフレーム転送部３５は、宛先ＭＡＣアドレス書換部３３において宛先ＭＡＣアドレスを本来のＭＡＣアドレスに書き換えられたイーサネットフレームをポート３７から通信装置４に送信する。イーサネットフレーム転送部３５の機能は、既存の市中／公開技術のOpen vSwitch（例えば、［online］、［平成３０年５月１０日検索］、インターネット＜ＵＲＬ：https://docs.openvswitch.org/en/latest/tutorials/faucet/＞参照）などに実装されている、ＭＡＣアドレス、ＩＰアドレス、ＩＰポート番号などを参照して、イーサネットフレームやそれに含まれるＩＰパケットを転送する機能を利用して実現できる。
【００５６】
イーサネットフレーム転送部３５は、宛先ＭＡＣアドレス書換部３３で宛先ＭＡＣアドレスを書き換えたイーサネットフレームを受け取り、そのイーサネットフレームをミラー用に用意されたポート３７に送信する。すなわち、イーサネットフレーム転送部３５は、宛先ＭＡＣアドレス書換部３３で宛先ＭＡＣアドレスを書き換えられたイーサネットフレームを、スイッチングハブ３のミラートラフィック取り出し用のポート３７に送信することにより、ホスト「MAC_B」からホスト「IP_A」への通信をミラーすることを可能にする。
【００５７】
そして、イーサネットフレーム転送部３５は、これと同時に宛先ＭＡＣアドレス書換部３３で宛先ＭＡＣアドレスを書き換えた該イーサネットフレームを複製し、送信元ＭＡＣアドレス書換部３４にも転送する。
【００５８】
送信元ＭＡＣアドレス書換部３４は、イーサネットフレーム転送部３５から受け取ったイーサネットフレームの送信元ＭＡＣアドレスを、偽装ＭＡＣアドレスに書き換える。イーサネットフレーム転送部３５から受け取ったイーサネットフレームは、宛先ＭＡＣアドレス書換部３３において宛先ＭＡＣアドレスを本来のＭＡＣアドレスに書き換えられた該イーサネットフレームを複製したものである。送信元ＭＡＣアドレス書換部３４は、イーサネットフレーム転送部３５から上記の手順で入力されたイーサネットフレームの送信元ＭＡＣアドレスを、自身の偽装ＭＡＣアドレスに書き換える。

【００５９】
例えば、図１において、宛先ＭＡＣアドレス書換部３３が宛先ＭＡＣアドレスをホスト「IP_A」の本来のＭＡＣアドレスである「MAC_A」に書き換え、さらにイーサネットフレーム転送部３５がミラーポートに送信すると同時に複製したイーサネットフレームを、送信元ＭＡＣアドレス書換部３４が受け取る。この場合、送信元ＭＡＣアドレス書換部３４は、その受け取ったイーサネットフレームの送信元ＭＡＣアドレスを偽装ＭＡＣアドレス「MAC_D」に書き換える。この結果、当該イーサネットフレームの宛先ＭＡＣアドレスは「MAC_A」、送信元ＭＡＣアドレスは偽装ＭＡＣアドレス「MAC_D」となる。
【００６０】
これらの処理の後、送信元ＭＡＣアドレス書換部３４は、そのイーサネットフレームをイーサネットフレーム転送部３５に送る。
【００６１】
イーサネットフレーム転送部３５は、送信元ＭＡＣアドレス書換部３４において送信元ＭＡＣアドレスを偽装ＭＡＣアドレスに書き換えられたイーサネットフレームを受け取り、ポート３６から、中継装置２に送信する。この結果、イーサネットフレームは、中継装置２に戻って再度中継装置２に受信され、中継装置２のスイッチングハブ機能によって中継装置２に接続するホスト１に転送される。
【００６２】
図１の例では、宛先ＭＡＣアドレスが「MAC_A」に書き換えられたイーサネットフレームが、送信元ＭＡＣアドレス書換部３４によって、再度中継装置２へ送信される。そのイーサネットフレームを受信した中継装置２は、宛先ＭＡＣアドレスを参照し、ホスト１Ａに対してイーサネットフレームを転送する。これにより、送信元ＭＡＣアドレスが偽装ＭＡＣアドレス「MAC_D」に書き換えられた「MAC_B」（ホスト１Ｂ）からのイーサネットフレームが、「IP_A」（ホスト１Ａ）に到達する。この時点で、ホスト１Ａからは、偽装ＭＡＣアドレス「MAC_D」から届いたように送信元ＭＡＣアドレスが見える。
【００６３】
以上のようなスイッチングハブ３の一連の動作によって、通信システム１００では、中継装置２を中継点として折り返すホスト１Ａ，１Ｂ間の通信をミラーすることが可能となる。通信システム１００では、ポートミラー機能を有するスイッチングハブを別途用意してホスト間の通信経路の途中に挿入することも不要になる。また、通信システム１００では、中継装置２がポートミラー機能を持たないスイッチングハブ或いは無線ＬＡＮのＡＰである場合にもミラーすることが可能となる。
【００６４】
［ミラー処理の流れ］
次に、本実施の形態に係る通信システムの通信トラフィックのミラー処理の流れについて説明する。図３～図８は、実施の形態に係る通信システムの通信トラフィックのミラー処理の流れを説明する図である。
【００６５】
まず、図３～図８に示す通信システム１００Ａは、無線ＬＡＮのＡＰ２Ａを中継装置２とする。ＡＰ２Ａは、無線ＬＡＮにより接続するホスト１を収容するアクセスポイント機能と、ケーブルでスイッチングハブ３と接続する有線インターフェース（ポート２２）とを有する。
【００６６】
ホスト１Ａ，１Ｂは、ＡＰ２に、無線ＬＡＮを介して接続する。ホスト１Ａとホスト１Ｂは、ＡＰ２Ａを中継点として折り返しの通信を行う。スイッチングハブ３は、ＡＰ２Ａに接続するホストＡＰ２Ａと同じＩＰサブネットに属する有線インターフェース（ポート２２）に接続する。端末４Ａは、スイッチングハブ３のポート３７に接続して、ミラーされた通信トラフィックをキャプチャする。
【００６７】
ＡＰ２Ａは、一般的なスイッチングハブの機能を有し、受信したイーサネットフレーム

ヘッダに含まれる宛先ＭＡＣアドレスにしたがって、宛先アドレスに該当するホスト１が接続されているポートに、受信したイーサネットフレームを転送する。図１の例と同様に、ホスト１ＡにはＩＰアドレス「IP_A」およびＭＡＣアドレス「MAC_A」が割り当てられており、ホスト１ＢにはＩＰアドレス「IP_B」およびＭＡＣアドレス「MAC_B」が割り当てられている。これらのホスト１Ａ，１Ｂがお互いに通信をする場合には、ＡＲＰにより相手のＩＰアドレスからＭＡＣアドレスを解決し、相手のＭＡＣアドレスを宛先ＭＡＣアドレスとするイーサネットフレームを、ＡＰ２Ａに送信する。

【００６８】

そして、スイッチングハブ３は、ＡＰ２Ａの有線インタフェースのポート２２に接続する。ＡＰ２Ａから見ると、スイッチングハブ３は、ホスト１Ａ，１Ｂと同様にＡＰ２Ａに接続するホストの１つである。

【００６９】

図３に示すように、通信システム１００Ａでは、まず、スイッチングハブ３において、ホストスキャン部３１が、ＡＰ２Ａのホストが属しているＩＰサブネットのネットワークアドレスとサブネットマスクとの２つの情報から、ホスト１のＩＰアドレスの値の範囲を計算する（図３の（１）参照）。このネットワークアドレスとサブネットマスクとの情報は、スイッチングハブ３の内部の記憶領域に予め記録しておいてもよいし、ＤＨＣＰプロトコルの応答に含まれるネットワークアドレスとサブネットマスクとを参照して取得してもよい。

【００７０】

次に、ホストスキャン部３１は、計算した範囲にある全てのＩＰアドレスに対応するＭＡＣアドレスを、ＡＲＰを用いてスキャンする（図３の（２）参照）。図３の例では、ホストスキャン部３１は、ホスト１ＡのＩＰアドレス「IP_A」に対応するＭＡＣアドレス「MAC_A」の組を取得する（図３の（３）参照）。そして、ホストスキャン部３１は、ホスト１ＢのＩＰアドレス「IP_B」に対応するＭＡＣアドレス「MAC_B」の組を取得する（図３の（４）参照）。

【００７１】

続いて、ホストスキャン部３１は、それらのホストＩＰアドレスとＭＡＣアドレスとの組をＩＰ－ＭＡＣリスト３０１としてメモリ３０に格納する。ホストスキャン部３１は、以上の処理を、スイッチングハブ３をＡＰ２Ａに接続してミラーを実施する前に１度だけ実施しておけばよい。

【００７２】

次に、図４～図８を参照して、ホスト１Ａを送信元として、ホスト１Ｂを宛先とする通信をミラーするための処理の流れについて説明する。偽装ＡＲＰリプライ送信部３２は、メモリ３０のＩＰ－ＭＡＣリスト３０１を検索して、ホスト１ＢのＩＰアドレス「IP_B」を取得する（図４の（１）参照）。同様に、偽装ＡＲＰリプライ送信部３２は、ＩＰ－ＭＡＣリスト３０１を検索して、ホスト１ＡのＭＡＣアドレス「MAC_A」を取得する（図４の（２）参照）。

【００７３】

そして、偽装ＡＲＰリプライ送信部３２は、ホスト「IP_B」に対応するＭＡＣアドレスを自身の偽装ＭＡＣアドレス「MAC_D」であるとするＡＲＰリプライメッセージと、それを含むイーサネットフレームを作成し、イーサネットフレームのヘッダにある宛先ＭＡＣアドレスを「MAC_A」に設定する。偽装ＡＲＰリプライ送信部３２は、作成したイーサネットフレーム（ＡＲＰリプライ）をポート３６から送信する（図４の（３）参照）。送信されたイーサネットフレームは、ＡＰ２Ａに届いた後、宛先ＭＡＣアドレスである「MAC_A」に従ってＡＰ２Ａによってホスト１Ａが接続する無線ＬＡＮのチャネルから伝送される。

【００７４】

偽装ＡＲＰリプライを受信したホスト１Ａは、ホスト１ＡのＩＰアドレス「IP_B」に対応するＭＡＣアドレスを偽装ＭＡＣアドレスである「MAC_D」として書き換える（図４の

（４），（５）参照）。ＡＲＰキャッシュ書き換え後は、「IP_B」宛のイーサネットフレームの宛先ＭＡＣアドレスは、「MAC_D」となって送信される。

【００７５】

ホスト１Ａから送信されるホスト１Ｂ宛ての無線ＬＡＮの通信（イーサネットフレーム）は、宛先ＭＡＣアドレス「MAC_D」を持つため（図５の（６），（７）参照）、ＡＰ２Ａによって受信された後、ＡＰ２Ａの有線インタフェース（ポート２２）からスイッチングハブ３に向けて転送される（図５の（８）参照）。

【００７６】

スイッチングハブ３は、ホスト１Ｂ宛てのイーサネットフレームをポート３６で受信し、イーサネットフレーム転送部３５は、宛先ＭＡＣアドレス書換部３３に、受信したイーサネットフレームを転送する（図５の（９）参照）。

【００７７】

宛先ＭＡＣアドレス書換部３３は、受け取ったイーサネットフレームに含まれるＩＰパケットの宛先ＩＰアドレス「IP_B」を取得する。そして、宛先ＭＡＣアドレス書換部３３は、ＩＰ－ＭＡＣリスト３０１を検索し（図６の（１０）参照）、「IP_B」に対応するＭＡＣアドレス「MAC_B」を取得する（図６の（１１）参照）。続いて、宛先ＭＡＣアドレス書換部３３は、受け取ったイーサネットフレームのヘッダの宛先ＭＡＣアドレスを「MAC_D」から「MAC_B」に書き換えて（図６の（１２）参照）、イーサネットフレーム転送部３５に送る。

【００７８】

イーサネットフレーム転送部３５は、受け取ったイーサネットフレームをポート３７から、ミラー送信する（図７の（１３）参照）。端末１４は、ミラー送信されたイーサネットフレームを受信し、イーサネットフレームを記録する。この処理によって、通信トラフィックのミラーが可能になる。

【００７９】

これとともに、イーサネットフレーム転送部３５は、ホスト１Ａとホスト１Ｂとの間の通信を成立させるため、宛先ＭＡＣアドレス書換部３３から受け取ったイーサネットフレームを複製（図７の（１３）参照）する。そして、イーサネットフレーム転送部３５は、複製したイーサネットフレームを送信元ＭＡＣアドレス書換部３４に転送する（図７の（１４）参照）。

【００８０】

続いて、送信元ＭＡＣアドレス書換部３４は、複製されたイーサネットフレームを受け取り、その送信元ＭＡＣアドレス「MAC_A」を、偽装ＭＡＣアドレス「MAC_D」に書き換えて（図８の（１５）参照）、再度イーサネットフレーム転送部３５に転送する（図８の（１６）参照）。

【００８１】

イーサネットフレーム転送部３５は、宛先ＭＡＣアドレスが「MAC_B」、送信元ＭＡＣアドレスが「MAC_D」となったイーサネットフレームを、送信元ＭＡＣアドレス書換部３４から受け取り、それをポート３６からパケット送信する（図８の（１７）参照）。ＡＰ２Ａは、イーサネットフレームを受信し、宛先ＭＡＣアドレスである「MAC_B」に従って（図８の（１８）参照）、受信したイーサネットフレームを、ホスト１Ｂが接続する無線ＬＡＮのチャネルから伝送する（図８の（１９）参照）。この結果、ホスト１Ｂに、ホスト１Ａから送信されたパケットが到達する。

【００８２】

なお、イーサネットフレームの送信元ＭＡＣアドレス「MAC_A」を偽装ＭＡＣアドレス「MAC_D」に書き換える理由を説明する。ＡＰ２Ａは、ホスト１Ａおよびホスト１Ｂが送信するＡＲＰパケット或いはイーサネットフレームの送信元ＭＡＣアドレスを参照し、自身のポートとそれに接続するホストのＭＡＣアドレスとを対応付けて一時的に記憶している。このため、書き換えを行わないと、スイッチングハブ３から受信するポートとホスト１Ａから受信するポートとの双方に同じ「MAC_A」が対応付けられてしまう。この状態は

ループと呼ばれ、一般的なスイッチングハブでは通信不能となるため、同じＭＡＣアドレスを複数のポートに対応付けることはできない。

【００８３】

スイッチングハブ３は、送信元ＭＡＣアドレスを「MAC_D」に書き換えることによって、ホスト１Ａ，１Ｂでは、スイッチングハブ３から受信するポートに「MAC_D」が対応付けられる。これによって、通信システム１００Ａホストでは、１Ａ，１Ｂにおいて、同じＭＡＣアドレスが複数のポートに対応付けられることはなくなり、一般的なスイッチングハブの通常の転送動作が可能となる。

【００８４】

［ホストスキャン処理の処理手順］

次に、本実施の形態に係る通信システム１００のホストスキャン処理の処理手順について説明する。図９は、実施の形態に係る通信システムのホストスキャン処理の処理手順を示すシーケンス図である。

【００８５】

通信システム１００では、ホストスキャン部３１が、ＡＰ２Ａのホストが属しているＩＰサブネットのネットワークアドレスとサブネットマスクとの２つの情報から、ホスト１のＩＰアドレスの値の範囲を計算する（ステップＳ１）。

【００８６】

そして、ホストスキャン部３１は、計算した範囲にある全てのＩＰアドレスに対応するＭＡＣアドレスを、ＡＲＰを用いてスキャンする（ステップＳ２～ステップＳ５）。そして、ホストスキャン部３１は、ホスト１のＩＰアドレスに対応するＭＡＣアドレスの組を取得し（ステップＳ６）、ＩＰ－ＭＡＣリスト３０１としてメモリ３０に格納する（ステップＳ７）。

【００８７】

［ミラー処理の処理手順］

次に、本実施の形態に係る通信システム１００のミラー処理の処理手順について説明する。図１０は、実施の形態に係る通信システムのミラー処理の処理手順を示すシーケンス図である。図１０の例では、ホスト１Ａからホスト１Ｂ宛に送信される通信トラフィックをミラーする場合について説明する。

【００８８】

まず、偽装ＡＲＰリプライ送信部３２は、メモリ３０のＩＰ－ＭＡＣリスト３０１を検索して（ステップＳ１１）、ホスト１ＢのＩＰアドレス「IP_B」を取得するとともに、ホスト１ＡのＭＡＣアドレス「MAC_A」を取得する（ステップＳ１２）。

【００８９】

そして、偽装ＡＲＰリプライ送信部３２は、ホスト「IP_B」に対応するＭＡＣアドレスを自身の偽装ＭＡＣアドレス「MAC_D」であるとするＡＲＰリプライメッセージと、それを含むイーサネットフレームを作成し、イーサネットフレームのヘッダにある宛先ＭＡＣアドレスを「MAC_A」に設定する。偽装ＡＲＰリプライ送信部３２は、作成したイーサネットフレームを、ＡＰ２Ａを介して、ホスト１Ａに、ＡＲＰリプライとして送信する（ステップＳ１３，Ｓ１４）。

【００９０】

ＡＲＰリプライを受信したホスト１Ａは、ホスト１ＡのＩＰアドレス「IP_B」に対応するＭＡＣアドレスを偽装ＭＡＣアドレスである「MAC_D」として書き換える（ステップＳ１５）。ＡＲＰキャッシュ書き換え後は、「IP_B」宛のイーサネットフレームの宛先ＭＡＣアドレスは、「MAC_D」となって送信される。

【００９１】

ホスト１Ａは、ホスト１Ｂ宛ての無線ＬＡＮの通信（イーサネットフレーム）を送信する（ステップＳ１６）。このイーサネットフレームは、宛先ＭＡＣアドレス「MAC_D」を持つため、ＡＰ２Ａによって受信された後、スイッチングハブ３に向けて転送される（ステップＳ１７）。

【００９２】
スイッチングハブ３では、イーサネットフレーム転送部３５は、受信したホスト１Ｂ宛てのイーサネットフレームを、宛先ＭＡＣアドレス書換部３３に転送する（ステップＳ１８）。
【００９３】
宛先ＭＡＣアドレス書換部３３は、受け取ったイーサネットフレームに含まれるＩＰパケットの宛先ＩＰアドレス「IP_B」を取得後、ＩＰ－ＭＡＣリスト３０１を検索し（ステップＳ１９）、宛先ＩＰアドレス「IP_B」に対応するＭＡＣアドレス「MAC_B」を取得する（ステップＳ２０）。続いて、宛先ＭＡＣアドレス書換部３３は、受け取ったイーサネットフレームのヘッダの宛先ＭＡＣアドレスを「MAC_B」に書き換えて（ステップＳ２１）、イーサネットフレーム転送部３５に送る（ステップＳ２２）。
【００９４】
イーサネットフレーム転送部３５は、受け取ったイーサネットフレームを、ポート３７を介して、通信装置４に、ミラー送信する（ステップＳ２３）。これとともに、イーサネットフレーム転送部３５は、宛先ＭＡＣアドレス書換部３３から受け取ったイーサネットフレームを複製する（ステップＳ２４）。そして、イーサネットフレーム転送部３５は、複製したイーサネットフレームを送信元ＭＡＣアドレス書換部３４に転送する（ステップＳ２５）。
【００９５】
続いて、送信元ＭＡＣアドレス書換部３４は、複製されたイーサネットフレームの送信元ＭＡＣアドレス「MAC_A」を、偽装ＭＡＣアドレス「MAC_D」に書き換えて（ステップＳ２６）、イーサネットフレーム転送部３５に転送する（ステップＳ２７）。
【００９６】
イーサネットフレーム転送部３５は、宛先ＭＡＣアドレスが「MAC_B」、送信元ＭＡＣアドレスが「MAC_D」となったイーサネットフレームを、ポート３６から送信する（ステップＳ２８）。ＡＰ２Ａは、イーサネットフレームを受信し、宛先ＭＡＣアドレスである「MAC_B」に従って、受信したイーサネットフレームを、ホスト１Ｂに転送する（ステップＳ２９）。
【００９７】
［実施の形態の効果］
このように、本実施の形態に係るスイッチングハブ３は、ＩＰ－ＭＡＣリスト３０１を保持する。そして、スイッチングハブ３は、ホスト１の通信先のＩＰアドレスに対応するＭＡＣアドレスを、スイッチングハブ３のＭＡＣアドレスである偽装ＭＡＣアドレスに書き換える偽装ＡＲＰリプライ送信部３２を有する。そして、スイッチングハブ３は、中継装置２から送信された、偽装ＭＡＣアドレスを宛先ＭＡＣアドレスとしたイーサネットフレームに対し、ＩＰ－ＭＡＣリストを検索して、宛先ＭＡＣアドレスを、該イーサネットフレームのＩＰアドレスに対応する本来のＭＡＣアドレスに書き換える宛先ＭＡＣアドレス書換部３３を有する。
【００９８】
そして、スイッチングハブ３は、宛先ＭＡＣアドレス書換部３３において宛先ＭＡＣアドレスを本来のＭＡＣアドレスに書き換えられたイーサネットフレームの送信元ＭＡＣアドレスを、偽装ＭＡＣアドレスに書き換える送信元ＭＡＣアドレス書換部３４を有する。そして、スイッチングハブ３は、宛先ＭＡＣアドレス書換部３３において宛先ＭＡＣアドレスを本来のＭＡＣアドレスに書き換えられたイーサネットフレームを、ミラートラフィック受信用装置に送信するとともに、送信元ＭＡＣアドレス書換部３４において送信元ＭＡＣアドレスを偽装ＭＡＣアドレスに書き換えられたイーサネットフレームを、中継装置２に送信するイーサネットフレーム転送部３５を有する。
【００９９】
本実施の形態では、上記の機能を有するスイッチングハブ３を、中継装置２に接続することによって、中継装置２を継点として折り返すホスト１Ａ，１Ｂ間の通信経路を操作す

る。この結果、本実施の形態によれば、ポートミラー機能を持たないスイッチングハブ或いは無線ＬＡＮのアクセスポイントである中継装置２を介するホスト１Ａ、１Ｂ間の通信トラフィックをミラー可能にする。また、本実施の形態では、ホスト１Ａ，１Ｂ間の通信経路間に他の装置を挿入することも必要ない。

【０１００】

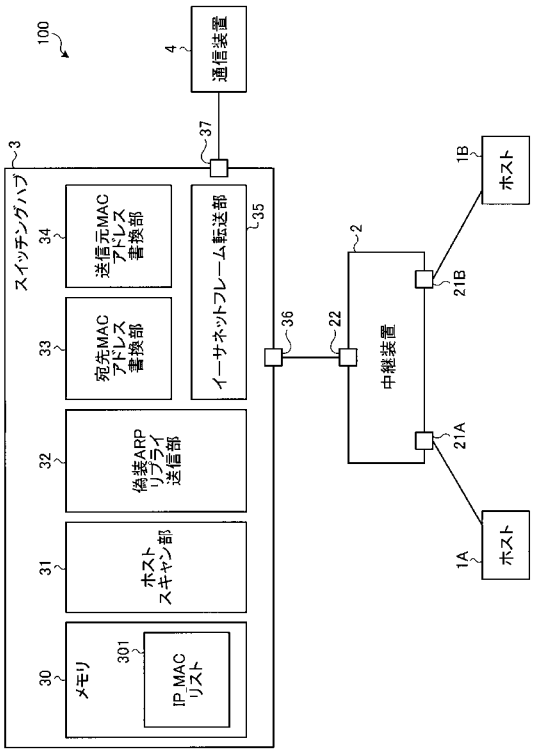
なお、本発明者によってなされた発明を適用した実施の形態について説明したが、本実施の形態による本発明の開示の一部をなす記述及び図面により本発明は限定されることはない。すなわち、本実施の形態に基づいて当業者等によりなされる他の実施の形態、実施例及び運用技術等は全て本発明の範疇に含まれる。

【符号の説明】

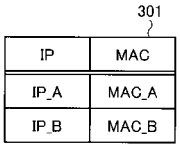
【０１０１】

１００，１００Ａ　通信システム
１Ａ、１Ｂ　ホスト
２　中継装置
２Ａ　ＡＰ
３　スイッチングハブ
２１Ａ，２１Ｂ，２２，３６，３７　ポート
３０　メモリ
３１　ホストスキャン部
３２　偽装ＡＲＰリプライ送信部
３３　宛先ＭＡＣアドレス書換部
３４　送信元ＭＡＣアドレス書換部
３５　イーサネットフレーム転送部

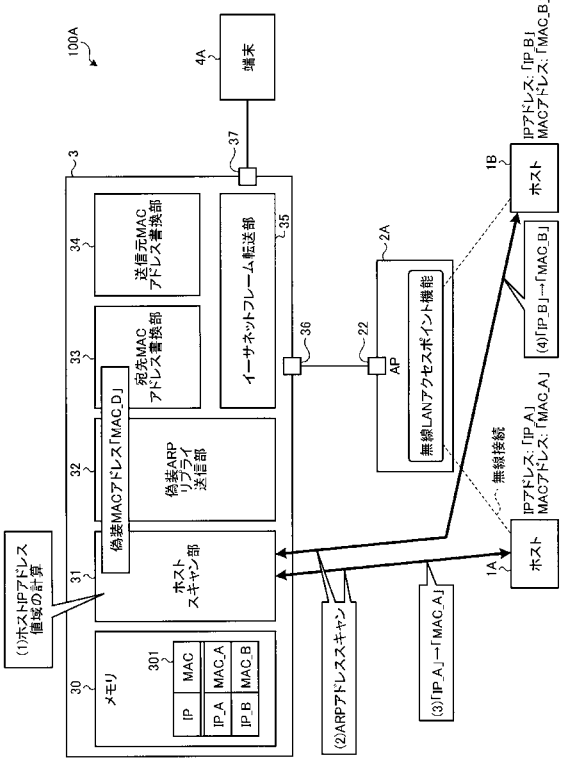
【図１】



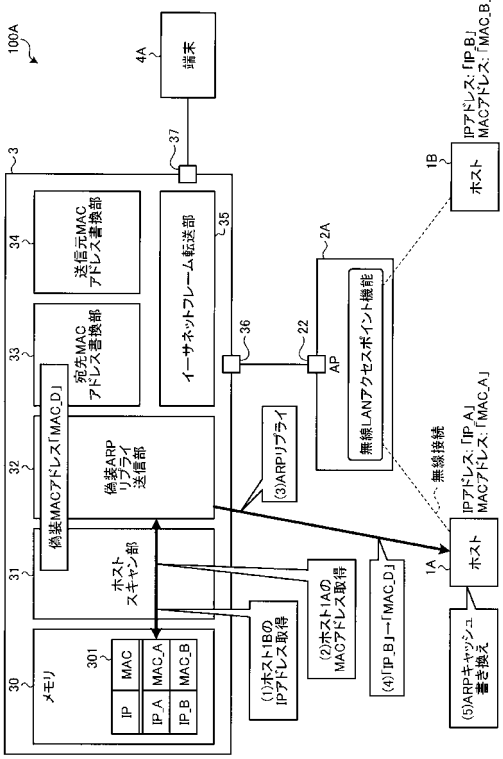
【図２】



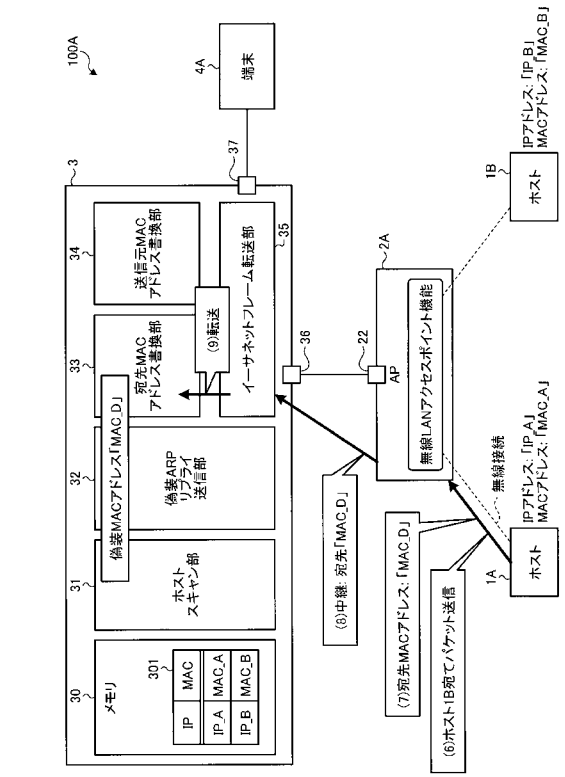
【図３】


100A
端末
4A
37
3
送信元MAC
アドレス書換部
34
宛先MAC
アドレス書換部
33
イーサネットフレーム転送部
35
偽装ARP
リプライ
送信部
32
偽装MACアドレス「MAC_D」
ホスト
スキャン部
31
36
22
AP
無線LANアクセスポイント機能
2A
メモリ
30
301
IP
MAC
IP_A
MAC_A
IP_B
MAC_B
ホスト
1B
IPアドレス:「IP_B」
MACアドレス:「MAC_B」
ホスト
1A
IPアドレス:「IP_A」
MACアドレス:「MAC_A」
無線接続
(1)ホストIPアドレス
僅域の計算
(2)ARPアドレススキャン
(3)「IP_A」→「MAC_A」
(4)「IP_B」→「MAC_B」

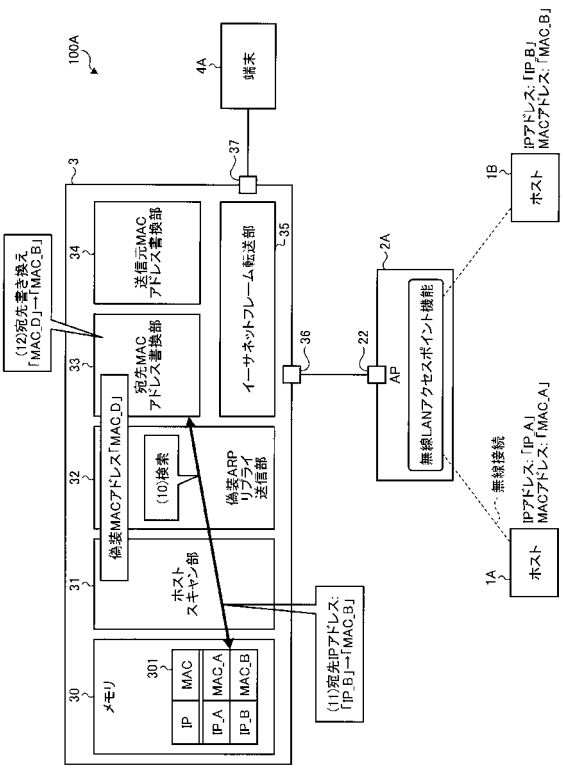
【図４】


100A
端末
4A
37
3
送信元MAC
アドレス書換部
34
宛先MAC
アドレス書換部
33
イーサネットフレーム転送部
35
偽装ARP
リプライ
送信部
32
偽装MACアドレス「MAC_D」
ホスト
スキャン部
31
36
22
AP
無線LANアクセスポイント機能
2A
メモリ
30
301
IP
MAC
IP_A
MAC_A
IP_B
MAC_B
ホスト
1B
IPアドレス:「IP_B」
MACアドレス:「MAC_B」
ホスト
1A
IPアドレス:「IP_A」
MACアドレス:「MAC_A」
無線接続
(1)ホスト1Bの
IPアドレス取得
(2)ホスト1Aの
MACアドレス取得
(3)ARPリプライ
(4)「IP_B」→「MAC_D」
(5)ARPキャッシュ
書き換え

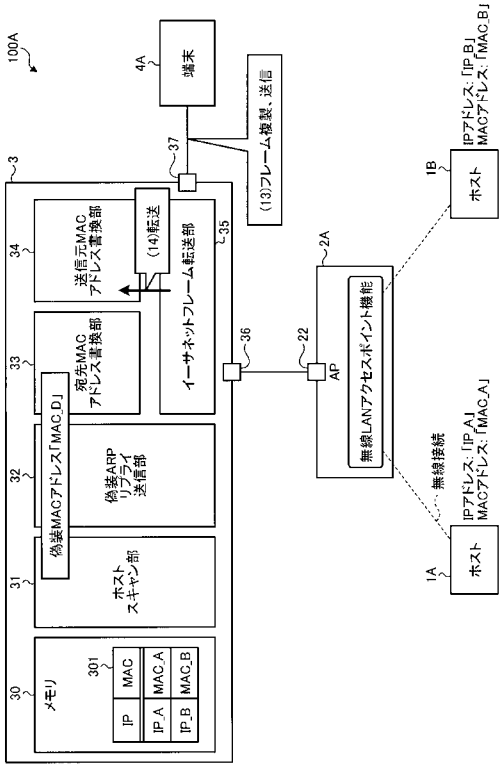
【図５】


100A
端末
4A
37
3
送信元MAC
アドレス書換部
34
宛先MAC
アドレス書換部
33
(9)転送
イーサネットフレーム転送部
35
偽装ARP
リプライ
送信部
32
偽装MACアドレス「MAC_D」
ホスト
スキャン部
31
36
22
AP
無線LANアクセスポイント機能
2A
メモリ
30
301
IP
MAC
IP_A
MAC_A
IP_B
MAC_B
ホスト
1B
IPアドレス:「IP_B」
MACアドレス:「MAC_B」
ホスト
1A
IPアドレス:「IP_A」
MACアドレス:「MAC_A」
無線接続
(6)ホスト1B宛てパケット送信
(7)宛先MACアドレス:「MAC_D」
(8)中継:宛先「MAC_D」

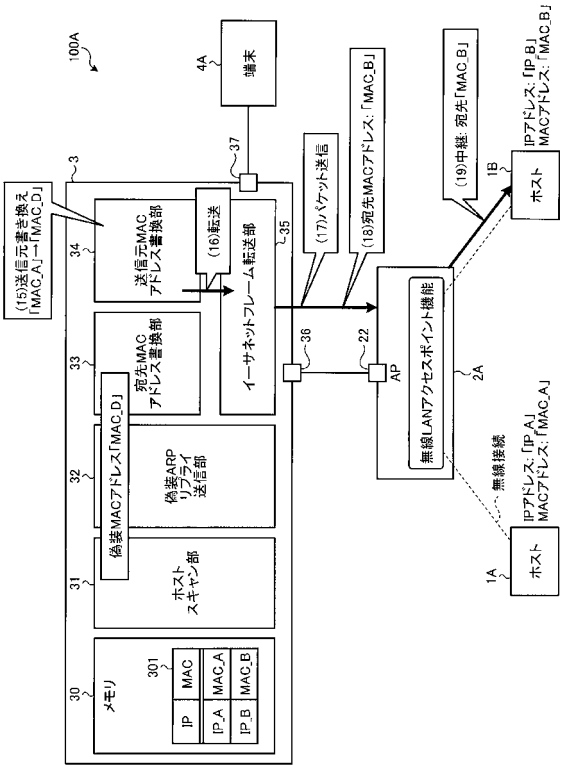
【図６】


100A
端末
4A
37
3
(12)宛先書き換え
「MAC_D」→「MAC_B」
送信元MAC
アドレス書換部
34
宛先MAC
アドレス書換部
33
イーサネットフレーム転送部
35
(10)検索
偽装ARP
リプライ
送信部
32
偽装MACアドレス「MAC_D」
ホスト
スキャン部
31
36
22
AP
無線LANアクセスポイント機能
2A
メモリ
30
301
IP
MAC
IP_A
MAC_A
IP_B
MAC_B
ホスト
1B
IPアドレス:「IP_B」
MACアドレス:「MAC_B」
ホスト
1A
IPアドレス:「IP_A」
MACアドレス:「MAC_A」
無線接続
(11)宛先IPアドレス:
「IP_B」→「MAC_B」

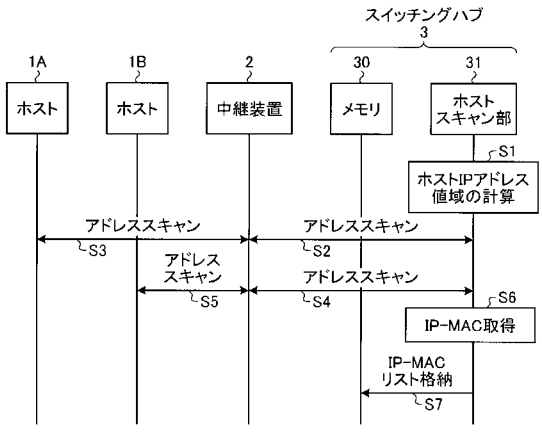
【図７】


100A
4A
端末
(13)フレーム複製、送信
IPアドレス:「IP_B」
MACアドレス:「MAC_B」
1B
ホスト
37
3
送信元MAC
アドレス書換部
34
(14)転送
35
イーサネットフレーム転送部
宛先MAC
アドレス書換部
33
偽装MACアドレス「MAC_D」
偽装ARP
リプライ
送信部
32
ホスト
スキャン部
31
メモリ
30
301
IP
MAC
IP_A
MAC_A
IP_B
MAC_B
36
22
2A
AP
無線LANアクセスポイント機能
無線接続
IPアドレス:「IP_A」
MACアドレス:「MAC_A」
1A
ホスト

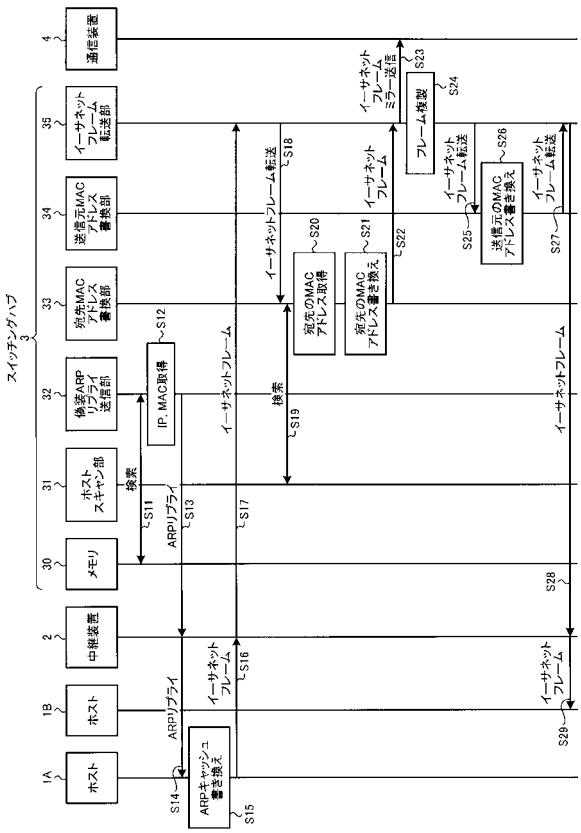
【図８】


100A
4A
端末
(15)送信元書き換え
「MAC_A」→「MAC_D」
(16)転送
(17)パケット送信
(18)宛先MACアドレス:「MAC_B」
(19)中継:宛先「MAC_B」
IPアドレス:「IP_B」
MACアドレス:「MAC_B」
1B
ホスト
37
3
送信元MAC
アドレス書換部
34
35
イーサネットフレーム転送部
宛先MAC
アドレス書換部
33
偽装MACアドレス「MAC_D」
偽装ARP
リプライ
送信部
32
ホスト
スキャン部
31
メモリ
30
301
IP
MAC
IP_A
MAC_A
IP_B
MAC_B
36
22
2A
AP
無線LANアクセスポイント機能
無線接続
IPアドレス:「IP_A」
MACアドレス:「MAC_A」
1A
ホスト

【図９】


スイッチングハブ
3
1A
ホスト
1B
ホスト
2
中継装置
30
メモリ
31
ホスト
スキャン部
S1
ホストIPアドレス
値域の計算
アドレススキャン
S3
アドレススキャン
S2
アドレス
スキャン
S5
アドレススキャン
S4
S6
IP-MAC取得
IP-MAC
リスト格納
S7

【図１０】


スイッチングハブ
3
4
通信装置
35
イーサネット
フレーム
転送部
34
送信元MAC
アドレス
書換部
33
宛先MAC
アドレス
書換部
32
偽装ARP
リプライ
送信部
31
ホスト
スキャン部
30
メモリ
2
中継装置
1B
ホスト
1A
ホスト
検索
IP, MAC取得
ARPリプライ
ARPキャッシュ
書き換え
イーサネットフレーム
イーサネットフレーム転送
イーサネットフレーム
ミラー送信
フレーム複製
イーサネット
フレーム転送
宛先のMAC
アドレス取得
宛先のMAC
アドレス書き換え
送信元のMAC
アドレス書き換え
S11
S12
S13
S14
S15
S16
S17
S18
S19
S20
S21
S22
S23
S24
S25
S26
S27
S28
S29