(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4732257号
(P4732257)
(45)発行日　平成23年7月27日(2011.7.27)　(24)登録日　平成23年4月28日(2011.4.28)

(51)Int.Cl.　　F I
H04L 12/44 (2006.01)　　H04L 12/44　Z
H04L 12/46 (2006.01)　　H04L 12/46　Z

請求項の数 10　(全 35 頁)

(21)出願番号　特願2006-187903(P2006-187903)
(22)出願日　平成18年7月7日(2006.7.7)
(65)公開番号　特開2008-17278(P2008-17278A)
(43)公開日　平成20年1月24日(2008.1.24)
審査請求日　平成21年4月9日(2009.4.9)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100094514
弁理士　林　恒徳
(74)代理人　100094525
弁理士　土井　健二
(72)発明者　的場　一峰
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　田畑　利幸

最終頁に続く

(54)【発明の名称】中継装置、経路制御方法、及び経路制御プログラム

(57)【特許請求の範囲】
【請求項１】
同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続された中継装置において、
前記端末ごとに、前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを保持するアドレス対応保持部と、
前記端末から前記仮想ＭＡＣアドレスの取得を求める第１のＡＲＰリクエストフレームを受信したときに、対応する前記端末の前記仮想ＭＡＣアドレスを前記アドレス対応保持部から読み出して、前記仮想ＭＡＣアドレスを前記端末に応答する代理応答部と、
前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣアドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答するＭＡＣアドレス変換部と、
を備えることを特徴とする中継装置。
【請求項２】
更に、前記レイヤ２スイッチを介して接続された前記端末の全てに対して、第２のＡＲＰリクエストフレームを定期的に送信し、前記第２のＡＲＰリクエストフレームに対する応答フレームにより、前記端末のＩＰアドレスとＭＡＣアドレスの対応を収集するアドレス収集部と、
収集された前記ＩＰアドレスと前記ＭＡＣアドレスに対して、前記仮想ＭＡＣアドレス

を割り当てる仮想ＭＡＣアドレス生成部とを備え、
前記仮想ＭＡＣアドレス生成部は、割り当てた前記仮想ＭＡＣアドレスと、前記ＩＰアドレス、及び前記ＭＡＣアドレスを前記アドレス対応保持部に登録することを特徴とする請求項１記載の中継装置。
【請求項３】
更に、前記端末から送信された第３のフレームを受信し、前記第３のフレームから前記端末のＩＰアドレスとＭＡＣアドレスの対応を収集するアドレス収集部と、
収集された前記ＩＰアドレスと前記ＭＡＣアドレスに対して、前記仮想ＭＡＣアドレスを割り当てる仮想ＭＡＣアドレス生成部とを備え、
前記仮想ＭＡＣアドレス生成部は、割り当てた前記仮想ＭＡＣアドレスと、前記ＩＰアドレス、及び前記ＭＡＣアドレスを前記アドレス対応保持部に登録することを特徴とする請求項１記載の中継装置。
【請求項４】
更に、接続先の物理ポート情報を保持する端末接続ポート保持部を備え、
前記代理応答部は、前記第１のＡＲＰリクエストフレームを受信したとき、前記物理ポート情報に基づいて同一物理ポート配下の通信と判断したときは前記仮想ＭＡＣアドレスを応答し、別物理ポート配下の通信と判断したときは前記実ＭＡＣアドレスを応答することを特徴とする請求項１記載の中継装置。
【請求項５】
更に、前記中継装置のアドレスとは異なる送信元アドレスで第３のＡＲＰリクエストフレームを送信する非対応端末検出部を備え、
前記非対応端末検出部は、前記第３のＡＲＰリクエストフレームに対する応答フレームに基づいて、前記第３のＡＲＰリクエストフレームを送信した前記端末が、前記中継装置を送信元アドレスとした前記第１のＡＲＰリクエストフレームのみ応答する対応端末か否か、を特定することを特徴とする請求項１記載の中継装置。
【請求項６】
更に、前記端末から送信された、送信元と宛て先のＩＰアドレスが同一の第４のＡＲＰリクエストフレームを受信したとき、前記ＩＰアドレスの重複を判断する応答判断部を備え、
前記応答代理部は、前記応答判断部の判断結果に応じて前記第４のＡＲＰリクエストフレームに対して応答する又は応答しないことを特徴とする請求項１記載の中継装置。
【請求項７】
更に、前記端末間で送受信される前記第１のフレームのログを採取するログ採取部を備えることを特徴とする請求項１記載の中継装置。
【請求項８】
中継装置の同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続されたネットワークシステムにおいて、
前記中継装置には、
前記端末ごとに、前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを保持するアドレス対応保持部と、
前記端末から前記仮想ＭＡＣアドレスの取得を求める第１のＡＲＰリクエストフレームを受信したときに、対応する前記端末の前記仮想ＭＡＣアドレスを前記アドレス対応保持部から読み出して、前記仮想ＭＡＣアドレスを前記端末に応答する代理応答部と、
前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣアドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答するＭＡＣアドレス変換部とを備え、
前記端末には、前記中継装置からの応答フレームに対してのみ応答する応答制御部を備える、

ことを特徴とするネットワークシステム。
【請求項９】
同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続された中継装置に対する経路制御方法おいて、
前記端末から第１のＡＲＰリプライフレームを受信し、
前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを前記端末ごとに保持するアドレス対応保持部から、受信した前記第１のＡＲＰリプライフレームに基づいて、対応する前記端末の前記仮想ＭＡＣアドレスを読み出して、前記仮想ＭＡＣアドレスを前記端末に応答し、
前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣアドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答する、
ことを特徴とする経路制御方法。
【請求項１０】
同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続された中継装置に対する経路制御プログラムおいて、
前記端末から第１のＡＲＰリプライフレームを受信する処理と、
前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを前記端末ごとに保持するアドレス対応保持部から、対応する前記端末の前記仮想ＭＡＣアドレスを読み出して、前記仮想ＭＡＣアドレスを前記端末に応答する処理と、
前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣアドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答する処理と、
をコンピュータに実行させることを特徴とする経路制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＬＡＮの経路制御を行う中継装置、経路制御方法、及び経路制御プログラムに関する。詳しくは、ログ採取を含めて、セキュリティの向上を実現した中継装置等に関する。
【背景技術】
【０００２】
近年、ネットワーク内において、ウィルスやワーム等による企業内の情報資源の損害が問題となっている。その対策の一つとしてセキュリティ機能を有するスイッチやルータを導入するケースが増加している。
【０００３】
このようなセキュリティスイッチには、自身を通過するトラフィックを常時監視し、Ｄｏｓ（Denial of Service attack）攻撃や、ワームの感染活動等、異常なトラフィックパターンを検知すると、そのトラフィックのフレームを廃棄して、被害の拡大を防ぐ機能を有している。
【０００４】
通常のフロアＬＡＮは、低機能のスイッチングハブやリピータハブにより、複数の端末が接続された形態が殆どである。このようなフロアＬＡＮに、セキュリティスイッチを接続するには、ネットワーク機器構成に影響を与えないようにするため、フロアＬＡＮとバックボーンＬＡＮの境界点に設置するのが通常である。
【０００５】
図２４（Ａ）は、フロアＬＡＮにセキュリティスイッチを設けた場合の従来の構成例を

示す図である。

【０００６】

セキュリティスイッチ２００は、バックボーンＬＡＮとフロアＬＡＮの間に設けられ、その配下に、レイヤ２スイッチ（Ｌ２ＳＷ）２１０、２２０が配置される。各レイヤ２スイッチ２１０、２２０には、クライアント端末Ａ２３０及びクライアント端末Ｂ２４０が夫々接続される。この場合、端末Ａ２３０及び端末Ｂ２４０は、同一フロア内に配置される。

【０００７】

このように構成されたネットワーク構成で、端末Ａ２３０と端末Ｂ２４０との間で通信を行う場合に、まず、ＡＲＰ（Address Resolution Protocol）と呼ばれるアドレス解決プロトコルを用いてアドレスの取得動作を行う。

【０００８】

図２４（Ａ）に示すように、（１）端末Ａ２３０は、端末Ｂ２４０のＩＰアドレスを含むＡＲＰリクエストフレームをブロードキャストで送信し、（２）端末Ｂ２４０は、このＡＲＰリクエストフレームに対して、自身のＭＡＣ（Media Access Control address）アドレスを含むＡＲＰリプライフレームを端末Ａに対して送信する。

【０００９】

この動作により、端末Ａ２３０は端末Ｂ２４０のＭＡＣアドレスを取得する。その後、端末Ａ２３０は、通信用のフレームを、端末Ｂ２４０のＭＡＣアドレス宛てに送信することができる（図２４（Ｂ）参照）。このとき、レイヤ２スイッチ２１０、２２０は、このＭＡＣアドレスを検索キーにして、自身で保持する学習テーブルを検索して、宛て先物理ポート（端末Ｂ２４０の接続された物理ポート）に対してフレームを送信する。そして、端末Ｂ２４０は、受信フレームが自身のＭＡＣアドレスのためフレームの受信処理を行う。

【００１０】

また、このような従来技術としては、例えば、宅側ポートに対応するダミーＭＡＣアドレスを記憶したテーブルを備え、宅側ポートから受信したフレームの宛て先ＭＡＣアドレスがダミーＭＡＣアドレスであれば、そのフレームの宛て先ＭＡＣアドレスを、そのダミーＭＡＣアドレスに対応する他の宅側ポートに接続されたノードのＭＡＣアドレスに置き換えて、フレームの中継を行うようにしたスイッチングハブが開示されている（例えば、以下の特許文献１）。

【特許文献１】特開２００３－３１８９３４号公報

【発明の開示】

【発明が解決しようとする課題】

【００１１】

しかしながら、図２４（Ａ）及び同図（Ｂ）に示すように、同一フロア内の端末間通信では、レイヤ２スイッチ２１０、２２０のみでフレームの転送が行われる。従って、セキュリティスイッチ２００にフレームが転送されないため、セキュリティスイッチ２００によるセキュリティの監視を行うことができない。

【００１２】

このような場合、例えば、ワームに感染した端末を接続すると、ワームの感染フレームがフロア内に拡散し、同一フロア内の全端末がワーム感染の被害を受ける事態が発生する。

【００１３】

また、特許文献１では、異なる物理ポートに接続されたノード間では、その転送されるフレームがスイッチングハブ１０１を経由するため問題は発生しないが、同一ポートの複数のノード１１３、１１４間のみで通信が行われる場合、フレームがスイッチングハブ１０１を経由しないことになり、同様にセキュリティの監視を行うことができない問題が発生する。

【００１４】

一方、図２４（Ａ）でレイヤ２スイッチ２１０、２２０にセキュリティ機能を持たせるようにすれば、上述の問題を回避することも考えられる。しかし、レイヤ２スイッチ２１０、２２０にそのような機能を持たせると、却ってコストアップや工数の増大を招く。従って、できるだけ、既存のネットワーク構成を変えずにセキュリティの向上を図ることが望まれる。

【００１５】

上述した例は、いずれもセキュリティについて述べたが、全く同様の理由により、端末２３０、２４０間のみで通信が行われる場合、セキュリティスイッチ２００は通信のログを採取することができない。

【００１６】

そこで、本発明は、上記問題点に鑑みてなされたもので、その目的は、既存のネットワーク構成を変えることなく、フロアＬＡＮ内の端末に対して、ログの採取を含めて、セキュリティの向上を実現した中継装置や、経路制御方法、及び経路制御プログラムを提供することにある。

【課題を解決するための手段】

【００１７】

上記目的を達成するために、本発明の一実施態様によれば、同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続された中継装置において、前記端末ごとに、前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを保持するアドレス対応保持部と、前記端末から前記仮想ＭＡＣアドレスの取得を求める第１のＡＲＰリクエストフレームを受信したときに、対応する前記端末の前記仮想ＭＡＣアドレスを前記アドレス対応保持部から読み出して、前記仮想ＭＡＣアドレスを前記端末に応答する代理応答部と、前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣアドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答するＭＡＣアドレス変換部とを備えることを特徴とする。

【００１８】

また、上記目的を達成するために、本発明の他の実施態様によれば、中継装置の同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続されたネットワークシステムにおいて、前記中継装置には、前記端末ごとに、前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを保持するアドレス対応保持部と、前記端末から前記仮想ＭＡＣアドレスの取得を求める第１のＡＲＰリクエストフレームを受信したときに、対応する前記端末の前記仮想ＭＡＣアドレスを前記アドレス対応保持部から読み出して、前記仮想ＭＡＣアドレスを前記端末に応答する代理応答部と、前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣアドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答するＭＡＣアドレス変換部とを備え、前記端末には、前記中継装置からの応答フレームに対してのみ応答する応答制御部を備える、ことを特徴とする。

【００１９】

更に、上記目的を達成するために、本発明の他の実施態様によれば、同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続された中継装置に対する経路制御方法おいて、前記端末から第１のＡＲＰリプライフレームを受信し、前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを前記端末ごとに保持するアドレス対応保持部から、受信した前記第１のＡＲＰリプライフレームに基づいて、対応する前記端末の前記仮想ＭＡＣアドレスを読み出して、前記仮想ＭＡＣアドレスを前記端末に応答し、前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前

記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣアドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答することを特徴とする。

【００２０】

更に、上記目的を達成するために、本発明の他の実施態様によれば、同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続された中継装置に対する経路制御プログラムおいて、前記端末から第１のＡＲＰリプライフレームを受信する処理と、前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを前記端末ごとに保持するアドレス対応保持部から、対応する前記端末の前記仮想ＭＡＣアドレスを読み出して、前記仮想ＭＡＣアドレスを前記端末に応答する処理と、前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣアドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答する処理とをコンピュータに実行させることを特徴とする。

【発明の効果】

【００２１】

本発明によれは、既存のネットワーク構成を変えることなく、フロアＬＡＮ内の端末に対して、ログ採取を含めて、セキュリティの向上を実現した中継装置や、経路制御方法、及び経路制御プログラムを提供することができる。

【発明を実施するための最良の形態】

【００２２】

以下、図面を参照して本発明を実施するための最良の形態を説明する。

【実施例１】

【００２３】

まず、実施例１について説明する。図１は、本実施例１におけるネットワーク構成例を示す図である。

【００２４】

セキュリティスイッチ１０は、フロアＬＡＮ１００とバックボーンＬＡＮとの間に配置され、その配下にレイヤ２スイッチＣ（Ｌ２ＳＷ＿Ｃ）３０が設けられている。また、レイヤ２スイッチＣ３０には、レイヤ２スイッチＤ（Ｌ２ＳＷ＿Ｄ）４０が接続される。各レイヤ２スイッチＣ３０、Ｄ４０には、それぞれクライアント端末Ａ５０、Ｂ６０が接続される。

【００２５】

各装置に対するＩＰアドレスとＭＡＣアドレスは、図１に示すように割り当てられているものとする。

【００２６】

図２は、セキュリティスイッチ１０とクライアント端末Ｂ６０の構成例を示す図である。セキュリティスイッチ１０は、フレーム送受信部１１と、セキュリティチェック部１２と、ＭＡＣアドレス変換部１３と、アドレス対応保持部１４と、アドレス収集部１５と、仮想ＭＡＣアドレス生成部１６、及びＡＲＰ代理応答部１７を備える。

【００２７】

フレーム送受信部１１は、レイヤ２スイッチＣ３０から種々のフレームを受信する。フレームがＡＲＰリプライフレームのときは、当該フレームをアドレス収集部１５に出力する。フレームがＡＲＰリクエストフレームのときは当該フレームをＡＲＰ代理応答部１７に出力する。それ以外のフレームは、セキュリティチェック部１２や、必要に応じバックボーンＬＡＮ１１０に出力する。

【００２８】

このようなフレームの種別の識別は、以下のようにして行う。即ち、通常、図１に示すネットワーク内にはＭＡＣフレームと呼ばれるフレームが送受信される。図３は、このよ

うなＭＡＣフレームの構成例を示す図である。ＭＡＣフレームには、ペイロードフィールドに「ＡＲＰ」プロトコルのパケットデータが含まれているか否かを示すフィールド３０１がある。このフィールドを確認することで、フレームがＡＲＰフレームかそれ以外のフレームかを判別できる。

【００２９】

また、ペイロードフィールドに格納されたＡＲＰパケットデータ中に、「リプライ」か「リクエスト」か、を示す動作コードフィールド３０２があり、このフィールドを確認することで、フレームがＡＲＰリプライフレームかＡＲＰリクエストフレームかを判別できる。

【００３０】

また、フレーム送受信部１１は、ＭＡＣアドレス変換部１３からの送信フレームと、アドレス収集部１５からのＡＲＰリクエストフレーム、及びＡＲＰ代理応答部１７からのＡＲＰリプライフレームを、夫々レイヤ２スイッチＣ３０に出力する。

【００３１】

セキュリティチェック部１２は、受信フレーム、つまりＡＲＰフレーム以外のすべてのフレームに対してセキュリティチェックを行う。

【００３２】

セキュリティチェックは、例えば、フレーム中のＭＡＣアドレスの送信元アドレスに“ＦＦ・・・”など、本来使用されない値が含まれるか否か、時間あたりの受信フレーム数をカウントし、それが閾値を超えるか否か（所謂、Ｄｏｓ攻撃が行われているか否か）等により、チェックを行う。セキュリティチェック部１２は、正常ではない受信フレームに対して、例えば廃棄する等の処理を行う。正常な受信フレームは、後段のＭＡＣアドレス変換部１３に出力する。

【００３３】

ＭＡＣアドレス変換部１３は、受信フレームから送信元ＭＡＣアドレスと宛て先ＭＡＣアドレスとを抽出し、アドレス対応保持部１４を検索して、受信フレーム中の仮想ＭＡＣアドレスを実ＭＡＣアドレスに、実ＭＡＣアドレスを仮想ＭＡＣアドレスに変換する。変換後のフレームを送信フレームとしてフレーム送受信部１１に出力する。仮想ＭＡＣアドレスを含め詳細は後述する。

【００３４】

アドレス対応保持部１４は、ＩＰアドレス、実ＭＡＣアドレス、仮想ＭＡＣアドレスを１エントリとするテーブルを保持する。

【００３５】

アドレス収集部１５は、例えば、タイマ割り込み等を契機にフロアＬＡＮ１００の所属するサブネット（10.0.0.0/24：即ち、フロアＬＡＮ１００内の全装置）内の各アドレスに、定期的にＡＲＰリクエストフレームを生成し、フレーム送受信部１１に出力する。また、アドレス収集部１５は、フレーム送受信部１１からのＡＲＰリプライフレームに対して、ＩＰアドレスと実ＭＡＣアドレスと抽出し、それらを仮想ＭＡＣアドレス生成部１６に出力する。

【００３６】

フレーム送受信部１１からのＡＲＰリプライフレームは、ＡＲＰリクエストフレームに対する応答フレームであり、各端末Ａ５０、Ｂ６０から送信される。

【００３７】

仮想ＭＡＣアドレス生成部１６は、アドレス収集部１５からのＩＰアドレスと実ＭＡＣアドレスとをキーにして、アドレス対応保持部１４を検索する。

【００３８】

この２つのアドレスの組がアドレス対応保持部１４に登録されていない場合、仮想ＭＡＣアドレス生成部１６は、収集したアドレスに対して仮想的なＭＡＣアドレス（仮想ＭＡＣアドレス）を生成し、この仮想ＭＡＣアドレスを含め、３つのアドレスの組を１エントリとしてアドレス対応保持部１４に格納する。

【００３９】
ＡＲＰ代理応答部１７は、フレーム送受信部１１からＡＲＰリクエストフレームを受け取ると、宛て先ＩＰアドレスをキーにして、アドレス対応保持部１４を検索する。
【００４０】
該当するＩＰアドレスがあれば、エントリ内の仮想ＭＡＣアドレスを読み出して、送信元ＭＡＣアドレスを仮想ＭＡＣアドレスにしたＡＲＰリプライフレームを生成し、フレーム送受信部１１に出力する。
【００４１】
フレーム送受信部１１からのＡＲＰリクエストフレームは、各端末Ａ５０、Ｂ６０から仮想ＭＡＣアドレス取得のために送信されたフレームであり、応答フレーム（ＡＲＰリプライフレーム）に仮想ＭＡＣアドレスを格納することで、各端末Ａ５０、Ｂ６０は仮想ＭＡＣアドレスを取得できる。
【００４２】
クライアント端末Ｂ６０には、端末側フレーム送受信部６１とＡＲＰ応答制御部６２とを備える。
【００４３】
端末側フレーム送受信部６１は、フロアＬＡＮ１００からフレームを受信し、自装置宛てのＡＲＰリクエストフレームを受信したとき、当該フレームをＡＲＰ応答制御部６２に出力する。自装置宛てでないと、当該フレームを廃棄する。また、端末側フレーム送受信部６１は、ＡＲＰ応答制御部６２からＡＲＰリプライフレームを受け取り、当該フレームをフロアＬＡＮ１００に送信する。
【００４４】
ＡＲＰ応答制御部６２は、ＡＲＰリクエストフレームを受け取ると、送信元ＩＰアドレスがセキュリティスイッチ１０のＩＰアドレス（「10.0.0.1」）のみＡＲＰリプライフレームを生成し、端末側フレーム送受信部６１に出力する。送信元がセキュリティスイッチ１０からのＡＲＰリクエストフレームでないとき、ＡＲＰ応答制御部６２は、当該フレームを廃棄する。ＩＰアドレスに代え、セキュリティスイッチ１０のＭＡＣアドレス（「00:11:11:11:11:01」）をチェックするようにしてもよい。
【００４５】
また、クライアント端末Ｂ６０には、ＡＲＰテーブルを備える。ＡＲＰ応答制御部６２により、端末Ａ５０からＡＲＰリプライフレームを受信するごと、端末Ａ５０のＭＡＣアドレス（仮想ＭＡＣアドレス又は実ＭＡＣアドレス）と端末Ａ５０のＩＰアドレスを組としたエントリをＡＲＰテーブルに追加する。
【００４６】
このＡＲＰテーブルに基づいて、端末Ｂ６０は端末Ａ５０の仮想ＭＡＣアドレスを用いてフレームの送受信を行うことができる。
【００４７】
尚、クライアント端末Ａ５０も同様に端末側フレーム送受信部とＡＲＰ応答制御部を備える。
【００４８】
更に、レイヤ２スイッチＣ３０とレイヤ２スイッチＤ４０には、ＭＡＣアドレス（仮想ＭＡＣアドレス又は実ＭＡＣアドレス）と出力ポートの組である学習テーブルを備える。レイヤ２スイッチＣ３０、Ｄ４０では、入力されたフレームに対して、送信元ＭＡＣアドレスと接続ポート先とから学習テーブルのエントリを追加することになる。
【００４９】
このように構成されたセキュリティスイッチ１０等の動作について以下説明する。図４はセキュリティスイッチ１０におけるフローチャートの例、図５は端末Ａ５０、Ｂ６０におけるフローチャートの例である。
【００５０】
以下に示す例では、端末Ａ５０から端末Ｂ６０に対して通信を行う場合で説明する。尚

、端末Ａ５０、Ｂ６０のＡＲＰテーブルと、レイヤ２スイッチＣ３０、Ｄ４０の学習テーブルにはエントリが登録されていないものとする。

【００５１】

全体の動作は、（１）セキュリティスイッチ１０によるアドレス収集（仮想ＭＡＣアドレスの生成）、（２）端末Ａ５０の端末Ｂ６０に対するアドレスの解決（生成した仮想ＭＡＣアドレスの取得）、（３）端末Ａ５０が端末Ｂ６０にフレーム送信（取得した仮想ＭＡＣアドレスに基づいてフレームの送信）、の３つのフェーズに分かれる。それぞれについて説明する。

【００５２】

（フェーズ１）セキュリティスイッチ１０によりアドレス収集

まず、セキュリティスイッチ１０のアドレス収集部１５は、タイマ割り込み（Ｓ３０）を契機に、収集先のＩＰアドレスを決定する（Ｓ３１）。ここでは、端末Ａ５０のＩＰアドレスを対象とする。

【００５３】

そして、アドレス収集部１５は、端末Ａ５０宛てにＡＲＰリクエストフレームを生成する（Ｓ３２）。ＡＲＰリクエストフレームは、送信元ＭＡＣアドレスを「00:11:11:11:11:01」（セキュリティスイッチ１０のＭＡＣアドレス）、送信元ＩＰアドレスを「10.0.0.1」（セキュリティスイッチ１０のＩＰアドレス）、宛て先ＭＡＣアドレスを「FF:FF:FF:FF:FF:FF」（ブロードキャスト送信）、宛て先ＩＰアドレスを「10.0.0.2」（端末Ａ５０のＩＰアドレス）とする。アドレス収集部１５は、生成したＡＲＰリクエストフレームを、フレーム送受信部１１に出力する。

【００５４】

フレーム送受信部１１は、このＡＲＰリクエストフレームをフロアＬＡＮ１００側に送信する。

【００５５】

レイヤ２スイッチＣ３０は、当該フレームを受信すると、学習テーブルにＭＡＣアドレス（送信元であるセキュリティスイッチ１０のＭＡＣアドレス「00:11:11:11:11:01」）と接続ポート（図１に示すように、「Port2」）を登録する。また、当該フレームの宛て先ＭＡＣアドレスがブロードキャストアドレスのため、レイヤ２スイッチＣ３０は全ポート（レイヤ２スイッチＣ３０の「Port1」及び「Port3」）に対して当該フレームを送信する。

【００５６】

レイヤ２スイッチＤ４０が、上記ＡＲＰリクエストフレームを受信すると、学習テーブルに、ＭＡＣアドレス（送信元であるセキュリティスイッチ１０のＭＡＣアドレス「00:11:11:11:11:01」）と接続ポート（レイヤ２スイッチＤ４０の「Port1」）とを登録する。また、当該フレームの宛て先ＭＡＣアドレスがブロードキャストアドレスのため、レイヤ２スイッチＤ４０は、全ポート（レイヤ２スイッチの「Port2」）に当該フレームを送信する。

【００５７】

端末Ｂ６０（の端末側フレーム送受信部６１）は、上記ＡＲＰフレームを受信する（図５のＳ４０）と、宛て先ＩＰアドレスが端末Ａ５０のＩＰアドレスであり、自身のＩＰアドレス宛てのＡＲＰリクエストフレームではないため（Ｓ４１で「Ｎ」）、当該フレームを廃棄する（Ｓ４７）。

【００５８】

一方、端末Ａ５０は、上記ＡＲＰフレームを受信する（Ｓ４０）と、自身のＩＰアドレス宛てのＡＲＰリクエストフレームのため（Ｓ４１で「Ｙ」、Ｓ４２で「Ｎ」）、端末側フレーム送受信部は当該フレームをＡＲＰ応答制御部に転送する。

【００５９】

ＡＲＰ応答制御部は、当該フレームの送信元はセキュリティスイッチ１０のため（Ｓ４４で「Ｙ」）、ＡＲＰリプライフレームを生成する（Ｓ４５）。そして、端末側フレーム

送受信部は当該フレームを送信する（Ｓ４６）。

【００６０】

このＡＲＰリプライフレームは、送信元ＭＡＣアドレスを「00:11:11:11:11:02」（端末Ａ５０のＩＰアドレス）、送信元ＩＰアドレスを「10.0.0.2」（端末Ａ５０のＩＰアドレス）、宛て先ＭＡＣアドレスを「00:11:11:11:11:01」（セキュリティスイッチ１０のＭＡＣアドレス）、宛て先ＩＰアドレスを「10.0.0.1」（セキュリティスイッチ１０のＩＰアドレス）としたフレームである。

【００６１】

このＡＲＰリプライフレームを受信したレイヤ２スイッチＣ３０は、当該フレームから、ＭＡＣアドレス（送信元である端末Ａ５０のＭＡＣアドレス「00:11:11:11:11:02」）と接続ポート（「Port1」）とを学習テーブルに登録する。レイヤ２スイッチＣ３０は、宛て先ＭＡＣアドレス（セキュリティスイッチ１０のＭＡＣアドレス）の接続するポート（「Port2」）に対して、当該フレームを送信する。

【００６２】

セキュリティスイッチ１０のフレーム送受信部１１は、このフレームを受信する（Ｓ１０）と、自装置宛てのＡＲＰリプライフレームか否かを判断する（Ｓ１１）。この場合、自装置宛てのＡＲＰリプライフレームのため（Ｓ１１で「Ｙ」）、当該フレームをアドレス収集部１５に出力する。

【００６３】

アドレス収集部１５は、ＡＲＰリプライフレームの送信元ＩＰアドレス（端末Ａ５０のＩＰアドレス「10.0.0.2」）と送信元ＭＡＣアドレス（端末Ａ５０のＭＡＣアドレス「00:11:11:11:11:02」）とを仮想ＭＡＣアドレス生成部１６に出力する。

【００６４】

仮想ＭＡＣアドレス生成部１６は、送信元ＩＰアドレスと送信元ＭＡＣアドレス（或いは、どちらか一方）をキーにしてアドレス対応保持部１４を検索し（Ｓ１２）、登録済みか否か判断する（Ｓ１３）。

【００６５】

この場合、該当するエントリはみつからない（Ｓ１３で「Ｎ」）ため、仮想ＭＡＣアドレス生成部１６は、仮想ＭＡＣアドレスを生成する（Ｓ１４）。

【００６６】

仮想ＭＡＣアドレスは、実ＭＡＣアドレス（この場合、送信元である端末Ａ５０のＭＡＣアドレス「00:11:11:11:11:02」）を基にして生成される。仮想ＭＡＣアドレスの生成ルールとして、例えば、ＡＲＰリプライフレーム（ＭＡＣフレーム）のＭＡＣヘッダのＧ／Ｌ（Global/Local）ビット（ＭＡＣアドレスの第１オクテットの下位２ビット目）を「１」にする。

【００６７】

この例では、ＭＡＣアドレスの第１オクテット「00」は、「１６進」のため、「２進」に直すと「0000 0000」であり、下位２ビット目を「１」にすると「0000 0010」となる。これを元の「１６進」に直すと、第１オクテットは「00」から「02」となり、仮想ＭＡＣアドレス「02:11:11:11:11:02」となる。

【００６８】

勿論、普段使用されない値を用いることにより仮想ＭＡＣアドレスを生成するようにしてもよい。

【００６９】

これにより、セキュリティスイッチ１０では、ＭＡＣアドレスのＧ／Ｌビットが「１」の場合、全て仮想ＭＡＣアドレスと判断することができる。

【００７０】

仮想ＭＡＣアドレス生成部１６は、生成した仮想ＭＡＣアドレス（端末Ａ５０の仮想ＭＡＣアドレス「02:11:11:11:11:02」）と、ＩＰアドレス（端末Ａ５０のＩＰアドレス「10.0.0.2」）、及び実ＭＡＣアドレス（端末Ａ５０のＭＡＣアドレス「00:11:11:11:11:02

」）を一つのエントリとしてアドレス対応保持部１４に登録する（Ｓ１５）。
【００７１】
上記と同様の手順により、セキュリティスイッチ１０は、端末Ｂ６０の仮想ＭＡＣアドレス（「02:11:11:11:11:03」）と、ＩＰアドレス（「10.0.0.3」）、及び実ＭＡＣアドレス（「00:11:11:11:11:03」）をアドレス対応保持部１４に登録する。
【００７２】
アドレス対応保持部１４に登録されたテーブルの例を図６（Ａ）に示す。
【００７３】
（フェーズ２）端末Ａ５０の端末Ｂ６０に対するアドレス解決
次に、端末Ａ５０が端末Ｂ６０のアドレス解決（生成した仮想ＭＡＣアドレスの取得）行うフェーズについて説明する。
【００７４】
まず、端末Ａ５０は、セキュリティスイッチ１０に対してＡＲＰリクエストフレームを送信する。このＡＲＰリクエストフレームの送信元ＭＡＣアドレスは「00:11:11:11:11:02」（端末Ａ５０のＭＡＣアドレス）、送信元ＩＰアドレスは「10.0.0.2」（端末Ａ５０のＩＰアドレス）、宛て先ＭＡＣアドレスは「FF:FF:FF:FF:FF:FF」（ブロードキャストアドレス）、宛て先ＩＰアドレスは「10.0.0.3」（端末Ｂ６０のＩＰアドレス）である。
【００７５】
レイヤ２スイッチＣ３０がＡＲＰリクエストフレームを受信すると、宛て先ＭＡＣアドレスがブロードキャストアドレスを示しているため、全ポートに対して当該フレームを送信する。
【００７６】
レイヤ２スイッチＤ４０がＡＲＰリクエストフレームを受信すると、学習テーブルに、送信元ＭＡＣアドレス（端末Ａ５０のＭＡＣアドレス「00:11:11:11:11:02」）と接続ポート（「Port1」）とを登録する。また、レイヤ２スイッチＤ４０は、宛て先ＭＡＣアドレスがブロードキャストアドレスのため、当該フレームを全ポートに送信する。
【００７７】
端末Ｂ６０は、このＡＲＰリクエストフレームを受信すると（Ｓ４０）、当該フレームをＡＲＰ応答制御部６２に出力する（Ｓ４１で「Ｙ」、Ｓ４２で「Ｙ」）。尚、端末側フレーム送受信部６１は受信フレームがＡＲＰリクエストフレームか否かを判断している（Ｓ４２）が、これは、上述したセキュリティスイッチ１０のフレーム送受信部１１と同様に、フレーム内の各フィールド３０１、３０２（図３参照）により判断する。
【００７８】
ＡＲＰ応答制御部６２は、送信元ＩＰアドレスが端末Ａ５０のアドレスのため（Ｓ４４で「Ｎ」）、当該フレームを廃棄し（Ｓ４７）、応答フレームを作成しない。
【００７９】
本実施例１において、各端末Ａ５０、Ｂ６０では、送信元がセキュリティスイッチ１０であるＡＲＰリクエストフレームを受信したときのみ応答フレーム（ＡＲＰリプライフレーム）を作成し、それ以外のフレームを受信したときは、当該フレームを破棄する機能を備える。
【００８０】
一方、セキュリティスイッチ１０のフレーム送受信部１１は、端末Ａ５０からのＡＲＰリクエストフレームを受信すると（Ｓ１０、Ｓ１１で「Ｎ」、Ｓ２０で「Ｙ」）、当該フレームをＡＲＰ代理応答部１７に転送する（Ｓ２１）。
【００８１】
ＡＲＰ代理応答部１７は、ＡＲＰリクエストフレームの宛て先ＩＰアドレス（端末Ｂ６０のＩＰアドレス「10.0.0.3」）をキーにしてアドレス対応保持部１４を検索する（Ｓ２２）。この例では、（フェーズ１）にて該当するエントリが登録されている（Ｓ２３で「Ｙ」）。尚、登録されていない場合（Ｓ２３で「Ｎ」）、（フェーズ１）において仮想ＭＡＣアドレスが生成されていないため、受信したＡＲＰリクエストフレームを破棄する（

Ｓ１６）。
【００８２】
ＡＲＰ代理応答部１７は、アドレス対応保持部１４から、対応する仮想ＭＡＣアドレス（端末Ｂ６０の仮想ＭＡＣアドレス「02:11:11:11:11:03」）を取得する。そして、ＡＲＰリクエストフレームに対するＡＲＰリプライフレームを作成する（Ｓ２４）。
【００８３】
ＡＲＰリプライフレームの送信元ＭＡＣアドレスは、「02:11:11:11:11:03」（端末Ｂ６０の仮想ＭＡＣアドレス）、送信元ＩＰアドレスは「10.0.0.3」（端末Ｂ６０のＩＰアドレス）、宛て先ＭＡＣアドレスは「00:11:11:11:11:02」（端末Ａ５０のＭＡＣアドレス）、宛て先ＩＰアドレスは「10.0.0.2」（端末Ａ５０のＩＰアドレス）である。
【００８４】
生成されたＡＲＰリプライフレームは、送信先物理ポートが決定され（Ｓ１７）、当該ポートから、フロアＬＡＮ１００側に送信される（Ｓ１８）。
【００８５】
レイヤ２スイッチＣ３０は、このＡＲＰリプライフレームを受信すると、学習テーブルに、送信元ＭＡＣアドレス（端末Ｂ６０の仮想ＭＡＣアドレス「02:11:11:11:11:03」）と、接続ポート（「Port2」）を登録する。また、レイヤ２スイッチＣ３０は、学習テーブルを参照し、宛て先ＭＡＣアドレス（「00:11:11:11:11:02」端末Ａ５０のＭＡＣアドレス）の接続するポート（「Port2」）に当該フレームを送信する。
【００８６】
端末Ａ５０は、ＡＲＰリプライフレームを受信して、端末Ｂ６０の仮想ＭＡＣアドレス（「02:11:11:11:11:03」）を取得する（Ｓ４０、Ｓ４１で「Ｙ」、Ｓ４２で「Ｎ」、Ｓ４３）。
【００８７】
尚、端末Ｂ６０もＡＲＰリクエストフレームをセキュリティスイッチ１０に送信し、その応答フレームであるＡＲＰリプライフレームから、端末Ａ５０の仮想ＭＡＣアドレスを取得できる。
【００８８】
（フェーズ３）端末Ａ５０が端末Ｂ６０にフレームを送信する
次に、端末Ａ５０が、取得した仮想ＭＡＣアドレスに基づいて、フレームを端末Ｂ６０に送信するフェーズについて説明する。
【００８９】
端末Ａ５０は、端末Ｂ６０宛てにフレームを送信する。このフレームの送信元ＭＡＣアドレスは、「00:11:11:11:11:02」（端末Ａ５０のＭＡＣアドレス）、送信元ＩＰアドレスは「10.0.0.2」（端末Ａ５０のＩＰアドレス）、宛て先ＭＡＣアドレスは「02:11:11:11:11:03」（端末Ｂ６０の仮想ＭＡＣアドレス）、宛て先ＩＰアドレスは「10.0.0.3」（端末Ｂ６０のＩＰアドレス）である。
【００９０】
レイヤ２スイッチＣ３０は、このフレームを受信すると、学習テーブルを参照して、宛て先ＭＡＣアドレス（端末Ｂ６０の仮想ＭＡＣアドレス「02:11:11:11:11:03」）の接続するポート（「Port2」）に当該フレームを送信する。このエントリは、フェーズ２で作成されたものである。
【００９１】
セキュリティスイッチ１０のフレーム送受信部１１がこのフレームを受信すると（Ｓ１０、Ｓ２０で「Ｎ」）、当該フレームをセキュリティチェック部１２に出力する。
【００９２】
セキュリティチェック部１２は、受信フレームのセキュリティをチェックし（Ｓ２５）、当該フレームをＭＡＣアドレス変換部１３に出力する（Ｓ２５で「Ｙ」）。
【００９３】
尚、セキュリティチェック部１２は受信フレームのセキュリティをチェックした結果、

問題が発生しているときは、当該フレームを廃棄する（Ｓ２７）。ワームやＤｏｓ攻撃等の問題が発生しているため、フロアＬＡＮ１００内の装置への感染を防ぐためである。

【００９４】

また、セキュリティチェック部１２は、当該フレームを廃棄するかわりに、問題が発生したことを示す情報を表示部に表示させたり、ログを取る等の処理を行ってもよい。

【００９５】

ＭＡＣアドレス変換部１３は、送信元ＭＡＣアドレス（端末Ａ５０のＭＡＣアドレス「00:11:11:11:11:02」）をキーにして、アドレス対応保持部１４を検索し、仮想ＭＡＣアドレス（端末Ａ５０の仮想ＭＡＣアドレス「02:11:11:11:11:02」、フェーズ１で生成）を取得する（Ｓ２６で「Ｙ」、Ｓ２８）。

【００９６】

そして、ＭＡＣアドレス変換部１３は、受信フレームの送信元ＭＡＣアドレスを、取得した仮想ＭＡＣアドレスに書き換える（Ｓ２９）。

【００９７】

また、ＭＡＣアドレス変換部１３は、受信フレーム内の宛て先ＭＡＣアドレス（端末Ｂ６０の仮想ＭＡＣアドレス「02:11:11:11:11:03」）をキーにして、アドレス対応保持部１４を検索し（Ｓ２８）、実ＭＡＣアドレス（端末Ｂ６０の実ＭＡＣアドレス「00:11:11:11:11:03」）を取得する。そして、受信フレームの宛て先ＭＡＣアドレス（仮想ＭＡＣアドレス）を、取得した実ＭＡＣアドレスに書き換える（Ｓ２９）。

【００９８】

つまり、書き換えられたフレームにおいて、送信元ＭＡＣアドレスは「02:11:11:11:02」（端末Ａ５０の仮想ＭＡＣアドレス）、送信元ＩＰアドレスは「10.0.0.2」（端末Ａ５０のＩＰアドレス）、宛て先ＭＡＣアドレスは「00:11:11:11:11:03」（端末Ｂ６０の実ＭＡＣアドレス）、宛て先ＩＰアドレスは「10.0.0.3」（端末Ｂ６０のＩＰアドレス）となる。

【００９９】

ＭＡＣアドレス変換部１３は、書き換えられたフレームをフレーム送受信部１１に出力し、フレーム送受信部１１は当該フレームをフロアＬＡＮ１００側に送信する（Ｓ１７、１８）。

【０１００】

レイヤ２スイッチＣ３０は、この送信フレームを受信すると、学習テーブルに、送信元ＭＡＣアドレス「02:11:11:11:11:02」（端末Ａ５０の仮想ＭＡＣアドレス）と、接続ポート（「Port1」）を登録し、宛て先ＭＡＣアドレス（「00:11:11:11:11:03」）の接続するポート（「Port2」）に当該フレームを送信する。

【０１０１】

そして、端末Ｂ６０は、この送信フレームを受信する（Ｓ４０、Ｓ４１で「Ｙ」、Ｓ４２で「Ｎ」、Ｓ４３）。

【０１０２】

尚、端末Ｂ６０から端末Ａ５０へのフレームの送信も、本フェーズ３と手順により同様に実現することができる。

【０１０３】

端末Ａ５０と端末Ｂ６０との間のフレームの送受信が完了した後、各レイヤ２スイッチＣ３０、Ｄ４０における学習テーブルの例を夫々図６（Ｂ）及び同図（Ｃ）に示し、各端末Ａ５０、Ｂ６０のＡＲＰテーブルの例を夫々図７（Ａ）及び同図（Ｂ）に示す。

【０１０４】

このように、本実施例１では、端末Ａ５０から端末Ｂ６０宛てにフレームを送信するときに、仮想ＭＡＣアドレスを用いて、レイヤ２スイッチＣ３０からセキュリティスイッチ１０に転送するようにしているため、セキュリティチェック部１２を経由させることができる。従って、フロアＬＡＮ１００内の端末Ａ５０、Ｂ６０に対してセキュリティの向上を実現したセキュリティスイッチ１０を提供できる。

【０１０５】
また、図２０（Ａ）と比較しても、全体のネットワーク構成を変えることなく上記機能を実現している。
【０１０６】
更に、レイヤ２スイッチＣ３０、Ｄ４０にセキュリティチェック部１２を追加させる必要もないため、コストアップに繋がることもなく、工数を増大させることもない。
【実施例２】
【０１０７】
次に、実施例２について説明する。本実施例２では、ＡＲＰリクエストフレームやＡＲＰリプライフレームを使用しないで仮想ＭＡＣアドレスを作成し、セキュリティの向上を図るようにした例である。
【０１０８】
図８は、本実施例２におけるセキュリティスイッチ１０等の構成例である。実施例１と比較して、バックボーンＬＡＮ１１０側にサーバ１２０（ＩＰアドレスは「20.0.0.1」）が設置される。また、セキュリティスイッチ１０とバックボーンＬＡＮ１１０との間にデフォルトゲートウェイ１３０（ＭＡＣアドレスは「00:11:11:11:11:10」）が設置される。それ以外のネットワーク構成例は、実施例１と略同様である。
【０１０９】
また、端末Ａ５０、Ｂ６０の構成は実施例１と同様で、セキュリティスイッチ１０の構成も実施例１と略同様である。
【０１１０】
但し、セキュリティスイッチ１０のアドレス収集部１５は、実施例１と異なり、フロアＬＡＮ１００側から受信するフレームのヘッダ情報から、送信元ＩＰアドレス及び送信元ＭＡＣアドレスを抽出し、仮想ＭＡＣアドレス生成部１６に出力する。
【０１１１】
仮想ＭＡＣアドレス生成後の処理は、実施例１と同様なので、以下の説明では、フェーズ１（セキュリティスイッチ１０によるアドレス収集フェーズ）について説明する。
【０１１２】
また、説明を容易にするため、端末Ａ５０がバックボーンＬＡＮ１１０側のサーバ１２０に対して、フレームを送信し、セキュリティスイッチ１０でアドレス収集して仮想ＭＡＣアドレスを生成する例で説明する。尚、レイヤ２スイッチＣ３０の学習テーブルには、予め、ＭＡＣアドレス「00:11:11:11:11:10」（ゲートウェイ１３０の実ＭＡＣアドレス）と接続ポート（「Port2」）が登録されているものとする。図９は、本実施例２におけるセキュリティスイッチ１０のフローチャートの例を示す図である。図４に示す例と同一の処理には同一の符号を付している。
【０１１３】
（フェーズ１）セキュリティスイッチ１０によるアドレス収集
端末Ａ５０は、サーバ１２０にフレームを送信すべく、当該フレームを生成する。フレームの送信元ＭＡＣアドレスは「00:11:11:11:11:02」（端末Ａ５０のＭＡＣアドレス）、送信元ＩＰアドレスは「10.0.0.2」（端末Ａ５０のＩＰアドレス）、宛て先ＩＰアドレスは「20.0.0.2」（サーバ１２０のＩＰアドレス）、宛て先ＭＡＣアドレスは「00:11:11:11:11:10」（ゲートウェイ１３０のＭＡＣアドレス）である。
【０１１４】
レイヤ２スイッチＣ３０が、このフレームを受信すると、学習テーブルを参照して、宛て先ＭＡＣアドレス（「00:11:11:11:11:10」）の接続するポート（「Port2」）に、当該フレームを送信する。
【０１１５】
セキュリティスイッチ１０のフレーム送受信部１１が、このフレームを受信する（Ｓ１０）と、当該フレームをバックボーンＬＡＮ１１０側に転送する。また、当該フレームはフロアＬＡＮ１００からの受信フレームのため、アドレス収集部１５にも複製して転送す

る。
【０１１６】
アドレス収集部１５は、受信フレームの送信元ＩＰアドレス（端末Ａ５０のＩＰアドレス「10.0.0.2」）及び送信元ＭＡＣアドレス（端末Ａ５０のＭＡＣアドレス「00:11:11:11:11:02」）を仮想ＭＡＣアドレス生成部１６に出力する。
【０１１７】
仮想ＭＡＣアドレス生成部１６は、送信元ＩＰアドレスと送信元ＭＡＣアドレス（或いはいずれか一方）をキーにして、アドレス対応保持部１４を検索する（Ｓ５０）。この例では、端末Ａ５０の仮想ＭＡＣアドレスは登録されていないので（Ｓ５１で「Ｎ」）、仮想ＭＡＣアドレスを生成する（Ｓ５２）。
【０１１８】
仮想ＭＡＣアドレス生成部１６は、実施例１と同様に実ＭＡＣアドレスを基に、仮想ＭＡＣアドレス（端末Ａ５０の仮想ＭＡＣアドレス「02:11:11:11:11:02」）を生成する。そして、この仮想ＭＡＣアドレスと、ＩＰアドレス（「10.0.0.2」）、及び実ＭＡＣアドレス（「00:11:11:11:11:02」）をアドレス対応保持部１４に登録する（Ｓ５３）。
【０１１９】
以上により、セキュリティスイッチ１０は、フロアＬＡＮ１００側からの受信フレームに基づいてアドレスの収集を行い、フロアＬＡＮ１００内の各端末Ａ５０、Ｂ６０の仮想ＭＡＣアドレスを生成することができる。以降の処理は、実施例１と同様である。
【０１２０】
この際に、実施例１と比較して、ＡＲＰフレーム（リプライ、リクエストの双方）の送受信が行われないため、その分フロアＬＡＮ１００内に転送されるデータ量を少なくでき、ネットワーク資源の有効活用を図ることができる。
【０１２１】
また、その後の処理で、例えば端末Ａ５０がセキュリティスイッチ１０に対してＡＲＰリクエストフレームを送信し、その応答フレームを受信することで、端末Ａ５０は端末Ｂ６０の仮想ＭＡＣアドレスを取得できる（フェーズ２）。
【０１２２】
更に、その仮想ＭＡＣアドレスを使用してフレームを送信することで、当該フレームがセキュリティスイッチ１０に転送できる（フェーズ３）。従って、本実施例２でも、本実施例１と同様に、ネットワーク構成を変えることなく、セキュリティの向上を図ることのできるセキュリティスイッチ１０を提供することができる。
【実施例３】
【０１２３】
次に実施例３について説明する。本実施例３は、セキュリティスイッチ１０の同一物理ポート配下の通信では、実施例１等と同様の仮想ＭＡＣアドレスを用いてセキュリティスイッチ１０を経由させ、他の物理ポート配下の通信では、これらの処理を行わないでセキュリティスイッチ１０を経由させるようにした例である。
【０１２４】
図１０は、本実施例３におけるネットワークの構成例を示す図である。実施例１等と同一の部分には同一の符号を付している。セキュリティスイッチ１０の別の物理ポート（例えば、「Port2」）に端末Ｃ７０が接続される。
【０１２５】
図１１は、セキュリティスイッチ１０等の構成例である。実施例１等と略同様であるが、端末接続ポート保持部１８が追加されている。
【０１２６】
端末接続ポート保持部１８は、端末の実ＭＡＣアドレスと接続先の物理ポート情報とを保持する。
【０１２７】
また、アドレス収集部１５は、ＡＲＰリプライフレームをフレーム送受信部１１から受

け取ると、当該フレームの受信物理ポート番号と送信元ＭＡＣアドレスとを端末接続ポート保持部１８に登録する。それ以外の機能は、実施例１等と同様である。

【０１２８】

更に、ＡＲＰ代理応答部１７は、フレーム送受信部１１からＡＲＰリクエストフレームと共に、受信ポート番号を受け取る。そして、ＡＲＰ代理応答部１７は、宛て先ＩＰアドレスを検索キーにしてアドレス対応保持部１４を検索する。更に、その得られた実ＭＡＣアドレスを検索キーにして端末接続ポート保持部１８を検索し、物理ポート番号を得る。得られた物理ポート番号と、フレーム送受信部１１からのポート番号とを比較して、受信ポートと同一物理ポート配下か否かを判断する。この判断結果により、受信ポートと同一ポート配下の場合は仮想ＭＡＣアドレスを応答し、別ポート配下の場合は実ＭＡＣアドレスを応答する。

【０１２９】

尚、フレーム送受信部１１は、受信物理ポート番号をアドレス収集部１５とＡＲＰ代理応答部１７に出力している。例えば、物理ポートの番号を示す情報がメモリに記憶され、ある物理ポートでフレームを受信すると、その情報をフレームと共に出力している。

【０１３０】

次に動作を説明する。図１２は、本実施例３におけるセキュリティスイッチ１０のフローチャートの例を示す図である。実施例１（図４）と同一の処理には同一の符号が付されている。また、各端末Ａ５０等の処理は実施例１と同様に図５のフローチャートに従う。実施例１と同様にフェーズ１～フェーズ３の各フェーズについて説明する。

【０１３１】

（フェーズ１）セキュリティスイッチ１０によるアドレス収集

セキュリティスイッチ１０のアドレス収集部１５により、ＡＲＰリクエストフレームが生成され、当該フレームに対して、端末Ａ５０がＡＲＰリプライフレームを送信するまでは、実施例１と同様である。

【０１３２】

この際、レイヤ２スイッチＣ３０、Ｄ４０で生成される学習テーブルも同様であり、端末Ｂ６０において受信したＡＲＰリクエストフレームを廃棄して応答しない点も実施例１同様である。

【０１３３】

セキュリティスイッチ１０のフレーム送受信部１１が、ＡＲＰリプライフレームを受信すると（図１２のＳ１０）、自装置宛てのリプライフレームのため（Ｓ１１で「Ｙ」）、当該ＡＲＰリプライフレームと受信物理ポート番号（「Port1」）をアドレス収集部１５に出力する。

【０１３４】

アドレス収集部１５は、ＡＲＰリプライフレームの送信元ＩＰアドレス（端末Ａ５０のＩＰアドレス「10.0.0.2」）と送信元ＭＡＣアドレス（「00:11:11:11:11:02」）を仮想ＭＡＣアドレス生成部１６に出力する。

【０１３５】

また、アドレス収集部１５は、送信元ＭＡＣアドレスと受信物理ポート番号（「Port1」）を端末接続ポート保持部１８に出力して、当該情報が保持される（Ｓ６０）。

【０１３６】

仮想ＭＡＣアドレス生成部１６は、送信元ＩＰ及びＭＡＣアドレス（或いはいずれか一方）を検索キーにしてアドレス対応保持部１４を検索するが該当するエントリはみつからない（Ｓ１２、Ｓ１３で「Ｎ」）ので、仮想ＭＡＣアドレスを生成する（Ｓ１４）。

【０１３７】

仮想ＭＡＣアドレス生成部１６は、実ＭＡＣアドレスに基づいて、仮想ＭＡＣアドレス（端末Ａ５０の仮想ＭＡＣアドレス「02:11:11:11:11:02」）を生成する。生成ルールは実施例１と同様である。生成された仮想ＭＡＣアドレスは、実ＭＡＣアドレス及びＩＰアドレスとともにアドレス対応保持部１４に登録される（Ｓ１５）。

【０１３８】
以上のようにして、仮想ＭＡＣアドレスが登録されるとともに、端末接続ポート保持部１８には、端末Ａ５０のエントリ（ＭＡＣアドレス「00:11:11:11:11:02」、ポート番号「Port1」）が登録される。
【０１３９】
上記と同様の手順により、端末接続ポート保持部１８には、端末Ｂ６０のエントリ（ＭＡＣアドレス「00:11:11:11:11:03」、ポート番号「Port1」）、及び端末Ｃ７０のエントリ（ＭＡＣアドレス「00:11:11:11:11:04」、ポート番号「Port2」）も登録される。
【０１４０】
（フェーズ２）端末Ａ５０の端末Ｂ６０に対するアドレス解決
端末Ａ５０がＡＲＰリクエストフレームをブロードキャストで送信するのは、実施例１と同様である。異なるのは、当該フレームを受信したセキュリティスイッチ１０側の処理（Ｓ６１～Ｓ６３）である。
【０１４１】
即ち、セキュリティスイッチ１０のフレーム送受信部１１が、ＡＲＰリクエストフレームを受信すると（Ｓ１０）、当該フレームと受信物理ポート番号（「Port1」）をＡＲＰ代理応答部１７に出力する（Ｓ１１で「Ｎ」、Ｓ２０で「Ｙ」、Ｓ２１）。
【０１４２】
ＡＲＰ代理応答部１７は、ＡＲＰリクエストフレームの宛て先ＩＰアドレス（端末Ｂ６０のＩＰアドレス「10.0.0.3」でアドレス対応保持部１４を検索し（Ｓ２２）、該当する実ＭＡＣアドレス「00:11:11:11:11:03」と仮想ＭＡＣアドレス「02:11:11:11:11:03」を取得する（Ｓ２３で「Ｙ」）。
【０１４３】
ＡＲＰ代理応答部１７は、得られた実ＭＡＣアドレスを検索キーにして、端末接続ポート保持部１８を検索し（Ｓ６１）、ポート番号「Port1」を取得する。このポート番号は、フレーム送受信部１１からの受信物理ポート番号「Port1」と同一である（Ｓ６２で「Ｙ」）。
【０１４４】
つまり、受信したポート（受信物理ポート番号）と、宛て先に送信するポート（ポート番号）とが同一である。従って、同一物理ポート配下の通信と判断できる。よって、実施例１と同様の処理、即ち、仮想ＭＡＣアドレスを用いた処理（Ｓ６３以降の処理）を行う。
【０１４５】
この例では、ＡＲＰ代理応答部１７は、ＡＲＰリプライフレームを作成し（Ｓ６３）、当該フレームを「Port1」に送信する（Ｓ１７）。端末Ａ５０は、端末Ｂ６０の仮想ＭＡＣアドレスを取得する。
【０１４６】
（フェーズ２－１）端末Ａ５０から端末Ｃ７０へのアドレス解決
次の例として、端末Ａ５０から端末Ｃ７０へのアドレス解決について説明する。
【０１４７】
まず、端末Ａ５０は、ＡＲＰリクエストフレームをブロードキャストで送信する。このＡＲＰリクエストフレームの送信元のＭＡＣアドレスとＩＰアドレスは、端末Ａのアドレス（夫々、「00:11:11:11:11:02」、「10.0.0.2」）で、宛て先ＭＡＣアドレスはブロードキャストアドレス「FF:FF:FF:FF:FF:FF」、宛て先ＩＰアドレスは端末Ｃ７０のアドレス「10.0.04」である。
【０１４８】
レイヤ２スイッチＣ３０、Ｄ４０は、このＡＲＰリクエストフレームを受信すると、ブロードキャストアドレスのため、全ポートに当該フレームを送信する。
【０１４９】
端末Ｂ６０は、自装置宛てのフレームではないため、ＡＲＰリクエストフレームを廃棄

する（Ｓ４１で「Ｎ」、Ｓ４７）。

【０１５０】

セキュリティスイッチ１０のフレーム送受信部１１がこのＡＲＰリクエストフレームを受信すると（Ｓ１０）、ブロードキャストアドレスのため、「Port2」に対して当該フレームを送信する。また、フレーム送受信部１１は、受信物理ポート番号「Port1」とＡＲＰリクエストフレームとＡＲＰ代理応答部１７に出力する（Ｓ１１で「Ｎ」、Ｓ２０で「Ｙ」、Ｓ２１）。

【０１５１】

ＡＲＰ代理応答部１７は、ＡＲＰリクエストフレームの宛て先ＩＰアドレス「10.0.0.4」でアドレス対応保持部１４を検索し、該当する実ＭＡＣアドレス「00:11:11:11:11:04」と仮想ＭＡＣアドレス「02:11:11:11:11:04」とを取得する（Ｓ２２、Ｓ２３で「Ｙ」）。

【０１５２】

そして、ＡＲＰ代理応答部１７は、得られた実ＭＡＣアドレスを検索キーにして、端末接続ポート保持部１８を検索し（Ｓ６１）、ポート番号「Port2」を取得する。この番号は、受信物路ポート番号「Port1」と異なる番号のため（Ｓ６２「Ｎ」）、実ＭＡＣアドレスでＡＲＰリプライフレームを作成する（Ｓ６４）。

【０１５３】

作成されたＡＲＰリプライフレームは、送信元を端末Ｃ７０としたアドレス（実ＭＡＣアドレス「00:11:11:11:11:04」、ＩＰアドレス「10.0.0.4」）、宛て先を端末Ａ５０のアドレス（ＭＡＣアドレス「00:11:11:11:11:02」、ＩＰアドレス「10.0.0.2」）としたフレームである。送信元のＭＡＣアドレスは、仮想ＭＡＣアドレスではなく、実ＭＡＣアドレスを用いている。

【０１５４】

フレーム送受信部１１は、「Port1」にＡＲＰリプライフレームを出力する。

【０１５５】

レイヤ２スイッチＣ３０が、このＡＲＰリプライフレームを受信すると、学習テーブルを参照して、宛て先ＭＡＣアドレス「00:11:11:11:11:02」の接続するポート「Port1」に当該フレームを送信する。

【０１５６】

端末Ａ５０は、ＡＲＰリプライフレームを受信し（Ｓ４０）、端末Ｃ７０の実ＭＡＣアドレスを取得する。その後、端末Ａ５０は、実ＭＡＣアドレスを用いて端末Ｃ７０と通信を行う。その際に、通常のレイヤ２中継により、セキュリティスイッチ１０を介して端末Ａ５０から端末Ｃ７０に対して通信が行われる。従って、送信されるフレームはセキュリティスイッチ１０のセキュリティチェック部１２を経由するため、セキュリティの向上を図ることができる。

【０１５７】

端末Ｃ７０から端末Ａ５０に対しても同様に処理を行うことで、端末Ｃ７０は端末Ａ５０の実ＭＡＣアドレスを取得し、当該アドレスを用いて通信を行う。この場合も、同様に、セキュリティスイッチ１０を経由してフレームの送受信が行われる。更に、端末Ｂ６０と端末Ｃ７０間においても全く同様に処理を行うことができる。

【０１５８】

以上のように、本実施例３では、同一物理ポート配下の通信では実施例１と同様の仮想ＭＡＣアドレスを用いた処理を行い、異なる物理ポート配下の通信では実施例１の処理を行わず通常のレイヤ２中継を行わせるようにしている。従って、いずれの場合も、フレームがセキュリティチェック部１２を経由するため、ネットワーク構成を変えることなく、セキュリティの向上を図ることができる。実施例１の他の作用効果も、本実施例３において奏することができる。

【０１５９】

本実施例３において、端末接続ポート保持部１８には、実ＭＡＣアドレスが登録される

ものとして説明したが、例えば、各端末Ａ５０等のＩＰアドレスとポート情報とが登録されるようにしてもよい。各端末Ａ５０を識別できる識別子であればよい。

【実施例４】

【０１６０】

次に、実施例４について説明する。

【０１６１】

上述した各実施例において、端末Ａ５０等には、セキュリティスイッチ１０からのＡＲＰリクエストフレームのみ、その応答フレーム（ＡＲＰリプライフレーム）を送信するものとして説明した（図４のＳ４１～Ｓ４５）。このような機能を有する（ＡＲＰ応答制御部のある）端末を対応端末と称す。一方、このような機能のない（ＡＲＰ応答制御部のない）端末を「非対応端末」と称す。

【０１６２】

フロアＬＡＮ１００内において、非対応端末がレイヤ２スイッチＣ３０、Ｄ４０の配下に接続された場合、例えば、対応端末である端末Ａ５０から非対応端末に対して、セキュリティスイッチ１０を経由せずに通信ができてしまう可能性がある。

【０１６３】

端末Ａ５０からのＡＲＰリクエストフレームに対して、非対応端末及びセキュリティスイッチ１０の双方が応答し、端末Ａ５０が非対応端末からのＡＲＰリプライを採用した場合、端末Ａ５０は非対応端末の実ＭＡＣアドレスを取得できる。従って、非対応端末が端末Ａ５０の仮想ＭＡＣアドレスを取得できること、並びに、本セキュリティスイッチ１０を経由して仮想ＭＡＣアドレスを利用した通信ができるようになる。

【０１６４】

このような事態を防止するため、本実施例４では、セキュリティスイッチ１０が非対応端末を検出すると、仮想ＭＡＣアドレスを取得できないようにする。

【０１６５】

図１３は、本実施例４におけるセキュリティスイッチ１０と、端末Ｂ６０の構成例である。実施例１（図２）と比較して、非対応端末検出部１９が付加される。

【０１６６】

非対応端末検出部１９は、アドレス対応保持部１４に登録されている実ＭＡＣアドレスに対して、装置自身のアドレスとは異なる送信元アドレスでＡＲＰリクエストフレームを作成し、フレーム送受信部１１に出力する。

【０１６７】

上述したように、対応端末には、セキュリティスイッチ１０からのＡＲＰリクエストフレームについてのみ、ＡＲＰリプライフレームを生成する機能がある。従って、セキュリティスイッチ１０でない送信元のアドレスでＡＲＰリクエストフレームをある端末に送信し、ＡＲＰリプライフレームが返信された場合、当該端末は非対応端末と判断できる。一方、ＡＲＰリプライフレームが返信されない場合、当該端末は対応端末と判断できる。

【０１６８】

非対応端末検出部１９は、このような判断結果に基づいて、非対応端末が対応端末か否かを示すフラグ情報をアドレス対応保持部１４に登録する。例えば、アドレス対応保持部１４には、対応端末は「１」、対応端末は「０」を記録する対応端末識別フィールドが追加される。

【０１６９】

尚、ＡＲＰ代理応答部１７は、アドレス対応保持部１４を検索した結果が非対応端末であったとき、ＡＲＰリプライフレームを生成しないようにする。それ以外は、実施例１と同様である。

【０１７０】

図１４は、本実施例４におけるセキュリティスイッチ１０のフローチャートの例である。ネットワーク構成は、実施例３（図１０）の例で説明する。端末Ｃ７０を検査対象の端末とする。

【０１７１】
まず、非対応端末検出部１９は、タイマ割り込み処理（Ｓ８０）により、アドレス対応保持部１４を読み込み、検査対象の宛て先ＩＰアドレスを取得する（Ｓ８１）。そして、タイマをセットし（例えば、「４」秒）（Ｓ８２）、送信元がセキュリティスイッチ１０ではないＡＲＰリクエストフレームを作成する（Ｓ８３）。
【０１７２】
例えば、送信元ＭＡＣアドレスを「00:11:11:11:11:99」、送信元ＩＰアドレスを「10.0.0.99」とする。セキュリティスイッチ１０以外の送信元アドレスを示し、かつ、他のフロアＬＡＮ１００内の装置で使用されないアドレスであればよい。宛て先ＭＡＣアドレスは「FF:FF:FF:FF:FF:FF」、宛て先ＩＰアドレスは「10.0.4」（端末Ｃ７０のＩＰアドレス）である。
【０１７３】
そして、フレーム送受信部１１から当該フレームが送信される（Ｓ１７、Ｓ１８）。
【０１７４】
端末Ｃ７０が、対応端末であれば、送信元のＩＰアドレス（又はＭＡＣアドレス）がセキュリティスイッチ１０のものでないため、応答フレームを作成しない。非対応端末であれば、ＡＲＰリクエストフレームに対して応答するため、ＡＲＰリプライフレームを送信する。
【０１７５】
図１５は、セキュリティスイッチ１０における非対応端末を識別するためのフローチャートの例である。
【０１７６】
非対応端末検出部１９は、「４」秒経過しても（Ｓ９０）、ＡＲＰリプライフレームを受信しないとき（Ｓ９１で「Ｙ」）、アドレス対応保持部１４に対応端末として記録する（Ｓ９２）。
【０１７７】
一方、ＡＲＰリプライフレームを受信したとき（Ｓ９１で「Ｎ」）、処理は図１４のＳ１０に移行し、他装置宛て（送信元ＭＡＣアドレスが「00:11:11:11:11:99」、送信元ＩＰアドレスが「10.0.0.99」）のＡＲＰリプライフレームか否かを判断する（Ｓ７０）。
【０１７８】
他装置宛てのＡＲＰリプライフレームであれば（Ｓ７０で「Ｙ」）、非対応端末検出部１９は、アドレス対応保持部１４に、検査対象の端末が非対応端末であるとして記録する（Ｓ７１）。
【０１７９】
図１６は、アドレス対応保持部１４に記憶されたテーブルの例である。端末Ｃ７０が非対応端末として記録された例である。
【０１８０】
また、仮想ＭＡＣアドレス取得のため、端末Ｃ７０が各フロア端末宛てのＡＲＰリクエストフレームを送信したとき（Ｓ２０で「Ｙ」）、ＡＲＰ代理応答部１７は、対応端末の場合のみ、ＡＲＰリプライフレームを生成する（Ｓ７２で「Ｙ」、Ｓ２４）。対応端末でないと（Ｓ７２で「Ｎ」）、受信したＡＲＰリクエストフレームを廃棄し（Ｓ１６）、ＡＲＰリプライフレームを生成しない。
【０１８１】
これにより、非対応端末では、仮想ＭＡＣアドレスを取得できないため、非対応端末から対応端末への通信を行うことができずに、通信を遮断できる。従って、セキュリティの脅威になるような端末がフロアＬＡＮ１００に接続されて、ワーム等の感染がフロアＬＡＮ１００内の他の端末に感染されることを防止できる。
【０１８２】
それ以外の処理は、実施例１と同様である。従って、本実施例４においても、ネットワークの構成を変えることなく、セキュリティの向上を図るセキュリティスイッチ１０を提

供することができる。

【実施例５】

【０１８３】

次に、実施例５について説明する。本実施例５は、他の端末が同一のＩＰアドレスを使用しているかをチェックすることで、端末のＩＰアドレスの変更や、設定ミス等によるＩＰアドレスの重複を防止するようにした例である。

【０１８４】

図１７は本実施例５におけるセキュリティスイッチ１０等の構成例を示し、図１８は本実施例５におけるセキュリティスイッチ１０のフローチャートの例を示す。

【０１８５】

図１７に示すように、本実施例５のセキュリティスイッチ１０は、実施例１（図２）に対して、ＡＲＰ応答判断部２０が付加される。

【０１８６】

ＡＲＰ応答判断部２０は、端末Ａ５０等から送信されたＧｒａｔｕｉｔｏｕｓＡＲＰフレームと呼ばれるＡＲＰリクエストフレームに対して、返答の有無を判断する。ＧｒａｔｕｉｔｏｕｓＡＲＰフレームとは、端末Ａ５０等のＩＰアドレスが変更された場合、変更後のＩＰアドレスが、ＡＲＰリクエストフレームの送信元ＩＰアドレスと宛て先ＩＰアドレスの双方のフィールドに格納されたフレームである。

【０１８７】

ＡＲＰ応答判断部２０は、ＡＲＰ代理応答部１７よりＧｒａｔｕｉｔｏｕｓＡＲＰフレームを受け取ると、送信元ＩＰアドレスと宛て先ＩＰアドレスとが同じ場合、該アドレスを検索キーにしてアドレス対応保持部１４を検索する。

【０１８８】

検索した結果得られた実ＭＡＣアドレスと、ＧｒａｔｕｉｔｏｕｓＡＲＰフレーム内の送信元ＭＡＣアドレスとが同じ場合、ＡＲＰ代理応答部１７に対して非応答指示を出力する。それ以外の場合は、応答指示を出力する。

【０１８９】

アドレス対応保持部１４には、送信元ＩＰアドレスと送信元ＭＡＣアドレスの組が登録、或いは、実施例１の（フェーズ１）が実行されていなければこれらの組は未登録となっている。ＧｒａｔｕｉｔｏｕｓＡＲＰフレームの送信元ＩＰアドレスがアドレス対応保持部１４に登録され、当該ＩＰアドレスに対応する送信元ＭＡＣアドレスが登録されていなければ、そのＩＰアドレスは他の端末のＩＰアドレスとして登録されていることになる。つまり、アドレスの重複が生じている。

【０１９０】

かかる場合に、セキュリティスイッチ１０は当該フレームを送信した端末Ａ５０等に対して、アドレスの重複が発生していることを通知する必要がある。本実施例５では、ＩＰアドレスの重複が発生すると、端末Ａ５０等に対してＡＲＰリプライフレームを送信し、重複が発生していなければかかるフレームを送信しないようにする。これにより、ＧｒａｔｕｉｔｏｕｓＡＲＰフレームを送信した端末Ａ５０等は、ＩＰアドレスの重複をチェックできる。

【０１９１】

尚、ＡＲＰ代理応答部１７は、フレーム送受信部１１からＧｒａｔｕｉｔｏｕｓＡＲＰフレームを受け取ると、当該フレームをＡＲＰ応答判断部２０に出力する。ＡＲＰ応答判断部２０から応答指示が入力されたときのみ、ＡＲＰリプライフレームを作成する。

【０１９２】

例えば、端末Ａ５０がＩＰアドレスの変更等を行い、ＧｒａｔｕｉｔｏｕｓＡＲＰフレームを送信する場合で考える。

【０１９３】

送信元ＭＡＣアドレスは端末Ａ５０のＭＡＣアドレス（「00:11:11:11:11:02」）、送信元ＩＰアドレスと宛て先ＩＰアドレスは双方とも端末Ａ５０のＩＰアドレス（「10.0.0

.2」）、宛て先ＭＡＣアドレスはブロードキャストアドレス（「FF:FF:FF:FF:FF:FF」）とする。

【０１９４】

セキュリティスイッチ１０のフレーム送受信部１１が当該フレームを受信すると（Ｓ１０）、ＡＲＰ代理応答部１７に転送する（Ｓ１１で「Ｎ」、Ｓ２０で「Ｙ」、Ｓ２１）。

【０１９５】

ＡＲＰ代理応答部１７は、宛て先ＩＰアドレス（「10.0.0.2」）でアドレス対応保持部１４を検索し（Ｓ２２）、該当する仮想ＭＡＣアドレス（「02:11:11:11:11:02」）を取得する（Ｓ２３で「Ｙ」）。また、ＡＲＰ代理応答部１７は、ＧｒａｔｕｔｉｏｕｓＡＲＰフレームをＡＲＰ応答判断部２０に出力する。

【０１９６】

ＡＲＰ応答判断部２０は、当該フレームの送信元ＩＰアドレスと宛て先ＩＰアドレスとは同じため、アドレス対応保持部１４を検索する（Ｓ１００）。検索により、該当する実ＭＡＣアドレス（「00:11:11:11:11:02」）を取得する。

【０１９７】

この取得した実ＭＡＣアドレスと、ＧｒａｔｕｔｉｏｕｓＡＲＰフレーム中のＭＡＣアドレス（「00:11:11:11:11:02」）とは同一のため（Ｓ１０１で「Ｙ」）、ＡＲＰ応答判断部２０はＡＲＰ代理応答部１７に対して非応答指示を出力する。

【０１９８】

ＡＲＰ代理応答部１７は、非応答指示を受けると、受信したＧｒａｔｕｔｉｏｕｓＡＲＰフレームを廃棄する（Ｓ１６）。これにより、ＡＲＰリプライフレームが端末Ａ５０に送信されず、端末Ａ５０はＧｒａｔｕｔｉｐｕｓＡＲＰフレーム中のＩＰアドレス（変更後のＩＰアドレス）は他の端末で使用されていないことを把握できる。

【０１９９】

一方、端末Ｂ６０が端末Ａ５０のＩＰアドレス（「10.0.0.2」）を送信元及び宛て先ＩＰアドレスとしたＧｒａｔｕｔｉｏｕｓＡＲＰフレームを送信したとき、送信元ＭＡＣアドレスは「00:11:11:11:11:03」であり、アドレス対応保持部１４から取得したＭＡＣアドレスは「00:11:11:11:11:02」となる。この場合、異なる値のため、応答指示が出力される。端末Ｂ６０では、ＡＲＰリプライフレームが返信されるため、当該ＩＰアドレス（「10.0.0.2」）は他の端末（端末Ａ５０）で使用中であり、アドレスの重複が発生していることを把握できる。

【０２００】

その後、実施例１と同様の処理を行うことで、ネットワーク構成を変えることなく、セキュリティの向上を図るセキュリティスイッチ１０を提供することができる。

【実施例６】

【０２０１】

次に実施例６について説明する。本実施例６では、各端末Ａ５０等に記憶されるＡＲＰテーブルについて、その更新による不具合を是正した例である。

【０２０２】

実施例１等で説明したように、各端末Ａ５０等には、他の端末に対してのＭＡＣアドレス（仮想ＭＡＣアドレス又は実ＭＡＣアドレス）とＩＰアドレスの組を記憶したＡＲＰテーブルがある。

【０２０３】

このＡＲＰテーブルは、端末Ａ５０からのＡＲＰリクエストフレームを受信するごとに、ＡＲＰテーブルのエントリを確認し、端末Ａ５０のエントリが存在した場合はエントリを更新し、エントリが存在しない場合はＡＲＰテーブルに対して何も行わない。

【０２０４】

例えば、図１０のようなネットワーク構成を考える。仮想ＭＡＣアドレス取得のため（実施例１におけるフェーズ２）、端末Ａ５０が端末Ｃ７０に対してＡＲＰリクエストフレームを送信する。当該フレームの送信元アドレスは、端末Ａ５０のＩＰ及び実ＭＡＣアド

レスである。
【０２０５】
端末Ｂ６０は、ＡＲＰテーブルに端末Ａ５０のＩＰアドレスが存在すれば、当該フレームを受信する。実施例１等で説明したように、当該フレームは自装置宛てのフレームではないため、当該フレームを廃棄する（Ｓ４１で「Ｎ」、Ｓ４７）。
【０２０６】
しかし、図１９に示すように、ＡＲＰテーブル６３に端末Ａ５０のＩＰアドレスが存在すれば、端末側フレーム送受信部６１は、対応する仮想ＭＡＣアドレスを端末Ａ５０の実ＭＡＣアドレスに書き換えてしまう。この実ＭＡＣアドレスへの書き換えにより、端末Ｂ６０は端末Ａ５０の実ＭＡＣアドレスを取得することになるため、セキュリティスイッチ１０を経由せずに直接通信を行うことができる。
【０２０７】
そこで、本実施例６では、このような事態を防止するため、各端末から仮想ＭＡＣアドレス取得のため、ＡＲＰリクエストフレームを送信するときに、送信元ＩＰアドレスを自身以外のＩＰアドレス（送信元ＭＡＣアドレスは自身のＭＡＣアドレス）としたＡＲＰリクエストフレームを送信する。
【０２０８】
この場合、他の端末では、ＡＲＰテーブル６３にかかるＩＰアドレスのエントリが登録されていないため、当該フレームを受信することはない。よって、ＡＲＰテーブル６３の仮想ＭＡＣアドレスが実ＭＡＣアドレスに書き換わることがないため、各端末から送信されたフレームは、セキュリティスイッチ１０を経由することができる。従って、より高いセキュリティを確保できる。
【０２０９】
端末Ａ５０の構成自体は、例えば実施例１（図２）同様で、フレームを送信するときに端末側フレーム送受信部が自身のＩＰアドレス以外のアドレスを当該フレームに格納して送信するようにすればよい。
【０２１０】
尚、ＡＲＰリクエストフレームに格納する自身以外の送信元ＩＰアドレスの例としては、同一サブネット内で端末に割り当てていないＩＰアドレス（例えば、図１０の例では、「10.0.5」～「10.0.0.256」など）を利用すればよい。
【０２１１】
このとき、本実施例６を実施例５のＧｒａｔｕｉｔｉｏｕｓＡＲＰフレームに利用した場合、送信元ＩＰアドレスと宛て先ＩＰアドレスとは異なるフレームとなる。ＡＲＰ応答制御部６２は、送信元ＩＰアドレスがかかる特殊なＩＰアドレスであること、又は、ＧｒａｔｕｉｔｏｕｓＡＲＰフレームであることを示す宛て先ＩＰアドレスと送信元アドレスの組がＡＲＰ応答制御部６２に登録されていることをチェックして、当該フレームの識別を行う。
【０２１２】
勿論、本実施例６は、上述した実施例１等を実施することが可能であり、実施例１等と同様の作用効果を奏する。
【実施例７】
【０２１３】
次に実施例７について説明する。本実施例７はログ採取についての例である。上述した実施例１乃至６のいずれにおいても実施可能である。
【０２１４】
図２０は、本実施例７におけるネットワーク構成例である。端末Ａ５０、Ｂ６０間で行われる通信のログをセキュリティスイッチ１０で採取、又は、ログ採取用端末９０で採取するようにしている。それ以外の構成は、実施例１等と同様である。
【０２１５】
ログをセキュリティスイッチ１０で採取する場合は、セキュリティスイッチ１０内に記

憶装置（ハードディスク又はメモリなど）を搭載し、セキュリティスイッチ１０が受信するフレームのログを記憶装置に記憶する。

【０２１６】

ログをログ採取用端末９０で採取する場合は、セキュリティスイッチ１０の特定ポートにログ採取用端末９０（図２０中、点線枠内）を接続し、セキュリティスイッチ１０がフレームを受信すると当該ポートにそのフレームをコピーし、ログ採取用端末９０がセキュリティスイッチ１０から転送されるフレームのログを採取する。

【０２１７】

例えば、実施例１の（フェーズ３）により、端末Ａ５０、Ｂ６０間で行われる通信ではセキュリティスイッチ１０を経由する経路が確立されているため、かかるログを採取することができる。

【０２１８】

図２１は、セキュリティスイッチ１０又はログ採取用端末９０において採取したログの例を示す図である。例えば、端末Ａ５０（「10.0.0.2」）から端末Ｂ６０（「10.0.0.3」）にｔｅｌｎｅｔ通信を行ったときの、「ｔｃｐｄｕｍｐ」というツールを使用したログデータの例である。４フレーム分のログデータの例である。このようなログデータが、セキュリティスイッチ１０の記憶装置やログ採取用端末９０に記録される。

【０２１９】

図２２及び図２３は、ログ採取を含めたセキュリティスイッチ１０におけるフローチャートの例である。

【０２２０】

図２２は、セキュリティチェックを行わずログの採取のみ行う場合の例を示し、図２３はセキュリティチェックもログの採取も両方行う場合の例を示す。

【０２２１】

図２２に示すように、受信したフレームが自装置宛てのＡＲＰリプライフレームではなく（図２２のＳ１１で「Ｎ」）、ＡＲＰリクエストフレームでもない（Ｓ２０で「Ｎ」）と、セキュリティスイッチ１０は、トラフィックログの採取を行う（Ｓ１２０）。例えば、セキュリティスイッチ１０の記憶装置に記憶されたり、ログ採取用端末９０に転送される。その後の処理は、実施例１等と同様である。

【０２２２】

一方、セキュリティチェックもログの採取も行う場合、図２３に示すように、セキュリティスイッチ１０はログの採取を行い（Ｓ１２０）、その後、正常フレームの確認（Ｓ２５）を行う。その後の処理は実施例１等を同様である。

【０２２３】

このように、本実施例７では、端末Ａ５０、Ｂ６０間で送信されるフレームのログを、セキュリティスイッチ１０又はログ採取用端末９０で採取することができる。実施例１等も実施できるため、実施例１等と同様の作用効果も奏する。

【０２２４】

以上まとめると付記のようになる。

【０２２５】

（付記１）

同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続された中継装置において、

前記端末ごとに、前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを保持するアドレス対応保持部と、

前記端末から前記仮想ＭＡＣアドレスの取得を求める第１のＡＲＰリクエストフレームを受信したときに、対応する前記端末の前記仮想ＭＡＣアドレスを前記アドレス対応保持部から読み出して、前記仮想ＭＡＣアドレスを前記端末に応答する代理応答部と、

前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣア

ドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答するＭＡＣアドレス変換部と、
を備えることを特徴とする中継装置。
【０２２６】
（付記２）
更に、前記レイヤ２スイッチを介して接続された前記端末の全てに対して、第２のＡＲＰリクエストフレームを定期的に送信し、前記第２のＡＲＰリクエストフレームに対する応答フレームにより、前記端末のＩＰアドレスとＭＡＣアドレスの対応を収集するアドレス収集部と、
収集された前記ＩＰアドレスと前記ＭＡＣアドレスに対して、前記仮想ＭＡＣアドレスを割り当てる仮想ＭＡＣアドレス生成部とを備え、
前記仮想ＭＡＣアドレス生成部は、割り当てた前記仮想ＭＡＣアドレスと、前記ＩＰアドレス、及び前記ＭＡＣアドレスを前記アドレス対応保持部に登録することを特徴とする付記１記載の中継装置。
【０２２７】
（付記３）
更に、前記端末から送信された第３のフレームを受信し、前記第３のフレームから前記端末のＩＰアドレスとＭＡＣアドレスの対応を収集するアドレス収集部と、
収集された前記ＩＰアドレスと前記ＭＡＣアドレスに対して、前記仮想ＭＡＣアドレスを割り当てる仮想ＭＡＣアドレス生成部とを備え、
前記仮想ＭＡＣアドレス生成部は、割り当てた前記仮想ＭＡＣアドレスと、前記ＩＰアドレス、及び前記ＭＡＣアドレスを前記アドレス対応保持部に登録することを特徴とする付記１記載の中継装置。
【０２２８】
（付記４）
更に、接続先の物理ポート情報を保持する端末接続ポート保持部を備え、
前記代理応答部は、前記第１のＡＲＰリクエストフレームを受信したとき、前記物理ポート情報に基づいて同一物理ポート配下の通信と判断したときは前記仮想ＭＡＣアドレスを応答し、別物理ポート配下の通信と判断したときは前記実ＭＡＣアドレスを応答することを特徴とする付記１記載の中継装置。
【０２２９】
（付記５）
更に、前記中継装置のアドレスとは異なる送信元アドレスで第３のＡＲＰリクエストフレームを送信する非対応端末検出部を備え、
前記非対応端末検出部は、前記第３のＡＲＰリクエストフレームに対する応答フレームに基づいて、前記第３のＡＲＰリクエストフレームを送信した前記端末が、前記中継装置を送信元アドレスとした前記第１のＡＲＰリクエストフレームのみ応答する対応端末か否か、を特定することを特徴とする付記１記載の中継装置。
【０２３０】
（付記６）
更に、前記端末から送信された、送信元と宛て先のＩＰアドレスが同一の第４のＡＲＰリクエストフレームを受信したとき、前記ＩＰアドレスの重複を判断する応答判断部を備え、
前記応答代理部は、前記応答判断部の判断結果に応じて前記第４のＡＲＰフレームに対して応答する又は応答しないことを特徴とする付記１記載の中継装置。
【０２３１】
（付記７）
更に、前記端末間で送受信される前記第１のフレームのログを採取するログ採取部を備えることを特徴とする付記１記載の中継装置。
【０２３２】

（付記８）
前記レイヤ２スイッチには、前記第１のＡＲＰリクエストフレームに対する応答フレームが前記中継装置から前記端末に送信されるときに前記応答フレームに含まれる前記仮想ＭＡＣアドレスと接続ポート情報とが格納される学習テーブルを保持し、
前記第１のフレームが前記端末から送信されるときに前記学習テーブルを参照して当該第１のフレームが前記中継装置に送信されることを特徴とする付記１記載の中継装置。
【０２３３】
（付記９）
更に、前記第１のフレームのセキュリティに問題があるときは当該第１のフレームを廃棄し、問題がないときは当該第１のフレームを前記ＭＡＣアドレス変換部に出力するセキュリティチェック部を備え、
前記ＭＡＣアドレス変換部は、正常な前記第１のフレームに対して前記ＭＡＣアドレスの変換を行うことを特徴とする付記１記載の中継装置。
【０２３４】
（付記１０）
前記仮想ＭＡＣアドレス生成部は、収集した前記ＩＰアドレスと前記ＭＡＣアドレスとから前記アドレス対応保持部を検索し、前記ＩＰアドレスと前記ＭＡＣアドレスに対応する前記仮想ＭＡＣアドレスが前記アドレス対応保持部に登録されていないときに前記仮想ＭＡＣアドレスを割り当てることを特徴とする付記２記載の中継装置。
【０２３５】
（付記１１）
前記代理応答部は、前記物理ポート情報と前記第１のＡＲＰリクエストフレームを受信した前記中継装置のポート番号とを比較し、一致するときは前記同一物理ポート配下の通信と判断し、そうでないときは前記別物理ポート配下の通信と判断することを特徴とする付記４記載の中継装置。
【０２３６】
（付記１２）
前記非対応端末検出部は、前記第３のＡＲＰフレームに対する応答フレームを前記端末から受信しないとき前記端末は前記対応端末として特定し、前記応答フレームを受信したとき前記端末は前記対応端末ではない端末として特定することを特徴とする付記５記載の中継装置。
【０２３７】
（付記１３）
前記応答判断部は、前記第４のＡＲＰリクエストフレームを前記端末から受信したとき、前記第４のＡＲＰリクエストフレームの送信元ＩＰアドレスを検索キーに前記アドレス対応保持部を検索し、前記送信元ＩＰアドレスに対応する前記実ＭＡＣアドレスが登録されていなければ前記送信元ＩＰアドレスは重複していると判断し、
前記応答代理部は、前記重複している判断結果を得たとき、前記端末に対して応答することを特徴とする付記６記載の中継装置。
【０２３８】
（付記１４）
中継装置の同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続されたネットワークシステムにおいて、
前記中継装置には、
前記端末ごとに、前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを保持するアドレス対応保持部と、
前記端末から前記仮想ＭＡＣアドレスの取得を求める第１のＡＲＰリクエストフレームを受信したときに、対応する前記端末の前記仮想ＭＡＣアドレスを前記アドレス対応保持部から読み出して、前記仮想ＭＡＣアドレスを前記端末に応答する代理応答部と、

前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣアドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答するＭＡＣアドレス変換部とを備え、

前記端末には、前記中継装置からの応答フレームに対してのみ応答する応答制御部を備える、

ことを特徴とするネットワークシステム。

【０２３９】

（付記１５）

同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続された中継装置に対する経路制御方法おいて、

前記端末から第１のＡＲＰリプライフレームを受信し、

前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを前記端末ごとに保持するアドレス対応保持部から、受信した前記第１のＡＲＰリプライフレームに基づいて、対応する前記端末の前記仮想ＭＡＣアドレスを読み出して、前記仮想ＭＡＣアドレスを前記端末に応答し、

前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣアドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答する、

ことを特徴とする経路制御方法。

【０２４０】

（付記１６）

同一物理ポート配下に単一又は複数のレイヤ２スイッチが接続され、更に当該レイヤ２スイッチの配下に単一又は複数の端末が接続された中継装置に対する経路制御プログラムおいて、

前記端末から第１のＡＲＰリプライフレームを受信する処理と、

前記端末のＩＰアドレスと実ＭＡＣアドレス、及び仮想的なＭＡＣアドレスである仮想ＭＡＣアドレスとを前記端末ごとに保持するアドレス対応保持部から、対応する前記端末の前記仮想ＭＡＣアドレスを読み出して、前記仮想ＭＡＣアドレスを前記端末に応答する処理と、

前記端末間で前記仮想ＭＡＣアドレス宛ての第１のフレームが送受信されるとき、前記第１のフレームを受信して、前記第１のフレームのＭＡＣアドレスについて仮想ＭＡＣアドレスと実ＭＡＣアドレスの変換を行い、変換後の第２のフレームを応答する処理と、

をコンピュータに実行させることを特徴とする経路制御プログラム。

【図面の簡単な説明】

【０２４１】

【図１】ネットワークの構成例を示す図である。

【図２】セキュリティスイッチ等の構成例を示す図である。

【図３】ＭＡＣフレームの構成例を示す図である。

【図４】セキュリティスイッチで実行されるフローチャートの例である。

【図５】各端末で実行されるフローチャートの例である。

【図６】図６（Ａ）はアドレス対応保持部の構成例、同図（Ｂ）はレイヤ２スイッチＣ（Ｌ２ＳＷ＿Ｃ）の学習テーブルの例、同図（Ｃ）はレイヤ２スイッチＤ（Ｌ２ＳＷ＿Ｄ）の学習テーブルの例を示す図である。

【図７】図７（Ａ）は端末ＡのＡＲＰテーブルの例、同図（Ｂ）は端末ＢのＡＲＰテーブルの例を示す図である。

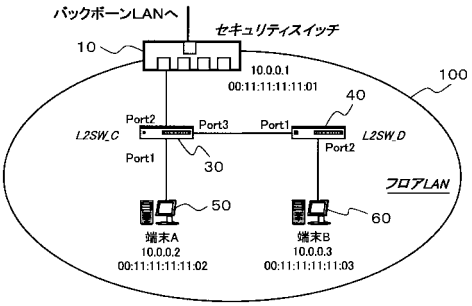
【図８】セキュリティスイッチ等の他の構成例を示す図である。

【図９】セキュリティスイッチで実行される他のフローチャートの例である。

【図１０】ネットワークの他の構成例を示す図である。

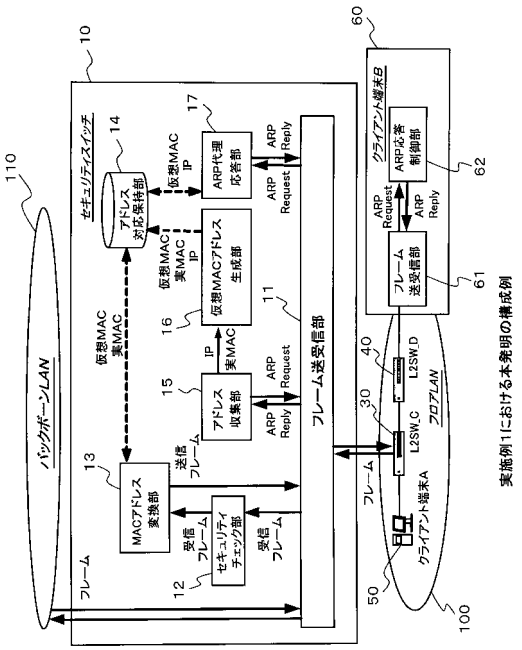
【図１１】セキュリティスイッチ等の他の構成例を示す図である。
【図１２】セキュリティスイッチで実行される他のフローチャートの例である。
【図１３】セキュリティスイッチ等の他の構成例を示す図である。
【図１４】セキュリティスイッチで実行される他のフローチャートの例である。
【図１５】セキュリティスイッチで実行される他のフローチャートの例である。
【図１６】アドレス対応保持部の他の構成例を示す図である。
【図１７】セキュリティスイッチ等の他の構成例を示す図である。
【図１８】セキュリティスイッチで実行される他のフローチャートの例である。
【図１９】端末Ｂの他の構成例を示す図である。
【図２０】ネットワークの他の構成例を示す図である。
【図２１】ログの例を示す図である。
【図２２】セキュリティスイッチで実行される他のフローチャートの例である。
【図２３】セキュリティスイッチで実行される他のフローチャートの例である。
【図２４】図２４（Ａ）は従来におけるＡＲＰ通信の例、同図（Ｂ）は従来のフロア内通信の例を示す図である。
【符号の説明】
【０２４２】
１０　セキュリティスイッチ
１１　フレーム送受信部
１２　セキュリティチェック部
１３　ＭＡＣアドレス変換部
１４　アドレス対応保持部
１５　アドレス収集部
１６　仮想ＭＡＣアドレス生成部
１７　ＡＲＰ代理応答部
１８　端末接続ポート保持部
１９　非対応端末検出部
２０　ＡＲＰ応答判断部
３０　レイヤ２スイッチＣ（Ｌ２ＳＷ＿Ｃ）
４０　レイヤ２スイッチＤ（Ｌ２ＳＷ＿Ｄ）
５０　クライアント端末Ａ
６０　クライアント端末Ｂ
６１　端末側フレーム送受信部
６２　ＡＲＰ応答制御部
６３　ＡＲＰテーブル
７０　クライアント端末Ｃ
９０　ログ採取用端末
１００　フロアＬＡＮ
１１０　バックボーンＬＡＮ

【図１】



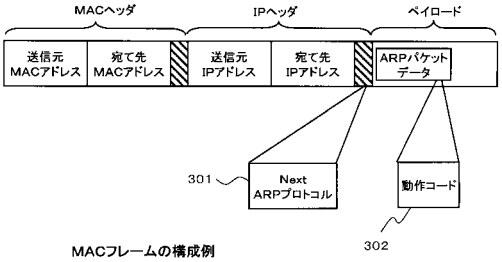
実施例1におけるネットワーク構成例

【図２】



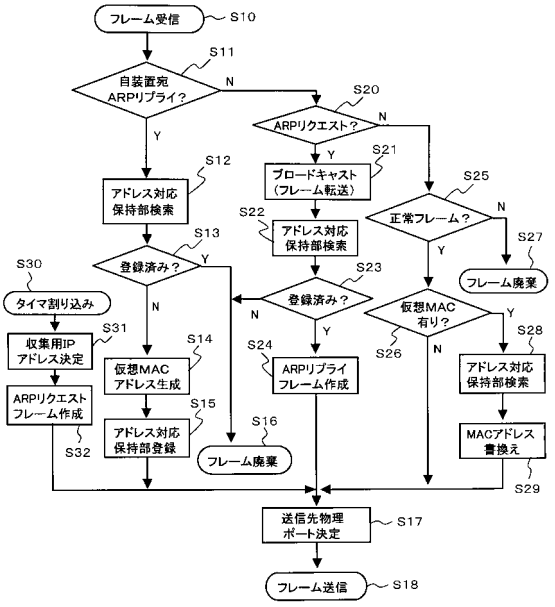
実施例1における本発明の構成例

【図３】



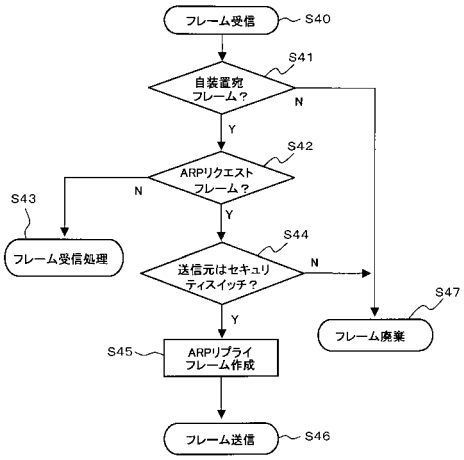
MACフレームの構成例

【図４】



実施例1におけるセキュリティスイッチのフローチャート

【図５】



各実施例における端末のフローチャート

【図６】

IPアドレス	仮想MACアドレス	実MACアドレス
10.0.0.2	02:11:11:11:11:02	00:11:11:11:11:02
10.0.0.3	02:11:11:11:11:03	00:11:11:11:11:03

(A)アドレス対応保持部の構成例

MACアドレス	Port番号
00:11:11:11:11:02	Port1
02:11:11:11:11:02	Port2
02:11:11:11:11:03	Port3
00:11:11:11:11:03	Port4

(B)L2SW_Cの学習テーブルの例

MACアドレス	Port番号
00:11:11:11:11:02	Port1
02:11:11:11:11:02	Port1
02:11:11:11:11:03	Port1
00:11:11:11:11:03	Port3

(C)L2SW_Dの学習テーブルの例

【図７】

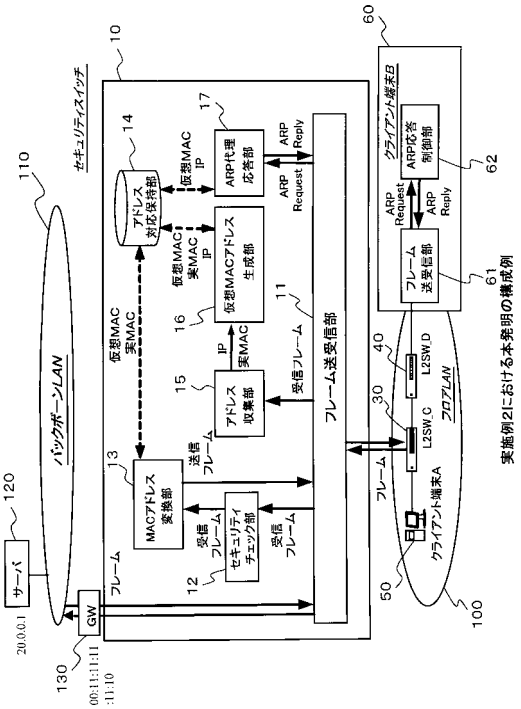
IPアドレス	MACアドレス
10.0.0.3	02:11:11:11:11:03

(A)端末AのARPテーブルの例

IPアドレス	MACアドレス
10.0.0.2	02:11:11:11:11:02

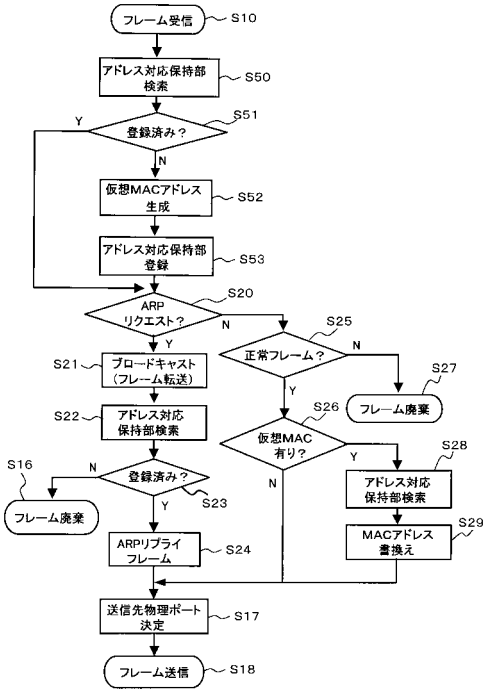
(B)端末BのARPテーブルの例

【図８】



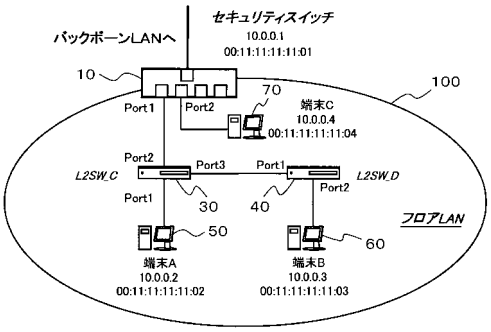
実施例2における本発明の構成例

【図９】



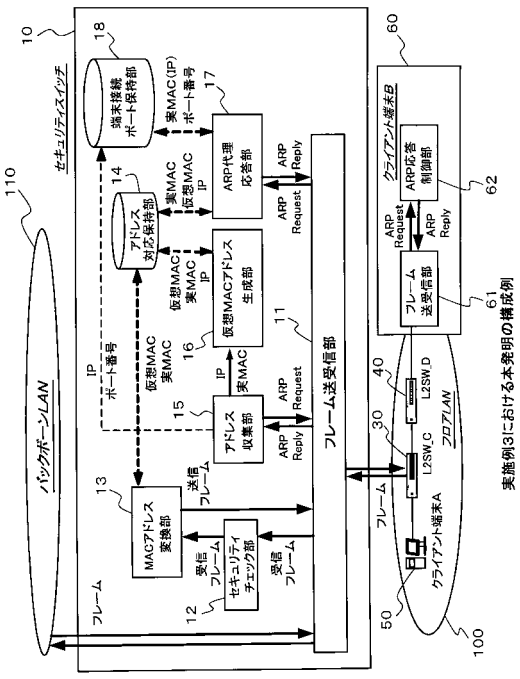
実施例2におけるセキュリティスイッチのフローチャート

【図１０】



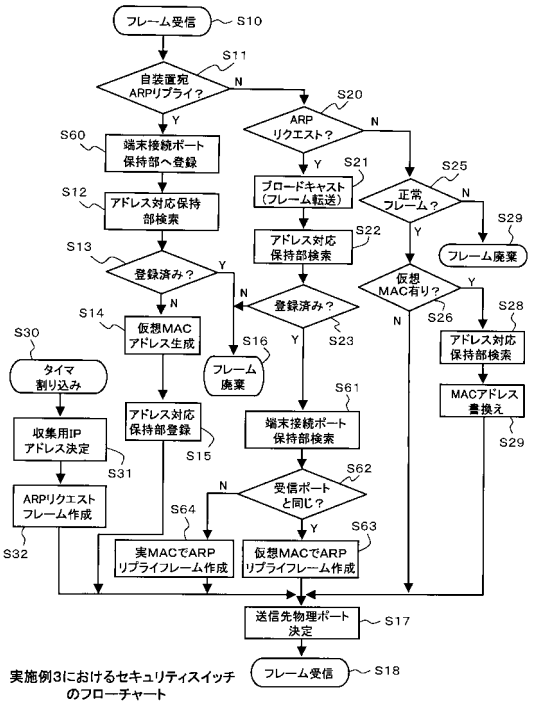
実施例3におけるネットワーク構成例

【図１１】



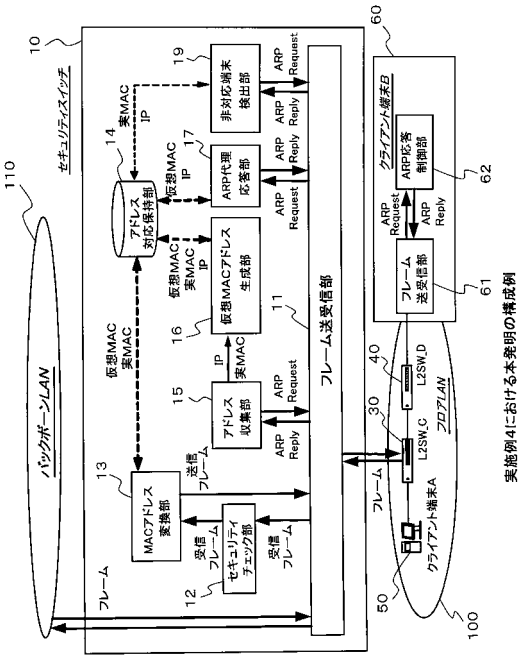
実施例3における本発明の構成例

【図１２】



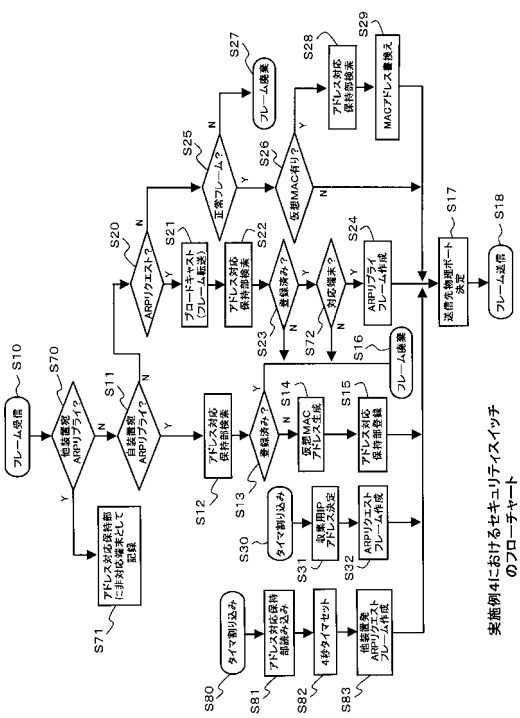
実施例3におけるセキュリティスイッチのフローチャート

【図１３】



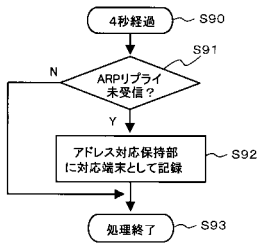
実施例4における本発明の構成例

【図１４】



実施例4におけるセキュリティスイッチのフローチャート

【図１５】



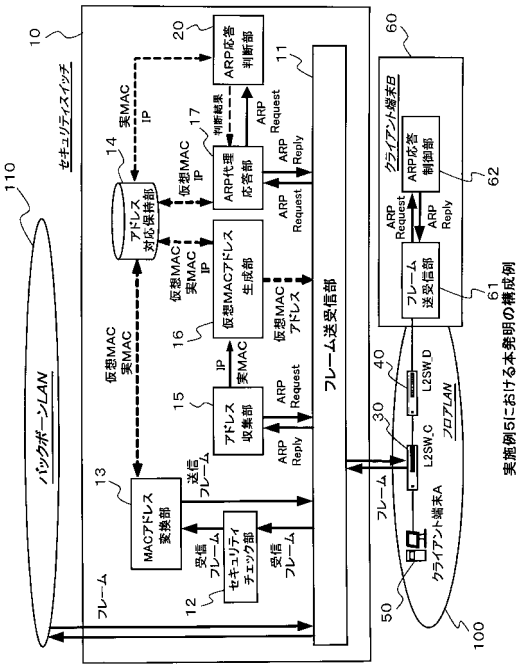
実施例4におけるセキュリティスイッチのフローチャート
（非対応端末の識別）

【図１６】

対応端末	IPアドレス	仮想MACアドレス	実MACアドレス
1	10.0.0.2	02:11:11:11:11:02	00:11:11:11:11:02
1	10.0.0.3	02:11:11:11:11:03	00:11:11:11:11:03
0	10.0.0.4	02:11:11:11:11:04	00:11:11:11:11:04

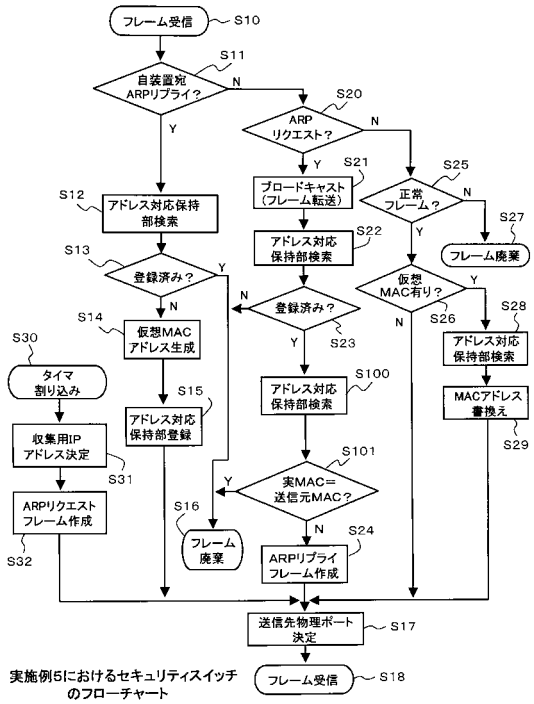
実施例4におけるアドレス対応保持部の構成例

【図１７】



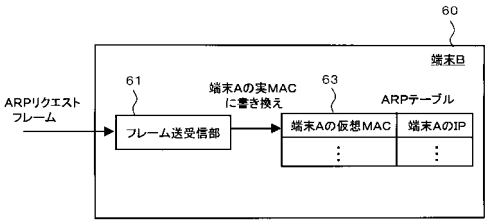
実施例5における本発明の構成例

【図１８】

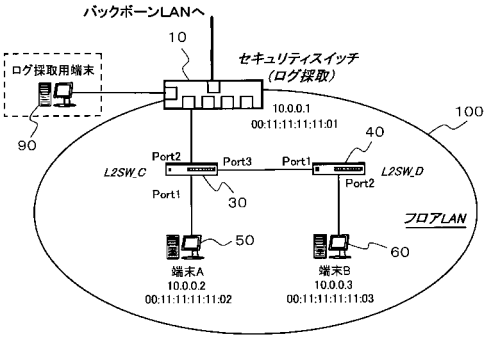


実施例5におけるセキュリティスイッチのフローチャート

【図１９】



【図２０】



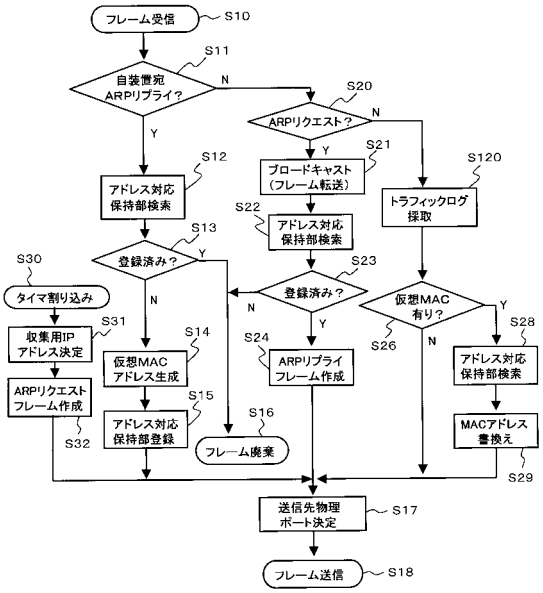
実施例7におけるネットワーク構成例

【図２１】

```
10:26:48.765497 IP 10.0.0.2.45588 > 10.0.0.3.23: . ack 2867514952 win 24820
10:26:48.765582 IP 10.0.0.3.23 > 10.0.0.2.45588: P 1:148(147) ack 0 win 5840
10:26:48:865468 IP 10.0.0.2.45588 > 10.0.0.3.23: . ack 148 win 24820
10:26:48.865532 IP 10.0.0.3.23 > 10.0.0.2.45588: P 148:325(177) ack 0 win 5840
```

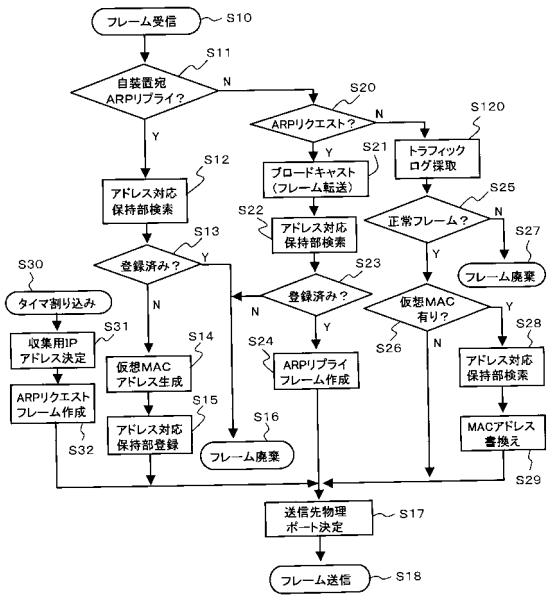
ログの例

【図２２】



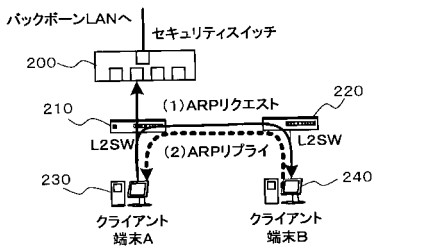
実施例7におけるセキュリティスイッチのフローチャート

【図２３】

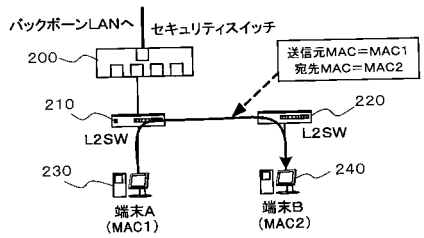


実施例7におけるセキュリティスイッチのフローチャート

【図２４】



（A） ARP通信の例



（B） 従来のフロア内通信の例

フロントページの続き

(56)参考文献 特開２００３－３１８９３４（ＪＰ，Ａ）
特開２００２－２３２４４８（ＪＰ，Ａ）
特開平０６－３１８９４５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／４４
Ｈ０４Ｌ　１２／４６