

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第3784269号
(P3784269)

(45) 発行日 平成18年6月7日(2006.6.7)

(24) 登録日 平成18年3月24日(2006.3.24)

(51) Int.C1.

F 1

HO4L 12/46 (2006.01)
HO4L 12/44 (2006.01)HO4L 12/46 V
HO4L 12/44 300
HO4L 12/44 M

請求項の数 12 (全 14 頁)

(21) 出願番号 特願2001-111109 (P2001-111109)
 (22) 出願日 平成13年4月10日 (2001.4.10)
 (65) 公開番号 特開2002-314573 (P2002-314573A)
 (43) 公開日 平成14年10月25日 (2002.10.25)
 審査請求日 平成15年10月30日 (2003.10.30)

(73) 特許権者 396008347
 アライドテレシスホールディングス株式会社
 東京都品川区西五反田7-22-17 T
 OCビル
 (74) 代理人 100104156
 弁理士 龍華 明裕
 (72) 発明者 佐藤 貴之
 東京都品川区西五反田7-22-17 T
 OCビル アライドテレシス株式会社内
 審査官 中木 努

最終頁に続く

(54) 【発明の名称】ネットワーク管理装置、ネットワーク管理プログラム、ネットワーク管理方法、及びコンピュータネットワークシステム

(57) 【特許請求の範囲】

【請求項 1】

コンピュータネットワークシステムであつて、
 ネットワークにおいて通信を行うネットワーク機器と、
 前記ネットワーク機器を管理するネットワーク管理装置と、
 前記ネットワーク機器と前記ネットワーク管理装置とを接続する中継機器と
 を備え、

前記中継機器は、前記ネットワークに前記ネットワーク機器が新たに接続された場合、
 又は前記ネットワーク機器に新たに電源が投入された場合、前記中継機器の接続ポートの
 情報に追加されたMACアドレスを前記ネットワーク管理装置に送信し、

10

前記ネットワーク管理装置は、
 前記中継機器からMACアドレスを受信することにより、新たに前記ネットワークに接
 続された前記ネットワーク機器、又は新たに電源が投入された前記ネットワーク機器を検
 出する検出部と、

前記検出部が検出した前記ネットワーク機器から、前記ネットワーク機器の利用者のユ
 ザIDを受信する受信部と、

ユーザIDとVLANグループと対応づけて予め格納するVLAN情報データベースと

、
 前記受信部が受信したユーザIDに対応づけて前記VLAN情報データベースが格納し
 ているVLANグループに対応づけて、前記中継機器から受信したMACアドレスを格納

20

するデータベース更新部と、

前記検出部が検出した前記ネットワーク機器を、前記中継機器から受信したMACアドレスに対応づけられて前記VLAN情報データベースに格納されているVLANグループに設定する設定部と

を有するコンピュータネットワークシステム。

【請求項2】

前記中継機器は、前記ネットワークに前記ネットワーク機器が新たに接続された場合、又は前記ネットワーク機器に新たに電源が投入された場合、前記中継機器の接続ポートの情報に追加されたMACアドレスを、linkupトラップで前記ネットワーク管理装置に送信する

10

請求項1に記載のコンピュータネットワークシステム。

【請求項3】

前記中継機器は、前記ネットワークから前記ネットワーク機器が取り外された場合、又は前記ネットワーク機器の電源が落とされた場合、前記中継機器の接続ポートの情報から削除されたMACアドレスを前記ネットワーク管理装置に送信し、

前記検出部は、前記中継機器からMACアドレスを受信することにより、前記ネットワークから取り外された前記ネットワーク機器、又は電源が落とされた前記ネットワーク機器をさらに検出し、

前記データベース更新部は、前記検出部が検出した前記ネットワーク機器のMACアドレスを前記VLAN情報データベースから削除し、

20

前記設定部は、前記検出部が検出した前記ネットワーク機器が接続された前記中継機器の接続ポートを、前記VLANグループのいずれにも登録されていないVLANグループであるデフォルトVLANグループに設定する

請求項1に記載のコンピュータネットワークシステム。

【請求項4】

前記中継機器は、前記ネットワークから前記ネットワーク機器が取り外された場合、又は前記ネットワーク機器の電源が落とされた場合、前記中継機器の接続ポートの情報から削除されたMACアドレスを、linkdownトラップで前記ネットワーク管理装置に送信する

請求項3に記載のコンピュータネットワークシステム。

30

【請求項5】

前記VLAN情報データベースは、ユーザID及びパスワードとVLANグループと対応づけて予め格納しており、

前記受信部は、前記検出部が検出した前記ネットワーク機器から、前記ネットワーク機器の利用者のユーザID及びパスワードを受信し、

前記データベース更新部は、前記VLAN情報データベースを参照して、前記受信部が受信したユーザID及びパスワードを認証し、認証が成立した場合に、前記受信部が受信したユーザIDに対応づけて前記VLAN情報データベースが格納しているVLANグループに対応づけて、前記中継機器から受信したMACアドレスを格納する

請求項1に記載のコンピュータネットワークシステム。

40

【請求項6】

前記ネットワーク機器は、前記ネットワーク機器の利用者に、前記ネットワーク機器を用いて前記ネットワーク管理装置にログインさせ、ユーザID及びパスワードを入力させ、

前記受信部は、前記検出部が検出した前記ネットワーク機器から、前記ネットワーク機器の利用者によって入力されたユーザID及びパスワードを受信する

請求項5に記載のコンピュータネットワークシステム。

【請求項7】

ネットワークにおいて通信を行うネットワーク機器と、前記ネットワーク機器を管理するネットワーク管理装置と、前記ネットワーク機器と前記ネットワーク管理装置とを接続

50

する中継機器とを備えるコンピュータネットワークにおけるネットワーク管理方法であつて、

前記ネットワークに前記ネットワーク機器が新たに接続された場合、又は前記ネットワーク機器に新たに電源が投入された場合、前記中継機器が、前記中継機器の接続ポートの情報に追加されたM A Cアドレスを前記ネットワーク管理装置に送信する第1の送信段階と、

前記ネットワーク管理装置が、前記中継機器からM A Cアドレスを受信することにより、新たに前記ネットワークに接続された前記ネットワーク機器、又は新たに電源が投入された前記ネットワーク機器を検出する第1の検出段階と、

前記ネットワーク管理装置が、前記第1の検出段階において検出した前記ネットワーク機器から、前記ネットワーク機器の利用者のユーザIDを受信する受信段階と、10

前記ネットワーク管理装置が、前記受信段階において受信したユーザIDに対応づけてV L A N情報データベースが予め格納しているV L A Nグループに対応づけて、前記中継機器から受信したM A Cアドレスを格納する第1のデータベース更新段階と、

前記ネットワーク管理装置が、前記第1の検出段階において検出した前記ネットワーク機器を、前記中継機器から受信したM A Cアドレスに対応づけられて前記V L A N情報データベースに格納されているV L A Nグループに設定する第1の設定段階とを備えるネットワーク管理方法。

【請求項8】

前記第1の送信段階は、前記ネットワークに前記ネットワーク機器が新たに接続された場合、又は前記ネットワーク機器に新たに電源が投入された場合、前記中継機器が、前記中継機器の接続ポートの情報に追加されたM A Cアドレスを、l i n k U pトラップで前記ネットワーク管理装置に送信する段階を有する20

請求項7に記載のネットワーク管理方法。

【請求項9】

前記中継機器が、前記ネットワークから前記ネットワーク機器が取り外された場合、又は前記ネットワーク機器の電源が落とされた場合、前記中継機器の接続ポートの情報から削除されたM A Cアドレスを前記ネットワーク管理装置に送信する第2の送信段階と、

前記ネットワーク管理装置が、前記中継機器からM A Cアドレスを受信することにより、前記ネットワークから取り外された前記ネットワーク機器、又は電源が落とされた前記ネットワーク機器を検出する第2の検出段階と、30

前記ネットワーク管理装置が、前記第2の検出段階において検出した前記ネットワーク機器のM A Cアドレスを前記V L A N情報データベースから削除する第2のデータベース更新段階と、

前記ネットワーク管理装置が、前記第2の検出段階において検出した前記ネットワーク機器が接続された前記中継機器の接続ポートを、前記V L A Nグループのいずれにも登録されていないV L A NグループであるデフォルトV L A Nグループに設定する第2の設定段階とをさらに備える請求項7に記載のネットワーク管理方法。

【請求項10】

前記第2の送信段階は、前記ネットワークから前記ネットワーク機器が取り外された場合、又は前記ネットワーク機器の電源が落とされた場合、前記中継機器が、前記中継機器の接続ポートの情報から削除されたM A Cアドレスを、l i n k D o w nトラップで前記ネットワーク管理装置に送信する段階を有する40

請求項9に記載のネットワーク管理方法。

【請求項11】

前記V L A N情報データベースは、ユーザID及びパスワードとV L A Nグループと対応づけて予め格納しており、

前記受信段階は、前記ネットワーク管理装置が、前記第1の検出段階において検出した前記ネットワーク機器から、前記ネットワーク機器の利用者のユーザID及びパスワード50

を受信する段階を有し、

前記データベース更新段階は、前記ネットワーク管理装置が、前記V L A N情報データベースを参照して、前記受信段階において受信したユーザID及びパスワードを認証し、認証が成立した場合に、前記受信段階において受信したユーザIDに対応づけて前記V L A N情報データベースが格納しているV L A Nグループに対応づけて、前記中継機器から受信したM A Cアドレスを格納する段階を有する

請求項7に記載のネットワーク管理方法。

【請求項12】

前記ネットワーク機器が、前記ネットワーク機器の利用者に、前記ネットワーク機器を用いて前記ネットワーク管理装置にログインさせ、ユーザID及びパスワードを入力させる入力段階

10

をさらに備え、

前記受信段階は、前記ネットワーク管理装置が、前記第1の検出段階において検出した前記ネットワーク機器から、前記ネットワーク機器の利用者によって入力されたユーザID及びパスワードを受信する段階を有する

請求項11に記載のネットワーク管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワーク管理装置、ネットワーク管理プログラム、ネットワーク管理方法、及びコンピュータネットワークシステムに関する。特に本発明は、効率よくV L A N設定ができ、且つセキュリティが高いM A C (Media Access Control)アドレスベースV L A N (Virtual Local Area Network)を形成するネットワーク管理装置、ネットワーク管理プログラム、ネットワーク管理方法、及びコンピュータネットワークシステムに関する。

20

【0002】

【従来の技術】

M A CアドレスベースV L A Nを構築するネットワーク管理装置又は中継機器は、M A CアドレスとV L A Nグループとが対応づけられて格納されるデータベースを有し、ネットワーク機器から受信した受信パケット内の送信元M A Cアドレスに基づいてネットワーク機器のV L A Nグループを認識し、ネットワーク機器のV L A Nグループを設定する。

30

【0003】

【発明が解決しようとする課題】

しかしながら、従来のM A CアドレスベースV L A Nを形成するコンピュータネットワークシステムにおいて、V L A Nグループの新規作成、ネットワーク機器のV L A Nグループの変更、新たなネットワーク機器のネットワークへの接続等の際、ネットワーク管理者は、M A CアドレスとV L A Nグループとが対応づけられて格納されるデータベースを更新しなければならない。

【0004】

そこで本発明は、上記の課題を解決することのできるネットワーク管理装置、ネットワーク管理プログラム、ネットワーク管理方法、及びコンピュータネットワークシステムを提供することを目的とする。この目的は特許請求の範囲における独立項に記載の特徴の組み合わせにより達成される。また従属項は本発明の更なる有利な具体例を規定する。

40

【0005】

【課題を解決するための手段】

即ち、本発明の第1の形態によると、コンピュータネットワークシステムは、ネットワークにおいて通信を行うネットワーク機器と、ネットワーク機器を管理するネットワーク管理装置とを備える。

【0006】

ネットワーク管理装置は、ネットワークに接続されたネットワーク機器の識別情報である

50

機器識別情報と、ネットワークにおいてネットワーク機器が属すべきV L A N グループとを対応づけて格納するV L A N 情報データベースと、ネットワーク機器から当該ネットワーク機器の機器識別情報を受信する受信部と、受信部が受信した機器識別情報を有するネットワーク機器が属すべきV L A N グループに対応づけて、機器識別情報をV L A N 情報データベースに格納するデータベース更新部と、機器識別情報を有するネットワーク機器を、機器識別情報に対応づけてV L A N 情報データベースに格納されるV L A N グループに設定する設定部とを有する。機器識別情報は、ネットワーク機器のM A C アドレスであつてもよい。

【 0 0 0 7 】

V L A N 情報データベースは、V L A N グループに対応づけて、ネットワーク機器の利用者識別情報である利用者識別情報をさらに格納し、受信部は、ネットワーク機器から利用者識別情報をさらに受信し、データベース更新部は、受信部が受信した利用者識別情報がV L A N 情報データベースに格納されている場合、利用者識別情報及びV L A N グループに対応づけて、機器識別情報をV L A N 情報データベースに格納してもよい。10

【 0 0 0 8 】

受信部は、V L A N グループのいずれにも登録されていないV L A N グループであるデフォルトV L A N グループに属するネットワーク機器から当該ネットワーク機器の機器識別情報を受信し、設定部は、受信部が受信した機器識別情報が、V L A N 情報データベースに格納されている場合、デフォルトV L A N グループに属するネットワーク機器を、機器識別情報に対応づけてV L A N 情報データベースに格納されるV L A N グループに設定してもよい。20

【 0 0 0 9 】

V L A N 情報データベースは、V L A N グループに対応づけて、ネットワーク機器の利用者識別情報である利用者識別情報をさらに格納し、受信部は、受信した機器識別情報がV L A N 情報データベースに格納されていない場合、デフォルトV L A N グループに属するネットワーク機器から利用者識別情報をさらに受信し、データベース更新部は、受信部が受信した利用者識別情報がV L A N 情報データベースに格納されている場合、利用者識別情報及びV L A N グループに対応づけて、受信部が受信した機器識別情報をV L A N 情報データベースに格納し、設定部は、デフォルトV L A N グループに属するネットワーク機器を、当該ネットワーク機器の機器識別情報に対応づけてV L A N 情報データベースに格納されるV L A N グループに設定してもよい。30

【 0 0 1 0 】

ネットワーク管理装置は、新たにネットワークに接続されたネットワーク機器、又は新たに電源が投入されたネットワーク機器を検出する検出部をさらに備え、受信部は、検出部によって検出されたネットワーク機器から当該ネットワーク機器の機器識別情報を受信してもよい。

【 0 0 1 1 】

検出部は、ネットワークから取り外されたネットワーク機器、又は電源が落とされたネットワーク機器をさらに検出し、データベース更新部は、検出部によって検出されたネットワーク機器が有する機器識別情報をV L A N 情報データベースから削除してもよい。40

【 0 0 1 2 】

検出部がネットワークから取り外されたネットワーク機器、又は電源が落とされたネットワーク機器を検出してから所定の時間が経過した後、データベース更新部は、検出部によって検出されたネットワーク機器が有する機器識別情報をV L A N 情報データベースから削除してもよい。

【 0 0 1 3 】

ネットワーク管理装置とネットワーク機器とを接続する中継機器をさらに備え、設定部は、検出部によって検出されたネットワーク機器が接続された中継機器の接続ポートを、V L A N グループのいずれにも登録されていないV L A N グループであるデフォルトV L A N グループに設定してもよい。

【0014】

ネットワーク管理装置は、デフォルトVLANグループに属しており、受信部は、デフォルトVLANグループの設定された接続ポートに接続されることによってデフォルトVLANグループに属したネットワーク機器から当該ネットワーク機器の機器識別情報を受信してもよい。

【0015】

なお上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではなく、これらの特徴群のサブコンビネーションも又発明となりうる。

【0016】**【発明の実施の形態】**

以下、発明の実施形態を通じて本発明を説明するが、実施形態はクレームにかかる発明を限定するものではなく、また実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

【0017】

図1は、本発明の一実施形態に係るコンピュータネットワークシステムの構成を示す。本実施形態に係るコンピュータネットワークシステムは、ネットワークにおいて通信を行うネットワーク機器14a、14b、14c、及び14dと、ネットワーク機器14a、14b、14c、及び14dを管理するネットワーク管理装置10と、ネットワーク機器14a、14b、14c、及び14dとネットワーク管理装置10とを接続する中継機器12a、12b、及び12cとを備える。

【0018】

ネットワーク管理装置10は、ネットワーク機器14a、14b、14c、及び14dからそれぞれのMACアドレスを受信する。なお、MACアドレスは、ネットワーク機器の識別情報である機器識別情報の一例である。そして、ネットワーク管理装置10は、受信したMACアドレスに基づいて、ネットワーク機器14a、14b、14c、及び14dのVLANグループを設定する。このとき、ネットワーク管理装置10は、ネットワーク機器14a、14b、14c、及び14dが接続された中継機器12b及び12cの接続ポート16c、16d、16e、及び16fを、ネットワーク機器14a、14b、14c、及び14dのそれぞれが属すべきVLANグループに設定することにより、ネットワーク機器14a、14b、14c、及び14dがそれぞれのVLANにおいて通信することを可能にする。

【0019】

中継機器12b及び12cは、ネットワーク機器14a、14b、14c、及び14dと無線で通信を行う無線中継機器であってもよい。無線中継機器により構成されたコンピュータネットワークシステムにおいて、MACアドレスベースVLANを形成することにより、ネットワーク機器は、ネットワーク機器の使用場所を移動された場合においても、ネットワーク機器の設定が変更されることなく、所定のVLANグループにおける通信が可能である。

【0020】

また、ネットワーク管理装置10は、中継機器12b及び12cからそれぞれのMACアドレスを受信し、受信したMACアドレスに基づいて、中継機器12b及び12cのVLANグループを設定する。このとき、ネットワーク管理装置10は、中継機器12b及び12cのそれぞれが接続された中継機器12aの接続ポート16a及び16bを、中継機器12b及び12cのそれぞれが属すべきVLANグループに設定することにより、中継機器12b及び12cがそれぞれのVLANにおいて通信することを可能にする。

【0021】

また、ネットワーク管理装置10は、中継機器12aの接続ポート16aを複数のVLANグループに設定することにより、中継機器12bが複数のVLANにおいて通信することを可能にしてもよい。例えば、ネットワーク管理装置10は、中継機器12aの接続ポート16aをVLAN1及びVLAN2において通信できるように設定することにより、

10

20

30

40

50

中継機器 12 b に接続されたネットワーク機器 14 a 及び 14 b が VLAN 1 又は VLAN 2 において通信することを可能とする。

【0022】

また、本実施形態によるコンピュータネットワークシステムは、イーサネットフレームに VLAN を識別するタグを付加し、タグの情報に基づいて VLAN を分割するタギング VLAN、又は任意の接続ポートを複数の VLAN グループに所属させるマルチプル VLAN を、本実施形態の MAC アドレスベース VLAN と組み合わせて用いてもよい。

【0023】

また、ネットワーク管理装置 10 は、中継機器 12 a の接続ポート 16 a 及び 16 b に VLAN グループを設定するポートベース VLAN により、中継機器 12 b 及び 12 c の VLAN グループを設定し、MAC アドレスベース VLAN により、中継機器 12 b にネットワーク機器 14 a 及び 14 b の VLAN グループを設定し、中継機器 12 c にネットワーク機器 14 c 及び 14 d の VLAN グループを設定してもよい。10

【0024】

本実施形態のコンピュータネットワークシステムによれば、ポートベース VLAN と、本実施形態による MAC アドレスベース VLAN とを組み合わせてネットワークを構築することにより、より柔軟性のあるネットワークを構築することができる。

【0025】

図 2 は、本実施形態に係るネットワーク管理装置 10 の構成を示す。ネットワーク管理装置 10 は、ネットワーク機器の MAC アドレスと VLAN グループとを対応づけて格納する VLAN 情報データベース 100 と、ネットワーク機器から当該ネットワーク機器の MAC アドレスを受信する受信部 102 と、受信部 102 が受信した MAC アドレスを VLAN 情報データベース 100 に格納するデータベース更新部 104 と、VLAN 情報データベース 100 に格納された情報に基づいてネットワーク機器を所望の VLAN グループに設定する設定部 106 と、新たにネットワークに接続されたネットワーク機器を検出する検出部 108 とを備える。20

【0026】

検出部 108 は、新たにネットワークに接続されたネットワーク機器、又は新たに電源が投入されたネットワーク機器を検出する。そして、受信部 102 は、検出部 108 によって検出されたネットワーク機器から当該ネットワーク機器の MAC アドレスを受信する。30 そして、データベース更新部 104 は、受信部 102 が受信した MAC アドレスを有するネットワーク機器が属すべき VLAN グループに対応づけて、当該 MAC アドレスを VLAN 情報データベース 100 に格納する。そして、設定部 106 は、MAC アドレスに対応づけて VLAN 情報データベース 100 に格納される VLAN グループに、当該 MAC アドレスを有するネットワーク機器を設定する。

【0027】

また、検出部 108 は、ネットワークから取り外されたネットワーク機器、又は電源が落とされたネットワーク機器を検出する。そして、データベース更新部 104 は、検出部 108 によって検出されたネットワーク機器が有する MAC アドレスを VLAN 情報データベース 100 から削除する。40 そして、設定部 106 は、検出部 108 によって検出されたネットワーク機器が接続された中継機器の接続ポートを、VLAN グループのいずれにも登録されていない VLAN グループであるデフォルト VLAN グループに設定する。また、検出部 108 がネットワークから取り外されたネットワーク機器、又は電源が落とされたネットワーク機器を検出してから所定の時間が経過した後、データベース更新部 104 は、検出部 108 によって検出されたネットワーク機器が有する MAC アドレスを VLAN 情報データベース 100 から削除してもよい。また、VLAN 情報データベース 100 は、検出によって検出されたネットワーク機器が有する MAC アドレスを、デフォルト LAN グループに対応づけて格納してもよい。

【0028】

本実施形態のネットワーク管理装置 10 によれば、受信部 102 がネットワーク機器から

50

20

30

40

50

受信したMACアドレスが、データベース更新部104によってVLAN情報データベース100に登録されるため、ネットワーク管理者は、VLAN情報データベース100にネットワーク機器のMACアドレスを予め登録することなく、簡易にMACアドレスベースVLANを形成することができる。また、ネットワークから取り外されたネットワーク機器、又は電源が落とされたネットワーク機器のMACアドレスをVLAN情報データベース100から削除し、当該ネットワーク機器をデフォルトVLANグループに設定することによって、VLANへの不正な進入を防ぐことができる。

【0029】

図3は、VLAN情報データベース100に格納されるVLAN情報ファイルのデータフォーマットを示す。VLAN情報ファイルは、VLANグループ、ユーザID、パスワード、及びMACアドレスのフィールドを有する。VLANグループフィールドは、VLANの種類を識別する情報を格納する。ユーザIDフィールドは、ネットワーク機器の利用者の識別情報である利用者識別情報を格納する。パスワードフィールドは、利用者識別情報で識別される利用者を認証するためのパスワードを格納する。MACアドレスフィールドは、それぞれのVLANグループに属すべきネットワーク機器のMACアドレスを格納する。

【0030】

ユーザIDフィールドに格納される利用者識別情報、及びパスワードフィールドに格納されるパスワードは、ネットワーク機器の利用者又はネットワーク管理者によって予め登録される。そして、MACアドレスフィールドに格納されるMACアドレスは、ネットワークを介して受信部102がネットワーク機器から受信したMACアドレスが格納される。ネットワーク機器の利用者は、ネットワーク機器を用いてネットワーク管理装置10にログインし、ユーザID及びパスワードを入力する。そして、データベース更新部104は、入力されたユーザID及びパスワードを、ユーザIDフィールドに格納される利用者識別情報、及びパスワードフィールドに格納されるパスワードによって認証した後、受信部102が受信したMACアドレスを格納する。

【0031】

また、ネットワークを介してネットワーク管理装置10にログインし、ユーザID及びパスワードをネットワーク管理装置10に送信することができないネットワーク機器の場合、当該ネットワーク機器のMACアドレスを所望のVLANグループに対応づけて予めVLAN情報データベース100のVLAN情報ファイルに登録してもよい。設定部106は、MACアドレスフィールドに格納されるMACアドレスを有するネットワーク機器を、VLANグループフィールドに格納されるVLANグループに設定する。

【0032】

本実施形態のネットワーク管理装置10によれば、ネットワーク機器において入力されたユーザID及びパスワードを、予め登録されたユーザID及びパスワードを用いて認証し、認証されたネットワーク機器が有するMACアドレスを登録することができる。そのため、ネットワーク管理者は、複雑な文字列であるMACアドレスをVLAN情報データベース100に登録する代わりに、ユーザID及びパスワードを登録することによって、MACアドレスベースVLANを形成することができる。

【0033】

図4は、ネットワーク管理装置10におけるVLAN設定処理のフローチャートを示す。まず、検出部108は、新たにネットワークに接続されたネットワーク機器、又は新たに電源が投入されたネットワーク機器を検出する(S100)。具体的には、検出部108は、中継機器からのLinkUpトラップに基づいて、中継機器の接続ポートの情報を受信し、新たにネットワークに接続されたネットワーク機器、又は新たに電源が投入されたネットワーク機器を検出する。

【0034】

また、中継機器は、接続ポートの情報にネットワーク機器のMACアドレスが追加された場合、追加されたMACアドレスをネットワーク管理装置10に送信してもよい。そして

10

20

20

30

30

40

40

50

、検出部108は、中継機器からMACアドレスを受信することにより、新たにネットワークに接続されたネットワーク機器、又は新たに電源が投入されたネットワーク機器を検出する。

【0035】

なお、中継機器の通信が行われていない接続ポートは、デフォルトVLANグループに設定されているため、新たにネットワークに接続されたネットワーク機器、又は新たに電源が投入されたネットワーク機器は、まずデフォルトVLANグループに設定され、ネットワーク管理装置10と通信を行う。次に、受信部102は、デフォルトVLANグループに設定されており、検出部108によって検出されたネットワーク機器から、当該ネットワーク機器のMACアドレスを受信する(S102)。

10

【0036】

次に、データベース更新部104は、VLAN情報データベース100を参照し(S104)、受信部102が受信したMACアドレスがVLAN情報データベース100に格納されているか否かを判断する(S106)。S106において、データベース更新部104が、受信部102が受信したMACアドレスがVLAN情報データベース100に格納されていると判断した場合、設定部106は、デフォルトVLANグループに属するネットワーク機器を、受信部102が受信したMACアドレスに対応づけてVLAN情報データベース100に格納されるVLANグループに設定する(S116)。

【0037】

また、S106において、データベース更新部104が、受信部102が受信したMACアドレスがVLAN情報データベース100に格納されていないと判断した場合、受信部102は、デフォルトVLANグループに属するネットワーク機器から、当該ネットワーク機器の利用者のユーザID及びパスワードを受信する(S108)。次に、データベース更新部104は、VLAN情報データベース100を参照し(S110)、受信部102が受信したユーザID及びパスワードを認証する(S112)。S112において、ユーザID及びパスワードの認証が成立しなかった場合、設定部106は、デフォルトVLANグループに属するネットワーク機器のVLAN設定を変更しない。

20

【0038】

また、S112において、ユーザID及びパスワードの認証が成立した場合、データベース更新部104は、受信部102が受信したユーザID及びパスワードに対応づけて、受信部102が受信したMACアドレスをVLAN情報データベース100に格納する(S114)。次に、設定部106は、デフォルトVLANグループに属するネットワーク機器を、受信部102が受信したユーザID及びパスワードに対応づけてVLAN情報データベース100に格納されるVLANグループに設定する(S116)。

30

【0039】

図5は、ネットワーク管理装置10におけるデフォルトVLAN設定処理のフローチャートを示す。まず、検出部108は、ネットワークから取り外されたネットワーク機器、又は電源が落とされたネットワーク機器を検出する(S200)。具体的には、検出部108は、中継機器からのLink Downトラップに基づいて、中継機器の接続ポートの情報を受信し、ネットワークから取り外されたネットワーク機器、又は電源が落とされたネットワーク機器を検出する。

40

【0040】

また、中継機器は、接続ポートの情報をからネットワーク機器のMACアドレスが削除された場合、削除されたMACアドレスをネットワーク管理装置10に送信してもよい。そして、検出部108は、中継機器からMACアドレスを受信することにより、ネットワークから取り外されたネットワーク機器、又は電源が落とされたネットワーク機器を検出する。

【0041】

次に、受信部102は、検出部108によって検出されたネットワーク機器が接続された中継機器から、当該ネットワーク機器のMACアドレスを受信する(S202)。そして

50

、受信部 102 が受信した MAC アドレスを有するネットワーク機器からの通信が停止してから所定の時間が経過した場合 (S204) 、データベース更新部 104 は、受信部 102 が受信した MAC アドレスを VLAN 情報データベース 100 から削除する (S206)。次に、設定部 106 は、検出部 108 によって検出されたネットワーク機器が接続された中継機器の接続ポートをデフォルト VLAN グループに設定する (S208)。

【0042】

また、他の例では、ネットワーク機器が VLAN において通信が可能な有効期限が予め定められており、データベース更新部 104 は、予め定められた有効期限が経過したネットワーク機器の MAC アドレスを VLAN 情報データベース 100 から削除してもよい。また、ネットワーク機器の利用者が登録削除の申請を行うことによって、ネットワーク管理者が、登録削除の申請が行われたネットワーク機器の MAC アドレスを VLAN 情報データベース 100 から削除してもよい。

10

【0043】

本実施形態のネットワーク管理装置 10 によれば、ネットワーク機器の利用者を認証し、認証された利用者のネットワーク機器の MAC アドレスを VLAN 情報データベース 100 に登録するため、セキュリティの高い MAC アドレスベース VLAN を形成することができる。また、通信を行っていないネットワーク機器の MAC アドレスを VLAN 情報データベース 100 から削除し、通信が行われていない中継機器の接続ポートをデフォルト VLAN グループに設定することにより、不正な利用者による VLAN への進入を防ぐことができる。

20

【0044】

図 6 は、ネットワーク管理装置 10 のハードウェア構成を示す。ネットワーク管理装置 10 は、CPU 700 と、ROM 702 と、RAM 704 と、通信インターフェース 706 と、ハードディスクドライブ 708 と、データベースインターフェース 710 と、フロッピーディスクドライブ 712 と、CD-ROM ドライブ 714 を備える。CPU 700 は、ROM 702 及び RAM 704 に格納されたプログラムに基づいて動作する。通信インターフェース 706 は、ネットワークを介してネットワーク管理装置と通信する。データベースインターフェース 710 は、データベースへのデータの書き込み、及びデータベースの内容の更新を行う。格納装置の一例としてのハードディスクドライブ 708 は、設定情報及び CPU 700 が動作するプログラムを格納する。

30

【0045】

フロッピーディスクドライブ 712 はフロッピーディスク 720 からデータまたはプログラムを読み取り CPU 700 に提供する。CD-ROM ドライブ 714 は CD-ROM 722 からデータまたはプログラムを読み取り CPU 700 に提供する。通信インターフェース 706 は、ネットワーク管理装置に接続してデータを送受信する。データベースインターフェース 710 は、各種データベース 724 と接続してデータを送受信する。

【0046】

CPU 700 が実行するソフトウェアは、フロッピーディスク 720 または CD-ROM 722 等の記録媒体に格納されて利用者に提供される。記録媒体に格納されたソフトウェアは圧縮されていても非圧縮であってもよい。ソフトウェアは記録媒体からハードディスクドライブ 708 にインストールされ、RAM 704 に読み出されて CPU 700 により実行される。

40

【0047】

記録媒体に格納されて提供されるソフトウェア、即ちハードディスクドライブ 708 にインストールされるソフトウェアは、機能構成として、受信モジュールと、検出モジュールと、記憶モジュールと、データベース更新モジュールと、設定モジュールとを有する。各モジュールがコンピュータに働きかけて、CPU 700 に行わせる処理は、それぞれ本実施形態のネットワーク管理装置 10 における、対応する部材の機能及び動作と同一であるから、説明を省略する。

【0048】

50

図6に示した、記録媒体の一例としてのフロッピーディスク720またはCD-ROM722には、本出願で説明した全ての実施形態におけるネットワーク管理装置10の動作の一部または全ての機能を格納することができる。

【0049】

これらのプログラムは記録媒体から直接RAMに読み出されて実行されても、一旦ハードディスクドライブにインストールされた後にRAMに読み出されて実行されてもよい。更に、上記プログラムは単一の記録媒体に格納されても複数の記録媒体に格納されてもよい。又、符号化した形態で格納されていてもよい。

【0050】

記録媒体としては、フロッピーディスク、CD-ROMの他にも、DVD、PD等の光学記録媒体、MD等の光磁気記録媒体、テープ媒体、磁気記録媒体、ICカードやミニチューアーカードなどの半導体メモリ等を用いることができる。又、専用通信ネットワークやインターネットに接続されたサーバシステムに設けたハードディスクまたはRAM等の格納装置を記録媒体として使用し、通信網を介してプログラムをネットワーク管理装置10に提供してもよい。このような記録媒体は、ネットワーク管理装置10を製造するためのみに使用されるものであり、そのような記録媒体の業としての製造および販売等が本出願に基づく特許権の侵害を構成することは明らかである。10

【0051】

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施形態に記載の範囲には限定されない。上記実施形態に、多様な変更または改良を加えることができる。そのような変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。20

【0052】

【発明の効果】

上記説明から明らかなように、本発明によれば、ネットワーク管理者がMACアドレスを設定することなく、効率よくVLAN設定ができ、且つセキュリティが高いMACアドレスベースVLANを形成するネットワーク管理装置、ネットワーク管理プログラム、ネットワーク管理方法、及びコンピュータネットワークシステムを提供することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るコンピュータネットワークシステムの構成図である。30

【図2】本実施形態に係るネットワーク管理装置10の構成図である。

【図3】VLAN情報データベース100に格納されるVLAN情報ファイルのデータフォーマットを示す。

【図4】ネットワーク管理装置10におけるVLAN設定処理のフローチャートである。

【図5】ネットワーク管理装置10におけるデフォルトVLAN設定処理のフローチャートである。

【図6】ネットワーク管理装置10のハードウェア構成図である。

【符号の説明】

10 ネットワーク管理装置

12a～12c 中継機器

14a～14d ネットワーク機器

16a～16f 接続ポート

100 VLAN情報データベース

102 受信部

104 データベース更新部

106 設定部

108 検出部

700 CPU

702 ROM

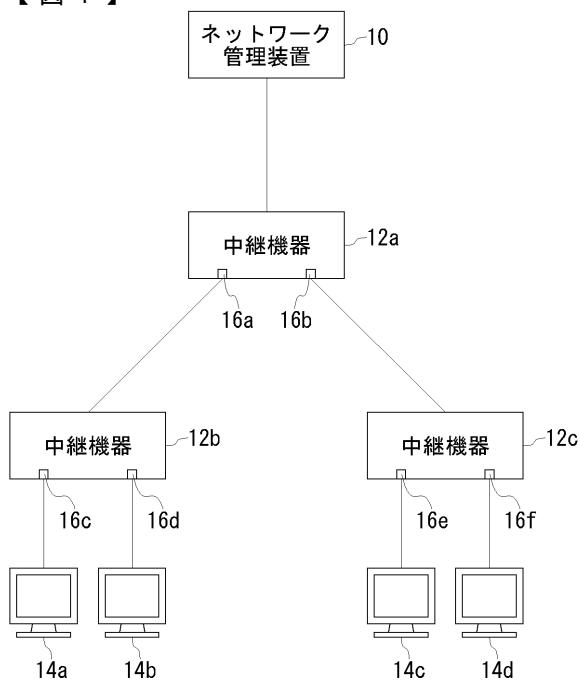
704 RAM

40

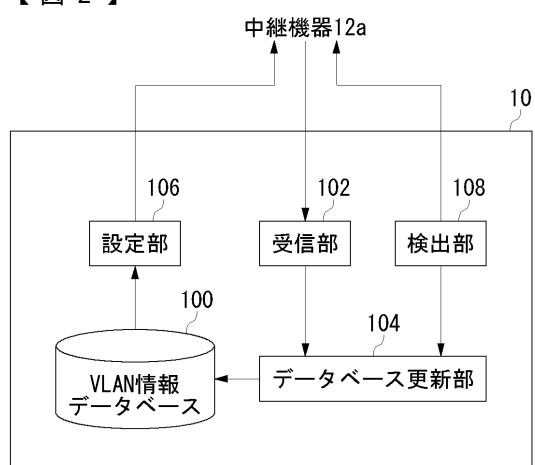
50

7 0 6 通信インターフェース
 7 0 8 ハードディスクドライブ
 7 1 0 データベースインターフェース
 7 1 2 フロッピーディスクドライブ
 7 1 4 C D - R O M ドライブ
 7 2 0 フロッピーディスク
 7 2 2 C D - R O M
 7 2 4 各種データベース

【図1】



【図2】

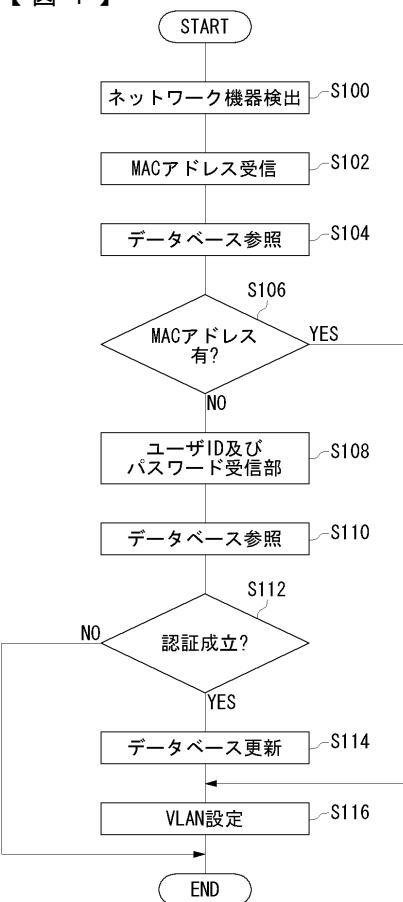


【図3】

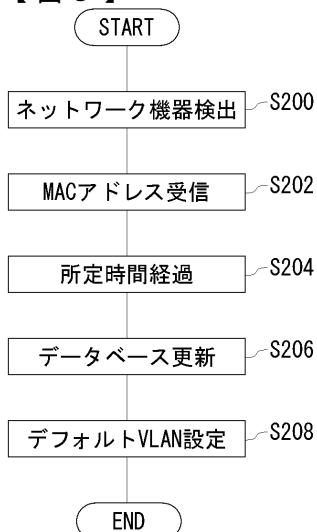
100

VLANグループ	ユーザID	パスワード	MACアドレス
VLAN1	aaaaa	*****	50-22-37-AB-66-83
	bbbbbb	*****	
			33-51-86-CD-76-10
	⋮	⋮	⋮
VLAN2	ddddd	*****	
			55-01-27-EF-60-11
	fffff	*****	61-00-10-GF-51-20
	⋮	⋮	⋮
VLAN3	ggggg	*****	53-11-02-HI-12-35
	hhhhh	*****	
	iiiii	*****	
	⋮	⋮	⋮
⋮	⋮	⋮	⋮

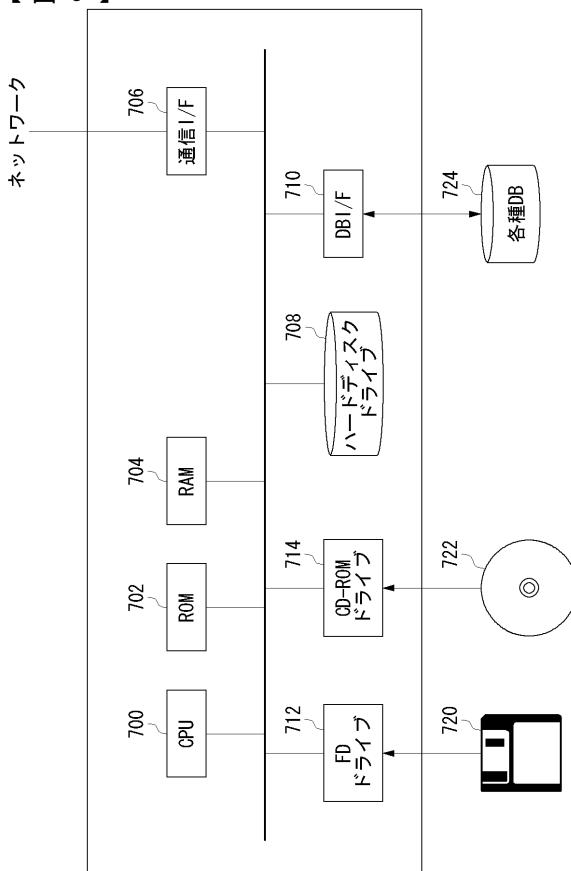
【図4】



【図5】



【図6】



フロントページの続き

(56)参考文献 特開平09-130421(JP,A)
特開2000-134207(JP,A)
特開2002-135282(JP,A)

(58)調査した分野(Int.Cl., DB名)

H04L 12/28-46