(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5364671号
(P5364671)

(45)発行日　平成25年12月11日(2013.12.11)　(24)登録日　平成25年9月13日(2013.9.13)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675D
H04L 12/58	(2006.01)	H04L	12/58	100F
G06F 21/44	(2013.01)	G06F	21/20	144C

請求項の数 7　(全 17 頁)

(21)出願番号　特願2010-225111 (P2010-225111)
(22)出願日　平成22年10月4日 (2010.10.4)
(65)公開番号　特開2012-80418 (P2012-80418A)
(43)公開日　平成24年4月19日 (2012.4.19)
審査請求日　平成24年9月13日 (2012.9.13)

前置審査

(73)特許権者　504411166
アラクサラネットワークス株式会社
神奈川県川崎市幸区鹿島田一丁目１番２号
(74)代理人　110000028
特許業務法人明成国際特許事務所
(72)発明者　樋口　秀光
神奈川県川崎市幸区鹿島田８９０　アラクサラネットワークス株式会社内
(72)発明者　能見　元英
神奈川県川崎市幸区鹿島田８９０　アラクサラネットワークス株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】ネットワーク認証における端末接続状態管理

(57)【特許請求の範囲】
【請求項１】
ＤＨＣＰサーバにネットワークを介して接続されるネットワーク中継装置であって、
通信データを送受信する通信部と、
前記ネットワーク中継装置と接続された端末装置による特定のネットワークへの接続の可否を判定するＷｅｂ認証の結果に従い認証済み端末装置を特定する第１の情報を作成し、前記第１の情報に基づき端末装置と前記特定のネットワーク上のノードとの間の通信データの前記通信部による中継の可否を管理する認証処理部と、
前記通信部により中継される端末装置と前記ＤＨＣＰサーバとの間のＤＨＣＰ通信データをスヌーピングし、前記ＤＨＣＰ通信データに基づき、各端末装置に割り当てられたレイヤ３アドレスを特定する第２の情報を作成するＤＨＣＰスヌーピング処理部と、
前記第１の情報に基づき認証済み端末装置を特定し、前記第２の情報に基づき前記特定された認証済み端末装置に割り当てられたレイヤ３アドレスを特定し、前記通信部に、前記特定された認証済み端末装置が前記特定のネットワークに接続されているか否かを確認する確認通信データを前記特定されたレイヤ３アドレス宛に送信させ、さらに、前記認証処理部に、前記確認の結果に基づいて前記可否を更新させる端末検索処理部と、を備える、ネットワーク中継装置。
【請求項２】
請求項１に記載のネットワーク中継装置であって、
前記端末検索処理部は、所定回数の前記確認通信データの送信に対して前記特定された

認証済み端末装置からの応答が無い場合には、前記認証処理部に、前記特定された認証済み端末装置についての認証を解除させる、ネットワーク中継装置。
【請求項３】
請求項１または請求項２に記載のネットワーク中継装置であって、
前記端末検索処理部は、前記第１の情報と前記第２の情報とに基づき、各認証済み端末装置について割り当てられたレイヤ３アドレスを特定する第３の情報を作成し、前記第３の情報に登録された認証済み端末装置を順に前記特定のネットワークに接続されているか否かの確認対象として選択する、ネットワーク中継装置。
【請求項４】
請求項３に記載のネットワーク中継装置であって、
前記端末検索処理部は、前記Ｗｅｂ認証によって端末装置が認証された際に認証済み端末装置を前記第３の情報に登録すると共に、前記確認対象として選択された認証済み端末装置について、前記第３の情報にレイヤ３アドレスが登録されていない場合、または、前記第３の情報に登録されたレイヤ３アドレスが前記第２の情報に登録されたレイヤ３アドレスと異なる場合には、前記第２の情報に登録されたレイヤ３アドレスを前記第３の情報に登録する、ネットワーク中継装置。
【請求項５】
請求項４に記載のネットワーク中継装置であって、
前記端末検索処理部は、前記確認対象として選択された認証済み端末装置について、前記第３の情報に登録された認証済み端末装置とレイヤ３アドレスとの対応関係と同一の対応関係が前記第２の情報には登録されておらず、かつ、前記第２の情報に認証済み端末装置と他のレイヤ３アドレスとの対応関係が登録されている場合には、前記選択された認証済み端末装置は前記特定のネットワークから一端離脱した後に再接続したものと判定する、ネットワーク中継装置。
【請求項６】
請求項１ないし請求項５のいずれかに記載のネットワーク中継装置であって、さらに、
端末装置に認証前のＶＬＡＮと認証後のＶＬＡＮとが必ずしも一致しないようにＶＬＡＮを設定するＶＬＡＮ設定部を備える、ネットワーク中継装置。
【請求項７】
請求項１ないし請求項６のいずれかに記載のネットワーク中継装置であって、
前記第１の情報と前記第２の情報と前記第３の情報とは、レイヤ２アドレスにより端末装置を特定する、ネットワーク中継装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワーク認証に関し、特に、ネットワーク認証済み端末装置のネットワーク接続状態の管理に関する。
【背景技術】
【０００２】
通信ネットワークのインフラ化とともに、ネットワークにおけるセキュリティを高めるための様々な仕組みが提案されている。ネットワーク認証もその内の１つである。ネットワーク認証は、パーソナルコンピュータ（ＰＣ）等の端末装置による特定のネットワークへの接続可否を管理するための認証の仕組みである（例えば特許文献１参照）。
【０００３】
ネットワーク認証としては、例えば、Ｗｅｂ認証やＩＥＥＥ８０２．１Ｘ認証が知られている。Ｗｅｂ認証は、Ｗｅｂブラウザが動作する端末装置からＷｅｂ認証機能を有するスイッチ等のネットワーク中継装置に対して発行される認証要求に応じて、認証サーバが端末装置の認証情報に基づき認証を行う認証方式である。Ｗｅｂ認証では、ネットワーク中継装置が、認証済み端末装置のＭＡＣアドレスやユーザＩＤ、ＶＬＡＮ情報等を認証済み端末登録テーブルに登録し、当該テーブルを参照して、端末装置とネットワーク上のノ

ード間の通信データの中継可否を判定する。Ｗｅｂ認証は、端末装置がＩＥＥＥ８０２．１Ｘ認証で使用されるような特別な認証用ソフトウェアを備えていなくてもＷｅｂブラウザさえ備えていれば実現可能であるため、汎用性の高い認証方式である。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２００３－３４８１１４号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

Ｗｅｂ認証では、ＩＥＥＥ８０２．１Ｘ認証のようなプロトコルが確立された認証方式と異なり、認証済み端末装置のネットワーク接続状態を管理する技術が知られていない。例えば、Ｗｅｂ認証では、認証済み端末装置がネットワークから離脱したことを迅速に検知する技術が確立されていない。認証済み端末装置がネットワークから離脱したことを迅速に検知できないと、認証済み端末装置がネットワークから離脱した後に、ＭＡＣアドレスを詐称した他の端末装置によるネットワークへの接続を許してしまう場合があり、セキュリティの点で向上の余地があった。

【０００６】

本発明は、上記の課題を解決するためになされたものであり、Ｗｅｂ認証における端末接続状態を管理してネットワークにおけるセキュリティを向上させることを目的とする。

【課題を解決するための手段】

【０００７】

上記課題の少なくとも一部を解決するために、本発明は、以下の形態または適用例として実現することが可能である。例えば、本発明は、ＤＨＣＰサーバにネットワークを介して接続されるネットワーク中継装置であって、通信データを送受信する通信部と、前記ネットワーク中継装置と接続された端末装置による特定のネットワークへの接続の可否を判定するＷｅｂ認証の結果に従い認証済み端末装置を特定する第１の情報を作成し、前記第１の情報に基づき端末装置と前記特定のネットワーク上のノードとの間の通信データの前記通信部による中継の可否を管理する認証処理部と、前記通信部により中継される端末装置と前記ＤＨＣＰサーバとの間のＤＨＣＰ通信データをスヌーピングし、前記ＤＨＣＰ通信データに基づき、各端末装置に割り当てられたレイヤ３アドレスを特定する第２の情報を作成するＤＨＣＰスヌーピング処理部と、前記第１の情報に基づき認証済み端末装置を特定し、前記第２の情報に基づき前記特定された認証済み端末装置に割り当てられたレイヤ３アドレスを特定し、前記通信部に、前記特定された認証済み端末装置が前記特定のネットワークに接続されているか否かを確認する確認通信データを前記特定されたレイヤ３アドレス宛に送信させ、さらに、前記認証処理部に、前記確認の結果に基づいて前記可否を更新させる端末検索処理部と、を備える、ネットワーク中継装置の形態として実現可能である。その他、本発明は、以下の適用例として実現することが可能である。

【０００８】

［適用例１］ネットワーク中継装置であって、

通信データを送受信する通信部と、

前記ネットワーク中継装置と接続された端末装置による特定のネットワークへの接続の可否を判定するＷｅｂ認証の結果に従い認証済み端末装置を特定する第１の情報を作成し、前記第１の情報に基づき端末装置と前記特定のネットワーク上のノードとの間の通信データの前記通信部による中継の可否を管理する認証処理部と、

前記通信部により中継される端末装置とＤＨＣＰサーバとの間のＤＨＣＰ通信データをスヌーピングし、前記ＤＨＣＰ通信データに基づき、各端末装置に割り当てられたレイヤ３アドレスを特定する第２の情報を作成するＤＨＣＰスヌーピング処理部と、

前記第１の情報に基づき認証済み端末装置を特定し、前記第２の情報に基づき前記特定された認証済み端末装置に割り当てられたレイヤ３アドレスを特定し、前記通信部に、前

記特定された認証済み端末装置が前記特定のネットワークに接続されているか否かを確認する確認通信データを前記特定されたレイヤ３アドレス宛に送信させる端末検索処理部と、を備える、ネットワーク中継装置。

【０００９】

このネットワーク中継装置では、端末検索処理部が、認証処理部により作成された認証済み端末装置を特定する第１の情報に基づき認証済み端末装置を特定し、ＤＨＣＰスヌーピング処理部により作成された各端末装置に割り当てられたレイヤ３アドレスを特定する第２の情報に基づき認証済み端末装置に割り当てられたレイヤ３アドレスを特定し、通信部に、特定された認証済み端末装置が特定のネットワークに接続されているか否かを確認する確認通信データを特定されたレイヤ３アドレス宛に送信させるため、認証済み端末装置がネットワークに接続されているか否か（つまり端末接続状態）を管理することができる。そのため、このネットワーク中継装置では、Ｗｅｂ認証における端末接続状態を管理してネットワークにおけるセキュリティを向上させることができる。

【００１０】

［適用例２］適用例１に記載のネットワーク中継装置であって、

前記端末検索処理部は、所定回数の前記確認通信データの送信に対して前記特定された認証済み端末装置からの応答が無い場合には、前記認証処理部に、前記特定された認証済み端末装置についての認証を解除させる、ネットワーク中継装置。

【００１１】

このネットワーク中継装置では、端末検索処理部が、所定回数の確認通信データの送信に対して認証済み端末装置からの応答が無い場合には、認証処理部に認証済み端末装置についての認証を解除させるため、認証済み端末装置がネットワークから離脱した後に、当該端末装置を詐称した他の端末装置によるネットワークへの接続を許してしまう事態の発生を抑制することができ、ネットワークにおけるセキュリティを向上させることができる。

【００１２】

［適用例３］適用例１または適用例２に記載のネットワーク中継装置であって、

前記端末検索処理部は、前記第１の情報と前記第２の情報とに基づき、各認証済み端末装置について割り当てられたレイヤ３アドレスを特定する第３の情報を作成し、前記第３の情報に登録された認証済み端末装置を順に前記特定のネットワークに接続されているか否かの確認対象として選択する、ネットワーク中継装置。

【００１３】

このネットワーク中継装置では、端末検索処理部が、第１の情報と第２の情報とに基づき、各認証済み端末装置について割り当てられたレイヤ３アドレスを特定する第３の情報を作成し、第３の情報に登録された認証済み端末装置を順に確認対象として選択するため、認証済み端末装置の端末接続状態を効果的にかつ効率的に管理することができ、ネットワークにおけるセキュリティを向上させることができる。

【００１４】

［適用例４］適用例３に記載のネットワーク中継装置であって、

前記端末検索処理部は、前記Ｗｅｂ認証によって端末装置が認証された際に認証済み端末装置を前記第３の情報に登録すると共に、前記確認対象として選択された認証済み端末装置について、前記第３の情報にレイヤ３アドレスが登録されていない場合、または、前記第３の情報に登録されたレイヤ３アドレスが前記第２の情報に登録されたレイヤ３アドレスと異なる場合には、前記第２の情報に登録されたレイヤ３アドレスを前記第３の情報に登録する、ネットワーク中継装置。

【００１５】

このネットワーク中継装置では、第３の情報に認証済み端末装置と各認証済み端末装置について割り当てられた最新のレイヤ３アドレスとを登録することができるため、第３の情報を利用して認証済み端末装置の端末接続状態を効果的にかつ効率的に管理することができ、ネットワークにおけるセキュリティを向上させることができる。

【００１６】
［適用例５］適用例４に記載のネットワーク中継装置であって、
前記端末検索処理部は、前記確認対象として選択された認証済み端末装置について、前記第３の情報に登録された認証済み端末装置とレイヤ３アドレスとの対応関係と同一の対応関係が前記第２の情報には登録されておらず、かつ、前記第２の情報に認証済み端末装置と他のレイヤ３アドレスとの対応関係が登録されている場合には、前記選択された認証済み端末装置は前記特定のネットワークから一端離脱した後に再接続したものと判定する、ネットワーク中継装置。
【００１７】
このネットワーク中継装置では、認証済み端末装置が特定のネットワークから一端離脱した後に再接続したことを検知することができ、ネットワークにおけるセキュリティをさらに向上させることができる。
【００１８】
［適用例６］適用例１ないし適用例５のいずれかに記載のネットワーク中継装置であって、さらに、
端末装置に認証前のＶＬＡＮと認証後のＶＬＡＮとが必ずしも一致しないようにＶＬＡＮを設定するＶＬＡＮ設定部を備える、ネットワーク中継装置。
【００１９】
このネットワーク中継装置では、認証前のＶＬＡＮと認証後のＶＬＡＮとが必ずしも一致しないように端末装置にＶＬＡＮが設定される場合にも、認証済み端末装置に割り当てられたレイヤ３アドレスを特定して、認証済み端末装置が特定のネットワークに接続されているか否かを確認する確認通信データを送信することができ、ネットワークにおけるセキュリティを向上させることができる。
【００２０】
［適用例７］適用例１ないし適用例６のいずれかに記載のネットワーク中継装置であって、
前記第１の情報と前記第２の情報と前記第３の情報とは、レイヤ２アドレスにより端末装置を特定する、ネットワーク中継装置。
【００２１】
なお、本発明は、種々の態様で実現することが可能であり、例えば、ネットワーク中継方法および装置、ネットワーク通信方法および装置、ネットワーク認証方法および装置、これらの方法または装置の機能を実現するためのコンピュータプログラム、そのコンピュータプログラムを記録した記録媒体、そのコンピュータプログラムを含み搬送波内に具現化されたデータ信号、等の形態で実現することができる。
【図面の簡単な説明】
【００２２】
【図１】本発明の実施例におけるネットワークシステム１０の構成を概略的に示す説明図である。
【図２】認証スイッチ１００の構成を概略的に示す説明図である。
【図３】ＭＡＣアドレステーブルＭＴの内容の一例を示す説明図である。
【図４】ＤＨＣＰスヌーピングテーブルＤＴの内容の一例を示す説明図である。
【図５】認証管理テーブルＡＴの内容の一例を示す説明図である。
【図６】ポーリング管理テーブルＰＴの内容の一例を示す説明図である。
【図７】ネットワークシステム１０におけるＷｅｂ認証処理の流れを示すフローチャートである。
【図８】本実施例の認証スイッチ１００による端末検索処理の流れを示すフローチャートである。
【発明を実施するための形態】
【００２３】
次に、本発明の実施の形態を実施例に基づいて以下の順序で説明する。

Ａ．実施例：
Ａ－１．ネットワークシステムの構成：
Ａ－２．Ｗｅｂ認証処理：
Ａ－３．端末検索処理：
Ｂ．変形例：
【００２４】
Ａ．実施例：
Ａ－１．ネットワークシステムの構成：
図１は、本発明の実施例におけるネットワークシステム１０の構成を概略的に示す説明図である。ネットワークシステム１０は、端末装置２１０と、端末装置２１０を収容するハブ２２０と、ハブ２２０を収容する認証スイッチ１００と、認証スイッチ１００に接続されたレイヤ３スイッチ２３０と、レイヤ３スイッチ２３０に接続された認証サーバ２４０およびＤＨＣＰサーバ２５０と、を備えている。ネットワークシステム１０内の各構成要素間は、リンクを介して接続されている。リンクは、通信データの伝送路であり、例えばＵＴＰケーブル、ＳＴＰケーブル、光ファイバ、同軸ケーブル、無線によって構成される。
【００２５】
端末装置２１０は、ユーザが使用する情報処理装置であり、例えばパーソナルコンピュータ（ＰＣ）により構成されている。ハブ２２０は、ネットワークにおける通信データをＯＳＩ参照モデルにおける第１層（物理層）で中継するネットワーク中継装置である。認証スイッチ１００は、ネットワークにおける通信データをＯＳＩ参照モデルにおける第２層（データリンク層）で中継するネットワーク中継装置（レイヤ２スイッチ）であると共に、端末装置２１０による特定のネットワークＮＥＴへの接続可否を管理するネットワーク認証機能を有している。レイヤ３スイッチ２３０は、ネットワークにおける通信データをＯＳＩ参照モデルにおける第３層（ネットワーク層）で中継するネットワーク中継装置である。認証サーバ２４０は、認証スイッチ１００からの認証要求に応じて、端末装置２１０によるネットワークＮＥＴへの接続可否を判定するＷｅｂ認証を行うＲＡＤＩＵＳサーバである。ＤＨＣＰサーバ２５０は、端末装置２１０にレイヤ３アドレスとしてのＩＰアドレス等を自動的に割り当てるサーバである。
【００２６】
図２は、認証スイッチ１００の構成を概略的に示す説明図である。認証スイッチ１００は、通信部１２４とＭＡＣアドレステーブルＭＴとを含んでいる。通信部１２４は、図示しない複数の物理ポートを有し、ＭＡＣアドレステーブルＭＴを参照して、物理ポートを介した通信データの送受信を行う。通信部１２４は、例えばＡＳＩＣ（特定用途ＩＣ）により構成される。
【００２７】
図３は、ＭＡＣアドレステーブルＭＴの内容の一例を示す説明図である。ＭＡＣアドレステーブルＭＴは、端末装置２１０のレイヤ２アドレスとしてのＭＡＣアドレスと、端末装置２１０の所属ＶＬＡＮの番号と、端末装置２１０が接続された物理ポートの番号と、の対応関係を規定する。例えば、図３の例では、ＭＡＣアドレステーブルＭＴは、ＭＡＣアドレス「ＭＡＣ－Ａ」の端末装置２１０が、ＶＬＡＮ番号「２００」のＶＬＡＮに所属し、ポート番号「１」の物理ポートに接続されていることを示している。なお、本実施例では、各テーブルにおける個々の対応関係をレコードとも呼ぶ。
【００２８】
通信部１２４は、通信データの送受信を行いつつ、通信データに含まれる宛先ＭＡＣアドレスや送信元ＭＡＣアドレス、ＶＬＡＮ番号等を示す情報を参照して、ＭＡＣアドレステーブルＭＴにレコードを新規登録したり、既に登録されているレコードを更新したりする。また、本実施例では、通信部１２４は、予め設定された長さのエージング時間中に通信データが中継されないＭＡＣアドレスについてのレコードをＭＡＣアドレステーブルＭＴから削除するエージング機能を有している。

【００２９】
認証スイッチ１００（図２）は、所定の処理を行う処理部として、認証処理部１２２と、ＤＨＣＰスヌーピング処理部１２６と、端末検索処理部１２８と、ＶＬＡＮ設定部１３２と、を含んでいる。これらの各処理部は、例えば図示しないＣＰＵが内部メモリに格納されたコンピュータプログラムを読み出して実行することにより実現される。また、認証スイッチ１００は、各処理部に使用される情報として、ＤＨＣＰスヌーピングテーブルＤＴと、認証管理テーブルＡＴと、ポーリング管理テーブルＰＴと、を含んでいる。
【００３０】
ＤＨＣＰスヌーピング処理部１２６は、通信部１２４を介して中継される端末装置２１０とＤＨＣＰサーバ２５０との間のＤＨＣＰ通信データ（ＤＨＣＰメッセージ）を検出し、ＤＨＣＰメッセージに基づき、ＤＨＣＰスヌーピングテーブルＤＴを作成・更新する。図４は、ＤＨＣＰスヌーピングテーブルＤＴの内容の一例を示す説明図である。ＤＨＣＰスヌーピングテーブルＤＴは、端末装置２１０のＭＡＣアドレスと、端末装置２１０に割り当てられたＩＰアドレスと、端末装置２１０の所属ＶＬＡＮの番号と、端末装置２１０が接続された物理ポートの番号と、の対応関係（レコード）を規定する。例えば、図４の例では、ＤＨＣＰスヌーピングテーブルＤＴは、ＭＡＣアドレス「ＭＡＣ－Ａ」の端末装置２１０が、ＶＬＡＮ番号「２００」のＶＬＡＮに所属し、ポート番号「１」の物理ポートに接続されていることや、端末装置２１０にＩＰアドレス「ＩＰ－Ａ」が割り当てられたことを示している。なお、ＤＨＣＰスヌーピングテーブルＤＴは、本発明における第２の情報に相当する。ＤＨＣＰスヌーピング処理部１２６は、通信部１２４がＤＨＣＰサーバ２５０から端末装置２１０に送信されるＩＰアドレス割り当てメッセージ（ＤＨＣＰＡＣＫメッセージ）を検出すると当該メッセージのコピーを通信部１２４から受領し、当該メッセージに含まれる宛先ＭＡＣアドレスや割り当てＩＰアドレス等を示す情報を参照して、ＤＨＣＰスヌーピングテーブルＤＴにレコードを新規登録したり、既に登録されているレコードを更新したりする。
【００３１】
認証処理部１２２は、認証サーバ２４０と協働して端末装置２１０のＷｅｂ認証を行い、Ｗｅｂ認証の結果に従い認証済み端末装置を特定する認証管理テーブルＡＴを作成し、認証管理テーブルＡＴに基づき端末装置２１０とネットワークＮＥＴ上のノードとの間の通信データの通信部１２４による中継の可否を管理する。図５は、認証管理テーブルＡＴの内容の一例を示す説明図である。認証管理テーブルＡＴは、認証済み端末装置２１０のＭＡＣアドレスと、端末装置２１０のユーザを特定するユーザＩＤと、端末装置２１０の所属ＶＬＡＮの番号と、端末装置２１０が接続された物理ポートの番号と、の対応関係（レコード）を規定する。例えば、図５の例では、認証管理テーブルＡＴは、ＭＡＣアドレス「ＭＡＣ－Ａ」の端末装置２１０が、認証済みであると共に、ＶＬＡＮ番号「２００」のＶＬＡＮに所属し、ポート番号「１」の物理ポートに接続されていることを示している。なお、認証管理テーブルＡＴは、本発明における第１の情報に相当する。認証処理部１２２は、Ｗｅｂ認証の結果や後述の端末検索処理の結果に応じて、認証管理テーブルＡＴにレコードを新規登録したり、既に登録されているレコードを削除したりする。認証処理部１２２によるＷｅｂ認証処理については、後に詳述する。
【００３２】
端末検索処理部１２８は、ポーリング管理テーブルＰＴを利用して、認証済みの端末装置２１０がネットワークＮＥＴに接続されているか否かを確認する端末検索処理を行う。図６は、ポーリング管理テーブルＰＴの内容の一例を示す説明図である。ポーリング管理テーブルＰＴは、端末装置２１０のＭＡＣアドレスと、端末装置２１０に割り当てられたＩＰアドレスと、端末装置２１０のユーザのユーザＩＤと、端末装置２１０の所属ＶＬＡＮの番号と、端末装置２１０が接続された物理ポートの番号と、の対応関係（レコード）を規定する。なお、ポーリング管理テーブルＰＴは、本発明における第３の情報に相当する。端末検索処理部１２８による端末検索処理については、後に詳述する。
【００３３】

ＶＬＡＮ設定部１３２は、通信部１２４の各物理ポートにＶＬＡＮを設定する。なお、本実施例の認証スイッチ１００は、認証の前後で端末装置２１０の所属ＶＬＡＮが変更されない固定ＶＬＡＮ方式と、認証の前後で端末装置２１０の所属ＶＬＡＮが変更されるダイナミックＶＬＡＮ方式と、のいずれかを選択的に適用することができる。以下の説明では、認証スイッチ１００においてダイナミックＶＬＡＮ方式が選択されているものとする。

【００３４】

Ａ－２．Ｗｅｂ認証処理：

図７は、ネットワークシステム１０におけるＷｅｂ認証処理の流れを示すフローチャートである。Ｗｅｂ認証処理は、端末装置２１０によるネットワークＮＥＴへの接続可否を管理するために端末装置２１０の認証を行う処理である。ある端末装置２１０についてのＷｅｂ認証実行前では、当該端末装置２１０（あるいは当該端末装置２１０のＭＡＣアドレスを詐称した他の端末装置２１０）によるネットワークＮＥＴへの接続は、認証スイッチ１００によって禁止される。

【００３５】

端末装置２１０のユーザが端末装置２１０をハブ２２０に接続すると、当該ハブ２２０を収容する認証スイッチ１００のＶＬＡＮ設定部１３２は、接続された端末装置２１０を認証前用のＶＬＡＮ（図７の例ではＶＬＡＮ「１００」）に所属させる。端末装置２１０が、認証前用のＶＬＡＮでＤＨＣＰサーバ２５０に対して認証前用のＩＰアドレスを要求すると（ステップＳ１１０）、ＤＨＣＰサーバ２５０は、端末装置２１０に対してＩＰアドレスを割り当てる（ステップＳ１２０）。このときに割り当てられるＩＰアドレスは、認証前の端末装置２１０が所属するＶＬＡＮに対応するＩＰサブネットを有するＩＰアドレスであり、Ｗｅｂ認証実行用の暫定的なＩＰアドレスである。なお、よく知られているように、ＩＰアドレスの割り当ては、具体的には、端末装置２１０によるＤＨＣＰ Ｄｉｓｃｏｖｅｒメッセージのブロードキャストと、Ｄｉｓｃｏｖｅｒメッセージを受信したＤＨＣＰサーバ２５０による割り当て可能なＩＰアドレスを通知するＤＨＣＰ Ｏｆｆｅｒメッセージの端末装置２１０への送信と、Ｏｆｆｅｒメッセージを受信した端末装置２１０による特定のＩＰアドレスを要求するＤＨＣＰ Ｒｅｑｕｅｓｔメッセージの ＤＨＣＰサーバ２５０への送信と、Ｒｅｑｕｅｓｔメッセージを受信したＤＨＣＰサーバ２５０による割り当てＩＰアドレスを通知するＤＨＣＰ ＡＣＫメッセージの端末装置２１０への送信と、が順に実行されることにより実現される。認証スイッチ１００は、端末装置２１０とＤＨＣＰサーバ２５０との間でやりとりされるＤＨＣＰの各メッセージを中継する。

【００３６】

このとき認証スイッチ１００のＤＨＣＰスヌーピング処理部１２６は、ＤＨＣＰの各メッセージをスヌーピングして端末装置２１０に割り当てられたＩＰアドレスを特定し、特定されたＩＰアドレスを、端末装置２１０のＭＡＣアドレスやＶＬＡＮ番号等に対応付けてＤＨＣＰスヌーピングテーブルＤＴ（図４）に登録する（ステップＳ１３０）。

【００３７】

ＩＰアドレスの割り当てを受けた端末装置２１０は、認証スイッチ１００に対して、ｈｔｔｐ／ｈｔｔｐｓにより、ネットワークＮＥＴに接続するための認証を要求する（ステップＳ１４０）。具体的には、Ｗｅｂブラウザが動作する端末装置２１０が、割り当てられたＩＰアドレスを用いて認証スイッチ１００に対して認証要求パケットを送信すると、Ｗｅｂサーバとしての機能を有する認証処理部１２２は、端末装置２１０に対して認証情報登録画面データを送信する。端末装置２１０は、認証情報登録画面データを受信して認証情報登録画面を表示し、画面上においてユーザにより入力された認証情報（例えばユーザＩＤとパスワード）を認証スイッチ１００に送信する。

【００３８】

認証スイッチ１００の認証処理部１２２は、端末装置２１０から認証情報を受け取ると、認証サーバ２４０に対して認証情報を転送して端末装置２１０の認証を要求する（ステ

ップＳ１５０）。認証サーバ２４０は、認証データベースに端末装置２１０の認証情報が登録されていなかった場合には（ステップＳ１６０：ＮＯ）、端末装置２１０の認証は不成功であると判定する。この場合には、認証サーバ２４０は、認証スイッチ１００に対して認証不成功を通知し、認証スイッチ１００は、端末装置２１０に対して認証不成功を通知する（ステップＳ２３０）。

【００３９】

一方、認証サーバ２４０は、認証データベースに対象の端末装置２１０の認証情報が登録されていた場合には（ステップＳ１６０：ＹＥＳ）、端末装置２１０の認証は成功であると判定する。この場合には、認証サーバ２４０は、認証スイッチ１００に対して認証成功を通知すると共に、端末装置２１０の認証後の所属ＶＬＡＮ（図７の例ではＶＬＡＮ「２００」）を特定する情報を通知する（ステップＳ１７０）。本実施例では、ダイナミックＶＬＡＮ方式が選択されているため、端末装置２１０の認証後の所属ＶＬＡＮは、認証前の所属ＶＬＡＮとは異なっている。

【００４０】

認証成功通知を受領した認証スイッチ１００の認証処理部１２２は、端末装置２１０の所属ＶＬＡＮを認証サーバ２４０から通知されたＶＬＡＮに変更して端末装置２１０に通知すると共に、認証管理テーブルＡＴ（図５）に、認証された端末装置２１０についてのレコードを追加登録する（ステップＳ１８０）。また、認証スイッチ１００の端末検索処理部１２８は、ポーリング管理テーブルＰＴ（図６）に、認証管理テーブルＡＴに追加登録されたレコードに対応するレコードを追加登録する（ステップＳ１９０）。従って、ポーリング管理テーブルＰＴに追加登録されるレコードには、ＭＡＣアドレスとユーザＩＤとＶＬＡＮ番号とポート番号とが記録され、ＩＰアドレスはこの時点では記録されない（空欄となる）。

【００４１】

認証成功通知を受領した端末装置２１０は、新たな所属ＶＬＡＮ（図７の例ではＶＬＡＮ「２００」）で、ＤＨＣＰサーバ２５０に対してＩＰアドレスを要求する（ステップＳ２００）。要求を受けたＤＨＣＰサーバ２５０は、端末装置２１０に対してＩＰアドレスを割り当てる（ステップＳ２１０）。このときに割り当てられるＩＰアドレスは、認証後の端末装置２１０が所属するＶＬＡＮに対応するＩＰサブネットを有するＩＰアドレスである。

【００４２】

このとき、認証スイッチ１００のＤＨＣＰスヌーピング処理部１２６は、認証前と同様に、端末装置２１０とＤＨＣＰサーバ２５０との間でやりとりされるＤＨＣＰの各メッセージをスヌーピングして端末装置２１０に割り当てられたＩＰアドレスを特定し、特定されたＩＰアドレスを、端末装置２１０のＭＡＣアドレスやＶＬＡＮ番号等に対応付けてＤＨＣＰスヌーピングテーブルＤＴ（図４）に登録する（ステップＳ２２０）。ＤＨＣＰスヌーピングテーブルＤＴには、この端末装置２１０についてのレコードが既に登録されており、ＤＨＣＰスヌーピング処理部１２６は、このレコードにおけるＩＰアドレスとＶＬＡＮ番号とを認証後のものに更新する。

【００４３】

以上説明したＷｅｂ認証処理により、端末装置２１０の認証が行われ、認証が成功した端末装置２１０に認証後に使用するためのＩＰアドレスが割り当てられる。認証スイッチ１００は、認証済みの端末装置２１０とネットワークＮＥＴ上のノードとの間の通信データを中継する。これにより、端末装置２１０によるネットワークＮＥＴへの接続が可能となる。

【００４４】

Ａ－３．端末検索処理：

図８は、本実施例の認証スイッチ１００による端末検索処理の流れを示すフローチャートである。端末検索処理は、認証済みの端末装置２１０がまだネットワークＮＥＴに接続されているか否かを確認し、既にネットワークＮＥＴから離脱したと判定された端末装置

２１０についての認証を解除する処理である。

【００４５】

認証スイッチ１００の端末検索処理部１２８は、所定のタイミングで、ポーリング管理テーブルＰＴに登録されたレコードの１つを選択することにより、選択されたレコードのＭＡＣアドレスに対応する端末装置２１０をポーリング対象端末装置に設定する（ステップＳ４１０）。なお、上述したように、ポーリング管理テーブルＰＴには、認証成功時に認証管理テーブルＡＴに追加登録されたレコードに対応するレコードが追加登録されるため、ポーリング管理テーブルＰＴに登録されたレコードのＭＡＣアドレスに対応する端末装置２１０は、認証済みの端末装置２１０である。すなわち、端末検索処理部１２８は、認証管理テーブルＡＴに基づき作成されたポーリング管理テーブルＰＴを用いて、認証済みの端末装置２１０の１つをポーリング対象端末装置として選択することとなる。

【００４６】

端末検索処理部１２８は、ポーリング対象端末装置のＩＰアドレスがポーリング管理テーブルＰＴに登録されているか否かを判定する（ステップＳ４２０）。なお、端末装置２１０が認証後初めてポーリング対象端末装置に設定されたときには、ＩＰアドレスはポーリング管理テーブルＰＴに登録されていない。

【００４７】

端末装置２１０のＩＰアドレスがポーリング管理テーブルＰＴに登録されていない場合には、端末検索処理部１２８は、ポーリング管理テーブルＰＴに登録されているＭＡＣアドレスをキーとして用いて、ＤＨＣＰスヌーピングテーブルＤＴを検索する（ステップＳ４３０）。ＤＨＣＰスヌーピングテーブルＤＴにおいて当該ＭＡＣアドレスに対応するレコードが検出された場合には（ステップＳ４４０：ＹＥＳ）、端末検索処理部１２８は、検出されたレコードにおけるＩＰアドレスを用いてポーリング処理を行う（ステップＳ４５０）。ここで、ポーリング処理は、通信部１２４に、検出されたレコードにおけるＩＰアドレスを宛先アドレスとして、応答を要求する確認パケットを送信させる処理である。

【００４８】

確認パケットに対して端末装置２１０からの応答があった場合には（ステップＳ４６０：ＹＥＳ）、端末装置２１０はネットワークＮＥＴに接続されていることが確認されたこととなる。この場合には、端末検索処理部１２８は、ポーリング管理テーブルＰＴにおけるポーリング対象端末装置に対応するレコードに、検出されたＩＰアドレスを追加登録する（ステップＳ４７０）。これにより、ポーリング管理テーブルＰＴに、ポーリング対象端末装置についてのＭＡＣアドレスとＩＰアドレスとの対応関係が登録される。その後、端末検索処理部１２８は、当該端末装置２１０のポーリング回数をリセットして（ステップＳ４８０）、次のポーリング対象端末装置の選択処理（ステップＳ４１０）を行う。

【００４９】

確認パケットに対して端末装置２１０から応答がなかった場合には（ステップＳ４６０：ＮＯ）、端末検索処理部１２８は、ポーリング処理実行回数（確認パケット送信回数）が予め設定された規定値を超えるまで、ポーリング処理（ステップＳ４５０）と応答有無の判定（ステップＳ４６０）とを繰り返し実行する。ポーリング処理実行回数が規定値を超えると（ステップＳ４９０：ＮＯ）、端末検索処理部１２８は、端末装置２１０が既にネットワークＮＥＴから離脱したものと判断する。この場合には、端末検索処理部１２８は、ポーリング管理テーブルＰＴから当該端末装置２１０についてのレコードを削除すると共に（ステップＳ５００）、認証処理部１２２に、認証管理テーブルＡＴから当該端末装置２１０についてのレコードの削除をさせて当該端末装置２１０についての認証を解除させる（ステップＳ５１０）。これにより、当該端末装置２１０（あるいは当該端末装置２１０のＭＡＣアドレスを詐称した他の端末装置２１０）によるネットワークＮＥＴへの接続は、認証スイッチ１００によって禁止される。

【００５０】

なお、ポーリング管理テーブルＰＴに登録されている端末装置２１０のＭＡＣアドレスをキーとして用いたＤＨＣＰスヌーピングテーブルＤＴの検索（ステップＳ４３０）にお

いて、当該ＭＡＣアドレスに対応するレコードが検出されなかった場合には（ステップＳ４４０：ＮＯ）、処理は次のポーリング対象端末装置の選択（ステップＳ４１０）に戻る。

【００５１】

ポーリング対象端末装置のＩＰアドレスがポーリング管理テーブルＰＴに登録されているか否かの判定（ステップＳ４２０）において、ＩＰアドレスがポーリング管理テーブルＰＴに既に登録されている場合には、端末検索処理部１２８は、ＰＴに登録されたポーリング対象端末装置のＭＡＣアドレスとＩＰアドレスとの組み合わせをキーとして用いて、ＤＨＣＰスヌーピングテーブルＤＴを検索する（ステップＳ５２０）。ＤＨＣＰスヌーピングテーブルＤＴにおいて当該組み合わせに対応するレコードが検出された場合には（ステップＳ５３０：ＹＥＳ）、端末検索処理部１２８は、ポーリング管理テーブルＰＴに登録されたＩＰアドレス（すなわちＤＨＣＰスヌーピングテーブルＤＴに登録されたＩＰアドレス）を用いてポーリング処理を行い（ステップＳ４５０）、ポーリング処理に対する応答の有無に応じて上述したのと同様の処理を行う（ステップＳ４６０～Ｓ５１０）。

【００５２】

ＰＴに登録されたポーリング対象端末装置のＭＡＣアドレスとＩＰアドレスとの組み合わせを用いたＤＨＣＰスヌーピングテーブルＤＴの検索（ステップＳ５２０）において、該当するレコードが検出されなかった場合には（ステップＳ５３０：ＮＯ）、端末検索処理部１２８は、ポーリング対象端末装置のＭＡＣアドレスのみをキーとして用いて、ＤＨＣＰスヌーピングテーブルＤＴを検索する（ステップＳ５４０）。ＤＨＣＰスヌーピングテーブルＤＴに該当するレコードがなかった場合には（ステップＳ５５０：ＮＯ）、ポーリング端末装置はまだＤＨＣＰによりＩＰアドレスを取得していないと考えられるため、接続状態の確認は後回しにし、処理は次のポーリング対象端末装置の選択（ステップＳ４１０）に戻る。

【００５３】

一方、ＤＨＣＰスヌーピングテーブルＤＴにおいて該当するレコードが検出された場合には（ステップＳ５５０：ＹＥＳ）、端末検索処理部１２８は、ポーリング対象端末装置がネットワークＮＥＴから一端離脱した後、離脱前の物理ポートと同一のまたは別の物理ポートを介してネットワークＮＥＴに再接続され、新たなＩＰアドレスを取得したものと判定する。この場合には、ＤＨＣＰスヌーピングテーブルＤＴにおいて検出されたレコードに登録されたＩＰアドレスを用いてポーリング処理（ステップＳ４５０）を行い、ポーリング処理に対する応答の有無に応じて上述したのと同様の処理を行う（ステップＳ４６０～Ｓ５１０）。

【００５４】

以上説明したように、本実施例の認証スイッチ１００による端末検索処理では、端末検索処理部１２８が、認証管理テーブルＡＴに基づき作成されたポーリング管理テーブルＰＴを用いて認証済みの端末装置２１０の１つをポーリング対象端末装置として選択し、ＤＨＣＰスヌーピングテーブルＤＴを用いてポーリング対象端末装置に割り当てられたＩＰアドレスを特定し、通信部１２４に、ポーリング対象端末装置がネットワークＮＥＴに接続されているか否かを確認する確認パケットを特定されたＩＰアドレス宛に送信させる。そのため、認証スイッチ１００は、認証済みの端末装置２１０が、まだネットワークＮＥＴに接続されているか否か（つまり端末接続状態）を管理することができる。そのため、本実施例の認証スイッチ１００では、認証済みの端末装置２１０がネットワークＮＥＴから離脱した後に、当該端末装置２１０のＭＡＣアドレスを詐称した他の端末装置２１０によるネットワークＮＥＴへの接続を許してしまう事態の発生を抑制することができ、ネットワークにおけるセキュリティを向上させることができる。

【００５５】

具体的には、認証スイッチ１００は、予め設定された回数の確認パケット送信に対して端末装置２１０から応答がなかった場合には、端末装置２１０が既にネットワークＮＥＴから離脱したものと判断し、当該端末装置２１０についての認証を解除する。そのため、

本実施例の認証スイッチ１００によれば、認証済みの端末装置２１０がネットワークＮＥＴから離脱したことを迅速に検知することができ、ネットワークＮＥＴから離脱した端末装置２１０についての認証を迅速に解除することができるため、ネットワークにおけるセキュリティを向上させることができる。

【００５６】

なお、端末装置２１０とＤＨＣＰサーバ２５０との間でやり取りされるＤＨＣＰメッセージをスヌーピングするＤＨＣＰスヌーピング機能や、端末装置２１０とＤＨＣＰサーバ２５０との間でやり取りされるＤＨＣＰメッセージをリレーするＤＨＣＰリレー機能は、既に知られた技術であり、これらの機能を用いて端末装置２１０のＩＰアドレスを検知することは可能である。しかしながら、ＤＨＣＰリレー機能やＤＨＣＰスヌーピング機能は、端末装置２１０の認証の有無を検知することはできない。また、本実施例の認証スイッチ１００では、認証の前後で端末装置２１０の所属ＶＬＡＮが変更され端末装置２１０に割り当てられるＩＰアドレスも変更されるダイナミックＶＬＡＮ方式が選択されている。さらに、認証済みの端末装置２１０がネットワークＮＥＴから離脱した後にネットワークＮＥＴに再接続した場合には、やはり端末装置２１０のＩＰアドレスは変更され得る。そのため、単に、ＤＨＣＰリレー機能やＤＨＣＰスヌーピング機能を用いて端末装置２１０のＩＰアドレスを検知しても、認証済み端末装置２１０のネットワーク接続状態を管理することはできなかった。本実施例の認証スイッチ１００では、認証管理テーブルＡＴに基づき作成されたポーリング管理テーブルＰＴを用いることにより、認証済みの端末装置２１０を把握することができ、ＤＨＣＰスヌーピングテーブルＤＴを用いて認証済みの端末装置２１０に割り当てられたＩＰアドレスを特定することにより、端末装置２１０のＩＰアドレスが変化し得る環境においても認証済み端末装置２１０のネットワーク接続状態を管理することができるため、ネットワークにおけるセキュリティを向上させることができる。

【００５７】

また、認証スイッチ１００において、ＭＡＣアドレステーブルＭＴのエージング機能を利用し、エージング機能により削除されたＭＡＣアドレスに対応する端末装置２１０については認証を解除するものとすることは可能であるが、この場合には、実際にはネットワークＮＥＴから離脱していない端末装置２１０であっても、例えばユーザが離席するなどして通信が行われなかった端末装置２１０についての認証が解除される可能性がある。このような場合には、端末装置２１０の再度のＷｅｂ認証処理が必要となる。このような事態の発生を回避するためにエージング時間を長めに設定すると、ネットワークにおけるセキュリティを十分に高めることができない。一方、エージング時間を短めに設定すると、上記事態が発生してユーザ利便性が損なわれる可能性があると共に、削除されたＭＡＣアドレスを有する端末装置２１０に関する通信をすべてのＶＬＡＮに転送するフラッディング処理のための通信負荷が増大する可能性があり、好ましくない。本実施例の認証スイッチ１００は、ネットワークＮＥＴに接続されている認証済み端末装置２１０に対して定期的に確認パケットを送信するため、エージング処理によってネットワークＮＥＴから離脱していない端末装置２１０の認証が解除される事態の発生を抑制することができる。

【００５８】

また、本実施例の認証スイッチ１００は、ポーリング対象端末装置として選択された認証済みの端末装置２１０について、ポーリング管理テーブルＰＴに登録されたＭＡＣアドレスとＩＰアドレスとの対応関係と同一の対応関係がＤＨＣＰスヌーピングテーブルＤＴには登録されておらず、かつ、ＤＨＣＰスヌーピングテーブルＤＴに当該ＭＡＣアドレスと他のＩＰアドレスとの対応関係が登録されている場合には、選択された認証済み端末装置２１０はネットワークＮＥＴから一端離脱した後に再接続したものと判定する。そのため、本実施例の認証スイッチ１００は、認証済み端末装置２１０の離脱や移動を検知することができ、ネットワークにおけるセキュリティをさらに向上させることができる。

【００５９】

Ｂ．変形例：

なお、この発明は上記の実施例や実施形態に限られるものではなく、その要旨を逸脱しない範囲において種々の態様において実施することが可能であり、例えば次のような変形も可能である。

【００６０】

Ｂ１．変形例１：

上記実施例におけるネットワークシステム１０の構成は、あくまで一例であり、種々変形可能である。例えば、図１に示すネットワークシステム１０は、端末装置２１０や認証スイッチ１００を複数備えているが、ネットワークシステム１０は、端末装置２１０および認証スイッチ１００をそれぞれ少なくとも１つ備えていればよい。また、ネットワークシステム１０において、端末装置２１０と認証スイッチ１００とは、ハブ２２０を介さずに直接接続されているとしてもよい。また、ネットワークシステム１０において、認証サーバ２４０およびＤＨＣＰサーバ２５０は、他のノードを介してレイヤ３スイッチ２３０と接続されているとしてもよい。

【００６１】

また、認証スイッチ１００は、Ｌ３スイッチとしての機能を有するとしてもよい。あるいは、認証スイッチ１００は、認証サーバおよびＤＨＣＰサーバとしての機能を有しているとしてもよい。この場合に、Ｗｅｂ認証処理は、認証スイッチ１００の有する認証サーバ機能および／またはＤＨＣＰサーバ機能を用いて実行されるとしてもよい。

【００６２】

Ｂ２．変形例２：

上記実施例における各テーブル（ＭＡＣアドレステーブルＭＴ、ＤＨＣＰスヌーピングテーブルＤＴ、認証管理テーブルＡＴ、ポーリング管理テーブルＰＴ（図３～６））の内容はあくまで一例であり、各テーブルが各図に示した内容の一部を含まなかったり、各図に示した内容以外の内容を含んだりしてもよい。

【００６３】

Ｂ３．変形例３：

上記実施例では、端末検索処理部１２８が、認証管理テーブルＡＴとＤＨＣＰスヌーピングテーブルＤＴとに基づきポーリング管理テーブルＰＴを生成し、ポーリング管理テーブルＰＴを用いて端末検索処理を行っているが、端末検索処理部１２８は、ポーリング管理テーブルＰＴを生成せず、認証管理テーブルＡＴとＤＨＣＰスヌーピングテーブルＤＴとを利用して、同様に端末検索処理を行うものとしてもよい。

【００６４】

Ｂ４．変形例４：

上記実施例の端末検索処理（図８）では、ポーリング管理テーブルＰＴにポーリング対象端末装置のＩＰアドレスが登録されているか否かの判定（ステップＳ４２０）の結果に応じて次の処理内容が変更されるとしているが、ポーリング管理テーブルＰＴにポーリング対象端末装置のＩＰアドレスが登録されているか否かにかかわらず（ステップＳ４２０の判定を実行せず）、ポーリング対象端末装置のＭＡＣアドレスをキーとして用いたＤＨＣＰスヌーピングテーブルＤＴの検索（ステップＳ４３０）が実行されるとしてもよい。ただし、上記実施例のように、ステップＳ４２０の判定を実行し、ポーリング管理テーブルＰＴにポーリング対象端末装置のＩＰアドレスが登録されている場合にはポーリング対象端末装置のＭＡＣアドレスとＩＰアドレスとの組み合わせをキーとして用いたＤＨＣＰスヌーピングテーブルＤＴの検索（ステップＳ５２０）が実行されるとすれば、認証済み端末装置２１０がネットワークＮＥＴから一端離脱した後に再接続したことを検知することができるため、好ましい。

【００６５】

Ｂ５．変形例５：

上記実施例では、ダイナミックＶＬＡＮ方式が適用される例について説明したが、固定ＶＬＡＮ方式が適用される場合にも、本実施例の端末検索処理により、認証済みの端末装置２１０がネットワークＮＥＴに接続されているか否か（端末接続状態）を管理すること

ができ、ネットワークにおけるセキュリティを向上させることができる。

【００６６】

Ｂ６．変形例６：

上記実施例では、レイヤ２アドレスとしてＭＡＣアドレスが用いられ、レイヤ３アドレスとしてＩＰアドレスが用いられているが、レイヤ２アドレスおよびレイヤ３アドレスとしては、Ｗｅｂ認証処理や端末検索処理に用いられるプロトコルに応じたアドレスが適宜用いられる。

【００６７】

Ｂ７．変形例７：

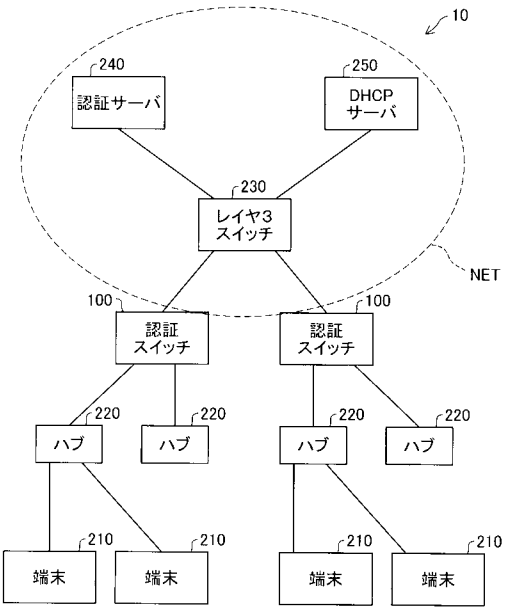
上各実施例において、ハードウェアによって実現されていた構成の一部をソフトウェアに置き換えるようにしてもよく、逆に、ソフトウェアによって実現されていた構成の一部をハードウェアに置き換えるようにしてもよい。

【符号の説明】

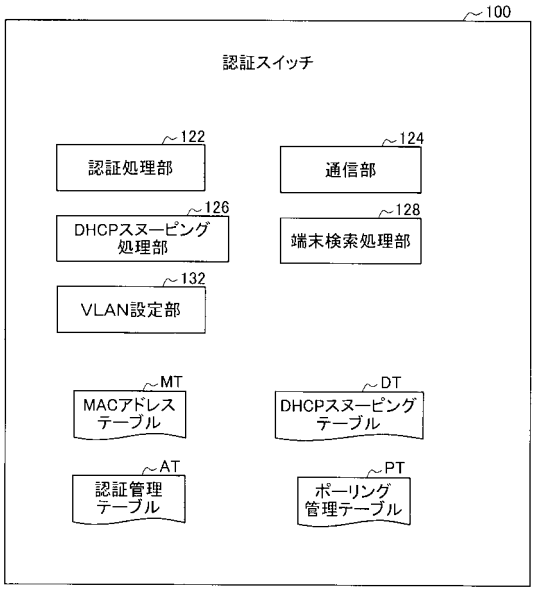
【００６８】

１０…ネットワークシステム
１００…認証スイッチ
１２２…認証処理部
１２４…通信部
１２６…ＤＨＣＰスヌーピング処理部
１２８…端末検索処理部
１３２…ＶＬＡＮ設定部
２１０…端末装置
２２０…ハブ
２３０…レイヤ３スイッチ
２４０…認証サーバ
２５０…ＤＨＣＰサーバ

【図１】



【図２】



【図３】

MT

MACアドレス	VLAN番号	ポート番号
MAC-A	200	1
MAC-B	300	1
MAC-C	200	2

【図４】

DT

MACアドレス	IPアドレス	VLAN番号	ポート番号
MAC-A	IP-A	200	1
MAC-B	IP-B	300	1
MAC-C	IP-C	200	2

【図５】

AT

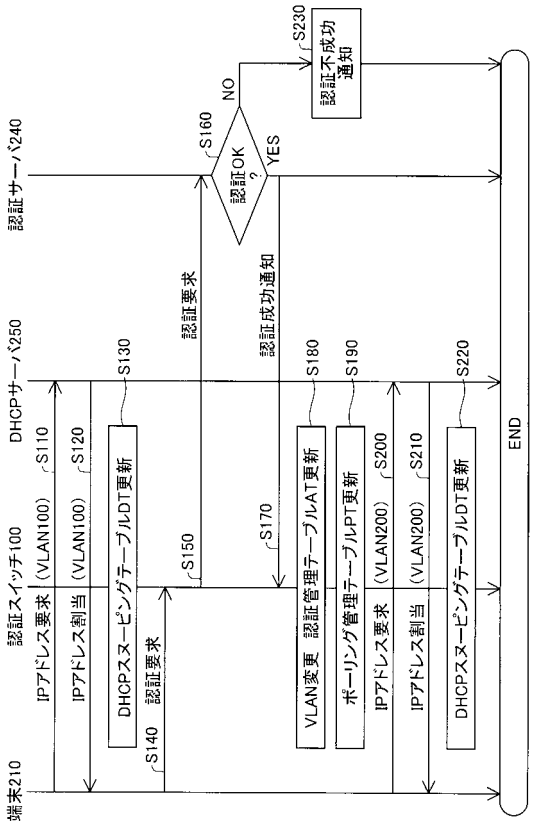
MACアドレス	ユーザID	VLAN番号	ポート番号
MAC-A	ユーザ-A	200	1
MAC-B	ユーザ-B	300	1
MAC-C	ユーザ-C	200	2

【図６】

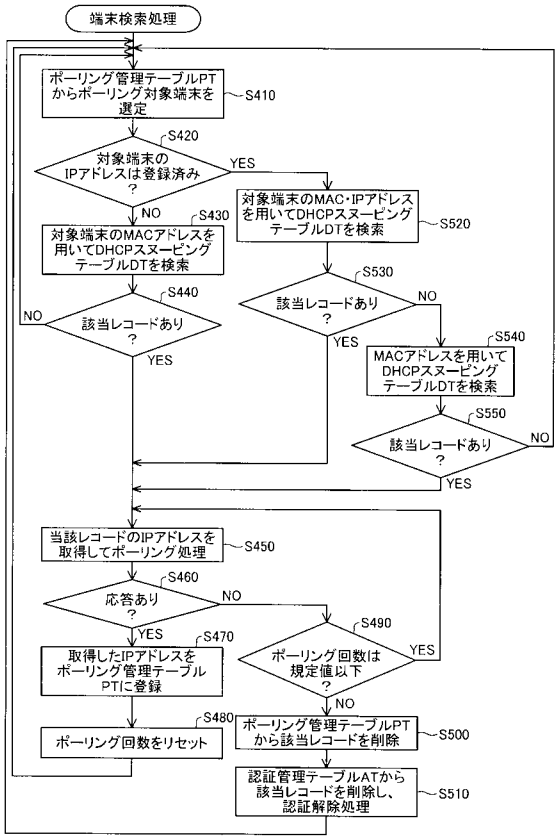
PT

MACアドレス	IPアドレス	ユーザID	VLAN番号	ポート番号
MAC-A	IP-A	ユーザ-A	200	1
MAC-B	IP-B	ユーザ-B	300	1
MAC-C	IP-C	ユーザ-C	200	2

【図７】



【図８】


端末検索処理
ポーリング管理テーブルPTからポーリング対象端末を選定
S410
S420
対象端末のIPアドレスは登録済み？
YES
NO
S430
対象端末のMACアドレスを用いてDHCPスヌーピングテーブルDTを検索
S440
該当レコードあり？
NO
YES
対象端末のMAC・IPアドレスを用いてDHCPスヌーピングテーブルDTを検索
S520
S530
該当レコードあり？
NO
YES
S540
MACアドレスを用いてDHCPスヌーピングテーブルDTを検索
S550
該当レコードあり？
NO
YES
当該レコードのIPアドレスを取得してポーリング処理
S450
S460
応答あり？
NO
YES
S470
取得したIPアドレスをポーリング管理テーブルPTに登録
S480
ポーリング回数をリセット
S490
ポーリング回数は規定値以下？
YES
NO
ポーリング管理テーブルPTから該当レコードを削除
S500
認証管理テーブルATから該当レコードを削除し、認証解除処理
S510

フロントページの続き

(56)参考文献 実用新案登録第３１５４６７９（ＪＰ，Ｙ２）
特開２００５－２８６５５８（ＪＰ，Ａ）
特開２００８－１９３２３１（ＪＰ，Ａ）
特開２００９－１３０８３８（ＪＰ，Ａ）
特開２０１１－１０７７９６（ＪＰ，Ａ）
“スイッチング／ポート認証”，CentreCOM 9424T/SP-E、9424Ts/XP-E コマンドリファレンス２．４，［オンライン］，２００８年 2月２０日，Ｒｅｖ．Ｃ（Ｖｅｒ．２．４．１Ｊ），［平成２４年１２月２８日検索］、インターネット，ＵＲＬ，<http://www.allied-telesis.co.jp/support/list/switch/9400ts_xp-e/comref/overview_08SWITCH_70PAUTH.html>
伊藤玄蕃，“セキュリティ、管理、ＱｏＳまで完全解剖最新スイッチ ユニークな独自認証技術”，ネットワーク マガジン，日本，株式会社アスキー，２００７年 1月 1日，第１２巻，第1号，ｐ．４４－４５

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ 9／３２
Ｇ０６Ｆ ２１／４４
Ｈ０４Ｌ １２／５８