(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2005-286558
(P2005-286558A)
(43)公開日　平成17年10月13日(2005.10.13)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/46	H04L 12/46	E	5J104
H04L 9/32	H04L 9/00	673A	5K033

審査請求 未請求　請求項の数 4　OL　（全 12 頁）

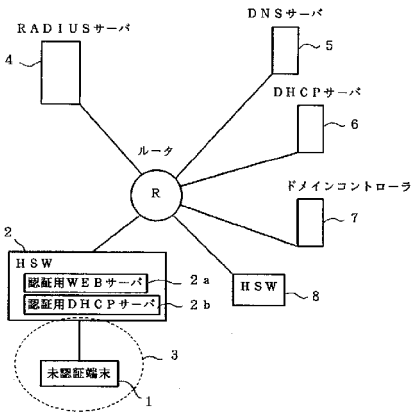
(21)出願番号　特願2004-95656(P2004-95656)
(22)出願日　平成16年3月29日(2004.3.29)

(71)出願人　000005120
日立電線株式会社
東京都千代田区大手町一丁目６番１号
(74)代理人　100068021
弁理士　絹谷　信雄
(72)発明者　巽　知厳
東京都千代田区大手町一丁目６番１号　日立電線株式会社内

Ｆターム(参考)　5J104 AA07 KA02 KA04 NA05 NA38 PA07
5K033 AA08 CC01 DA05 DB16 DB18 EC03

(54)【発明の名称】端末認証システム

(57)【要約】
【課題】　端末が新規なハードウェアであっても認証の手続きが可能な認証システムを提供する。
【解決手段】　ユーザを特定するための認証ワードが登録されているＲＡＤＩＵＳサーバ４をネットワーク中に設け、このネットワークに対してフレーム中継を行う中継装置２に認証用ＤＨＣＰサーバ２ｂを設けておき、この中継装置２に物理的に接続された端末１がＤＨＣＰによりＩＰアドレスを要求したとき、前記認証用ＤＨＣＰサーバ２ｂから暫定ＩＰアドレスを付与することにより、前記中継装置２と前記端末１との間でのみ通信可能な閉じた認証用サブネットを形成し、前記中継装置２が前記端末１から入力された認証ワードを前記ＲＡＤＩＵＳサーバ４に問い合わせ、このＲＡＤＩＵＳサーバ４より認証が得られたとき、前記端末１から前記ネットワークへの通信を許容する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ユーザを特定するための認証ワードが登録されているＲＡＤＩＵＳサーバをネットワーク中に設け、このネットワークに対してフレーム中継を行う中継装置に認証用ＤＨＣＰサーバを設けておき、この中継装置に物理的に接続された端末がＤＨＣＰによりＩＰアドレスを要求したとき、前記認証用ＤＨＣＰサーバから暫定ＩＰアドレスを付与することにより、前記中継装置と前記端末との間でのみ通信可能な閉じた認証用サブネットを形成し、前記中継装置が前記端末から入力された認証ワードを前記ＲＡＤＩＵＳサーバに問い合わせ、このＲＡＤＩＵＳサーバより認証が得られたとき、前記端末から前記ネットワークへの通信を許容することを特徴とする端末認証システム。
【請求項２】
前記中継装置に認証用ＷＥＢサーバを設けておき、この認証用ＷＥＢサーバが前記端末より送信されたＨＴＴＰパケットを傍受したとき、認証ワードを入力するための認証用ＷＥＢページを前記端末に送信することを特徴とする請求項１記載の端末認証システム。
【請求項３】
前記ＲＡＤＩＵＳサーバは、ユーザ毎のＶＬＡＮ情報が登録されており、前記端末を認証したときにそのユーザのＶＬＡＮ情報を前記中継装置に通知し、前記中継装置は、通知されたＶＬＡＮ情報により前記端末が接続されているポートをＶＬＡＮ設定することを特徴とする請求項１又は２記載の端末認証システム。
【請求項４】
前記中継装置は、前記端末がログイン時に所定プロトコルのサーバを参照する場合には、前記認証用サブネット外への通信を許容することを特徴とする請求項１～３いずれか記載の端末認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークに物理的に接続された端末に対して論理的な接続を許容する認証システムに係り、特に、端末が新規なハードウェアであっても認証の手続きが可能な認証システムに関するものである。
【背景技術】
【０００２】
ダイナミック仮想ＬＡＮ（ＤＶＬＡＮ）機能は、端末がネットワークのどの中継装置に物理的に接続しても、その端末が同じサブネットに論理的に接続できる機能である。
【０００３】
このＤＶＬＡＮ機能は次のように実現される。端末とその端末が属する仮想ＬＡＮグループの識別番号（ＶＩＤ）との対応関係が予めＤＶＬＡＮサーバに設定してあり、スイッチ等の中継装置は、当該中継装置の仮想ＬＡＮの設定可能なポート（ＤＶＬＡＮポート）に接続する端末を検出すると、ＤＶＬＡＮサーバに問い合わせを行い、その問い合わせに対するＤＶＬＡＮサーバからの応答を得て、その結果が肯定的であれば、前記ＶＬＡＮポートを所定のＶＩＤに設定し、ＧＶＲＰ（ＧＡＲＰ　ＶＬＡＮ　Ｒｅｇｉｓｔｒａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）によりバックボーン（中継装置が接続されているネットワーク）にそのＶＬＡＮを通知する。
【０００４】
例えば、図４において、スイッチ５２のポート＃４はＶＩＤ未設定のＤＶＬＡＮポートである。端末５１のＭＡＣアドレスは“ＭＡＣ１”である。スイッチ５２には、ポート番号と当該ポートの状態や設定内容とが対応付けて記憶されている。その記憶内容がテーブル５３に示してある。この例では、ポート＃１はダウンしており、ポート＃４はＶＩＤ未設定であり、ポート＃ｓはバックボーンポートである。一方、ＤＶＬＡＮサーバ５４にはＭＡＣアドレスとＶＩＤとの対応が記憶されている。その記憶内容がテーブル５５に示してある。この例では、“ＭＡＣ１”の端末に設定されているＶＩＤは“ＶＩＤ－１”、“

ＭＡＣ２”の端末に設定されているＶＩＤは“ＶＩＤ－２”、…である。
【０００５】
上記端末５１をＶＩＤ未設定のＤＶＬＡＮポートであるポート＃４に接続した場合、まず、図中の丸数字１で示すように（以下、単に（丸１），（丸２）…と記す）、（丸１）端末５１より送信元ＭＡＣアドレスが“ＭＡＣ１”のフレームが送信される。（丸２）スイッチ５２は、ＭＡＣアドレスが“ＭＡＣ１”である端末ＰＣ１のＶＩＤをＳＮＭＰ（Ｓｉｍｐｌｅ Ｎｅｔｗｏｒｋ Ｎａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ）によりＤＶＬＡＮサーバ５４に問い合わせる。（丸３）スイッチ５２は、ＤＶＬＡＮサーバ５４が応答した内容から端末５１のＶＩＤが“ＶＩＤ－１”であることを認識し、端末５１が接続されているＤＶＬＡＮポートのＶＩＤを“ＶＩＤ－１”に設定する。（丸４）スイッチ５２は、ＧＶＲＰによってバックボーンのＶＬＡＮ情報を更新する。
【０００６】
また、図５において、スイッチ５２のポート＃４は既にＶＩＤが設定されているＤＶＬＡＮポートである。端末５１のＭＡＣアドレスは“ＭＡＣ１”、端末５６のＭＡＣアドレスは“ＭＡＣ２”である。スイッチ５２のテーブル５３には、ポート＃１はダウンし、ポート＃４は“ＶＩＤ－１”に設定され、ポート＃ｓはバックボーンポートであることが記憶されている。ＤＶＬＡＮサーバ５４のテーブル５５には、“ＭＡＣ１”の端末に設定されているＶＩＤは“ＶＩＤ－１”、“ＭＡＣ２”の端末に設定されているＶＩＤは“ＶＩＤ－２”、…という対応関係が記憶されている。そして、端末５１は集線装置（ＨＵＢ）５７を介してポート＃４に接続されている。この集線装置５７に新たな端末５６が接続されたとする。
【０００７】
このように既にＶＩＤが設定されているＤＶＬＡＮポートに、異なるＶＬＡＮグループに所属する端末が送信したフレームが受信された場合、所定時間、そのポートがディセーブルされる。即ち、（丸１）集線装置５７が接続されているポート＃４が“ＶＩＤ－１”に設定されている状態で端末５６より送信元ＭＡＣアドレスが“ＭＡＣ２”のフレームが送信される。（丸２）スイッチ５２は、ＭＡＣアドレスが“ＭＡＣ２”である端末５６のＶＩＤをＳＮＭＰによりＤＶＬＡＮサーバに問い合わせる。（丸３）スイッチ５２は、ＤＶＬＡＮサーバが応答した内容から端末５６のＶＩＤが“ＶＩＤ－２”であることを認識し、ポート＃４は“ＶＩＤ－１”に設定されているので、ポート＃４を１０秒間ディセーブル（図中ではロックと表記）にする。
【０００８】
以上のように、ＤＶＬＡＮサーバ５４にひとつひとつの端末固有のＭＡＣアドレスを登録しておき、端末がネットワークに接続されると、その接続ポートを提供した中継装置５２がＤＶＬＡＮサーバ５４に対して認証の手続きを行うことで、端末がＶＬＡＮに接続することができる。
【０００９】
【特許文献１】特開２０００－５９３９３号公報
【発明の開示】
【発明が解決しようとする課題】
【００１０】
上記従来の技術では、ＭＡＣアドレスを根拠にして認証が行われるよう、ＤＶＬＡＮサーバにＭＡＣアドレスが登録されているが、このためには認証の対象になるであろう端末の全てのＭＡＣアドレスをＤＶＬＡＮサーバに予め登録しておかなければならない。しかし、認証の対象になるかもしれないＭＡＣアドレスを前もって登録することは不可能である。例えば、ユーザがパソコンの買い替えなどにより端末を変更した場合、この新しい端末のＭＡＣアドレスがＤＶＬＡＮサーバに既に登録されていることは有り得ない。従って、この新しい端末をネットワークに接続すると、認証の手続きに際して既登録のＭＡＣアドレスが見付からず、認証は否定される。認証が否定されないためには、ユーザが端末を変更する都度、ＤＶＬＡＮサーバにＭＡＣアドレスを登録しなければならず、ユーザやＤ

ＶＬＡＮサーバの管理者に余計な負担がかかるという欠点がある。
【００１１】
以上の問題点をまとめると、次のようになる。
【００１２】
（１）新規なハードウェア（新製品など）が端末として使われると、認証ができない。
【００１３】
（２）一つの端末には固定の一つのＶＩＤ（ＶＬＡＮ情報）が割り振られ、同じ端末を使用するユーザによってＶＩＤが変化しない。
【００１４】
（３）ＤＶＬＡＮサーバ５４とスイッチ５２との間のプロトコルにＳＮＭＰを使用しているため、パスワードの暗号化がなされない。
【００１５】
そこで、本発明の目的は、上記課題を解決し、端末が新規なハードウェアであっても認証の手続きが可能な認証システムを提供することにある。
【課題を解決するための手段】
【００１６】
上記目的を達成するために本発明は、ユーザを特定するための認証ワードが登録されているＲＡＤＩＵＳサーバをネットワーク中に設け、このネットワークに対してフレーム中継を行う中継装置に認証用ＤＨＣＰサーバを設けておき、この中継装置に物理的に接続された端末がＤＨＣＰによりＩＰアドレスを要求したとき、前記認証用ＤＨＣＰサーバから暫定ＩＰアドレスを付与することにより、前記中継装置と前記端末との間でのみ通信可能な閉じた認証用サブネットを形成し、前記中継装置が前記端末から入力された認証ワードを前記ＲＡＤＩＵＳサーバに問い合わせ、このＲＡＤＩＵＳサーバより認証が得られたとき、前記端末から前記ネットワークへの通信を許容するものである。
【００１７】
前記中継装置に認証用ＷＥＢサーバを設けておき、この認証用ＷＥＢサーバが前記端末より送信されたＨＴＴＰパケットを傍受したとき、認証ワードを入力するための認証用ＷＥＢページを前記端末に送信してもよい。
【００１８】
前記ＲＡＤＩＵＳサーバは、ユーザ毎のＶＬＡＮ情報が登録されており、前記端末を認証したときにそのユーザのＶＬＡＮ情報を前記中継装置に通知し、前記中継装置は、通知されたＶＬＡＮ情報により前記端末が接続されているポートをＶＬＡＮ設定してもよい。
【００１９】
前記中継装置は、前記端末がログイン時に所定プロトコルのサーバを参照する場合には、前記認証用サブネット外への通信を許容してもよい。
【発明の効果】
【００２０】
本発明は次の如き優れた効果を発揮する。
【００２１】
（１）端末が新規なハードウェアであっても認証の手続きが可能になり、ユーザがパソコンの買い替えなどにより端末を変更した場合でも、変更前の端末で使用していたユーザ名やパスワードを用いて認証を受けることができる。
【発明を実施するための最良の形態】
【００２２】
以下、本発明の一実施形態を添付図面に基づいて詳述する。
【００２３】
図１に示した本発明に係る端末認証システムにおいて、認証の対象となる端末１はＤＨＣＰクライアントである。この端末１がスイッチングハブ（ＨＳＷ）２に接続されたとき、本発明に係る認証の手順が開始される。この手順において、これから認証を受けようとする端末１を未認証端末１と呼び、未認証端末１とスイッチングハブ２との間で暫定的に

形成される閉じたネットワークを認証用サブネット３と呼ぶ。スイッチングハブ２は、パケットの中継を行う従来より知られているスイッチングハブであると共に、本発明に係る認証用ＷＥＢサーバ２ａと認証用ＤＨＣＰサーバ２ｂとを搭載している。

【００２４】

このスイッチングハブ２はルータＲに接続され、ルータＲには、ＲＡＤＩＵＳサーバ４、ＤＮＳサーバ５、ＤＨＣＰサーバ６、ドメインコントローラ７、他のスイッチングハブ（ＨＳＷ）８などが接続されて、バックボーンとなるネットワークが形成されている。ルータＲは、ネットワーク上の各機器からのパケットをルーティングするもので、これから言及する本発明の動作に直接的には影響を与えない。

【００２５】

認証用ＷＥＢサーバ２ａは、未認証端末１からのＨＴＴＰ（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）パケットをスヌーピング（Ｓｎｏｏｐｉｎｇ；吸い上げる）する機能と、未認証端末１に対して認証用ＷＥＢページを送信する機能と、未認証端末１において認証用ＷＥＢページに入力された認証ワードを受信する機能とを有する。

【００２６】

認証用ＤＨＣＰサーバ２ｂは、未認証端末１からのＩＰアドレスを要求するＤＨＣＰパケットを受信したとき、正式なＤＨＣＰサーバ６に代わって未認証端末１に対して暫定的なＩＰアドレス（暫定ＩＰアドレスという）を提供する機能と、その暫定ＩＰアドレスの有効期限を管理する機能とを有する。

【００２７】

ＲＡＤＩＵＳ（Ｒｅｍｏｔｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｄｉａｌ ｉｎ Ｕｓｅｒ Ｓｅｒｖｉｃｅ）サーバ４は、一種のデータベースであり、認証ワード（例えば、ユーザ名とパスワード）を管理し、その認証結果やユーザ名に対応した種々の情報（例えば、ＶＩＤ）を記憶する。本発明においては、ＲＡＤＩＵＳサーバ４は、スイッチングハブ２からの認証ワードによる問い合わせに対して、データベースから当該認証ワードを検索して許可／不許可の判定を行い、その認証結果及び認証されたＶＩＤをスイッチングハブ２に応答する機能を有する。従来技術においてＤＶＬＡＮサーバが担っていたＤＶＬＡＮ機能は、ＲＡＤＩＵＳサーバ４により実現される。

【００２８】

ＤＮＳ（Ｄｏｍａｉｎ Ｎａｍｅ Ｓｙｓｔｅｍ）サーバ５は、ＴＣＰ／ＩＰのネットワークにおいてＩＰアドレスとホスト名とを対応させたテーブルを管理し、要求されたホスト名に対応するＩＰアドレスを応答することができる。

【００２９】

ＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）サーバ６は、ＩＰアドレスを動的にＤＨＣＰクライアントに配付するもので、本発明に係る認証の手順には関与しないが、認証済み端末からの要求に対しては正式なＩＰアドレスを提供することができる。

【００３０】

ドメインコントローラ７は、ウインドゥズ（登録商標）の規格に従うウインドゥズネットワークを管理するもので、本発明に係る認証の手順には関与しないが、未認証端末１からのウインドゥズネットワークに関する参照要求に対しては応答する。

【００３１】

他のスイッチングハブ８においても、スイッチングハブ２と同様に認証用サブネットが形成できることは言うまでもない。

【００３２】

図１の端末認証システムでは、未認証端末１よりＲＡＤＩＵＳサーバ４へ認証の根拠となる認証ワードを提出し、ＲＡＤＩＵＳサーバ４が認証ワードを検証して認証を行う。認証ワードは、ハードウェアに依存しないデータであって予めユーザ毎に登録されたものである。例えば、認証ワードとして登録時にユーザが任意に定義したユーザ名及びパスワー

ドの２語を用いるとよい。
【００３３】
また、図１の端末認証システムでは、上記した「ユーザ名とパスワード」による認証の他に、認証ワードとハードウェア固有のデータとを併用した「ユーザ名とパスワードとＭＡＣアドレス」による認証、及びハードウェア固有のデータのみで行う「ＭＡＣアドレス」による認証の３通りを選択することができる。以下では、認証に使用するデータ別に認証の手順を説明する。
１）ユーザ名とパスワードを使用する場合（図２参照）
まず、第１のステップ２１は、端末１が電源をオンしてスイッチングハブ２に接続するステップである。ネットワークへの正式な接続（認証された接続）を希望する新たな端末１がスイッチングハブ２の任意のポートに物理的に接続され、かつその端末の電源がオンされたときから、この新規に接続された端末１は、このネットワークにおける未認証端末１となる。
【００３４】
第２のステップ２２は、未認証端末１がＩＰアドレスを要求するステップである。未認証端末１は、ＤＨＣＰサーバ６に対して自身のＩＰアドレスの付与を要求するＤＨＣＰパケットを送信する。
【００３５】
第３のステップ２３は、認証用ＤＨＣＰサーバ２ｂが未認証端末１に暫定ＩＰアドレスを付与するステップである。スイッチングハブ２内の認証用ＤＨＣＰサーバ２ｂは、未認証端末１が送信したＤＨＣＰパケットを受信すると、未認証端末１に対して暫定ＩＰアドレスを格納した応答パケットを送信する。これにより、未認証端末１は暫定ＩＰアドレスが付与され、その後、この暫定ＩＰアドレスを自アドレスとしてスイッチングハブ２との通信を行うことができる。即ち、未認証端末１とこの未認証端末１が接続されているスイッチングハブ２のポートとの間で認証用サブネット３が形成される。ただし、上記暫定ＩＰアドレスには有効期限があり、この有効期限は認証用ＤＨＣＰサーバ２ｂによって管理される。
【００３６】
このように、暫定ＩＰアドレス及び認証用サブネット３は、認証用ＷＥＢサーバ２ａと認証される端末（未認証端末１）との間の通信のために設けられる。また、未認証端末１が認証されると、ＶＩＤ（ＶＬＡＮ）情報が変更され、その変更に伴い端末１の属するサブネットも変更される。そのため、認証前には暫定ＩＰアドレスを一時的に付与しておき、認証後に、変更されたサブネットに属するＩＰを割り当てることになる。
【００３７】
スイッチングハブ２は、未認証端末１に対するデフォルトゲートウェイ及びＤＮＳの設定を行う。図示例では、デフォルトゲートウェイはルータＲであり、ＤＮＳはＤＮＳサーバ５であるから、スイッチングハブ２には、未認証端末１の暫定ＩＰアドレスとルータＲのＩＰアドレスとＤＮＳサーバ５のＩＰアドレスとを対応付けたテーブルが作成される。
【００３８】
第４のステップ２４は、特定のパケットの通過を設定するステップである。未認証端末１にユーザがログインする際に、ドメインコントローラ７やユニックス（登録商標）におけるユーザ名とパスワードとを管理するＮＩＳ（Ｎｅｔｗｏｒｋ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｒｖｉｃｅ）サーバ（図示せず）を参照する必要がある場合がある。このような場合に備えて、予めスイッチングハブ２は、未認証端末１から受信したパケットの宛先がドメインコントローラ７又はＮＩＳサーバであればそのパケットをルータＲに中継するよう、自身に設定をしておく。これにより、その後、未認証端末１が送信したドメインコントローラ７やＮＩＳサーバの宛先を含むパケットは、宛先が認証用サブネット３外にあるにもかかわらず、その宛先へ中継されるようになる。従って、ログインに際して未認証端末１よりドメインコントローラ７やＮＩＳサーバを参照することが可能となる。
【００３９】

第５のステップ２５は、未認証端末１より認証ワードを提出するステップである。ユーザ名とパスワードによる認証を行う場合は、ユーザが未認証端末１においてブラウザを立ち上げる。未認証端末１は、ブラウザの中で適宜なＷＥＢサーバに宛ててＨＴＴＰパケットを送信する。このＨＴＴＰパケットがスイッチングハブ２に到着したとき、スイッチングハブ２内の認証用ＷＥＢサーバ２ａは、この未認証端末１からのＨＴＴＰパケットをスヌーピングする。スヌーピングとは、次のような動作である。例えば、未認証端末１が暫定的に与えられたＩＰアドレスを“１０．１．２．１”だったとすると、認証用サブネット３のサブネットアドレスは“１０．１．２．０”である。一方、未認証端末１が送信したＨＴＴＰパケットの宛先アドレスが“１．１．１．１”であったとすると、この宛先アドレスのサブネットアドレスは認証用サブネット３のサブネットアドレスと一致しない。このようなサブネットアドレスの不一致があったときに、そのパケットの全体を取り込んで何等かの処理を行うことをスヌーピングという。認証用ＷＥＢサーバ２ａは、スヌーピングの結果、未認証端末１に対して認証用ＷＥＢページを返送する。これにより、未認証端末１の表示デバイスには認証用ＷＥＢページが表示される。認証用ＷＥＢページにはユーザ名の記入欄及びパスワードの記入欄があるので、ユーザは自身のユーザ名とパスワードとを記入する。記入するユーザ名及びパスワードは、ユーザが未認証端末１を使用する以前から使用しており、ＲＡＤＩＵＳサーバ４に登録済みのものであることは勿論である。

【００４０】

第６のステップ２６は、スイッチングハブ２よりＲＡＤＩＵＳサーバ４に認証ワードの問い合わせを行うステップである。スイッチングハブ２は、前ステップ２５において未認証端末１を使用するユーザのユーザ名とパスワードとを得ているので、これらの認証ワードを認証問い合わせパケットに格納してＲＡＤＩＵＳサーバ４宛に通知する。

【００４１】

第７のステップ２７は、ＲＡＤＩＵＳサーバ４がスイッチングハブ２に応答を返すステップである。ＲＡＤＩＵＳサーバ４は、認証問い合わせパケットに格納されている認証ワードと自身のデータベースに登録されている認証ワードとを照合し、一致する認証ワードがあるときには、未認証端末１を認証（接続を許可）する。ＲＡＤＩＵＳサーバ４は、認証結果（許可／不許可）をスイッチングハブ２に応答する。また、当該認証ワードで特定されるユーザがＶＬＡＮグループに所属している場合には、そのＶＩＤをスイッチングハブ２に応答する。

【００４２】

第８のステップ２８は、端末１の未認証が解除されるステップである。認証結果が許可であればスイッチングハブ２は、未認証であった端末１からのパケットを無条件でルータＲに中継するようになる。これにより、未認証端末１は認証済み端末１としてネットワークへのフルアクセスが可能になる。前ステップ２７においてＶＩＤが応答された場合には、スイッチングハブ２は、認証用サブネット３を解消し、認証済み端末１が接続されているポートにＶＩＤを設定する。認証結果が不許可であれば、これらの動作は行われない。

【００４３】

第９のステップ２９は、認証済み端末１に正式なＩＰアドレスが付与されるステップである。認証済み端末１は、スイッチングハブ２の認証用ＤＨＣＰサーバ２ｂから与えられた暫定ＩＰアドレスがリースアップ（期限切れ）すると、再度、ＤＨＣＰサーバ６に対して自身のＩＰアドレスの付与を要求するＤＨＣＰパケットを送信する。このとき、認証用ＤＨＣＰサーバ２ｂは、ＤＨＣＰパケットを受信したポートがリースアップしているので、このＤＨＣＰパケットには応答せず、スイッチングハブ２は、このＤＨＣＰパケットをルータＲに中継する。従って、ＤＨＣＰパケットは、正式なＤＨＣＰサーバ６に受信される。ＤＨＣＰサーバ６は、正式なＩＰアドレスを応答するので、認証済み端末１は、正式なＩＰアドレスを獲得することができる。

【００４４】

次に、ログアウトについて説明する。以下のイベントのいずれかが起きると、認証済み

端末は未認証状態になる。
ａ）認証用ＷＥＢサーバ２ａは、宛先が認証用ＷＥＢサーバ２ａになっているＨＴＴＰパケットをスヌーピングし、そのＨＴＴＰパケットの送信元へ認証用ＷＥＢページを返送するようになっている。従って、認証済み端末１が認証用ＷＥＢページにアクセスを試みると、認証用ＷＥＢサーバ２ａから認証用ＷＥＢページが返送される。認証用ＷＥＢページにはログアウトのボタンがあるので、ユーザがそのログアウトのボタンをクリックすると、認証用ＷＥＢサーバはユーザがログアウトを選んだことを認識し、スイッチングハブ２は、このログアウトを希望した認証済み端末１及びその接続ポートを未認証状態にする。
ｂ）スイッチングハブ２は、ポートのリンクが断すると、このポートを未認証状態にする。従って、ユーザが認証済み端末１の電源をオフするか、スイッチングハブ２への伝送路を切り離すと、スイッチングハブ２が当該ポートのリンク断を検出し、そのポートを未認証状態にする。
ｃ）スイッチングハブ２は、各ポートの各種設定に対して時間管理を行っている。認証済み端末１が接続されているポートにおいて、最後のパケットを受信してから所定時間が経過しても新しいパケットが受信されないとき、タイムアウトとなり、スイッチングハブ２はそのポートを未認証状態にする。

【００４５】

以上のログアウト処理により、ユーザが積極的にログアウトを希望した場合、ユーザが端末１を電源オフ又は除去した場合、或いはユーザが端末１を長時間放置している場合には、認証済み端末１は未認証状態になる。

【００４６】

以上、認証ワードとしてユーザ名及びパスワードの２語を用いる場合、次のような効果が得られる。

【００４７】

（１）新規なハードウェア（新製品など）が端末１として使われたときでも、認証ができる。

【００４８】

（２）端末１を使用するユーザによってＶＩＤ（ＶＬＡＮ情報）を変えることができる。

【００４９】

（３）ユーザは、任意のハードウェアを端末１として使用できる。

【００５０】

（４）ＤＶＬＡＮサーバ（図示せず）とスイッチングハブ２との間のプロトコルにＲＡＤＩＵＳを使用することができ、認証ワードの暗号化ができる。

２）ユーザ名とパスワードとＭＡＣアドレスを使用する場合（図３参照）

まず、第１のステップ３１は、端末１が電源をオンしてスイッチングハブ２に接続するステップである。ネットワークへの正式な接続（認証された接続）を希望する新たな端末１がスイッチングハブ２の任意のポートに物理的に接続され、かつその端末の電源がオンされたときから、この新規に接続された端末１は、このネットワークにおける未認証端末１となる。

【００５１】

第２のステップ３２は、未認証端末１がＩＰアドレスを要求するステップである。未認証端末１は、ＤＨＣＰサーバ６に対して自身のＩＰアドレスの付与を要求するＤＨＣＰパケットを送信する。

【００５２】

第３のステップ３３は、認証用ＤＨＣＰサーバ２ｂが未認証端末１に暫定ＩＰアドレスを付与するステップである。スイッチングハブ２内の認証用ＤＨＣＰサーバ２ｂは、未認証端末１が送信したＤＨＣＰパケットを受信すると、未認証端末１に対して暫定ＩＰアドレスを格納した応答パケットを送信する。これにより、未認証端末１は暫定ＩＰアドレスが付与され、その後、この暫定ＩＰアドレスを自アドレスとしてスイッチングハブ２との

通信を行うことができる。即ち、未認証端末１とこの未認証端末１が接続されているスイッチングハブ２のポートとの間で認証用サブネット３が形成される。ただし、上記暫定ＩＰアドレスには有効期限があり、この有効期限は認証用ＤＨＣＰサーバ２ｂによって管理される。

【００５３】

スイッチングハブ２は、未認証端末１に対するデフォルトゲートウェイ及びＤＮＳの設定を行う。図示例では、デフォルトゲートウェイはルータＲであり、ＤＮＳはＤＮＳサーバ５であるから、スイッチングハブ２には、未認証端末１の暫定ＩＰアドレスとルータＲのＩＰアドレスとＤＮＳサーバ５のＩＰアドレスとを対応付けたテーブルが作成される。

【００５４】

第４のステップ３４は、未認証端末１が認証用ＷＥＢサーバ２ａにアクセスし、ユーザ名とパスワードを入力するステップである。未認証端末１が認証用ＷＥＢサーバ２ａにアクセスすると、認証用ＷＥＢサーバ２ａが入力用のページ（ダイアログボックス）を返してくるので、未認証端末１にはそのダイアログボックスが表示される。ダイアログボックスには、ユーザ名を記入する欄とパスワードを記入する欄がある。ユーザがこれらの欄にユーザ名及びパスワードを記入すると、認証用ＷＥＢサーバ２ａにそのユーザ名及びパスワードが入力される。

【００５５】

第５のステップ３５は、スイッチングハブ２がユーザ名とパスワードとＭＡＣアドレスをＲＡＤＩＵＳサーバ４に問い合わせるステップである。ＲＡＤＩＵＳサーバ４には、あらかじめ認証可能なユーザ名とパスワードと端末のＭＡＣアドレスが登録されている。スイッチングハブ２（認証用ＷＥＢサーバ２ａ）は、入力されたユーザ名及びパスワードと端末１からのパケットの送信元ＭＡＣアドレスとをもとにＲＡＤＩＵＳサーバ４に認証問い合わせを行う。

【００５６】

第６のステップ３６は、ＲＡＤＩＵＳサーバ４がスイッチングハブ２に応答を返すステップである。ＲＡＤＩＵＳサーバ４は、認証問い合わせパケットに格納されている認証ワードと自身のデータベースに登録されている認証ワードとを照合し、一致する認証ワードがあるときには、未認証端末１を認証（接続を許可）する。ＲＡＤＩＵＳサーバ４は、認証結果（許可／不許可）をスイッチングハブ２に応答する。また、当該認証ワードで特定されるユーザがＶＬＡＮグループに所属している場合には、そのＶＩＤをスイッチングハブ２に応答する。

【００５７】

第７のステップ３７は、端末１の未認証が解除されるステップである。認証結果が許可であればスイッチングハブ２は、未認証であった端末１からのパケットを無条件でルータＲに中継するようになる。これにより、未認証端末１は認証済み端末１としてネットワークへのフルアクセスが可能になる。前ステップ２７においてＶＩＤが応答された場合には、スイッチングハブ２は、認証用サブネット３を解消し、認証済み端末１が接続されているポートにＶＩＤを設定する。認証結果が不許可であれば、これらの動作は行われない。

【００５８】

第８のステップ３８は、認証済み端末１に正式なＩＰアドレスが付与されるステップである。認証済み端末１は、スイッチングハブ２の認証用ＤＨＣＰサーバ２ｂから与えられた暫定ＩＰアドレスがリースアップ（期限切れ）すると、再度、ＤＨＣＰサーバ６に対して自身のＩＰアドレスの付与を要求するＤＨＣＰパケットを送信する。このとき、認証用ＤＨＣＰサーバ２ｂは、ＤＨＣＰパケットを受信したポートがリースアップしているので、このＤＨＣＰパケットには応答せず、スイッチングハブ２は、このＤＨＣＰパケットをルータＲに中継する。従って、ＤＨＣＰパケットは、正式なＤＨＣＰサーバ６に受信される。ＤＨＣＰサーバ６は、正式なＩＰアドレスを応答するので、認証済み端末１は、正式なＩＰアドレスを獲得することができる。

【００５９】

以上、認証ワードとしてユーザ名とパスワードとＭＡＣアドレスの３語を用いる場合、次のような効果が得られる。

【００６０】

（１）端末１を使用するユーザによってＶＩＤ（ＶＬＡＮ情報）を変えることができる。

【００６１】

（２）ユーザが端末１として使用するハードウェアを制限することができる。

【００６２】

（３）ＤＶＬＡＮサーバ（図示せず）とスイッチングハブ２との間のプロトコルにＲＡＤＩＵＳを使用することができ、認証ワードの暗号化ができる。

【００６３】

以上説明したように、本発明では、未認証端末１よりＲＡＤＩＵＳサーバ４へ認証の根拠となる認証ワードを提出し、ＲＡＤＩＵＳサーバ４が認証ワードを検証して認証を行うようにしたので、端末が新規なハードウェアであっても認証の手続きが可能である（認証ワードにＭＡＣアドレスを含まない場合）。

【００６４】

また、ＲＡＤＩＵＳサーバ４にユーザ毎のＶＩＤを登録しておき、認証の応答と共にＶＩＤを応答するようにしたので、中継装置では新たに認証された端末が接続されているポートにＶＩＤを設定することができる。即ち、ＶＬＡＮの動的割当が可能である。

【００６５】

また、本発明においては、スイッチングハブ２は、既に認証されたポートは認証された一つの端末１からのパケットしか中継しない。このため、認証された端末以外の端末からのパケットが認証済みポートで受信されても、そのパケットは廃棄される。

【００６６】

なお、ＲＡＤＩＵＳサーバ４とスイッチングハブ２との間の通信は暗号化されているものとする。従って、未認証端末１からパスワードを入力するステップが手順に含まれていても、そのパスワードを伝送路上で盗聴することは難しい。

【図面の簡単な説明】

【００６７】

【図１】本発明の一実施形態を示す端末認証システムが動作するネットワークの構成図である。

【図２】本発明の認証手順のうち認証ワードがユーザ名とパスワードである場合の流れ図である。

【図３】本発明の認証手順のうち認証ワードがユーザ名とパスワードとＭＡＣアドレスである場合の流れ図である。

【図４】従来のＤＶＬＡＮ機能が動作するネットワークの構成図である。

【図５】従来のＤＶＬＡＮ機能が動作するネットワークの構成図である。

【符号の説明】

【００６８】

１　端末（未認証端末、認証済み端末）

２　スイッチングハブ

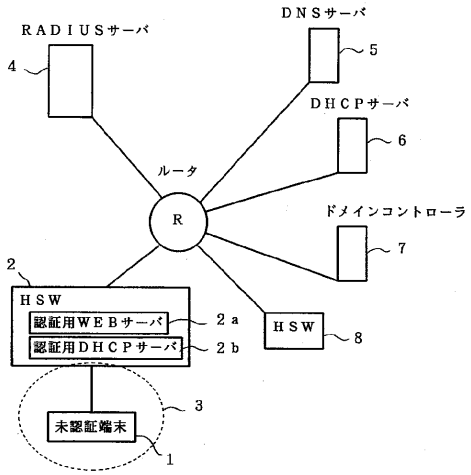
２ａ　認証用ＷＥＢサーバ

２ｂ　認証用ＤＨＣＰサーバ

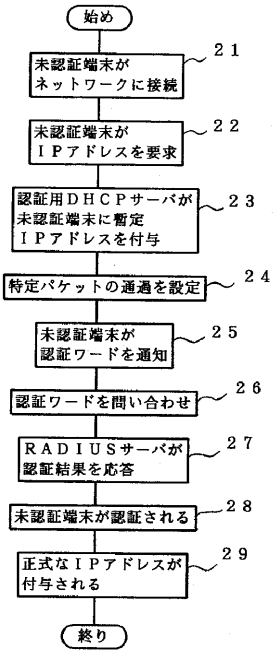
３　認証用サブネット

４　ＲＡＤＩＵＳサーバ

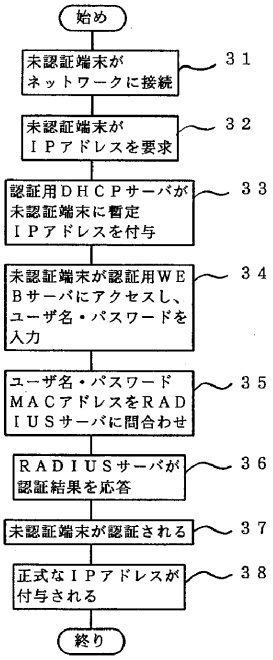
【図１】


ＲＡＤＩＵＳサーバ
4
ＤＮＳサーバ
5
ＤＨＣＰサーバ
6
ルータ
R
ドメインコントローラ
7
2
ＨＳＷ
認証用ＷＥＢサーバ
2ａ
認証用ＤＨＣＰサーバ
2ｂ
ＨＳＷ
8
3
未認証端末
1

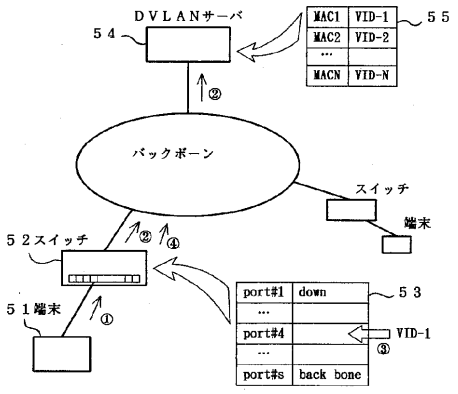
【図２】


始め
未認証端末が
ネットワークに接続
21
未認証端末が
ＩＰアドレスを要求
22
認証用ＤＨＣＰサーバが
未認証端末に暫定
ＩＰアドレスを付与
23
特定パケットの通過を設定
24
未認証端末が
認証ワードを通知
25
認証ワードを問い合わせ
26
ＲＡＤＩＵＳサーバが
認証結果を応答
27
未認証端末が認証される
28
正式なＩＰアドレスが
付与される
29
終り

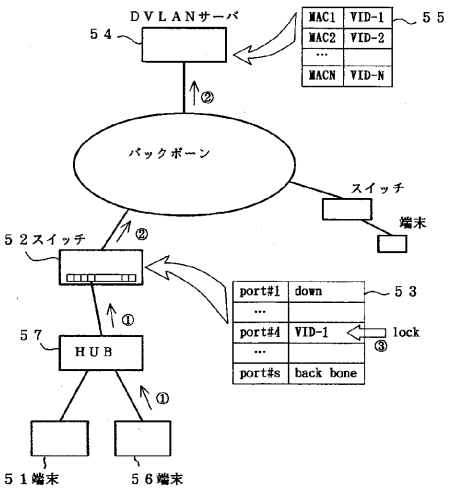
【図３】


始め
未認証端末が
ネットワークに接続
31
未認証端末が
ＩＰアドレスを要求
32
認証用ＤＨＣＰサーバが
未認証端末に暫定
ＩＰアドレスを付与
33
未認証端末が認証用ＷＥＢサーバにアクセスし、
ユーザ名・パスワードを
入力
34
ユーザ名・パスワード
ＭＡＣアドレスをＲＡＤＩＵＳサーバに問合わせ
35
ＲＡＤＩＵＳサーバが
認証結果を応答
36
未認証端末が認証される
37
正式なＩＰアドレスが
付与される
38
終り

【図４】


ＤＶＬＡＮサーバ
54
MAC1 VID-1
MAC2 VID-2
MACN VID-N
55
②
バックボーン
スイッチ
端末
52スイッチ
②
④
51端末
①
port#1 down
port#4
port#s back bone
53
VID-1
③

【図５】


ＤＶＬＡＮサーバ
５４
MAC1 VID-1
MAC2 VID-2
MACN VID-N
５５
②
バックボーン
スイッチ
端末
５２スイッチ
②
port#1 down
port#4 VID-1
port#s back bone
５３
lock
③
①
５７
ＨＵＢ
①
５１端末
５６端末