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

特許第5937563号
(P5937563)

(45)発行日　平成28年6月22日(2016.6.22)　(24)登録日　平成28年5月20日(2016.5.20)

(51)Int.Cl.		F I		
H04W 8/26	(2009.01)	H04W	8/26	110
H04W 84/10	(2009.01)	H04W	84/10	
H04W 88/08	(2009.01)	H04W	88/08	
H04L 12/28	(2006.01)	H04L	12/28	200Z

請求項の数 4　(全 17 頁)

(21)出願番号　特願2013-226219(P2013-226219)
(22)出願日　平成25年10月31日(2013.10.31)
(65)公開番号　特開2014-212507(P2014-212507A)
(43)公開日　平成26年11月13日(2014.11.13)
審査請求日　平成25年10月31日(2013.10.31)
(31)優先権主張番号　特願2013-78487(P2013-78487)
(32)優先日　平成25年4月4日(2013.4.4)
(33)優先権主張国　日本国(JP)

前置審査

(73)特許権者　397036309
株式会社インターネットイニシアティブ
東京都千代田区富士見二丁目10番2号
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100101373
弁理士　竹内　茂雄
(74)代理人　100118902
弁理士　山本　修
(74)代理人　100196508
弁理士　松尾　淳一

最終頁に続く

(54)【発明の名称】通信基地局およびその制御方法

(57)【特許請求の範囲】
【請求項１】
複数の通信端末と、
前記複数の通信端末のためのアクセスポイントとして機能する複数の通信基地局と、
前記複数の通信端末のそれぞれを物理的に識別する物理アドレスと前記複数の通信基地局のそれぞれを識別するデータとのすべての組合せと、前記組合せのそれぞれが用いることができるネットワークのネットワークアドレスとの対応関係が記憶されているデータベースと、
前記複数の通信基地局の中の１つの通信基地局において前記複数の通信端末の中の１つの通信端末から受信された通信リクエストに応答して、前記通信リクエストに含まれている物理アドレスと前記通信リクエストを受信した前記１つの通信基地局を識別するデータとの組合せに対応するネットワークアドレスを前記データベースから取得し、取得された前記ネットワークアドレスを前記１つの通信端末に提供することにより、前記１つの通信端末が、前記１つの通信基地局と前記提供されたネットワークアドレスによって識別されるネットワークとを経由して通信することを可能にするように構成された通信制御手段と、を備えていることにより、
前記複数の通信端末のそれぞれが、相互に論理的に隔離されたネットワークを経由して通信をすることを可能にする通信システム。
【請求項２】
複数の通信端末と、前記複数の通信端末のためのアクセスポイントとして機能する複数

の通信基地局と、前記複数の通信端末のそれぞれを物理的に識別する物理アドレスと前記複数の通信基地局のそれぞれを識別するデータとの組合せと、前記組合せのそれぞれが用いることができるネットワークのネットワークアドレスとの対応関係が記憶されているデータベースと、前記複数の通信端末のそれぞれから前記ネットワークを介する論理的に隔離された複数の通信回線を形成する通信制御手段とを備えている通信システムを制御する方法であって、

前記通信制御手段が、前記複数の通信基地局の中の１つの通信基地局において前記複数の通信端末の中の１つの通信端末から受信された通信リクエストに応答して、前記通信リクエストに含まれている物理アドレスと前記通信リクエストを受信した前記１つの通信基地局を識別するデータとの組合せに対応するネットワークアドレスを前記データベースから取得するステップと、

前記通信制御手段が、前記取得された前記ネットワークアドレスを前記１つの通信端末に提供することにより、前記１つの通信端末が前記提供されたネットワークアドレスによって識別されるネットワークを経由して通信することを可能にするステップと、を含んでいることにより、

前記複数の通信端末のそれぞれが、相互に論理的に隔離されたネットワークを経由して通信をすることを可能にする方法。

【請求項３】

請求項２に記載された方法をコンピュータに実行させるコンピュータプログラム。

【請求項４】

請求項３に記載されたコンピュータプログラムが記憶されているコンピュータ可読な記憶媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、通信技術に関する。より詳しくは、本発明は、ノートＰＣやスマートホンなどの通信端末をネットワークに接続するための通信基地局に関する。

【０００２】

以下では無線通信を例に用いて説明を行う。しかし、本発明は、有線通信であるか無線通信であるかを問わずに適用可能である。

【背景技術】

【０００３】

近年、ＷｉＦｉなどの無線通信を介してネットワークに接続し、リモートオフィスなどにアクセスする機会が増えている。しかし、ネットワークを介した不正アクセスが横行し、より安全な通信手段の実現が必要とされている。

【０００４】

従来の無線通信では、１つの無線基地局（アクセスポイント）に接続される複数の無線端末は、同一のＩＰアドレスレンジを用いることが一般的である。その結果として、これら複数の無線端末間の通信はＩＰレイヤで接続され、ＩＰレイヤで個々の無線端末を隔離できない。また、１つのアクセスポイントにおいて、複数の論理アクセスポイント識別子であるサービスセット識別子（ＳＳＩＤ）を利用した場合であっても、一つのＳＳＩＤに接続する複数の無線端末間では、同一のＩＰアドレスやＩＰアドレスレンジが割り振られるため、やはり、ＩＰレイヤで個々の無線端末を隔離することができない。

【０００５】

その結果、これら複数の無線端末は、論理的に分離されていないネットワークを介して通信を行うことになる。例えば、転送されるパケットの識別子を用いて、仮想回線相互間が分離されているだけである。このように、従来の無線通信では、同一の無線基地局を介して通信をする複数の無線端末間の通信を分離する仕組みは存在していない。また、無線基地局で利用できるＩＰアドレス数や、ＩＰアドレスレンジを容易に増やせる仕組みは存在しない。このような技術的な状況が、無線通信の安全性に問題が生じる原因となってい

る。
【０００６】
本発明と関連する可能性がある先行技術文献をサーチしたところ、下記の３つの特許文献が発見された。しかし、特許文献１は、端末固有の識別子ではなく、呼の識別子を利用しているところが本発明とは異なる。また、特許文献１記載の発明は、ＩＰアドレスや、ＩＰアドレスレンジを払い出す仕組みを持っていない。また、特許文献２は、リング構成のネットワークに複数の無線基地局が接続され、その無線基地局間でＡＴＭなどを利用した論理回線（仮想回線）を構築する方法であり、本発明とは異なる。更に、特許文献３は、無線端末から仮想回線識別を受信し、ＯＡＭセルを利用して仮想回線を管理する仕組みであり、本発明とは異なっている。
【０００７】
また、公刊された文献ではないが、<http://www.connect802.com/download/aruba/AP-2E.pdf>では、米国アルバネットワークス社（Aruba Networks）から市販されている製品に関する説明がなされている。この文書には、全ての無線基地局から一元的にＩＰレベルのＧＲＥトンネルを利用して管理サーバ（コントローラ）にトンネルを構築する技術が記載されている。しかし、アルバネットワークス社のこの製品は、個々の無線端末毎に仮想回線を作る事はできない点で、本発明とは異なっている。
【先行技術文献】
【特許文献】
【０００８】
【特許文献１】特開平０６－０８６３５６
【特許文献２】特開平０７－２１２３７５
【特許文献３】特開平０８－２４２２３１
【発明の概要】
【発明が解決しようとする課題】
【０００９】
本発明は、上述した従来の無線通信における問題点を解決するために、ＡＰに接続する複数の無線端末がそれぞれ論理的に閉じた閉域ネットワークを構成できることを可能にすることによって、無線通信の安全性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】
【００１０】
本発明によると、複数の通信端末がネットワークに接続する際にネットワークへのアクセスポイントとして機能する通信基地局であって、複数の通信端末のそれぞれを物理的に識別する物理アドレスに対応するネットワークアドレスが記憶されているデータベースと、複数の通信端末から受信された通信リクエストに応答して、通信リクエストに含まれているそれぞれの通信端末の物理アドレスに対応するネットワークアドレスをデータベースから取得し、取得されたネットワークアドレスを用いて複数の通信端末のそれぞれからネットワークを介する論理的に隔離された複数の通信回線を形成する通信制御手段と、を備えている通信基地局が提供される。
【００１１】
このような通信制御手段において、ネットワーク経路制御や通信回線の帯域制御の機能をネットワークスイッチなどのネットワーク装置から分離して、サーバなどのコントローラで一元管理する仕組みであるＳＤＮ（Software Defined Network）と称される技術が存在する。本発明でも、このＳＤＮの技術を利用することが可能である。
【００１２】
また、本発明によると、上述した通信制御手段が、複数の通信端末のそれぞれに異なるＩＰアドレスまたはＩＰレンジを割り当てる手段を更に備えていることを特徴とする通信基地局が提供される。
【００１３】
更にまた、本発明によると、ネットワーク上に形成される複数の論理的通信回線をＶＸ

ＬＡＮなどのレイヤ３で構成することにより、インターネットなどの広域ＩＰネットワーク上に複数の論理的通信回線を形成する手段を更に備えていることを特徴とする通信基地局が提供される。

【００１４】

更にまた、本発明によると、ネットワーク上に形成される複数の論理的通信回線をＶＬＡＮやＭＰＬＳなどのレイヤ２で構成することにより、複数の論理的通信回線を形成する手段を更に備えていることを特徴とする通信基地局が提供される。

【００１５】

更にまた、本発明によると、複数の通信端末と、複数の通信端末がネットワークに接続する際にネットワークへのアクセスポイントとして機能する複数の通信基地局と、複数の通信端末のそれぞれの物理アドレスと複数の通信基地局のそれぞれの識別データとの組に対応するネットワークアドレスが記憶されているデータベースと、複数の通信端末から受信された通信リクエストに応答して、通信リクエストに含まれているそれぞれの通信端末の物理アドレスとそれぞれの通信端末がアクセスしている通信基地局の識別データとに対応するネットワークアドレスをデータベースから取得し、取得されたネットワークアドレスを用いて複数の通信端末のそれぞれからネットワークを介する論理的に隔離された複数の通信回線を形成する通信制御手段と、を備えている通信システムが提供される。

【００１６】

本発明によると、複数の通信端末がネットワークに接続する際にネットワークへのアクセスポイントとして機能する通信基地局であって、複数の通信端末を物理的に識別する物理アドレスに対応するネットワークアドレスが記憶されているデータベースと、複数の通信端末のそれぞれからネットワークを介する論理的に隔離された複数の通信回線を形成する通信制御手段とを備えている通信基地局を制御する方法であって、通信制御手段が、複数の通信端末から受信された通信リクエストに応答して、通信リクエストに含まれているそれぞれの通信端末の物理アドレスに対応するネットワークアドレスをデータベースから取得するステップと、通信制御手段が、取得されたネットワークアドレスを用いて複数の通信端末のそれぞれから前記ネットワークを介する論理的に隔離された複数の通信回線を形成するステップと、を含む方法が提供される。

【００１７】

更にまた、本発明によると、上述した通信制御手段が、複数の通信端末のそれぞれに異なるＩＰアドレスまたはＩＰアドレスレンジを割り当てる手段を更に備えていることを特徴とする方法が提供される。

【００１８】

更にまた、本発明によると、上述した通信基地局が、ネットワーク上に形成される複数の論理的通信回線をＶＸＬＡＮなどのレイヤ３で構成することにより、インターネットなどの広域ＩＰネットワーク上に複数の論理的通信回線を形成する手段を更に備えていることを特徴とする方法が提供される。

【００１９】

更にまた、本発明によると、上述した通信基地局が、ネットワーク上に形成される複数の論理的通信回線をＶＬＡＮやＭＰＬＳなどのレイヤ２で構成することにより、複数の論理的通信回線を形成する手段を更に備えていることを特徴とする方法が提供される。

【００２０】

更にまた、本発明によると、複数の通信端末と、複数の通信端末がネットワークに接続する際にネットワークへのアクセスポイントとして機能する複数の通信基地局と、複数の通信端末のそれぞれの物理アドレスと複数の通信基地局のそれぞれの識別データとの組に対応するネットワークアドレスが記憶されているデータベースと、複数の通信端末のそれぞれからネットワークを介する論理的に隔離された複数の通信回線を形成する通信制御手段とを備えている通信システムを制御する方法であって、通信制御手段が、複数の通信端末のそれぞれから受信された通信リクエストに応答して、通信リクエストに含まれているそれぞれの通信端末の物理アドレスとそれぞれの通信端末がアクセスしている通信基地局

の識別データとの組に対応するネットワークアドレスをデータベースから取得するステップと、通信制御手段が、取得されたネットワークアドレスを用いて複数の通信端末のそれぞれからネットワークを介する論理的に隔離された複数の通信回線を形成するステップと、を含む方法が提供される。

【００２１】

更にまた、本発明によると、上述した方法をコンピュータに実行させるコンピュータプログラムが提供される。

【００２２】

更にまた、本発明によると、上述したコンピュータプログラムが記憶されているコンピュータ可読な記憶媒体が提供される。

【図面の簡単な説明】

【００２３】

【図１】本発明の実施例１の構成を概略的に示すブロック図である。

【図２】実施例１において、コントローラＣＴＬに接続されたデータベースＤＢに格納されているデータの対応関係を示す図である。

【図３】実施例１において、コントローラＣＴＬに接続された別のデータベースＤＢに格納されているデータの対応関係を示す図である。

【図４】実施例１におけるコントローラＣＴＬの構成を示す図である。

【図５】実施例１における無線基地局ＡＰの構成図である。

【図６】実施例１におけるフローＤＢの構成図である。

【図７】実施例１におけるサーバに格納されているデータを示す図である。

【図８】実施例１の無線基地局ＡＰによる個別的な処理を示すフローチャートである。

【図９】実施例１において、ＩＰアドレスを割り当てる際の処理を示すフローチャートである。

【図１０】実施例１における、フロー設定とＩＰアドレスの問合せ処理のシーケンス図である。

【図１１】本発明の実施例２の構成を概略的に示すブロック図である。

【図１２】実施例２におけるルータＲＴの構成図である。

【図１３】実施例２におけるスイッチＤＢの構成図である。

【図１４】本発明の実施例３の構成を概略的に示すブロック図である。

【図１５】本発明の実施例４の構成を概略的に示すブロック図である。

【図１６】本発明の実施例５の構成を概略的に示すブロック図である。

【図１７】実施例５において、コントローラＣＴＬに接続されたデータベースＤＢに格納されているデータの対応関係を示す図である。

【図１８】実施例５において、コントローラＣＴＬに接続された別のデータベースＤＢに格納されているデータの対応関係を示す図である。

【図１９】本発明の実施例５の別の構成を概略的に示すブロック図である。

【発明を実施するための形態】

【実施例１】

【００２４】

図１は、本発明の実施例１の構成を示すブロック図であり、２つの異なる無線端末ＮＤ１およびＮＤ２が、無線基地局ＡＰにアクセスし、ネットワークを経由して、サーバＳＶ１およびＳＶ２に接続する様子を概略的に示している。例えばノートＰＣやスマートホンである無線端末ＮＤ１およびＮＤ２は、同じ無線基地局ＡＰをネットワークへのアクセスポイントとして用い、ネットワークを経由して、２つの異なるサーバＳＶ１およびＳＶ２にそれぞれ接続される。本発明によると、無線端末ＮＤ１からサーバＳＶ１への通信と無線端末ＮＤ１からサーバＳＶ２への通信とを、論理的に分離することが可能である。以下では、どのような仕組みによって通信の論理的分離が可能になるのかについて、具体的な実施例を用いて説明する。

【００２５】

まず、無線端末ＮＤ１は、ＩＥＥＥ８０２．１ａなどのＷｉＦｉ通信（３ＧやＬＴＥなどでも構わない）を用いて無線基地局ＡＰに通信リクエストを送信する。無線基地局ＡＰは、受信した通信リクエストから無線端末ＮＤ１を物理的に識別するＭＡＣアドレスを取得し、コントローラＣＴＬに、無線基地局ＮＤ１の通信許可と、無線基地局ＮＤ１が利用できる仮想回線のネットワークアドレスとを求める。

【００２６】

コントローラＣＴＬは、データベースＤＢを検索することにより、通信リクエストを送信してきた無線端末ＮＤ１の通信を許可すべきかどうか判断して、無線端末ＮＤ１の接続ネットワークアドレスＮＥＴＡＤＤＲ１を無線基地局ＡＰに返す。ＮＥＴＡＤＤＲ１は、ＩＰアドレスでも、ＭＰＬＳなどのＳＩＭヘッダでも構わない。無線基地局ＡＰは通信端末ＮＤ１にネットワークアドレスＮＥＴＡＤＤＲ１を与える。ＮＥＴＡＤＤＲ１は、複数のネットワークアドレスで構成されるアドレスレンジの場合、そのアドレスレンジから一つのネットワークアドレスが、無線基地局ＡＰによって提供される。以上のようにして、無線基地局ＡＰは、無線端末ＮＤ１と同じネットワークアドレスレンジのＳＶ１との間を接続する通信回路を構築し、無線端末ＮＤ１とサーバＳＶ１とが通信できるようになる。この通信回路は予め作られていても構わない。同様に無線端末ＮＤ２はサーバＳＶ２と通信出来るようになる。しかし、複数の無線端末と複数のサーバとの間の通信は相互に論理的に隔離されている。つまり、無線端末ＮＤ１やサーバＳＶ１は、無線端末ＮＤ２やサーバＳＶ２と通信することができない。

【００２７】

以上の処理をより詳細に説明する。コントローラＣＴＬに接続された（または、内蔵された）データベースＤＢには、図２に示されているように、通信を許可する無線端末のＭＡＣアドレスと、そのＭＡＣアドレスを持つ無線端末が利用する仮想回線のネットワークアドレスと、無線基地局ＡＰ内で利用するポート番号とが予め格納されている。コントローラＣＴＬは、ＭＡＣアドレスをキーとしてデータベースＤＢを検索し、対応するネットワークアドレスとポート番号とを取得して、無線基地局ＡＰに与える。

【００２８】

また、仮想回線を利用して無線基地局ＡＰを介したネットワークを構成する場合には、図３に示されているように、データベースＤＢには、仮想回線を構成する通信プロトコル、その通信プロトコルで利用する仮想回線のネットワークアドレス（例えば、Ｌ２ネットワーク仮想化識別子）が予め管理されていることになる。無線基地局ＡＰによって、無線端末ＮＤ１が利用するＩＰアドレスまたはＩＰアドレスレンジが与えられる場合には、Ｌ３ネットワークアドレス範囲をＤＢで管理しておく。これにより、コントローラＣＴＬは、無線端末ＮＤ１のＭＡＣアドレスに基づく無線基地局ＡＰからの問い合わせに対し、利用する仮想回線ＩＤ（仮想化識別子）やそのプロトコルの種類（仮想化プロトコル）を、更には、必要な場合には無線端末ＮＤ１に割り当てるＩＰアドレスレンジを、無線基地局ＡＰに送信する。

【００２９】

次に、コントローラＣＴＬの機能とデータベースＤＢの構成との詳細を説明する。図４に示されているように、コントローラＣＴＬは、フロー規制生成装置とフロー規制送信装置とを含む。データベースＤＢは、図２に示されている対応関係が格納されたＭＡＣアドレス・ネットワークアドレスデータベースと、図３に示されている対応関係が格納されたＬ３アドレス割当状態データベースとから構成される。

【００３０】

コントローラＣＴＬは、無線基地局ＡＰからのＭＡＣアドレスに基づく問い合わせに対し、フロー規制生成装置により、無線端末ＮＤ１が利用できる通信（フロー）を制御する。具体的には、ＭＡＣアドレス・ネットワークアドレスデータベースを利用し、該当するＭＡＣアドレスに対して仮想回線ＩＤと無線基地局ＡＰ上で利用するポート情報とを生成する。コントローラＣＴＬは、フロー規制送信装置を利用して生成したこれらの情報を、無線基地局ＡＰに送信する。

【００３１】
無線基地局ＡＰから無線端末ＮＤ１にＩＰアドレスまたはＩＰアドレスレンジを割り当てる必要がある場合には、コントローラＣＴＬの中のフロー規制生成装置がＬ３アドレス割当状態データベースを検索して、無線端末ＮＤ１に割り当てるＩＰアドレスまたはＩＰアドレスレンジを決定し、フロー規制送信装置から無線基地局ＡＰに、割り当てられたＩＰアドレスまたはＩＰアドレスレンジを送信する。
【００３２】
次に、上記ＣＴＬより送信された情報に基づく無線基地局ＡＰの動作について説明する。図５は無線基地局ＡＰの構成図である。図５の右端にある有線ポートはサーバＳＶ１やＳＶ２に接続され、または、他のネットワーク装置を経由してサーバＳＶ１およびＳＶ２と通信する。無線基地局ＡＰは、制御ポートを介してコントローラＣＴＬと接続され通信するが、必要に応じて、有線ポートを介してＣＴＬと接続される場合もある。無線ポートは、ＷｉＦｉなどの無線プロトコルを介して複数の無線端末ＮＤ１やＮＤ２と通信する。ＣＴＬより受信する仮想回線ＩＤとポート番号は、フローＤＢに記録される。フローは、個々の無線端末が利用することになる仮想回線ＩＤとポート番号とによって管理される。フローＤＢに記録された仮想回線ＩＤに基づいて、Ｌ２ネットワーク仮想化装置により仮想回線が形成される。この際、有線ポートを出力ポートとして仮想回線が形成される。フローＤＢの構成は、図６に示されている。
【００３３】
コントローラＣＴＬから受信するＩＰアドレスまたはＩＰアドレスレンジは、Ｌ３アドレス割当装置を介して個々の無線端末に割り当てられる。割り当てられたＩＰアドレスまたはＩＰアドレスレンジは無線端末で利用される。マッチング回路では、未知のＭＡＣアドレスを無線端末より受信した場合に、制御ポートを介してコントローラＣＴＬに通信許可とフロー制御やＩＰアドレスの新たな割り当てを要求する。また、マッチング回路では、無線基地局ＡＰで管理されたフロー（フローＤＢ内に記録されたフロー）に対して、個々の仮想回線とＩＰアドレスを接続する。これにより、個々の無線端末とそれぞれの無線端末に対応するサーバとの間で、論理的に隔離された通信環境の中で通信出来るようになり、通信セキュリティが格段に向上する。
【００３４】
なお、以上の説明では、無線基地局ＡＰを介してコントローラＣＴＬから無線端末ＮＤ１やＮＤ２にＩＰアドレスまたはＩＰアドレスレンジを割り当てた。しかし、ＩＰアドレスまたはＩＰアドレスレンジは、サーバＳＶ１やＳＶ２によって割り当てられてもよい。サーバによる割り当てがなされる場合には、サーバに、図７に示されたデータが予め格納されている。この場合、コントローラＣＴＬから無線基地局ＡＰへはフロー情報である仮想回線のネットワークアドレスとポート情報とが送信され、無線端末とサーバとの間は、仮想回線を介して接続される。次に、無線端末からはＤＨＣＰなどのプロトコルを通じて、サーバに利用するＩＰアドレスの問い合わせを行い、サーバは、図７の情報を用いて、問い合わせに来た無線端末のＭＡＣアドレスに基づいてＩＰアドレスを払い出す。
【００３５】
以上で本発明による無線基地局ＡＰの動作の概略を説明したが、個別的な処理が図８のフローチャートに示されている。図８に示されているように、ＡＰでパケットを受信した場合、受信ポートが有線ポートからのものか、無線ポートからのものかを判定する。有線ポートからパケットを受信した場合には、宛先ＭＡＣルールマッチング処理により通信先の無線端末のＭＡＣアドレスが登録されているかどうかを判断し、登録されてない場合には受信パケットを破棄する。一方で宛先ＭＡＣルールマッチングに登録されている場合には、仮想ネットワークのヘッダを除去（仮想ネットワークのトンネルを除去）して、対象となる無線端末の無線ポートへパケットを送出する。
【００３６】
一方で、無線ポートからパケットを受信した場合には、送信元ＭＡＣルールマッチングにより、既に登録されている場合には、アドレス要求パケット処理によりＩＰアドレスを

割り当てる要求のパケットかどうかを判断し、ＩＰアドレス要求のパケットであれば、アドレス割当処理にてＩＰアドレス、またはＩＰアドレスレンジを割り当てる。受信したパケットがアドレス要求パケットではない場合には、仮想ネットワーク回線にトンネリング処理するために、Ｌ２仮想化ヘッダ挿入し、有線ポートへパケットを送出する。

【００３７】

また、送信元ＭＡＣルールマッチングにて、登録されていないパケットの場合には、コントローラＣＴＬにＭＡＣアドレス問合せを実施し、フロールールを受信し、ルール種別にてルールの登録許可の場合には、ルールを登録し、ルール種別にてルール登録拒絶の場合には、パケットを破棄する。

【００３８】

また、ＩＰアドレスを割り当てる際の処理フローチャートが図９に示されている。アクセスポイントＡＰからコントローラＣＴＬにＩＰアドレス、またはＩＰアドレスレンジを要求する場合には、ＣＴＬにアドレス要求を出し、その結果としてＣＴＬより返答受信する。返答受信した結果、ＩＰアドレス、またはＩＰアドレスレンジの割当に成功した場合には、無線端末にアドレス割当の情報を送出する。ＩＰアドレス、またはＩＰアドレスレンジの割当に失敗した場合には、パケット破棄処理により、無線端末への応答を中止したり、割当失敗を通知したりする。

【００３９】

更に、フロー設定とＩＰアドレスの問合せ処理のシーケンス図が図１０に示されている。無線端末ＮＤは、アクセスポイントＡＰに無線接続した後にアドレス要求をおこなう。ＡＰはＮＤのＭＡＣアドレスの情報を検索・認証キーとして、コントローラＣＴＬにＭＡＣ問合せをおこない、ＣＴＬからＡＰにフロールールが送信される。フロールールはＡＰ内で登録などの処理が行われる。続いてＡＰからＣＴＬに対してアドレス要求を行い、ＣＴＬからＡＰに対してＩＰアドレス、またはＩＰアドレスレンジのアドレス割当てを行う。続いて、ＡＰからＮＤに対してＩＰアドレス、またはＩＰアドレスレンジのアドレス割当てを行う。続いてＮＤからサーバＳＶへのアクセス処理が開始され、ＡＰを介して仮想ネットワーク回線等を通してＳＶにサーバアクセス情報が送信される。ＳＶからサーバアクセスに対するサーバレスポンスがＡＰに送信され、ＡＰはそのサーバレスポンスをＮＤに送信する。

【実施例２】

【００４０】

以上は、図１のネットワーク構成に基づく実施例１について説明を行ったが、次に、図１１に示されている異なるネットワーク構成の実施例２の場合について説明する。図１１の構成と図１の構成との違いは、図１１では、無線基地局ＡＰにネットワーク装置であるルータＲＴが接続され、サーバＳＶ１やＳＶ２がルータに接続されていることである。処理のシーケンスの違いは、ＣＴＬからＲＴに対して、ＲＴ上で設定するフロー情報である仮想回線のネットワークアドレスと利用するポート（必要に応じて仮想化プロトコルの種類の情報）が送信されることである。そして、ＡＰとＲＴ間で仮想回線が形成されることである。

【００４１】

実施例２では、Ｗｉ Ｆｉ無線端末ＮＤ１が無線基地局ＡＰにＷｉ Ｆｉまたは３ＧやＬＴＥ無線通信を利用して接続する。無線基地局ＡＰは無線通信を用いてＮＤ１の個体識別ＩＤ（ＭＡＣアドレス）を取得し、ＡＰの制御システムＣＴＬにＭＡＣアドレスを識別にした通信許可を問い合わせる。ＣＴＬはＭＡＣアドレス毎の通信許可を登録したデータベースＤＢを用いて通信許可を判断し、ＡＰとルータＲＴ間の論理トンネルを作成しＮＤ１がリモートに位置するサーバＳＶ１とＥｔｈｅｒｎｅｔ（登録商標）などで接続できるようにする。このトンネルは予め作られていても構わない。Ｅｔｈｅｒｎｅｔの代わりにＶＬＡＮやＡＴＭ回線レベルで接続するようにしても構わない。

【００４２】

ＥｔｈｅｒｎｅｔレベルでＮＤ１とＳＶ１が接続された後、ＳＶ１からＮＤ１に対して

ＮＥＴＡＤＤＲ１を払い出す。ＮＥＴＡＤＤＲ１はＩＰアドレスでも、ＭＰＬＳなどのＳＩＭヘッダでも構わない。ＮＥＴＡＤＤＲ１は、複数のネットワークアドレスで構成されるアドレスレンジの場合、そのアドレスレンジから一つのネットワークアドレスがＡＰにより払いださせる。このようにして、ＡＰはＮＤ１と同じネットワークアドレスレンジのＳＶ１間を接続する通信回路を構築し、ＮＤ１はサーバＳＶ１と通信できるようになる。同様に無線端末ＮＤ２はサーバＳＶ２と通信出来るようになる。しかし、実施例１の場合と同様に、この実施例２でも、上記ＮＤ１とＳＶ１は、ＮＤ２やＳＶ２と通信することが出来ず、隔離される通信回路を構築できる。

【００４３】

なお、図１２には、ルータＲＴの構成図が示されている。制御ポートを介してＣＴＬよりフロー設定情報を受信し、スイッチＤＢに格納する。スイッチＤＢの構成は、図１３に示されている。ＲＴは複数のＳＶポートを具備している。Ｌ２ネットワーク仮想化装置は、ＡＰとの間で仮想回線を構成する。スイッチング回路は、ＡＰで管理されたフロー（フローＤＢ内に記録されたフロー）に対して、個々の仮想回線とＩＰアドレスを接続する。これにより、個々の無線端末とサーバと間で論理的に隔離された通信環境の中での通信が可能になる。

【実施例３】

【００４４】

図１４には、実施例３が示されている。実施例２ではＡＰとＲＴ間の論理トンネルがＯＳＩ上のレイヤ２であるＥｔｈｅｒｎｅｔやＶＬＡＮやＡＴＭで構成されていたのと異なり、実施例３では、無線基地局ＡＰとルータＲＴとの間がＶＸＬＡＮやＧＲＥなどのレイヤ３で論理トンネルが構成されている。このように構成される場合であっても、本発明によると、個々の無線端末とサーバと間で論理的に隔離された通信環境の中での通信が可能になる。

【実施例４】

【００４５】

図１５には、実施例４が示されている。実施例４は、複数のＡＰと複数のＲＴで構成するネットワークにおいて、上記実施例２と３の機能を実現するものである。このように構成される場合であっても、本発明によると、個々の無線端末とサーバと間で論理的に隔離された通信環境の中での通信が可能になる。

【実施例５】

【００４６】

以上は、平成２５年４月４日に出願した特願２０１３－０７８４８７号（以下では、「先の出願」と称する）に記載されていた内容である。先の出願に記載された発明は、上述されているように、論理的に隔離された複数の通信回線を形成するために、通信基地局（アクセスポイント）にアクセスしている通信端末の物理アドレスを用いることを特徴としていた。しかし、発明者は、先の出願の後に、更なる研究開発活動を継続した。その成果として、発明者は、通信端末の物理アドレスに加えて、その通信端末がどのアクセスポイントにアクセスしているのかというアクセスポイントの識別データも同時に考慮することで、より柔軟なネットワークの構築が可能になることを見いだした。すなわち、端末情報とアクセスポイント情報との組合せを用いることにより、先の出願に記載されていた発明によって達成された作用効果に加えて、追加的な作用効果が得られることを見いだしたのである。以下では、その新たな実施例について説明したい。

【００４７】

図１６には、本出願で追加する第５の実施例の概略的な構成が、ブロック図として示されている。ただし、図１６は、第１の通信端末と第２の通信端末とが同一のアクセスポイントにアクセスする場合である。この場合、第１の端末ＮＤ１がアクセスポイントＡＰに接続すると、アクセスポイントＡＰは、第１の端末ＮＤ１のＭＡＣアドレスと自分自身であるアクセスポイントＡＰに関するデータとの組合せ情報を用いて、コントローラＣＴＬに問い合わせる。コントローラＣＴＬは、データベースＤＢから得られるＮＤ１とＡＰと

の組合せ情報に基づいて、接続ネットワークＮＥＴＡＤＤＲ１をアクセスポイントＡＰに返す。そして、アクセスポイントＡＰは第１の端末ＮＤ１にＮＥＴＡＤＤＲ１のＩＰアドレスを与える。こうして、アクセスポイントＡＰを経由して第１の通信端末ＮＤ１と第１のサーバＳＶ１との間を接続する通信回線が構築され、第１の通信端末ＮＤ１と第１のサーバＳＶ１とが通信することが可能になる。第２の通信端末ＮＤ２についても同様である。このように、図１６の場合には、単に、第１の通信端末ＮＤ１と第２の通信端末ＮＤ２とが区別されるだけでない。アクセスポイントＡＰにアクセスしている第１の通信端末ＮＤ１にはどのようなネットワークアドレスを与え、アクセスポイントＡＰにアクセスしている第２の通信端末ＮＤ２にはどのようなネットワークアドレスを与えるのか、が問題になる。例えば、もし、同じ第１の通信端末ＮＤ１であっても、別のアクセスポイントＡＰ’にアクセスする場合には、別のネットワークアドレスが付与される可能性がある。

【００４８】

先の出願に記載された発明では、コントローラＣＴＬに接続されたデータベースＤＢに格納されている通信端末のＭＡＣアドレスとネットワークアドレスとの対応関係が図２に示されていた。また、図３には、別のデータベースに格納されているネットワークアドレスに関する対応関係が示されていた。これに対して、アクセスポイントに関する情報も考慮する本実施例の場合の対応関係は、図１７および図１８に示されている。図１７では、端末の物理アドレスの下に、アクセスポイントに関する情報が含まれている。アクセスポイント情報の具体例としては、ＩＰアドレスやＭＡＣアドレスが考えられるし、それ以外の管理情報でもかまわない。図１８は、図３と同一である。

【００４９】

次に、図１９にも、本実施例の概略的な構成がブロック図として示されている。ただし、同じ実施例ではあるが、図１９は図１６と異なり、同じ２つの通信端末が別のアクセスポイントにアクセスする場合であり、本実施例の特徴的な作用効果をより明瞭にするための図解である。図１９の構成では、第１の通信端末ＮＤ１が第１のアクセスポイントＡＰ１に接続すると、第１のアクセスポイントＡＰ１は、第１の通信端末ＮＤ１のＭＡＣアドレスと第１のアクセスポイントＡＰ１に関するデータとの組合せ情報に基づいてコントローラＣＴＬに問い合わせる。コントローラＣＴＬは、データベースＤＢから得た第１の通信端末ＮＤ１と第１のアクセスポイントＡＰ１との組合せに対応するネットワークアドレスをＡＰ１に返す。第１のアクセスポイントとルータＲＴとは、このネットワークアドレスを用いて、第１の通信端末ＮＤ１と第１のサーバＳＶ１との間を接続する通信回線を構築する。第１の通信端末ＮＤ１は第１のサーバＳＶ１にＩＰアドレスの払い出し要求を送出するが、第１のサーバＳＶ１は、その要求に応答して、ＮＤ１にＩＰアドレスを払い出す。

【００５０】

次に、同じ第１の通信端末ＮＤ１が、別のアクセスポイントである第２のアクセスポイントＡＰ２に接続する場合である。この場合、第２のアクセスポイントＡＰ２は、第１の通信端末ＮＤ１のＭＡＣアドレスと自分自身である第２のアクセスポイントＡＰ１に関するデータとの組合せ情報に基づいてコントローラＣＴＬに問い合わせる。コントローラＣＴＬは、データベースＤＢから得た第１の通信端末ＮＤ１と第２のアクセスポイントＡＰ２との組合せに対応するネットワークアドレスをＡＰ２に返す。第２のアクセスポイントＡＰ２とルータＲＴとは、このネットワークアドレスを用いて、第１の通信端末ＮＤ１と第２のサーバＳＶ２との間を接続する通信回線を構築する。第１の通信端末ＮＤ１は第２のサーバＳＶ２にＩＰアドレスの払い出し要求を送出し、その要求に応答して、第２のサーバＳＶ２は第１の通信端末ＮＤ１にＩＰアドレスを払い出す。

【００５１】

次に、本実施例のように、通信端末の物理アドレスだけでなく、その通信端末のよって接続されているアクセスポイントに関するデータも考慮し、これら２つのデータの組に基づいてネットワークアドレスを決定することで、どのような効果が得られるかを、いくつかの例を挙げることによって説明する。

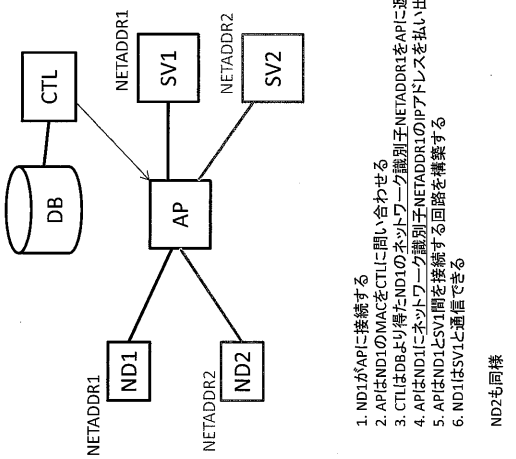
【００５２】
本実施例によると、第１に、従来では発見できなかった不正アクセスを発見できる。例えば、ＷｉＦｉのアクセスポイントは、通信距離が一般的に２０ｍ程度であり、見晴らしが良い場合でも１００ｍ程度が限界である。そのために、ビル内のオフィスには、取締役室、応接室、実験室、営業会議室など、複数の箇所にアクセスポイントを設置する必要がある。例えば、実験エンジニアは１階の実験室に配置したアクセスポイントを経由する場合にのみ社内ネットワークにアクセスできる、というルールがある場合を想定しよう。この場合、実験エンジニアの端末であると称する端末から、５階の取締役室のアクセスポイント経由での通信要求があった場合には、拒絶する必要がある。この例では、（１）ユーザの端末ＩＤ（ＭＡＣアドレスや個体識別番号（例えば、シリアル番号、ＩＭＥＩ、ＭＥＩＤ、ＣＤＮ、およびＩＣＣＩＤ）など）と、（２）アクセスポイントＡＰの識別データ（ＩＰアドレス、ＭＡＣアドレス、個体識別番号（例えば、シリアル番号、データパスＩＤ、ＥＳＳＩＤ、ＩＭＥＩ、ＭＥＩＤ、ＣＤＮ、およびＩＣＣＩＤ）など）との組合せを用いて、通信許可認証処理を行うことにより、不正アクセスを防止することが可能になる。なお、ここで挙げた端末およびアクセスポイントの識別データは、あくまでも例示であり、必要や状況に応じて別の識別データを用いることも可能である。また、アクセスポイント以外に、有線接続するＬ２スイッチや、Ｌ３スイッチの場合でも同様に不正アクセスを発見できる。

【００５３】
本実施例によると、第２に、先の出願に記載された発明では依然として通信が困難となる可能性のあるときでも、アクセス状態を改善できる。先の出願に記載された発明では、ＭＡＣアドレスやシリアル番号などを用いて端末だけを識別している。したがって、端末を識別することを通じてネットワークへの接続を許可または拒絶する。つまり、その端末が現在どこにあるのかという場所を特定した制御はできないため、特定の場所だけからの接続を許可するという制御は不可能である。本実施例による端末とアクセスポイントとの組に基づく認証が可能であれば、ある通信端末について、特定の場所（アクセスポイント）だけからのアクセスを許可することができる。逆に、ある場所（アクセスポイント）への接続については、特定の通信端末だけ許可することも可能になる。

【００５４】
本実施例によると、第３に、ある企業や団体における個人の所属部署や担当の変更を、アクセス権限に適切に反映させることができる。例えば、ある企業のオフィスビルにおいて、開発１部（１階）と開発２部（９階）とが存在し、それぞれが、相互に競合関係にある顧客（ライバルの自動車製造会社Ａ社およびＢ社）のシステムを開発しているとする。エンジニアＳは、２０１３年１２月末までは開発１部に所属しており、その期間は、１階に設置されたＡＰやＬ２／Ｌ３スイッチからしかネットワーク接続させない運用を行っていたとする。ところが、エンジニアＳが２０１４年１月から開発２部に異動になった場合には、９階に設置されたＡＰやＬ２／Ｌ３スイッチからしかネットワーク接続させない運用に変更する必要がある。このような場合、本実施例によると、エンジニアＸの所属組織と利用端末とを関連させて２つのデータの組として管理することになる。この管理により、所属組織の情報がコントローラ（ＣＴＬ）に通知され、上記のアクセス権限の制御を適切に行うことができる。

【００５５】
先の出願に記載されていた発明では、通信端末の物理アドレスを利用して論理的に独立な通信回線の構築を可能にしていた。しかし、以上で説明したように、更にアクセスポイントに関するデータも考慮し、端末の物理アドレスとアクセスポイントデータとの組を用いてネットワークアドレスを決定するという特徴的な構成を採用することにより、更に多様な制御を可能にする柔軟な通信制御が可能になる。

【図１】



【図２】

MAC⇔ネットワーク識別子マッピングデータベース

カラム	内容
端末個体識別子	MACアドレス
ネットワーク識別子	一意なID
ポート番号	送受信する有線ポート番号

ネットワーク識別子ごとにアドレス範囲を管理することが特徴

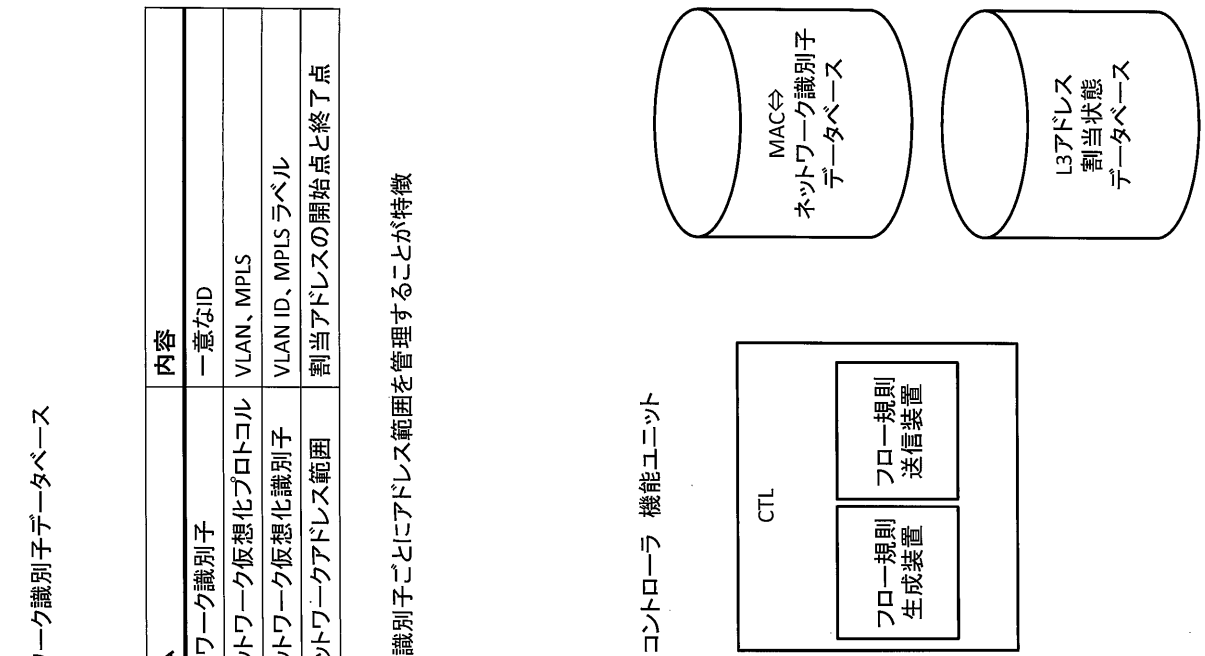
【図３】

ネットワーク識別子データベース

カラム	内容
ネットワーク識別子	一意なID
L2ネットワーク仮想化プロトコル	VLAN、MPLS
L2ネットワーク仮想化識別子	VLAN ID、MPLS ラベル
L3ネットワークアドレス範囲	割当アドレスの開始点と終了点

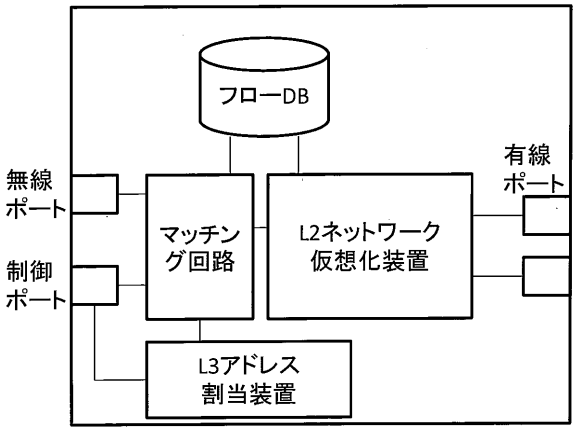
ネットワーク識別子ごとにアドレス範囲を管理することが特徴

【図４】



【図５】

アクセスポイント機能ユニット



【図６】

フローデータベース

カラム	内容
端末個体識別子	MACアドレス
L2ネットワーク仮想化プロトコル	VLAN、MPLS
L2ネットワーク仮想化識別子	VLAN ID、MPLS ラベル
ポート番号	アクセスポイントの有線ポート番号

アクセスポイントのマッチング回路用ルールの集合

【図７】

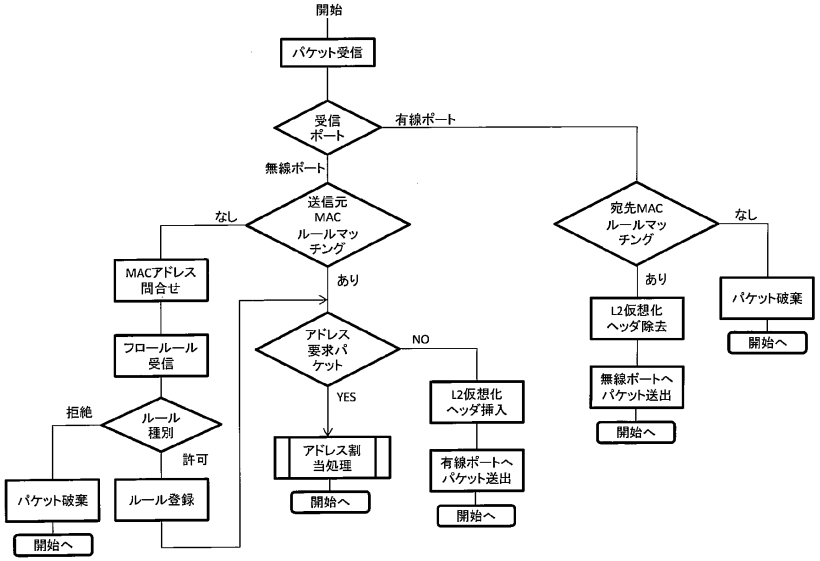
L3アドレス割当状態データベース

カラム	内容
端末個体識別子	MACアドレス
L3ネットワークアドレス	IPアドレス

ネットワーク識別子ごとにアドレス範囲を管理することが特徴

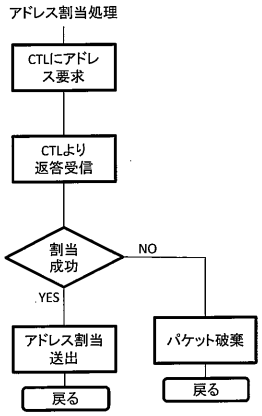
【図８】

アクセスポイント フローチャート1

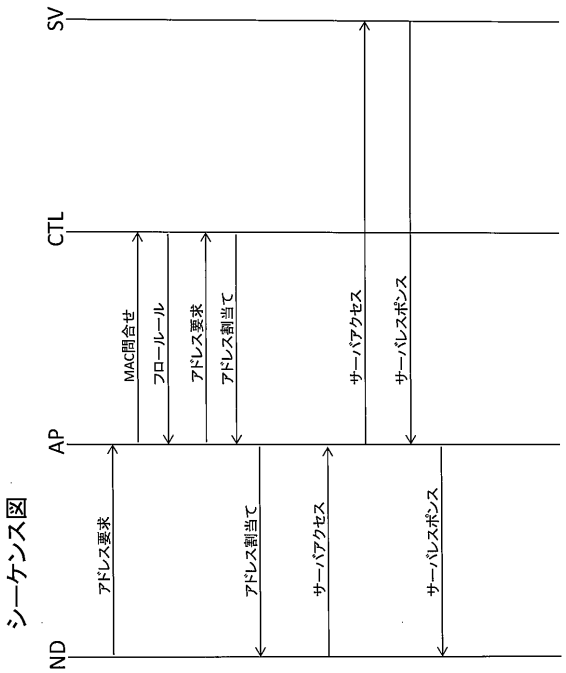


【図９】

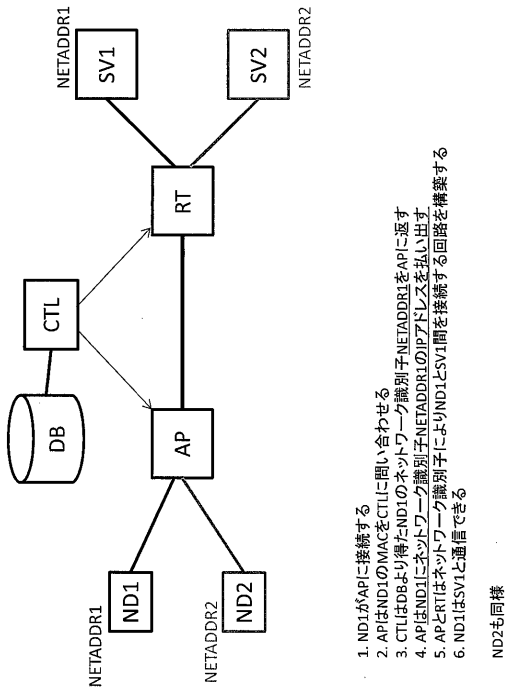
アクセスポイント フローチャート2



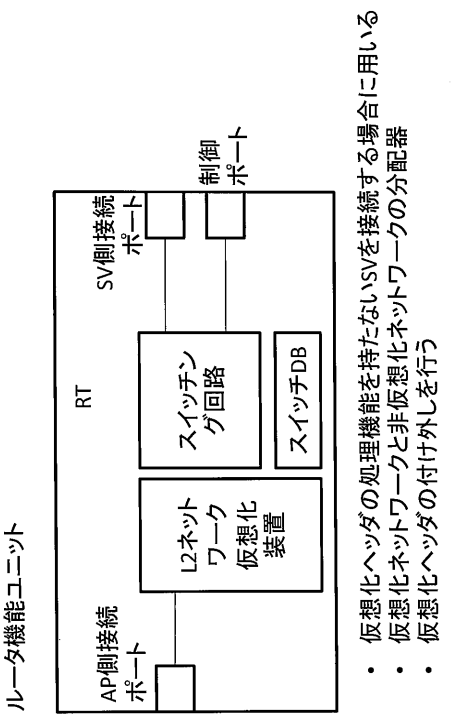
【図１０】



【図１１】



【図１２】

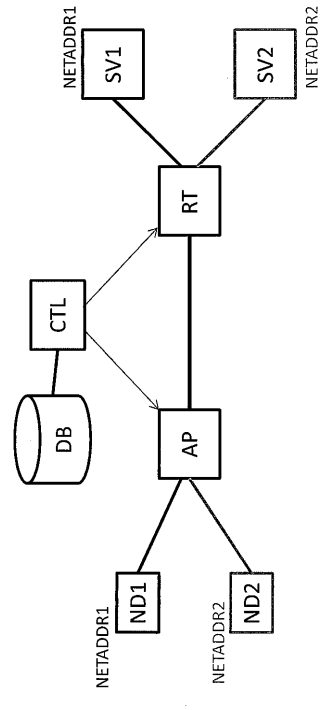


【図１３】

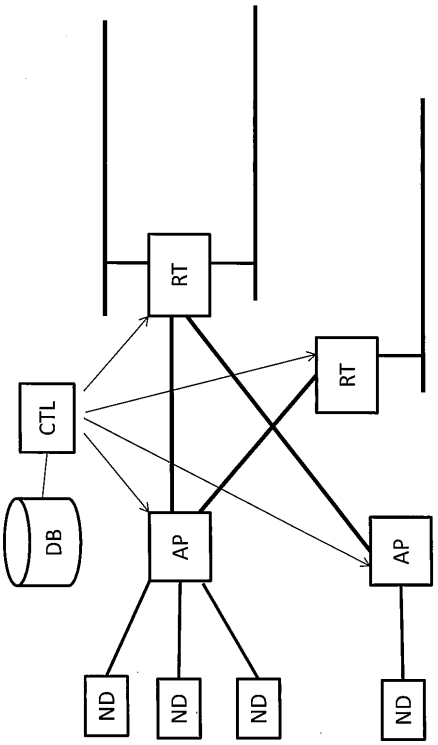
スイッチデータベース

カラム	内容
L2ネットワーク仮想化プロトコル	VLAN、MPLS
L2ネットワーク仮想化識別子	VLAN ID、MPLS ラベル
ポート番号	SV側接続ポート番号

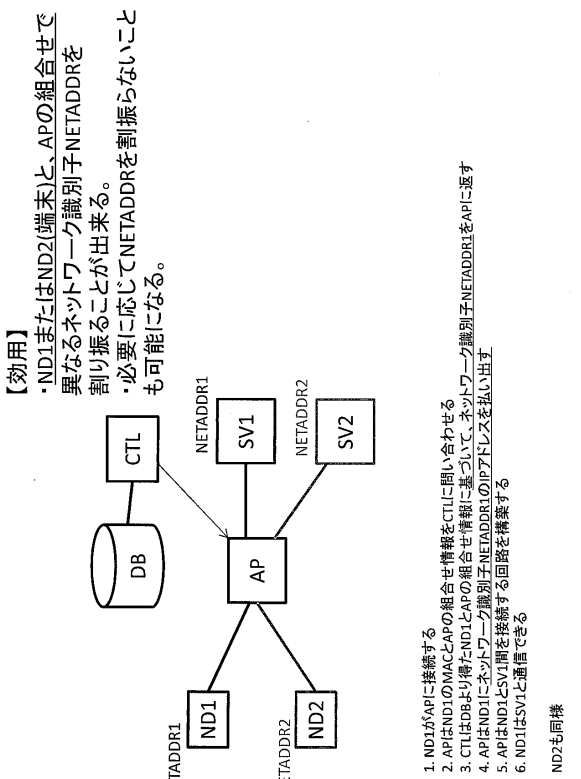
【図１４】



【図１５】



【図１６】



【図１７】

MAC＋APの管理IPアドレス（又はAPのMACアドレス、
又はAPに付与された管理情報）
⇔ネットワーク識別子マッピングデータベース

カラム	内容
端末個体識別子	MACアドレス
AP情報	IP or MAC or その他管理情報
ネットワーク識別子	一意なID
ポート番号	送受信する有線ポート番号

ネットワーク識別子ごとにアドレス範囲を管理することが特徴

【図１８】

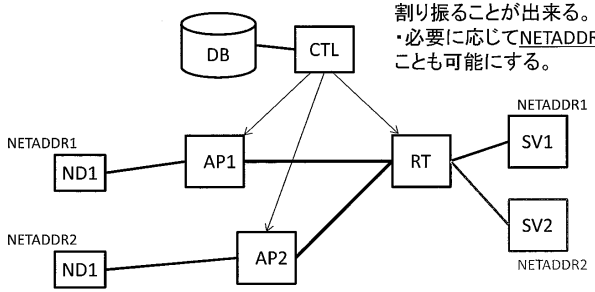
ネットワーク識別子データベース

カラム	内容
ネットワーク識別子	一意なID
L2ネットワーク仮想化プロトコル	VLAN、MPLS
L2ネットワーク仮想化識別子	VLAN ID、MPLS ラベル
L3ネットワークアドレス範囲	割当アドレスの開始点と終了点

ネットワーク識別子ごとにアドレス範囲を管理することが特徴

【図１９】

【効用】
・ND1(端末)と、AP1またはAP2の組合せで異なるネットワーク識別子NETADDRを割り振ることが出来る。
・必要に応じてNETADDRを割振らないことも可能にする。



1. ND1がAP1に接続する
2. AP1はND1のMACとAP1の組合せ情報をCTLに問い合わせる
3. CTLはDBより得たND1とAP1のネットワーク識別子NETADDR1をAP1に返す
4. AP1はND1にネットワーク識別子NETADDR1のIPアドレスを払い出す
5. AP1とRTはネットワーク識別子によりND1とSV1間を接続する回路を構築する
6. ND1はSV1と通信できる

1. ND1がAP2に接続する
2. AP2はND1のMACとAP2の組合せ情報をCTLに問い合わせる
3. CTLはDBより得たND1とAP2のネットワーク識別子NETADDR2をAP2に返す
4. AP2はND1にネットワーク識別子NETADDR2のIPアドレスを払い出す
5. AP2とRTはネットワーク識別子によりND1とSV2間を接続する回路を構築する
6. ND1はSV2と通信できる

JP 5937563 B2 2016.6.22

フロントページの続き

(72)発明者　白崎　博生
東京都千代田区神田神保町一丁目１０５番地　株式会社ストラトスフィア内

審査官　篠田　享佑

(56)参考文献　特開２００７－１５０６３３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　　７／２４－　７／２６
Ｈ０４Ｗ　　４／００－９９／００