(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5454399号
(P5454399)
(45)発行日　平成26年3月26日(2014.3.26)　(24)登録日　平成26年1月17日(2014.1.17)

(51)Int.Cl.　F I
H04L 12/28 (2006.01)　H04L 12/28　200M

請求項の数 7　(全 18 頁)

(21)出願番号　特願2010-160375(P2010-160375)
(22)出願日　平成22年7月15日(2010.7.15)
(65)公開番号　特開2012-23591(P2012-23591A)
(43)公開日　平成24年2月2日(2012.2.2)
審査請求日　平成25年7月3日(2013.7.3)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100109667
弁理士　内藤　浩樹
(74)代理人　100120156
弁理士　藤井　兼太郎
(74)代理人　100137202
弁理士　寺内　伊久郎
(72)発明者　前川　肇
福岡県福岡市博多区美野島４丁目１番６２号　パナソニックシステムネットワークス株式会社内

審査官　大石　博見

最終頁に続く

(54)【発明の名称】ラージスケールＮＡＴ検出装置、アプリケーション切替装置、ラージスケールＮＡＴ検出方法およびアプリケーション切替方法

(57)【特許請求の範囲】
【請求項１】
ネットワークを経由して接続されたサーバにパケットを送るラージスケールＮＡＴ検出装置であって、
前記パケットの送信元ポート番号を変更しながら前記ネットワークにパケットを送信するパケット送信制御部と、
前記ネットワークからＩＣＭＰ１３－Ａｄｍｉｎｉｓｔｒａｔｉｖｅｌｙ　Ｐｒｏｈｉｂｉｔｅｄを受信した場合に前記ネットワーク上にラージスケールNATが存在すると判断するＬＳＮ検出部と
からなるラージスケールNAT検出装置。
【請求項２】
前記パケット送信制御部は、所定の時間内に送信元ポート番号を変更しながらあらかじめ決められたポート総数Ｎ回になるまで、前記ネットワークにパケットを送信し、
前記ＬＳＮ検出部は、ＩＣＭＰ１３－Ａｄｍｉｎｉｓｔｒａｔｉｖｅｌｙ　Ｐｒｏｈｉｂｉｔｅｄを受信した場合に前記ネットワーク上にN個のポートが使用可能でないラージスケールNATが存在すると判断する、
請求項１記載のラージスケールＮＡＴ検出装置。
【請求項３】
請求項１あるいは請求項２に記載のラージスケールNAT検出装置に加え、
所定のポート数で動作する通常アプリケーションと前記所定のポート数より少ないポート

数で動作するＬＳＮ用アプリケーションとを保持するアプリ保持部と、
アプリケーション動作時に前記ＬＳＮ検出部が検出したラージスケールＮＡＴの有無に応じて、前記アプリ保持部で保持しているアプリケーションを切り替えるアプリスイッチ部と、
を有するアプリケーション切替装置。
【請求項４】
前記通常アプリケーションは分割された小分割地図画像を、前記小分割地図画像毎に異なるポートで受信して、受信した前記小分割地図画像を合成して地図を表示するアプリケーションであり、
前記ＬＳＮ用アプリケーションは、前記分割された小分割地図画像に比べて大きい画像サイズで分割された大分割地図画像を、前記大分割地図画像毎に異なるポートで受信して、受信した前記大分割地図画像を合成して地図を表示する、
請求項３記載のアプリケーション切替装置。
【請求項５】
中継ノードを経由してネットワークに接続された中継ノードに向けて、近くの前記中継ノードから順にトレースルートを実行したとき、
所定のメッセージを送ることにより前記中継ノードの中でプライベートアドレスを有する中継ノードから最初にグローバルアドレスを有する中継ノードに変わる中継ノードを発見し、
前記中継ノードの中で、前記グローバルアドレスを有する中継ノードを最初に送信した中継ノードの一つ手前の中継ノードをＬＳＮ候補中継ノードとして発見し、前記ＬＳＮ候補中継ノードに推定ルータパケットをユニキャストで送信したとき、前記ＬＳＮ候補中継ノードがＵＰｎＰに基づいて応答を返してきたとき、前記ＬＳＮ候補中継ノードをＬＳＮでないと判断し、前記ＬＳＮ候補中継ノードが所定の時間内に応答を返してこないとき、前記ＬＳＮ候補中継ノードをＬＳＮと判断することを特徴とするラージスケールＮＡＴ検出装置。
【請求項６】
ネットワークを経由して接続されたサーバにパケットを送るラージスケールＮＡＴ検出方法であって、
前記パケットの送信元ポート番号を変更しながら前記ネットワークにパケットを送信するパケット送信制御ステップと、
前記ネットワークからＩＣＭＰ１３－Ａｄｍｉｎｉｓｔｒａｔｉｖｅｌｙ　Ｐｒｏｈｉｂｉｔｅｄを受信した場合に前記ネットワーク上にラージスケールNATが存在すると判断するＬＳＮ検出ステップと
からなるラージスケールNAT検出方法。
【請求項７】
請求項６に記載のラージスケールNAT検出方法に加え、
所定のポート数で動作する通常アプリケーションと前記所定のポート数より少ないポート数で動作するＬＳＮ用アプリケーションとを保持するアプリ保持ステップと、
アプリケーション動作時に前記ＬＳＮ検出ステップが検出したラージスケールＮＡＴの有無に応じて、前記アプリ保持ステップで保持しているアプリケーションを切り替えるアプリスイッチステップと、
を有するアプリケーション切替方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、IPｖ４アドレス枯渇時に適応されるラージスケールＮＡＴ（以下ＬＳＮと呼ぶ）、別名、キャリアグレードＮＡＴ（以下ＣＧＮと呼ぶ）がネットワークに接続されているとき、そのネットワークに接続された端末が、ネットワーク経路上にＬＳＮが存在することを発見するための手法および装置に関する。

【背景技術】
【０００２】
２０１０年４月現在、ＩＰｖ４アドレスが次第に枯渇してきており、ＩＰｖ４ネットワークの延命策が検討されている。また、インターネットプロバイダなどの通信キャリアにおいてプライベートネットワークを構築し複数のユーザでＩＰアドレスを共有する装置であるラージスケールＮＡＴの導入が検討されている。ラージスケールＮＡＴは、アドレス変換（ＮＡＴ：Ｎｅｔｗｏｒｋ Ａｄｄｒｅｓｓ Ｔｒａｎｓｌａｔｉｏｎ）機能を備え、大規模なトラフィックに耐えうるように作られたＮＡＴである。ラージスケールＮＡＴのユーザ側ネットワークは、通常、プライベートＩＰアドレス（以下、プライベートアドレスという）によって構築される。
ラージスケールＮＡＴ（以下ＬＳＮ）は、ＩＰｖ４アドレスの使用数を抑制することができる一方で、さまざまな弊害をもたらすことがわかっている。例えば、ＬＳＮは複数のユーザによってひとつのグローバルＩＰアドレスが共有される結果、１ユーザあたりのポート数を制限せざるを得ず、その結果としてユーザアプリケーションの一部には通信ができなかったり、不具合を生じさせたりといった問題点が指摘されている。
【０００３】
こういった不具合は一般のユーザにとっては、不具合を発生させている問題点の切り分け、すなわち、ネットワークの問題なのか、機器の問題なのかの判断が難しいために、ユーザが、機器の故障ではないにもかかわらず、ネットワークの問題とは判断できずに機器の故障と判断してしまうというケースも想定できる。
【０００４】
このため機器が自分が接続されたネットワーク上にＬＳＮが存在しているかどうかを知り、例えば、不具合を起こさないように動作をスイッチしたり、あるいは、メッセージとしてＬＳＮがネットワーク上にあり正しく動作しない旨を何らかの形で機器がユーザにメッセージを送るといった方法が考えられる。また、アプリケーションが必要とするポートの数が使えるのかどうかあらかじめテストしておきたい、といったこともある。
【０００５】
このようにネットワークに接続された端末が自身のネットワーク上にＬＳＮがあるかどうかを調べることは重要なことである。
一般的にＮＡＴを発見する技術は開示されている。例えば非特許文献１で開示されているＩＥＴＦにて標準化されたＳＴＵＮなどを用いればＮＡＴの存在や型を調べることができるが、そのＮＡＴがＬＳＮであるかどうかは判定できない。
【０００６】
また、特許文献１、２では、パケットの送信方法を工夫することでＮＡＴの種類を判定する（Ｆｕｌｌ Ｃｏｎｅ ＮＡＴ、Ｒｅｓｔｒｉｃｔｅｄ Ｃｏｎｅ ＮＡＴ、Ｐｏｒｔ Ｒｅｓｔｒｉｃｔｅｄ Ｃｏｎｅ ＮＡＴ、Ａｄｒｅｓｓ Ｓｅｎｓｉｔｉｖｅ Ｓｙｍｍｅｔｒｉｃ ＮＡＴのどれであるかを判定する）技術は開示されているが、ＮＡＴがＬＳＮであるかどうかは判定できない。
【先行技術文献】
【特許文献】
【０００７】
【特許文献１】特開２００６－２９５９０９号公報
【特許文献２】特開２００８－２８９１０９号公報
【特許文献３】特開２００５－３２３０３３号公報
【特許文献４】特開２００６－２８７４７８号公報
【非特許文献】
【０００８】
【非特許文献１】「ＲＦＣ３４８９ ＳＴＵＮ Ｓｉｍｐｌｅ Ｔｒａｖｅｒｓａｌ ｏｆ ＵＤＰ ｔｈｏｕｇｈ ＮＡＴｓ」［ｏｎｌｉｎｅ］、２０１０年４月５日、インターネット ＜ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．ｉｅｔｆ．ｏｒｇ／ｒｆｃ／ｒｆｃ３４８９

．ｔｘｔ＞
【非特許文献２】「Ｃｏｍｍｏｎ Ｆｕｎｃｔｉｏｎｓ ｏｆ Ｌａｒｇｅ Ｓｃａｌｅ Ｎａｔ（ＬＳＮ）」［ｏｎｌｉｎｅ］、２０１０年４月５日、インターネット ＜ＵＲＬ：http://tools.ietf.org/html/draft-nishitani-cgn-02＞
【発明の概要】
【発明が解決しようとする課題】
【０００９】
上記したようにＮＡＴを発見する手法についてはいくつかの技術が存在している。ただ、ＬＳＮはＮＡＴではあるがポートに対するユーザ制限などがある特殊なＮＡＴであり、従来の技術を用いてもＬＳＮであるかどうかを判定することは不可能である。また、ＮＡＴの種類を判定する技術も存在しているが、ＬＳＮであるかどうかを判定することはできない。
このため、ネットワークに接続された端末が自身が通信する通信経路上にＬＳＮが存在していることを発見するための方法が必要となる。
【課題を解決するための手段】
【００１０】
本発明のＬＳＮ検出装置は、ネットワークを経由して接続されたサーバにパケットを送るラージスケールＮＡＴ検出装置であって、前記パケットの送信元ポート番号を変更しながら前記ネットワークにパケットを送信するパケット送信制御部と、前記ネットワークからＩＣＭＰ１３－Ａｄｍｉｎｉｓｔｒａｔｉｖｅｌｙ Ｐｒｏｈｉｂｉｔｅｄを受信した場合に前記ネットワーク上にラージスケールNATが存在すると判断するLSN検出部とからなる構成を有している。
【００１１】
この構成により、ＬＳＮ検出装置はネットワーク上にラージスケールＮＡＴがあることを知ることが出来る。
【００１２】
また、本発明のＬＳＮ検出装置は、前記パケット送信制御部は、所定の時間内に送信元ポート番号を変更しながらあらかじめ決められたポート総数Ｎ回になるまで、前記ネットワークにパケットを送信し、前記LSN検出部は、ＩＣＭＰ１３－Ａｄｍｉｎｉｓｔｒａｔｉｖｅｌｙ Ｐｒｏｈｉｂｉｔｅｄを受信した場合に前記ネットワーク上にN個のポートが使用可能でないラージスケールNATが存在すると判断する、構成を有している。
【００１３】
この構成により、ＬＳＮ検出装置は、ネットワーク上にＮ個のポートが使用可能でないラージスケールＮＡＴが存在することを知ることが出来る。
【００１４】
さらに、本発明のアプリケーション切替装置は、前記記載のラージスケールNAT検出装置に加え、所定のポート数で動作する通常アプリケーションと前記所定のポート数より少ないポート数で動作するＬＳＮ用アプリケーションとを保持するアプリ保持部と、アプリケーション動作時に前記ＬＳＮ検出部が検出したラージスケールＮＡＴの有無に応じて、前記アプリ保持部で保持しているアプリケーションを切り替えるアプリスイッチ部と、からなる構成を有している。
【００１５】
この構成により、ラージスケールＮＡＴが使用可能なポート数に応じてアプリケーションを切り替えることが出来る。
【００１６】
さらに、本発明のアプリケーション切替装置は、前記通常アプリケーションは分割された小分割地図画像を、前記小分割地図画像毎に異なるポートで受信して、受信した前記小分割地図画像を合成して地図を表示するアプリケーションであり、前記ＬＳＮ用アプリケーションは、前記分割された小分割地図画像に比べて大きい画像サイズで分割された大分割地図画像を、前記大分割地図画像毎に異なるポートで受信して、受信した前記大分割地

図画像を合成して地図を表示する、構成を有している。

【００１７】

この構成により、利用可能なポート数が多い場合に実行される通常アプリケーションのときは、分割する画像サイズを小さくして、分割された画像をそれぞれ異なる多くのポートで受け取ることにより、地図を高速にスクロールして表示可能であり、利用可能なポート数が少ない場合に実行されるＬＳＮ用アプリケーションのときは、分割する画像サイズを大きくして、少ないポートでそれぞれの分割された画像を受け取って、地図をスクロールして表示することが可能である。

【００１８】

さらに、本発明のＬＳＮ検出装置は、中継ノードを経由してネットワークに接続された中継ノードに向けて、近くの前記中継ノードから順にトレースルートを実行したとき、所定のメッセージを送ることにより前記中継ノードの中でプライベートアドレスを有する中継ノードから最初にグローバルアドレスを有する中継ノードに変わる中継ノードを発見し、記中継ノードの中で、前記グローバルアドレスを有する中継ノードを最初に送信した中継ノードの一つ手前の中継ノードをＬＳＮ候補中継ノードとしてを発見し、前記ＬＳＮ候補中継ノードに推定ルータパケットをユニキャストで送信したとき、前記ＬＳＮ候補中継ノードがＵＰｎＰに基づいて応答を返してきたとき、前記ＬＳＮ候補中継ノードをＬＳＮでないと判断し、前記ＬＳＮ候補中継ノードが所定の時間内に応答を返してこないとき、前記ＬＳＮ候補中継ノードをＬＳＮと判断する、構成を有している。

【００１９】

この構成により、ＬＳＮにはセキュリティ上の観点よりＵＰｎＰ－ＩＧＤによるルータ制御の仕組みは搭載されていないため、ＵＰｎＰによるルータ制御よるＵＰｎＰに基づいた応答を返してこないため、ＬＳＮ候補中継ノードがＬＳＮであると判断することが可能である。

【発明の効果】

【００２２】

本発明によれば、ＬＳＮに備えられた送受信部により、端末がチェックパケットを送信することにより、ＬＳＮ識別子を端末が受け取ることができ、ＬＳＮの存在を短時間に確実に確認することができる。

【００２３】

また、本発明によればパケットを送信してＮＡＴを検査することにより、当該ＮＡＴがＬＳＮであるかどうかを判別することができる。

【００２４】

また、本発明によれば、端末が必要とするポート数Ｎについて、ネットワーク上で確保が可能かどうかをあらかじめ確認することができる。

【００２５】

また、本発明によれば、端末がＬＳＮを発見したときに適切な動作にスイッチを行うことでトラブルを回避することが可能になる。

【図面の簡単な説明】

【００２６】

【図１】第１の実施形態に係る装置の構成を示すブロック図
【図２】第１の実施形態におけるＬＳＮ識別子を示す図
【図３】第２の実施形態に係る装置の構成を示すネットワーク図
【図４】第２の実施の形態におけるパケットの内容を示す説明図
【図５】第２の実施の形態における装置の構成を示すブロック図
【図６】第２の実施の形態の処理の流れを示すフロー図
【図７】第３の実施形態に係る装置の構成を示すネットワーク図
【図８】第３の実施形態に係る装置の構成を示すブロック図
【図９】第３の実施の形態の処理の流れを示すフロー図
【図１０】第４の実施形態に係る装置の構成を示すブロック図

【図１１】第４の実施の形態の動作を示す説明図
【図１２】第５の実施形態に係る装置の構成を示すブロック図
【図１３】第６の実施形態に係る装置の構成を示すブロック図
【図１４】第７の実施形態に係る装置の構成を示すネットワーク図
【図１５】第７の実施形態に係る装置のトレースルート結果を示す図
【図１６】第７の実施形態に係る装置のＵＰｎＰメッセージを示す図
【発明を実施するための形態】
【００２７】
（第１の実施形態）
以下、本発明の第１の実施形態について、図面を参照しながら説明する。図1は、本発明の第１の実施形態に係るＬＳＮ検出装置の一例を示す図である。
図１において１はＬＳＮ，２は端末、１１はＬＳＮ１に実装された送受信部、１２はＬＳＮ識別子、２１は端末に実装された送受信部であり、ＬＳＮ１と端末２はネットワーク４によって接続されている。
【００２８】
ＬＳＮ識別子１２には、図２に示すように、ＬＳＮの名称（ＬＳＮ名）、ＷＡＮ（インターネット）側のＩＰアドレス(ＷＡＮアドレス)およびＬＳＮに設定されたユーザごとの制限ポート数が含まれている。図２は、ＬＳＮ名がｌｓｎ１．ｌｓｎ．ｃｏｍ、ＷＡＮアドレスが、１１．２２．３３．４４、制限ポート数が２０００の場合を示している。
【００２９】
端末２は送受信部２１よりＬＳＮ１に向かって、ＬＳＮ識別子リクエストを送信し、このリクエストをＬＳＮ１は送受信部１１で受信する。ＬＳＮ１はＬＳＮ識別子リクエストを受信すると、ＬＳＮ識別子レスポンスとしてＬＳＮ識別子１２を返送する。端末２はＬＳＮ識別子２１を受け取ることにより、経路上にＬＳＮ１があり、ポート制限があることを検知することができる。
【００３０】
（第２の実施形態）
以下、本発明の第２の実施形態について、図面を参照しながら説明する。図３は、本発明の第２の実施形態に係るＬＳＮ検出装置の一例を示す図である。図３において、ＬＳＮ１と端末２はネットワークによって接続されており、また、ＬＳＮ１とサーバ３もネットワークにより接続されている。ＬＳＮ１とサーバ３の間をＷＡＮ側４と呼ぶ。
【００３１】
図３において、端末２はサーバ３に対してＵＤＰパケット(1)を送信する。このとき、端末２から送信されたＵＤＰパケット（１）はＬＳＮ１を経由してＵＤＰパケット（４）としてサーバ３に届くことになる。ＬＳＮ１ではＵＤＰパケットが通過するたびに、アドレス変換テーブルを作成して、ＷＡＮ側４のポートとの割り当てを確立する。このＷＡＮ側４に割り当てられたポート番号を用いてサーバへの通信を実行することになる。
ＬＳＮ１では、ＷＡＮ側４のポート数がユーザ毎に制限をされており、ユーザ毎のポート数の制限値を保持している。ユーザの通信において、ポート数の制限値を越える通信が行われたとき、ＬＳＮ１から端末２に対し、ＩＣＭＰ　１３－Ａｄｍｉｎｉｓｔｒａｔｉｖｅｌｙ　Ｐｒｏｈｉｂｉｔｅｄ（以下ＩＣＭＰ１３と呼ぶ。ＩＣＭＰ１３については非特許文献２を参照）が返送される。すなわち、ＩＣＭＰ１３を端末が受信すると、通信経路上にＬＳＮ１が存在するということを判定できることになる。
【００３２】
なお、ＩＣＭＰ１３はＬＳＮ１が端末２に対してポート使用制限数を越えた際に送出するエラーメッセージである。ＬＳＮ１を経由してインターネットにアクセスしている端末２がポートをＬＳＮ１の制限数以上に消費した場合にＩＣＭＰ１３を受け取るので、アプリケーションが実行時にポートを消費することにより端末２はＬＳＮ１を経由してサーバ３に接続していること知ることはあるが、常に知ることができるわけではない。また、端末２がＩＣＭＰ１３を受け取ったとき、端末はポート数の制限を越えたことは分かるが、

そのポート数の制限数がいくつなのかについては知ることができない。
【００３３】
本実施の実施形態では、あらかじめＬＳＮ１を経由しているかどうかを知ることができかつその際ポート数がいくつ確保できるかについて知ることができる検出装置を提供する。
このＬＳＮ１におけるユーザあたりの使用可能なポート数の制限値はプロバイダなどＬＳＮ運用者の運用ポリシーにより異なることが予想される。ここでは例えばポート数の制限値が２００個であったとする。本実施例では端末２がＵＤＰパケットを送信する構成であるので、端末２はサーバに向けて複数のＵＤＰパケットを送信する。この複数のＵＤＰパケットの送出の際には、端末２からネットワークに送る際の、送信元ポート番号が前回のポート番号とは異なるように次々と送信していく。
【００３４】
ＬＳＮ１は、端末２から制限値を超えるポート番号の異なるＵＤＰパケットを受け取ると、ＩＣＭＰ１３メッセージを端末２に返す。ポート数の制限値が２００個になっているので、ネットワーク上にＬＳＮ１があると端末２がポート番号の異なる２００個のＵＤＰパケットを送出すると、端末２はＬＳＮ１からＩＣＭＰ１３のメッセージを受け取ることになる。
【００３５】
なお、端末2からネットワークに向けて、ＵＤＰパケットを送信する際の送信元ポート番号については、逐次的にひとつずつ増やしてもよいし、減らしてもよいし、また、ランダムに選択してもよい。
【００３６】
第２の実施の形態の端末２の構成を、図５を用いて、さらに詳しく説明する。図５において３１は送信ポートの制御を行う送信ポート制御部、３２はパケット送信部、３３はパケット受信部、３４はネットワーク制御部、３５は受信したパケットの内容を検査するパケット検査部である。
【００３７】
図５において、パケット送信部３２は複数のパケットを送信する。ただし、パケットのポート番号の数には限界があり、その数はＵＤＰ／ＩＰの送信においては論理的な限界である６５５３６個である。
【００３８】
送信ポート制御部３１は、パケット送信部３２から送出されたＵＤＰパケットを受け取り、送信元ポート番号の重複利用が発生しないように制御しながらネットワーク制御部３４に受け渡し、ネットワーク制御部３４がＵＤＰのパケットを送出する。
【００３９】
ネットワーク制御部３４はネットワークインタフェースを制御し、パケットの送信および受信を行う。パケット受信部３３はネットワークインタフェースに入力されたパケットをネットワーク制御部３４を経由して受け取り、受信パケットのうち自分宛のパケットを受信する。
【００４０】
パケット検査部３５は自分宛に送られたパケットの中に、ＩＣＭＰ１３が含まれるか否かを調査する。もしＩＣＭＰ１３が含まれていると経路上にＬＳＮ１が存在すると判定する。
【００４１】
本実施例の検査装置は、端末の電源投入時、ユーザの指示、またはタイマーなどのタイミングで検査を開始する。端末２の本体のアプリケーションが動作中には実行しないことが望ましいが、必要に応じて動作させることも可能である。
【００４２】
動作の具体例について、さらに詳しく説明する。本実施例の検査が始まると、パケット送信部３２よりパケットの送信を開始する。パケットは時系列的に送出することになる。

パケット形式はＵＤＰ／ＩＰが選択される。パケットのペイロードの内容はとくに何でもよいが、本実施例ではパケット送出の際のポート番号をつめておく。ポート番号の理論上の最大値は６５，５３６個であるが、本実施例ではウェルノウンポートを考慮して、使用するポート番号の個数は最大値から１０２４を減じた６４５１２個とする。

【００４３】

検査が始まり、パケット送出が始まると、送信ポート制御部３１が送信元ポート番号を変更しながら連続してパケットを送信し始める。送信元ポート番号の初期値はとくに何を選択してもよいが、ウェルノウンポートである１０２３以下は用いないことが望ましい。本実施例では、初期値は１０２４とし、ここから連続してポート番号を増加させていくようになっている。

【００４４】

ＩＰアドレスやポート番号について、図３および図４を用いて説明する。図３において、端末２から送出される送信パケットの宛先はサーバ３である。サーバ３のＩＰアドレスは１１．２２．３３．４４であり、端末２のＩＰアドレスは１９２．１６８．１．１０とする。また、ＬＳＮ１のＷＡＮ側４のアドレスは１１．２２．３３．５５とする。

端末２からは、サーバの宛先ポートを８０とすると、ＩＰアドレス１１．２２．３３．４４のポート番号８０に向けてパケットが送信される。そして、初期送信元ポート番号が１０２４なので、ＵＤＰパケットとしては、図４の（１）となる。このパケットはＬＳＮ１を通過する際に書き換えが実施され、ＵＤＰパケット（４）となる。この際、ＬＳＮ１の送信元ポート番号が２０００だとすると、ＬＳＮ１からサーバ３には、図４の（４）のようなＵＤＰパケットが送出される。

【００４５】

続けて端末２からＬＳＮ１に向けて、送信元ポート番号１０２５のＵＤＰパケット（２）が送信される。このパケットはＬＳＮ１を通過する際に書き換えが実施され、ＬＳＮ１により、新たにポートが割り当てられ、例えば、送信元ポート番号が２００１になり、サーバ３に向けて新たなパケットが送出される。

【００４６】

この動作を次々繰り返すと、端末２からＬＳＮ１に送られる２０１個目のパケットの送信元ポート番号は、１２２４となる（図４の（３））。このとき、ポート数の制限値を２００としているため、ＵＤＰパケット（３）がＬＳＮ１を通過しようとした際にポート番号の上限の制限に引っかかり、ＬＳＮ１より、端末２に向けて、ＩＣＭＰ１３を含むＩＣＭＰパケット（５）が送られることになる。端末２に送られたＩＣＭＰ１３のメッセージを含むＩＣＭＰパケット（５）は端末２に送信され、ネットワーク制御部３４、パケット受信部３３へと送られる。パケット受信部からさらにパケット検査部３５に送られて、パケットの検査を受けることになる。

【００４７】

パケット検査部３５においてＩＣＭＰ１３が検知されると、検査の判断としてＬＳＮ１が経路上に存在する、と判定され、処理が終了する。

【００４８】

図６を用いて本願の第２の実施の形態の処理の流れについてさらに説明する。ポート番号の理論上の上限値までパケットを送るためのカウンターをｉとして初期値として１０２４をセットする（Ｓ６１）。次に、パケット送信部３２は、ペイロードにｉを記入したＵＤＰパケットを作成する（Ｓ６２）。送信ポート制御部３１は、過去に使用していない送信元ポート番号(例えば１０２４)を使用してネットワーク制御部３４を経由してパケットをネットワークに送信する（Ｓ６３）。次に、パケット受信部３３は、ネットワーク制御部３４を経由してパケットを受信し（Ｓ６４）、このとき、パケット検査部３５によって、パケットの中にＩＣＭＰ１３のメッセージが入っているどうかを判定する（Ｓ６５）。

【００４９】

ここで検査結果が、ＩＣＭＰ１３のメッセージがパケットに入っていない場合は（Ｓ６５のＮｏ）ｉの値に１を加え（Ｓ６６）、ｉがパケット数の理論上の上限値である６５５

３５を超えているか否かを調べる（Ｓ６７）。ｉが６５５３５に到達した場合、ＬＳＮ１がネットワーク上にないと判断し（Ｓ６９）、ｉが６５５３５を超えていない場合は、パケット送信部３２はペイロードに新たに更新されたｉを用いてを記入した新たなＵＤＰパケットを作成する（再びＳ６２からの動作を繰り返す）。

【００５０】

Ｓ６５の検査結果が、ＩＣＭＰ１３のメッセージがパケットに入っていることが発見された場合（Ｓ６５のＹｅｓ）は、ネットワークの途中にＬＳＮ１があると判定する（Ｓ６８）。また、このときのｉをみると、端末２が使用できるポートの上限値（ｉ－１０２３）を知ることができる。

【００５１】

（第３の実施形態）

以下、本発明の第３の実施形態について、図面を参照しながら説明する。図７は、本発明の第３の実施形態に係るＬＳＮ検出装置の一例を示す図であるが、端末２、ＬＳＮ１、サーバ３の間を流れるＵＤＰパケットの関係は実施の形態１と同じである。

図８は、本発明の第３の実施の形態のブロック構成図を示している。実施の形態３の構成は、実施の形態２とほぼ同じであるが、パケット数保持部３６を有している点が実施の形態２と異なる。

【００５２】

第３の実施の形態では、パケット数保持部３６にユーザが必要なポート数Ｎを保持しており、ＬＳＮ１が端末２に割り当てているパケットのポート数がＮ以上であるか否かを検出することを目的としている。これにより、ユーザが必要なポート数が確保できるか否かを判断することができるようになる。

【００５３】

図８において、パケット送信部３２は複数のパケットを送信するが、実施の形態３では、ポート番号を変えたパケットの送信数の最大数はパケット数保持部３６が保持している数Ｎである。

【００５４】

図８において、実施の形態２と同じように、パケット検査部３５は自分宛に送られたパケットの中に、ＩＣＭＰ１３が含まれるか否かを調査する。もしＩＣＭＰ１３が含まれていると経路上にＬＳＮ１が存在すると判定する。

【００５５】

ネットワーク上にＬＳＮ１が存在し、ＬＳＮ１が端末２に割り当てているアドレスを変えたポート番号の数が２００とすると、Ｎの値が２０１以上であればＩＣＭＰ１３がＬＳＮ１より発行され、Ｎが２００以下であれば、ＩＣＭＰ１３は発行されないこととなる。端末２からネットワークに向けて、ポート番号を変えたＵＤＰパケットをＮ個送信する間に、ＩＣＭＰ１３のパケットを端末２が受け取り、パケットの検査結果がＩＣＭＰ１３であることを判別したときには、検査結果はＮＧ（ユーザの必要なポート数が確保できない）であり、ＩＣＭＰ１３が検出されなかった場合はＯＫ（ユーザの必要なポート数が確保できる）となる。

【００５６】

パケット検査部３５においてＩＣＭＰ１３番が検知されると、検査装置の判断としてＬＳＮが経路上に存在し、アプリケーションが必要とするポート数Ｎを確保できないことが判定され、処理が終了する。

【００５７】

図９は本発明の第３の実施の形態の動作を示している。実施の形態２とほぼ同じで、ＩＣＭＰ１３を含むパケットが受信されたとき（Ｓ６５）、必要なポート数が確保できないと判断する（Ｓ９２）。一方、ｉがＮ－１を超えたとき（Ｓ９１）、必要なポート数が確保できると判断する（Ｓ９３）。

【００５８】

なお、一般的にNATではNAT機能を使用する際のIPアドレス／ポート番号の動的変換テー

ブルの有効保持時間が定められており、有効保持時間を過ぎたIPアドレス／ポート番号は開放されて再度利用されることになる。本実施の形態で送信元ポート番号を変えてパケットを送ることでNAT機能でのポート番号を消費をしているが、パケットの送出間隔が長いとNAT側でポート番号が開放されてしまう場合がある（一般的にUDPでは5分程度の場合が多い）。そのため、パケット送信部３２は全てのパケット送信を有効保持期間内に行うようにすると確実にＬＳＮのポートを消費しているため検査の精度を向上させることができる。

【００５９】

また、端末上で検査処理以外にポートを利用するアプリケーションが動作しているとポート制限数を正確に検知することができない。そのため、他のアプリケーションで利用しているポート数を把握するか、端末起動時など他のアプリケーションが動作していな状態で検査装置を実行することでより精度の高い検査を行うことができる。

【００６０】

（第４の実施形態）

以下、本発明の第４の実施形態について、図面を参照しながら説明する。図１０は、本発明の第４の実施形態に係るアプリケーション切替装置４０の一例を示す図である。図１０において、４１はＬＳＮ発見部であり、内部は実施の形態２または３の端末２と同じである。４２はプログラム切替部、４３はポート制限型アプリケーション（ＬＳＮ用アプリケーション）、４４は通常のアプリケーションである。

【００６１】

ＬＳＮ発見部４１はアプリケーション切替装置４０がＬＳＮの下にいるかどうかを判定する。例えば実施形態の２または３で示したパケット検査部３５において、ＬＳＮを発見するとプログラム切替部４２にＬＳＮの有り無しを伝えることができる。プログラム切替部４２は、通常は通常アプリケーション４４を起動するが、ＬＳＮを発見したときにはポート制限型アプリケーション４３を起動する。

【００６２】

すなわち、本発明のアプリケーション切替装置４０では、例えば装置の電源が投入されたとき、ＬＳＮ発見部４１により通信経路上のＬＳＮの存在をチェックする。もしもＬＳＮが発見されなかったときには、通常アプリケーション４４を起動し通常の動作を行うが、ＬＳＮが発見されたときには、ポート制限型アプリケーション４３を起動する。ポート制限型アプリケーションは通常アプリケーションに比べて機能上の制限あるいは動作速度などに制限を生じるが、ＬＳＮによって使用可能なポート数が制限されることにより動作を停止してしまうことが無いように作られている。

【００６３】

このようにプログラム切替え装置を構成することにより、ＬＳＮの存在如何にかかわらず装置は動作を実行することができるように構成可能である。

【００６４】

ポート制限型アプリケーションとしては、インターネット上の地図アプリケーションが考えられる。例えばGoogle Map（登録商標）のような地図アプリにおいては、ユーザがマウスなどで自由に地図をスクロールできるようになっているが、これは地図を一定の大きさの小さな画像に分割して端末に送ることで実現されている。つまり、１つの地図のように見えても、実際は複数の画像の組み合わせで構成されており、各画像ごとにポートを消費している。

【００６５】

ここで、ポート数の制限があった場合、地図画像を通常よりも粗い単位で区切り一つあたりの画像サイズを大きくすることで使用するポート数を減らすことができる。ただし、画像サイズが大きくなるため表示までに時間がかかったり、表示されない領域の画像も読み込むことになるなど効率が下がる可能性がある。例えば、図１１のように送信する画像を通常アプリの縦横ともに2倍のサイズにすることでポートの数を4分の1に減らすことができる。なお、ＬＳＮ発見部が検知した使用可能なポート数に応じて動的にアプリの動作

を変えても良い。例えば地図アプリであれば1つの画像サイズをポート数に合わせて動的に変えることで最適な動作となる。さらにポートを消費する別アプリが起動したら、別アプリの使用するポート数も考慮して動作を決めてもよい。

【００６６】

（第５の実施形態）

以下、本発明の第５の実施形態について、図面を参照しながら説明する。図１２は、本発明の第５の実施形態に係るＬＳＮ検出装置の一例を示す図である。図１２において、４１はＬＳＮ発見部、４５はメッセージ表示部、４６はディスプレイである。

ＬＳＮ発見部４１の内部は、実施の形態２または３の端末２と同じである。すなわち、ＬＳＮ発見部４１内部のパケット検査部３５がＬＳＮを発見するとメッセージ表示部４５にＬＳＮの有り無しを伝えることができる。メッセージ表示部４５は、通信経路上にＬＳＮが存在する旨のメッセージを構成し、ディスプレイ４６上に表示する。

【００６７】

すなわち、本検出装置が起動されると、ＬＳＮ発見部４１によりネットワークをチェックする。ＬＳＮ発見部４１がＬＳＮを発見すると、メッセージ表示部４５にＬＳＮの存在を通知する。メッセージ表示部は、“本装置はＬＳＮを介在するネットワークに接続されました”なるメッセージを構成する。

【００６８】

このように構成することで、このＬＳＮメッセージをディスプレイ４６上に表示することにより、ユーザはネットワーク上にＬＳＮが存在することを認知する。

【００６９】

（第６の実施形態）

以下、本発明の第６の実施形態について、図面を参照しながら説明する。図１３は、本発明の第５の実施形態に係るＬＳＮ検出装置の一例を示す図である。図１３において、４１はＬＳＮ発見部、４７は結果構成部、４８は結果送信部、４９は、結果を集積する結果集積サーバである。

【００７０】

ＬＳＮ発見部４１の内部は、実施の形態２または３の端末２と同じである。すなわち、ＬＳＮ発見部４１内部のパケット検査部３５がＬＳＮを発見すると、結果構成部４７にＬＳＮの有り無しを伝えることができる。結果構成部４７は、通信経路上にＬＳＮが存在する旨のメッセージを構成し、結果送信部４８に伝送する。結果送信部４８は、結果をネットワークを通じて結果集積サーバ４９に伝送する。

【００７１】

すなわち、本検出装置が起動されると、ＬＳＮ発見部４１によりネットワークをチェックする。ＬＳＮ発見部４１がＬＳＮを発見すると、結果構成部４７にＬＳＮの存在を通知する。結果構成部４７は、“本装置はＬＳＮを介在するネットワークに接続されました”ことを意味するメッセージを構成し、結果送信部４８に伝送する。結果送信部４８は結果をネットワークを通じて４９結果集積サーバに伝送する。

【００７２】

このように構成することにより、端末がＬＳＮネットワークに接続されたことをサーバに蓄積し、このことにより、端末管理者あるいは、サービスプロバイダがＬＳＮの存在を宅外より認知することが可能になる。

【００７３】

（第７の実施形態）

以下、本発明の第７の実施形態について、図面を参照しながら説明する。図１４は、本発明の第４から６の実施形態に係るＬＳＮ検出装置の別の実現方法の一例を示す図である。図１４において、１０１は通信端末、１０２、１０３，１０５はルータ、１０４はＬＳＮ，１０６はサーバである。

【００７４】

ＵＰｎＰにより試験を行うべきＮＡＴを発見するためには、まず、トレースルート等に

より経路上のルータ（中継ノード）を探索（特許文献３または４にも方法が開示されている）し、経路上のルータをすべて発見する。

【００７５】

発見したルータのうち、プライベートＩＰアドレスから、グローバルＩＰアドレスへの変換点に該当、すなわち、端末から見て初めてグローバルアドレスになるルータが検査すべき該当ルータとなる。

【００７６】

通信端末１０１は、まず、サーバ１０６に向けてトレースルートを実行する。トレースルートとは、ＩＣＭＰやＵＤＰのパケットにおいてＴＴＬ値（ＴＩＭＥ　ＴＯ　ＬＩＶＥ）を１，２，３、、、、Ｎと順番に増やしながらパケットをサーバに向かって複数送信し、ルータをひとつ超えるたびにＴＴＬが一つ減ぜられることにより、ルータ一段超えるごとに、ＴＴＬ値がゼロになっていくことで、ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ　Ｐｒｏｔｏｃｏｌ）　ＴＩＭＥ　ＥＸＣＥＥＤＥＤ　ＭＥＳＳＡＧＥが返送されてくることを観測することにより、送信先に至るルータの個数、アドレスを検査するものである。ＩＣＭＰ　ＴＩＭＥ　ＥＸＣＥＥＤＥＤ　ＭＥＳＳＡＧＥとは、中継するパケットの生存時間（ＴＴＬ：Ｔｉｍｅ　Ｔｏ　Ｌｉｖｅ）の超過によるパケットの破棄を、送信元に報告するメッセージである。

【００７７】

図１５は、図１４における端末１０１において、サーバ１０６に向けてトレースルートを実行した結果である。図１５において、項目３と項目４のところでグローバルアドレスとプライベートアドレスとの切替が起こることがわかる。この切替が起こる点が、ネットワーク上にＬＳＮが存在するとした際には、ＬＳＮの位置を示すことになる。つまり、端末１０１から見て、最初にグローバルアドレスに切替が起こった点より、一つ手前、すなわち、一段端末に近いところのプライベートアドレスのルータがＬＳＮの候補ということになる。

【００７８】

このときのトレースルートの結果を見ると、プライベートのＩＰアドレスが得られる。このＩＰアドレスは、ルータが、ユニバーサル・プラグ・アンド・プレイ（ＵＰｎＰ）の対応であれば、ＵＰｎＰ－ＩＧＤにおけるコントロールポイントである。ＵＰｎＰ　ＩＧＤ（Ｉｎｔｅｒｎｅｔ　Ｇａｔｅｗａｙ　Ｄｅｖｉｃｅ）の詳細な仕様については、非特許文献２及び非特許文献３に詳しく記載されている。

【００７９】

このアドレスに対し、端末は、ＵＰｎＰのディスカバリメッセージである“Ｍ－Ｓｅａｒｃｈ”を用いたルータディスカバリ用パケット（以下、推定ルータパケットという）を作成して、ユニキャストで送信する。このときのパケットを図１６に示す。
この“Ｍ－Ｓｅａｒｃｈ”に対して、ユニバーサル・プラグ・アンド・プレイ（ＵＰｎＰ）に基づいて応答を返してくるルータはこれはＬＳＮではなく、一定時間内に応答を返してこない、ルータはＬＳＮであると判定をする。一定時間とはネットワークデバイスとしての十分な応答時間を考慮して設定するとよい。例えば３０秒などを選択することが可能である。

【産業上の利用可能性】

【００８０】

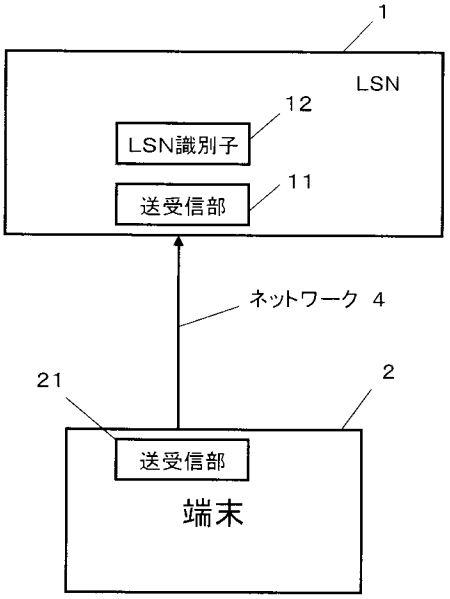
本発明に係るラージスケールＮＡＴ検出方法および装置は、端末とネットワーク上のサーバ間にＬＳＮが存在する場合、ＬＳＮが実際に存在するか否か、を判断するのに有用であり、また、ＬＳＮが存在した場合、ＬＳＮに対応したアプリケーションに動作をスイッチさせたり、または、ユーザにＬＳＮの存在を知らせたりすることでアプリケーションの動作を保障し、安定化させることでユーザへの不要な混乱をさけることができ、産業上非常に有用である。

【符号の説明】

【００８１】

１－ＬＳＮ
２－端末
３－サーバ
４－ネットワーク
１１－送受信部
１２－ＬＳＮ識別子
２１－送受信部
３１－送信ポート制御部
３２－パケット送信部
３３－パケット受信部
３４－ネットワーク制御部
３５－パケット検査部
３６－パケット数保持部
４０－アプリケーション切替装置
４１－ＬＳＮ発見部
４２－プログラム切替部
４３－ポート制限型アプリケーション
４４－通常アプリケーション
４５－メッセージ表示部
４６－ディスプレイ
４７－結果構成部
４８－結果送信部
４９－結果集積サーバ
１０１－通信端末
１０２－ルータ
１０３－ルータ
１０４－ＬＳＮ
１０５－ルータ
１０６－サーバ

【図１】

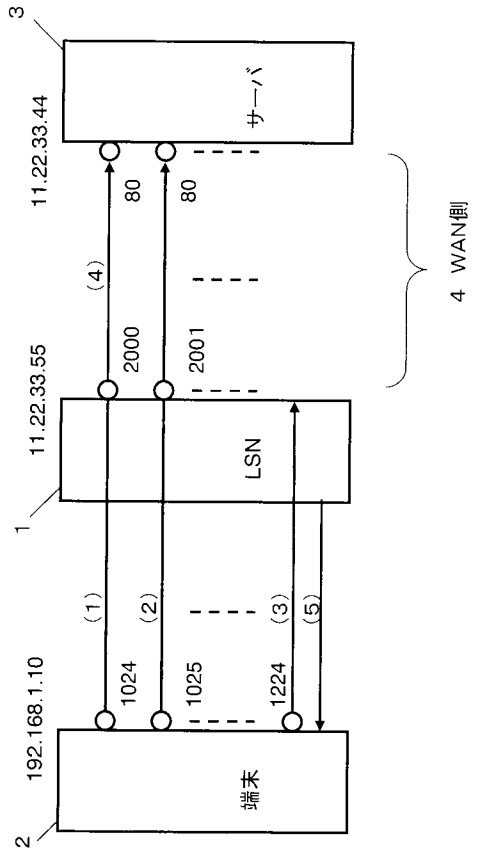


【図２】

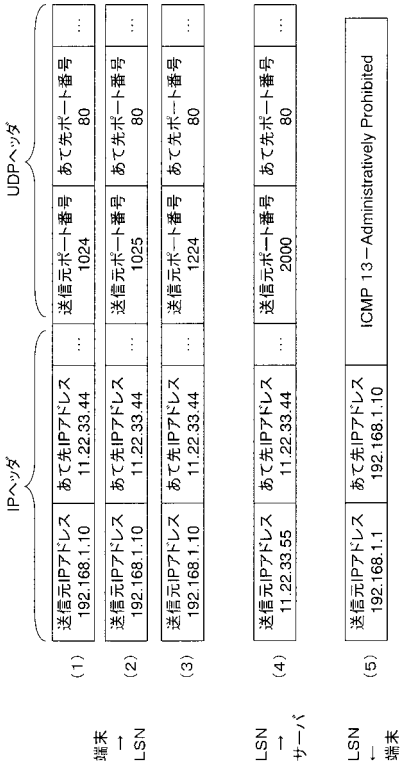
LSN識別子 12

LSN名	WANアドレス	制限ポート数
lsn1.lsn.com	11.22.33.44	2000

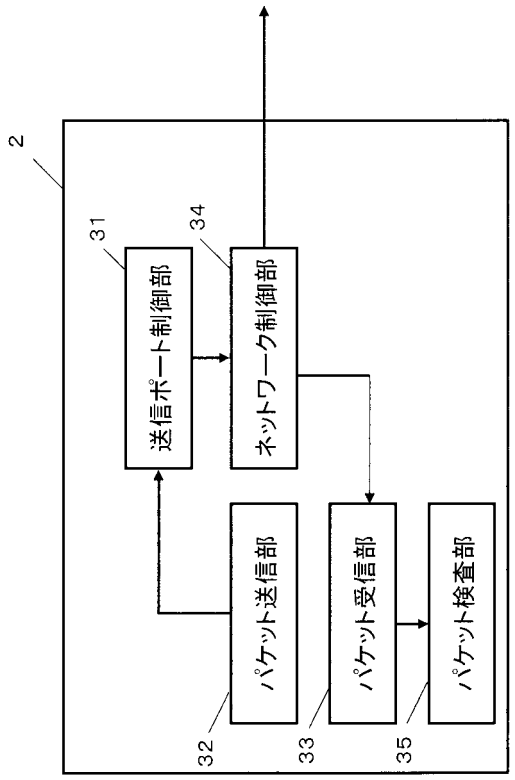
【図３】



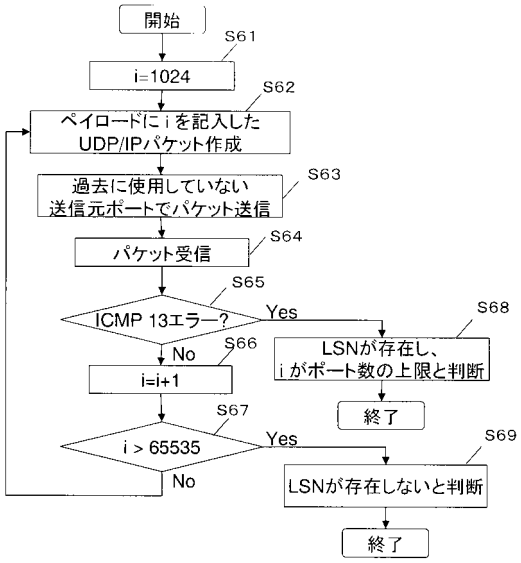
【図４】



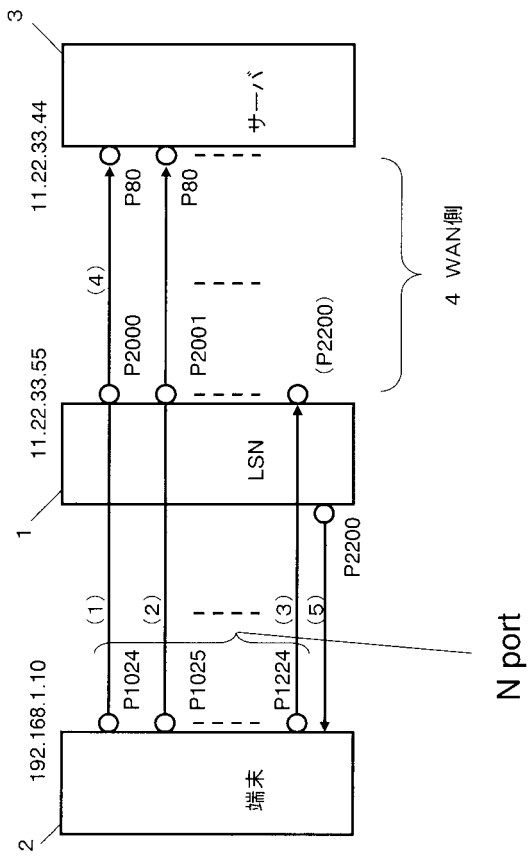
【図５】


2
31
34
送信ポート制御部
ネットワーク制御部
パケット送信部
パケット受信部
パケット検査部
32
33
35

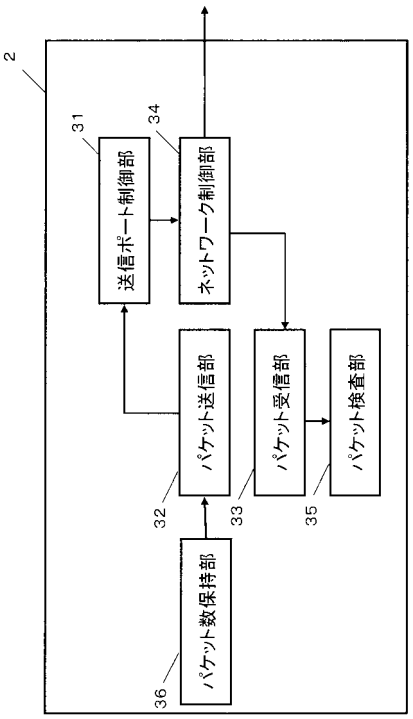
【図６】


開始
S61
i=1024
S62
ペイロードにiを記入した
UDP/IPパケット作成
S63
過去に使用していない
送信元ポートでパケット送信
S64
パケット受信
S65
ICMP 13エラー？
Yes
S68
LSNが存在し、
iがポート数の上限と判断
終了
No
S66
i=i+1
S67
i > 65535
Yes
S69
LSNが存在しないと判断
終了
No

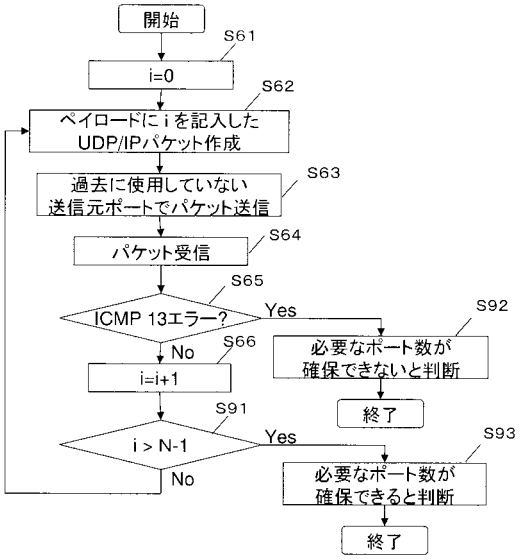
【図７】


3
11.22.33.44
サーバ
P80
P80
(4)
P2000
P2001
(P2200)
4 WAN側
11.22.33.55
LSN
1
P2200
(1)
(2)
(3)
(5)
P1024
P1025
P1224
N port
192.168.1.10
端末
2

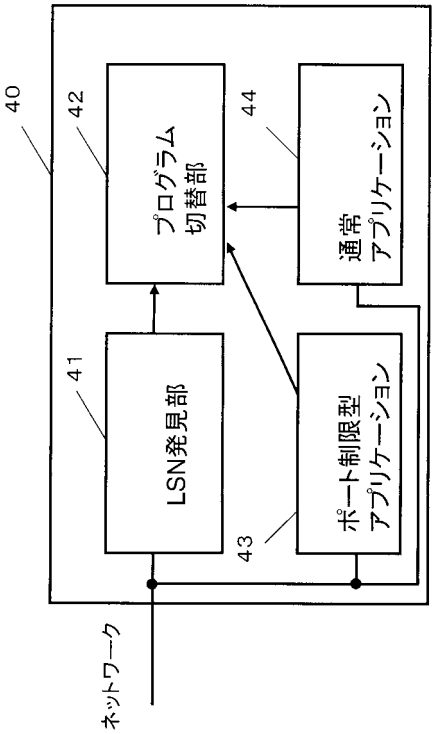
【図８】


2
31
34
送信ポート制御部
ネットワーク制御部
パケット送信部
パケット受信部
パケット検査部
32
33
35
パケット数保持部
36

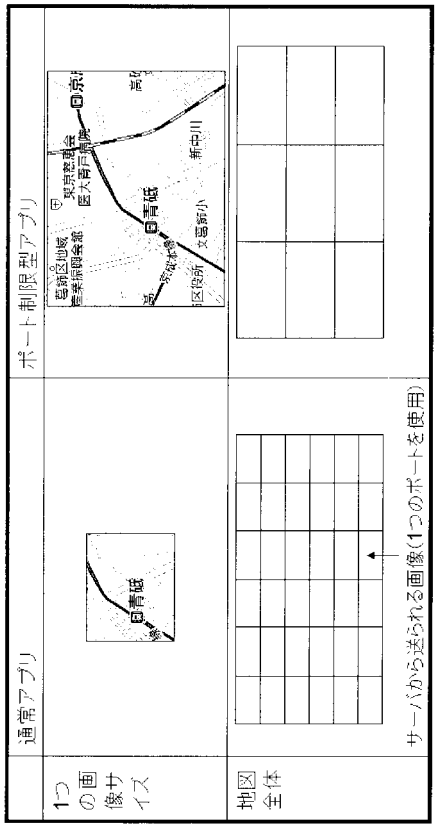
【図９】



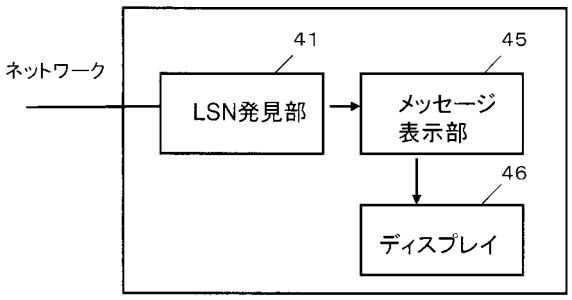
【図１０】



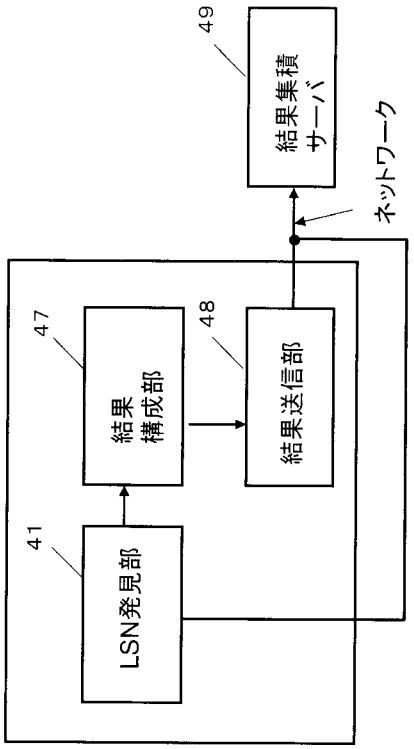
【図１１】



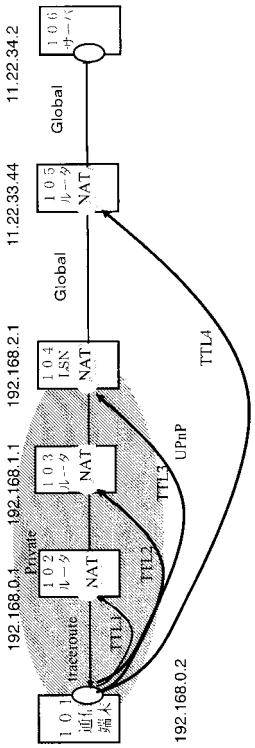
【図１２】



【図１３】



【図１４】



【図１５】

% traceroute 11.22.34.2

1. 192.168.0.1
2. 192.168.1.1
3. 192.168.2.1
4. 11.22.33.44
5. 11.22.34.2

【図１６】

・・・・・★M-SEARCH（WANPPPConnection）
・・・・・M-SEARCH * HTTP/1.1
・・・・・HOST: 192.168.2.1:1900
・・・・・MAN: "ssdp:discover"MX: 3
・・・・・ST: urn:schemas-upnp-org:service:WANPPPConnection:1

・・・・・★M-SEARCH（WANIPConnection）
・・・・・M-SEARCH * HTTP/1.1
・・・・・HOST: 192.168.2.1:1900
・・・・・MAN: "ssdp:discover"MX: 3
・・・・・ST: urn:schemas-upnp-org:service:WANIPConnection:1

フロントページの続き

(56)参考文献　特表２００５－５０５１７５（ＪＰ，Ａ）
国際公開第２００９／００１４３４（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／２８