

(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2007-201564

(P2007-201564A)

(43) 公開日 平成19年8月9日(2007.8.9)

(51) Int.Cl.

H04L 12/56 (2006.01)

F I

H04L 12/56 100Z

テーマコード (参考)

5K030

審査請求 有 請求項の数 42 O L (全 54 頁)

(21) 出願番号 特願2006-14472 (P2006-14472)

(22) 出願日 平成18年1月23日 (2006.1.23)

(特許庁注：以下のものは登録商標)

1. L i n u x

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(74) 代理人 100079005

弁理士 宇高 克己

(72) 発明者 吉見 英朗

東京都港区芝五丁目7番1号 日本電気株式会社内

(72) 発明者 榎本 敦之

東京都港区芝五丁目7番1号 日本電気株式会社内

(72) 発明者 崔 珍龍

東京都港区芝五丁目7番1号 日本電気株式会社内

最終頁に続く

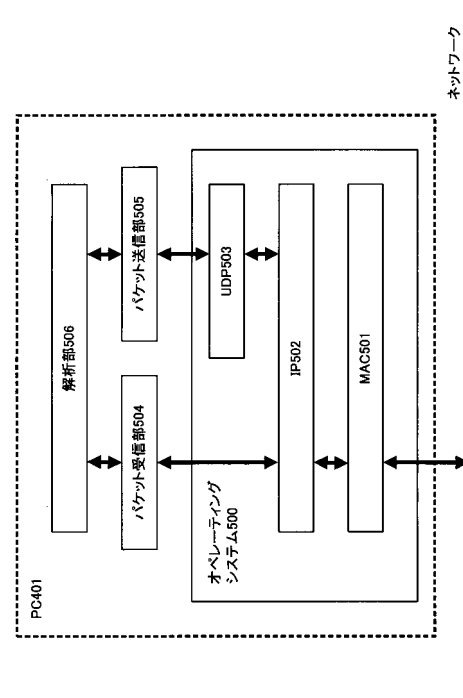
(54) 【発明の名称】 推定システム、端末、推定方法、およびプログラム

(57) 【要約】

【課題】 ネットワーク上でのヘッダ変換を推定するための専用サーバを設置することなく、推定に必要な情報を収集してネットワーク上でのヘッダ変換を推定できる技術を提供することにある。

【解決手段】 ネットワーク上の装置に関する情報を推定するシステムであって、送信したパケットに応答して送られてくる通信用のプロトコルで定められているエラーメッセージ又は制御メッセージを用いてネットワーク上の装置に関する情報を推定するシステム。

【選択図】 図5



【特許請求の範囲】

【請求項 1】

ネットワーク上の装置に関する情報を推定する推定システムであって、
送信されて来た情報収集用のパケットに応答して制御用のメッセージを返信する返信手段と、

前記返信手段からの制御用のメッセージに基づいて、前記ネットワーク上の装置に関する情報を推定する推定手段と

を備えたことを特徴とする推定システム。

【請求項 2】

前記返信手段は、待ち受け状態となっていないポート番号を宛先とした情報収集用のパケットに
10 応答して、到達不能を示す制御用のメッセージを返信する手段であることを特徴とする請求項 1 に記載の推定システム。

【請求項 3】

前記返信手段は、前記情報収集用のパケットをヘッダのデータ部に格納した制御用のメッセージを返信する手段であることを特徴とする請求項 1 又は請求項 2 に記載の推定システム。

【請求項 4】

前記返信手段は、前記情報収集用のパケットが通過できる装置の個数を示す情報が 0 である情報収集用のパケットに
20 応答して、前記情報収集用のパケットを破棄したことを示す制御用のメッセージを返信する手段であることを特徴とする請求項 1 から請求項 3 のいずれかに記載の推定システム。

【請求項 5】

前記推定手段は、品質を示す情報に基づいて推定する手段であることを特徴とする請求項 1 から請求項 4 のいずれかに記載の推定システム。

【請求項 6】

前記推定手段は、前記情報収集用のパケットが分割されたことを示す情報に基づいて推定する手段であることを特徴とする請求項 1 から請求項 4 のいずれかに記載の推定システム。

【請求項 7】

前記推定手段は、チェックサム値に基づいて推定する手段であることを特徴とする請求項 1 から請求項 4 のいずれかに記載の推定システム。
30

【請求項 8】

前記推定手段は、IP チェックサム値に基づいて、前記制御用のメッセージのデータ部の送信元 IP アドレスを変更した装置に関する情報を推定し、UDP チェックサム値または TCP チェックサム値に基づいて前記制御用のメッセージのデータ部の送信元ポート番号を変更した装置に関する情報を推定する手段であることを特徴とする請求項 7 に記載の推定システム。

【請求項 9】

前記推定手段は、UDP チェックサム値または TCP チェックサム値に基づいて、前記制御用のメッセージのデータ部の送信元 IP アドレスを変更した装置に関する情報を推定する手段であることを特徴とする請求項 8 に記載の推定システム。
40

【請求項 10】

前記推定手段は、ネットワークの経路調査試験の結果を加味して、推定する手段であることを特徴とする請求項 7 から請求項 9 のいずれかに記載の推定システム。

【請求項 11】

前記経路調査試験は、通過できる装置の個数を示す情報の数値が互いに異なる複数の情報収集用のパケットを送信することによって行われる調査試験であることを特徴とする請求項 10 に記載の推定システム。

【請求項 12】

前記経路調査試験は、以前推定された端末までに通過する装置の個数を調査する試験で
50

あることを特徴とする請求項 10 又は請求項 11 に記載の推定システム。

【請求項 13】

前記経路調査試験は、プライベートIPアドレスとグローバルIPアドレスとが切り替わる位置に設置されている装置までに通過した装置の個数を調査する試験であることを特徴とする請求項 10～請求項 12 に記載の推定システム。

【請求項 14】

前記推定手段は、推定結果を前記ネットワーク上の端末に通知する手段であることを特徴とする請求項 1 から請求項 13 にいずれかに記載の推定システム。

【請求項 15】

前記推定手段は、前記ネットワーク上の他の端末から推定結果を受け取ると、その推定結果を記憶するように構成されていることを特徴とする請求項 14 に記載の推定システム。

10

【請求項 16】

前記推定手段は、複数の推定結果に基づいて前記ネットワーク上のコンピュータのポート番号の割り当て処理の規則性を推定する手段であることを特徴とする請求項 14 又は請求項 15 に記載の推定システム。

【請求項 17】

前記推定手段は、前記推定結果をメールまたは電話を用いて通信相手に通知するように構成されていることを特徴とする請求項 14 から請求項 16 にいずれかに記載の推定システム。

20

【請求項 18】

前記推定手段は、前記情報収集用のパケットが通過できる装置の個数を示す情報を前記推定結果に基づいて取得した宛先に届かない値に設定して、この宛先に SYN パケットを送信し、この SYN パケットのシーケンス番号を前記宛先に通知する手段であることを特徴とする請求項 1 から請求項 17 のいずれかに記載の推定システム。

【請求項 19】

前記推定手段は、前記送信された SYN パケットのシーケンス番号を受け取ると、このシーケンス番号を考慮した応答確認パケットを送信する手段であることを特徴とする請求項 18 に記載の推定システム。

【請求項 20】

ネットワーク上の装置に関する情報を推定するシステムであって、
通信用のプロトコルで定められているエラーメッセージ又は制御メッセージを用いて前記ネットワーク上の装置に関する情報を推定することを特徴とする推定システム。

30

【請求項 21】

端末であって、
情報収集用のパケットを送信する手段と、
前記情報収集用のパケットに応答して送信された制御用のメッセージに基づいて、ネットワーク上の装置に関する情報を推定する推定手段と、
を有することを特徴とする端末。

【請求項 22】

ネットワーク上の装置に関する情報を推定する推定方法であって、
送信されて来た情報収集用のパケットに応答して制御用のメッセージを返信する返信ステップと、
受信したメッセージが前記情報収集用のパケットに応答して返信された制御用のメッセージであるかを判断する判断ステップと、
前記判断の結果、受信したメッセージが前記情報収集用のパケットに応答して返信された制御用のメッセージであると判断された場合、この制御用のメッセージに基づいて、前記ネットワーク上の装置に関する情報を推定する推定ステップと
を備えたことを特徴とする推定方法。

40

【請求項 23】

50

前記返信ステップは、待ち受け状態となっていないポート番号を宛先とした情報収集用のパケットに応答して、到達不能を示す制御用のメッセージを返信するステップであることを特徴とする請求項 22 に記載の推定方法。

【請求項 24】

前記返信ステップは、前記情報収集用のパケットをヘッダのデータ部に格納した制御用のメッセージを返信するステップであることを特徴とする請求項 22 又は請求項 23 に記載の推定方法。

【請求項 25】

前記返信ステップは、前記情報収集用のパケットが通過できる装置の個数を示す情報が 0 である情報収集用のパケットに応答して、前記情報収集用のパケットを破棄したことを示す制御用のメッセージを返信するステップであることを特徴とする請求項 22 から請求項 24 のいずれかに記載の推定方法。

10

【請求項 26】

前記推定ステップは、品質を示す情報に基づいて推定するステップであることを特徴とする請求項 22 から請求項 25 のいずれかに記載の推定方法。

【請求項 27】

前記推定ステップは、前記情報収集用のパケットが分割されたことを示す情報に基づいて推定するステップであることを特徴とする請求項 22 から請求項 25 のいずれかに記載の推定方法。

【請求項 28】

前記推定ステップは、チェックサム値に基づいて推定するステップであることを特徴とする請求項 22 から請求項 25 のいずれかに記載の推定方法。

20

【請求項 29】

前記推定ステップは、
IP チェックサム値に基づいて、前記制御用のメッセージのデータ部の送信元 IP アドレスを変更した装置に関する情報を推定するステップと、
UDP チェックサム値または TCP チェックサム値に基づいて前記制御用のメッセージのデータ部の送信元ポート番号、若しくは IP アドレスを変更した装置に関する情報を推定するステップと
を有することを特徴とする請求項 28 に記載の推定方法。

30

【請求項 30】

前記推定ステップは、
ネットワークの経路調査試験を実行する経路調査実行ステップと、
前記実行結果を加味して装置に関する情報を推定する詳細情報推定ステップと
を有することを特徴とする請求項 28 又は請求項 29 に記載の推定方法。

【請求項 31】

前記経路調査実行ステップは、通過できる装置の個数を示す情報の数値が互いに異なる複数の情報収集用のパケットを送信するステップであることを特徴とする請求項 30 に記載の推定方法。

【請求項 32】

前記経路調査実行ステップは、以前推定された装置までに通過する装置の個数を調査するステップであることを特徴とする請求項 30 又は請求項 31 に記載の推定方法。

40

【請求項 33】

前記経路調査実行ステップは、プライベート IP アドレスとグローバル IP アドレスとが切り替わる位置に設置されている装置までに通過した装置の個数を調査するステップであることを特徴とする請求項 30 ～請求項 32 に記載の推定方法。

【請求項 34】

前記推定ステップは、推定結果を前記ネットワーク上の端末に通知するステップを有することを特徴とする請求項 22 から請求項 33 のいずれかに記載の推定方法。

【請求項 35】

50

前記推定ステップは、前記ネットワーク上の他の端末から推定結果を受け取ると、その推定結果を記憶するステップを有することを特徴とする請求項 3 4 に記載の推定方法。

【請求項 3 6】

前記推定ステップは、複数の推定結果に基づいて前記ネットワーク上のコンピュータのポート番号の割り当て処理の規則性を推定するステップであることを特徴とする請求項 3 4 又は請求項 3 5 に記載の推定方法。

【請求項 3 7】

前記推定ステップは、前記推定結果をメールまたは電話を用いて通信相手である端末に通知する推定ステップを有することを特徴とする請求項 3 4 から請求項 3 6 にいずれかに記載の推定方法。

10

【請求項 3 8】

前記推定ステップは、前記情報収集用のパケットが通過できる装置の個数を示す情報を前記推定結果に基づいて取得した宛先に届かない値に設定して、この宛先に SYN パケットを送信し、この SYN パケットのシーケンス番号を前記宛先に通知するステップを有することを特徴とする請求項 2 2 から請求項 3 7 のいずれかに記載の推定方法。

【請求項 3 9】

前記推定ステップは、
前記送信された SYN パケットのシーケンス番号を受け取る受取ステップと、
前記受け取ったシーケンス番号を考慮した応答確認パケットを送信するステップと
を有することを特徴とする請求項 3 8 に記載の推定方法。

20

【請求項 4 0】

ネットワーク上の装置に関する情報を推定する推定システムのプログラムであって、前記プログラムは前記システムを、
送信されて来た情報収集用のパケットに応答して制御用のメッセージを返信する返信手段と、
前記返信手段からの制御用のメッセージに基づいて、前記ネットワーク上の装置に関する情報を推定する推定手段と
して機能させることを特徴とするプログラム。

【請求項 4 1】

端末のプログラムであって、前記プログラムは前記端末を、
受信したメッセージが情報収集用のパケットに応答して返信された制御用のメッセージであるかを判断する判断手段と、
前記判断の結果、受信したメッセージが前記情報収集用のパケットに応答して返信された制御用のメッセージであると判断された場合、この制御用のメッセージに基づいて、前記ネットワーク上の装置に関する情報を推定する推定手段
として機能させることを特徴とするプログラム。

30

【請求項 4 2】

ネットワーク上の装置に関する情報を推定するシステムのプログラムであって、前記プログラムは前記システムを、
通信用のプロトコルで定められているエラーメッセージ又は制御メッセージを用いて前記ネットワーク上の装置に関する情報を推定する手段として機能させることを特徴とするプログラム。

40

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は、I C M P メッセージを利用したネットワークの環境を推定する技術に関し、特に、ネットワークに接続されている通信装置に関する情報を推定するための技術に関する。

【背景技術】

【0 0 0 2】

50

ローカルエリアネットワーク（LAN）やインターネットといった情報通信ネットワークは、様々な通信装置を組み合わせることにより構成されている。

【0003】

まず、ネットワークの構成例として、図1のようなネットワークを考える。

【0004】

図1には、インターネットのようなネットワーク4と、アドレス変換を行うNATルータ2、NATルータ6と、ユーザが操作するPC1、PC7と、インターネット上に設置されている任意のPC5と、パケットの経路を行うルータ3が含まれる。また、ネットワーク4は、パケットの経路制御を行うルータ8～11を含んでいる。

【0005】

10

以下において、図1の構成要素の機能について述べる。

【0006】

まず、NATルータ2の機能について説明する（以下の説明は、NATルータ6にも当てはまる）。

【0007】

NATルータ2の主な機能としては、アドレス変換（NAT：Network Address Translation）機能が挙げられる。LANのPC1には、プライベートIPアドレスが割り当てられているのが一般的であるが、LANのPC1をネットワーク4と接続するには、グローバルIPアドレスを割り当てる必要がある。この問題を解決するために、NATルータ2では、PC1がネットワーク4と接続できるように、プライベートIPアドレスとグローバルIPアドレスのアドレス変換を行う。具体的な処理としては、LANのPC1から送信されたパケットの送信元IPアドレスをグローバルIPアドレスに書き換えた後、ルータ3に転送する。図2には、参考のため、IPヘッダとUDPヘッダのフォーマットを示している。

20

【0008】

また、NATルータ2は、上記のようにPC1から送信されたパケットの送信元IPアドレスの変換だけでなく、送信元ポート番号までも変換するNAPT（NAPT：Network Address Port Translation）機能を搭載していることもある。NAPTはNATと同様の技術であるが、NATではIPアドレスしか変換しないのに対して、NAPTではさらにTCPやUDPのポート番号も変換するという特徴がある。これにより、1つのグローバルIPアドレスで、プライベートIPアドレスを持つ複数のPCを収容することができる。例えば、ダイヤルアップ接続では、インターネットサービスプロバイダ（ISP）から割り当てられるグローバルIPアドレスは1つしかないが、NAPTを使えば、LAN上の複数のPCが同時にネットワーク4へ接続できるようになる。

30

【0009】

次に、ルータ3の機能について説明する（以下の説明は、ルータ8～11にも当てはまる）。

【0010】

ルータ3の主な機能として、パケットの経路制御機能が挙げられるが、この機能に加えて、ルータ3には優先制御機能も搭載されている。優先制御機能とは、トラフィックの集中によりネットワーク内でパケット破棄が発生することが明白な場合には、重要なパケットを優先的に処理し、パケットが破棄されないようにする技術である。例えば、図1ではトラフィックの集中によりネットワーク4内でパケットが破棄される可能性がある。パケットが破棄されると、重要な通信サービスまでも応答が遅くなったり、サービスが異常終了してしまったりするという現象が発生してしまう。優先制御機能は、これらの問題を解決し、重要なサービスの安定稼動を実現するために利用されるものである。

40

【0011】

優先制御の実現方法としては、図1にその例を示しているが、ルータ3において、ネットワークの輻輳状態を監視するとともに、流入してくるパケットのToS値を書き換える。ここで、ToS値にはパケットの優先度など、パケットの品質を決める情報が書き込まれる

50

。ネットワーク 4 内のルータでは、この ToS 値に従ったパケットの優先制御を行うことにより、特定のフローにのみ高品質の通信サービスが提供される。

【0012】

また、ルータには、この優先制御機能に加えて、パケットのフラグメント機能も搭載されている。IP パケットを送信する PC 1 は、接続しているネットワーク 4 の最大転送単位 (MTU: Maximum Transfer Unit) を最大サイズとするパケットを送信することが理想的である。このような理想的な環境下では、PC 1 から送信された IP パケットは生成されたサイズそのまま宛先ホストに到達することになるが、図 1 のルータ 8 とルータ 9 の間のように、通信経路上に小さな MTU を持つネットワークが存在する場合、IP パケットはその境界のルータで細分化して送られる。これがルータのフラグメント機能である。フラグメントを行ったルータ 8 は、パケットのフラグフィールドの第 3 ビットを 1 に設定するとともに、最終パケットのフラグフィールドに 0 を設定する。また、フラグメントオフセットフィールドにはデータのオフセット値を設定する。

10

【0013】

フラグメント化された IP パケットを元の形に戻すのは、最終的な宛先ホストの役割である。宛先ホストでは、フラグフィールドとフラグメントオフセットフィールドの情報を基にして、フラグメント化された IP パケットを再構成する。

【0014】

以上のように、NAT ルータやルータはパケットヘッダに様々な変換処理を施すが、このような変換処理が発生したという事象は送信元 PC 1 には隠蔽されている。このため、送信元 PC 1 では、ネットワークがどのように構成されており、どんな制御機能が働いているのかを把握することは出来ない。このようにネットワークがブラックボックス化され、ヘッダ変換を送信元 PC 側で検出できなくなると、様々な問題が出てくる。以下において、これらの問題点について述べる。

20

【0015】

まず、NAT ルータ 2 で実行されたヘッダ変換の内容を PC 1 が検出できない場合の問題について述べる。

【0016】

NAT ルータ 2 の内側にある PC 1 と、NAT ルータ 6 の内側にある PC 7 との間でパケットをやり取りするには、双方に設置された NAT ルータのグローバル IP アドレスとポート番号を宛先としたパケットを送信する必要がある。つまり、あらかじめ通信相手の NAT ルータの情報を取得しておく必要があり、例えば、PC 7 から PC 1 にパケットを送信するには、NAT ルータ 2 の情報が必要になる。NAT ルータ 2 の情報を取得する方法として、NAT ルータ 2 に繋がれている PC 1 から教えてもらうという方法が考えられるが、上述したように、NAT ルータ 2 のアドレス変換内容は PC 1 に隠蔽されているので、この方法は破綻してしまう。

30

【0017】

以上のことから、NAT ルータのアドレス変換処理を検出できなければ、NAT ルータに繋がれた PC 間でパケットをやり取りすることは出来ない。

【0018】

次に、ルータで行われた ToS 値の変換処理を PC 側で検出できない場合の問題について述べる。

40

【0019】

ネットワークで ToS 値による優先制御機能が働いていなければ、IP 電話や IP テレビなど高度な優先制御機能が必要されるリアルタイム型アプリケーションを利用することは難しい。この優先制御が働いているかどうかを判別する方法として、ToS 値の変化を検出することは効果的であるが、上述のように ToS 値の変換処理は PC 側には隠蔽されているので、この方法は破綻してしまう。

以上のことから、ルータの ToS 値の変換処理を検出できなければ、アプリケーションを利用できるかどうか事前に認識することは出来ない。

50

【0020】

次に、ルータで行われたフラグメント処理を、P C 側で検出できない場合の問題について述べる。

【0021】

パケットのフラグメントが発生しても通信自体に支障はないが、転送効率が落とされてしまう。例えば、図1のように、ネットワーク4のルータ8とルータ9の間のM T Uが1000バイトである環境において、P C 1から1500バイトのパケットが送信された場合、ルータ8において、1500バイトのデータは1000バイトと残りの500バイトの2つのデータにフラグメントされる。このようにフラグメントされると、ルータ8でフラグメント処理が発生するだけでなく、ルータ9では1つでなく2つのパケットを処理する必要となる。この結果、各ルータの負荷が増えるだけでなく、2つに分割されたパケットのうち、どちらかが壊れると、両方のパケットを廃棄しなければならなくなるため、ネットワーク4の負荷も増えてしまう。このようなフラグメントの発生を防ぐ方法として、P C 1においてフラグメントが起こらないパケットサイズを調べ、そのサイズに合わせたパケットを送信することが考えられるが、上述したように、フラグメントの発生はP C 1に隠蔽されているので、この方法は破綻してしまう。

【0022】

以上のことから、ルータのフラグメント処理を検出できなければ、パケットの転送効率の低下を防ぐことが出来ない。

【0023】

以上述べたように、通信経路上で行われたヘッダ変換を送信元P Cで検出できないと、様々な問題が生じてしまう。

【0024】

この課題を解決する方法の一例が、非特許文献1や特許文献1に記載されている。

【0025】

非特許文献1に記載の方法は、図3に示すように、ネットワーク304のようなインターネット上に専用サーバ312を設置する。図3のP C 301は、この専用サーバ312にパケットを送信する。専用サーバ312では、このP C 301から受信したパケットのヘッダ情報を拾い上げ、P C 301に折り返し通知してやる。ここで、専用サーバ312からP C 301に折り返し通知する情報としては、I Pアドレスやポート番号、そしてT o S値やフラグフィールドなどが挙げられる。

【0026】

一方、P C 301では、上記のように折り返し通知されたヘッダ情報から、通信経路上でヘッダ変換が行われたか否かを検出するとともに、そのヘッダ変換の内容を把握することができる。さらに、このヘッダ変換の情報を利用することにより、上述の各課題に対して対処することができる。

【0027】

例えば、N A Tルータのアドレス変換処理について言えば、非特許文献1の方法により、P C 301は、専用サーバ312からN A Tルータ302のI Pアドレスとポート番号を通知してもらった後、このN A Tルータ302の情報をP C 307に通知してやれば、P C 307からP C 301にパケットを送信することができる。

【0028】

また、ルータのToS値の変換処理について言えば、非特許文献1の方法により、P C 301は、専用サーバ312からパケットのToS値を通知してもらえば、ネットワーク内で優先制御機能が働いているかどうか認識できる。

【0029】

また、ルータのフラグメント処理について言えば、非特許文献1の方法により、P C 301は、専用サーバ312からパケットのフラグメントフィールドを通知してもらえば、フラグメントが起こらないようなパケットサイズを検出することができ、パケットの転送効率を最大化できる。

10

20

30

40

50

【非特許文献 1】 J・ローゼンバーグ (J. Rosenberg)、他 3 名、“RFC 3489: STUN 技術” [online]、[平成 16 年 9 月 1 日検索]、インターネット <http://www.faqs.org/rfcs/rfc3489.html>

【特許文献 1】 特開 2005-102196

【発明の開示】

【発明が解決しようとする課題】

【0030】

以下において、非特許文献 1 に記載の方法の問題点を述べる。

【0031】

非特許文献 1 に記載の方法は、専用サーバ 312 をインターネット上に設置しなければならないため、専用サーバ 312 の保守/運用作業が必要であり、手間がかかる。 10

【0032】

また、専用サーバ 312 へのインターネット上の悪意のある第 3 者からの攻撃を防ぐために、専用サーバ 312 のセキュリティレベルを維持する作業が必要であり、手間がかかる。

【0033】

さらに、専用サーバ 312 の処理負荷の急増を防ぐために、専用サーバ 312 の負荷分散作業が必要であり、手間がかかる。

【0034】

本特許は、これら全ての問題を解決するためになされたものであり、その目的とするところは、専用サーバ 312 を設置することなく、通信経路上でのヘッダ変換を推定できる方法を提供することにある。 20

【課題を解決するための手段】

【0035】

上記課題を解決するための第 1 の発明は、
ネットワーク上の装置に関する情報を推定する推定システムであって、
送信されて来た情報収集用のパケットに応答して制御用のメッセージを返信する返信手段と、

前記返信手段からの制御用のメッセージに基づいて、前記ネットワーク上の装置に関する情報を推定する推定手段と
を備えたことを特徴とする。 30

【0036】

上記課題を解決するための第 2 の発明は、上記第 1 の発明において、
前記返信手段は、待ち受け状態となっていないポート番号を宛先とした情報収集用のパケットに応答して、到達不能を示す制御用のメッセージを返信する手段であることを特徴とする。

【0037】

上記課題を解決するための第 3 の発明は、上記第 1 又は第 2 の発明において、
前記返信手段は、前記情報収集用のパケットをヘッダのデータ部に格納した制御用のメッセージを返信する手段であることを特徴とする。 40

【0038】

上記課題を解決するための第 4 の発明は、上記第 1 から第 3 のいずれかの発明において、
前記返信手段は、前記情報収集用のパケットが通過できる装置の個数を示す情報が 0 である情報収集用のパケットに応答して、前記情報収集用のパケットを破棄したことを示す制御用のメッセージを返信する手段であることを特徴とする。

【0039】

上記課題を解決するための第 5 の発明は、上記第 1 から第 4 のいずれかの発明において、
前記推定手段は、品質を示す情報に基づいて推定する手段であることを特徴とする。 50

【0040】

上記課題を解決するための第6の発明は、上記第1から第4のいずれかの発明において、

前記推定手段は、前記情報収集用のパケットが分割されたことを示す情報に基づいて推定する手段であることを特徴とする。

【0041】

上記課題を解決するための第7の発明は、上記第1から第4のいずれかの発明において、

前記推定手段は、チェックサム値に基づいて推定する手段であることを特徴とする。

【0042】

上記課題を解決するための第8の発明は、上記第7の発明において、

前記推定手段は、IPチェックサム値に基づいて、前記制御用のメッセージのデータ部の送信元IPアドレスを変更した装置に関する情報を推定し、UDPチェックサム値またはTCPチェックサム値に基づいて前記制御用のメッセージのデータ部の送信元ポート番号を変更した装置に関する情報を推定する手段であることを特徴とする。

【0043】

上記課題を解決するための第9の発明は、上記第8の発明において、

前記推定手段は、UDPチェックサム値またはTCPチェックサム値に基づいて、前記制御用のメッセージのデータ部の送信元IPアドレスを変更した装置に関する情報を推定する手段であることを特徴とする。

【0044】

上記課題を快活するための第10の発明は、上記第7から第8のいずれかの発明において、

前記推定手段は、ネットワークの経路調査試験の結果を加味して、推定する手段であることを特徴とする。

【0045】

上記課題を解決するための第11の発明は、上記第10の発明において、

前記経路調査試験は、通過できる装置の個数を示す情報の数値が互いに異なる複数の情報収集用のパケットを送信することによって行われる調査試験であることを特徴とする。

【0046】

上記課題を解決するための第11の発明は、上記第10又は第11の発明において、

前記経路調査試験は、以前推定された端末までに通過する装置の個数を調査する試験であることを特徴とする。

【0047】

上記課題を解決するための第13の発明は、上記第10から第12のいずれかの発明において、

前記経路調査試験は、プライベートIPアドレスとグローバルIPアドレスとが切り替わる位置に設置されている装置までに通過した装置の個数を調査する試験であることを特徴とする。

【0048】

上記課題を解決するための第14の発明は、上記第1から第13のいずれかの発明において、

前記推定手段は、推定結果を前記ネットワーク上の端末に通知する手段であることを特徴とする。

【0049】

上記課題を解決するための第15の発明は、上記第14の発明において、

前記推定手段は、前記ネットワーク上の他の端末から推定結果を受け取ると、その推定結果を記憶するように構成されていることを特徴とする。

【0050】

上記課題を解決するための第14又は第15の発明において、

前記推定手段は、複数の推定結果に基づいて前記ネットワーク上のコンピュータのポート番号の割り当て処理の規則性を推定する手段であることを特徴とする。

【0051】

上記課題を解決するための第17の発明は、上記第14から第16のいずれかの発明において、

前記推定手段は、前記推定結果をメールまたは電話を用いて通信相手に通知するように構成されていることを特徴とする。

【0052】

上記課題を解決するための第18の発明は、上記第1から第17のいずれかの発明において

前記推定手段は、前記情報収集用のパケットが通過できる装置の個数を示す情報を前記推定結果に基づいて取得した宛先に届かない値に設定して、この宛先にSYNパケットを送信し、このSYNパケットのシーケンス番号を前記宛先に通知する手段であることを特徴とする。

【0053】

上記課題を解決するための第19の発明は、上記第18の発明において、

前記推定手段は、前記送信されたSYNパケットのシーケンス番号を受け取ると、このシーケンス番号を考慮した応答確認パケットを送信する手段であることを特徴とする。

【0054】

上記課題を解決するための第20の発明は、

ネットワーク上の装置に関する情報を推定するシステムであって、

通信用のプロトコルで定められているエラーメッセージ又は制御メッセージを用いて前記ネットワーク上の装置に関する情報を推定することを特徴とする。

【0055】

上記課題を解決するための第21の発明は、

端末であって、

情報収集用のパケットを送信する手段と、

前記情報収集用のパケットに応答して送信された制御用のメッセージに基づいて、ネットワーク上の装置に関する情報を推定する推定手段とを有することを特徴とする。

【0056】

上記課題を解決するための第22の発明は、

ネットワーク上の装置に関する情報を推定する推定方法であって、

送信されて来た情報収集用のパケットに応答して制御用のメッセージを返信する返信ステップと、

受信したメッセージが前記情報収集用のパケットに応答して返信された制御用のメッセージであるかを判断する判断ステップと、

前記判断の結果、受信したメッセージが前記情報収集用のパケットに応答して返信された制御用のメッセージであると判断された場合、この制御用のメッセージに基づいて、前記ネットワーク上の装置に関する情報を推定する推定ステップとを備えたことを特徴とする。

【0057】

上記課題を解決するための第23の発明は、上記第22の発明において、

前記返信ステップは、待ち受け状態となっていないポート番号を宛先とした情報収集用のパケットに応答して、到達不能を示す制御用のメッセージを返信するステップであることを特徴とする。

【0058】

上記課題を解決するための第24の発明は、上記第22又は第23の発明において、

前記返信ステップは、前記情報収集用のパケットをヘッダのデータ部に格納した制御用のメッセージを返信するステップであることを特徴とする。

10

20

30

40

50

【0059】

上記課題を解決するための第25の発明は、上記第22から第24のいずれかの発明において、

前記返信ステップは、前記情報収集用のパケットが通過できる装置の個数を示す情報が0である情報収集用のパケットに応答して、前記情報収集用のパケットを破棄したことを示す制御用のメッセージを返信するステップであることを特徴とする。

【0060】

上記課題を解決するための第26の発明は、上記第22から第25のいずれかの発明において、

前記推定ステップは、品質を示す情報に基づいて推定するステップであることを特徴とする。 10

【0061】

上記課題を解決するための第27の発明は、上記第22から第25のいずれかの発明において、

前記推定ステップは、前記情報収集用のパケットが分割されたことを示す情報に基づいて推定するステップであることを特徴とする。

【0062】

上記課題を解決するための第28の発明は、上記第22から第25のいずれかの発明において、

前記推定ステップは、チェックサム値に基づいて推定するステップであることを特徴とする。 20

【0063】

上記課題を解決するための第29の発明は、上記第28の発明において、

前記推定ステップは、

IPチェックサム値に基づいて、前記制御用のメッセージのデータ部の送信元IPアドレスを変更した装置に関する情報を推定するステップと、

UDPチェックサム値またはTCPチェックサム値に基づいて前記制御用のメッセージのデータ部の送信元ポート番号、若しくはIPアドレスを変更した装置に関する情報を推定するステップと

を有することを特徴とする。 30

【0064】

上記課題を解決するための第30の発明は、上記第28又は第29の発明において、

前記推定ステップは、

ネットワークの経路調査試験を実行する経路調査実行ステップと、

前記実行結果を加味して装置に関する情報を推定する詳細情報推定ステップとを有することを特徴とする。

【0065】

上記課題を解決するための第31の発明は、上記第30の発明において、

前記経路調査実行ステップは、通過できる装置の個数を示す情報の数値が互いに異なる複数の情報収集用のパケットを送信するステップであることを特徴とする。 40

【0066】

上記課題を解決するための第32の発明は、上記第30又は上記第31の発明において、

、

前記経路調査実行ステップは、以前推定された装置までに通過する装置の個数を調査するステップであることを特徴とする。

【0067】

上記課題を解決するための第33の発明は、上記第30から第32のいずれかの発明において、

前記経路調査実行ステップは、プライベートIPアドレスとグローバルIPアドレスとが切り替わる位置に設置されている装置までに通過した装置の個数を調査するステップである 50

ことを特徴とする。

【0068】

上記課題を解決するための第34の発明は、上記第22から第33のいずれかの発明において、

前記推定ステップは、推定結果を前記ネットワーク上の端末に通知するステップを有することを特徴とする。

【0069】

上記課題を解決するための第35の発明は、上記第34の発明において、

前記推定ステップは、前記ネットワーク上の他の端末から推定結果を受け取ると、その推定結果を記憶するステップを有することを特徴とする。

10

【0070】

上記課題を解決するための第36の発明は、上記第34又は第35の発明において、

前記推定ステップは、複数の推定結果に基づいて前記ネットワーク上のコンピュータのポート番号の割り当て処理の規則性を推定するステップであることを特徴とする。

【0071】

上記課題を解決するための第37の発明は、上記第34から第36のいずれかの発明において、

前記推定ステップは、前記推定結果をメールまたは電話を用いて通信相手である端末に通知する推定ステップを有することを特徴とする。

【0072】

上記課題を解決するための第38の発明は、上記第22から第37のいずれかの発明において、

前記推定ステップは、前記情報収集用のパケットが通過できる装置の個数を示す情報を、前記推定結果に基づいて取得した宛先に届かない値に設定して、この宛先にSYNパケットを送信し、このSYNパケットのシーケンス番号を前記宛先に通知するステップを有することを特徴とする。

20

【0073】

上記課題を解決するための第39の発明は、上記第38の発明において、

前記推定ステップは、

前記送信されたSYNパケットのシーケンス番号を受け取る受取ステップと、

前記受け取ったシーケンス番号を考慮した応答確認パケットを送信するステップとを有することを特徴とする。

30

【0074】

上記課題を解決するための第40の発明は、

ネットワーク上の装置に関する情報を推定する推定システムのプログラムであって、前記プログラムは前記システムを、

送信されて来た情報収集用のパケットに応答して制御用のメッセージを返信する返信手段と、

前記返信手段からの制御用のメッセージに基づいて、前記ネットワーク上の装置に関する情報を推定する推定手段と

して機能させることを特徴とする。

40

【0075】

上記課題を解決するための第41の発明は、

端末のプログラムであって、前記プログラムは前記端末を、

受信したメッセージが情報収集用のパケットに応答して返信された制御用のメッセージであるかを判断する判断手段と、

前記判断の結果、受信したメッセージが前記情報収集用のパケットに応答して返信された制御用のメッセージであると判断された場合、この制御用のメッセージに基づいて、前記ネットワーク上の装置に関する情報を推定する推定手段

として機能させることを特徴とする。

50

【0076】

上記課題を解決するための第42の発明は、

ネットワーク上の装置に関する情報を推定するシステムのプログラムであって、前記プログラムは前記システムを、

通信用のプロトコルで定められているエラーメッセージ又は制御メッセージを用いて前記ネットワーク上の装置に関する情報を推定する手段として機能させることを特徴とする。

本発明の第1の推定システムは、ネットワーク上のPCの待ち受け状態となっていないポート番号宛にパケットを送信するパケット送信部と、ネットワーク上のPCから送り返されてきたICMPポート到達不能メッセージを受信するパケット受信部と、受信したICMPポート到達不能メッセージのチェックサムからネットワークで行われたヘッダ変換を検出する解析部とを有する。本発明の第1の推定システムは、このような構成を採用し、ネットワーク上のPCから送り返されてきたICMPポート到達不能メッセージのチェックサムを元にして、ヘッダ変換を推定することにより、専用サーバを設置することなく、NATルータによるヘッダ変換の内容を把握することができる。以上の理由により、本発明の目的を達成することができる。

【0077】

本発明の第2の推定システムは、本発明の第1の推定システムの解析部において実行する処理を変更している。そして、本発明の第2の推定システムの解析部は、本発明の第1の推定システムの解析部の処理に加えて、ネットワークの経路調査試験を行い、ヘッダ変換の推定精度を高めている。本発明の第2の推定システムは、このような構成を採用し、ネットワークの経路調査試験の結果を加味して、ヘッダ変換を推定することにより、本発明の第1の推定システムで完全に絞り込めていない場合でも、ヘッダ変換の内容を正確に把握することができる。以上の理由により、本発明の目的を達成することができる。

【0078】

本発明の第3の推定システムは、本発明の第1の推定システムの解析部、パケット送信部、およびパケット受信部において実行する処理を変更している。本発明の第3の推定システムは、ネットワーク上のPC宛にTTLの値を小さく設定したパケットを送信するパケット送信部と、ネットワーク上のルータから送り返されてきたICMP Time Exceededメッセージを受信するパケット受信部と、受信したICMP Time Exceededメッセージのチェックサムからネットワークで行われたヘッダ変換を検出する解析部とを有する。本発明の第3の推定システムは、このような構成を採用し、ネットワーク上のルータから送り返されてくるICMP Time Exceededメッセージのチェックサムを元にして、ヘッダ変換を推定することにより、ICMPポート到達不能メッセージがネットワーク内で破棄されてしまった場合でも、専用サーバを設置することなく、NATルータによるヘッダ変換の内容を把握することができる。以上の理由により、本発明の目的を達成することができる。

【0079】

本発明の第4の推定システムは、本発明の第3の推定システムの解析部、パケット送信部、およびパケット受信部において実行する処理を変更している。本発明の第4の推定システムは、ネットワーク上のPC宛にTTLの値を小さく設定したパケットを送信するパケット送信部と、ネットワーク上のルータから送り返されてきたICMP Time Exceededメッセージを受信するパケット受信部と、受信したICMP Time Exceededメッセージのチェックサムからネットワークで行われたヘッダ変換を検出する解析部とを有する。本発明の第4の推定システムは、このような構成を採用し、NATルータにおいて、ICMP Time ExceededメッセージのIPチェックサムが正しい値に変換されてしまう場合でも、専用サーバを設置することなく、ICMP Time ExceededメッセージのUDPチェックサムを元にして、NATルータによるヘッダ変換の内容を把握することができる。以上の理由により、本発明の目的を達成することができる。

【0080】

本発明の第5の推定システムは、本発明の第3の推定システムの解析部、パケット送信

部、およびパケット受信部において実行する処理を変更するとともに、アプリケーション部を含んでいる。本発明の第5の推定システムは、ネットワーク上のPC宛にTTLの値を小さく設定したパケットを送信するパケット送信部と、ネットワーク上のルータから送り返されてきたICMP Time Exceededメッセージを受信するパケット受信部と、受信したICMP Time Exceededメッセージのチェックサムからネットワークで行われたヘッダ変換を検出するとともに、その検出結果を通信相手となるPCに通知する解析部と、通信相手となるPCとパケットのやり取りを行うアプリケーション部とを有する。本発明の第5の推定システムは、このような構成を採用し、お互いのPCがNATルータの配下に設置されている場合でも、ICMP Time ExceededメッセージのチェックサムからNATルータによるヘッダ変換の内容を把握するとともに、PC間でその情報を通知しあうことにより、専用サーバを設置することなく、PC間でパケットをやり取りするために必要な情報を把握することができる。以上の理由により、本発明の目的を達成することができる。

10

【0081】

本発明の第6の推定システムは、本発明の第3の推定システムの解析部において実行する処理を変更している。本発明の第6の推定システムの解析部は

受信したICMP Time Exceededメッセージからネットワークで行われたToSフィールドの変化を検出している。本発明の第6の推定システムは、このような構成を採用し、ネットワーク上のルータから送り返されてくるICMP Time Exceededメッセージを元にして、ToSフィールドの変化を推定することにより、専用サーバを設置することなく、ネットワーク内で優先制御機能が働いているかどうかを把握できる。以上の理由により、本発明の目的を達成することができる。

20

【0082】

本発明の第7の推定システムは、本発明の第3の推定システムの解析部において実行する処理を変更している。本発明の第7の推定システムは、受信したICMP Time Exceededメッセージからネットワークで行われたフラグメントフィールドの変化を検出している。本発明の第7の推定システムは、このような構成を採用し、ネットワーク上のルータから送り返されてくるICMP Time Exceededメッセージを元にして、フラグメントフィールドの変化を推定することにより、専用サーバを設置することなく、ネットワーク内でフラグメントが発生したかどうかを把握できる。以上の理由により、本発明の目的を達成することができる。

30

【0083】

本発明の第8の推定システムは、本発明の第5の推定システムの解析部、パケット送信部、パケット受信部において実行する処理を変更するとともに、TCP部4008を追加している。本発明の第8の推定システムは、このような構成を採用し、通信相手と3way handshake処理を行うことにより、専用サーバを設置することなく、PC間でTCPパケットをやり取りするのに必要な情報を把握することができる。以上の理由により、本発明の目的を達成することができる。

【発明の効果】

【0084】

本発明によると、専用サーバをインターネット上に設置することなく、既存の標準的な通信プロトコルでICMPを巧みに利用することにより、ICMPヘッダのチェックサムの値から、ネットワーク内におけるヘッダ変換を推定できるので、本発明の目的を達成することができる。

40

【0085】

このため、専用サーバの保守/運用コストが不要になるとともに、専用サーバが外部の不正なユーザから攻撃されるといったこともないので安全である。さらに、LANのPCの数が増加した場合でも、各PCごとにUDPパケットの宛先を変えれば、ICMPパケットを送り返すPC405の負荷も大きくならないので、スケーラビリティの面でも優れている。

【0086】

50

本発明の上述の特徴と優位点を得ることができる形態を説明するために、以下において、図面を参照して具体的な実施例を述べるものとする。しかしながら、これらの図面および説明は、本発明の典型的な実施形態のみを示しており、その範囲を限定するものではないことを理解すれば、本発明は、以下に添付する図面を用いて、さらに明確および詳細に記載され、説明されるであろう。

【発明を実施するための最良の形態】

【0087】

本発明を実施するための第1の実施の形態について図面を参照して詳細に説明する。

【0088】

<構成>

図4を参照すると、本発明の第1の実施の形態は、インターネットのようなネットワーク404と、アドレス変換を行うNATルータ402、NATルータ406と、ユーザが操作するPC401、PC407と、インターネット上に設置されている任意のPC405と、パケットの経路制御を行うルータ403とを含む。

【0089】

また、ネットワーク4は、パケットの経路制御を行うルータ408～411を含む。

【0090】

ここで、PC405には非特許文献1に記載の専用サーバ312のような特別な機能は搭載されておらず、PC405は標準的な任意の端末であるとする。

【0091】

PC401の内部構成を図5に示す。

【0092】

図5に示されるように、PC401は、解析部506と、パケット受信部504と、パケット送信部505と、オペレーティングシステム500とを含んでいる。ここで、オペレーティングシステム500は、UDP部503と、IP部502と、MAC部501とを含んでいる。

【0093】

解析部506は、ネットワーク内で行われたヘッダ変換の内容を検出するために必要な情報を収集するためのUDPパケットを、設定されたIPアドレス及びポート番号宛に送信するようにパケット送信部505に命令する。また、解析部506は、パケット受信部504から渡されるICMPパケットのヘッダ情報から、ネットワーク内で行われたヘッダ変換の内容を検出する。尚、UDPパケットはダミーパケットであってもよい。

【0094】

パケット送信部505は、解析部506からUDPパケットの送信命令を受け取ると、解析部506によって指定された宛先に向けてUDPパケットの送信処理を行うために、データをUDP部503に渡す。

【0095】

パケット受信部504は、IP部502からICMPパケットを受け取り、そのデータを解析部504に渡す。

【0096】

UDP部503は、パケット送信部505から渡されたデータにUDPヘッダを追加した後、IP部502に渡す。

【0097】

IP部502は、UDP部503から渡されたデータにIPヘッダを追加した後、MAC部501に渡す。

【0098】

また、IP部502は、MAC部501からデータを受け取ると、そのデータがUDPパケットに回答して送信されたICMPパケットのデータ部分であるかを判断し、判断の結果、UDPパケットに回答して送信されたICMPパケットである場合には、パケット受信部504に渡す。

10

20

30

40

50

【0099】

MAC部501は、IP部502から渡されたデータにMACヘッダを追加した後、伝送路に送信する。また、MAC部501は、伝送路からデータを受け取ると、MACヘッダを外した後、IP部502に渡す。

【0100】

ここで、UDP部503、IP部502、およびMAC部501には、オペレーティングシステム500が標準的に搭載しているTCP/IP機能を流用するのが一般的である。

【0101】

<動作>

続いて、図4～図18を参照しながら、本発明を実施するための実施の形態の動作について詳細に説明する。 10

【0102】

まず、図5の解析部506は、何らかのタイミングを契機に、UDPパケットを送信する（図6のステップS602）。

【0103】

このUDPパケットを送信するタイミングとしては、下記のうちのいずれか、および組み合わせが考えられる。

【0104】

- ・ ユーザインターフェースや他のアプリケーションから命令された時
- ・ 解析部のサービス起動時
- ・ PCの電源投入時
- ・ 一定の時間間隔毎
- ・ PCのIPアドレスの更新時

ただし、前述の送信タイミングは単なる例であることが理解されるべきである。本説明を再検討すれば、送信タイミングとして多種多様なものが存在することは、本技術分野の当業者にとって明らかであろう。

【0105】

また、UDPパケットの宛先としては、下記のうちのいずれか、および組み合わせが考えられる。

【0106】

- ・ ユーザインターフェースや他のアプリケーションから指定された、IPアドレスとポート番号に向けて送信する
- ・ 設定ファイルなどに予め設定されているIPアドレスとポート番号に向けて送信する
- ・ ランダムに選んだIPアドレスとポート番号に向けて送信する

ただし、前述のパケットの宛先は単なる例であることが理解されるべきである。本説明を再検討すれば、パケットの宛先として多種多様なものが存在することは、本技術分野の当業者にとって明らかであろう。

【0107】

以下の動作説明では、解析部506のサービス起動時に、PC401からUDPパケットを予め設定ファイルに登録されているIPアドレス及びポート番号に向けて送信する方法を採用した場合を例に説明する。 40

【0108】

ここで、設定ファイルには、IPアドレスとして図4のPC405の200.20.1.1、ポート番号として9999が登録されているものとする。このポート番号9999は、PC405で待ち受け状態になっていないポート番号であるとする。このようなポート番号を宛先に設定している理由は、PC405からICMPポート到達不能メッセージを返してもらうためである。

【0109】

図5の解析部506は、パケット送信部505に上記のIPアドレスとポート番号を通知し、ネットワーク内で行われたヘッダ変換の内容を検出するためのパケットであるUD 50

Pパケットの送信を依頼する（図6のステップS603）。

【0110】

パケット送信部505は、解析部506からUDPパケットの送信依頼を受けると（図7のステップS701）、指定されたIPアドレスとポート番号宛のUDPソケットをオープンし、UDP部503にデータを渡す（図7のステップS702）。

【0111】

UDP部503は、パケット送信部505からデータ送信の依頼を受けると（図8のステップS801）、データにUDPヘッダを付加してUDPパケットを生成し（図8のステップS802）、IP部502に転送する（図8のステップS803）。

【0112】

IP部502は、UDP部503からUDPパケットを受け取ると、IPパケットを付加してIPパケットを生成し、MAC部501に転送する（図9のステップS903）。

【0113】

MAC部501は、IP部502からIPパケットを受け取ると（図10のステップS1001）、MACヘッダを付加してMACフレームを生成し（図10のステップS1002）、伝送路に送信する（図10のステップS1003）。

【0114】

図11（a）には、上記の処理により、PC401から送信されるパケットを示している。

【0115】

このように送信されたデータは、まず、図4のNATルータ402において、送信元IPアドレスと送信元ポート番号が変換される。この例では、送信元IPアドレスが192.168.0.2から200.10.1.1へ、送信元ポート番号が65000から65001に変更される。また、これらの変更に伴い、IPヘッダのチェックサムとUDPヘッダのチェックサムも再計算される。この例では、IPヘッダのチェックサムが0x10から0x20に、UDPヘッダのチェックサムが0x100から0x200に変更されたとする。

【0116】

図11（b）には、上記の処理により、NATルータ402から送信されるパケットを示している。

【0117】

このように変更されたパケットは、幾つものルータを経由しながら、PC405に届けられる。説明を簡単にするために、この例では、NATルータ以外の通信装置はヘッダを変換しないものとする。

【0118】

PC405は、このパケットを受信するが、宛先ポート番号である9999は待ち受け状態になっていない。このため、パケットの送信元であるNATルータ402に、ICMPポート到達不能メッセージを送り返す。

【0119】

このICMPポート到達不能メッセージは、図11（c）のように、ICMPパケットとして送られるが、ICMPパケットのデータ部には、先程受信した図11（b）のパケットがそのまま付加される。

【0120】

図11（c）には、上記の処理により、PC405から送信されるパケットを示している。

【0121】

NATルータ402は、このICMPパケットを受信すると、ICMPパケットをPC401に転送するために、そのIPヘッダの宛先IPアドレスを200.10.1.1から192.168.0.2に変更する。また、この変更に伴い、IPヘッダのチェックサムも再計算し、0x30から0x40に変更している。

【0122】

10

20

30

40

50

また、N A T ルータ 4 0 2 は、I C M P ヘッダのデータ部も変更する。具体的には、送信元 I P アドレスを 2 0 0 . 1 0 . 1 . 1 から 1 9 2 . 1 6 8 . 0 . 2 へ、送信元ポート番号を 6 5 0 0 1 から 6 5 0 0 0 に変更する。このように I C M P ヘッダのデータ部も変更してやることにより、あくまで P C 4 0 1 への I C M P ポート到達不能メッセージであるかのように見せかけることができる。

【0 1 2 3】

ここで、N A T ルータ 4 0 2 では、図 1 1 (d) に示されるように、I C M P ヘッダのデータ部のチェックサムまでは変更されないため、チェックサムは誤った値となっている。

【0 1 2 4】

P C 4 0 1 は、この I C M P パケットを N A T ルータ 4 0 2 から受け取ると (図 1 2 のステップ S 1 2 0 1)、まず M A C 部 5 0 1 で M A C ヘッダを外した後 (図 1 2 のステップ S 1 2 0 2)、I P 部 5 0 2 に転送する (図 1 2 のステップ S 1 2 0 3)。

【0 1 2 5】

I P 部 5 0 2 は、M A C 部 5 0 1 から I C M P パケットを受け取ると (図 1 3 のステップ S 1 3 0 1)、I P ヘッダを外した後 (図 1 3 のステップ S 1 3 0 2)、そのデータが U D P パケットに応答して送信された I C M P パケットのデータ部分であるかを判断する。判断の結果、U D P パケットに応答して送信された I C M P パケットである場合には、パケット受信部 5 0 4 に転送する (図 1 3 のステップ S 1 3 0 3)。

【0 1 2 6】

パケット受信部 5 0 4 は、I P 部 5 0 2 から I C M P データを受け取ると (図 1 4 のステップ S 1 4 0 1)、その I C M P ヘッダのデータ部を解析部 5 0 6 に転送する (図 1 4 のステップ S 1 4 0 2)。

【0 1 2 7】

解析部 5 0 6 は、パケット受信部 5 0 4 からデータ部を受け取ると (図 1 5 のステップ S 1 5 0 1)、そのチェックサムの状態から、ネットワークでヘッダ変換が行われたのかどうか検出する。以下において、その方法について述べる。

【0 1 2 8】

まず、解析部 5 0 6 では、受け取ったデータの I P ヘッダから、I P チェックサムを計算する (図 1 5 のステップ S 1 5 0 2)。

【0 1 2 9】

続いて、この計算された I P チェックサムが、受け取ったデータの I P チェックサムと一致するかどうか確認する (図 1 5 のステップ S 1 5 0 3)。

【0 1 3 0】

ここで、N A T ルータ 4 0 2 において I P アドレスの変換が行われた場合には、I P チェックサムが一致しないので、I P アドレス変換の発生を検出することができる。

【0 1 3 1】

一致しなかった場合には、I P アドレスの変換が起こったと考え、N A T ルータ 4 0 2 の I P アドレスを推定するために、図 1 5 のステップ S 1 5 0 4 に進む。

【0 1 3 2】

一致した場合には、I P アドレスの変換が起こらなかったものとして、ステップ S 1 5 0 5 に進み、受け取ったデータの U D P ヘッダから、U D P チェックサムを計算する。

【0 1 3 3】

そして、この計算された U D P チェックサムが、受け取ったデータの U D P チェックサムと一致するかどうかを確認する (図 1 5 のステップ S 1 5 0 6)。

【0 1 3 4】

ここで、N A T ルータ 4 0 2 においてポート番号の変換が行われた場合には、U D P チェックサムが一致しないので、ポート番号変換の発生を検出することができる。

【0 1 3 5】

一致しなかった場合には、ポート番号の変換が起こったと考え、N A T ルータ 4 0 2 の

10

20

30

40

50

ポート番号を推定するために、図15のステップS1507に進む。

【0136】

一致した場合には、ポート番号の変換が起らなかったものとして、処理を終了する。

【0137】

以下では、IPチェックサムとUDPチェックサムの両方が誤っている場合の推定処理について説明する。

【0138】

図16には、図15のステップS1504で実行されるIPアドレスの推定処理を示している。

【0139】

IPアドレスは32ビットで構成されるが、解析部506では、まずIPアドレスの上位16ビットをXとし、下位16ビットがYであると仮定する。送信元IPアドレスをこのように仮定して、受け取ったデータのIPチェックサムの方程式を立てる（図16のステップS1602）。

【0140】

ここでIPチェックサムの計算方法について補足すると、IPチェックサムは、IPヘッダを16ビットごとに分割して、それぞれの「1の補数」の総和を求めた後、その総和の「1の補数」がIPチェックサムとなる。

【0141】

解析部506では、IPアドレスを推定するために、ステップS1602で求められた方程式を満足するXとYを総当り計算する（図16のステップS1604～ステップS1607）。

【0142】

この方程式を満足するIPアドレスには、NATのIPアドレスと一致するものが存在するが、上記方程式を満足するXとYの組み合わせは32768通り存在する。第1の実施の形態では、これらの組み合わせ候補を絞り込む方法については言及しない。

【0143】

一方、図17には、図15のステップS1507で実行されるポート番号の推定処理を示している。

【0144】

ポート番号は16ビットで構成されるが、解析部506では、答えとなるポート番号がWであると仮定する。送信元ポート番号をこのように仮定して、受け取ったデータのUDPチェックサムの方程式を立てる（図17のステップS1702）。

【0145】

ここでUDPチェックサムの計算方法について補足すると、UDPチェックサムは、「UDPヘッダ」と「ペイロードデータ」、そして図18に示される「UDP擬似ヘッダ」の3つの部分が計算の対象となる。

【0146】

ここで、「UDP擬似ヘッダ」とは、チェックサムの計算時だけに使われる仮想的なヘッダであり、実際のUDPパケット中には含まれていない。UDPチェックサムは、この「UDP擬似ヘッダ」を含んだヘッダ全体を16ビットごとに分割して、それぞれの「1の補数」の総和を求めた後、その総和の「1の補数」がUDPチェックサムとなる。

【0147】

解析部506では、ポート番号を推定するために、ステップS1702で求められた方程式を満足するWを計算する（図17のステップS1703）。ここで、擬似ヘッダ中の送信元IPアドレスには、上述の図16の処理によって求められたIPアドレスが代入されることになる。

【0148】

この方程式を満足するポート番号には、NATのポート番号と一致するものが存在する。

10

20

30

40

50

【0149】

以上の処理により、ICMPヘッダのチェックサムから、NATの送信元IPアドレスとポート番号を推定できることが示された。

【0150】

尚、上記実施の形態では、待ち受け状態になっていないポート番号を宛先に設定してパケットを送信し、ICMPポート到達不能メッセージ（エラーメッセージ）を返してもらう構成について説明したが、この限りではない。即ち、PC401がPC405宛にパケットを送信し、PC401がこのパケットに応答して制御メッセージをPC401に返信する構成であればよい。また、本明細書では、エラー（到達不能）メッセージや制御メッセージ等のように、通信のプロトコルで定められている通信の手続上のメッセージ（パケット）を総称して制御用のメッセージ（パケット）とする。 10

【0151】

<効果>

続いて、本発明を実施するための第1の実施の形態の効果について説明する。

【0152】

本発明を実施するための第1の実施の形態では、専用サーバをインターネット上に設置することなく、既存の標準的な通信プロトコルでICMPを巧みに利用することにより、ICMPヘッダのチェックサムの値から、ネットワーク内におけるヘッダ変換を推定できるので、本発明の目的を達成することができる。

【0153】

このため、専用サーバの保守/運用コストが不要になるとともに、専用サーバが外部の不正なユーザから攻撃されるといったこともないので安全である。さらに、LANのPCの数が増加した場合でも、各PCにUDPパケットの宛先を変えれば、ICMPパケットを送り返すPC405の負荷も大きくならないので、スケーラビリティの面でも優れている。 20

【0154】

次に、本発明を実施するための第2の実施の形態について図面を参照して詳細に説明する。

【0155】

<構成>

本発明の第1の実施の形態では、ICMPポート到達不能メッセージのチェックサムから、NATルータのIPアドレスとポート番号を推定していた。しかしながら、IPチェックサムとIPアドレスの情報量に差が存在するため、IPチェックサムからIPアドレスを推定しようとしても、IPアドレスを一意に絞り込むことができない可能性がある。 30

【0156】

この理由は、IPチェックサムが16ビット、つまり32768通りの組み合わせしか持たないのに対して、IPアドレスは32ビット、つまり32768×32768通りものの組み合わせを持っており、同じIPチェックサムを計算結果とするIPアドレスが32768通りも存在してしまうからである。

【0157】

以上のことから、本発明の第1の実施の形態では、チェックサムからNATルータのIPアドレスとポート番号を絞り込むことができず、推定精度が悪かった。 40

【0158】

本発明の第2の実施の形態では、図5の解析部506とパケット送信部505、およびパケット受信部504で実行する処理を変更する。本発明の第2の実施の形態の構成を図19に示す。

【0159】

解析部1906は、図5の解析部506の処理に加えて、IPアドレスの推定精度を高めるために、ネットワークの経路調査用パケットを送信するようにパケット送信部1905に命令する。また、解析部1906は、パケット受信部1904から渡されるネットワ 50

ークの経路調査結果から、IPアドレスの絞込み処理を行う。

【0160】

パケット送信部1905は、図5のパケット送信部505の処理に加えて、解析部1906から経路調査用パケットの送信命令を受け取ると、経路調査用パケットを送信する。ここで行う経路調査方法は、あるPCから別のPCまでの経路上にどのようなルータが位置しているかを調べることである。

【0161】

パケット受信部1904は、図5のパケット受信部504の処理に加えて、経路調査結果をネットワークから受け取ると、その結果を解析部1906に渡す。

【0162】

その他の構成は、第1の実施の形態の図5と同じであるため、説明を省略する。

【0163】

<動作>

続いて、図19を参照して本発明を実施するための第2の実施の形態の動作について詳細に説明する。

【0164】

まず、本発明の第1の実施の形態と同じ処理を実行することにより、NATルータのIPアドレスとポート番号とを推定する。ただし、この時点では、上述したように、まだIPアドレスとポート番号を一意に値に絞り込めておらず、32768通りの組み合わせが存在する。

【0165】

続いて、解析部1906は、ネットワークの経路調査試験を行う。この経路調査試験では、経路上に存在する各ルータを割り出すために、IPパケットにおけるTTL (Time To Live) の仕組みを利用する。TTLとは、IPパケットヘッダに指定可能な「生存時間」である。ただし、実際には時間ではなく、「ホップ数」を意味している。つまり、そのパケットが「生存」できるホップ数を指定するのがTTLである。

【0166】

TTLには最大255が設定可能で、ルータをホップするごとに必ずTTLが1ずつ減らされる。そして、TTLが0に達するとパケットがルータで破棄されるとともに、パケットを破棄したルータはICMP Time Exceededエラーを送信元PCに送り返す。このICMP Time Exceededエラーには、破棄したルータのIPアドレスが含まれる。送信元PCはこのICMP Time Exceededエラーを受け取ること、その送信元IPアドレスから、破棄したルータのIPアドレスを検出することができる。

【0167】

上記のネットワークの経路調査試験では、TTLを1から順に増やしながら試行を重ねることにより、経路上に存在する各ルータの情報を得ている。例えば、PC401から、まず最初にTTLを1としたIPパケットをPC405に送出すると、1番目のNATルータ402 (1ホップ目) が受け取った時点でTTLを減算した結果、0となってしまうので、NATルータ402からICMP Time Exceededエラーが送り返される。これが1台目のルータの結果となる。ただし、ここで得られるIPアドレスは、NATルータ402の内側 (LAN側) IPアドレス (192.168.0.1) である。次にTTLを2にして送出すれば、2台目のルータ403のIPアドレス (200.10.1.2) が得られる。

【0168】

上記の処理を実行するために、解析部1906は、まず、設定ファイルに登録されている宛先IPアドレスを取得し (図20のステップS2001)、PC405のIPアドレスとTTL値1をパケット送信部1905に通知する (図20のステップS2003)。

【0169】

パケット送信部1905は、解析部1906から宛先IPアドレスを受け取り (図21のステップS2101)、この受け取った宛先IPアドレスとTTL値から、ICMP Echoリクエストパケットを生成し、MAC部1901に渡す (図21のステップS2102)。

10

20

30

40

50

【0170】

MAC部1901は、パケット送信部1905からICMP Echoリクエストパケットを受け取ると（図22のステップS2201）、MACヘッダを追加し（図22のステップS2202）、ネットワークに転送する（図22のステップS2203）。

【0171】

ネットワークに送出されたパケットは、各ルータにおいてTTLが1ずつ減算されていき、TTLが0となった時点でルータからICMP Time ExceededパケットがPC401に返される。

【0172】

MAC部1901は、ネットワークからICMP Time Exceededパケットを受け取ると（図23のステップS2301）、MACヘッダを削除し（図23のステップS2302）、パケット受信部1904に転送する（図23のステップS2303）。

【0173】

パケット受信部1904は、MAC部1901からICMP Time Exceededパケットを受け取ると（図24のステップS2401）、パケットの送信元IPアドレスGを解析部1906に通知する（図24のステップS2402）。

【0174】

解析部1906は、パケット受信部1904からIPアドレスGを受け取ると（図25のステップS2501）、そのIPアドレスGがグローバルIPアドレスとなっているかどうかをチェックする（図25のステップS2502）。ここで、IPアドレスGがグローバルIPアドレスとなっていない場合には、次ホップのルータのIPアドレスを取得することを試みる。具体的な処理としては、PC405のIPアドレスとTTL値2をパケット送信部1905に通知する（図25のステップS2504）。

【0175】

一方、上述の図25のステップS2502において、受け取ったIPアドレスGがグローバルIPアドレスとなっている場合には、このときのTTL値（ここではXとする）とIPアドレスGを記憶する。

【0176】

そして、解析部1906は、まずこのIPアドレスGを元にして、第1の実施の形態で推定されたIPアドレスの絞込みを行う。

【0177】

絞込み方法としては、図16のステップS1606で求められたIPアドレスのうち、IPアドレスGと近いものを抽出し、この抽出されたIPアドレスをNATルータのIPアドレスであると推定する（図25のステップS2507）。

【0178】

この絞込み方法の正当性を以下に述べる。

【0179】

解析部1906では、上記のネットワークの経路情報の取得処理により、ルータ403のIPアドレスG（200.10.1.2）を検出できる。ここで、ルータ403はNATルータ402と同じサブネットワークに入っているため、サブネットマスクで決められたネットワークアドレスは、ルータ403とNATルータ402は同じ値となっている。例えば、図4の例では、ルータ403のIPアドレスとNATルータ402のIPアドレスは、200.10.1.までは同じ値となっている。

【0180】

解析部1906では、この特徴を利用し、本発明の第1の実施の形態において推定されたIPアドレスのうち、ルータ403のIPアドレスG（200.10.1.2）と近いものを検索することにより、NATルータ402のIPアドレスとして確からしいものを選択することができる。

【0181】

ただし、このとき、ルータ403のIPアドレスG（200.10.1.2）を検出で

10

20

30

40

50

きても、そのサブネットマスクが何ビットであるかまでは検出できない。このため、サブネットマスクを想定する必要があるが、サブネットマスクの想定値によって、本発明の第1の実施の形態において推定されたIPアドレスのうち、ルータ403のIPアドレスG(200.10.1.2)と近いと判定されるものが複数でてきてしまう。

【0182】

たとえば、サブネットマスクを8ビットと想定した場合、本発明の第1の実施の形態において推定されたIPアドレスのうち、ルータ403のIPアドレスG(200.10.1.2)と近いと判定されるものは、256通りほど出てくる可能性がある。

【0183】

また、サブネットマスクを16ビットと想定した場合には、本発明の第1の実施の形態において推定されたIPアドレスのうち、ルータ403のIPアドレスG(200.10.1.2)と近いと判定されるものは、1つに絞りこめる。

【0184】

このように、IPアドレスを絞り込めるか否かは、サブネットマスクの想定値に依存する。

【0185】

以下では、サブネットマスクを8ビットと想定した場合の、さらなる絞り込み方式について述べる。

【0186】

ここで、サブネットマスクを8ビットとしているのは、サブネットマスクは8ビット以下に設定されることがなく、このような想定を行うことにより、本絞り込み方式をあらゆるネットワークに適用できるためである。

【0187】

上述したように、サブネットマスクを8ビットと想定すると、本発明の第1の実施の形態において推定されたIPアドレスは256通り程度に絞り込める。

【0188】

このように絞り込まれたIPアドレスを、さらに絞り込んで一意に特定するために、解析部1906は以下のような処理を行う。

【0189】

解析部1906では、まず、上記のように256通りに絞り込まれた各IPアドレスに対して、そのIPアドレスを持つ端末に到達するのに必要なホップ数を調査する。

【0190】

ここで、端末までのホップ数は、LinuxやWindows(登録商標)などのOSに標準的に搭載されているtraceroute(tracert)などのコマンドを使って調べることができる。

【0191】

次に、プライベートIPアドレスとグローバルIPアドレスが切り替わるルータまでのホップ数を調査する。

【0192】

このルータまでのホップ数の調査方法としては、PC405のようなグローバルIPアドレスをもつ端末に向けてtraceroute(tracert)コマンドを使用して、PC401とPC405の間のルータを調査することによって調査することができる。

例えば、PC401からPC405に向けて、traceroute(tracert)コマンドを使用した場合、以下のような結果が返される。

ホップ数	端末
1	NATルータ402(192.168.0.1)
2	ルータ403(200.10.1.2)
3	ルータ408
4	ルータ411
5	ルータ410
6	PC405(200.20.1.1)

この場合、ホップ数1と2の間で、端末のIPアドレスがプライベートIPアドレスからグローバルIPアドレスに切り替わっている。この結果から、プライベートIPアドレスとグローバルIPアドレスが切り替わるルータまでのホップ数は1であると判定する。

【0193】

解析部1906では、256通りに絞り込まれた各IPアドレスを一意に絞り込むために、上述のルータまでのホップ数を用いる。具体的には、256通りに絞り込まれた各IPアドレスのうち、上述のルータまでのホップ数（この場合1であるが）と一致するものを検索し、そのIPアドレスをNATルータ402の外部IPアドレスと判定する。

【0194】

以上の処理により、ネットワークの経路調査結果から、NATルータのIPアドレスを絞り込めることが示された。 10

【0195】

また、このIPアドレスに対応するポート番号は一意に定まるので、ポート番号も絞り込める。

【0196】

<効果>

続いて、本発明を実施するための第2の実施の形態の効果について説明する。

本発明を実施するための第2の実施の形態では、専用サーバをインターネット上に設置することなく、ICMPヘッダのチェックサムの値とネットワークの経路調査結果からヘッダ変換を推定することにより、ヘッダ変換の内容を高精度に検出できるので、本発明の 20
目的を達成することができる。

【0197】

次に、本発明を実施するための第3の実施の形態について図面を参照して詳細に説明する。

【0198】

<構成>

本発明の第1および第2の実施の形態では、PC405から送り返されるICMPポート到達不能メッセージのチェックサムを元にして、NATルータのIPアドレスとポート番号を推定していた。しかしながら、ICMPポート到達不能メッセージは特殊なパケットであるので、NATルータによっては破棄してしまう可能性がある。 30

【0199】

このように、NATルータにおいてICMPポート到達不能メッセージが破棄されてしまった場合、第1および第2の実施の形態では、ヘッダ変換の有無を検出することはできない。

【0200】

以上のことから、本発明の第1および第2の実施の形態では、NATルータの種類によっては、ヘッダ変換の内容を推定できない可能性があり、使い勝手が悪い。

【0201】

本発明の第3の実施の形態では、上記の問題を解決するために、図5の解析部506、パケット送信部505、およびパケット受信部504で実行する処理を変更する。本発明 40
の第3の実施の形態の構成を図26に示す。

【0202】

解析部は、図5の解析部506の処理に加えて、ネットワークのヘッダ変換を検出できるNATルータの種類を増やすために、ICMPポート到達不能メッセージの代わりに、より標準的なメッセージであるICMP Time Exceededエラーを利用する。このICMP Time Exceededエラーをルータから送り返してもらうために、解析部2606は、TTLの値を小さく設定したUDPパケットを送信するようにパケット送信部2605に命令する。また、解析部2606は、パケット受信部2604から渡されるICMP Time Exceededメッセージのヘッダ情報から、ネットワーク内で行われたヘッダ変換の内容を推定する。

【0203】

パケット送信部 2605 は、解析部 2606 から U D P パケットの送信命令を受け取ると、指定された宛先に向けて U D P パケットの送信処理を行うために、データを M A C 部 2601 に渡す。

【0204】

パケット受信部 2604 は、ルータから送られてきた ICMP Time Exceeded メッセージを受信し、そのヘッダ情報を解析部 2606 に渡す。

【0205】

その他の構成は、第 2 の実施の形態の図 19 と同じであるため、説明を省略する。

【0206】

<動作>

続いて、図 26 を参照して本発明を実施するための第 3 の実施の形態の動作について詳細に説明する。

【0207】

まず、解析部 2606 は、何らかのタイミングを契機に、U D P パケットまたは T C P パケットを送信する。

【0208】

U D P パケット、または T C P パケットを送信するタイミングとしては、下記のうちのいずれか、および組み合わせが考えられる。

【0209】

- ・ ユーザーインターフェースや他のアプリケーションから命令された時
- ・ 解析部のサービス起動時
- ・ PC の電源投入時
- ・ 一定の時間間隔毎
- ・ PC の IP アドレスの更新時

ただし、前述の送信タイミングは単なる例であることが理解されるべきである。本説明を再検討すれば、送信タイミングとして多種多様なものが存在することは、本技術分野の当業者にとって明らかであろう。

【0210】

また、U D P パケット、または T C P パケットの宛先としては、下記のうちのいずれか、および組み合わせが考えられる。

【0211】

- ・ ユーザーインターフェースや他のアプリケーションから指定された、I P アドレスとポート番号に向けて送信する
- ・ 設定ファイルなどに予め設定されている I P アドレスとポート番号に向けて送信する
- ・ ランダムに選んだ I P アドレスとポート番号に向けて送信する

ただし、前述のパケットの宛先は単なる例であることが理解されるべきである。本説明を再検討すれば、パケットの宛先として多種多様なものが存在することは、本技術分野の当業者にとって明らかであろう。

【0212】

以下の動作説明では、解析部のサービス起動時に、U D P パケットを予め設定ファイルに登録されている I P アドレスとポート番号に向けて送信する方法を採用した場合を例に説明する。

【0213】

ここで、設定ファイルには、I P アドレスとして P C 4 0 5 の 2 0 0 . 2 0 . 1 . 1、ポート番号として 9 9 9 9 が登録されているものとする。

【0214】

ただし、ポート番号として 9 9 9 9 番を想定しているが、第 3 の実施の形態は、第 1 の実施の形態と異なり、I C M P ポート到達不能メッセージを送り返してもらう必要がないので、ポート番号として任意のものを選択することができることは、本技術分野の当業者にとって明らかであろう。

10

20

30

40

50

【0215】

さらに、ここで送信するUDPパケットのTTLには、2や3といった非常に小さな値が設定される。

【0216】

TTLに小さな値を設定している理由は、ネットワーク内のルータからICMP TTL Exceededメッセージを返してもらうためである。

【0217】

解析部2606は、パケット送信部2605に上記のIPアドレスとポート番号、およびTTL値を通知し、UDPパケットの送信を依頼する(図27のステップS2703)。

10

【0218】

パケット送信部2605は、解析部2606から受け取った宛先IPアドレスとポート番号、およびTTL値から、UDPベースのIPパケットを生成し、MAC部2601に渡す(図28のステップS2802)。

【0219】

MAC部2601は、パケット送信部2605からIPパケットを受け取ると、MACヘッダを付加してMACフレームを生成し、伝送路に送信する(図11(a))。

【0220】

このように送信されたデータは、まず、図4のNATルータ402において、送信元IPアドレスと送信元ポート番号が変換される。この例では、送信元IPアドレスが192.168.0.2から200.10.1.1へ、送信元ポート番号が65000から65001に変更されたとする。また、これらの変更に伴い、IPヘッダのチェックサムとUDPヘッダのチェックサムも再計算される。この例では、IPヘッダのチェックサムが0x10から0x20に、UDPヘッダのチェックサムが0x100から0x200に変更されたとする。さらに、NATルータでは、TTLを2から1に書き換える。(図11(b))

20

このように変更されたパケットは、つぎにルータ403に届けられる。ルータ403では、TTLを1から0に書き換えるが、TTLが0になったので、このパケットを破棄する。そして、ルータ403はパケットの送信元であるNATルータ402にICMP Time Exceededメッセージを送り返す。

【0221】

このICMP Time Exceededメッセージは、図11(c)のようなパケットとして送られるが、そのデータ部には先程ルータ403が受信したパケットがそのまま付加される。

30

【0222】

NATルータ402は、このICMP Time Exceededメッセージを受信すると、PC401に転送するために、そのIPヘッダの宛先IPアドレスを200.10.1.1から192.168.0.2に変更する。また、この変更に伴い、IPヘッダのチェックサムも再計算し、0x30から0x40に変更している。

【0223】

また、NATルータ402では、ICMP Time Exceededメッセージのデータ部も変更している。具体的には、送信元IPアドレスと200.10.1.1から192.168.0.2へ、送信元ポート番号を65001から65000に変更する。このようにICMPヘッダのデータ部も変更してやることにより、このICMP Time ExceededメッセージをあくまでPC401へのICMP Time Exceededメッセージであるかのようにできる。

40

【0224】

ただし、NATルータ402では、ICMPヘッダのデータ部のチェックサムまでは変更されないため、チェックサムは誤った値となっている(図11(d))。

【0225】

PC402は、このICMPパケットをNATルータ402から受け取ると、まずMAC部2601でMACヘッダを外した後、IP部2602に転送する。

【0226】

50

I P 部 2 6 0 2 は、M A C 部 2 6 0 1 から I C M P パケットを受け取ると、I P ヘッダを外した後、そのデータが U D P パケットに応答して送信された I C M P パケットのデータ部分であるかを判断する。判断の結果、U D P パケットに応答して送信された I C M P パケットである場合には、パケット受信部 2 6 0 4 に転送する。

【0 2 2 7】

パケット受信部 2 6 0 4 は、I P 部 2 6 0 2 から I C M P パケットを受け取ると、その I C M P ヘッダのデータ部を解析部 2 6 0 6 に転送する。

【0 2 2 8】

解析部 2 6 0 6 は、パケット受信部からデータ部を受け取ると、そのチェックサムの状態から、ネットワークでヘッダ変換が行われたのかどうかを検出する。

10

【0 2 2 9】

具体的には、I P アドレスの変換が行われた場合には、データ部の I P チェックサムが誤った値となるので、検出することができる。また、ポート番号の変換が行われた場合には、データ部の U D P チェックサムが誤った値となるので、同様に検出することができる。

【0 2 3 0】

解析部 2 6 0 6 は、ヘッダ変換の発生を検出すると、ヘッダの変更内容の推定処理を開始する。この解析部で行われる推定処理は、第 1 の実施の形態の解析部 5 0 6 で行われる推定処理と同じであるため、説明を省略する。

【0 2 3 1】

20

また、本発明の第 3 の実施の形態だけでは、本発明の第 1 の実施の形態と同じ理由により、I P アドレスとポート番号を一意に絞り込むことはできないが、本発明の第 2 の実施の形態と組み合わせることにより、推定精度を高めることができる。

【0 2 3 2】

以上の処理により、I C M P ポート到達不能メッセージが N A T ルータで破棄されてしまう場合でも、より標準的なメッセージである ICMP Time Exceeded エラーを利用することにより、N A T の送信元 I P アドレスとポート番号を推定できることが示された。

【0 2 3 3】

<効果>

続いて、本発明を実施するための第 3 の実施の形態の効果について説明する。

30

【0 2 3 4】

本発明を実施するための第 3 の実施の形態では、ルータから送り返されてくる ICMP Time Exceeded メッセージの情報を元にして、ネットワーク内におけるヘッダ変換を推定することにより、ICMP ポート到達不能メッセージがネットワーク内で破棄されてしまった場合でも、専用サーバをインターネット上に設置することなく、ネットワークのヘッダ変換を検出することができ、本発明の目的を達成することができる。

【0 2 3 5】

次に、本発明を実施するための第 4 の実施の形態について図面を参照して詳細に説明する。

【0 2 3 6】

40

<構成>

本発明の第 1、第 2、および第 3 の実施の形態では、図 1 1 (b) のように、N A T ルータ 4 0 2 において、I P アドレスだけでなく、ポート番号も変換されることを仮定していた。すなわち、N A T ルータ 4 0 2 において、N A P T の処理が実行されることを想定していた。また、図 1 1 (d) のように、N A T ルータ 4 0 2 において、ネットワークから送り返される I C M P パケットのチェックサムのうち、I P チェックサムと U D P チェックサムの両方が誤った値のまま転送されることを仮定していた。

【0 2 3 7】

しかしながら、N A T ルータによっては、そのヘッダ変換の動作が、図 1 1 (b) とは異なり、I P アドレスのみを変換し、ポート番号は変換しないという単純な N A T 動作であ

50

るものも多い。また、N A T ルータによっては、そのヘッダ変換の動作が、図 1 1 (d) とは異なり、ネットワークから送り返される I C M P パケットのチェックサムのうち、I P チェックサムについては正しい値に変換してから転送するものも多い。

【0238】

本発明の第 4 の実施の形態では、N A T ルータ 4 0 2 の動作として上記のように、N A T 処理を行うとともに、I P チェックサムは正しく訂正するようなものを想定し、このような状況においても、I C M P パケットのチェックサムの値から、N A T ルータの I P アドレスを推定する方法について述べる。

【0239】

本発明の第 4 の実施の形態では、上記の問題を解決するために、図 2 6 の解析部 2 6 0 6、パケット送信部 2 6 0 5、およびパケット受信部 2 6 0 4 で実行する処理を変更する。本発明の第 4 の実施の形態の構成を図 2 9 に示す。 10

【0240】

解析部 2 9 0 6 は、図 2 6 の解析部の処理に加えて、N A T ルータ 4 0 2 が N A T の動作を実行しているかどうかを確かめるために、ある宛先に向けてパケットを送信するようにパケット送信部 2 9 0 5 に命令する。また、解析部 2 9 0 6 は、パケット受信部 2 9 0 4 から渡される I C M P Time Exceeded メッセージのヘッダ情報から、ネットワーク内で行われたヘッダ変換の内容を検出する。

【0241】

パケット送信部 2 9 0 5 は、解析部 2 9 0 6 からパケットの送信命令を受け取ると、指定された宛先に向けてパケットの送信処理を行うために、データを M A C 部 2 6 0 1 に渡す。 20

【0242】

パケット受信部 2 9 0 4 は、ルータから送り返されてきた I C M P Time Exceeded メッセージを受信し、そのヘッダ情報を解析部 2 9 0 6 に渡す。

【0243】

<動作>

続いて、図 2 9 を参照して本発明を実施するための第 4 の実施の形態の動作について詳細に説明する。

【0244】

解析部 2 9 0 6 からパケットを P C 4 0 5 に向けて送信する処理は、第 3 の実施の形態と同じであるため、説明を省略する。 30

【0245】

以降の動作説明では、第 3 の実施の形態と同様に、U D P パケットを P C 4 0 1 から送信することを想定しているが、U D P パケットの代わりに T C P パケットを送信しても支障がないことは、本技術分野の当業者にとって明らかであろう。

【0246】

このように送信されたデータは、まず、図 4 の N A T ルータ 4 0 2 において、送信元 I P アドレスが変換される。この例では、図 3 0 (b) のように、送信元 I P アドレスが 1 9 2 . 1 6 8 . 0 . 2 から 2 0 0 . 1 0 . 1 . 1 に変換される。ここで、送信元ポート番号は 6 5 0 0 0 番から変更されないものとする。また、この変更に伴い、I P ヘッダのチェックサムと U D P ヘッダのチェックサムも再計算される。 40

【0247】

この例では、I P ヘッダのチェックサムが 0x10 から 0x20 に、U D P ヘッダのチェックサムが 0x100 から 0x200 に変更されたとする。さらに、N A T ルータ 4 0 2 では、T T L を 2 から 1 に書き換える。

【0248】

このように変更されたパケットは、つぎにルータ 4 0 3 に届けられる。ルータ 4 0 3 では、T T L を 1 から 0 に書き換えるが、T T L が 0 になったので、このパケットを破棄する。そして、ルータ 4 0 3 はパケットの送信元である N A T ルータ 4 0 2 に I C M P Time Ex 50

ceededメッセージを送り返す。

【0249】

このICMP Time Exceededメッセージは、図30(c)のようなパケットとして送られるが、そのデータ部には先程ルータ403が受信したパケットがそのまま付加される。

【0250】

NATルータ402は、このICMP Time Exceededメッセージを受信すると、PC401に転送するために、そのIPヘッダの宛先IPアドレスを200.10.1.1から192.168.0.2に変更する。また、この変更に伴い、IPヘッダのチェックサムも再計算し、0x30から0x40に変更している。

【0251】

また、NATルータ402では、ICMP Time Exceededメッセージのデータ部も変更している。具体的には、送信元IPアドレスと200.20.1.1から192.168.0.2に変更する。このようにICMPヘッダのデータ部も変更してやることにより、このICMP Time ExceededメッセージをあくまでPC401へのICMP Time Exceededメッセージであるかのようにできる。また、この変更に伴い、図30(d)に示されるように、ICMPヘッダのチェックサムのうち、IPチェックサムを再計算し、0x20から0x50に変更している。

【0252】

ただし、NATルータ402では、UDPチェックサムまでは変更しないため、UDPチェックサムは誤った値となっている。

【0253】

PC401は、このICMPパケットをNATルータ402から受け取ると、第3の実施の形態で述べた処理により、ICMPヘッダのデータ部が解析部2906に転送される。

【0254】

解析部2906は、パケット受信部2904からICMPヘッダのデータ部を受け取ると、そのチェックサムの状態から、ネットワークでヘッダ変換が行われたかどうかを検出する。

【0255】

ここで、データ部のIPチェックサムは正しい値となっているので、IPチェックサムから、NATルータ402でIPアドレスの変換が行われたかどうかを検出することはできない。

【0256】

しかしながら、UDPチェックサムは誤った値となっているので、NATルータ402において、IPアドレスまたはポート番号の変換が行われたことを検出することができる。

【0257】

このように、UDPチェックサムが誤っている原因がIPアドレスの変換にあると考えられる理由としては、UDPチェックサムが図18のように、IPアドレスを含む擬似ヘッダを加味した形で計算されるからである。

【0258】

よって、解析部2906では、NATルータ402でIPアドレスの変換が行われたと想定して、UDPチェックサムからNATルータ402のIPアドレスを推定する。この推定処理は、本発明の第1の実施の形態と同様であるため、説明を省略する。また、この推定処理だけでは、NATルータ402のIPアドレスを一意に絞り込むことはできないため、第2の実施の形態のように、さらにネットワークの経路調査試験を行うことにより、推定精度を上げることが望ましい。

【0259】

以上の処理により、NATルータ402において、IPチェックサムが正しい値に変換されてしまう場合でも、UDPチェックサムの値から、NATルータ402のIPアドレ

10

20

30

40

50

スを推定できることが示された。

【0260】

<効果>

続いて、本発明を実施するための第4の実施の形態の効果について説明する。

【0261】

本発明を実施するための第4の実施の形態では、NATルータにおいて、IPチェックサムが正しい値に変換されてしまう場合でも、ICMPパケットのUDPチェックサムの値からNATルータのIPアドレスを推定できるため、専用サーバをインターネット上に設置することなく、ヘッダ変換を検出するという本発明の目的を達成することができる。

【0262】

次に、本発明を実施するための第5の実施の形態について図面を参照して詳細に説明する。

【0263】

<構成>

本発明の第1から第4の実施の形態では、NATルータのIPアドレスとポート番号の推定方法について述べた。本発明の第5の実施の形態では、このようにNATルータの情報を推定するのに加えて、NATルータの配下に繋がれているPC間でパケットを送受信するのに必要な情報の推定方法について述べる。

【0264】

具体的には、図4のPC401とPC407の間でパケットをやり取りするのに必要な情報の推定方法について述べる。

【0265】

本発明の第5の実施の形態の構成を図31に示す。本発明の第5の実施の形態では、上記の問題を解決するために、図26の解析部2606、パケット送信部2605、およびパケット受信部2604で実行する処理を変更するとともに、アプリケーション部3107を含む。

【0266】

図31の解析部3106は、図26の解析部2606の処理に加えて、自ノードが繋がれているNATルータのIPアドレスとポート番号を通信相手となるPCに通知する。また、解析部3106は、通信相手となるPCから、そのPCが繋がれているNATルータのIPアドレスとポート番号を受け取り、そのIPアドレスとポート番号宛にUDPパケットを送信するようにパケット送信部3105に命令する。

【0267】

アプリケーション部3107は、通信相手となるPCにデータを送信する場合、解析部3106にデータ送信要求を発行する。また、アプリケーション部3107は、通信相手となるPCからデータを受信する場合、解析部3106からデータを受け取る。

【0268】

その他の構成は、第1から第4の実施の形態と同じであるため、説明を省略する。

【0269】

<動作>

続いて、図31を参照して本発明を実施するための第5の実施の形態の動作について詳細に説明する。

【0270】

まず、解析部3106は、何らかのタイミングを契機に、UDPパケットまたはTCPパケットを送信する。

【0271】

UDPパケット、またはTCPパケットを送信するタイミングとして、下記のうちのいずれか、および組み合わせが考えられる。

【0272】

・ユーザインターフェースや他のアプリケーションから命令された時

10

20

30

40

50

- ・解析部のサービス起動時
- ・PCの電源投入時
- ・一定の時間間隔毎
- ・PCのIPアドレスの更新時

ただし、前述の送信タイミングは単なる例であることが理解されるべきである。本説明を再検討すれば、送信タイミングとして多種多様なものが存在することは、本技術分野の当業者にとって明らかであろう。

【0273】

また、UDPパケット、またはTCPパケットの宛先として、下記のうちのいずれか、および組み合わせが考えられる。

【0274】

- ・ユーザインターフェースや他のアプリケーションから指定された、IPアドレスとポート番号に向けて送信する
- ・設定ファイルなどに予め設定されているIPアドレスとポート番号に向けて送信する
- ・ランダムに選んだIPアドレスとポート番号に向けて送信する

ただし、前述のパケットの宛先は単なる例であることが理解されるべきである。本説明を再検討すれば、パケットの宛先として多種多様なものが存在することは、本技術分野の当業者にとって明らかであろう。

【0275】

以下の動作説明では、アプリケーション部3107からの命令を契機に、UDPパケットを予め設定ファイルに登録されているIPアドレスとポート番号に向けて送信する方法を採用した場合を例に説明する。

【0276】

以降の動作説明では、第3の実施の形態と同様に、UDPパケットをPC401から送信することを想定しているが、UDPパケットの代わりにTCPパケットを送信しても支障がないことは、本技術分野の当業者にとって明らかであろう。

【0277】

ここで、解析部3106からUDPベースのIPパケットが送信される処理は、第3の実施の形態と同じであるため、説明を省略する。

【0278】

また、NATルータ402でのヘッダ変換処理、およびルータ403でのICMP Time Exceededパケットの返信処理についても、第3の実施の形態と同じであるため、説明を省略する。

【0279】

PC401は、ルータ403から送り返されたICMP Time Exceededパケットを受け取る。

【0280】

このICMP Time Exceededパケットのヘッダのデータ部が解析部3106に渡される処理は、第3の実施の形態と同じであるため、説明を省略する。

【0281】

解析部3106は、パケット受信部3104からICMP Time Exceededパケットのヘッダのデータ部を受け取ると、そのチェックサムの状態から、ネットワークでヘッダ変換が行われたのかどうかを検出する。

【0282】

解析部3106は、ヘッダ変換の発生を検出すると、ヘッダの変更内容の推定処理を開始するが、ここで行われる推定処理は、第3の実施の形態の解析部で行われる推定処理と同じであるため、説明を省略する。

【0283】

解析部3106では、このように推定されたNATルータ402のIPアドレスとポート番号を通信相手となるPC407に通知する。

10

20

30

40

50

【0284】

この通知手段としては、通信相手となるPC407のユーザに向けてメールを送信したり、そのユーザに電話をかけたり、FAXを送信して伝える等といったことが考えられる。この通知の様子が、図33に経路1として示されている。

【0285】

次に、通信相手となるPC407側の動作について述べる。

【0286】

PC407では、前記通知手段により、PC401からNATルータ402のIPアドレスとポート番号を受け取ると、PC407の解析部3106はそのIPアドレスとポート番号をパケット送信部3105に通知し、UDPパケットの送信を依頼する（図32のステップS3203）。 10

【0287】

以降のパケット送信処理は、第1の実施の形態の図7～図10と同じであるため、説明を省略する。

【0288】

このようにPC407から送信されたデータは、図4のNATルータ406において、送信元IPアドレスと送信元ポート番号が変換される。この例では、送信元IPアドレスが192.168.1.2から200.30.1.1へ、送信元ポート番号が65000から65001に変更されたとする。

【0289】

このように変更されたパケットは、通信相手側のNATルータ402に届けられる。 20

【0290】

NATルータ402の動作モードが非特許文献1に示されるような「Full Cone NAT」と呼ばれるタイプであれば、このように届けられたパケットは、NATルータ402で破棄されることなく、NATルータ402からPC401に転送される。

【0291】

PC401は、このパケットをNATルータ402から受け取ると、このパケットをMAC部3101からパケット受信部3104に吸い上げる。

【0292】

解析部3106は、パケット受信部3104からパケットを受け取ると、そのヘッダから通信相手のNATルータ406のIPアドレスとポート番号を取得できる。 30

【0293】

以上の処理により、NATルータに繋がれたPC401とPC407の間でパケットをやり取りするために必要な情報を推定することができた。

【0294】

この後、PC401とPC407のアプリケーション間で通信する際には、アプリケーション部3107は解析部3106を介してデータをやり取りする。例えば、解析部3106は、アプリケーション部3107からデータを受け取ると、通信相手となるNATルータのIPアドレスとポート番号をパケット送信部3105に通知し、UDPパケットの送信を依頼する。以降の送信処理は、第1の実施の形態の図7～図10と同じであるため、説明を省略する。 40

【0295】

一方、PC407では、PC401から送信されたパケットを、第1の実施の形態の図12～図14の処理により、MAC部3101から解析部3106に吸い上げる。この後、解析部3106からアプリケーション部3107にデータを転送する。

【0296】

以上、NATルータの動作モードが「Full Cone NAT」と呼ばれるタイプの場合の動作について説明した。

【0297】

一方、NATルータの動作モードが非特許文献1に示されるような「Restricted Cone 50

NAT」、または「Port Restricted Cone NAT」と呼ばれるタイプの場合、図 3 2 のステップ S 3 2 0 3 で、P C 4 0 7 から N A T ルータ 4 0 2 宛に送信されたパケットは N A T ルータ 4 0 2 において破棄されてしまう。

【0 2 9 8】

このように破棄されてしまう理由は、これらの N A T ルータでは、非特許文献 1 に示されるように、一度パケットを送信したことがある I P アドレス/ポート番号からのパケットしか受け付けられないためである。

【0 2 9 9】

本発明の第 5 の実施の形態では、N A T ルータがこのようなタイプの場合でも、パケットをやり取りするのに必要な情報を推定するために、以下のような処理を行う。

10

【0 3 0 0】

まず、前述の通知手段により、P C 4 0 7 は、P C 4 0 1 から N A T ルータ 4 0 2 の I P アドレスとポート番号を受け取ると、N A T ルータ 4 0 6 の I P アドレスとポート番号を取得することを試みる。N A T ルータ 4 0 6 の情報の取得方法としては、第 3 の実施の形態と同様に、TTL 値を小さくした UDP パケットを送信する。ただし、ここで送信する UDP パケットの宛先としては、P C 4 0 1 から通知された N A T ルータ 4 0 2 の I P アドレスとポート番号を指定するものとする。

【0 3 0 1】

ここで行われるパケット送信処理は、第 3 の実施の形態の図 2 7 ～図 2 8 と同じであるため、説明を省略する。

20

【0 3 0 2】

このように P C 4 0 7 から送信されたパケットは、まず、図 4 の N A T ルータ 4 0 7 において、送信元 I P アドレスと送信元ポート番号が変換される。変換処理の内容は、図 1 1 と同じであるため、説明を省略する。

【0 3 0 3】

このように変更されたパケットは、つぎにルータ 4 1 1 に届けられる。ルータ 4 1 1 では、TTL を 1 から 0 に書き換えるが、TTL が 0 になったので、このパケットを破棄する。そして、ルータ 4 1 1 はパケットの送信元である N A T ルータ 4 0 6 に ICMP Time Exceeded メッセージを送り返す。

【0 3 0 4】

30

P C 4 0 7 は、この ICMP Time Exceeded メッセージを N A T ルータ 4 0 6 から受け取ると、第 3 の実施の形態と同様にして、そのチェックサムから NAT ルータ 4 0 6 の I P アドレスとポート番号を取得することができる。

【0 3 0 5】

ここで行われるパケット受信処理とヘッダの変更内容の推定処理は、第 3 の実施の形態と同じであるため、説明を省略する。

【0 3 0 6】

P C 4 0 7 の解析部 3 1 0 6 では、このように推定された N A T ルータ 4 0 6 の I P アドレスとポート番号を通信相手となる P C 4 0 1 に通知する。

【0 3 0 7】

40

この通知手段としては、通信相手の P C 4 0 1 のユーザに向けてメールを送信したり、そのユーザに電話をかけたり、F A X を送信して伝える等といったことが考えられる。この通知の様子が、図 3 3 に経路 2 として示されている。

【0 3 0 8】

P C 4 0 1 では、前記通知手段により、P C 4 0 7 から N A T ルータ 4 0 6 の I P アドレスとポート番号を受け取ると、P C 4 0 1 の解析部 3 1 0 6 はその I P アドレスとポート番号をパケット送信部 3 1 0 5 に通知し、U D P パケットを送信を依頼する（図 3 2 のステップ S 3 2 0 3）。

【0 3 0 9】

ここで行われるパケット送信処理は、第 1 の実施の形態の図 7 ～図 1 0 と同じであるた

50

め、説明を省略する。

【0310】

このように送信されたデータは、図4のNATルータ402において、送信元IPアドレスと送信元ポート番号が変換された後、通信相手側のNATルータ406に届けられる。

【0311】

NATルータ406は、先程の通信処理において、このパケットの送信元であるNATルータ402にパケットを送信したことがあるので、パケットを破棄することなく、PC407に転送する。

【0312】

PC407は、このパケットをNATルータ402から受け取ると、このパケットをMAC部3101から解析部3106に吸い上げるが、この処理は第1の実施の形態の図12～図14と同じであるため、説明を省略する。

【0313】

解析部3106は、パケット受信部3104からパケットを受け取ると、そのヘッダから通信相手のNATルータ406のIPアドレスとポート番号を取得できる。

【0314】

以上の処理により、NATルータに繋がれたPC401とPC407の間でパケットをやり取りするために必要な情報を推定することができた。

【0315】

この後、PC401とPC407のアプリケーション間で通信する際には、アプリケーション部3107は解析部3106を介してデータをやり取りする。

【0316】

以上のように、PCがNATルータに繋がれている場合でも、ICMPパケットのチェックサムから推定されたNATルータのIPアドレスとポート番号を通信相手に通知し合うことにより、PC間でパケットをやり取りするのに必要な情報を推定できることが示された。

【0317】

以上、NATルータの動作モードが「Restricted Cone NAT」、または「Port Restricted Cone NAT」と呼ばれるタイプの場合の動作について説明した。

【0318】

一方、NATルータの動作モードが非特許文献1に示されるような「Symmetric NAT」と呼ばれるタイプの場合、上述のような処理を行っても、PC401からNATルータ406に送信されたパケットはNATルータ406において破棄されてしまう。

【0319】

破棄されてしまう理由は、このようなNATルータでは、非特許文献1に示されるように、NATルータにおける送信元ポート番号が宛先IPアドレス／宛先ポート番号に応じて変化してしまうためである。例えば、図33の経路1で、PC401からPC407にNATルータ402のPC405との通信用ポート番号を通知しているが、PC407では受け取ったポート番号を宛先としたパケットを送信する。また、PC407は、図33の経路2において、このときの送信パケットにNATルータ406から割り当てられる送信元ポート番号をPC401に通知する。PC401では、受け取ったポート番号を宛先としたパケットを送信する。ここで注意すべきことは、このときPC401から送信されたパケットの送信元ポート番号には、「Symmetric NAT」の特性から、PC405との通信用ポート番号と異なる値が付与されていることである。このようなパケットをNATルータ406が受信すると、その送信元ポート番号とのマッピングテーブルはまだ作成されていないので、パケットを破棄してしまう。以上のことから、上述の方法では「Symmetric NAT」の場合には対応できない。

【0320】

本発明の第5の実施の形態では、NATルータがこのような「Symmetric NAT」の場合

10

20

30

40

50

でも、パケットをやり取りするのに必要な情報を推定するために、以下のような処理を行う。

【0321】

まず、前述の通知手段により、PC407は、PC401からNATルータ402のIPアドレスとポート番号を受け取ると、NATルータ406のIPアドレスとNATルータ402との通信用ポート番号を推定する。

【0322】

ここで行われる推定処理は、NATルータが「Restricted Cone NAT」、または「Port Restricted Cone NAT」の場合の動作と同じであり、既に説明しているため、説明を省略する。

10

【0323】

ただし、このとき推定できるポート番号は、あくまで、NATルータ406において、NATルータ402のPC405との通信用ポート番号に対して割り当てられたポート番号である。

【0324】

PC407では、このようにNATルータ406のIPアドレスとNATルータ402との通信用ポート番号を取得すると、次に、NATルータ406のポート番号の割り当て処理の規則性を調査する。非特許文献1には、「Symmetric NAT」の規則性について示されている。非特許文献1によると、「Symmetric NAT」の特性を持つNATルータは、その送信元ポート番号として、1ずつ増えるような値を割り当てることが多い。

20

【0325】

本発明の第5の実施の形態では、この規則性を調査するために、PC407からグローバルIPアドレスの端末を宛先としたパケットを複数送信するとともに、第3の実施の形態に従って、NATルータ406において、その宛先毎に割り当てられた送信元ポート番号を推定する。以上のように推定された送信元ポート番号を元にして、PC407は、「Symmetric NAT」の規則性を把握し、NATルータ402との通信用に設定される「真」のポート番号を推定する。

【0326】

PC407は、このように推測されたポート番号と、NATルータ406のIPアドレスをPC401に通知する。

30

【0327】

一方、PC401では、このとき、PC407から受け取ったIPアドレスとポート番号を宛先としたパケットを送信するとともに、NATルータ402からそのパケットに割り当てられた送信元ポート番号を推定する。この推定処理は、第3の実施の形態と同じであるため、説明を省略する。PC401は、このように推定されたポート番号を、再度、PC407に通知する。

【0328】

PC407は、このようにPC401から受け取ったポート番号を宛先としたパケットを送信する（宛先IPアドレスもPC401とする）。ここで、NATルータ406では、パケットの送信元ポート番号を、前述の「Symmetric NAT」の規則性から推定されているポート番号に変換するものとする。このように変換されたパケットが、NATルータ402に到達すると、NATルータ402では、前述のパケット送信処理によって既にマッピングテーブルが作成されているので、このパケットを破棄せずにPC401に転送する。

40

【0329】

以上のように、PCがNATルータに繋がれている場合でも、ICMPパケットのチェックサムから推定されたNATルータのIPアドレスとポート番号を通信相手に通知し合うことにより、PC間でパケットをやり取りするのに必要な情報を推定できることが示された。

【0330】

以上、NATルータの動作モードが「Symmetric NAT」と呼ばれるタイプの場合の動作につ

50

いて説明した。

【0331】

一方、上記の説明では、本発明の第1～第4の実施の形態の方法を用いることにより、NATルータのIPアドレスやポート番号を一意に絞り込めることを前提としていた。これに対して、上記の方法で、IPアドレスやポート番号を一意に絞り込むことができず、複数の候補が残っている場合には、間違った通信相手から接続要求を受けてしまう可能性がある。

【0332】

このような問題を回避するために、第5の実施の形態では、パケットの中にメールアドレスや識別子など、通信相手を特定する情報を付加しておくことにより、所望の相手以外からの接続要求を防止できる。 10

【0333】

<効果>

続いて、本発明を実施するための第5の実施の形態の効果について説明する。

【0334】

本発明を実施するための第5の実施の形態では、通信相手となるPCがNATルータの配下に設置されている場合でも、ICMPパケットのチェックサムからNATルータのIPアドレスとポート番号を推定するとともに、お互いにその情報を通知しあうことにより、専用サーバをインターネット上に設置することなく、PC間でパケットをやり取りするのに必要な情報を推定でき、本発明の目的を達成することができる。 20

【0335】

次に、本発明を実施するための第6の実施の形態について図面を参照して詳細に説明する。

【0336】

<構成>

本発明の第1から第5の実施の形態では、NATルータのIPアドレスとポート番号の推定方法について述べたが、本発明の第6の実施の形態では、ToSフィールドの変化を推定する方法について述べる。

【0337】

図34を参照すると、本発明の第6の実施の形態は、インターネットのようなネットワーク3404と、ユーザが操作するPC3401と、インターネット上に設置されている任意のPC3405と、パケットの経路制御を行うルータ3403とを含む。また、ネットワーク3404は、パケットの経路制御を行うルータ3408～3411を含む。 30

【0338】

ここで、ルータ3403では、特定のフローを優先的に取り扱うために、パケットのToSフィールドが変更されるものとする。

【0339】

PC3401の内部構成を図35に示す。

【0340】

図35に示されるように、PC3401の内部構成は、図26のPC401の内部構成と同じである。ただし、本発明の第6の実施の形態では、上記の問題を解決するために、図26の解析部2606で実行する処理を変更している。 40

【0341】

本発明の第5の実施の形態の解析部3506では、図26の解析部2606の処理に加えて、パケット受信部2604から渡されるICMP Time Exceededメッセージから、ネットワーク内で行われたToSフィールドの変化を検出する処理を行う。

【0342】

他の処理は、第3の実施の形態の図26と同じであるため、説明を省略する。

【0343】

<動作>

P C 3 4 0 1 から、TTL 値の小さなパケットを送信する処理については、第 3 の実施の形態と同じであるため、説明を省略する（図 3 6 (a)）。

【0 3 4 4】

以降の動作説明では、第 3 の実施の形態と同様に、U D P パケットを P C 3 4 0 1 から送信することを想定しているが、U D P パケットの代わりに T C P パケットを送信しても支障がないことは、本技術分野の当業者にとって明らかであろう。

【0 3 4 5】

P C 3 4 0 1 から送信されたデータは、まず、図 3 4 のルータ 3 4 0 3 において、I P ヘッダの ToS フィールドが変更される。この例では、ToS フィールドが 0x00 から 0xc0 に変更されたとする。また、これらの変更に伴い、I P ヘッダのチェックサムも再計算される。この例では、I P ヘッダのチェックサムが 0x10 から 0x20 に変更されたとする（図 3 6 (b)）。さらに、ルータ 3 4 0 3 は T T L を 2 から 1 に書き換える。

10

【0 3 4 6】

このように変更されたパケットは、つぎにルータ 3 4 0 8 に届けられる。ルータ 3 4 0 8 では、T T L を 1 から 0 に書き換えるが、T T L が 0 になったので、このパケットを破棄する。そして、ルータ 3 4 0 8 はパケットの送信元である P C 3 4 0 1 に ICMP Time Exceeded メッセージを送り返す。この ICMP Time Exceeded メッセージは、図 3 6 (c) のようなパケットして送られるが、そのデータ部には先程ルータ 3 4 0 8 が受信したパケットがそのまま付加される。

【0 3 4 7】

20

P C 3 4 0 1 は、この I C M P パケットをルータ 3 4 0 8 から受け取ると、第 3 の実施の形態と同じように、M A C 部 3 5 0 1 から解析部 3 5 0 6 まで吸い上げられる。

【0 3 4 8】

解析部 3 5 0 6 は、パケット受信部 3 5 0 4 から ICMP Time Exceeded メッセージのヘッダのデータ部を受け取ると、そのデータの状態から、ネットワークで ToS フィールドが変換されかどうか検出できる。

【0 3 4 9】

具体的には、ICMP Time Exceeded メッセージの ToS フィールドをチェックし、ToS フィールドが 0 となっていない場合には ToS フィールドの書き換えが発生したと判断することにより、ネットワーク内における優先制御機能の稼動状況を検出できる（図 3 6 (c)）。

30

【0 3 5 0】

以上の処理により、ICMP Time Exceeded メッセージを利用することにより、ネットワーク内における ToS フィールドの変化を推定できることが示された。

【0 3 5 1】

<効果>

続いて、本発明を実施するための第 6 の実施の形態の効果について説明する。

【0 3 5 2】

本発明を実施するための第 6 の実施の形態では、ルータから送り返されてくる ICMP Time Exceeded メッセージの情報を元にして、ネットワーク内における ToS フィールドの変化を推定することにより、専用サーバをインターネット上に設置することなく、ネットワーク内で優先制御機能が働いていることを検出することができ、本発明の目的を達成することができる。

40

【0 3 5 3】

次に、本発明を実施するための第 7 の実施の形態について図面を参照して詳細に説明する。

【0 3 5 4】

<構成>

本発明の第 6 の実施の形態では、ToS フィールドの推定方法について述べたが、本発明の第 7 の実施の形態では、フラグメントが発生したかどうかを推定する方法について述べる。

50

【0355】

図37を参照すると、本発明の第7の実施の形態は、インターネットのようなネットワーク3704と、ユーザが操作するPC3701と、インターネット上に設置されている任意のPC3705と、パケットの経路制御を行うルータ3703とを含む。また、ネットワーク3704は、パケットの経路制御を行うルータ3708～3711を含む。

【0356】

ここで、ルータ3708では、データサイズが回線のMTUを越えないように、パケットのフラグメントが行われるものとする。

【0357】

PC3701の内部構成を図38に示す。

10

【0358】

図38に示されるように、PC3701の内部構成は、図35に示される本発明の第6の実施の形態のPC3401の内部構成と同じである。ただし、本発明の第7の実施の形態では、上記の問題を解決するために、図35の解析部3506で実行する処理を変更している。

【0359】

本発明の第7の実施の形態の解析部3806では、図35の解析部3506の処理に加えて、パケット受信部3804から渡されるICMP Time Exceededメッセージから、ネットワーク内で行われたフラグメントの発生を検出する。

【0360】

20

他の内部構成は、第6の実施の形態の図35と同じであるため、説明を省略する。

【0361】

<動作>

PC3701から、TTL値の小さなパケットを送信する処理については、第6の実施の形態と同じであるため、説明を省略する(図39(a))。

【0362】

以降の動作説明では、第3の実施の形態と同様に、UDPパケットをPC3701から送信することを想定しているが、UDPパケットの代わりにTCPパケットを送信しても支障がないことは、本技術分野の当業者にとって明らかであろう。

【0363】

30

PC3701から送信されたパケットサイズが1300byteであると仮定する(図39(a))。

【0364】

PC3701から送信されたデータは、まず、図37のルータ3708において、IPパケットのフラグメントが行われる。この例では、パケットサイズが800byteと500byteの2つのパケットに分割されるものとする。フラグメントを行ったルータ3708は、パケットのフラグフィールドの第3ビットを1に設定するとともに、最終パケットのフラグフィールドに0を設定する。また、フラグメントオフセットフィールドにはデータのオフセット値を設定する。

【0365】

40

また、これらの変更に伴い、IPヘッダのチェックサムも再計算される(図39(b)、図39(c))。さらに、ルータ3708では、TTLを2から1に書き換える。

【0366】

このように変更されたパケットは、つぎにルータ3709に届けられる。ルータ3709では、TTLを1から0に書き換えるが、TTLが0になったので、このパケットを破棄する。そして、ルータ3709はパケットの送信元であるPC3701にICMP Time Exceededメッセージを送り返す。このICMP Time Exceededメッセージは、図39(d)、図39(e)ののようなパケットして送られるが、そのデータ部には先程ルータ3709が受信したパケットがそのまま付加される。

【0367】

50

PC3701は、このICMPパケットをルータ3709から受け取ると、第6の実施の形態と同じように、MAC部3801から解析部3806まで吸い上げられる。

【0368】

解析部3806は、パケット受信部3804からICMP Time Exceededメッセージのヘッダのデータ部を受け取ると、そのデータの状態から、ネットワークでフラグメントが発生したかどうか検出できる。

【0369】

具体的には、ICMP Time Exceededメッセージのフラグメントフィールドとオフセットフィールドをチェックし、両方のフィールドが0となっていない場合にはフラグメントが発生したものと判断することにより、ネットワーク内におけるフラグメントの発生状況を検出できる（図39(d)、図39(e)）。 10

【0370】

以上の処理により、ICMP Time Exceededメッセージを利用することにより、ネットワーク内におけるフラグメントの発生を検出できることが示された。

【0371】

<効果>

続いて、本発明を実施するための第7の実施の形態の効果について説明する。

【0372】

本発明を実施するための第7の実施の形態では、ルータから送り返されてくるICMP Time Exceededメッセージの情報を元にして、ネットワーク内におけるフラグメントの発生状況を推定することにより、専用サーバをインターネット上に設置することなく、ネットワーク内でフラグメントが発生したかどうかを検出することができ、本発明の目的を達成することができる。 20

【0373】

続いて、本発明を実施するための第8の実施の形態について図面を参照して詳細に説明する。

【0374】

<構成>

本発明の第5の実施の形態では、PC間でUDPパケットをやり取りするために必要な情報を把握する方法について述べたが、本発明の第8の実施の形態では、PC間でTCPパケットをやり取りするために必要な情報を把握するための方法について述べる。 30

【0375】

具体的には、図4のPC401とPC407との間でTCPパケットをやり取りするのに必要な情報の推定方法について述べる。

【0376】

本発明の第8の実施の形態の構成を図40に示す。本発明の第8の実施の形態では、上記の問題を解決するために、図31の解析部3106、パケット送信部3105、およびパケット受信部3104で実行する処理を変更するとともに、TCP部4008を含む。

【0377】

図40の解析部4006は、図31の解析部3106の処理に加えて、TCPパケットのシーケンス番号を通信相手に通知する。また、相手からNATルータのIPアドレスとポート番号、およびシーケンス番号を受け取り、これらの情報を元にしたTCPパケットを送信するようにパケット送信部4105に命令する。 40

【0378】

TCP部4008は、パケット送信部から渡されたデータにTCPヘッダを追加した後、IP部4002に渡す。また、IP部4002から渡されたデータからTCPヘッダを外した後、パケット受信部4004に渡す。

【0379】

その他の構成は、第5の実施の形態と同じであるため、説明を省略する。

【0380】

<動作>

続いて、図40を参照して本発明を実施するための第8の実施の形態の動作について詳細に説明する。

【0381】

第8の実施の形態では、まず、NATルータのIPアドレスとUDPパケット用のポート番号を推定するとともに、それらの情報を通信相手に通知することを行うが、これらの処理は第5の実施の形態とまったく同じであるため、説明を省略する。よって、以下の説明では、図4のPC401とPC407の間において、通信相手のNATルータのIPアドレスとUDPパケット用のポート番号を既に取得していることを前提にして話を進める。

【0382】

10

次に、PC401とPC407の解析部4006は、TTL値を小さく設定したTCPのSYNパケットを通信相手のNATルータに向けて送信するようにパケット送信部4005に命令する。尚、このTTL値はネットワークの輻輳を考慮すると小さい値の方が良いが、PC407に届かない値にすれば良い。

【0383】

パケット送信部4005は、解析部4006からSYNパケットの送信命令を受け取ると、指定された宛先に向けてSYNパケットの送信処理を行うために、データをTCP部4008に渡す。

【0384】

TCP部4008は、このデータを受け取ると、宛先ポート番号が既に取得しているNATルータのポート番号となっているTCPヘッダを付与して、SYNパケットを生成する。このように、PC401とPC407の双方からSYNパケットを送信するが、この際、SYNパケットに付与されるTCPシーケンス番号を記録しておく。ここで、PC401が送信したSYNパケットのTCPシーケンス番号をXとし、PC407が送信したSYNパケットのTCPシーケンス番号をYとする。TCP部4008は、このSYNパケットをIP部4002に渡す。

20

【0385】

IP部4002は、TCP部4008からSYNパケットを受け取ると、宛先IPアドレスがNATルータのIPアドレスとなっているIPヘッダを付与し、MAC部4001に渡す。

【0386】

MAC部4001は、IP部4002からパケットを受け取ると、MACヘッダを付与し、伝送路に送信する。

30

【0387】

ただし、このように送信されたSYNパケットは、TTL値が小さいので、途中経路のルータにおいてパケットが破棄される。

【0388】

次に、PC401とPC407の解析部4006は、先ほど記録したTCPシーケンス番号を通信相手にメールで通知する。

【0389】

PC401とPC407の解析部4006は、通信相手からTCPシーケンス番号をメールで受け取ると、このTCPシーケンス番号を考慮したSYN+ACKパケットを送信するように、パケット送信部4005に命令する。

40

【0390】

パケット送信部4005は、解析部4006からSYN+ACKパケットの送信命令を受け取ると、指定された宛先に向けてSYN+ACKパケットの送信処理を行うために、データをTCP部4008に渡す。

【0391】

TCP部4008は、このデータを受け取ると、宛先ポート番号がNATルータのポート番号、TCPシーケンス番号とTCP確認応答番号に適切な値が設定されているTCPヘッダを付与して、SYN+ACKパケットを生成する。ここで、PC401から送信するSYN+ACKパケットについて考えると、その宛先ポート番号にNATルータ406のポート番号、TCPシーケンス番号

50

にX、TCP確認応答番号にY+1が設定される。一方、PC 4 0 7から送信するSYN+ACKパケットについて考えると、その宛先ポート番号にNATルータ4 0 2のポート番号、TCPシーケンス番号にY、TCP確認応答番号にX+1が設定される。PC 4 0 1とPC 4 0 7のTCP部4 0 0 8は、このようなSYN+ACKパケットをIP部4 0 0 2に渡す。

【0 3 9 2】

IP部4 0 0 2は、TCP部4 0 0 8からSYN+ACKパケットを受け取ると、宛先IPアドレスが通信相手のNATルータのIPアドレスとなっているIPヘッダを付与し、MAC部4 0 0 1に渡す。

【0 3 9 3】

MAC部4 0 0 1は、IP部4 0 0 2からパケットを受け取ると、MACヘッダを付与し、伝送路に送信する。 10

【0 3 9 4】

ここで注目すべき点として、SYN+ACKパケットを送信する前にあらかじめSYNパケットを送信しておくことにより、各NATルータにマッピングテーブルが作成されていることが挙げられる。これにより、PC 4 0 1およびPC 4 0 7から送信されたSYN+ACKパケットは、通信相手のNATルータで破棄されることなく、通信相手まで届けられる。

【0 3 9 5】

ここで、注意すべき点として、NATルータの種類によっては、NATルータがUDPパケット用に開けるポート番号とTCPパケット用に開けるポート番号が異なる可能性が挙げられる。たとえば、UDPパケット用のポート番号とTCPパケット用のポート番号に1程度のズレが生じることがある。このような場合に、上述のように、SYNパケットやSYN+ACKパケットの宛先TCPポート番号にUDPパケット用のポート番号を設定していると、マッピングテーブルのポート番号と一致しないため、SYN+ACKパケットがNATルータで破棄されてしまう。このような事態にも対応できるように、SYNパケットやSYN+ACKパケットの宛先TCPポート番号にUDPパケット用のポート番号に1を足した値を設定するように変更することも可能である。 20

【0 3 9 6】

ただし、前述の宛先ポート番号の設定方法例は単なる例であることが理解されるべきである。本説明を再検討すれば、宛先ポート番号の設定方法が多種多様な方法で実施されることは、本技術分野の当業者にとって明らかであろう。 30

【0 3 9 7】

次に、PC 4 0 1とPC 4 0 7の解析部4 0 0 6は、通信相手からSYN+ACKパケットを受け取ると、ACKパケットを送信するように、パケット解析部4 0 0 5に命令する。

【0 3 9 8】

パケット送信部4 0 0 5は、解析部4 0 0 6からACKパケットの送信命令を受け取ると、指定された宛先に向けてACKパケットの送信処理を行うために、データをTCP部4 0 0 8に渡す。

【0 3 9 9】

TCP部4 0 0 8は、このデータを受け取ると、宛先ポート番号がNATルータのポート番号、TCP確認応答番号に適切な値が設定されているTCPヘッダを付与して、ACKパケットを生成する。ここで、PC 4 0 1から送信するACKパケットについて考えると、その宛先ポート番号にNATルータ4 0 6のポート番号、TCP確認応答番号にY+1が設定される。一方、PC 4 0 7から送信するACKパケットについて考えると、その宛先ポート番号にNATルータ4 0 2のポート番号、TCP確認応答番号にX+1が設定される。PC 4 0 1とPC 4 0 7のTCP部4 0 0 8は、このようなACKパケットをIP部4 0 0 2に渡す。 40

【0 4 0 0】

IP部4 0 0 2は、TCP部4 0 0 8からACKパケットを受け取ると、宛先IPアドレスが通信相手のNATルータのIPアドレスとなっているIPヘッダを付与し、MAC部4 0 0 1に渡す。

【0 4 0 1】

MAC部4 0 0 1は、IP部4 0 0 2からパケットを受け取ると、MACヘッダを付与し、伝送 50

路に送信する。

【0402】

これらのACKパケットは、通信相手のNATルータで破棄されることなく、通信相手まで届けられる。以上の処理により、TCPセッションの確立に必要な3 way handshake処理が完了した。

【0403】

<効果>

続いて、本発明を実施するための第8の実施の形態の効果について説明する。

【0404】

本発明を実施するための第8の実施の形態では、通信相手となるPCがNATルータの配下に設置されている場合でも、専用サーバをインターネット上に設置することなく、TCPパケットをやり取りするのに必要な情報を推定でき、本発明の目的を達成することができる。

【図面の簡単な説明】

【0405】

【図1】 ネットワークを説明するための図である。

【図2】 パケットの各ヘッダを説明するための図である。

【図3】 従来技術のネットワーク構成図である。

【図4】 本発明の第1の実施の形態を説明するためのネットワーク構成図である。

【図5】 本発明の第1の実施の形態の端末のブロック図である。

【図6】 本発明の第1の実施の形態における解析部の送信動作を説明するためのフロー図である。

【図7】 本発明の第1の実施の形態におけるパケット送信部の送信動作を説明するためのフロー図である。

【図8】 本発明の第1の実施の形態におけるUDP部の送信動作を説明するためのフロー図である。

【図9】 本発明の第1の実施の形態におけるIP部の送信動作を説明するためのフロー図である。

【図10】 本発明の第1の実施の形態におけるMAC部の送信動作を説明するためのフロー図である。

【図11】 本発明の第1の実施の形態におけるパケットヘッダの変更を説明するための図である。

【図12】 本発明の第1の実施の形態におけるMAC部の受信動作を説明するためのフロー図である。

【図13】 本発明の第1の実施の形態におけるIP部の受信動作を説明するためのフロー図である。

【図14】 本発明の第1の実施の形態におけるパケット受信部の受信動作を説明するためのフロー図である。

【図15】 本発明の第1の実施の形態における解析部の受信動作を説明するためのフロー図である。

【図16】 本発明の第1の実施の形態における解析部のIP推定処理の動作を説明するためのフロー図である。

【図17】 本発明の第1の実施の形態における解析部のポート推定処理の動作を説明するためのフロー図である。

【図18】 UDPの擬似ヘッダを説明するための動作である。

【図19】 本発明の第2の実施の形態の端末のブロック図である。

【図20】 本発明の第2の実施の形態における解析部の送信動作を説明するためのフロー図である。

【図21】 本発明の第2の実施の形態におけるパケット送信部の送信動作を説明するためのフロー図である。

10

20

30

40

50

【図 2 2】本発明の第 2 の実施の形態における M A C 部の送信動作を説明するためのフロー図である。

【図 2 3】本発明の第 2 の実施の形態における M A C 部の受信動作を説明するためのフロー図である。

【図 2 4】本発明の第 2 の実施の形態におけるパケット受信部の受信動作を説明するためのフロー図である。

【図 2 5】本発明の第 2 の実施の形態における解析部の受信動作を説明するためのフロー図である。

【図 2 6】本発明の第 3 の実施の形態の端末のブロック図である。

【図 2 7】本発明の第 3 の実施の形態における解析部の送信動作を説明するためのフロー図である。 10

【図 2 8】本発明の第 3 の実施の形態におけるパケット送信部の送信動作を説明するためのフロー図である。

【図 2 9】本発明の第 4 の実施の形態の端末のブロック図である。

【図 3 0】本発明の第 4 の実施の形態におけるパケットヘッダの変更を説明するための図である。

【図 3 1】本発明の第 5 の実施の形態の端末のブロック図である。

【図 3 2】本発明の第 5 の実施の形態におけるパケット送信部の送信動作を説明するためのフロー図である。

【図 3 3】本発明の第 5 の実施の形態におけるヘッダ変換情報の交換を説明するためのフロー図である。 20

【図 3 4】本発明の第 6 の実施の形態のネットワーク構成を説明するための図である。

【図 3 5】本発明の第 6 の実施の形態の端末のブロック図である。

【図 3 6】本発明の第 6 の実施の形態におけるパケットヘッダの変更を説明するための図である。

【図 3 7】本発明の第 7 の実施の形態のネットワーク構成を説明するための図である。

【図 3 8】本発明の第 7 の実施の形態におけるパケットヘッダの変更を説明するための図である。

【図 3 9】本発明の第 7 の実施の形態におけるパケットヘッダの変更を説明するための図である。 30

【図 4 0】本発明の第 8 の実施の形態の端末のブロック図である。

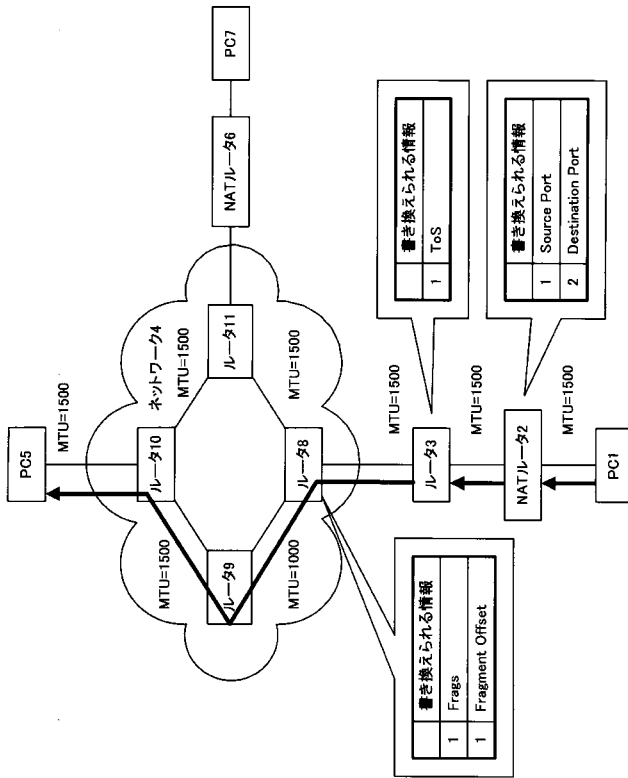
【符号の説明】

【0 4 0 6】

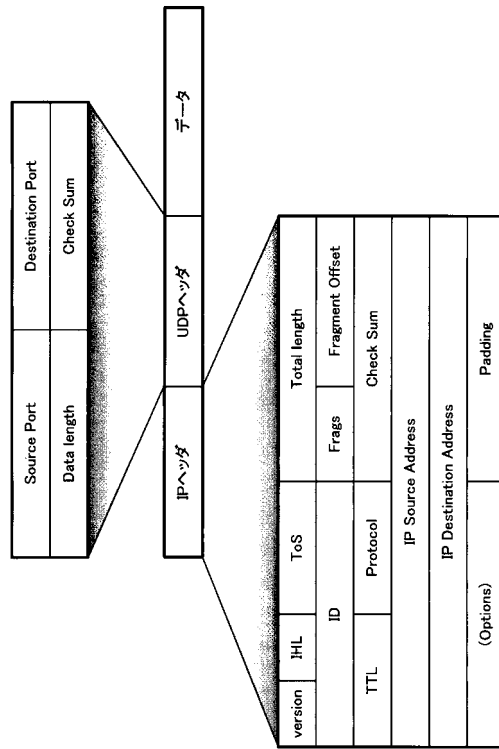
4 0 1 , 4 0 7 P C

4 0 2 , 4 0 6 N A T ルーター

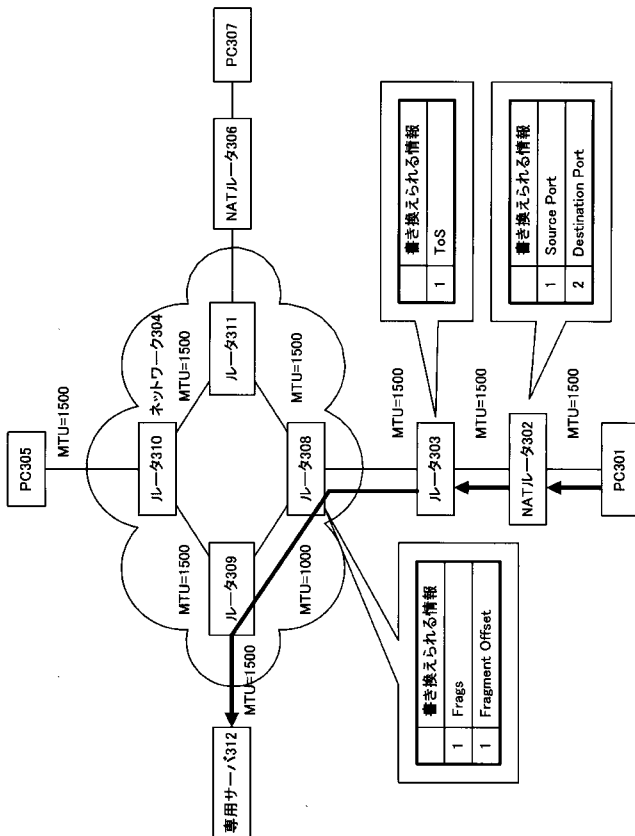
【図 1】



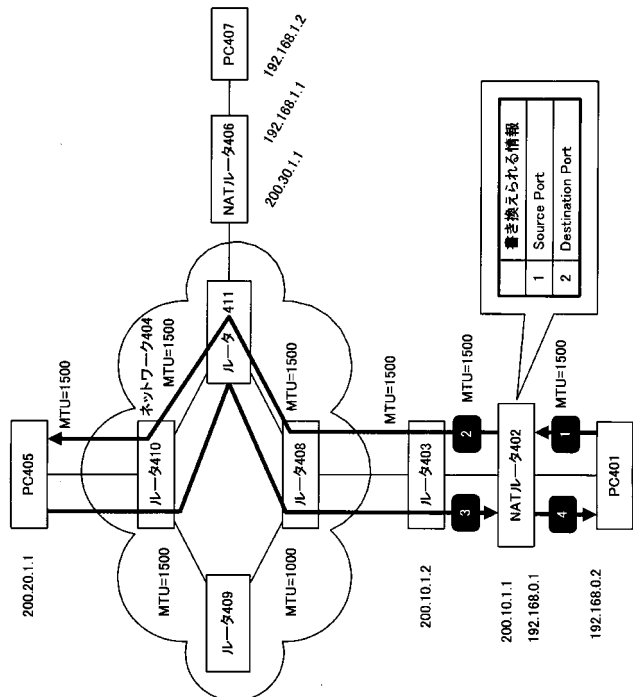
【図 2】



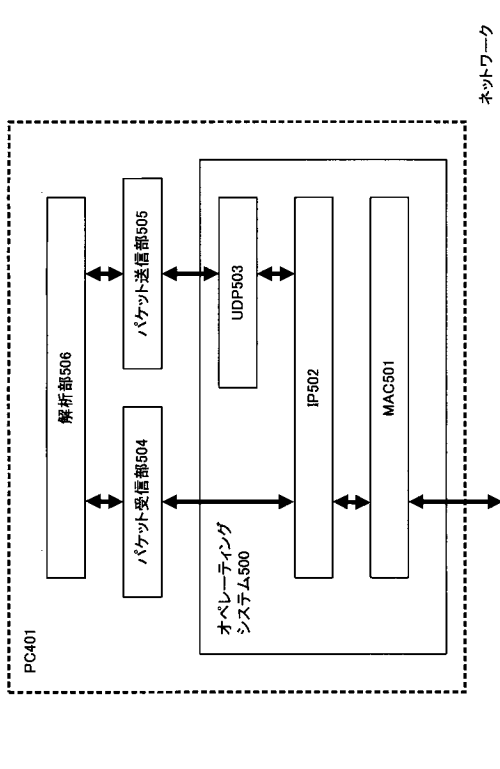
【図 3】



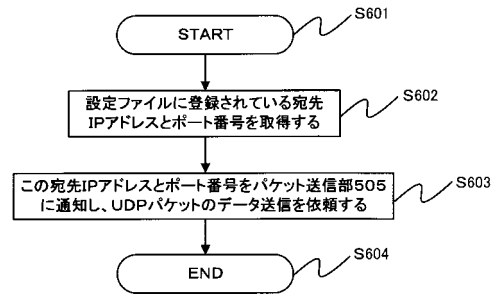
【図 4】



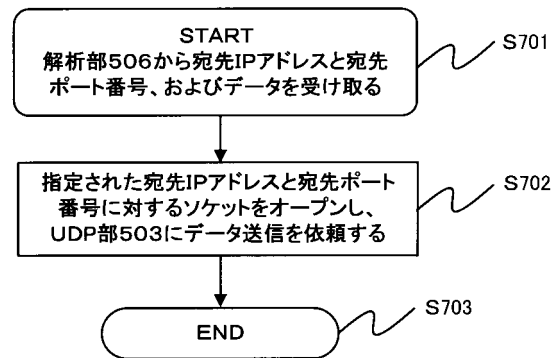
【図 5】



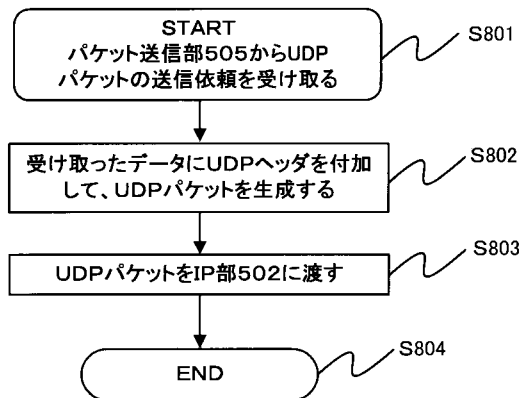
【図 6】



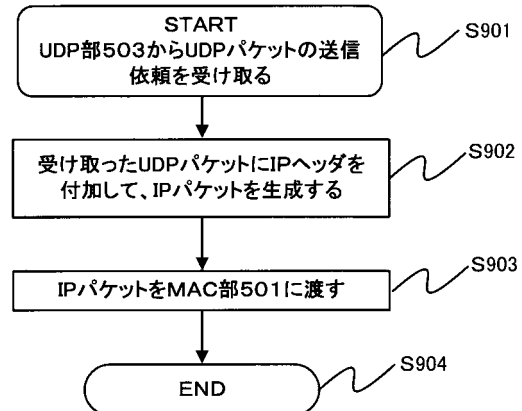
【図 7】



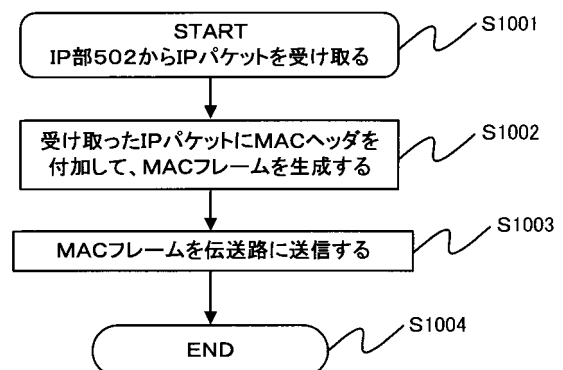
【図 8】



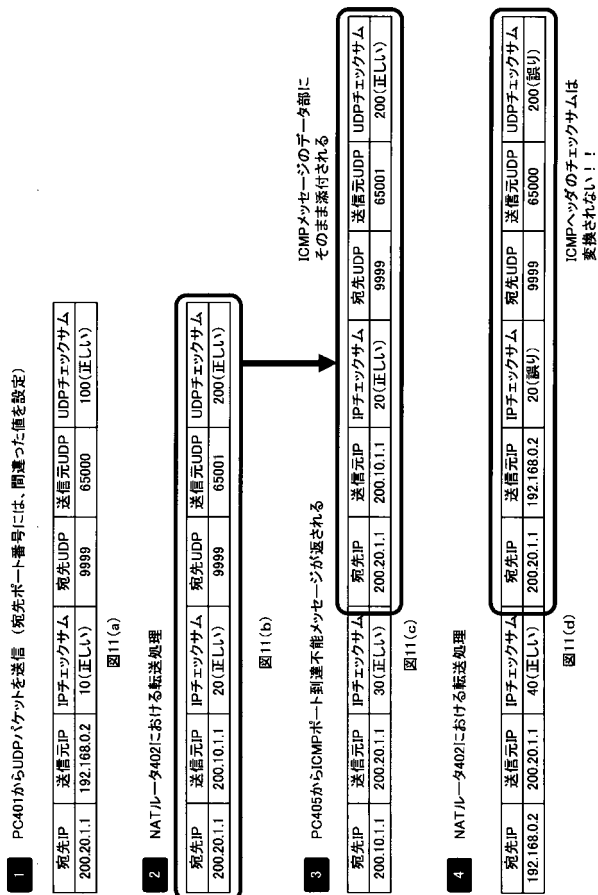
【図 9】



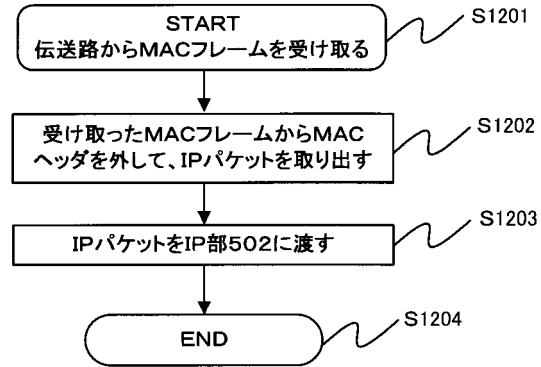
【図 10】



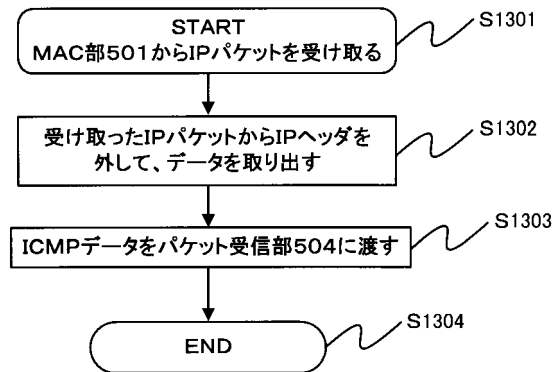
【図 1 1】



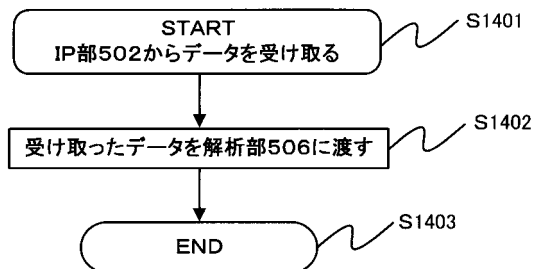
【図 1 2】



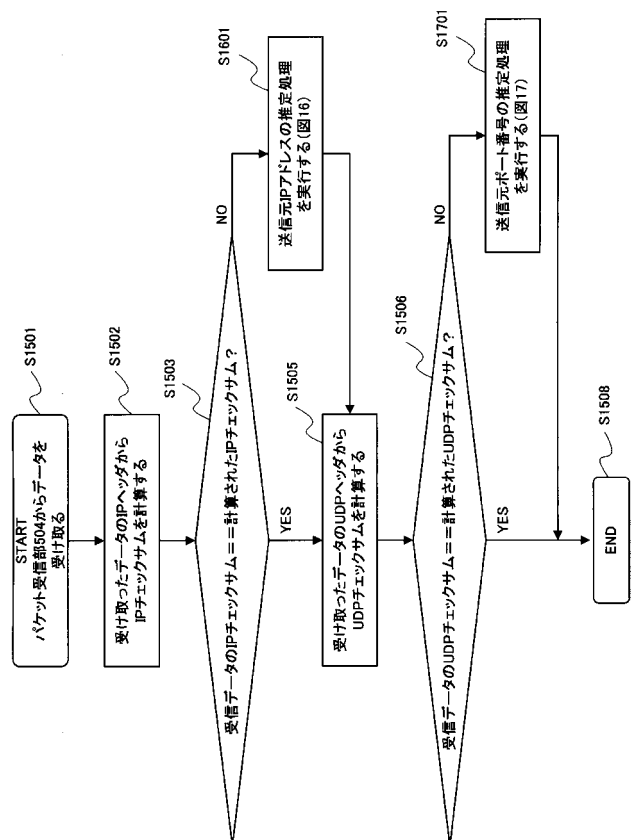
【図 1 3】



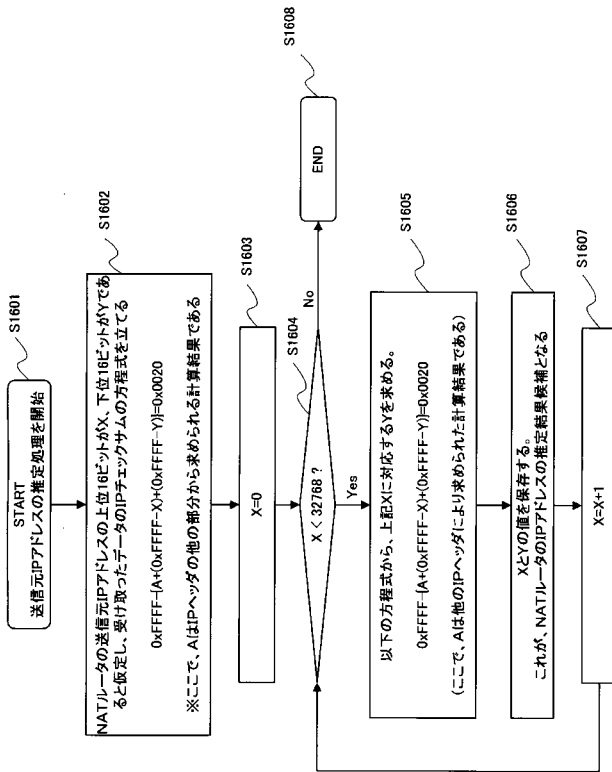
【図 1 4】



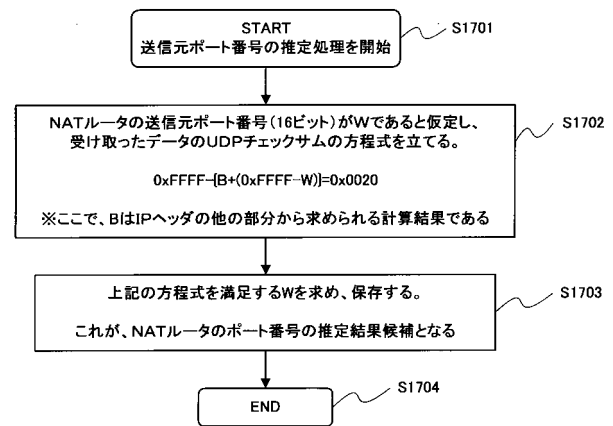
【図 1 5】



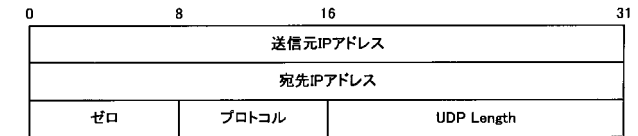
【図 16】



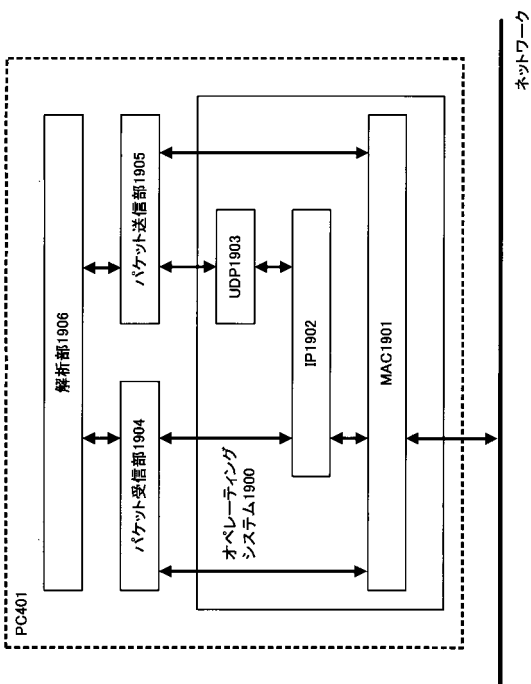
【図 17】



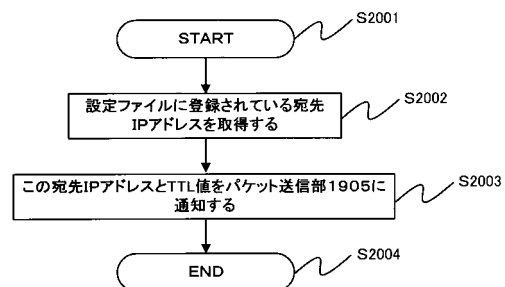
【図 18】



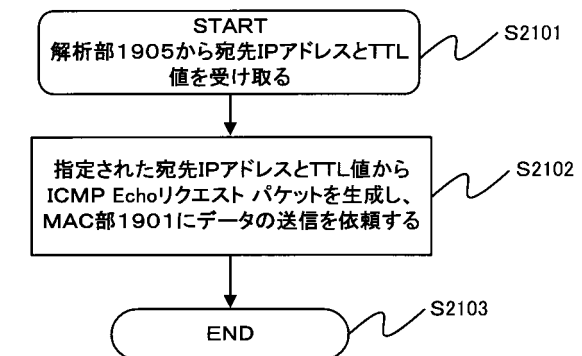
【図 19】



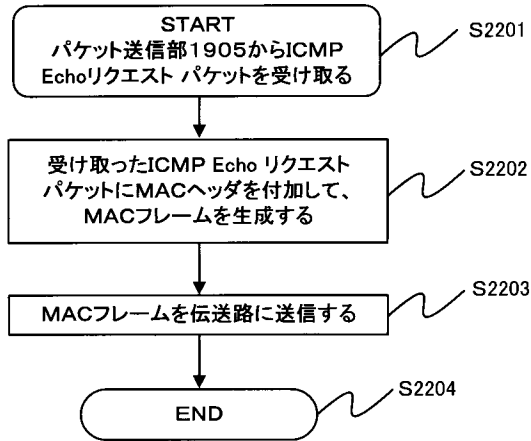
【図 20】



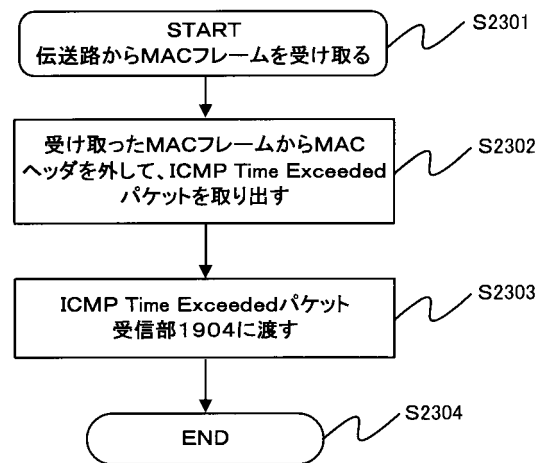
【図 21】



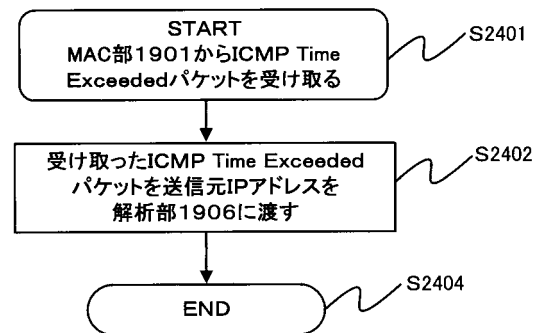
【図 2 2】



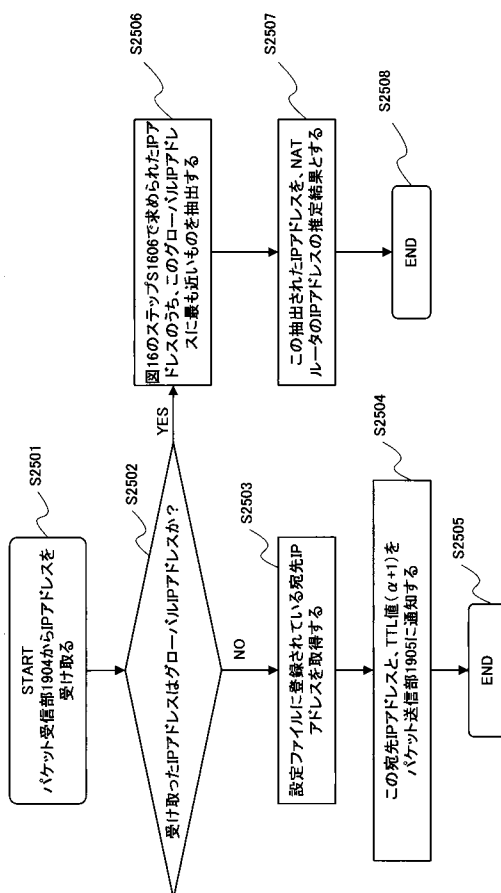
【図 2 3】



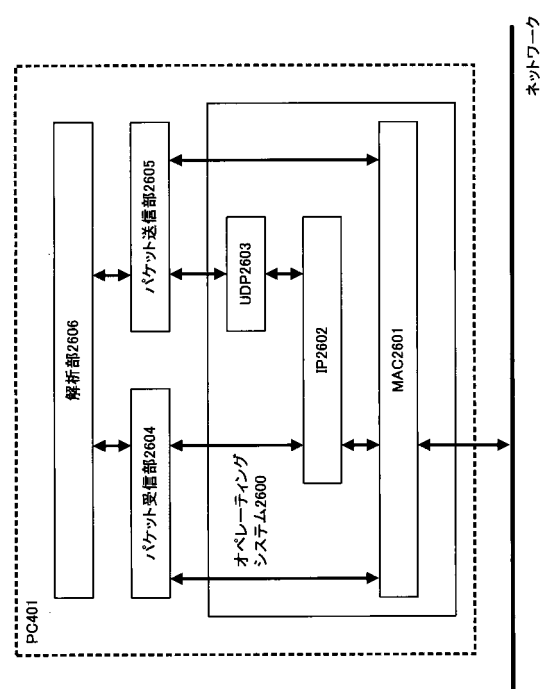
【図 2 4】



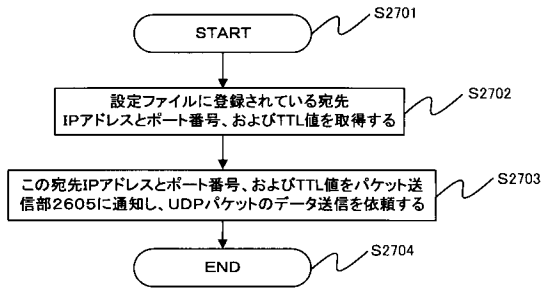
【図 2 5】



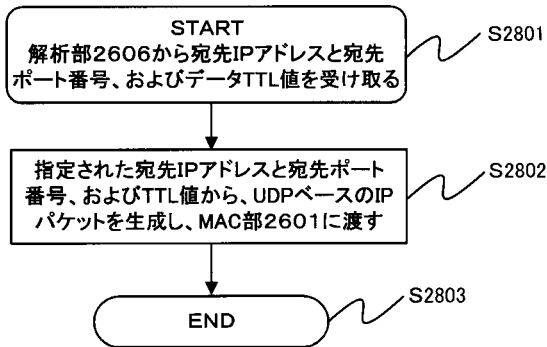
【図 2 6】



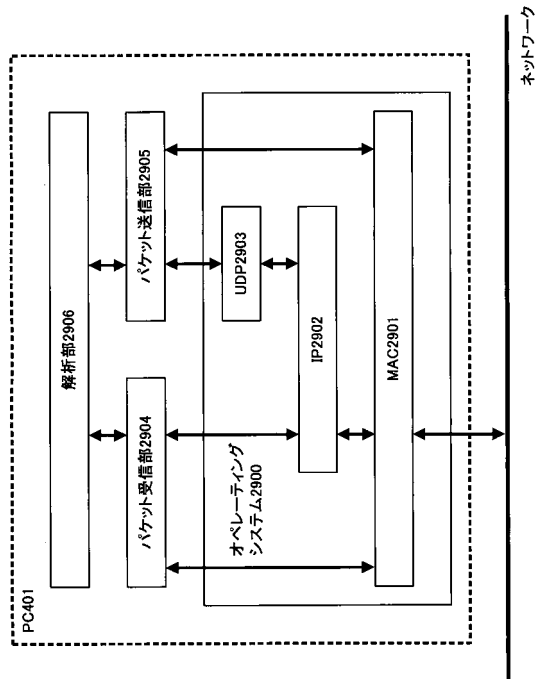
【図 27】



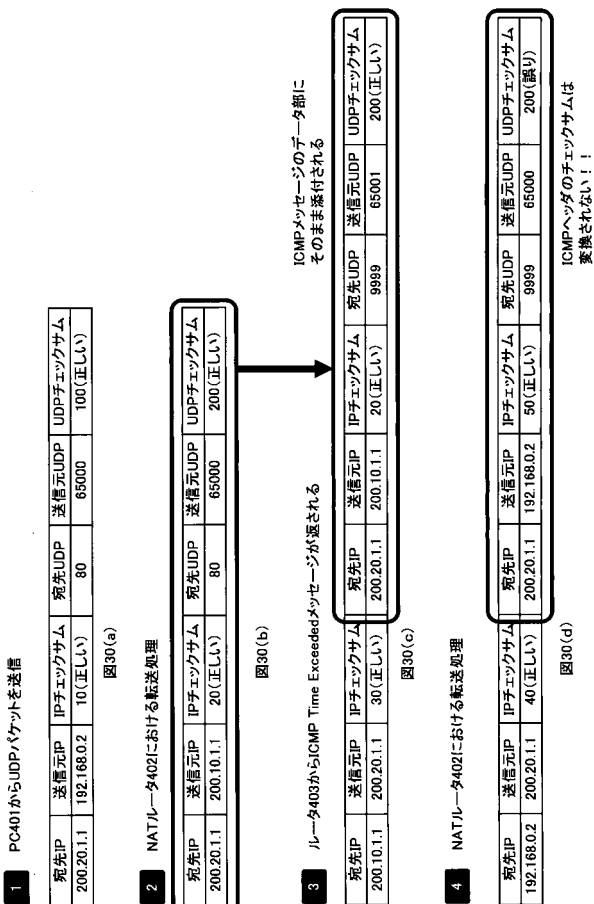
【図 28】



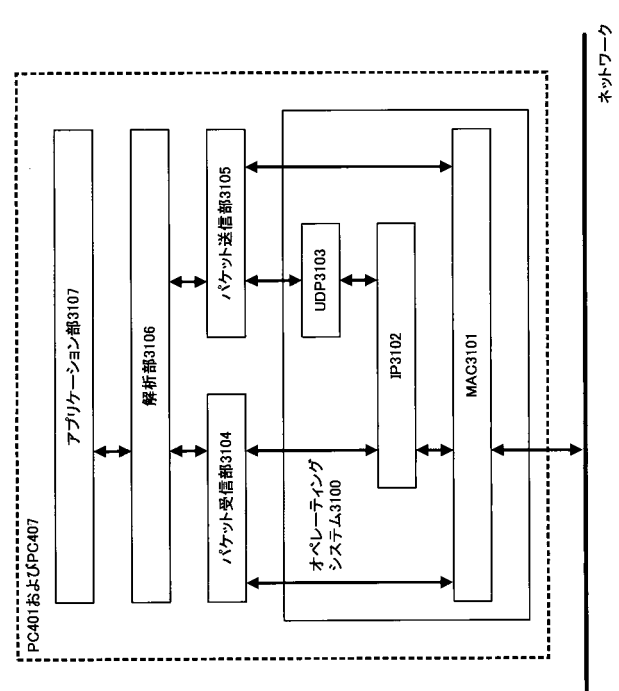
【図 29】



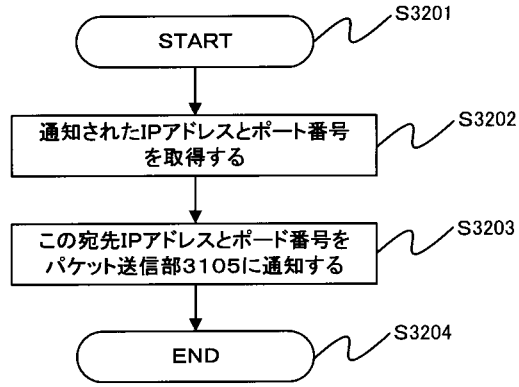
【図 30】



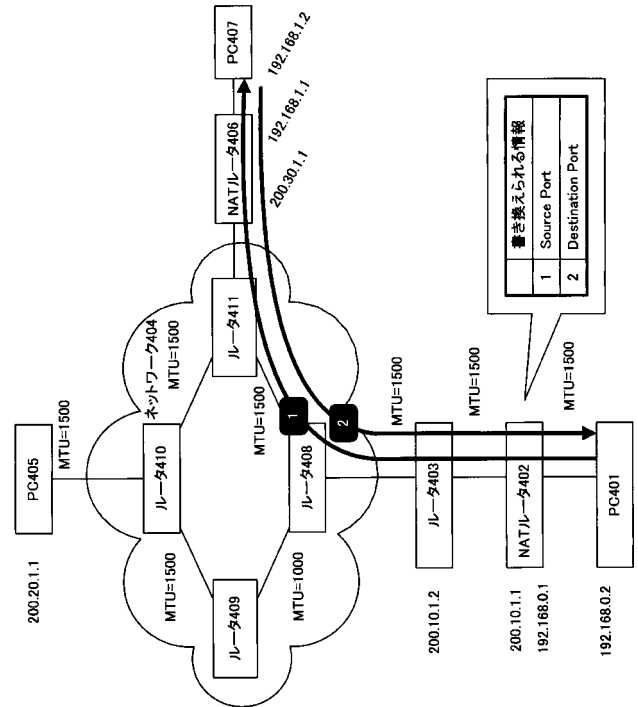
【図 31】



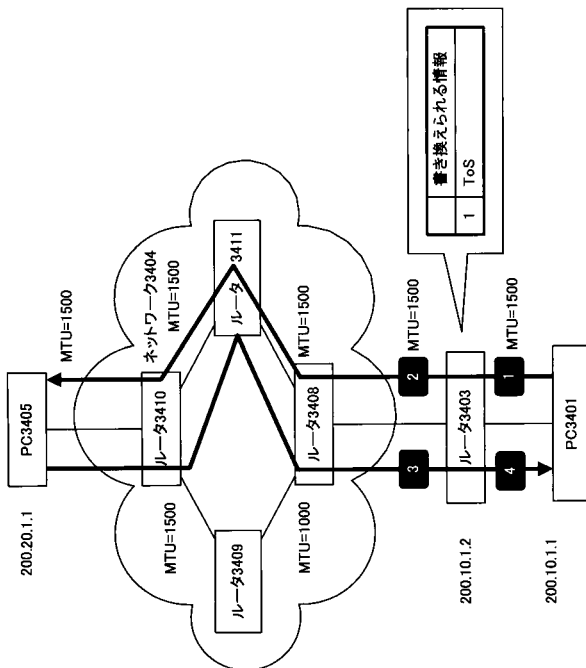
【図 3 2】



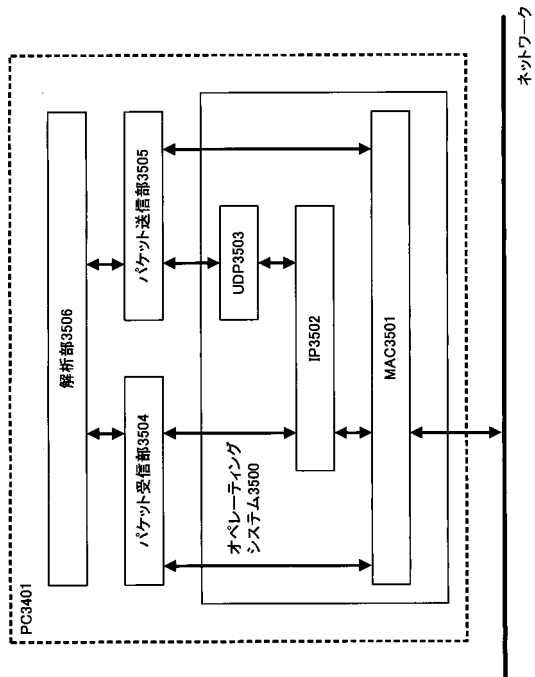
【図 3 3】



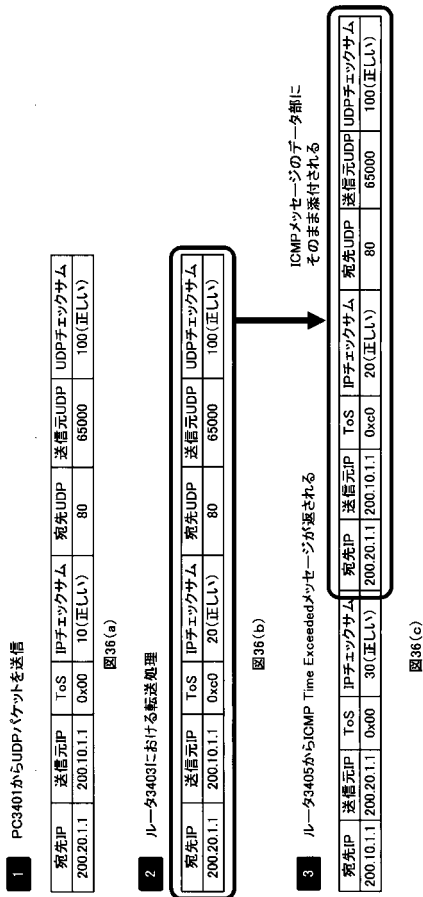
【図 3 4】



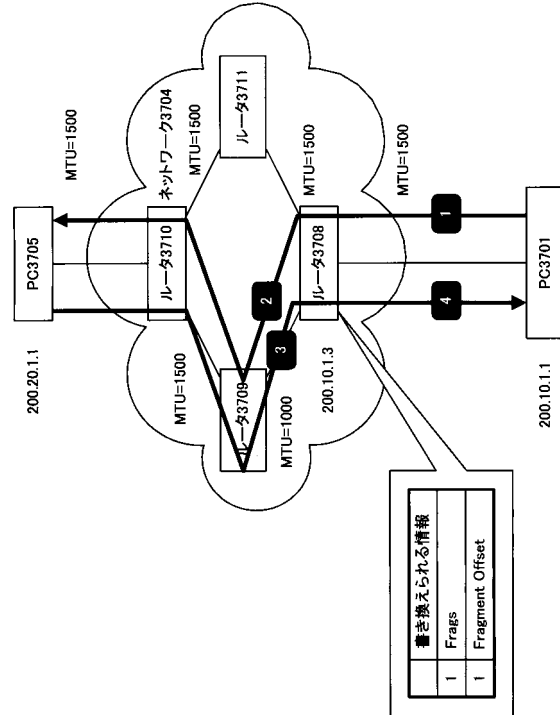
【図 3 5】



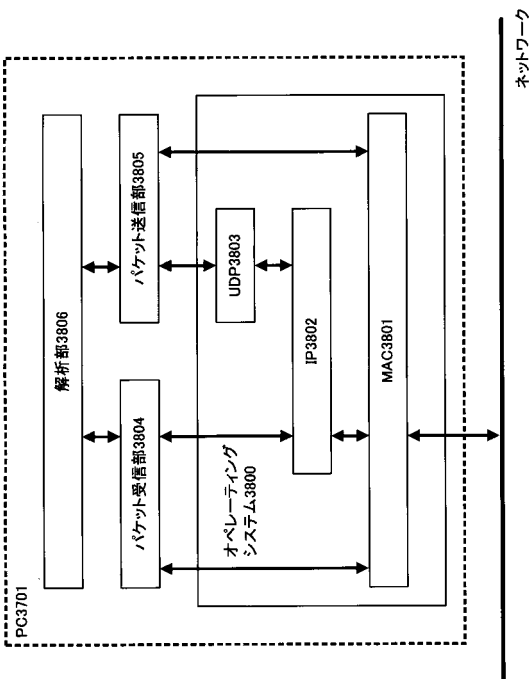
【図 36】



【図 37】



【図 38】



1 PC3701からUDPパケットを送信

宛先IP	送信元IP	Flags	Fragment Offset	IPチェックサム	宛先UDP	送信元UDP	UDPチェックサム	ペイロード
200.20.1.1	200.10.1.1	000	000	10(正しい)	80	65000	100(正しい)	1300byte

図39(a)

2 ルータ3708の転送処理

宛先IP	送信元IP	Flags	Fragment Offset	IPチェックサム	宛先UDP	送信元UDP	UDPチェックサム	ペイロード
200.20.1.1	200.10.1.1	001	000	20(正しい)	80	65000	100(正しい)	800byte

図39(b)

宛先IP	送信元IP	Flags	Fragment Offset	IPチェックサム	宛先UDP	送信元UDP	UDPチェックサム	ペイロード
200.20.1.1	200.10.1.1	000	100	30(正しい)	80	65000	100(正しい)	500byte

3 ルータ3709からICMPパケットが返される(Flagsの再変換なし)

宛先IP	送信元IP	Flags	Fragment Offset	IPチェックサム	宛先UDP	送信元UDP	UDPチェックサム	ペイロード
200.20.1.1	200.10.1.1	001	000	20(正しい)	80	65000	100(正しい)	800byte

図39(c)

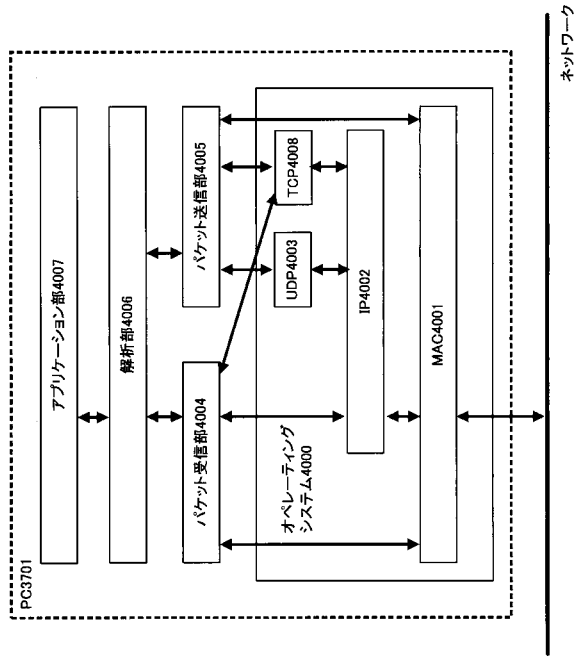
宛先IP	送信元IP	Flags	Fragment Offset	IPチェックサム	宛先UDP	送信元UDP	UDPチェックサム	ペイロード
200.20.1.1	200.10.1.1	000	100	30(正しい)	80	65000	100(正しい)	500byte

図39(d)

宛先IP	送信元IP	Flags	Fragment Offset	IPチェックサム	宛先UDP	送信元UDP	UDPチェックサム	ペイロード
200.10.1.1	200.20.1.1	000	100	20(正しい)	80	65000	100(正しい)	500byte

図39(e)

【図 40】



フロントページの続き

(72)発明者 高木 和男

東京都港区芝五丁目7番1号 日本電気株式会社内

(72)発明者 岩田 淳

東京都港区芝五丁目7番1号 日本電気株式会社内

Fターム(参考) 5K030 GA19 HA08 HD03 HD06 HD09 KA05 KA15 LB05 LE16