

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5335886号
(P5335886)

(45) 発行日 平成25年11月6日 (2013. 11. 6)

(24) 登録日 平成25年8月9日 (2013. 8. 9)

(51) Int. Cl.

F I

H 0 4 L 12/46 (2006. 01)

H 0 4 L 12/46

E

H 0 4 L 12/46

A

請求項の数 15 (全 17 頁)

(21) 出願番号 特願2011-500742 (P2011-500742)
 (86) (22) 出願日 平成21年3月20日 (2009. 3. 20)
 (65) 公表番号 特表2011-515945 (P2011-515945A)
 (43) 公表日 平成23年5月19日 (2011. 5. 19)
 (86) 国際出願番号 PCT/SE2009/050297
 (87) 国際公開番号 W02009/116948
 (87) 国際公開日 平成21年9月24日 (2009. 9. 24)
 審査請求日 平成24年2月20日 (2012. 2. 20)
 (31) 優先権主張番号 61/038, 192
 (32) 優先日 平成20年3月20日 (2008. 3. 20)
 (33) 優先権主張国 米国 (US)

(73) 特許権者 598036300
 テレフオンアクチーボラゲット エル エ
 ム エリクソン (パブル)
 スウェーデン国 ストックホルム エスー
 1 6 4 8 3
 (74) 代理人 100076428
 弁理士 大塚 康德
 (74) 代理人 100112508
 弁理士 高柳 司郎
 (74) 代理人 100115071
 弁理士 大塚 康弘
 (74) 代理人 100116894
 弁理士 木村 秀二
 (74) 代理人 100130409
 弁理士 下山 治

最終頁に続く

(54) 【発明の名称】 ローカル・ネットワーク間でデータ・パケットを通信するための方法および装置

(57) 【特許請求の範囲】

【請求項 1】

第 1 のローカル・ネットワーク内の第 1 の通信デバイス (D 1) と第 2 のローカル・ネットワーク内の第 2 の通信デバイス (D 2) との間でデータ・パケットの通信をできるようにする方法であり、前記第 1 のローカル・ネットワークおよび前記第 2 のローカル・ネットワーク内にあるデバイスに、前記第 1 のローカル・ネットワークおよび前記第 2 のローカル・ネットワーク内で潜在的に重複しているプライベート IP アドレスが用いられており、前記第 1 のローカル・ネットワークの第 1 のゲートウェイ (1 0 0) 内で実行されるところの方法であって、

前記第 1 のゲートウェイにおいて、ローカル・ネーム・サーバ・レコード (1 0 0 a) を、前記第 2 のローカル・ネットワークの第 2 のゲートウェイ (1 0 2) のドメイン名および IP アドレスで更新する工程 (3 0 0) であって、前記第 1 のゲートウェイおよび前記第 2 のゲートウェイの各々はローカル DNS 機能を有しているところの工程と、

前記第 2 の通信デバイスのホスト名を参照する発信 DNS 要求を前記第 1 の通信デバイスから受信する工程 (3 0 2) と、

前記第 2 のゲートウェイであるプライマリ DNS の前記 IP アドレスを、前記ホスト名内のドメイン名に基づいて前記ローカル・ネーム・サーバ・レコードから決定する工程 (3 0 4) と、

前記決定された IP アドレスを用いて、前記第 2 のゲートウェイに DNS 要求を転送する工程 (3 0 6) と、

10

20

前記第2のゲートウェイからDNS応答を受信し、前記第2の通信デバイスの現時点のプライベートIPアドレスを前記DNS応答から取得する工程(306)であって、前記現時点のプライベートIPアドレスが前記第2の通信デバイスに対して前記第2のローカル・ネットワーク内で用いられるところの工程と、

前記第2の通信デバイスの前記現時点のプライベートIPアドレスを、前記第2の通信デバイスに対して前記第1のローカル・ネットワーク内で用いられる修正プライベートIPアドレスに変換する工程(312)であって、前記修正プライベートIPアドレスは、前記第1のローカル・ネットワークと前記第2のローカル・ネットワークとの間のVPNトンネルに対して定義され、かつ、前記第1のローカル・ネットワーク内のデバイスに対して前記第1のローカル・ネットワークで用いられる内部IPアドレス空間から区別されているアドレス空間内にあるところの工程と、

前記第2の通信デバイスの前記現時点のプライベートIPアドレスを参照して、前記第1の通信デバイスにDNS応答を転送する工程(310)と、

前記第1の通信デバイスから、前記第2の通信デバイスの前記修正プライベートIPアドレスを宛先アドレスとして含むデータ・パケットを受信する工程と、

前記データ・パケットを、前記宛先アドレスを変換することなく前記第2のゲートウェイに転送する工程と

を有することを特徴とする方法。

【請求項2】

前記修正プライベートIPアドレスは、第2のオクテットまたは第3のオクテット内の一意的な数字が前記第2のローカル・ネットワークを表わすように配分されているIPv4ベースのアドレスであることを特徴とする

請求項1に記載の方法。

【請求項3】

前記第2のゲートウェイからの前記DNS応答はさらに、前記第2の通信デバイスの前記現時点のプライベートIPアドレスに対する有効期間を決定するタイムアウト・パラメータを含むことを特徴とする請求項1または2に記載の方法。

【請求項4】

前記第2の通信デバイスの前記現時点のプライベートIPアドレスが前記タイムアウト・パラメータに従って前記第1のゲートウェイ内で一時的にキャッシュされることを特徴とする請求項3に記載の方法。

【請求項5】

前記ホスト名に前記第2の通信デバイスを識別する第1の部分および前記ドメイン名を持つ第2の部分を含むことを特徴とする請求項1乃至4のいずれか一項に記載の方法。

【請求項6】

前記VPNトンネルが前記第1のゲートウェイと前記第2のゲートウェイ(100、102)との間でデータ・パケット通信のために確立されており、パブリックIPアドレスが各ゲートウェイに割り当てられていることを特徴とする請求項1乃至5のいずれか一項に記載の方法。

【請求項7】

第1のローカル・ネットワークに在圏する第1のゲートウェイ内の装置(100、400)であり、前記第1のローカル・ネットワーク内の第1の通信デバイス(D1)と第2のローカル・ネットワーク内の第2の通信デバイス(D2)との間でデータ・パケットの通信を可能にでき、前記第1のローカル・ネットワークおよび前記第2のローカル・ネットワーク内にあるデバイスに、前記第1のローカル・ネットワークおよび前記第2のローカル・ネットワーク内で潜在的に重複しているプライベートIPアドレスが用いられるところの装置であって、

ローカル・ネーム・サーバ・レコード(400b)を前記第2のローカル・ネットワークの第2のゲートウェイ(102)のドメイン名およびIPアドレスで更新するように構成されたネーム・サーバ・レコード・マネージャ(400a)であって、前記第1のゲ

10

20

30

40

50

トウェイおよび前記第2のゲートウェイの各々がローカルDNS機能を有しているところの
のネーム・サーバ・レコード・マネージャと、

前記第2の通信デバイスのホスト名を参照する発信DNS要求を前記第1の通信デバイス
から受信するように構成された内部通信部(400c)と、

前記第2のゲートウェイであるプライマリDNSの前記IPアドレスを、前記ホスト名
内のドメイン名に基づいて前記ローカル・ネーム・サーバ・レコードから決定するように
構成されたDNS決定部(400d)と、

前記決定されたIPアドレスを用いて、前記第2のゲートウェイにDNS要求を送信し、
前記第2のゲートウェイからのDNS応答で前記第2の通信デバイスの現時点のプライ
ベートIPアドレスを取得するように構成された外部通信部(400e)であって、前記
現時点のプライベートIPアドレスが前記第2の通信デバイスに対して前記第2のローカ
ル・ネットワーク内で用いられるところの外部通信部(400e)と、

前記現時点のプライベートIPアドレスを、前記第2の通信デバイスに対して前記第1
のローカル・ネットワーク内で用いられる修正プライベートIPアドレスに変換するIP
アドレス変換部(400f)であって、前記修正プライベートIPアドレスは、前記第1
のローカル・ネットワークと前記第2のローカル・ネットワークとの間のVPNトンネル
に対して定義され、かつ、前記第1のローカル・ネットワーク内のデバイスに対して前記
第1のローカル・ネットワークで用いられる内部IPアドレス空間から区別されているア
ドレス空間内にあるところのIPアドレス変換部と

を備え、

前記内部通信部(400c)は、前記第2の通信デバイスの前記修正プライベートIP
アドレスを参照して、前記DNS応答を前記第1の通信デバイスに転送し、前記第1の通
信デバイスから、前記第2の通信デバイスの前記修正プライベートIPアドレスを宛先ア
ドレスとして含むデータ・パケットを受信し、

前記外部通信部はさらに、前記データ・パケットを、前記宛先アドレスを変換すること
なく前記第2のゲートウェイに転送するようにさらに構成されることを特徴とする装置。

【請求項8】

前記修正プライベートIPアドレスは、第2オクテットまたは第2オクテット内の一意
的な数字が前記第2のローカル・ネットワークを表わすように配分されているIPv4ベ
ースのアドレスであることを特徴とする請求項7に記載の装置。

【請求項9】

前記第2のゲートウェイからの前記DNS応答はさらに前記第2の通信デバイスの前記
現時点のプライベートIPアドレスに対する有効期間を決定するタイムアウト・パラメ
ータを含むことを特徴とする請求項7または8に記載の装置。

【請求項10】

前記タイムアウト・パラメータに従って前記現時点のプライベートIPアドレスを一時的
にキャッシュするように構成されたことを特徴とする請求項9に記載の装置。

【請求項11】

前記ホスト名は前記第2の通信デバイスを識別する第1の部分および前記ドメイン名を
持つ第2の部分を含むことを特徴とする請求項7乃至10のいずれか一項に記載の装置。

【請求項12】

前記VPNトンネルが第1のゲートウェイと第2のゲートウェイ(100、102)と
の間のデータ・パケット通信のために確立されており、かつパブリックIPアドレスが各
ゲートウェイに割り当てられていることを特徴とする請求項7乃至11のいずれか一項に
記載の装置。

【請求項13】

第1のローカル・ネットワークに在圏する第1のゲートウェイ(A)用に構成され、前
記第1のローカル・ネットワーク内の第1の通信デバイス(D1)と第2のローカル・ネ
ットワーク内の第2の通信デバイス(D2)との間でデータ・パケットの通信を可能にで
きるコンピュータ・プログラム(402)であって、前記第1のローカル・ネットワーク

および前記第2のローカル・ネットワーク内にあるデバイスに、前記第1のローカル・ネットワークおよび前記第2のローカル・ネットワーク内で潜在的に重複しているプライベートIPアドレスが用いられており、前記コンピュータ・プログラムは、前記第1のゲートウェイ上で実行される場合、前記第1のゲートウェイに、

ローカル・ネーム・サーバ・レコード(100a)を前記第2のローカル・ネットワークの第2のゲートウェイ(102)のドメイン名およびIPアドレスで更新させ(300)、前記第1のゲートウェイおよび前記第2のゲートウェイの各々がローカルDNS機能を有しており、

前記第2の通信デバイスのホスト名を参照する発信DNS要求を前記第1の通信デバイスから受信させ(302)、

10

前記第2のゲートウェイであるプライマリDNSの前記IPアドレスを、前記ホスト名内のドメイン名に基づいて前記ローカル・ネーム・サーバ・レコードから決定させ(304)、

前記決定されたIPアドレスを用いてDNS要求を前記第2のゲートウェイに送信させ(306)、

前記第2のゲートウェイからのDNS応答内の、前記第2の通信デバイスの現時点でのプライベートIPアドレスを取得させ、前記取得したプライベートIPアドレスが前記第2の通信デバイスに対して前記第2のローカル・ネットワーク内で用いられ、

前記現時点のプライベートIPアドレスを前記第2の通信デバイスに対して前記第1のローカル・ネットワーク内で用いられる修正プライベートIPアドレスに変換させ(312)、前記修正プライベートIPアドレスは、前記第1のローカル・ネットワークと前記第2のローカル・ネットワークとの間のVPNトンネルに対して定義され、かつ、前記第1のローカル・ネットワーク内のデバイスに対して前記第1のローカル・ネットワークで用いられる内部IPアドレス空間から区別されているアドレス空間内にあり、

20

前記第2の通信デバイスの前記現時点のプライベートIPアドレスを参照して、前記DNS応答を前記第1の通信デバイスに転送させ、

前記第1の通信デバイスから、前記第2の通信デバイスの前記修正プライベートIPアドレスを宛先アドレスとして含むデータ・パケットを受信させ、

前記データ・パケットを、前記宛先アドレスを変換することなく前記第2のゲートウェイに転送させる(310)ためのコンピュータ・プログラム。

30

【請求項14】

請求項13に記載のコンピュータ・プログラムが格納されたコンピュータで読み取り可能な記憶媒体。

【請求項15】

第1のローカル・ネットワーク内の第1の通信デバイス(D1)と第2のローカル・ネットワーク内の第2の通信デバイス(D2)との間でデータ・パケットの通信をできるようにする方法であり、前記第1のローカル・ネットワークおよび前記第2のローカル・ネットワーク内にあるデバイスに、前記第1のローカル・ネットワークおよび前記第2のローカル・ネットワーク内で潜在的に重複しているプライベートIPアドレスが用いられており、前記第2のローカル・ネットワークの第2のゲートウェイ(102)内で実行されるところの方法であって、

40

前記第2の通信デバイスのホスト名を含むDNS要求を前記第1のゲートウェイから受信する工程と

前記第2のゲートウェイにより、前記第2の通信デバイスの現時点のプライベートIPアドレスを含むDNS応答を前記第1のゲートウェイに送信する工程であって、前記現時点のプライベートIPアドレスは前記第2のローカル・ネットワーク内で前記第2の通信デバイスに対して用いられるところの工程と、

前記第2のローカル・ネットワーク内では無効なIPアドレスである宛先IPアドレスを含む、前記第2の通信デバイスに向けられたデータ・パケットを受信する工程と、

前記無効なIPアドレスを、前記第2の通信デバイスの前記現時点のプライベートIP

50

アドレスに変換する工程と、

前記データ・パケットを、前記第2の通信デバイスの前記現時点のプライベートIPアドレスを用いて前記第2の通信デバイスに転送する工程と

を有することを特徴とする方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、広く、重複するアドレス空間を用いることができるような異なるローカル・ネットワーク内にある通信デバイス間で、データ・パケットの通信を可能にするための方法および装置に関する。

【背景技術】

【0002】

IP（インターネット・プロトコル）ネットワークを介して異なる当事者間でデジタル・コード化した情報のパケット・ベースの伝送は、様々な通信サービス、たとえば電子メール・メッセージング、ファイル転送、インターネット・ブラウジング、音声およびテレビ電話、コンテンツ・ストリーミング、ゲームなどに用いられる。デジタル・コード化した情報は、送信側でデータ・パケットに整えられ、それから送信側が伝送パスを介して宛先の受信側に向けてパケットを送信する。データ・パケットは、基本的に、ペイロード・データが入っているデータ・フィールドおよび、受信側の宛先アドレスおよび送信側の発信元アドレスが入っているヘッダ・フィールドで構成される。

【0003】

データ・パケットは異なるローカル・ネットワークまたは私設網内にある様々な通信デバイス間で通信される場合があり、各ネットワークは、ネットワーク外の発信元からデバイスへのパケットを受信するために、そしてまたデバイスからネットワーク外の宛先にパケットを送るために、ゲートウェイを採用している。異なるローカル・ネットワーク内のそのようなデバイス間で通信されるパケットは、それからパブリックIPネットワーク、たとえばインターネットを介してそれぞれのネットワーク・ゲートウェイ間で運ばれる。

【0004】

本明細書では、用語“ローカル・ネットワーク”は、広く、内部のプライベート・アドレッシングを用いる任意のネットワークおよび、ネットワーク外の当事者との外部通信のためのゲートウェイを表わすのに用いられる。共通的に用いられる他の等価な用語には、“プライベート・ネットワーク（private network）”、“住居ネットワーク（residential network）”、“ホームネットワーク（home network）”を含む。さらに、“ゲートウェイ”は、ローカル・ネットワーク内のデバイスとネットワーク外のエンティティとの間でデータ・パケットを通信できる、住居ゲートウェイ（RGW）、IPルータまたは他の任意の種類のネットワーク・エンティティであることができよう。用語“デバイス”は、さらに本明細書では、他のデバイスとデータ・パケットを通信できる任意の端末、コンピュータ、電話またはサーバを表わすのに用いられる。

【0005】

パブリックIPネットワークを介しての通信は、通常、データ保護およびプライバシーに関して“安全でない”と見なされているので、パケット内のペイロード・データおよび他の機密情報を不法な傍受または改ざんから防護することが望ましい。この課題を克服する1つの方法は、パブリックIPネットワークを介して通信する当事者間にVPN（仮想プライベート・ネットワーク）を確立することである。

【0006】

VPNは、基本的には、端末とサーバとの間でデータ・パケットを転送するための、パブリックIPネットワークを通る暗号化されたトンネルと見なされることができる。VPNは、通例、パブリック・インターネットを通る安全な通信のために用いられる。様々なQoS（サービス品質）パラメータは、VPN顧客とVPNサービス提供者との間で、VPNが期待された振舞いを達成するように定義される場合がある。通常、VPNは、

10

20

30

40

50

ユーザ・コミュニティ内の２つ以上の通信デバイスが、ある点で当該コミュニティに関係している一定の機能を提供するために、確立される場合がある。

【 0 0 0 7 】

インターネットの人気および使用が増大するにつれて、インターネット上でプライベート・ネットワークおよびローカル・ネットワークを同様に拡大することが益々望ましくなる。たとえば、ローカル・ネットワークを有する多くの会社および企業は、それらの従業員が遠隔でローカル・ネットワークにアクセスできるようにするために、自身のVPNを確立する。

【 0 0 0 8 】

VPNは、このようにして、公衆ネットワーク・インフラストラクチャ上で走行する論理的および“分散された(distributed)”ローカル・ネットワークと見なされることができる。これらのネットワークは、データに関するトラヒックの秘匿性、トラヒック分離およびQoSを得るために広範な技術を使用する。VPNは、イントラネット、インターネットまたはサービス提供者のネットワーク・インフラストラクチャ上で確立できる。一般に、“アクセスVPN”および“LAN(ローカル・エリア・ネットワーク)対LAN VPN”と呼ばれる２つの基本的な種類の利用できるVPNサービスがあり、アクセスVPNは遠隔アクセスに用いられ、そしてLAN対LAN VPNは、異なるローカル・ネットワークがイントラネットまたはエクストラネットを提供するために相互接続される場合に用いられる。

【 0 0 0 9 】

ローカル・ネットワーク内のデバイスは、通常、プライベート・アドレス空間からのIPアドレスを用いていて、そのようなプライベートIPアドレスは、ローカルな管理者または同様なものにより内部的にデバイスに自由に割り当てできる。用いられるプライベートIPアドレスは、このようにして基本的には他のユーザには、明確に告げられない限り知られず、そしてまた、パブリックIPアドレスを加入者に提供するインターネット・サービス提供者にも知られない。

【 0 0 1 0 】

現今、これらのプライベート・アドレス空間は、一般に複数のローカル・ネットワークで再使用され、そしてしたがって、異なるローカル・ネットワークによりそれらのデバイスに用いられるプライベートIPアドレスは、特によく用いられるIPv4ベースのプライベート・アドレス空間では、互いに重複する場合がある。たとえば、１つのローカル・ネットワーク内のデバイスにより用いられるプライベートIPアドレスは、別の対向するローカル・ネットワーク内の別のデバイスにより用いられるものと同じアドレスである場合があり、通信されるデータ・パケットにおける曖昧なアドレッシングをもたらす。そのような重複するまたは再使用されるプライベート・アドレス空間および、デバイスへのローカルな割り当てのために、プライベートIPアドレスは、パブリック・インターネットで効率よく“ルーティングできない(unroutable)”し、そしてプライベートIPアドレスがローカル・ネットワーク領域外でのルーティングには用いられないので、パブリックIPアドレスは、したがってまた、パケット内で用いられなければならない。

【 発明の概要 】

【 発明が解決しようとする課題 】

【 0 0 1 1 】

残っている課題は、しかしながら、１つのローカル・ネットワーク内でパケットを送るデバイスは、対向するローカル・ネットワーク内の受信デバイスのプライベートIPアドレスを含まなければならないということであり、これには送信デバイスに、受信デバイスを適切に識別するための何らかの適当な機能が必要である。さらに、動的なアドレス割り当てがローカル・ネットワーク内のデバイスに用いられると、特定のデバイスのプライベートIPアドレスは、随時変えられるであろう。このようにして、発信パケット内に適切な宛先アドレスを提供するために、対向するネットワークでのそのようなアドレス変更についての知識を、ローカル・デバイスで保持することはかなり困難でありえよう。

【課題を解決するための手段】

【0012】

本発明の目的は、上記で概略した課題の少なくとも一部に対処することである。第1のローカル・ネットワーク内の第1のデバイスから第2のローカル・ネットワーク内の第2のデバイスにデータ・パケットを通信するために、送信デバイスまたは送信ユーザが、どのプライベートIPアドレスが現時点で第2のデバイスに対して有効であるかを知っていることを必要としないで、宛先アドレスを得るためのメカニズムを提供することが、また目的の1つである。

【0013】

様々な態様に従って、第1のローカル・ネットワーク内の第1の通信デバイスと第2のローカル・ネットワーク内の第2の通信デバイスとの間で、データ・パケットの通信を可能にするために、方法、ゲートウェイ内の装置、コンピュータ・プログラムおよびコンピュータ・プログラム製品が提供されていて、プライベートIPアドレスが、第1のローカル・ネットワークおよび第2のローカル・ネットワークにあるデバイスに用いられている。

10

【0014】

1つの態様では、第1のゲートウェイにおいて、第1のゲートウェイ内のローカル・ネーム・サーバ・レコードが、第2のネットワークの第2のゲートウェイのドメイン名およびIPアドレスで更新される方法が提供され、各ゲートウェイはローカルDNS機能を有している。第1のゲートウェイが、第2のデバイスのホスト名を参照する発信DNS要求を、第1のデバイスから受信する場合、第2のゲートウェイであるプライマリDNSのIPアドレスが、ホスト名内のドメイン名に基づいてローカル・ネーム・サーバ・レコードから決定される。DNS要求はそれから、第2のゲートウェイからのDNS応答で第2のデバイスの現時点のプライベートIPアドレスを得るために、決定されたIPアドレスを用いて第2のゲートウェイに送信される。DNS応答はまた、第2のデバイスの現時点のプライベートIPアドレスを参照して、第1のデバイスに転送される。

20

【0015】

別の態様では、第1のゲートウェイにおいて、第1のローカル・ネットワークを在圏とする装置が提供される。ゲートウェイ装置は、ローカル・ネーム・サーバ・レコードを第2のネットワークの第2のゲートウェイのドメイン名およびIPアドレスで更新するように構成されたネーム・サーバ・レコード・マネージャを備えていて、第1のゲートウェイおよび第2のゲートウェイの各々は、ローカルDNS機能を有している。ゲートウェイ装置はまた、第2のデバイスのホスト名を参照する発信DNS要求を第1のデバイスから受信するように構成された内部通信部を備える。ゲートウェイ装置はまた、第2のゲートウェイであるプライマリDNSのIPアドレスを、ホスト名内のドメイン名に基づいてローカル・ネーム・サーバ・レコードから決定するように構成されたDNS決定部を備える。

30

【0016】

ゲートウェイ装置はまた、決定されたIPアドレスを用いて、DNS要求を第2のゲートウェイに送信するように、そして第2のゲートウェイからのDNS応答で第2のデバイスの現時点のプライベートIPアドレスを得るように構成された外部通信部を備える。内部通信部はさらに、第2のデバイスの現時点のプライベートIPアドレスを参照するDNS応答を第1のデバイスに転送するように構成される。

40

【0017】

さらに別の態様では、コンピュータ・プログラムは、第1のローカル・ネットワークを在圏とする第1のゲートウェイ用に構成される。コンピュータ・プログラムは、第1のゲートウェイで実行される場合、第1のゲートウェイに、ローカル・ネーム・サーバ・レコードを第2のネットワークの第2のゲートウェイのドメイン名およびIPアドレスで更新させるコード手段を備えており、第1のゲートウェイおよび第2のゲートウェイの各々は、ローカルDNS機能を有する。前記コード手段はまた、第1のゲートウェイに、第2のデバイスのホスト名を参照する発信DNS要求を第1のデバイスから受信させ、そして第

50

2のゲートウェイであるプライマリDNSのIPアドレスを、ホスト名内のドメイン名に基づいてローカル・ネーム・サーバ・レコードから決定させる。

【0018】

コード手段はまた、第1のゲートウェイに、決定されたIPアドレスを用いて、DNS要求を第2のゲートウェイに送信させ、第2のゲートウェイからのDNS応答で第2のデバイスの現時点のプライベートIPアドレスを得させ、そして第2のデバイスの現時点のプライベートIPアドレスを参照して、DNS応答を第1のデバイスに転送させる。

【0019】

さらに別の態様では、上記コンピュータ・プログラムが格納されるコンピュータで読み取り可能な記憶媒体を備える。

10

【0020】

上記方法の各々、ゲートウェイ装置、コンピュータ・プログラムおよびコンピュータ・プログラム・製品はさらに、以下の実施形態に従って構成される特徴および機能を備える場合がある。

【0021】

たとえば、第1のローカル・ネットワークおよび第2のローカル・ネットワーク内のデバイスに用いられるプライベートIPアドレスが潜在的に重複しており、そして得られたプライベートIPアドレスが第2のデバイスに対して第2のネットワーク内で用いられると、得られたプライベートIPアドレスは、第2のデバイスに対して第1のネットワーク内で用いられる修正プライベートIPアドレスに変換される。修正プライベートIPアドレスは、その場合、第1のネットワークと第2のネットワークとの間のVPNトンネルに対して定義され、そして第1のローカル・ネットワーク内のデバイスに対して第1のローカル・ネットワーク内で用いられる内部IPアドレス空間と区別される、すなわち重複しないアドレス空間内にある。DNS応答は、その場合、修正IPアドレスを備える場合がある。

20

【0022】

修正プライベートIPアドレスは、第2のオクテットまたは第3のオクテット内の一意的な数字が第2のローカル・ネットワークを表わすのに配分されている、IPv4ベースのアドレスである場合がある。

【0023】

第2のゲートウェイからのDNS応答にはさらに、第2のデバイスの現時点のプライベートIPアドレスに対する有効期間を決定するタイムアウト・パラメータが入っている場合がある。かかる場合、第2のデバイスの現時点のプライベートIPアドレスは、タイムアウト・パラメータに従って、第1のゲートウェイ内で一時的にキャッシュされる場合がある。

30

【0024】

ホスト名には、第2のデバイスを識別する第1の部分および、ドメイン名を持つ第2の部分が含まれる場合がある。さらに、VPNトンネルは、第1のゲートウェイと第2のゲートウェイとの間でのデータ・パケット通信に対して確立されている場合があり、そしてパブリックIPアドレスが各ゲートウェイに割り当てられている場合がある。

40

【0025】

本発明のさらに見込まれる特徴および恩恵が、以下で詳細な明細書から明らかになるであろう。

【0026】

本発明は、これから典型的な実施形態によって、そして添付の図面を参照してより詳細に説明することとする。

【図面の簡単な説明】

【0027】

【図1】図1は、一部の典型的な実施形態に従って、2つの異なるローカル・ネットワークにわたってデータ・パケットの通信を可能にするためのシナリオおよび手順を説明する

50

概略ブロック図である。

【図2】図2は、さらなる典型的な実施形態に従って、対向するローカル・ネットワークにおける宛先デバイスの有益なIPアドレスがどのようにして得ることができるかを説明する信号図である。

【図3】図3は、さらに別の実施形態に従って、対向するローカル・ネットワーク内の2つのデバイス間でデータ・パケットの通信を可能にするための手順を説明するフロー図である。

【図4】図4は、さらなる典型的な実施形態に従って、ローカルDNS機能を装備したネットワーク・ゲートウェイをより詳細に説明する概略ブロック図である。

【発明を実施するための形態】

10

【0028】

本発明は、第1のローカル・ネットワーク内の第1のデバイスから第2のローカル・ネットワーク内の第2のデバイスにデータ・パケットを通信するために、送信デバイスまたは送信ユーザが、どのプライベートIPアドレスが現時点で第2のデバイスに有効であるかを知っていることを必要とせずに、有益な宛先アドレスを得るためのメカニズムを提供する。このメカニズムは、たとえば、ネットワーク内でパケットの一義的なアドレス指定を保証するためにアドレス変換を必要とする場合がある第1のネットワークおよび第2のネットワークで、潜在的に重複するアドレス空間が用いられる場合、そして特に、個々のデバイスが自身のアドレスを頻繁に変えるような動的ベースで、プライベートIPアドレスがローカル・デバイスに割り当てられる場合に有益である。

20

【0029】

この解決策では、第1のデバイスは簡単に、発信DNS要求で第2のデバイスのホスト名を参照でき、DNS要求は、それから第1のネットワークの第1のゲートウェイから第2のネットワークの第2のゲートウェイに送信され、各ゲートウェイは、DNS要求を処理するためのローカルDNS機能を有している。第1のゲートウェイは、それから、第2のネットワークで用いられる第2のデバイスの現時点で有効なプライベートIPアドレスの入っているDNS応答を第2のゲートウェイから受信し、そして当該アドレスを参照しているDNS応答はまた、第1のデバイスに転送される。それにより、第1のデバイスは、パケットのヘッダ・フィールド内の宛先アドレスとして第2のデバイスの現時点で有効なプライベートIPアドレスを用いて、データ・パケットを第2のデバイスに伝えることができる。

30

【0030】

DNS応答内のIPアドレスは、このようにして第2のデバイスに対して第2のネットワーク内で用いられ、そしてまた、第2のネットワーク内で用いられるアドレス空間が第1のネットワーク内で用いられるアドレス空間と重複しないことが分かっていると、第1のネットワーク内で用いられることができる。かかる場合、第1のデバイスへのDNS応答には、受信したIPアドレスを“そのまま(as is)”含む。

【0031】

他方、潜在的に重複するアドレス空間が第1のローカル・ネットワークおよび第2のローカル・ネットワーク内のデバイスに用いられていると、第1のゲートウェイは、受信したプライベートIPアドレスを、第2のデバイスに対して第1のネットワーク内で用いられるプライベートIPアドレスに好適に変換し、そして変換されたプライベートIPアドレスは、第1のネットワーク内のローカル・デバイスに用いられるプライベートIPアドレス空間と区別され、すなわち重複しない。かかる場合、第1のデバイスへのDNS応答には、変換されたIPアドレスを含む。

40

【0032】

上記がどのようにして成し遂げられることができるかの例は、図1に示す通信シナリオを参照してこれから説明することとする。第1のネットワークAおよび第2のネットワークBをそれぞれ在圏とする、第1のゲートウェイ100および第2のゲートウェイ102が示されていて、複数のデバイスが、ネットワークA内の第1のデバイスD1およびネッ

50

トワークB内の第2のデバイスD2を含めて存在している。プライベート・アドレス空間が、各々のローカル・ネットワークA、ローカル・ネットワークB内で、デバイスの内部通信のために用いられると仮定する。この例では、2つのネットワーク内で用いられるプライベートIPアドレス空間は、そのようなアドレス空間が一般に数多くのローカル・ネットワークで広く再使用されることが多いので、お互いに潜在的に重複する場合がある。

【0033】

各々のゲートウェイ100、ゲートウェイ102は、以下で説明するようにDNS要求を処理するためのDNS機能を装備している。ネットワークAのユーザは、ネットワークBとの通信ができると基本的に決めていると仮定する。第1の工程1:1は、ローカルNS(ネーム・サーバ)レコード100aが第1のゲートウェイ100内に格納され、または“更新され”、そして第2のゲートウェイ102のドメイン名およびIPアドレスを含むことを概略的に説明する。たとえば、ローカル・ネットワークAおよびローカル・ネットワークBのユーザは、インターネットのようなパブリックIPネットワークを介して対向するネットワーク内のデバイス間でデータ・パケットの“安全な(safe)”通信ができるように、ネットワーク間にVPNトンネルを確立することに同意している場合がある。工程1:1はその場合、VPNトンネルによる通信に備えてなされるであろう。

【0034】

その後のある時点で、デバイスD1のユーザは、デバイスD2のユーザと通信することを望み、そして本解決策では、デバイスD2のIPアドレスがユーザ/デバイスD1に知られている必要はない。D1のユーザは、デバイスD1からDNS要求をかけるのにデバイスD2のホスト名を単純に入力できる。次の工程1:2では、デバイスD1はこれのようにして、デバイスD2のホスト名を参照して第1のゲートウェイ100にDNS要求を送り、ホスト名には第2のデバイスを識別する第1の部分および、第2のゲートウェイ102およびネットワークBを識別するドメイン名を持つ第2の部分を含む。

【0035】

続く工程1:3では、ゲートウェイ100は、当該ドメイン名の、この場合は第2のゲートウェイ102である、いわゆる“プライマリDNS”のIPアドレスを決定するためにNSレコード100aを調べる。このIPアドレスは、工程1:1でNSレコード100aに格納されていて、そしてこのようにしてそこから読み出すことができる。ゲートウェイ100はそれから、さらなる工程1:4で、決定されたIPアドレスを用いて、そしてデバイスD2のホスト名を参照して、別のDNS要求を第2のゲートウェイ102に送る。ゲートウェイ102はそれから、次の工程1:5で、第2のデバイスD2に対して現時点で有効であるプライベートIPアドレスの入っているDNS応答で返信する。

【0036】

この時点で、種々の選択肢が、状況に応じて可能である。ローカル・ネットワークAおよびローカル・ネットワークB内で用いられるアドレス空間が潜在的に重複していると、受信したデバイスD2のIPアドレスが、ネットワークA内でローカルに用いる、デバイスのIPアドレスと混同される場合があるという潜在的な恐れがある。かかる場合、各々のゲートウェイ100、ゲートウェイ102は、対向するローカル・ネットワーク内のデバイスに対して、自身のデバイスに対して内部的に用いるIPアドレス空間との重複を回避するように選択されている、IPアドレス空間を定義する。受信したDNS応答内のデバイスD2のプライベートIPアドレスは、このようにしてネットワークB内で有効であるが、しかしネットワークA内では一意的でない場合がある。ネットワークA内でアドレス衝突を回避するために、ゲートウェイ100はしたがって、さらなる工程1:6で、デバイスD2に対してネットワークB内で用いられるIPアドレスを、デバイスD2に対してネットワークA内で用いられるIPアドレスに変換していて、デバイスD2に対してネットワークA内で用いられるIPアドレスは、ネットワークB内のデバイスに対してゲートウェイ100により前もって定義されているIPアドレス空間から取られる。

【0037】

他方、ローカル・ネットワークAおよびローカル・ネットワークB内で用いられるアド

10

20

30

40

50

レス空間が、互いに区別されている、すなわち重複していないことが知られていると、受信したDNS応答内のデバイスD2のプライベートIPアドレスは、同様にネットワークA内で一意的であろうし、そしてしたがって変換は必要ないであろう。工程1:6はその場合割愛できる。

【0038】

工程1:5のDNS応答でデバイスD2のIPアドレスを受信していて、ゲートウェイ100はまた、さらなるオプションの工程1:7により示しているように、ローカル・ストレージまたは同様のものにD2のアドレスをキャッシュする場合がある。1つの実施形態では、ゲートウェイ102からのDNS応答には、デバイスD2の現時点のプライベートIPアドレスに対する有効期間を決定するタイムアウト・パラメータが入っている。かかるIPアドレスは、それからタイムアウト・パラメータに従って第1のゲートウェイ内に一時的にキャッシュされる場合がある。

10

【0039】

最後に、ゲートウェイ100は、上記に従って場合により変換された、D2デバイスの現時点のプライベートIPアドレスの入っているDNS応答を、工程1:8でデバイスD1に転送する。それにより、デバイスD1は、宛先アドレスとして受信したD2のIPアドレスを用いることにより、データ・パケットをデバイスD2に伝えることができる。VPNトンネルが、ゲートウェイ100とゲートウェイ102との間でデータ・パケット通信のために確立されていると、ネットワークAとネットワークBとの間で通信される場合、各パケットに付加される外部ヘッダにおいて、それぞれ、宛先アドレスおよび発信元アドレスとして用いられるパブリックIPアドレスが、各ゲートウェイに割り当てられている。D2のIPアドレスは、変換されるかそのままのいずれかで、それから、D1からD2へのパケットの内部ヘッダ内で宛先アドレスとして用いられるであろう。

20

【0040】

図2は、図1に示す手順に従って、第1のデバイスD1、第1のゲートウェイ100および第2のゲートウェイ102に係わるメッセージ通信の例を、信号図によって説明している。ゲートウェイ100のNSレコードが、上記工程1:1に対して説明したように、ゲートウェイ102のドメイン名およびIPアドレスで更新されていると仮定する。プライベートIPアドレス空間10.0.0.0/24が、ネットワークA内の自身のローカル・デバイスに対してネットワークA内で用いられると、また仮定する。

30

【0041】

最初に示す工程2:1では、ゲートウェイ100は、デバイスD2のホスト名、この場合はD2.networkB.dyndns.orgを参照するDNS要求をデバイスD1から受信する。このホスト名には、宛先のデバイスD2を識別する第1の部分“D2”および、第2のゲートウェイ102およびネットワークBを識別するドメイン名である第2の部分“networkB.dyndns.org”を含む。注目すべきは、第1の部分は、いかなる方法によっても、たとえば“Dx”、“www”または“mail”で自由に構成される場合があり、ネットワークAとネットワークBの間で事前に、合意され、そしてデバイスに対して定義済みであることである。

【0042】

次の工程2:2では、ゲートウェイ100は、上記工程1:3に対して説明したように、ドメイン名“networkB.dyndns.org”に対してNSレコードを調べることによりプライマリDNSを決定し、そしてそれにより、ゲートウェイ102のIPアドレスを得る。ゲートウェイ100は、今度は、上記ホスト名を参照して、次の工程2:3で、得られたIPアドレスに、すなわちゲートウェイ102にDNS要求を送ることができる。DNS要求を受信すると、ゲートウェイ102は、この例ではネットワークB内で有効であるが、しかしネットワークA内では有効でない、デバイスD2のプライベートIPアドレス10.0.0.10を決定するために、次の工程2:4で、通常の手順に従ってホスト名を解決する。

40

【0043】

50

ゲートウェイ 102 はそれから、さらなる工程 2 : 5 で、DNS 応答パケット内のペイロードとして提示されるデバイス D2 のプライベート IP アドレス 10 . 0 . 0 . 10 が入っている DNS 応答をゲートウェイ 100 に送る。潜在的に重複しているアドレス空間がネットワーク A およびネットワーク B 内で使用されているので、ゲートウェイ 100 は、次の工程 2 : 6 で、受信した IP アドレス 10 . 0 . 0 . 10 を、第 1 のネットワークで用いるために第 2 のデバイスに割り当てられている修正プライベート IP アドレス 10 . 0 . 1 . 10 に変換する。変換された新しいアドレスは、第 1 のネットワーク内のローカル・デバイスに対して用いられるプライベート IP アドレス空間と区別され、すなわち、重複しない。

【 0044 】

10

この例では、修正プライベート IP アドレスは、IPv4 ベースのアドレスであり、第 3 オクテット内の一意的な数字が対向するネットワーク B を表すように配分されており、この場合は “ 1 ” である。しかしながら、任意のアドレス指定方式が、ネットワーク B 内のデバイスに対してネットワーク A で用いられる場合があり、そして本発明は、この点において限定されない。デバイス D2 の修正 IP アドレスはまた、オプションの工程 2 : 7 により示しているように、ゲートウェイ 100 でキャッシュされる場合がある。

【 0045 】

ゲートウェイはそれから、さらなる工程 2 : 8 で、DNS 応答パケット内のペイロードとして提示されるデバイス D2 の変換された IP アドレス 10 . 0 . 1 . 10 が入っている DNS 応答をデバイス D1 に送信する。また、デバイス D1 は、別のオプションの工程 2 : 9 により示すように、受信したアドレスをローカル・ストレージにキャッシュする場合がある。デバイス D1 は、今度は、さらなる工程 2 : 10 に示すように、D1 から D2 へのパケットの内部ヘッダ内の宛先アドレスとして受信した D2 の IP アドレスを用いることにより、データ・パケットをデバイス D2 に伝えることができる。ゲートウェイ 102 はそれから、最後の工程 2 : 11 に示すように、宛先アドレスを 10 . 0 . 1 . 10 から、デバイス D2 に対してネットワーク B 内で有効である 10 . 0 . 0 . 10 に変換するであろう。

20

【 0046 】

第 1 のデバイスが存在する第 1 のローカル・ネットワーク内の第 1 のゲートウェイにより行われる、対向する第 2 のローカル・ネットワーク内の第 2 のデバイスとのパケット通信を可能にするための手順は、これから、図 3 のフロー図を参照して簡潔に説明することとする。上記の例と同じように、第 1 のゲートウェイおよび、第 2 のローカル・ネットワーク内の第 2 のゲートウェイは、DNS 機能を装備している。

30

【 0047 】

第 1 の工程 300 では、第 1 のゲートウェイ内のローカル NS レコードを、第 2 のゲートウェイのドメイン名およびパブリック IP アドレスを格納することにより更新する。次の工程 302 では、発信 DNS 要求を第 1 のデバイスから受信し、DNS 要求は第 2 のデバイスのホスト名を参照している。続く工程 304 では、第 2 のゲートウェイであるプライマリ DNS のパブリック IP アドレスを、ローカル NS レコードを調べることにより決定する。DNS 要求はそれから、第 2 のデバイスに対して第 2 のネットワークで用いられる現時点のプライベート IP アドレスを得るために、さらなる工程 306 で、第 2 のゲートウェイに送信される。

40

【 0048 】

上記例に対して述べたように、潜在的に重複するアドレス空間が 2 つのネットワーク内で用いられると、得られた第 2 のデバイスの IP アドレスを変換する必要がある場合がある。このようにして、工程 308 では、そのような重複しているアドレス空間が第 1 のネットワークおよび第 2 のネットワークでそれら自身のデバイスに対して用いられるおそれがあるかどうかによって、処理が分岐する場合がある。第 1 のネットワークおよび第 2 のネットワークがそのような重複するアドレス空間を用いないことが知られていると、工程 306 で得られる第 2 のデバイスの IP アドレスは、第 1 のネットワーク内で一義的に用

50

いることができ、そして工程 310 で、IP アドレスを、得られたとおりに、すなわち変換することなく、DNS 応答で第 1 のデバイスに転送できよう。

【0049】

そうでなければ、得られた IP アドレスを、工程 312 で、第 1 のネットワーク内で用いるために、第 2 のデバイスに割り当てられている修正プライベート IP アドレスに変換する。変換され、そして修正された IP アドレスは、それから、最後に示した工程 314 で、第 1 のデバイスに DNS 応答で最終的に転送する。

【0050】

図 3 の典型的な手順は、実装によっては多少修正される場合がある。実際的な例では、得られた IP アドレスは、2 つのネットワークが重複しているアドレス空間を用いる恐れがあるか否かに係わらず、上記に従って修正プライベート IP アドレスに変換される場合がある。かかる場合、工程 308 および工程 310 は割愛できるであろうし、そして工程 312 および工程 314 は、工程 306 の直後に実行することができよう。

【0051】

ゲートウェイ 100 の上記工程および機能を基本的に行うように構成された機能部を持つ第 1 のネットワーク・ゲートウェイは、図 4 の概略ブロック図を参照して、より詳細にこれから説明することとする。この例では、第 1 のゲートウェイ 400 は、第 1 のローカル・ネットワークを在圏とし、そして第 1 のローカル・ネットワーク内の第 1 の通信デバイスと第 2 のローカル・ネットワーク内の第 2 の通信デバイスとの間で、データ・パケットの通信を可能にすることができる。プライベート IP アドレスは、第 1 のローカル・ネットワークおよび第 2 のローカル・ネットワーク内にあるデバイスに用いられる。

【0052】

ゲートウェイ 400 は、図 1 および図 2 におけるサーバ 100 の機能を果たすように、または図 3 に示す処理を実行するように、またはその両方を行うように、基本的に構成される場合がある。特に、ネットワーク・ゲートウェイ 400 は、基本的に上記の例に対して説明した方法で、DNS 要求を処理するためのローカル DNS 機能を用いて構成される。

【0053】

ゲートウェイ 400 は、ローカル・ネーム・サーバ・レコード 400b を、第 2 のネットワークの第 2 のゲートウェイ 102 のドメイン名および IP アドレスで更新するように構成された、ネーム・サーバ (NS) レコード・マネージャ 400a を備えており、第 1 のゲートウェイおよび第 2 のゲートウェイの各々はローカル DNS 機能を有する。ゲートウェイ 400 はまた、第 2 のデバイスのホスト名を参照する発信 DNS 要求を、第 1 のデバイス (図示していない) から受信するように構成された内部通信部 400c を備える。ゲートウェイ 400 はまた、第 2 のゲートウェイであるプライマリ DNS の IP アドレスを、ホスト名内のドメイン名に基づいて、ローカル・ネーム・サーバ・レコードから決定するように構成された DNS 決定部 400d を備える。

【0054】

ゲートウェイ 400 はさらに、決定された IP アドレスを用いて第 2 のゲートウェイ (図示していない) に DNS 要求を送信するように、そして第 2 のゲートウェイからの DNS 応答で第 2 のデバイスの現時点のプライベート IP アドレスを得るように構成された外部通信部 400e を備える。内部通信部 400c はさらに、第 2 のデバイスの現時点のプライベート IP アドレスを参照する DNS 応答を第 1 のデバイスに転送する。

【0055】

ゲートウェイ 400 はまた、第 1 のローカル・ネットワークおよび第 2 のローカル・ネットワーク内のデバイスに用いられるプライベート IP アドレスが潜在的に重複しており、そして得られたプライベート IP アドレスが第 2 のデバイスに対して第 2 のネットワーク内で用いられていると、得られたプライベート IP アドレスを、第 2 のデバイスに対して第 1 のネットワーク内で用いられる修正プライベート IP アドレスに変換するように構成された IP アドレス変換部 400f を備える。かかる場合、修正プライベート IP アド

レスは、第1のネットワークと第2のネットワークとの間のVPNトンネルに対して定義されている場合があり、そして第1のローカル・ネットワーク内のデバイスに対して、第1のローカル・ネットワーク内で用いられる内部IPアドレスと区別され、すなわち重複しない。さらに、修正プライベートIPアドレスは、ゲートウェイ400内で創出され、そして少なくともトンネル識別子および、第2のネットワークにあるデバイスに対して第1のネットワーク内で用いられる重複しないIPアドレス空間が入っている変換テーブル400gから読み出される場合がある。

【0056】

図4でさらに示しているように、第1のゲートウェイ400上で実行される場合、第1のゲートウェイに第1のゲートウェイの上記機能および工程を行うようにさせるコード手段を備えているコンピュータ・プログラム402のプログラム・モジュールとして、上記の機能部は実装できる。この実施形態では、コンピュータ・プログラム402は、コンピュータ・プログラムが格納されているコンピュータで読み取り可能な記憶媒体を備えているコンピュータ・プログラム・プロダクト404により実行される。

【0057】

コンピュータ・プログラム402のプログラム・モジュールには、
- ローカル・ネーム・サーバ・レコード400bを第2のネットワークの第2のゲートウェイのドメイン名およびIPアドレスで更新できる更新モジュール402a、（第1のゲートウェイおよび第2のゲートウェイの各々がローカルDNS機能を有する）、
- 第2のデバイスのホスト名を参照する発信DNS要求を第1のデバイスから受信できる受信モジュール402b、
- 第2のゲートウェイであるプライマリDNSのIPアドレスを、ホスト名内のドメイン名に基づいてローカル・ネーム・サーバ・レコードから決定できる決定モジュール402c、
- 決定されたIPアドレスを用いて、DNS要求を第2のゲートウェイに送信し、そして第2のゲートウェイからのDNS応答で第2のデバイスの現時点のプライベートIPアドレスを得ることができる送信および獲得モジュール402d、
- 第2のデバイスの現時点のプライベートIPアドレスを参照して、DNS応答を第1のデバイスに転送できる転送モジュール402e、
を含む。

【0058】

コンピュータ・プログラム402のコード手段およびコンピュータ・プログラム・プロダクト404はまた、第1のゲートウェイに以下の機能を行わせる場合がある。

【0059】

第1のローカル・ネットワークおよび第2のローカル・ネットワーク内のデバイスに用いられるプライベートIPアドレスが潜在的に重複していて、そして得られたプライベートIPアドレスが第2のデバイスに対して第2のネットワーク内で用いられていると、コード手段は、第1のゲートウェイに、得られたプライベートIPアドレスを第2のデバイスに対して第1のネットワーク内で用いられる修正プライベートIPアドレスに変換させる場合がある。修正プライベートIPアドレスは、第1のネットワークと第2のネットワークとの間のVPNトンネルに対して定義された、そして第1のローカル・ネットワーク内のデバイスに対して第1のローカル・ネットワーク内で用いられる内部IPアドレス空間と区別されている（すなわち重複しない）アドレス空間内にある。第1のデバイスに転送されたDNS応答は、それから修正IPアドレスを備えるであろう。

【0060】

第2のゲートウェイからのDNS応答にさらに、第2のデバイスの現時点のプライベートIPアドレスに対する有効期間を決定するタイムアウト・パラメータが入っていると、コード手段は、第1のゲートウェイに、タイムアウト・パラメータに従って、第1のゲートウェイ内の第2のデバイスの現時点のプライベートIPアドレスを一時的にキャッシュするようにさせる場合がある。

【 0 0 6 1 】

注目すべきは、図 4 は、論理的意味合いで、ゲートウェイ 4 0 0 内の様々な典型的な機能部およびプログラム・モジュールをただ示しているだけであり、一方当業者は、任意の適切なソフトウェア手段およびハードウェア手段を用いて、説明した機能を実際に自由に実装できる。このようにして、本発明は広く、ゲートウェイ 4 0 0 の図示した構成に限定されない。たとえば、コンピュータ・プログラム・プロダクトは、フラッシュ・メモリ、ROM (リード・オンリ・メモリ) または EEPROM (電氣的に消去可能なプログラマブル ROM) である場合があり、そして上記のコンピュータ・プログラム・モジュールは、代替の実施形態では、ゲートウェイ 4 0 0 内のメモリの形式で種々のコンピュータ・プログラム・プロダクトに分散されることができよう。

10

【 0 0 6 2 】

以下の恩恵および長所が、上記の実施形態によって得られる場合がある。

- 1) 本解決策は、ローカル・ネットワーク内のユーザにネットワークを通して安全でプライベートな通信をするようにできる。
- 2) DNS 変換は、対向するデバイスの現時点の IP アドレスを知っている必要がなく、より使い易い機能を可能にさせる。
- 3) すべてのプライベート IP アドレスが、ネットワーク間でデータ・パケットを通信する場合、一意的になる。
- 4) DNS 応答のペイロードにおける変換が、VPN トンネルを確立しているローカル・ネットワーク間でのよりよい相互作用を可能にさせる。
- 5) 本解決策は、各ゲートウェイがトンネリング機能およびアドレス変換機能に関与するので、拡張性がある。
- 6) ローカル DNS 機能は、現存するグローバル DNS 機能に影響しない、または妨げない。
- 7) 本解決策はまた、移動網に対して多国にわたる解決策をサポートするのに用いることができる。

20

【 0 0 6 3 】

本発明は特定の典型的な実施形態を参照して説明してきたが、明細書は概論的に、本発明の構想を説明しようとしているだけであり、そして本発明の範囲を限定すると見なされるべきではない。本発明は、添付の請求項により規定される。

30

【図 1】

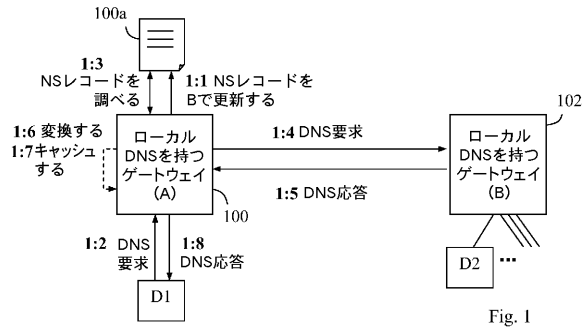


Fig. 1

【図 2】

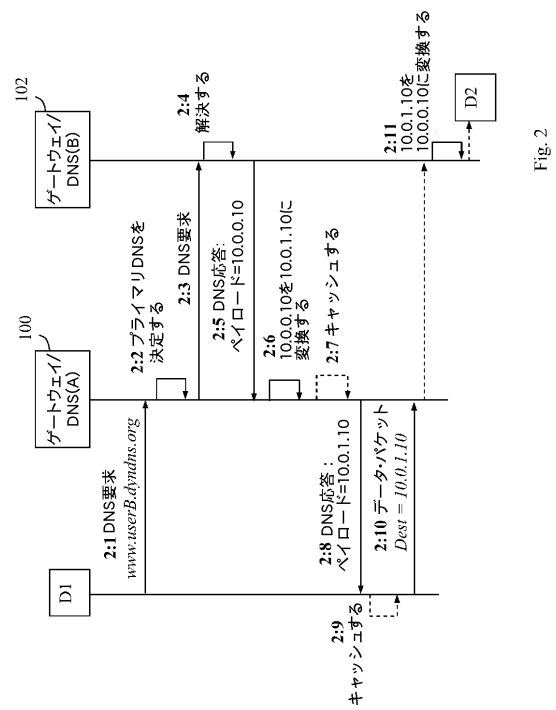


Fig. 2

【図 3】

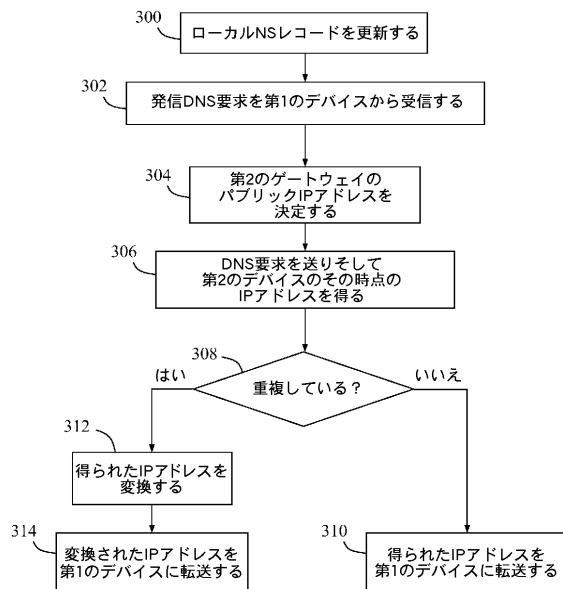


Fig. 3

【図 4】

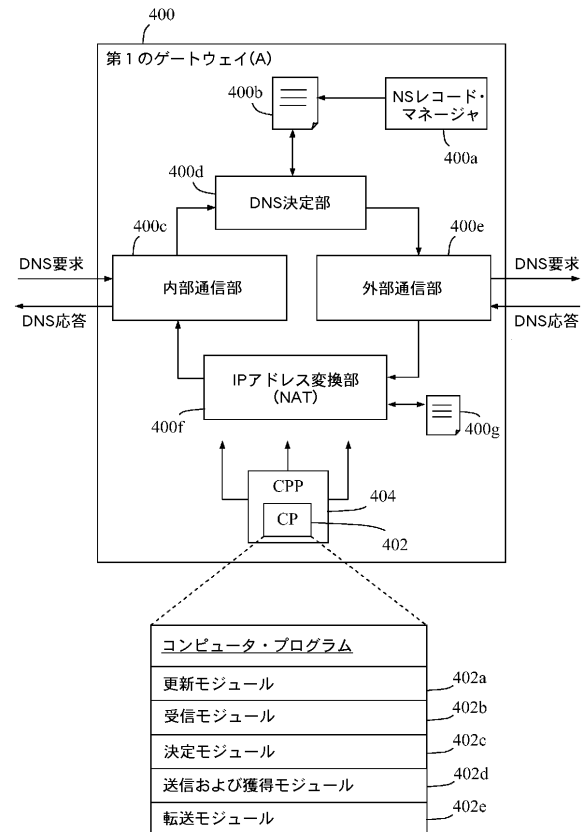


Fig. 4

フロントページの続き

- (72)発明者 ケルヒ, ヨハン
スウェーデン国 ヴァクスホルム エス - 1 8 5 3 9 , スロンベルスリンガン 2 2
- (72)発明者 ゴタレ, クリスティアン
スウェーデン国 ゲティンゲ エス - 3 1 0 4 4 , ヴェステルガタン 5
- (72)発明者 ティーニ, トマス
スウェーデン国 イェルフェツラ エス - 1 7 5 6 6 , ニダロスリンガン 5 8
- (72)発明者 ウェリン, アンニッキ
スウェーデン国 ソルナ エス - 1 7 1 6 0 , ウィボムス ヴェグ 1 0

審査官 岩田 玲彦

(56)参考文献 特開2004-229299(JP,A)

(58)調査した分野(Int.Cl., DB名)
H04L 12/46