(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2011-515944
(P2011-515944A)
(43)公表日　平成23年5月19日(2011.5.19)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/66	(2006.01)	H04L	12/66	B	5K030
H04L 12/56	(2006.01)	H04L	12/56	B	
		H04L	12/56	H	

審査請求 未請求　予備審査請求 有　（全 26 頁）

(21)出願番号　特願2011-500741 (P2011-500741)
(86)(22)出願日　平成21年3月20日 (2009.3.20)
(85)翻訳文提出日　平成22年10月4日 (2010.10.4)
(86)国際出願番号　PCT/SE2009/050292
(87)国際公開番号　WO2009/116945
(87)国際公開日　平成21年9月24日 (2009.9.24)
(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)

(71)出願人　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－１６４　８３
(74)代理人　100076428
弁理士　大塚　康徳
(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のデータパケットの通信方法および装置

(57)【要約】
重複する可能性のあるプライベートＩＰアドレス空間を用いて２つの異なるローカルネットワーク（Ａ、Ｂ）内のデバイス（Ｅ１Ｂ、Ｅ３Ａ）間で通信されるデータパケットについて、一義的なアドレス指定を行うための方法および装置である。２つのローカルネットワーク内のゲートウェイ（１０２、１０４）間で、まず、ＶＰＮトンネルが確立され、そして、各ネットワークにおいて、自分自身のデバイスについて使用される内部ＩＰアドレス空間とは重複しない内部ＩＰアドレス空間が、対向ネットワーク内のデバイスについて定義される。一方のネットワークのゲートウェイ（１０２）が対向ネットワーク内のデバイス（Ｅ１Ｂ）からデータパケットを受信すると、パケットのヘッダが、対向ネットワーク内で有効なアドレス空間に属する宛先アドレスとソースアドレスとを現在のネットワーク内で有効なアドレス空間に属するアドレスに変更することによって、修正される。
【選択図】　なし

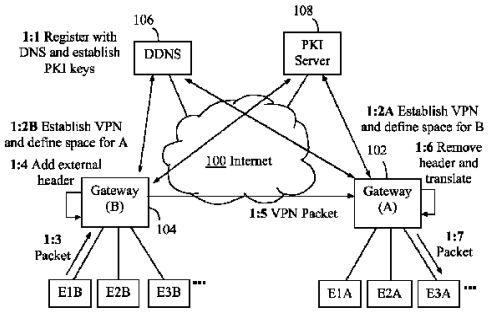

Fig.1

【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デバイスおよび第２のローカルネットワーク内のデバイスについて重複する可能性のあるプライベートＩＰアドレスが使用されている場合に、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（Ｅ３Ａ）と前記第２のローカルネットワーク内の第２の通信デバイス（Ｅ１Ｂ）との間でデータパケットを通信する方法であって、
前記第１のローカルネットワークにサービスを提供する第１のゲートウェイ（Ａ）と、前記第２のローカルネットワークにサービスを提供する第２のゲートウェイ（Ｂ）との間にＶＰＮトンネルを確立するステップであって、パブリックＩＰアドレスが前記第１のゲートウェイ（Ａ）と前記第２のゲートウェイ（Ｂ）との各ゲートウェイに割り当てられている、ステップと、
前記第１のゲートウェイにおいて、前記第２のローカルネットワーク内のデバイスについて、前記第１のローカルネットワーク内で使用される、選択された内部ＩＰアドレス空間を定義するステップであって、前記選択された内部ＩＰアドレス空間は、前記第１のローカルネットワーク内のデバイスについて前記第１のローカルネットワーク内で使用される内部ＩＰアドレス空間とは異なる、重複していないＩＰアドレス空間である、ステップと、
前記第１のゲートウェイにおいて、前記ＶＰＮトンネルを介して前記第２のデバイス（Ｅ１Ｂ）からの着信パケットを受信するステップであって、前記着信パケットは、前記第１のデバイスについて前記第２のローカルネットワーク内で使用される内部宛先アドレスと、前記第２のデバイスについて前記第２のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する、ステップと、
前記内部宛先アドレスを、前記第１のデバイスについて前記第１のローカルネットワーク内で使用される内部宛先アドレスに変更するステップと、
前記内部ソースアドレスを、前記第２のデバイスについて前記第１のローカルネットワーク内で使用され、かつ、前記選択された内部ＩＰアドレス空間の中にある、選択されたアドレス空間の内部ソースアドレスへと変更するステップと、
前記着信パケットを、変更された内部宛先アドレスと変更された内部ソースアドレスとを含む修正された内部ＩＰヘッダと共に、前記第１のデバイス（Ｅ３Ａ）に転送するステップと
を備えることを特徴とする方法。
【請求項２】
前記着信パケットは、更に、それぞれ外部宛先アドレスと外部ソースアドレスとして、前記第１のゲートウェイのパブリックＩＰアドレスと前記第２のゲートウェイのパブリックＩＰアドレスを含む外部ＩＰヘッダを有し、
前記外部ＩＰヘッダは、前記第１のゲートウェイによって前記着信パケットから削除される
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１のゲートウェイにおいて、前記第１のデバイスから発信パケットを受信するステップであって、前記発信パケットは、前記第２のデバイスについて前記第１のローカルネットワーク内で使用される内部宛先アドレスと、前記第１のデバイスについて前記第１のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する、ステップと、
それぞれ外部宛先アドレスと外部ソースアドレスとして、前記第１のゲートウェイのパブリックＩＰアドレスと前記第２のゲートウェイのパブリックＩＰアドレスを含む外部ＩＰヘッダで、前記発信パケットをカプセル化するステップと、
前記内部宛先アドレスに基づいて、前記発信パケットについての正確なＶＰＮトンネルを判定するステップと、

前記発信パケットを、前記ＶＰＮトンネルを介して前記第２のゲートウェイへ送信するステップと
を更に備える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ＶＰＮトンネルは、前記第１のローカルネットワークと複数の対向ローカルネットワークとの間で確立され、
前記複数の対向ローカルネットワークそれぞれの対向ネットワーク内のデバイスについて前記第１のローカルネットワーク内で使用されることになる選択された内部ＩＰアドレス空間が、前記それぞれの対向ネットワークについて定義され、
前記選択された内部ＩＰアドレス空間それぞれは、前記第１のローカルネットワーク内で使用される任意の他のアドレス空間と異なる、重複していないＩＰアドレス空間である
ことを特徴とする請求項１乃至３のいずれか１項に記載の方法。
【請求項５】
前記選択された内部ＩＰアドレス空間は、ＩＰｖ４ベースのアドレス群を含み、
前記アドレス群のそれぞれの第２または第３オクテットの一意の数が、対応する前記対向ローカルネットワークを表すために割り当てられる
ことを特徴とする請求項４に記載の方法。
【請求項６】
前記発信パケットそれぞれについて、前記発信パケットの中の内部宛先アドレスの中の前記一意の数に基づいて、ＶＰＮトンネルが判定され、
前記発信パケットは、判定されたＶＰＮトンネルを介して送信される
ことを特徴とする請求項５に記載の方法。
【請求項７】
前記ＶＰＮトンネルを確立することは、ローカルネットワークそれぞれのゲートウェイの中に、対向ゲートウェイそれぞれのＤＮＳ登録名と対応する公開ＰＫＩ鍵とを追加することを含んでいる
ことを特徴とする請求項４乃至６のいずれか１項に記載の方法。
【請求項８】
前記公開ＰＫＩ鍵と対応する秘密ＰＫＩ鍵は、ゲートウェイそれぞれについて生成されていて、
前記公開ＰＫＩ鍵は、前記ゲートウェイがアクセス可能なＰＫＩサーバに記憶されている
ことを特徴とする請求項７に記載の方法。
【請求項９】
信頼されたパーティ群を含む信頼リストが、前記第１のローカルネットワークについて作成されていて、
候補ローカルネットワークが、前記信頼リストの中に存在する第１のパーティと関連付けられている場合、前記第１のローカルネットワークと前記候補ローカルネットワークとの間でＶＰＮトンネルの確立が許可される
ことを特徴とする請求項１乃至８のいずれか１項に記載の方法。
【請求項１０】
前記第１のパーティの前記信頼リストの中に存在する第２のパーティと関連付けられることによって、前記候補ローカルネットワークが、前記信頼リストの中の前記第１のパーティと間接的に関連付けられている場合、前記ＶＰＮトンネルは、確立が許可される
ことを特徴とする請求項９に記載の方法。
【請求項１１】
前記ＶＰＮトンネルは、前記第１のローカルネットワークについて承認される所定数の信頼レベルに依存して、確立が許可される
ことを特徴とする請求項１０に記載の方法。
【請求項１２】

前記候補ローカルネットワークは、当該候補ローカルネットワークからのＶＰＮトンネルリクエストに応じて、ＶＰＮトンネルの確立について評価される
ことを特徴とする請求項９乃至１１のいずれか１項に記載の方法。
【請求項１３】
２つのローカルネットワーク間で確立されたＶＰＮトンネルは、いずれかのローカルネットワークに関連付けられている信頼リストが、前記ＶＰＮトンネルを不適格とみなすように修正されている場合、自動的に終了される
ことを特徴とする請求項９乃至１２のいずれか１項に記載の方法。
【請求項１４】
第１のローカルネットワークにサービスを提供する第１のゲートウェイ（Ａ）における装置であって、
当該装置は、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（Ｅ１Ａ）と第２のゲートウェイ（Ｂ）によってサービスが提供される第２のローカルネットワーク内の第２の通信デバイス（Ｅ１Ｂ）との間でデータパケットを通信することができ、
前記第１のゲートウェイは、前記第１のゲートウェイと前記第２のゲートウェイとの間でＶＰＮトンネルを確立するように構成されていて、
パブリックＩＰアドレスが前記第１のゲートウェイと前記第２のゲートウェイそれぞれに割り当てられていて、かつ前記第１のローカルネットワーク内のデバイスおよび前記第２のローカルネットワーク内のデバイスについて重複する可能性のあるプライベートＩＰアドレスが使用されており、
前記装置は、
前記第２のローカルネットワーク内のデバイスについて、前記第１のローカルネットワーク内で使用される、選択された内部ＩＰアドレス空間を定義するように構成されているＩＰアドレス定義手段（４００ａ）であって、前記選択された内部ＩＰアドレス空間は、前記第１のローカルネットワーク内のデバイスについて前記第１のローカルネットワーク内で使用される内部ＩＰアドレス空間とは異なる、重複していないＩＰアドレス空間である、ＩＰアドレス定義手段（４００ａ）と、
前記ＶＰＮトンネルを介して前記第２のデバイスからの着信パケットを受信するように構成されている受信手段（４００ｂ）であって、前記着信パケットは、前記第１のデバイスについて前記第２のローカルネットワーク内で使用される内部宛先アドレスと、前記第２のデバイスについて前記第２のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する、受信手段（４００ｂ）と、
前記内部宛先アドレスを、前記第１のデバイスについて前記第１のローカルネットワーク内で使用される前記内部宛先アドレスに変更し、かつ前記内部ソースアドレスを、前記第２のデバイスについて前記第１のローカルネットワーク内で使用され、かつ、前記選択された内部ＩＰアドレス空間の中にある、選択されたアドレス空間の内部ソースアドレスへと変更するように構成されているＩＰアドレス変更手段（４００ｃ）と、
前記着信パケットを、変更された内部宛先アドレスと変更された内部ソースアドレスとを含む修正された内部ＩＰヘッダと共に、前記第２のデバイスに転送するように構成されている転送手段（４００ｄ）と
を備えることを特徴とする装置。
【請求項１５】
前記着信パケットは、更に、それぞれ外部宛先アドレスと外部ソースアドレスとして、前記第１のゲートウェイのパブリックＩＰアドレスと前記第２のゲートウェイのパブリックＩＰアドレスを含む外部ＩＰヘッダを有し、
前記ＩＰアドレス変更手段は、更に、前記外部ＩＰヘッダを、前記第１のゲートウェイによって前記着信パケットから削除するように構成されている
ことを特徴とする請求項１４に記載の装置。
【請求項１６】
前記第１のデバイスから受信する発信パケットとして、前記第２のデバイスについて前

記第１のローカルネットワーク内で使用される内部宛先アドレスと、前記第１のデバイスについて前記第１のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する発信パケットを、受信し、
それぞれ外部宛先アドレスと外部ソースアドレスとして、前記第１のゲートウェイのパブリックＩＰアドレスと前記第２のゲートウェイのパブリックＩＰアドレスを含む外部ＩＰヘッダで、前記発信パケットをカプセル化し、
前記内部宛先アドレスに基づいて、前記発信パケットについての正確なＶＰＮトンネルを判定し、
前記発信パケットを、前記ＶＰＮトンネルを介して前記第２のゲートウェイへ送信するように更に構成されている
ことを特徴とする請求項１４または１５に記載の装置。
【請求項１７】
前記ＶＰＮトンネルは、前記第１のローカルネットワークと複数の対向ローカルネットワークとの間で確立され、
前記複数の対向ローカルネットワークそれぞれの対向ネットワーク内のデバイスについて前記第１のローカルネットワーク内で使用されることになる選択された内部ＩＰアドレス空間が、前記それぞれの対向ネットワークについて定義され、
前記選択された内部ＩＰアドレス空間それぞれは、前記第１のローカルネットワーク内で使用される任意の他のアドレス空間と異なる、重複していないＩＰアドレス空間である
ことを特徴とする請求項１４乃至１６のいずれか１項に記載の装置。
【請求項１８】
前記選択された内部ＩＰアドレス空間は、ＩＰｖ４ベースのアドレス群を含み、
前記アドレス群のそれぞれの第２または第３オクテットの一意の数が、対応する対向ローカルネットワークを表すために割り当てられる
ことを特徴とする請求項１７に記載の装置。
【請求項１９】
更に、前記発信パケットそれぞれについて、前記発信パケットの中の内部宛先アドレスの中の前記一意の数に基づいて、ＶＰＮトンネルを判定し、かつ前記発信パケットを、判定されたＶＰＮトンネルを介して送信するように構成されている
ことを特徴とする請求項１４乃至１８のいずれか１項に記載の装置。
【請求項２０】
前記ＶＰＮトンネルを確立することは、ローカルネットワークそれぞれのゲートウェイの中に、対向ゲートウェイそれぞれのＤＮＳ登録名と対応する公開ＰＫＩ鍵とを追加することを含んでいる
ことを特徴とする請求項１９に記載の装置。
【請求項２１】
前記公開ＰＫＩ鍵と対応する秘密ＰＫＩ鍵は、ゲートウェイそれぞれについて生成されていて、
前記公開ＰＫＩ鍵は、前記ゲートウェイがアクセス可能なＰＫＩサーバに記憶されている
ことを特徴とする請求項２０に記載の装置。
【請求項２２】
信頼されたパーティ群を含む信頼リストを、前記第１のローカルネットワークについて作成し、かつ候補ローカルネットワークが、前記信頼リストの中に存在する第１のパーティと関連付けられている場合、前記第１のローカルネットワークと前記候補ローカルネットワークとの間でＶＰＮトンネルの確立を許可するように更に構成されている
ことを特徴とする請求項１４乃至２１のいずれか１項に記載の装置。
【請求項２３】
前記第１のパーティの前記信頼リストの中に存在する第２のパーティと関連付けられることによって、前記候補ローカルネットワークが前記信頼リストの中の前記第１のパーテ

ィと間接的に関連付けられている場合、前記ＶＰＮトンネルの確立を許可するように更に構成されている
ことを特徴とする請求項２２に記載の装置。
【請求項２４】
前記第１のローカルネットワークについて承認される所定数の信頼レベルに依存して、前記ＶＰＮトンネルの確立を許可するように更に構成されている
ことを特徴とする請求項２３に記載の装置。
【請求項２５】
前記候補ローカルネットワークからのＶＰＮトンネルリクエストに応じて、ＶＰＮトンネルの確立について前記候補ローカルネットワークを評価するように更に構成されている
ことを特徴とする請求項２２乃至２４のいずれか１項に記載の装置。
【請求項２６】
いずれかのローカルネットワークに関連付けられている信頼リストが、前記ＶＰＮトンネルを不適格とみなすように修正されている場合、２つのローカルネットワーク間で確立されたＶＰＮトンネルを自動的に終了するように更に構成されている
ことを特徴とする請求項２２乃至２５のいずれか１項に記載の装置。
【請求項２７】
第１のローカルネットワークにサービスを提供し、かつ前記第１のローカルネットワーク内の第１の通信デバイス（Ｅ１Ａ）と第２のゲートウェイ（Ｂ）によってサービスが提供される第２のローカルネットワーク内の第２の通信デバイス（Ｅ３Ｂ）との間でデータパケットを通信することができる、第１のゲートウェイ（Ａ）に対するコンピュータプログラム（４００ｅ）であって、
前記第１のゲートウェイ（Ａ）と前記第２のゲートウェイ（Ｂ）との間にはＶＰＮトンネルが確立されていて、
前記第１のゲートウェイと前記第２のゲートウェイそれぞれにパブリックＩＰアドレスが割り当てられていて、かつ前記第１のローカルネットワーク内のデバイスおよび前記第２のローカルネットワーク内のデバイスについて重複する可能性のあるプライベートＩＰアドレスが使用されていて、
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動作する場合に前記第１のゲートウェイに、
前記第２のローカルネットワーク内のデバイスについて、前記第１のローカルネットワーク内で使用される、選択された内部ＩＰアドレス空間を定義させるコード手段であって、前記選択された内部ＩＰアドレス空間は、前記第１のローカルネットワーク内のデバイスについて前記第１のローカルネットワーク内で使用される内部ＩＰアドレス空間とは異なる、重複していないＩＰアドレス空間である、コード手段と、
前記ＶＰＮトンネルを介して前記第２のデバイスからの着信パケットとして、前記第１のデバイスについて前記第２のローカルネットワーク内で使用される内部宛先アドレスと、前記第２のデバイスについて前記第２のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する着信パケットを受信する場合に、
前記内部宛先アドレスを、前記第１のデバイスについて前記第１のローカルネットワーク内で使用される前記内部宛先アドレスに変更させるコード手段と、、
前記内部ソースアドレスを、前記第２のデバイスについて前記第１のローカルネットワーク内で使用され、かつ、前記選択された内部ＩＰアドレス空間の中にある、選択されたアドレス空間の内部ソースアドレスへと変更させる手段とを備え、
その後、前記着信パケットは、変更された内部宛先アドレスと変更された内部ソースアドレスとを含む修正された内部ＩＰヘッダと共に、前記第２のデバイスに転送される
ことを特徴とするコンピュータプログラム。
【請求項２８】
請求項２７の記載に従うコンピュータプログラムが記憶されているコンピュータ可読記憶媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、重複するアドレス空間を使用する可能性がある、異なるローカルネットワークの中に位置する通信デバイス間のＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）トンネルで、データパケットを通信するための方法および装置に関するものである。
【背景技術】
【０００２】
ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワーク上の異なる当事者（パーティ）間におけるデジタル符号化情報のパケットベースでの送信は、各種の通信サービスに対して使用される。この通新サービスには、例えば、電子メールメッセージング、ファイル転送、インターネット閲覧、音声電話およびテレビ電話、コンテンツストリーミング、ゲーム等がある。デジタル符号化情報は、送信側でデータパケットに構成され、次いで、送信側は、このパケットを、送信経路を介して目標の受信側へ送信する。データパケットは、基本的に、ペイロードデータを含むデータフィールドと、受信側の宛先アドレスと送信側のソースアドレスとを含むヘッダフィールドとで構成される。
【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プライベートネットワーク内に位置する各種の通信デバイス間で通信されることがあり、各ネットワークは、ゲートウェイを用いてネットワーク外のソースからデバイスへのパケットを受信し、また、デバイスからネットワーク外の宛先へパケットを送信する。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、次いで、例えば、インターネットのようなパブリックＩＰネットワーク上でそれぞれのネットワークゲートウェイ間でトランスポートされる。
【０００４】
本明細書では、「ローカルネットワーク」という用語は、内部のプライベートアドレス指定と、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とを使用する、任意のネットワークを一般に表すために使用される。他によく使用される同等の用語には、「プライベートネットワーク」、「住宅用ネットワーク」、「ホームネットワーク」等がある。また、「ゲートウェイ」とは、住宅用ゲートウェイ（ＲＧＷ）、ＩＰルータ、または、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することのできる、任意の他のタイプのネットワークエンティティであってもよい。
【０００５】
パブリックＩＰネットワークでの通信は、一般に、データ保護とプライバシに関して「安全でない」と考えられているので、パケットの中のペイロードデータと他の機密情報とを不正な傍受または操作から保護することが望ましい。この問題を克服する１つの方法は、パブリックＩＰネットワーク上では通信の当事者間でＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：仮想プライベートネットワーク）トンネルを確立することである。
【０００６】
ＶＰＮは、基本的に、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であると考えることができる。ＶＰＮは、公衆インターネットを通るセキュアな通信のためによく使用される。ＶＰＮの顧客とＶＰＮのサービスプロバイダとの間で期待される振る舞いを実現するため、各種のＱｏＳ（Ｑｕａｌｉｔｙ　ｏｆ　Ｓｅｒｖｉｃｅ）パラメータが、ＶＰＮについて定義されてもよい。一般に、ＶＰＮは、ユーザのコミュニティの中で、そのコミュニティに何らかの点で関連する一定の機能性を提供するために、２つ以上の通信デバイスについて確立されてもよい。

【０００７】
インターネットの人気や用途が成長するにつれて、プライベートネットワークやローカルネットワークがインターネット全体にも拡大することがますます望まれるようになっている。例えば、ローカルネットワークを有する多くの会社や企業は、自社独自のＶＰＮを確立して、従業員がリモートでローカルネットワークにアクセスすることを許容している。

【０００８】
ＶＰＮは、従って、公衆ネットワークインフラストラクチャ上で実行される、論理的かつ「分散型」のローカルネットワークとみなすことができる。これらのネットワークは、さまざまな技術を使用して、トラフィックのプライバシと、トラフィックの分離と、データのＱｏＳとを得る。ＶＰＮは、イントラネット、インターネット、またはサービスプロバイダのネットワークインフラストラクチャ上で確立することができる。一般に、利用可能なＶＰＮサービスには、「Ａｃｃｅｓｓ　ＶＰＮ」と「ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）－ｔｏ－ＬＡＮ　ＶＰＮ」と呼ばれる２つの基本的なタイプがあり、前者は、リモートアクセス用に使用され、後者は、異なるローカルネットワークが相互接続される時に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使用される。

【０００９】
しかしながら、ローカルネットワーク内のデバイス間にＶＰＮを確立すると、その結果、さまざまな問題が生じることがある。１つの問題は、ローカルネットワーク内のデバイスは、典型的には、プライベートアドレス空間からのＩＰアドレスを使用するということであり、そのようなプライベートＩＰアドレスは、ローカルなアドミニストレータ等によって内部的にデバイスに対して自由に割り当てることができる。使用されるプライベートＩＰアドレスは、従って、明示的に告げられない限り、基本的に他のユーザには知られていないし、また、加入者にパブリックＩＰアドレスを提供するインターネットサービスプロバイダにも知られていない。

【００１０】
もう１つの問題は、異なるローカルネットワークによって自分たちのデバイスについて使用されるプライベートＩＰアドレスは、概して相互に重複するということであり、特に、複数のローカルネットワークで再使用される一般的なＩｐｖ４ベースのプライベートアドレス空間にはそれが言える。例えば、あるローカルネットワーク内のデバイスによって使用されるプライベートＩＰアドレスが、対向ローカルネットワーク内の別のデバイスによって使用されるものと同一のアドレスであることがあり、結果として、これらの２つのネットワーク間で通信されるデータパケットのアドレス指定があいまいになる。これによって、ＶＰＮトンネルを使って異なるローカルネットワークを一緒に接続することが、面倒なことになる。そのような重複するかまたは再使用されるアドレス空間が原因で、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は、事実上「ルーティング不可能」となり、従って、パブリックＩＰアドレスは、パケットの中でも使用されなければならなくなる。

【発明の概要】
【発明が解決しようとする課題】
【００１１】
上記に概説したいくつかの問題の少なくとも一部に対処することが本発明の目的である。また、２つの異なるローカルネットワーク内のデバイスが、重複する可能性のあるアドレス空間を使用して通信する場合でさえ、データパケットを一義的にアドレス指定できるようにするメカニズムを提供することも目的である。

【００１２】
さまざまな態様に従えば、第１のローカルネットワーク内のデバイスおよび第２のローカルネットワーク内のデバイスについて重複する可能性のあるプライベートＩＰアドレスが使用されている場合に、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のデータパケットの通信を可能にす

るための、方法と、ゲートウェイの中の装置と、コンピュータプログラムと、コンピュータプログラム製品とを提供する。

【課題を解決するための手段】

【００１３】

一態様では、第１のローカルネットワークにサービスを提供する第１のゲートウェイと第２のローカルネットワークにサービスを提供する第２のゲートウェイとの間にＶＰＮトンネルが確立される方法が提供される。ここで、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。第２のローカルネットワーク内のデバイスについて第１のローカルネットワーク内で使用されることを目的として、選択された１つのＩＰアドレス空間が、第１のゲートウェイの中で定義される。選択されたＩＰアドレス空間は、第１のローカルネットワーク内のデバイスについて第１のローカルネットワーク内で使用される内部ＩＰアドレス空間とは別であり、すなわち、重複していない。

【００１４】

第１のゲートウェイは、次いで、ＶＰＮトンネルを介して第２のデバイスからの着信データパケットを受信する。この着信パケットは、第１のデバイスについて第２のローカルネットワーク内で使用される内部宛先アドレスと、第２のデバイスについて第２のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する。次いで、第１のゲートウェイは、受信した内部宛先アドレスを、第１のデバイスについて第１のローカルネットワーク内で使用される内部宛先アドレスに変更し、そして、受信した内部ソースアドレスを、第２のデバイスについて第１のローカルネットワーク内で使用され、かつ、選択された内部ＩＰアドレス空間の中にある、選択されたアドレス空間の内部ソースアドレスへと変更する。次いで、第１のゲートウェイは、着信パケットを、変更された内部宛先アドレスと内部ソースアドレスとを含む修正された内部ＩＰヘッダと共に、第１のデバイスに転送する。

【００１５】

別の態様では、第１のローカルネットワークにサービスを提供し、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のゲートウェイによってサービスが提供される第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を通信することができる装置が、第１のゲートウェイの中で提供される。第１のゲートウェイは、第１のゲートウェイと第２のゲートウェイとの間にＶＰＮトンネルを確立するように構成されている。ここで、パブリックＩＰアドレスは、各ゲートウェイに割り当てられており、重複する可能性のあるプライベートＩＰアドレスが、各ローカルネットワーク内のデバイスについて使用される。

【００１６】

ゲートウェイ装置は、第２のローカルネットワーク内のデバイスについて第１のローカルネットワーク内で使用されることになる、選択された内部ＩＰアドレス空間を定義するように構成されている、ＩＰアドレス定義手段を備えている。ここで、選択されたＩＰアドレス空間は、第１のローカルネットワーク内のデバイスについて第１のローカルネットワーク内で使用される内部ＩＰアドレスとは別であり、すなわち、重複していない。

【００１７】

また、ゲートウェイ装置は、着信データパケットを第２のデバイスからＶＰＮトンネルを介して受信するように構成されている受信手段を備えている。この着信パケットは、第１のデバイスについて第２のローカルネットワーク内で使用される内部宛先アドレスと、第２のデバイスについて第２のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する。

【００１８】

また、ゲートウェイ装置は、内部宛先アドレスを、第１のデバイスについて第１のローカルネットワーク内で使用される内部宛先アドレスに変更し、そして、内部ソースアドレスを、第２のデバイスについて第１のローカルネットワーク内で使用され、かつ、選択された内部ＩＰアドレス空間の中にある、選択されたアドレス空間の内部ソースアドレスに

変更するように構成されている、ＩＰアドレス変更手段を備えている。

【００１９】

また、ゲートウェイ装置は、着信パケットを、変更された内部宛先アドレスと内部ソースアドレスとを含む修正された内部ＩＰヘッダと共に第２のデバイスに転送するように構成されている、転送手段を備えている。

【００２０】

別の態様では、第１のローカルネットワークにサービスを提供し、かつ、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のゲートウェイによってサービスが提供される第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を通信することができる第１のゲートウェイのための、コンピュータプログラムが構成される。さらに、ＶＰＮトンネルが第１のゲートウェイと第２のゲートウェイとの間に確立され、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おり、そして、重複する可能性のあるプライベートＩＰアドレスが、各ローカルネットワーク内のデバイスについて使用される。

【００２１】

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時には第１のゲートウェイに、第２のローカルネットワーク内のデバイスについて第１のローカルネットワーク内で使用されることになる、選択された内部ＩＰアドレス空間を定義させる、コード手段を備えている。この選択されたＩＰアドレス空間は、第１のローカルネットワーク内のデバイスについて第１のローカルネットワーク内で使用される内部ＩＰアドレス空間とは別であり、すなわち、重複していない。

【００２２】

ＶＰＮトンネルを介して第２のデバイスから、第１のデバイスについて第２のローカルネットワーク内で使用される内部宛先アドレスと、第２のデバイスについて第２のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する着信パケットを受信する場合、コード手段は、第１のゲートウェイに、内部宛先アドレスを、第１のデバイスについて第１のローカルネットワーク内で使用される内部宛先アドレスに変更させ、そして、内部ソースアドレスを、第２のデバイスについて第１のローカルネットワーク内で使用され、かつ、選択された内部ＩＰアドレス空間の中にある、選択されたアドレス空間の内部ソースアドレスへと変更させる。次いで、着信パケットは、変更された内部宛先アドレスと内部ソースアドレスとを含む修正された内部ＩＰヘッダと共に、第１のデバイスへ転送される。

【００２３】

別の態様では、コンピュータプログラム製品が、上記のコンピュータプログラムと、コンピュータプログラムが記憶されるコンピュータ可読媒体とを備える。

【００２４】

上記の方法と、ゲートウェイ装置と、コンピュータプログラムと、コンピュータプログラム製品とはそれぞれ、以下のいくつかの実施形態に従って構成される特徴と機能とをさらに含んでもよい。

【００２５】

着信パケットが、それぞれ外部宛先アドレスおよび外部ソースアドレスとして第１のゲートウェイと第２のゲートウェイとのパブリックＩＰアドレスを含む外部ＩＰヘッダをも有する場合、外部ＩＰヘッダは、第１のゲートウェイによって着信パケットから削除される。

【００２６】

別の実施形態では、第１のゲートウェイは、さらに、第１のデバイスから発信データパケットを受信する。この、発信データパケットは、第２のデバイスについて第１のローカルネットワーク内で使用される内部宛先アドレスと、第１のデバイスについて第１のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する。次いで、パケットは、それぞれ外部宛先アドレスおよび外部ソースアドレスとしてゲート

ウェイのパブリックＩＰアドレスを含む外部ＩＰヘッダを使ってカプセル化される。内部宛先アドレスに基づいて、発信パケットについての正確なＶＰＮトンネルを判定することができ、また、発信パケットは、次いで、ＶＰＮトンネルを介して第２のゲートウェイへ送信される。

【００２７】

別の実施形態では、第１のローカルネットワークと複数の対向ローカルネットワークとの間にＶＰＮトンネルが確立される。次いで、それぞれの対向ネットワーク内のデバイスについて第１のローカルネットワーク内で使用されることになる選択された内部ＩＰアドレス空間が、各対向ネットワークについて定義され、選択された各ＩＰアドレス空間は、第１のローカルネットワーク内で使用される他のいずれのアドレス空間とも別であり、すなわち、重複していない。選択されたＩＰアドレス空間は、ＩＰｖ４ベースのアドレスを含んでもよく、次いで、各ＩＰアドレスの第２または第３オクテットの中の一意の数が、対応する対向ローカルネットワークを表すために割り当てられてもよい。次いで、各発信パケットについて、発信パケットの中の内部宛先アドレスの中の一意の数に基づいて、ＶＰＮトンネルを判定することができ、次いで、パケットは、判定されたＶＰＮトンネルを介して送信される。ＶＰＮトンネルを確立することには、各ローカルネットワークのゲートウェイの中に、各対向ゲートウェイのＤＮＳ登録名と対応する公開ＰＫＩ鍵とを追加することが含まれてもよい。また、公開ＰＫＩ鍵と対応する秘密ＰＫＩ鍵とが、各ゲートウェイについて生成されてもよく、この公開ＰＫＩ鍵は、ゲートウェイがアクセス可能なＰＫＩサーバに記憶される。

【００２８】

別の実施形態では、信頼されたパーティ群を含む信頼リストが、第１のローカルネットワークについて作成されており、候補ローカルネットワークが、信頼リストの中に存在する第１のパーティと関連付けられている場合、第１のローカルネットワークと候補ローカルネットワークとの間でＶＰＮトンネルの確立が許可される。さらに、候補ローカルネットワークが第１のパーティの信頼リストの中に存在する第２のパーティと関連付けられることによって信頼リストの中の第１のパーティと間接的に関連付けられている場合、ＶＰＮトンネルの確立が許可されてもよい。例えば、ＶＰＮトンネルは、第１のローカルネットワークについて承認される所定数の信頼レベルに依存して、確立が許可されてもよい。

【００２９】

候補ローカルネットワークは、候補ローカルネットワークからのＶＰＮトンネルリクエストに応じて、ＶＰＮトンネルの確立について評価されてもよいだろう。また、２つのローカルネットワーク間で確立されたＶＰＮトンネルは、いずれかのネットワークに関連付けられている信頼リストが、そのＶＰＮトンネルを不適格とみなすように修正された場合、自動的に終了されてもよいだろう。

【００３０】

本発明の見込まれるさらなる特徴および利点が、以下の詳細説明から明らかになるであろう。

【００３１】

次に、本発明について、例示的な実施形態によって、かつ、添付の図面を参照しながら、詳細に記述しよう。

【図面の簡単な説明】

【００３２】

【図１】一部の例示的な実施形態に従う、ＶＰＮトンネルに関わる通信シナリオを図示する概略ブロック図である。

【図２】別の実施形態に従う、対向ゲートウェイにおいてデータパケットのヘッダがどのように修正されるかを図示する概略送信スキームの図である。

【図３】別の実施形態に従う、着信データパケットを処理するためにローカルネットワーク内のゲートウェイによって実行される手順のステップを示すフローチャートである。

【図４】別の実施形態に従う、ゲートウェイをより詳細に図示する概略ブロック図である

。
【図５】別の実施形態に従う、発信データパケットを処理するためにゲートウェイによって実行される手順のステップを示す別のフローチャートである。
【図６】別の実施形態に従う、ＶＰＮリクエストを処理するためにゲートウェイによって実行される手順のステップを示す別のフローチャートである。
【発明を実施するための形態】
【００３３】
本発明は、２つの異なるローカルネットワーク内のデバイスが、重複するアドレス空間を使用して通信する場合でさえ、データパケットを一義的にアドレス指定できるようにするメカニズムを提供する。簡単に言うと、最初に、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２つのローカルネットワーク内のゲートウェイの間で、ＶＰＮトンネルが確立される。加えて、対向ローカルネットワーク内のデバイスについて本ネットワーク内で使用されるために、選択された内部ＩＰアドレス空間が、各ローカルネットワーク内で定義される。ここで、それは、本ローカルネットワーク内でそれ自身のデバイスについて使用される内部ＩＰアドレス空間とは別であり、すなわち、重複していない。
【００３４】
対向ネットワーク内のデバイスからの任意の着信データパケットが、本ローカルネットワークのゲートウェイで受信される場合、そのパケットのヘッダは、本ネットワーク内でそれ自身のデバイスについて使用されるアドレス空間と重複する可能性のある、プライベートＩＰ宛先アドレスおよびソースアドレスを有する内部ＩＰヘッダを有する。次いで、ヘッダは、宛先アドレスおよびソースアドレスを、本ネットワーク内で２つのデバイスについて使用される上記のアドレス空間に属するアドレスへとそれぞれ変更することによって、受信側ゲートウェイで修正される。特に、送信側デバイスのソースアドレスは、対向ネットワーク内のデバイスについて上記で定義される内部ＩＰアドレス空間から取り込まれる。それによって、着信パケットの内部ＩＰヘッダの中のソースアドレスは、本ネットワーク内の任意のデバイスのプライベートＩＰアドレスとも混同され得ない。
【００３５】
ここで、上記のことをどのようにして達成できるかの一例を、図１に示される通信シナリオを参照しながら説明する。つまり、２つの異なるローカルネットワークＡおよびＢのユーザ同士が、パブリックＩＰネットワーク１００上で、この例では、インターネット上で、例えば、上記に提示した理由のために対向ネットワーク内のデバイス間のデータパケットの「安全な」通信を可能にするため、ネットワーク間にＶＰＮトンネルを設定することに同意していると仮定する。
【００３６】
図１では、第１のゲートウェイ１０２と第２のゲートウェイ１０４とが、それぞれ第１のネットワークＡおよび第２のネットワークＢにサービスを提供していることを示している。ここで、複数のデバイスＥ１Ａ、Ｅ２Ａ、Ｅ３Ａ等は第１のネットワーク内に存在し、複数のデバイスＥ１Ｂ、Ｅ２Ｂ、Ｅ３Ｂ等は第２のネットワーク内に存在する。内部の通信用にプライベートアドレス空間が各ローカルネットワーク内で使用されるが、一般に、そのようなアドレス空間は多数のローカルネットワーク内で広範に再使用されるため、アドレス空間が相互に重複する可能性がある。さらに、各ゲートウェイ１０２および１０４は、以下に説明する方法でプライベートネットワークアドレスを変換する機能を含むと仮定する。ここで、この機能は、「ＮＡＴ」（Ｎｅｔｗｏｒｋ　Ａｄｄｒｅｓｓ　Ｔｒａｍｓｌａｔｉｏｎ）機能と呼ぶことがある。
【００３７】
ＶＰＮトンネルを確立する前に、ゲートウェイ１０２および１０４はそれぞれ、最初にそれらの名前とパブリックＩＰアドレスとをＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｅｒｖｅｒ）に登録することになる。この場合は、動的ＩＰアドレスと固定ＩＰアドレスとを両方とも可能にするＤＤＮＳ１０６（Ｄｙｎａｍｉｃ　ＤＮＳ）に登録することになる。ここで、これは、典型的にはゲートウェイを起動する時に行われる。また、ゲートウェイ１

０２および１０４は、それらの公開鍵と秘密鍵または暗号化用の証明書を、周知のＰＫＩ（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）メカニズムに従って生成し、そして、公開鍵がＰＫＩサーバ１０８に登録される。第１のステップ１：１は、図中の双方向矢印によって示されるように、両方のゲートウェイによって行われるＤＮＳ登録と鍵の確立とを略示する。従って、このステップは、通常の手順に従って実行することができ、ここでは、これ以上、この例を説明するために記述する必要はない。

【００３８】

その後のステップ１：２Ａと１：２Ｂとは、ゲートウェイ間でＶＰＮトンネルが確立されることを示し、また、各ゲートウェイが、自分自身のデバイスについて内部的に使用されるＩＰアドレス空間との重複を避けるように選択されている、対向ローカルネットワーク内のデバイスのためのＩＰアドレス空間を定義することを示している。従って、ゲートウェイ１０２は、ステップ１：２Ａでネットワーク Ｂのデバイス用のＩＰアドレス空間を定義し、一方、ゲートウェイ１０４は、ステップ１：２Ｂでネットワーク Ａのデバイス用のＩＰアドレス空間を定義する。ＶＰＮを確立することには、特に、各ゲートウェイの中に、上記で定義されたＩＰアドレス空間を、または少なくともその識別情報を、対向ゲートウェイの名前と関連のパブリックＩＰアドレスと共に記憶することが含まれる。ここで、それらは、ＤＤＮＳ１０６で利用可能であり、かつ検索される。

【００３９】

このようにして、あるローカルネットワーク内のゲートウェイが、他のローカルネットワークのゲートウェイとの複数のＶＰＮトンネルを確立することができ、少なくともトンネル識別情報と、そのネットワーク内で各対向ローカルネットワークについて使用される、重複しないＩＰアドレス空間とを含む変換テーブル等を、ゲートウェイの中に作成することができる。従って、これらのＩＰアドレス空間はいずれも、そのネットワーク内で使用される他のいかなるＩＰアドレス空間とも重複しないはずである。任意の対向ローカルネットワークの中のデバイスから着信データパケットが受信される度に、着信ＶＰＮトンネルが識別され、そして、変換テーブルの中のそのトンネルに関連するＩＰアドレス空間から取り込まれるローカルＩＰアドレスが、送信側ネットワークのデバイスについて受信側ネットワーク内で使用される。ここで、これについては、以下でより詳述する。

【００４０】

上記のように、変換テーブルは、各トンネル識別情報に関連付けられている、定義されたＩＰアドレス空間の識別表示を含んでもよい。例えば、ＩＰアドレス空間が、ＩＰｖ４（ＩＰ第４バージョン）に基づくアドレスを含む場合、各ＩＰアドレスの第２または第３オクテットの中の一意の数が、対応する対向ローカルネットワークを表すために、割り当てられてもよい。その結果、その一意の数が、変換テーブルの中のネットワークを識別するために十分である場合もある。例えば、１０．０．０．０／２４というアドレス空間が本ネットワークの中のデバイスについて使用される場合、ネットワーク識別表示として第３オクテットを使用して、例示的なＩＰアドレス空間、すなわち、１０．０．１．０／２４、１０．０．２．０／２４、１０．０．３．０／２４等が、異なる対向ネットワークについて定義されてもよい。しかしながら、他のアドレス指定スキームおよび適切なネットワーク識別表示が、同様に使用されてもよいのであって、本発明は、上記の例に限定されるものではない。

【００４１】

また、それによって、発信パケットのために正確なＶＰＮトンネルを、そのパケットの内部宛先アドレスの中の一意の数に基づいて判定することができ、次いで、その結果、そのパケットを、判定されたＶＰＮトンネルを介して送信することができる。送信側デバイスは、対向ローカルネットワーク内のデバイスについて定義されたＩＰアドレス空間の知識を得ることができ、かつ、パケット内の宛先アドレスは、受信側デバイスに割り当てられたものであると仮定する。

【００４２】

図１に戻ると、データパケットが、ローカルネットワーク Ｂの中の１つのデバイスＥ１

Ｂから、ローカルネットワークＡの中の別のデバイスＥ３Ａに向けて送信される。パケットは、ローカル宛先ＩＰアドレスとソースＩＰアドレスとを有する内部ヘッダを有しており、次のステップ１：３で、最初にゲートウェイ１０４で受信される。内部ヘッダでは、Ｅ３ＡとＥ１Ｂとの宛先ＩＰアドレスおよびソースＩＰアドレスはそれぞれ、送信側ネットワークＢで使用されているアドレスであるが、受信側ネットワークＡでは使用されていない。従って、受信側ネットワークＡの中で一義的なアドレス指定を行うには、これらのアドレスの変換が必要であり、それは、受信側ネットワークＡのゲートウェイ１０２によって行われることになる。従って、これによって、パケットが意図されている宛先デバイスに到達することが保証されることになる。

【００４３】

パケットを送信する前に、ゲートウェイ１０４は、他の識別スキームも可能であるけれども、内部ヘッダの中のプライベート宛先ＩＰアドレスに基づいて、例えば、上記の方法で、第２または第３オクテットから、ネットワークＡとのＶＰＮトンネルを識別し、そして、次のステップ１：４で、ゲートウェイ１０２および１０４のパブリックＩＰアドレスをそれぞれ宛先ＩＰアドレスおよびソースＩＰアドレスとして有する外部ヘッダを追加する。次いで、パケットが、次のステップ１：５で、パブリックＩＰネットワーク１００によってネットワークＡのゲートウェイ１０２へ送信される。次いで、外部ヘッダの中のパブリック宛先ＩＰアドレスを、パケットを従来の方法でパブリックＩＰネットワーク１００を経由してゲートウェイ１０２へとルーティングするために使用することができる。

【００４４】

データパケットを受信する場合、ゲートウェイ１０２は、その目的を満足する外部ヘッダを削除し、他方、送信側ネットワークを、パケットを送信するために使用されるＶＰＮトンネルから推定することができる。ここで、覚えておくべきことは、受信されるパケットは、受信側ネットワークＡではなくて送信側ネットワークＢの中で有効であったプライベート宛先アドレスとソースアドレスとを含むことである。従って、ゲートウェイ１０２は、次のステップ１：６で、受信側ネットワークＡで使用されるアドレスへと変換することによって、パケットの内部ヘッダの中の宛先アドレスとソースアドレスとを変更する。

【００４５】

詳細には、宛先アドレスは、デバイスＥ３ＡについてネットワークＡ内で使用される宛先アドレスへと変更され、そして、ソースアドレスは、デバイスＥ１ＢについてネットワークＡ内で使用される選択されたアドレス空間の内部ソースアドレスへと変更され、後者のアドレスは、従前にステップ１：２Ａでネットワーク内のデバイスについてゲートウェイ１０２によって定義された内部ＩＰアドレス空間から取り込まれる。後者のアドレスは、ＶＰＮトンネルの確立の間に、他のデバイスのアドレス割当に従って、デバイスＥ１Ｂに割り当てられているものであり、この情報は、着信パケットのためのアドレス変換を可能にするため、各ゲートウェイ１０２および１０４に記憶されているものである。アドレス割当は、所定のスキームに従って、例えば、カウンタが、第１の対向ローカルネットワークへの第３オクテットにおいて「１」を割り当て、第２の対向ローカルネットワークへの第３オクテットにおいて「２」を割り当て、以下同様にして割り当てることによって実行されても良い。また、アドレス割当は、固定であっても動的であってもよい。

【００４６】

図２は、上記で論じたデータパケットのヘッダが、図１について説明されるパケット送信の様々な段階でどのように構成されうるかの一例をより詳細に図示する。従って、図２の左側は、送信側デバイスＥ１Ｂと、それぞれネットワークＢのゲートウェイ１０４およびネットワークＡのゲートウェイ１０２と、そして、受信側デバイスＥ３Ａとを示している。

【００４７】

この例では、ネットワークＢは、自分自身のデバイスについてアドレス空間１０．０．０．０／２４を使用し、そして、アドレス空間１０．０．１．０／２４は、対向ネットワークＡのデバイスについて定義されている。従って、これらのアドレス空間における第３

オクテットは、デバイスのネットワークを示し、すなわち、ネットワークＢでは、「０」はネットワークＢを示し、「１」はネットワークＡを示している。また、反対側では、ネットワークＡは、自分自身のデバイスについてアドレス空間１０．０．０．０／２４を使用し、そして、アドレス空間１０．０．１．０／２４は、同様に、対向ネットワークＢのデバイスについて定義されている。従って、ネットワークＡでは、ネットワークＢでの状況とは逆に、「０」はネットワークＡを示し、「１」はネットワークＢを示している。

【００４８】

デバイスＥ１Ｂから送信されるパケットが、上記のステップ１：３に従って最初にゲートウェイ１０４で受信される場合、パケットは、デバイスＥ３Ａについて有効な宛先アドレス１０．０．１．１１と、デバイスＥ１Ｂについて有効なソースアドレス１０．０．０．４とを有する、ネットワークＢ内で有効な内部ヘッダを有する。上記のステップ１：４に従って、ゲートウェイ１０４は、ゲートウェイ１０２のパブリック宛先アドレスＩＰＡとゲートウェイ１０４のパブリックソースアドレスＩＰＢとを使って、外部ヘッダを追加する。次いで、ゲートウェイ１０４は、ネットワークＡを指し示す「１」というネットワーク指標から正確なＶＰＮトンネルを識別し、そして、上記のステップ１：５に従って、トンネルを介してパケットをゲートウェイ１０２へ送信する。

【００４９】

パケットを受信しているゲートウェイ１０２は、次いで、外部ヘッダを削除し、そして、プライベート宛先アドレスを１０．０．０．１１へ、かつ、ソースアドレスを１０．０．１．４へと変換することによって、内部ヘッダを変更する。ここで、それらは、ネットワークＡにおいてそれぞれデバイスＥ１ＢとＥ３Ａとについて有効である。内部ヘッダが修正されたパケットは、次いで、最終的には、上記のステップ１：７に従って、デバイスＥ３Ａへ転送される。ゆえに、上記のように、ネットワークＡおよびＢにおいて重複するアドレス空間が使用される場合であっても、内部ヘッダの中の宛先アドレスおよびソースアドレスは、それぞれのデバイスを適切に、かつ、受信側ネットワークＡにおける混乱のリスクを伴わずに、識別することになる。

【００５０】

また、デバイスＥ３Ａは、受信したソースアドレスを宛先アドレスとして、かつ、自分自身のプライベートアドレスをソースアドレスとして使用して、デバイスＥ１Ｂへのリプライとしてデータパケットを送信することができる。ここで、どちらのアドレスもネットワークＡでは有効である。その場合、上記の手順は、逆方向に繰り返されるでことになり、従って、受信側ゲートウェイ１０４は、宛先アドレスとソースアドレスとをネットワークＢで有効なもの変換戻すことによって、すなわち、１０．０．０．４（ソース）と１０．０．１．１１（宛先）とに変換することによって、内部ヘッダを変更することになる。

【００５１】

ここで、第１のローカルネットワークのゲートウェイによって実行される、第１のローカルネットワーク内の第１の通信デバイスと対向する第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を通信するための手順について、図３のフローチャートを参照しながら説明する。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で自身のそれぞれのデバイスについて使用されるプライベートＩＰアドレスが、例えば、典型的には、複数のローカルネットワーク内で再使用されるアドレス空間に属することによって、相互に重複する可能性があると仮定する。

【００５２】

第１のステップ３００で、対向する第２のローカルネットワーク内のゲートウェイとのＶＰＮトンネルが確立される。これには、特に、ＤＤＮＳから利用可能であって、かつ、検索することもできる、対向ゲートウェイの名前と関連のパブリックＩＰアドレスとを記憶することが含まれる。第２のステップ３０２で、プライベートＩＰアドレス空間が、第１のネットワーク内で自身のデバイスについて使用されるプライベートＩＰアドレス空間とは重複しないように選択されている、第２のネットワークについて定義される。さらに、対向する第２のゲートウェイが、同様に、重複しないプライベートＩＰアドレス空間を

第１のネットワークについても定義すると仮定する。ステップ３００および３０２は、基本的に、ステップ１：２Ａと１：２Ｂについて上述したように実行することができる。

【００５３】

次のステップ３０４では、後の何らかの時点で着信データパケットがＶＰＮトンネルを介して受信される。ここで、そのパケットは、第２のデバイスから送信されているものであって、それぞれ第１のデバイスおよび第２のデバイスについて第２のネットワーク内で使用される宛先アドレスとソースアドレスとを有する内部ヘッダを有する。次いで、次のステップ３０６で、第１のゲートウェイが、内部ヘッダの中の宛先アドレスとソースアドレスとを、それぞれ第１のデバイスと第２のデバイスについて第１のネットワーク内で使用される宛先アドレスとソースアドレスとに変更する。最後に示されるステップ３０８で、パケットは、内部ヘッダを修正された上で、第１のデバイスへ転送される。次いで、第１のデバイスは、受信したソースアドレスを宛先アドレスとして使用して、データパケットを第２のデバイスへ送信することによって、応答することができる。ここで、そのアドレスは、上記の方法で、受信側の第１のゲートウェイによって再び変換されることになる。

【００５４】

ここで、第１のゲートウェイ４００における装置について、図４のブロック図を参照しながら、より詳細に説明する。ゲートウェイ４００は、第１のローカルネットワークにサービスを提供していて、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のゲートウェイによってサービスが提供される第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、データパケットを通信できると仮定する。また、第１のゲートウェイと第２のゲートウェイとの間でＶＰＮトンネルが確立されていて、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おり、そして、各ローカルネットワーク内のデバイスについて、重複する可能性のあるプライベートＩＰアドレスが使用されていると仮定する。

【００５５】

ゲートウェイ４００は、第２のローカルネットワーク内のデバイスについて第１のローカルネットワーク内で使用されることになる、選択された内部ＩＰアドレス空間を定義するように構成されているＩＰアドレス定義手段４００ａを備える。選択された内部ＩＰアドレス空間は、第１のローカルネットワーク内のデバイスについて第１のローカルネットワーク内で使用される内部ＩＰアドレス空間とは別であり、すなわち、重複していない。

【００５６】

ゲートウェイ４００は、さらに、着信データパケットＰを第２のデバイスから受信するように構成されている受信手段４００ｂを備える。着信パケットＰは、外部ＩＰヘッダおよび内部ＩＰヘッダを有しており、後者は、第１のデバイスについて第２のローカルネットワーク内で使用される内部宛先アドレスと、第２のデバイスについて第２のローカルネットワーク内で使用される内部ソースアドレスとを含んでいる。

【００５７】

また、ゲートウェイ４００は、内部宛先アドレスを、第１のデバイスについて第１のローカルネットワーク内で使用される内部宛先アドレスに変更し、そして、内部ソースアドレスを、第２のデバイスについて第１のローカルネットワーク内で使用され、かつ、選択された内部ＩＰアドレス空間の中にある、選択されたアドレス空間の内部ソースアドレスに変更するように構成されている、ＩＰアドレス変更手段４００ｃを備える。また、ＩＰアドレス変更手段４００ｃは、受信したパケットから外部ＩＰヘッダを削除するように構成されている。

【００５８】

また、ゲートウェイ４００は、着信パケットＰ’を、変更された内部宛先アドレスおよびソースアドレスを含む、修正された内部ＩＰヘッダを使って第２のデバイスに転送するように構成されている転送手段４００ｄを備える。それによって、パケットヘッダの中のアドレスは、第２のローカルネットワーク内で有効な他のデバイスの任意のアドレスとも

別であって、混同され得ない。

【００５９】

ここまでは、基本的に、データパケット送信の受信側で何が行われるかについて、例えば、図１のネットワークＡのゲートウェイ１０２における手順と機能とについて、図３のフローチャートによって説明している。次に、図５のフローチャートを参照しながら、データパケット送信の送信側のゲートウェイによって何が行われるかについても、例えば、図１のネットワークＢのゲートウェイ１０４における手順と機能とについて、説明する。図３の場合と同一の状況を使用して、対向する第２のネットワーク内の第２のデバイスに向けられている第１のデバイスからの発信データパケットを受信する場合、以下のさらなる手順が、第１のゲートウェイによって実行されてもよい。

【００６０】

第１のステップ５００は、従って、第１のデバイスから到来する発信データパケットが受信されることを示している。この発信パケットは、第２のデバイスについて第１のローカルネットワーク内で使用される内部宛先アドレスと、第１のデバイスについて第１のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する。次のステップ５０２では、発信パケットについて、正確なＶＰＮトンネルが、内部宛先アドレスに基づいて判定される。例えば、使用されるＩＰアドレス空間が、ＩＰｖ４ベースのアドレスを含んでいる場合、対応する対向ローカルネットワークを表すために、各ＩＰアドレスの第２または第３オクテットに一意の番号を割り当てることができ、そうすれば、正確なＶＰＮトンネルが、その番号から判定される。

【００６１】

次のステップ５０４で、パケットが、パブリックＩＰネットワーク上でのルーティングを可能にする、それぞれ外部宛先アドレスおよびソースアドレスとして第１のゲートウェイおよび第２のゲートウェイのパブリックＩＰアドレスを含む外部ＩＰヘッダを使ってカプセル化される。最後のステップ５０６で、発信パケットが、判定されたＶＰＮトンネルを介してパブリックＩＰネットワーク上で第２のゲートウェイへ送信される。

【００６２】

第１のローカルネットワークと複数の対向ローカルネットワークとの間でＶＰＮトンネルを確立することは可能である。その場合、各対向ネットワーク内のデバイスについて第１のローカルネットワーク内で使用されることになる、選択された内部ＩＰアドレス空間が、各対向ネットワークについて定義される。そして、選択された各ＩＰアドレス空間は、第１のローカルネットワーク内で使用される任意の他の内部ＩＰアドレス空間とも別であり、すなわち、重複しないはずである。

【００６３】

さらに、対応する各対向ローカルネットワークを表すために、各ＩＰアドレスの第２または第３オクテットに一意の番号を割り当てることができる。その場合、各発信パケットについて、発信パケットの中の内部宛先アドレスにおけるその一意の番号に基づいて正確なＶＰＮトンネルを判定することができ、次いで、パケットは、判定されたＶＰＮトンネルを介して送信されることになる。さらに、ＶＰＮトンネルを確立することには、各ローカルネットワークのゲートウェイに、ＤＮＳに登録されている名前と各対向ゲートウェイの対応する公開ＰＫＩ鍵とを追加することが含まれる。

【００６４】

さらに、図４に示される実施形態に従って、信頼される当事者（パーティ群）が含まれた信頼リスト４００ｅを、第１のゲートウェイ４００内で第１のローカルネットワークについて作成することができる。候補ネットワーク４０２のゲートウェイとのＶＰＮトンネルを確立するためのリクエストの類が受信される場合、候補ローカルネットワークが信頼リスト４００ｅの中に存在する第１のユーザと関連付けられている場合、ＶＰＮトンネルの確立が許可されてもよい。さらに、ゲートウェイ４００は、候補ローカルネットワーク４０２が第１のパーティの信頼リストの中に存在する第２のユーザと関連付けられていることによって信頼リストの中の第１のパーティと間接的に関連付けられている場合、ＶＰ

Ｎトンネルの確立が許可されるように構成されてもよい。さらに、ゲートウェイ４００は、第１のローカルネットワークについて承認される所定数の信頼性レベルに依存して、ＶＰＮトンネルの確立が許可されるように構成されてもよい。

【００６５】

上記のように、候補ローカルネットワーク４０２は、候補ローカルネットワークからのＶＰＮトンネルリクエストＲに応じて、信頼リスト４００ｅに基づいて、ＶＰＮトンネルの確立について評価されてもよい。さらに、ゲートウェイ４００は、２つのローカルネットワーク間で確立されたＶＰＮトンネルが、いずれかのネットワークに関連付けられている信頼リストが、そのＶＰＮトンネルを不適格とみなすように修正される場合、自動的に終了されるように構成されてもよい。

【００６６】

ここで、ＶＰＮトンネルリクエストのために第１のゲートウェイにおいて上記の方法で信頼リストを使用するための例示的な手順について、図６のフローチャートを参照しながら簡単に説明する。まず、最初のステップ６００によって略示されるように、信頼されたパーティユーザを含む信頼リストが、第１のローカルネットワークについて作成される。次のステップ６０２に従って、ある時点で、候補ネットワーク内のゲートウェイとのＶＰＮトンネルを確立するためのリクエストが受信される場合、次のステップ６０４で、候補ネットワークが、作成された信頼リストに基づいて評価される。

【００６７】

次いで、リクエストされたＶＰＮトンネルが許可されるかどうかが、ステップ６０６で判定される。ここでは、例えば、すでに信頼されている当事者（パーティ群）の信頼リストの複数のレベルを考慮して、上記のように、信頼リストから導出することができる。許可される場合、最後のステップ６０８で示されるように、ＶＰＮトンネルが確立され、データパケットを、上記の記述に従って通信することができる。信頼リストがＶＰＮトンネルを許可しない場合、ステップ６１０で、リクエストは拒否されるか、または単純に無視される。

【００６８】

さらに図４に示されるように、上記のゲートウェイ４００の中の機能性ユニットが、第１のゲートウェイ４００上で実行される場合には、第１のゲートウェイの上記の機能群とステップ群とを第１のゲートウェイに実行させるコード手段を備える、コンピュータプログラム４０４のプログラムモジュールとして実装することができる。この実施形態では、コンピュータプログラム４０４は、コンピュータプログラムが記憶されているコンピュータ可読媒体を含むコンピュータプログラム製品４０６によって搬送される。

【００６９】

コンピュータプログラム４０４のプログラムモジュールは、少なくとも、アドレス空間定義モジュール４０４ａとアドレス変更モジュール４０４ｂとを含んでいる。アドレス空間定義モジュール４０４ａは、第２のローカルネットワーク内のデバイスについて第１のローカルネットワーク内で使用されることになる、選択された内部ＩＰアドレス空間を定義することができ、この選択されたＩＰアドレス空間は、第１のローカルネットワーク内のデバイスについて第１のローカルネットワーク内で使用される内部ＩＰアドレス空間とは別であり、すなわち、重複していない。

【００７０】

アドレス変更モジュール４０４ｂは、第１のデバイスについて第２のローカルネットワーク内で使用される内部宛先アドレスと第２のデバイスについて第２のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する着信パケットを、第２のデバイスからＶＰＮトンネルを介して受信する場合に、内部宛先アドレスを、第１のデバイスについて第１のローカルネットワーク内で使用される内部宛先アドレスに変更することと、内部ソースアドレスを、第２のデバイスについて第１のローカルネットワーク内で使用される選択されたアドレス空間の内部ソースアドレスであって、選択された内部ＩＰアドレス空間の中にある内部ソースアドレスに変更することとができる。次いで

、着信パケットが、変更された宛先アドレスとソースアドレスとを含む修正された内部ＩＰヘッダを使って、第１のデバイスに転送される。

【００７１】

また、コンピュータプログラム４０４およびコンピュータプログラム製品４０６のコード手段は、第１のゲートウェイに、下記の機能群を実行させてもよい。

【００７２】

着信パケットが、第１のゲートウェイのパブリックＩＰアドレスおよび第２のゲートウェイのパブリックＩＰアドレスをそれぞれ外部宛先アドレスおよび外部ソースアドレスとして含む外部ＩＰヘッダを有する場合、コード手段が、第１のゲートウェイに着信パケットから外部ＩＰヘッダを削除させてもよい。

【００７３】

また、発信データパケットが第１のデバイスから受信され、その発信パケットが、第２のデバイスについて第１のローカルネットワーク内で使用される内部宛先アドレスと、第１のデバイスについて第１のローカルネットワーク内で使用される内部ソースアドレスとを含む内部ＩＰヘッダを有する場合、コード手段が、第１のゲートウェイに、

－それぞれ外部宛先アドレスおよび外部ソースアドレスとして、ゲートウェイのパブリックＩＰアドレスを含む外部ＩＰヘッダを使ってパケットをカプセル化させ、そして

－発信パケットがＶＰＮトンネルを介して第２のゲートウェイへ送信される前に、内部宛先アドレスに基づいて、その発信パケットについての正確なＶＰＮトンネルを判定させる

ようにしてもよい。

【００７４】

また、コード手段は、第１のゲートウェイに、第１のローカルネットワークと複数の対向ローカルネットワークとの間にＶＰＮトンネルを確立させ、そして、各対向ネットワーク内のデバイスについて第１のネットワーク内で使用されることになる、選択された内部ＩＰアドレス空間を、各対向ネットワークについて定義させてもよく、この選択された各ＩＰアドレス空間は、第１のローカルネットワーク内で使用される任意の他のアドレス空間とも別であり、すなわち、重複していない。

【００７５】

選択されたＩＰアドレス空間は、ＩＰｖ４ベースのアドレスを含んでもよく、次いで、各ＩＰアドレスの第２または第３オクテットの中の一意の数が、対応する対向ローカルネットワークを表すために割り当てられてもよい。また、その場合、コード手段は、第１のゲートウェイに、各発信パケットについて、発信パケットの中の内部宛先アドレスの中の一意の数に基づいて、ＶＰＮトンネルを判定させてもよく、その場合、パケットは、次いで、判定されたＶＰＮトンネルを介して送信される。

【００７６】

また、コード手段は、第１のゲートウェイに、各対向ゲートウェイのＤＮＳ登録名と対応する公開ＰＫＩ鍵とを追加することによって、ＶＰＮトンネルを確立させてもよい。公開ＰＫＩ鍵および対応する秘密ＰＫＩ鍵が、各ゲートウェイについて生成されていてもよく、公開ＰＫＩ鍵は、ゲートウェイに対してアクセス可能なＰＫＩサーバの中に記憶される。

【００７７】

信頼されたパーティ群が含まれた信頼リストが第１のローカルネットワークについて作成されている場合、候補ローカルネットワークが信頼リストの中に存在する第１のパーティと関連付けられている場合、コード手段は、第１のゲートウェイに、第１のローカルネットワークと候補ローカルネットワークとの間でのＶＰＮトンネルの確立を許可させてもよい。

【００７８】

また、コード手段は、候補ローカルネットワークが第１のパーティの信頼リストの中に存在する第２のパーティと関連付けられることによって、信頼リストの中の第１のパーテ

ィと間接的に関連付けられる場合、第１のゲートウェイに、ＶＰＮトンネルの確立を許可させてもよい。

【００７９】

また、コード手段は、第１のローカルネットワークについて許可される、所定数の信頼性レベルに依存して、第１のゲートウェイに、ＶＰＮトンネルの確立を許可させてもよい。

【００８０】

また、コード手段は、候補ローカルネットワークからのＶＰＮトンネルリクエストに応じて、第１のゲートウェイに、ＶＰＮトンネルの確立について候補ローカルネットワークを評価させてもよい。

【００８１】

また、コード手段は、いずれかのネットワークに関連付けられている信頼リストが、そのＶＰＮトンネルを不適格とみなすように修正される場合、第１のゲートウェイに、２つのローカルネットワーク間で、確立されたＶＰＮトンネルを自動的に終了させてもよい。

【００８２】

留意すべきことは、図４は、ゲートウェイ４００の中の各種の例示的な機能性ユニットとプログラムモジュールとを単に論理的な意味で示しているにすぎず、他方、当業者であれば、実際には、任意の適切なソフトウェアおよびハードウェア手段を使用して自由に実装することができることである。従って、本発明は、一般に、ゲートウェイ４００の図示する構造に限定されるものではない。例えば、コンピュータプログラム製品は、フラッシュメモリ、ＲＯＭ（Ｒｅａｄ－Ｏｎｌｙ　Ｍｅｍｏｒｙ）またはＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　ＲＯＭ）であってもよいし、上記のコンピュータプログラムモジュールは、代替実施形態では、ゲートウェイ４００の範囲内のメモリという形で、異なるコンピュータプログラム製品上に分散されてもよいだろう。

【００８３】

本発明について、特定の実施形態を参照して記載しているが、この記載は、一般に、発明の概念を例示することだけを意図しており、本発明の範囲を限定していると解釈されるべきではない。本発明は、添付の請求項によって定義される。

【図１】

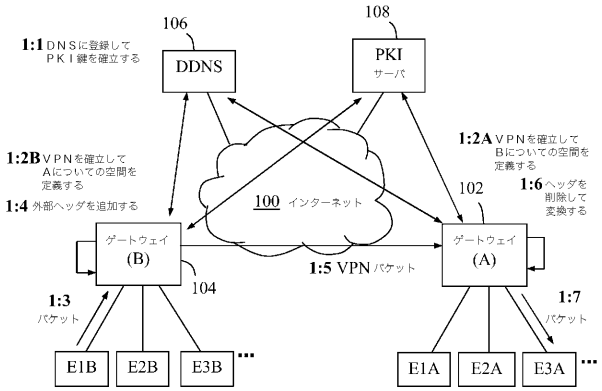

Fig.1

【図２】

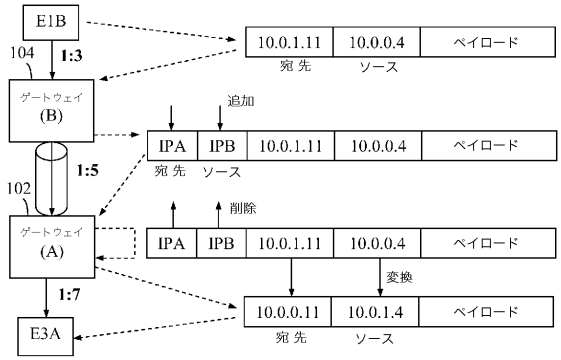

Fig.2

【図３】

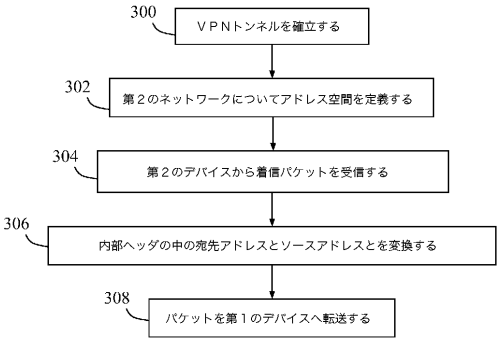

Fig.3

【図４】

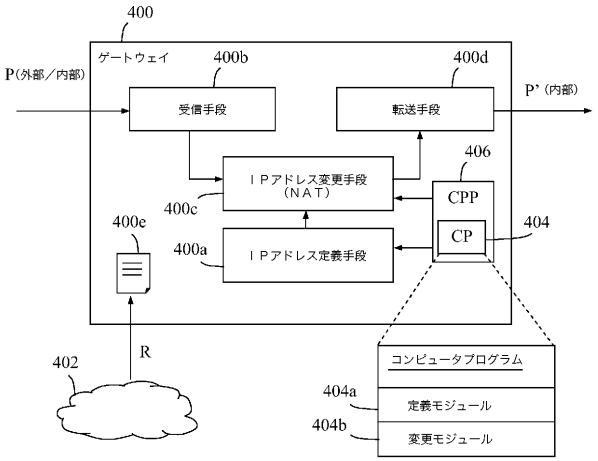

Fig.4

【図５】

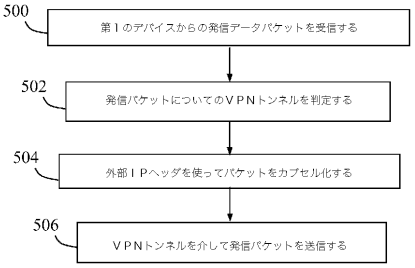

Fig.5

【図６】

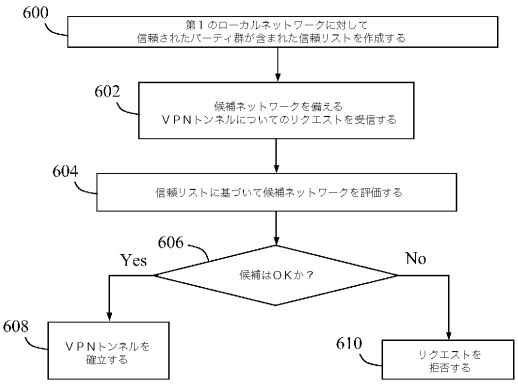

Fig.6

【国際調査報告】

1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2009/050292

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ, INTERNET

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 20070097977 A1 (E.B. BODEN ET AL), 3 May 2007 (03.05.2007), figure 4, abstract, paragraphs (0001)-(0007), (0018), (0038), (0056)-(0057) --	1-28
Y	US 6888837 B1 (T. CUNNINGHAM ET AL), 3 May 2005 (03.05.2005), column 11, line 50 - column 12, line 56, figures 1,7, abstract --	1-28
A	US 20040218611 A1 (J.-H. KIM), 4 November 2004 (04.11.2004), figures 1,5,6, abstract, paragraphs (0015)-(0019), (0059)-(0062), (0075)-(0078), (0095)-(0107) --	1-28

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 June 2009	29-06-2009
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Hassan Khatoun Neama / MRo Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2009/050292

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 7333510 B1 (M.G. HIES ET AL), 19 February 2008 (19.02.2008), column 1, line 61 - column 2, line 57, abstract -- ---------	1-28

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2009/050292

International patent classification (IPC)

H04L 29/12 (2006.01)
H04L 12/46 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded:
- From "Cited documents" found under our online services at www.prv.se (English version)
- From "Anförda dokument" found under "e-tjänster" at www.prv.se (Swedish version)

Use the application number as username. The password is **RMKSSSTAWT.**

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SE2009/050292

US	20070097977	A1	03/05/2007	NONE
US	6888837	B1	03/05/2005	NONE
US	20040218611	A1	04/11/2004	NONE
US	7333510	B1	19/02/2008	NONE

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(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－１８５ ３９, スロンベルスリンガン ２２
(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－３１０ ４４, 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 イェルフェッラ エス－１７５ ６６, ニダロスリンガン ５８
(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－１７１ ６０, ウィボムス ヴェグ １０

Ｆターム(参考) 5K030 GA15 HA08 HC01 HD03 HD06 HD09