

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第6073338号  
(P6073338)

(45) 発行日 平成29年2月1日(2017.2.1)

(24) 登録日 平成29年1月13日(2017.1.13)

(51) Int. Cl.	F I				
<b>GO6F 13/00</b>	<b>(2006.01)</b>	GO6F	13/00	510A	
<b>HO4W 12/08</b>	<b>(2009.01)</b>	HO4W	12/08		
<b>HO4W 76/02</b>	<b>(2009.01)</b>	HO4W	76/02		
<b>HO4L 12/66</b>	<b>(2006.01)</b>	HO4L	12/66	A	
<b>HO4L 12/70</b>	<b>(2013.01)</b>	HO4L	12/70	A	
請求項の数 14 (全 20 頁) 最終頁に続く					

(21) 出願番号	特願2014-535202 (P2014-535202)	(73) 特許権者	598036300
(86) (22) 出願日	平成24年10月9日 (2012.10.9)		テレフオンアクチーボラゲット エルエム
(65) 公表番号	特表2015-504192 (P2015-504192A)		エリクソン (パブル)
(43) 公表日	平成27年2月5日 (2015.2.5)		スウェーデン国 ストックホルム エスー
(86) 国際出願番号	PCT/IB2012/055459		164 83
(87) 国際公開番号	W02013/054260	(74) 代理人	100095957
(87) 国際公開日	平成25年4月18日 (2013.4.18)		弁理士 亀谷 美明
審査請求日	平成27年9月9日 (2015.9.9)	(74) 代理人	100096389
(31) 優先権主張番号	13/271,056		弁理士 金本 哲男
(32) 優先日	平成23年10月11日 (2011.10.11)	(74) 代理人	100101557
(33) 優先権主張国	米国 (US)		弁理士 萩原 康司
		(74) 代理人	100128587
			弁理士 松本 一騎
最終頁に続く			

(54) 【発明の名称】 仮想化されたホームIPサービスデリバリのためのアーキテクチャ

(57) 【特許請求の範囲】

【請求項1】

インターネットサービスプロバイダのネットワークエレメントにより実装される、訪問先ネットワークオーナーに関連付けられる訪問先ネットワークを通じてネットワークアクセスを前記訪問先ネットワークに接続する訪問ユーザのデバイスに提供するための方法であって、前記訪問先ネットワークオーナーは、前記インターネットサービスプロバイダの顧客であり、前記ネットワークエレメントは、遠隔のホームネットワークのリソースへのアクセスを前記訪問ユーザの前記デバイスへ提供するように前記訪問先ネットワークを設定し、前記遠隔のホームネットワークは、ワイドエリアネットワーク上で前記訪問先ネットワークとの通信関係にあり、前記方法は、

前記訪問ユーザの前記デバイスから、前記訪問先ネットワークの第1のアクセスポイントを通じて接続リクエストを受信するステップと、

前記第1のアクセスポイントを通じて、前記訪問先ネットワークと前記訪問ユーザの前記デバイスとの間の前記接続を確立するステップと、

前記第1のアクセスポイントを通じて、前記訪問ユーザの前記デバイスから、前記遠隔のホームネットワークのリソースへ接続するためのリクエストを受信するステップと、

前記遠隔のホームネットワークの仮想ゲートウェイコントローラへ接続して、前記デバイスと前記遠隔のホームネットワークとの間の接続を確立するための設定情報を取得するステップと、

前記遠隔のホームネットワークの前記仮想ゲートウェイコントローラから取得される前

記設定情報に基づいて、前記遠隔のホームネットワークのリソースへ接続するための第2のアクセスポイントを、前記訪問先ネットワーク上に設定するステップと、

前記訪問ユーザの前記デバイスと前記第2のアクセスポイントとの間の接続を確立するステップと、

前記遠隔のホームネットワークのために前記デバイスの認証を遂行するステップと、

前記第2のアクセスポイントを通じて、前記遠隔のホームネットワークの前記リソースへのアクセスを提供するステップと、

を含む方法。

【請求項2】

前記訪問先ネットワークのために前記デバイスを認証するステップ、

をさらに含む、請求項1の方法。

10

【請求項3】

前記第2のアクセスポイントは、仮想ローカルエリアネットワークポート及び無線ローカルエリアネットワークのサービスセット識別子(SSID)のうちのいずれか1つである、請求項1の方法。

【請求項4】

前記遠隔のホームネットワークの前記仮想ゲートウェイコントローラと前記訪問先ネットワーク上の前記デバイスとの間で、仮想ローカルエリアネットワーク接続を確立するステップ、

をさらに含む、請求項1の方法。

20

【請求項5】

前記訪問先ネットワークのネットワーク設定インタフェースを通じた前記訪問先ネットワークオーナーの承認に応じて、前記訪問先ネットワーク上のリソースへのアクセスを前記デバイスへ提供するステップ、

をさらに含む、請求項1の方法。

【請求項6】

前記第1のアクセスポイントは、前記訪問先ネットワークのゲストネットワークである、請求項1の方法。

【請求項7】

前記デバイスのリソースリクエストに応じて、前記ネットワーク設定インタフェースを通じて、前記訪問先ネットワークの前記訪問先ネットワークオーナーへ承認を問い合わせるステップ、

をさらに含む、請求項5の方法。

30

【請求項8】

訪問先ネットワークオーナーに関連付けられる訪問先ネットワークを通じてネットワークアクセスを前記訪問先ネットワークオーナーの前記訪問先ネットワークを訪問している訪問ユーザのデバイスに提供するための、インターネットサービスプロバイダのネットワークエレメントであって、前記訪問先ネットワークオーナーは、前記インターネットサービスプロバイダの顧客であり、前記ネットワークエレメントは、遠隔のホームネットワークのリソースへのアクセスを前記訪問ユーザの前記デバイスへ提供するように前記訪問先ネットワークオーナーの前記訪問先ネットワークを設定し、前記遠隔のホームネットワークは、ワイドエリアネットワーク上で前記訪問先ネットワークとの通信関係にあり、前記ネットワークエレメントは、

仮想ゲートウェイコントローラとインターネットサービスルータとを実行するネットワークプロセッサ、を備え、

前記インターネットサービスルータは、前記訪問先ネットワークとの間でデータトラフィックを転送し、

前記仮想ゲートウェイコントローラは、前記インターネットサービスルータに通信可能に結合され、レジデンシャルゲートウェイを通じて前記訪問先ネットワークとの通信関係にあり、前記仮想ゲートウェイコントローラは、前記訪問先ネットワークの設定を管理し

40

50

前記仮想ゲートウェイコントローラは、前記デバイスが第1のアクセスポイントを通じて前記訪問先ネットワークへ接続した後、遠隔仮想ゲートウェイコントローラへ接続して前記デバイスと前記遠隔のホームネットワークとの間の接続を確立するための設定情報を取得することにより、前記訪問ユーザの前記デバイスのために前記訪問先ネットワークを通じて前記遠隔のホームネットワークのリソースへのアクセスを可能とするように、前記仮想ゲートウェイコントローラを前記遠隔のホームネットワークの前記遠隔仮想ゲートウェイコントローラへ接続する遠隔アクセスモジュールを含み、

前記仮想ゲートウェイコントローラは、前記デバイスが前記遠隔のホームネットワークと通信するため及び前記遠隔のホームネットワークのリソースにアクセスするために、前記遠隔仮想ゲートウェイコントローラから取得される前記設定情報に基づいて、前記訪問先ネットワーク内の別個のアクセスポイントを提供するように、前記訪問先ネットワークを設定する、

ネットワークエレメント。

【請求項9】

前記仮想ゲートウェイコントローラは、  
前記訪問先ネットワークのために前記デバイスを認証する認証モジュール、  
をさらに備える、請求項8のネットワークエレメント。

【請求項10】

前記仮想ゲートウェイコントローラは、前記別個のアクセスポイントを、仮想ローカルエリアネットワークポート及び無線ローカルエリアネットワークのサービスセット識別子（SSID）のうちのいずれか1つとして設定する、請求項8のネットワークエレメント

【請求項11】

前記遠隔アクセスモジュールは、前記遠隔のホームネットワークの前記遠隔仮想ゲートウェイコントローラと前記訪問先ネットワーク上の前記デバイスとの間で仮想ローカルエリアネットワーク接続を確立するように構成される、請求項8のネットワークエレメント

【請求項12】

前記訪問先ネットワークオーナーの承認に応じて、前記デバイスによる前記訪問先ネットワーク上のリソースへのアクセスを管理するように構成されるネットワーク設定モジュール、

をさらに備える、請求項8のネットワークエレメント。

【請求項13】

前記第1のアクセスポイントは、前記訪問先ネットワークのゲストネットワークである、請求項8のネットワークエレメント。

【請求項14】

ネットワーク設定インターフェースを通じて、前記デバイスのリソースリクエストに応じて、前記訪問先ネットワークオーナーへ承認を問い合わせるように構成されるネットワーク設定モジュール、

をさらに備える、請求項12のネットワークエレメント。

【発明の詳細な説明】

【技術分野】

【0001】

[関連出願への相互参照]

本出願と同日に提出され共通に所有されているWassim Haddadらによる“PROVIDING VIRTUALIZED VISIBILITY THROUGH ROUTERS”についての同時係属中の特許出願への相互参照がなされる。相互参照される当該出願は、参照によりここに取り入れられる。

【0002】

10

20

30

40

50

## 【発明の分野】

本発明の実施形態は、インターネットアクセスを訪問ユーザデバイスと共有することに関する。より具体的には、本発明の実施形態は、他のホームネットワークを訪問しているユーザデバイスについて、遠隔のホームネットワークからのリソースへのアクセスを可能とするための方法及びシステムに関する。

## 【背景技術】

## 【0003】

ホームネットワークは、ホーム内のデバイスを互いに及びインターネットへ接続するために利用される。それらホームネットワークは、レジデンシャルゲートウェイ（R G W）として知られるデバイスを介して、住宅用のインターネットサービスプロバイダへ接続される。このデバイスは、ホームネットワークとアクセスネットワーク（即ち、ブロードバンドリモートアクセスサーバ（B R A S）ルータ又はブロードバンドネットワークゲートウェイ（B N G）といった、インターネットサービスプロバイダのアクセス制御デバイスを含む、インターネットサービスプロバイダのコアネットワーク）との間の物理的な及びプロトコルの接続性を提供する。

10

## 【0004】

R G Wは、ホームネットワークについてのブリッジング又はルーティングのサポートを提供することができる。R G Wは、典型的には、ファイアウォール保護及びネットワークアドレス変換といった追加的なサービスをも提供する。R G Wは、有線及び無線の双方のプロトコル及び接続を用いて、ホーム内のデバイスと接続することができる。R G Wは、イーサネット接続のセットと共に、I E E E 8 0 2 . 1 1 ( a / b / g / n ) を用いた無線ローカルエリアネットワークを提供することができる。R G Wは、V O I P (Voice Over Internet Protocol) といったサービスのためのサービスデリバリ、又は共有テレビジョンデリバリのようなサービスのための逆多重化のポイントであることもできる。

20

## 【0005】

いくつかの状況において、ホームネットワークは、1つより多くのアタッチされたルータを有し得る。それら追加的なルータは、ベース又はルートを形成するR G Wと共に、階層又はツリーを形成する。好適なアーキテクチャはそうしたルータを回避することになる一方で、そうしたホームネットワークのトポロジー内のデバイスについての可視性をインターネットサービスプロバイダが有することは、それらが使用される場合には有益である。しかしながら、それらトポロジー内のルータに接続されたデバイスのアドレスは、当該デバイスに最も近いルータがR G Wの代わりに当該デバイスのためのI Pアドレスを設定することに起因して、隠蔽される。

30

## 【0006】

個人が他の個人のホームを訪問する場合に、当該個人は、ホームネットワークへコンピューティングデバイスを接続することを望むかもしれない。訪問先ネットワーク内のR G W又は他のルータは、無線サービスセット識別子（S S I D）といったゲストネットワークアクセスポイントを提供しなければならず、又はパスワード若しくはネットワークへのダイレクトアクセスを提供しなければならず、それは訪問先ネットワークのセキュリティを低下させる。いずれのケースでも、訪問ユーザは、訪問先ネットワークがそれを許可するように設定されなければならない仮想プライベートネットワークソフトウェアといった特殊なソフトウェアを使用しなければ、当該ユーザ自身のホームネットワークのリソースへのアクセスを有しない。それらホームネットワークのリソースは、プリンタ、ネットワークストレージ、メディアサーバ及び類似のネットワークリソースであり得る。当該リソースは、サービス品質レベル、ビデオストリーミングサービス、V O I Pサービス、共有テレビジョンデリバリ及び類似のサービスといった、ホームネットワークのためのインターネットサービスプロバイダのサービスでもあり得る。

40

## 【発明の概要】

## 【課題を解決するための手段】

## 【0007】

50

インターネットサービスプロバイダのネットワークエレメントにより実装される、訪問先ネットワークオーナーに関連付けられる訪問先ネットワークを通じてネットワークアクセスを訪問先ネットワークへ接続する訪問ユーザのデバイスに提供するための方法であって、訪問先ネットワークオーナーは、インターネットサービスプロバイダの顧客であり、ネットワークエレメントは、遠隔のホームネットワークのリソースへのアクセスを訪問ユーザのデバイスへ提供するように訪問先ネットワークを設定し、遠隔のホームネットワークは、ワイドエリアネットワーク上で訪問先ネットワークとの通信関係にあり、方法は、訪問ユーザのデバイスから、訪問先ネットワークの第1のアクセスポイントを通じて接続リクエストを受信するステップと、第1のアクセスポイントを通じて、訪問先ネットワークと訪問ユーザのデバイスとの間の接続を確立するステップと、第1のアクセスポイントを通じて、訪問ユーザのデバイスから、遠隔のホームネットワークのリソースへ接続するためのリクエストを受信するステップと、遠隔のホームネットワークの仮想ゲートウェイコントローラへ接続して、デバイスと遠隔のホームネットワークとの間の接続を確立するための設定情報を取得するステップと、遠隔のホームネットワークのリソースへ接続するための第2のアクセスポイントを、訪問先ネットワーク上に設定するステップと、訪問ユーザのデバイスと第2のアクセスポイントとの間の接続を確立するステップと、遠隔のホームネットワークのためにデバイスの認証を遂行するステップと、第2のアクセスポイントを通じて、遠隔のホームネットワークのリソースへのアクセスを提供するステップと、を含む方法。

10

**【0008】**

20

ホームネットワークオーナーに関連付けられる訪問先ネットワークを通じてネットワークアクセスをホームネットワークオーナーの訪問先ネットワークへ接続された訪問ユーザのデバイスに提供するための、インターネットサービスプロバイダのネットワークエレメントであって、訪問先ネットワークオーナーは、インターネットサービスプロバイダの顧客であり、ネットワークエレメントは、遠隔のホームネットワークのリソースへのアクセスを訪問ユーザのデバイスへ提供するように訪問先ネットワークオーナーの訪問先ネットワークを設定し、遠隔のホームネットワークは、ワイドエリアネットワーク上で訪問先ネットワークとの通信関係にあり、ネットワークエレメントは、仮想ゲートウェイコントローラとインターネットサービスルータとを実行するネットワークプロセッサ、を備え、インターネットサービスルータは、訪問先ネットワークとの間でデータトラフィックを転送し、仮想ゲートウェイコントローラは、インターネットサービスルータに通信可能に結合され、レジデンシャルゲートウェイを通じて訪問先ネットワークとの通信関係にあり、仮想ゲートウェイコントローラは、訪問先ネットワークの設定を管理し、仮想ゲートウェイコントローラは、遠隔仮想ゲートウェイコントローラへ接続してデバイスと遠隔のホームネットワークとの間の接続を確立するための設定情報を取得することにより、訪問ユーザのデバイスのために訪問先ネットワークを通じて遠隔のホームネットワークのリソースへのアクセスを可能とするように、仮想ゲートウェイコントローラを遠隔のホームネットワークの遠隔仮想ゲートウェイコントローラへ接続する遠隔アクセスモジュールを含み、仮想ゲートウェイコントローラは、デバイスが遠隔のホームネットワークと通信するため及び遠隔のホームネットワークのリソースにアクセスするために、訪問先ネットワーク内の別個のアクセスポイントを提供するように、訪問先ネットワークを設定する、ネットワークエレメント。

30

40

**【図面の簡単な説明】****【0009】**

本発明は、限定としてではなく例示として、添付の図面の各図に示されており、図面において、類似の参照符号は類似の要素を指す。本開示の異なる箇所では「一(“an”)又は1つの“one”）」実施形態という場合、それらは必ずしも同じ実施形態を指すとは限らず、そうした言及は、少なくとも1つを意味するものであることに留意すべきである。さらに、特定の特徴、構造、又は特性が一実施形態との関連で記述される場合、それは、明示的に記述されているか否かにかかわらず、他の実施形態との関連でそうした特徴、構造

50

、又は特性を作用させることが当業者の知識の範囲内であることが提起される。

【0010】

【図1】ルータを通じて仮想化された可視性を実装するネットワークの1つの実施形態の図である。

【図2】ホームネットワークルータと仮想ゲートウェイコントローラとの間のメッセージングの1つの実施形態の図である。

【図3】レジデンシャルルータを通じて仮想化された可視性を可能とするための処理の1つの実施形態の流れ図である。

【図4】仮想ゲートウェイコントローラにインタフェースするマシンツーマシンシステムのためのアーキテクチャの1つの実施形態の図である。

【図5】遠隔のホームネットワーク及び訪問先ネットワークの1つの実施形態の図である。

【図6】遠隔のホームネットワークリソースへのアクセスを可能とするための処理の1つの実施形態の流れ図である。

【発明を実施するための形態】

【0011】

これ以降の記述では、多数の具体的詳細が示される。しかしながら、本発明の実施形態はそれら具体的詳細なしでも実施され得ることが理解される。場合によっては、この記述の理解を曖昧にしないように、周知の回路、構造及び技法は詳細に示されていない。しかしながら、当業者には、本発明がそうした具体的詳細なしでも実施され得ることが理解されるであろう。当業者は、本明細書に含まれる記述を読めば、過度の実験なしで適切な機能性を実装することができるであろう。

【0012】

流れ図の動作は、図1、図2及び図5の例示的な実施形態を参照して記述される。しかしながら、図3及び図6の流れ図の動作は、図1、図2及び図5を参照して論じられる実施形態以外の本発明の実施形態によっても実行することができ、図1、図2及び図5を参照して論じられる実施形態は、図3及び図6の流れ図を参照して論じられる動作とは異なる動作を実行することもできることを理解すべきである。

【0013】

各図に示す技法は、1若しくは複数の電子デバイス（端局、ネットワークエレメント、サーバ又は類似の電子デバイスなど）上で記憶され、実行されるコード及びデータを用いて実装され得る。そうした電子デバイスは、非一時的な機械読取可能な又はコンピュータ読取可能な記憶媒体（磁気ディスク、光ディスク、ランダムアクセスメモリ、読取り専用メモリ、フラッシュメモリデバイス、及び相変化メモリなど）といった、非一時的な機械読取可能な又はコンピュータ読取可能な媒体を用いて、コード及びデータを記憶し、（内部で、及び/又はネットワーク上で他の電子デバイスと）通信する。加えて、そうした電子デバイスは、典型的には、1若しくは複数のストレージデバイス、ユーザ入力/出力デバイス（キーボード、タッチスクリーン、及び/又はディスプレイなど）、並びにネットワーク接続といった1若しくは複数の他の構成要素に結合された1若しくは複数のプロセッサのセットも含む。プロセッサのセットと他の構成要素との結合は、典型的には、1若しくは複数のバス及び（バスコントローラとも呼ばれる）ブリッジを通じたものである。ストレージデバイスは、1若しくは複数の非一時的な機械読取可能若しくはコンピュータ読取可能な記憶媒体又は非一時的な機械読取可能若しくはコンピュータ読取可能な通信媒体を表す。よって、所与の電子デバイスのストレージデバイスは、典型的には、当該電子デバイスの1若しくは複数のプロセッサのセット上で実行するためのコード及び/又はデータを記憶する。当然ながら、本発明の実施形態の1若しくは複数の部分が、ソフトウェア、ファームウェア、及び/又はハードウェアの異なる組み合わせを用いて実装されてもよい。

【0014】

本明細書で使用される場合、ネットワークエレメント（ルータ、スイッチ、ブリッジ、

10

20

30

40

50

又は類似のネットワーキングデバイスなど)とは、ネットワーク上の他の設備(他のネットワークエレメント、端局、又は類似のネットワーキングデバイスなど)を通信可能に相互接続するハードウェア及びソフトウェアを含むネットワーキング設備である。あるネットワークエレメントは、複数のネットワーキング機能(ルーティング、ブリッジング、スイッチング、レイヤ2集約、セッションポード制御、マルチキャスト、及び/若しくは加入者管理など)のサポートを提供し、並びに/又は複数のアプリケーションサービス(データ収集など)のサポートを提供する、“マルチサービスネットワークエレメント”である。

**【0015】**

本発明の実施形態は、先行技術の不都合点を回避するための方法及びシステムを提供する。ホームネットワーキングの必要が増すにつれて、レジデンシャルゲートウェイに対する要求も高まっている。よって、レジデンシャルゲートウェイはより複雑で、誤りがち(error prone)で、高価なものとなっている。また、インターネットサービスプロバイダの顧客又はレジデンシャルゲートウェイの購入者へ新しい特徴的機能を提供するためには、レジデンシャルゲートウェイのためのソフトウェアアップグレードが行われる必要もあり、これは、多くのホームユーザが困難であると認める課題である。この問題は、ホームユーザにそれら新しいサービスを利用することを躊躇させるおそれがある。

10

**【0016】**

レジデンシャルゲートウェイ及び他の宅内ネットワーク接続デバイスを適正に設定することの複雑さは、多くのユーザにとってそのホームネットワーク及びアタッチされるデバイスを設定するのが極めて困難であるほどにまで増大している。この結果として、インターネットサービスプロバイダ及びレジデンシャルゲートウェイの製造者のサポートコストが増加している。

20

**【0017】**

レジデンシャルゲートウェイが単にブリッジとして機能する場合といった、レジデンシャルゲートウェイに限られた機能性しか有しない場合でさえも、ホームネットワーク内に、レジデンシャルゲートウェイにアタッチされた追加的なルータがあれば、2つの重大な問題が生じる。第1の問題は、それら追加的なルータは、当該ルータがサポートするサブネット(即ち、各ルータ自体のローカルエリアネットワーク(LAN))と共に使用するためのインターネットプロトコルバージョン6のアドレスプレフィックスを必要とすることである。第2の問題は、そうしたルータは、上流側ルータ及びサービスプロバイダから、当該ルータがサポートするLAN上あらゆるデバイスを完全に隠蔽することである。これは、サービスプロバイダがそれら隠蔽されたデバイスにある特定のサービスを提供し、又は当該サービスをモニタリングすることを困難にする。

30

**【0018】**

ホームネットワークへのアクセスを訪問者に与えるには2つの選択肢があり、双方とも重大な問題を有する。典型的な手法は、それが容易だからであるが、訪問先のホームネットワークオーナーが単に、使用される暗号化の種類及びルータへ接続するためのパスコードに関する情報を含む、ホームネットワークを使用するのに必要な情報を訪問者に与えることである。これは、訪問者が、デバイス、サービス、及びネットワーク設定を含む、訪問先ホームネットワーク上のすべてのリソースへの完全なアクセスを有することを意味する。訪問先ホームネットワークオーナーがより高度な技術を有し、アクセスが無線である場合には、ゲストネットワークを提供するように、訪問デバイスのために別個のSSIDが設定され得る。これは、よく言っても、面倒である。(プリンタのような)ある宅内サービスへのアクセスは提供し但し他のサービスへのアクセスは提供しないといったことは、特に複雑である。また一般には、加入者の上流側帯域幅のすべてが、訪問者によって望まれる任意の優先度で、訪問デバイスから利用できる。

40

**【0019】**

本発明の実施形態は、ホテル又はレストランといった企業によって提供されるネットワークを訪問する場合の、ホームネットワークリソースへのアクセスの提供も包含する。そ

50

うした種類の訪問先ネットワークもまた、本明細書で記述されるアーキテクチャ及び処理を実装することができる。本明細書で使用される“訪問先ネットワーク”は、訪問先のホームネットワーク又はレジデンシャルネットワーク及び訪問先の企業ネットワーク又は法人ネットワークの双方を包含する。明確さのために、本明細書で提供される事例は、訪問先ネットワークがホームネットワークである文脈でのものである。

【0020】

本発明の実施形態は、先行技術のそれら不都合点を克服する。多くのソフトウェア機能がホームユーザによって設定される複雑なレジデンシャルゲートウェイを使用する代わりに、本発明の実施形態は、ブロードバンドリモートアクセスサーバ(BRAS)若しくはブロードバンドネットワークゲートウェイ(BNG)といった上流側デバイス、又は他の上流側サービスステディバリプラットフォームにおいて、すべての複雑な処理をインターネットサービスプロバイダに委ねる、単純なレジデンシャルゲートウェイを使用する。本発明の実施形態は、このサービスを提供するためのアーキテクチャ及び構成要素を包含するものである。上流側サービスステディバリプラットフォームは、仮想レジデンシャルゲートウェイとして機能する制御ロジックのセットを実行し、仮想レジデンシャルゲートウェイは、加入者がインターネットサービスプロバイダのネットワークに求める、サービスのためにインターネットの残りの部分を活用することを含むサービスを提供する。制御ロジックは、上流側サービスステディバリプラットフォーム及びレジデンシャルゲートウェイの双方を制御する。

【0021】

ネットワークアーキテクチャは、インターネットサービスプロバイダが、あたかもサービスがホーム内のデバイスによって提供されるかのように、サービスを透過的に提供することができる、ホームネットワークへの十分な可視性を可能にする。個々のデバイスを設定する代わりに、ホームユーザはウェブインタフェースを有し、ウェブインタフェースは、各デバイスをどのように設定すべきか心配しなくてはならない代わりに、ユーザの設備のすべてを統合し、サービスビューへの共通の、明確な構造のアクセスを提供するため、ユーザのネットワーク環境に対する十分な制御を、無理なく、使いやすいやり方で提供する。サービスアップグレードは、その場合、ウェブページ上でのリクエストの問題となる。即ち、インターネットサービスプロバイダは、その場合、当該ホームネットワークへ適用される設定を修正することができる。

【0022】

加えて、レジデンシャルゲートウェイを仮想化していることによって、同じサービスのセットが他の場所にいるユーザにも提供され得る。ホームネットワークへの適切に認証された遠隔アクセスが、その場合、全体のネットワークアーキテクチャの自然な一部になる。ホームネットワーク及び訪問先ネットワークの双方が、仮想化されたレジデンシャルコントローラを利用しなければならない。インターネットサービスプロバイダは、仮想ゲートウェイコントローラを通じて、訪問先ネットワーク内でゲストサービス機能(仮想ローカルエリアネットワーク(VLAN)及びSSIDなど)を自動的に設定することができる。レジデンシャルゲートウェイは、仮想ゲートウェイコントローラによって、訪問ユーザへ提供される訪問先ネットワーク及び遠隔のホームネットワークのサービスの双方にサービス提供するための適切なサービス品質(QoS)及び帯域幅の制限と共に設定される。

【0023】

いくつかの実施形態では、訪問者のモバイルデバイスは、訪問先ネットワークの仮想ゲートウェイコントローラ及び/又は遠隔のホームネットワークのための仮想ゲートウェイコントローラとインタラクションするためのソフトウェアを含む。最初に、訪問ユーザのデバイスは、訪問先ネットワーク内のゲストサービスアクセスへ接続する。訪問先ネットワークの仮想ゲートウェイコントローラは、訪問ユーザデバイスへ接続して、訪問先ネットワークのために認証を行い、次いで訪問ユーザデバイスへ接続して、遠隔のホームネットワークのリソースにアクセスするための訪問先ネットワーク内の新しいアクセスポイン

10

20

30

40

50

トに関して認証を行う。多くのケースでは、遠隔のホームネットワークは、訪問ユーザによって所有されている。遠隔のホームネットワークからの訪問ユーザのリソースは、その場合、訪問先ネットワーク上で使用され、共有され得るはずである。加えて、訪問者がゲストサービス上に留まるにせよ、新しいアクセスポイントによって提供される専用サービスへ移動するにせよ、訪問先ネットワークオーナーは、訪問先ネットワークのリソースへのアクセスを管理するように、どちらのサービスも、事前に、又はオンデマンドで、設定することができる。一例では、すべての訪問者が、訪問先ネットワークオーナーのプリンタを使用することができるように設定され得るはずである。

#### 【 0 0 2 4 】

他の例では、Bobを訪問しているAliceが、Bobのネットワーク上でAlice自身 10  
のデバイスからBobのテレビで何かを見たいと頼む場合に、Bobは当該の機能を使用可能とすることができる。Bobが、Bob自身のデバイスのうちの1つを通じて構成設定にアクセスして、Aliceのデバイスがテレビへ接続することを可能にすることもでき、又は仮想ゲートウェイコントローラがAliceのデバイスからアクセスのためのリクエストを受信したことに応じて、仮想ゲートウェイコントローラが、Bobのデバイスのうちの1つを通じてBobに、リクエストされたリソースアクセスを許可するようメッセージを送り、若しくは問い合わせることもできる。

#### 【 0 0 2 5 】

仮想ゲートウェイコントローラを用いたネットワーク内のデバイスへのサービスの提供 20  
は、宅内ルータがプレフィックス委譲を伴うダイナミックホスト設定プロトコルバージョン6 (DHCPv6) の使用に依拠している場合、アドレス割り当てによる影響を受ける。プレフィックス委譲を伴うDHCPv6は、宅内ルータに、ルータがサポートするLAN上のデバイスに使用するための設定情報及びプレフィックスのセットを提供する。プレフィックス委譲は、共有プレフィックス (即ち、冒頭の数値のセット) を有するIPv6アドレスの範囲の割り当てであり、例えば、2001:0db8:85a3:0000:0000:8a2e:0370:xxxxであり、xxxxは割り当て可能なアドレス範囲を示す。

#### 【 0 0 2 6 】

インターネットサービスプロバイダにホームネットワーク上のエンドデバイスへの可視 30  
性を提供するために、DHCPv6へ組み込まれる追加的なフラグ及び追加的な振る舞いが存在する。追加的な振る舞いとは、ホームネットワーク内のルータがルータのローカルLAN上に新しいデバイスが存在することを検出する度に、当該ルータがBNG又はBRASにある仮想レジデンシャルコントローラへ通知を送信すること、である。そうした通知をトリガするために、DHCPv6アドレス委譲メッセージに含められる、それら通知が必要とされることを指示するフラグが存在する。整合性のために、DHCPv6プレフィックスリクエストメッセージにも、ルータがこの振る舞いを行うことができることを指示するフラグが存在する。

#### 【 0 0 2 7 】

図1は、仮想レジデンシャルゲートウェイを用いた、レジデンシャルルータのための仮想 40  
化された可視性をサポートするネットワークアーキテクチャの一実施形態の図である。仮想化された可視性の実装は、3つの主要構成要素、及びいくつかの関連した項目の間で分割される。3つの主要構成要素は、レジデンシャルゲートウェイ (RGW) 115、上流側IPサービスルータ105 (即ち、BNG101、BRAS又は等価物内)、及び仮想ゲートウェイコントローラ107である。

#### 【 0 0 2 8 】

BNG101は、帯域幅及びサービス品質 (QoS) のポリシーが適用されるIPエッジルータであり、BRASによって果たされる機能はBNGによって果たされる機能の上位セットである。BRASはBNG101であり、加入者トラフィックのための集約ポイントである。BRASは、アクセスネットワークとインターネットサービスプロバイダ131のコアネットワーク111との間の集約機能 (IP、PPP、イーサネットなど) を 50

提供する。BRASは、その集約機能以上に、アクセスネットワーク内のポリシー管理及びIP QoSのための注入ポイントでもある。明確さのために、BNG101を用いてIPサービスルータ105を実装するネットワークの実例が示されている。しかしながら、BRAS又は類似のデバイスも使用され得ることを当業者は理解するはずである。また、明確さのために、単一のBNG101及びRGW115を有するインターネットサービスプロバイダネットワーク131も示されている。BNG101は、任意の数のホームネットワーク121及びRGW115を、コアネットワーク111へと共に一般的なインターネット113へも接続することができることを当業者は理解するはずである。また、インターネットサービスプロバイダ131は、任意の数のBNG101及びBRAS又は類似のデバイスを、ホームネットワーク121及びRGW115のセットへ接続するために含むこともできる。

10

**【0029】**

仮想ゲートウェイコントローラ107は、複数のやり方で実装され得る。仮想ゲートウェイコントローラ107は、IPサービスルータ103の制御プレーンの一部であることができ、IPサービスルータ103の制御プレーンはBNG又は類似のデバイスのネットワークプロセッサ103によって実行される。仮想ゲートウェイコントローラ107は、(例えば、BNG101内の)IPサービスルータ105のシャーシ内のブレード上で提供されることもでき、又は、ネットワークプロトコル(IP)を介してIPサービスルータ107へ接続された別個のデバイス109であることもできる。このデバイスは、加入者の仮想動作状態を維持する役割を果たす。これは、すべてのデータプレーン機能の動作状態を決定することを含む。これは、状態をモデル化すること、及び、必要とされる振る舞いを提供するように、RGW10及びBNG101といった適切なデバイスを設定することの双方を意味する。

20

**【0030】**

よって、仮想ゲートウェイコントローラ107は、BNG101上でファイアウォール機能141を設定する役割を果たす。仮想ゲートウェイコントローラ107は、SSID151及びRGW115上での無線アクセスについてのSSID151のポリシーを設定する役割を果たす。仮想ゲートウェイコントローラ107は、不要なトラフィックを低減させる一方で、必要な接続性を提供するように、双方のデバイス上のマルチキャストフィルタ153を管理する役割を果たす。仮想ゲートウェイコントローラ107は、UPnPコントローラ157といった家庭用制御機能も提供することができる。仮想ゲートウェイコントローラ107は、DNSエントリ155を作成することといったサービスのサポートを提供することができる。仮想ゲートウェイコントローラの動作は、インターネットサービスプロバイダによって使用される既存の認証インフラストラクチャー117(RADIUS及び/又はDiameterなど)へ結合されている。これは、固定と移動の融合に、又はSIMベースのレジデンシャルゲートウェイのサポートに必要な動作といった、追加的な認証動作を可能とする。

30

**【0031】**

IPサービスルータ105は、加入者のためのデータプレーンサービスを提供するルータである。IPサービスルータ105は、すべての加入者データプレーンパケットを扱う。IPサービスルータ105は、通常はRGW115によって提供される機能である、ネットワークアドレス変換(NAT)及びファイアウォール機能といった機能の多くを果たす。これらの機能の動作は、仮想ゲートウェイコントローラ107によって制御される。このデバイスは、現在そうしたプラットフォーム上で提供されている、トラフィックポリシング及びQoSといったデータプレーン機能も果たす。しかしながら、本実施形態では、加入者ごとの動作はIPサービスルータ105へ委譲され得るが、そうした機能の動作は、仮想ゲートウェイコントローラの制御下にある。IPサービスルータ105又はこのデバイスの適切なコントローラは、事業者のIPネットワークのIPルーティングに関与し、加入者の代わりにトラフィックを送信し、受信することができる。

40

**【0032】**

50

レジデンシャルゲートウェイ115は、ホーム内の様々な媒体（イーサネット、802.11b/g/n Wifi、Zigbee、及び類似の媒体）間の物理的な接続性、及びサービスプロバイダへの接続性（DSL、ケーブル、パッシブオプティカル、LTE、及び類似の技術）を提供する。レジデンシャルゲートウェイ115は、それが、ホーム内のデバイスとIPサービスプロバイダネットワークとの間のパケット通信を提供することができるのに十分なロジック動作を提供する。このデバイスは、加入者によって所有されることも、事業者によって所有されることも可能である。しかしながら、このデバイスは、事業者によって管理される仮想ゲートウェイコントローラ107によって制御される。

#### 【0033】

ホームネットワーク121内の他のデバイスは、仮想ゲートウェイコントローラとインタラクションするプロトコルを使用することができる。概して、このインタラクションはホームネットワークデバイス内で変更されず、但し、RGWから仮想ゲートウェイコントローラへの機能のシフトは、動作の管理及び有効性を改善する。例えば、ホームネットワーク121上のデバイスは、ユニバールプラグアンドプレイプロトコル（UPnP）157を使用して、仮想ゲートウェイコントローラに到達し、又はホームネットワーク121上のストレージサービスを発見することができ、これは以前には、完全にホームネットワーク121内で実装されていたものである。仮想ゲートウェイコントローラを使用する場合、UPnP157、並びにドメインネームサービス155、DHCP159、SSID設定151、マルチキャスト設定153及び類似のサービスを含む他のサービスは、ホームネットワーク121内で、又はRGWで実装されているように見えるが、実際には、インターネットサービスプロバイダネットワーク131内の仮想ゲートウェイコントローラ107又は類似のデバイスを通じた、BNG101からインターネットサービス事業者による提供が可能である。仮想ゲートウェイコントローラの制御プレーンがRGWのデータプレーンから分離されている分離アーキテクチャの使用は、インターネットサービスプロバイダネットワーク131のサービスを、ユーザから容易に発見することができ、透過的にアクセスできるように見せる。そうしたサービスは、VOIP（Voice Over Internet Protocol）対応サービス、ストレージサービス、又はアプリケーションサービスを含むことができる。同様に、ホームネットワーク121及びホームネットワークベースのサービスへのアクセスも、ユーザが、インターネットサービスプロバイダによって提供される認証サーバ117といった認証及び関連付けのための追加的なソフトウェアを使用して他のネットワークからホームネットワークにアクセスする場合に、ユーザへより容易に提供され得る。

#### 【0034】

仮想ゲートウェイコントローラ107の制御動作に関係する、2つの主要なコンセプトが存在する。第1のコンセプトは、仮想ゲートウェイコントローラ107がBNG101及びRGW115の機能を制御するための制御プロトコルである。この第1の制御プロトコルは、国際技術標準化委員会（IETF: International Engineering Task Force）によって標準化されたForCESプロトコルの修正といったプロトコルであり得る。ForCESプロトコルは、必要な機能を表すように拡張され得る。簡易ネットワーク管理プロトコル（SNMP）若しくはNETConfといった従来のネットワーク管理プロトコルを含む他のプロトコル、又はウェブベースのインタラクションのコンピュータ利用でさえも、この制御のために使用され得る。

#### 【0035】

仮想ゲートウェイコントローラ107の制御動作に関係する第2の主要なコンセプトは、仮想ゲートウェイコントローラが、DHCP、IPv6近隣探索、及びUPnP探索機構といったネットワーク動作プロトコルのための制御側エレメントであり得るための制御プロトコルである。

#### 【0036】

いくつかのホームネットワーク121では、ホームネットワーク121内のレジデンシャルゲートウェイから分離されたルータ181があることになる。それらルータ181は

10

20

30

40

50

、DHCPv6を使用して、ルータがサポートしているホスト（即ち、エンドデバイス183）に使用するためのIPv6プレフィックスを受信するように設定され得る。仮想化された可視性をサポートする追加的なホームネットワークルータ181は、このサポートを、それらのDHCPv6リクエストメッセージにフラグを含めることによって指し示し、当該DHCPv6リクエストメッセージは、RGW115へ送信され、次いでBNG101上の仮想ゲートウェイコントローラ107へ転送される。仮想ゲートウェイコントローラ107は、DHCPv6サービス159を提供する。仮想化された可視性をサポートすることを指し示したルータに回答する際、仮想ゲートウェイコントローラ107は、新しいホスト183が発見されればそれらへ割り当てられるアドレスを仮想ゲートウェイコントローラ107へ報告するものとする、ということを示すフラグを設定することになる。

10

#### 【0037】

仮想化された可視性をサポートするホームネットワークルータ181は、そのLAN上でホームネットワークルータ181にアタッチされているホスト183に関する状態をモニタリングし、維持するであろう。それらホームネットワークルータ181によって提供されるLANは、有線LAN及び無線LANの任意の組み合わせであり得る。各ルータ181は、各ルータ181が中継するIPv6近隣探索リクエスト及びIPv6DHCPv6リクエストをモニタリングすることによって仮想化された可視性をサポートすることになる。新しいホスト183が発見される場合、通知メッセージがルータ181によって仮想ゲートウェイコントローラ107へ送信される。ホスト183がもはや存在していないとみなされる場合、通知メッセージがやはり仮想ゲートウェイコントローラ107へ送信される。仮想ゲートウェイコントローラ107は、それら通知へ確認応答メッセージで回答する。一実施形態では、通知は、確認応答が受信されるまで再送される。それらメッセージは、ICMP又は他の制御プロトコルを用いて送信されてもよい。他の実施形態では、UDP又は仮想ゲートウェイコントローラへのTCP接続上のプロトコルが使用されてもよいであろう。そうしたメッセージが送信される度に、効率性のために、すべての確認応答がなされていない情報が当該メッセージに含まれてもよい。

20

#### 【0038】

ホームネットワークルータがそのホストに関して記憶するエントリについて再検証時間（revalidation time）及び寿命（lifetime）を有することによって、ステートレスアドレス自動設定（SLAAC）が使用される場合には、ホスト除去を検出することができる。この情報は、ホストIPv6テーブル185又は類似のデータ構造に記憶され得る。再検証時間に到達した場合、ホームネットワークルータ181は、LAN上でのホスト183の継続した存在を検証するためにIPv6近隣要請メッセージを送信し、次いで新しい時間制限を設定することになる。ホスト183が応答しない場合には、ホームネットワークルータ181は、メッセージを再送することになる。メッセージの数回の再送の後で、ルータ181はホスト183が除去されると宣言し、仮想ゲートウェイコントローラ107に通知することになる。仮想ゲートウェイコントローラ107は、ホストIPv6テーブル109内のホームネットワーク内のホスト183を追跡することができる。接続されたホームネットワーク又は割り当てられたプレフィックスごとに、テーブルの別のインスタンスが維持され得る。

30

40

#### 【0039】

ホームネットワークルータが、6LowPanといった他のホスト通知プロトコルを有する他の通信媒体をサポートしている場合には、それら媒体からの手順を使用してホスト183の存在が検出され、仮想ゲートウェイコントローラ107への登録に必要な情報が決定されてもよい。ホスト183は、パーソナルコンピュータ、テレビ、タブレットコンピュータ及びセルラーフォンなどのハンドヘルドデバイス、ネットワークストレージデバイス、電化製品及び類似のデバイスといった任意の種類のネットワーク接続されたデバイスであってよい。一実施形態では、ホームネットワーク121は、マシンツーマシン通信もサポートすることができる。マシンツーマシン通信は、ホームネットワークルータ18

50

1へ接続されたセンサのセットからデータを収集するのに使用され得る。マシンツーマシン通信を用いてセンサ及びデバイスと通信するミドルウェア161は、典型的には、レジデンシャルゲートウェイによって実行されるが、仮想ゲートウェイコントローラへ移動されることもできる。

#### 【0040】

このネットワークアーキテクチャは、仮想化されたレジデンシャルゲートウェイ及び仮想化されたホームサービスデリバリのためのコヒーレントなシステムを提供する。設定、強化、並びに、整合性の取れた遠隔サービス、及びホーム情報、リソースへの遠隔アクセスは、すべて、コヒーレントなアーキテクチャの自然な部分となる。このアーキテクチャの重要な利点は、事業者、ホームネットワーク121内のレジデンシャルゲートウェイへ接続されたすべてのデバイスへの十分な可視性を提供することである。これは、インターネットサービスプロバイダが、ホームへ様々な(シームレスな)サービス、例えば、ネットワーク管理、サービスデリバリ、及び類似のサービスを提供することを可能とする。他の利点は、インターネットサービスプロバイダが、ホームネットワーク121を通じて正しいデバイスにアクセスする際に、サードパーティ、例えば、公益事業提供者又は機器製造者を支援することを可能とすることである。例えば、電力会社が、家庭の電気システム内の特定のデバイスのサーモスタット又はスイッチのオン/オフを設定するために、ホームネットワーク121にアクセスすることを必要とする場合がある。一実施形態では、これが、マシンツーマシンミドルウェア161又はそのインスタンスを通じて行われ得る。

#### 【0041】

一実施形態では、仮想ゲートウェイコントローラ107は、遠隔アクセスモジュール163、認証モジュール165、ネットワーク設定モジュール167及び類似の構成要素も含む。これらの構成要素は、ホームネットワークのオーナー又はホームネットワークのオーナーのアカウントに関連付けられる任意のユーザによるホームネットワーク121の管理を円滑化する。明確さのために、ホームネットワークオーナーとは、ホームネットワーク121についての管理権限を有する任意の個人をいう。ホームネットワークユーザとは、ホームネットワーク121へ接続されたコンピューティングデバイス又はホスト183を使用する個人をいう。

#### 【0042】

遠隔アクセスモジュール163は、遠隔のホームネットワークからのリソースへのアクセスを訪問ユーザデバイスへ提供する。遠隔アクセスモジュール163は、遠隔ネットワークリソースへのアクセスを提供するための別個の仮想ローカルエリアネットワーク(VLAN)又はSSIDを確立することができる。遠隔アクセスモジュール163は、遠隔のホームネットワークの仮想ゲートウェイコントローラと通信して、遠隔のホームネットワークについての設定情報及び遠隔のホームネットワーク上のリソースにアクセスするのに必要な情報を取得することもできる。遠隔アクセスモジュール163は、認証モジュール165と協働して、訪問ユーザデバイスがホームネットワーク121のリソースにアクセスすることを可能とするために、訪問ユーザデバイスをホームネットワーク121上で認証することができる。認証モジュール165も、遠隔のホームネットワークへの接続を確立するために訪問ユーザデバイスの認証を円滑化することができる。それらモジュールの機能を、図5及び図6に関連して以下でさらに詳細に論じる。

#### 【0043】

ネットワーク設定モジュール167は、ホームネットワークオーナーがホームネットワークの設定を変更することを可能とするためのユーザインタフェースを提供することができる。ネットワーク設定モジュール167は、ウェブベースのインタフェースを提供することができ、ホストデバイス183のローカルクライアントとインタラクションすることができ、又は同様に、ホームネットワークオーナーが設定インタフェースにアクセスすることを可能とすることができる。訪問ユーザがローカル又は遠隔のホームネットワークリソースにアクセスし、又はそれらを共有するようリクエストしている例では、ホームネットワークオーナーは、リクエストを通知され、ネットワーク設定モジュール167によって提供

10

20

30

40

50

されるインタフェースを用いてリクエストを承認し、又は拒否することを可能とされ得る。

【 0 0 4 4 】

図 2 は、ホームネットワークルータと仮想ゲートウェイコントローラとの間のメッセージングの一実施形態の図である。この例示的な実施形態では、ホームネットワーク 1 2 1 は、仮想ゲートウェイコントローラ ( V G C ) 1 0 7 を提供する B N G 1 0 1 へ接続されている。他の実施形態では、仮想ゲートウェイコントローラ 1 0 7 は、インターネットサービスプロバイダネットワーク 1 3 1 内の B N G 1 0 1 の外部に位置することができる。ホームネットワーク 1 2 1 は、レジデンシャルゲートウェイ ( R G W ) 1 1 5 及びホームネットワークルータのセット 1 8 1 A ~ C を含む。ホームネットワークルータ 1 8 1 A 及び 1 8 1 C はネスト化されており、又はカスケード式に設定される。これは、ホームネットワーク 1 2 1 のための D H C P サービスを提供する V G S 1 0 7 と、ホスト 1 8 3 A といったホスト ( 即ちエンドデバイス ) との間に複数の間接参照レベルを生じさせる。図は、ホスト 1 8 3 A がホームネットワークルータ 1 8 1 C によって発見されている例を示している。

10

【 0 0 4 5 】

この例では、ホームネットワークルータ 1 8 1 C は、すでに、中間ホームネットワークルータ 1 8 1 A へ送信された D H C P v 6 プレフィックスリクエストを通じて間接的に、 V G C 1 0 7 の D H C P サービスによってプレフィックスを提供されている。 D H C P v 6 プレフィックスリクエストは、仮想化された可視性のサポートのフラグ又は類似の標識を含んでいた。この D H C P v 6 プレフィックスリクエストは、中間ルータ 1 8 1 A によって転送されたものであり、中間ルータ 1 8 1 A は、次いで、この D H C P v 6 プレフィックスリクエストを、前述のようにこのアーキテクチャではブリッジとして機能する R G V 上で V G C へ転送した。 V G C は次いで、発見されたホストについて通知が必要であることが指示された D H C P v 6 メッセージを用いて、割り当てられたプレフィックス又は中間ホームネットワークルータ 1 8 1 A に割り当てられたプレフィックスのサブセットで応答した。中間ホームネットワークルータ 1 8 1 A は、次いで、このアドレス範囲又はプレフィックスを記録し、メッセージをリクエスト側のホームネットワークルータ 1 8 1 C へ転送した。

20

【 0 0 4 6 】

ホスト 1 8 3 A は、任意の種類の間近探索プロトコルを用いて発見され得る。発見された後で、ホームネットワークルータ 1 8 1 C は、ホスト 1 8 3 A に、 V G C 1 0 7 の D H C P v 6 サービスによってルータ 1 8 1 C に割り当てられたプレフィックスに基づく I P v 6 アドレスを提供する。しかしながら、この新しく割り当てられた I P v 6 アドレスは、 V G C 1 0 7 が新しいホスト発見の通知を必要としていることを除いて、 V G C 1 0 7 に知られていないはずである。通知は、 I C M P メッセージ又は類似の種類のコントロールメッセージの形であり得る。一実施形態では、ホームネットワークルータは、 I C M P \_ N T Y メッセージ 2 0 1 と呼ばれる通知メッセージを生成する。 I C M P \_ N T Y メッセージ 2 0 1 A は、ホスト 1 8 3 A の割り当て I P v 6 アドレス、ホスト 1 8 3 A の M A C アドレス、寿命又はライセンスデータ及び V G C 1 0 7 がホスト 1 8 3 A を追跡することを可能とする類似の情報を含むことができる。中間ホームネットワークルータ 1 8 1 A 及び V G C 1 0 7 は、この情報をホスト I P v 6 テーブルに記録する。

30

40

【 0 0 4 7 】

V G C 1 0 7 は、次いで、確認応答メッセージを生成する。確認応答メッセージは、 I C M P メッセージであり得る。 I C M P メッセージは、本明細書で I C M P \_ N T A メッセージ 2 0 3 A と呼ぶ通知確認応答メッセージであり得る。 I C M P \_ N T A メッセージ 2 0 3 A は中間ホームネットワークルータ 1 8 1 A へ送信され、そこでホームネットワークルータ 1 8 1 C へ転送される。ホームネットワークルータ 1 8 1 C は、 I C M P \_ N T A メッセージ 2 0 3 A が返信として受信されるまで I C M P \_ N T Y メッセージ 2 0 1 A を再送し続けるはずである。

50

## 【 0 0 4 8 】

同様に、第3のホームネットワークルータ181Bがホスト183Bを発見する、より簡単なシナリオも提供される。このケースでは、同じ種類のICMP\_\_NTYメッセージ201B及びICMP\_\_NTAメッセージ203Bが、ホームネットワークルータ181B及びVGC107によって、いかなる中間ルータの関与もなしで交換される。通知の処理は、よって、任意の数のホームネットワークルータを、任意の階層の深さのカスケードルータを含む任意の配置で関与させることができる。

## 【 0 0 4 9 】

図3は、レジデンシャルルータを通じて仮想化された可視性を可能とするための処理の一実施形態の流れ図である。図示した処理は、仮想化可視性システムを実装するために仮想ゲートウェイコントローラによって講じられる措置を示している。一実施形態では、処理は、ホームネットワークルータからプレフィックス委譲のためのDHCPv6リクエストを受信したことに応じて開始される(ブロック301)。リクエストは、仮想化可視性システムのサポートを示すフラグ又は設定フィールドといった標識を含むことができる。

10

## 【 0 0 5 0 】

VGCは受信したリクエストに回答して、割り当てられたプレフィックスを含むDHCPv6メッセージをホームネットワークルータへ送信する(ブロック303)。応答メッセージは、ホスト発見又はIPv6アドレス設定の通知がVGCへ報告される必要があることを指示するフラグ又は設定フィールドの形の標識を含むことができる。このメッセージは、レジデンシャルゲートウェイ及び任意の数の中間ホームネットワークルータを通じて、要求側ホームネットワークルータへ送信され得る。

20

## 【 0 0 5 1 】

処理は、ホームネットワークルータがホストを発見し、ホストのためのIPv6アドレスを設定したことに応じて、随時ホームネットワークルータからICMP\_\_NTY通知メッセージをさらに受信することができる(ブロック305)。ICMP\_\_NTYメッセージは、ホストのIPv6アドレス、ホストのMACアドレス、寿命の満了又はライセンス失効、及びホストIPv6設定に関する類似の情報を含むことができる。この情報は、ホストへのデータプレーン転送及びサービス提供を円滑化するためにホストIPv6テーブルに記録され得る。VGCは次いで、ICMP\_\_NTAメッセージを生成し、ホームネットワークルータへ送信する(ブロック307)。ICMP\_\_NTAメッセージは、ホストのIPv6アドレス及びMACアドレスを含むICMP\_\_NTAメッセージからのデータの受信及び記録を確認する。

30

## 【 0 0 5 2 】

図4は、仮想ゲートウェイコントローラにインタフェースするマシンツーマシンシステムのためのアーキテクチャの一実施形態の図である。一実施形態では、仮想ゲートウェイコントローラ107は、マシンツーマシン通信又はマシンツーマシン通信ネットワークを用いてホーム内のセンサ401からの通信を可能とし、又はセンサ401からデータを収集するミドルウェア403を含み、又はサポートする。従来はレジデンシャルゲートウェイ405によって実行されていたミドルウェア403は、仮想ゲートウェイコントローラ107へ移動されている。前述のような可視性のための処理及びネットワークの一般的機能も、それらシステムでRGWの機能の代わりにする仮想ゲートウェイコントローラを有するそれらマシンツーマシンネットワークをサポートするように適用され得る。

40

## 【 0 0 5 3 】

ミドルウェア405は、サードパーティエンティティ413と継続して通信することができる。この機能は、仮想ゲートウェイコントローラ107において、セキュリティ及び柔軟性の点で強化される。仮想ゲートウェイコントローラ107は、サードパーティエンティティに、ホームネットワーク又はRGWへの実際のアクセスを与えずに、ミドルウェア405へのアクセスを提供し、それによってホーム内のセンサネットワークへのアクセスを提供することができる。ミドルウェア405の別個のインスタンスが、別個のサードパーティアクセスのために提供され得る。

50

## 【 0 0 5 4 】

図5は、遠隔のホームネットワーク及び訪問先ネットワークの一実施形態の図である。遠隔のホームネットワーク121は、この例では、'Alice'によって所有され、又は制御されている。遠隔のホームネットワーク121は、パーソナルコンピュータ、テレビ、ハンドヘルドデバイス、ネットワークストレージ(NAS)及び類似のホストといった任意の数のホストを含むことができる。遠隔のホームネットワーク121は、BNG101上の仮想ゲートウェイコントローラから任意の数のサービスを受信することもできる。仮想ゲートウェイコントローラは、図1に関連して前述した任意の数のサービスを提供することができる。BNG101は、訪問先ネットワーク523にサービス提供するBNG501と同じインターネットプロバイダネットワークの一部であることも、別個のインターネットプロバイダネットワークであることも可能である。各仮想ゲートウェイコントローラの遠隔アクセスモジュールは、あるホームネットワークのオーナー又はデバイスが、遠隔アクセスサービスをサポートしている他のホームネットワークを訪問する場合に、リソースの遠隔アクセスを可能とするために、2つのBNG101、501の間の接続を確立する。

10

## 【 0 0 5 5 】

訪問先ネットワーク523は、住居又はビジネスの場における有線ネットワーク及び/又は無線ネットワークを含む任意の種類ホーム又は企業ネットワークであり得る。訪問先ネットワーク523は、パーソナルコンピュータ、テレビ、センサ、ネットワークストレージ、プリンタ及び任意の他の種類のネットワークリソースを含むホストデバイスのセットを含むことができる。図示の例では、訪問先ネットワーク523は'Bob'によって所有されている。図示の例は、Aliceがハンドヘルドデバイスを用いてBobの訪問先ネットワーク523へ接続するところを示している。ハンドヘルドデバイスは、有線接続又は無線接続を用いてレジデンシャルゲートウェイ515へ接続することができる。レジデンシャルゲートウェイ515は、BNG501内の仮想ゲートウェイコントローラによって制御され、設定される。Aliceの訪問ハンドヘルドデバイスの接続を扱う際の仮想ゲートウェイコントローラの機能を、図6に関連して以下でさらに説明する。Aliceの訪問ハンドヘルドデバイス(又は任意の訪問デバイス)は、訪問先ネットワークの仮想ゲートウェイコントローラ及び遠隔のホームネットワークの遠隔のゲートウェイコントローラへ接続するように特に設計されているソフトウェアを含むことができる。このソフトウェアは、遠隔のホームネットワークへ直接接続されない場合に、訪問先ネットワーク及び遠隔のホームネットワークの上のリソースへのアクセスを直接的に交渉することができる。

20

30

## 【 0 0 5 6 】

図6は、遠隔のホームネットワークリソースへのアクセスを可能とするための処理の一実施形態の流れ図である。処理は、ユーザデバイスが他のユーザのホームネットワークへ接続しようとしている図5の簡略化された例示的アーキテクチャに関連して記述されている。一実施形態では、処理は、仮想ゲートウェイコントローラが、訪問ユーザのデバイスから訪問先ネットワークのアクセスポイントを通じて接続リクエストを受信したことに応じて開始される(ブロック601)。アクセスポイントは、無線アクセスポイント又は直接配線接続を提供するレジデンシャルゲートウェイであり得る。アクセスポイントは、接続リクエストを、レジデンシャルゲートウェイを通じて仮想ゲートウェイコントローラへ渡す訪問先ネットワーク内の他のレジデンシャルルータでもあり得る。接続リクエストは、訪問先ネットワークの有線LAN、保護された無線LAN、ゲスト無線LAN又は訪問先ネットワーク内の類似のLANに関連付けられ得る。訪問先ネットワーク及び遠隔のホームネットワークへのアクセスポイント接続は、SSID又はVLANであり得る。

40

## 【 0 0 5 7 】

訪問先ネットワークを管理する仮想ゲートウェイコントローラの認証モジュールは、訪問先ネットワークのために訪問ユーザのデバイスを認証することができる(ブロック603)。デバイスの認証は、訪問先ネットワークのホームネットワークオーナーによる訪問先

50

ネットワークの設定に応じて、訪問先ネットワークのリソースへの任意のレベルのアクセスを付与することができる。他の実施形態では、訪問先ネットワークは、訪問先ネットワークのリソースの使用についていかなる認証も必要としない。

【0058】

仮想ゲートウェイコントローラは、第1のアクセスポイントを通じて、訪問ユーザのデバイスと訪問先ネットワークとの間の接続を確立する(ブロック605)。接続を通じたリソースへのアクセスのレベルは、訪問先ネットワークオーナーによって付与されるアクセスのレベルに依存する。訪問ユーザは、次いで、訪問ユーザの遠隔のホームネットワークとの接続をリクエストすることができ、その場合、訪問ユーザは、当該の遠隔のホームネットワークのホームネットワークオーナー又はユーザである(ブロック607)。接続リクエストは、遠隔のホームネットワークの特定のリソースについてのものとするともでき、遠隔のホームネットワークへ接続するための一般的なリクエストとするともできる。

10

【0059】

訪問先ネットワークの仮想ゲートウェイの遠隔アクセスモジュールは、このリクエストを処理し、訪問先ネットワークのBNG及び仮想ゲートウェイコントローラを、遠隔のホームネットワークの仮想ゲートウェイコントローラと接続して、遠隔のホームネットワークについての設定情報を取得する(ブロック609)。設定情報は、遠隔のホームネットワークのためにインターネットサービスプロバイダによって提供された遠隔のホームネットワークのオーナーのサービスの定義を含むことができる。訪問先ネットワークの遠隔アクセスモジュールは、次いで、訪問デバイスへ遠隔のホームネットワークのリソース及びサービスへのアクセスを提供するように、訪問先ネットワークの設定を調整することができる。

20

【0060】

遠隔アクセスモジュールは、第1のアクセスポイントを介して遠隔のホームネットワークリソースを提供することもでき、訪問デバイスへのそれらリソースの提供に専用の新しい第2のアクセスポイントを設定することもできる(ブロック611)。第2のアクセスポイントが作成される場合、遠隔アクセスモジュールは、訪問デバイスを第2のアクセスポイントへ自動的に移すこともでき、訪問デバイスが双方のアクセスポイントを使用できるように、第2のアクセスポイントへのアクセスを付与することもできる(ブロック613)。訪問先ネットワークの認証モジュールは、次いで、遠隔のホームネットワークの仮想ゲートウェイコントローラによって提供された設定情報に基づいて訪問デバイスを認証することによって、又は訪問デバイスからの認証情報を遠隔のホームネットワークの仮想ゲートウェイコントローラと交換することによって、訪問デバイスの認証を遂行することができる(ブロック615)。一実施形態では、第2のアクセスポイント及び関連付けられるSSID又はVLANは、遠隔のホームネットワークについての類似のアクセス権を有する複数の訪問デバイスによって共有され得る。例えば、ある家族が訪問しており、家族の各メンバが別個のデバイスを有し、各々が第2のアクセスポイントを通じて遠隔のホームネットワークリソースへアクセスすることができる場合などである。

30

【0061】

訪問デバイスが遠隔のホームネットワークからのリソースのアクセスについて認証された後で、訪問デバイスは、第2のアクセスポイントを通じて接続され、遠隔のホームネットワークのリソースにアクセスすることができる(ブロック617)。いくつかの実施形態では、訪問先ネットワークのオーナーは、ネットワーク設定インタフェースを用いて遠隔のホームネットワークリソースへのアクセスのレベルを設定する。また、訪問先ネットワークのオーナーは、初期接続が訪問デバイスへ許可された後で、新しい種類のアクセスごとに問合せを受ける(prompted)こともできる。オーナーのために必要とされる制御又はインタラクションのレベルは、ネットワーク設定インタフェースを通じて設定され得る。

40

【0062】

以上の説明は、例示のためであり、限定のためではないことが理解されるであろう。以上の説明を読み、理解すれば、当業者には、多くの他の実施形態が明らかになるであろう

50

。本発明の範囲は、したがって、添付の特許請求の範囲を参照して、そうした特許請求の範囲に付与される均等の全ての範囲と共に決定されるべきである。

【図1】

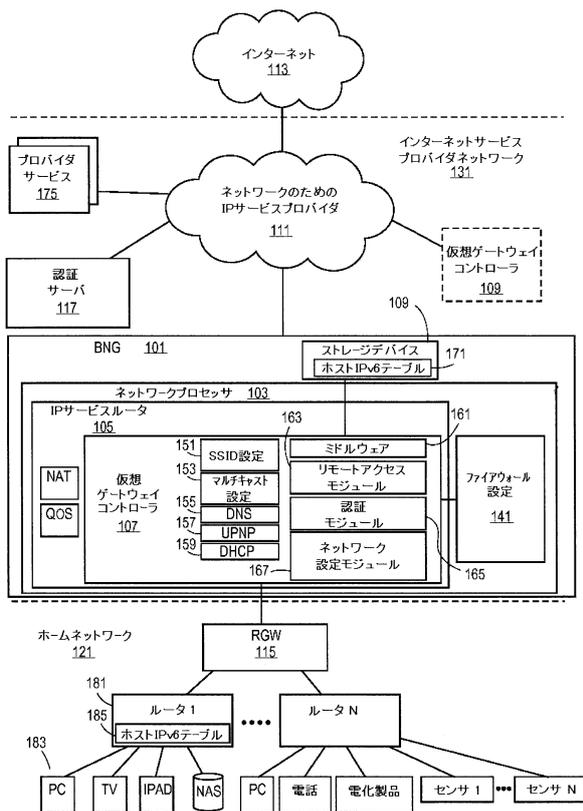


FIG. 1

【図2】

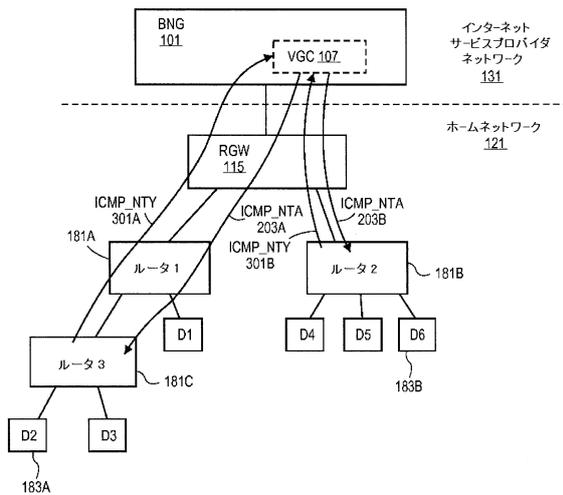


FIG. 2

【 図 3 】

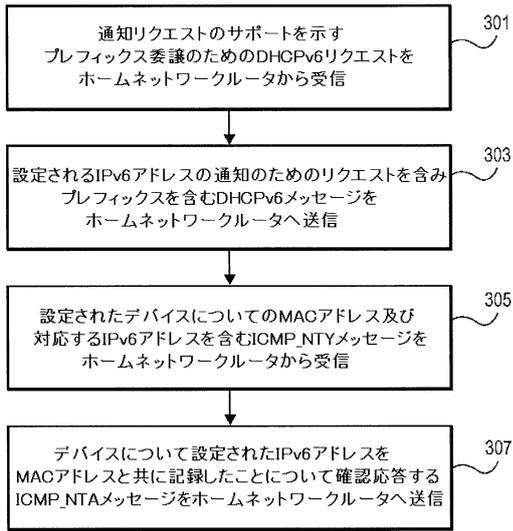


FIG. 3

【 図 4 】

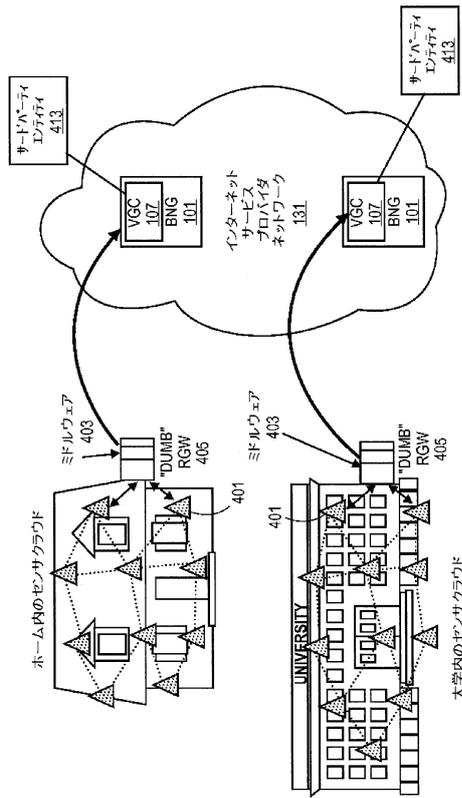


FIG. 4

【 図 5 】

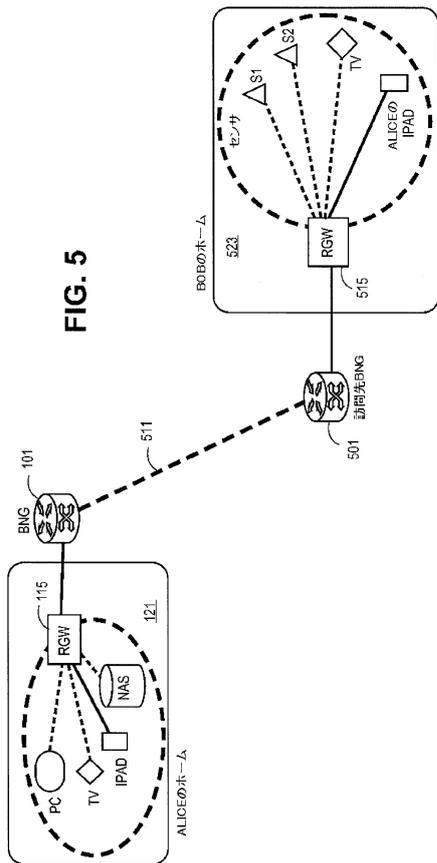


FIG. 5

【 図 6 】

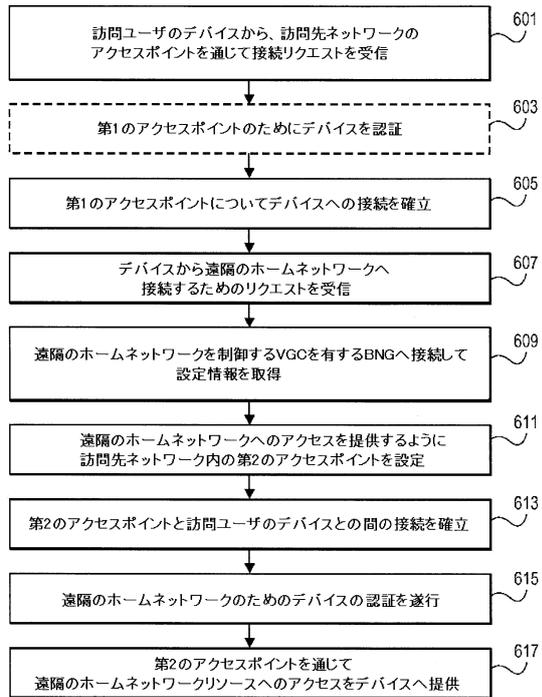


FIG. 6

## フロントページの続き

(51)Int.Cl.		F I			
H 0 4 M	11/00	(2006.01)	H 0 4 M	11/00	3 0 1
H 0 4 Q	9/00	(2006.01)	H 0 4 Q	9/00	3 0 1 D

(72)発明者 ハッダド、ワッシム  
 アメリカ合衆国 カリフォルニア州 9 5 1 2 6 サンノゼ アパートメント ナンバー 3 3 3  
 1 5 4 0 サウスウエスト エクスプレスウェイ

(72)発明者 ハルパーン、ジョエル  
 アメリカ合衆国 ヴァージニア州 2 0 1 7 6 リースバーグ 3 0 9 チョーサー プレイス  
 エヌイー

審査官 寺谷 大亮

(56)参考文献 米国特許出願公開第2010/0080238(US, A1)  
 特開2009-065610(JP, A)  
 特開2004-007671(JP, A)

(58)調査した分野(Int.Cl., DB名)

G 0 6 F	1 3 / 0 0
H 0 4 L	1 2 / 6 6
H 0 4 L	1 2 / 7 0
H 0 4 M	1 1 / 0 0
H 0 4 Q	9 / 0 0
H 0 4 W	1 2 / 0 8
H 0 4 W	7 6 / 0 2