

(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2016-526319

(P2016-526319A)

(43) 公表日 平成28年9月1日(2016.9.1)

(51) Int.Cl.	F I	テーマコード (参考)
H04L 12/70 (2013.01)	H04L 12/70	5K030
	H04L 12/70	B

審査請求 未請求 予備審査請求 未請求 (全 25 頁)

(21) 出願番号	特願2016-513139 (P2016-513139)	(71) 出願人	515312597 リレイ2・インコーポレーテッド アメリカ合衆国・95035・カリフォル ニア州・ミルピタス・マッカーシー プー ルバード・1525・スイート・209
(86) (22) 出願日	平成26年5月11日 (2014.5.11)	(74) 代理人	100064621 弁理士 山川 政樹
(85) 翻訳文提出日	平成28年1月8日 (2016.1.8)	(74) 代理人	100098394 弁理士 山川 茂樹
(86) 国際出願番号	PCT/US2014/037613	(72) 発明者	チェン, ジン-シアルン アメリカ合衆国・94538・カリフォル ニア州・フレモント・レセダ サークル・ 5478
(87) 国際公開番号	W02014/183107		
(87) 国際公開日	平成26年11月13日 (2014.11.13)		
(31) 優先権主張番号	61/821, 852		
(32) 優先日	平成25年5月10日 (2013.5.10)		
(33) 優先権主張国	米国 (US)		

最終頁に続く

(54) 【発明の名称】 仮想企業アクセスポイントの制御及び管理

(57) 【要約】

アクセスポイントの仮想化のための方法及びシステムが、開示される。現地オーナー又はマネージャは、物理的な現地ロケーションで複数のワイヤレスアクセスポイントハードウェアユニットを展開することができる。所定の実施形態に従い、複数のワイヤレスアクセスポイントハードウェアユニットに対応する仮想ワイヤレスアクセスポイントの様々なセットを、様々なWLANネットワークオペレータにリースすることが可能である。

【選択図】 図1

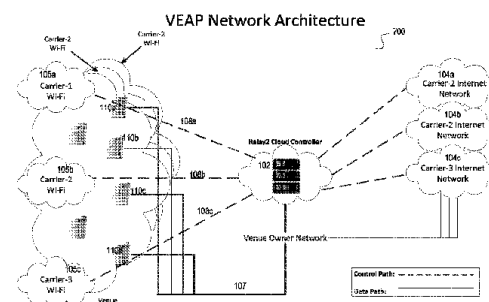


FIG. 1

【特許請求の範囲】**【請求項 1】**

物理ロケーションに、複数のワイヤレスアクセスポイントハードウェアユニットを配備すること、

前記物理ロケーションで、複数の仮想ワイヤレスアクセスポイントを、前記複数のワイヤレスアクセスポイントハードウェアユニットの対応するワイヤレスアクセスポイントハードウェアユニットに関連させること、

前記複数の仮想ワイヤレスアクセスポイントの仮想ワイヤレスアクセスポイントの第 1 のサブセットを、第 1 の W L A N ネットワークオペレータにリースすること、及び、

前記複数の仮想ワイヤレスアクセスポイントの仮想ワイヤレスアクセスポイントの第 2 のサブセットを、第 2 の W L A N ネットワークオペレータにリースすること、
を備える方法。

10

【請求項 2】

前記複数の仮想ワイヤレスアクセスポイントを管理するために、クラウドベースのコントローラを用いることを、さらに備える、請求項 1 に記載の方法。

【請求項 3】

前記第 1 の W L A N ネットワークオペレータは、前記物理ロケーションに関連する他のいずれかの前記 W L A N ネットワークオペレータとは独立して、その I P アドレス割当てを管理することができるようになることをさらに備える、請求項 1 に記載の方法。

【請求項 4】

前記第 2 の W L A N ネットワークオペレータは、前記物理ロケーションに関連する他のいずれかの前記 W L A N ネットワークオペレータとは独立して、その I P アドレス割当てを管理することができるようになることをさらに備える、請求項 1 に記載の方法。

20

【請求項 5】

前記物理ロケーションのオーナーは、前記複数の仮想ワイヤレスアクセスポイントの少なくとも仮想ワイヤレスアクセスポイントサブセットをリースすることを通して、収益を得ることができるようになることをさらに備える、請求項 1 に記載の方法。

【請求項 6】

前記物理ロケーションのオーナーは、複数のワイヤレスアクセスポイントハードウェアユニットに亘る仮想ワイヤレスアクセスポイントをグループ化することができるようになることをさらに備える、請求項 1 に記載の方法。

30

【請求項 7】

ワイヤレスネットワークであって、

現地で配備される複数のワイヤレスアクセスポイントハードウェアユニットを備え、

前記複数のワイヤレスアクセスポイントハードウェアユニットのワイヤレスアクセスポイントハードウェアユニットは、複数の仮想ワイヤレスアクセスポイントを提供し、

前記複数のワイヤレスアクセスポイントハードウェアユニットは、現地のオペレータにより所有され、

前記複数の仮想ワイヤレスアクセスポイントの仮想ワイヤレスアクセスポイントの第 1 のサブセットは、第 1 の W L A N プロバイダにより所有され、

40

前記複数の仮想ワイヤレスアクセスポイントの仮想ワイヤレスアクセスポイントの第 2 のサブセットは、第 2 の W L A N プロバイダにより所有される、
ワイヤレスネットワーク。

【請求項 8】

前記複数の仮想ワイヤレスアクセスポイントを管理するために、少なくとも 1 台のクラウドベースのコントローラをさらに備える、請求項 7 に記載のワイヤレスネットワーク。

【請求項 9】

前記仮想ワイヤレスアクセスポイントは、前記複数のワイヤレスアクセスポイントハードウェアユニットに亘ってグループ化することができる、請求項 7 に記載のワイヤレスネットワーク。

50

【請求項 10】

前記複数の仮想ワイヤレスアクセスポイントの仮想ワイヤレスアクセスポイントの前記第1のサブセットは、IPアドレスの第1のセットに関連し、前記IPアドレスの第1のセットは、前記仮想ワイヤレスアクセスポイントの前記第2のサブセットに関連するIPアドレスの第2のセットに対して独立して割り当てられることができる、請求項7に記載のワイヤレスネットワーク。

【請求項 11】

前記仮想ワイヤレスアクセスポイントの各グループは、サービスセット識別子(SSID)に関連する、請求項7に記載のワイヤレスネットワーク。

【請求項 12】

前記仮想ワイヤレスアクセスポイントの各グループは、固有のグループ名に関連する、請求項7に記載のワイヤレスネットワーク。

【請求項 13】

クラウドベースのコントローラを用いる際に、L3モビリティを支援する方法であって、

ローミングワイヤレスクライアントデバイスに関連するマスターセッションキー(MSK)情報を保存すること、

ここで、前記マスターセッションキー(MSK)情報は、前記ローミングワイヤレスクライアントデバイスのためのアンカーアクセスポイントで、前記ローミングワイヤレスクライアントデバイスに関連する認証を行う間に発生し、

前記アンカーアクセスポイントから、前記ローミングワイヤレスクライアントデバイスがローミングを行うアクセスポイントの第1のローミング範囲を予測すること、

前記マスターセッションキー(MSK)情報を、前記アクセスポイントの前記第1のローミング範囲の少なくとも第1のサブセットに、コピーすること、及び、

前記ローミングワイヤレスクライアントデバイスが現在ローミングを行っている現在のアクセスポイントと、前記アンカーアクセスポイントとの間に、インターネットプロトコルトンネルを形成できるようにすること、

を備え、

前記インターネットプロトコルトンネルは、前記ワイヤレスクライアントデバイスが、前記アンカーアクセスポイントに関連するその元々のIPアドレスを保持することを可能にする、方法。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、電子通信に関し、より具体的には、WiFiネットワークアーキテクチャ及びサービスの態様に関する。

【図面の簡単な説明】**【0002】**

【図1】所定の実施形態に従った、仮想企業アクセスポイントネットワークアーキテクチャの態様を示す高水準のネットワーク図である。

【図2】所定の実施形態に従った、発見の態様及びアクセスポイントに関連した登録手順を示す高水準参照図である。

【図3】所定の実施形態に従った、クラウドベースのサイト間VPN動的接続の態様を示す高水準ネットワーク図である。

【図4】所定の実施形態に従った、ワイヤレスモビリティドメインの管理の態様を示す高水準参照図である。

【図5】所定の実施形態に従った、ローミング範囲予測の態様を示す高水準参照図である。

【図6】所定の実施形態に従った、サブネットアドレス情報及びローミングアンカーAPアドレスのサンプルデータフォーマットの表である。

10

20

30

40

50

【図 7】所定の実施形態に従った、クラウドベースのレイヤ 3 モビリティ制御の態様を示す高水準ネットワーク図である。

【図 8】所定の実施形態に従い、アクセスポイント（ＡＰ）において経路を格納する高速ネットワークデータのデザインの態様を示す高水準ネットワーク図である。

【図 9】所定の実施形態に従った、ＡＰ間通信の態様を示す高水準ネットワーク図である。

【発明を実施するための形態】

【０００３】

本発明の方法、システム、ユーザインターフェース及びその他の態様を説明する。

【０００４】

本発明の所定の実施形態が参照され、その例が、添付の図面に図示される。

【０００５】

本発明を、実施形態に関連して説明していくが、それが本発明を、これらの特定の実施形態単独に限定することを意図するものではないことが、理解されよう。

【０００６】

逆に、本発明は、本発明の精神及び範囲内にある代替物、修正物及び等価物をカバーすることを意図するものである。

【０００７】

従って、明細書及び図面は、制限的な感覚ではなく、例示的なものと認識されよう。

【０００８】

さらに、以下の説明において、多数の具体的な詳細が、本発明の完全な理解を提供するために述べられる。

【０００９】

しかしながら、本発明がこれらの特定の詳細なしでも実行可能であることは、当業者にとって明らかである。

【００１０】

他の例では、当該技術分野の通常の知識を有する者に周知である方法、手順、構成要素及びネットワークについては、本発明の態様を不明瞭にすることを回避するために、詳細に説明しないこととする。

【００１１】

所定の実施形態に従い、仮想企業アクセスポイント（ＶＥＡＰ）制御及び管理システムを用いて、企業グレード仮想アクセスポイント（ＡＰ）及び高い性能企業ＡＰハードウェアを提供する。

【００１２】

所定の実施形態に従い、企業グレードの仮想ＡＰを配備することにより、ＡＰを多数配備する必要性を排除し、したがって信号障害を低減する。

【００１３】

さらに、ＶＥＡＰシステムは、集中化かつ連係した方法で、ＡＰを管理する。ここでは、ＶＥＡＰを、仮想アクセスポイント（ＶＡＰ）とも呼ぶ。

【００１４】

所定の実施形態に従い、ＶＥＡＰシステムは、２階層のオーナーシップモデルをカバーする：１）企業ＡＰハードウェアのオーナーシップ、及び
２）企業ＡＰハードウェアを用いたネットワークサービスのオーナーシップ（以下「仮想ＡＰ」と呼ぶ）。

【００１５】

例えば、企業ＡＰハードウェアのオーナーは、好ましくは不動産の地主又はオーナー（以下、「ネットワーク現地オーナー」と呼ぶ）であり、そこでは、物理ワイヤレスネットワークインフラ（企業ＡＰハードウェアを含む）が展開されている。物理ワイヤレスネットワークインフラ上で動作するＷＬＡＮのオーナーは、好ましくは、仮想ＡＰをネットワーク現地オーナーからリースするサービス提供者（ＳＰ）又はキャリアである。

10

20

30

40

50

【 0 0 1 6 】

所定の実施形態に従い、ネットワーク現地オナは、企業 A P ハードウェアリソースの取扱いを管理及び制御する。例えば、企業 A P ハードウェアは、8 ~ 16 個の仮想 A P を提供することができる。仮想 A P のコストは、物理企業 A P わずかなコストのみである。さらに、物理 A P ネットワークのサービスを提供する現地オナにより集中的管理を行うことにより、A P の管理及びトラブルシューティングを低減することができる。S P は、仮想 A P を用いて、W L A N を作成及び操作することができる。したがって、S P は、企業 A P ハードウェア及びこれに関連したインフラを配備することを必要とせず、W L A N を管理することが可能となる。

【 0 0 1 7 】

図 1 は、所定の実施形態に従った、仮想企業アクセスポイントネットワークアーキテクチャの態様を示す高水準のネットワーク図である。図 1 は、所定の実施形態に従って、クラウドコントローラ 102、1 つ以上のキャリアインターネット網 104 a ~ c、1 つ以上のキャリア W i F i 105 a ~ c、及び複数の A P 110 a ~ d を含む、V E A P ネットワークアーキテクチャ 100 を示す。クラウドコントローラ 102 は、制御経路 108 a ~ c を通して、キャリア W i F i 105 a ~ c を制御する。クラウドコントローラ 102 は、データ経路 107 a ~ d を通して複数の A P 110 a ~ d と通信を行う。V E A P アーキテクチャは、外部ネットワーク（例えば、キャリアネットワーク）による、クラウドを介した効果的な垂直管理のために、既存の W i F i チップセットベンダの仮想 A P (V A P) 技術を活用する。所定の実施形態に従い、V A P の管理技術は、外部ネットワークとのネットワークインターフェースを提供する。さらに、V E A P アーキテクチャは、A P インフラの管理を共有するために、複数のキャリアのためにマルチテナンシーサポートを提供する。ネットワーク現地オナ（不動産及び A P ハードウェア及びインフラのオナ）は、現地を管理することに熟達している。したがって、所定の実施形態に従い、ネットワーク現地オナ又はマネージャは、キャリア / S P に対して、W L A N の企業グレード仮想 A P、高品質ワイヤレスネットワークインフラサービス及びリモート集中管理を、企業グレード A P ハードウェア及び関連したインフラを配備するわずかな価格で、提供することができる。

【 0 0 1 8 】

したがって、上記の V E A P アーキテクチャは、W i F i ネットワークサービスの全てのパーティーに対して有益である。モバイルクライアントは、企業グレードワイヤレスネットワークサービスを楽しむ。現地オナは、複数のキャリア / S P に A P インフラをリースすることにより、繰り返し収益を享受する。キャリア / S P は、高価な企業グレード A P ハードウェアを購入して展開する必要無しに、高品質 W L A N を操業することが可能となる。したがって、キャリア / S P は、貯蓄を用いて、追加の価値を付加するサービスをモバイルクライアントに提供して部門収益を増大することが、可能となる。

【 0 0 1 9 】

所定の実施形態に従い、アクセスポイント (A P) を仮想化することにより、アクセスポイントハードウェアリソースを、ネットワークリソースとは別々に管理できるようになるという利益がもたらされる。非限定的な例として、アクセスポイントハードウェアリソースは、無線通信スペースリソース、メモリ及びイーサネット（登録商標）インターフェースを含む。非限定的な例として、ネットワークリソースは、アクセスポイントネットワークブリッジ、インターネットプロトコル (I P) ネットワーク及びネットワークサーバを含む。所定の実施形態に従い、現地オナ又はマネージャは、アクセスポイントハードウェア及びアクセスポイントハードウェアに関連するリソースを管理及び制御する。W L A N オペレータは、ネットワークリソース及び仮想アクセスポイントを管理及び制御することが可能である。

【 0 0 2 0 】

さらに、所定の実施形態に従い、A P リソースを、仮想化することができる。非限定的な例として、W L A N オペレータは、アクセスポイントに関連するメモリリソースの使用

10

20

30

40

50

を、1つ以上の企業体（たとえば、1つ以上のウェブ取引企業）にリースすることができる。現地オーナー/マネージャが、キャリアネットワークでもあるという場合もある。そのような場合、1つ以上のウェブ取引企業は、現地オーナー/マネージャから、APメモリリソースのレンタルを受けることも可能である。非限定的な例として、所定の実施形態に従い、1つ以上のウェブ取引企業は、広告及びプロモーション活動、アプリケーションの保管、ビデオの保管、コンテンツの保管、クライアントトラフィックの分析、インターネットアクセスの制御、アプリケーションの配信及びコンテンツの配信のための、メモリリソースをリースすることができる。また、WLANオペレータは、ウェブ取引企業又は他の企業にリースしなかった自分のAPメモリリソースを、例えば広告及びプロモーション活動、アプリケーションの保管、ビデオの保管、コンテンツの保管、クライアントトラフィックの分析、インターネットアクセスの制御、アプリケーションの配信及びコンテンツの配信等の同様の目的のために用いることもできる。

10

20

30

40

50

【0021】

所定の実施形態に従い、クラウドコントローラは、マルチテナンシークラウドコントローラである。マルチテナンシークラウドコントローラは、別々のテナントコントローラ又は仮想コントローラを実行する複数のクラスタサーバを含む。所定の実施形態に従い、所定のAPが、クラスタサーバの中からAPの対応する仮想コントローラを特定することを援助するために、クラウドサイトコントローラマネージャ（SCM）が用いられる。例えば、所定のAPが「ワイヤレスアクセスポイントの制御及び供給」（CAPWAP）発見リクエストを送信するとき、SCMは、このCAPWAPリクエストをインターセプトする。このCAPWAPリクエストには、APのメディアアクセス制御アドレス（MACアドレス）及びAPに関連した固有のテナントアカウントのための証明書が含まれている。したがって、SCMはAPのMACアドレスを調べることができ、特定のAPに関連する固有テナントコントローラのアドレスを、そのAPに戻すことができる。APはその後、リクエストを各々のテナントコントローラに送信する試行錯誤方式ではなく、正しいテナントコントローラアドレスを用いて、CAPWAPプロトコルセッションを直接開始することができる。

【0022】

図2は、所定の実施形態に従った、発見の態様及びアクセスポイントに関連した登録手順を示す高水準参照図である。図2には、AP201、SCM202、データベース203、サーバクラスタ（又は、コントローラクラスタ）204、ネットワーク管理システム205及びDNSサーバ206が示される。SCM202とAP201が通信を行い（207を参照）、適切なテナントコントローラ212をAP201に（例えば、割り当てられたテナントアカウントID、APのデバイスID、APのプライベートIPアドレス及びAPの一般IPアドレスに基づいて）割り当てることにより、サーバクラスタ/コントローラクラスタ204内のAP201と、対応するテナントコントローラとの間で、データトランスポートレイヤセキュリティ（DTLS）セッション208を確立する。AP201は、DNSサーバ206からSCMのリストを見つけることができる。DTLSセッション208が確立されれば、APは、サーバクラスタ/コントローラクラスタ204内のAPの対応するテナントコントローラに、「結合」リクエスト209を送信することができる。結合が成功した場合は、テナントコントローラは、成功したAPの結合213を報告する。さらに、テナントコントローラ及び他のサーバクラスタが、情報210をデータベース203に報告することができる。その情報には、コントローラのロード、キャパシティ及び健全性を含めることができる。

【0023】

所定の実施形態の他の態様に従い、ここに説明するように、SCMは、VEAPネットワークアーキテクチャ下のAPディストリビューションに対する、複数のデータセンターロケーション間のコーディネータとしての機能も果たす。VEAPネットワークアーキテクチャ下では、データセンターロケーションは、現地オーナーには、明白である。所定の実施形態に従い、各々のデータセンターは、VEAPネットワークアーキテクチャ下のいず

れかの A P によりアクセス可能となっている。データセンターは、主サイト又はバックアップサイトとして、いずれかの現地オーナーに対するサービスを提供する。所与の A P が現地オーナーの施設に配備されれば、その A P は、現地オーナーによる機器構成を必要とすることなく、対応するデータセンターを自動的に決定して、そこへ接続することができる。したがって、データセンターは、A P により自動的に発見される必要がある。現地オーナーの施設に配備される A P が、適切なデータセンターとデータセンター内の対応するテナントコントローラとを結合することができるよう、S C M は、データセンター間及びデータセンター内部のコーディネータとなることができる。

【 0 0 2 4 】

S C M は、各々のデータセンターの第 1 の接点である。所定の実施形態に従い、S C M は、以下の特性を有する： 1) S C M はそれぞれのデータセンターに配備され、S C M は第 1 の接点である。S C M は、A P の発見リクエストを適切なデータセンター及びそのデータセンター内の正しいテナントコントローラにリダイレクトして、A P とその対応するテナントコントローラとの間にセッションを確立するために、必要な知識を有している。 2) S C M は、同じ地域のロケーションから異なるデータセンターロケーションに亘って A P を広げる代わりに、正しいデータセンターロケーションとの A P 接続を確定的にリダイレクトして統合することができる。 3) S C M のリストは、標準 D N S プロトコルを用いて、所与のいずれかの A P によって発見可能である。A P は、D N S 情報 (D N S 記録) を用いて、S C M のいずれかと通信することができる。したがって、A P は、総当たり戦方法で S C M のリストと通信して、登録のために適切なデータセンターのロケーションを見出すことが可能である。登録が成功すれば、A P は、次の登録リクエストのブートアップ又はスタートアップのために、S C M のアドレスをキャッシュに格納することができる。

【 0 0 2 5 】

所定の実施形態に従い、クラウドベースのサイト間 V P N ネットワークを用いて、企業の支社に対して、従来のハードウェア V P N ゲートウェイソリューションに関連した問題を、未然に防ぐ。クラウドベースのサイト間 V P N ネットワークを採用することにより、企業のそれぞれのオフィスサイトに、別々の V P N ゲートウェイを設置することに関連した配備及び維持にかかるコスト上昇が、回避される。

【 0 0 2 6 】

所定の実施形態に従い、クラウドベースのサイト間 V P N ネットワークは、 1) ソフトウェア実行 V P N ゲートウェイ (ソフト V P N ゲートウェイ)、及び、 2) クラウド V P N コントローラ、を含む。リアルタイムトラフィックポリシングに対して、クラウド V P N コントローラからプッシュダウンされたポリシーを実行することができるゲートウェイを、ソフト V P N として実行するように、企業の支社サイトに配備される A P を設定することができる。クラウド V P N コントローラは、セントラル V P N ポリシーマネジメント及び V P N トンネルネットワークを提供する。したがって、クラウドベースのサイト間 V P N ネットワークは、I T 人員が、それぞれのサイトでハードウェア V P N ゲートウェイをインストール又はこれにアクセスする必要無く、様々なサイト間での動的な V P N トラフィック経路ルーティングを、容易に変更 / 更新することを可能にするソフトウェアソリューションである。無線ネットワークのためのクラウドベースのソリューションを採用する企業は、企業の支社、小売店、P O S サイト等を接続するために、クラウドベースの V P N ソリューションを採用する可能性が高い。したがって、V P N 市場は、数十億ドルの規模で運営されている。

【 0 0 2 7 】

図 3 は、所定の実施形態に従った、クラウドベースのサイト間 V P N 動的接続の態様を示す高水準ネットワーク図である。図 3 は、クラウドベースの V P N ネットワークが、クラウド企業 W L A N コントローラ 3 0 4 a ~ e、V P N サービスエンジン 3 0 6 a ~ d、A P 3 0 2 a ~ b 及びセキュアトンネル 3 0 5 a ~ b を含んでいることを示す。A P 3 0 2 a ~ b は、ソフト V P N ゲートウェイとして実行される。例えば、A P 3 0 2 a は、企

10

20

30

40

50

業サイト301のソフトVPNゲートウェイとして実行される。AP302bは、企業サイト303のソフトVPNゲートウェイとして実行される。クラウド企業WLANコントローラ304c、304eは、セントラルVPNポリシーマネジメントを、AP302a、302bそれぞれに提供する。VPNサービスエンジン306a～dは、企業サイト301、303の間のVPNトラフィック307に対して、セキュアトンネル305a～bを動的に提供する。無線デバイス308aと308bとは、それらのそれぞれのAP302a、302b及びクラウド企業WLANコントローラ304c、304e、並びに、対応するセキュアトンネル305bを通して、通信を行う。

【0028】

従来のハードウェアで実行される企業WLANコントローラに関しては、それぞれのハードウェアコントローラは、一群のAPに物理的に接続されている。したがって、APのグループは、バッチで設定及び管理が可能である。しかしながら、ここに説明されるWLAN用のクラウドベースのコントローラの場合、APは、コントローラに物理的に接続されていない。したがって、このような一組のAPは、従来の意味では、グループ化されないことになる。所定の現地オーナーのサイトにありかつクラウドベースのWLANコントローラに関連する多数のAPに対して、バッチ設定を適用することは、困難である。所定の実施形態に従い、クラウドベースのWLANコントローラと関連するAPのバッチ設定を容易にするため、ワイヤレスモビリティドメインが作成される。所定の実施形態に従い、ワイヤレスモビリティドメインは、同じドメイン下で管理される一群のAPを定義する。所定のワイヤレスモビリティドメインのAPは、地理的に、相互及びAPが取り扱うワイヤレスクライアントの比較的近くに位置する。所定のワイヤレスモビリティドメインのAPは、同じWLAN設定及びポリシーを共有する。例えば、ワイヤレスモビリティドメインを用いて、企業本社からリモートに位置するそれぞれの企業支社等、特定のロケーションに配備されるAPの範囲を定義することができる。上記の例では、ワイヤレスモビリティドメインは企業支社ごとに、WLANマネジメントの設定が異なってもよい。したがって、企業のIT社員は、ワイヤレスモビリティドメインを用いることにより、それぞれの支社ごとに異なるWLANネットワークの設定及びポリシーを、容易かつ柔軟に適用することができる。

【0029】

図4は、所定の実施形態に従って、ワイヤレスモビリティドメインを用いるAPのマネジメントの態様を示す高水準参照図である。図4は、本社ワイヤレスモビリティドメイン402及び対応する出張ワイヤレスモビリティドメイン403、404及び405を含む、ワイヤレスモビリティドメインネットワーク401を示す。ワイヤレスモビリティドメイン402、403、404及び405は、別々のWLAN設定及びポリシーを有していてもよい。

【0030】

他の例として、大学キャンパスが、その学部の建物のそれぞれに、APを配備していると仮定する。大学は、1つのワイヤレスモビリティドメインを用いて、大学キャンパスの全てのAPを管理するか、又は、アセットトラッキングのため、又は、同じロケーション中の各学部又は各階に固有の、それとは異なるマネジメント目的のため、その学部の別々のワイヤレスモビリティドメインを用いるかの、選択権を有する。

【0031】

L3(レイヤ3)モビリティ又はローミングは、別々の会社サブネットをローミングで結ぶワイヤレスクライアントのために、継ぎ目のないワイヤレス接続性を提供する企業WLANの特徴である。例えば、会社が適切なWLANRFカバレッジを有する場合は、L3モビリティは、ワイヤレスクライアント(スマートフォン、タブレット又はノートブック等)が、会社キャンパスの周囲でローミングを行いながら、VoIP及びビデオストリーミング等のリアルタイムアプリケーションをワイヤレスクライアント上で連続的に実行させることが、可能となる。

【0032】

10

20

30

40

50

L3モビリティを達成するため、WLAN製品は、以下を実行する必要がある：1) 一方のAPから他方へのワイヤレスクライアントの接続の高速ハンドオーバー；及び、2) 別々のサブネットドメイン間で同じワイヤレスクライアントのIPアドレスを保持すること。

【0033】

高速ハンドオーバーは、ワイヤレスクライアント上でのリアルタイムアプリケーション稼働の中断又は切断を回避するために必要である。一方のAPから他方へ、ワイヤレスクライアント接続の高速ハンドオーバーを実行するためには、ワイヤレスクライアントがローミングを行う新しいAPを再認証するために必要な時間は、40ms未満、又はアプリケーションによっては20ms未満、でなければならない。新しいAPの再認証は、新しいAPによる「再接続」ともいわれる。新しいAPを再認証するために必要な時間が20msによりも長い場合は、VoIPのようなリアルタイムアプリケーションに対して、ジッター又は切断が起こりうる。認証のために必要な時間は、ポートベースのアクセス制御AAAサーバ802.1Xによる良好なLAN環境では、約40ms～80msである。

【0034】

さらに、ワイヤレスクライアントが、別々のネットワークアドレスを有するサブネットに関連した新しいAPとのローミングを行う場合は、ワイヤレスクライアントは、サブネットのIPアドレスを取得する。ワイヤレスクライアントのIPアドレスが新しく取得されたIPアドレスに変更されれば、ワイヤレスクライアント上で実行しているアプリケーション（例えば、VoIP又はビデオストリーミング）は中断する。このような中断は、ビジネスコミュニケーションには不适当であり、ネットワークセキュリティポリシーの保持には不十分である。

【0035】

適切なレイヤ3（L3）モビリティを提供するため、ワイヤレスクライアントがAPからAPへとローミングを行う際に、従来の企業WLANは、中央に位置するハードウェアコントローラを、唯一の認証者として利用することにより、ローミング中にそれぞれのAPで完全な再認証を実行する必要性が不要になる。セントラルハードウェアコントローラは、セントラルコントローラとワイヤレスクライアントのホームサブネットとの間のIPTunnelを容易にセットアップすることができ、この場合、ワイヤレスクライアントのIPアドレスはもともと割り当てられていたため、ワイヤレスクライアントが、そのもとのIPアドレスを用い続けることができるのである。しかしながら、会社ネットワークに関連するコントローラが、セントラルにインストールされていないため、クラウドベースのコントローラを企業/会社ネットワークに用いる従来のハードウェアコントローラソリューションは、WLANに適用できない。クラウド（インターネット）では、予測不能で長期にわたるインターネット待ち時間が発生するので、クラウドベースのコントローラは、高速のハンドオーバーを実行することができない。さらに、クラウドベースのコントローラが、会社WLANのセントラルロケーションではなく、クラウドの中にあるため、クラウドベースのコントローラは、ワイヤレスクライアントのホームサブネットとクラウドベースのコントローラとの間で、IPTunnelをセットアップすることができない。また、インターネット接続がダウンしている場合は、クラウドベースのコントローラは、ワイヤレスクライアントのためのL3モビリティを保持することができない。

【0036】

上記を考慮し、所定の実施形態に従い、以下の方法を用いて、クラウドベースのコントローラを用いるWLANでのL3モビリティをサポートする。1) クライアントローミング範囲を予測する、及び、2) ローミングアンカーAPを用いる。

【0037】

所定の実施形態に従い、ワイヤレスクライアントによるローミング中に各APでワイヤレスクライアントの再認証/再接続処理を行う間の往復の数を低減することにより、高速ハンドオーバー機能を可能にすることに関連して、クライアントローミング範囲予測を用いる。最初のAPでの認証プロセスの一部を行っている間（ワイヤレスクライアントがロー

10

20

30

40

50

ミングを行い始める前)に発生するマスターセッションキー(MSK)を、キャッシュに格納する又は別段に保存することにより、この往復の数を低減することは可能である。クラウドコントローラは、ワイヤレスクライアントがローミングを行う新しいAPに、MSKをコピーすることができる。したがって、ワイヤレスクライアントがその新しいAPにローミングを行う際に、新しいAPに求められるのは、バックエンドAAAサーバで完全な再認証プロセスを実行することではなく、ただトラフィックキー(TK)を再生して、再認証/再接続プロセスを完了するだけである。MSKを適切なAPにコピーするため、クラウドコントローラは、ワイヤレスクライアントがどのAPにローミングを行うかを事前に知っている必要がある。所定の実施形態に従い、各ワイヤレスクライアントのMSKを、会社ネットワークで全てのAPにコピーすることができる。この方法は、APが多数のキーに圧倒されてしまわないよう、少数のAPに有用である。他の具体例に従い、ワイヤレスクライアントのMSKは、ワイヤレスクライアントがローミングを行うことができると思われる一組のAPのみにコピーされ、そしてエージアウトタイマーを実行してこのAPからMSKを除去し、APがキーで渋滞することを回避する。説明すると、ワイヤレスクライアントがローミングを行うことができる近隣のAPの範囲(「ローミング範囲」)は、所定の実施形態によれば、確定的に特定される。

【0038】

図5は、所定の実施形態に従ったワイヤレスクライアントのローミング範囲を予測する態様を示す高水準参照図である。図5は、APの「A」、「B」、「C」、「D」、「E」、「F」、「G」、「H」を示す。この実施形態では、いずれかの数のAPを含むことができるが、説明の容易性のため、APを8個だけ示すこととする。ワイヤレスクライアントが先ずAP「C」に関連するとき、ワイヤレスクライアントのローミング範囲は、緑色の破線502により示される近傍「A」、「B」、「D」、「E」を含むことが予測される。ワイヤレスクライアントが「E」へ移動すれば、ワイヤレスクライアントのローミング範囲は、赤色破線503により示される近傍「C」、「D」、「F」、「H」を含むと予測される。同様に、ワイヤレスクライアントが「F」へ移動すれば、ワイヤレスクライアントのローミング範囲は、青色破線504により示される、近傍「D」、「E」、「H」、「G」を含むと予測される、等である。したがって、MSKは、ワイヤレスクライアントのローミング範囲の中で限られたAPのセットにコピーされ得るのであり、オーナーの現地又は企業ネットワーク中の全てのAPにコピーされるのではない。しかしながら、クラウドベースのコントローラが連絡可能でない場合、例えば会社のWAN又はインターネットがダウンしているような場合は、ワイヤレスクライアントの予測されたローミング範囲でAPにMSKをコピーするクラウドコントローラが存在しないことになる。所定の実施形態に従い、図9は、AP間通信の態様を示す高水準ネットワーク図である。図9は、会社WLAN900、AP901a~m、ローミング範囲902、AP間通信903及びワイヤレスクライアント905を示す。所定の実施形態に従い、ワイヤレスクライアント905の予測されたローミング範囲902でAPにMSKをコピーするためのクラウドベースのコントローラが、連絡可能でない場合は、AP901a~mは、バックホール有線ネットワークインターフェースによってAP間通信903を実行して、ワイヤレスクライアント905のローミング範囲でAP間に必要であるMSK及びその他の情報を交換することができる。802.11対応のAPは、ワイヤレスクライアント905が検出可能なビーコンフレームを、周期的にブロードキャストする。所定の実施形態に従い、APは、WLANSSID及び802.11ベンダー固有IE(情報要素)を埋め込んだAPIPアドレスを、APのビーコンフレームに有する。この802.11ベンダー固有IEを有してブロードキャストされるビーコンフレームは、ローミング範囲内のAPにのみ受信されるだろう。ローミング範囲外にあるAPは、このブロードキャストされたビーコンフレームを受信しないだろう。したがって、ローミング範囲内のAPは、クラウドコントローラへの接続を行わずに、相互を検出することができ、また、相互とMSK情報を通信及び交換することができる。同様に、「ローミングアンカーAP」に関してここに説明する機能を提供するために、AP間通信を適用することができる。

【 0 0 3 9 】

所定の実施形態に従い、ローミングアンカー A P を用いることにより、ワイヤレスクライアントが同じサブネットの中で A P から A P までローミングを行う際、又は、別々のサブネットにローミングを行う際に、ワイヤレスクライアントが同じ I P アドレスを保つことが可能になる。ローミングアンカー A P は、ワイヤレスクライアントがサブネットからその I P アドレスを当初取得した A P である。ローミングアンカー A P は、ローミングワイヤレスクライアントのためのアンカーポイントになる。クラウドコントローラは、ローミングアンカー A P の近傍 A P に、ローミングアンカー A P の I P アドレス情報を掲示することができる。例えば、ワイヤレスクライアントが近隣の A P にローミングを行えば、近隣の A P (例えば「 X 」) は、ローミングアンカー A P を有する I P トンネルを形成することができることになるので、ワイヤレスクライアントがそのもともとの I P アドレスを保つことができるようになる。ワイヤレスクライアントがさらに別の A P (例えば、「 Y 」) にローミングを行えば、新しい I P トンネルは、「 Y 」と、「 X 」ではなくローミングアンカー A P との間で形成されるようになる。この I P トンネルを形成する方法により、A P に対して過剰な数の I P トンネルを詰め込むことが、回避される。さらに、ローミングアンカー A P の情報が各 A P に保存されるため、所定の A P がクラウドコントローラへの接続を失った場合でも、L 3 モビリティ機能は、実行可能なままで保たれる。ワイヤレスクライアントがそのもともとの I P アドレスを取得した当初に、ローミングワイヤレスクライアントのアンカー A P を決定するためのクラウドコントローラが利用できない場合には、上記の A P 間通信のためにブロードキャストされたビーコンフレームを使用して、アンカー A P 情報を「ローミング範囲」の A P に提供することが可能となる。図 6 は、所定の実施形態に従った、サブネットアドレス情報 6 0 1 及びローミングアンカー A P アドレス 6 0 2 のサンプルデータフォーマットの表である。

【 0 0 4 0 】

図 7 は、所定の実施形態に従った、クラウドベースのレイヤ 3 モビリティ制御の態様を示す高水準ネットワーク図である。図 7 は、クラウドコントローラ 7 0 1、A P 7 0 2 a ~ 1、ローミングアンカー A P 7 0 3、ワイヤレスクライアント 7 0 6 及びサブネット 7 0 7、7 0 8 及び 7 0 9 を示す。L 3 モビリティを制御するため、クラウドコントローラ 7 0 1 は、ワイヤレスクライアント 7 0 6 のローミング範囲内の「近傍 A P」に、M S K をコピーする。ワイヤレスクライアント 7 0 6 の I P アドレスを保持するため、例えばワイヤレスクライアント 7 0 6 が、サブネット 7 0 7 から、サブネット 7 0 8 へサブネット 7 0 9 へとローミングを行う際に、ローミングアンカー A P と所定の A P 7 0 2 の間に I P トンネルが形成される。ここに記載される制御 L 3 モビリティのための方法を、クラウドベースのコントローラを利用する大企業営業所ネットワークに用いることで、連続ワイヤレス V o I P 通信及びネットワークセキュリティポリシーをモバイル機器に提供することが可能となる。

【 0 0 4 1 】

所定の実施形態に従い、ワイヤレスクライアントデバイスのローミング範囲内にある「近傍 A P」は、クライアントデバイスに関連する無線通信信号強度指数 (R S S I) 情報をクラウドコントローラに送信する。さらに、所定のローミング範囲のアクセスポイント同士は、W i - F i 又は有線のネットワークインターフェースによって相互間で情報を交換し合う。交換される情報には、アクセスポイントのローミング範囲内の各アクセスポイントの W L A N S S I D (サービスセット識別名) 情報及び I P アドレス情報が含まれる。

【 0 0 4 2 】

ワイヤレスアクセスポイントの制御及び供給 (「 C A P W A P 」) は、コントローラがワイヤレスアクセスポイントの収集を管理することを可能にする相互運用可能なプロトコルである。C A P W A P プロトコルは、制御チャネル用の U D P ポート 5 2 4 6 及びデータチャネル用のポート 5 2 4 7 の使用を含んでいる。C A P W A P 標準は、設定マネジメント及びデバイスマネジメントを、A P の方にプッシュできるようにする。C A P W A P

プロトコルは、いくつかの段階を含む。１）発見、２）結合、３）、設定、４）ファームウェアアップデート、及び、５）マネジメント。UDPブロードキャストは会社ネットワークに限定されインターネットに転送されないため、既存のCAPWAP発見プロトコルは、インターネット対しては有効でない。さらに、社内ネットワーク内のファイアウォールが、インターネットへのUDPユニキャストをブロックし得る。CAPWAP発見プロトコルは、専用の予め設定されたハードウェアコントローラでのみ有効なだけある。ここに記載されるように、CAPWAP発見プロトコルはマルチテナントクラウド構造で実行される仮想コントローラを発見することができない。

【 0 0 4 3 】

所定の実施形態に従い、ここに記載されるマルチテナントクラウド構造に使用するため、従来のCAPWAPを、標準HTTPS（ハイパーテキストトランスファープロトコルセキュア）プロトコルを用いるクラウドコントローラCAPWAP発見プロトコルを用いて置換する。クラウドコントローラCAPWAP発見プロトコルは、社内ネットワークに関連する潜在的ファイアウォールの問題を解決し得る。クラウドコントローラCAPWAP発見プロトコルは、対応する仮想コントローラを先ず発見して、適切な輸送プロトコルをネゴシエートする。例えば、輸送プロトコルは、社内ネットワークファイアウォール条件により、もともとのUDPプロトコル又はHTTP（ハイパーテキストトランスファープロトコル）プロトコルとすることができる。HTTPセッションがクラウドリソースに関してスケーリング問題を引き起こし得るため、UDPは、クラウドベースコントローラのための好ましい輸送手段である。クラウドコントローラCAPWAP発見プロトコルは、クラウドベースのコントローラでのリソースの使用を最適化する。クラウドコントローラCAPWAP発見プロトコルは、CAPWAPプロトコルを、会社のプライベートなLAN又はVPNネットワーク内に制限するのに代えて、外部のインターネット網に延長することに対する最初のステップを確立する。したがって、クラウドベースのコントローラに連携したクラウドベースのCAPWAP発見プロトコルは、内部の企業ネットワーク又はVPNの使用に限定するのではなく、例えばマルチプロトコル標識スイッチング仮想専用ネットワーク（MPLSVPN）等の広域ネットワークにわたるインターネットソリューションを提供する。

【 0 0 4 4 】

発見段階の結果によっては、会社ファイアウォールがインターネットへのUDPプロトコルをブロックする際に、クラウドベースのコントローラと結合して通信するために、クラウドベースのCAPWAP発見プロトコルは、APに対するHTTPプロトコルの使用をネゴシエートすることができる。所定の実施形態に従い、レガシーCAPWAPUDPプロトコルに対して領域互換性があるため、クラウドベースのCAPWAPUDPプロトコルは、HTTPトンネルに供給される。AP及びクラウドベースのコントローラの両方は任意に、HTTPプロトコルでCAPWAPUDPパケットをカプセル化することができ、また、カプセル開放を行うことができる。HTTPプロトコルは、UDP輸送手段とは完全に別々なTCP輸送手段プロトコルである。各UDPパケットは、受信により命令されるパケット境界の指示を含む。受信者側でのUDPメッセージの読み込み操作により、もともと送信されたメッセージ全体の長さがわかる。対照的に、TCPプロトコルデータは、バイトストリームとして読み出され、信号メッセージ境界には、特徴的な指示は伝送されない。さらに、TCPプロトコルデータは、バイトストリームとして読み出されるため、元々のUDPメッセージパケットの途中で、受信者側に読み取り中断が発生する可能性は、非常に高い。所定の実施形態に従い、HTTPプロトコルにおけるUDPパケット境界指示を含む専用のライトウェイトプロトコルが用いられる。さらに、このライトウェイトプロトコルは、受信者側のUDPメッセージの読み取りが、元々のUDPパケットの途中で切断されないことを確実にする方法で、プロトコルを保持する。このプロトコルは、会社LAN環境からインターネット環境（クラウド環境）へのCAPWAPプロトコル移動を完了させる一方、元々の標準CAPWAPUDPプロトコルとの互換性を保持して、従来の企業APや従来の企業コントローラでの相互運用性を確保する。

10

20

30

40

50

【 0 0 4 5 】

所定の実施形態に従い、A Pとこれに対応するクラウドコントローラとの間のファイアウォールをA Pが検出した時に、A Pは、データグラムトランスポートレイヤセキュリティ(D T L S)プロトコル上のC A P W A Pから、H T T Pプロトコル上のC A P W A Pへと切り替える情報を有している。換言すれば、発見が終了した後、ファイアウォールがA Pとクラウドコントローラとの間にない場合に、デフォルトとして、所定のA Pは、D T L Sプロトコル上のC A P W A Pを用いて、U D Pのデータ輸送手段の安全な通信に関連したクラウドコントローラと、接続及び通信を行う。しかしながら、A Pとクラウドコントローラとの間にファイアウォールがある場合は、A Pは、ファイアウォールを検出するのに十分情報を有しており、H T T P又はH T T Pプロトコルを用いて、クラウドコントローラと、接続及び通信を行うだろう。

10

【 0 0 4 6 】

高速ネットワークリンクからの全てのH T T P U R L /ヘッダ等のパケットトレースを捕捉して、さらに後処理のためにハードディスクにこのトレースを保存することは、高コストのハードウェア・プラットフォームが必要となり、又は、O Sネットワークスタックを最適化してメモリコピーの数を削減することが必要となる。しかしながら、最適化されたネットワークスタックを有する一般的なオペレーティングシステム、又は、例えばリテール版W i F i A P又は事業グレードライトA P等の低コストプラットフォームは、開発されていない。したがって、A Pパフォーマンスとのトレードオフなしで、高速パケットトレースを収集することは、困難である。

20

【 0 0 4 7 】

一般的なオペレーティングシステムでは、取得されたネットワークパケットをハードディスクに保存する経路は、以下を含む：1) ネットワークプロセッサは、取得されたパケットに対してフィルタリングを行うために、ディープパケットインスペクションを実行する；2) ネットワークプロセッサはパケットを取得して、そのパケットをD M A (ダイレクトメモリアクセス)にコピーし、C P UによりO Sを起動させ、ディスクファイルへの読み書きをするよう、ユーザスペースソフトウェアアプリケーションをスケジューリングする；3) O Sファイルシステムオペレーションはコストが高く、特にデータをディスクファイルへ書き込むために大量のC P Uタイムを消費する。例えば、L i n u x (登録商標) E X T 3 ファイルシステムでは、データオペレーションのタイプにもよるが、C P U使用率は、2 7 % ~ 9 9 %である。さらに、ディスクファイルへの高速ネットワークリンクを用いて、パケットを取得して保存する際は、C P U使用率は著しく上昇し、A Pパフォーマンスに影響を及ぼしうることになる。

30

【 0 0 4 8 】

所定の実施形態に従い、パケットを保存するための、A PネットワークプロセッサからA Pのハードディスクまでの高速経路が、用いられる。所定の実施形態に従い、A Pネットワークプロセッサがパケットを取得してD M Aに関するデータを保存した後、A PのO Sを起動して、A Pディスクファイルにデータを読み書きするよう、ユーザスペースソフトウェアアプリケーションをリスケジューリングする代わりに、A Pカーネルスペースドライバを呼び出して、D M AからA Pのハードディスクへと直接データを伝送し、したがって、A PのO Sファイルシステムを完全にバイパスするよう、A PのO Sは設定される。カーネルスペースドライバのC P U使用率は、比較的低い。しかしながら、ディスク上に保存されるデータを、一般的なO Sファイルシステムが処理することができるフォーマットとすることができない点が、トレードオフになる。したがって、所定の実施形態に従い、A PのO Sファイルシステムによってディスクファイルからデータを読み出す代わりに、カーネルドライバA P Iを用いて、ユーザスペース読み取り書き込みアプリケーションのためにパケットを保存しているディスクから、直接データを読み出す。このプロセスは再び、A PのO Sファイルシステムオペレーションをバイパスする。この方法によれば、取得された各パケットトレースに対しての、往復のファイルシステムI / Oプロセスが排除される。この方法では、ごくわずかなC P Uタイムしか用いずに、ネットワークプロセッサが

40

50

らハードディスクへと、ほぼ直接にハードウェアをコピーする。

【0049】

図8は、所定の実施形態に従い、アクセスポイント（AP）において経路を格納する高速ネットワークデータのデザインの態様を示す高水準ネットワーク図である。図8は、APWiFiドライバ801、APネットワークドライバ802、APディスクドライバ803、APOSファイルシステム805、読取り書込みアプリケーション806及びAPOSカーネル808を示す。データ保存のための高速経路を、赤色（破線矢印）で示し、それにより、ネットワークドライバ802は、OSファイルシステム805をバイパスし、読取り書込みアプリケーション806を用いて、データをAPハードディスクへ書き込む。

10

【0050】

所定の実施形態に従い、ワイヤレスネットワークを管理する方法は、以下を含む：現地で複数のワイヤレスアクセスポイントハードウェアユニットを配備すること；ここで、少なくともワイヤレスアクセスポイントハードウェアユニットのサブセットのそれぞれは、ワイヤレスアクセスポイントメモリ構成要素を含み；現地で、複数の仮想ワイヤレスアクセスポイントを、複数のワイヤレスアクセスポイントハードウェアユニットの対応するワイヤレスアクセスポイントハードウェアユニットに関連させること；仮想ワイヤレスアクセスポイントの複数のグループを形成すること；第1の複数の企業体のそれぞれに、仮想ワイヤレスアクセスポイントの1つ以上のグループを管理及び制御できるようにすること；及び、仮想ワイヤレスアクセスポイントの第1の複数のグループの少なくとも1つのサブセットの各グループを、1つ以上のワイヤレスアクセスポイントメモリ構成要素に関連した対応するメモリアロケーションに関連させること。所定の実施形態に従い、この方法は、第1の複数の企業体のそれぞれの企業体に対して、第2の複数の企業体の他の企業体に、その対応するメモリアロケーションをサブリースないし転貸できるようにすることをさらに備え、また、第1又は第2の複数の企業体のそれぞれの企業体に対して、以下の1つ以上のために、その対応するメモリアロケーションを用いることができるようにすることを、さらに備える。広告及びプロモーション活動、アプリケーション保管、ビデオ保管、及びコンテンツ保管、並びにさらに、ロケーションベースの広告及び/又は時系列式の広告を用いることを含む。また、この方法は、第1又は第2の複数の企業体のそれぞれの企業体に対して、クライアントトラフィック分析、インターネットアクセス制御、アプリケーション配信及びコンテンツ配信、の1つ以上のために、その対応するメモリアロケーションを用いることができるようにすることを、さらに備える。

20

30

【0051】

所定の実施形態によると、ワイヤレスネットワークは、以下を備える：現地で配備される複数のワイヤレスアクセスポイントハードウェアユニット、ここで、少なくともワイヤレスアクセスポイントハードウェアユニットのサブセットのそれぞれは、ワイヤレスアクセスポイントを含み；メモリ要素、ここで、複数の仮想ワイヤレスアクセスポイントは、現地の複数のワイヤレスアクセスポイントハードウェアユニットの対応するワイヤレスアクセスポイントハードウェアユニットに関連し；仮想ワイヤレスアクセスポイントの複数のグループが、形成され；複数の企業体のそれぞれが、仮想ワイヤレスアクセスポイントの1つ以上のグループを管理及び制御できるようにし；及び、仮想ワイヤレスアクセスポイントの複数のグループの少なくとも1つのサブセットの各グループは、1つ以上のワイヤレスアクセスポイントメモリ構成要素に関連した対応するメモリアロケーションに関連する。所定の実施形態に従い、複数の企業体のそれぞれの企業体は、以下に記載する1つ以上のために、対応するメモリアロケーションを用いることが可能である：広告及びプロモーション活動、アプリケーションの保管、ビデオの保管及びコンテンツの保管、及び、ロケーションベースの広告及び/又は時系列式の広告。さらに、複数の企業体のそれぞれの企業体は、以下の1つ以上のために、その対応するメモリアロケーションを他の企業体に転貸することができるようになる：広告及びプロモーション活動、アプリケーションの保管、ビデオの保管及びコンテンツの保管。また、複数の企業体のそれぞれの企業体は、

40

50

以下の1つ以上のために、対応するメモリアロケーションを用いることができるようになる：クライアントトラフィック分析、インターネットアクセス制御、アプリケーション配信及びコンテンツ配信。

【0052】

所定の実施形態に従い、ワイヤレスアクセス方法は、ワイヤレスアクセスポイントにより送信される発見リクエストを受信すること、ワイヤレスアクセスポイントに関連するメディアアクセス制御アドレス情報を、発見リクエストから取得すること、ワイヤレスアクセスポイントがテナントコントローラにあらかじめ割り当てられていたならば、ワイヤレスアクセスポイントに関連するテナントアカウント情報を、発見リクエストから取得すること、及び、テナントアカウント情報に関連するテナントコントローラのIPアドレス及びポート情報を、ワイヤレスアクセスポイントに送信すること、を備える。この方法はさらに、ワイヤレスアクセスポイントがテナントアカウントIDをすでに有しないならば、テナントアカウントIDをワイヤレスアクセスポイントに割り当てること、及び、ワイヤレスアクセスポイントを、新しく割り当てられたテナントアカウントID、ワイヤレスアクセスポイントのデバイスID、ワイヤレスアクセスポイントのプライベートIPアドレス、及びワイヤレスアクセスポイントのパブリックIPアドレスに基づき、適切なテナントコントローラに割り当てること、を備える。この方法はさらに、テナントコントローラに関連した複数のサーバクラスタから、テナントコントローラに関する情報を受信することを備える。さらに、この方法は、地域のロケーションに関連するワイヤレスアクセスポイントを、同じデータセンターの対応するテナントコントローラに割り当てることにより、ワイヤレスアクセスポイント接続を統合することをさらに備える。また、この方法はさらに、テナントアカウント情報が、固有サイトコントローラマネージャに対応するテナントコントローラに関連するならば、ワイヤレスアクセスポイントを、固有サイトコントローラマネージャに向けることを、備える。

10

20

【0053】

所定の実施形態に従い、ワイヤレスアクセス方法は、ワイヤレスアクセスポイントにより、発見リクエストを、サイトコントローラマネージャに送信すること、ここでテナントアカウントがワイヤレスアクセスポイントにあらかじめ割り当てられるならば、発見リクエストは、ワイヤレスアクセスポイントに関連するメディアアクセス制御アドレス情報及びテナントアカウント情報を含む、テナントアカウント情報に関連するテナントコントローラのIPアドレス及びポート情報を、ワイヤレスアクセスポイントにより受信すること、及び、ワイヤレスアクセスポイントにより、テナントコントローラとのデータトランスポートレイヤセキュリティセッションを確立すること、を備える。この方法はさらに、ワイヤレスアクセスポイントがテナントアカウントIDをすでに有しないならば、ワイヤレスアクセスポイントによりテナントアカウントIDを受信することを、備える。この方法はさらに、ワイヤレスアクセスポイントにより、複数のサイトコントローラマネージャのそれぞれに関連するDNS情報を、発見すること、及び、発見されたDNS情報を用いて、複数のサイトコントローラマネージャのいずれか1つと交信すること、を備える。

30

【0054】

所定の実施形態によると、ワイヤレスネットワークは、複数のサイトコントローラマネージャを備え、少なくとも複数のサイトコントローラマネージャのサブセットの各々のサイトコントローラマネージャは、少なくとも1つの対応するデータセンターと関連し、ここで、複数のサイトコントローラマネージャの少なくとも1人のサイトコントローラマネージャは、ワイヤレスアクセスポイントにより送信される発見リクエストを受信し、ワイヤレスアクセスポイントに関連するメディアアクセス制御アドレス情報を、発見リクエストから取得し、ワイヤレスアクセスポイントがテナントコントローラにあらかじめ割り当てられていたならば、ワイヤレスアクセスポイントに関連するテナントアカウント情報を、発見リクエストから取得し、及び、テナントアカウント情報に関連するテナントコントローラのIPアドレス及びポート情報を、ワイヤレスアクセスポイントに送信する。所定の実施形態に従い、ワイヤレスアクセスポイントがテナントアカウントIDをすでに有し

40

50

ないならば、複数のサイトコントローラマネージャの少なくとも1人のサイトコントローラマネージャが、テナントアカウントIDをワイヤレスアクセスポイントに割り当て、ワイヤレスアクセスポイントを、新しく割り当てられたテナントアカウントID、ワイヤレスアクセスポイントのデバイスID、ワイヤレスアクセスポイントのプライベートIPアドレス、及びワイヤレスアクセスポイントのパブリックIPアドレスに基づき、適切なテナントコントローラに割り当てる。さらに、複数のサイトコントローラマネージャの少なくとも1つのサイトコントローラマネージャは、テナントコントローラに関連する複数のサーバクラスタから、テナントコントローラに関する情報を受信する。また、複数のサイトコントローラマネージャの少なくとも1つのサイトコントローラマネージャは、地域のロケーションに関連するワイヤレスアクセスポイントを同じデータセンターの対応するテナントコントローラに割り当てることにより、ワイヤレスアクセスポイント接続を統合する。所定の実施形態に従い、テナントアカウント情報が、固有サイトコントローラマネージャに対応するテナントコントローラに関連するならば、複数のサイトコントローラマネージャの少なくとも1つのサイトコントローラマネージャは、ワイヤレスアクセスポイントを固有サイトコントローラマネージャに向ける。

10

【0055】

所定の実施形態に従い、ワイヤレスネットワークは、複数のワイヤレスアクセスポイントを備え、複数のワイヤレスアクセスポイントの少なくとも1つのワイヤレスアクセスポイントは、発見リクエストをサイトコントローラマネージャに送信し、ここでこの発見リクエストは、テナントアカウントが少なくとも1つのワイヤレスアクセスポイントにあら

かじめ割り当てられるならば、少なくとも1つのワイヤレスアクセスポイントに関連するメディアアクセス制御アドレス情報及びテナントアカウント情報を含み、テナントアカウント情報に関連するテナントコントローラのIPアドレス及びポート情報を受信し、テナントコントローラとのデータトランスポートレイヤセキュリティセッションを確立する。さらに、少なくとも1つのワイヤレスアクセスポイントがテナントアカウントIDをすでに有しないならば、少なくとも1つのワイヤレスアクセスポイントはテナントアカウントIDを受信する。また、少なくとも1つのワイヤレスアクセスポイントは、複数のサイトコントローラマネージャのそれぞれに関連するDNS情報を発見し、発見されたDNS情報を用いて、複数のサイトコントローラマネージャのいずれか1つと交信する。

20

【0056】

所定の実施形態に従い、ワイヤレスアクセス方法は、第1のワイヤレスアクセスポイントが、第1の仮想専用ネットワークゲートウェイとして動作できるように、第1の仮想専用ネットワークサイトで、第1のワイヤレスアクセスポイントを設計すること、第1のワイヤレスアクセスポイントを、第1のWLANクラウドコントローラ及び対応する第1の仮想専用ネットワークサービスエンジンに関連させること、第2のワイヤレスアクセスポイントが第2の仮想専用ネットワークゲートウェイとして動作できるように、第2の仮想専用ネットワークサイトで、第2のワイヤレスアクセスポイントを設計すること、第2のワイヤレスアクセスポイントを、第2のWLANクラウドコントローラ及び対応する第2の仮想専用ネットワークサービスエンジンに関連させること、及び、第1の仮想専用ネットワークサービスエンジンと第2の仮想専用ネットワークサービスエンジンとの間に、セ

キュアトンネルを動的に提供することにより、第1の仮想専用ネットワークサイトの第1のワイヤレスクライアントデバイスが、第2の仮想専用ネットワークサイトの第2のワイヤレスクライアントデバイスと、通信できるようにすること、を備える。この方法は、第1及び第2のワイヤレスアクセスポイントによる実行のために、第1及び第2のワイヤレスアクセスポイントに、一組の仮想専用ネットワークトラフィックポリシーを提供することを、さらに備える。さらに、この方法は、第1及び第2のワイヤレスアクセスポイントで、仮想専用ネットワークゲートウェイソフトウェア(ソフトVPNゲートウェイ)を実行すること、及び、対応するWLANクラウドコントローラにより管理される対応するルーティングテーブルを変更することにより、仮想専用ネットワークサイト間のトラフィック経路ルーティングを変更すること、を備える。さらに、第1及び第2のワイヤレスアク

30

40

50

セスポイントは、仮想ワイヤレスアクセスポイントである。

【0057】

所定の実施形態に従い、仮想専用ネットワークは、以下を含む：第1の仮想専用ネットワークサイトの第1のワイヤレスアクセスポイント、ここで、第1のワイヤレスアクセスポイントは、第1のワイヤレスアクセスポイントが、第1の仮想専用ネットワークゲートウェイとして動作できるように設計され、かつ、第1のWLANクラウドコントローラ及び対応する第1の仮想専用ネットワークサービスエンジンに関連し；第2の仮想専用ネットワークサイトの第2のワイヤレスアクセスポイント、ここで、第2のワイヤレスアクセスポイントは、第2のワイヤレスアクセスポイントが、第2の仮想専用ネットワークゲートウェイとして動作できるように設計され、かつ、第2のワイヤレスアクセスポイントは、第2のWLANクラウドコントローラ及び対応する第2の仮想専用ネットワークサービスエンジンに関連し；ここで、セキュアトンネルは、第1の仮想専用ネットワークサービスエンジンと第2の仮想専用ネットワークサービスエンジンとの間で動的に提供され、第1の仮想専用ネットワークサイトの第1のワイヤレスクライアントデバイスが、第2の仮想専用ネットワークサイトの第2のワイヤレスクライアントデバイスと通信できるようになる。この仮想専用ネットワークは、第1及び第2のワイヤレスアクセスポイントによる実行のために、第1及び第2のワイヤレスアクセスポイントに提供される一組の仮想専用ネットワークトラフィックポリシーを、さらに備える。さらに、仮想専用ネットワークは、第1及び第2のワイヤレスアクセスポイントで実行される仮想専用ネットワークゲートウェイソフトウェア（ソフトVPNゲートウェイ）を備える。また、第1及び第2のワイヤレスアクセスポイントは、仮想ワイヤレスアクセスポイントである。さらに、対応するWLANクラウドコントローラにより管理される対応するルーティングテーブルを変更することにより、仮想専用ネットワークサイトの間のトラフィック経路ルーティングを変更することができる。

【0058】

所定の実施形態に従い、ワイヤレスアクセスポイント（CAPWAP）の制御及び供給のためのワイヤレスアクセス方法は、以下を含む：クラウドベースのCAPWAP発見プロトコルの一部として、HTTPSプロトコル（ハイパーテキストトランスファーセキュリティプロトコル）を用いて、ワイヤレスアクセスポイントが、HTTP接続に対応するクラウドベースの仮想コントローラの位置情報を発見することができるようにすること、ここで、対応するクラウドベースの仮想コントローラは、ワイヤレスアクセスポイントを管理する；ワイヤレスアクセスポイントと、輸送手段プロトコルをネゴシエートすること；及び、ワイヤレスアクセスポイントと対応するクラウドベースの仮想コントローラとの間のユーザーデータグラムプロトコル（UDP）通信が、ファイアウォールによりブロックされるならば、ワイヤレスアクセスポイントと対応するクラウドベースの仮想コントローラとの間のHTTPSトンネルを、UDP通信に用いること。さらに、この方法は、HTTPSプロトコル中にUDPパケット境界情報を含めることをさらに備える。この方法は、UDPメッセージの受信者によるUDPメッセージの連続的な読取りを保持することをさらに備える。所定の実施形態に従い、マルチテナントクラウドベースコントローラに関連するワイヤレスアクセスポイント（CAPWAP）を制御及び供給するためのワイヤレス方法は、アクセスポイントと対応するクラウドベースのコントローラとの間の通信のためのデフォルトプロトコルとして、データグラムトランスポートレイヤセキュリティ（DTLS）プロトコル上のCAPWAPを用いること、及び、アクセスポイントと対応するクラウドベースのコントローラとの間でファイアウォールが検出された場合に、アクセスポイントと対応するクラウドベースのコントローラとの間の通信のために、ハイパーテキストトランスファープロトコル（HTTP）上又はハイパーテキストトランスファープロトコルセキュア（HTTPS）上のCAPWAPを用いること、を備える。

【0059】

所定の実施形態に従い、ワイヤレスアクセス方法は、ワイヤレスアクセスポイントのオペレーティングシステムのファイルシステムをバイパスするため、及び、ワイヤレスアク

10

20

30

40

50

セスポイントのダイレクトメモリアクセス（DMA）からワイヤレスアクセスポイントのハードディスクにネットワークパケット化情報を直接書き込むために、ワイヤレスアクセスポイントのカーネルスペースドライバが、ワイヤレスアクセスポイントのハードディスクドライバと直接通信できるようにするために、ワイヤレスアクセスポイントのオペレーティングシステムを設計することを備える。この方法はさらに、ワイヤレスアクセスポイントのハードディスクからネットワークパケット化情報を直接読み出すために、カーネルスペースドライバが、ワイヤレスアクセスポイントのハードディスクドライバと直接通信できるようにすることを備える。所定の実施形態に従い、ワイヤレスアクセスポイントは、ワイヤレスアクセスポイントのオペレーティングシステム、ワイヤレスアクセスポイントのカーネルスペースドライバ、及び、ワイヤレスアクセスポイントのハードディスクドライバ、を備え、ワイヤレスアクセスポイントのオペレーティングシステムのファイルシステムをバイパスするように、及び、所定の実施形態に従って、ワイヤレスアクセスポイントのダイレクトメモリアクセス（DMA）からワイヤレスアクセスポイントのハードディスクにネットワークパケット化情報を直接書き込むために、ワイヤレスアクセスポイントのカーネルスペースドライバが、ワイヤレスアクセスポイントのハードディスクドライバと直接通信できるようにするよう、ワイヤレスアクセスポイントのオペレーティングシステムは設計される。

10

【0060】

所定の実施形態に従い、ワイヤレスの方法は、クラウドベースのコントローラにより管理されるアクセスポイントの複数のグループを、各グループのアクセスポイントとの設定類似点に基づき、形成すること、アクセスポイントの複数のグループの各グループを、それぞれのワイヤレスモビリティドメインに指定すること、及び、各ワイヤレスモビリティドメインに固有のWLANの設定及びポリシーを用いて、各ワイヤレスモビリティドメインのアクセスポイントを管理すること、を備える。この方法では、一組の地理ロケーション基準に基づき、アクセスポイントの複数のグループが形成される。さらに、一連の論理的基準に基づき、アクセスポイントの複数のグループが形成される。さらに、所定の実施形態に従い、この方法は、ワイヤレスモビリティドメインをアセットトラッキングに用いることをさらに備える。

20

【0061】

所定の実施形態に従い、ワイヤレスネットワークは、各グループのアクセスポイントとの設定類似点に基づくアクセスポイントの複数のグループを備え、アクセスポイントの複数のグループの各グループは、それぞれのワイヤレスモビリティドメインとして指定され、アクセスポイントは、クラウドベースのコントローラにより、それぞれのワイヤレスモビリティドメインに固有のWLANの設定及びポリシーを用いて、管理されている。さらに、アクセスポイントの複数のグループは、一連の地理ロケーション基準に基づく。さらに、アクセスポイントの複数のグループは、一連の論理的基準に基づく。また、所定の実施形態によれば、ワイヤレスモビリティドメインは、アセットをトラッキングすることが可能である。さらに、所定の実施形態に従い、カーネルスペースドライバは、ワイヤレスアクセスポイントのハードディスクからネットワークパケット化情報を直接読み出すために、ワイヤレスアクセスポイントのハードディスクドライバと直接通信できるようになる。

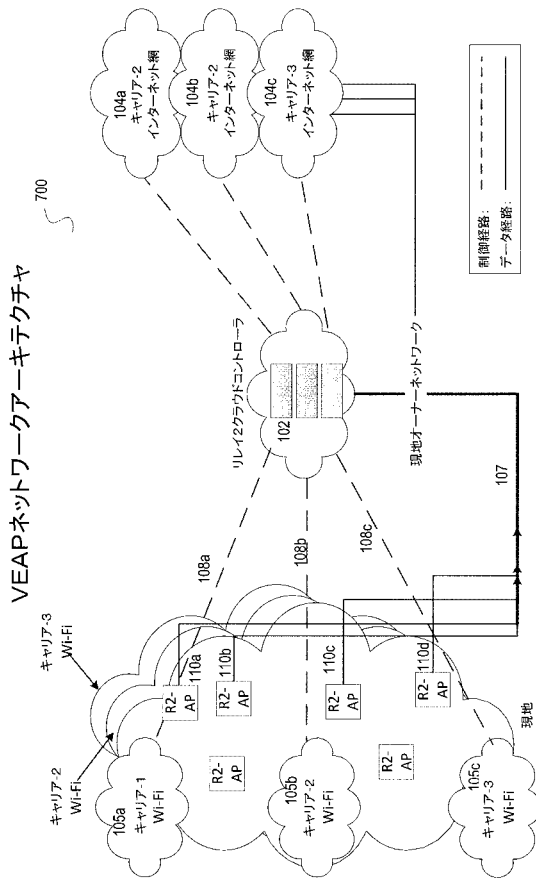
30

40

【0062】

前記の記載は、説明の目的のために、特定の実施形態を参照して記載してきた。しかしながら、上記の例示的な議論は、網羅的であること又は開示される厳密な形態に本発明を限定することを、意図するものではない。多くの変形及び変更は、上記の教示を考慮して可能である。本発明及びその実際の応用の原理を最も適切に説明するために、実施形態を選択して説明し、それによって、当業者は、想定される特定の使用に適するよう様々な変形することにより、本発明及び様々な実施形態を最も適切に利用することができる。

【図 1】



【図 3】

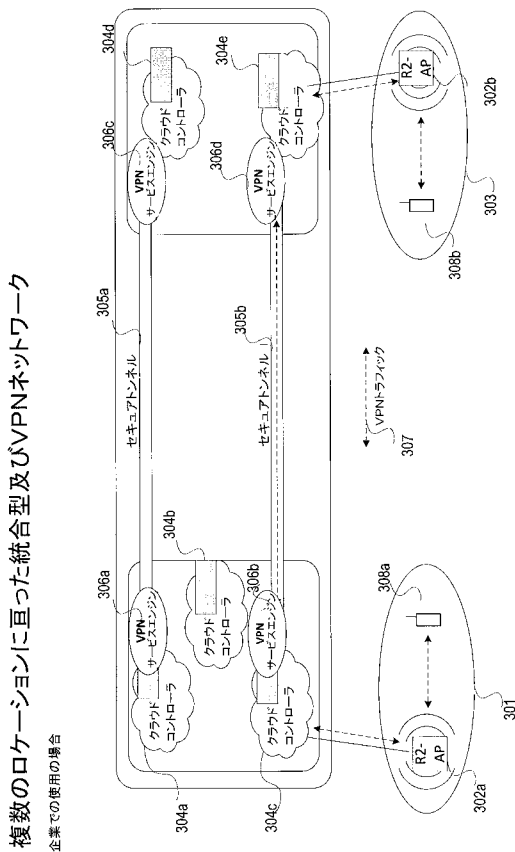


FIG. 3

ワイヤレスモビリティドメイン管理

社内ネットワークの使用の場合

【図 4】

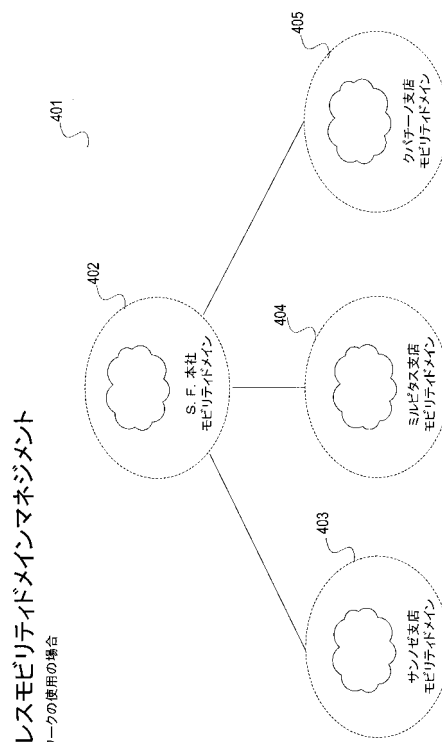


FIG. 4

FIG. 1

【図 2】

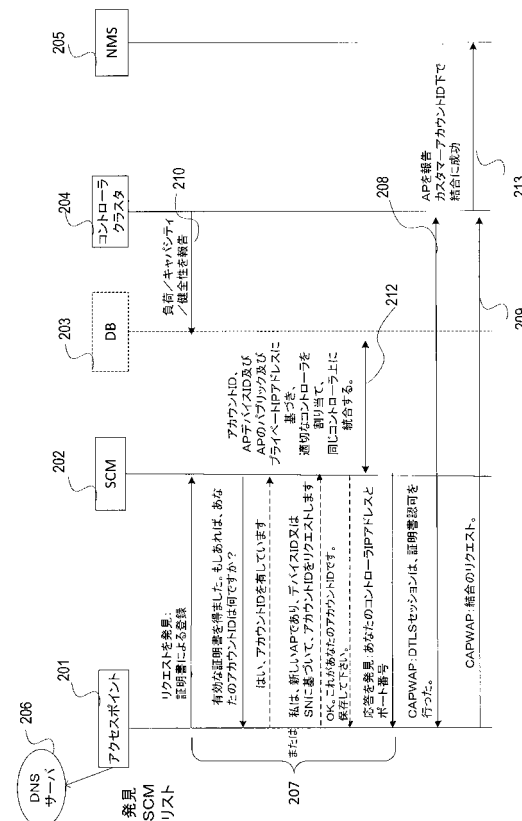


FIG. 2

【図 5】

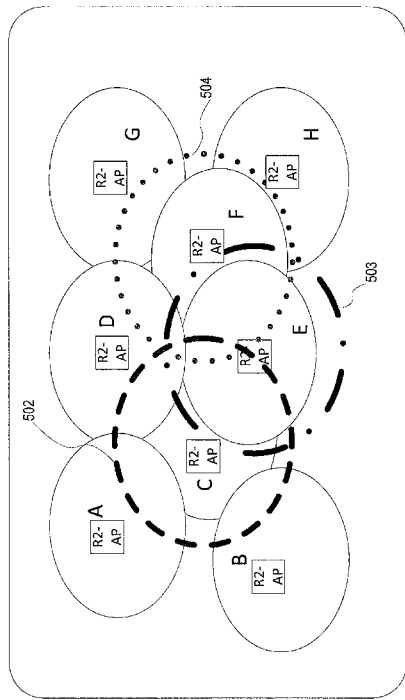


FIG. 5

【図 6】

サブネットアドレス	アンカー-APアドレス
192.168.2.0/24	192.168.2.254
192.168.2.0/24	192.168.3.215
...	...

FIG. 6

【図 7】

クラウドベースのL3モビリティ制御

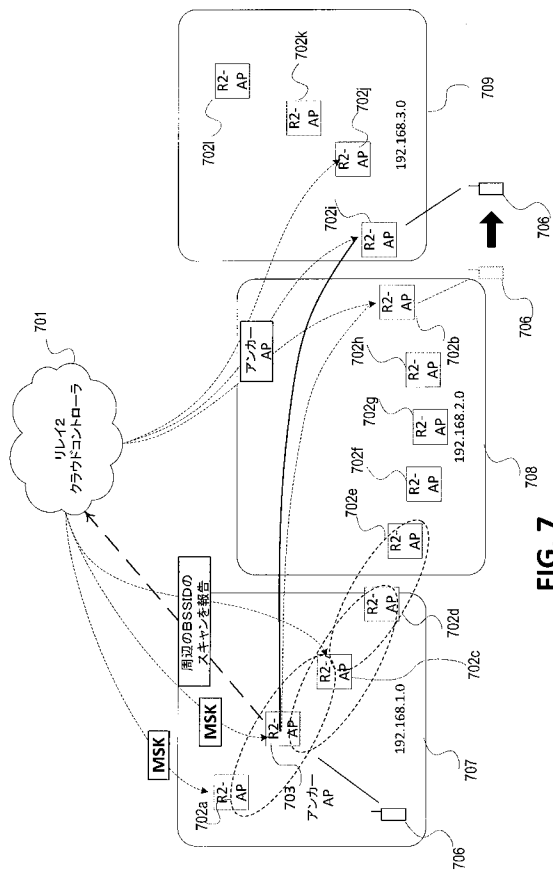


FIG. 7

【図 8】

高速ネットワークデータ保管経路

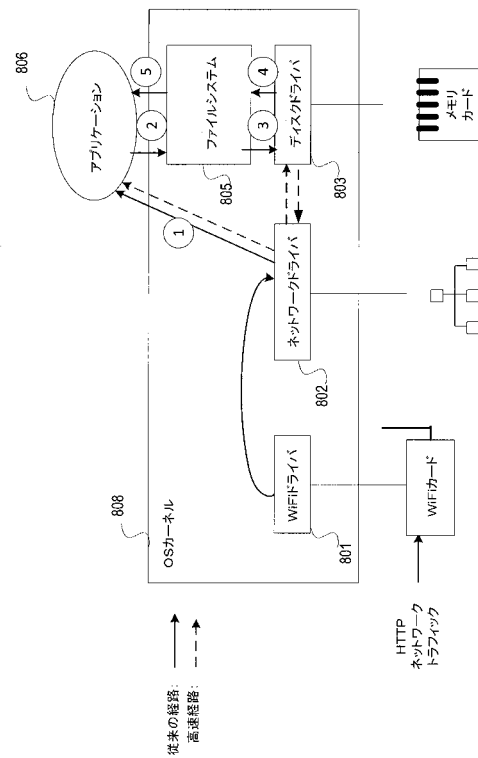
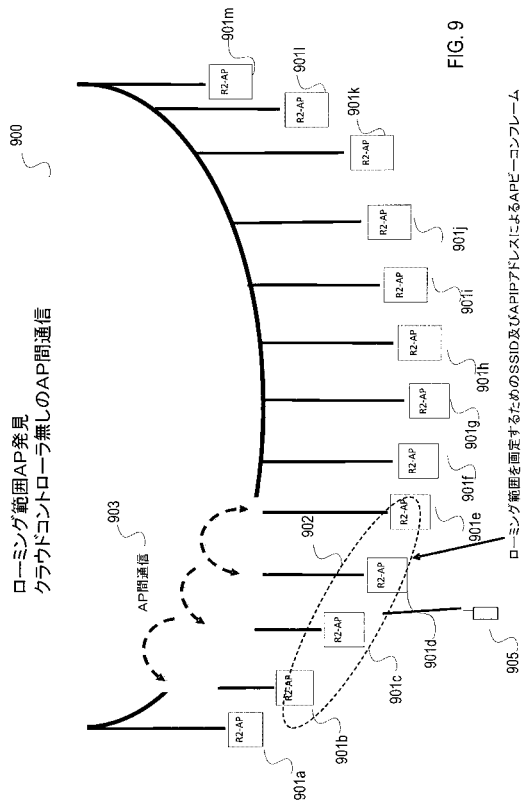


FIG. 8

【図 9】



【 国際調査報告 】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/037613

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04L 12/00 (2014.01)

CPC - H04L 12/00 (2014.09)

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(8) - G06F 15/173; H04B 7/00; H04L 12/00 (2014.01)

USPC - 370/310.2, 401, 412; 709/223

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - G06F 15/173; H04B 7/00; H04L 12/00 (2014.09) (keyword delimited)

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

Google, Orbit, Google Patents

Search terms used: Assigning, plurality of virtual access points, physical access point, subscribe, lease, WLAN

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006/0165103 A1 (TRUDEAU et al) 27 July 2006 (27.07.2006) entire document	1-6
Y	US 2006/0094400 A1 (BEACHEM et al) 04 May 2006 (04.05.2006) entire document	1-6
Y	US 2005/0180348 A1 (BURDICK et al) 18 August 2005 (18.08.2005) entire document	3,4
Y	US 2009 0198808 A1 (CAI et al) 06 August 2009 (06.08.2009) entire document	5
A	US 2010/0027516 A1 (NAGARAJAN) 04 February 2010 (04.02.2010) entire document	1-6

☐ Further documents are listed in the continuation of Box C.

* 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

13 November 2014

Date of mailing of the international search report

11 DEC 2014

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents

P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2014/037613

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
see extra sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-6

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2014/037613

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-6, drawn to a method comprising: deploying a plurality of wireless access point hardware units at a physical location.

Group II, claims 7-12, drawn to a wireless network.

Group III, claims 13, drawn to a method of supporting L3 mobility.

The inventions listed as Groups I, II and III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: associating a plurality of virtual wireless access points with a corresponding wireless access point hardware unit of the plurality of wireless access point hardware units at the physical location; leasing a first subset of virtual wireless access points of the plurality of virtual wireless access points to a first WLAN network operator as claimed therein is not present in the invention of Groups II and III. The special technical feature of the Group II invention: wherein, the plurality of wireless access point hardware units are owned by an operator of the venue; a first subset of virtual wireless access points of the plurality of virtual wireless access points is owned by a first WLAN provider; and a second subset of virtual wireless access points of the plurality of virtual wireless access points is owned by a second WLAN provider as claimed therein is not present in the invention of Groups I or III. The special technical feature of the Group III invention: a cloud based controller comprising: storing a master session key (MSK) information associated with a roaming wireless client device, wherein the master session key (MSK) information is generated during an authentication associated with the roaming wireless client device at an anchor access point for the roaming wireless client device; predicting a first roaming range of access points to which the roaming wireless client device will roam from the anchor access point as claimed therein is not present in the invention of Groups I or II.

Groups I, II and III lack unity of invention because even though the inventions of these groups require the technical feature of deploying a plurality of wireless access point hardware units; a first subset of virtual wireless access points of the plurality of virtual wireless access points, this technical feature is not a special technical feature as it does not make a contribution over the prior art.

Specifically, US 2010/0027516 A1 (NAGARAJAN) 04 February 2010 (04.02.2010) teaches deploying a plurality of wireless access point hardware units (wireless switch device 12 supports the subnet (A) 10 and is coupled to access ports (APs) 14, 16, wireless switch device 22 supports subnet (B) 20 and is coupled to access ports (APs) 24, 26, wireless switch device 42 supports subnet (C) 40 and is coupled to access ports (APs) 44, 46, and wireless switch device 32 supports subnet (D) 30 and is coupled to access ports (APs) 34, 36, Para. 18); a first subset of virtual wireless access points of the plurality of virtual wireless access points (a wireless switch device includes hardware, middleware and software resources in a single unit or housing, wherein the hardware resources are virtually divided among a group of virtual wireless switch modules 413, 415, 417, Para. 42).

Since none of the special technical features of the Group I, II or III inventions are found in more than one of the inventions, unity of invention is lacking.

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, 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, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US

(72)発明者 ルー , ウェイ

中華人民共和国・ 1 0 0 0 0 0 ・ ペイジン・ ハイディアン ディストリクト・ エイジメン ペイダ
ジエ・ ナンバー 2 8 ・ ビルディング・ 5 ・ ルーム・ 1 3 0 2

(72)発明者 シリブラブ , ラメシュ

アメリカ合衆国・ 9 4 5 3 9 ・ カリフォルニア州・ フレモント・ ヴェルタ オリヴォス・ 1 1 2 9
F ターム(参考) 5K030 GA04 HA08 HC13 HD03 JA11