

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号
特表2024-503322
(P2024-503322A)

(43)公表日 令和6年1月25日(2024.1.25)

(51)国際特許分類	F I	テーマコード (参考)
H O 4 L 41/0895(2022.01)	H O 4 L 41/0895	5 K 0 3 0
H O 4 L 47/10 (2022.01)	H O 4 L 47/10	
H O 4 L 47/32 (2022.01)	H O 4 L 47/32	

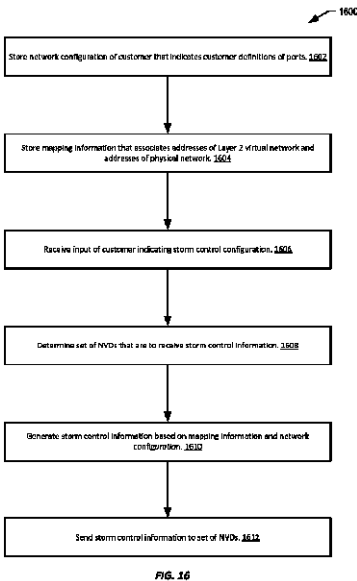
審査請求 未請求 予備審査請求 未請求 (全99頁)

(21)出願番号	特願2023-540141(P2023-540141)	(71)出願人	502303739
(86)(22)出願日	令和3年11月24日(2021.11.24)		オラクル・インターナショナル・コーポレーション
(85)翻訳文提出日	令和5年8月25日(2023.8.25)		アメリカ合衆国カリフォルニア州94065レッドウッド・シティ、オラクル・パークウェイ500
(86)国際出願番号	PCT/US2021/060820		
(87)国際公開番号	WO2022/146588	(74)代理人	110001195
(87)国際公開日	令和4年7月7日(2022.7.7)		弁理士法人深見特許事務所
(31)優先権主張番号	63/132,377	(72)発明者	ブラール, ジャグウィンダー・シング
(32)優先日	令和2年12月30日(2020.12.30)		アメリカ合衆国、94065 カリフォルニア州、レッドウッド・シティ、オラクル・パークウェイ、500、オラクル・インターナショナル・コーポレーション内
(33)優先権主張国・地域又は機関	米国(US)	(72)発明者	クレーガースティクルズ, ルーカス・
(31)優先権主張番号	17/494,729		最終頁に続く
(32)優先日	令和3年10月5日(2021.10.5)		
(33)優先権主張国・地域又は機関	米国(US)		
(81)指定国・地域	AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA		
	最終頁に続く		

(54)【発明の名称】 仮想化されたクラウド環境におけるレイヤ2 ネットワーキングストーム制御

(57)【要約】

L 2 仮想ネットワークにおける通信のための技術が説明される。ある例では、L 2 仮想ネットワークは、ホストマシンのセット上でホストされる複数のL 2 計算インスタンスと、ネットワーク仮想化デバイスのセット上でホストされる複数のL 2 仮想ネットワークインターフェースおよびL 2 仮想スイッチとを含む。L 2 仮想ネットワークインターフェースは、L 2 仮想ネットワークのL 2 ポートをエミュレートする。L 2 ポートに適用可能なストーム制御情報が、L 2 仮想ネットワークインターフェースをホストするネットワーク仮想化デバイスに送信される。



【特許請求の範囲】

【請求項 1】

方法であって、

顧客のレイヤ 2 仮想ネットワークのアドレスと、前記レイヤ 2 仮想ネットワークをホストする物理ネットワークのアドレスとを関連付けるマッピング情報を記憶することを含み、

前記レイヤ 2 仮想ネットワークは、複数の計算インスタンスと、複数のレイヤ 2 仮想ネットワークインターフェースと、複数のレイヤ 2 仮想スイッチとを備え、

前記物理ネットワークは、複数のネットワーク仮想化デバイス（NVD）と複数のホストマシンとを備え、

前記複数の計算インスタンスのうちのある計算インスタンスは、前記複数のホストマシンのうちのあるホストマシン上でホストされ、

前記ある計算インスタンスは、前記複数のレイヤ 2 仮想ネットワークインターフェースのうちのあるレイヤ 2 仮想ネットワークインターフェースと、前記複数のレイヤ 2 仮想スイッチのうちのあるレイヤ 2 仮想スイッチとに関連付けられ、

前記あるレイヤ 2 仮想ネットワークインターフェースおよび前記あるレイヤ 2 仮想スイッチは、前記複数の NVD のうちのある NVD 上でホストされ、

前記ある NVD と前記あるホストマシンとは通信可能に結合され、前記方法はさらに、

顧客の入力を受信することを含み、前記入力、前記レイヤ 2 仮想ネットワークにおけるトラフィックフローのためにストーム制御構成を指定し、前記方法はさらに、

前記ストーム制御構成および前記マッピング情報に基づいて、前記ある NVD のためにストーム制御情報を生成することと、

前記ストーム制御情報を前記ある NVD に送信することを含む、方法。

【請求項 2】

前記入力は、前記ストーム制御構成がポートに適用されることを示し、トラフィックフロー条件で実行されるべきアクションを指定し、前記方法はさらに、

前記ポートは前記あるレイヤ 2 仮想ネットワークインターフェースの媒体アクセス制御（MAC）アドレスに対応すると判断することと、

前記マッピング情報に基づいて、前記 MAC アドレスは前記ある NVD のインターネットプロトコル（IP）アドレスに関連付けられている、と判断することと、

前記ストーム制御情報において、前記 MAC アドレスおよび前記 IP アドレスに基づいて前記トラフィックフロー条件および前記アクションを示すことを含む、請求項 1 に記載の方法。

【請求項 3】

前記トラフィックフロー条件は、フレーム伝送レートを含み、前記アクションは、フレームをドロップすること、または前記ポートをリンクダウンすることを含む、請求項 2 に記載の方法。

【請求項 4】

前記トラフィックフロー条件は、最大フレーム伝送レートおよび持続時間を含み、前記アクションは、フレーム伝送レートが前記最大フレーム伝送レートを超過するとフレームをドロップすることと、前記持続時間を超える時間長にわたって前記超過が検出されると前記ポートをリンクダウンすることを含む、請求項 2 に記載の方法。

【請求項 5】

前記入力は、前記ストーム制御構成のストーム制御ポリシーが、ユニキャストされるフレーム、ブロードキャストされるフレーム、またはマルチキャストされるフレームのうちの少なくとも 1 つに適用されることを示し、前記ストーム制御情報は、前記ストーム制御ポリシーと、前記あるレイヤ 2 仮想ネットワークインターフェースに関連付けられるフレームの流れを制御するための、前記ある NVD へのフレームブロードキャストまたはフレームマルチキャストのうちの前記少なくとも 1 つに対する前記ストーム制御ポリシーの適用可能性とを示す、請求項 1～4 のいずれか 1 項に記載の方法。

【請求項 6】

前記入力は、前記ストーム制御構成のストーム制御ポリシーと、前記ストーム制御ポリシーの違反で実行される前記ストーム制御ポリシーのアクションと、前記ストーム制御ポリシーの反復違反で適用される前記ストーム制御構成のエスカレーションポリシーとを示し、前記ストーム制御情報は、前記ストーム制御ポリシーと、前記アクションと、前記エスカレーションポリシーとを、前記あるレイヤ 2 仮想ネットワークインターフェースに関連付けられるフレームの流れを制御するために、前記ある N V D に示す、請求項 1 ～ 5 のいずれか 1 項に記載の方法。

【請求項 7】

前記入力は、前記ストーム制御構成の伝送レートのタイプを示し、前記伝送レートのタイプは、フレーム／秒またはビット／秒のうちの少なくとも 1 つを含み、前記ストーム制御情報は、前記伝送レートのタイプを、前記あるレイヤ 2 仮想ネットワークインターフェースに関連付けられるフレームの流れを制御するために、前記ある N V D に示す、請求項 1 ～ 6 のいずれか 1 項に記載の方法。

【請求項 8】

前記入力は、前記ストーム制御構成の統計のタイプを示し、前記ストーム制御情報は、前記統計のタイプを、前記あるレイヤ 2 仮想ネットワークインターフェースに関連付けられるフレームの流れに関する統計を収集するために、前記ある N V D に示す、請求項 1 ～ 7 のいずれか 1 項に記載の方法。

【請求項 9】

前記入力は、前記ストーム制御構成が複数のポートに適用されることを示し、前記方法はさらに、

前記複数のポートは前記複数のレイヤ 2 仮想ネットワークインターフェースのうちのあるレイヤ 2 仮想ネットワークインターフェースのセットに対応する、と判断することと、

前記マッピング情報に基づいて、前記あるレイヤ 2 仮想ネットワークインターフェースのセットが前記複数の N V D のうちのある N V D のセットに関連付けられる、と判断することと、

前記ある N V D のセットの各 N V D に前記ストーム制御情報を送信することを含む、請求項 1 ～ 8 のいずれか 1 項に記載の方法。

【請求項 10】

前記ストーム制御構成、前記ストーム制御情報、前記ある N V D、および前記あるレイヤ 2 仮想ネットワークインターフェースは、それぞれ、第 1 のストーム制御構成、第 1 のストーム制御情報、第 1 の N V D、および第 1 のレイヤ 2 仮想ネットワークインターフェースであり、前記方法はさらに、

前記入力は、(i) 第 2 のストーム構成と、(i i) 前記第 1 のストーム制御構成は第 1 のポートに適用されることと、(i i i) 前記第 2 のストーム構成は第 2 のポートに適用されることと示す、と判断することと、

前記第 1 のポートは前記第 1 のレイヤ 2 仮想ネットワークインターフェースに対応し、前記第 2 のポートは前記複数のレイヤ 2 仮想ネットワークインターフェースのうち第 2 のレイヤ 2 仮想ネットワークインターフェースに対応する、と判断することと、

前記マッピング情報に基づいて、前記第 1 のレイヤ 2 仮想ネットワークインターフェースは前記第 1 の N V D によってホストされ、前記第 2 のレイヤ 2 仮想ネットワークインターフェースは前記複数の N V D のうち第 2 の N V D によってホストされる、と判断することと、

前記第 2 のストーム構成に基づいて第 2 のストーム制御情報を生成することと、

前記第 2 の N V D に前記第 2 のストーム制御情報を送信することを含む、請求項 1 ～ 9 のいずれか 1 項に記載の方法。

【請求項 11】

前記ストーム制御構成は、伝送レートに対する第 1 の制限を示し、前記ストーム制御構成は、乗数による前記第 1 の制限の調整に対応する第 2 の制限を示す、請求項 1 ～ 10 の

いずれか 1 項に記載の方法。

【請求項 1 2】

前記方法はさらに、

前記トラフィックフローに関するメトリックを収集することと、

前記メトリックに基づいて前記乗数を更新することと、

前記ストーム制御構成に関する更新を前記ある N V D に送信することとを含み、当該更新は、前記更新された乗数または前記更新された乗数に基づく更新された第 2 の制限のうちの少なくとも 1 つを含む、請求項 1 1 に記載の方法。

【請求項 1 3】

ネットワーク仮想化デバイスであって、

1 つ以上のプロセッサと、

命令を記憶する 1 つ以上のコンピュータ可読記憶媒体とを備え、前記命令は、前記 1 つ以上のプロセッサによって実行されると、前記ネットワーク仮想化デバイスを、

顧客のレイヤ 2 仮想ネットワークに属するレイヤ 2 仮想ネットワークインターフェースおよびレイヤ 2 仮想スイッチをホストするよう構成し、

前記レイヤ 2 仮想ネットワークインターフェースおよび前記レイヤ 2 仮想スイッチは、前記レイヤ 2 仮想ネットワークに属するレイヤ 2 計算インスタンスに関連付けられ、

前記レイヤ 2 計算インスタンスは、前記ネットワーク仮想化デバイスを備える物理ネットワークのホストマシン上でホストされ、前記ホストマシンおよび前記ネットワーク仮想化デバイスは、通信可能に結合され、

前記レイヤ 2 仮想ネットワークは、前記物理ネットワーク上でホストされ、複数のレイヤ 2 計算インスタンスと、複数のレイヤ 2 仮想ネットワークインターフェースと、複数のレイヤ 2 仮想スイッチとを備え、前記命令は、さらに、前記 1 つ以上のプロセッサによって実行されると、前記ネットワーク仮想化デバイスを、

ストーム制御ポリシーと、前記ストーム制御ポリシーの違反で実行されるべきアクションとを示すストーム制御情報を記憶するよう構成し、

前記レイヤ 2 仮想ネットワークインターフェースへのトラフィックフローおよび／または前記レイヤ 2 仮想ネットワークインターフェースからのトラフィックフローを監視するよう構成し、

前記トラフィックフローは前記ストーム制御ポリシーに違反する、と判断するよう構成し、

前記ストーム制御ポリシーに違反する前記トラフィックフローに基づいて前記アクションを開始するよう構成する、ネットワーク仮想化デバイス。

【請求項 1 4】

前記ストーム制御ポリシーは、前記レイヤ 2 仮想ネットワークインターフェースへの着信トラフィックに対する最大伝送レートを示し、前記アクションは、フレームをドロップすることを含み、前記トラフィックフローは前記ストーム制御ポリシーに違反する、と判断することは、前記レイヤ 2 仮想ネットワークインターフェースへの着信フレームの伝送レートが前記最大伝送レートを超える、と判断することを含み、前記アクションを開始することは、着信フレームをドロップすることを含む、請求項 1 3 に記載のネットワーク仮想化デバイス。

【請求項 1 5】

前記ストーム制御ポリシーはさらに、エスカレーションアクションのための持続時間を示し、前記エスカレーションアクションはリンクダウンを含み、前記トラフィックフローは前記ストーム制御ポリシーに違反する、と判断することは、前記伝送レートは前記持続時間よりも長く持続した、と判断することをさらに含み、前記アクションを開始することは、前記レイヤ 2 仮想ネットワークインターフェースをリンクダウンすることをさらに含む、請求項 1 4 に記載のネットワーク仮想化デバイス。

【請求項 1 6】

前記レイヤ 2 仮想ネットワークインターフェースは、第 1 のレイヤ 2 仮想ネットワーク

10

20

30

40

50

インターフェースであり、前記ストーム制御ポリシーは、第2のレイヤ2仮想ネットワークインターフェースへの着信トラフィックに対する最大伝送レートを示し、前記アクションは、フレームをドロップすることを含み、前記トラフィックフローは前記ストーム制御ポリシーに違反する、と判断することは、前記第1のレイヤ2仮想ネットワークインターフェースから前記第2のレイヤ2仮想ネットワークインターフェースへのフレームの伝送レートが前記最大伝送レートを超える、と判断することを含み、前記アクションを開始することは、前記第1のレイヤ2仮想ネットワークインターフェースから前記第2のレイヤ2仮想ネットワークインターフェースへのフレームをドロップすることを含む、請求項14に記載のネットワーク仮想化デバイス。

【請求項17】

前記ストーム制御情報は、前記顧客の入力によって示されるストーム制御構成と、前記レイヤ2仮想ネットワークのアドレスと前記物理ネットワークのアドレスとを関連付けるマッピング情報とに基づいて生成される、請求項14に記載のネットワーク仮想化デバイス。

【請求項18】

前記顧客の前記入力は、前記ストーム制御構成が適用されるポートを示し、前記ストーム制御情報はさらに、前記ポートと前記レイヤ2仮想ネットワークインターフェースとの間の対応関係に基づいて生成され、前記対応関係に基づいて前記レイヤ2仮想ネットワークインターフェースに適用される、請求項17に記載のネットワーク仮想化デバイス。

【請求項19】

システムであって、
1つ以上のプロセッサと、
命令を記憶する1つ以上のコンピュータ可読記憶媒体とを備え、前記命令は、前記1つ以上のプロセッサによって実行されると、前記システムを、
顧客のレイヤ2仮想ネットワークのアドレスと、前記レイヤ2仮想ネットワークをホストする物理ネットワークのアドレスとを関連付けるマッピング情報を記憶するよう構成し、

前記レイヤ2仮想ネットワークは、複数の計算インスタンスと、複数のレイヤ2仮想ネットワークインターフェースと、複数のレイヤ2仮想スイッチとを備え、

前記物理ネットワークは、複数のネットワーク仮想化デバイス（NVD）と複数のホストマシンとを備え、

前記複数の計算インスタンスのうちのある計算インスタンスは、前記複数のホストマシンのうちのあるホストマシン上でホストされ、

前記ある計算インスタンスは、前記複数のレイヤ2仮想ネットワークインターフェースのうちのあるレイヤ2仮想ネットワークインターフェースと、前記複数のレイヤ2仮想スイッチのうちのあるレイヤ2仮想スイッチとに関連付けられ、

前記あるレイヤ2仮想ネットワークインターフェースおよび前記あるレイヤ2仮想スイッチは、前記複数のNVDのうちのあるNVD上でホストされ、

前記あるNVDと前記あるホストマシンとは通信可能に結合され、前記命令は、さらに、前記1つ以上のプロセッサによって実行されると、前記システムを、

顧客の入力を受信するよう構成し、前記入力は、前記レイヤ2仮想ネットワークにおけるトラフィックフローのためにストーム制御構成を指定し、前記命令は、さらに、前記1つ以上のプロセッサによって実行されると、前記システムを、

前記ストーム制御構成および前記マッピング情報に基づいて、前記あるNVDのためにストーム制御情報を生成するよう構成し、

前記ストーム制御情報を前記あるNVDに送信するよう構成する、システム。

【請求項20】

前記あるNVDをさらに備え、前記あるNVDは、

前記ストーム制御情報を記憶するよう構成され、前記ストーム制御情報は、ストーム制御ポリシーと、前記ストーム制御ポリシーの違反で実行されるべきアクションとを示し、

10

20

30

40

50

前記ある N V D はさらに、

前記レイヤ 2 仮想ネットワークインターフェースへのトラフィックフローおよび／または前記レイヤ 2 仮想ネットワークインターフェースからのトラフィックフローを監視するよう構成され、

前記トラフィックフローは前記ストーム制御ポリシーに違反する、と判断するよう構成され、

前記ストーム制御ポリシーに違反する前記トラフィックフローに基づいて前記アクションを開始するよう構成される、請求項 19 に記載のシステム。

【発明の詳細な説明】

【技術分野】

10

【0001】

関連出願の参照

この国際特許出願は、2020年12月30日に提出された「LAYER-2 NETWORKING STORM CONTROL IN A VIRTUALIZED CLOUD ENVIRONMENT」と題される米国仮出願 63 / 132, 377 の利益を主張する、2021年10月5日に提出された「LAYER-2 NETWORKING USING ACCESS CONTROL LISTS IN A VIRTUALIZED CLOUD ENVIRONMENT」と題される米国特許出願 17 / 494, 729 に対する優先権を主張し、その内容は、あらゆる目的のためにその全体が参照により本明細書に組み込まれる。

【背景技術】

20

【0002】

背景

クラウドコンピューティングは、コンピューティングリソースのオンデマンド可用性を提供する。クラウドコンピューティングは、インターネットを介してユーザに利用可能なデータセンタに基づくことができる。クラウドコンピューティングは、サービスとしてのインフラストラクチャ (IaaS) を提供することができる。仮想ネットワークは、ユーザによる使用のために作成されてもよい。しかしながら、これらの仮想ネットワークは、それらの機能性および価値を制約する制限を有する。したがって、さらなる改善が望まれる。

【発明の概要】

30

【課題を解決するための手段】

【0003】

概要

本開示は、仮想化されたクラウド環境に関する。仮想化されたクラウド環境においてレイヤ 2 ネットワーキング機能を提供するための技術が説明される。レイヤ 2 機能は、仮想化されたクラウド環境によって提供されるレイヤ 3 ネットワーキング機能に加えて、およびそれと関連して、提供される。

【0004】

本開示のいくつかの実施形態は、顧客の仮想クラウドネットワーク (VCN) など、プライベートネットワーク内でレイヤ 2 仮想ローカルエリアネットワーク (VLAN) を顧客に提供することに関する。レイヤ 2 VLAN においては、異なる計算インスタンスが接続される。顧客は、計算インスタンスを接続するエミュレートされた単一スイッチの認知を与えられる。実際、このエミュレートされたスイッチは、ローカルスイッチの集合を含む無限にスケーラブルな分散型スイッチとして実現される。より具体的には、各計算インスタンスは、ネットワーク仮想化デバイス (NVD) に接続されたホストマシン上で実行される。NVD に接続されたホスト上の各計算インスタンスについて、NVD は、計算インスタンスに関連付けられるレイヤ 2 仮想ネットワークインターフェースカード (VNIC) およびローカルスイッチをホストする。レイヤ 2 VNIC は、レイヤ 2 VLAN 上において計算インスタンスのポートを表す。ローカルスイッチは、VNIC を、レイヤ 2 VLAN の他の計算インスタンスに関連付けられる他の VNIC (例えば、他のポート) に

40

50

接続する。例えば、ストーム制御を含む、様々なレイヤ 2 ネットワークサービスがサポートされる。

【0005】

ここでは、方法、システム、1つ以上のプロセッサによって実行可能なプログラム、コード、または命令を記憶する非一時的コンピュータ可読記憶媒体などを含む様々な実施形態について説明する。

【図面の簡単な説明】

【0006】

【図1】 特定の実施形態に従って、クラウドサービスプロバイダインフラストラクチャによってホストされている仮想またはオーバーレイクラウドネットワークを示す分散環境のハイレベル図である。

10

【図2】 特定の実施形態に従って、C S P I 内の物理ネットワークの物理要素を示すアーキテクチャ概略図である。

【図3】 特定の実施形態に従って、ホストマシンが複数のネットワーク仮想化デバイス（N V D）に接続されている C S P I の例示的な配置を示す図である。

【図4】 特定の実施形態に従って、ホストマシンとマルチテナント機能をサポートするための I / O 仮想化を提供する N V D との間の接続を示す図である。

【図5】 特定の実施形態に従って、C S P I によって提供される物理ネットワークを示す概略ブロック図である。

【図6】 ある実施形態によるコンピューティングネットワークの概略図である。

20

【図7】 ある実施形態による、V L A N の論理およびハードウェア概略図である。

【図8】 ある実施形態による、複数の接続された L 2 V L A N の論理概略図である。

【図9】 ある実施形態による、複数の接続された L 2 V L A N およびサブネット 9 0 0 の論理概略図である。

【図10】 ある実施形態による、V L A N 内通信および V L A N 内の学習の概略図である。

【図11】 ある実施形態による V L A N の概略図である。

【図12】 ある実施形態による、V L A N 内通信のためのプロセス 1 2 0 0 を示すフローチャートである。

【図13】 ある実施形態による、L 2 仮想ネットワークのためにストーム制御の構成を定義するのに好適な例示的環境を図示する。

30

【図14】 いくつかの実施形態による、レイヤ仮想ネットワークにおける例示的なストーム制御技術を示す図である。

【図15】 いくつかの実施形態による、L 2 仮想ネットワークにおいてストーム制御情報を使用するためのプロセスを示すシーケンス図である。

【図16】 いくつかの実施形態による、ストーム制御情報の生成および配信を判断するためのプロセスを示すフローチャートである。

【図17】 いくつかの実施形態による、収集されたメトリックに基づいてストーム制御ポリシーを更新するためのプロセスを示すフローチャートである。

【図18】 いくつかの実施形態による、ストーム制御情報を更新するためのプロセスを示すフローチャートである。

40

【図19】 少なくとも1つの実施形態に従って、クラウドインフラストラクチャをサービスシステムとして実現するための1つのパターンを示すブロック図である。

【図20】 少なくとも1つの実施形態に従って、クラウドインフラストラクチャをサービスシステムとして実現するための別のパターンを示すブロック図である。

【図21】 少なくとも1つの実施形態に従って、クラウドインフラストラクチャをサービスシステムとして実現するための別のパターンを示すブロック図である。

【図22】 少なくとも1つの実施形態に従って、クラウドインフラストラクチャをサービスシステムとして実現するための別のパターンを示すブロック図である。

【図23】 少なくとも1つの実施形態に従って、例示的なコンピュータシステムを示すブ

50

ロック図である。

【発明を実施するための形態】

【0007】

詳細な説明

以下の説明では、説明の目的のために、特定の詳細が、特定の実施形態の完全な理解を促すために記載される。しかしながら、様々な実施形態がこれらの具体的な詳細なしに実施されてもよいことは明らかであろう。図および記載は、限定することを意図したものではない。「例示的」という文言は、ここでは、「例、事例、または例示として供される」ことを意味するために用いられる。「例示的」としてここに記載される任意の実施形態または設計は、必ずしも、他の実施形態もしくは設計よりも好ましいまたは有利であると解釈されるべきではない。

10

【0008】

A. 例示的な仮想ネットワークアーキテクチャ

クラウドサービスという用語は、一般的に、クラウドサービスプロバイダ（CSP）が、システムおよびインフラストラクチャ（クラウドインフラストラクチャ）を用いて、ユーザまたは顧客がオンデマンドで（例えば、サブスクリプションモデルを介して）利用できるサービスを指す。通常、CSPのインフラストラクチャを構成するサーバおよびシステムは、顧客自身のオンプレミスサーバおよびシステムから離れている。したがって、顧客は、サービス用のハードウェアおよびソフトウェア資源を別途購入することなく、CSPによって提供されるクラウドサービスを利用することができる。クラウドサービスは、サービスを提供するために使用されるインフラストラクチャの調達に顧客が投資する必要がなく、アプリケーションおよび計算リソースへの容易且つ拡張可能なアクセスを加入している顧客に提供するように設計されている。

20

【0009】

様々な種類のクラウドサービスを提供するクラウドサービスプロバイダがいくつかある。クラウドサービスは、SaaS（Software-as-a-Service）、PaaS（Platform-as-a-Service）、IaaS（Infrastructure-as-a-Service）などの様々な異なる種類またはモデルを含む。

【0010】

顧客は、CSPによって提供される1つ以上のクラウドサービスに加入することができる。顧客は、個人、組織、企業などの任意のエンティティであってもよい。顧客がCSPによって提供されるサービスに加入または登録すると、その顧客に対してテナントまたはアカウントが作成される。その後、顧客は、このアカウントを介して、アカウントに関連付けられた1つ以上の加入済みクラウドリソースにアクセスすることができる。

30

【0011】

上述したように、IaaS（Infrastructure as a Service）は、1つの特定種類のクラウドコンピューティングサービスである。IaaSモデルにおいて、CSPは、顧客が自身のカスタマイズ可能なネットワークを構築し、顧客リソースを展開するために使用できるインフラストラクチャ（クラウドサービスプロバイダインフラストラクチャまたはCSP Iと呼ばれる）を提供する。したがって、顧客のリソースおよびネットワークは、CSPによって提供されたインフラストラクチャによって分散環境にホストされる。これは、顧客のインフラストラクチャが顧客のリソースおよびネットワークをホストする従来のコンピューティングとは異なる。

40

【0012】

CSP Iは、基板ネットワークまたはアンダーレイネットワークとも呼ばれる物理ネットワークを形成する、様々なホストマシン、メモリリソース、およびネットワークリソースを含む相互接続された高性能の計算リソースを含んでもよい。CSP Iのリソースは、1つ以上の地理的な地域にわたって地理的に分散されている1つ以上のデータセンタに分散されてもよい。仮想化ソフトウェアは、これらの物理リソースによって実行され、仮想化分散環境を提供することができる。仮想化は、物理ネットワーク上に（ソフトウェアベ

50

ースネットワーク、ソフトウェア定義ネットワーク、または仮想ネットワークとも呼ばれる) オーバーレイネットワークを作成する。C S P I 物理ネットワークは、物理ネットワークの上に1つ以上のオーバーレイまたは仮想ネットワークを作成するための基礎を提供する。仮想ネットワークまたはオーバーレイネットワークは、1つ以上の仮想クラウドネットワーク (V C N) を含むことができる。仮想ネットワークは、ソフトウェア仮想化技術 (例えば、ハイパーバイザ、ネットワーク仮想化デバイス (N V D) (例えば、スマートN I C) によって実行される機能、トップオブブラック (T O R) スイッチ、N V D によって実行される1つ以上の機能を実装するスマートT O R、および他のメカニズム) を用いて実装され、物理ネットワークの上で実行できるネットワーク抽象化層を作成する。仮想ネットワークは、ピアツーピアネットワーク、I P ネットワークなどの様々な形態をとることができる。仮想ネットワークは、典型的には、レイヤ3 I P ネットワークまたはレイヤ2 V L A N のいずれかである。このような仮想ネットワークまたはオーバーレイネットワークは、しばしば仮想レイヤ3 ネットワークまたはオーバーレイレイヤ3 ネットワークと呼ばれる。仮想ネットワークのために開発されたプロトコルの例は、I P - i n - I P (またはG R E (Generic Routing Encapsulation))、仮想拡張可能L A N (V X L A N - I E T F R F C 7 3 4 8)、仮想プライベートネットワーク (V P N) (例えば、M P L S レイヤ3 仮想プライベートネットワーク (R F C 4 3 6 4))、V M w a r e N S X、G E N E V E (Generic Network Virtualization Encapsulation) などを含む。

10

20

30

40

50

【0013】

I a a S の場合、C S P I によって提供されたインフラストラクチャ (C S P I) は、パブリックネットワーク (例えば、インターネット) を介して仮想化計算リソースを提供するように構成されてもよい。I a a S モデルにおいて、クラウドコンピューティングサービスプロバイダは、インフラストラクチャ要素 (例えば、サーバ、記憶装置、ネットワークノード (例えば、ハードウェア)、展開ソフトウェア、プラットフォーム仮想化 (例えば、ハイパーバイザ層) など) をホストすることができる。場合によっては、I a a S プロバイダは、それらのインフラストラクチャ要素に付随する様々なサービス (例えば、課金、監視、ロギング、セキュリティ、負荷分散およびクラスタリングなど) を提供することができる。これらのサービスがポリシー駆動型であるため、I a a S ユーザは、負荷分散を駆動するためのポリシーを実装することによって、アプリケーションの可用性および性能を維持することができる。C S P I は、インフラストラクチャおよび一連の補完的なクラウドサービスを提供する。これによって、顧客は、可用性の高いホスト型分散環境で幅広いアプリケーションおよびサービスを構築し、実行することができる。C S P I は、顧客オンプレミスネットワークなどの様々なネットワーク拠点から安全にアクセスできる柔軟な仮想ネットワーク上で高性能の計算リソースおよび能力ならびに記憶容量を提供する。顧客がC S P I によって提供されたI a a S サービスに加入または登録すると、その顧客のために作成されたテナンシは、C S P I から安全に分離されたパーティションとなり、顧客は、クラウドリソースを作成、整理、管理することができる。

【0014】

顧客は、C S P I によって提供された計算リソース、メモリリソース、およびネットワークリソースを使用して、独自の仮想ネットワークを構築することができる。これらの仮想ネットワーク上に、計算インスタンスなどの1つ以上の顧客リソースまたはワークロードを展開することができる。例えば、顧客は、C S P I によって提供されたリソースを使用して、仮想クラウドネットワーク (V C N) と呼ばれる1つ以上のカスタマイズ可能なプライベート仮想ネットワークを構築することができる。顧客は、顧客V C N 上で1つ以上の顧客リソース、例えば計算インスタンスを展開することができる。計算インスタンスは、仮想マシン、ベアメタルインスタンスなどであってもよい。したがって、C S P I は、顧客が可用性の高い仮想ホスト環境において様々なアプリケーションおよびサービスを構築および実行することを可能にするインフラストラクチャおよび一連の相補的なクラウドサービスを提供する。顧客は、C S P I によって提供された基礎的な物理リソース

を管理または制御しないが、オペレーティングシステム、記憶、および展開されたアプリケーションを制御し、場合によっては一部のネットワーキングコンポーネント（例えば、ファイアウォール）を限定的に制御する。

【0015】

CSPは、顧客およびネットワーク管理者がCSP Iリソースを使用してクラウドに展開されたリソースを構成、アクセス、および管理することを可能にするコンソールを提供することができる。特定の実施形態において、コンソールは、CSP Iを利用および管理するために使用することができるウェブベースのユーザインターフェイスを提供する。いくつかの実施形態において、コンソールは、CSPによって提供されたウェブベースのアプリケーションである。

10

【0016】

CSP Iは、シングルテナンシアーキテクチャまたはマルチテナンシアーキテクチャをサポートすることができる。シングルテナンシアーキテクチャにおいて、ソフトウェア（例えば、アプリケーション、データベース）またはハードウェア要素（例えば、ホストマシンまたはサーバ）は、単一の顧客またはテナントにサービスを提供する。マルチテナンシアーキテクチャにおいて、ソフトウェアまたはハードウェア要素は、複数の顧客またはテナントにサービスを提供する。したがって、マルチテナンシアーキテクチャにおいて、CSP Iリソースは、複数の顧客またはテナントの間で共有される。マルチテナンシ環境において、各テナントのデータが分離され、他のテナントから見えなくするために、CSP Iには予防措置および保護措置が講じられる。

20

【0017】

物理ネットワークにおいて、ネットワークエンドポイント（エンドポイント）は、物理ネットワークに接続され、接続されているネットワークと双方向に通信するコンピューティング装置またはシステムを指す。物理ネットワークのネットワークエンドポイントは、ローカルエリアネットワーク（LAN）、ワイドエリアネットワーク（WAN）、または他の種類の物理ネットワークに接続されてもよい。物理ネットワークの従来のエンドポイントの例は、モデム、ハブ、ブリッジ、スイッチ、ルータ、および他のネットワーキング装置、物理コンピュータ（またはホストマシン）などを含む。物理ネットワークの各物理装置は、当該装置と通信するために使用できる固定ネットワークアドレスを有する。この固定ネットワークアドレスは、レイヤ2アドレス（例えば、MACアドレス）、固定レイヤ3アドレス（例えば、IPアドレス）などであってもよい。仮想化環境または仮想ネットワークにおいて、エンドポイントは、物理ネットワークの要素によってホストされている（例えば、物理ホストマシンによってホストされている）仮想マシンなどの様々な仮想エンドポイントを含むことができる。仮想ネットワークのこれらのエンドポイントは、オーバーレイレイヤ2アドレス（例えば、オーバーレイMACアドレス）およびオーバーレイレイヤ3アドレス（例えば、オーバーレイIPアドレス）などのオーバーレイアドレスによってアドレス指定される。ネットワークオーバーレイは、ネットワーク管理者がソフトウェア管理を用いて（例えば、仮想ネットワークの制御プレーンを実装するソフトウェアを介して）ネットワークエンドポイントに関連付けられたオーバーレイアドレスを移動できるようにすることによって柔軟性を実現する。したがって、物理ネットワークとは異なり、仮想ネットワークにおいて、ネットワーク管理ソフトウェアを使用して、オーバーレイアドレス（例えば、オーバーレイIPアドレス）を1つのエンドポイントから別のエンドポイントに移動することができる。仮想ネットワークが物理ネットワーク上に構築されているため、仮想ネットワークおよび基礎となる物理ネットワークの両方は、仮想ネットワークの要素間の通信に関与する。このような通信を容易にするために、CSP Iの各要素は、仮想ネットワークのオーバーレイアドレスを基板ネットワークの実際の物理アドレスにまたは基板ネットワークの実際の物理アドレスを仮想ネットワークのオーバーレイアドレスにマッピングするマッピングを学習および記憶するように構成されている。これらのマッピングは、通信を容易にするために使用される。仮想ネットワークのルーティングを容易にするために、顧客トラフィックは、カプセル化される。

30

40

50

【0018】

したがって、物理アドレス（例えば、物理IPアドレス）は、物理ネットワークの要素に関連付けられ、オーバーレイアドレス（例えば、オーバーレイIPアドレス）は、仮想ネットワークのエンティティに関連付けられる。物理IPアドレスとオーバーレイIPアドレスは、いずれも実IPアドレスである。これらは、仮想IPアドレスとは別物であり、仮想IPアドレスは、複数の実IPアドレスにマッピングされる。仮想IPアドレスは、仮想IPアドレスと複数の実IPアドレスの間の1対多のマッピングを提供する。

【0019】

クラウドインフラストラクチャまたはCSPは、世界中の1つ以上の地域の1つ以上のデータセンタに物理的にホストされる。CSPは、物理ネットワークまたは基板ネットワークの要素と、物理ネットワーク要素上に構築された仮想ネットワークの仮想化要素（例えば、仮想ネットワーク、計算インスタンス、仮想マシン）とを含んでもよい。特定の実施形態において、CSPは、レルム（realm）、地域（region）、および利用可能なドメイン（domain）において編成およびホストされる。地域は、典型的には、1つ以上のデータセンタを含む局所的な地理的領域である。地域は、一般的に互いに独立しており、例えば、国または大陸を跨ぐ広大な距離によって分離されてもよい。例えば、第1の地域は、オーストラリアにあってもよく、別の地域は、日本にあってもよく、さらに別の地域は、インドにあってもよい。CSPリソースは、各地域が独立したCSPリソースのサブセットを有するようにこれらの地域間で分割される。各地域は、一連のコアインフラストラクチャサービスおよびリソース、例えば、計算リソース（例えば、ベアメタルサーバ、仮想マシン、コンテナおよび関連インフラストラクチャ）、記憶リソース（例えば、ブロックボリューム記憶、ファイル記憶、オブジェクト記憶、アーカイブ記憶）、ネットワーキングリソース（例えば、仮想クラウドネットワーク（VCN）、負荷分散リソース、オンプレミスネットワークへの接続）、データベースリソース、エッジネットワーキングリソース（例えば、DNS）、アクセス管理および監視リソースなどを提供することができる。各地域は、一般的に、当該地域をレルム内の他の地域に接続するための複数の経路を持つ。

【0020】

一般的に、アプリケーションは、近くのリソースを使用することが遠くのリソースを使用することよりも速いため、最も多く使用される地域に展開される（すなわち、その地域に関連するインフラストラクチャ上に展開される）。また、アプリケーションは、大規模な気象システムまたは地震などの地域全体のイベントのリスクを軽減するための冗長性、法的管轄、税金ドメイン、および他のビジネスまたは社会的基準に対する様々な要件を満たすための冗長性など、様々な理由で異なる地域に展開されてもよい。

【0021】

地域内のデータセンタは、さらに編成され、利用可能なドメイン（availability domain：AD）に細分化されてもよい。利用可能なドメインは、ある地域に配置された1つ以上のデータセンタに対応してもよい。地域は、1つ以上の利用可能なドメインから構成されてもよい。このような分散環境において、CSPリソースは、仮想クラウドネットワーク（VCN）などの地域に固有なものまたは計算インスタンスなどの利用可能なドメインに固有のものである。

【0022】

1つの地域内のADは、フォールトトレラント（fault tolerant）になるように互いに分離され、同時に故障する可能性が非常になくなるように構成されている。これは、1つの地域内の1つのADの障害が同じ地域内の他のADの可用性に影響を与えることが殆どないように、ネットワーキング、物理ケーブル、ケーブル経路、ケーブル入口などの重要なインフラストラクチャリソースを共有しないように、ADを構成することによって達成される。同じ地域内のADを低遅延広帯域のネットワークで互いに接続することによって、他のネットワーク（例えば、インターネット、顧客オンプレミスネットワーク）への高可用性接続を提供し、複数のADにおいて高可用性および災害復旧の両方のための複製

システムを構築することができる。クラウドセンアイスは、複数の A D を利用して、高可用性を確保すると共に、リソースの障害から保護する。I a a S プロバイダによって提供されたインフラストラクチャが成長するにつれて、追加の容量と共により多くの地域および A D を追加してもよい。利用可能なドメイン間のトラフィックは、通常、暗号化される。

【 0 0 2 3 】

特定の実施形態において、地域は、レルムにグループ化される。レルムは、地域の論理的な集合である。レルムは、互いに隔離されており、いかなるデータを共有しない。同じレルム内の地域は、互いに通信することができるが、異なるレルム内の地域は、通信することができない。C S P の顧客のテナンシまたはアカウントは、単一のレルムに存在し、その単一のレルムに属する 1 つ以上の地域を跨ることができる。典型的には、顧客が I a a S サービスに加入すると、レルム内の顧客指定地域（「ホーム」地域と呼ばれる）に、その顧客のテナンシまたはアカウントが作成される。顧客は、顧客のテナンシをレルム内の 1 つ以上の他の地域に拡張することができる。顧客は、顧客のテナンシが存在するレルム内に存在していない地域にアクセスすることができない。

10

【 0 0 2 4 】

I a a S プロバイダは、複数のレルムを提供することができ、各レルムは、特定の組の顧客またはユーザに対応する。例えば、商用レルムは、商用顧客のために提供されてもよい。別の例として、レルムは、特定の国のためにまたはその国の顧客のために提供されてもよい。さらに別の例として、政府用レルムは、例えば政府のために提供されてもよい。例えば、政府用レルムは、特定の政府のために作成されてもよく、商用レルムよりも高いセキュリティレベルを有してもよい。例えば、オラクル（登録商標）クラウドインフラストラクチャ（O C I）は、現在、商用領域向けのレルムと、政府クラウド領域向けの 2 つのレルム（例えば、F e d R A M P 認可および I L 5 認可）とを提供する。

20

【 0 0 2 5 】

特定の実施形態において、A D は、1 つ以上の障害ドメイン（fault domain）に細分化することができる。障害ドメインは、反親和性（anti-affinity）を提供するために、A D 内のインフラストラクチャリソースをグループ化したものである。障害ドメインは、計算インスタンスを分散することができる。これによって、計算インスタンスは、1 つの A D 内の同じ物理ハードウェア上に配置されない。これは、反親和性として知られている。障害ドメインは、1 つの障害点を共有するハードウェア要素（コンピュータ、スイッチなど）の集合を指す。計算プールは、障害ドメインに論理的に分割される。このため、1 つの障害ドメインに影響を与えるハードウェア障害または計算ハードウェア保守イベントは、他の障害ドメインのインスタンスに影響を与えない。実施形態によっては、各 A D の障害ドメインの数は、異なってもよい。例えば、特定の実施形態において、各 A D は、3 つの障害ドメインを含む。障害ドメインは、A D 内の論理データセンタとして機能する。

30

【 0 0 2 6 】

顧客が I a a S サービスに加入すると、C S P I からのリソースは、顧客にプロビジョニングされ、顧客のテナンシに関連付けられる。顧客は、これらのプロビジョニングされたリソースを使用して、プライベートネットワークを構築し、これらのネットワーク上にリソースを展開することができる。C S P I によってクラウド上でホストされている顧客ネットワークは、仮想クラウドネットワーク（V C N）と呼ばれる。顧客は、顧客用に割り当てられた C S P I リソースを使用して、1 つ以上の仮想クラウドネットワーク（V C N）を構成することができる。V C N とは、仮想またはソフトウェア定義のプライベートネットワークである。顧客の V C N に配備された顧客リソースは、計算インスタンス（例えば、仮想マシン、ベアメタルインスタンス）および他のリソースを含むことができる。これらの計算インスタンスは、アプリケーション、ロードバランサ、データベースなどの様々な顧客作業負荷を表してもよい。V C N 上に配備された計算インスタンスは、インターネットなどのパブリックネットワークを介して公的にアクセス可能なエンドポイント（パブリックエンドポイント）と通信することができ、同じ V C N または他の V C N（例え

40

50

ば、顧客の他の V C N、または顧客に属さない V C N) 内の他のインスタンスと通信することができ、顧客オンプレミスデータセンタまたはネットワークと通信することができ、センディエンドポイントと通信することができ、および他の種類のエンドポイントと通信することができる。

【 0 0 2 7 】

C S P は、C S P I を用いて多様なサービスを提供することができる。場合によっては、C S P I の顧客自身は、サービスプロバイダのように振る舞い、C S P I リソースを使用してサービスを提供することができる。サービスプロバイダは、識別情報（例えば、I P アドレス、D N S 名およびポート）によって特徴付けられるサービスエンドポイントを公開することができる。顧客のリソース（例えば、計算インスタンス）は、サービスによって公開されたその特定のサービスのサービスエンドポイントにアクセスすることによって、特定のサービスを消費することができる。これらのサービスエンドポイントは、一般に、ユーザがエンドポイントに関連付けられたパブリック I P アドレスを使用して、インターネットなどのパブリック通信ネットワークを介して公的にアクセス可能なエンドポイントである。公的にアクセス可能なネットワークエンドポイントは、パブリックエンドポイントと呼ばれることもある。

10

【 0 0 2 8 】

特定の実施形態において、サービスプロバイダは、（サービスエンドポイントと呼ばれることもある）サービスのエンドポイントを介してサービスを公開することができる。サービスの顧客は、このサービスエンドポイントを使用してサービスにアクセスすることができる。特定の実施形態において、サービスのために提供されたサービスエンドポイントは、そのサービスを消費しようとする複数の顧客によってアクセスすることができる。他の実装形態において、専用のサービスエンドポイントを顧客に提供してもよい。したがって、その顧客のみは、その専用センディエンドポイントを使用してサービスにアクセスすることができる。

20

【 0 0 2 9 】

特定の実施形態において、V C N は、作成されると、その V C N に割り当てられたプライベートオーバーレイ I P アドレス範囲（例えば、1 0 . 0 / 1 6）であるプライベートオーバーレイクラスレスドメイン間ルーティング（Classless Inter-Domain Routing : C I D R）アドレス空間に関連付けられる。V C N は、関連するサブネット、ルートテーブル、およびゲートウェイを含む。V C N は、単一の地域内に存在するが、地域の 1 つ以上または全ての利用可能なドメインに拡張することができる。ゲートウェイは、V C N 用に構成され、V C N と V C N 外部の 1 つ以上のエンドポイントとの間のトラフィック通信を可能にする仮想インターフェースである。V C N の 1 つ以上の異なる種類のゲートウェイを構成することによって、異なる種類のエンドポイント間の通信を可能にすることができる。

30

【 0 0 3 0 】

V C N は、1 つ以上のサブネットなどの 1 つ以上のサブネットワークに細分化されてもよい。したがって、サブネットは、V C N 内で作成され得る構成単位または区画である。V C N は、1 つ以上のサブネットを持つことができる。V C N 内の各サブネットは、当該 V C N 内の他のサブネットと重複せず、当該 V C N のアドレス空間のアドレス空間サブセットを表すオーバーレイ I P アドレス（例えば、1 0 . 0 . 0 . 0 / 2 4 および 1 0 . 0 . 1 . 0 / 2 4）の連続範囲に関連付けられる。

40

【 0 0 3 1 】

各計算インスタンスは、仮想ネットワークインターフェイスカード（V N I C）に関連付けられる。これによって、各計算インスタンスは、V C N のサブネットに参加することができる。V N I C は、物理ネットワークインターフェイスカード（N I C）の論理表現である。一般的に、V N I C は、エンティティ（例えば、計算インスタンス、サービス）と仮想ネットワークとの間のインターフェースである。V N I C は、サブネットに存在し、1 つ以上の関連する I P アドレスと、関連するセキュリティルールまたはポリシーとを

50

有する。VNICは、スイッチ上のレイヤ2ポートに相当する。VNICは、計算インスタンスと、VCN内のサブネットとに接続されている。計算インスタンスに関連付けられたVNICは、計算インスタンスがVCNのサブネットの一部であることを可能にし、計算インスタンスが、計算インスタンスと同じサブネット上にあるエンドポイントと、VCN内の異なるサブネット内のエンドポイントと、またはVCN外部のエンドポイントと通信する（例えば、パケットを送信および受信する）ことを可能にする。したがって、計算インスタンスに関連するVNICは、計算インスタンスがVCNの内部および外部のエンドポイントとどのように接続しているかを判断する。計算インスタンスのVNICは、計算インスタンスが作成され、VCN内のサブネットに追加されるときに作成され、その計算インスタンスに関連付けられる。サブネットは、計算インスタンスのセットからなる場合、計算インスタンスのセットに対応するVNICを含み、各VNICは、コンピュータインスタンスのセット内の計算インスタンスに接続されている。

10

【0032】

計算インスタンスに関連するVNICを介して、各計算インスタンスにはプライベートオーバーレイIPアドレスが割り当てられる。このプライベートオーバーレイIPアドレスは、計算インスタンスの作成時に計算インスタンスに関連するVNICに割り当てられ、計算インスタンスのトラフィックをルーティングするために使用される。特定のサブネット内の全てのVNICは、同じルートテーブル、セキュリティリスト、およびDHCPオプションを使用する。上述したように、VCN内の各サブネットは、当該VCN内の他のサブネットと重複せず、当該VCNのアドレス空間のアドレス空間サブセットを表すオーバーレイIPアドレス（例えば、10.0.0.0/24および10.0.1.0/24）の連続範囲に関連付けられる。VCNの特定のサブネット上のVNICの場合、VNICに割り当てられたオーバーレイIPアドレスは、サブネットに割り当てられたオーバーレイIPアドレスの連続範囲からのアドレスである。

20

【0033】

特定の実施形態において、必要に応じて、計算インスタンスには、プライベートオーバーレイIPアドレスに加えて、追加のオーバーレイIPアドレス、例えば、パブリックサブネットの場合に1つ以上のパブリックIPアドレスを割り当てることができる。これらの複数のアドレスは、同じVNIC、または計算インスタンスに関連付けられた複数のVNICに割り当てられる。しかしながら、各インスタンスは、インスタンス起動時に作成され、インスタンスに割り当てられたオーバーレイプライベートIPアドレスに関連付けられたプライマリVNICを有する。このプライマリVNICは、削除することができない。セカンダリVNICと呼ばれる追加のVNICは、プライマリVNICと同じ利用可能なドメイン内の既存のインスタンスに追加することができる。全てのVNICは、インスタンスと同じ利用可能なドメインにある。セカンダリVNICは、プライマリVNICと同じVCNのサブネットにあってもよく、または同じVCNまたは異なるVCNの異なるサブネットにあってもよい。

30

【0034】

計算インスタンスは、パブリックサブネットにある場合、オプションでパブリックIPアドレスを割り当てられることができる。サブネットを作成するときに、当該サブネットをパブリックサブネットまたはプライベートサブネットのいずれかとして指定することができる。プライベートサブネットとは、当該サブネット内のリソース（例えば、計算インスタンス）および関連するVNICがパブリックオーバーレイIPアドレスを持つことができないことを意味する。パブリックサブネットとは、サブネット内のリソースおよび関連するVNICがパブリックIPアドレスを持つことができることを意味する。顧客は、地域またはレルム内の単一の利用可能なドメインまたは複数の利用可能なドメインにわたって存在するサブネットを指定することができる。

40

【0035】

上述したように、VCNは、1つ以上のサブネットに細分化されてもよい。特定の実施形態において、VCNのために構成された仮想ルータ（VCN VRまたは単にVRと呼

50

ばれる)は、V C Nのサブネット間の通信を可能にする。V C N内のサブネットの場合、V Rは、サブネット(すなわち、当該サブネット上の計算インスタンス)と、V C N内部の他のサブネット上のエンドポイントおよびV C N外部の他のエンドポイントとの通信を可能にする当該サブネットの論理ゲートウェイを表す。V C N V Rは、V C N内のV N I Cと、V C Nに関連する仮想ゲートウェイ(ゲートウェイ)との間のトラフィックをルーティングするように構成された論理エンティティである。ゲートウェイは、図1に関して以下でさらに説明される。V C N V Rは、レイヤ3 / I Pレイヤの概念である。一実施形態において、1つのV C Nに対して1つのV C N V Rが存在する。このV C N V Rは、I Pアドレスによってアドレス指定された無制限の数のポートを潜在的に有し、V C Nの各サブネットに対して1つのポートを有する。このようにして、V C N V Rは、V C N V Rが接続されているV C Nの各サブネットに対して異なるI Pアドレスを有する。また、V Rは、V C Nのために構成された様々なゲートウェイに接続されている。特定の実施形態において、サブネットのオーバーレイI Pアドレス範囲からの特定のオーバーレイI Pアドレスは、そのサブネットのV C N V Rのポートに保留される。例えば、関連するアドレス範囲10.0 / 16および10.1 / 16を各々有する2つのサブネットを有するV C Nを考える。アドレス範囲10.0 / 16を有するV C Nの第1のサブネットの場合、この範囲からのアドレスは、そのサブネットのV C N V Rのポートに保留される。場合によっては、この範囲からの第1のI Pアドレスは、V C N V Rに保留されてもよい。例えば、オーバーレイI Pアドレス範囲10.0 / 16を有するサブネットの場合、I Pアドレス10.0.0.1は、そのサブネットのV C N V Rのポートに保留されてもよい。同じV C N内のアドレス範囲10.1 / 16を有する第2のサブネットの場合、V C N V Rは、I Pアドレス10.1.0.1を有する第2のサブネットのポートを有してもよい。V C N V Rは、V C N内の各サブネットに対して異なるI Pアドレスを有する。

10

20

30

40

50

【0036】

いくつかの他の実施形態において、V C N内の各サブネットは、V Rに関連付けられた保留またはデフォルトI Pアドレスを使用してサブネットによってアドレス指定可能な、それ自身に関連するV Rを有してもよい。保留またはデフォルトI Pアドレスは、例えば、そのサブネットに関連付けられたI Pアドレスの範囲からの第1のI Pアドレスであってもよい。サブネット内のV N I Cは、このデフォルトまたは保留I Pアドレスを使用して、サブネットに関連付けられたV Rと通信(例えば、パケットを送信および受信)することができる。このような実施形態において、V Rは、そのサブネットの着信 / 送信ポイントである。V C N内のサブネットに関連付けられたV Rは、V C N内の他のサブネットに関連付けられた他のV Rと通信することができる。また、V Rは、V C Nに関連付けられたゲートウェイと通信することができる。サブネットのV R機能は、サブネット内のV N I CのV N I C機能を実行する1つ以上のN V D上で実行され、またはそれによって実行される。

【0037】

ルートテーブル、セキュリティルール、およびD H C Pオプションは、V C Nのために構成されてもよい。ルートテーブルは、V C Nの仮想ルートテーブルであり、ゲートウェイまたは特別に構成されたインスタンスを経由して、トラフィックをV C N内部のサブネットからV C N外部の宛先にルーティングするためのルールを含む。V C Nとの間でパケットの転送 / ルーティングを制御するために、V C Nのルートテーブルをカスタマイズすることができる。D H C Pオプションは、インスタンスの起動時にインスタンスに自動的に提供される構成情報を指す。

【0038】

V C Nのために構成されたセキュリティルールは、V C Nのオーバーレイファイアウォールルールを表す。セキュリティルールは、受信ルールおよび送信ルールを含むことができ、(例えば、プロトコルおよびポートに基づいて) V C N内のインスタンスに出入りすることを許可されるトラフィックの種類を指定することができる。顧客は、特定の規則を

ステートフルまたはステートレスにするかを選択することができる。例えば、顧客は、送信元 C I D R 0 . 0 . 0 . 0 / 0 および宛先 T C P ポート 2 2 を含むステートフル受信ルールを設定することによって、任意の場所から 1 組のインスタンスへの着信 S S H トラフィックを許可することができる。セキュリティルールは、ネットワークセキュリティグループまたはセキュリティリストを使用して実装されてもよい。ネットワークセキュリティグループは、そのグループ内のリソースのみに適用されるセキュリティルールのセットからなる。一方、セキュリティリストは、そのセキュリティリストを使用するサブネット内の全てのリソースに適用されるルールを含む。V C N は、デフォルトセキュリティルールとデフォルトセキュリティリストを含んでもよい。V C N のために構成された D H C P オプションは、V C N 内のインスタンスが起動するときに自動的に提供される構成情報を提供する。

10

【 0 0 3 9 】

特定の実施形態において、V C N の構成情報は、V C N 制御プレーンによって決定され、記憶される。V C N の構成情報は、例えば、V C N に関連するアドレス範囲、V C N 内のサブネットおよび関連情報、V C N に関連する 1 つ以上の V R、V C N 内の計算インスタンスおよび関連 V N I C、V C N に関連する種々の仮想化ネットワーク機能（例えば、V N I C、V R、ゲートウェイ）を実行する N V D、V C N の状態情報、および他の V C N 関連情報を含んでもよい。特定の実施形態において、V C N 配信サービスは、V C N 制御プレーンによって記憶された構成情報またはその一部を N V D に公開する。配信された情報を用いて、N V D によって記憶および使用される情報（例えば、転送テーブル、ルーティングテーブルなど）を更新することによって、V C N 内のコンピュータインスタンスとの間でパケットを転送することができる。

20

【 0 0 4 0 】

特定の実施形態において、V C N およびサブネットの作成は、V C N 制御プレーン（C P）によって処理され、計算インスタンスの起動は、計算制御プレーンによって処理される。計算制御プレーンは、計算インスタンスの物理リソースを割り当て、次に V C N 制御プレーンを呼び出して、V N I C を作成し、計算インスタンスに接続するように構成される。また、V C N C P は、パケットの転送およびルーティング機能を実行するように構成された V C N データプレーンに、V C N データマッピングを送信する。特定の実施形態において、V C N C P は、更新を V C N データプレーンに提供するように構成された配信サービスを提供する。V C N 制御プレーンの例は、図 1 7、1 8、1 9 および 2 0（参照番号、1 7 1 6、1 8 1 6、1 9 1 6 および 2 0 1 6 を参照）に示され、以下に説明される。

30

【 0 0 4 1 】

顧客は、C S P I によってホストされているリソースを用いて、1 つ以上の V C N を作成することができる。顧客 V C N 上に展開された計算インスタンスは、異なるエンドポイントと通信することができる。これらのエンドポイントは、C S P I によってホストされているエンドポイントおよび C S P L 外部のエンドポイントを含むことができる。

【 0 0 4 2 】

C S P I を用いてクラウドベースのサービスを実装するための様々な異なるアーキテクチャは、図 1、2、3、4、5、1 7、1 8、1 9 および 2 1 に示され、以下に説明される。図 1 は、特定の実施形態に従って、C S P I によってホストされているオーバーレイ V C N または顧客 V C N を示す分散環境 1 0 0 のハイレベル図である。図 1 に示された分散環境は、オーバーレイネットワーク内の複数の要素を含む。図 1 に示された分散環境 1 0 0 は、単なる例であり、特許請求された実施形態の範囲を不当に限定することを意図していない。多くの変形例、代替例、および修正例が可能である。例えば、いくつかの実装形態において、図 1 に示された分散環境は、図 1 に示されたものより多いまたは少ないシステムまたは要素を有してもよく、2 つ以上のシステムを組み合わせてもよく、または異なるシステムの構成または配置を有してもよい。

40

【 0 0 4 3 】

50

図1の例に示されたように、分散環境100は、顧客が加入して仮想クラウドネットワーク（VCN）を構築するために使用することができるサービスおよびリソースを提供するCSP101を含む。特定の実施形態において、CSP101は、加入顧客にIaaSサービスを提供する。CSP101内のデータセンタは、1つ以上の地域に編成されてもよい。図1は、地域の一例である「US地域」102を示す。顧客は、地域102に対して顧客VCN104を構成している。顧客は、VCN104上に様々な計算インスタンスを展開することができ、計算インスタンスは、仮想マシンまたはベアメタルインスタンスを含むことができる。インスタンスの例は、アプリケーション、データベース、ロードバランサなどを含む。

【0044】

図1に示された実施形態において、顧客VCN104は、2つのサブネット、すなわち、「サブネットー1」および「サブネットー2」を含み、各サブネットは、各自のCIDR IPアドレス範囲を有する。図1において、サブネットー1のオーバーレイIPアドレス範囲は、10.0/16であり、サブネットー2のアドレス範囲は、10.1/16である。VCN仮想ルータ105は、VCN104のサブネット間の通信およびVCN外部の他のエンドポイントとの通信を可能にするVCNの論理ゲートウェイを表す。VCNVR105は、VCN104内のVNICとVCN104に関連するゲートウェイとの間でトラフィックをルーティングするように構成される。VCNVR105は、VCN104の各サブネットにポートを提供する。例えば、VR105は、IPアドレス10.0.0.1を有するポートをサブネットー1に提供することができ、IPアドレス10.1.0.1を有するポートをサブネットー2に提供することができる。

【0045】

各サブネット上に複数の計算インスタンスを展開することができる。この場合、計算インスタンスは、仮想マシンインスタンスおよび／またはベアメタルインスタンスであってもよい。サブネット内の計算インスタンスは、CSP101内の1つ以上のホストマシンによってホストされてもよい。計算インスタンスは、当該計算インスタンスに関連するVNICを介してサブネットに参加する。例えば、図1に示すように、計算インスタンスC1は、当該計算インスタンスに関連するVNICを介したサブネットー1の一部である。同様に、計算インスタンスC2は、C2に関連するVNICを介したサブネットー1の一部である。同様に、仮想マシンインスタンスまたはベアメタルインスタンスであり得る複数の計算インスタンスは、サブネットー1の一部であってもよい。各計算インスタンスには、関連するVNICを介して、プライベートオーバーレイIPアドレスおよびMACアドレスが割り当てられる。例えば、図1において、計算インスタンスC1は、オーバーレイIPアドレス10.0.0.2およびMACアドレスM1を有し、計算インスタンスC2は、プライベートオーバーレイIPアドレス10.0.0.3およびMACアドレスM2を有する。計算インスタンスC1およびC2を含むサブネットー1内の各計算インスタンスは、サブネットー1のVCNVR105のポートのIPアドレスであるIPアドレス10.0.0.1を使用して、VCNVR105へのデフォルトルートを有する。

【0046】

サブネットー2には、仮想マシンインスタンスおよび／またはベアメタルインスタンスを含む複数の計算インスタンスを展開することができる。例えば、図1に示すように、計算インスタンスD1およびD2は、それぞれの計算インスタンスに関連するVNICを介したサブネットー2の一部である。図1に示す実施形態において、計算インスタンスD1は、オーバーレイIPアドレス10.1.0.2およびMACアドレスMM1を有し、計算インスタンスD2は、プライベートオーバーレイIPアドレス10.1.0.3およびMACアドレスMM2を有する。計算インスタンスD1およびD2を含むサブネットー2内の各計算インスタンスは、サブネットー2のVCNVR105のポートのIPアドレスであるIPアドレス10.1.0.1を使用して、VCNVR105へのデフォルトルートを有する。

【0047】

また、V C N A 1 0 4 は、1 つ以上のロードバランサを含んでもよい。例えば、ロードバランサは、サブネットに対して提供されてもよく、サブネット上の複数の計算インスタンス間でトラフィックをロードバランスするように構成されてもよい。また、ロードバランサは、V C N 内のサブネット間でトラフィックをロードバランスするように提供されてもよい。

【 0 0 4 8 】

V C N 1 0 4 上に展開された特定の計算インスタンスは、様々な異なるエンドポイントと通信することができる。これらのエンドポイントは、C S P I 2 0 0 によってホストされているエンドポイントと、C S P I 2 0 0 外部のエンドポイントとを含んでもよい。C S P I 1 0 1 によってホストされているエンドポイントは、特定の計算インスタンスと同じサブネット上のエンドポイント（例えば、サブネットー1の2つの計算インスタンス間の通信）、異なるサブネットにあるが同じV C N 内のエンドポイント（例えば、サブネットー1の計算インスタンスとサブネットー2の計算インスタンスとの間の通信）、同じ地域の異なるV C N 内のエンドポイント（例えば、サブネットー1の計算インスタンスと、同じ地域1 0 6 または1 1 0 のV C N 内のエンドポイントとの間の通信、サブネットー1内の計算インスタンスと、同じ地域のサービスネットワーク1 1 0 内のエンドポイントとの間の通信）、または異なる地域のV C N 内のエンドポイント（例えば、サブネットー1の計算インスタンスと、異なる地域1 0 8 のV C N 内のエンドポイントとの間の通信）を含んでもよい。また、C S P I 1 0 1 によってホストされているサブネット内の計算インスタンスは、C S P I 1 0 1 によってホストされていない（すなわち、C S P I 1 0 1 の外部にある）エンドポイントと通信することができる。これらの外部のエンドポイントは、顧客オンプレミスネットワーク1 1 6 内のエンドポイント、他のリモートクラウドホストネットワーク1 1 8 内のエンドポイント、インターネットなどのパブリックネットワークを介してアクセス可能なパブリックエンドポイント1 1 4、および他のエンドポイントを含む。

【 0 0 4 9 】

同じサブネット上の計算インスタンス間の通信は、送信元計算インスタンスおよび宛先計算インスタンスに関連するV N I C を使用して促進される。例えば、サブネットー1内の計算インスタンスC 1 は、サブネットー1内の計算インスタンスC 2 にパケットを送信したいことがある。送信元計算インスタンスから送信され、その宛先が同じサブネット内の別の計算インスタンスであるパケットの場合、このパケットは、まず、送信元計算インスタンスに関連するV N I C によって処理される。送信元計算インスタンスに関連するV N I C によって実行される処理は、パケットヘッダからパケットの宛先情報を決定することと、送信元計算インスタンスに関連するV N I C に対して構成された任意のポリシー（例えば、セキュリティリスト）を識別することと、パケットのネクストホップ（next hop）を決定することと、必要に応じて任意のパケットのカプセル化／カプセル除去機能を実行することと、パケットの意図した宛先への通信を容易にするためにパケットをネクストホップに転送／ルーティングすることとを含んでもよい。宛先計算インスタンスが送信元計算インスタンスと同じサブネットにある場合、送信元計算インスタンスに関連するV N I C は、宛先計算インスタンスに関連するV N I C を識別し、処理するためのパケットをそのV N I C に転送するように構成されている。次いで、宛先計算インスタンスに関連するV N I C は、実行され、パケットを宛先計算インスタンスに転送する。

【 0 0 5 0 】

サブネット内の計算インスタンスから同じV C N の異なるサブネット内のエンドポイントにパケットを通信する場合、通信は、送信元計算インスタンスおよび宛先計算インスタンスに関連するV N I C と、V C N V R とによって促進される。例えば、図1のサブネットー1の計算インスタンスC 1 がサブネットー2の計算インスタンスD 1 にパケットを送信したい場合、パケットは、まず、計算インスタンスC 1 に関連するV N I C によって処理される。計算インスタンスC 1 に関連するV N I C は、V C N V R のデフォルトルートまたはポート1 0 . 0 . 0 . 1 を使用して、パケットをV C N V R 1 0 5 にルーテ

イングするように構成されている。VCN VR105は、ポート10.1.0.1を使用してパケットをサブネット-2にルーティングするように構成されている。その後、パケットは、D1に関連するVNICによって受信および処理され、VNICは、パケットを計算インスタンスD1に転送する。

【0051】

VCN104内の計算インスタンスからVCN104の外部のエンドポイントにパケットを通信するために、通信は、送信元計算インスタンスに関連するVNIC、VCN VR105、およびVCN104に関連するゲートウェイによって促進される。1つ以上の種類のゲートウェイをVCN104に関連付けることができる。ゲートウェイは、VCNと別のエンドポイントとの間のインターフェースであり、別のエンドポイントは、VCNの外部にある。ゲートウェイは、レイヤ3 / IPレイヤ概念であり、VCNとVCNの外部のエンドポイントとの通信を可能にする。したがって、ゲートウェイは、VCNと他のVCNまたはネットワークとの間のトラフィックフローを容易にする。異なる種類のエンドポイントとの異なる種類の通信を容易にするために、様々な異なる種類のゲートウェイをVCNに設定することができる。ゲートウェイによって、通信は、パブリックネットワーク（例えば、インターネット）またはプライベートネットワークを介して行われてもよい。これらの通信には、様々な通信プロトコルを使用してもよい。

【0052】

例えば、計算インスタンスC1は、VCN104の外部のエンドポイントと通信したい場合がある。パケットは、まず、送信元計算インスタンスC1に関連するVNICによって処理されてもよい。VNIC処理は、パケットの宛先がC1のサブネット-1の外部にあると判断する。C1に関連するVNICは、パケットをVCN104のVCN VR105に転送することができる。次いで、VCN VR105は、パケットを処理し、処理の一部として、パケットの宛先に基づいて、VCN104に関連する特定のゲートウェイをパケットのネクストホップとして決定する。その後、VCN VR105は、パケットを特定のゲートウェイに転送することができる。例えば、宛先が顧客のオプレンスネットワーク内のエンドポイントである場合、パケットは、VCN VR105によって、VCN104のために構成された動的ルーティングゲートウェイ（DRG）122に転送されてもよい。その後、パケットは、ゲートウェイからネクストホップに転送され、意図した最終の宛先へのパケットの通信を容易にすることができる。

【0053】

VCNのために様々な異なる種類のゲートウェイを構成してもよい。VCNのために構成され得るゲートウェイの例は、図1に示され、以下に説明される。VCNに関連するゲートウェイの例は、図17、18、19および20（例えば、参照番号1734、1736、1738、1834、1836、1838、1934、1936、1938、2034、2036、および2038によって示されたゲートウェイ）にも示され、以下に説明される。図1に示された実施形態に示されるように、動的ルーティングゲートウェイ（DRG）122は、顧客VCN104に追加されてもよく、またはそれに関連付けられてもよい。DRG122は、顧客VCN104と別のエンドポイントとの間のプライベートネットワークトラフィック通信を行うための経路を提供する。別のエンドポイントは、顧客オンプレミスネットワーク116、CSP101の異なる地域内のVCN108、またはCSP101によってホストされていない他のリモートクラウドネットワーク118であってもよい。顧客オンプレミスネットワーク116は、顧客のリソースを用いて構築された顧客ネットワークまたは顧客データセンタであってもよい。顧客オンプレミスネットワーク116へのアクセスは、一般的に厳しく制限される。顧客オンプレミスネットワーク116と、CSP101によってクラウドに展開またはホストされる1つ以上のVCN104との両方を有する顧客の場合、顧客は、オンプレミスネットワーク116およびクラウドベースのVCN104が互いに通信できることを望む場合がある。これによって、顧客は、CSP101によってホストされている顧客のVCN104とオンプレミスネットワーク116とを含む拡張ハイブリッド環境を構築することができる。DRG1

22は、このような通信を可能にする。このような通信を可能にするために、通信チャネル124が設定される。この場合、通信チャネルの一方のエンドポイントは、顧客オンプレミスネットワーク116にあり、他方のエンドポイントは、CSP101にあり、顧客VCN104に接続されている。通信チャネル124は、インターネットなどのパブリック通信ネットワーク、またはプライベート通信ネットワークを経由することができる。インターネットなどのパブリック通信ネットワーク上のIPsecVPN技術、パブリックネットワークの代わりにプライベートネットワークを使用するオラクル（登録商標）のFastConnect技術などの様々な異なる通信プロトコルを使用することができる。通信チャネル124の1つのエンドポイントを形成する顧客オンプレミスネットワーク116内の装置または機器は、図1に示されたCPE126などの顧客構内機器（CPE）と呼ばれる。CSP101側のエンドポイントは、DRG122を実行するホストマシンであってもよい。

10

【0054】

特定の実施形態において、リモートピアリング接続（RPC）をDRGに追加することができる。これによって、顧客は、1つのVCNを別の地域内の別のVCNとピアリングすることができる。このようなRPCを使用して、顧客VCN104は、DRG122を使用して、別の地域内のVCN108に接続することができる。また、DRG122は、CSP101によってホストされていない他のリモートクラウドネットワーク118、例えば、マイクロソフト（登録商標）Azureクラウド、アマゾン（登録商標）AWSクラウドと通信するために使用されてもよい。

20

【0055】

図1に示すように、顧客VCN104上の計算インスタンスがインターネットなどのパブリックネットワークを介してアクセス可能なパブリックエンドポイント114と通信することを可能にするように、顧客VCN104にインターネットゲートウェイ（IGW）120を構成することができる。IGW120は、VCNをインターネットなどのパブリックネットワークに接続するためのゲートウェイである。IGW120は、VCN104などのVCN内のパブリックサブネット（パブリックサブネット内のリソースは、パブリックオーバーレイIPアドレスを有する）がインターネットなどのパブリックネットワーク114上のパブリックエンドポイント112に直接アクセスすることを可能にする。IGW120を使用して、VCN104内のサブネットからまたはインターネットからの接続を開始することができる。

30

【0056】

顧客VCN104にネットワークアドレス変換（NAT）ゲートウェイ128を構成することができる。NATゲートウェイ128は、顧客VCN内の専用のパブリックオーバーレイIPアドレスを有しないクラウドリソースを、直接着信インターネット接続（例えば、L4-L7接続）に曝すことなくインターネットにアクセスすることを可能にする。これによって、VCN104のプライベートサブネット1などのVCN内のプライベートサブネットがインターネット上のパブリックエンドポイントにプライベートアクセスすることを可能にする。NATゲートウェイにおいて、プライベートサブネットからパブリックインターネットに接続を開始することができるが、インターネットからプライベートサブネットに接続を開始することができない。

40

【0057】

特定の実施形態において、顧客VCN104にサービスゲートウェイ（SGW）126を構成することができる。SGW126は、VCN104とサービスネットワーク110にサポートされているサービスエンドポイントとの間のプライベートネットワークトラフィックの経路を提供する。特定の実施形態において、サービスネットワーク110は、CSPによって提供されてもよく、様々なサービスを提供することができる。このようなサービスネットワークの例は、顧客が使用できる様々なサービスを提供するオラクル（登録商標）サービスネットワークである。例えば、顧客VCN104のプライベートサブネット内の計算インスタンス（例えば、データベースシステム）は、パブリックIPアドレス

50

またはインターネットへのアクセスを必要とすることなく、サービスエンドポイント（例えば、オブジェクト記憶装置）にデータをバックアップすることができる。いくつかの実施形態において、V C Nは、1つのみのS G Wを有することができ、V C N内のサブネットのみから接続を開始することができ、サービスネットワーク110から接続を開始することができない。V C Nを他のV C Nにピアリングする場合、他のV C N内のリソースは、通常S G Wにアクセスすることができない。FastConnectまたはVPN ConnectでV C Nに接続されているオンプレミスネットワーク内のリソースも、そのV C Nに構成されたサービスゲートウェイを使用することができる。

【0058】

いくつかの実装形態において、S G W126は、サービスクラスレスドメイン間ルーティング（C I D R）ラベルを使用する。C I D Rラベルは、関心のあるサービスまたはサービスのグループに対する全ての地域公開I Pアドレス範囲を表す文字列である。顧客は、S G Wおよび関連するルーティングルールを設定する際に、サービスC I D Rラベルを使用してサービスへのトラフィックを制御する。顧客は、サービスのパブリックI Pアドレスが将来に変化する場合、セキュリティルールを調整する必要なく、セキュリティルールを設定するときにオプションとしてサービスC I D Rラベルを使用することができる。

【0059】

ローカルピアリングゲートウェイ（L P G）132は、顧客V C N104に追加可能なゲートウェイであり、V C N104が同じ地域内の別のV C Nとピアリングすることを可能にするものである。ピアリングとは、トラフィックがインターネットなどのパブリックネットワークを経由することなく、または顧客オンプレミスネットワーク116を通してトラフィックをルーティングすることなく、V C NがプライベートI Pアドレスを使用して通信することを意味する。好ましい実施形態において、V C Nは、確立した各ピアリングに対して個別のL P Gを有する。ローカルピアリングまたはV C Nピアリングは、異なるアプリケーション間またはインフラストラクチャ管理機能間のネットワーク接続を確立するために使用される一般的な慣行である。

【0060】

サービスネットワーク110のサービスのプロバイダなどのサービスプロバイダは、異なるアクセスモデルを使用してサービスへのアクセスを提供することができる。パブリックアクセスモデルによれば、サービスは、インターネットなどのパブリックネットワークを介して顧客V C N内の計算インスタンスによって公的にアクセス可能なパブリックエンドポイントとして公開されてもよく、またはS G W126を介してプライベートにアクセスされてもよい。特定のプライベートアクセスモデルによれば、サービスは、顧客V C N内のプライベートサブネット内のプライベートI Pエンドポイントとしてアクセスされてもよい。これは、プライベートエンドポイント（P E）アクセスと呼ばれ、サービスプロバイダがそのサービスを顧客のプライベートネットワーク内のインスタンスとして公開することを可能にする。プライベートエンドポイントリソースは、顧客V C N内のサービスを表す。各P Eは、顧客が顧客V C N内のサブネットから選択したV N I C（P E - V N I Cと呼ばれ、1つまたは複数のプライベートI Pを持つ）として現れる。従って、P Eは、V N I Cを使用して顧客のプライベートV C Nサブネット内でサービスを提供する方法を提供する。エンドポイントがV N I Cとして公開されるため、P E V N I Cは、V N I Cに関連する全ての機能、例えば、ルーティングルールおよびセキュリティリストなどを利用することができる。

【0061】

サービスプロバイダは、サービスを登録することによって、P Eを介したアクセスを可能にする。プロバイダは、顧客テナントへのサービスの表示を規制するポリシーをサービスに関連付けることができる。プロバイダは、特にマルチテナントサービスの場合、単一の仮想I Pアドレス（V I P）の下に複数のサービスを登録することができる。（複数のV C Nにおいて）同じサービスを表すプライベートエンドポイントが複数存在する場合もある。

10

20

30

40

50

【0062】

その後、プライベートサブネット内の計算インスタンスは、PE VNICのプライベートIPアドレスまたはサービスDNS名を用いて、サービスにアクセスすることができる。顧客VCN内の計算インスタンスは、顧客VCN内のPEのプライベートIPアドレスにトラフィックを送信することによって、サービスにアクセスすることができる。プライベートアクセスゲートウェイ(PAGW)130は、顧客サブネットプライベートエンドポイントから／への全てのトラフィックの受信ポイント／送信ポイントとして機能するサービスプロバイダVCN(例えば、サービスネットワーク110内のVCN)に接続できるゲートウェイリソースである。PAGW130によって、プロバイダは、内部IPアドレスリソースを利用することなく、PE接続の数を拡張することができる。プロバイダは、単一のVCNに登録された任意の数のサービスに対して1つのPAGWを設定するだけでよい。プロバイダは、1人以上の顧客の複数のVCNにおいて、サービスをプライベートエンドポイントとして示すことができる。顧客の観点から、PE VNICは、顧客のインスタンスに接続されているのではなく、顧客が対話したいサービスに接続されているように見える。プライベートエンドポイントに向けられたトラフィックは、PAGW130を介してサービスにルーティングされる。これらは、顧客対サービスプライベート接続(C2S接続)と呼ばれる。

10

【0063】

また、PE概念を用いて、トラフィックがFastConnect/IPsecリンクおよび顧客VCN内のプライベートエンドポイントを通して流れることを可能にすることで、サービスのプライベートアクセスを顧客オンプレミスネットワークおよびデータセンタに拡張することもできる。また、トラフィックがLPG132および顧客VCN内のPE間を通して流れることを可能にすることで、サービスのプライベートアクセスを顧客ピアリングVCNに拡張することもできる。

20

【0064】

顧客は、サブネットレベルでVCNのルーティングを制御することができるため、VCN104などの顧客VCNにおいて各ゲートウェイを使用するサブネットを指定することができる。VCNのルートテーブルを用いて、特定のゲートウェイを介してトラフィックをVCNの外部にルーティングできるか否かを判断することができる。例えば、特定の事例において、顧客VCN104内のパブリックサブネットのルートテーブルは、IGW120を介して非ローカルトラフィックを送信することができる。同じ顧客VCN104内のプライベートサブネットのルートテーブルは、SGW126を介してCSPサービスへのトラフィックを送信することができる。残りの全てのトラフィックは、NATゲートウェイ128を介して送信されてもよい。ルートテーブルは、VCNから出るトラフィックのみを制御する。

30

【0065】

VCNに関連するセキュリティリストは、インバウンド接続およびゲートウェイを介してVCNに入来するトラフィックを制御するために使用される。サブネット内の全てのリソースは、同じミュータブルおよびセキュリティリストを使用する。セキュリティリストは、VCNのサブネット内のインスタンスに出入りする特定の種類のトラフィックを制御するために使用されてもよい。セキュリティリストルールは、受信(インバウンド)ルールと、送信(アウトバウンド)ルールとを含んでもよい。例えば、受信ルールは、許可された送信元アドレス範囲を指定することができ、送信ルールは、許可された宛先アドレス範囲を指定することができる。セキュリティルールは、特定のプロトコル(例えば、TCP、ICMP)、特定のポート(例えば、SSHの場合ポート22、ウィンドウズ(登録商標)RDPの場合ポート3389)などを指定することができる。特定の実装形態において、インスタンスのオペレーティングシステムは、セキュリティリストルールと一致する独自のファイアウォールルールを実施することができる。ルールは、ステートフル(例えば、接続が追跡され、応答トラフィックに対する明示的なセキュリティのリストルールなしで応答が自動的に許可される)またはステートレスであってもよい。

40

50

【0066】

顧客VCN（すなわち、VCN104上に展開されたリソースまたは計算インスタンス）からのアクセスは、パブリックアクセス、プライベートアクセス、または専用アクセスとして分類されることができる。パブリックアクセスは、パブリックIPアドレスまたはNATを用いてパブリックエンドポイントにアクセスするためのアクセスモデルを指す。プライベートアクセスは、プライベートIPアドレス（例えば、プライベートサブネット内のリソース）を持つVCN104内の顧客ワークロードが、インターネットなどのパブリックネットワークを経由することなく、サービスにアクセスすることを可能にする。特定の実施形態において、CSP101は、プライベートIPアドレスを持つ顧客VCNワークロードが、サービスゲートウェイを使用して、サービスのパブリックサービスエンドポイントにアクセスすることを可能にする。したがって、サービスゲートウェイは、顧客VCNと顧客プライベートネットワークの外部に存在するサービスのパブリックエンドポイントとの間に仮想リンクを確立することによって、プライベートアクセスモデルを提供する。

10

【0067】

さらに、CSPは、FastConnectパブリックピアリングなどの技術を使用する専用パブリックアクセスを提供することができる。この場合、顧客オンプレミスインスタンスは、インターネットなどのパブリックネットワークを経由することなく、FastConnect接続を用いて顧客VCN内の1つ以上のサービスにアクセスすることができる。また、CSPは、FastConnectプライベートピアリングを使用する専用プライベートアクセスを提供することもできる。この場合、プライベートIPアドレスを持つ顧客オンプレミスインスタンスは、FastConnect接続を用いて顧客VCNワークロードにアクセスすることができる。FastConnectは、パブリックインターネットを用いて顧客オンプレミスネットワークをCSPおよびそのサービスに接続する代わりに使用されるネットワーク接続である。FastConnectは、インターネットベースの接続と比較して、より高い帯域幅オプションと信頼性の高い一貫したネットワーキング体験を持つ専用のプライベート接続を、簡単、柔軟且つ経済的に作成する方法を提供する。

20

【0068】

図1および上記の添付の説明は、例示的な仮想ネットワークにおける様々な仮想化要素を説明する。上述したように、仮想ネットワークは、基礎となる物理ネットワークまたは基板ネットワーク上に構築される。図2は、特定の実施形態に従って、仮想ネットワークの基盤を提供するCSP200内の物理ネットワーク内の物理要素を示す簡略化アーキテクチャ図である。図示のように、CSP200は、クラウドサービスプロバイダ（CSP）によって提供された要素およびリソース（例えば、計算リソース、メモリリソース、およびネットワーキングリソース）を含む分散環境を提供する。これらの要素およびリソースは、加入している顧客、すなわち、CSPによって提供された1つ以上のサービスに加入している顧客にクラウドサービス（例えば、IaaSサービス）を提供するために使用される。顧客が加入しているサービスに基づいて、CSP200は、一部のリソース（例えば、計算リソース、メモリリソース、およびネットワーキングリソース）を顧客に提供する。その後、顧客は、CSP200によって提供された物理的な計算リソース、メモリリソース、およびネットワーキングリソースを使用して、独自のクラウドベースの（すなわち、CSP101ホスト型）カスタマイズ可能なプライベート仮想ネットワークを構築することができる。前述したように、これらの顧客ネットワークは、仮想クラウドネットワーク（VCN）と呼ばれる。顧客は、これらの顧客VCNに、計算インスタンスなどの1つ以上の顧客リソースを展開することができる。計算インスタンスは、仮想マシン、ベアメタルインスタンスなどであってもよい。CSP200は、顧客が高可用性のホスト環境において広範なアプリケーションおよびサービスを構築および実行することを可能にする、インフラストラクチャおよび一連の補完的なクラウドサービスを提供する。

30

40

【0069】

図2に示す例示的な実施形態において、CSP200の物理要素は、1つ以上の物理

50

ホストマシンまたは物理サーバ（例えば、202、206、208）、ネットワーク仮想化デバイス（NVD）（例えば、210、212）、トップオブブラック（TOR）スイッチ（例えば、214、216）、物理ネットワーク（例えば、218）、および物理ネットワーク218内のスイッチを含む。物理ホストマシンまたはサーバは、VCNの1つ以上のサブネットに参加している様々な計算インスタンスをホストし、実行することができる。計算インスタンスは、仮想マシンインスタンスおよびベアメタルインスタンスを含んでもよい。例えば、図1に示された様々な計算インスタンスは、図2に示された物理的ホストマシンによってホストされてもよい。VCN内の仮想マシン計算インスタンスは、1つのホストマシンによって実行されてもよく、または複数の異なるホストマシンによって実行されてもよい。また、物理ホストマシンは、仮想ホストマシン、コンテナベースのホストまたは機能などをホストすることができる。図1に示されたVICおよびVCN VRは、図2に示されたFTVDによって実行されてもよい。図1に示されたゲートウェイは、図2に示されたホストマシンおよび／またはNVDによって実行されてもよい。

10

【0070】

ホストマシンまたはサーバは、ホストマシン上で仮想化環境を作成するおよび可能にするハイパーバイザ（仮想マシンモニタまたはVMMとも呼ばれる）を実行することができる。仮想化または仮想化環境は、クラウドベースコンピューティングを容易にする。1つ以上の計算インスタンスは、ホストマシン上のハイパーバイザによって、ホストマシン上で作成され、実行され、管理されてもよい。ホストマシン上のハイパーバイザは、ホストマシンの物理的な計算リソース（例えば、計算リソース、メモリリソース、およびネットワークリソース）をホストマシン上で実行される様々な計算インスタンス間で共有させることができる。

20

【0071】

例えば、図2に示すように、ホストマシン202および208は、ハイパーバイザ260および266をそれぞれ実行する。これらのハイパーバイザは、ソフトウェア、ファームウェア、ハードウェア、またはそれらの組み合わせを使用して実装されてもよい。典型的には、ハイパーバイザは、ホストマシンのオペレーティングシステム（OS）に常駐するプロセスまたはソフトウェア層であり、OSは、ホストマシンのハードウェアプロセッサ上で実行される。ハイパーバイザは、ホストマシンの物理的な計算リソース（例えば、プロセッサ／コア、メモリリソース、ネットワークリソースなどの処理リソース）を、ホストマシンによって実行される様々な仮想マシン計算インスタンスの間で共有させる仮想化環境を提供する。例えば、図2において、ハイパーバイザ260は、ホストマシン202のOSに常駐し、ホストマシン202の計算リソース（例えば、処理リソース、メモリリソース、およびネットワークリソース）を、ホストマシン202によって実行されるコンピューティングインスタンス（例えば、仮想マシン）間で共有させることができる。仮想マシンは、独自のOS（ゲストOSと呼ばれる）を持つことができる。このゲストOSは、ホストマシンのOSと同じであってもよく、異なってもよい。ホストマシンによって実行される仮想マシンのOSは、同じホストマシンによって実行される他の仮想マシンのOSと同じであってもよく、異なってもよい。したがって、ハイパーバイザは、ホストマシンの同じ計算リソースを共有させながら、複数のOSを並行して実行することができる。図2に示されたホストマシンは、同じ種類のハイパーバイザを有してもよく、異なる種類のハイパーバイザを有してもよい。

30

40

【0072】

計算インスタンスは、仮想マシンインスタンスまたはベアメタルインスタンスであってもよい。図2において、ホストマシン202上の計算インスタンス268およびホストマシン208上の計算インスタンス274は、仮想マシンインスタンスの一例である。ホストマシン206は、顧客に提供されるベアメタルインスタンスの一例である。

【0073】

特定の例において、ホストマシンの全体は、単一の顧客に提供されてもよく、そのホストマシンによってホストされている1つ以上の計算インスタンス（仮想マシンまたはベア

50

メタルインスタンスのいずれか)は、全て同じ顧客に属してもよい。他の例において、ホストマシンは、複数の顧客(すなわち、複数のテナント)間で共有されてもよい。このようなマルチテナントシナリオにおいて、ホストマシンは、異なる顧客に属する仮想マシン計算インスタンスをホストすることができる。これらの計算インスタンスは、異なる顧客の異なるV C Nのメンバであってもよい。特定の実施形態において、ベアメタル計算インスタンスは、ハイパーバイザを設けていないベアメタルサーバによってホストされている。ベアメタル計算インスタンスが提供される場合、単一の顧客またはテナントは、ベアメタルインスタンスをホストするホストマシンの物理C P U、メモリ、およびネットワークインターフェースの制御を維持し、ホストマシンは、他の顧客またはテナントに共有されない。

10

【0074】

前述したように、V C Nの一部である各計算インスタンスは、計算インスタンスがV C Nのサブネットのメンバになることを可能にするV N I Cに関連付けられる。計算インスタンスに関連付けられたV N I Cは、計算インスタンスとの間のパケットまたはフレームの通信を容易にする。V N I Cは、計算インスタンスが作成されるときに当該計算インスタンスに関連付けられる。特定の実施形態において、ホストマシンによって実行される計算インスタンスについて、その計算インスタンスに関連付けられたV N I Cは、ホストマシンに接続されたN V Dによって実行される。例えば、図2において、ホストマシン202は、V N I C 276に関連付けられた仮想マシン計算インスタンス268を実行し、V N I C 276は、ホストマシン202に接続されたN V D 210によって実行される。別の例として、ホストマシン206によってホストされているベアメタルインスタンス272は、ホストマシン206に接続されたN V D 212によって実行されるV N I C 280に関連付けられる。さらに別の例として、V N I C 284は、ホストマシン208によって実行される計算インスタンス274に関連付けられ、V N I C 284は、ホストマシン208に接続されているN V D 212によって実行される。

20

【0075】

ホストマシンによってホストされている計算インスタンスについて、そのホストマシンに接続されたN V Dは、計算インスタンスがメンバであるV C Nに対応するV C N V Rを実行する。例えば、図2に示された実施形態において、N V D 210は、計算インスタンス268がメンバであるV C Nに対応するV C N V R 277を実行する。また、N V D 212は、ホストマシン206および208によってホストされている計算インスタンスに対応するV C Nに対応する1つ以上のV C N V R 283を実行することができる。

30

【0076】

ホストマシンは、当該ホストマシンを他の装置に接続するための1つ以上のネットワークインターフェイスカード(N I C)を含むことができる。ホストマシン上のN I Cは、ホストマシンを別の装置に通信可能に接続するための1つ以上のポート(またはインターフェイス)を提供することができる。例えば、ホストマシンおよびN V Dに設けられた1つ以上のポート(またはインターフェイス)を用いて、当該ホストマシンを当該N V Dに接続することができる。また、ホストマシンを他のホストマシンなどの他の装置に接続することもできる。

40

【0077】

例えば、図2において、ホストマシン202は、ホストマシン202のN I C 232によって提供されるポート234とN V D 210のポート236との間に延在するリンク220を使用してN V D 210に接続されている。ホストマシン206は、ホストマシン206のN I C 244によって提供されるポート246とN V D 212のポート248との間に延在するリンク224を使用してN V D 212に接続されている。ホストマシン208は、ホストマシン208のN I C 250によって提供されるポート252とN V D 212のポート254との間に延在するリンク226を使用してN V D 212に接続されている。

【0078】

50

同様に、NVDは、通信リンクを介して、（スイッチファブリックとも呼ばれる）物理ネットワーク218に接続されているトップオブラック（TOR）スイッチに接続されている。特定の実施形態において、ホストマシンとNVDとの間のリンクおよびNVDとTORスイッチとの間のリンクは、イーサネット（登録商標）リンクである。例えば、図2において、NVD210および212は、リンク228および230を介して、TORスイッチ214および216にそれぞれ接続される。特定の実施形態において、リンク220、224、226、228、および230は、イーサネット（登録商標）リンクである。TORに接続されているホストマシンおよびNVDの集合体は、ラックと呼ばれることがある。

【0079】

物理ネットワーク218は、TORスイッチの相互通信を可能にする通信ファブリックを提供する。物理ネットワーク218は、多層ネットワークであってもよい。特定の装形態において、物理ネットワーク218は、スイッチの多層Closネットワークであり、TORスイッチ214および216は、多層およびマルチノード物理スイッチングネットワーク218のリーフレベルノードを表す。2層ネットワーク、3層ネットワーク、4層ネットワーク、5層ネットワーク、および一般に「n」層ネットワークを含むがこれらに限定されない異なるClosネットワーク構成は、可能である。Closネットワークの一例は、図5に示され、以下に説明される。

【0080】

ホストマシンとN個のVDとの間には、1対1構成、多対1構成、および1対多構成などの様々な異なる接続構成が可能である。1対1構成の実装例において、各ホストマシンは、それ自体の別個のNVDに接続されている。例えば、図2において、ホストマシン202は、ホストマシン202のNIC232を介してNVD210に接続されている。多対1の構成において、複数のホストマシンは、1つのNVDに接続されている。例えば、図2において、ホストマシン206および208は、それぞれNIC244および250を介して同じNVD212に接続されている。

【0081】

1対多の構成において、1つのホストマシンは、複数のNVDに接続されている。図3は、ホストマシンが複数のNVDに接続されているCSPi300内の一例を示す。図3に示すように、ホストマシン302は、複数のポート306および308を含むネットワークインターフェースカード（NIC）304を備える。ホストマシン302は、ポート306およびリンク320を介して第1のNVD310に接続され、ポート308およびリンク322を介して第2のNVD312に接続されている。ポート306および308は、イーサネット（登録商標）ポートであってもよく、ホストマシン302とNVD310および312との間のリンク320および322は、イーサネット（登録商標）リンクであってもよい。NVD310は、第1のTORスイッチ314に接続され、NVD312は、第2のTORスイッチ316に接続されている。NVD310および312とTORスイッチ314および316との間のリンクは、イーサネット（登録商標）リンクであってもよい。TORスイッチ314および316は、多層物理ネットワーク318内の層-0スイッチング装置を表す。

【0082】

図3に示す構成は、物理スイッチネットワーク318からホストマシン302への2つの別々の物理ネットワーク経路、すなわち、TORスイッチ314からNVD310を経由してホストマシン302への第1の経路と、TORスイッチ316からNVD312を経由してホストマシン302への第2の経路とを提供する。別々の経路は、ホストマシン302の強化された可用性（高可用性と呼ばれる）を提供する。経路の一方に問題がある（例えば、経路の一方のリンクが故障する）場合または装置に問題がある（例えば、特定のNVDが機能していない）場合、ホストマシン302との間の通信に他方の経路を使用することができる。

【0083】

10

20

30

40

50

図 3 に示された構成において、ホストマシンは、ホストマシンの N I C によって提供された 2 つの異なるポートを用いて 2 つの異なる N V D に接続されている。他の実施形態において、ホストマシンは、ホストマシンと複数の N V D との接続を可能にする複数の N I C を含んでもよい。

【 0 0 8 4 】

再び図 2 を参照して、N V D は、1 つ以上のネットワーク仮想化機能および／または記憶仮想化機能を実行する物理装置または要素である。N V D は、1 つ以上の処理ユニット（例えば、C P U、ネットワーク処理ユニット（N P U）、F P G A、パケット処理パイプライン）、キャッシュを含むメモリ、およびポートを有する任意の装置であってもよい。様々な仮想化機能は、N V D の 1 つ以上の処理ユニットによって実行されるソフトウェア／ファームウェアによって実行されてもよい。

10

【 0 0 8 5 】

N V D は、様々な異なる形で実装されてもよい。例えば、特定の実施形態において、N V D は、内蔵プロセッサを搭載したスマート N I C またはインテリジェント N I C と呼ばれるインターフェイスカードとして実装される。スマート N I C は、ホストマシン上の N I C とは別個の装置である。図 2 において、N V D 2 1 0 は、ホストマシン 2 0 2 に接続されているスマート N I C として実装されてもよく、N V D 2 1 2 は、ホストマシン 2 0 6 および 2 0 8 に接続されているスマート N I C として実装されてもよい。

【 0 0 8 6 】

しかしながら、スマート N I C は、N V D 実装の一例にすぎない。様々な他の実装が可能である。例えば、いくつかの他の実装例において、N V D または N V D によって実行される 1 つ以上の機能は、C S P I 2 0 0 の 1 つ以上のホストマシン、1 つ以上の T O R スイッチ、および他の要素に組み込まれてもよく、またはそれらによって実行されてもよい。例えば、N V D は、ホストマシンに統合されてもよい。この場合、N V D によって実行される機能は、ホストマシンによって実行される。別の例として、N V D は、T O R スイッチの一部であってもよく、または T O R スイッチは、T O R スイッチがパブリッククラウドに使用される様々な複雑なパケット変換を実行することを可能にする N V D によって実行される機能を実行するように構成されてもよい。N V D の機能を実行する T O R は、スマート T O R と呼ばれることがある。ベアメタル（B M）インスタンスではなく仮想マシン（V M）インスタンスを顧客に提供するさらに他の実装形態において、N V D によって提供される機能は、ホストマシンのハイパーバイザの内部に実装されてもよい。いくつかの他の実装形態において、N V D の機能の一部は、一組のホストマシン上で動作する集中型サービスにオフロードされてもよい。

20

30

【 0 0 8 7 】

図 2 に示すように、スマート N I C として実装される場合などの特定の実施形態において、N V D は、当該 N V D を 1 つ以上のホストマシンおよび 1 つ以上の T O R スイッチに接続することを可能にする複数の物理ポートを備えてもよい。N V D 上のポートは、ホスト向きポート（「サウスポート」（south port）とも呼ばれる）またはネットワーク向きもしくは T O R 向きポート（「ノースポート」（north port）とも呼ばれる）に分類することができる。N V D のホスト向きポートは、N V D をホストマシンに接続するために使用されるポートである。図 2 においてホスト向きポートの例は、N V D 2 1 0 のポート 2 3 6、および N V D 2 1 2 のポート 2 4 8 および 2 5 4 を含む。N V D のネットワーク向きポートは、N V D を T O R スイッチに接続するために使用されるポートである。図 2 のネットワーク向きポートの例は、N V D 2 1 0 のポート 2 5 6、および N V D 2 1 2 のポート 2 5 8 を含む。図 2 に示すように、N V D 2 1 0 は、N V D 2 1 0 のポート 2 5 6 から T O R スイッチ 2 1 4 まで延びるリンク 2 2 8 を介して T O R スイッチ 2 1 4 に接続されている。同様に、N V D 2 1 2 は、N V D 2 1 2 のポート 2 5 8 から T O R スイッチ 2 1 6 まで延びるリンク 2 3 0 を介して T O R スイッチ 2 1 6 に接続されている。

40

【 0 0 8 8 】

N V D は、ホスト向きポートを介して、ホストマシンからパケットおよびフレーム（例

50

えば、ホストマシンによってホストされている計算インスタンスによって生成されたパケットおよびフレーム）を受信し、必要なパケット処理を実行した後、NVDのネットワーク向きポートを介してパケットおよびフレームをTORスイッチに転送することができる。NVDは、NVDのネットワーク向きポートを介してTORスイッチからパケットおよびフレームを受信し、必要なパケット処理を実行した後、NVDのホスト向きポートを介してパケットおよびフレームをホストマシンに転送することができる。

【0089】

特定の実施形態において、NVDとTORスイッチとの間に複数のポートおよび関連するリンクを設けてもよい。これらのポートおよびリンクを集約することによって、複数のポートまたはリンクのリンクアグリゲータグループ（LAGと称される）を形成することができる。リンクの集約は、2つのエンドポイント間（例えば、NVDとTORスイッチとの間）の複数の物理リンクを単一の論理リンクとして扱うことを可能にする。所定のLAG内の全ての物理リンクは、同じ速度で全二重モードで動作することができる。LAGは、2つのエンドポイント間の接続の帯域幅および信頼性を高めるのに役立つ。LAG内の物理リンクのうちの1つが故障した場合、トラフィックは、LAG内の別の物理リンクに動的かつ透過的に再割り当てられる。集約された物理リンクは、個々のリンクよりも高い帯域幅を提供する。LAGに関連付けられた複数のポートは、単一の論理ポートとして扱われる。トラフィックをLAGの複数の物理リンクに負荷分散することができる。2つのエンドポイント間に1つ以上のLAGを構成することができる。2つのエンドポイントは、例えば、NVDとTORスイッチとの間にあってもよく、ホストマシンとNVDとの間にあってもよい。

【0090】

NVDは、ネットワーク仮想化機能を実装または実行する。これらの機能は、NVDによって実行されるソフトウェア／ファームウェアによって実行される。ネットワーク仮想化機能の例は、限定されないが、パケットのカプセル化およびカプセル解除機能、VCNネットワークを作成するための機能、VCNセキュリティリスト（ファイアウォール）機能などのネットワークポリシーを実装するための機能、VCN内の計算インスタンスとの間のパケットのルーティングおよび転送を容易にするための機能などを含む。特定の実施形態において、パケットを受信すると、NVDは、パケットを処理し、パケットをどのように転送またはルーティングするかを判断するパケット処理パイプラインを実行するように構成されている。このパケット処理パイプラインの一部として、NVDは、VCN内のシス（cis）に関連するVNICの実行、VCNに関連する仮想ルータ（VR）の実行、仮想ネットワーク内の転送またはルーティングを容易にするためのパケットのカプセル化およびカプセル解除、特定のゲートウェイ（例えば、ローカルピアリングゲートウェイ）の実行、セキュリティリストの実装、ネットワークセキュリティグループ、ネットワークアドレス変換（NAT）機能（例えば、ホスト毎にパブリックIPからプライベートIPへの変換）、スロットリング機能、および他の機能を提供する。

【0091】

いくつかの実施形態において、NVDにおけるパケット処理データ経路は、複数のパケットパイプラインを含んでもよい。各々のパケットパイプラインは、一連のパケット変換ステージから構成される。いくつかの実装形態において、パケットを受信すると、当該パケットは、解析され、単一のパイプラインに分類される。次いで、パケットは、破棄されるまたはNVDのインターフェースを介して送出されるまで、線形方式でステージ毎に処理される。これらのステージは、基本機能のパケット処理ビルディングブロック（例えば、ヘッダの検証、スロットルの実行、新しいレイヤ2ヘッダの挿入、L4ファイアウォールの実行、VCNカプセル化／カプセル解除）を提供し、その結果、既存のステージを組み立てることによって新しいパイプラインを構築することができ、新しいステージを作成して既存のパイプラインに挿入することによって新しい機能を追加することができる。

【0092】

NVDは、VCNの制御プレーンおよびデータプレーンに対応する制御プレーン機能お

10

20

30

40

50

よびデータプレーン機能の両方を実行することができる。VCN制御プレーンの例は、図17、18、19および20（参照番号1716、1816、1916および2016参照）に示され、以下に説明される。VCNデータプレーンの例は、図17、18、19および20（参照番号1718、1818、1918および2018参照）に示され、以下に説明される。制御プレーン機能は、データをどのように転送するかを制御するためのネットワークの構成（例えば、ルートおよびルートテーブルの設定、VNICの構成）に使用される機能を含む。特定の実施形態において、全てのオーバーレイと基板とのマッピングを集中的に計算し、NVDおよび仮想ネットワークエッジ装置（例えば、DRG、SGW、IGWなどの様々なゲートウェイ）に公開するVCN制御プレーンが提供される。また、同じメカニズムを使用してファイアウォールルールを公開することができる。特定の
10 実施形態において、NVDは、当該NVDに関連するマッピングのみを取得する。データプレーン機能は、制御プレーンを使用して設定された構成に基づいて、パケットの実際のルーティング／転送を行う機能を含む。VCNデータプレーンは、顧客のネットワークパケットが基幹ネットワークを通過する前に、当該ネットワークパケットをカプセル化することによって実装される。カプセル化／カプセル解除機能は、NVDに実装される。特定の
20 実施形態において、NVDは、ホストマシンに出入りする全てのネットワークパケットを傍受し、ネットワーク仮想化機能を実行するように構成されている。

【0093】

上述したように、NVDは、VNICおよびVCN VRを含む様々な仮想化機能を実行する。NVDは、VNICに接続された1つ以上のホストマシンによってホストされて
20 いる計算インスタンスに関連するVNICを実行することができる。例えば、図2に示すように、NVD210は、NVD210に接続されたホストマシン202によってホストされている計算インスタンス268に関連するVNIC276の機能を実行する。別の例として、NVD212は、ホストマシン206によってホストされているベアメタル計算インスタンス272に関連するVNIC280を実行し、ホストマシン208によってホストされている計算インスタンス274に関連するVNIC284を実行する。ホストマシンは、異なる顧客に属する異なるVCNに属する計算インスタンスをホストすることができる。ホストマシンに接続されたNVDは、計算インスタンスに対応するVNICを実行する（すなわち、VNICに関連する機能を実行する）ことができる。

【0094】

また、NVDは、計算インスタンスのVCNに対応するVCN仮想ルータを実行する。例えば、図2に示された実施形態において、NVD210は、計算インスタンス268が属するVCNに対応するVCN VR277を実行する。NVD212は、ホストマシン206および208にホストされている計算インスタンスが属する1つ以上のVCNに対応する1つ以上のVCN VR283を実行する。特定の実施形態において、VCNに対応するVCN VRは、そのVCNに属する少なくとも1つの計算インスタンスをホストするホストマシンに接続された全てのNVDによって実行される。ホストマシンが異なるVCNに属する計算インスタンスをホストする場合、そのホストマシンに接続されたNVDは、異なるVCNに対応するVCN VRを実行することができる。

【0095】

VNICおよびVCN VRに加えて、NVDは、様々なソフトウェア（例えば、デーモン）を実行し、NVDによって実行される様々なネットワーク仮想化機能を容易にする1つ以上のハードウェア要素を含むことができる。簡略化のために、これらの様々な要素は、図2に示す「パケット処理要素」としてグループ化される。例えば、NVD210は、パケット処理要素286を含み、NVD212は、パケット処理要素288を含む。例えば、NVDのパケット処理要素は、NVDのポートおよびハードワーキングインターフェイスと相互作用することによって、NVDを使用して受信され、通信される全てのパケットを監視し、ネットワーク情報を記憶するように構成されたパケットプロセッサを含んでもよい。ネットワーク情報は、例えば、NVDによって処理される異なるネットワークフローを特定するためのネットワークフロー情報および各フローの情報（例えば、各フロ
40
50

一の統計情報)を含んでもよい。特定の実施形態において、ネットワークフロー情報は、VNIC単位で記憶されてもよい。別の例として、パケット処理要素は、NVDによって記憶された情報を1つ以上の異なる複製ターゲットストアに複製するように構成された複製エージェント(replication agent)を含むことができる。さらに別の例として、パケット処理要素は、NVDのロギング機能を実行するように構成されたロギングエージェント(logging agent)を含んでもよい。また、パケット処理要素は、NVDの性能および健全性を監視し、場合によっては、NVDに接続されている他の要素の状態および健全性を監視するためのソフトウェアを含んでもよい。

【0096】

図1は、VCNと、VCN内のサブネットと、サブネット上に展開された計算インスタンスと、計算インスタンスに関連付けられたVNICと、VCNのVRと、VCNのために構成された一組のゲートウェイを含む例示的な仮想またはオーバーレイネットワークの要素を示す。図1に示されたオーバーレイ要素は、図2に示された物理的要素のうちの1つ以上によって実行またはホストされてもよい。例えば、VCN内の計算インスタンスは、図2に示された1つ以上のホストマシンによって実行またはホストされてもよい。ホストマシンによってホストされている計算インスタンスの場合、その計算インスタンスに関連するVNICは、典型的には、そのホストマシンに接続されたNVDによって実行される(すなわち、VNIC機能は、そのホストマシンに接続されたNVDによって提供される)。VCNのVCN VR機能は、そのVCNの一部である計算インスタンスをホストまたは実行するホストマシンに接続されている全てのNVDによって実行される。VCNに関連するゲートウェイは、1つ以上の異なる種類のNVDによって実行されてもよい。例えば、いくつかのゲートウェイは、スマートNICによって実行されてもよく、他のゲートウェイは、1つ以上のホストマシンまたはNVDの他の実装形態によって実行されてもよい。

【0097】

上述したように、顧客VCN内の計算インスタンスは、様々な異なるエンドポイントと通信することができる。これらのエンドポイントは、送信元計算インスタンスと同じサブネットにあってはよく、異なるサブネット内であるが送信元計算インスタンスと同じVCNにあってはよく、または送信元計算インスタンスのVCN外部のエンドポイントを含んでもよい。これらの通信は、計算インスタンスに関連付けられたVNIC、VCN VR、およびVCNに関連付けられたゲートウェイを用いて促進される。

【0098】

VCN内の同じサブネット上の2つの計算インスタンス間の通信は、送信元計算インスタンスおよび宛先計算インスタンスに関連付けられたVNICを用いて促進される。送信元計算インスタンスおよび宛先計算インスタンスは、同じホストマシンによってホストされてもよく、異なるホストマシンによってホストされてもよい。送信元計算インスタンスから発信されたパケットは、送信元計算インスタンスをホストするホストマシンから、そのホストマシンに接続されたNVDに転送されてもよい。NVDにおいて、パケットは、パケット処理パイプラインを用いて処理され、このパイプラインは、送信元計算インスタンスに関連するVNICの実行を含むことができる。パケットの宛先エンドポイントが同じサブネットにあるため、送信元計算インスタンスに関連付けられたVNICの実行により、パケットは、宛先計算インスタンスに関連付けられたVNICを実行するNVDに転送され、NVDは、パケットを処理し、宛先計算インスタンスに転送する。送信元計算インスタンスおよび宛先計算インスタンスに関連するVNICは、(例えば、送信元計算インスタンスと宛先計算インスタンスの両方が同じホストマシンによってホストされている場合)同じNVD上で実行されてもよく、または(例えば、送信元計算インスタンスおよび宛先計算インスタンスが異なるNVDに接続された異なるホストマシンによってホストされている場合)異なるNVD上で実行されてもよい。VNICは、NVDによって記憶されたルーティング/転送テーブルを使用して、パケットのネクストホップを決定することができる。

10

20

30

40

50

【0099】

サブネット内の計算インスタンスから同じV C N内の異なるサブネット内のエンドポイントにパケットを通信する場合、送信元計算インスタンスから発信されたパケットは、送信元計算インスタンスをホストするホストマシンから、そのホストマシンに接続されたN V Dに通信される。N V Dにおいて、パケットは、1つ以上のV N I Cの実行を含むことができるパケット処理パイプラインおよびV C Nに関連するV Rを用いて処理される。例えば、N V Dは、パケット処理パイプラインの一部として、送信元計算インスタンスに関連するV N I Cに対応する機能を実行または呼び出す（V N I Cを実行するとも呼ばれる）。V N I Cによって実行される機能は、パケット上のV L A Nタグを調べることを含んでもよい。パケットの宛先がサブネットの外部にあるため、V C N V R機能は、呼び出され、N V Dによって実行される。その後、V C N V Rは、パケットを、宛先計算インスタンスに関連付けられたV N I Cを実行するN V Dにルーティングする。そして、宛先計算インスタンスに関連付けられたV N I Cは、パケットを処理し、パケットを宛先計算インスタンスに転送する。送信元計算インスタンスおよび宛先計算インスタンスに関連するV N I Cは、（例えば、送信元計算インスタンスと宛先計算インスタンスの両方が同じホストマシンによってホストされている場合）同じN V D上で実行されてもよく、（例えば、送信元計算インスタンスおよび宛先計算インスタンスが異なるN V Dに接続された異なるホストマシンによってホストされている場合）異なるN V D上で実行されてもよい。

10

【0100】

パケットの宛先が送信元計算インスタンスのV C Nの外部にある場合、送信元計算インスタンスから発信されたパケットは、送信元計算インスタンスをホストするホストマシンから、そのホストマシンに接続されたN V Dに通信される。N V Dは、送信元計算インスタンスに関連するV N I Cを実行する。パケットの宛先エンドポイントがV C Nの外部にあるため、パケットは、そのV C NのV C N V Rによって処理される。N V Dは、V C N V R機能呼び出し、その結果、パケットは、V C Nに関連付けられた適切なゲートウェイを実行するN V Dに転送される場合がある。例えば、宛先が顧客オンプレミスネットワーク内のエンドポイントである場合、パケットは、V C N V Rによって、V C Nのために構成されたD R Gゲートウェイを実行するN V Dに転送されてもよい。V C N V Rは、送信元計算インスタンスに関連するV N I Cを実行するN V Dと同じN V D上で実行されてもよく、異なるN V Dによって実行されてもよい。ゲートウェイは、スマートN I C、ホストマシン、または他のN V D実装であるN V Dによって実行されてもよい。次いで、パケットは、ゲートウェイによって処理され、意図した宛先エンドポイントへのパケットの通信を容易にするためのネクストホップに転送される。例えば、図2に示された実施形態において、計算インスタンス268から発信されたパケットは、（N I C232を用いて）リンク220を介してホストマシン202からN V D210に通信されてもよい。N V D210上のV N I C276は、送信元計算インスタンス268に関連するV N I Cであるため、呼び出される。V N I C276は、パケット内のカプセル化された情報を検査し、意図した宛先エンドポイントへのパケットの通信を容易にする目的でパケットを転送するためのネクストホップを決定し、決定したネクストホップにパケットを転送するように構成されている。

20

30

40

【0101】

V C N上に展開された計算インスタンスは、様々な異なるエンドポイントと通信することができる。これらのエンドポイントは、C S P I 200によってホストされているエンドポイントと、C S P I 200外部のエンドポイントとを含んでもよい。C S P I 200によってホストされているエンドポイントは、（顧客V C N、または顧客に属さないV C Nであり得る）同じV C Nまたは他のV C N内のインスタンスを含んでもよい。C S P I 200によってホストされているエンドポイント間の通信は、物理ネットワーク218を介して実行されてもよい。また、計算インスタンスは、C S P I 200によってホストされていないまたはC S P I 200の外部にあるエンドポイントと通信することもできる。これらのエンドポイントの例は、顧客オンプレミスネットワークまたはデータセンタ内の

50

エンドポイント、またはインターネットなどのパブリックネットワークを介してアクセス可能なパブリックエンドポイントを含む。C S P I 2 0 0 外部のエンドポイントとの通信は、様々な通信プロトコルを用いて、パブリックネットワーク（例えば、インターネット）（図 2 に図示せず）またはプライベートネットワーク（図 2 に図示せず）を介して実行されてもよい。

【0102】

図 2 に示された C S P I 2 0 0 のアーキテクチャは、単なる一例であり、限定することを意図していない。代替的な実施形態において、変形、代替、および修正が可能である。例えば、いくつかの実装形態において、C S P I 2 0 0 は、図 2 に示されたものよりも多いまたは少ないシステムまたは要素を有してもよく、2 つ以上のシステムを組み合わせてもよく、または異なるシステム構成または配置を有してもよい。図 2 に示されたシステム、サブシステム、および他の要素は、それぞれのシステムの 1 つ以上の処理ユニット（例えば、プロセッサ、コア）によって実行されるソフトウェア（例えば、コード、命令、プログラム）、ハードウェア、またはそれらの組み合わせで実装されてもよい。ソフトウェアは、非一時的な記憶媒体（例えば、メモリ装置）に記憶されてもよい。

10

【0103】

図 4 は、特定の实施形態に従って、マルチテナント機能をサポートするための I / O 仮想化を提供するためのホストマシンと N V D との間の接続を示す図である。図 4 に示すように、ホストマシン 4 0 2 は、仮想化環境を提供するハイパーバイザ 4 0 4 を実行する。ホストマシン 4 0 2 は、2 つの仮想マシンインスタンス、すなわち、顧客 / テナント # 1 に属する V M 1 4 0 6 と、顧客 / テナント # 2 に属する V M 2 4 0 8 とを実行する。ホストマシン 4 0 2 は、リンク 4 1 4 を介して N V D 4 1 2 に接続されている物理 N I C 4 1 0 を含む。計算インスタンスの各々は、N V D 4 1 2 によって実行される V N I C に接続されている。図 4 の実施形態において、V M 1 4 0 6 は、V N I C - V M 1 4 2 0 に接続され、V M 2 4 0 8 は、V N I C - V M 2 4 2 2 に接続されている。

20

【0104】

図 4 に示すように、N I C 4 1 0 は、2 つの論理 N I C、すなわち、論理 N I C A 4 1 6 および論理 N I C B 4 1 8 を含む。各仮想マシンは、それ自身の論理 N I C に接続され、それ自身の論理 N I C と共に動作するように構成される。例えば、V M 1 4 0 6 は、論理 N I C A 4 1 6 に接続され、V M 2 4 0 8 は、論理 N I C B 4 1 8 に接続されている。ホストマシン 4 0 2 が複数のテナントによって共有されている 1 つの物理 N I C 4 1 0 のみからなるにもかかわらず、論理 N I C により、各テナントの仮想マシンは、自分自身のホストマシンおよび N I C を所有していると信じている。

30

【0105】

特定の实施形態において、各論理 N I C には、それ自身の V L A N I D が割り当てられる。したがって、テナント # 1 の論理 N I C A 4 1 6 には特定の V L A N I D が割り当てられ、テナント # 2 の論理 N I C B 4 1 8 には別の V L A N I D が割り当てられる。V M 1 4 0 6 からパケットが通信されると、ハイパーバイザは、テナント # 1 に割り当てられたタグをパケットに取り付けた後、リンク 4 1 4 を介してパケットをホストマシン 4 0 2 から N V D 4 1 2 に通信する。同様に、V M 2 4 0 8 からパケットが通信されると、ハイパーバイザは、テナント # 2 に割り当てられたタグをパケットに取り付けた後、リンク 4 1 4 を介してパケットをホストマシン 4 0 2 から N V D 4 1 2 に通信する。したがって、ホストマシン 4 0 2 から N V D 4 1 2 に通信されたパケット 4 2 4 は、特定のテナントおよび関連する V M を識別する関連タグ 4 2 6 を有する。N V D 上でホストマシン 4 0 2 からパケット 4 2 4 を受信した場合、当該パケットに関連するタグ 4 2 6 を用いて、当該パケットが V N I C - V M 1 4 2 0 によって処理されるべきか、V N I C - V M 2 4 2 2 によって処理されるべきかを判断する。そして、パケットは、対応する V N I C によって処理される。図 4 に示された構成は、各テナントの計算インスタンスが、自分自身のホストマシンおよび N I C を所有していると信じることを可能にする。図 4 に示された構成は、マルチテナント機能をサポートするための I / O 仮想化を提供す

40

50

る。

【0106】

図5は、特定の実施形態に従って、物理ネットワーク500を示す概略ブロック図である。図5に示された実施形態は、Closネットワークとして構築される。Closネットワークは、高い二分割帯域幅および最大リソース利用率を維持しながら、接続冗長性を提供するように設計された特定の種類のネットワークトポロジである。Closネットワークは、一種の非ブロッキング、多段または多層スイッチングネットワークであり、段または層の数は、2、3、4、5などであってもよい。図5に示された実施形態は、層1、2および3を含む3層ネットワークである。TORスイッチ504は、Closネットワークの層-0スイッチを表す。1つ以上のNVDは、TORスイッチに接続されている。層-0スイッチは、物理ネットワークのエッジ装置とも呼ばれる。層-0スイッチは、リーフスイッチとも呼ばれる層-1スイッチに接続されている。図5に示された実施形態において、「n」個の層-0 TORスイッチは、「n」個の層-1スイッチに接続され、ポッドを形成する。ポッド内の各層-0スイッチは、ポッド内の全ての層-1スイッチに相互接続されるが、ポッド間のスイッチは、接続されない。特定の実装例において、2つのポッドは、ブロックと呼ばれる。各ブロックは、「n」個の層-2スイッチ（スパインスイッチとも呼ばれる）によってサービスを提供されるまたはそれに接続されている。物理ネットワークトポロジは、複数のブロックを含んでもよい。同様に、層-2スイッチは、「n」個の層-3スイッチ（スーパースパインスイッチとも呼ばれる）に接続されている。物理ネットワーク500を介したパケットの通信は、典型的には、1つ以上のレイヤ3通信プロトコルを使用して実行される。典型的には、TOR層を除く物理ネットワークの全ての層は、nウェイ冗長であり、したがって高い可用性を実現することができる。ポッドおよびブロックにポリシーを指定して、物理ネットワークのスイッチの相互可視性を制御することによって、物理ネットワークを拡張することができる。

【0107】

Closネットワークの特徴は、ある層-0スイッチから別の層-0スイッチに到達する（または、層-0スイッチに接続されたNVDから層-0スイッチに接続された別のNVDに到達する）最大ホップカウントが一定であることである。例えば、3層のClosネットワークにおいて、パケットが1つのNVDから別のNVDに到達するために最大7つのホップが必要とされる。この場合、送信元NVDおよびターゲットNVDは、Closネットワークのリーフ層に接続されている。同様に、4層のClosネットワークにおいて、パケットが1つのNVDから別のNVDに到達するために最大9つのホップが必要とされる。この場合、送信元NVDおよびターゲットNVDは、Closネットワークのリーフ層に接続されている。したがって、Closネットワークアーキテクチャは、データセンタ内およびデータセンタ間の通信に重要なネットワーク全体の遅延を一定に保つ。Closトポロジは、水平方向に拡張可能であり、コスト効率に優れている。各階層により多くのスイッチ（例えば、より多くのリーフスイッチおよびスパインスイッチ）を増設すること、および隣接する階層のスイッチ間にリンク数を増やすことによって、ネットワークの帯域幅／スループット容量を容易に増加させることができる。

【0108】

特定の実施形態において、CSP I内の各リソースには、クラウド識別子（CID）と呼ばれる固有識別子が割り当てられる。この識別子は、リソースの情報の一部として含まれる。この識別子を用いて、例えば、コンソールまたはAPIを介してリソースを管理することができる。CIDの例示的なシンタックスは、以下の通りである。

【0109】

ocid1.<RESOURCE TYPE>.<REALM>.[REGION].[FUTURE USE].<UNIQUE ID>である。式中、

「ocid1」は、CIDのバージョンを示す文字列である。

【0110】

「RESOURCE TYPE」は、リソースの種類（例えば、インスタンス、ボリューム、V

10

20

30

40

50

C N、サブネット、ユーザ、グループ)を表す。

【0111】

「REALM」は、リソースが存在する領域を表す。例示的な値として、「c 1」は、商業領域を表し、「c 2」は、政府クラウド領域を表し、または「c 3」は、連邦政府クラウド領域を表す。各領域は、独自のドメイン名を持つことができる。

【0112】

「REGION」は、リソースが属する地域を表す。地域がリソースに適用されない場合、この部分は空白であってもよい。

【0113】

「FUTURE USE」は、将来使用のために保留されていることを示す。

「UNIQUE ID」は、固有IDの部分である。このフォーマットは、リソースまたはサービスの種類によって異なる場合がある。

【0114】

B. 例示的なレイヤ2 V L A Nアーキテクチャ

このセクションでは、仮想化されたクラウド環境においてレイヤ2 ネットワーキング機能を提供するための技術を説明する。レイヤ2 機能は、仮想化されたクラウド環境によって提供されるレイヤ3 ネットワーキング機能に加えて、およびそれに関連して、提供される。特定の実施形態では、仮想レイヤ2 およびレイヤ3 機能は、Oracle Corporation が提供するOracle Cloud Infrastructure (OCI)によって提供される。

【0115】

レイヤ2 ネットワーク機能の導入後、このセクションでは、V L A Nのレイヤ2 実現を説明する。その後、ストーム制御を含むレイヤ2 V L A Nサービスについて説明する。

【0116】

序

企業顧客のオンプレミスアプリケーションをクラウドサービスプロバイダ(C S P)によって提供されるクラウド環境に移行させる企業顧客の数は、急速に増加し続けている。しかしながら、これらの顧客の多くは、クラウド環境に移行する道程が非常に多難であり得、顧客の既存のアプリケーションを、クラウド環境において動作可能にするために、再構築および再設計する必要があることを、すぐに認識する。これは、オンプレミス環境のために書かれたアプリケーションは、しばしば、監視、可用性、および規模に関して物理ネットワークの特徴に依存するからである。したがって、これらのオンプレミスアプリケーションは、クラウド環境において動作することができるようになる前に、再構築および再設計される必要がある。

【0117】

オンプレミスアプリケーションがクラウド環境に容易に移行できない理由はいくつかある。主な理由の1つは、現在のクラウド仮想ネットワークがO S Iモデルのレイヤ3、例えばIPレイヤで動作し、アプリケーションによって必要とされるレイヤ2 機能を提供しないことである。レイヤ3 ベースのルーティングまたは転送は、パケットのレイヤ3 ヘッダに含まれる情報に基づいて、たとえば、パケットのレイヤ3 ヘッダに含まれる宛先IPアドレスに基づいて、パケットがどこに(たとえば、どの顧客インスタンスに)送信されるべきかを判断することを含む。これを容易にするために、仮想化されたクラウドネットワーク内のIPアドレスの位置は、集中制御および編成システムまたはコントローラを介して判断される。これらは、例えば、仮想化されたクラウド環境内の顧客エンティティまたはリソースに関連付けられたIPアドレスを含んでもよい。

【0118】

多くの顧客は、現在のクラウド提供およびI a a Sサービスプロバイダによっては現在のところ対処されていない、レイヤ2 ネットワーキング能力に対する厳格な要件を有するアプリケーションを、顧客のオンプレミス環境において動作させている。例えば、トラフィックは、現在のクラウド提供であり、レイヤ3 ヘッダを使用するレイヤ3 プロトコルを使用してルーティングされ、アプリケーションによって必要とされるレイヤ2 機能はサポ

10

20

30

40

50

ートされない。これらのレイヤ2機能は、アドレス解決プロトコル（ARP）処理、メディアアクセス制御（MAC）アドレス学習、およびレイヤ2ブロードキャスト能力、レイヤ2（MACベースの）転送、レイヤ2ネットワーキング構築物などの機能を含み得る。本開示で説明されるように、仮想化されたクラウドネットワークにおいて、仮想化されたレイヤ2ネットワーキング機能を提供することによって、顧客は、いかなる実質的な再構築または再設計も必要とせず、今や、顧客のレガシーアプリケーションをクラウド環境にシームレスに移行させることができる。例えば、ここで説明される仮想化されたレイヤ2ネットワーキング能力は、そのようなアプリケーション（例えば、VMware vSphere, vCenter, vSAN および NSX-Tコンポーネント）が、オンプレミス環境で行われるようにレイヤ2で通信することを可能にする。これらのアプリケーションは、パブリッククラウドにおいて同じバージョンおよび構成を実行することが可能であり、それによって、顧客は、レガシーアプリケーションに関連付けられる既存の知識、ツール、およびプロセスを含むレガシーオンプレミスアプリケーションを使用することが可能になる。顧客は、（例えば、VMware ソフトウェア定義データセンター（SDDC）を使用して）自身のアプリケーションからネイティブクラウドサービスにアクセスすることもできる。

10

20

30

40

50

【0119】

別の例として、フェイルオーバーのためにレイヤ2ブロードキャストサポートを必要とするいくつかのレガシーオンプレミスアプリケーション（例えば、企業クラスタ化ソフトウェアアプリケーション、ネットワーク仮想アプライアンス）がある。例示的なアプリケーションは、Fortinet FortiGate, IBM（登録商標）QRadar, Palo Alto firewalls, Cisco ASA, Juniper SRX, および Oracle RAC（Real Application Clustering）を含む。本開示で説明するように、仮想化されたパブリッククラウドにおいて、仮想化されたレイヤ2ネットワーキングを提供することによって、これらのアプライアンスは、今や、変更されずに、仮想化されたパブリッククラウド環境において動作することができる。ここに記載されるように、オンプレミスに匹敵する仮想化されたレイヤ2ネットワーキング機能が提供される。本開示で説明する仮想化されたレイヤ2ネットワーキング機能は、従来のレイヤ2ネットワーキングをサポートする。これは、顧客定義のVLAN、ならびにユニキャスト、ブロードキャスト、およびマルチキャストレイヤ2トラフィック機能のサポートを含む。レイヤ2ベースのパケットのルーティングおよび転送は、レイヤ2プロトコルを使用することと、たとえば、パケットのレイヤ2ヘッダに含まれる情報を使用して、たとえばレイヤ2ヘッダに含まれる宛先MACアドレスに基づいて、パケットをルーティングまたは転送することを含む。ARP, Gratuitousアドレス解決プロトコル（GARP）、および逆アドレス解決プロトコル（RARP）などの企業アプリケーション（例えば、クラスタリングソフトウェアアプリケーション）によって使用されるプロトコルも、今や、クラウド環境において機能し得る。

【0120】

従来の仮想化されたクラウドインフラストラクチャが、仮想化されたレイヤ3ネットワーキングをサポートし、レイヤ2ネットワーキングをサポートしない、いくつかの理由がある。レイヤ2ネットワークは、通常、レイヤ3ネットワークと同様にスケーリングしない。レイヤ2ネットワーク制御プロトコルは、スケーリングのために望まれる高度化のレベルを有していない。例えば、レイヤ3ネットワークは、レイヤ2ネットワークが組み込まなければならないパケットループ化について心配する必要がない。IPパケット（すなわち、レイヤ3パケット）は、有効期間（TTL）という概念を有するが、レイヤ2パケットはそうではない。レイヤ3パケットの内部に含まれるIPアドレスは、サブネット、CIDR範囲などのトポロジの概念を有するが、レイヤ2アドレス（例えば、MACアドレス）はそうではない。レイヤ3IPネットワークは、経路情報を見つけるための、パケットインターネット探索、経路探索といった、トラブルシューティングを容易にする組み込みツールを有する。そのようなツールは、レイヤ2については利用可能ではない。レイヤ3ネットワークは、レイヤ2では利用可能ではないマルチパス機能をサポートする。特にネットワークにおいてエンティティ間で情報を交換するための高度な制御プロトコル（例

例えば、Border Gateway Protocol (BGP) および Open Shortest Path First (OSPF) の欠如のため、レイヤ2ネットワークは、ネットワークについて学習するためにブロードキャストおよびマルチキャストに依拠しなければならず、これはネットワーク性能に悪影響を与え得る。ネットワークが変化すると、レイヤ2のための学習プロセスは繰り返されなければならないが、これはレイヤ3では必要ではない。これらおよび他の理由から、クラウドIaaSサービスプロバイダにとっては、レイヤ2ではなくレイヤ3で動作するインフラストラクチャを提供する方が、より望ましい。

【0121】

しかしながら、レイヤ2機能は、その複数の欠点にもかかわらず、多くのオンプレミスアプリケーションによって必要とされる。例えば、インスタンスが計算インスタンス（例えば、ベアメタル、仮想マシンもしくはコンテナ）もしくはロードバランサ、nfsmountポイント、または他のサービスインスタンスなどのサービスインスタンスであり得る仮想ネットワーク「V」において、顧客（顧客1）がIP1を有するインスタンスAおよびIP2を有するインスタンスBの2つのインスタンスを有する、仮想化されたクラウド構成を仮定する。仮想ネットワークVは、他の仮想ネットワークおよび下層の物理ネットワークから隔離された別個のアドレス空間である。たとえば、この隔離は、パケットカプセル化またはNATを含む様々な技術を使用して達成され得る。このため、顧客の仮想ネットワーク内のインスタンスのIPアドレスは、それがホストされる物理ネットワーク内のアドレスとは異なる。物理IPおよびすべての仮想IPアドレスの仮想インターフェースを知っている集中型SDN（ソフトウェア定義ネットワークング）制御プレーンが提供される。パケットがインスタンスAから仮想ネットワークV内のIP2の宛先に送信されるとき、仮想ネットワークSDNスタックは、IP2がどこに位置するかを知る必要がある。それは、V用の仮想IPアドレスIP2がホストされている物理ネットワーク内のIPにパケットを送信することができるように、これを事前に知らなければならない。仮想IPアドレスの位置は、クラウド内で修正することができ、したがって、物理IPと仮想IPアドレスとの間の関係を変更する。仮想IPアドレスを移動させる（例えば、仮想マシンに関連付けられるIPアドレスを別の仮想マシンに移動させるか、または仮想マシンを新たな物理ホストにマイグレートする）たびに、SDN制御プレーンに対してAPI呼出しを行って、コントローラに、IPが移動されていることを知らせて、それが、SDNスタックにおいてパケットプロセッサ（データプレーン）を含むすべての参加者を更新することができるようにしなければならない。しかし、そのようなAPI呼出しを行わないアプリケーションのクラスがある。例は、様々なオンプレミスアプリケーション、VMwareなどの様々な仮想化ソフトウェアベンダによって提供されるアプリケーションなどを含む。仮想化されたクラウド環境において仮想レイヤ2ネットワークを容易にすることの価値は、そのようなAPI呼出しを行うようにプログラムされていないようなアプリケーションのサポート、または非IPレイヤ3およびMAC学習のためのサポートなど、他のレイヤ2ネットワークング機能に依存するアプリケーションのサポートを可能にする。

【0122】

仮想レイヤ2ネットワークは、ブロードキャストドメインを作成し、学習は、ブロードキャストドメインのメンバによって実行される。仮想レイヤ2ドメインでは、このレイヤ2ドメイン内の任意のホスト上の任意のMAC上に任意のIPが存在し得、システムは、標準的なレイヤ2ネットワークングプロトコルを使用して学習し、システムは、MACおよびIPがその仮想レイヤ2ネットワーク内のどこに存在するかに関して中央コントローラによって明示的に伝えられる必要がなく、これらのネットワークングプリミティブを仮想化する。これは、低レイテンシフェイルオーバーを必要とするアプリケーション、複数のノードに対するブロードキャストまたはマルチキャストプロトコルをサポートする必要があるアプリケーション、ならびにIPアドレスおよびMACアドレスがどこで有効であるかを判断するためにSDN制御プレーンまたはAPIエンドポイントへのAPI呼出しをどのように行うかを知らないレガシーアプリケーションが実行されることを可能にする。したがって、仮想化されたクラウド環境においてレイヤ2ネットワークング能力を提供す

10

20

30

40

50

ることは、IPレイヤ3レベルでは利用可能でない機能性をサポートできるよう求められる。

【0123】

仮想化されたクラウド環境において仮想レイヤ2を提供することの別の技術的利点は、非IPプロトコルを含む様々な異なるレイヤ3プロトコル（IPv4、IPv6など）がサポートされることを可能にすることである。例えば、IPX、AppleTalkなどの様々な非IPプロトコルをサポートすることができる。既存のクラウドIaaSプロバイダは、それらの仮想化されたクラウドネットワークにおいてレイヤ2機能を提供しないので、それらは、これらの非IPプロトコルをサポートすることはできない。本開示で説明されるようなレイヤ2ネットワーキング機能を提供することによって、レイヤ3におけるプロトコル、およびレイヤ2レベル機能の可用性を必要とし、それに依存するアプリケーションに対するサポートを提供することができる。

10

【0124】

本開示で説明される技術を使用して、レイヤ3およびレイヤ2機能の両方が、仮想化されたクラウドインフラストラクチャにおいて提供される。前述のように、レイヤ3ベースのネットワーキングは、レイヤ2ネットワーキングによっては提供されない特定の効率、特にスケーリングに充分に適している効率を提供する。レイヤ3機能に加えてレイヤ2機能を提供することにより、レイヤ2機能をよりスケーラブルな態様で提供しながら、レイヤ3によって提供されるそのような効率性を（たとえば、よりスケーラブルなソリューションを提供するために）活用することが可能になる。例えば、仮想化されたレイヤ3は、学習目的のためにブロードキャストを使用しなければならないことを回避する。レイヤ3を、その効率性のために提供し、ならびに、同時に、仮想化されたレイヤ2を、それを必要とするアプリケーション、およびレイヤ2機能を有さずに機能することはできないアプリケーションを有効にするため、および非IPプロトコルなどをサポートするために提供することによって、仮想化されたクラウド環境における完全な柔軟性が顧客に提供される。

20

【0125】

顧客ら自身は、レイヤ2環境がレイヤ3環境とともに存在するハイブリッド環境を有し、仮想化されたクラウド環境は、今やこれらの環境の両方をサポートすることができる。顧客は、サブネットなどのレイヤ3ネットワークおよび／またはVLANなどのレイヤ2ネットワークを有することができ、これらの2つの環境は、仮想化されたクラウド環境内で互いにやりとりすることができる。

30

【0126】

仮想化されたクラウド環境はまた、マルチテナンシをサポートする必要もある。マルチテナンシは、レイヤ3機能およびレイヤ2機能の両方を同じ仮想化されたクラウド環境においてプロビジョニングすることを技術的に困難かつ複雑にする。例えば、レイヤ2ブロードキャストドメインは、クラウドプロバイダのインフラストラクチャ内で多くの異なる顧客にわたって管理されなければならない。本開示に記載される実施形態は、これらの技術的問題を克服する。

【0127】

仮想化プロバイダ（例えば、VMware）の場合、物理レイヤ2ネットワークをエミュレートする仮想化されたレイヤ2ネットワークは、ワークロードが変更されずに実行されることを可能にする。次いで、そのような仮想化プロバイダによって提供されるアプリケーションは、クラウドインフラストラクチャによって提供される仮想化されたレイヤ2ネットワーク上で実行することができる。たとえば、そのようなアプリケーションは、レイヤ2ネットワーク上で実行される必要があるインスタンスのセットを含み得る。顧客がそのようなアプリケーションを自身のオンプレミス環境から仮想化されたクラウド環境にリフトおよびシフトすることを望む場合、単にアプリケーションを取り込んでそれをクラウド内で実行することはできず、なぜならば、これらのアプリケーションは、現在の仮想化されたクラウドプロバイダによっては提供されない下層のレイヤ2ネットワークに依拠す

40

50

るからである（例えば、レイヤ2ネットワーク機能は、仮想マシンのマイグレーションを実行するため、またはMACおよびIPアドレスが有効であるところで移動するために使用される）。これらの理由から、そのようなアプリケーションは、仮想化されたクラウド環境においてネイティブに動作することはできない。ここで説明される技術を使用して、クラウドプロバイダは、仮想化されたレイヤ3ネットワークを提供することに加えて、仮想化されたレイヤ2ネットワークも提供する。ここで、そのようなアプリケーションスタックは、クラウド環境内で変更されずに実行することができ、クラウド環境内でネスト化された仮想化を実行することができる。顧客は今や、クラウド内で自分自身のレイヤ2アプリケーションを実行し、それらを管理することができる。アプリケーションプロバイダは、これを容易にするために、自身のソフトウェアに変更を加える必要はない。そのようなレガシーアプリケーションまたはワークロード（例えば、レガシーロードバランサ、レガシーアプリケーション、KVM、Openstack、クラスタリングソフトウェア）は、今や、仮想化されたクラウド環境で変更されずに実行することができる。

10

20

30

40

50

【0128】

ここに説明されるような仮想化されたレイヤ2機能を提供することによって、非IPプロトコルを含む、種々のレイヤ3プロトコルが、今や、仮想化されたクラウド環境によってサポートされることができる。イーサネットを例にとると、様々な非IPプロトコルを含む様々な異なるEtherTypes（どのようなタイプのレイヤ3パケットが送信されているかを伝え；レイヤ3においてどのようなプロトコルを期待すべきかを伝える、レイヤ2ヘッダ内のフィールド）をサポートすることができる。EtherTypesは、イーサネット（登録商標）フレーム内の2オクテットフィールドである。これは、どのプロトコルがフレームのペイロードにカプセル化され、ペイロードがどのように処理されるかを判断するためにデータリンク層によって受信端で使用されるかを示すために使用される。EtherTypesはまた、802.1Q VLANタグ付けの基礎として使用され、VLANからのパケットを、イーサネットリンク上で他のVLANトラフィックと多重化される送信のために、カプセル化する。EtherTypesの例は、IPv4、IPv6、アドレス解決プロトコル（ARP）、AppleTalk、IPXなどを含む。レイヤ2プロトコルをサポートするクラウドネットワークは、レイヤ3レイヤにおいて任意のプロトコルをサポートすることができる。同様に、クラウドインフラストラクチャがレイヤ3プロトコルに対するサポートを提供するとき、クラウドインフラストラクチャは、TCP、UDP、ICMPなどのレイヤ4における様々なプロトコルをサポートすることができる。ネットワークは、仮想化がレイヤ3で提供されるとき、レイヤ4プロトコルにアグノスティックであり得る。同様に、ネットワークは、仮想化がレイヤ2において提供されるとき、レイヤ3プロトコルにアグノスティックであり得る。この技術は、FDDI、インフィニバンドなどを含む任意のレイヤ2ネットワークタイプをサポートするように拡張することができる。

【0129】

したがって、物理ネットワーク用に記述された多くのアプリケーション、特にブロードキャストドメインを共有するコンピュータノードのクラスタとともに動作するアプリケーションは、L3仮想ネットワークにおいてサポートされないレイヤ2機能を使用する。以下の6つの例は、レイヤ2ネットワーク能力を提供しないことから生じ得る複雑さを強調する：

（1）先行するAPI呼出しなしでのMACおよびIPの割り当て。ネットワークアプリケーションおよびハイパーバイザ（VMware等）は、クラウド仮想ネットワークのために構築されなかった。それらは、MACが一意である限りMACを使用することができ、DHCPサーバから動的アドレスを取得するか、またはクラスタに割り当てられた任意のIPを使用することができる、と仮定する。それらがこれらレイヤ2アドレスおよびレイヤ3アドレスの割り当てについて制御プレーンに通知するように構成できる機構は、存在しないことが多い。MACおよびIPがどこにあるかが分からない場合、レイヤ3仮想ネットワークは、トラフィックをどこに送るべきかがわからない。

（2）高可用性およびライブマイグレーションのためのMACならびにIPの低レイテン

シ再割り当て。多くのオンプレミスアプリケーションは、高可用性のためにARPを使用してIPおよびMACを再割り当てし、一クラスタまたはHAペア内のインスタンスが応答することを停止すると、新たにアクティブなインスタンスは、Gratuitous ARP (GAR P)を送信して、サービスIPをそのMACに再割り当てするか、または逆ARP (RARP)を送信して、サービスMACをそのインターフェースに再割り当てする。これは、ハイパーバイザ上でインスタンスをライブマイグレーションするときにも重要であり：新たなホストは、ゲストトラフィックが新たなホストに送信されるようにゲストが移動するとRARPを送信しなければならない。割り当ては、API呼出しなしで行われるだけでなく、非常に低いレイテンシ（サブミリ秒）であることも必要である。これは、RESTエンドポイントへのHTTPS呼出しでは達成できない。

10

(3) MACアドレスによるインターフェース多重化。ハイパーバイザが単一のホスト上で複数の仮想マシンをホストし、そのすべてが同じネットワーク上にあるとき、ゲストインターフェースは、それらのMACによって区別される。これは、同じ仮想インターフェース上の複数のMACに対するサポートを必要とする。

(4) VLANサポート。単一の物理仮想マシンホストは、VLANタグの使用によって示されるように、複数のブロードキャストドメイン上にある必要があることになる。例えば、VMware ESXはトラフィック分離のためにVLANを使用する（例えば、ゲスト仮想マシンは、あるVLAN上で通信し、ストレージは別のVLAN上で通信し、ホスト仮想マシンはさらに別のVLAN上で通信してもよい）。

(5) ブロードキャストおよびマルチキャストトラフィックの使用。ARPはL2ブロードキャストを必要とし、クラスタおよびHAアプリケーションのためにブロードキャストおよびマルチキャストトラフィックを使用するオンプレミスアプリケーションの例がある。

20

(6) 非IPトラフィックのサポート。L3ネットワークは、通信するためにIPv4またはIPv6ヘッダを必要とするので、IP以外のL3プロトコルの使用は機能しないことになる。L2仮想化は、VLAN内のネットワークがL3プロトコルに依存しないものであり得ることを意味し、L3ヘッダは、IPv4、IPv6、IPX、または他の何かによるかかもしれず、さらには全く存在しないこともあり得る。

【0130】

レイヤ2 VLAN実現例

30

ここで開示されるように、レイヤ2 (L2) ネットワークは、クラウドネットワーク内で作成することができる。この仮想L2ネットワークは、ここではVLANと呼ばれる仮想化されたL2 VLANなどの1つまたはいくつかのレイヤ2仮想ネットワークを含む。各VLANは、複数の計算インスタンスを含むことができ、それらの各々は、少なくとも1つのL2仮想ネットワークインターフェース（例えば、L2 VNIC）およびL2仮想スイッチに関連付けることができる。いくつかの実施形態では、L2仮想ネットワークインターフェースおよびL2仮想スイッチの各ペアは、NVD上でホストされる。NVDは、複数のそのようなペアをホストすることができ、各ペアは、異なる計算インスタンスに関連付けられる。L2仮想スイッチの集合は、VLANのエミュレートされた単一のL2スイッチを表す。L2仮想ネットワークインターフェースは、エミュレートされた単一のL2スイッチ上のL2ポートの集合を表す。VLANは、ここでは実体仮想ルータ (RVR) またはL2 VSR Sとも呼ばれるVLANスイッチングおよびルーティングサービス (VSR S) を介して、他のVLAN、レイヤ3 (L3) ネットワーク、オンプレミスネットワーク、および／または他のネットワークに接続することができる。このアーキテクチャの例を以下で説明する。

40

【0131】

ここで図6を参照すると、コンピューティングネットワークの一実施形態の概略図が示されている。VCN 602は、CSP 601に存在する。VCN 602は、VCN 602を他のネットワークに接続する複数のゲートウェイを含む。これらのゲートウェイは、VCN 602を、例えば、オンプレミスデータセンタ606などのオンプレミスネットワ

50

ークに接続することができるDRG604を含む。ゲートウェイは、たとえば、VCN602を別のVCNに接続するためのLPG、ならびに／またはVCN602をインターネットに接続するためのIGWおよび／もしくはNATゲートウェイを含み得るゲートウェイ600をさらに含み得る。VCN602のゲートウェイは、VCN602をサービスネットワーク612に接続することができるサービスゲートウェイ610をさらに含み得る。サービスネットワーク612は、例えば、自律型データベース614および／もしくはオブジェクトストア616を含む、1つまたはいくつかのデータベースならびに／またはストアを含み得る。サービスネットワークは、例えばパブリックIP範囲であり得るIP範囲の集約を含む概念的なネットワークを含み得る。いくつかの実施形態では、これらのIP範囲は、CPSI601プロバイダによって提供されるパブリックサービスのいくつかまたはすべてをカバーすることができる。これらのサービスは、例えば、インターネットゲートウェイまたはNATゲートウェイを介してアクセスすることができる。いくつかの実施形態では、サービスネットワークは、サービスネットワーク内のサービスが、ローカル領域から、その目的のための専用ゲートウェイ（サービスゲートウェイ）を通して、アクセスされる方法を提供する。いくつかの実施形態では、これらのサービスのバックエンドは、例えば、それら自体のプライベートネットワークにおいて実現することができる。いくつかの実施形態では、サービスネットワーク612は、さらなる追加のデータベースを含むことができる。

10

【0132】

VCN602は、複数の仮想ネットワークを含むことができる。これらのネットワークは、各々、1つまたはいくつかの計算インスタンスを含むことができ、1つまたはいくつかの計算インスタンスは、それらのそれぞれのネットワーク内、ネットワーク間、またはVCN602の外部で通信することができる。VCN602の仮想ネットワークの1つは、L3サブネット620である。L3サブネット620は、VCN602内で作成された構成の単位または細分化である。サブネット620は、VCN602の仮想化されたクラウド環境において仮想レイヤ3ネットワークを含むことができ、VCN602は、CPSI601の下層の物理ネットワーク上でホストされる。図6は単一のサブネット620を示すが、VCN602は1つ以上のサブネットを有することができる。VCN602内の各サブネットは、そのVCN内の他のサブネットと重複せず、VCNのアドレス空間内のアドレス空間サブセットを表す、オーバーレイIPアドレス（例えば、10.0.0.0/24および10.0.1.0/24）の連続範囲と関連付けられることができる。いくつかの実施形態では、このIPアドレス空間は、CPSI601に関連付けられるアドレス空間から隔離することができる。

20

30

【0133】

サブネット620は、1つ以上の計算インスタンスを含み、具体的には、第1の計算インスタンス622-Aおよび第2の計算インスタンス622-Bを含む。計算インスタンス622-A、622-Bは、サブネット620内で互いに通信することができ、またはサブネット620の外部の他のインスタンス、デバイス、および／もしくはネットワークと通信することができる。サブネット620の外部の通信は、仮想ルータ（VR）624によって可能にされる。VR624は、サブネット620とVCN602の他のネットワークとの間の通信を可能にする。サブネット620の場合、VR624は、サブネット620（例えば、計算インスタンス622-A、622-B）が、VCN602内の他のネットワーク上のエンドポイント、およびVCN602の外部の他のエンドポイントと通信することを可能にする論理ゲートウェイを表す。

40

【0134】

VCN602は、追加のネットワークをさらに含むことができ、具体的には、仮想L2ネットワークの例である1つまたはいくつかのL2 VLAN（ここではVLANと呼ばれる）を含むことができる。これらの1つまたはいくつかのVLANは、各々、VCN602のクラウド環境に局在化され、および／またはCPSI601の下層の物理ネットワークによってホストされる、仮想レイヤ2ネットワークを含むことができる。図6の実施

50

形態では、V C N 6 0 2 は、V L A N A 6 3 0 および V L A N B 6 4 0 を含む。V C N 6 0 2 内の各 V L A N 6 3 0、6 4 0 は、その V C N 内の他のサブネットまたは V L A N 等の、当該 V C N 内の他のネットワークと重複せず、V C N のアドレス空間内のアドレス空間サブセットを表す、オーバーレイ IP アドレス（例えば、10.0.0.0/24 および 10.0.1.0/24）の連続範囲と関連付けられることができる。いくつかの実施形態では、V L A N のこの IP アドレス空間は、C P S I 6 0 1 に関連付けられるアドレス空間から隔離され得る。V L A N 6 3 0、6 4 0 の各々は、1 つ以上の計算インスタンスを含むことができ、具体的には、V L A N A 6 3 0 は、たとえば、第 1 の計算インスタンス 6 3 2 - A および第 2 の計算インスタンス 6 3 2 - B を含むことができる。いくつかの実施形態では、V L A N A 6 3 0 は、追加の計算インスタンスを含むことができる。V L A N B 6 4 0 は、例えば、第 1 の計算インスタンス 6 4 2 - A と、第 2 の計算インスタンス 6 4 2 - B とを含むことができる。計算インスタンス 6 3 2 - A、6 3 2 - B、6 4 2 - A、6 4 2 - B の各々は、IP アドレスおよび M A C アドレスを有することができる。これらのアドレスは、任意の所望の方法で割り当てられるかまたは生成され得る。いくつかの実施形態では、これらのアドレスは、計算インスタンスの V L A N の C I D R 内にあり得、いくつかの実施形態では、これらのアドレスは、任意のアドレスであり得る。V L A N の計算インスタンスが V L A N の外部のエンドポイントと通信する実施形態では、これらのアドレスの一方または両方は V L A N C I D R からのものであるが、すべての通信が V L A N 内である場合、これらのアドレスは V L A N C I D R 内のアドレスに限定されない。アドレスが制御プレーンによって割り当てられるネットワークとは対照的に、V L A N 内の計算インスタンスの IP および／または M A C アドレスは、その V L A N のユーザ／顧客によって割り当てられ得、次いで、これらの IP および／または M A C アドレスは、以下に論じられる学習のためのプロセスに従って、V L A N 内の計算インスタンスによって発見および／または学習され得る。

10

20

30

40

50

【0135】

各 V L A N は V L A N スイッチングおよびルーティングサービス（V S R S）を含むことができ、具体的には、V L A N A 6 3 0 は V S R S A 6 3 4 を含み、V L A N B 6 4 0 は V S R S B 6 4 4 を含む。各 V S R S 6 3 4、6 4 4 は、V L A N 内でレイヤ 2 スイッチングおよびローカル学習に参加し、また、A R P、N D P、およびルーティングを含むすべての必要なレイヤ 3 ネットワーク機能を実行する。V S R S は、IP を M A C にマッピングしなければならないので、A R P（レイヤ 2 プロトコルである）を実行する。

【0136】

これらのクラウドベースの V L A N では、各仮想インターフェースまたは仮想ゲートウェイは、仮想 M A C アドレスであり得る、1 つ以上の媒体アクセス制御（M A C）アドレスと関連付けられることができる。V L A N 内で、例えば、ベアメタル、V M、もしくはコンテナであり得る 1 つ以上の計算インスタンス 6 3 2 - A、6 3 2 - B、6 4 2 - A、6 4 2 - B、および／または 1 つ以上のサービスインスタンスは、仮想スイッチを介して互いに直接通信することができる。他の V L A N または L 3 ネットワークなどとの、V L A N の外部の通信は、V S R S 6 3 4、6 4 4 を介して可能にされる。V S R S 6 3 4、6 4 4 は、V L A N ネットワークに対して IP ルーティングなどのレイヤ 3 機能を提供する分散型サービスである。いくつかの実施形態では、V S R S 6 3 4、6 4 4 は、IP ネットワークおよび L 2 ネットワークの交差点に位置し、クラウドベースの L 2 ドメイン内で IP ルーティングおよび L 2 学習に参加することができる、水平にスケーラブルな高可用性ルーティングサービスである。

【0137】

V S R S 6 3 4、6 4 4 は、インフラストラクチャ内で複数のノードにわたって分散され得、V S R S 6 3 4、6 4 4 機能は、スケーラブルであり得、具体的には、水平にスケーラブルであり得る。いくつかの実施形態では、V S R S 6 3 4、6 4 4 の機能を実現するノードの各々は、ルータおよび／またはスイッチの機能を互いに共有および複製する。

さらに、これらのノードは、それら自体を、単一のVSR S 6 3 4、6 4 4として、VLAN 6 3 0、6 4 0内のインスタンスのすべてに対して提示することができる。VSR S 6 3 4、6 4 4は、CSP I 6 0 1内の、具体的には仮想ネットワーク内の、任意の仮想化デバイス上に実現され得る。したがって、いくつかの実施形態では、VSR S 6 3 4、6 4 4は、NIC、SmartNIC、スイッチ、Smartスイッチまたは汎用計算ホストを含む仮想ネットワーク仮想化デバイスのいずれか上で実現され得る。

【0138】

VSR S 6 3 4、6 4 4は、クラウドネットワークをサポートする、例えば、1つまたはいくつかのx 8 6サーバ等の1つもしくはいくつかのサーバ、もしくは1つもしくはいくつかのNIC、具体的には、1つもしくはいくつかのSmartNIC等の1つもしくはいくつかのネットワーキングデバイス等の、1つまたはいくつかのハードウェアノード上に常駐するサービスであることができる。いくつかの実施形態では、VSR S 6 3 4、6 4 4は、サーバフリート上に実現され得る。したがって、VSR S 6 3 4、6 4 4は、ルーティングおよびセキュリティポリシーを評価することとともにL 2およびL 3学習に参加し、それを共有する、仮想ネットワーキング実施者の、集中管理されるフリートであるかまたはエッジに分散されてもよい、ノードのフリートにわたって分散されるサービスであり得る。いくつかの実施形態では、VSR S インスタンスの各々は、新たなマッピング情報がVSR S インスタンスによって学習されるので、この新たなマッピング情報で他のVSR S インスタンスを更新することができる。例えば、VSR S インスタンスが、そのVLAN内の1つまたはいくつかのCIについてIP、インターフェース、および／またはMACマッピングを学習すると、VSR S インスタンスは、その更新された情報をVCN内の他のVSR S インスタンスに提供することができる。このクロスアップデートを介して、第1のVLANに関連付けられるVSR S インスタンスは、他のVLAN内のCIについてのIP、インターフェース、および／またはMACマッピングを含むマッピングを知ることができる。いくつかの実施形態では、VCN 6 0 2内の他のVLAN内のCIについてのIP、インターフェース、および／またはMACマッピングを含むマッピングを知ることができる。VSR S がサーバフリート上に存在し、および／またはノードのフリートにわたって分散されるとき、これらの更新は大幅に促進され得る。

【0139】

いくつかの実施形態では、VSR S 6 3 4、6 4 4はまた、DHCPリレー；DHCP（ホスティング）；DHCP v 6；IPv 6 近隣探索プロトコルなどの近隣探索プロトコル；DNS；ホスティングDNS v 6；IPv 6 のためのSLAAC；NTP；メタデータサービス；およびブロックストアマウントポイントを含むが、それらに限定されない、ネットワーキングに必要な1つまたはいくつかのより上位のサービスをホストしてもよい。いくつかの実施形態では、VSR S は、複数のネットワークアドレス空間の間で変換するための1つ以上のネットワークアドレス変換（NAT）機能をサポートすることができる。いくつかの実施形態では、VSR S は、アンチスプーフィング、アンチMACスプーフィング、IPv 4 のためのARPキャッシュポイズニング対策、IPv 6 ルータ広告（RA）ガード、DHCPガード、アクセス制御リスト（ACL）を使用したパケットフィルタリング；および／または逆経路転送チェックを組み込むことができる。VSR S は、例えば、ARP、GARP、パケットフィルタ（ACL）、DHCPリレー、および／またはIPルーティングプロトコルを含む機能を実現することができる。VSR S 6 3 4、6 4 4は、例えば、MACアドレスを学習し、有効期限切れのMACアドレスを無効にし、MACアドレスの移動を取り扱い、MACアドレス情報を調べることができ、MAC情報のフラグgingの取り扱い、ストーム制御の取り扱い、ループ防止、例えば、クラウド内のIGMP等のプロトコルを介したレイヤ2マルチキャスト、ログを含む統計収集、SNMPを使用する統計、監視、ならびに／またはブロードキャスト、総トラフィック、ビット、スパニングツリーパケットなどについての統計を収集および使用することができる。

【0140】

仮想ネットワーク内で、VSR S 6 3 4、6 4 4は、異なるインスタンス化として現れ得る。いくつかの実施形態では、VSR Sのこれらのインスタンス化の各々は、VLAN 6 3 0、6 4 0に関連付けることができ、いくつかの実施形態では、各VLAN 6 3 0、6 4 0は、VSR S 6 3 4、6 4 4のインスタンス化を有することができる。いくつかの実施形態では、VSR S 6 3 4、6 4 4の各インスタンス化は、VSR S 6 3 4、6 4 4のインスタンス化に関連付けられるVLAN 6 3 0、6 4 0に対応する1つまたはいくつかの固有のテーブルを有することができる。VSR S 6 3 4、6 4 4の各インスタンス化は、VSR S 6 3 4、6 4 4のそのインスタンス化に関連付けられる固有のテーブルを生成および／またはキュレートすることができる。したがって、単一のサービスが1つまたはいくつかのクラウドネットワークのためにVSR S 6 3 4、6 4 4機能を提供してもよい一方で、クラウドネットワーク内のVSR S 6 3 4、6 4 4の個々のインスタンス化は、固有のレイヤ2転送テーブルおよびレイヤ3転送テーブルを有することができ、一方で、複数のそのような顧客ネットワークは、重なるレイヤ2転送テーブルおよびレイヤ3転送テーブルを有することができる。

10

20

30

【0141】

いくつかの実施形態では、VSR S 6 3 4、6 4 4は、複数のテナントにわたって競合するVLANおよびIP空間をサポートし得る。これは、同じVSR S 6 3 4、6 4 4上に複数のテナントを有することを含み得る。いくつかの実施形態では、これらのテナントのいくつかまたはすべては、同じIPアドレス空間、同じMAC空間、および同じVLAN空間のうちのいくつかまたはすべてを使用するよう選択することができる。これは、アドレスを選択する際にユーザに極度の柔軟性を提供することができる。いくつかの実施形態では、このマルチテナンシは、各テナントに別個の仮想ネットワークを提供することによってサポートされ、この仮想ネットワークは、クラウドネットワーク内のプライベートネットワークである。各仮想ネットワークには一意の識別子が与えられる。同様に、いくつかの実施形態では、各ホストは、一意の識別子を有することができ、および／または各仮想インターフェースもしくは仮想ゲートウェイは、一意の識別子を有することができる。いくつかの実施形態では、これらの一意の識別子、具体的にはテナントに対する仮想ネットワークの一意の識別子は、各通信において符号化することができる。各仮想ネットワークに一意の識別子を提供し、これを通信内に含めることによって、VSR S 6 3 4、6 4 4の単一のインスタンス化は、重複するアドレスおよび／または名前空間を有する複数のテナントに対応することができる。

【0142】

VSR S 6 3 4、6 4 4は、VLAN 6 3 0、6 4 0内でのL2ネットワークとの作成および／もしくはそれとの通信を容易にし、ならびに／またはそれを可能にするために、これらのスイッチング機能および／またはルーティング機能を実行することができる。このVLAN 6 3 0、6 4 0は、クラウドコンピューティング環境内で、より具体的には、そのクラウドコンピューティング環境における仮想ネットワーク内において、見出され得る。

【0143】

例えば、VLAN 6 3 0、6 4 0の各々は、複数の計算インスタンス6 3 2-A、6 3 2-B、6 4 2-A、6 4 2-Bを含む。VSR S 6 3 4、6 4 4は、あるVLAN 6 3 0、6 4 0における計算インスタンスと、別のVLAN 6 3 0、6 4 0またはサブネット6 2 0における計算インスタンスとの間の通信を可能にする。いくつかの実施形態では、VSR S 6 3 4、6 4 4は、あるVLAN 6 3 0、6 4 0内の計算インスタンスと、別のVCN、インターネットを含むVCNの外部の別のネットワーク、オンプレミスデータセンタなどとの間の通信を可能にする。そのような実施形態では、例えば、計算インスタンス6 3 2-Aなどの計算インスタンスは、VLAN、この例ではVLAN A 6 3 0の外側のエンドポイントに通信を送信することができる。計算インスタンス(6 3 2-A)は、VSR S A 6 3 4に通信を送信することができ、VSR S A 6 3 4は、その通信を、所望のエンドポイントと通信可能に結合されたルータ6 2 4、6 4 4またはゲートウェ

40

50

イ 6 0 4、6 0 8、6 1 0 に向けることができる。所望のエンドポイントと通信可能に結合されたルータ 6 2 4、6 4 4 またはゲートウェイ 6 0 4、6 0 8、6 1 0 は、計算インスタンス（6 3 2 - A）から通信を受信することができ、その通信を所望のエンドポイントに向けることができる。

【0 1 4 4】

ここで図 7 を参照すると、V L A N 7 0 0 の論理およびハードウェア概略図が示されている。理解されるように、V L A N 7 0 0 は、複数のエンドポイントを含み、具体的には、複数の計算インスタンスおよび V S R S を含む。複数の計算インスタンス（C I）は、1 つまたはいくつかのホストマシン上でインスタンス化される。いくつかの実施形態では、これは、各 C I が固有のホストマシン上でインスタンス化されるように一対一の関係にあることができ、および／またはいくつかの実施形態では、これは、複数の C I が単一の共通ホストマシン上でインスタンス化されるように多対一の関係にあることができる。様々な実施形態では、C I は、L 2 プロトコルを使用して互いに通信するように構成されることによって、レイヤ 2 C I であることができる。図 7 は、いくつかの C I が固有のホストマシン上でインスタンス化され、いくつかの C I が共通のホストマシンを共有するシナリオを示す。図 7 に見られるように、インスタンス 1（C I 1）7 0 4 - A はホストマシン 1 7 0 2 - A 上でインスタンス化され、インスタンス 2（C I 2）7 0 4 - B はホストマシン 2 7 0 2 - B 上でインスタンス化され、インスタンス 3（C I 3）7 0 4 - C およびインスタンス 4（C I 4）7 0 4 - D は共通のホストマシン 7 0 2 - C 上でインスタンス化される。

【0 1 4 5】

C I 7 0 4 - A、7 0 4 - B、7 0 4 - C、7 0 4 - D の各々は、V L A N 7 0 0 内の他の C I 7 0 4 - A、7 0 4 - B、7 0 4 - C、7 0 4 - D、および V S R S 7 1 4 と通信可能に結合される。具体的には、C I 7 0 4 - A、7 0 4 - B、7 0 4 - C、7 0 4 - D の各々は、V L A N 7 0 0 内の他の C I 7 0 4 - A、7 0 4 - B、7 0 4 - C、7 0 4 - D、および V S R S 7 1 4 に、L 2 V N I C およびスイッチを介して接続される。各 C I 7 0 4 - A、7 0 4 - B、7 0 4 - C、7 0 4 - D は、固有の L 2 V N I C およびスイッチに関連付けられる。スイッチは、ローカルであり、L 2 V N I C に固有に関連付けられ、L 2 V N I C のために展開される、L 2 仮想スイッチであり得る。具体的には、C I 1 7 0 4 - A は L 2 V N I C 1 7 0 8 - A およびスイッチ 1 7 1 0 - A に関連付けられ、C I 2 7 0 4 - B は L 2 V N I C 2 7 0 8 - B およびスイッチ 7 1 0 - B に関連付けられ、C I 3 7 0 4 - C は L 2 V N I C 3 7 0 8 - C およびスイッチ 3 7 1 0 - C に関連付けられ、C I 4 7 0 4 - D は、L 2 V N I C 4 7 0 8 - D およびスイッチ 4 7 1 0 - D に関連付けられる。

【0 1 4 6】

いくつかの実施形態では、各 L 2 V N I C 7 0 8 およびその関連付けられるスイッチ 7 1 0 は、N V D 7 0 6 上でインスタンス化され得る。このインスタンス化は、単一の L 2 V N I C 7 0 8 およびその関連付けられるスイッチ 7 1 0 が固有の N V D 7 0 6 上でインスタンス化されるように一対一の関係にあることができ、またはこのインスタンス化は、複数の L 2 V N I C 7 0 8 およびそれらの関連付けられるスイッチ 7 1 0 が単一の共通の N V D 7 0 6 上でインスタンス化されるように多対一の関係にあることができる。具体的には、L 2 V N I C 1 7 0 8 - A およびスイッチ 1 7 1 0 - A は、N V D 1 7 0 6 - A 上でインスタンス化され、L 2 V N I C 2 7 0 8 - B およびスイッチ 2 7 1 0 - B は、N V D 2 上でインスタンス化され、L 2 V N I C 3 7 0 8 - C およびスイッチ 3 7 1 0 - C ならびに L 2 V N I C 4 7 0 8 - D およびスイッチ 7 1 0 - D の両方は、共通の N V D、すなわち N V D 7 0 6 - C 上でインスタンス化される。

【0 1 4 7】

いくつかの実施形態では、V S R S 7 1 4 は、複数のテナントにわたって競合する V L A N および I P 空間をサポートすることができる。これは、同じ V S R S 7 1 4 上に複数のテナントを有することを含むことができる。いくつかの実施形態では、これらのテナン

トのいくつかまたはすべては、同じIPアドレス空間、同じMAC空間、および同じVLAN空間のうちのいくつかまたはすべてを使用するよう選択することができる。これは、アドレスを選択する際にユーザに極度の柔軟性を提供することができる。いくつかの実施形態では、このマルチテナンシは、各テナントに別個の仮想ネットワークを提供することによってサポートされ、この仮想ネットワークは、クラウドネットワーク内のプライベートネットワークである。各仮想ネットワーク（例えば、各VLANまたはVCN）には、VLAN識別子であり得るVCN識別子などの一意の識別子が与えられる。この一意の識別子は、例えば、制御プレーンによって、具体的には、CSPの制御プレーンによって選択されることができる。いくつかの実施形態では、この一意のVLAN識別子は、パケットカプセル化において含まれ得る、および／または使用され得る、1つまたはいくつかのビットを含み得る。同様に、いくつかの実施形態では、各ホストは、一意の識別子を有することができる、および／または各仮想インターフェースもしくは仮想ゲートウェイは、一意の識別子を有することができる。いくつかの実施形態では、これらの一意の識別子、具体的にはテナントに対する仮想ネットワークの一意の識別子は、各通信において符号化することができる。各仮想ネットワークに一意の識別子を提供し、これを通信内に含めることによって、VSRの単一のインスタンス化は、重複するアドレスおよび／または名前空間を有する複数のテナントに対応することができる。いくつかの実施形態では、VSR 714は、通信に関連付けられる、具体的には通信のVCNヘッダ内の、VCN識別子および／またはVLAN識別子に基づいて、パケットがどのテナントに属するかを判断することができる。ここで開示される実施形態では、VLANに出入りする通信は、VLAN識別子を含むことができるVCNヘッダを有することができる。VLAN識別子を含むVCNヘッダに基づいて、VSR 714はテナンシを判断することができ、言い換えれば、受信側VSRは、どのVLANおよび／またはどのテナントに通信を送信するかを判断することができる。加えて、VLANに属する各計算インスタンス（例えば、L2計算インスタンス）には、その計算インスタンスに関連付けられるL2 VNICを識別する一意のインターフェース識別子が与えられる。インターフェース識別子は、（例えば、フレームのヘッダに含まれることによって）コンピュータインスタンスからのトラフィックおよび／またはコンピュータインスタンスへのトラフィックに含まれ得、計算インスタンスに関連付けられるL2 VNICを識別するためにNVDによって使用され得る。言い換えれば、インターフェース識別子は、計算インスタンスおよび／またはその関連付けられるL2 VNICを一意に示すことができる。

10

20

30

40

50

【0148】

図7に示されるように、スイッチ710-A、710-B、710-C、710-Dは共に、ここでは分散型スイッチ712とも呼ばれる、L2分散型スイッチ712を形成することができる。顧客の観点からは、L2分散型スイッチ712内の各スイッチ710-A、710-B、710-C、710-Dは、VLAN内のCIのすべてに接続する単一のスイッチである。しかしながら、単一のスイッチのユーザエクスペリエンスをエミュレートするL2分散型スイッチ712は、無限にスケーラブルであり、ローカルスイッチ（たとえば、図7の例示的な例では、スイッチ710-A、710-B、710-C、710-D）の集合を含む。図7に示すように、各CIは、NVDに接続されたホストマシン上で実行される。NVDに接続されたホスト上の各CIについて、NVDは、計算インスタンスに関連付けられるレイヤ2 VNICおよびローカルスイッチ（たとえば、NVDにローカルであり、レイヤ2 VNICに関連付けられ、L2分散型スイッチ712の1つのメンバまたは構成要素であるL2仮想スイッチ）をホストする。レイヤ2 VNICは、レイヤ2 VLAN上において計算インスタンスのポートを表す。ローカルスイッチは、VNICをレイヤ2 VLANの他の計算インスタンスに関連付けられる他のVNIC（例えば、他のポート）に接続する。

【0149】

CI 704-A、704-B、704-C、704-Dの各々は、VLAN 700内のCI 704-A、704-B、704-C、704-Dの他のものと、またはVSR 7

14と通信することができる。CI704-A、704-B、704-C、704-Dのうちの1つは、CI704-A、704-B、704-C、704-Dのうちの受信側CIまたはVSRS714のMACアドレスおよびインターフェース識別子にフレームを送信することによって、フレームをCI704-A、704-B、704-Cのうちの別のCIまたはVSRS714に送信する。MACアドレスおよびインターフェース識別子は、フレームのヘッダに含まれ得る。ここで上記で説明したように、インターフェース識別子は、CI704-A、704-B、704-C、704-Dのうちの受信側CIまたはVSRS714のL2 VNICを示すことができる。

【0150】

一実施形態では、CI1 704-Aは送信元CIであり得、L2 VNIC708-Aは送信元L2 VNICであり得、スイッチ710-Aは送信元L2仮想スイッチであり得る。この実施形態では、CI3 704-Cは宛先CIであり得、L2 VNIC3 708-Cは宛先L2 VNICであり得る。送信元CIは、フレームを、送信元MACアドレスおよび宛先MACアドレスとともに送信することができる。このフレームは、送信元VNICおよび送信元スイッチをインスタンス化するNVD706-Aによってインターセプトされ得る。

【0151】

L2 VNIC708-A、708-B、708-C、708-Dは、VLAN700について、各々、MACアドレスをL2 VNICのインターフェース識別子にマッピングすることを学習することができる。このマッピングは、VLAN700内から受信されるフレームおよび／または通信に基づいて学習されることができる。この、以前に決定されたマッピングに基づいて、送信元VNICは、VLAN内の宛先CIに関連付けられた宛先インターフェースのインターフェース識別子を判断することができ、フレームをカプセル化することができる。いくつかの実施形態では、このカプセル化は、GENEVEカプセル化、具体的には、カプセル化されるフレームのL2（イーサネット（登録商標））ヘッダを含むL2 GENEVEカプセル化を含むことができる。カプセル化されたフレームは、宛先MAC、宛先インターフェース識別子、送信元MAC、および送信元インターフェース識別子を識別することができる。

【0152】

送信元VNICは、カプセル化されたフレームを送信元スイッチに渡すことができ、送信元スイッチは、フレームを宛先VNICに向けることができる。フレームを受信すると、宛先VNICは、フレームをカプセル化解除し、次いで、フレームを宛先CIに提供することができる。

【0153】

ここで図8を参照すると、複数の接続されたL2 VLAN800の論理概略図が示されている。図8に示される特定の実施形態では、両方のVLANは同じVCNに位置する。理解されるように、複数の接続されたL2 VLAN800は、第1のVLANであるVLAN A802-Aと、第2のVLANであるVLAN B802-Bとを含むことができる。これらのVLAN802-A、802-Bの各々は、1つまたはいくつかのCIを含むことができ、それらの各々は、関連付けられたL2 VNICおよび関連付けられたL2仮想スイッチを有することができる。さらに、これらのVLAN802-A、802-Bの各々は、VSRSを含むことができる。

【0154】

具体的には、VLAN A802-Aは、L2 VNIC1 806-Aおよびスイッチ1 808-Aに接続されたインスタンス1 804-Aと、L2 VNIC2 806-Bおよびスイッチ808-Bに接続されたインスタンス2 804-Bと、L2 VNIC3 806-Cおよびスイッチ3 808-Cに接続されたインスタンス3 804-Cとを含むことができる。VLAN B802-Bは、L2 VNIC4 806-Dおよびスイッチ4 808-Dに接続されたインスタンス4 804-Dと、L2 VNIC5 806-Eおよびスイッチ808-Eに接続されたインスタンス5 804

10

20

30

40

50

－Eと、L2 VNIC 6 806－Fおよびスイッチ3 808－Fに接続されたインスタンス6 804－Fとを含むことができる。VLAN A 802－AはVSRS A 810－Aをさらに含むことができ、VLAN B 802－BはVSRS B 810－Bを含むことができる。VLAN A 802－AのCI 804－A、804－B、804－Cの各々は、VSRS A 810－Aに通信可能に結合されることができ、VLAN B 802－BのCI 804－D、804－E、804－Fの各々は、VSRS B 810－Bに通信可能に結合されることができる。

【0155】

VLAN A 802－Aは、VLAN B 802－Bに、それぞれのVSRS 810－A、810－Bを介して、通信可能に結合されることができる。各VSRSは、同様に、ゲートウェイ812に結合されることができ、ゲートウェイは、各VLAN 802－A、802－B内のCI 804－A、804－B、804－C、804－D、804－E、804－Fに対するアクセスを、VLAN 802－A、802－Bが位置するVCNの外部の他のネットワークに提供することができる。いくつかの実施形態では、これらのネットワークは、例えば、1つまたはいくつかのオンプレミスネットワーク、別のVCN、サービスネットワーク、インターネットなどの公衆ネットワークなどを含むことができる。

10

【0156】

VLAN A 802－A内のCI 804－A、804－B、804－Cの各々は、各VLAN 802－A、802－BのVSRS 810－A、810－Bを介して、VLAN B 802－B内のCI 804－D、804－E、804－Fと通信することができる。たとえば、VLAN 802－A、802－Bのうちの1つにおけるCI 804－A、804－B、804－C、804－D、804－E、804－Fのうちの1つは、VLAN 802－A、802－Bの他方におけるCI 804－A、804－B、804－C、804－D、804－E、804－Fに、フレームを送信することができる。このフレームは、送信元VLANのVSRSを介して送信元VLANを出ることができ、宛先VLANに入り、宛先VSRSを介して宛先CIにルーティングされることができる。

20

【0157】

一実施形態では、CI 1 804－Aは送信元CIであり得、VNIC 806－Aは送信元VNICであり得、スイッチ808－Aは送信元スイッチであり得る。この実施形態では、CI 5 804－Eは宛先CIであり得、L2 VNIC 5 806－Eは宛先VNICであり得る。VSRS A 810－Aは、SVSRSとして識別される送信元VSRSであり得、VSRS B 810－Bは、DVSRSとして識別される宛先VSRSであり得る。

30

【0158】

送信元CIは、フレームをMACアドレスとともに送信することができる。このフレームは、送信元VNICおよび送信元スイッチをインスタンス化するNVDによってインターセプトされ得る。送信元VNICは、フレームをカプセル化する。いくつかの実施形態では、このカプセル化は、GENEVEカプセル化、具体的にはL2 GENEVEカプセル化を含むことができる。カプセル化されたフレームは、宛先CIの宛先アドレスを識別することができる。いくつかの実施形態では、この宛先アドレスはまた、宛先VSRSの宛先アドレスを含むこともできる。宛先CIの宛先アドレスは、宛先IPアドレス、宛先CIの宛先MAC、および／または宛先CIに関連付けられる宛先VNICの宛先インターフェース識別子を含むことができる。宛先VSRSの宛先アドレスは、宛先VSRSのIPアドレス、宛先VSRSに関連付けられる宛先VNICのインターフェース識別子、および／または宛先VSRSのMACアドレスを含むことができる。

40

【0159】

送信元VSRSは、送信元スイッチからフレームを受信することができ、フレームの宛先アドレスからVNICマッピングを検索することができ、その宛先アドレスは宛先IPアドレスであり得、パケットを宛先VSRSに転送することができる。宛先VSRSは、フレームを受信することができる。フレームに含まれる宛先アドレスに基づいて、宛先V

50

S R S は、フレームを宛先 V N I C に転送することができる。宛先 V N I C は、フレームを受信し、カプセル化解除することができ、次いで、宛先 C I にフレームを提供することができる。

【0160】

ここで図9を参照すると、複数の接続された L 2 V L A N およびサブネット 9 0 0 の論理概略図が示されている。図9に示す特定の実施形態では、V L A N およびサブネットの両方が同じ V C N に位置する。これは、V L A N およびサブネットの両方の、仮想ルータおよび V S R S が、ゲートウェイを介して接続されるのではなく、直接接続されるために、示される。

【0161】

理解されるように、これは、第1の V L A N、V L A N A 9 0 2 - A、第2の V L A N、V L A N B 9 0 2 - B、およびサブネット 9 3 0 を含むことができる。これらの V L A N 9 0 2 - A、9 0 2 - B の各々は、1つまたはいくつかの C I を含むことができ、それらの各々は、関連付けられた L 2 V N I C および関連付けられた L 2 スイッチを有することができる。さらに、これらの V L A N 9 0 2 - A、9 0 2 - B の各々は、V S R S を含むことができる。同様に、L 3 サブネットであり得るサブネット 9 3 0 は、1つまたはいくつかの C I を含むことができ、それらの各々は、関連付けられた L 3 V N I C を有することができる。L 3 サブネット 9 3 0 は仮想ルータ 9 1 6 を含むことができる。

【0162】

具体的には、V L A N A 9 0 2 - A は、L 2 V N I C 1 9 0 6 - A およびスイッチ 1 9 0 8 - A に接続されたインスタンス 1 9 0 4 - A と、L 2 V N I C 2 9 0 6 - B およびスイッチ 2 9 0 8 - B に接続されたインスタンス 2 9 0 4 - B と、L 2 V N I C 3 9 0 6 - C およびスイッチ 3 9 0 8 - C に接続されたインスタンス 3 9 0 4 - C とを含むことができる。V L A N B 9 0 2 - B は、L 2 V N I C 4 9 0 6 - D およびスイッチ 4 9 0 8 - D に接続されたインスタンス 4 9 0 4 - D と、L 2 V N I C 5 9 0 6 - E およびスイッチ 5 9 0 8 - E に接続されたインスタンス 5 9 0 4 - E と、L 2 V N I C 6 9 0 6 - F およびスイッチ 6 9 0 8 - F に接続されたインスタンス 6 9 0 4 - F とを含むことができる。V L A N A 9 0 2 - A はさらに、V S R S A 9 1 0 - A を含むことができ、V L A N B 9 0 2 - B は V S R S B 9 1 0 - B を含むことができる。V L A N A 9 0 2 - A の C I 9 0 4 - A、9 0 4 - B、9 0 4 - C の各々は、V S R S A 9 1 0 - A に通信可能に結合されることができ、V L A N B 9 0 2 - B の C I 9 0 4 - D、9 0 4 - E、9 0 4 - F の各々は、V S R S B 9 1 0 - B に通信可能に結合されることができ、L 3 サブネット 9 3 0 は、1つまたはいくつかの C I を含むことができ、具体的には、L 3 V N I C 7 9 0 6 - G に通信可能に結合されるインスタンス 7 9 0 4 - G を含むことができる。L 3 サブネット 9 3 0 は仮想ルータ 9 1 6 を含むことができる。

【0163】

V L A N A 9 0 2 - A は、V L A N B 9 0 2 - B に、それぞれの V S R S 9 1 0 - A、9 1 0 - B を介して通信可能に結合されることができ、L 3 サブネット 9 3 0 は、仮想ルータ 9 1 6 を介して V L A N A 9 0 2 - A および V L A N B 9 0 2 - B と通信可能に結合されることができ、仮想ルータ 9 1 6 および V S R S インスタンス 9 1 0 - A、9 1 0 - B の各々は、同様に、ゲートウェイ 9 1 2 に結合されることができ、ゲートウェイ 9 1 2 は、各 V L A N 9 0 2 - A、9 0 2 - B およびサブネット 9 3 0 における C I 9 0 4 - A、9 0 4 - B、9 0 4 - C、9 0 4 - D、9 0 4 - E、9 0 4 - F、9 0 4 - G に対するアクセスを、V L A N 9 0 2 - A、9 0 2 - B およびサブネット 9 3 0 が位置する V C N の外部の他のネットワークに、与えることができる。いくつかの実施形態では、これらのネットワークは、例えば、1つまたはいくつかのオンプレミスネットワーク、別の V C N、サービスネットワーク、インターネットなどの公衆ネットワークなどを含むことができる。

【0164】

各 V S R S インスタンス 9 1 0 - A、9 1 0 - B は、関連付けられた V L A N 9 0 2 - A、9 0 2 - B を出るフレームのための発信経路と、関連付けられた V L A N 9 0 2 - A、9 0 2 - B に入るフレームのための着信経路とを提供することができる。V L A N 9 0 2 - A、9 0 2 - B の V S R S インスタンス 9 1 0 - A、9 1 0 - B から、フレームは、同じ V C N 上もしくは異なる V C N もしくはネットワーク上のいずれかの別の V L A N 内の L 2 C I 等の L 2 エンドポイント、および／または同じ V C N もしくは異なる V C N もしくはネットワーク上のサブネット内の L 3 C I などの L 3 エンドポイントを含む、任意の所望のエンドポイントに送信されることができる。

【0165】

一実施形態では、C I 1 9 0 4 - A は送信元 C I であり得、V N I C 9 0 6 - A は送信元 V N I C であり得、スイッチ 9 0 8 - A は送信元スイッチであり得る。この実施形態では、C I 7 9 0 4 - G は宛先 C I であり得、V N I C 7 9 0 6 - G は宛先 V N I C であり得る。V S R S A 9 1 0 - A は、S V S R S として識別される送信元 V S R S であり得、仮想ルータ (V R) 9 1 6 は、宛先 V R であり得る。

【0166】

送信元 C I は、フレームを M A C アドレスとともに送信することができる。このフレームは、送信元 V N I C および送信元スイッチをインスタンス化する N V D によってインターセプトされ得る。送信元 V N I C は、フレームをカプセル化する。いくつかの実施形態では、このカプセル化は、G E N E V E カプセル化、具体的には L 2 G E N E V E カプセル化を含むことができる。カプセル化されたフレームは、宛先 C I の宛先アドレスを識別することができる。いくつかの実施形態では、この宛先アドレスはまた、送信元 C I の V L A N の V S R S の宛先アドレスを含むこともできる。宛先 C I の宛先アドレスは、宛先 I P アドレス、宛先 C I の宛先 M A C、および／または宛先 C I の宛先 V N I C の宛先インターフェース識別子を含むことができる。

【0167】

送信元 V S R S は、送信元スイッチからフレームを受信することができ、フレームの宛先アドレスから V N I C マッピングを検索することができ、その宛先アドレスは宛先 I P アドレスであり得、フレームを宛先 V R に転送することができる。宛先 V R は、フレームを受信することができる。フレームに含まれる宛先アドレスに基づいて、宛先 V R は、フレームを宛先 V N I C に転送することができる。宛先 V N I C は、フレームを受信し、カプセル化解除することができ、次いで、宛先 C I にフレームを提供することができる。

【0168】

仮想 L 2 ネットワーク内における L 2 V N I C および／または L 2 仮想スイッチによる学習

ここで図 10 を参照すると、V L A N 1 0 0 0 内の V L A N 内通信および学習の一実施形態の概略図が示されている。ここでの学習は、L 2 V N I C、送信元 C I の V L A N の V S R S、および／または L 2 仮想スイッチが、M A C アドレスと L 2 V N I C / V S R S V N I C との間 (より具体的には、L 2 計算インスタンスまたは V S R S に関連付けられる M A C アドレスと、V S R S V N I C に関連付けられるこれらの L 2 計算インスタンスの L 2 V N I C に関連付けられるインターフェース識別子との間) の関連付けをどのように学習するかの特有である。一般に、学習は着信トラフィックに基づく。この学習は、インターフェース対 M A C アドレス学習の局面に関して、L 2 計算インスタンスが宛先 M A C アドレスを学習するために実現し得る学習プロセス (たとえば、A R P プロセス) とは異なる。(例えば、L 2 V N I C / L 2 仮想スイッチおよび L 2 計算インスタンスの) 2 つの学習プロセスは、図 12 において共同で実現されるとしてもものとして示されている。

【0169】

理解されるように、V L A N 1 0 0 0 は、L 2 V N I C 1 1 0 0 2 - A および L 2 スイッチ 1 1 0 0 4 - A をインスタンス化する N V D 1 1 0 0 1 - A と通信可能に結合される計算インスタンス 1 1 0 0 0 - A を含む。V L A N 1 0 0 0 はまた、L 2 V

N I C 2 1 0 0 2 - B および L 2 スイッチ 2 1 0 0 4 - A をインスタンス化する N V D 2 1 0 0 1 - B と通信可能に結合される計算インスタンス 2 1 0 0 0 - B を含む。V L A N 1 0 0 0 はまた、サーバフリート上で実行され、V S R S V N I C 1 0 0 2 - C および V S R S スイッチ 1 0 0 4 - C を含む V S R S 1 0 1 5 を含む。スイッチ 1 0 0 4 - A 、 1 0 0 4 - B 、 1 0 0 4 - C のすべては、共に、L 2 分散型スイッチ 1 0 5 0 を形成する。V S R S 1 0 1 5 は、エンドポイント 1 0 0 8 と通信可能に結合され、エンドポイント 1 0 0 8 は、ゲートウェイを含むことができ、具体的には、例えば別の V S R S の形態の L 2 / L 3 ルータ、または例えば仮想ルータの形態の L 3 ルータを含むことができる。

【0170】

V L A N 1 0 0 0 をホストする V C N の制御プレーン 1 0 1 0 は、V L A N 1 0 0 0 上の各 L 2 V N I C および各 L 2 V N I C のネットワーク配置を識別する情報を維持する。たとえば、この情報は、L 2 V N I C について、L 2 V N I C に関連付けられたインターフェース識別子、および／または L 2 V N I C をホストする N V D の物理 IP アドレスを含むことができる。制御プレーン 1 0 1 0 は、V L A N 1 0 0 0 内のインターフェースをこの情報で（例えば、周期的に、またはオンデマンドで）更新する。したがって、V L A N 1 0 0 0 内の各 L 2 V N I C 1 0 0 2 - A 、 1 0 0 2 - B 、 1 0 0 2 - C は、制御プレーン 1 0 1 0 から情報を受信し、V L A N 内のインターフェースを識別し、この情報をテーブルにポピュレートする。L 2 V N I C によってポピュレートされたテーブルは、L 2 V N I C をホストする N V D にローカルに記憶され得る。V N I C 1 0 0 2 - A 、 1 0 0 2 - B 、 1 0 0 2 - C がすでに現在のテーブルを含む場合、V N I C 1 0 0 2 - A 、 1 0 0 2 - B 、 1 0 0 2 - C は、V N I C 1 0 0 2 - A 、 1 0 0 2 - B 、 1 0 0 2 - C の現在のテーブルと制御プレーン 1 0 1 0 から受信された情報／テーブルとの間のいかなる矛盾も判断することができる。V N I C 1 0 0 2 - A 、 1 0 0 2 - B 、 1 0 0 2 - C は、いくつかの実施形態では、制御プレーン 1 0 1 0 から受信した情報と一致するようにそのテーブルを更新することができる。

【0171】

図 10 に見られるように、フレームは、L 2 スイッチ 1 0 0 4 - A 、 1 0 0 4 - B 、 1 0 0 4 - C を介して送信され、受信側 V N I C 1 0 0 2 - A 、 1 0 0 2 - B 、 1 0 0 2 - C によって受信される。フレームが V N I C 1 0 0 2 - A 、 1 0 0 2 - B 、 1 0 0 2 - C によって受信されると、その V N I C は、そのフレームの送信元インターフェース（送信元 V N I C ）および送信元 M A C アドレスのマッピングを学習する。制御プレーン 1 0 1 0 から受信された情報のそのテーブルに基づいて、V N I C は、（受信されたフレームからの）送信元 M A C アドレスを、送信元 V N I C のインターフェース識別子ならびにその V N I C の IP アドレスおよび／またはその V N I C をホストする N V D の IP アドレスにマッピングすることができる（インターフェース識別子および IP アドレスが表から入手可能である場合）。したがって、L 2 V N I C 1 0 0 2 - A 、 1 0 0 2 - B 、 1 0 0 2 - C は、受信された通信および／またはフレームに基づいて、インターフェース識別子の M A C アドレスへのマッピングを学習する。各 V N I C 1 0 0 2 - A 、 1 0 0 2 - B 、 1 0 0 2 - C は、その L 2 転送（FWD）テーブル 1 0 0 6 - A 、 1 0 0 6 - B 、 1 0 0 6 - C を、この学習されたマッピング情報とともに、有することができる。いくつかの実施形態では、L 2 転送テーブルは、M A C アドレスを含み、インターフェース識別子または物理 IP アドレスのうちの少なくとも 1 つと関連付ける。そのような実施形態では、M A C アドレスは、L 2 計算インスタンスに割り当てられたアドレスであり、L 2 計算インスタンスに関連付けられる L 2 V N I C によってエミュレートされるポートに対応し得る。インターフェース識別子は、L 2 V N I C および／または L 2 計算インスタンスを一意に識別することができる。仮想 IP アドレスは、L 2 V N I C のそれとすることができる。また、物理 IP アドレスは、L 2 V N I C をホストする N V D のそれとすることができる。L 2 V N I C によって更新された L 2 転送は、L 2 V N I C をホストする N V D 上にローカルに記憶され得、フレームを方向付けるために L 2 V N I C に関連

10

20

30

40

50

付けられた L 2 仮想スイッチによって使用され得る。いくつかの実施形態では、共通 V L A N 内の V N I C は、それらのマッピングテーブルのすべてまたは部分を互いに共有することができる。

【0172】

上記のネットワークアーキテクチャに照らして、トラフィックフローがここにおいて次に説明される。説明を明確にするために、トラフィックフローは、計算インスタンス 2 1000-B、L 2 V N I C 2 10002-B、L 2 スイッチ 2 1004-B、および N V D 2 1001-B に関連して説明される。この説明は、他の計算インスタンスとの間のトラフィックフローに等価に適用される。

【0173】

ここで上述したように、V L A N は、L 3 物理ネットワークの上のオーバーレイ L 2 ネットワークとして、V C N 内で実現される。V L A N の L 2 計算インスタンスは、送信元 M A C アドレスおよび宛先 M A C アドレスとしてオーバーレイ M A C アドレス（仮想 M A C アドレスとも呼ばれる）を含む L 2 フレームを送信または受信することができる。L 2 フレームはまた、送信元 I P アドレスおよび宛先 I P アドレスとしてオーバーレイ I P アドレス（仮想 I P アドレスとも呼ばれる）を含むパケットをカプセル化することもできる。計算インスタンスのオーバーレイ I P アドレスは、いくつかの実施形態では、V L A N の C I D R 範囲に属することができる。他のオーバーレイ I P アドレスは、C I D R 範囲（この場合、L 2 フレームは V L A N 内を流れる）または C I D R 範囲外（この場合、L 2 フレームは、他のネットワークに宛てられるか、または他のネットワークから受信される）に属することができる。L 2 フレームはまた、V L A N を一意に識別し、同じ N V D 上の複数の L 2 V N I C と区別するために使用され得る、V L A N タグを含むことができる。L 2 フレームは、計算インスタンスのホストマシンから、別の N V D から、または V S R S をホストするサーバフリートから、トンネルを介して、N V D によって、カプセル化されたパケットで、受信され得る。これらの異なる場合において、カプセル化されたパケットは、物理ネットワーク上で送信される L 3 パケットであり得、送信元 I P アドレスおよび宛先 I P アドレスは、物理 I P アドレスである。G E N E V E カプセル化を含む、異なるタイプのカプセル化が可能である。N V D は、受信したパケットをカプセル化解除して L 2 フレームを抽出することができる。同様に、L 2 フレームを送信するために、N V D は、それを L 3 パケットにカプセル化し、それを物理基板上で送信することができる。

【0174】

インスタンス 2 1000-B からの V L A N 内発信トラフィックの場合、N V D 2 1001-B は、イーサネットリンクを介してインスタンス 2 1000-B のホストマシンからフレームを受信する。フレームは、L 2 V N I C 2 1000-B を識別するインターフェース識別子を含む。フレームは、送信元 M A C アドレスとしてインスタンス 2 1000-B のオーバーレイ M A C アドレス（例えば、M.2）を含み、宛先 M A C アドレスとしてインスタンス 1 1000-A のオーバーレイ M A C アドレス（例えば、M.1）を含む。インターフェース識別子が与えられると、N V D 2 1001-B は、さらなる処理のためにフレームを L 2 V N I C 2 1002-B に渡す。L 2 V N I C 2 1002-B は、フレームを L 2 スイッチ 2 1004-B に転送する。L 2 転送テーブル 1006-B に基づいて、L 2 スイッチ 2 1004-B は、宛先 M A C アドレスが既知であるかどうかを判断する（たとえば、L 2 転送テーブル 1006-B 中のエントリと突き合わせる）。

【0175】

既知である場合、L 2 スイッチ 2 1004-B は、L 2 V N I C 1 1002-A が、関連するトンネルエンドポイントである、と判断し、フレームを L 2 V N I C 1 1002-A に転送する。転送は、フレームのパケットにおけるカプセル化およびパケットのカプセル化解除（たとえば、G E N E V E カプセル化およびカプセル化解除）を含むことができ、パケットは、フレームと、宛先アドレスとしての N V D 1 1001-A の

10

20

30

40

50

物理IPアドレス（たとえば、IP.1）と、送信元アドレスとしてのNVD 2 1001-Bの物理IPアドレス（例えば、IP.2）を含む。

【0176】

未知の場合、L2スイッチ2 1004-Bは、VLANの様々なVNIC（たとえば、VLANのL2 VNIC1 1002-Aおよび任意の他のL2 VNICを含む）にフレームをブロードキャストし、ブロードキャストされたフレームは、関連するNVD間で処理（たとえば、カプセル化、送信、カプセル化解除）される。いくつかの実施形態では、このブロードキャストは、物理ネットワークにおいて実行され、またはより具体的には、物理ネットワークにおいてエミュレートされ、VLAN内のVSRSを含んで、各L2 VNICに、別々に、フレームをカプセル化することができる。したがって、ブロードキャストは、物理ネットワークにおいて一連の複製されたユニキャストパケットを介してエミュレートされる。次いで、各L2 VNICは、フレームを受信し、L2 VNIC2 1002-Bのインターフェース識別子と送信元MACアドレス（例えば、M.2）と送信元物理IPアドレス（例えば、IP.2）との間の関連付けを学習する。

10

【0177】

計算インスタンス1 1000-Aから計算インスタンス2 1000-BへのVLAN内着信トラフィックの場合、NVD2 1001-Bは、NVD1からパケットを受信する。パケットは、送信元アドレスとしてのIP.1およびフレームを有し、フレームは、宛先MACアドレスとしてM.2および送信元MACアドレスとしてM.1を含む。フレームはまた、L2 VNIC1 1002-Aのネットワーク識別子を含む。カプセル化解除で、VNIC2は、フレームを受信し、このインターフェース識別子がM.1および／またはIP.1に関連付けられていることを学習し、以前に未知である場合には、この学習された情報を、L2転送テーブル1006-Bにおいて、スイッチ2に、後の発信トラフィックのために、記憶する。代替として、カプセル化解除で、L2 VNIC2 1002-Bは、フレームを受信し、このインターフェース識別子がM.1および／またはIP.1に関連付けられることを学習し、この情報が既知である場合には、有効時間をリフレッシュする。

20

【0178】

VLAN1000内のインスタンス2 1000-Bから別のVLAN内のインスタンスに送信される発信トラフィックについては、VSRS VNICおよびVSRSスイッチが使用されることを除いて、上記の発信トラフィックと同様の流れが存在し得る。特に、宛先MACアドレスは、VLAN1000のL2ブロードキャスト内にない（それは、他のL2VLAN内にある）。したがって、宛先インスタンスのオーバーレイ宛先IPアドレス（たとえば、IP.A）が、この発信トラフィックのために使用される。例えば、L2 VNIC2 1002-Bは、IP.AがVLAN1000のCIDR範囲外にある、と判断する。したがって、L2 VNIC2 1002-Bは、宛先MACアドレスをデフォルトゲートウェイMACアドレス（たとえば、M.DG）に設定する。M.DGに基づいて、L2スイッチ2 1004-Bは、発信トラフィックをVSRS VNICに（例えば、トンネルを介して、適切なエンドツーエンドカプセル化で）送信する。VSRS VNICは、発信トラフィックをVSRSスイッチに転送する。次に、VSRSスイッチは、ルーティング機能を実行し、ここで、オーバーレイ宛先IPアドレス（例えば、IP.A）に基づいて、VLAN1000のVSRSスイッチは、発信トラフィックを他のVLANのVSRSスイッチに（例えば、これら2つのVLAN間の仮想ルータを介して、適切なエンドツーエンドカプセル化で）送信する。次に、他のVLANのVSRSスイッチは、IP.AがこのVLANのCIDR範囲内にある、と判断することによって、スイッチング機能を実行し、IP.Aに基づいてそのARPキャッシュの検索を実行して、IP.Aに関連付けられる宛先MACアドレスを判断する。ARPキャッシュ内に一致がない場合、宛先MACアドレスを判断するために、他のVLANの異なるL2 VNICに、ARP要求が送信される。そうでない場合には、VSRSスイッチは、発信トラフィックを、関連するVNICに、（例えば、トンネルを介して適切なカプセル化で）送信

30

40

50

する。

【0179】

別のVLAN内のインスタンスからVLAN1000内のインスタンスへの着信トラフィックの場合、トラフィックフローは、逆方向であること除いて上記と同様である。VLAN1000内のインスタンスからL3ネットワークへの発信トラフィックの場合、トラフィックフローは、VLAN1000のVSRSスイッチが仮想ルータを介して仮想L3ネットワーク内の宛先VNICにパケットを直接ルーティングする（例えば、パケットを別のVSRSスイッチを介してルーティングする必要がない）ことを除いて、上記と同様である。仮想L3ネットワークからVLAN1000内のインスタンスへの着信トラフィックの場合、トラフィックフローは、パケットが、パケットをVLAN内でフレームとして送信するVLAN1000AのVSRSスイッチによって受信されることを除いて、上記と同様である。VLAN1000と他のネットワークとの間のトラフィック（発信または着信）については、VSRSスイッチが同様に使用され、そのルーティング機能が発信で使用されて、適切なゲートウェイ（例えば、IGW、NGW、DRG、SGW、LPG）を介してパケットを送信し、そのスイッチング機能が着信で使用されて、VLAN1000内でフレームを送信する。

10

【0180】

ここで図11を参照すると、VLAN1100（例えば、クラウドベースの仮想L2ネットワーク）の実施形態の概略図が示されており、具体的には、VLANの実現図が示されている。

20

【0181】

ここで上述したように、VLANは、「n」個の計算インスタンス1102-A、1102-B、1102-Nを含むことができ、その各々はホストマシン上で実行される。前述のように、計算インスタンスとホストマシンとの間の一対一の関連付け、または複数の計算インスタンスと単一のホストマシンとの間の多対一の関連付けが存在し得る。各計算インスタンス1102-A、1102-B、1102-Nは、L2計算インスタンスとすることができ、その場合、それは、少なくとも1つの仮想インターフェース（例えば、L2 VNIC）1104-A、1104-B、1104-Nおよびスイッチ1106-A、1106-B、1106-Nに関連付けられる。スイッチ1106-A、1106-B、1106-Nは、L2仮想スイッチであり、共にL2分散スイッチ型1107を形成する。

30

【0182】

ホストマシン上の計算インスタンス1102-A、1102-B、1102-Nに関連付けられるL2 VNIC1104-A、1104-B、1104-Nおよびスイッチ1106-A、1106-B、1106-Nのペアは、ホストマシンに接続されたNVD1108-A、1108-B、1108-N上のソフトウェアモジュールのペアである。各L2 VNIC1104-A、1104-B、1104-Nは、顧客の認知された単一スイッチ（ここではvスイッチと呼ぶ）のL2ポートを表す。一般に、ホストマシン「i」は、計算インスタンス「i」を実行し、NVD「i」に接続される。次いで、NVD「i」は、L2 VNIC「i」およびスイッチ「i」を実行する。L2 VNIC「i」は、vスイッチのL2ポート「i」を表す。「i」は1と「n」との間の正の整数である。ここでも、一対一の関連付けが説明されるが、他のタイプの関連付けも可能である。例えば、単一のNVDを複数のホストに接続することができ、各々が、VLANに属する1つ以上の計算インスタンスを実行する。そうである場合、NVDは、計算インスタンスのうちの1つに各々が対応する、L2 VNICおよびスイッチの複数のペアをホストする。

40

【0183】

VLANは、VSRS1110のインスタンスを含むことができる。VSRS1110は、スイッチングおよびルーティング機能を実行し、VSRS VNIC1112およびVSRSスイッチ1114のインスタンスを含む。VSRS VNIC1112は、vスイッチ上のポートを表し、このポートは、仮想ルータを介してvスイッチを他のネットワ

50

ークに接続する。示されるように、VSR S 1 1 1 0は、サーバフリート 1 1 1 6上でインスタンス化され得る。

【0184】

制御プレーン 1 1 1 8は、L 2 V N I C 1 1 0 4 - A、1 1 0 4 - B、1 1 0 4 - N およびV L A Nにおけるそれらの配置を識別する情報を追跡することができる。制御プレーン 1 1 1 0はさらに、この情報をV L A N内のL 2インターフェース 1 1 0 4 - A、1 1 0 4 - B、1 1 0 4 - Nに提供することができる。

【0185】

図 1 1に示すように、V L A Nは、物理ネットワーク 1 1 2 0の上に構築することができるクラウドベースの仮想L 2ネットワークとすることができる。いくつかの実施形態では、この物理ネットワーク 1 1 2 0は、N V D 1 1 0 8 - A、1 1 0 8 - B、1 1 0 8 - Nを含むことができる。

【0186】

概して、V L A Nの第1のL 2計算インスタンス（例えば、計算インスタンス1 1 1 0 2 - A）は、L 2プロトコルを使用してV L A Nの第2の計算インスタンス（例えば、計算インスタンス2 1 1 0 2 - B）と通信することができる。例えば、あるフレームは、V L A Nを介してこれらの2つのL 2計算インスタンス間で送信されることができる。それにもかかわらず、フレームは、フレームが下層の物理ネットワーク 1 1 2 0を介して送信され得るように、カプセル化され、トンネリングされ、ルーティングされ、および／または他の処理を受けることができる。

【0187】

例えば、計算インスタンス1 1 1 0 2 - Aは、計算インスタンス2 1 1 0 2 - B宛てのフレームを送信する。ホストマシン1とN V D 1との間のネットワーク接続、N V D 1と物理ネットワーク 1 1 2 0との間のネットワーク接続、物理ネットワーク 1 1 2 0とN V D 2との間のネットワーク接続、およびN V D 2とホストマシン2との間のネットワーク接続（例えば、T C P / I P接続、イーサネット（登録商標）接続、トンネリング接続など）に応じて、異なるタイプの処理がフレームに適用され得る。例えば、フレームは、フレームが計算インスタンス2に到達するまで、N V D 1によって受信され、カプセル化され、以下同様である。フレームが下層の物理リソース間で送信され得るようにこの処理が仮定され、簡潔かつ明瞭にするために、その説明は、V L A Nおよび関連するL 2動作の説明から省略する。

【0188】

仮想L 2ネットワーク通信

複数の形態の通信が、仮想L 2ネットワーク内で、または仮想L 2ネットワークを用いて生じ得る。これらは、V L A N内通信を含み得る。そのような実施形態では、送信元計算インスタンスは、送信元計算インスタンス（C I）と同じV L A Nにある宛先計算インスタンスに通信を送信することができる。通信は、送信元C IのV L A Nの外部のエンドポイントに送信することもできる。これは、たとえば、第1のV L A N内の送信元C Iと第2のV L A N内の宛先C Iとの間の通信、第1のV L A N内の送信元C IとL 3サブネット内の宛先C Iとの間の通信、および／または第1のV L A N内の送信元C Iから送信元C IのV L A Nを含むV C Nの外部の宛先C Iへの通信を含むことができる。この通信は、さらに、例えば、宛先C IのV L A Nの外部の送信元C Iから、宛先C Iにおいて、通信を受信することを含むことができる。この送信元C Iは、別のV L A N内、L 3サブネット内、または送信元C IのV L A Nを含むV C Nの外部にあり得る。

【0189】

V L A N内の各C Iは、トラフィックフローにおいて能動的役割を果たすことができる。これは、ここではインターフェース対M A Cアドレスとも称される、インターフェース識別子対M A Cアドレスの学習、V L A N内のL 2転送テーブルを維持するためのV L A N内のインスタンスのマッピング、ならびに通信（例えば、L 2通信の場合ではフレーム）の送信および／または受信を含む。V S R Sは、V L A N内の通信において、およびV

10

20

30

40

50

L A Nの外部の送信元C Iまたは宛先C Iとの通信において、能動的役割を果たすことができる。V S R Sは、L 2ネットワーク内およびL 3ネットワーク内における存在を維持して、発信および着信通信を可能にすることができる。

【0190】

ここで図12を参照すると、V L A N内通信のためのプロセス1200の一実施形態を示すフローチャートが示されている。いくつかの実施形態では、プロセス1200は、共通V L A N内の計算インスタンスによって実行され得る。このプロセスは、具体的には、送信元C IがV L A N内の宛先C Iに通信を送信するが、その宛先C IのI P対M A Cアドレスマッピングを知らない場合に実行され得る。これは、例えば、送信元C Iが、V L A NにおいてI Pアドレスを有する宛先C Iにパケットを送信するが、送信元C IがそのI Pアドレスに対するM A Cアドレスを知らない場合に起こり得る。この場合、A R Pプロセスを実行して、宛先M A CアドレスおよびI P対M A Cアドレスマッピングを学習することができる。

10

【0191】

送信元C IがI P対M A Cアドレスマッピングを知っている場合、送信元C Iは、宛先C Iに直接パケットを送信することができ、A R Pプロセスが実行される必要はない。いくつかの実施形態では、このパケットは、V L A N内通信における送信元V N I CがL 2 V N I Cである送信元V N I Cによってインターセプトされ得る。送信元V N I Cが宛先M A Cアドレスについてインターフェース対M A Cアドレスマッピングを知っている場合、送信元V N I Cは、パケットを例えばL 2カプセル化でカプセル化することができ、対応するフレームを、宛先M A Cアドレスに向けて、V L A N内通信における宛先V N I CがL 2 V N I Cである宛先V N I Cに、転送することができる。

20

【0192】

送信元V N I CがM A Cアドレスについてインターフェース対M A Cアドレスマッピングを知らない場合、送信元V N I Cは、インターフェース対M A Cアドレス学習プロセスの局面を実行することができる。これは、送信元V N I CがV L A N内のすべてのインターフェースにフレームを送信することを含むことができる。いくつかの実施形態では、このフレームは、ブロードキャストを介してV L A N内のインターフェースのすべてに送信され得る。いくつかの実施形態では、このブロードキャストは、物理ネットワークにおいてシリアルユニキャストの形態で実現され得る。このフレームは、宛先M A CおよびI Pアドレスと、インターフェース識別子と、送信元V N I CのM A CアドレスおよびI Pアドレスとを含むことができる。V L A N内のV N I Cの各々は、このフレームを受信することができ、送信元V N I Cのインターフェース対M A Cアドレスマッピングを学習することができる。

30

【0193】

受信側V N I Cの各々はさらに、フレームをカプセル化解除し、カプセル化解除されたフレーム（たとえば、対応するパケット）をそれらの関連付けられるC Iに転送することができる。各C Iは、転送されたパケットを評価することができるネットワークインターフェースを含むことができる。転送されたパケットを受信したC Iが宛先M A Cおよび／またはI Pアドレスと一致しない、とネットワークインターフェースが判断した場合、パケットはドロップされる。転送されたフレームを受信したC Iが宛先M A Cおよび／またはI Pアドレスと一致する、とネットワークインターフェースが判断した場合、パケットはC Iによって受信される。いくつかの実施形態では、パケットの宛先M A Cおよび／またはI Pアドレスに一致するM A Cおよび／またはI Pアドレスを有するC Iは、送信元C Iに応答を送信することができ、それによって、送信元V N I Cは、宛先C Iのインターフェース対M A Cアドレスマッピングを学習することができ、それによって、送信元C Iは、宛先C IのI P対M A Cアドレスマッピングを学習することができる。

40

【0194】

送信元C IがI P対M A Cアドレスマッピングを知らない場合、または宛先C Iに対する送信元C IのI P対M A Cアドレスマッピングが古い場合、プロセス1200を実行す

50

ることができる。かくして、IP対MACアドレスマッピングが既知となると、送信元CIはパケットを送信することができる。IP対MACアドレスマッピングが既知でない場合、プロセス1200を実行することができる。インターフェース対MACアドレスマッピングが既知でない場合、上で概説したインターフェース対MACアドレス学習プロセスを実行することができる。インターフェース対MACアドレスマッピングが既知である場合、送信元VNICは、対応するフレームを宛先VNICに送信することができる。プロセス1200はブロック1202から始まり、送信元CIは、宛先CIのIP対MACアドレスマッピングが送信元CIに未知である、と判断する。いくつかの実施形態では、これは、送信元CIが、パケットについて宛先IPアドレスを判断することと、その宛先IPアドレスが送信元CIのマッピングテーブルに記憶されたMACアドレスに関連付けられていないと判断することとを含み得る。代替として、送信元CIは、その宛先CIについてIP対MACアドレスマッピングが古い、と判断し得る。マッピングは、いくつかの実施形態では、マッピングがある時間制限内で更新および／または検証されていない場合、古くあり得る。宛先CIのIP対MACアドレスマッピングが未知である、および／または送信元CIに古いと判断すると、送信元CIは、宛先IPアドレスについてARP要求を開始し、イーサネットブロードキャストのためにARP要求を送信する。

10

【0195】

ブロック1204において、ここでは送信元インターフェースとも呼ばれる送信元VNICは、送信元CIからARP要求を受信する。送信元インターフェースは、VLAN上のすべてのインターフェースを識別し、VLANブロードキャストドメイン上のすべてのインターフェースにARP要求を送信する。前述のように、制御プレーンは、VLAN上のインターフェースのすべてを知っており、その情報をVLANとのインターフェースに提供するので、送信元インターフェースは、同様に、VLAN内のインターフェースのすべてを知っており、VLAN内のインターフェースの各々にARP要求を送信することができる。これを行うために、送信元インターフェースは、ARP要求を複製し、VLAN上のインターフェースの各々のためにARP要求のうちの1つをカプセル化する。各カプセル化されたARP要求は、送信元CIインターフェース識別子と、送信元CI MACアドレスおよびIPアドレスと、ターゲットIPアドレスと、宛先CIインターフェース識別子とを含む。送信元CIインターフェースは、複製されカプセル化されたARP要求（たとえば、ARPメッセージ）をシリアルユニキャストとして送ることによってイーサネットブロードキャストを複製し、1つのARP要求がVLAN内の各インターフェースに送られる。

20

30

【0196】

ブロック1206において、VLANブロードキャストドメイン内の各インターフェースは、ARPメッセージを受信し、カプセル化解除する。ARPメッセージを受信するVLANブロードキャストドメイン内のインターフェースの各々は、このメッセージが送信元CI MACアドレスおよびIPアドレスならびに送信元CIインターフェース識別子を識別するので、送信元CIの送信元VNICのインターフェース対MACアドレスマッピング（例えば、送信元CIのMACアドレスに対する送信元インターフェースのインターフェース識別子）を学習する。送信元CIについてインターフェース対MACアドレスマッピングを学習することの一部として、インターフェースの各々は、そのマッピングテーブル（たとえば、そのL2転送テーブル）を更新することができ、更新されたマッピングをその関連付けられたスイッチおよび／またはCIに提供することができる。各受信側インターフェースは、VSRsを除いて、カプセル化解除されたパケットをそれらの関連付けられたCIに転送することができる。転送されたカプセル化解除されたパケットのCI受信者、具体的にはそのCIのネットワークインターフェースは、ターゲットIPアドレスがCIのIPアドレスと一致するかどうかを判断することができる。そのインターフェースに関連付けられるCIのIPアドレスが宛先CI IPアドレスと一致しない場合、いくつかの実施形態では、パケットはそのCIによってドロップされ、さらなるアクションは行われない。VSRsの場合、VSRsは、ターゲットIPアドレスがVSRsの

40

50

IPアドレスと一致するかどうかを判断することができる。VSR SのIPアドレスが、受信されたパケットにおいて指定されたターゲットIPアドレスと一致しない場合、いくつかの実施形態では、パケットはVSR Sによってドロップされ、さらなるアクションは行われない。

【0197】

受信されたパケットにおいて指定された宛先CI IPアドレスが、受信側インターフェースに関連付けられるCI（宛先CI）のIPアドレスと一致する、と判断された場合、ブロック1208に示すように、宛先CIは、ユニキャストARP応答であり得る応答を送信元インターフェースに送信する。この応答は、宛先CI MACアドレスおよび宛先CI IPアドレスと、送信元CI IPアドレスおよびMACアドレスを含む。この応答は、ブロック1210に示すように、宛先インターフェースによって受信され、それは、ユニキャストARP応答をカプセル化する。いくつかの実施形態では、このカプセル化は、GENEVEカプセル化を含むことができる。宛先インターフェースは、カプセル化されたARP応答を、宛先スイッチを介して送信元インターフェースに転送することができる。この応答は、宛先CI MACアドレスおよびIPアドレスならびに宛先CIインターフェース識別子と、送信元CI MACアドレスおよびIPアドレスならびに送信元CIインターフェース識別子とを含む。

10

【0198】

ブロック1212において、送信元インターフェースは、ARP応答を受信し、それをカプセル化解除する。送信元インターフェースはさらに、カプセル化および／またはカプセル化されたフレームに含まれる情報に基づいて、宛先CIについてのインターフェース対MACアドレスマッピングを学習することができる。送信元インターフェースは、いくつかの実施形態では、ARP応答を送信元CIに転送することができる。

20

【0199】

ブロック1214において、送信元CIはARP応答を受信する。いくつかの実施形態では、送信元CIは、ARP応答に含まれる情報に基づいてマッピングテーブルを更新することができる、具体的には、宛先CIのMACアドレスおよびIPアドレスに基づいてIP対MACアドレスマッピングを反映するようにマッピングテーブルを更新することができる。その後、送信元CIは、このMACアドレスに基づいて宛先CIにパケットを送信することができる。このパケットは、送信元CIのMACアドレスおよびインターフェース識別子を送信元MACアドレスおよび送信元インターフェースとして含み、宛先CIのMACアドレスおよびインターフェース識別子を宛先MACアドレスおよび宛先インターフェースとして含むことができる。

30

【0200】

ブロック1216において、送信元インターフェースは、送信元CIからパケットを受信することができる。送信元インターフェースは、パケットをカプセル化することができる、いくつかの実施形態では、このカプセル化は、GENEVEカプセル化を使用する。送信元インターフェースは、対応するフレームを宛先CIに、具体的には宛先インターフェースに転送することができる。カプセル化されたフレームは、送信元CIのMACアドレスおよびインターフェース識別子を送信元MACアドレスおよび送信元インターフェース識別子として含み、宛先CIのMACアドレスおよびインターフェース識別子を宛先MACアドレスおよび宛先インターフェースとして含むことができる。

40

【0201】

ブロック1218において、宛先インターフェースは、送信元インターフェースからフレームを受信する。宛先インターフェースは、フレームをカプセル化解除することができる、次いで、対応するパケットを宛先CIに転送することができる。ブロック1220において、宛先CIは、宛先インターフェースからパケットを受信する。

【0202】

ストーム制御

物理L2ネットワークは、エンドステーションが大量のフレームを迅速なトラフィック

50

のバーストで送信し得るフレームストームを被る可能性がある。そのようなトラフィックのバーストは、未知のユニキャスト宛先アドレスを有するフレームまたはブロードキャストもしくはマルチキャスト宛先アドレスを有するフレームが複製されるL2ネットワークのフラディング特性によってさらに増幅され得る。そのような「増幅されたトラフィックバースト」は、ネットワーク全体をすばやく停止させ得る。これは、特に、ネットワークがループを有たとえほんの短い期間であっても有する場合に当てはまる。したがって、L2トラフィックストームは、ネットワーク全体の障害を引き起こす可能性がある。スパンニングツリーの使用を含む、L2トラフィックストームを防止するための異なる技術が存在する。しかしながら、そのような技術は、典型的には、物理L2ネットワーク内でのマルチパス通信の使用を禁止する。

10

【0203】

本開示の実施形態は、ここで上述したように、物理ネットワーク（例えば、L3物理ネットワーク）の上にオーバーレイされるL2仮想ネットワークを提供する。仮想化されたL2 V L A N（ここではV L A Nと呼ぶ）などのL2仮想ネットワークは、マルチパス通信を可能にしながらストーム制御を提供する技術を用いて実現される。

【0204】

V L A Nでは、ブロードキャストまたはマルチキャストを使用して、1つの計算インスタンスからV L A N内にある複数の計算インスタンスにフレームを送信することができる。2つの計算インスタンス間にループが存在する場合、ブロードキャストまたはマルチキャストは、フレームストームをもたらし得る。このストームを防止するために、異なる技術が可能である。例示的な技術では、フレーム伝送のレート（例えば、フレーム／秒および／またはビット／秒）は、顧客のスイッチ（ここでは、「vスイッチ」と呼ばれ、それは、顧客の、単一の仮想スイッチの認知に対応することを示す）のポートを表す異なるV N I Cにわたって監視される。ここにおいて上記で説明したように、このvスイッチは、実際には、複数のN V DにわたるL2分散型スイッチであり、各N V Dは、L2分散型スイッチに属する1つ以上のL2仮想スイッチをホストする。レートは、制限ポリシーと比較される。レートがこのポリシーに違反する場合、違反するV N I Cをシャットダウンすることができ、または違反のタイプに応じて、それが処理しているフレームのいくつかをドロップすることができる。ストーム制御のこれらおよび他の局面は、ここにおいて次に記載される。

20

30

【0205】

図13は、ある実施形態に従った、L2仮想ネットワークのためにストーム制御の構成（コンフィグレーション）を定義するのに適した例示的な環境を示す。実施形態では、環境は、1つ以上のネットワーク（図示せず）を介して顧客デバイス1320と通信するコンピュータシステム1310を含む。コンピュータシステム1310は、V C N 1312をホストするハードウェアコンピューティングリソースのセットを含むことができる。ハードウェアコンピューティングリソースのうちの1つ以上によってホストされる制御プレーンは、顧客デバイス1320から入力を受信し、処理し、V C N 1312内にL2仮想ネットワーク（図13ではL2 V L A N 1314として示される）を展開することができる。

40

【0206】

ある例では、顧客デバイス1320からの入力は、様々なタイプの情報を含むことができる。この情報は、コンソールまたはA P I呼出しを介して指定することができ、顧客指定される構成情報の中でもとりわけ、L2 V L A N構成1322およびストーム制御構成1324を含むことができる。

【0207】

L2 V L A N構成1322は、例えば、L2 V L A N 1314に含まれるべきL2計算インスタンスの数、タイプ、および構成を示すことができる。加えて、L2 V L A N構成1322は、顧客認知vスイッチ上のポートの顧客指定名、（L2計算インスタンスであり得る）計算インスタンスのM A Cアドレス、およびポートとM A Cアドレス（ま

50

たは、より一般的には、計算インスタンス）との間の関連付けを示すことができる。例えば、顧客は、L 2 V L A N 1 3 1 4 が 2 つの L 2 計算インスタンスを含む必要があることを指定することができ、第 1 の L 2 計算インスタンスは M A C アドレス M . 1 を有し、P 1 と名付けられた第 1 のポートに関連付けられ、第 2 の L 2 計算インスタンスは M A C アドレス M . 2 を有し、P 2 と名付けられた第 2 のポートに関連付けられる。

【 0 2 0 8 】

ストーム制御構成 1 3 2 4 は、例えば、L 2 V L A N 1 3 1 4 内の、V L A N 1 3 1 4 への、および／または V L A N 1 3 1 4 からのフレームを含むトラフィックの流れを制御するストーム制御ポリシーを示すことができる。ストーム制御ポリシーは、アクションのセットおよびトラフィックフロー条件のセットを示すことができる。あるトラフィックフロー条件が検出されるか、またはその違反が検出される（例えば、測定される）と、対応するアクションが開始または実行され得る。ストーム制御構成 1 3 2 4 は、トラフィックフロー条件の違反のタイプに応じてトラフィックのフローをさらに制御するエスカレーションポリシーをさらに示すことができる。例えば、エスカレーションポリシーは、違反が、ある持続時間内で（例えば、特定の違反頻度もしくは回数で）繰り返し検出されるか、またはある持続時間を超える時間長にわたって持続する場合、別のアクションのセット（例えば、エスカレーションアクション）が開始または実行され得ることを示す。

【 0 2 0 9 】

実施形態では、異なるストーム制御構成タイプが可能であり、互いに併せてまたは独立して使用することができる。第 1 のストーム制御構成タイプは、ストーム制御が v スイッチの特定のポート（またはそのポートのサブセット）に適用されるか、またはポートの全セットに（たとえば、V L A N 全体に）適用されるかを示す。特に、顧客は、ポートごと、ポートのセット、および／またはポートの全セットの許容伝送レート（例えば、フレーム／秒および／またはビット／秒の単位で定義される最大伝送レート）を指定することができる。第 2 のストーム制御構成タイプは、ストーム制御がユニキャストされるフレーム、ならびに／またはブロードキャストされるフレームおよび／もしくはマルチキャストされるフレームに適用されるかどうかを示す。第 3 のストーム制御構成タイプは、ストーム制御のために使用すべき伝送レートのタイプ（例えば、フレーム／秒および／またはビット／秒）を示す。第 4 のストーム制御構成タイプは、ストーム制御ポリシーの違反に対して実行されるべきアクションを示す。例えば、顧客は、許可された伝送レートを超えるフレームがドロップされるべきであることを指定することができる。代替的に、顧客は、許可された伝送レートに違反するポート（例えば、そのポートは、許可された伝送レートを超えるフレームを受信および／または送信する）をシャットダウンし動作停止する（例えば、リンク状態をダウンする）べきであると指定することができる。第 5 のストーム制御構成タイプは、フレームをドロップし、続いてポートシャットダウンを含む、エスカレーションポリシーを定義することができる（例えば、違反が断続的である場合、超過フレームを破棄することができる。しかし、違反が、ある期間にわたって、より持続的である場合、違反するポートはシャットダウンされるべきである）。第 6 のストーム制御構成タイプは、報告されるべきメトリックおよび／または統計を示し、これらのメトリックおよび／または統計は、トラブルシューティングのために使用され得る。例えば、顧客は、システムログ（syslog）、フローログ、特定のメトリック（例えば、どれだけのフレームが送信されたか、どれだけのフレームがドロップされたか、どのようなポートが使用されたか、どれだけの頻度でフレームがドロップされたか（例えば、フレームドロップレート）、どれだけの頻度でフレーム伝送スパイク（例えば、許可された伝送レートのある量だけを超える）が観察されたかなど）、ウォーターマーク（例えば、最も高い送信スパイクおよびそのタイミング）、ならびに違反に関する警告を要求することができる。

【 0 2 1 0 】

上記の入力は、制御プレーンによって受信されることができ、顧客は、各ストーム制御構成タイプのパラメータを、それ自体の顧客プレゼンテーションを使用して（例えば、v スイッチのポートの、それ自体の命名法を使用することによって）、指定する。制御プレ

10

20

30

40

50

ーンは、実際のネットワーク実現例（たとえば、L2分散型スイッチ）およびL2VLAN構成1322（たとえば、ポートの顧客定義）に基づいてストーム制御情報を生成する。制御プレーンはまた、生成されたストーム制御情報をNVDに配信し、NVDによるストーム制御の実施を編成する。

【0211】

したがって、制御プレーンは、種々の情報を受信し、次いで、L2VLAN1314の異なるリソースを展開および管理し、関連するストーム制御構成を生成し、これらのリソースに配信する。例えば、L2VLAN1314は、L2VLAN構成1322に従って構成され、ホストマシン上でホストされる要求された計算インスタンスと、NVD上でホストされるL2VNIC-L2仮想スイッチのペアを含む。ストーム制御構成を生成するために、制御プレーンは、顧客定義をストーム制御構成からL2VLAN1314の実際のトポロジに変換する。たとえば、各L2VNICはポートをエミュレートし、制御プレーンは、L2VNIC（例えば、そのインターフェース識別子、そのMACアドレス（指定されない場合）、および／またはL2VNICをホストするNVDのIPアドレス）を、ポートの名前（および、指定される場合には、指定されたMACアドレス）と、関連付ける。ポート名を使用するのではなく、ストーム制御構成は、関連するL2VNIC（例えば、それらのインターフェース識別子、それらのMACアドレス、および／またはL2VNICをホストするNVDのIPアドレス）を識別することによって、ストーム制御を示す。L2VNICをホストするNVDは、L2VNICに関連付けられるストーム制御構成を受信して適用し、NVDはトラフィックフロー実施を実行することができる。

10

20

【0212】

図14は、ある実施形態による、レイヤ2仮想ネットワークにおける例示的なストーム制御技術を図示する。レイヤ2仮想ネットワークは、ここではVLANと呼ばれる。図14の上部は、VLANの実現図1410を示す。図14の下部は、VLANの顧客プレゼンテーション1420を示す。

【0213】

ここで上述したように、VLANは、「n」個の計算インスタンスを含むことができ、それらの各々はホストマシン上で実行される。図14は、計算インスタンスとホストマシンとの間の一対一の関連付けを示しているが、1つのホストマシンが複数の計算インスタンスを実行することができる、多対一の関連付けが可能である。各計算インスタンスは、少なくとも1つの仮想インターフェース（例えば、L2VNIC）およびスイッチ（例えば、L2仮想スイッチ）に関連付けられる。ホストマシン上の計算インスタンスに関連付けられるVNICおよびスイッチのペアは、ホストマシンに接続されたNVD上のソフトウェアモジュールのペアであり得る。各L2VNICは、顧客のvスイッチのL2ポートを表す。図14の例示では、ホストマシン「i」は、計算インスタンス「i」を実行し、NVD「i」に接続される。次に、NVD「i」は、VNIC「i」およびスイッチ「i」を実行する。VNIC「i」は、vスイッチのL2ポート「i」を表す。iは1～nの正の整数である。ここでもまた、一対一の関連付けが説明されるが、他のタイプの関連付けも可能である。例えば、単一のNVDを複数のホストに接続することができ、それらの各々が、VLANに属する1つ以上の計算インスタンスを実行する。その場合、NVDは、各々が計算インスタンスのうちの1つに対応するVNICおよびスイッチの複数のペアをホストする。

30

40

【0214】

顧客の入力は、制御プレーン（例えば、VLANを含むVCNの制御プレーン）によって受信され得る。入力は、API呼出しおよび／またはコンソールを介して受信することができ、ストーム制御の異なる次元を指定することができる。ストーム制御の編成は、制御プレーンによって管理することができ、ストーム制御の実施は、NVD（データプレーン）のレベルで行うことができる。

【0215】

50

ある例では、ここにおいて上記で説明したように、NVDのL2 VNICは、着信トラフィックに基づいてインターフェース対MACアドレスマッピングを学習する。そのようなマッピングは、VLANの識別子とともに制御プレーンに送られ得る。制御プレーンは、異なるL2 VNICをホストする異なるNVDから同様のマッピングを受信し、インターフェース識別子と、MACアドレスと、（たとえば、NVDの）物理IPアドレスと、VLAN識別子と、ストーム制御パラメータとの間のマッピングを生成することができる。

【0216】

例えば、VNIC1は、M.2（計算インスタンス2のオーバーレイMACアドレス）はID.2（L2 VNIC2のインターフェース識別子）およびIP.2（NVD2の物理アドレス）に関連付けられること、ならびにM.n（計算インスタンスnのオーバーレイMACアドレス）はID.n（L2 VNIC nのインターフェース識別子）およびIP.n（NVD nの物理アドレス）に関連付けられることを学習する。同様に、VNIC2は、M.1（計算インスタンス1のオーバーレイMACアドレス）はID.1（L2 VNIC1のインターフェース識別子）およびIP.1（NVD1の物理アドレス）に関連付けられることを学習する。これらの関連付けは、マッピングの一部として制御プレーンに報告され、制御プレーンは、{顧客1；M.1→ID.1；IP.1；VLAN A}、{顧客1，M.2→ID.2，IP.2；VLAN A}，...，{顧客1，M.n→ID.n，IP.n；VLAN A}のマッピングを生成することができる。

【0217】

顧客入力または、図13に関連して説明したL2 VLAN構成に加えて、ストーム制御構成1422を指定することができる。説明のため、顧客入力は、ストーム制御構成1422の一部として、ポート1、2、およびnの各々は、それぞれ1,000FPS、2,000FPS、および3,000FPSの制限を有し、違反が生じる場合、フレームをドロップすべきであることを指定する。（例えば、L2 VLAN構成からの）そのVLANの顧客定義と実際の実現例との間の関連付け（例えば、VNIC1,2,...,nは、それぞれポート1,2,...,nに対応する）に基づいて、制御プレーンは、VLAN全体に対するストーム制御情報1411、すなわち、{顧客1；M.1→ID.1，IP.1；VLAN A；制限：1,000FPS；アクション：ドロップ}，{顧客1，M.2→ID.2，IP.2；VLAN A；制限：2,000FPS；アクション：ドロップ}，...，{顧客1，M.n→ID.n，IP.n；VLAN A，制限：3,000FPS；アクション：ドロップ}を含むことができる。この例示的な例では、「制限」はトラフィックフロー条件に対応し、その値（例えば、「1,000FPS」）は最大FPSレートに対応し、「アクション：ドロップ」は、最大FPSレートを越えたときにフレームをドロップするアクションに対応する。

【0218】

別の例示では、顧客入力は、断続的な違反時にフレームをドロップし、持続的な違反時に違反ポートをシャットダウンするために、VLAN内で許容される総制限（たとえば、6,000FPS）を指定することができる。制御プレーンは、ポート（例えば、L2 VNIC）にわたって総制限を割り当て、ポートごとの個別の制限（例えば、総制限を「n」で割ったものなど、L2 VNICあたり）を判断することができる。動的乗数「X」は、各個別の制限に関連付けられ、確認された違反に応じて経時的に調整され得る（例えば、L2 VNIC1に対する動的乗数「X」は、最初に「2」に設定され、違反が確認される場合、増加され、ある期間内に違反が確認されない場合、減少される）。さらに、制御プレーンは、FPSに基づいて違反時にフレームがドロップされるべきであること、およびある期間内に閾値を超えるフレームの総数に基づいて違反ポートがシャットダウンされるべきであることを定義することができる。例えば、L2 VNIC1の場合、制御プレーンは、以下の個別のストーム制御情報 {制限：(6,000/3)*X；X=2；アクション：フレームをドロップする；エスカレーション：1時間以内のフレームの総数が10,000,000フレームを超える場合、シャットダウン} を生成する。制御

プレーンは、残りの L2 VNIC について同様の個別のストーム情報を生成し、そのような情報の各々は、VLAN 全体の全体的なストーム制御情報 1411（例えば、{顧客 1, M.1→ID.1, IP.1; VLAN A; 制限: (6, 000/3) * X; X=2; アクション: フレームをドロップする; エスカレーション: 1 時間以内のフレームの総数が 10, 000, 000 フレームを超える場合、シャットダウン}）に含めることができる。

【0219】

その VLAN の顧客定義と実際の実現との間の関連付け（例えば、L2 VNIC 1 はポート 1 に対応する）およびマッピング（例えば、顧客 1, M.1→ID.1; IP.1; VLAN A）に基づいて、制御プレーンは、ストーム制御のローカル実施のために、関連する個別のストーム制御部分を NVD に配信することができる。例えば、L2 VNIC 1 に適用可能な個別のストーム制御情報 1414 (1) は、L2 VNIC 1 をホストする NVD 1 に送信される。例示の目的で、この個別のストーム制御情報 1414 (1) は {VNIC 1→制限: 1, 000 FPS; アクション: ドロップ} を含むか、または、適応可能な場合、{VNIC 1→制限: (6, 000/3) * X; X=2; アクション: フレームをドロップする; エスカレーション: 1 時間以内のフレームの総数が 10, 000, 000 フレームを超える場合、シャットダウン} が NVD 1 に送信される。同様に、L2 VNIC 2 に適用可能な個別のストーム制御情報 1414 (2) が、L2 VNIC 2 をホストする NVD 2 に送信される。顧客はまた、ポートのセット（例えば、ポート n）についてストーム制御を要求しなくてもよい。したがって、個別のストーム制御情報は生成されず、関連する NVD に送信されなくてもよい（例えば、L2 VNIC n に対して個別のストーム制御情報が定義されず、NVD n に送信されない）。

【0220】

ストーム制御の実施は、NVD によって、着信トラフィックおよび／または発信トラフィックに対して実行され得る。着信実施のため、および例示目的で NVD 1 を参照して、NVD 1 は、適用可能なトラフィックフロー条件（例えば、ストーム制御ポリシーおよび／もしくはエスカレーションポリシーの FPS ならびに／または BPS 制限）と比較するために、L2 VNIC 1 へのトラフィックフロー（例えば、L2 VNIC 1 に送信されるフレームの FPS および／もしくは BPS などの伝送レート、ならびに／または L2 VNIC 1 に送信される 1 時間以内のフレームもしくはビットの総数などの総伝送量）を監視する。違反が検出された場合、NVD 1 は適用可能なアクションを実行する（例えば、L2 VNIC 1 に送信されたフレームをドロップするか、または L2 VNIC 1 をリンクダウンし停止する）。対照的に、発信実施のため、および例示目的で NVD 1 も参照すると、NVD 1 は、残りの NVD の個別のストーム制御情報を受信し、この情報を L2 VNIC 1 からの発信実施のために使用する。例えば、NVD 1 は、制御プレーンから、NVD 2 に対して設定された適用可能な制限を受信する。L2 VNIC 1 によって L2 VNIC 2 に送信されるフレームの伝送レート（例えば、FPS および／または BPS）が FPS 制限および／または BPS 制限を超える場合、そのようなフレームは、NVD 2 に送信され、次いでそこでドロップされるのではなく、NVD 1 によってドロップされる。そのようなフレームの総伝送量が許容時間単位制限を超える場合、L2 VNIC 1 はリンクダウンされる。

【0221】

異なる NVD は、フレーム伝送およびフレームドロップに関する情報を制御プレーンに報告することができる。この情報は、伝送レート、総伝送量（たとえば、送信されるフレームの総数、および／または送信されるビットの総数）、ドロップレート、総ドロップ量（例えば、ドロップされたフレームの総数および／またはドロップされたビットの総数）、実行されるアクション（例えば、ドロップ、シャットダウン、エスカレーション）などを含むことができる。NVD から送信される情報は、関連する L2 VNIC および／または VLAN に関するメタデータで注釈を付けることができる（例えば、メタデータは、関連する L2 VNIC を識別することができ、VLAN ID を含むことができる）。

【0222】

次に、制御プレーンは、異なるNVDから情報を収集し、顧客によって要求されるメトリックおよび／または統計を生成することができる。警告をプッシュすることができる。他のタイプのメトリックおよび／または統計を、顧客の要求に応じてプッシュまたは提示することができる。

【0223】

動的乗数「X」がストーム制御の構成情報において使用される場合、制御プレーンは、伝送レートおよび／または総伝送量が設定された制限とどのように対比されるかの比較をすることができる。比較に応じて、動的乗数「X」は、各VNICについて増加または減少させることができる。

【0224】

ここにおいて上記でさらに説明されるように、顧客のVLANは、VSR Sのインスタンスを含むことができる（図14に図示せず）。VSR Sは、スイッチングおよびルーティング機能を実行し、vスイッチ上のポートを表すVSR S VNICを含み、このポートは、仮想ルータを介してvスイッチを他のネットワークに接続する。ストーム制御の同様の構成情報が、VSR Sのために生成され、ローカル実施のためにVSR Sに送信され得る。さらに、VSR Sが別のネットワークとの間でルーティングするであろうトラフィックのドロップをサポートするために、マッピングは、計算インスタンスのオーバーレイIPアドレスを含むことができる。（例えば、送信元または宛先IPアドレスとしての）計算インスタンスのオーバーレイIPアドレスを有するトラフィックが違反をもたらす場合、VSR Sは、このトラフィックをドロップすることができ、エスカレーション構成に応じて適用可能な場合、VSR S VNICをリンクダウンすることができる。

【0225】

図15は、いくつかの実施形態による、L2仮想ネットワークにおいてストーム制御情報を使用するためのプロセスを示すシーケンス図である。実施形態では、顧客によって操作されるリモートデバイス1510（例えば、顧客のオンプレミスネットワークからのデバイスであって、顧客デバイス1320等の、VCNに遠隔接続されるデバイス）は、制御プレーン1520と通信して、顧客のVLANのためにストーム制御を構成する。制御プレーン1520は、VLANのL2 VNICおよびL2仮想スイッチをホストするNVD1530によるストーム制御の実施を編成する。

【0226】

図示のように、シーケンス図は、顧客デバイス1510が顧客の入力を制御プレーン1520に送信する状態でストーム制することができる。入力、他の情報（例えば、VLAN構成）の中でも、とりわけ、ストーム制御構成を示す。ストーム制御構成は、顧客が認知するvスイッチの、あるポート、ポートのセット、またはポートの全セットに特定であり得る。次に、制御プレーン1520は、ストーム制御構成に基づいてストーム制御情報を生成する。ストーム制御情報は、VLANに適用されるグローバルストーム制御情報を含むことができ、および／またはL2 VNICごとに個別のストーム制御情報を含むことができる。概して、制御プレーン1520は、ストーム制御構成をポートの顧客定義からL2 VNIC実現例に変換し、ストーム制御ポリシー、エスカレーションポリシー、またはそれに対する修正（例えば、動的乗数「X」に基づいて伝送制限を調整することによる）をストーム制御情報に含ませることができる。制御プレーン1520はまた、ストーム制御情報を受信することになるNVD130のセットを判断する。概して、ストーム制御が適用されるポートを顧客が指定する場合、制御プレーン1520は、対応するL2 VNICと、このL2 VNIC1530をホストするNVD1530とを判断する。L2 VNICに対して定義され（顧客によってポートに対して定義されるストーム制御構成に対応する）個別のストーム制御情報が、NVD1530に送信される。

【0227】

次に、NVD1530は、関連するストーム制御情報を受信して記憶する。NVD1530によってホストされ、個別のストーム制御情報が記憶されるL2 VNICへの着信

10

20

30

40

50

トラフィックは、NVDによって制御される。同様に、L2 VNICから（異なるNVD上でホストされ得る）別のL2 VNICへの発信トラフィックは、NVDによって、このストーム制御情報および／または別のL2 VNICのストーム制御情報を使用して、制御され得る。制御は、トラフィックフロー条件またはその違反が検出されたかどうか、ならびに／またはストーム制御ポリシーおよび／もしくはエスカレーションポリシーを実施するための違反のタイプを判断することを含むことができる。

【0228】

さらに、NVD1530は、L2 VNICの着信および／もしくは発信トラフィックフローに関するメトリックならびに／または統計を収集することができる。そのようなメトリックおよび／または統計は、プッシュ機構（例えば、周期的）またはプル機構（例えば、制御プレーン1520からのオンデマンド）を使用して制御プレーン1520に報告される。制御プレーン1520は、NVD1530から受信されたメトリック／統計を顧客デバイス1510に送信することができ、ならびに／または複数のNVD1530から報告されたメトリックおよび／もしくは統計の集約または組合せに基づいて新たなメトリックおよび／もしくは統計を生成し、顧客デバイス1510に送信することができる。さらに、制御プレーン1520は、NVD1530のうちの1つ以上から報告されたメトリックおよび／または統計に基づいて、ストーム制御情報に対する更新を生成することができる。例えば、L2 VNICに対して設定されたFPS制限を参照して、この制限が部分的に乗数「X」を使用して定義される場合、この乗数は、L2 VNICに対する着信および／もしくは発信トラフィックの量を示すメトリックならびに／もしくは統計、ならびに／またはL2 VNICに対して定義されるストーム制御ポリシーおよび／もしくはエスカレーションポリシーの違反タイプに応じて調整（例えば、増加または減少）することができる。NVD1530に関連付けられる個別のストーム制御情報に対する更新は、NVD1530に（例えば、プッシュ機構で）送信することができる。追加または代替として、更新されたストーム制御情報全体がこのNVD1530に送られ得る。

【0229】

図16は、いくつかの実施形態による、ストーム制御情報を判断し、生成し、配信するためのプロセス1600を示すフローチャートである。いくつかの実施形態では、プロセス1600は、下層の物理ネットワーク上でのレイヤ2仮想ネットワークの展開を管理する制御プレーンによって実行されることができる。

【0230】

プロセス1600はブロック1602で開始し、制御プレーンは顧客のネットワーク構成を記憶し、この構成はポートの定義を示す。いくつかの実施形態では、顧客の入力は、API呼出しおよび／またはコンソールを介して顧客デバイスから受信され、L2仮想ネットワーク構成（例えば、図13に関連して説明されたようなL2 VLAN構成）を示す。この入力または、L2仮想ネットワークの顧客認知vスイッチのためのポートの顧客定義を示すことができる。この入力または、ネットワーク構成の一部として記憶することができる。

【0231】

ブロック1604において、制御プレーンは、L2仮想ネットワークのアドレスとL2仮想ネットワークをホストする物理ネットワークのアドレスとを関連付けるマッピング情報を記憶する。例えば、L2仮想ネットワークは、計算インスタンスと、計算インスタンス毎に、L2 VNICとL2仮想スイッチとのペアを含む。物理ネットワークは、計算インスタンスを実行するホストマシンと、L2 VNIC-L2仮想スイッチのペアを実行するNVDとを含む。計算インスタンスのアドレス（例えば、IPアドレス）および／またはL2 VNICのアドレス（例えば、MACアドレスおよびインターフェース識別子）は、ホストマシンおよびNVDのアドレス（例えば、IPアドレス）にマッピングすることができる。

【0232】

ブロック1606において、制御プレーンは、ストーム制御構成を示す顧客入力を受信

する。いくつかの実施形態では、顧客入力、ストーム制御構成（例えば、図 13 に関連して説明したストーム制御構成）を示すために、API 呼出しおよび／またはコンソールを介して顧客デバイスから受信される。

【0233】

ブロック 1608 において、制御プレーンは、ストーム制御情報を受信すべき NV D のセットを判断する。いくつかの実施形態では、ストーム制御構成は、v スイッチのポートに対して指定される。ネットワーク構成に基づいて、制御プレーンは、ポートと L 2 仮想ネットワークの L 2 V N I C との間の対応関係を判断する。マッピング情報に基づいて、制御プレーンは、L 2 V N I C と物理ネットワークの NV D との間の関連付けを判断し、この NV D は L 2 V N I C をホストする。したがって、制御プレーンは、制御情報が L 2 V N I C のために定義され、NV D に送信されるべきであると判断する。同様の判断を、ポートのセットまたはポートの全セットにストーム制御構成が適用されることを顧客の入力が示すかどうかに応じて、NV D のセット上でホストされる L 2 V N I C のセットに対して、または複数の NV D 上でホストされるすべての L 2 V N I C に対して、行うことができる。

10

【0234】

ブロック 1610 において、制御プレーンは、マッピング情報およびネットワーク構成に基づいてストーム制御情報を生成する。いくつかの実施形態では、制御プレーンは、ネットワーク構成に基づいて、顧客指定ポートを L 2 V N I C に変換し、マッピング情報に基づいて、関連付けられる NV D を判断する。制御プレーンはまた、図 14～図 15 に関連して説明したように、ストーム制御構成から、L 2 V N I C のために定義されるストーム制御情報に含めるために、および NV D に展開されるよう、ストーム制御ポリシー、エスカレーションポリシー、および／またはそれに対する修正を判断することができる。

20

【0235】

ブロック 1612 において、制御プレーンは、NV D のセットにストーム制御情報を送信する。いくつかの実施形態では、適用可能な場合には、個別のストーム制御情報が、L 2 V N I C のために生成される。この個別のストーム制御情報は、L 2 V N I C をホストする NV D に送信される。

【0236】

図 17 は、いくつかの実施形態による、収集されたメトリックに基づいてストーム制御ポリシーを更新するためのプロセス 1700 を示すフローチャートである。いくつかの実施形態では、プロセス 1700 は、NV D に以前に送信されたストーム制御情報を更新するために制御プレーンによって実行され得る。

30

【0237】

プロセス 1700 はブロック 1702 で始まり、制御プレーンは、収集するメトリック／統計のタイプを NV D のセットに示す。いくつかの実施形態では、NV D は L 2 V N I C をホストする。メトリック／統計のタイプは、L 2 V N I C の着信トラフィックフローおよび／または発信トラフィックフローに関連し得る（例えば、着信および／または発信フローの FPS、BPS、違反数、違反率、違反の時間長の持続性など）。この L 2 V N I C は、顧客がメトリック／統計監視について顧客の入力において識別したポートに対応することができる。メトリック／統計のタイプは、顧客によって入力において指定され得る。追加または代替として、制御プレーンは、ストーム制御ポリシーおよび／またはエスカレーションポリシーに対する更新を行うことができるように、監視すべきメトリック／統計のタイプを定義することができる。メトリック／統計のタイプは、定義され、NV D に送信されるストーム制御情報に、または NV D に送信される別個の情報に、含まれ得る。

40

【0238】

ブロック 1704 において、制御プレーンは、NV D のセットから、L 2 仮想ネットワーク内のトラフィックフローに関するメトリックおよび／または統計を受信する。いくつ

50

かの実施形態では、上記の情報を受信したNVDは、示されたタイプごとにメトリックおよび／または統計を収集することができ、それらを制御プレーンに報告することができる。次に、制御プレーンは、そのようなメトリックおよび／または統計を複数のNVDから経時的に収集することができる。

【0239】

ブロック1706において、制御プレーンは、フロー制御情報に対する更新を判断する。いくつかの実施形態では、フロー制御情報は、複数のL2 VNICに適用されるグローバルフロー制御情報である。この場合、更新は、複数のL2 VNICに関連するメトリックおよび／または統計値に応じて、関連するNVDに対する制御パラメータ（たとえば、制限、乗数）またはアクション（例えば、ドロップする代わりに、リンクダウンを実行する）を変更することであり得る。他の実施形態では、フロー制御情報は、特定のL2 VNICに適用される個別のフロー制御情報である。この場合、更新は、そのL2 VNICもしくは複数のL2 VNICに固有のメトリックおよび／または統計に応じて、L2 VNICをホストするNVDについて制御パラメータ（たとえば、制限、乗数）またはアクション（例えば、ドロップする代わりに、リンクダウンを実行する）を変更することであり得る。

10

【0240】

ブロック1708において、制御プレーンは、更新を受信するNVDのセットを判断する。いくつかの実施形態では、更新はグローバルストーム制御情報に対するものである。この場合、この情報を受信したNVDが識別される。いくつかの実施形態では、更新は、NVD上でホストされるあるL2 VNICの個別のストーム制御情報に対するものである。この場合、このNVDが識別される。

20

【0241】

ブロック1710において、制御プレーンは、更新または更新されたストーム制御情報をNVDのセットに送信する。いくつかの実施形態では、プッシュ機構が使用される。

【0242】

図18は、いくつかの実施形態による、ストーム制御情報を更新するためのプロセス1800を示すフローチャートである。いくつかの実施形態では、プロセス1800は、制御プレーンと通信しており、計算インスタンスとペアとして関連付けられるL2 VNICおよびL2仮想スイッチを実行するNVDによって実行され得る。L2 VNIC、L2仮想スイッチ、および計算インスタンスは、顧客のL2仮想ネットワークに属することができる。

30

【0243】

プロセス1800は、ブロック1802で開始し、NVDは、L2 VNICおよびL2仮想スイッチをホストし、L2 VNICに関連付けられるストーム制御情報を受信し、記憶する。いくつかの実施形態では、このストーム制御情報は、L2 VNICのために定義された個別のストーム制御情報であり、制御プレーンから受信される。いくつかの実施形態では、このストーム制御情報は、複数のNVDによってホストされる複数のL2 VNICのために定義されたグローバルストーム制御情報であり、制御プレーンによって複数のNVDに送信される。

40

【0244】

ブロック1804において、NVDは、L2 VNICへのトラフィックフローおよび／またはL2 VNICからのトラフィックフローを監視する。いくつかの実施形態では、監視は、L2 VNICへの着信トラフィックに対してであり、ストーム制御情報によって示されるストーム制御ポリシーおよび／またはエスカレーションポリシーに基づいて実行される。例えば、ストーム制御情報は、L2 VNICに対する着信フレームのFPSおよび／または着信ビットのBPSに対する制限を示す。したがって、L2 VNICへのトラフィックのFPSおよび／またはBPSは、経時的に監視される。他の実施形態では、監視は、L2 VNICからの発信トラフィックに対してであり、L2 VNICまたは別のL2 VNICに対して定義されたストーム制御情報によって示されるストー

50

ム制御ポリシーおよび／またはエスカレーションポリシーに基づいて実行される。例えば、ストーム制御情報は、L2 VNICに対する発信フレームのFPSおよび／または発信ビットのBPSに対する制限を示す。したがって、L2 VNICからのトラフィックのFPSおよび／またはBPSは、経時的に監視される。

【0245】

ブロック1806において、NVDは、ストーム制御ポリシー違反が検出されたかどうかを判断する。いくつかの実施形態では、ストーム制御情報は、トラフィックフロー条件を指定したストーム制御ポリシーを示す。監視されるトラフィックフローは、トラフィックフロー条件と比較されて、違反が生じているか否かが判断される。たとえば、FPS／BPS制限がストーム制御ポリシーによって定義され、監視されるFPS／BPSがこの制限（たとえば、最大伝送レート）を超える場合、違反が検出される。ストーム制御ポリシー違反が検出された場合、ブロック1810がブロック1806に続く。そうでない場合、ブロック1820がブロック1806に続く。

10

【0246】

ブロック1810において、NVDは、違反のタイプを判断する。いくつかの実施形態では、ストーム制御ポリシーは、ある持続時間を示す。違反の時間長がその持続時間を超える場合、許容できない持続的違反が検出される。そうでない場合、違反は非持続的であると判断される。他の実施形態では、ストーム制御ポリシーは違反率（例えば、単位時間内の違反の数）を示す。単位時間当たりの違反の検出数が違反率を超える場合、許容できない頻繁な違反が検出される。そうでなければ、違反はまれであると判断される。

20

【0247】

ブロック1812において、NVDは、違反のタイプに基づいてアクションを開始する。いくつかの実施形態では、ストーム制御ポリシーは、違反が持続的でないおよび／またはまれであるときに実行されるべきアクションを示す。そうでない場合、ストーム制御ポリシーは、アクション（例えば、違反が持続的および／または頻繁であるときに実行される時のエスカレートしたアクション）を示すエスカレーションポリシーを指す。NVDは、アクションを実行する（例えば、フレームをドロップする、L2 VNICをリンクダウンするなど）。

【0248】

ブロック1820において、NVDは、L2 VNICから、および／またはL2 VNICに、フレームを送信する。特に、違反は検出されない。したがって、ストーム制御を適用する必要はなく、着信トラフィックおよび／または発信トラフィックは変更されない。

30

【0249】

ブロック1822において、NVDは、メトリックおよび／または統計を収集し、制御プレーンに送信する。メトリックおよび／または統計のタイプは、ここで上記で説明したように、制御プレーンによってNVDに事前に示され得る。NVDは、収集されたメトリックおよび／または統計をプッシュまたはプル機構で報告することができる。

【0250】

C. 例示的なサービスとしてのインフラストラクチャのアーキテクチャ

40

上述したように、IaaS (Infrastructure as a Service) は、1つの特定の種類のクラウドコンピューティングである。IaaSは、パブリックネットワーク（例えば、インターネット）を介して仮想化計算リソースを提供するように構成されてもよい。IaaSモデルにおいて、クラウドコンピューティングプロバイダは、インフラストラクチャ要素（例えば、サーバ、記憶装置、ネットワークノード（例えば、ハードウェア）、展開ソフトウェア、プラットフォーム仮想化（例えば、ハイパーバイザ層）など）をホストすることができる。場合によっては、IaaSプロバイダは、インフラストラクチャ要素に付随する様々なサービス（例えば、課金、監視、ロギング、セキュリティ、負荷分散およびクラスターリングなど）を提供することができる。したがって、これらのサービスがポリシー駆動型であり得るため、IaaSユーザは、アプリケーションの可用性および性能を

50

維持するために、負荷分散を駆動するためのポリシーを実装することができる。

【0251】

いくつかの例において、IaaS顧客は、インターネットなどの広域ネットワーク（WAN）を介してリソースおよびサービスにアクセスすることができ、クラウドプロバイダのサービスを使用してアプリケーションスタックの残りの要素をインストールすることができる。例えば、ユーザは、IaaSプラットフォームにログインして、仮想マシン（VM）を作成し、各VMにオペレーティングシステム（OS）をインストールし、データベースなどのミドルウェアを展開し、ワークロードおよびバックアップの記憶バケットを作成し、VMに企業ソフトウェアをインストールすることができる。顧客は、プロバイダのサービスを使用して、ネットワークトラフィックのバランシング、アプリケーションのトラブルシューティング、パフォーマンスの監視、災害復旧の管理などを含む様々な機能を実行することができる。

10

【0252】

殆どの場合、クラウドコンピューティングモデルは、クラウドプロバイダの参加を必要とする。クラウドプロバイダは、IaaSの提供（例えば、オファー、レンタル、販売）に特化した第3者サービスであってもよいが、その必要はない。また、企業は、プライベートクラウドを配置し、インフラストラクチャサービスを提供するプロバイダになることもできる。

【0253】

いくつかの例において、IaaSの配置は、用意したアプリケーションサーバなどに新しいアプリケーションまたは新しいバージョンのアプリケーションを配置するプロセスである。IaaSの配置は、サーバを用意する（例えば、ライブラリ、デーモンなどをインストールする）プロセスを含んでもよい。IaaSの配置は、多くの場合、クラウドプロバイダによって、ハイパーバイザ層（例えば、サーバ、記憶装置、ネットワークハードウェア、および仮想化）の下で管理される。したがって、顧客は、OS、ミドルウェア、および／またはアプリケーションの展開（例えば、セルフサービス仮想マシン（例えば、オンデマンドでスピンアップできるもの）などを行うことができる。

20

【0254】

いくつかの例において、IaaSのプロビジョニングは、使用されるコンピュータまたは仮想ホストを取得すること、およびコンピュータまたは仮想ホスト上に必要なライブラリまたはサービスをインストールすることを含んでもよい。殆どの場合、配置は、プロビジョニングを含まず、まずプロビジョニングを実行する必要がある。

30

【0255】

場合によっては、IaaSのプロビジョニングには2つの異なる課題がある。第1に、何かを実行する前に、インフラストラクチャの初期セットをプロビジョニングするという課題がある。第2に、全てのものをプロビジョニングした後に、既存のインフラストラクチャを進化させる（例えば、新しいサービスの追加、サービスの変更、サービスの削除）という課題がある。場合によっては、インフラストラクチャの構成を宣言的に定義することを可能にすることによって、これらの2つの課題に対処することができる。言い換えれば、インフラストラクチャ（例えば、どの要素が必要とされるか、およびこれらの要素がどのように相互作用するか）は、1つ以上の構成ファイルによって定義されてもよい。したがって、インフラストラクチャの全体的なトポロジ（例えば、どのリソースがどれに依存し、どのように連携するか）は、宣言的に記述することができる。いくつかの例において、トポロジが定義されると、構成ファイルに記述された異なる要素を作成および／または管理するためのワークフローを生成することができる。

40

【0256】

いくつかの例において、インフラストラクチャは、多くの相互接続された要素を含むことができる。例えば、コアネットワークとしても知られている1つ以上の仮想プライベートクラウド（VPC）（例えば、構成可能な計算リソースおよび／または共有されている計算リソースの潜在的なオンデマンドプール）が存在してもよい。いくつかの例において

50

、ネットワークのセキュリティがどのように設定されるかを定義するためにプロビジョニングされる1つ以上のセキュリティグループルールと、1つ以上の仮想マシン（VM）とが存在する可能性がある。ロードバランサ、データベースなどの他のインフラストラクチャ要素もプロビジョニングされてもよい。ますます多くのインフラストラクチャ要素が望まれるおよび／または追加されるにつれて、インフラストラクチャは、漸進的に進化することができる。

【0257】

いくつかの例において、様々な仮想コンピューティング環境にわたってインフラストラクチャコードの展開を可能にするために、連続展開技法を採用してもよい。また、記載された技法は、これらの環境内のインフラストラクチャ管理を可能にすることができる。いくつかの例において、サービスチームは、1つ以上の、通常多くの異なる生産環境（例えば、時には全世界に及ぶ種々の異なる地理的場所にわたって）に展開されることが望まれるコードを書き込むことができる。しかしながら、いくつかの例において、コードを展開するためのインフラストラクチャを最初に設定しなければならない。いくつかの例において、プロビジョニングは、手動で行うことができ、プロビジョニングツールを用いてリソースをプロビジョニングすることができ、および／またはインフラストラクチャをプロビジョニングした後に、展開ツールを用いてコードを展開することができる。

【0258】

図19は、少なくとも1つの実施形態に従って、IaaSアーキテクチャの例示的なパターンを示すブロック図1900である。サービスオペレータ1902は、仮想クラウドネットワーク（VCN）1906およびセキュアホストサブネット1908を含み得るセキュアホストテナンシ1904に通信可能に結合されてもよい。いくつかの例において、サービスオペレータ1902は、1つ以上のクライアントコンピューティング装置を使用することができる。1つ以上のクライアントコンピューティング装置は、例えば、Microsoft Windows Mobile（登録商標）のようなソフトウェア、および／またはiOS、Windowsフォン、アンドロイド（登録商標）、ブラックベリー8およびパームOSなどのさまざまなモバイルオペレーティングシステムを実行することができ、インターネット、電子メール、ショートメッセージサービス（SMS）、ブラックベリー（登録商標）または他の通信プロトコルが有効化された手持ち式携帯装置（例えば、iPhone（登録商標）、携帯電話、Ipad（登録商標）、タブレット、携帯情報端末（PDA）またはウェアラブル装置（Google（登録商標）Glass（登録商標）ヘッドマウントディスプレイ）であってもよい。クライアントコンピューティング装置は、例示として、Microsoft Windows（登録商標）オペレーティングシステム、Apple Macintosh（登録商標）オペレーティングシステムおよび／またはLinux（登録商標）オペレーティングシステムのさまざまなバージョンを実行するパーソナルコンピュータおよび／またはラップトップコンピュータを含む汎用のパーソナルコンピュータであってもよい。代替的には、クライアントコンピューティング装置は、例えば、さまざまなGNU/Linuxオペレーティングシステム、例えば、Google Chrome（登録商標）OSを含むがこれに限定されない市販のUNIX（登録商標）またはUNIXに類似するさまざまなオペレーティングシステムを実行するワークステーションコンピュータであってもよい。代替的にまたは追加的には、クライアントコンピューティング装置は、VCN1906および／またはインターネットにアクセスできるネットワークを介して通信可能な他の電子機器、例えば、シンクライアントコンピュータ、インターネット対応のゲームシステム（例えば、Kinect（登録商標）ジェスチャ入力装置を備えるまたは備えないMicrosoft Xbox（登録商標）ゲームコンソール）、および／またはパーソナルメッセージング装置であってもよい。

【0259】

VCN1906は、SSH VCN1912に含まれるLPG1910を介して、セキュアシェル（SSH）VCN1912に通信可能に結合できるローカルピアリングゲートウェイ（LPG）1910を含むことができる。SSH VCN1912は、SSHサブネット1914を含むことができ、SSH VCN1912は、制御プレーンVCN19

16に含まれるLPG1910を介して、制御プレーンVCN1916に通信可能に結合されることができる。また、SSH VCN1912は、LPG1910を介して、データプレーンVCN1918に通信可能に結合されることができる。制御プレーンVCN1916およびデータプレーンVCN1918は、IaaSプロバイダによって所有および／または運営され得るサービステナンシ1919に含まれてもよい。

【0260】

制御プレーンVCN1916は、境界ネットワーク（例えば、企業イントラネットと外部ネットワークとの間の企業ネットワークの部分）として機能する制御プレーンDMZ（demilitarized zone）層1920を含むことができる。DMZベースのサーバは、特定の信頼性を有し、セキュリティ侵害を封じ込めることができる。さらに、DMZ層1920は、1つ以上のロードバランサ（LB）サブネット1922と、アプリサブネット1926を含むことができる制御プレーンアプリ層1924と、データベース（DB）サブネット1930（例えば、フロントエンドDBサブネットおよび／またはバックエンドDBサブネット）を含むことができる制御プレーンデータ層1928とを含むことができる。制御プレーンDMZ層1920に含まれたLBサブネット1922は、制御プレーンアプリ層1924に含まれるアプリサブネット1926と制御プレーンVCN1916に含まれ得るインターネットゲートウェイ1934とに通信可能に結合されてもよく、アプリサブネット1926は、制御プレーンデータ層1928に含まれるDBサブネット1930と、サービスゲートウェイ1936と、ネットワークアドレス変換（NAT）ゲートウェイ1938とに通信可能に結合されてもよい。制御プレーンVCN1916は、サービスゲートウェイ1936およびNATゲートウェイ1938を含むことができる。

10

20

【0261】

制御プレーンVCN1916は、データプレーンミラーアプリ層1940を含むことができ、データプレーンミラーアプリ層1940は、アプリサブネット1926を含むことができる。データプレーンミラーアプリ層1940に含まれたアプリサブネット1926は、計算インスタンス1944を実行することができる仮想ネットワークインターフェイスコントローラ（VNIC）1942を含むことができる。計算インスタンス1944は、データプレーンミラーアプリ層1940のアプリサブネット1926を、データプレーンアプリ層1946に含まれ得るアプリサブネット1926に通信可能に結合することができる。

30

【0262】

データプレーンVCN1918は、データプレーンアプリ層1946と、データプレーンDMZ層1948と、データプレーンデータ層1950とを含むことができる。データプレーンDMZ層1948は、データプレーンアプリ層1946のアプリサブネット1926およびデータプレーンVCN1918のインターネットゲートウェイ1934に通信可能に結合され得るLBサブネット1922を含むことができる。アプリサブネット1926は、データプレーンVCN1918のサービスゲートウェイ1936およびデータプレーンVCN1918のNATゲートウェイ1938に通信可能に結合されてもよい。また、データプレーンデータ層1950は、データプレーンアプリ層1946のアプリサブネット1926に通信可能に結合され得るDBサブネット1930を含むことができる。

40

【0263】

制御プレーンVCN1916のインターネットゲートウェイ1934およびデータプレーンVCN1918のインターネットゲートウェイ1934は、パブリックインターネット1954に通信可能に結合され得るメタデータ管理サービス1952に通信可能に結合されてもよい。パブリックインターネット1954は、制御プレーンVCN1916のNATゲートウェイ1938およびデータプレーンVCN1918のNATゲートウェイ1938に通信可能に結合されてもよい。制御プレーンVCN1916のサービスゲートウェイ1936およびデータプレーンVCN1918のサービスゲートウェイ1936は、クラウドサービス1956に通信可能に結合されてもよい。

【0264】

50

いくつかの例において、制御プレーンV C N 1 9 1 6またはデータプレーンV C N 1 9 1 8のサービスゲートウェイ1 9 3 6は、パブリックインターネット1 9 5 4を経由することなく、クラウドサービス1 9 5 6へのアプリケーションプログラミングインターフェイス（A P I）呼び出しを行うことができる。サービスゲートウェイ1 9 3 6からのクラウドサービス1 9 5 6へのA P I呼び出しは、一方向であり得る。サービスゲートウェイ1 9 3 6は、クラウドサービス1 9 5 6へのA P I呼び出しを行うことができ、クラウドサービス1 9 5 6は、要求データをサービスゲートウェイ1 9 3 6に送信することができる。しかしながら、クラウドサービス1 9 5 6は、サービスゲートウェイ1 9 3 6へのA P I呼び出しを開始しないことがある。

【0 2 6 5】

10

いくつかの例において、セキュアホストテナンシ1 9 0 4は、孤立であり得るサービステナンシ1 9 1 9に直接に接続されてもよい。セキュアホストサブネット1 9 0 8は、孤立のシステムとの双方向通信を可能にするL P G 1 9 1 0を介して、S S Hサブネット1 9 1 4と通信することができる。セキュアホストサブネット1 9 0 8をS S Hサブネット1 9 1 4に接続することによって、セキュアホストサブネット1 9 0 8は、サービステナンシ1 9 1 9内の他のエンティティにアクセスすることができる。

【0 2 6 6】

制御プレーンV C N 1 9 1 6は、サービステナンシ1 9 1 9のユーザが所望のリソースを設定またはプロビジョニングすることを可能にする。制御プレーンV C N 1 9 1 6においてプロビジョニングされた所望のリソースは、データプレーンV C N 1 9 1 8において展開または使用されてもよい。いくつかの例において、制御プレーンV C N 1 9 1 6は、データプレーンV C N 1 9 1 8から隔離されてもよく、制御プレーンV C N 1 9 1 6のデータプレーンミラーアプリ層1 9 4 0は、データプレーンミラーアプリ層1 9 4 0およびデータプレーンアプリ層1 9 4 6に含まれ得るV N I C 1 9 4 2を介して、データプレーンV C N 1 9 1 8のデータプレーンアプリ層1 9 4 6と通信することができる。

20

【0 2 6 7】

いくつかの例において、システムのユーザまたは顧客は、要求をメタデータ管理サービス1 9 5 2に通信することができるパブリックインターネット1 9 5 4を介して、例えば、作成、読み取り、更新、または削除（C R U D）操作などの要求を行うことができる。メタデータ管理サービス1 9 5 2は、インターネットゲートウェイ1 9 3 4を介して、要求を制御プレーンV C N 1 9 1 6に通信することができる。要求は、制御プレーンD M Z層1 9 2 0に含まれるL Bサブネット1 9 2 2によって受信されてもよい。L Bサブネット1 9 2 2は、要求が有効であると判断することができ、この判断に応答して、L Bサブネット1 9 2 2は、要求を制御プレーンアプリ層1 9 2 4に含まれるアプリサブネット1 9 2 6に送信することができる。要求が検証され、パブリックインターネット1 9 5 4への呼び出しを必要とする場合、パブリックインターネット1 9 5 4への呼び出しを、パブリックインターネット1 9 5 4への呼び出しを行うことができるN A Tゲートウェイ1 9 3 8に送信することができる。要求を記憶するためのメモリは、D Bサブネット1 9 3 0に格納されてもよい。

30

【0 2 6 8】

40

いくつかの例において、データプレーンミラーアプリ層1 9 4 0は、制御プレーンV C N 1 9 1 6とデータプレーンV C N 1 9 1 8との間の直接通信を容易にすることができる。例えば、構成に対する変更、更新、または他の適切な修正は、データプレーンV C N 1 9 1 8に含まれるリソースに適用されることが望ましい場合がある。制御プレーンV C N 1 9 1 6は、V N I C 1 9 4 2を介してデータプレーンV C N 1 9 1 8に含まれるリソースと直接に通信することができるため、構成に対する変更、更新、または他の適切な修正を実行することができる。

【0 2 6 9】

いくつかの実施形態において、制御プレーンV C N 1 9 1 6およびデータプレーンV C N 1 9 1 8は、サービステナンシ1 9 1 9に含まれてもよい。この場合、システムのユー

50

ザまたは顧客は、制御プレーンVCN1916またはデータプレーンVCN1918のいずれかを所有または操作しなくてもよい。代わりに、IaaSプロバイダは、制御プレーンVCN1916およびデータプレーンVCN1918を所有または操作してもよく、これらの両方は、サービステナンシ1919に含まれてもよい。この実施形態は、ネットワークの隔離を可能にすることによって、ユーザまたは顧客が他のユーザのリソースまたは他の顧客のリソースと対話することを防止できる。また、この実施形態は、システムのユーザまたは顧客が、記憶するための所望のレベルのセキュリティを有しない可能性のあるパブリックインターネット1954に依存する必要なく、データベースをプライベートに記憶することを可能にすることができる。

【0270】

10

他の実施形態において、制御プレーンVCN1916に含まれるLBサブネット1922は、サービスゲートウェイ1936から信号を受信するように構成されてもよい。この実施形態において、制御プレーンVCN1916およびデータプレーンVCN1918は、パブリックインターネット1954を呼び出すことなく、IaaSプロバイダの顧客によって呼び出されるように構成されてもよい。顧客が使用するデータベースは、IaaSプロバイダによって制御され、パブリックインターネット1954から隔離され得るサービステナンシ1919に格納され得るため、IaaSプロバイダの顧客は、この実施形態を望む場合がある。

【0271】

図20は、少なくとも1つの実施形態に従って、IaaSアーキテクチャの別の例示的なパラメータを示すブロック図2000である。サービスオペレータ2002（例えば、図19のサービスオペレータ1902）は、仮想クラウドネットワーク（VCN）2006（例えば、図19のVCN1906）およびセキュアホストサブネット2008（例えば、図19のセキュアホストサブネット1908）を含み得るセキュアホストテナンシ2004（例えば、図19のセキュアホストテナンシ1904）に通信可能に結合されてもよい。VCN2006は、SSH VCN2012に含まれるLPG1910を介してセキュアシェル（SSH）VCN2012（例えば、図19のSSH VCN1912）に通信可能に結合され得るローカルピアリングゲートウェイ（LPG）2010（例えば、図19のLPG1910）を含むことができる。SSH VCN2012は、SSHサブネット2014（例えば、図19のSSHサブネット1914）を含むことができ、SSH VCN2012は、制御プレーンVCN2016に含まれるLPG2010を介して制御プレーンVCN2016（例えば、図19の制御プレーンVCN1916）に通信可能に結合することができる。制御プレーンVCN2016は、サービステナンシ2019（例えば、図19のサービステナンシ1919）に含まれてもよく、データプレーンVCN2018（例えば、図19のデータプレーンVCN1918）は、システムのユーザまたは顧客によって所有または運営され得る顧客テナンシ2021に含まれてもよい。

20

30

【0272】

制御プレーンVCN2016は、LBサブネット2022（例えば、図19のLBサブネット1922）を含むことができる制御プレーンDMZティア2020（例えば、図19の制御プレーンDMZ層1920）と、アプリサブネット2026（例えば、図19のアプリサブネット1926）を含むことができる制御プレーンアプリ層2024（例えば、図19の制御プレーンアプリ層1924）と、データベース（DB）サブネット2030（例えば、図19のDBサブネット1930と同様）を含むことができる制御プレーンデータティア2028（例えば、図19の制御プレーンデータ層1928）とを含むことができる。制御プレーンDMZ層2020に含まれるLBサブネット2022は、制御プレーンアプリ層2024に含まれるアプリサブネット2026と、制御プレーンVCN2016に含まれ得るインターネットゲートウェイ2034（例えば、図19のインターネットゲートウェイ1934）とに通信可能に結合されてもよい。アプリサブネット2026は、制御プレーンデータ層2028に含まれるDBサブネット2030、サービスゲートウェイ2036（例えば、図19のサービスゲートウェイ）およびネットワークアドレ

40

50

ス変換（NAT）ゲートウェイ2038（例えば、図19のNATゲートウェイ1938）に通信可能に結合されてもよい。制御プレーンVCN2016は、サービスゲートウェイ2036およびNATゲートウェイ2038を含むことができる。

【0273】

制御プレーンVCN2016は、アプリサブネット2026を含むことができるデータプレーンミラーアプリ層2040（例えば、図19のデータプレーンミラーアプリ層1940）を含むことができる。データプレーンミラーアプリ層2040に含まれるアプリサブネット2026は、（例えば、図19の計算インスタンス1944と同様の）計算インスタンス2044を実行することができる仮想ネットワークインターフェイスコントローラ（VNIC）2042（例えば、VNIC1942）を含むことができる。計算インスタンス2044は、データプレーンミラーアプリ層2040に含まれるVNIC2042およびデータプレーンアプリ層2046に含まれるVNIC2042を介して、データプレーンミラーアプリ層2040のアプリサブネット2026と、データプレーンアプリ層2046（例えば、図19のデータプレーンアプリ層1946）に含まれ得るアプリサブネット2026との間の通信を促進することができる。

10

【0274】

制御プレーンVCN2016に含まれるインターネットゲートウェイ2034は、パブリックインターネット2054（例えば、図19のパブリックインターネット1954）に通信可能に結合され得るメタデータ管理サービス2052（例えば、図19のメタデータ管理サービス1952）に通信可能に結合されてもよい。パブリックインターネット2054は、制御プレーンVCN2016に含まれるNATゲートウェイ2038に通信可能に結合されてもよい。制御プレーンVCN2016に含まれるサービスゲートウェイ2036は、クラウドサービス2056（例えば、図19のクラウドサービス1956）に通信可能に結合されてもよい。

20

【0275】

いくつかの例において、データプレーンVCN2018は、顧客テナンシ2021に含まれてもよい。この場合、IaaSプロバイダは、顧客ごとに制御プレーンVCN2016を提供することができる。IaaSプロバイダは、顧客ごとに、サービステナンシ2019に含まれる固有の計算インスタンス2044を構成することができる。各計算インスタンス2044は、サービステナンシ2019に含まれる制御プレーンVCN2016と、顧客テナンシ2021に含まれるデータプレーンVCN2018との間の通信を許可することができる。計算インスタンス2044は、サービステナンシ2019に含まれる制御プレーンVCN2016においてプロビジョニングされるリソースを、顧客テナンシ2021に含まれるデータプレーンVCN2018に展開することまたは使用することを許可することができる。

30

【0276】

他の例において、IaaSプロバイダの顧客は、顧客テナンシ2021に存在するデータベースを有することができる。この例において、制御プレーンVCN2016は、アプリサブネット2026を含むことができるデータプレーンマイナーアプリ層2040を含むことができる。データプレーンミラーアプリ層2040は、データプレーンVCN2018に存在してもよいが、データプレーンミラーアプリ層2040は、データプレーンVCN2018に存在しなくてもよい。すなわち、データプレーンミラーアプリ層2040は、顧客テナンシ2021にアクセスすることができるが、データプレーンミラーアプリ層2040は、データプレーンVCN2018に存在しなくてもよく、IaaSプロバイダの顧客によって所有または運営されなくてもよい。データプレーンミラーアプリ層2040は、データプレーンVCN2018への呼び出しを行うように構成されてもよいが、制御プレーンVCN2016に含まれる任意のエンティティへの呼び出しを行うように構成されなくてもよい。顧客は、制御プレーンVCN2016にプロビジョニングされたデータプレーンVCN2018内のリソースを展開することまたは使用することを望むことができ、データプレーンミラーアプリケーション階層2040は、顧客のリソースの所望

40

50

の展開または他の使用を促進することができる。

【0277】

いくつかの実施形態において、IaaSプロバイダの顧客は、フィルタをデータプレーンVCN2018に適用することができる。この実施形態において、顧客は、データプレーンVCN2018がアクセスできるものを決定することができ、顧客は、データプレーンVCN2018からのパブリックインターネット2054へのアクセスを制限することができる。IaaSプロバイダは、データプレーンVCN2018から任意の外部ネットワークまたはデータベースへのアクセスにフィルタを適用するまたは制御することができない場合がある。顧客が顧客テナンシ2021に含まれるデータプレーンVCN2018にフィルタおよび制御を適用することは、データプレーンVCN2018を他の顧客およびパブリックインターネット2054から隔離することを支援することができる。

10

【0278】

いくつかの実施形態において、クラウドサービス2056は、サービスゲートウェイ2036によって呼び出されて、パブリックインターネット2054上に、制御プレーンVCN2016上に、またはデータプレーンVCN2018上に存在していない可能性があるサービスにアクセスすることができる。クラウドサービス2056と制御プレーンVCN2016またはデータプレーンVCN2018との間の接続は、ライブまたは連続的でなくてもよい。クラウドサービス2056は、IaaSプロバイダによって所有または運営されている別のネットワーク上に存在してもよい。クラウドサービス2056は、サービスゲートウェイ2036から呼び出しを受信するように構成されてもよく、パブリックインターネット2054から呼び出しを受信しないように構成されてもよい。いくつかのクラウドサービス2056は、他のクラウドサービス2056から隔離されてもよく、制御プレーンVCN2016は、制御プレーンVCN2016と同じ地域に配置していない可能性があるクラウドサービス2056から隔離されてもよい。例えば、制御プレーンVCN2016は、「地域1」に配置されてもよく、クラウドサービス「展開19」は、「地域1」および「地域2」に配置されてもよい。展開19への呼び出しが地域1に配置された制御プレーンVCN2016に含まれるサービスゲートウェイ2036によって行われる場合、この呼び出しは、地域1内の展開19に送信されてもよい。この例において、制御プレーンVCN2016または地域1の展開19は、地域2の展開19と通信可能に結合されなくてもよい。

20

30

【0279】

図21は、少なくとも1つの実施形態に従って、IaaSアーキテクチャの別の例示的なパターンを示すブロック図2100である。サービスオペレータ2102（例えば、図19のサービスオペレータ1902）は、仮想クラウドネットワーク（VCN）2106（例えば、図19のVCN1906）およびセキュアホストサブネット2108（例えば、図19のセキュアホストサブネット1908）を含み得るセキュアホストテナンシ2104（例えば、図19のセキュアホストテナンシ1904）に通信可能に結合されてもよい。VCN2106は、SSH VCN2112に含まれるLPG2110を介してSSH VCN2112（例えば、図19のSSH VCN1912）に通信可能に結合され得るLPG2110（例えば、図19のLPG1910）を含むことができる。SSH VCN2112は、SSHサブネット2114（例えば、図19のSSHサブネット1914）を含むことができ、SSH VCN2112は、制御プレーンVCN2116に含まれるLPG2110を介して制御プレーンVCN2116（例えば、図19の制御プレーンVCN1916）に通信可能に結合されてもよく、データプレーンVCN2118に含まれるLPG2110を介してデータプレーンVCN2118（例えば、図19のデータプレーン1918）に通信可能に結合されてもよい。制御プレーンVCN2116およびデータプレーンVCN2118は、サービステナンシ2119（例えば、図19のサービステナンシ1919）に含まれてもよい。

40

【0280】

制御プレーンVCN2116は、ロードバランサ（LB）サブネット2122（例えば

50

、図19のLBサブネット1922)を含むことができる制御プレーンDMZ層2120(例えば、図19の制御プレーンDMZ層1920)と、アプリサブネット2126(例えば、図19のアプリサブネット1926と同様)を含むことができる制御プレーンアプリ層2124(例えば、図19の制御プレーンアプリ層1924)と、DBサブネット2130を含むことができる制御プレーンデータ層2128(例えば、図19の制御プレーンデータ層1928)とを含むことができる。制御プレーンDMZ層2120に含まれるLBサブネット2122は、制御プレーンアプリ層2124に含まれるアプリサブネット2126と、制御プレーンVCN2116に含まれ得るインターネットゲートウェイ2134(例えば、図19のインターネットゲートウェイ1934)とに通信可能に結合されてもよい。アプリサブネット2126は、制御プレーンデータ層2128に含まれるDBサブネット2130と、サービスゲートウェイ2136(例えば、図19のサービスゲートウェイ)およびネットワークアドレス変換(NAT)ゲートウェイ2138(例えば、図19のNATゲートウェイ1938)とに通信可能に結合されてもよい。制御プレーンVCN2116は、サービスゲートウェイ2136およびNATゲートウェイ2138を含むことができる。

10

【0281】

データプレーンVCN2118は、データプレーンアプリ層2146(例えば、図19のデータプレーンアプリ層1946)と、データプレーンDMZ層2148(例えば、図19のデータプレーンDMZ層1948)と、データプレーンデータ層2150(例えば、図19のデータプレーンデータ階層1950)とを含むことができる。データプレーンDMZ層2148は、データプレーンVCN2118に含まれるデータプレーンアプリ層2146およびインターネットゲートウェイ2134の信頼できるアプリサブネット2160および信頼できないアプリサブネット2162に通信可能に結合され得るLBサブネット2122を含むことができる。信頼できるアプリサブネット2160は、データプレーンVCN2118に含まれるサービスゲートウェイ2136、データプレーンVCN2118に含まれるNATゲートウェイ2138、およびデータプレーンデータ層2150に含まれるDBサブネット2130に通信可能に結合されてもよい。信頼できないアプリサブネット2162は、データプレーンVCN2118に含まれるサービスゲートウェイ2136、およびデータプレーンデータ層2150に含まれるDBサブネット2130に通信可能に結合されてもよい。データプレーンデータ層2150は、データプレーンVCN2118に含まれるサービスゲートウェイ2136に通信可能に結合され得るDBサブネット2130を含むことができる。

20

30

【0282】

信頼できないアプリサブネット2162は、テナント仮想マシン(VM)2166(1)~(N)に通信可能に結合され得る1つ以上のプライマリVNIC2164(1)~(N)を含むことができる。各テナントVM2166(1)~(N)は、それぞれの顧客テナンシ2170(1)~(N)に含まれ得るそれぞれのコンテナ送信VCN2168(1)~(N)に含まれ得るそれぞれのアプリサブネット2167(1)~(N)に通信可能に結合されてもよい。それぞれのセカンダリVNIC2172(1)~(N)は、データプレーンVCN2118に含まれる信頼できないアプリサブネット2162と、コンテナ送信VCN2168(1)~(N)に含まれるアプリサブネットとの間の通信を促進することができる。各コンテナ送信VCN2168(1)~(N)は、パブリックインターネット2154(例えば、図19のパブリックインターネット1954)に通信可能に結合され得るNATゲートウェイ2138を含むことができる。

40

【0283】

制御プレーンVCN2116に含まれるインターネットゲートウェイ2134およびデータプレーンVCN2118に含まれるインターネットゲートウェイ2134は、パブリックインターネット2154に通信可能に結合され得るメタデータ管理サービス2152(例えば、図19のメタデータ管理システム1952)に通信可能に結合されてもよい。パブリックインターネット2154は、制御プレーンVCN2116に含まれるNATゲ

50

ートウェイ 2 1 3 8 およびデータプレーン V C N 2 1 1 8 に含まれる N A T ゲートウェイ 2 1 3 8 に通信可能に結合されてもよい。制御プレーン V C N 2 1 1 6 に含まれるサービスゲートウェイ 2 1 3 6 およびデータプレーン V C N 2 1 1 8 に含まれるサービスゲートウェイ 2 1 3 6 は、クラウドサービス 2 1 5 6 に通信可能に結合されてもよい。

【0284】

いくつかの実施形態において、データプレーン V C N 2 1 1 8 は、顧客テナンシ 2 1 7 0 に統合されてもよい。この統合は、コードを実行するときにサポートを望む場合がある場合などのいくつかの場合において、I a a S プロバイダの顧客にとって有用または望ましい場合がある。顧客は、実行すると、破壊的であり得る、他の顧客リソースと通信し得る、または望ましくない影響を引き起こし得るコードを提供することがある。従って、I a a S プロバイダは、顧客が I a a S プロバイダに提供したコードを実行するか否かを判断することができる。

10

【0285】

いくつかの例において、I a a S プロバイダの顧客は、一時的なネットワークアクセスを I a a S プロバイダに許可することができる。データプレーンアプリ層 2 1 4 6 に追加する機能を要求することができる。機能を実行するためのコードは、V M 2 1 6 6 (1) ~ (N) で実行されてもよいが、データプレーン V C N 2 1 1 8 上の他の場所で実行されるように構成されることができない。各 V M 2 1 6 6 (1) ~ (N) は、1つの顧客テナンシ 2 1 7 0 に接続されてもよい。V M 2 1 6 6 (1) ~ (N) に含まれるそれぞれのコンテナ 2 1 7 1 (1) ~ (N) は、コードを実行するように構成されてもよい。この場合、二重の隔離（例えば、コンテナ 2 1 7 1 (1) ~ (N) は、コードを実行し、コンテナ 2 1 7 1 (1) ~ (N) は、少なくとも、信頼できないアプリサブネット 2 1 6 2 に含まれる V M 2 1 6 6 (1) ~ (N) に含まれ得る）が存在してもよく、これは、誤ったコードまたは望ましくないコードが I a a S プロバイダのネットワークに損傷を与えること、または異なる顧客のネットワークに損傷を与えることを防止することを支援することができる。コンテナ 2 1 7 1 (1) ~ (N) は、顧客テナンシ 2 1 7 0 に通信可能に結合されてもよく、顧客テナンシ 2 1 7 0 からデータを送信または受信するように構成されてもよい。コンテナ 2 1 7 1 (1) ~ (N) は、データプレーン V C N 2 1 1 8 内の任意の他のエンティティからデータを送信または受信するように構成されなくてもよい。コードの実行が完了すると、I a a S 提供者は、コンテナ 2 1 7 1 (I) ~ (N) をキルするまたは廃棄することができる。

20

30

【0286】

いくつかの実施形態において、信頼できるアプリサブネット 2 1 6 0 は、I a a S プロバイダによって所有または運営され得るコードを実行することができる。この実施形態において、信頼できるアプリサブネット 2 1 6 0 は、D B サブネット 2 1 3 0 に通信可能に結合され、D B サブネット 2 1 3 0 において C R U D 操作を実行するように構成されてもよい。信頼できないアプリサブネット 2 1 6 2 は、D B サブネット 2 1 3 0 に通信可能に結合され得るが、この実施形態において、信頼できないアプリサブネットは、D B サブネット 2 1 3 0 内で読み取り操作を実行するように構成されてもよい。各顧客の V M 2 1 6 6 (1) ~ (N) に含まれ、顧客からのコードを実行することができるコンテナ 2 1 7 1 (1) ~ (N) は、D B サブネット 2 1 3 0 と通信可能に結合されなくてもよい。

40

【0287】

他の実施形態において、制御プレーン V C N 2 1 1 6 およびデータプレーン V C N 2 1 1 8 は、通信可能に直接に結合されなくてもよい。この実施形態において、制御プレーン V C N 2 1 1 6 とデータプレーン V C N 2 1 1 8 との間に直接的な通信は、存在しないことがある。しかしながら、少なくとも1つの方法による間接的な通信は、存在してもよい。制御プレーン V C N 2 1 1 6 とデータプレーン V C N 2 1 1 8 との間の通信を容易にすることができる L P G 2 1 1 0 が、I a a S プロバイダによって確立されてもよい。別の例において、制御プレーン V C N 2 1 1 6 またはデータプレーン V C N 2 1 1 8 は、サービスゲートウェイ 2 1 3 6 を介してクラウドサービス 2 1 5 6 への呼び出しを行うことが

50

できる。例えば、制御プレーンVCN2116からクラウドサービス2156への呼び出しは、データプレーンVCN2118と通信することができるサービスの要求を含むことができる。

【0288】

図22は、少なくとも1つの実施形態に従って、IaaSアーキテクチャの別の例示的なパラメータを示すブロック図2200である。サービスオペレータ2202（例えば、図19のサービスオペレータ1902）は、仮想クラウドネットワーク（VCN）2206（例えば、図19のVCN1906）およびセキュアホストサブネット2208（例えば、図19のセキュアホストサブネット1908）を含み得るセキュアホストテナンシ2204（例えば、図19のセキュアホストテナンシ1904）に通信可能に結合されてもよい。VCN2206は、SSH VCN2212に含まれるLPG2210を介してSSH VCN2212（例えば、図19のSSH VCN1912）に通信可能に結合され得るLPG2210（例えば、図19のLPG1910）を含むことができる。SSH VCN2212は、SSHサブネット2214（例えば、図19のSSHサブネット1914）を含むことができ、SSH VCN2212は、制御プレーンVCN2216に含まれるLPG2210を介して制御プレーンVCN2216（例えば、図19の制御プレーンVCN1916）に通信可能に結合されてもよく、データプレーンVCN2218に含まれるLPG2210を介してデータプレーンVCN2218（例えば、図19のデータプレーン1918）に通信可能に結合されてもよい。制御プレーンVCN2216およびデータプレーンVCN2218は、サービステナンシ2219（例えば、図19のサービステナンシ1919）に含まれてもよい。

10

20

【0289】

制御プレーンVCN2216は、LBサブネット2222（例えば、図19のLBサブネット1922）を含み得る制御プレーンDMZ層2220（例えば、図19の制御プレーンDMZ層1920）、アプリサブネット2226（例えば、図19のアプリサブネット1926）を含み得る制御プレーンアプリ層2224（例えば、図19の制御プレーンアプリ層1924）、DBサブネット2230（例えば、図21のDBサブネット2130）を含み得る制御プレーンデータティア2228（例えば、図19の制御プレーンデータティア1928）を含むことができる。制御プレーンDMZ層2220に含まれるLBサブネット2222は、制御プレーンアプリ層2224に含まれるアプリサブネット2226と、制御プレーンVCN2216に含まれ得るインターネットゲートウェイ2234（例えば、図19のインターネットゲートウェイ1934）とに通信可能に結合されてもよい。アプリサブネット2226は、制御プレーンデータ層2228に含まれるDBサブネット2230と、サービスゲートウェイ2236（例えば、図19のサービスゲートウェイ）およびネットワークアドレス変換（NAT）ゲートウェイ2238（例えば、図19のNATゲートウェイ1938）とに通信可能に結合されてもよい。制御プレーンVCN2216は、サービスゲートウェイ2236およびNATゲートウェイ2238を含むことができる。

30

【0290】

データプレーンVCN2218は、データプレーンアプリ層2246（例えば、図19のデータプレーンアプリ層1946）、データプレーンDMZ層2248（例えば、図19のデータプレーンDMZ層1948）、およびデータプレーンデータ層2250（例えば、図19のデータプレーンデータ層1950）を含むことができる。データプレーンDMZ層2248は、データプレーンアプリ層2246の信頼できるアプリサブネット2260（例えば、図21の信頼できるアプリサブネット2160）および信頼できないアプリサブネット2262（例えば、図21の信頼できないアプリサブネット2162）およびデータプレーンVCN2218に含まれるインターネットゲートウェイ2234に通信可能に結合され得るLBサブネット2222を含むことができる。信頼できるアプリサブネット2260は、データプレーンVCN2218に含まれるサービスゲートウェイ2236、データプレーンVCN2218に含まれるNATゲートウェイ2238、およびデ

40

50

ータプレーンデータ層 2250 に含まれる DB サブネット 2230 に通信可能に結合されてもよい。信頼できないアプリサブネット 2262 は、データプレーン VCN 2218 に含まれる サービスゲートウェイ 2236、およびデータプレーンデータ層 2250 に含まれる DB サブネット 2230 に通信可能に結合されてもよい。データプレーンデータ層 2250 は、データプレーン VCN 2218 に含まれる サービスゲートウェイ 2236 に通信可能に結合され得る DB サブネット 2230 を含むことができる。

【0291】

信頼できないアプリサブネット 2262 は、信頼できないアプリサブネット 2262 に常駐するテナント仮想マシン (VM) 2266 (1) ~ (N) に通信可能に結合され得るプライマリ VNIC 2264 (1) ~ (N) を含むことができる。各テナント VM 2266 (1) ~ (N) は、それぞれのコンテナ 2267 (1) ~ (N) においてコードを実行することができ、コンテナ送信 VCN 2268 に含まれ得るデータプレーンアプリ層 2246 に含まれ得るアプリサブネット 2226 に通信可能に結合されてもよい。各セカンダリ VNIC 2272 (1) ~ (N) は、データプレーン VCN 2218 に含まれる信頼できないアプリサブネット 2262 とコンテナ送信 VCN 2268 に含まれるアプリサブネットとの間の通信を促進することができる。コンテナ送信 VCN は、パブリックインターネット 2254 (例えば、図 19 のパブリックインターネット 1954) に通信可能に結合することができる NAT ゲートウェイ 2238 を含むことができる。

【0292】

制御プレーン VCN 2216 に含まれるインターネットゲートウェイ 2234 およびデータプレーン VCN 2218 に含まれるインターネットゲートウェイ 2234 は、パブリックインターネット 2254 に通信可能に結合され得るメタデータ管理サービス 2252 (例えば、図 19 のメタデータ管理システム 1952) に通信可能に結合されてもよい。パブリックインターネット 2254 は、制御プレーン VCN 2216 に含まれるインターネットゲートウェイ 2234 およびデータプレーン VCN 2218 に含まれる NAT ゲートウェイ 2238 に通信可能に結合されてもよい。制御プレーン VCN 2216 に含まれるインターネットゲートウェイ 2234 およびデータプレーン VCN 2218 に含まれる サービスゲートウェイ 2236 は、クラウドサービス 2256 に通信可能に結合されてもよい。

【0293】

いくつかの例において、図 22 のブロック図 2200 のアーキテクチャによって示されたパターンは、図 21 のブロック図 2100 のアーキテクチャによって示されたパターンの例外と考えられ、IaaS プロバイダが顧客と直接に通信できない (例えば、非接続地域) 場合、IaaS プロバイダの顧客にとって望ましいことがある。顧客は、各顧客の VM 2266 (1) ~ (N) に含まれるそれぞれのコンテナ 2267 (1) ~ (N) にリアルタイムでアクセスすることができる。コンテナ 2267 (1) ~ (N) は、コンテナ送信 VCN 2268 に含まれ得るデータプレーンアプリ層 2246 のアプリサブネット 2226 に含まれるそれぞれのセカンダリ VNIC 2272 (1) ~ (N) を呼び出すように構成されてもよい。セカンダリ VNIC 2272 (1) ~ (N) は、パブリックインターネット 2254 に呼び出しを送信することができる NAT ゲートウェイ 2238 に呼び出しを送信することができる。この例において、顧客がリアルタイムでアクセスできるコンテナ 2267 (1) ~ (N) は、制御プレーン VCN 2216 から隔離されてもよく、データプレーン VCN 2218 に含まれる他のエンティティから隔離されてもよい。また、コンテナ 2267 (1) ~ (N) は、他の顧客のリソースから隔離されてもよい。

【0294】

他の例において、顧客は、コンテナ 2267 (1) ~ (N) を使用して、クラウドサービス 2256 を呼び出すことができる。この例では、顧客は、コンテナ 2267 (1) ~ (N) において、クラウドサービス 2256 からサービスを要求するコードを実行することができる。コンテナ 2267 (1) ~ (N) は、要求をパブリックインターネット 2254 に送信することができる NAT ゲートウェイに要求を送信することができるセカンダ

リ V N I C 2 2 7 2 (1) ~ (N) にこの要求を送信することができる。パブリックインターネット 2 2 5 4 は、インターネットゲートウェイ 2 2 3 4 を介して、制御プレーン V C N 2 2 1 6 に含まれる L B サブネット 2 2 2 2 にこの要求を送信することができる。要求が有効であるとの判断に応答して、L B サブネットは、この要求をアプリサブネット 2 2 2 6 に送信することができ、アプリサブネット 2 2 2 6 は、サービスゲートウェイ 2 2 3 6 を介して、この要求をクラウドサービス 2 2 5 6 に要求を送信することができる。

【 0 2 9 5 】

なお、図示された I a a S アーキテクチャ 1 9 0 0、2 0 0 0、2 1 0 0 および 2 2 0 0 は、図示されたもの以外の要素を含んでもよい。また、図示された実施形態は、本開示の実施形態を組み込むことができるクラウドインフラストラクチャシステムの一部の例に過ぎない。他のいくつかの実施形態において、I a a S システムは、図示されたものよりも多いまたは少ない要素を有してよく、2 つ以上の要素を組み合わせてもよく、または要素の異なる構成または配置を有してよい。

【 0 2 9 6 】

特定の実施形態において、本明細書に記載された I a a S システムは、セルフサービス、サブスクリプションベース、柔軟な拡張可能性、信頼性、高可用性、および安全な方法で顧客に提供されるアプリケーション、ミドルウェア、およびデータベースサービスのスイートを含むことができる。このような I a a S システムの一例は、本出願人によって提供されたオラクル（登録商標）クラウドインフラストラクチャ（O C I）である。

【 0 2 9 7 】

図 2 3 は、様々な実施形態が実装され得る例示的なコンピュータシステム 2 3 0 0 を示す。システム 2 3 0 0 は、上述したコンピュータシステムのいずれかを実装するために使用されてもよい。図示のように、コンピュータシステム 2 3 0 0 は、バスサブシステム 2 3 0 2 を介して多数の周辺サブシステムと通信する処理ユニット 2 3 0 4 を含む。これらの周辺サブシステムは、処理加速ユニット 2 3 0 6、I / O サブシステム 2 3 0 8、記憶サブシステム 2 3 1 8、および通信サブシステム 2 3 2 4 を含んでもよい。記憶サブシステム 2 3 1 8 は、有形のコンピュータ可読記憶媒体 2 3 2 2 およびシステムメモリ 2 3 1 0 を含む。

【 0 2 9 8 】

バスサブシステム 2 3 0 2 は、コンピュータシステム 2 3 0 0 の様々な構成要素およびサブシステムを意図したように相互に通信させるための機構を提供する。バスサブシステム 2 3 0 2 は、単一のバスとして概略的に示されているが、バスサブシステムの代替的な実施形態は、複数のバスを利用してもよい。バスサブシステム 2 3 0 2 は、メモリバスまたはメモリコントローラ、周辺バス、および様々なバスアーキテクチャのいずれかを使用するローカルバスを含む、いくつかの種類のバス構造のいずれかであってもよい。例えば、このようなアーキテクチャは、業界標準アーキテクチャ（I S A）バス、マイクロチャネルアーキテクチャ（M C A）、バス拡張 I S A（E I S A）バス、ビデオ電子標準協会（V E S A）ローカルバス、および I E E E P 1 3 8 6 . 1 標準に準拠して製造されたメザニンバスとして実装できる周辺機器相互接続（P C I）バスなどを含むことができる。

【 0 2 9 9 】

1 つ以上の集積回路（例えば、従来のマイクロプロセッサまたはマイクロコントローラ）として実装され得る処理ユニット 2 3 0 4 は、コンピュータシステム 2 3 0 0 の動作を制御する。処理ユニット 2 3 0 4 は、1 つ以上のプロセッサを含んでもよい。これらのプロセッサは、シングルコアまたはマルチコアプロセッサを含んでもよい。いくつかの実施形態において、処理ユニット 2 3 0 4 は、各処理ユニットに含まれるシングルコアまたはマルチコアプロセッサを有する 1 つ以上の独立した処理ユニット 2 3 3 2 および / または 2 3 3 4 として実装されてもよい。他の実施形態において、処理ユニット 2 3 0 4 は、2 つのデュアルコアプロセッサを単一のチップに統合することによって形成されたクワッドコア（quad-core）処理ユニットとして実装されてもよい。

【0300】

様々な実施形態において、処理ユニット2304は、プログラムコードにตอบสนองして様々なプログラムを実行することができ、同時に実行する複数のプログラムまたはプロセスを維持することができる。任意の時点で、実行されるプログラムコードの一部または全部は、プロセッサ2304および／または記憶サブシステム2318に常駐することができる。プロセッサ2304は、適切なプログラミングを通して、上述した様々な機能性を提供することができる。コンピュータシステム2300は、デジタル信号プロセッサ（DSP）、専用プロセッサおよび／または同種のものを含むことができる処理加速ユニット2306をさらに含んでもよい。

【0301】

I/Oサブシステム2308は、ユーザインターフェイス入力装置と、ユーザインターフェイス出力装置とを含むことができる。ユーザインターフェイス入力装置は、キーボード、マウスまたはトラックボールなどのポインティング装置、ディスプレイに組み込まれたタッチパッドまたはタッチスクリーン、スクロールホイール、クリックホイール、ダイヤル、ボタン、スイッチ、キーパッド、音声命令認識システムを備える音声入力装置、マイクロフォン、および他の種類の入力装置を含んでもよい。また、ユーザインターフェイス入力装置は、例えば、Microsoft Kinect（登録商標）モーションセンサのようなモーション検知および／またはジェスチャ認識装置を含んでもよい。Microsoft Kinect（登録商標）モーションセンサは、ジェスチャおよび音声命令を利用する自然ユーザインターフェイス（NUI）を介して、Microsoft Xbox（登録商標）360ゲームコントローラなどの入力装置を制御することができ、それと対話することができる。また、ユーザインターフェイス入力装置は、Google Glass（登録商標）瞬き検出器のような眼球ジェスチャ認識装置を含むことができる。Google Glass（登録商標）瞬き検出器は、ユーザの眼球活動（例えば、写真を撮るときおよび／またはメニューを選択するときの「瞬き」）を検出し、眼球活動を入力装置（例えば、Google Glass（登録商標））に入力する入力に変換する。さらに、ユーザインターフェイス入力装置は、音声命令を介してユーザと音声認識システム（例えば、Siri（登録商標）ナビゲータ）との対話を可能にする音声認識検出装置を含んでもよい。

【0302】

また、ユーザインターフェイス入力装置は、三次元（3D）マウス、ジョイスティックまたはポインティングスティック、ゲームパッド、グラフィックタブレット、スピーカなどのオーディオ／ビジュアル装置、デジタルカメラ、デジタルビデオカメラ、ポータブルメディアプレーヤ、ウェブカメラ、イメージスキャナ、指紋スキャナ、バーコードリーダー、3Dスキャナ、3Dプリンタ、レーザ距離計、および視線追跡装置を含むがこれらに限定されない。さらに、ユーザインターフェイス入力装置は、例えば、コンピュータ断層撮影装置、磁気共鳴像装置、超音波放射断層撮影装置、または医療用超音波装置などのような医用画像入力装置を含んでもよい。また、ユーザインターフェイス入力装置は、例えば、MIDIキーボードおよび電子楽器などの音声入力装置を含んでもよい。

【0303】

ユーザインターフェイス出力装置は、ディスプレイサブシステム、インジケータライト、またはオーディオ出力装置などの非視覚ディスプレイを含んでもよい。ディスプレイサブシステムは、例えば、陰極線管（CRT）、液晶ディスプレイ（LCD）またはプラズマディスプレイを使用するフラットパネル装置、投射装置またはタッチスクリーンであってもよい。一般に、「出力装置」という用語を使用する場合、コンピュータシステム2300から情報をユーザまたは他のコンピュータに出力するためのすべての可能な種類の装置および機構を含むことを意図している。例えば、ユーザインターフェイス出力装置は、文字、画像およびオーディオ／ビデオ情報を視覚的に伝達するさまざまな表示装置、例えば、モニタ、プリンタ、スピーカ、ヘッドフォン、カーナビゲーションシステム、プロッタ、音声出力装置、およびモデムを含むがこれらに限定されない。

【0304】

コンピュータシステム 2300 は、記憶サブシステム 2318 を含むことができる。記憶サブシステム 2318 は、ソフトウェア要素を備え、図示では、これらのソフトウェア要素は、システムメモリ 2310 内に配置されている。システムメモリ 2310 は、処理ユニット 2304 にロード可能かつ実行可能なプログラム命令、およびこれらのプログラムの実行により生成されたデータを記憶することができる。

【0305】

コンピュータシステム 2300 の構成およびタイプに応じて、システムメモリ 2310 は、揮発性メモリ（例えば、ランダムアクセスメモリ（random access memory：RAM））であってもよく、および／または、不揮発性メモリ（例えば、読取り専用メモリ（read-only memory：ROM）、フラッシュメモリ）であってもよい。一般に、RAM は、処理ユニット 2304 がすぐにアクセス可能なデータおよび／またはプログラムモジュール、および／または、処理ユニット 2304 によって現在操作および実行されているデータおよび／またはプログラムモジュールを収容する。いくつかの実現例では、システムメモリ 2310 は、スタティックランダムアクセスメモリ（static random access memory：SRAM）またはダイナミックランダムアクセスメモリ（dynamic random access memory：DRAM）などの複数の異なるタイプのメモリを含み得る。いくつかの実現例では、始動中などにコンピュータシステム 2300 内の要素間で情報を転送することを助ける基本ルーチンを含む基本入力／出力システム（basic input/output system：BIOS）が、一般に ROM に格納され得る。一例としておよび非限定的に、システムメモリ 2310 は、クライアントアプリケーション、ウェブブラウザ、中間層アプリケーション、リレーショナルデータベース管理システム（relational database management system：RDBMS）などを含み得るアプリケーションプログラム 2312、プログラムデータ 2314 およびオペレーティングシステム 2316 も示す。一例として、オペレーティングシステム 2316 は、マイクロソフトウィンドウズ（登録商標）、Apple Macintosh（登録商標）および／もしくは Linux（登録商標）オペレーティングシステムのさまざまなバージョン、さまざまな市販の UNIX（登録商標）もしくは UNIX ライクオペレーティングシステム（さまざまな GNU／Linux オペレーティングシステム、Google Chrome（登録商標）OS などを含むが、これらに限定されるものではない）、および／または、iOS、Windows（登録商標）フォン、アンドロイド（登録商標）OS、ブラックベリー（登録商標）23 OS および パーム（登録商標）OS オペレーティングシステムなどのモバイルオペレーティングシステムを含み得る。

【0306】

また、記憶サブシステム 2318 は、いくつかの実施例の機能を提供する基本的なプログラミングおよびデータ構造を格納するための有形のコンピュータ可読記憶媒体を提供することができる。プロセッサによって実行されたときに上記の機能を提供するソフトウェア（プログラム、コードモジュール、命令）は、記憶サブシステム 2318 に記憶されてもよい。これらのソフトウェアモジュールまたは命令は、処理ユニット 2304 によって実行されてもよい。また、記憶サブシステム 2318 は、本開示に従って使用されるデータを記憶するためのリポジトリを提供することができる。

【0307】

また、記憶サブシステム 2300 は、コンピュータ可読記憶媒体 2322 にさらに接続可能なコンピュータ可読記憶媒体リーダ 2320 を含むことができる。コンピュータ可読記憶媒体 2322 は、システムメモリ 2310 とともに、または必要に応じてシステムメモリ 2310 と組み合わせて、コンピュータ可読情報を一時的におよび／または永久に収容、格納、送信および検索するための記憶媒体に加えて、リモート記憶装置、ローカル記憶装置、固定的な記憶装置および／または取外し可能な記憶装置を包括的に表すことができる。

【0308】

また、コードまたはコードの一部を含むコンピュータ可読記憶媒体 2322 は、当該技

術分野において公知のまたは使用される任意の適切な媒体を含んでもよい。当該媒体は、情報の格納および／または送信のための任意の方法または技術において実現される揮発性および不揮発性の、取外し可能および取外し不可能な媒体などであるが、これらに限定されるものではない記憶媒体および通信媒体を含む。これは、RAM、ROM、電子的消去・プログラム可能ROM (electronically erasable programmable ROM: EEPROM)、フラッシュメモリもしくは他のメモリ技術、CD-ROM、デジタル多用途ディスク (digital versatile disk: DVD)、または他の光学式記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置もしくは他の磁気記憶装置、または他の有形のコンピュータ可読媒体などの有形のコンピュータ可読記憶媒体を含むことができる。また、これは、データ信号、データ送信などの無形のコンピュータ可読媒体、または、所望の情報を送信するために使用可能であり且つコンピュータシステム2300によってアクセス可能なその他の媒体を含むことができる。

10

【0309】

一例として、コンピュータ可読記憶媒体2322は、取外し不可能な不揮発性磁気媒体から読取るまたは当該媒体に書込むハードディスクドライブ、取外し可能な不揮発性磁気ディスクから読取るまたは当該ディスクに書込む磁気ディスクドライブ、ならびに、CD-ROM、DVDおよびブルーレイ（登録商標）ディスクまたは他の光学式媒体などの取外し可能な不揮発性光学ディスクから読取るまたは当該ディスクに書込む光学式ディスクドライブを含んでもよい。コンピュータ可読記憶媒体2322は、ジップ（登録商標）ドライブ、フラッシュメモリカード、ユニバーサルシリアルバス (universal serial bus: USB) フラッシュドライブ、セキュアデジタル (secure digital: SD) カード、DVDディスク、デジタルビデオテープなどを含み得るが、これらに限定されるものではない。また、コンピュータ可読記憶媒体2322は、フラッシュメモリベースのSSD、企業向けフラッシュドライブ、ソリッドステートROMなどの不揮発性メモリに基づくソリッドステートドライブ (solid-state drive: SSD)、ソリッドステートRAM、ダイナミックRAM、スタティックRAMなどの揮発性メモリに基づくSSD、DRAMベースのSSD、磁気抵抗RAM (magnetoresistive RAM: MRAM) SSD、およびDRAMとフラッシュメモリベースのSSDとの組み合わせを使用するハイブリッドSSDを含んでもよい。ディスクドライブおよびそれらの関連のコンピュータ可読媒体は、コンピュータ可読命令、データ構造、プログラムモジュールおよび他のデータの揮発性記憶装置をコンピュータシステム2300に提供することができる。

20

30

【0310】

通信サブシステム2324は、他のコンピュータシステムおよびネットワークとのインターフェースを提供する。通信サブシステム2324は、他のシステムからデータを受信したり、コンピュータシステム2300から他のシステムにデータを送信するためのインターフェースの役割を果たす。例えば、通信サブシステム2324は、コンピュータシステム2300がインターネットを介して1つ以上の装置に接続することを可能にし得る。いくつかの実施例では、通信サブシステム2324は、（例えば3G、4GまたはEDGE (enhanced data rates for global evolution) などの携帯電話技術、高度データネットワーク技術を用いて）無線音声および／またはデータネットワークにアクセスするための無線周波数 (radio frequency: RF) トランシーバ構成要素、WiFi (IEEE 802.11ファミリ標準または他のモバイル通信技術またはそれらの任意の組み合わせ)、全地球測位システム (global positioning system: GPS) レシーバ構成要素、および／または、他の構成要素を含んでもよい。いくつかの実施例では、通信サブシステム2324は、無線インターフェースに加えて、または無線インターフェースの代わりに、有線ネットワーク接続（例えばイーサネット）を提供することができる。

40

【0311】

また、いくつかの実施例において、通信サブシステム2324は、コンピュータシステム2300を使用し得る1人以上のユーザを代表して、構造化されたおよび／または構造化されていないデータフィード2326、イベントストリーム2328、イベント更新2

50

330などの形態で入力通信を受信することができる。

【0312】

一例として、通信サブシステム2324は、ツイッター（登録商標）フィード、フェースブック（登録商標）更新、リッチ・サイト・サマリ（Rich Site Summary：RSS）フィードなどのウェブフィードなどのデータフィード2326をリアルタイムでソーシャルネットワークおよび／または他の通信サービスのユーザから受信し、および／または、1つ以上の第三者情報源からリアルタイム更新を受信するように構成されてもよい。

【0313】

また、通信サブシステム2324は、連続的なデータストリームの形態でデータを受信するように構成され得て、当該データは、連続的である場合もあれば本質的に明確な端部を持たない状態で境界がない場合もあるリアルタイムイベントのイベントストリーム2328および／またはイベント更新2330を含んでもよい。連続的なデータを生成するアプリケーションの例としては、例えばセンサデータアプリケーション、金融ティッカ、ネットワーク性能測定ツール（例えばネットワークモニタリングおよびトラフィック管理アプリケーション）、クリックストリーム分析ツール、自動車交通モニタリングなどを含んでもよい。

【0314】

また、通信サブシステム2324は、構造化されたおよび／または構造化されていないデータフィード2326、イベントストリーム2328、イベント更新2330などを、コンピュータシステム2300に結合された1つ以上のストリーミングデータソースコンピュータと通信し得る1つ以上のデータベースに出力するように構成されてもよい。

【0315】

コンピュータシステム2300は、手持ち式携帯機器（例えば、iPhone（登録商標）携帯電話、Ipad（登録商標）計算タブレット、PDA）、ウェアラブル装置（例えば、Google Glass（登録商標）ヘッドマウントディスプレイ）、PC、ワークステーション、メインフレーム、キオスク、サーバラックまたはその他のデータ処理システムを含む様々な種類のうちの1つであってもよい。

【0316】

前述の説明において、説明の目的で、本開示の実施例を完全に理解できるようにするために、具体的な詳細を記載する。しかしながら、これらの具体的な詳細がなくても、様々な実施例を実施できることは明らかであろう。以下の説明は、例のみを提供し、本開示の範囲、適用性、または構成を制限することを意図していない。むしろ、実施例の以下の説明は、実施例を実施するための可能な説明を当業者に提供するものである。添付の特許請求の範囲に規定される本開示の精神及び範囲から逸脱することなく、要素の機能および配置に様々な変更を加えることができることを理解されたい。図面および説明は、制限的であることを意図していない。回路、システム、ネットワーク、プロセス、および他の構成要素は、不必要な詳細で実施例を不明瞭にしないために、ブロック図の形態で構成要素として示されてもよい。他の実施例では、周知の回路、プロセス、アルゴリズム、構造、および技術は、実施例を不明瞭にしないために、不必要な詳細なしに示されてもよい。本開示の教示は、モバイルアプリケーション、非モバイルアプリケーション、デスクトップアプリケーション、ウェブアプリケーション、エンタープライズアプリケーションなどの様々な種類のアプリケーションに適用することもできる。また、本開示の教示は、特定の動作環境（例えば、オペレーティングシステム、デバイス、プラットフォームなど）に限定されるものではなく、複数の異なる動作環境に適用することができる。

【0317】

また、留意すべきことは、各々の実施例は、フローチャート、フロー図、データフロー図、構造図、またはブロック図として示された処理として説明されていることである。フローチャートは、操作を順次処理として説明しているが、多くの操作は、並行でまたは同時に実行することができる。さらに、操作の順序を再配置してもよい。処理は、その操作が完了した時点で終了するが、図に示されていない追加のステップを含んでもよい。処理

は、メソッド、関数、プロシージャ、サブルーチン、サブプログラムなどに対応することができる。処理が関数に対応する場合、その終了は、呼び出し関数またはメイン関数の戻りに対応することができる。

【0318】

「例」および「例示的」という用語は、本明細書において、「例、事例、または例示として役立つ」という意味で使用される。本明細書において「例示的」または「例」として説明された任意の実施形態または設計は、必ずしも他の実施形態または設計よりも好ましいまたは有利であると解釈されるべきではない。

【0319】

「機械可読記憶媒体」または「コンピュータ可読記憶媒体」という用語は、携帯型または非携帯型の記憶装置、光記憶装置、ならびに命令および／またはデータを記憶、格納、または搬送することができる様々な他の媒体を含むが、これらに限定されない。機械可読記憶媒体またはコンピュータ可読記憶媒体は、データを記憶することができ、無線または有線接続を介して伝搬する搬送波および／または一時的な電子信号を含まない非一時的な媒体を含んでもよい。非一時的な媒体の例は、磁気ディスクまたはテープ、コンパクトディスク（CD）またはデジタル多用途ディスク（DVD）などの光記憶媒体、フラッシュメモリ、メモリまたはメモリ装置を含み得るが、これらに限定されない。コンピュータプログラム製品は、プロシージャ、関数、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、命令、データ構造、またはプログラム文の任意の組み合わせを表し得るコードおよび／または機械実行可能命令を含んでもよい。コードセグメントは、情報、データ、引数、パラメータ、またはメモリ内容を転送および／または受取ることによって、別のコードセグメントまたはハードウェア回路に結合されてもよい。情報、引数、パラメータおよびデータなどは、メモリ共有、メッセージ転送、トークン転送、ネットワーク送信などの任意の適切な手段を介して、伝達され、転送され、または送信されてもよい。

【0320】

さらに、実施形態は、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語、またはそれらの任意の組み合わせによって実施されてもよい。ソフトウェア、ファームウェア、ミドルウェアまたはマイクロコードに実施される場合、必要な作業を実行するプログラムコードまたはコードセグメントは、機械可読媒体に記憶されてもよい。プロセッサは、必要な作業を実行することができる。一部の図面に示されたシステムは、様々な構成で提供されてもよい。いくつかの例において、システムは、システムの1つ以上の要素がクラウドコンピューティングシステム内の1つ以上のネットワークにわたって分散される分散システムとして構成されてもよい。要素が特定の動作を実行するように「構成されている」として説明される場合、このような構成は、例えば、動作を実行するように電子回路または他のハードウェアを設計することによって、動作を実行するように電子回路（例えば、マイクロプロセッサまたは他の適切な電子回路）をプログラミングまたは制御することによって、またはそれらの任意の組み合わせによって達成されてもよい。

【0321】

本開示の特定の実施形態を説明してきたが、さまざまな変更、改変、代替構成、および同等物も本開示の範囲内に包含される。本開示の実施形態は、特定のデータ処理環境内で動作するのに限定されず、複数のデータ処理環境内で自由に動作することができる。さらに、一連の特定の処置およびステップを用いて本開示の実施形態を説明してきたが、本開示の範囲が説明された一連の処置およびステップに限定されないことは、当業者にとって明らかであろう。上述した実施形態のさまざまな特徴および態様は、個別にまたは共同で使用することができる。

【0322】

さらに、ハードウェアおよびソフトウェアの特定の組み合わせを用いて本開示の実施形態を説明してきたが、ハードウェアおよびソフトウェアの他の組み合わせも本開示の範囲

10

20

30

40

50

内に含まれることを認識すべきである。ハードウェアのみ、ソフトウェアのみ、またはそれらの組み合わせを用いて、本開示の実施形態を実現することができる。本開示に記載されたさまざまなプロセスは、同一のプロセッサまたは任意の組み合わせの異なるプロセッサ上で実行することができる。したがって、特定の処理を実行するように構成要素またはモジュールを構成すると説明する場合、その構成は、例えば、その処理を実行するように電子回路を設計することによって、その処理を実行するようにプログラム可能な電子回路（マイクロプロセッサなど）をプログラムすることによって、またはそれらの組み合わせによって実現することができる。プロセスは、プロセス間の通信を行う従来技術を含むがこれに限定されないさまざまな技術を用いて通信を行うことができる。異なる対のプロセスは、異なる技術を使用することができ、または同一対のプロセスは、異なる時間で異なる技術を使用することができる。

10

【0323】

したがって、明細書および図面は、限定的な意味ではなく例示的な意味であるとみなすべきである。しかしながら、特許請求の範囲により定められた幅広い主旨および範囲から逸脱することなく、追加、削減、削除および他の修飾および変更を行ってもよいことは、明らかであろう。したがって、本開示の特定の実施形態を説明したが、これらの実施形態は、限定することを意図していない。さまざまな変更およびその等価物は、添付の特許請求の範囲に含まれる。

【0324】

本開示の実施形態の例は、以下の項に照らして説明することができる。

20

項1．方法であって、顧客のレイヤ2仮想ネットワークのアドレスと、上記レイヤ2仮想ネットワークをホストする物理ネットワークのアドレスとを関連付けるマッピング情報を記憶することを含み、上記レイヤ2仮想ネットワークは、複数の計算インスタンスと、複数のレイヤ2仮想ネットワークインターフェースと、複数のレイヤ2仮想スイッチとを備え、上記物理ネットワークは、複数のネットワーク仮想化デバイス（NVD）と複数のホストマシンとを備え、上記複数の計算インスタンスのうちのある計算インスタンスは、上記複数のホストマシンのうちのあるホストマシン上でホストされ、上記ある計算インスタンスは、上記複数のレイヤ2仮想ネットワークインターフェースのうちのあるレイヤ2仮想ネットワークインターフェースと、上記複数のレイヤ2仮想スイッチのうちのあるレイヤ2仮想スイッチとに関連付けられ、上記あるレイヤ2仮想ネットワークインターフェースおよび上記あるレイヤ2仮想スイッチは、上記複数のNVDのうちのあるNVD上でホストされ、上記あるNVDと上記あるホストマシンとは通信可能に結合され、上記方法はさらに、顧客の入力を受信することを含み、上記入力、上記レイヤ2仮想ネットワークにおけるトラフィックフローのためにストーム制御構成を指定し、上記方法はさらに、上記ストーム制御構成および上記マッピング情報に基づいて、上記あるNVDのためにストーム制御情報を生成することと、上記ストーム制御情報を上記あるNVDに送信することとを含む、方法。

30

【0325】

項2．上記入力は、上記ストーム制御構成がポートに適用されることを示し、トラフィックフロー条件で実行されるべきアクションを指定し、上記方法はさらに、上記ポートは上記あるレイヤ2仮想ネットワークインターフェースの媒体アクセス制御（MAC）アドレスに対応すると判断することと、上記マッピング情報に基づいて、上記MACアドレスは上記あるNVDのインターネットプロトコル（IP）アドレスに関連付けられている、と判断することと、上記ストーム制御情報において、上記MACアドレスおよび上記IPアドレスに基づいて上記トラフィックフロー条件および上記アクションを示すこととを含む、項1に記載の方法。

40

【0326】

項3．上記トラフィックフロー条件は、フレーム伝送レートを含み、上記アクションは、フレームをドロップすること、または上記ポートをリンクダウンすることを含む、項2に記載の方法。

50

【0327】

項4．上記トラフィックフロー条件は、最大フレーム伝送レートおよび持続時間を含み、上記アクションは、フレーム伝送レートが上記最大フレーム伝送レートを超過するとフレームをドロップすることと、上記持続時間を超える時間長にわたって上記超過が検出されると上記ポートをリンクダウンすることを含む、項2に記載の方法。

【0328】

項5．上記入力は、上記ストーム制御構成のストーム制御ポリシーが、ユニキャストされるフレーム、ブロードキャストされるフレーム、またはマルチキャストされるフレームのうちの少なくとも1つに適用されることを示し、上記ストーム制御情報は、上記ストーム制御ポリシーと、上記あるレイヤ2仮想ネットワークインターフェースに関連付けられるフレームの流れを制御するための、上記あるNVDへのフレームブロードキャストまたはフレームマルチキャストのうちの上記少なくとも1つに対する上記ストーム制御ポリシーの適用可能性とを示す、項1～4のいずれか1項に記載の方法。

10

【0329】

項6．上記入力は、上記ストーム制御構成のストーム制御ポリシーと、上記ストーム制御ポリシーの違反で実行される上記ストーム制御ポリシーのアクションと、上記ストーム制御ポリシーの反復違反で適用される上記ストーム制御構成のエスカレーションポリシーとを示し、上記ストーム制御情報は、上記ストーム制御ポリシーと、上記アクションと、上記エスカレーションポリシーとを、上記あるレイヤ2仮想ネットワークインターフェースに関連付けられるフレームの流れを制御するために、上記あるNVDに示す、項1～5

20

【0330】

項7．上記入力は、上記ストーム制御構成の伝送レートのタイプを示し、上記伝送レートのタイプは、フレーム／秒またはビット／秒のうちの少なくとも1つを含み、上記ストーム制御情報は、上記伝送レートのタイプを、上記あるレイヤ2仮想ネットワークインターフェースに関連付けられるフレームの流れを制御するために、上記あるNVDに示す、項1～6のいずれか1項に記載の方法。

【0331】

項8．上記入力は、上記ストーム制御構成の統計のタイプを示し、上記ストーム制御情報は、上記統計のタイプを、上記あるレイヤ2仮想ネットワークインターフェースに関連付けられるフレームの流れに関する統計を収集するために、上記あるNVDに示す、項1～7のいずれか1項に記載の方法。

30

【0332】

項9．上記入力は、上記ストーム制御構成が複数のポートに適用されることを示し、上記方法はさらに、上記複数のポートは上記複数のレイヤ2仮想ネットワークインターフェースのうちのあるレイヤ2仮想ネットワークインターフェースのセットに対応する、と判断することと、上記マッピング情報に基づいて、上記あるレイヤ2仮想ネットワークインターフェースのセットが上記複数のNVDのうちのあるNVDのセットに関連付けられる、と判断することと、上記あるNVDのセットの各NVDに上記ストーム制御情報を送信することを含む、項1～8のいずれか1項に記載の方法。

40

【0333】

項10．上記ストーム制御構成、上記ストーム制御情報、上記あるNVD、および上記あるレイヤ2仮想ネットワークインターフェースは、それぞれ、第1のストーム制御構成、第1のストーム制御情報、第1のNVD、および第1のレイヤ2仮想ネットワークインターフェースであり、上記方法はさらに、上記入力は、(i)第2のストーム構成と、(i i)上記第1のストーム制御構成は第1のポートに適用されることと、(i i i)上記第2のストーム構成は第2のポートに適用されることと示す、と判断することと、上記第1のポートは上記第1のレイヤ2仮想ネットワークインターフェースに対応し、上記第2のポートは上記複数のレイヤ2仮想ネットワークインターフェースのうち第2のレイヤ2仮想ネットワークインターフェースに対応する、と判断することと、上記マッピング情

50

報に基づいて、上記第1のレイヤ2仮想ネットワークインターフェースは上記第1のNVDによってホストされ、上記第2のレイヤ2仮想ネットワークインターフェースは上記複数のNVDのうちの第2のNVDによってホストされる、と判断することと、上記第2のストーム構成に基づいて第2のストーム制御情報を生成することと、上記第2のNVDに上記第2のストーム制御情報を送信することを含む、項1～9のいずれか1項に記載の方法。

【0334】

項11．上記ストーム制御構成は、伝送レートに対する第1の制限を示し、上記ストーム制御構成は、乗数による上記第1の制限の調整に対応する第2の制限を示す、項1～10のいずれか1項に記載の方法。

【0335】

項12．上記方法はさらに、上記トラフィックフローに関するメトリックを収集することと、上記メトリックに基づいて上記乗数を更新することと、上記ストーム制御構成に関する更新を上記あるNVDに送信することを含む、上記更新は、上記更新された乗数または上記更新された乗数に基づく更新された第2の制限のうちの少なくとも1つを含む、項11に記載の方法。

【0336】

項13．ネットワーク仮想化デバイスであって、1つ以上のプロセッサと、命令を記憶する1つ以上のコンピュータ可読記憶媒体とを備え、上記命令は、上記1つ以上のプロセッサによって実行されると、上記ネットワーク仮想化デバイスを、顧客のレイヤ2仮想ネットワークに属するレイヤ2仮想ネットワークインターフェースおよびレイヤ2仮想スイッチをホストするよう構成し、上記レイヤ2仮想ネットワークインターフェースおよび上記レイヤ2仮想スイッチは、上記レイヤ2仮想ネットワークに属するレイヤ2計算インスタンスに関連付けられ、上記レイヤ2計算インスタンスは、上記ネットワーク仮想化デバイスを備える物理ネットワークのホストマシン上でホストされ、上記ホストマシンおよび上記ネットワーク仮想化デバイスは、通信可能に結合され、上記レイヤ2仮想ネットワークは、上記物理ネットワーク上でホストされ、複数のレイヤ2計算インスタンスと、複数のレイヤ2仮想ネットワークインターフェースと、複数のレイヤ2仮想スイッチとを備え、上記命令は、さらに、上記1つ以上のプロセッサによって実行されると、上記ネットワーク仮想化デバイスを、ストーム制御ポリシーと、上記ストーム制御ポリシーの違反で実行されるべきアクションとを示すストーム制御情報を記憶するよう構成し、上記レイヤ2仮想ネットワークインターフェースへのトラフィックフローおよび／または上記レイヤ2仮想ネットワークインターフェースからのトラフィックフローを監視するよう構成し、上記トラフィックフローは上記ストーム制御ポリシーに違反する、と判断するよう構成し、上記ストーム制御ポリシーに違反する上記トラフィックフローに基づいて上記アクションを開始するよう構成する、ネットワーク仮想化デバイス。

【0337】

項14．上記ストーム制御ポリシーは、上記レイヤ2仮想ネットワークインターフェースへの着信トラフィックに対する最大伝送レートを示し、上記アクションは、フレームをドロップすることを含み、上記トラフィックフローは上記ストーム制御ポリシーに違反する、と判断することは、上記レイヤ2仮想ネットワークインターフェースへの着信フレームの伝送レートが上記最大伝送レートを超える、と判断することを含み、上記アクションを開始することは、着信フレームをドロップすることを含む、項13に記載のネットワーク仮想化デバイス。

【0338】

項15．上記ストーム制御ポリシーはさらに、エスカレーションアクションのための持続時間を示し、上記エスカレーションアクションはリンクダウンを含み、上記トラフィックフローは上記ストーム制御ポリシーに違反する、と判断することは、上記伝送レートは上記持続時間よりも長く持続した、と判断することをさらに含み、上記アクションを開始することは、上記レイヤ2仮想ネットワークインターフェースをリンクダウンすることを含む、

10

20

30

40

50

さらに含む、項 1 4 に記載のネットワーク仮想化デバイス。

【0339】

項 1 6 . 上記レイヤ 2 仮想ネットワークインターフェースは、第 1 のレイヤ 2 仮想ネットワークインターフェースであり、上記ストーム制御ポリシーは、第 2 のレイヤ 2 仮想ネットワークインターフェースへの着信トラフィックに対する最大伝送レートを示し、上記アクションは、フレームをドロップすることを含み、上記トラフィックフローは上記ストーム制御ポリシーに違反する、と判断することは、上記第 1 のレイヤ 2 仮想ネットワークインターフェースから上記第 2 のレイヤ 2 仮想ネットワークインターフェースへのフレームの伝送レートが上記最大伝送レートを超える、と判断することを含み、上記アクションを開始することは、上記第 1 のレイヤ 2 仮想ネットワークインターフェースから上記第 2 のレイヤ 2 仮想ネットワークインターフェースへのフレームをドロップすることを含む、項 1 4 に記載のネットワーク仮想化デバイス。

10

【0340】

項 1 7 . 上記ストーム制御情報は、上記顧客の入力によって示されるストーム制御構成と、上記レイヤ 2 仮想ネットワークのアドレスと上記物理ネットワークのアドレスとを関連付けるマッピング情報とに基づいて生成される、項 1 4 に記載のネットワーク仮想化デバイス。

【0341】

項 1 8 . 上記顧客の上記入力は、上記ストーム制御構成が適用されるポートを示し、上記ストーム制御情報はさらに、上記ポートと上記レイヤ 2 仮想ネットワークインターフェースとの間の対応関係に基づいて生成され、上記対応関係に基づいて上記レイヤ 2 仮想ネットワークインターフェースに適用される、項 1 7 に記載のネットワーク仮想化デバイス。

20

【0342】

項 1 9 . システムであって、1 つ以上のプロセッサと、命令を記憶する 1 つ以上のコンピュータ可読記憶媒体とを備え、上記命令は、上記 1 つ以上のプロセッサによって実行されると、上記システムを、顧客のレイヤ 2 仮想ネットワークのアドレスと、上記レイヤ 2 仮想ネットワークをホストする物理ネットワークのアドレスとを関連付けるマッピング情報を記憶するよう構成し、上記レイヤ 2 仮想ネットワークは、複数の計算インスタンスと、複数のレイヤ 2 仮想ネットワークインターフェースと、複数のレイヤ 2 仮想スイッチとを備え、上記物理ネットワークは、複数のネットワーク仮想化デバイス (NVD) と複数のホストマシンとを備え、上記複数の計算インスタンスのうちのある計算インスタンスは、上記複数のホストマシンのうちのあるホストマシン上でホストされ、上記ある計算インスタンスは、上記複数のレイヤ 2 仮想ネットワークインターフェースのうちのあるレイヤ 2 仮想ネットワークインターフェースと、上記複数のレイヤ 2 仮想スイッチのうちのあるレイヤ 2 仮想スイッチとに関連付けられ、上記あるレイヤ 2 仮想ネットワークインターフェースおよび上記あるレイヤ 2 仮想スイッチは、上記複数の NVD のうちのある NVD 上でホストされ、上記ある NVD と上記あるホストマシンとは通信可能に結合され、上記命令は、さらに、上記 1 つ以上のプロセッサによって実行されると、上記システムを、顧客の入力を受信するよう構成し、上記入力、上記レイヤ 2 仮想ネットワークにおけるトラフィックフローのためにストーム制御構成を指定し、上記命令は、さらに、上記 1 つ以上のプロセッサによって実行されると、上記システムを、上記ストーム制御構成および上記マッピング情報に基づいて、上記ある NVD のためにストーム制御情報を生成するよう構成し、上記ストーム制御情報を上記ある NVD に送信するよう構成する、システム。

30

40

【0343】

項 2 0 . 上記ある NVD をさらに備え、上記ある NVD は、上記ストーム制御情報を記憶するよう構成され、上記ストーム制御情報は、ストーム制御ポリシーと、上記ストーム制御ポリシーの違反で実行されるべきアクションとを示し、上記ある NVD はさらに、上記レイヤ 2 仮想ネットワークインターフェースへのトラフィックフローおよび / または上記レイヤ 2 仮想ネットワークインターフェースからのトラフィックフローを監視するよう

50

構成され、上記トラフィックフローは上記ストーム制御ポリシーに違反する、と判断するよう構成され、上記ストーム制御ポリシーに違反する上記トラフィックフローに基づいて上記アクションを開始するよう構成される、項19に記載のシステム。

【0344】

本開示を説明する文脈に（特に特許請求の範囲の文脈に）使用された不定冠詞「a」／「an」、定冠詞「the」および同様の参照は、本明細書に特に明記しない限りまたは内容上明らかに他の意味を示す場合を除き、単数および複数の両方を含むように解釈すべきである。用語「含む（comprising）」、「有する（having）」、「含む（including）」、および「含有する（containing）」は、特に明記しない限り、非限定的な用語（すなわち、「含むがこれに限定されない」という意味）として解釈されるべきである。「接続されている」という用語は、たとえ何かが介在していても、その一部または全部が内部に含まれている、取り付けられている、または一緒に結合されていると解釈されるべきである。本明細書において、値の範囲の列挙は、単にその範囲内に含まれる各個別の値を各々言及する速記方法として意図され、本明細書に特に明記しない限り、各個別の値は、本明細書に個別に記載されるように、本明細書に組み込まれる。本明細書に特に明記しない限りまたは内容上明らかに他の意味を示す場合を除き、本明細書に記載の全ての方法は、任意の適切な順序で行うことができる。本明細書において、任意の例および全ての例または例示的な言語（例えば、「～のような」）の使用は、本開示の実施形態をより明瞭にするよう意図されており、特に明記しない限り、本開示の範囲を限定するものではない。明細書内の用語は、本開示の実施に不可欠な任意の非請求要素を示すものと解釈すべきではない。

10

20

【0345】

句「X、Y、またはZの少なくとも1つ」というフレーズのような選言的言語は、特に断らない限り、項目、用語などがX、YもしくはZ、またはそれらの任意の組み合わせ（例えば、X、Y、および／またはZ）のいずれかであってもよいことを示すために一般的に用いられるものとして文脈内で理解されることを意図している。したがって、このような選言的言語は、特定の実施形態が、Xの少なくとも1つ、Yの少なくとも1つ、またはZの少なくとも1つが存在することを必要とすることを一般に意図しておらず、また、それを暗示していない。

【0346】

本開示を実施するために知られている最良の形態を含み、本開示の好ましい実施形態が本明細書に記載されている。これらの好ましい実施形態の変形形態は、前述の説明を読めば当業者には明らかになるであろう。当業者は、適宜、このような変形例を採用することができ、本開示は、本明細書に具体的に記載されている以外の方法で実施されてもよい。したがって、本開示は、適用される法律によって許可され、本明細書に添付された請求項に記載された主題の全ての変形および等価物を含む。さらに、その全ての可能な変形における上記の要素の任意の組み合わせは、本明細書において別段の指示がない限り、本開示に包含される。

30

【0347】

本明細書に引用された刊行物、特許出願、および特許を含む全ての参考文献は、各文献が参照により組み込まれることが個別にかつ明確に示され、その全体が本明細書に記載された場合と同じ程度に、参照により組み込まれるものとする。

40

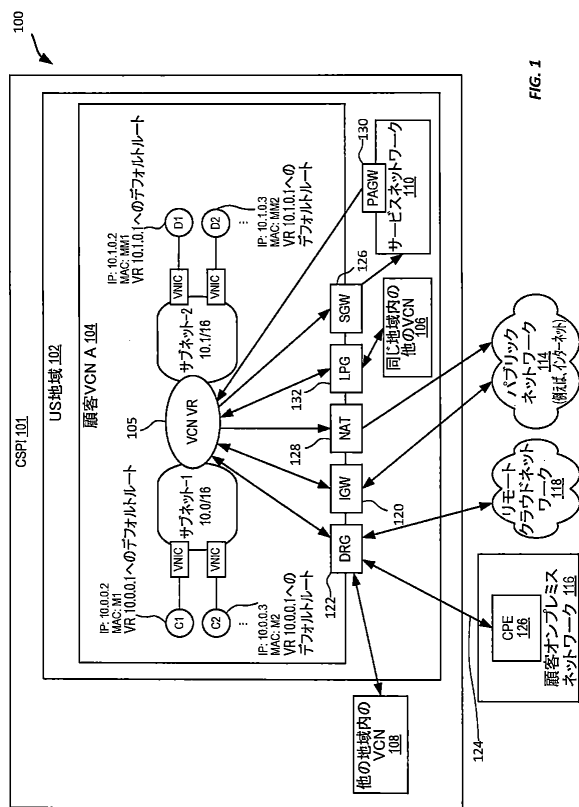
【0348】

前述の明細書において、本開示の態様は、その特定の実施形態を参照して説明されているが、当業者は、本開示がそれに限定されないことを認識するであろう。上述の開示の様々な特徴および態様は、個々にまたは共同で使用されてもよい。さらに、実施形態は、本明細書のより広い精神および範囲から逸脱することなく、本明細書に説明されるものを超える任意の数の環境および用途において利用されることができる。したがって、明細書および図面は、限定的ではなく例示的であると見なされるべきである。

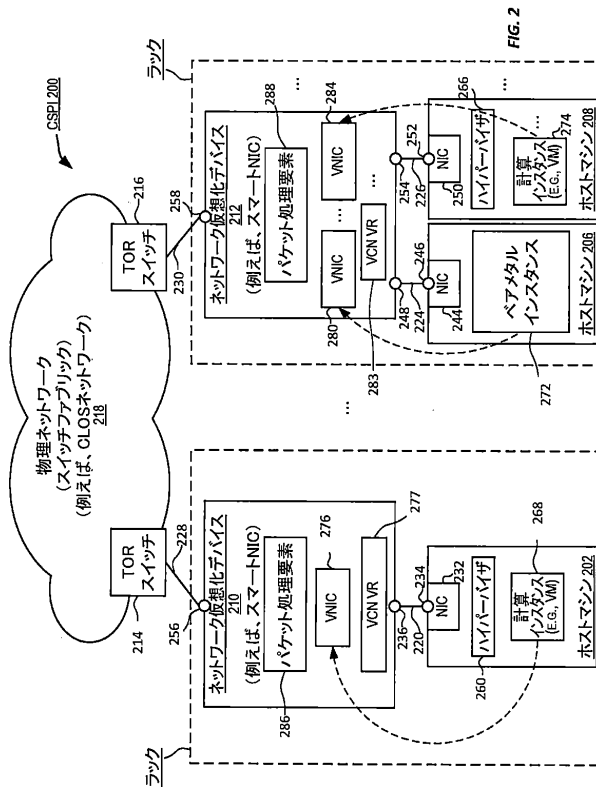
50

【図面】

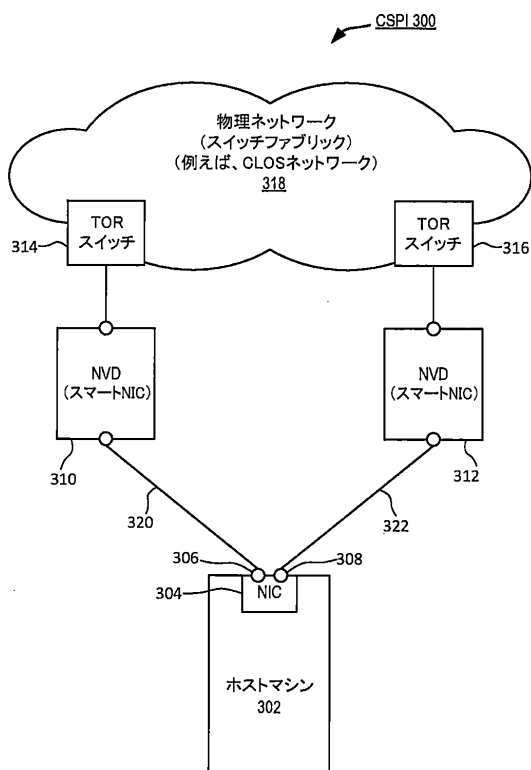
【図 1】



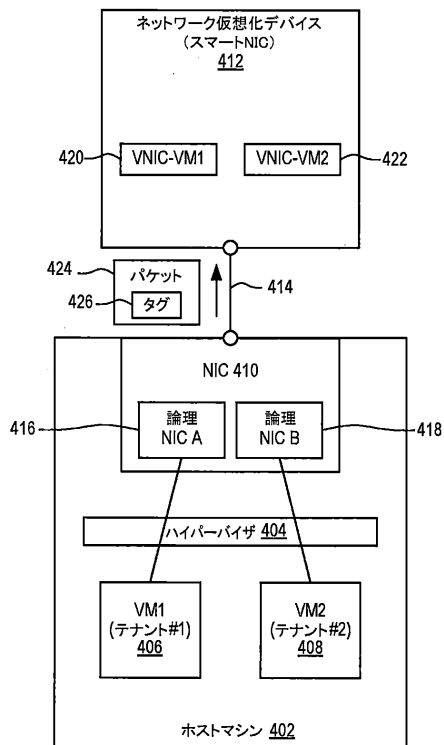
【図 2】



【図 3】



【図 4】



【図 5】

物理ネットワーク (例えば、3階CLOSネットワーク) 500

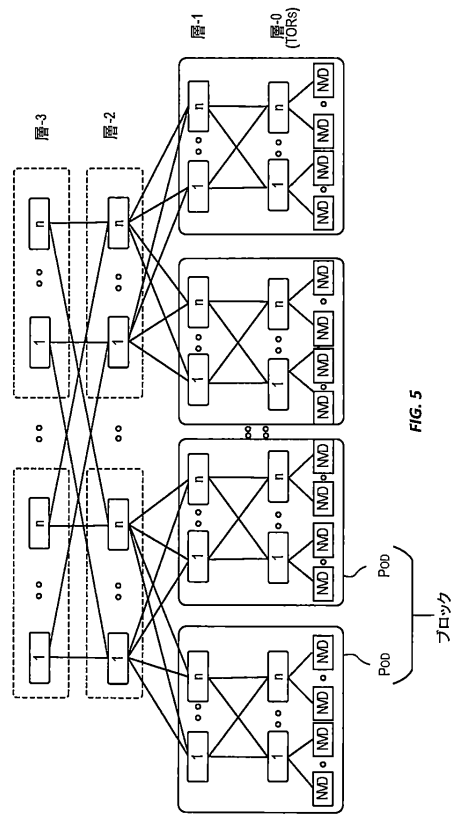


FIG. 5

【図 6】

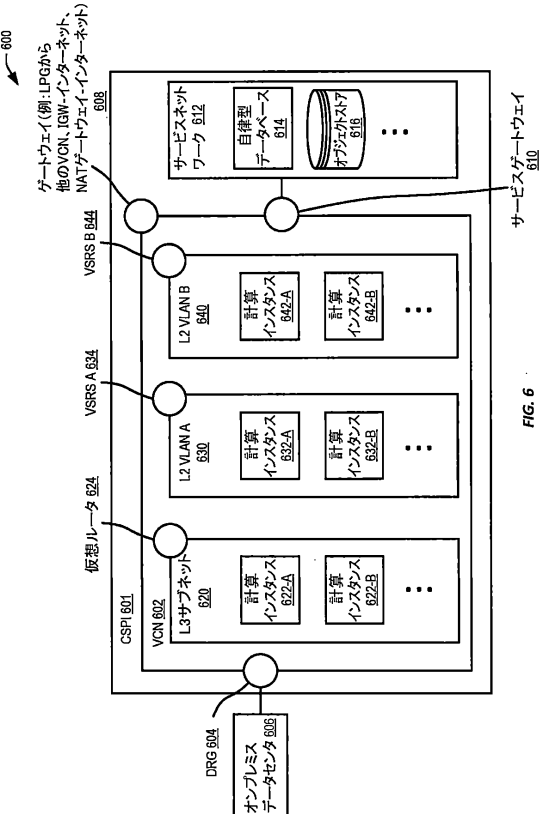


FIG. 6

【図 7】

700

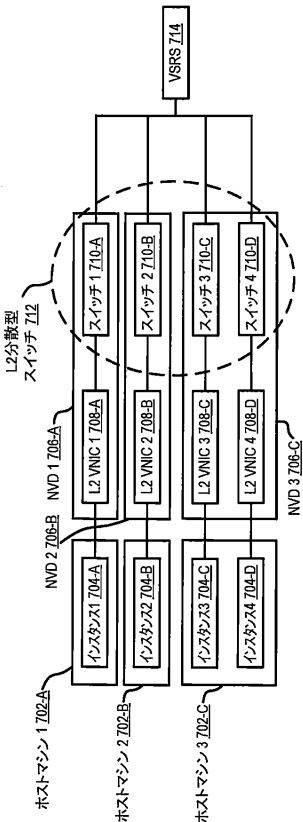


FIG. 7

【図 8】

800

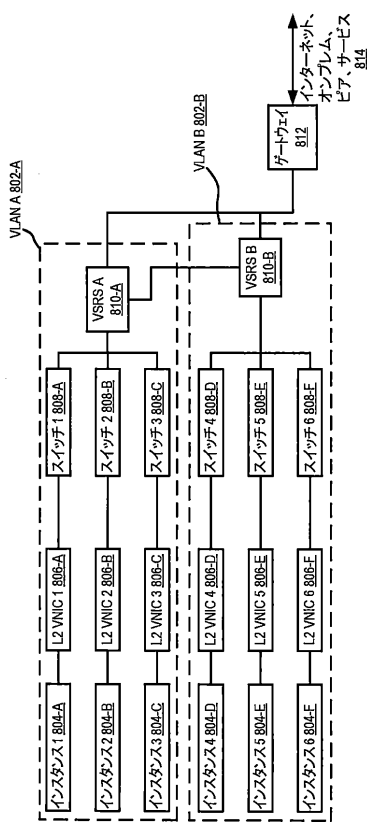
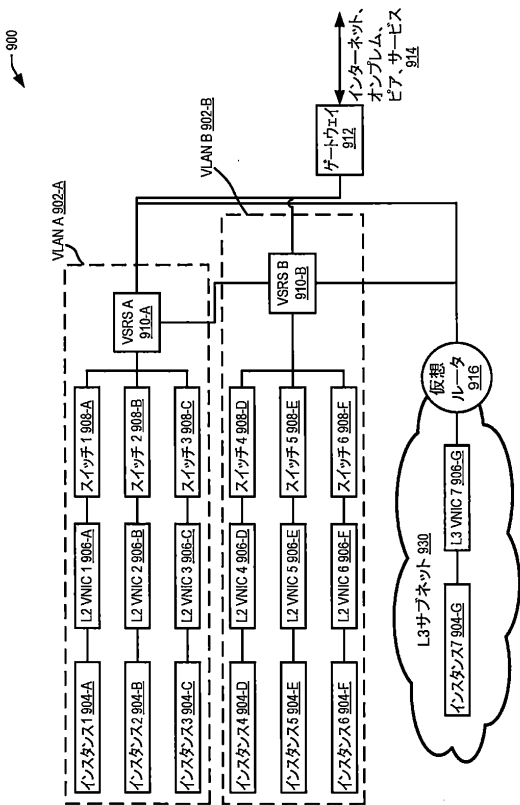
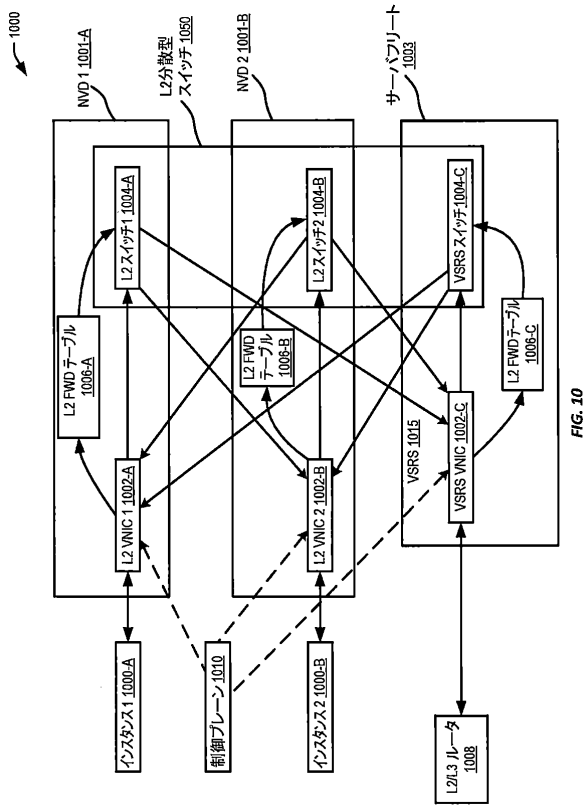


FIG. 8

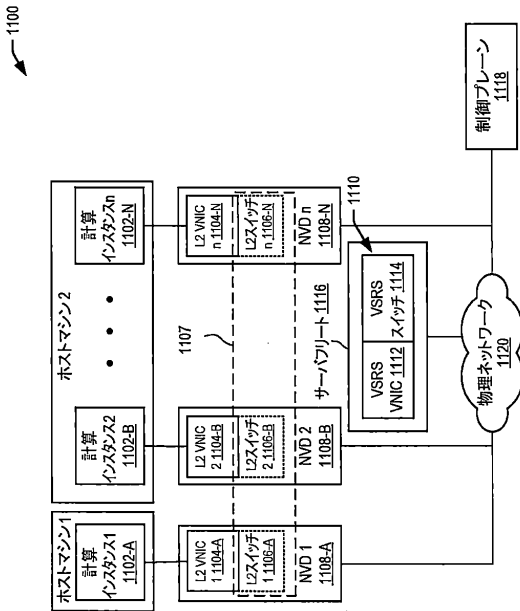
【図 9】



【図 10】



【図 11】



【図 12】

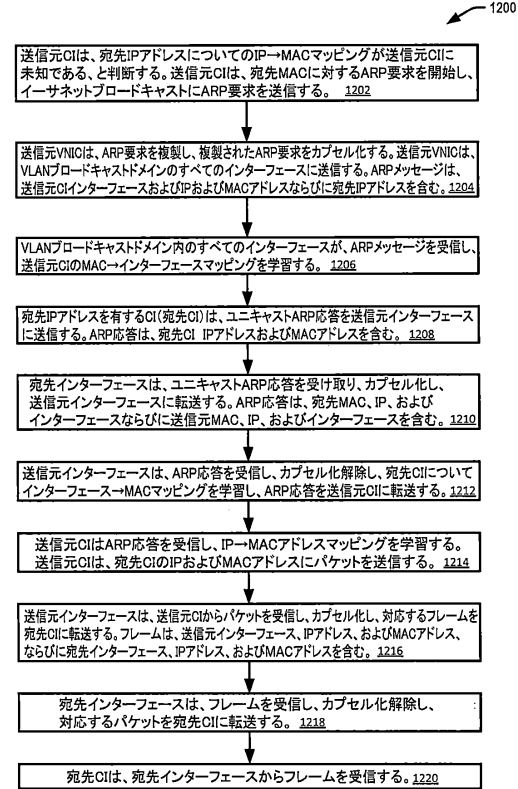


FIG. 12

【図 13】

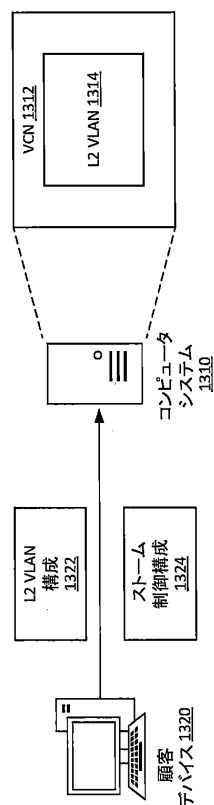


FIG. 13

【図 14】

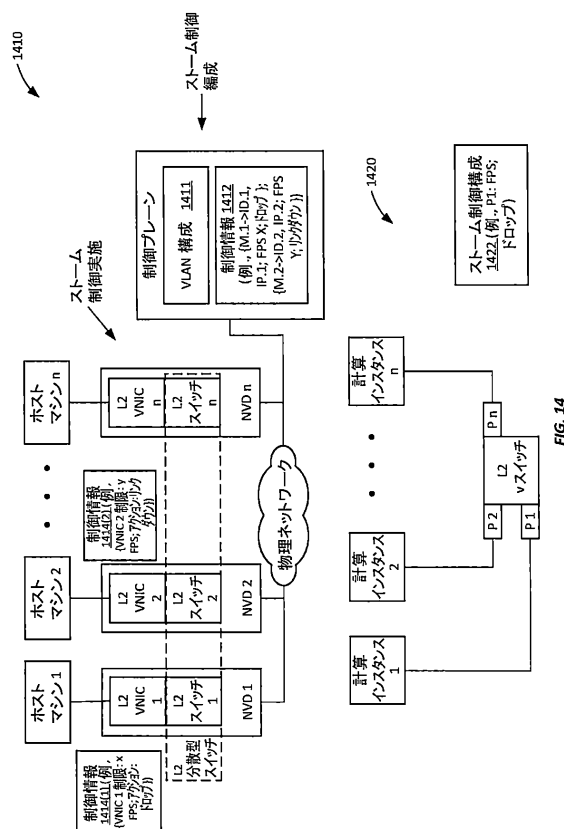


FIG. 14

【図 15】

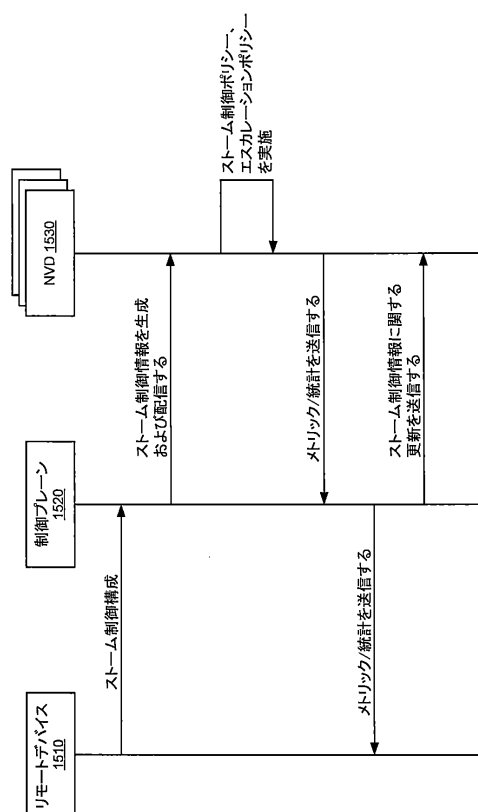


FIG. 15

【圖 16】

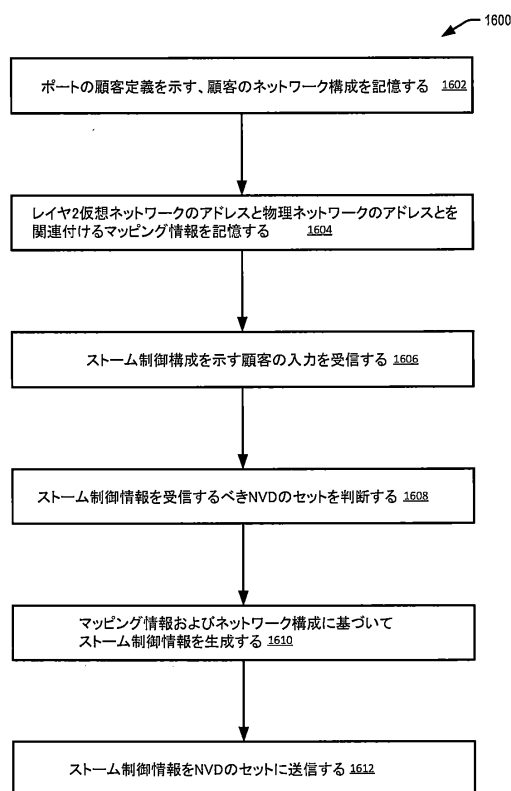


FIG. 16

【図 17】

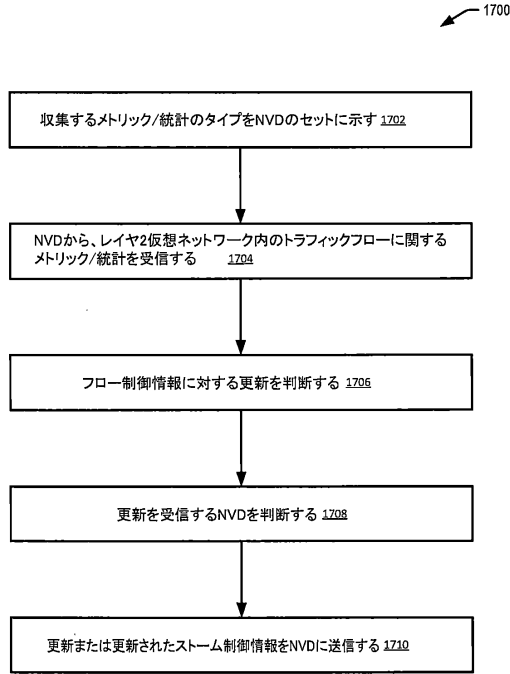


FIG. 17

【図 18】

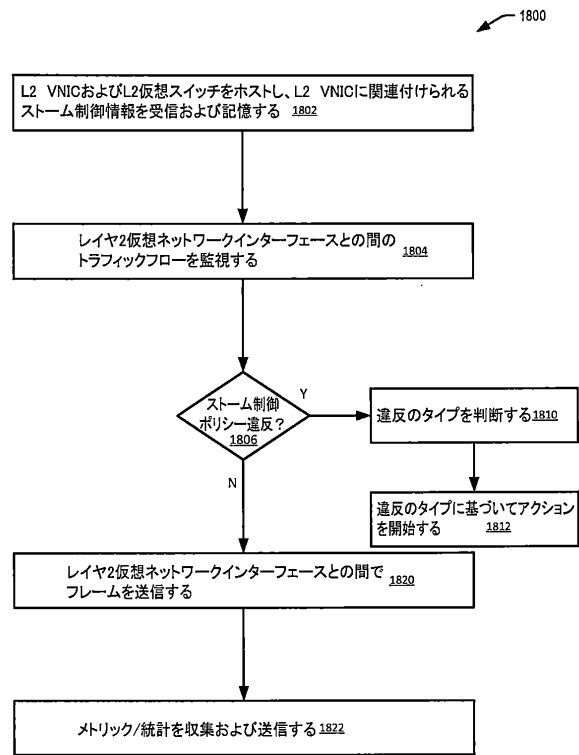
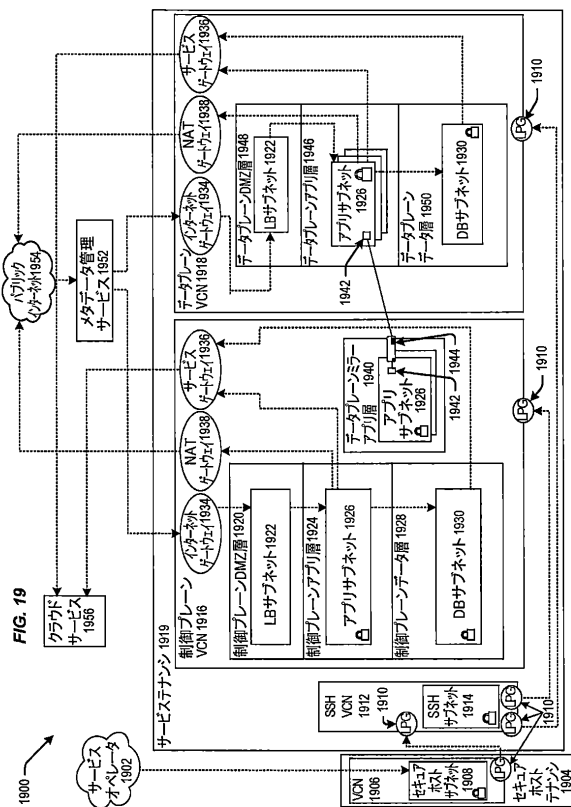
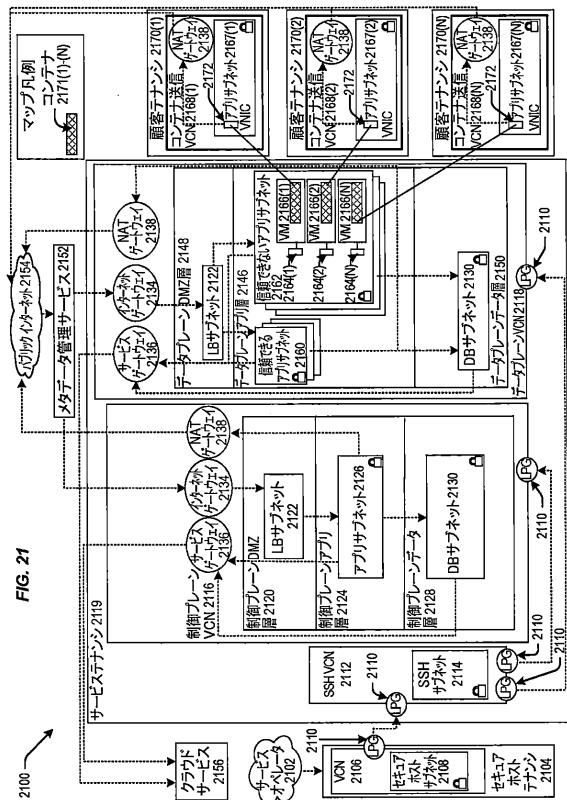


FIG. 18

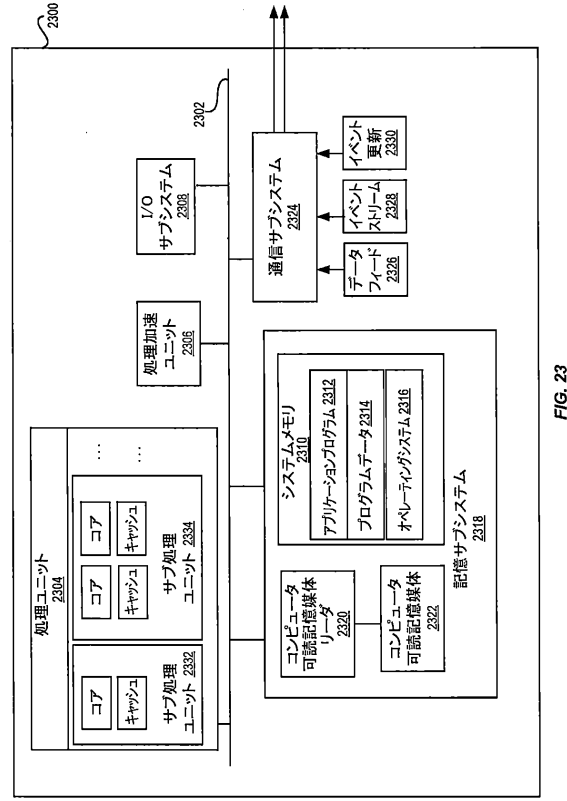
【図 19】



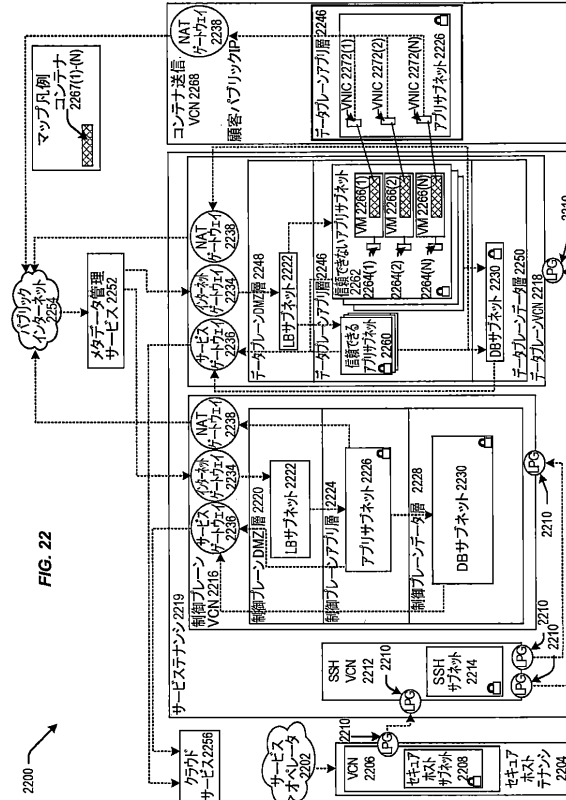
【図 2 1】



【図 2 3】



【図 2 2】



10

20

30

40

50

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2021/060820

A. CLASSIFICATION OF SUBJECT MATTER					
INV.	H04L45/00	H04L45/586	H04L45/745	H04L45/12	H04L45/24
	H04L45/18	H04L47/10	H04L45/16		
ADD.					
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)					
H04L					
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched					
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)					
EPO-Internal, WPI Data, INSPEC					
C. DOCUMENTS CONSIDERED TO BE RELEVANT					
Category*	Citation of document, with indication, where appropriate, of the relevant passages				Relevant to claim No.
X,P	EP 3 783 835 A1 (JUNIPER NETWORKS INC [US]) 24 February 2021 (2021-02-24) abstract paragraphs [0003], [0016], [0017] paragraph [0020] - paragraph [0032] paragraphs [0035], [0038] - [0042] paragraph [0044] - paragraph [0056] paragraph [0059] - paragraph [0063]; claims 1-10; figures 1-5 -----				1-20
X	US 10 009 371 B2 (NICIRA INC [US]; NICIRA INC [US]) 26 June 2018 (2018-06-26) abstract column 1, line 60 - column 4, line 15; claims 1-14; figures 1-5 ----- -/--				1-20
☒ Further documents are listed in the continuation of Box C. ☒ 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			"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		
"E" earlier application or patent but published on or after the international filing date			"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		
"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)			"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		
"O" document referring to an oral disclosure, use, exhibition or other means			"&" document member of the same patent family		
"P" document published prior to the international filing date but later than the priority date claimed					
Date of the actual completion of the international search			Date of mailing of the international search report		
11 March 2022			21/03/2022		
Name and mailing address of the ISA/ European Patent Office, P.B. 5618 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016			Authorized officer Todorut, Cosmin		

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2021/060820

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/158248 A1 (VORUNGANTI SREENIVAS [IN] ET AL) 30 June 2011 (2011-06-30) abstract paragraph [0004] - paragraph [0008] paragraph [0025] - paragraph [0030] paragraph [0036] - paragraph [0058]; claims 1-20; figures 1-7 -----	1-20
X	CN 106 936 777 B (CHINA MOBILE (SUZHOU) SOFTWARE TECH CO LTD; CHINA MOBILE COMM CORP) 14 February 2020 (2020-02-14) the whole document -----	1-20
A	EP 2 680 514 A1 (TELLABS OY [FI]) 1 January 2014 (2014-01-01) abstract paragraph [0020] - paragraph [0038]; claims 1-15; figures 1,2 -----	1-20
A	US 2013/286832 A1 (RAJAH RAJESH AMARESH [US] ET AL) 31 October 2013 (2013-10-31) paragraphs [0002], [0013] paragraph [0016] - paragraph [0018] paragraph [0021] - paragraph [0025] paragraph [0038] - paragraph [0043]; claims 1-20; figures 1-6 -----	1-20
A	Cisco: "Configuring Traffic Storm Control This chapter describes how to configure traffic storm control on Cisco Nexus 5000 Series switches. It contains the following sections: @BULLET Information About Traffic Storm Control, page 1 @BULLET Traffic Storm Guidelines and Limitations, page 2 @BULLET Configurin", / 29 July 2011 (2011-07-29), XP055229267, Retrieved from the Internet: URL:http://www.cisco.com/c/en/us/td/docs/s witches/datacenter/nexus5000/sw/layer2/503 _n2_1/503_n2_inw/Cisco_n5k_layer2_config_g d_rel_503_N2_1_chapter16.pdf [retrieved on 2015-11-18] the whole document -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2021/060820

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 3783835	A1	24-02-2021	CN 112398676 A	23-02-2021
			EP 3783835 A1	24-02-2021
			US 2021058295 A1	25-02-2021

US 10009371	B2	26-06-2018	NONE	

US 2011158248	A1	30-06-2011	NONE	

CN 106936777	B	14-02-2020	NONE	

EP 2680514	A1	01-01-2014	CN 103532775 A	22-01-2014
			EP 2680514 A1	01-01-2014
			US 2014006608 A1	02-01-2014

US 2013286832	A1	31-10-2013	NONE	

10

20

30

40

50

フロントページの続き

,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,D
K,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),O
A(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,B
B,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD
,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,IT,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,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,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,Z
W

マイケル

アメリカ合衆国、94065 カリフォルニア州、レッドウッド・シティ、オラクル・パークウ
エイ、500、オラクル・インターナショナル・コーポレーション内

(72)発明者 ボックマン、ブライス・ユージーン

アメリカ合衆国、94065 カリフォルニア州、レッドウッド・シティ、オラクル・パークウ
エイ、500、オラクル・インターナショナル・コーポレーション内

(72)発明者 ジョーンズ、ピーター・クロフト

アメリカ合衆国、94065 カリフォルニア州、レッドウッド・シティ、オラクル・パークウ
エイ、500、オラクル・インターナショナル・コーポレーション内

(72)発明者 ベイカー、シェーン

アメリカ合衆国、94065 カリフォルニア州、レッドウッド・シティ、オラクル・パークウ
エイ、500、オラクル・インターナショナル・コーポレーション内

Fターム (参考) 5K030 GA13 HD03 LC01 MA04 MB02 MC08 MD07