I531185

(19)中華民國智慧財產局

(12)發明說明書公告本 (11)證書號數：TW I531185 B

(45)公告日： 中華民國 105 (2016) 年 04 月 21 日

(21)申請案號：100117829 (22)申請日： 中華民國 100 (2011) 年 05 月 20 日

(51)Int. Cl.： *H04L12/66 (2006.01)* *H04L29/06 (2006.01)*

(30)優先權：2010/06/22 美國 12/820,896

(71)申請人：微軟技術授權有限責任公司 (美國) MICROSOFT TECHNOLOGY LICENSING, LLC (US)

美國

(72)發明人：艾爾卡堤伯哈森 ALKHATIB, HASAN (US) ；奧斯瑞德傑歐夫 OUTHRED, GEOFF (AU)

(74)代理人：蔡坤財；李世章

(56)參考文獻：

TW I310275 US 6697872B1

US 2007/0280243A1

審查人員：蔡鴻璟

申請專利範圍項數：19 項 圖式數：5 共 48 頁

(54)名稱

分散式虛擬網路閘道

DISTRIBUTED VIRTUAL NETWORK GATEWAYS

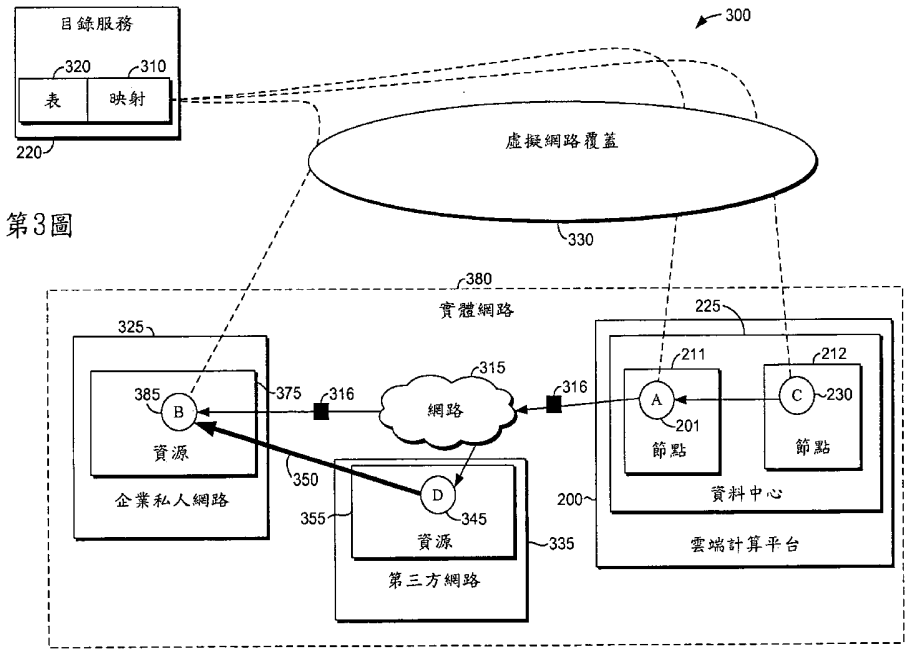
(57)摘要

提供用於分散虛擬閘道功能至一實體網路之中的多重節點的電腦化方法、系統、及電腦可讀取媒體。首先，供應執行閘道功能的驅動程式與在網路節點上例示的端點合作，同時實施一目錄服務，以在虛擬網際網路協定(IP)位址及位置相依位址之間維持一映射，並且根據在一網路之中連接端點的已知路徑，而維持一列舉轉換動作表。在操作中，目錄服務以適當的位置相依位址(利用映射)及適當的轉換動作(利用表)而對來自驅動程式(攜帶資料封包的來源及目的 IP 位址)的請求回應。轉換動作包括重新寫入資料封包的標頭以包括位置相依位址、在分別的外部資料封包之中包覆資料封包作為內部資料封包、或以一通道協定配置資料封包。

Computerized methods, systems, and computer-readable media are provided for distributing virtualized gateway functionality to multiple nodes within a physical network. Initially, drivers that carry out the gateway functionality are provisioned to cooperate with endpoints instantiated on the network nodes, while a directory service is implemented to maintain a mapping between virtual internet protocol (IP) addresses and location-dependent addresses, as well as a table enumerating transformation actions according to known pathways connecting the endpoints within a network. In operation, the directory service replies to requests from the driver (carrying source and destination IP addresses of data packets) with the appropriate location-dependent addresses (utilizing the mapping) and the appropriate transformation action(s) (utilizing the table). The transformation action(s) include rewriting headers of the data packets to include the location-dependent addresses, encapsulating the data packets as inner data packets within respective outer data packets, or configuring the data packets with a tunneling protocol.

TW I531185 B

指定代表圖：



第3圖

符號簡單說明：

201・・・端點

211・・・節點

212・・・節點

220・・・目錄服務

225・・・資料中心

230・・・端點

300・・・分散式計算環境

310・・・映射

315・・・網路

316・・・資料封包

320・・・表

325・・・企業私人網路

330・・・虛擬網路覆蓋

335・・・第三方網路

345・・・端點

350・・・安全通道

355・・・資源

375・・・資源

380・・・實體網路

385・・・端點

六、發明說明：

【發明所屬之技術領域】

本發明係關於分散式虛擬網路閘道。

【先前技術】

大規模的網路化系統係利用於各種設定的普通平台，該等各種設定包括對商業及操作功能而運行服務應用程式及維持資料。舉例而言，一資料中心（例如，實體雲端計算基礎建設）可同時對複數個客戶提供各種服務（例如，網頁應用程式、電子郵件服務、搜尋引擎服務等等）。此等大規模的網路化系統典型地包括大量的資源分散遍及資料中心，其中各個資源類似運行於一實體主機上的一實體機器或一虛擬機器（VM）。當資料中心裝載多重住戶（例如，客戶程式）時，此等資源從資料中心被分配至不同的住戶以滿足該等住戶的使用要求。分配到一住戶的資源集可被分組於一邏輯或虛擬子集中，以方便管理及安全隔離。

資料中心的客戶常常要求運行於一企業私人網路中的服務應用程式（例如，由地理上遠離資料中心的一客戶所管理的伺服器）或要求其他第三方網路，與資料中心之中運行在資源上的軟體互動。為了實施此互動同時將分配至一住戶的資源安全地與分配至其他住戶的資源分開，一主機服務提供者可利用一單一、集中路由的機制，

供以在屬於一虛擬子集之中的一住戶的所有機器之間，或由一主機超管理器所管理的資源及住戶的遠端資源之間，作為一網路閘道。然而，利用集中路由機制的此架構係效率不彰的，因為操作取決於機制實體靠近該機制所服務的機器/資源。舉例而言，若機器/資源係在資料中心的不同部分或在不同位置中（例如，散佈於資料中心及企業私人網路），則至少某些機器/資源在由其他機器/資源利用的同時，將面對較高的潛伏期及與驅動程式連接的較低的頻寬。因此，集中路由機制成為用於進入及離開一特定虛擬子集的通訊的一常常壅塞的點。再者，當配置為所有通訊透過此集中路由機制通過時，機器/資源將被迫傳送資料封包通過次佳的路由。

如此，利用新興技術，以藉由將驅動程式安裝於實體機器（併入本端機器網路堆疊中）或虛擬機器（併入虛擬交換網路堆疊中）之中，而分散虛擬網路閘道或驅動程式遍及一資料中心，此舉將藉由發現及利用最佳的網路途徑而增進資料封包的傳送、藉由分散閘道功能而減少網路配置、且供以進一步隔離資料中心客戶的通訊。

【發明內容】

提供此發明內容以一簡化的形式介紹概念，此概念於以下的詳細實施方式進一步說明。此發明內容並非意圖識別所主張的標的之關鍵特徵或重要特徵，亦非意圖被

用於幫助決定所主張標的之範疇。

本發明的實施例提供分散式虛擬網路閘道的一架構，該架構解決上述之問題。此等閘道可採取驅動程式的形式，而可藉由裝設驅動程式在實體機器（併入本端機器網路堆疊之中）或虛擬機器（併入虛擬交換網路堆疊之中）之中而供應遍及一資料中心。如以下將詳細的說明，驅動程式藉由發現及利用最佳網路途徑來增進資料封包的傳送、藉由分散閘道功能來降低網路壅塞、且供以進一步隔離資料中心客戶的通訊。再者，驅動程式保護運行於一雲端計算平台中的一客戶的服務應用程式的完整性，該雲端計算平台係配置成允許多重住戶（例如，每一個雲端具有數萬個住戶）在一雲端服務資料中心分享計算資源。

一般而言，驅動程式支援在端點之間選擇一最適當的格式及一通訊的途徑，而分配至服務應用程式，同時驅動程式支援虛擬地在一資料中心之中將分配的網路轉接器與其他資源分隔。藉由澄清的方式，端點可包含網路轉接器，該等網路轉接器在虛擬機器（VMs）及/或實體機器上初始化。為了達成在通訊之中的格式選擇及資料封包的途徑，在實施例中，驅動程式向外伸展至目錄服務，該等目錄服務幫助驅動程式對驅動程式的分別的來源及目標端點作成路由決策。藉由來自目錄服務所返回的資訊的援助，驅動程式能夠適當地從目錄服務管理資料封包的路由，且同時，驅動程式能夠藉由適當地轉換

資料封包而防止未授權的通訊。

在一範例實施例中，驅動程式供以散佈虛擬式閘道功能至一實體網路之中節點的多重虛擬的端點。初始，供應驅動程式以與在網路節點上初始化的端點合作。再者，實施目錄服務以維持虛擬網際網路協定（IP）位址及位置相依位址之間的一映射，並且根據在一網路之中連接端點的已知途徑實施一列舉轉換動作表。當將各個驅動程式從一中心位置處的驅動程式調離時，或當將各個驅動程式整體併入驅動程式之中而本端地存取目錄服務時，驅動程式之各者能夠與目錄服務通訊。

在操作中，鏈結至一特定驅動程式的一接收者端點可接收一或更多資料封包。驅動程式可讀取資料封包的一標頭，以確認一來源 IP 位址及一目標 IP 位址。驅動程式可進一步在一請求之中打包來源及目標IP位址用於路由資訊，且內部地或外部地將請求傳達至目錄服務。目錄服務可藉由檢閱來源及目標 IP 位址的映射，以一遞送路徑的適當位置相依位址，從驅動程式回應請求。此外，目錄服務可藉由檢閱遞送路徑的表，以適當的轉換動作而回應請求。轉換動作可包括以下一或多者：重新寫入資料封包的標頭以包括位置相依位址、在分別的外部資料封包之中包覆資料封包作為內部資料封包，其中該等外部資料封包以攜帶位置相依位址的標頭所組成、或以一通道協定配置資料封包（例如，對資料中心的每一個安全策略，或由一客戶所建立的一服務模式）。

在於驅動程式處接收路由資訊之後，驅動程式可立即對接收者端點驅動遞送路徑及轉換動作。反之，當從接收者端點傳送資料封包時，接收者端點實施遞送路徑且應用轉換動作。在其他實施例中，驅動程式可直接對資料封包實行適當的轉換動作，而非依賴一端點（例如，接收者端點）以實行此功能。

因此，在驅動程式及目錄服務協力作用以作成一根據情報的路由決策之後，鏈結至驅動程式的接收者端點可立即被提供網路途徑的一最佳選項，藉此降低網路擁塞；且接收者端點可立即被提供一適當的轉換動作，藉此強制在資料中心之外部隔離傳送。

【實施方式】

此處明確地說明本發明的實施例的標的以滿足法規的要求。然而，說明本身並非意圖限制此專利的範疇。反之，發明人已經考慮所主張的標的亦可以其他方式體現、包括不同的步驟或與此文件中所述的步驟相似的步驟之結合、與其他現有或未來的技術之連結。再者，儘管此處所使用的「步驟」及/或「方塊」一詞可表示方法所體現的不同元件，但此等詞彙不應被詮釋為暗示此處所揭示的各種步驟之中或之間任何特定的順序，除非且不計當個別步驟的順序被明確地說明。

本發明的實施例關於在分散式驅動程式處用於作成根

據情報的路由決策的方法、電腦系統、及電腦可讀取媒體，該等分散式驅動程式以一局部的方式提供虛擬的閘道功能。

在一個態樣中，本發明的實施例係關於具有電腦可執行指令安裝於其上的一或更多電腦可讀取媒體，當執行該等指令時，電腦可讀取媒體實行用於管理端點之間的資料封包的分散的一方法。在實施例中，該方法包括於一第一端點偵測一或更多資料封包的步驟。典型地，資料封包之各者包括一標頭，該標頭包含一來源位址及一目標位址。與第一端點相關聯的一驅動程式可發送一請求至一目錄服務。在一範例實施例中，請求攜帶來源位址及目標位址，或攜帶某些指標。在接收請求之後，目錄服務立即實行一查詢，以將來源位址及目標位址轉譯成一遞送路徑及一轉換動作。遞送路徑及轉換動作可在對驅動程式的一回應之中，而從目錄服務發送。然而，驅動程式及/或端點亦維持丟棄一或更多資料封包的能力，該一或更多資料封包無法匹配在目錄服務中關於起源、接收者及標靶端點的一規則。丟棄資料封包的此能力提供驅動程式強制網路之中的隔離的授權。

在收到回應之後，驅動程式可立即實行一路由決策，該路由決策係部分基於第一端點是否為資料封包的一起源端點、作用以遞送資料封包至一標靶端點上的一接收者端點、或標靶端點。當第一端點代表起源端點（由來源位址識別）時，路由決策可導致以下一或更多轉換動

作：（a）重新寫入資料封包的標頭，以包括位置相依位址；（b）在分別的外部資料封包之中包覆資料封包作為內部資料封包，其中外部資料封包之各者包括一標頭，該標頭攜帶位置相依位址；或（c）以一通道協定配置資料封包。當第一端點代表接收者端點時，路由決策可導致以下一或更多轉換動作：（a）遞送經包覆的資料封包或具有重新寫入的標頭之資料封包通過另一網路途徑；（b）重新導向經包覆的資料封包或具有重新寫入的標頭之資料封包通過一通道；或（c）從資料封包移除（removing）通道協定。當第一端點代表標靶端點（由目標位址識別）時，路由決策可導致以下一或更多轉換動作：（a）解開經包覆的資料封包；（b）重新儲存已重新寫入的資料封包的標頭；或（c）從資料封包移除通道協定以準備用於消耗（consumption）。

在另一態樣中，本發明的實施例係關於在端點之間用於支援及隔離通訊的一電腦系統。初始，電腦系統包括一目錄服務、一第一端點、一第二端點、及本端地供應至第一端點的一驅動程式。一般而言，目錄服務在虛擬網際網路協定（IP）位址及一實體網路的位置相依位址之間維持一映射。在操作中，第一端點可著手與標頭一起構成產生一或更多資料封包，該等標頭包括一來源IP位址及一目標IP位址。在此實例中，來源IP位址指向第一（起源）端點，且目標IP位址指向第二（標靶）端點。

在偵測到第一端點嘗試從一節點（例如，實體機器或虛擬機器）傳送資料封包至第二端點之後，驅動程式立即實行一路由決策。在一範例實施例中，由驅動程式對各個連接引發且執行一獨特的路由決策，各個連接係由第一端點作成。在實施例中，實行路由決策牽涉但非限於以下步驟：與目錄服務通訊，以部分基於來源 IP 位址及目標 IP 位址，來決定一遞送路徑及一轉換動作；決定第一端點及第二端點是否駐居於一通用資料中心之中；及決定若來源 IP 位址及目標 IP 位址被移除（removed），則第二端點是否無法轉譯資料封包的標頭。

當決定第一端點及第二端點係駐居於一通用資料中心之中時，驅動程式可以遞送路徑的分別的位置相依位址，來重新寫入來源 IP 位址及目標 IP 位址。在另一實施例中，驅動程式可在分別的外部資料封包之中包覆資料封包作為內部資料封包，其中外部資料封包之各者包括一標頭，該標頭揭露遞送路徑的位置相依位址。存在著引發包覆的轉換動作的數個情境。在一個情境中，當決定若來源位址及目標位址被移除，則第二端點無法轉譯資料封包的標頭時，包覆係被觸發。可能需要包覆的其他潛在情境包括（a）偵測網路轉譯的某些形式（NAT）存在於來源及目標 IP 位址之間，及/或（b）從來源及目標 IP 位址認知到第一及第二端點（例如，起源及標靶網路轉接器）橫跨多重虛擬網路，使得並不存在來自端點的位置相依位址及端點的虛擬 IP 位址的一對一映射。

當決定轉換動作支配一層保護以保衛提供於該第一端點及該第二端點之間的連接時，驅動器可基於所接收的轉換動作而轉換資料封包。在一個實例中，轉換動作牽涉將通道協定（例如，安全插座通道協定（SSTP）或網際網路協定安全（IPsec））應用至資料封包。

仍在另一態樣中，本發明的實施例關於回應於來自一分散式、虛擬網路閘道的一請求而用於識別一網路途徑及轉換動作的一電腦化方法。初始，本方法牽涉提供一目錄服務，該目錄服務在虛擬IP位址及位置相依位址之間維持一映射。目錄服務亦可維持一表，該表認知一適當的轉換動作。在一個實例中，表係根據通訊策略而設計，該等通訊策略確保在一網路之中連接端點的途徑上的資料封包流量。在另一實例中，表係基於一服務模式（例如，服務等級協議（SLA）），該服務模式被建立用於一資料中心的一客戶，該資料中心裝載客戶的服務應用程式。

本方法可進一步涉及從一虛擬網路閘道接收一請求的步驟與一接收者端點通訊。典型地，該請求包括一來源IP位址及一目標IP位址的指標，該來源IP位址及該目標IP位址透過一或更多資料封包攜帶而藉由接收者端點接受。在收到請求之後，目錄服務可立即實行以下至少一個查詢程序：以來源IP位址及目標IP位址檢閱映射，以識別透過一實體網路構成的資料封包的一遞送路徑的相對應的位置相依位址；或以遞送路徑檢閱表，以識別

一相對應的轉換動作。如以下更加完整的討論，轉換動作可牽涉但非限於以下一或更多者：重新寫入資料封包的標頭，以包括位置相依位址；在分別的外部資料封包之中包覆資料封包作為內部資料封包，其中該等外部資料封包之各者包括一標頭，該標頭攜帶位置相依位址；或以一通道協定配置資料封包。最終，目錄服務可返回一回應，該回應對虛擬網路閘道傳達經識別的遞送路徑及經識別的轉換動作的指標。

在簡要地說明本發明的實施例的一概觀之後，以下說明適以實施本發明的實施例的一範例操作環境。

大致參考圖式，且具體而言初始參考第 1 圖，顯示且大致指定用於實施本發明的實施例的一範例操作環境為計算設備 100。計算設備 100 係僅為一適合的計算環境的範例，且並非意圖對本發明的實施例的使用或功能的範疇建議任何限制。計算環境 100 亦不應被詮釋為對關於圖示的元件的任何一者或結合具有任何依附或要求。

本發明的實施例可以電腦編碼或機器可使用的指令的一般情境說明，電腦編碼或機器可使用的指令包括諸如程式元件的電腦可執行指令，而程式元件由一電腦或其他機器執行，例如一個人資料助理或其他手持設備。一般而言，程式元件包括常式、程式、物件、元件、資料結構、及論及實行特定任務或實施特定抽象資料類型的編碼的諸如此類者。本發明的實施例可實施於各種系統配置之中，包括手持設備、客戶電子設備、一般功能的

電腦、專門計算設備等等。本發明的實施例亦可實施於分散式計算環境中，其中任務係藉由透過一通訊網路鏈結的遠端處理設備實行。

繼續參照第 1 圖，計算設備 100 包括一匯流排 110，該匯流排 110 直接或間接與以下設備耦接；記憶體 112、一或更多處理器 114、一或更多展示元件 116、輸入/輸出（I/O）埠 118、I/O 元件 120、及一圖示性電源供應器 122。匯流排 110 代表一或更多匯流排（例如，一位址匯流排、資料匯流排、或此等之結合）。儘管為了清楚起見以線條顯示第 1 圖的各種方塊，實際上，各種元件的界線並非如此清楚，且比喻來說，線條應更明確地為灰色及模糊的。舉例而言，吾人可考慮諸如一顯示設備的一展示元件為一 I/O 元件。而且，處理器具有記憶體。此處的本發明認知到此為本領域的天性且重申第 1 圖僅為圖示性的一範例計算設備，該範例計算設備可與本發明的一或更多實施例連接使用。此等類別之間所述的「工作站」、「伺服器」、「膝上型電腦」、「手持設備」等等並無區別，以上所有均考慮在第 1 圖的範疇之中，且稱為「電腦」或「計算設備」。

計算設備 100 典型地包括各種電腦可讀取媒體。藉由範例的方式且非限制，電腦可讀取媒體可包含隨機存取記憶體（RAM）；唯讀記憶體（ROM）；電子可抹除可程式唯讀記憶體（EEPROM）；快閃記憶體或其他記憶技術；CDROM，數位光碟（DVDs）或其他光學或影像媒

體；磁性卡匣、磁帶、磁碟儲存或其他磁性儲存設備，或可用以編碼所欲資訊且可由計算設備 100 存取的其他媒體。

記憶體 112 包括電腦儲存媒體，具有可揮發及/或不可揮發記憶體的形式。記憶體可為可移除、不可移除、或此等之結合。範例硬體設備包括固態記憶體、硬碟、光碟驅動等等。計算設備 100 包括一或更多處理器，該一或更多處理器從諸如記憶體 112 或 I/O 元件 120 的各種實體讀取資料。展示元件 116 呈現資料指令至一使用者或其他設備。範例展示元件包括一顯示設備、喇叭、列印元件、振動元件等等。I/O 埠 118 允許計算設備 100 邏輯性地耦接至其他設備，包括耦接至 I/O 元件 120，其中某些可為內建的。圖示性元件包括一麥克風、操縱桿、遊戲板、天線接收器、掃描機、印表機、無線設備等等。

參照第 1 及 2 圖，一節點 211 及一節點 212 可由第 1 圖的範例計算設備 100 所實施。再者，端點 201、202 及 230 可存取第 1 圖的部分記憶體，且運行於第 1 圖的部分處理器上。類似地，在 VM 開關 222 的虛擬交換網路堆疊之中（在虛擬式機器 270 及 275 上支援端點 201 及 202）及/或在用於實體機器的本端機器網路堆疊之中（支援端點 230），安裝了本端閘道功能的驅動程式 223 及 233，可存取第 1 圖的部分記憶體 112，且運行於第 1 圖的部分處理器上。

現在轉向第 2 圖，根據本發明的一實施例圖示一方塊

圖，顯示一範例雲端計算平台 200，該範例雲端計算平台 200 配置成藉由利用路由資訊而於驅動程式 223 及 233 實行路由策略，該路由資訊係從使用各種形式的轉換的一目錄服務 220 蒐集到。在實施例中，儘管圖示為可耦接至一個雲端計算平台 200 而操作，但目錄服務 220 可存在於一特定雲端的範疇的外部（即，目錄服務 220 可代表共享於公共及私人雲端上的一雲端服務）。與各種雲端一起操作的能力允許目錄服務啟用橫跨多重雲端的網路。

應瞭解且體會第 2 圖中所顯示的雲端計算平台 200 僅為一個合適的計算系統環境的一範例，且並非意圖對本發明的實施例的使用或功能的範疇建議任何限制。舉例而言，雲端計算平台 200 可為一公共雲端、一私人雲端、或一專用雲端。雲端計算平台 200 之任一者不應詮釋為關於此處所圖示的元件的任何單一元件或結合而具有任何依賴或要求。再者，儘管為了清楚起見以線條顯示第 2 圖的各種方塊，實際上，各種元件的界線並非如此清楚，且比喻來說，線條應更明確地為灰色及模糊的。此外，可利用任何數量的實體機器、虛擬機器、資料中心、端點、或以上之結合，以達成在本發明的實施例的範疇之中的所欲功能。

雲端計算平台 200 可包括一或更多資料中心（例如，資料中心 225），該資料中心包含節點（例如，節點 211 及 212）用於裝載服務應用程式及其他軟體。對於本發

明的每一個實施例，節點 211 及/或 212 可代表包含任何形式的計算設備的實體機器，舉例而言，一個人電腦、一桌上型電腦、一膝上型電腦、一行動設備、一消費電子設備、伺服器、第 1 圖的計算設備 100、及諸如此類者。在另一實施例中，節點 211 及/或 212 可代表虛擬機器或可對虛擬機器的操作提供基礎的支援，例如虛擬機器 270 及 275。在操作中，虛擬機器 270 及 275 支援資料中心 225 的住戶的操作。如此處所使用，「住戶」一詞一般代表由雲端計算平台 200 的一客戶所擁有的服務應用程式的元件程式（例如，各種角色的實例）。

一般而言，虛擬機器 270 及 275 基於置於服務應用程式上的要求（例如，處理負載的量）而分配至服務應用程式的端點 201 及 202。如此處所使用，「虛擬機器」一詞並非意味著限制，且可代表任何軟體、應用程式、操作系統、或由一處理單元執行的程式，以構成端點 201 及 202 的基礎。在另一實施例中，虛擬機器代表由一節點劃分出，用於支援資料中心 225 的住戶的處理能力及記憶資源。以此方式，節點 211 裝載且支援虛擬機器 270 及 275 的操作，同時裝載劃分出而用於支援資料中心 225 的其他住戶的其他虛擬機器，其中住戶包括由不同客戶所擁有的其他服務應用程式的端點。因此，虛擬機器 270 及 275 可包括處理能力、儲存位置、及在資料中心 225 之中的其他資產，適以支援節點 201 及 202。

在操作中，虛擬機器 270 及 275 在資料中心 225 的資

源（例如，節點 211）之中動態地被分配，且端點（例如，端點 201 及 202）動態地被放置於經分配的虛擬機器 270 及 275 上，以滿足當前處理負載。在一個實例中，一結構控制器（fabric controller）232 係負責自動地分配虛擬機器 270 及 275，且用於放置端點 201 及 202 於資料中心 225 之中。藉由範例的方式，結構控制器 232 可依賴一服務模式（例如，由擁有服務應用程式的一客戶指派），以提供如何且何時分配虛擬機器 270 及 275 及如何且何時放置端點 201 及 202 在虛擬機器上的方針。

在一個實例中，節點 211 及 212 裝載支援端點 201、202、及 230 的操作。「端點」一詞並非意味著限制，但可涵蓋一服務應用程式的一程式元件（例如，資料中心 225 的住戶），或運行於一節點、實體機器、或 VM 上的網路轉接器。在一個態樣中，端點 201、202 及 230 在雲端計算平台 200 的情境之中操作，且因此，透過在端點之間作成的動態連接而內部地通訊。在另一態樣中，端點 201、202、及 230 透過一實體網路拓撲而外部地通訊至一遠端網路的資源（例如，第 3 圖的企業私人網路 325 的資源 375）。外部連接可進一步牽涉透過一網路（未顯示）而互相連接至分散於資料中心 225 的實體資源上的端點。在一個實施例中，如端點 230 所圖示，網路直接互相連接此等資源，使得一起源端點（用於產生資料封包）可認知一接收者端點的一位置（用於遞送資料封包至一標靶端點）或標靶端點的一位置（用於消耗資料封

包），以便於此等端點之間建立一通訊。在另一實施例中，網路間接地互相連接資源，使得定址至端點 201 或 202（此等端點係分別裝載於虛擬機器 270 及 275 上）的資料的一封包，可在邏輯上分散至駐居於相同節點上的一適當端點之前，透過網路路由且傳遞至 VM 開關 222。此外，網路可在通道上（例如，安全通道）建立一通訊，藉此實施一額外的保護層，或利用標準的保衛量測以連接於服務應用程式的端點之間。藉由範例的方式，通道可包括但非限於一或更多區域網路（LANs）及/或廣域網路（WANs）。此等網路化環境係通常可見於辦公室、企業範圍的電腦網路、企業內部網路、及網際網路。因此，此處不進一步說明網路。

雲端計算平台 200 包括資料中心 225，配置成裝載且支援端點 201、202、及 230 的操作，該等端點分配至一特定的服務應用程式。此處所使用的「服務應用程式」一詞廣泛地代表任何軟體或部分的軟體，該軟體運行於資料中心 225 的頂端或存取資料中心 225 之中的儲存位置、在雲端計算平台 200 之中的另一資料中心、位於一客戶的前提之下而在一企業私人網路中的資源（例如，第 3 圖的企業私人網路 325 的資源 375）、及/或在一第三方網路中的資源（例如，第 3 圖的第三方網路 335 的資源 325）。如上所討論，端點 201、202、及 230 可代表部分的軟體、元件程式、或參與服務應用程式之中的角色的實例。在另一實施例中，端點 201、202、及 230 可代

表可存取至服務應用程式的經儲存的資料。應瞭解且體會第2圖中所顯示的端點201、202、及230僅為支援服務應用程式的合適部分的一範例，且並非意圖對本發明的實施例的使用或功能的範疇建議任何限制。

儘管說明一個服務應用程式在一單一資料中心225中分散於兩個節點211及212上，但應瞭解且體會在各種資料中心之中或其他合適的設備而駐居於任何數量的節點的任何數量的服務應用程式可被使用，且本發明的實施例並非限於此處所述的此等節點、服務應用程式、及資料中心。再者，任何數量的端點可舉例於節點之中及/或分配至服務應用程式，且圖示於第2圖及第3圖中的端點係僅為了說明的目的而顯示。

在一個實例中，資料中心225的構造允許一管理系統（例如，結構控制器232）或雲端計算平台200的管理員舉例新的端點或重新分配現有的端點，以支援一服務應用程式。結構控制器232亦可建立且記下網路途徑及通道，以連接端點201、202、及230。再者，結構控制器232可週期性地對資料中心225的一拓樸進行快照。此等快照可透過資料中心網路及端點的位址，而記錄目前所建立的網路途徑及通道。此等快照可接替至目錄服務220而儲存於目錄服務220之中。在實施例中，目錄服務220可配置成根據一實體網路的位置相依位址而儲存虛擬IP位址。再者，目錄服務220可配置成儲存轉換動作，該等轉換動作與資料中心網路的分別的網路途徑

及通道相關聯。以此方式，服務應用程式的服務模式的保衛策略係藉由在資料封包上的目錄服務 220 而強制實施，其中資料封包在服務應用程式的住戶之間傳送。

如上所討論，當前發明的實施例介紹一架構，該架構藉由利用實體層（實線）之中的網路途徑及通道，允許一虛擬層（虛線）上端點之間的通訊。在實體層之中，端點可透過鏈結的一網路而達到。一般而言，較佳地為基於互動端點的一位置而明智地選擇網路的適當鏈結，以便避免將所有通訊通過一中央路由機制，因此而避免網路壅塞。為了達成實體層鏈結的明智地選擇以及資料封包橫越所選擇的鏈結的適當轉換，在實施例中，藉由兩個不同的技術支援架構，該等兩個技術協力操作：驅動程式 223 及 233，及目錄服務 220。

驅動程式 223 及 233 係與一或更多端點相關聯，且係安裝於資料中心 225 之中，作為驅動程式幫助的終點的一類型的一功能。若端點（例如，端點 230）係裝載於一實體機器（例如，節點 212）上，則驅動程式 233 係在主機開關（未顯示）之中實施，該主機開關直接放置資料封包至端點之間的流量。在此實施例中，當偵測到一或更多資料封包到達或離開端點 230 之後，驅動程式 233 可立即藉由發送一請求 273 至目錄服務 220 而徵詢路由資訊，該請求 273 攜帶併入資料封包的一標頭之中的來源 IP 位址及目標 IP 位址。在接收路由資訊的請求 273 之後，目錄服務 220 可以一回應 274 來回覆，該回

應 274 攜帶用於資料封包的一遞送路徑及適合用於遞送路徑的一轉換動作。

若端點（例如，端點 201 及 202）係裝載於一虛擬機器上（例如，虛擬機器 270 及 275），則驅動程式（例如，驅動程式 223）係實施於網路堆疊之中、隱藏所有存在的轉接器、且呈現網路的一單一虛擬式的介面。在此實施例中，驅動程式 223 可代表一獨立 VM 開關，或可併入一存在的 VM 開關（例如，VM 開關 222）之中。在實施例中，提供 VM 開關以在資料中心 225 的內部及外部的端點之間給予隔離的連接，如下參照第 3 圖更完整地討論。如此處所使用，「虛擬機器開關」或「VM 開關」一詞並非意味著限制，但可涵蓋駐居於一資料中心、企業私人網路、第三方網路等等之中任何基於軟體的元件，且負責安全地路由資料封包橫跨一服務應用程式的端點之間的網路。藉由範例的方式，VM 開關可為任何網路週邊設備（例如，機架頂端開關、在節點中的實體網路介面、在 VMs 中的虛擬介面卡、或在非虛擬式主機中的一網路堆疊），該設備揭露用於網路管理的某些應用程式介面（API）。在其他範例中，藉由 VM 開關所執行的所有或部分的操作（例如，與目錄服務 220 通訊、封包的包覆、解除、修改、及其他動作）可藉由一路由模組而實行。如此，VM 開關可安裝一或更多路由模組、網路週邊設備、實體開關、路由設備、及諸如此類者。

與驅動程式 233 類似，驅動程式 223 可在偵測到一或

更多資料封包到達或離開端點 201 或 202 之任一者之後，驅動程式 233 可藉由發送一請求 271 至目錄服務 220 而徵詢路由資訊，該請求 271 攜帶在資料封包的一標頭之中的來源 IP 位址及目標 IP 位址。在接收到用於路由資訊的請求 271 之後，目錄服務 220 可立即以一回應 272 來回覆，該回應 272 攜帶用於資料封包的一遞送路徑及適合用於遞送路徑的一轉換動作。

現參照第 2 圖及第 3 圖，現在將討論介於驅動程式 223 及 233，及目錄服務 220 之間的額外的互動。如上所討論，驅動程式可分散於資料中心 225 的多重節點上，且在資料中心 225 外部的資源上。驅動程式 223 及 233 可以一或更多因素的一函數，而動態地被舉例於資料中心 225 之中的一節點上或從資料中心 225 之中的一節點撤除，該一或更多因素例如 IP 流量的一比率、由資料中心 225 的住路消耗的一計算負載、及一節點是否被連上線或離線。在一個實施例中，結構控制器 232 係負責舉例或撤除 VM 開關。

在操作中，驅動程式 223 及 233 代表對分別節點的一虛擬網路轉接器，且供以對一服務應用程式或子網路之中的一特定端點作為一閘道。在此實施例中，提供一拓撲，其中當傳送資料封包時閘道以關於何處、如何、及何者實體層鏈結應於使用而作成路由決策。藉由分散驅動程式橫跨內部及外部節點，此閘道功能如今被虛擬化且散佈於網路上。

在一範例實施例中，路由決策幫助決定一遞送路徑，該遞送路徑無須總是要求透過中央伺服器發送資料封包。再者，路由決策可專門為對每一連接/每一機器的基礎。在一個實例中，一路由決策可決定將一高度保護的轉換動作應用至利用安全通道鏈結端點橫跨遠端資料中心的資料封包。在另一實例中，一路由決策可決定利用更輕量的轉換動作，例如當端點同時存在於一通用安全網路上時，包覆或重新寫入資料封包的標頭。在此實例中，端點可駐居於相同的子網路之中，且可透過介於一資料中心網路的伺服器之間的一直接路徑而彼此可見。因此，路由決策可權衡相同子網路之中的端點的能力，以使用路由在不具有共同壅塞點的實體層鏈結上，以便最佳化端點的互相連接。此等及其他路由決策參照第 4 圖而更完整地說明。

在實施例中，路由/重新寫入元件（RCs）224 及 234 係分別提供於驅動器 223 及 233 之中。在操作中，RCs 224 及 234 能夠接受起源自一節點或端點的一操作系統的各個資料封包，或接受透過一安全通道或網路途徑所傳送的各個資料封包，且基於資料封包（例如，攜帶於標頭之中的資訊）而決定任何的修正遞送路徑及轉換動作。在一個實例中，RCs 224 及 234 檢驗所接受的各個資料封包的來源 IP 位址及/或目標 IP 位址，且查詢路由資訊的目錄服務 220（例如，透過請求 271 及 273）。目錄服務 220 可分別以回應 272 及 274 回答請求 271 及 273，

該等回應包括各種類型的路由資訊。因此，RCs 224 及234 供應管理多重通道/重新寫入協定的能力，該能力回應路由資訊且對資料封包支援不同的遞送處理。

一般而言，目錄服務 220 保留網路 315 的知識以及網路 315 之中的網路途徑及安全通道 350。藉由範例的方式，此知識包括關於端點的資訊、端點駐居於何者網路之中、在此等網路之中建立何者網路途徑、何者轉換動作係適於橫跨網路途徑的特定遞送路徑、及如何實行轉換動作。在操作中，RCs 224 及 234 的事件徵詢路由資訊，目錄服務 220 可應用此網路知識以通知一第一端點如何搜尋在網路 315 之中的一第二端點。說明至此，目錄服務 220 在虛擬 IP 位址及位置相依位址之間維持一映射 310。在一範例實施例中，映射在互相連接的端點之間維持一或更多邏輯關聯，且強制與端點相關聯的存取控制，以便達成網路可達性。在一個實例中，邏輯關聯屬於介於一子網路的成員的端點之間的一關聯。

目錄服務 220 亦可維持一表 320，該表 320 認知一適當的轉換動作。在一個實例中，表 320 係經設計以強制一通訊策略，該通訊策略典型地藉由一客戶透過一服務等級協議（SLA）而設定在適當位置。在另一實例中，通訊策略特定地經設計用於一服務應用程式及/或子網路，且可包括准許的一清單，該清單確保何者系統處理係被同意存取子網路的成員端點，及端點是否可直接被連接而無須牽涉一中央路由設備。仍在另一實例中，通

訊策略可表達應對特定端點確保何者保衛等級。在另一實例中，通訊策略供以作為保衛模式，該保衛模式在從驅動程式接收請求之後，立即對可應用的入口掃描映射310，且決定起源資料傳送是否基於可應用入口之中的資訊而被授權。仍在另一實例中，通訊策略可代表應用至一埠號或一網路轉接器的規則，該等規則可從資料中心225的一節點取得，以便確認埠號或網路轉接器是否被准許實行某些操作。

在目錄服務220從一驅動器接收請求之後，目錄服務220可立即實行以下查詢程序：以來源IP位址及目標IP位址檢閱映射310，以識別相對應的位置相依位址，該位置相依位址透過一實體網路380構成資料封包的一遞送路徑；或以遞送路徑檢閱表320，以識別一相對應的轉換動作。換句話說，目錄服務接收一資料組（來源IP位址、目標IP位址），且透過針對映射310及表320的轉譯，而返回資料組（遞送路徑、轉換動作）。返回的資料組在請求驅動程式之中支援路由決策作成處理。

如以下更完整地討論，轉換動作可牽涉但非限於以下一或更多者：重新寫入資料封包的包頭，以包括位置相依位址；在分別的外部資料封包之中包覆資料封包作為內部資料封包，其中各個外部資料封包包括一標頭，該標頭攜帶位置相依位址；或以一通道協定配置資料封包。最終，目錄服務220可返回一回應，該回應傳達至經識別的遞送路徑及經識別的轉換動作的請求驅動程式

（虛擬網路閘道）指標。

儘管第 2 圖及第 3 圖中描繪為一單一中央伺服器，該伺服器推送資訊至一請求驅動程式，但目錄服務 220 的功能可透過連結且存檔至一組機器的本端檔案而實施。或者，目錄服務 220 的功能可於請求驅動程式之前的一段時間先行快取，若此舉先前被推送出，則刪除發送一外部請求的步驟。

現參照第 3 圖，根據本發明的一實施例，顯示一分散式計算環境 300 的一範例架構的一概要圖，該分散式計算環境 300 將虛擬網路位址解析為實體網路途徑及轉換動作。初始，分散式計算環境 300 包括一實體網路 380，如參考第 2 圖所討論，該實體網路包括一企業私人網路 325、一第三方網路 335、及一雲端計算平台 200。如此處所使用，「實體網路」一詞並非意味著限制，但可涵蓋有形的機制及裝備（例如，光纖線、電路箱、開關、天線、IP 路由器、及諸如此類者），以及無形的通訊及成載波，該等通訊及成載波於地理上遠端的位置促進端點之間的通訊。藉由範例的方式，實體網路 380 可包括在網際網路之中所利用的任何有線或無線技術，或可取得用於提昇不同網路之間的通訊的技術。

一般而言，企業私人網路 325 包括資源，例如由雲端計算平台 200 的一客戶所管理的資源 375。通常，此等資源裝載且支援由客戶所擁有的服務應用程式的元件的操作。端點 B 385 代表服務應用程式的一或更多元件。

在實施例中，諸如第 2 圖的虛擬機器 270 的資源被分配於第 2 圖的資料中心 225 之中，以裝載且支援服務應用程式的遠端地分散的元件的操作。端點 A 211 及 C 212 代表服務應用程式的兩個此等遠端地分散的元件。在操作中，端點 A 211、B 385、及 C 212 彼此協力工作，以確保服務應用程式適當地運行。在一個實例中，協力工作牽涉在端點 A 211、B 385、及 C 212 之間通過實體網路 380 的網路 315 傳送資料封包 316。

亦提供第三方網路 335 在實體網路 380 之中。在實施例中，第三方網路 335 可代表並非第 3 圖的企業私人網路 325 或雲端計算平台 200 的任何其他網路。藉由範例的方式，第三方網路 335 可包括持有由服務應用程式所使用的資訊的一資料儲存，或提供軟體以支援服務應用程式的一或更多操作的一供應商。在實施例中，第三方網路 335 代表資源的一網路，包括具有一端點 D 345 安裝於其上的資源 355，該資源 355 可取得第 6 圖的雲端計算平台 200。

典型地，資源 355 及 375，及資料中心 225 包括或鏈結至一計算單元的某些形式（例如，中央處理單元、微處理器等等），以支援運行於計算單元之上的端點及/或元件的操作。如此處所使用，「計算單元」一詞一般代表具有處理能力及儲存記憶體的一專門計算設備，該專門計算設備支援一或更多操作系統或其他下方的軟體。在一個實例中，計算單元以有形的硬體元件或機器配置，

該等硬體元件或機器係為整體的或可操作地耦接至資源355及375，以及資料中心225，以使得各個設備能夠實行各種處理及操作。在另一實例中，計算單元可涵蓋耦接至電腦可讀取媒體的一處理器（未顯示），該電腦可讀取媒體由各個資源355及375以及資料中心225所容納。一般而言，電腦可讀取媒體至少暫時地儲存複數個電腦軟體組件（例如，端點A211、B385、C212、及D345），該等電腦軟體組件可由處理器執行。如此處所使用，「處理器」一詞並非意味著限制且可涵蓋計算單元的任何元件，該等元件以一計算能力作用。在此能力中，處理器可配置為處理指令的一有形物件。在一範例實施例中，處理可牽涉擷取、解碼/詮釋、執行、及回寫指令。

虛擬網路覆蓋330（「覆蓋330」）係典型地被建立用於一單一服務應用程式，例如包括端點A 211、B 385、C 212、及D345的服務應用程式，以便提昇且保衛服務應用程式的端點之間的通訊。一般而言，覆蓋330代表一層虛擬IP位址，而非實體IP位址，其中虛擬IP位址虛擬地代表服務應用程式的端點且連接虛擬表徵。在其他實施例中，覆蓋330係建立於實體網路380的頂部上的一虛擬網路，該實體網路380包括分配至控制服務應用程式的客戶的資源。在操作中，覆蓋330維持互相連接的端點A211、B385、C212、及D345的一或更多邏輯性相關聯，且可強制與端點A211、B385、C212、及D345相關聯的存取控制/安全，以便達成實體網路的可達

性（例如，使用一實體運輸）。

現參照第 3 圖及第 4 圖，將說明各種可能的路由決策。具體而言，第 4 圖顯示一範例決策樹 400 的一概要圖，根據本發明的一實施例，用於將從目錄服務 220 分散的路由資訊應用至一路由決策。如上所述，一驅動程式可部分基於鏈結至驅動程式的一對象端點是否代表資料封包的一起源端點、作用以遞送資料封包至一標靶端點上的一接收者端點、或標靶端點，而實行一路由決策。在一第一實例中，當對象端點代表起源端點（例如，端點 C 212）時，與起源端點相關聯的驅動程式可偵測起源端點，如方塊 401 所描繪，嘗試傳送從起源端點產生的一或更多資料封包。如方塊 402 所描繪，驅動程式可接著徵詢目錄服務 220 以藉由發送一請求實行一查找程序，該請求包含指向對象端點的一來源 IP 位址及一目標 IP 位址的指標。

如方塊 403 所描繪，路由決策係部分基於從目錄服務 220 傳送至驅動程式的路由資訊而執行。路由決策可導致但非限於以下一或更多轉換動作：重新寫入資料封包的標頭，以包括位置相依位址（見方塊 404）；以一通道協定配置資料封包且透過一安全通道重新導向資料封包（見方塊 405）；或在分別的外部資料封包之中包覆資料封包作為內部資料封包（見方塊 406），其中外部資料封包之各者包括攜帶位置相依位址的一標頭。

在一範例實施例中，當驅動程式決定起源端點及標靶

端點兩者均駐居於一通用資料中心或子網路之中之後，路由可導致轉換動作，該轉換動作針對分別的位置相依位址而重新寫入來源 IP 位址及目標 IP 位址。然而，當驅動程式決定若來源 IP 位址及目標 IP 位址被移除（removed）（例如，接收者/標靶端點係在不同於起源端點所駐居的資料中心或子網路中的一資料中心或子網路之中）則接收者端點或標靶端點無法轉譯資料封包的標頭時，路由決策可導致在分別的外部資料封包之中包覆資料封包作為內部資料封包，以便保留來源及目標 IP 位址在資料封包的一酬載之中。在以上即刻所述的此實施例中，驅動程式亦可認知介於端點之間的一網路途徑係實質上足夠地被保護以滿足一確保服務模式的安全策略。反之，當驅動程式認知到連接一或更多端點的網路途徑缺乏由確保服務模式所支配的保護或保衛連接的一級別時，路由決策可導致轉換動作，該轉換動作轉換資料封包以包括安全通道協定，藉此嘗試避免被惡意動作攔截資料封包。

如方塊 407 所描繪，在執行路由決策的之後，起源端點可立即著手傳送經處理的資料封包至一接收者端點（例如，端點 A 211 或 D 345）或一標靶端點（例如，端點 B 385）。儘管此處所述的接收者端點係為一單一網路躍點，但應體會且瞭解網路中可存在不只一個的中間躍點，該等躍點允許接收者端點能夠遞送至另外的一或更多接收者端點。在一第二實例中，當對象端點代表接收

者端點時，如方塊 408 所描繪，與接收者端點相關聯的驅動程式可偵測經處理的資料封包到達此端點。如方塊 409 所描繪，驅動程式可接著徵詢目錄服務 220，以藉由發送包含來源 IP 位址及目標 IP 位址的指標的一請求，來實行一查詢程序。

如方塊 410 所描繪，路由決策係部分基於從目錄服務 220 傳遞至驅動程式的路由資訊而執行。路由決策可導致以下一或更多轉換動作：重新導向經包覆的資料封包或具有重新寫入的標頭的資料封包通過一通道 550（見方塊 411）（例如，見端點 D 345）；從資料封包移除通道協定（見方塊 412）；或遞送經包覆的資料封包或具有重新寫入的標頭的資料封包通過另一網路途徑（見方塊 413）（例如，見端點 A 211）。再一次地，是否引發遞送資料封包通過一網路途徑的轉換動作，或引發重新導向資料封包通過一通道的轉換動作的路由決策，係牽涉到識別端點係分別地鏈結在安全連接上或鏈結在橫跨未保護的網路（例如，網際網路）的連接上。

在執行路由決策之後，如方塊 414 所描繪，接收者端點可立即著手傳送經處理的資料封包至標靶端點（例如，端點 B 385）。在一第三實例中，當對象端點代表標靶端點時，如方塊 415 所描繪，與標靶端點相關聯的驅動程式可偵測到經處理的資料封包的到達。如方塊 416 所描繪，驅動程式可接著徵詢目錄服務 220 以藉由發送一請求而實行一查詢程序，該請求包含來源 IP 位址及指

向標靶端點的目標 IP 位址的指標。

如方塊 417 所描繪，路由決策係部分基於路由資訊而執行，該路由資訊係從目錄服務 220 傳遞至驅動程式。當對象端點代表標靶端點時，路由決策可導致一或更多以下的轉換動作：重新儲存已重新寫入的資料封包的標頭（見方塊 418）；從資料封包移除（removing）通道協定以準備用於消耗（consumption）（見方塊 419）；或解開經包覆的資料封包（見方塊 420）。

現在轉向第 5 圖，圖示一流程圖，根據本發明的一實施例，顯示一方法 500 用於回應於來自驅動程式的一請求，而識別適當的實體網路途徑及轉換動作。如可從以上的討論所搜集到，方法 500 的步驟係撰寫自第 2 圖及第 3 圖的目錄服務 220 的觀點。初始，如方塊 510 所描繪，方法 500 牽涉提供目錄服務，該目錄服務維持虛擬 IP 位址及位置相依位址之間的一映射。目錄服務亦可維持一表，該表認知一適當的轉換動作。在一個實例中，表係根據通訊策略而設計，該等通訊策略確保在一網路之中連接端點的途徑上的資料封包流量。在另一實例中，表係基於一服務模式（例如，服務等級協議（SLA）），該服務模式被建立用於一資料中心的一客戶，該資料中心裝載客戶的服務應用程式。

如方塊 520 所描繪，方法 500 可進一步牽涉從一虛擬網路閘道或驅動程式接收一請求的步驟，該虛擬網路閘道或驅動程式係與一對象端點相關聯，或被建立用於與

一對相端點本端通訊。典型地，請求包括一來源 IP 位址及一目標 IP 位址的指標，該來源 IP 位址及該目標 IP 位址藉由接收者端點所接受的一或更多資料封包的一標頭攜帶。在接收請求之後，目錄服務可立即實行以下的查詢程序（見方塊 530）：以來源 IP 位址及目標 IP 位址檢閱映射，以識別相對應的位置相依位址，該位置相依位址透過一實體網路以資料封包的一遞送路徑構成（見方塊 540）；及/或以遞送路徑檢閱表，以識別一相對應的轉換動作（見方塊 550）。轉換動作可牽涉但非限於以下一或多者：重新寫入資料封包的標頭以包括位置相依位址；重新儲存此重新寫入；在分別的外部資料封包之中包覆資料封包作為內部資料封包，該等外部封包之各者包括一標頭，該標頭攜帶位置相依位址；解開所包覆的資料封包；以一通道協定配置資料封包；或移除通道協定。如於方塊 560 所描繪，目錄服務可返回一回應，該回應對虛擬網路閘道傳達經識別的遞送路徑及經識別的轉換動作的指標。

已說明關於特定實施例的本發明的實施例，該等特定實施例意圖以所有的態樣圖示而非限制。替代實施例將對技藝人士而言成為顯而易見的，其中替代實施例附屬於本發明的實施例而不悖離本發明的實施例的範疇。

從以上所述，將可見本發明係良好適以達成以上所述的所有終端及態樣的一者，並與系統及方法的顯見及隱含的其他優點一起。應瞭解可利用某些特徵及子結合，

且無須參考其他特徵及子結合而可被利用。此發明被考慮且在申請專利範圍的範疇之中。

【圖式簡單說明】

以下參考隨附的圖式說明本發明的實施例，其中：

第 1 圖係一範例計算環境的一方塊圖，適以用於實施本發明的實施例；

第 2 圖係一方塊圖，圖式一範例雲端計算平台，適以用於實施本發明的實施例，該等實施例配置成在一資料中心之中供應且促進驅動程式的操作；

第 3 圖係一範例架構的一概要圖，該範例架構根據本發明的一實施例，將虛擬網路位址解析為實體網路途徑及轉換動作；

第 4 圖係一範例決策樹的一概要圖，該範例決策樹根據本發明的一實施例，用於將從一目錄服務分散的路由資訊應用至一路由決策；及

第 5 圖係一流程圖，根據本發明的一實施例，顯示一種回應於來自驅動程式的一請求而用於識別適當的實體網路途徑及轉換動作的方法。

【主要元件符號說明】

100 計算設備	112 記憶體
110 匯流排	114 處理器

116 展示元件
118 I/O 埠
120 I/O 元件
122 電源供應器
200 範例雲端計算平台
201 端點
202 端點
211 節點
212 節點
220 目錄服務
222 VM 開關
223 驅動程式
224 RC
225 資料中心
230 端點
232 結構控制器
233 驅動程式
234 RC
270 虛擬式機器
271 請求
272 回應
273 請求
274 回應
275 虛擬式機器
300 分散式計算環境
310 映射
315 網路
316 資料封包
320 表
325 企業私人網路
330 虛擬網路覆蓋
335 第三方網路
345 端點
350 安全通道
355 資源
375 資源
380 實體網路
385 端點

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫；惟已有申請案號者請填寫）

※ 申請案號：100117829

※ 申請日期：2011 年 5 月 20 日　　※IPC 分類 H04L 12/66 (2006.01)
H04L 29/06 (2006.01)

一、發明名稱：（中文/英文）

分散式虛擬網路閘道

DISTRIBUTED VIRTUAL NETWORK GATEWAYS

二、中文發明摘要：

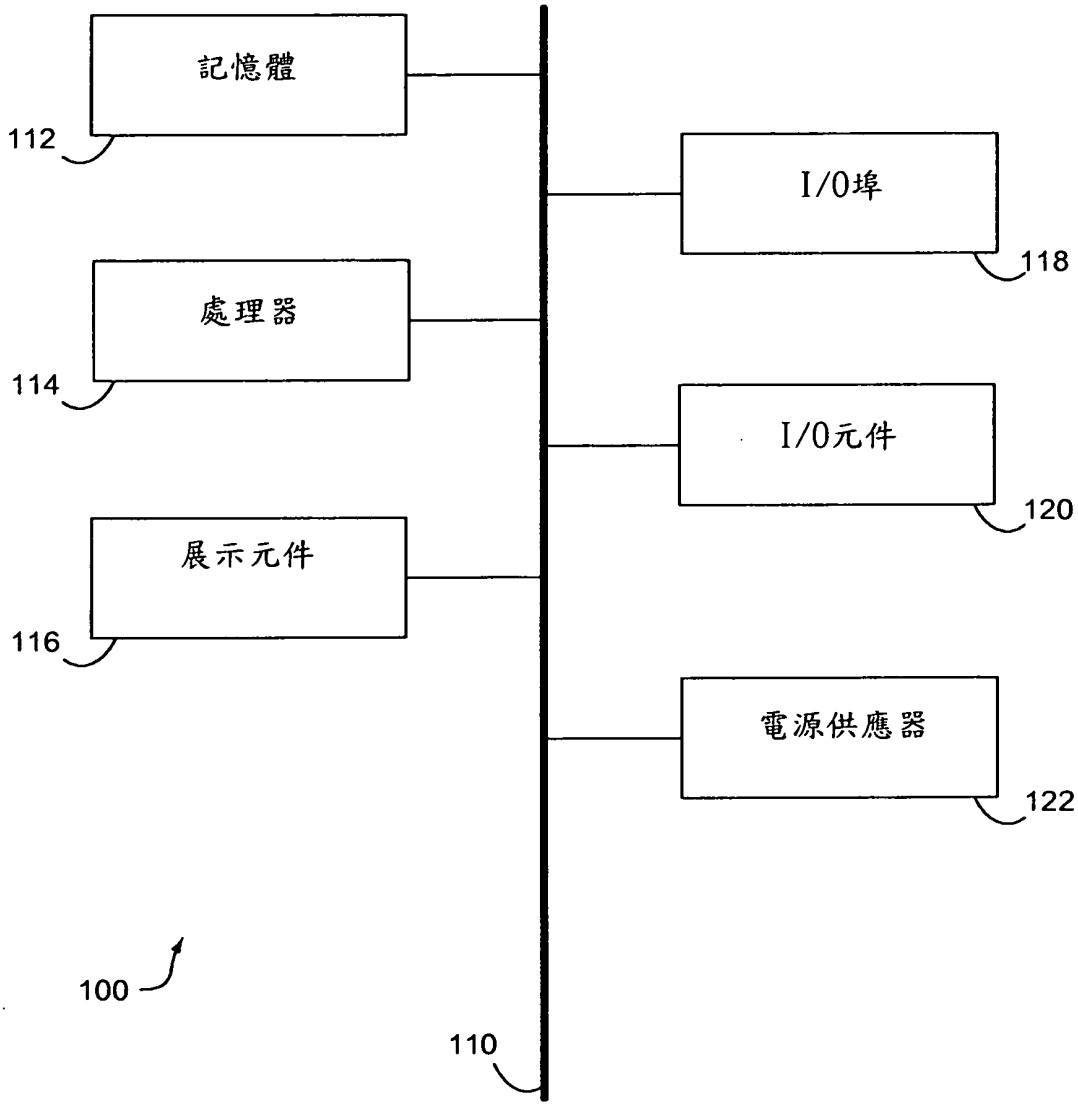
提供用於分散虛擬閘道功能至一實體網路之中的多重節點的電腦化方法、系統、及電腦可讀取媒體。首先，供應執行閘道功能的驅動程式與在網路節點上例示的端點合作，同時實施一目錄服務，以在虛擬網際網路協定（IP）位址及位置相依位址之間維持一映射，並且根據在一網路之中連接端點的已知路徑，而維持一列舉轉換動作表。在操作中，目錄服務以適當的位置相依位址（利用映射）及適當的轉換動作（利用表）而對來自驅動程式（攜帶資料封包的來源及目的 IP 位址）的請求回應。轉換動作包括重新寫入資料封包的標頭以包括位置相依位址、在分別的外部資料封包之中包覆資料封包作為內部資料封包、或以一通道協定配置資料封包。

三、英文發明摘要：

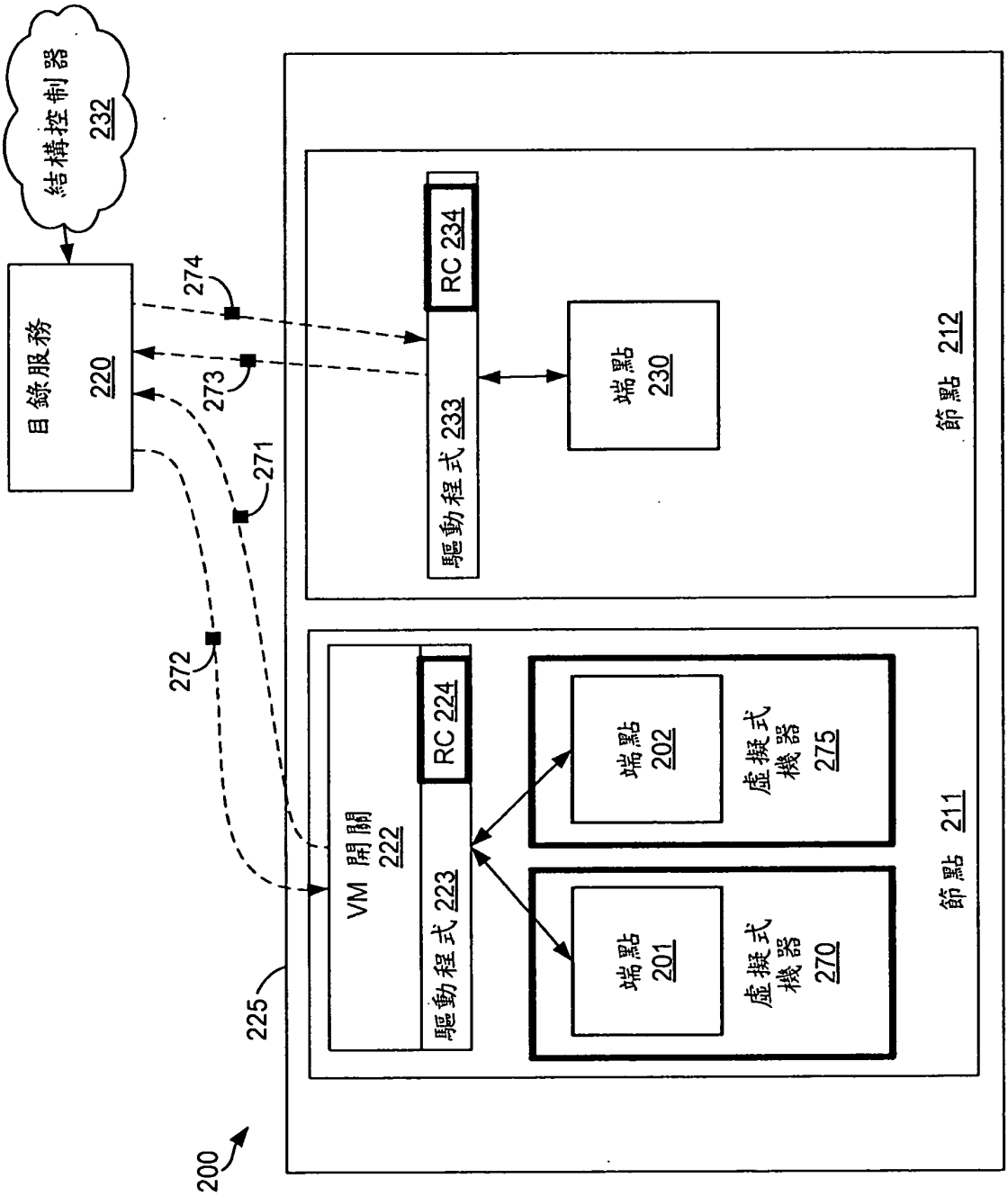
Computerized methods, systems, and computer-readable media are provided for distributing virtualized gateway functionality to multiple nodes within a physical network. Initially, drivers that carry out the gateway functionality are

provisioned to cooperate with endpoints instantiated on the network nodes, while a directory service is implemented to maintain a mapping between virtual internet protocol (IP) addresses and location-dependent addresses, as well as a table enumerating transformation actions according to known pathways connecting the endpoints within a network. In operation, the directory service replies to requests from the driver (carrying source and destination IP addresses of data packets) with the appropriate location-dependent addresses (utilizing the mapping) and the appropriate transformation action(s) (utilizing the table). The transformation action(s) include rewriting headers of the data packets to include the location-dependent addresses, encapsulating the data packets as inner data packets within respective outer data packets, or configuring the data packets with a tunneling protocol.

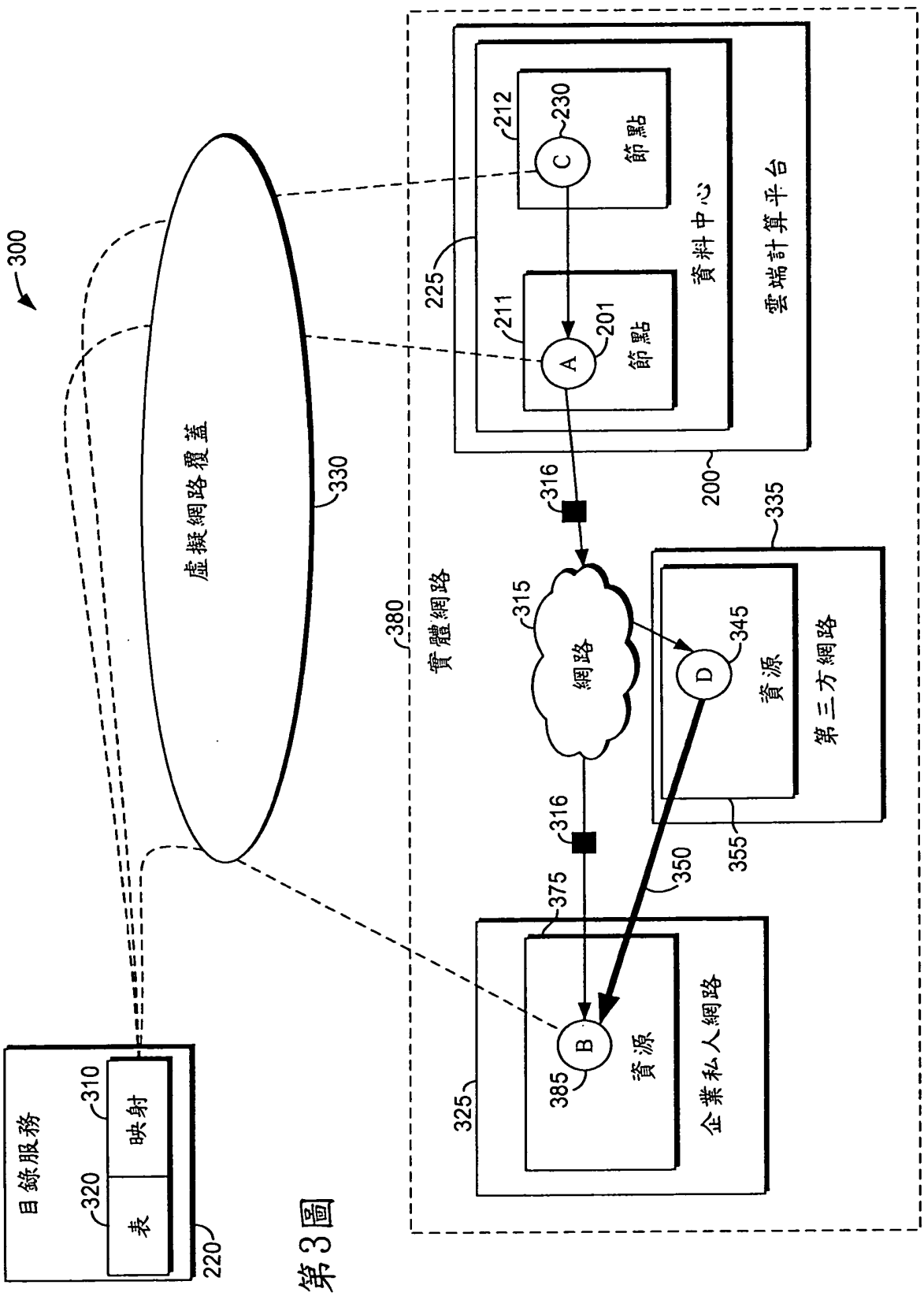
八、圖式：



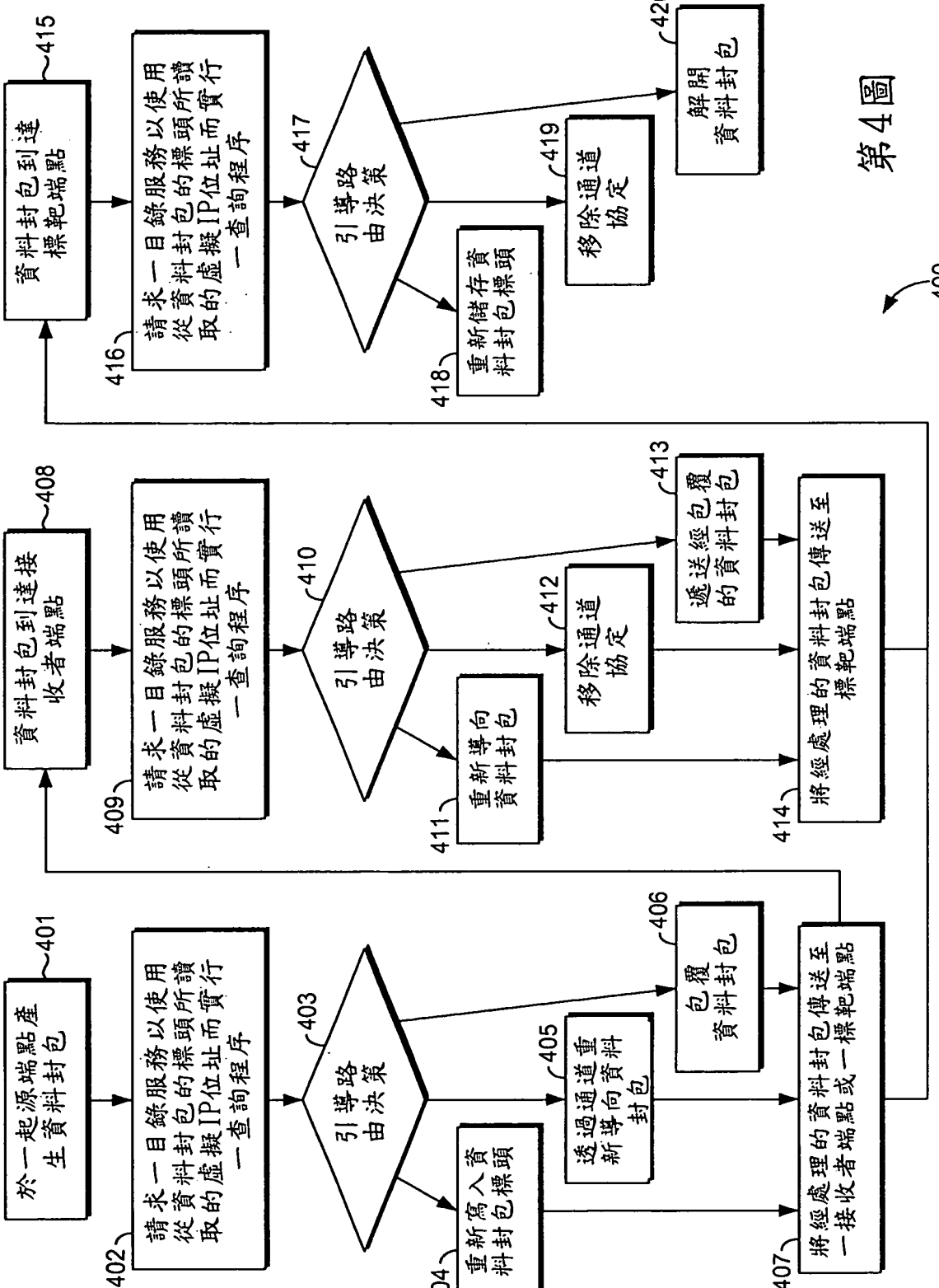
第1圖


結構控制器
232
目錄服務
220
274
273
271
272
225
200
RC 234
驅動程式 233
端點
230
節點 212
VM 開關
222
RC 224
驅動程式 223
端點
202
虛擬式
機器
275
端點
201
虛擬式
機器
270
節點 211

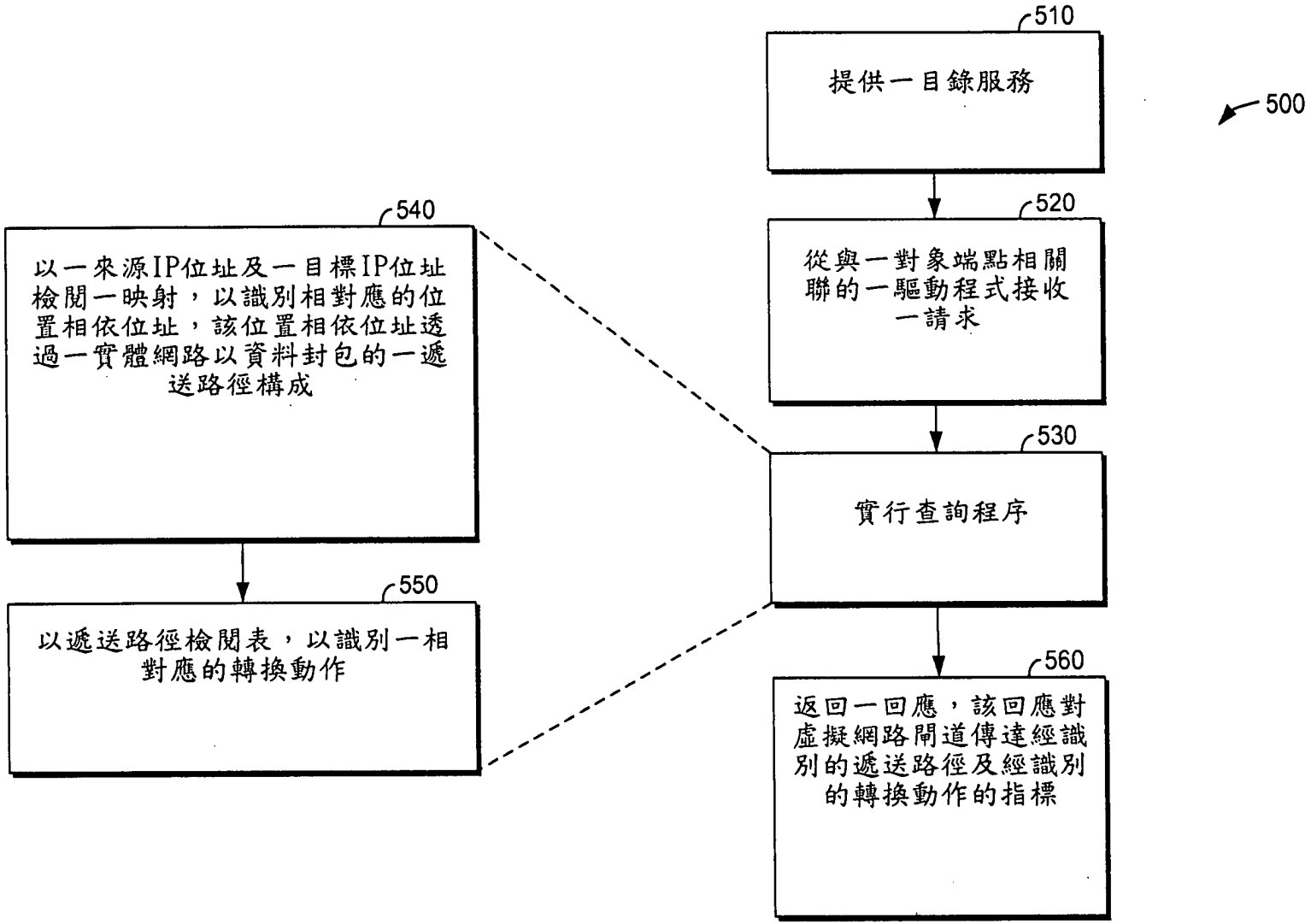
第2圖


300
虛擬網路覆蓋
330
目錄服務
310
映射
320
表
220
實體網路
380
雲端計算平台
200
資料中心
225
212
230
C
節點
211
201
A
節點
316
316
315
網路
335
D
345
資源
第三方網路
355
350
375
B
385
資源
325
企業私人網路

第3圖


於一起源端點產生資料封包
401
請求一目錄服務以使用從資料封包的標頭所讀取的虛擬IP位址而實行一查詢程序
402
引導路由決策
403
重新寫入資料封包標頭
404
透過通道重新導向資料封包
405
包覆資料封包
406
將經處理的資料封包傳送至一接收者端點或一標靶端點
407
資料封包到達接收者端點
408
請求一目錄服務以使用從資料封包的標頭所讀取的虛擬IP位址而實行一查詢程序
409
引導路由決策
410
重新導向資料封包
411
移除通道協定
412
透送經包覆的資料封包
413
將經處理的資料封包傳送至標靶端點
414
資料封包到達標靶端點
415
請求一目錄服務以使用從資料封包的標頭所讀取的虛擬IP位址而實行一查詢程序
416
引導路由決策
417
重新儲存資料封包標頭
418
移除通道協定
419
解開資料封包
420
400

第4圖


510
提供一目錄服務
500
520
從與一對象端點相關聯的一驅動程式接收一請求
530
實行查詢程序
540
以一來源IP位址及一目標IP位址檢閱一映射，以識別相對應的位置相依位址，該位置相依位址透過一實體網路以資料封包的一遞送路徑構成
550
以遞送路徑檢閱表，以識別一相對應的轉換動作
560
返回一回應，該回應對虛擬網路閘道傳達經識別的遞送路徑及經識別的轉換動作的指標

第5圖

四、指定代表圖：

(一)本案指定代表圖為：第（ 3 ）圖。

(二)本代表圖之元件符號簡單說明:

201 端點	320 表
211 節點	325 企業私人網路
212 節點	330 虛擬網路覆蓋
220 目錄服務	335 第三方網路
225 資料中心	345 端點
230 端點	350 安全通道
300 分散式計算環境	355 資源
310 映射	375 資源
315 網路	380 實體網路
316 資料封包	385 端點

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

七、申請專利範圍：

1. 一種電腦可讀取儲存媒體，該電腦可讀取儲存媒體排除信號本身而具有電腦可執行指令安裝於該電腦可讀取儲存媒體上，當執行該等指令時，實行用於管理端點之間的資料封包的分散的一方法，該方法包含以下步驟：

於一第一端點處偵測一個或更多個資料封包，其中該一個或更多個資料封包之各者包括一標頭，該標頭包含一來源位址及一目標位址；

發送一請求至一目錄服務，該請求攜帶該來源位址及該目標位址；

從該目錄服務接收一回應，該回應攜帶一遞送路徑；

實行一路由決策，該決策包含基於該所接收的遞送路徑而重新定址該一個或更多個資料封包，其中部分基於該遞送路徑而重新定址該一個或更多個資料封包之步驟包含以下步驟：於分別的外部資料封包之中包覆該一個或更多個資料封包作為內部資料封包，其中該等外部封包之各者包括一標頭，該標頭揭露一實體網路的位置相依位址；及

部分基於該位置相依位址而傳送該一個或更多個重新定址的資料封包至一第二端點。

2. 如申請專利範圍第1項之電腦可讀取儲存媒體，其中該方法進一步包含以下步驟：從該目錄服務接收攜帶一

轉換動作的該回應。

3. 如申請專利範圍第 2 項之電腦可讀取儲存媒體，其中實行一路由決策的步驟進一步包含以下步驟：基於該所接收的轉換動作轉換該一個或更多個資料封包。

4. 如申請專利範圍第 3 項之電腦可讀取儲存媒體，其中轉換該一個或更多個資料封包之步驟係在以下情況之後立即發生：存取一服務模式，且決定該服務模式指示提供一層保護，以保衛該第一端點及該第二端點之間的連接。

5. 如申請專利範圍第 1 項之電腦可讀取儲存媒體，其中該第一端點代表產生該一個或更多個資料封包的一端點，且其中該第二端點代表由該一個或更多個重新定址的資料封包的一標頭所標定的一端點。

6. 如申請專利範圍第 1 項之電腦可讀取儲存媒體，其中該第一端點代表運行於一實體機器上或一虛擬機器（VM）上，產生該一個或更多個資料封包的一網路轉接器。

7. 如申請專利範圍第 6 項之電腦可讀取儲存媒體，其中該第二端點代表運行於一實體機器上或一 VM 上，由該

一個或更多個重新定址的資料封包的一標頭所標定的一網路轉接器。

8. 如申請專利範圍第 1 項之電腦可讀取儲存媒體，其中該來源位址及該目標位址分別代表一虛擬空間的網路指派位址、虛擬網際網路協定（IP）位址。

9. 如申請專利範圍第 1 項之電腦可讀取儲存媒體，其中基於該遞送路徑而重新定址該一個或更多個資料封包的步驟包含以下步驟：

將在該一個或更多個資料封包的該標頭之中的該來源位址及該目標位址移除（removing）；及

分別以一實體網路的位置相依位址取代該來源位址及該目標位址。

10. 如申請專利範圍第 9 項之電腦可讀取儲存媒體，其中取代該來源位址及該目標位址之步驟係在以下情況之後立即發生：識別該第一端點及該第二端點係駐居於一通用資料中心之中，且識別該來源位址及該目標位址屬於一通用虛擬空間。

11. 如申請專利範圍第 1 項之電腦可讀取儲存媒體，其中包覆該一個或更多個資料封包之步驟在以下情況之後立即發生：決定若該來源位址及該目標位址被移除

（removed），則該第二端點無法轉譯該一個或更多個資料封包的該等標頭。

12. 如申請專利範圍第 1 項之電腦可讀取儲存媒體，其中安裝一驅動程式以實行該路由決策，且其中該驅動程式係安裝於一資料中心之中的一節點上，該節點裝載該第一端點。

13. 如申請專利範圍第 12 項之電腦可讀取儲存媒體，其中該第一端點每一次對傳送資料封包建立一連接時，該驅動程式實行一路由決策。

14. 如申請專利範圍第 13 項之電腦可讀取儲存媒體，其中該驅動程式包括一路由元件，該路由元件配置成接受該一個或更多個資料封包，且從該一個或更多個資料封包的該標頭讀取該來源位址及該目標位址。

15. 如申請專利範圍第 14 項之電腦可讀取儲存媒體，其中該驅動程式配置成在該第一端點建立與該第二端點的一連接之後，立即將該來源位址及該網路位址與該目錄服務通訊。

16. 一種用於在端點之間支援且隔離通訊的電腦系統，該電腦系統包含：

一目錄服務，該目錄服務在一實體網路的虛擬網際網路協定（IP）位址及位置相依位址之間維持一映射；

一第一端點，該第一端點產生一個或更多個資料封包，該一個或更多個資料封包以包括一來源 IP 位址及一目標 IP 位址的標頭構成，其中該來源 IP 位址指向該第一端點，且其中該目標 IP 位址指向一第二端點；及

一驅動程式，該驅動程式對每一個由該第一端點作成的連接實行一路由決策，其中實行該路由決策的步驟包含以下步驟：

（a）與該目錄服務通訊，以該來源 IP 位址及該目標 IP 位址的一函數關係，來決定一遞送路徑及一轉換動作；

（b）在決定該第一端點及該第二端點係駐居於一通用資料中心之中之後，立即以該遞送路徑的分別的位置相依位址，重新寫入該來源 IP 位址及該目標 IP 位址；

（c）在決定若該來源 IP 位址及該目標 IP 位址被移除，則該第二端點無法轉譯該一個或更多個資料封包的該等標頭之後，立即在分別的外部資料封包之中包覆該一個或更多個資料封包作為內部資料封包，其中該等外部封包之各者包括一標頭，該標頭揭露該遞送路徑的位置相依位址；及

（d）在決定該轉換動作支配一層保護以保衛提供於該第一端點及該第二端點之間的連接之後，立即基於該所接收的轉換動作轉換該一個或更多個資料封包。

17. 如申請專利範圍第 16 項之電腦系統，其中該來源 IP 位址及該目標 IP 位址係分別根據該第一端點及該第二端點所揭露的功能性而指派，其中該位置相依位址係分別根據該實體網路之中的該第一端點及該第二端點的位置而指派。

18. 如申請專利範圍第 16 項之電腦系統，其中該目錄服務維持一表，該表根據預先建立的通道或網路途徑的一記錄而給予該適當的轉換動作，該記錄與該第一端點及該第二端點鏈結。

19. 一種回應於來自一分散式、虛擬網路閘道的一請求而用於識別一網路途徑及轉換動作的電腦化方法，該方法包含以下步驟：

提供一目錄服務，該目錄服務在虛擬網際網路協定（IP）位址及位置相依位址之間維持一映射，且維持認知一適當的轉換動作的一表，其中該表係根據通訊策略而設計，該等通訊策略確保在一網路之中連接端點的途徑上的資料封包流量；

從與一接收者終端通訊的一虛擬網路閘道接收一請求，其中該請求包括一來源 IP 位址及一目標 IP 位址的指標，該來源 IP 位址及該目標 IP 位址透過一個或更多個資料封包的一標頭攜帶，該標頭由該接收者終端接受；

以該來源 IP 位址及該目標 IP 位址檢閱該映射，以識別相對應的位置相依位址，該等位置相依位址透過一實體網路組成該一個或更多個資料封包的一遞送路徑；

以該遞送路徑檢閱該表，以識別一相對應的轉換動作，其中該轉換動作包含以下至少一者：

（a）重新寫入該一個或更多個資料封包的該標頭，以包括該位置相依位址；

（b）在分別的外部資料封包之中包覆該一個或更多個資料封包作為內部資料封包，其中該等外部封包之各者包括攜帶該位置相依位址的一標頭；或

（c）以一通道協定配置該一個或更多個資料封包；及

返回一回應，該回應係傳遞至該經識別的遞送路徑及該經識別的轉換動作的該虛擬網路閘道指標，其中該虛擬網路閘道將該回應通訊至該接收者端點，且其中當從該虛擬網路閘道傳送該一個或更多個資料封包時，該接收者端點實施該經識別的遞送路徑及該經識別的轉換動作。