常見問題

常見問題與回答分類如下：

網路頻寬負載平衡

網路負載平衡技術利用多組廣域網路連線，將網路流量有效分配在多組線路上，頻寬資源得以充分被利用。無需網路服務供應商的額外設置或任何設備，企業網路即可建立可靠且高速的網路連線。

> 廣域網路負載平衡

廣域網路負載平衡功能透過連接多組廣域網路連線，在多組廣域網路上分配外送流量負載。這幫助企業能以低成本方式建立具高可靠度的對外網路連線。

> 廣域網路故障轉移

當主要對外鏈路故障時，網路故障轉移功能將網路流量轉移至其餘狀態正常的鏈路。當主要對外鏈路恢復正常運作後，流量則恢復原有機制透過主要鏈路連結網際網路。

> 頻寬整併

以封包為單位分配流量至所有可用對外線路，達到多鏈路頻寬整併功能。理論上，可增加的頻寬等於所有連接線路頻寬的總和。

> 行動網路頻寬整併

行動網路頻寬整併技術利用多個 4G LTE 網路連線，為分支機構提供高彈性與擴展性網路回程 (Backhaul) 至企業總部。

> 內送流量備援與負載平衡

當外部請求透過 DNS 機制要求存取企業的伺服器時，內送網路流量負載平衡功能則透過設備內建 DNS 機制，將內送請求引導至狀態最佳或流量負載最少的路徑上，亦或平均分配在所有可用路徑上。確保企業網路服務不受線路故障而中斷。

> 政策性路由

運用 MAC、IP 位址、網路埠口、網域 (內建與自訂)、應用程序與時程等，為企業網路策略制定路由政策。除了傳統基於網路第三層與第四層轉址 (NAT) 技術的網路負載平衡技術，次世代廣域網路負載平衡技術，更可以辨識網路應用程式，並基於網路第七層為流量做路徑分配。資訊人員可以更細膩的方式，為企業網路策略制定路由政策與頻寬資源分配，優化關鍵應用的交付，提供更好的使用著經驗。

> 基於網域的路由能力

域名路由技術使資訊部門能夠運用網域名稱作為路由依據，基於企業策略需求彈性制定網路路由，為不同業務性質的流量設置主要路徑 (WAN 與 VPN)。

> 會話保持 (Session Persistence)
為確保網路連接 (Connections) 持續性地透過同一對外鏈路傳輸，會話保持功能依據流量來源 IP 地址和目標 IP 地址，將外送流量保持在同一路徑上，直到會話結束。

> 路徑監控
路徑監視功能持續監控所有對外鏈路狀態，與動態路徑選擇功能 (DPS) 結合使用。基於路徑監控收集的信息，動態路徑選擇功能可在多組對外鏈路上，智能地進行故障轉移與流量有效分配。

> 對外線路斷斷續續
當對外線路品質不佳發生斷斷續續等情況時，雖然仍具某些程度的連線能力，但封包丟失、延遲增加、或抖動將會降低網路效能。

VPN 負載平衡與故障轉移

> 自動 VPN 通道故障轉移
透過 VPN 兩端設備持續不斷監控 VPN 會話狀態，在主要鏈路出現故障時，自動將 VPN 通道轉移至其餘可用路徑上。自動 VPN 通道故障轉移技術提高 VPN 通道的可靠性。

> 點對點 VPN 頻寬整併
點對點 VPN 頻寬整併功能將單一 VPN 會話細分為以封包為單位做分配，點對點 VPN 的流量透過多組對外鏈路做傳輸，提高 VPN 傳輸速度。所有線上活動，包含瀏覽、視頻與檔案傳輸等都可透過 VPN 頻寬整併技術快速地傳輸。

> VPN 頻寬整併功能自動配置
VPN 頻寬整併中的覆蓋網路與政策路由設置，透過自動配置進行，無需太多人力設置即可自動完成，降低設備上線時間與成本。

> IPSec VPN 通道建立
點對點網路架構可透過兩台 VPN 設備，在兩個不同地理位置之間建立安全的 IPSec VPN 通道。Q-Balancer 設備支援與其他品牌設備建立 IPSec VPN 通道。

> IPSec VPN 通道故障移轉
在點對點網路間利用 Q-Balancer 設備建立多組 IPSec 通道，透過 IPSec 通道故障移轉機制，點對點網路流量傳輸能有效避開故障 VPN 通道。當傳輸過程中發生 IPSec 通道故障中斷時，設備能將點對點網路流量轉移至運作正常的 IPSec 通道上。

> IPSec 通道負載平衡
在點對點網路間利用 Q-Balancer 設備建立多組 IPSec 通道，在多組通道間分配點對點網路流量，達成點對點間網路流量傳輸的負載平衡。

MPLS 網路強化

MPLS 線路已無法完全滿足企業用戶的需求，例如: 連線備援、前置作業時間冗長、昂貴成本、頻寬升級、雲端應用程序交付等問題。MPLS 線路強化方案可協助 MPLS 企業用戶克服這些問題。

> 混合廣域網路
混合廣域網路透過不同類型的網路連線，連接兩個不同地理位置上的站點。通常，主要線路類型是 MPLS 線路，另一類型大多是寬頻網路。在混合廣域網路中，分支機構透過 MPLS 線路連接企業總部或數據中心，而同時透過寬頻網路存取公有雲應用服務，寬頻網路通常亦做為 MPLS 線路的備援。

> 廣域網路虛擬化
廣域網路虛擬化概念上結合不同類型多組廣域網路連線，邏輯上建立一組單一鏈路。可結合 MPLS 線路與其他低成本寬頻網路的頻寬，以增強或替代分支機構連線能力。

> 覆蓋網路
覆蓋網路使用軟體虛擬化技術建立通道，或基於軟體功能在實體線路 (公有或私有網路) 上運行的通道技術附加層方法。覆蓋網路可提供應用程序安全與加速交付等優勢。

> 覆蓋網路自動配置
覆蓋網路與相關路由策略可在設備上自動設置。將新設立的分支站點網路連線到企業網路僅需幾分鐘時間，因此可大大減少安裝時間和人工成本。

> 覆蓋網路支援動態路由
透過了解 (並參與) 常用動態路由協議 (例如: OSPF 與 BGP 等) 的能力，設備能夠建立和維護現有的路由表。 因此，在私有網路發生故障中斷情況時，私有網路間的路由可被引導至覆蓋網路上的虛擬路徑。

> 虛擬設備
虛擬設備是一套軟體平台，可供多組不同設備在平台上運行，它簡化了複雜的安裝與組態過程，具有高容量擴充性、高可靠性、降低營運與維護成本等優勢。Q-Balancer 虛擬設備是執行於 VMware 虛擬化平台之上。

> 簡化分支機構網路
憑藉整合多項功能，方案導入後無需其他專用網路設備，例如: 防火牆、路由器等，這降低了分支機構的網路建置與管理複雜度。

> 支援各種傳輸層技術
覆蓋網路建立在實體廣域網路上，但不限定其網路傳輸型態。 因此當建立覆蓋網路時，管理者無需考慮網路是 MPLS 或 ADSL 或 4G LTE 等線路。

> 網路控制器
網路控制器維護與所有邊緣設備的覆蓋網路連接，並監控所有不同廣域網路類型鏈路上覆蓋通道運行狀態，幫助企業網路動態和智能網路。

> 邊緣設備
邊緣設備大多部屬在分支機構，連接 MPLS 與寬頻網路連線，網路流量可透過最佳路徑動態地引導至目的地，並可在多組不同類型廣域網路間做負載平衡與備援。

> 動態路徑選擇
動態路徑選擇功能與路徑監控結合使用，使設備得以將流量在多組對外路徑上有效分

配。動態路徑選擇功能依據負載平衡策略和即時線路訊息將流量引導至最佳路徑。亦可將流量有效地分配在多組對外路徑上，達到更高頻寬使用率。

> 應用程式感知路由機制
應用程式感知路由機制能辨識關鍵應用程序，針對特定關鍵應用程序將流量透過指定路徑派送至目的地。

> 本地網路流量分流
邊緣設備在本地端，透過不同類型網路連線，分別將公有與私有雲流量智能地引導到正確的目的地。

> 前向錯誤更正
前向錯誤更正技術修補丟失封包與封包順序，修正更正封包順序功能，改善網路品質，排除通道上不可靠或吵雜的資料傳輸錯誤。

企業級網路功能

設備配備多項高階網路功能，讓企業網路的部署與管理更為容易，滿足企業各種使用需求，管理人員得以單一設備應用多種用途。

> 頻寬管理
頻寬管理使企業能夠根據業務導向主動管理頻寬。因此，關鍵應用程序得以分配所需的頻寬，同時也避免業務無關應用程序消耗重要頻寬資源。頻寬管理使網路管理人員能夠依據負載平衡策略，設置最大與保證頻寬給予關鍵應用或重要使用者，策略包括MAC、IP、服務埠口、Domain Name 與應用程式等，也可僅依據特定應用程式類別保障頻寬。

> 頻寬減量
頻寬減量技術將檔案在通過廣域網路前，透過壓縮技術將它們容量變得更小，大幅減少檔案傳輸的頻寬資源使用，這使發送方可以讓同一檔案傳輸使用更少的封包與時間。

> 伺服器負載平衡與故障轉移
於使用者與後端伺服器群組間分配傳入的請求，有效使用所有伺服器資源。當設備偵測到伺服器群組中有設備發生故障時，設備會將故障伺服器從群組中暫時剔除，並將流量重新分配給其餘狀態正常的伺服器。

> 全球伺服器負載平衡與故障轉移
將使用者的請求平均分配至多部服務主機上，有效利用整體伺服器群組資源。如其中一個機房發生問題無法提供服務時 (例如斷電)，全球伺服器負載平衡會將使用者請求重新導向其餘區域的機房可用主機，類似於伺服器負載平衡與故障轉移。惟伺服器負載平衡只侷限於單一或鄰近機房內內進行，但全球伺服器負載平衡卻能夠跨越不同地區，例如:紐約與台北兩地的機房，共同執行負載平衡與備援功能對使用者提供服務。

> 雙機備援高可用性
雙機備援高可用性確保企業網路保持設備容錯能力，應付意外的硬體故障。對於預期系統維護之類的停機時間，也可將其影響減少，無需再付出額外網路設置。

> 透通模式 (Multiple Transparent Bridges)
透通模式讓設備扮演網路 OSI 模式的第二層角色，設備導入不必修改既有網路架構設置，安裝快速。

> 遠端存取虛擬私有網路 (Remote Access VPN)
讓主機自外部連回企業網路的虛擬私有網路，遠端與移動設備得以像在企業區網內般地存取企業網路資源，例如，PPTP、L2TP / IPSec、與 IPSec。

> 鏈路聚合控制協議 (LACP)
指將多個實體埠綁定在一起，邏輯上形成一個虛擬單一實體埠，流量在各成員埠間平均分配，提高了吞吐量。當偵測到其中一個成員埠的鏈路發生故障時，就停止在此埠口上發送封包，故障埠口恢復後則再次擔任收發埠口。鏈路聚合技術旨在增加鏈路帶寬、實現鏈路傳輸彈性與備援等。

網路安全

透過內建安全機制 (包括 ARP 欺騙攻擊防護、防火牆、Domain Names 過濾與 DDoS 攻擊防護)，保護企業網路免遭受未經授權的訪問攻擊。

> ARP 欺騙攻擊防護
ARP 欺騙是一種網路攻擊手段，攻擊者發送 ARP 欺騙到區網上。這導致攻擊者與網路上合法主機或伺服器或網路閘道做連結，導致該 IP 地址的任何流量都發送給攻擊者。ARP 攻擊防護技術使用靜態 IP-MAC 綁定來保護企業網路免受 ARP 欺騙攻擊。

> 防火牆
防火牆的狀態檢查會監控一段時間內傳入和傳出的封包與連接 (Connections) 狀態，並將數據儲存在動態連接表中，基於先前連接 (Connections) 以及屬於同一連接的流量封包建立的前後文做過濾。同時，也能基於預先定義的過濾規則做封包過濾。

> 網域名稱 (Domain Names) 過濾
網域名稱過濾功能與傳統防火牆相似，網域名稱過濾防止網路用戶或系統連接到已知位址的主機。但網域名稱過濾功能在第七層網路層過濾特定位址主機的存取。

> 阻斷服務 (DoS) 攻擊防護
阻斷服務 (DoS) 攻擊是一種嘗試對合法最終使用者進行惡意攻擊，以影響其目標系統 (例如: 網站或應用程式) 可用性的行為。通常，攻擊者會產生大量的封包或請求，最終使得目標系統無法負荷。如果是分散式阻斷服務 (DDoS) 攻擊，攻擊者會使用多個盜用或受控的來源來產生攻擊。DDoS 攻擊防護將可能受攻擊的區域降到最低並迅速緩解它，為企業網路基礎架構，提供強大的安全性。

> 連接限制 (Connections Limit)
連接 (Connections) 限制配置為控制來自單一 IP 主機或網段最大連接數量，當連接數超過最大允許數量時，連接限制功能將過濾超額連接並做記錄 ，確保企業網路不超載或資源不被濫用。

商業有關的問題

> 關於德餘科技

德餘科技致力於企業網路產品設計研發，幫助企業打造優質網路環境，確保企業網路傳輸暢通快速，強化業務營運在網路上的連續性。透過與優質經銷夥伴合作，提供產品導入網路整合與售後服務。自成立以來，Q-Balancer 產品已在 20 多個國家，數千家知名企業成功部署與運作。

> 解決方案
德餘科技為企業分支機構、總部網路、大型組織與數據中心打造可靠且高擴展性的軟體定義廣域網路解決方案。產品配備負載平衡、路由與流量管理等多項功能於單一平台上，並透過直覺網頁式操作界面執行配置。

> 我們的軟體定義廣域網路解決方案帶給企業的主要好處是什麼？
>> 優化應用程式交付。
>> 增強企業 MPLS 網路可靠性與性能。
>> 透過低成本寬頻技術提高企業網路頻寬 。
>> 使用頻寬管理，實現高頻寬利用率。
>> 透過內送流量負載均衡技術，提升企業網路服務的可用性與服務品質。
>> 內建網路安全與加密機制功能，保護分支機構與資料傳輸的安全。
>> 自動化網路設置降低設備配置與維護成本。
>> 覆蓋網路動態路由確保私有網路間路由暢通。
>> 降低企業分支網路成本與複雜度。
>> 支援 4G LTE 網路連線能力，業務不再受到網路專線冗長前置作業時間與地理位置所侷限。

> 部署一台 Q-Balancer 設備通常需要多長時間？
任何一位具備 TCP / IP 知識且了解 Q-Balancer 產品的工程師，都可以在幾分鐘內讓企業網路透過 Q-Balancer 設備上網。

> Q-Balancer 解決方案如何為客戶省錢?
>> 利用寬頻網路取代昂貴的 MPLS 服務實現成本降低，第一個月企業就開始享受節費的效果。
>> 規劃分支機構網路時，分支機構不再需要專屬路由器、防火牆或其他功能專用的網路硬體設備。
>> 透過集中管理系統，單一網路管理員即可為所有分支機構做管理維護。同時，排除高階技能工程師的人力需求。
>> 排除網路品質不佳造成網路斷線所造成的隱藏成本。

> 如何為客戶選擇的合適型號？
解決方案支援分支機構、企業總部，大型組織與數據中心等各種客戶群。且有實體與虛擬設備可供客戶選擇。

>> 虛擬設備
QB-2000 專為教育，大型企業和數據中心而設計，支持多達 52 組廣域網路和高達 20 Gbps 的吞吐量。大型組織可以使用 QB-2000 作為鏈路負載平衡器來確保網路連接，而在分散式網路架構中，QB-2000 可以用作中央網路控制器。

QB-500 旨在為中型和大型企業和區域數據中心帶來高網路可靠性和效能。這款 1U 機

架式設備最多可支持 52 組廣域網路和高達 3 Gbps 的吞吐量。QB-500 可保護企業免受任何潛在的網路故障和中斷等威脅。

QB-300 專為中小型企業設計，支持多達 25 組廣域網路和高達 1.5 Gbps 的吞吐量。這款 1U 機架式設備可確保企業網路連線能力，同時為企業提供多項網路功能，包括路由，防火牆和頻寬管理等。

QB-150 是一款緊湊型設計設備，適用於需要高頻寬的小型和分支機構。 該項目設備最多支持 10 組廣域網路和高達 300 Mbps 的網路吞吐量。QB-150 具有一體化功能、低成本、高可靠性等優點。

QB-Mesh 的設計旨在為任何無固定線路之分支機構例如:偏遠地區分支機構、臨時店鋪、戶外專案、大型活動等等，即刻提供企業級廣域網路解決方案。QB-Mesh 憑藉其優越智能演算法和內建工業等級 4G LTE 模組，滿足分支網路使用者與關鍵應用的頻寬需求，確保業務暢通無阻。

>> 虛擬設備
QB-V2000 是一款在 VMware 平台上運行的虛擬設備，提供與實體 QB-2000 設備相同的功能。

如果您還有其他有關產品方面的問題，請與您的經銷商或與我們聯繫。