

ASCENLINK

智慧型寬頻整合管理器



使用手冊



ASCENLINK

使用手冊

版權聲明

寬宇資訊技術將不對本手冊內存在的錯誤或相關事宜以及在包裝、執行或使用中造成的損壞負法律責任。寬宇資訊技術保留修改手冊內容的權利。產品規格如有更動恕不另行通知。

本文中使用的產品名稱及商標，隸屬於各公司註冊所有。

2009© 寬宇資訊技術有限公司版權所有並保留所有權利。

Xtera® 為寬宇資訊技術有限公司所有之註冊商標。其餘所有名稱則為其擁有者所屬之註冊商標。

Document Number: AL-MENU-AL-C6.0

Document Revision: TC 6.0-Rev1-B2646

©Copyright2009, Xtera Communications Inc.

前言

歡迎使用 AscenLink 智慧型頻寬整合管理器！

AscenLink 是一個多功能的頻寬整合管理器，它結合了線路負載平衡 (Load Balancing)、網路備份 (Fault Tolerance)、多重定址 (Multihoming)、頻寬管理 (Bandwidth Management)、防火牆 (Firewall) 等功能，讓您的對外網路頻寬可以做最有效的應用。

AscenLink 是寬宇科技所研發的網路傳輸管理系列 (Network Management Product Family) 中的重要產品，網路傳輸管理系列的目標是實現受到完善管理的網路環境。本系列還包括另一個重要產品：AscenFlow 高性能網路流量管理器；以及三款配套軟體：LinkReport，FlowReport 和 Central Management。

AscenLink 適用於同時使用多條網路連線的環境。利用 AscenLink 所提供的線路負載平衡功能，使用者可以針對往外送出的封包在適當的時機使用特定的網路連線 (Auto Routing)；此外，當其中任何一條聯外線路中斷時 AscenLink 能夠在短時間內察覺到網路的異常情況，動態地修正封包路由 (Packet Route)，避免接下來的資料傳輸受到線路中斷的影響，達到對外連線的容錯與備份。當內部網路有設置對外服務的企業網站時，僅僅靠著對外連線的容錯與備份是不夠的；AscenLink 的 SwiftDNS™ 專利技術可以視情況而調整網域名稱系統 (DNS, Domain Name System) 的查詢結果，達到多重定址的目的，確保企業網站能夠常態地提供不中斷的服務。

AscenLink 靈活的頻寬管理 (BM, Bandwidth Management) 功能可以滿足使用者各式各樣的管理需求，能夠針對不同的通訊協定，例如檔傳輸協定 (FTP, File Transfer Protocol) 與超文本傳輸協定 (HTTP, HyperText Transfer Protocol)，以及不同的時段（網路繁忙時段與空閒時段），設定所容許使用頻寬的最大值與最小值，提升網路的服務品質 (QoS, Quality of Service)。針對維護網路安全 (Network Security) 的需要，AscenLink 也內建了防火牆 (Firewall) 及非軍事區 (DMZ, DeMilitarized Zone) 功能，能夠隔絕大多數來自外界對內部網路的惡意攻擊。

AscenLink 智慧型頻寬整合管理器的適用環境非常廣泛，從一般的小型企業與中、小學，一直到大型企業、大專院校、Internet 服務提供廠商 (Internet Service

Provider, ISP) 及各大區網中心等，都可以視網路環境的複雜程度與個別需求，在 AscenLink 的產品線中，找到適用的型號。任何對於網路頻寬的管理及穩定性有高度要求的機構，都可以考慮使用 AscenLink。

如何使用本手冊

本手冊主要由六個章節所組成，介紹 AscenLink 的主要功能及應用環境。

第一章快速入門，讓使用者能對 AscenLink 的網路架構與硬體安裝有初步的瞭解。並簡單介紹 AscenLink 的管理介面 (包括 Web 介面與命令列介面)。

第二章～第五章分別就產品的功能架構，逐一介紹各項功能和設定，並配合適當的範例，來解釋功能的使用。

第六章主要是應用討論，對常用的功能作進一步的討論。

附錄主要是介紹使用者在主控台模式下，使用控制台指令，以及如何更新 AscenLink 的韌體，包括更新的步驟與錯誤訊息參考及對應處理的方式。

我們在準備這本使用手冊之前，已經假設使用者是一個專業的網路管理人員，對於基本的網路知識，如 TCP/IP，Public IP，Private IP，子網路，路由概念，網路常用的各種服務，如 SSH，POP3，SMTP，FTP 等，不再作原理上的解釋。

目錄

第一章 快速入門	1-4
1.1 使用環境的準備	1-4
1.2 登入 AscenLink 的網頁管理介面	1-6
1.3 AscenLink 網頁管理介面介紹	1-8
1.4 通用功能介紹	1-10
1.4.1 AscenLink 操作畫面	1-10
1.4.2 規則列增減之使用介面和方式	1-11
1.4.3 切換語言	1-12
1.5 基本網路設定	1-13
1.5.1 WAN 端介面基本設定	1-15
1.5.2 LAN 端介面基本設定	1-18
1.6 典型多廣域網路連線網路架構	1-20
1.7 Public IP-Address Pass-Through	1-26
1.7.1 AscenLink 和現有防火牆配合使用	1-27
1.8 硬體安裝須注意事項	1-28
1.8.1 如何安裝於機架上	1-28
1.8.2 AscenLink 與其他網路設備連線的線材規格	1-29
1.9 AscenLink HA 模式下的安裝及 HA 設定方式	1-30
1.9.1 AscenLink HA(High Availability)模式的安裝方法	1-30
1.9.2 HA 的設定方式	1-31
第二章 System(系統)功能表	2-6
2.1 Summary(系統資訊)	2-7
2.2 Network Setting (網路設定)	2-10
2.2.1 DNS Server(網域名稱伺服器)子功能	2-12
2.2.2 VLAN and Port Mapping(VLAN 與網路介面對應)子功能	2-14
2.2.3 WAN Setting(廣域網路設定)子功能	2-22

2.2.4	WAN/DMZ Private Subnet(廣域網路/隔離區私有子網路)子功能	2-42
2.2.5	LAN Private Subnet 子功能(區域網路私有子網路)	2-54
2.3	WAN Link Health Detection (廣域網路連線狀態偵測)	2-62
2.4	Optimum Route Detection (最佳路徑偵測)	2-64
2.5	Port Speed/Duplex Setting (網路介面傳輸模式設定)	2-67
2.6	Backup Line Setting (備援線設定)	2-69
2.7	IP Grouping (IP 群組設定)	2-71
2.8	Service Grouping (網路服務群組設定)	2-73
2.9	Busyhour Setting (尖峰時段設定)	2-75
2.10	Diagnostic Tools (網路診斷工具)	2-78
2.11	Date/Time (系統時間)	2-83
2.12	Administration (系統管理)	2-84
第三章	Service (服務) 功能表	3-8
3.1	Firewall (防火牆)	3-9
3.2	NAT (位址轉換)	3-15
3.3	Persistent Routing (持續路由)	3-19
3.4	Auto Routing (自動路由)	3-29
3.5	Virtual Server (虛擬主機)	3-45
3.6	Inbound BM (對內頻寬管理)	3-52
3.7	Outbound BM (對外頻寬管理)	3-62
3.8	Connection Limit (連線限制)	3-69
3.9	Cache Redirect (快取重定向)	3-72
3.10	Tunnel Routing (通道路由)	3-77
3.11	Multihoming (多重定址)	3-103
3.11.1	在設定 Multihoming 前須有以下的準備工作	3-105
3.11.2	Multihoming 啟用設定	3-106
3.12	Internal DNS (內建 DNS)	3-118
3.13	SNMP (簡單網路管理)	3-120
3.14	IP-MAC Mapping (IP-MAC 對應)	3-122
第四章	Statistics (統計) 功能表	4-4

4.1	Traffic (短期流量)	4-5
4.2	BM (頻寬管理)	4-7
4.3	Persistent Routing (持續路由)	4-8
4.4	WAN Link Health Detection (廣域網路連線狀態偵測)	4-10
4.5	Dynamic IP WAN Link (動態 IP 廣域網路)	4-12
4.6	DHCP lease info	4-14
4.7	RIP&OSPF Status (RIP&OSPF 狀態資訊)	4-16
4.8	Tunnel Status (通道狀態)	4-18
4.9	Tunnel Traffic (通道流量)	4-20
4.10	Connection Limit (連線限制)	4-21
4.11	Virtual Server Status (虛擬伺服器狀態)	4-22
第五章 Log (記錄) 功能表		5-4
5.1	View (記錄流覽)	5-5
5.2	Control (傳輸設定)	5-7
5.3	Notification (重要通知)	5-10
5.4	LinkReport	5-13
第六章 應用討論		6-3
6.1	廣域網路類型之應用實例	6-3
6.1.1	Bridge Mode: One Static IP 之廣域網路	6-3
6.1.2	AscenLink 在 Routing Mode 之廣域網路設定	6-7
6.2	Auto Routing(自動路由) 應用探討	6-16
6.2.1	使用 Auto Routing 的優點	6-17
6.2.2	AscenLink 提供線路中斷時自動備援的運作方式	6-19
6.2.3	Persistent Routing 和 Auto Routing	6-22
6.3	流量負載平衡應用探討	6-23
6.4	Virtual Server (虛擬主機) 的應用	6-25
6.5	Multihoming 的應用	6-26
6.6	DNS 服務簡介	6-29
6.6.1	SwiftDNS	6-31
6.7	HA 應用討論	6-33

6.7.1	HA 模式下的 firmware 更新方式	6-33
6.7.2	HA 模式下復原至單機的操作方式	6-35
6.7.3	Slave 接管 Master 之原則	6-35
附錄目錄.....		A-I
附錄 A.1	系統預設值.....	A-II
附錄 A.2	序列埠控制臺指令.....	A-V
附錄 A.3	AscenLink 軟體更新.....	A-X
附錄 A.4	Configuration File 備援	A-XII

圖目錄

圖 1.1	取消設定 Proxy	1-7
圖 1.2	AscenLink WebUI 標題	1-10
圖 1.3	WAN 端介面基本設定圖	1-13
圖 1.4	VLAN Port Mapping 設定圖	1-14
圖 1.5	Basic Subnet 基本設定	1-17
圖 1.6	Basic Subnet 完成設定	1-19
圖 1.7	多廣域網路連線網路架構	1-20
圖 1.8	VLAN and Port Mapping 設定內容	1-21
圖 1.9	WAN Link 1 參數之設定	1-22
圖 1.10	WAN Link 2 參數之設定	1-23
圖 1.11	DMZ Private Subnet 參數之設定	1-24
圖 1.12	LAN Private Subnet 設定	1-25
圖 1.13	Public IP-Address Pass-Through 網路架構法	1-26
圖 1.14	AscenLink 和防火牆配合使用	1-27
圖 1.15	於標準機架上安裝 AscenLink	1-28
圖 1.16	AscenLink 的高可用性連接埠之設定	1-30
圖 2.1	System 功能表	2-6
圖 2.2	System/Summary 所處位置	2-7
圖 2.3	System/Network Setting 功能所處位置與其子功能	2-10
圖 2.4	System/Network Setting/DNS Server 功能所處位置	2-12
圖 2.5	System/Network Setting/VLAN and Port Mapping 功能所處位置	2-14
圖 2.6	VLAN 與 AscenLink 的配合使用	2-15
圖 2.7	備援 LAN 及備援 DMZ 埠 範例 1 網路架構	2-18
圖 2.8	備援 LAN 及備援 DMZ 埠 範例 1 埠設定	2-19
圖 2.9	備援 LAN 及備援 DMZ 埠 範例 2 網路架構	2-20
圖 2.10	備援 LAN 及備援 DMZ 埠 範例 2 埠設定－VLAN 與埠映射部分	2-21

圖 2.11	備援 LAN 及備援 DMZ 埠 範例 2 埠設定－LAN 私有子網部分	2-21
圖 2.12	System/Network Setting/WAN Setting 功能所處位置.....	2-22
圖 2.13	WAN Setting 基本設定	2-23
圖 2.14	Basic Subnet 中 Subnet 類型.....	2-25
圖 2.15	Static Routing Subnet 中 Subnet 類型.....	2-25
圖 2.16	Basic Subnet Mode 下 Subnet in WAN 之架構	2-26
圖 2.17	Basic Subnet 模式下有關 Subnet in WAN 的架構設定.....	2-27
圖 2.18	Basic Subnet 模式 Subnet in DMZ 之網路架構圖	2-28
圖 2.19	Basic Subnet 中 Subnet Detail 中有關 DMZ 之設定.....	2-29
圖 2.20	Basic Subnet 模式 Subnet in WAN and DMZ 之網路架構圖	2-30
圖 2.21	Basic Subnet 模式下有關 Subnet in WAN and DMZ 的架構設定.....	2-31
圖 2.22	Basic Subnet 模式下 Subnet on Localhost 之網路架構圖.....	2-32
圖 2.23	Basic Subnet 模式下有關 Subnet on Localhost 的架構設定	2-32
圖 2.24	Static Routing Subnet 模式下 Subnet in WAN 架構圖	2-33
圖 2.25	Static Routing Subnet 模式下有關 Subnet in WAN 架構的設定	2-33
圖 2.26	Static Routing Subnet 模式下 Subnet in DMZ 之架構圖	2-34
圖 2.27	Static Routing Subnet 模式下有關 Subnet in DMZ 架構的設定.....	2-34
圖 2.28	Bridge Mode: One Static IP 網路架構圖.....	2-35
圖 2.29	Bridge Mode: One Static IP 的 Basic Setting 設定	2-36
圖 2.30	Bridge Mode: Multiple Static IP 網路架構圖	2-38
圖 2.31	Bridge Mode: Multiple Static IP 下，Basic Setting 設定.....	2-39
圖 2.32	Bridge Mode: PPPoE 下，Basic Setting 設定.....	2-40
圖 2.33	Bridge Mode: DHCP Client 下，Basic Setting 設定.....	2-41
圖 2.34	System/Network Setting/WAN/DMZ Private Subnet 子功能位置.....	2-42
圖 2.35	WAN/DMZ Private Subnet 中 Subnet 種類	2-43
圖 2.36	Static Routing Subnet 中 Subnet 種類.....	2-43
圖 2.37	Basic Subnet 模式之 Subnet in WAN 網路架構圖	2-44
圖 2.38	Basic Subnet 模式下有關 Subnet in WAN 的架構設定.....	2-45
圖 2.39	Basic Subnet 模式 Subnet in DMZ 之網路架構圖	2-46

圖 2.40	Basic Subnet 模式 Subnet in DMZ 之架構設定	2-47
圖 2.41	Basic Subnet 模式 Subnet in WAN/DMZ 之網路架構圖	2-48
圖 2.42	Basic Subnet 模式下有關 Subnet in WAN and DMZ 的架構設定	2-49
圖 2.43	Basic Subnet 模式 Subnet on Localhost 之網路架構圖	2-50
圖 2.44	Basic Subnet 模式下有關 Subnet in WAN and DMZ 的架構設定	2-50
圖 2.45	Static Routing Subnet 模式下 Subnet in WAN 之網路架構圖	2-51
圖 2.46	Static Routing Subnet 模式下有關 Subnet in WAN 架構的設定	2-52
圖 2.47	Static Routing Subnet 模式下 Subnet in DMZ 之網路架構圖	2-53
圖 2.48	Static Routing Subnet 模式下有關 Subnet in DMZ 架構的設定	2-53
圖 2.49	System/Network Setting/ LAN Private Subnet 功能所處位置	2-54
圖 2.50	區域網路模式下 basic 子網路之網路架構圖	2-55
圖 2.51	LAN Private Subnet/ Basic Subnet 的設定	2-56
圖 2.52	LAN Private Subnet/ RIP 的設定	2-57
圖 2.53	LAN Private Subnet/ OSPF 的設定	2-58
圖 2.54	Static Routing Subnet 網路架構圖	2-60
圖 2.55	LAN Private Subnet/ Static Routing Subnet 的設定	2-61
圖 2.56	System/WAN Link Health Detection 功能所處位置	2-62
圖 2.57	System/ Optimum Route Detection 功能所處位置	2-64
圖 2.58	System/ Duplex Setting 功能所處位置	2-67
圖 2.59	System/ Backup Line Setting 功能所處位置	2-69
圖 2.60	System/ IP Grouping 功能所處位置	2-71
圖 2.61	System/Service Grouping 功能所處位置	2-73
圖 2.62	System/ Busyhour Setting 功能所處位置	2-75
圖 2.63	Busyhour Setting 設定範例	2-77
圖 2.64	System/ Diagnostic Tools 功能所處位置	2-78
圖 2.65	Tcpdump 功能	2-80
圖 2.66	System/ Date/Time 功能所處位置	2-83
圖 2.67	System/ Administration 功能所處位置	2-84
圖 3.1	Service 功能圖	3-8

圖 3.2	Service/Firewall 功能所處位置	3-9
圖 3.3	Firewall 範例 1 架構示意圖	3-12
圖 3.4	Firewall 範例 2 架構示意圖	3-13
圖 3.5	Service /NAT 功能所處位置	3-15
圖 3.6	NAT 設定圖一	3-17
圖 3.7	NAT 設定圖二	3-17
圖 3.8	Non-NAT 模式簡易範例架構示意圖	3-18
圖 3.9	Service /Persistent Routing 功能所處位置	3-19
圖 3.10	Persistent Routing 範例 1 架構示意圖	3-23
圖 3.11	Persistent Routing 範例 2 架構示意圖	3-25
圖 3.12	Persistent Routing 範例 3 架構示意圖	3-27
圖 3.13	Service /Auto Routing 功能所處位置	3-29
圖 3.14	Auto Routing 範例 1 架構示意圖	3-33
圖 3.15	Auto Routing 範例 2 架構示意圖	3-36
圖 3.16	Auto Routing 範例 3 架構示意圖	3-40
圖 3.17	Service/Virtual Server 功能所處位置	3-45
圖 3.18	Virtual Server 範例 1 架構示意圖	3-47
圖 3.19	Vitrual Server 範例 2 架構示意圖	3-50
圖 3.20	Service/Inbound BM 功能所處位置	3-52
圖 3.21	Inbound BM Classes 設定表格	3-53
圖 3.22	Inbound BM 範例 1 架構示意圖	3-56
圖 3.23	Inbound BM 範例 2 架構示意圖	3-59
圖 3.24	Service /Outbound BM 功能所處位置	3-62
圖 3.25	Outbound BM 範例 1 架構示意圖	3-65
圖 3.26	Outbound BM 範例 2 架構示意圖	3-67
圖 3.27	Service /Connection Limit 功能所處位置	3-69
圖 3.28	Connection Limit 欄位介紹	3-70
圖 3.29	Connection Limit 設定範例	3-71
圖 3.30	Service /Cache Redirect 功能所處位置	3-72

圖 3.31	Cache Redirect 設定欄位.....	3-73
圖 3.32	Cache Miss 狀態下資料流走向	3-75
圖 3.33	Cache Hit 狀態下資料流走向	3-76
圖 3.34	Service / Tunnel Routing 功能所處位置.....	3-77
圖 3.35	Tunnel Routing 範例 2 架構示意圖.....	3-88
圖 3.36	Tunnel Routing 範例 3 架構示意圖.....	3-91
圖 3.37	Tunnel Routing 範例 4 架構示意圖.....	3-95
圖 3.38	Service /Multihoming 功能所處位置.....	3-103
圖 3.39	Multihoming 全局設定	3-106
圖 3.40	Multihoming Policy 設定.....	3-107
圖 3.41	Domain Setting	3-108
圖 3.42	Domain Setting in relay	3-111
圖 3.43	啓用災備功能	3-112
圖 3.44	Multihoming 範例 (1) 架構示意圖	3-113
圖 3.45	Multihoming 範例 (2) 架構示意圖	3-115
圖 3.46	Service / Internal DNS 功能所處位置	3-118
圖 3.47	Service / Tunnel Routing 功能所處位置.....	3-120
圖 3.48	Service / IP-MAC MAPPING 功能所處位置.....	3-122
圖 4.1	Statistic 功能圖.....	4-4
圖 4.2	Statistics/Traffic 功能所處位置	4-5
圖 4.3	Statistics/BM 功能所處位置.....	4-7
圖 4.4	Statistics/Persistent Routing 功能所處位	4-8
圖 4.5	Statistics/WAN Link Health Detection 功能所處位置	4-10
圖 4.6	Statistics/Dynamic IP WAN Link 功能所處位	4-12
圖 4.7	Statistics/DHCP lease info 功能所處位.....	4-14
圖 4.8	Statistics/RIP&OSPF Status 功能所處位置.....	4-16
圖 4.9	Statistics/Tunnel Status 功能所處位置	4-18
圖 4.10	Tunnel Traffic 功能所處位置.....	4-20
圖 4.11	Statistics/Connection Limit 功能所處位置	4-21
圖 4.12	Virtual Server Status 功能所處位置	4-22

圖 5.1	Log 功能圖.....	5-4
圖 5.2	Log/View 功能所處位置.....	5-5
圖 5.3	Log/Control 功能所處位置.....	5-7
圖 5.4	log/Notification 功能所處位置.....	5-10
圖 5.5	Notification 功能設定.....	5-11
圖 5.6	Log/LinkReport 功能所處位置.....	5-13
圖 5.7	LinkReport 欄位.....	5-14
圖 6.1	Bridge Mode: One Static IP 之廣域網路架構圖.....	6-4
圖 6.2	Routing Mode 連線之廣域網路.....	6-7
圖 6.3	以 Router 與 AscenLink 間私有網路模式連線之廣域網路.....	6-10
圖 6.4	多條廣域網路模式連線之廣域網路.....	6-12
圖 6.5	網路中斷時採用手動方式變更網路組態.....	6-18
圖 6.6	網路中斷時以 Auto Routing 方式選擇線路.....	6-19
圖 6.7	固定分配線路斷線時自動切換至備用模式.....	6-20
圖 6.8	典型的多重定址網路連線方式.....	6-26
圖 6.9	Multihoming 設定圖.....	6-32

表目錄

表 1.1	頁面按鈕介紹.....	1-10
表 1.2	規則列增減的操作方式.....	1-11
表 1.3	方格的表示.....	1-11
表 1.4	AscenLink 與其他網路設備連線之線路型態.....	1-29
表 2.1	System Information 信息列表	2-8
表 2.2	Peer Information 信息列表	2-8
表 2.3	License Information 信息列表	2-9
表 2.4	VLAN Tag 及對應 AscenLink 網路介面的位置	2-16
表 2.5	備援 LAN 及備援 DMZ 欄位說明	2-17
表 2.6	Routing Mode 下 Basic Setting 表格欄位說明	2-24
表 2.7	OSPF 路由協定設定.....	2-59
表 2.8	動態偵測設定欄位說明.....	2-65
表 2.9	靜態 IP 列表偵測設定欄位說明	2-66
表 2.10	網路介面傳輸模式設定欄位說明	2-68
表 2.11	Threshold 欄位說明	2-70
表 2.12	Backup Line Rule 欄位說明表.....	2-70
表 2.13	IP Grouping 欄位說明表.....	2-72
表 2.14	Rules Setting 欄位說明表	2-72
表 2.15	Service Grouping 欄位說明表.....	2-74
表 2.16	Busychour Setting 欄位說明表	2-76
表 2.17	Administor 密碼管理	2-85
表 2.18	Monitor 密碼管理	2-86
表 2.19	AscenLink 保留埠	2-87
表 3.1	System Information 信息列表	3-11
表 3.2	Firewall 範例 1 設定內容.....	3-13
表 3.3	Firewall 範例 2 製作內容	3-14
表 3.4	NAT 各功能選項解釋之參照表	3-16

表 3.5	Persistent Routing 各功能選項解釋之參照表	3-21
表 3.6	Persistent Routing 範例 1 設定內容	3-24
表 3.7	Persistent Routing 範例 2 設定內容	3-26
表 3.8	Persistent Routing 範例 3 根據 Web 服務設定內容.....	3-28
表 3.9	Persistent Routing 範例 3 根據 IP 位址設定內容.....	3-28
表 3.10	Policies 欄位設定說明表.....	3-30
表 3.11	Auto Routing 各功能選項解釋之參照表.....	3-32
表 3.12	AutoRouting 範例 1 Policies 設定內容	3-34
表 3.13	AutoRouting 範例 1 Filters 設定內容	3-35
表 3.14	AutoRouting 範例 2 Policies 設定內容	3-37
表 3.15	AutoRouting 範例 2 Filters 設定內容	3-39
表 3.16	Auto Routing 範例 3 相關資訊	3-41
表 3.17	Auto Routing 範例 3:記錄及本機 ID 設定(Beijing 總公司).....	3-41
表 3.18	Auto Routing 範例 3:Tunnel Group 設定(Beijing 總公司)	3-41
表 3.19	Auto Routing 範例 3:Routing Rules 設定(Beijing 總公司)	3-42
表 3.20	Auto Routing 範例 3:Auto Routing Policies 設定(Beijing 總公司).....	3-42
表 3.21	Auto Routing 範例 3:Auto Routing Filters 設定(Beijing 總公司)	3-42
表 3.22	Auto Routing 範例 3:記錄及本機 ID 設定(Shanghai 分公司)	3-43
表 3.23	Auto Routing 範例 3:Tunnel Group 設定(Shanghai 分公司).....	3-43
表 3.24	Auto Routing 範例 3:Routing Rules 設定(Shanghai 分公司)	3-43
表 3.25	Auto Routing 範例 3:Auto Routing Policies 設定(Shanghai 分公司)	3-44
表 3.26	Auto Routing 範例 3:Auto Routing Filters 設定(Shanghai 分公司).....	3-44
表 3.27	Virtual Server 各功能選項解釋之參照表	3-46
表 3.28	Virtual Server 範例 1 設定內容	3-49
表 3.29	Virtual Server 範例 2 設定內容	3-51
表 3.30	Inbound BM Classes 欄位說明表	3-54
表 3.31	Inbount BM 各功能選項解釋之參照表	3-55
表 3.32	Inbount BM 範例 1 Class 設定內容	3-57
表 3.33	Inbount BM 範例 1 Filters 設定內容	3-58

表 3.34	Inbount BM 範例 2 Class 設定內容	3-60
表 3.35	Inbount BM 範例 2 Filters 設定內容.....	3-61
表 3.36	Outbound BM Class 欄位說明表	3-63
表 3.37	Outbound BM Filters 欄位說明表.....	3-64
表 3.38	Outbound BM 範例 1Classes 設定內容	3-66
表 3.39	Outbound BM 範例 1Filters 設定內容	3-66
表 3.40	Outbound BM 範例 2 Classes 設定內容.....	3-68
表 3.41	Outbound BM 範例 2 Filters 設定內容.....	3-68
表 3.42	Connection Limit 記錄週期設定	3-70
表 3.43	Connection Limit Rule 設定	3-71
表 3.44	Cache Redirect 欄位說明表.....	3-73
表 3.45	Cache Redirect 各功能選項解釋之參照表	3-74
表 3.46	Tunnel Group 記錄及本地端 ID 設定.....	3-79
表 3.47	Tunnel Group 各功能選項解釋之參照表	3-80
表 3.48	Routing Rules 各功能選項解釋之參照表	3-81
表 3.49	Routing Rules 各功能選項解釋之參照表	3-82
表 3.50	Tunnel Routing 範例 1 設定	3-83
表 3.51	Tunnel Routing 範例 1:Tunnel Group 設定(1).....	3-84
表 3.52	Tunnel Routing 範例 1:Routing Rules 設定(1).....	3-85
表 3.53	Tunnel Routing 範例 1:Tunnel Group 設定(2).....	3-85
表 3.54	Tunnel Routing 範例 1:Routing Rules 設定(2).....	3-85
表 3.55	Tunnel Routing 範例 1:Tunnel Group 設定(3).....	3-86
表 3.56	Tunnel Routing 範例 1:Routing Rules 設定(3).....	3-86
表 3.57	Tunnel Routing 範例 1: Inbound BM Filter 設定.....	3-87
表 3.58	Tunnel Routing 範例 1: Outbound BM Filter 設定.....	3-87
表 3.59	Tunnel Routing 範例 2 相關資訊.....	3-89
表 3.60	Tunnel Routing 範例 2:記錄及本機 ID 設定(Beijing 總公司).....	3-89
表 3.61	Tunnel Routing 範例 2:Tunnel Group 設定(Beijing 總公司)	3-89
表 3.62	Tunnel Routing 範例 2:Routing Rules 設定(Beijing 總公司)	3-90

表 3.63	Tunnel Routing 範例 2:記錄及本機 ID 設定(Shanghai 分公司).....	3-90
表 3.64	Tunnel Routing 範例 2:Tunnel Group 設定(Shanghai 分公司)	3-90
表 3.65	Tunnel Routing 範例 2:Routing Rules 設定(Shanghai 分公司)	3-90
表 3.66	Tunnel Routing 範例 3 相關資訊.....	3-92
表 3.67	Tunnel Routing 範例 3:記錄及本機 ID 設定(Beijing 總公司)	3-92
表 3.68	Tunnel Routing 範例 3:Tunnel Group 設定(Beijing 總公司).....	3-92
表 3.69	Tunnel Routing 範例 3:Routing Rules 設定(Beijing 總公司)	3-93
表 3.70	Tunnel Routing 範例 3:記錄及本機 ID 設定(Shanghai 分公司).....	3-93
表 3.71	Tunnel Routing 範例 3:Tunnel Group 設定(Shanghai 分公司)	3-93
表 3.72	Tunnel Routing 範例 3:Routing Rules 設定(Shanghai 分公司)	3-93
表 3.73	Tunnel Routing 範例 3:記錄及本機 ID 設定(Tianjin 分公司)	3-94
表 3.74	Tunnel Routing 範例 3:Tunnel Group 設定(Tianjin 分公司).....	3-94
表 3.75	Tunnel Routing 範例 3:Routing Rules 設定(Tianjin 分公司)	3-94
表 3.76	Tunnel Routing 範例 4:相關資訊	3-96
表 3.77	Tunnel Routing 範例 4:記錄及本機 ID 設定(Beijing 總公司)	3-96
表 3.78	Tunnel Routing 範例 4:Tunnel Group 設定(Beijing 總公司).....	3-96
表 3.79	Tunnel Routing 範例 4:Routing Rules 設定(Beijing 總公司)	3-97
表 3.80	Tunnel Routing 範例 4:Auto Routing Policies 設定(Beijing 總公司)	3-97
表 3.81	Tunnel Routing 範例 4:Auto Routing Filters 設定(Beijing 總公司).....	3-97
表 3.82	Tunnel Routing 範例 4:記錄及本機 ID 設定(Shanghai 分公司).....	3-98
表 3.83	Tunnel Routing 範例 4:Tunnel Group 設定(Shanghai 分公司)	3-98
表 3.84	Tunnel Routing 範例 4:Routing Rules 設定(Shanghai 分公司)	3-98
表 3.85	Tunnel Routing 範例 4:Auto Routing 設定(Shanghai 分公司)	3-99
表 3.86	Tunnel Routing 範例 4:Auto Routing Filters 設定(Shanghai 分公司)	3-99
表 3.87	Tunnel Routing 範例 4:記錄及本機 ID 設定(Tianjin 分公司)	3-100
表 3.88	Tunnel Routing 範例 4:Tunnel Group 設定(Tianjin 分公司)	3-100
表 3.89	Tunnel Routing 範例 4:Routing Rules 設定(Tianjin 分公司)	3-100
表 3.90	Tunnel Routing 範例 5 設定.....	3-101
表 3.91	Tunnel Routing 範例 5:Tunnel Group 設定(1)	3-101

表 3.92	Tunnel Routing 範例 5:Routing Rules 設定(1)	3-101
表 3.93	Tunnel Routing 範例 5:Tunnel Group 設定(2)	3-102
表 3.94	Tunnel Routing 範例 5:Routing Rules 設定(2)	3-102
表 3.95	Tunnel Routing 範例 5: Persistent Rules 設定	3-102
表 3.96	Multihoming 全域設定欄位說明表	3-106
表 3.97	Multihoming Policy 欄位說明表	3-107
表 3.98	Multihoming 各功能選項解釋之參照表	3-110
表 3.99	Relay 模式下網域設定說明	3-111
表 3.100	Multihoming 範例 1 Virtual Server 設定	3-114
表 3.101	Multihoming 範例 1 Policy 設定	3-114
表 3.102	Multihoming 範例 1 Domain 設定	3-114
表 3.103	Multihoming 範例 2 Virtual Server 設定	3-117
表 3.104	Multihoming 範例 2 Policy 設定	3-117
表 3.105	Multihoming 範例 2 Domain 設定	3-117
表 3.106	Global Setting 各功能選項解釋之參照表	3-119
表 3.107	Domain Setting 各功能選項解釋之參照表	3-119
表 3.108	SNMP v1/2 各功能選項解釋之參照表	3-121
表 3.109	SNMP v3 各功能選項解釋之參照表	3-121
表 3.110	IP-MAC MAPPING 各功能選項解釋之參照表	3-122
表 4.1	短期流量統計表中各項資料解釋	4-6
表 4.2	BM 統計表中各項資料之解釋	4-7
表 4.3	Persistent Routing 各項資料之解釋	4-9
表 4.4	WAN Link Health Detection 各項資料之解釋	4-11
表 4.5	Dynamic IP WAN Link 各項資料之解釋	4-13
表 4.6	DHCP lease info 各項資料之解釋	4-15
表 4.7	RIP&OSPF Status 各項資料之解釋	4-17
表 4.8	Tunnel Status 各項資料之解釋	4-19
表 4.9	Tunnel Traffic 各項資料的解釋	4-20
表 4.10	Connection Limit 各項資料之解釋	4-21
表 4.11	Virtual Server Status 各項功能之解釋	4-22

表 5.1	Log/View 各功能選項解釋之參照表.....	5-6
表 5.2	Log/Control 各功能選項解釋之參照.....	5-8
表 5.3	傳輸方式:電子郵件欄位說明.....	5-9
表 5.4	傳輸方:FTP 式欄位說明.....	5-9
表 5.5	Notification 各功能.....	5-12
表 5.6	SNMP Trap Setting 欄位說明.....	5-12
表 5.7	Event Types to Notify 欄位說明.....	5-12
表 5.8	LinkReport 欄位說明.....	5-14
表 5.9	記錄種類欄位說明.....	5-14

目錄

第一章 快速入門	1-4
1.1 使用環境的準備	1-4
1.2 登入 AscenLink 的網頁管理介面	1-6
1.3 AscenLink 網頁管理介面介紹	1-8
1.4 通用功能介紹	1-10
1.4.1 AscenLink 操作畫面	1-10
1.4.2 規則列增減之使用介面和方式	1-11
1.4.3 切換語言	1-12
1.5 基本網路設定	1-13
1.5.1 WAN 端介面基本設定	1-15
1.5.2 LAN 端介面基本設定	1-18
1.6 典型多廣域網路連線網路架構	1-20
1.7 Public IP-Address Pass-Through	1-26
1.7.1 AscenLink 和現有防火牆配合使用	1-27
1.8 硬體安裝須注意事項	1-28
1.8.1 如何安裝於機架上	1-28
1.8.2 AscenLink 與其他網路設備連線的線材規格	1-29
1.9 AscenLink HA 模式下的安裝及 HA 設定方式	1-30
1.9.1 AscenLink HA(High Availability)模式的安裝方法	1-30
1.9.2 HA 的設定方式	1-31

圖目錄

圖 1.1	取消設定 Proxy	1-7
圖 1.2	AscenLink WebUI 標題	1-10
圖 1.3	WAN 端介面基本設定圖	1-13
圖 1.4	VLAN Port Mapping 設定圖	1-14
圖 1.5	Basic Subnet 基本設定	1-17
圖 1.6	Basic Subnet 完成設定	1-19
圖 1.7	多廣域網路連線網路架構	1-20
圖 1.8	VLAN and Port Mapping 設定內容	1-21
圖 1.9	WAN Link 1 參數之設定	1-22
圖 1.10	WAN Link 2 參數之設定	1-23
圖 1.11	DMZ Private Subnet 參數之設定	1-24
圖 1.12	LAN Private Subnet 設定	1-25
圖 1.13	Public IP-Address Pass-Through 網路架構法	1-26
圖 1.14	AscenLink 和防火牆配合使用	1-27
圖 1.15	於標準機架上安裝 AscenLink	1-28
圖 1.16	AscenLink 的高可用性連接埠之設定	1-30

表目錄

表 1.1	頁面按鈕介紹.....	1-10
表 1.2	規則列增減的操作方式.....	1-11
表 1.3	方格的表示.....	1-11
表 1.4	AscenLink 與其他網路設備連線之線路型態.....	1-29

第一章 快速入門

當首次使用 AscenLink 產品時，您可能面對複雜的設定而不知如何開始，本章的目的是很讓您在很短的時間，可以很快的掌握 AscenLink 基本工作原理和執行基本的操作。

本章會提到 AscenLink 的基本設定，常見到的網路環境規劃，以及硬體環境的架設等，這些工作都是您首次操作時會遇到的問題。

1.1 使用環境的準備

在開始之前，您需要先知道下面的內容。

- AscenLink 區域網路介面的位址。AscenLink 有不同的型號，組態不同數量的網路介面，例如 Model 530 就有五個網路介面。出廠預設值設定倒數第二個網路埠為 LAN 介面，倒數第一個網路介面為 DMZ 介面，例如 Model 680 有五個網路介面，第四個就是 LAN 介面，第五個就是 DMZ 介面。
- AscenLink LAN 介面的預設 IP 位址為 192.168.0.1。您的電腦的網路介面 IP 位址改設定為 192.168.0.2 (或是其他 192.168.0.x)
- 使用一條 Cross Over 網線連線電腦和 AscenLink 之 LAN 介面。
- 用 IE（版本不低於 6.0）或 Firefox（版本不低於 2.0）網路瀏覽器啓用 AscenLink 網頁管理介面，請輸入 <https://192.168.0.1>。
- 進入管理介面的預設密碼，Administrator 預設密碼是 1234，Monitor 是 5678。您可以參考下列程式進行修改。

在使用 AscenLink 之前您先檢查一下設備環境。在此建議您，當 AscenLink 要導入您的網路環境之前，最好將網路架構完整的規劃好，IP 位址分配妥當，然後再根據網路規劃圖，完整的設定 AscenLink 的各項參數。

AscenLink 採用 Web-Based 管理介面，也就是使用網頁瀏覽器管理介面，由於設計版本的緣故，須使用微軟的網路瀏覽器（版本不低於 6.0）或 Firefox（版本不低於 2.0），並且將使用的電腦解析度調為 800 x 600 及以上。

要進入 AscenLink 的網頁管理介面，需用一條 Cross Over 的網線，連線到 AscenLink 的 LAN 埠。千萬要記得使用 Cross Over 線連線電腦和 AscenLink LAN 埠。如果連線正確，AscenLink LAN 埠上的燈會正常點亮。

1.2 登入 AscenLink 的網頁管理介面

AscenLink 的網頁管理介面，可以讓您很容易的進行各項設定，請依照下列的步驟開始進行。電腦連線到 AscenLink 的 LAN 埠需用跳接網線 (Cross Over Cable)。AscenLink 有數個實體網路埠，其中倒數第二個預設為 LAN 埠，如果實體網路埠有五個，則第四個為 LAN 埠，餘此類推。

登入 AscenLink 管理介面可以依據以下步驟：

1. 將電腦的 LAN 埠連線到 AscenLink LAN 埠。使用者在正式使用時可以依實際需求，規劃網路介面的用途為 WAN、LAN 或 DMZ。
2. 開機後 AscenLink 會出現三聲 Beep 聲響，表示 AscenOS 已經正常啟動，LAN 埠的指示燈閃爍，表示連線正常。
3. 調整電腦的網路設置，將電腦的 LAN 埠 IP 位址設成 192.168.0.2，子網遮罩設成 255.255.255.0。
4. 啟動 IE 瀏覽器，取消 Proxy 設定，如圖 1.1。首先選取 IE「工具(T)」功能表中的「Internet 選項 (O)」。點選「連線」標籤，再按下「區域網設置 (L)」。在代理伺服器欄位上確定〔使用伺服器〕為空白沒有勾選。
5. AscenLink 使用者用 <https://192.168.0.1> 登入 AscenLink 網路管理介面。這裏請特別注意是 https 而非 http，基於安全的考慮，電腦和 AscenLink 溝通聯繫時，採用有加密的安全通訊模式。

Administrator (管理員)可以查看並修改系統設定。Monitor (普通使用者)只能查看系統設定而不能進行修改。AscenLink 僅允許同一個時間讓一個 Administrator 帳號以及五個 Monitor 帳號登入進去，並且後登入的 Administrator 會自動替換掉前一個 Administrator，使之成為 Monitor。Administrator 的預設密碼為 1234，Monitor 預設密碼為 5678。建議在第一次使用設定時，將出廠預設密碼改為自己可以管控的密碼。

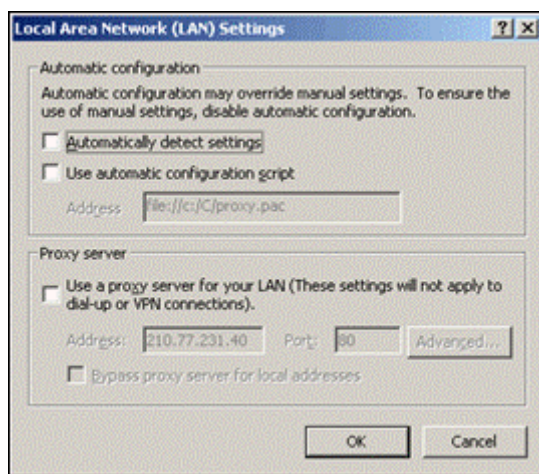


圖 1.1 取消設定 Proxy

1.3 AscenLink 網頁管理介面介紹

成功登入 AscenLink 網路管理介面後，您可以開始操作必要的設定或是觀察現有的設定。爲了讓您熟悉在網路管理介面下的操作，特對介面上的基本操作功能做如下說明。

五大功能選項介紹

五大功能選項區在畫面的左上角位置，所以有關 AscenLink 的操作設定都在這五大項功能裏。這五項功能分別是：

- System (系統)
- Service (服務)
- Statistics (統計)
- Log (記錄)
- Language (語言)

在往後的章節中，我們會分別介紹這五項功能的運用。在這個首次使用的階段，您會使用的功能爲 System 下 Administration (系統管理) 以及 Language (語言)。說明如下：

System 裏選擇 Administration (系統管理)，在這個功能下，您可以輸入 Administrator 和 Monitor 的新密碼，確認後下次登入就使用新的密碼進入。

Language (語言)，你可以切換管理畫面的語言。

如果忘掉新的密碼該如何處理？

這種情況如果發生了，您必須使用 RS-232 介面連線 AscenLink 的 Console 埠。在 AscenLink 出廠時附有一條 Null Modem Cable 用於連線電腦之 RS-232 和 AscenLink Console 埠，預設帳號：Administrator，密碼：ascenlink。然後執行終端通訊程式(Terminal，如“超級終端”)進入控制臺，可執行幾項控制命令，其中執行 `resetpasswd` 命令可以回復為原廠密碼設定值。詳細的 Console 控制命令在本手冊的附錄中有介紹。

重新獲得密碼後，啟動 IE 瀏覽器，進入網頁管理介面。

· 註：要記住變更後的密碼，否則將無法進入 AscenLink 管理介面。 ·

1.4 通用功能介紹

本節介紹登入管理介面之後一些基本的操作方法，以及使用介面如何安排，下圖是您登入後，所看到的上半部畫面。



圖 1.2 AscenLink WebUI 標題

1.4.1 AscenLink 操作畫面

主功能表分五個功能 (System, Service, Statistics, Log, Language)，每個功能下，有各項子功能，如 System/Summary 表示目前所在的頁面是主功能表下的 [System]->[Summary] 子功能。

右上角的 Monitor@192.168.0.1 表示目前以 Monitor 身分登入系統，此系統的 IP 為 192.168.0.1。右邊的 Logout 可點選以登出系統。

每個頁面都可以看到 Apply, Reload, Help (Hide Help) 三個功能鍵：

Apply	每當設定變動後，必須點選 Apply 來執行新的設定，並保存舊設定。當設定是在同一個功能下進行，例如在 WAN Setting 下進行各項設定，離開到另一個功能下，如果沒有按 Apply 鍵，所有設定會遺失並不會寫入記憶體中。
Reload	恢復 Apply 所保存的舊設定，並將畫面更新。
Help	可顯示目前頁面的線上說明，當切換頁面或切換語系時也會切換至相對應的線上說明。
Hide Help	當點選 Help 後會出現此按鈕，點選可關閉線上說明。

表 1.1 頁面按鈕介紹

1.4.2 規則列增減之使用介面和方式

在 AscenLink 中，有相當多的部分依靠表格式的規則列，所有的規則皆為由上而下比對 (top-down evaluation)，第一個比對成功的規則即為執行的規則。簡言之，比對範圍越小的規則放置於表格的上層，比對範圍較大的規則放置於表格的下層。

規則列增減的操作方式






	表示將目前位址新增一條新的規則
	表示將目前規則向下移動一列
	表示將目前規則向上移動一列
	表示將目前規則刪去
	表示為此規則增加新的批註

表 1.2 規則列增減的操作方式

新增規則時會將新規則加在目前規則的下一列。向上或向下移動表示與上方或下方的規則交換位置。

方格的表示

在控制表格中，常見如下表需要勾選的專案，意義是 **Enable** 或 **Disable**。Enable 的作用是表示此條規則啟用，或是啟用資料記錄檔，規則行為所產生的資料寫入 Log 檔中。

<input type="checkbox"/>	表示不使用此功能
<input checked="" type="checkbox"/>	表示使用此功能

表 1.3 方格的表示

到目前為止，我們先介紹介面的使用，接下來進入基本網路設定的作業。舉例一些常見的網路環境，如何將 AscenLink 放置在其中。

1.4.3 切換語言

在 Language（語言）功能選項上，可以選擇所使用的語言，並可立即切換頁面的語系。AscenLink 提供繁體中文與英文兩種語言，頁面內容語系切換的同時會切換到相對應的線上說明。

1.5 基本網路設定

根據下圖的範例，本節中將詳細說明如何設定 AscenLink 進行。這個範例是一個相對簡單的網路架構。

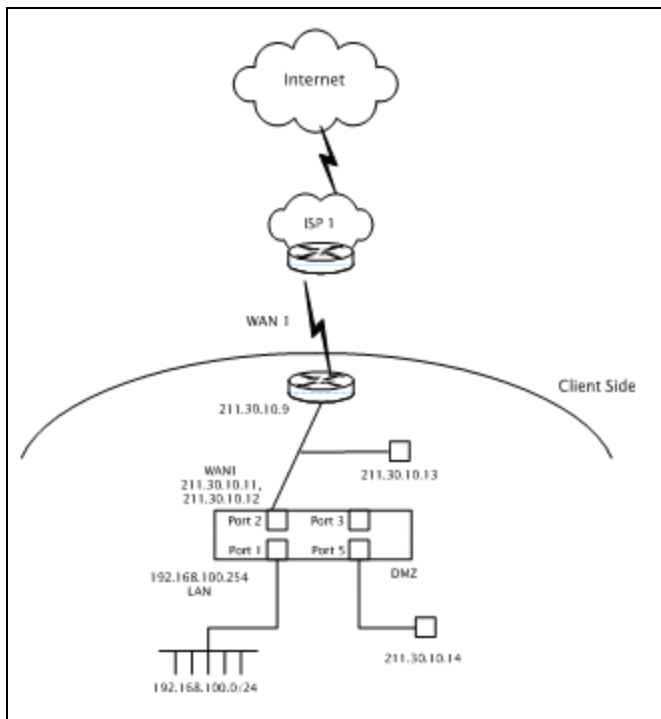


圖 1.3 WAN 端介面基本設定圖

根據以上的網路拓撲圖，開始進行各項網路設定，由於 AscenLink 允許每一個網路介面都可以依據功能設定，因此設定 AscenLink 的第一步是先規劃好每個網路介面的功能，是用於 WAN、LAN 或是 DMZ。

在這個例子中，AscenLink 的 Port2 規劃為 WAN 埠，Port 1 規劃為 LAN 埠，Port 5 規劃為 DMZ。

AscenLink 網路介面之設定，選擇[System] → [Network Setting]→ [VLAN and Port Mapping]，在這個管理畫面中，對每個網路介面進行設定。

VLAN and Port Mapping			
Port	VLAN Tag		Mapping
Port1	<input type="checkbox"/>	VLAN not supported	LAN <input type="button" value="v"/>
Port2	<input type="checkbox"/>	VLAN not supported	WAN <input type="button" value="v"/>
Port3	<input type="checkbox"/>	VLAN not supported	WAN <input type="button" value="v"/>
Port4	<input type="checkbox"/>	VLAN not supported	WAN <input type="button" value="v"/>
Port5	<input type="checkbox"/>	VLAN not supported	DMZ <input type="button" value="v"/>

圖 1.4 VLAN Port Mapping 設定圖

1.5.1 WAN 介面基本設定

完成網路介面的設定規劃後，同樣在 [Network Setting] 設定畫面下，點選 [WAN Setting] (廣域網路設定)，設定廣域網路連線方式。廣域網路 (WAN) 連線 AscenLink 到路由器的部分，作為區域網路 (LAN) 資料通往 Internet 的出口，需要在此項中，為連接 WAN 的網路介面設定 Public IP (公開 IP)。使用者在向 ISP 申請網路連線時，這些線路都會設定 Public IP，Netmask，以及 Gateway 等資料，這些資料都會在以下的設定中用到。

進入 [WAN Setting] 畫面後，設定如下：

1. 表示要設定廣域網路 (WAN) 第一條線路。如果您的對外連線路有多條則必須逐一設定。
2. 在[Basic Setting](基本設定)這個表格中，第一個欄位[Enable] 打勾，啟用 WAN 對外連線路。
3. 第二個欄位 [WAN Type] (線路模式) 選擇 [Routing Mode]。這個欄位有幾個值可供選擇，一般而言，如果 ISP 配給使用者是一個 Subnet (子網路)，則會有一組 Public IP，這種情況就選用 [Routing Mode]。相對的，如果 ISP 配給使用者是一個公開 IP，這種情況的網路架構是屬於橋接模式 (Bridge Mode)，則須選用 [One Static IP]。
4. 第三，四欄位填入 WAN Link 1 的上傳/下載頻寬數值。如果對外連線頻寬 Down Stream 為 512K，Upstream 為 512K，則此兩個欄位分別填入 512K/512K。
5. 第五欄位 [Default Gateway] (預設閘道)填入 Gateway 的 IP 位址。在此例中的 IP 為 211.33.10.9，也就是 Router (路由器)的位址。
6. 第六欄位 [MTU] 指傳輸過程中每個數據包的大小，如 1500。
7. 第七個欄位[WAN Port] 指定對外連線在 AscenLink 的那一個網路介面，例如，如果對外連線在 AscenLink 網路介面第一個連接埠 (編號為 “1”)，則此欄位選擇 “Port 1”，依此類推。本例對外連線是連在第二個網路介面，因此須設定為 “Port 2”。

接下來的設定是有關 **Basic Subnet** (子網路設定)，在 **Subnet Detail** 這個表格中有幾個欄位需要填寫。

1. **[Subnet Type]** 有幾個數值可選擇，本例中選擇 **[Subnet in WAN and DMZ]**，一般的網路架構絕大部份都使用這個選項。
2. **[IP(s) on Localhost]** 這個欄位填入 **AscenLink** 連外網路介面的 IP 位址，這些位址都是申請線路時，ISP 配給的 IP。在這個例子中，**AscenLink** 的對外網路介面 **Port 2** 綁定 (**Binding**) 兩個 IP 分別是 **211.30.10.11**，**211.30.10.12**。在填入第二個 IP 時，可點按 “+” 表示新增一行，以填寫第二個 IP 位址或是用下列格式：**211.30.10.11-211.30.10.12** 表示一個區段位址。輸入頭尾有效位址，中間用 “-” 連結。
3. **[IP(s) in WAN]** 這個欄位是指位於廣域網路所用到的 IP 位址，在這個範例中，**AscenLink** 的廣域網路所用的 IP 位址有兩個，分別是 **211.30.10.9**，**211.30.10.13**，其中 **211.30.10.9** 就是預設閘道位址，**211.30.10.13** 則是位於 WAN 的主機位址。
4. **[Netmask]** 欄位，請輸入 ISP 提供的 **Netmask** IP 位址。此例為 **255.255.255.248**。
5. **[DMZ Port]** 欄位，請指定 **AscenLink** 那一個網路介面用 **DMZ**，在此範例中，**DMZ** 為第五個網路介面。要指定 **AscenLink** 的網路介面用於 **WAN** 或是 **LAN**、**DMZ** 等不同功能，請在 **[VLAN and Port Mapping]** 選擇設定對應。
6. 如果 WAN 的電腦是以 **AscenLink** 為 **DHCP Server**，動態分配 IP 位址，您可以將 **DHCP** 功能 **Enable**，然後填入要分配給使用者端之 IP 位址範圍。如果有些主機是用固定 IP 的，則須在 **Static Mapping** 這個欄位填入指定的 IP，同時也需要將這幾台主機的網路埠 **MAC** 位址填入。
7. 完成這些設定之後記得要按 **[Apply]** 鍵，將這些參數寫入。

Basic Subnet				
+				
Subnet Detail				
Subnet Type		Subnet in WAN and DMZ		
+ - ↑ ↓	IP(s) on Localhost	+ - ↑ ↓ 211.21.30.11		
		+ - ↑ ↓ 211.21.30.12		
	IP(s) in WAN	+ - ↑ ↓ 211.21.30.13		
		+ - ↑ ↓ 211.21.30.9		
	Netmask		255.255.255.248	
	DMZ Port		Port5	
Enable DHCP		<input checked="" type="checkbox"/>		
DHCP Range		+ Starting Address Ending Address		
Static Mapping		+ MAC Address IP Address		

圖 1.5 Basic Subnet 基本設定

完成這些設定基本上 WAN 的網路環境已經設定完成，接下來就要進入 LAN 的設定。

1.5.2 LAN 介面基本設定

同樣在[System]→[Networking Setting]功能畫面下選擇[LAN Private Subnet] (區域網路私有子網路)功能，進入設置區域網路(LAN)之設定畫面。區域網路 (LAN) 連線是指接入本地網路的部分，即內部網路。通常會在區域網路中使用大量的私用 IP 位址，在此項設定中需要設置供內部網路使用的 IP 位址。

由於 AscenLink 的 DMZ 介面具有 Public IP Pass Through 的功能，因此這個範例中連線於 DMZ 區域的主機設定一個 Public IP，其封包將以透通的方式穿過 AscenLink 直接與 WAN 進行通訊。

現在剩下的工作只是設定 LAN 介面的 IP 位址。範例中 LAN 介面的 IP 位址為 192.168.100.254，子網路遮罩為 255.255.255.0，這兩項資料分別填入 [IP(s) on localhost] 以及 [Netmask] 這兩個欄位。

如果當 LAN 的使用者存取虛擬伺服器的 WAN IP 位址時，為避免使用者的封包繞過 AscenLink 直接送到內部的伺服器，可以啟用“虛擬伺服器位址轉換”。

如果 LAN 的電腦是以 AscenLink 為 DHCP Server，動態分配 IP 位址，您可以將 DHCP 功能 Enable，然後設定 DNS Server (功能變數名稱伺服器)地址。一般網路環境中多會指定網域名稱伺服器，作為查詢地址之用。DNS Server 可以放置在 AscenLink 所在的局域網路內，必須是 AscenLink 所能與之建立通訊的位址。接下來填入要分配給使用者端之 IP 位址範圍。如果有些主機是用固定 IP 的，則須在 Static Mapping 這個欄位填入指定的 IP，同時也需要將這幾台主機的網路介面 MAC 位址填入。

同樣的當完成設定後，要記得按下 [Apply] 鍵，將這些參數寫入記憶體中。完成設定的畫面請參考下圖。

Basic Subnet				
+				
+ - ↑ ↓	Subnet Detail			
	IP(s) on Localhost	+	192.168.100.254	
	Netmask	255.255.255.0		
	LAN Port	Port4		
	NAT Subnet for VS	<input checked="" type="checkbox"/>		
	Enable DHCP	<input checked="" type="checkbox"/>		
	Domain Name Server	10.17.0.3		
	Domain Name Suffix	ALL		
	DHCP Range	+	Starting Address	Ending Address
		+ - ↑ ↓	192.168.100.175	192.168.100.199
	Static Mapping	+	MAC Address	IP Address
		+ - ↑ ↓	00:10:a4:e6:21:18	192.168.100.103
+ - ↑ ↓		00:50:22:00:b5:6f	192.168.100.169	

圖 1.6 Basic Subnet 完成設定

1.6 典型多廣域網路連線網路架構

AscenLink 使用在多條對外連線的網路架構下更能發揮功效，我們在下一個範例中，將討論兩條對外連線的網路架構設定。以下圖為例，WAN1 及 WAN2 介面分別連線至兩個 ISP (網際網路服務提供廠商)。這兩個網路介面使用公開的 IP 位址；LAN 介面使用私有 IP 而將 AscenLink 設定為 Gateway (閘道)，DMZ 介面則使用私有 IP 成為額外的另一個 Gateway。此時內部網路上的主機 (例如使用 IP 位址 192.168.0.100 及 192.168.10.200 的主機) 將利用 NAT (網路位址轉換) 或網路位址及連接埠轉換 (NAPT, Network Address/Port Translation) 功能，經由 WAN 網路介面連線到 Internet。

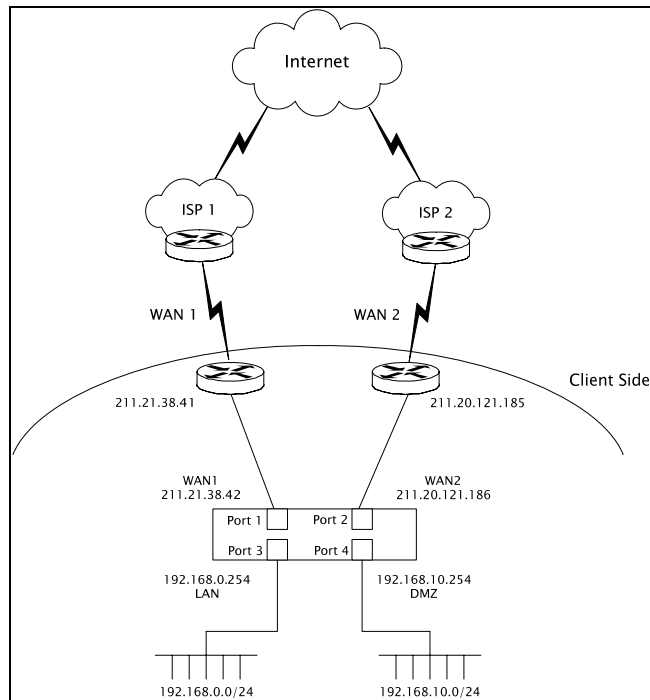


圖 1.7 多廣域網路連線網路架構

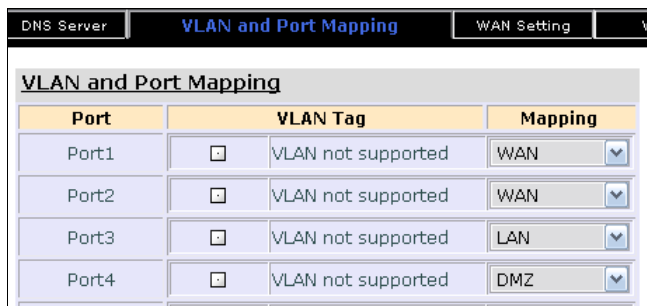
以上範例的設定會用到 **Network Setting** 功能下的四個管理畫面，分別是：

- **VLAN and Port Mapping** 畫面，設定 AscenLink 的網路介面
- **WAN Setting** 畫面，設定兩條對外連線的網路參數
- **WAN/DMZ Private Subnet** 畫面，設定 DMZ 介面之網路參數
- **LAN Private Subnet** 畫面，設定 LAN 介面之網路參數

您可以參照上圖所表示的各項網路介面規劃，網路參數，IP 位址分別在以上各個管理畫面中設定。結果分別如下

VLAN and Port Mapping 設定內容

- Port1 WAN
- Port2 WAN
- Port3 LAN
- Port4 DMZ



Port	VLAN Tag	Mapping
Port1	<input type="checkbox"/> VLAN not supported	WAN
Port2	<input type="checkbox"/> VLAN not supported	WAN
Port3	<input type="checkbox"/> VLAN not supported	LAN
Port4	<input type="checkbox"/> VLAN not supported	DMZ

圖 1.8 VLAN and Port Mapping 設定內容

WAN Setting

WAN Link 1 參數之設定如圖 假設為雙向 512K 頻寬，Netmask 為 255.255.255.248。

Basic Setting

Enable	<input checked="" type="checkbox"/>
WAN Type	Routing Mode
Down Stream	512 Kbps
Up Stream	512 Kbps
Default Gateway	211.21.38.41
MTU	1500
WAN Port	Port1

Basic Subnet

Subnet Detail

Subnet Type	Subnet in WAN and DMZ		
IP(s) on Localhost	<div></div>	211.21.38.42	
IP(s) in WAN	<div></div>	211.21.38.41	
Netmask	255.255.255.248		
DMZ Port	Port4		
Enable DHCP	<input checked="" type="checkbox"/>		
DHCP Range	<div></div>	Starting Address	Ending Address
Static Mapping	<div></div>	MAC Address	IP Address

圖 1.9 WAN Link 1 參數之設定

類似的設定方法來設定 WAN Link 2

Basic Setting	
Enable	<input checked="" type="checkbox"/>
WAN Type	Routing Mode
Down Stream	512 Kbps
Up Stream	512 Kbps
Default Gateway	211.20.121.185
MTU	1500
WAN Port	Port2

Basic Subnet		
+		
+ - ↑ ↓	Subnet Detail	
	Subnet Type	Subnet in WAN and DMZ
	IP(s) on Localhost	+ 211.20.121.186
	IP(s) in WAN	+ 211.20.121.185
	Netmask	255.255.255.248
	DMZ Port	Port4
	Enable DHCP	<input checked="" type="checkbox"/>
	DHCP Range	+ Starting Address Ending Address
	Static Mapping	+ MAC Address IP Address

圖 1.10 WAN Link 2 參數之設定

WAN/DMZ Private Subnet

這部份主要是設定 DMZ 介面之參數。在這個範例中 DMZ 介面設定私有 IP，因此對連線在 DMZ 的網路而言，DMZ 介面是其 Gateway。

Basic Subnet

+

+

-

↑

↓

Subnet Detail

Subnet Type

Subnet in DMZ

IP(s) on Localhost

+

192.168.10.254

Netmask

255.255.255.0

DMZ Port

Port4

Enable DHCP

☐

圖 1.11 DMZ Private Subnet 參數之設定

LAN Private Subnet

最後是有關 LAN 介面設定。下圖設定結果表示啓用 DHCP 功能，分配 IP 位址給 LAN 區域內的主機。

Basic Subnet			
+			
Subnet Detail			
IP(s) on Localhost	+	192.168.0.254	
Netmask	255.255.255.0		
LAN Port	Port4		
NAT Subnet for VS	<input checked="" type="checkbox"/>		
Enable DHCP	<input checked="" type="checkbox"/>		
Domain Name Server	10.17.0.3		
Domain Name Suffix	ALL		
DHCP Range	+	Starting Address	Ending Address
	+ - ↑ ↓	192.168.0.0	192.168.0.24
Static Mapping	+	MAC Address	IP Address

圖 1.12 LAN Private Subnet 設定

1.7 Public IP-Address Pass-Through

公開 IP 位址穿越的優勢在於不需變更現有的網路設定，對於內部網路中同時使用私有和公開 IP 位址時，使用者只需將具有公開 IP 位址的設備或網路區段建置在 DMZ 區即可，不需另外在 AscenLink 設定中做額外調整。

例如下圖範例，放置在 DMZ 區的主機設定一個公開 IP 位址，211.21.38.43 和 WAN 1 Port 屬於同一網路區段，因此公開 IP 穿透的功能，意味著 Port1 和 Port 4 是透過相連。用虛線表示兩個網路埠其實相連。因此這一台放置在 DMZ 的主機的 Gateway 為 WAN1 Port 所設定的 Gateway IP 位址。

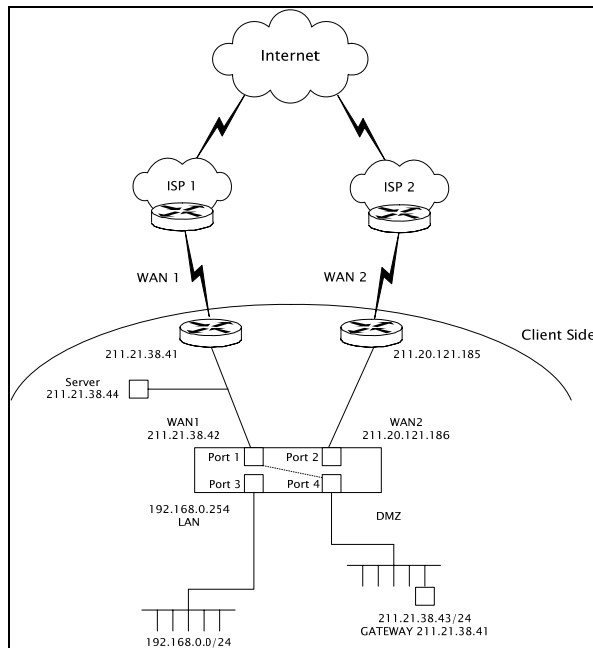


圖 1.13 Public IP-Address Pass-Through 網路架構法

1.7.1 AscenLink 和現有防火牆配合使用

對於已經安裝防火牆的網路環境，可將防火牆安裝在 AscenLink 的 DMZ 介面，完全不用更改設定；AscenLink 也適用於防火牆上已設定公開及私用位址或子網區段的環境。

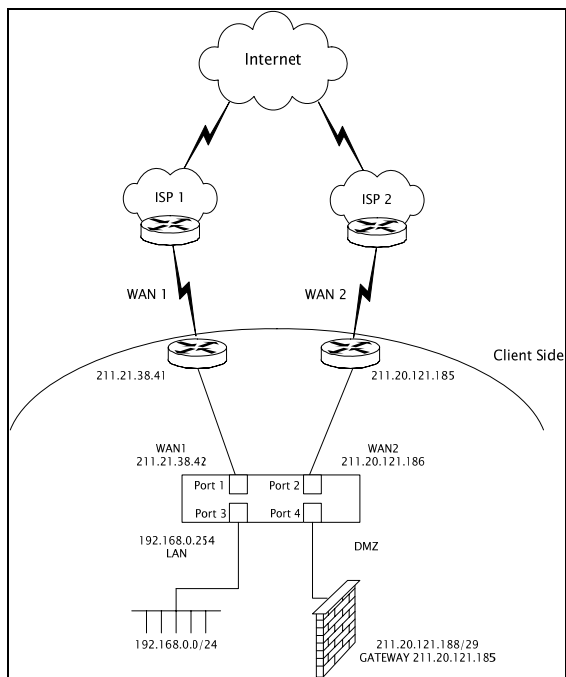


圖 1.14 AscenLink 和防火牆配合使用

1.8 硬體安裝須注意事項

1.8.1 如何安裝於機架上

AscenLink 出貨時在包裝配件中，附有機架配件，方便使用者將機器安裝在標準工業機架上。避免將螺牙鎖壞，確實地設置於標準機架上，請使用內附的配件及螺絲，並依照圖 1.15 所示的方式施工。

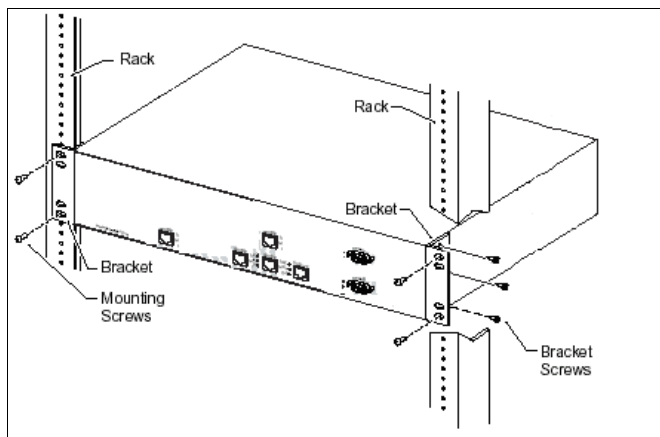


圖 1.15 於標準機架上安裝 AscenLink

1.8.2 AscenLink 與其他網路設備連線的線材規格

依據網路環境的不同，AscenLink 可能需要同時使用直連式 (Straight-Through) 網線和跳接式 (Cross-Over) 網線，如表一所示。

WAN 或 LAN 連線設備	線序
Router (路由器)	跳接式網線
Firewall (防火牆)	跳接式網線
Server (伺服器)	跳接式網線
Hub (集線器)	直連式網線
Switch (交換器)	直連式網線

表 1.4 AscenLink 與其他網路設備連線之線路型態

1.9 AscenLink HA 模式下的安裝及 HA 設定方式

1.9.1 AscenLink HA(High Availability)模式的安裝方法

兩部 AscenLink 一起上線工作時，可設定成高可用性 (HA, High Availability) 模式雙機備援。

這樣的架構，讓兩台 AscenLink 互為備援。其中一台稱之為 **Master**，即是平時上線工作的主機，另一台稱之為 **Slave**，即是平時處於備援狀態的副機。

單一 AscenLink 已內建良好的容錯機制，作業系統 (OS, Operating System) 本身及所有的控制程式都儲存在快閃記憶體 (Flash Memory) 中，不必擔心意外的斷電會造成系統損壞。

但是當網路環境必須提供關鍵任務 (Mission-Critical) 所需要的不間斷服務 (Non-Stop Service) 時，高可用性的設定方式，將成為不可或缺的必備功能；AscenLink 提供了雙機備援的高可用性方案，實現真正流量備援容錯機制。

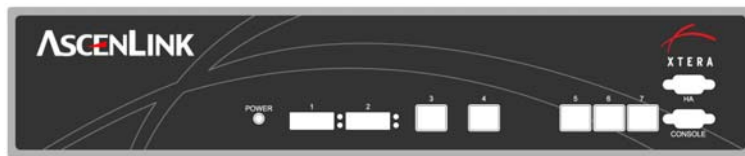


圖 1.16 AscenLink 的高可用性連接埠之設定

使用雙機備援的設定時，AscenLink 採用簡化的直覺式連線，只需使用一條可以對接的 9-PIN RS-232 序列埠連線(Null Modem Cable)，分別連線兩台 AscenLink 的 HA 連接埠即可。Null Modem Cable 是設備出貨的標準配備之一。

1.9.2 HA 的設定方式

1. HA 實施環境

AscenLink HA 雙機備援提供系統熱備援功能。當兩台都正常設定時，第一台主機處於工作狀態，而另一台處於待命狀態；主機因為故障或斷電而停機時，副機會自動啟動 HA 功能，繼續執行路由政策和流量管理的控制動作，保障關鍵任務的線路正常。

2. HA 啟動設定

- 首先，建置第一台 **AscenLink Master** 主機於目前網路中，並確定工作方式正常。
- 其次，將第二台 **AscenLink Slave** 副機之 HA 埠用 9-pin 的串行埠連結線與主機連線。開啓副機的電源。
- 啟動成功後，主機發出四聲 “Beep” 聲，副機發出三聲 “Beep” 聲，同時在主機的系統設定頁面上可看到副機目前之狀態 (Peer Information)。
- 當主機 (Master) 發生故障停止工作時，副機 (Slave) 將在發出一聲 “Beep” 聲的同時自動取代主機的任務，繼續維持網路的工作。

註：

1. 連結線拔掉，會引起不可預期的錯誤。
2. 當 Master 主機找到 Slave 副機後，系統即有 HA 的功能。

目錄

第二章 System(系統)功能表	2-6
2.1 Summary(系統資訊).....	2-7
2.2 Network Setting (網路設定)	2-10
2.2.1 DNS Server(網域名稱伺服器)子功能.....	2-12
2.2.2 VLAN and Port Mapping(VLAN 與網路介面對應)子功能.....	2-14
2.2.3 WAN Setting(廣域網路設定)子功能	2-22
2.2.4 WAN/DMZ Private Subnet(廣域網路/隔離區私有子網路)子功能	2-42
2.2.5 LAN Private Subnet 子功能(區域網路私有子網路)	2-54
2.3 WAN Link Health Detection (廣域網路連線狀態偵測)	2-62
2.4 Optimum Route Detection (最佳路徑偵測)	2-64
2.5 Port Speed/Duplex Setting (網路介面傳輸模式設定).....	2-67
2.6 Backup Line Setting (備援線設定)	2-69
2.7 IP Grouping (IP 群組設定)	2-71
2.8 Service Grouping (網路服務群組設定).....	2-73
2.9 Busyhour Setting (尖峰時段設定)	2-75
2.10 Diagnostic Tools (網路診斷工具)	2-78
2.11 Date/Time (系統時間).....	2-83
2.12 Administration (系統管理)	2-84

圖目錄

圖 2.1	System 功能表.....	2-6
圖 2.2	System/Summary 所處位置	2-7
圖 2.3	System/Network Setting 功能所處位置與其子功能	2-10
圖 2.4	System/Network Setting/DNS Server 功能所處位置.....	2-12
圖 2.5	System/Network Setting/VLAN and Port Mapping 功能所處位置	2-14
圖 2.6	VLAN 與 AscenLink 的配合使用	2-15
圖 2.7	備援 LAN 及備援 DMZ 埠 範例 1 網路架構.....	2-18
圖 2.8	備援 LAN 及備援 DMZ 埠 範例 1 埠設定	2-19
圖 2.9	備援 LAN 及備援 DMZ 埠 範例 2 網路架構.....	2-20
圖 2.10	備援 LAN 及備援 DMZ 埠 範例 2 埠設定－VLAN 與埠映射部分.....	2-21
圖 2.11	備援 LAN 及備援 DMZ 埠 範例 2 埠設定－LAN 私有子網部分	2-21
圖 2.12	System/Network Setting/WAN Setting 功能所處位置.....	2-22
圖 2.13	WAN Setting 基本設定	2-23
圖 2.14	Basic Subnet 中 Subnet 類型.....	2-25
圖 2.15	Static Routing Subnet 中 Subnet 類型.....	2-25
圖 2.16	Basic Subnet Mode 下 Subnet in WAN 之架構	2-26
圖 2.17	Basic Subnet 模式下有關 Subnet in WAN 的架構設定.....	2-27
圖 2.18	Basic Subnet 模式 Subnet in DMZ 之網路架構圖	2-28
圖 2.19	Basic Subnet 中 Subnet Detail 中有關 DMZ 之設定.....	2-29
圖 2.20	Basic Subnet 模式 Subnet in WAN and DMZ 之網路架構圖	2-30
圖 2.21	Basic Subnet 模式下有關 Subnet in WAN and DMZ 的架構設定.....	2-31
圖 2.22	Basic Subnet 模式下 Subnet on Localhost 之網路架構圖.....	2-32
圖 2.23	Basic Subnet 模式下有關 Subnet on Localhost 的架構設定	2-32
圖 2.24	Static Routing Subnet 模式下 Subnet in WAN 架構圖	2-33
圖 2.25	Static Routing Subnet 模式下有關 Subnet in WAN 架構的設定	2-33
圖 2.26	Static Routing Subnet 模式下 Subnet in DMZ 之架構圖	2-34

圖 2.27	Static Routing Subnet 模式下有關 Subnet in DMZ 架構的設定	2-34
圖 2.28	Bridge Mode: One Static IP 網路架構圖	2-35
圖 2.29	Bridge Mode: One Static IP 的 Basic Setting 設定	2-36
圖 2.30	Bridge Mode: Multiple Static IP 網路架構圖	2-38
圖 2.31	Bridge Mode: Multiple Static IP 下，Basic Setting 設定	2-39
圖 2.32	Bridge Mode: PPPoE 下，Basic Setting 設定	2-40
圖 2.33	Bridge Mode: DHCP Client 下，Basic Setting 設定	2-41
圖 2.34	System/Network Setting/WAN/DMZ Private Subnet 子功能位置	2-42
圖 2.35	WAN/DMZ Private Subnet 中 Subnet 種類	2-43
圖 2.36	Static Routing Subnet 中 Subnet 種類	2-43
圖 2.37	Basic Subnet 模式之 Subnet in WAN 網路架構圖	2-44
圖 2.38	Basic Subnet 模式下有關 Subnet in WAN 的架構設定	2-45
圖 2.39	Basic Subnet 模式 Subnet in DMZ 之網路架構圖	2-46
圖 2.40	Basic Subnet 模式 Subnet in DMZ 之架構設定	2-47
圖 2.41	Basic Subnet 模式 Subnet in WAN/DMZ 之網路架構圖	2-48
圖 2.42	Basic Subnet 模式下有關 Subnet in WAN and DMZ 的架構設定	2-49
圖 2.43	Basic Subnet 模式 Subnet on Localhost 之網路架構圖	2-50
圖 2.44	Basic Subnet 模式下有關 Subnet in WAN and DMZ 的架構設定	2-50
圖 2.45	Static Routing Subnet 模式下 Subnet in WAN 之網路架構圖	2-51
圖 2.46	Static Routing Subnet 模式下有關 Subnet in WAN 架構的設定	2-52
圖 2.47	Static Routing Subnet 模式下 Subnet in DMZ 之網路架構圖	2-53
圖 2.48	Static Routing Subnet 模式下有關 Subnet in DMZ 架構的設定	2-53
圖 2.49	System/Network Setting/ LAN Private Subnet 功能所處位置	2-54
圖 2.50	區域網路模式下 basic 子網路之網路架構圖	2-55
圖 2.51	LAN Private Subnet/ Basic Subnet 的設定	2-56
圖 2.52	LAN Private Subnet/ RIP 的設定	2-57
圖 2.53	LAN Private Subnet/ OSPF 的設定	2-58
圖 2.54	Static Routing Subnet 網路架構圖	2-60
圖 2.55	LAN Private Subnet/ Static Routing Subnet 的設定	2-61

圖 2.56 System/WAN Link Health Detection 功能所處位置 2-62

圖 2.57 System/ Optimum Route Detection 功能所處位置 2-64

圖 2.58 System/ Duplex Setting 功能所處位置 2-67

圖 2.59 System/ Backup Line Setting 功能所處位置 2-69

圖 2.60 System/ IP Grouping 功能所處位置 2-71

圖 2.61 System/Service Grouping 功能所處位置 2-73

圖 2.62 System/ Busyhour Setting 功能所處位置 2-75

圖 2.63 Busyhour Setting 設定範例 2-77

圖 2.64 System/ Diagnostic Tools 功能所處位置 2-78

圖 2.65 Tcpcmdump 功能 2-80

圖 2.66 System/ Date/Time 功能所處位置 2-83

圖 2.67 System/ Administration 功能所處位置 2-84

表目錄

表 2.1	System Information 信息列表	2-8
表 2.2	Peer Information 信息列表	2-8
表 2.3	License Information 信息列表	2-9
表 2.4	VLAN Tag 及對應 AscenLink 網路介面的位置	2-16
表 2.5	備援 LAN 及備援 DMZ 欄位說明	2-17
表 2.6	Routing Mode 下 Basic Setting 表格欄位說明	2-24
表 2.7	OSPF 路由協定設定	2-59
表 2.8	動態偵測設定欄位說明	2-65
表 2.9	靜態 IP 列表偵測設定欄位說明	2-66
表 2.10	網路介面傳輸模式設定欄位說明	2-68
表 2.11	Threshold 欄位說明	2-70
表 2.12	Backup Line Rule 欄位說明表	2-70
表 2.13	IP Grouping 欄位說明表	2-72
表 2.14	Rules Setting 欄位說明表	2-72
表 2.15	Service Grouping 欄位說明表	2-74
表 2.16	Busyhour Setting 欄位說明表	2-76
表 2.17	Administor 密碼管理	2-85
表 2.18	Monitor 密碼管理	2-85
表 2.19	AscenLink 保留埠	2-86

第二章 System(系統)功能表

本章將進一步的解釋 System 功能表下各項功能的使用，爲了讓使用者對整個系統有個清楚的輪廓，先完整的列出功能表，以及各個功能表下的子功能。同時也提供範例，讓使用者對功能的使用和設定的觀念更加深刻。

在介紹網頁管理系統功能時以英文爲主，會附加中文說明。

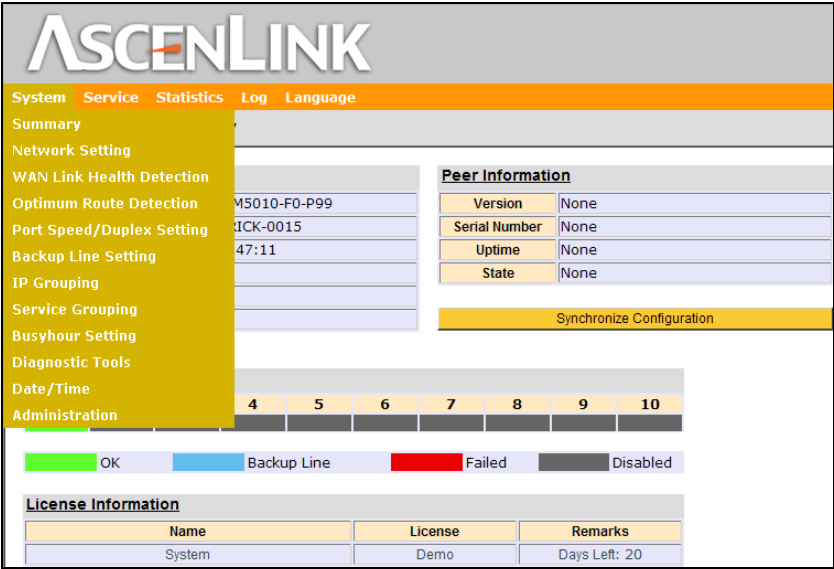


圖 2.1 System 功能表

2.1 Summary(系統資訊)

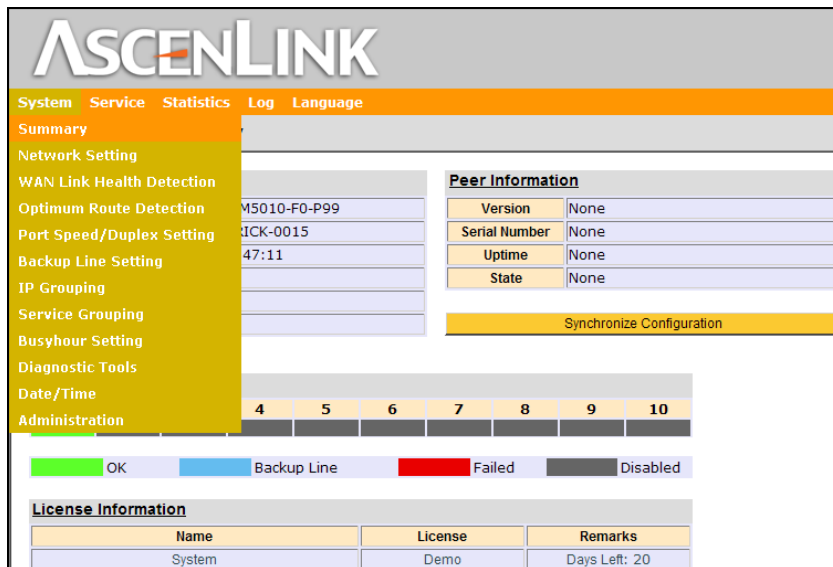


圖 2.2 System/Summary 所處位置

[Summary]這項功能位於 [System] 功能表之下，主要是提供 AscenLink 系統管理者，可以很快掌握系統資訊。當您登入時，[Summary] 就是網頁管理系統之首頁。

[Summary] 提供下列資訊，System Information，Peer Information，WAN Link State，License Information 等信息。如果您的 AscenLink 是執行 HA 模式，也就是兩台 AscenLink 系統，一台是 Master，一台是 Slave，這是一種備援設計，在前一章已提過這樣的操作模式。如果 AscenLink 在 HA 模式下操作，才會出現 Peer Information 這類資訊。

System Information 及 Peer Information 所呈現的資訊意義

資訊類別	顯示專案	資訊意義
System Information	Version	本台 AscenLink 的版本
	Serial Number	本台 AscenLink 的序列號
	Up Time	從開機到現在的時間
	Connections	目前總共的連線數
	CPU Usage%	CPU 的負載量
	Packets/Second	每秒處理的封包數

表 2.1 System Information 信息列表

資訊類別	顯示專案	資訊意義
Peer Information	Version	HA 模式下，扮演 Slave 的 AscenLink 的版本
	Serial Number	序列號
	Up Time	從開機到現在的時間
	State	Slave

表 2.2 Peer Information 信息列表

註：Connections 在啟動 AscenLink 時可能會出現約略 100 多的數量，這是由於 AscenLink 送出 ICMP 封包測試網路，稍後會恢復成正常狀況。

工作在 HA 模式下時，在 Master 的 Summary 頁面中點一下 [Synchronize Configuration]，AscenLink 可以強制傳輸 AscenLink 的設定至 Slave 中，(Master 在每次改變任何設定時也會自動同步 Slave 的設定值)，只有 Administrator 才能執行此動作。

WAN Link State 呈現廣域網路連線的狀態

這個部份是呈現廣域網路的連線狀態，是以顏色來區別連線狀態。

AscenLink 會因為型號不同，可以允許連線的 WAN Link 數目也有所不同。在畫面上會呈現這個型號允許使用的 WAN Link 數目。在畫面中利用不同顏色來表示 WAN Link 之連線狀態。圖示為：

- 綠色：目前正在使用的廣域網路連線。
- 藍色：設定為備援線路。
- 紅色：線路故障。
- 灰色：目前沒有使用或定義的網路介面。

License Information 呈現授權狀態

資訊類別	顯示專案	資訊意義
License Information	Name (名稱)	顯示授權的種類名稱
	License (授權)	顯示目前的授權狀態
	Remarks (備註)	顯示試用版的剩餘使用日期

表 2.3 License Information 信息列表

2.2 Network Setting (網路設定)

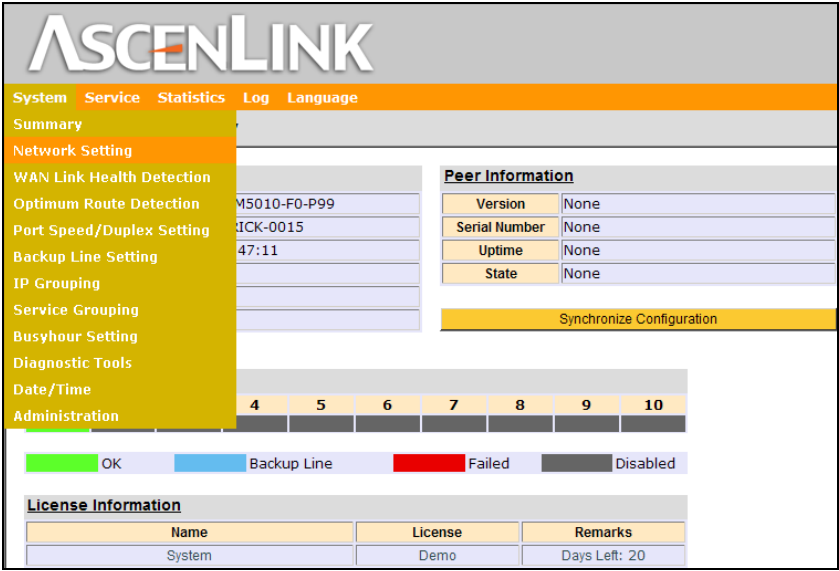


圖 2.3 System/Network Setting 功能所處位置與其子功能

[Network Setting] 功能是相當重要的部份，WAN/LAN 的設定都在這個管理介面中完成。

[Network Setting] 共有五項子功能可供使用，分別是：

1. DNS Server (網域名稱伺服器)

指定 AscenLink 設備所在網路下的名稱伺服器位址。

2. VLAN and Port Mapping (VLAN 與網路介面對應)

這個功能可以讓網路的系統管理者設定 AscenLink 網路介面的使用方式，如用於 WAN、LAN 或是 DMZ。也可以搭配 VLAN Switch (Virtual LAN Switch)的使用，將 AscenLink 的網路介面對應至 VLAN Switch 的介面。在大型網路架構下 VLAN Switch 可以切割不同的子網路，這些不同的子網路都可以經由 AscenLink 進行資料交換，也可以搭配 AscenLink 的使用，設定 VLAN Tag，讓 VLAN Switch 的網路介面執行不同的功能，如 DMZ、WAN 或是 LAN。

3. WAN Setting (廣域網路設定)

這個功能下提供各個 WAN 連線所需的各項參數設定。

4. WAN/DMA Private Subnet (廣域網路/隔離區 私有子網路)

這個功能提供在 WAN 端或 DMZ 端有私有子網路的網路架構下，各項參數的設定。

5. LAN Private Subnet (區域網路私有子網路)

這個功能提供區域網路下各項參數的設定。

2.2.1 DNS Server(網域名稱伺服器)子功能

The screenshot shows the AscenLink web interface. At the top, there's a navigation bar with 'System', 'Service', 'Statistics', 'Log', and 'Language'. The user is logged in as 'Administrator@10.13.2.0'. The main title is 'System/Network Settings'. Below this, there are tabs for 'DNS Server' (highlighted), 'VLAN and Port Mapping', 'WAN Settings', 'WAN/DMZ Private Subnet', and 'LAN Private Subnet'. The 'DNS Server' section contains three main fields: 'Hostname' (set to 'AscenLink'), 'Domain Name Server' (with a 'Server List' table containing '202.99.96.68' and '10.13.0.3'), and 'Domain Name Suffix' (with a 'Suffix List' table containing 'www.a.cn').

Domain Name Server	
+	Server List
+	202.99.96.68
+	10.13.0.3

Domain Name Suffix	
+	Suffix List
+	www.a.cn

圖 2.4 System/Network Setting/DNS Server 功能所處位置

這項功能是設定 AscenLink 所使用的 DNS Server 的 IP 位址。AscenLink 系統在上線使用到下列功能時會需要查詢 DNS Server，以獲得主機實際 IP 位址，如果這個欄位不指定 DNS Server IP，並不會影響系統工作。有兩種設定方式：一種是 DNS 伺服器的 IP 位址，另一種是 DNS 的域名后綴。

AscenLink 會用到 DNS 伺服器的功能分別為以下五種，這些功能或指令為：

- System/Diagnostic Tools 中的 Ping 與尋徑。
- Service/Cache 中的 Cache Server 設定。
- Log/Control 中的 SMTP 及 FTP Server 設定。
- Log/Notification 中的 SMTP Server 設定。
- Serial Console 中的 ping 與尋徑指令。

2.2.2 VLAN and Port Mapping(VLAN 與網路介面對應) 子功能

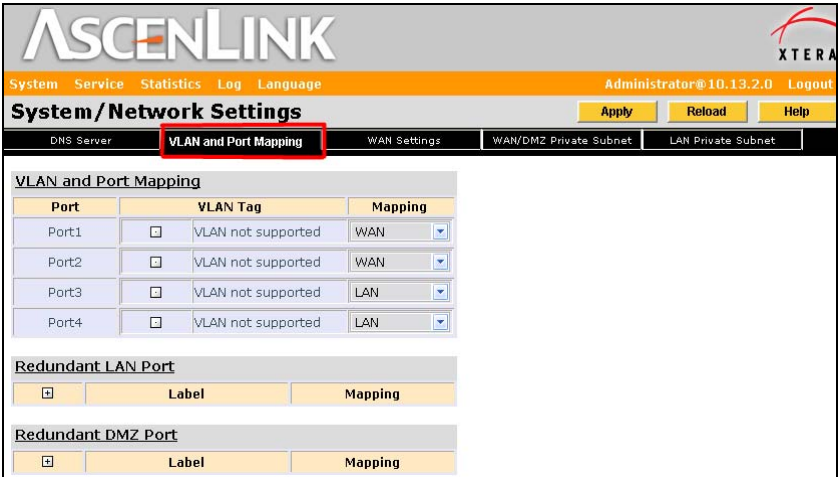


圖 2.5 System/Network Setting/VLAN and Port Mapping 功能所處位置

VLAN and Port Mapping 設定

AscenLink 支援 VLAN，使用 802.1q 的封包，但不支援 Cisco 的 ISL。當 AscenLink 要加入網路上線使用時，須先對網路介面預作規劃，我們在前一章提到，例如 AscenLink 的 Port 1 要當作 WAN 介面，則需要在這個功能畫面下進行設定。

為了解釋如何配合 VLAN Switch 的使用，請看下頁的網路架構：

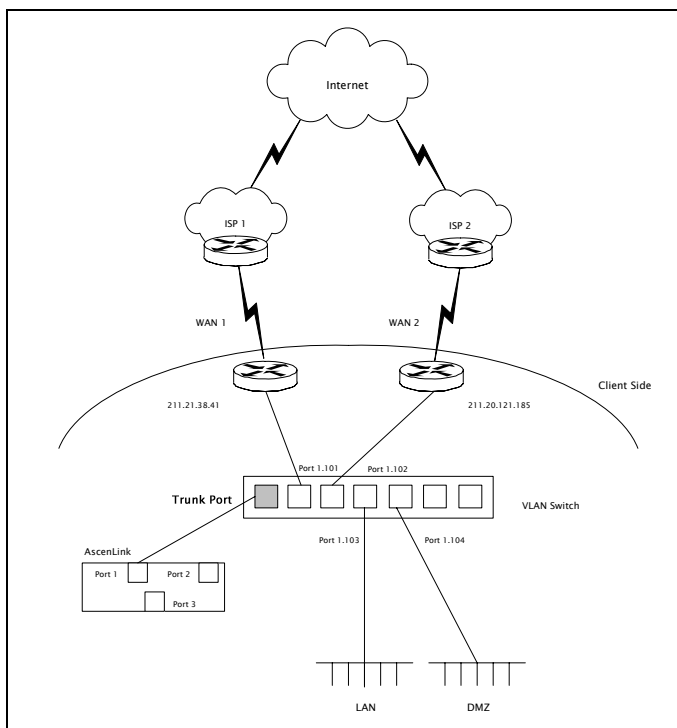


圖 2.6 VLAN 與 AscenLink 的配合使用

在這個範例中 AscenLink Port 1 連線到 VLAN Switch。在這樣的網路應用架構下，需要將 VLAN Tag 設定到 VLAN tag setting 這個欄位，同時設定這個 tag 所對應的網路介面功能。在這個例子中：

tag 101 對應為 WAN

tag 102 對應為 WAN

tag 103 對應為 LAN

tag 104 對應為 DMZ

這樣的設定後 AscenLink 的 Port 1 將不再接受非 VLAN Tag 的封包。VLAN Switch 上標號為 101 和 102 的網路介面，將直接連線 WAN 線路，而內部區域網路的電腦就連線到標號為 103 的 VLAN Switch 介面，DMZ 的電腦就連線於標號 104 的 VLAN Switch 介面。這樣的應用 AscenLink 扮演類似路由器的角色，DMZ 的電腦可設定 Public IP，封包直接透過進出廣域網路。

除了設定 AscenLink 的網路介面外，您也需要至 VLAN Switch 的管理功能下，執行各個 Tag 設定，以及 IP 位址設置。

Port	VLAN tag setting	Mapping
Port 1	101	WAN
	102	WAN
	103	LAN
	104	DMZ
Port 2	no VLAN tag	None
Port 3	no VLAN tag	None
Port 4	no VLAN tag	None

表 2.4 VLAN Tag 及對應 AscenLink 網路介面的位置

備援 LAN 埠及備援 DMZ 埠

當 AscenLink 工作在 HA 狀態下時，若沒有備援 LAN 及 DMZ 埠，則 LAN 及 DMZ 網路中與 AscenLink 的 LAN 和 DMZ 埠間的連結線路仍然存在單點故障（single point of failure）隱患。為解決這個問題，AscenLink 在採用了備援 LAN 及 DMZ 埠。這樣就可以解決該隱患。AscenLink 的備援 LAN 及 DMZ 採用橋接的方式，支援 Spanning Tree，且優先權設置為最高（0xffff），這樣在通常的情況下，可以避免資料封包形成環路造成的網路癱瘓。

欄位	值	說明
Redundant LAN Port (備援 LAN 埠)	Lable (標識)	給組合後的備援 LAN 埠做一個相應的標識。可使用的符號為“0-9 a-z A-Z .-_"例如：12xyz.b_d-xxx。在有關 LAN 的設定部分會出現形如：Bridge 12xyz.b_d-xxx 的選項。例如在“LAN Private Subnet”中設定 bridge-LAN 的 IP 為：192.168.0.1
	Mapping (映射)	選擇相應的兩個 LAN 埠，設置為備援 LAN。例如，選擇 Port2 和 Port3 為備援 LAN。
Redundant DMZ Port (備援 DMZ 埠)	Lable (標識)	給組合後的備援 DMZ 埠做一個相應的標識。可使用的符號為“0-9 a-z A-Z .-_"例如：12xyz.b_d-xxx。在有關 DMZ 的設定部分會出現形如：Bridge 12xyz.b_d-xxx 的選項給定一個名稱，作為後面規則設定用。例如在“WAN setting”中設定 bridge-DMZ 的 IP 為：17.10.12.11
	Mapping (映射)	選擇相應的兩個 DMZ 埠，設定為備援 DMZ。例如，選擇 Port4 和 Port5 為備援 DMZ。

表 2.5 備援 LAN 及備援 DMZ 欄位說明

範例 1：

Redundant LAN / DMZ Port：Single AscenLink（備援 LAN / DMZ 埠：AscenLink 單機）

在這個範例中 AscenLink 的 Port 1 作為 WAN 埠，Port2 和 Port3 設定為備援 LAN 埠連線到 Switch1 上；Port4 和 Port5 設定為備援 DMZ 埠，連線到 Switch2 上。在這樣的網路應用架構下，當一條 LAN 或者 DMZ 區域的連線出現問題時，AscenLink 將啟用另外一條線路來保障流量的正常傳輸。

網路架構如下：

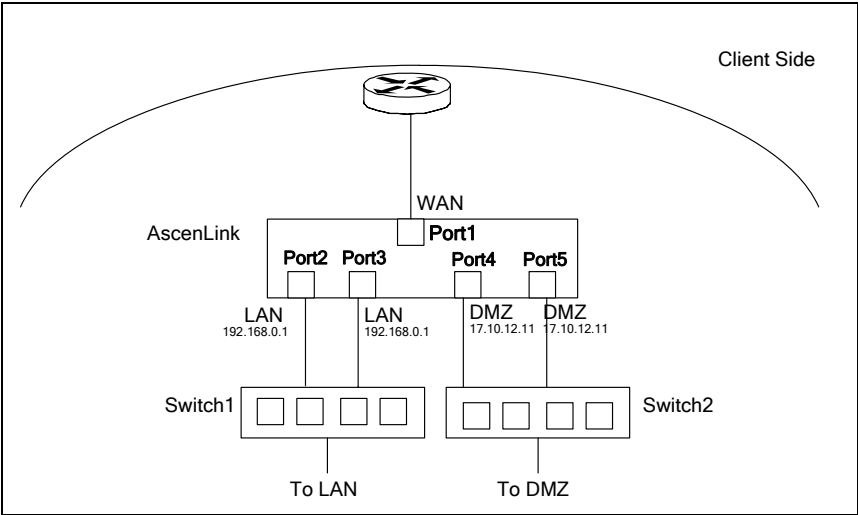


圖 2.7 備援 LAN 及備援 DMZ 埠 範例 1 網路架構

在 AscenLink 頁面的相應參數設定如下：

System/Network Setting					
DNS Server		VLAN and Port Mapping		WAN Setting	
VLAN and Port Mapping					
Port		VLAN Tag		Mapping	
Port1	<input type="checkbox"/>	VLAN not supported		WAN	▼
Port2	<input type="checkbox"/>	VLAN not supported		LAN	▼
Port3	<input type="checkbox"/>	VLAN not supported		LAN	▼
Port4	<input type="checkbox"/>	VLAN not supported		DMZ	▼
Port5	<input type="checkbox"/>	VLAN not supported		DMZ	▼
Redundant LAN Port					
<input type="checkbox"/>		Label		Mapping	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	bridge-LAN	
					Port2 ▼
					Port3 ▼
Redundant DMZ Port					
<input type="checkbox"/>		Label		Mapping	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	bridge-DMZ	
					Port4 ▼
					Port5 ▼

圖 2.8 備援 LAN 及備援 DMZ 埠 範例 1 埠設定

範例 2：

Redundant LAN / DMZ Port：AscenLink HA（備援 LAN / DMZ 埠：AscenLink HA 雙機）

在這個範例中 AscenLink 採用 HA 雙機備援，提供系統 Active / Standby 功能，實現雙機熱備。並透過備援 LAN / DMZ 埠，排除以往 AscenLink 在啓用 HA 時產生的 LAN 及 DMZ 網路中的 Single Point of Failure（單點故障）問題。

架構中 Port1、Port2 互為備援埠。

網路架構如下：

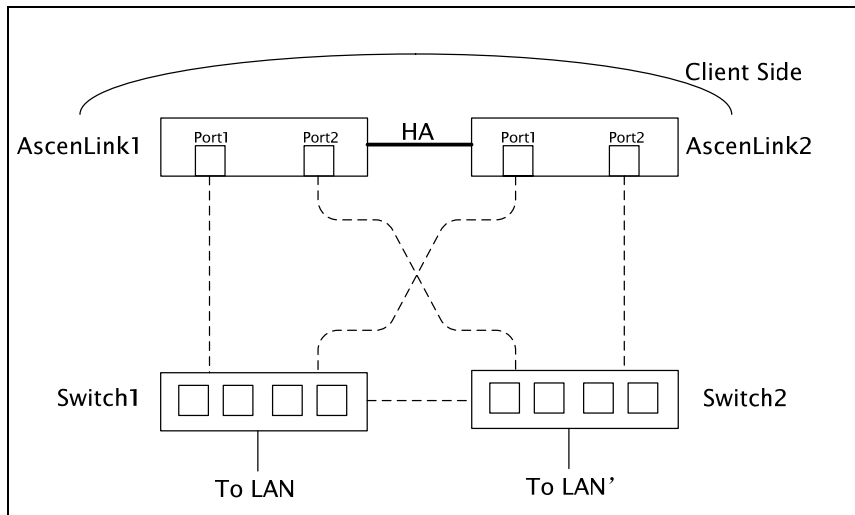


圖 2.9 備援 LAN 及備援 DMZ 埠 範例 2 網路架構

在 AscenLink 頁面的相應參數 VLAN and Port Mapping 設定如下：

System/Network Setting

DNS Server | **VLAN and Port Mapping** | WAN Setting | WAN/DMZ Private Subnet

VLAN and Port Mapping

Port	VLAN Tag	Mapping
Port1	<input type="checkbox"/> VLAN not supported	LAN
Port2	<input type="checkbox"/> VLAN not supported	LAN
Port3	<input type="checkbox"/> VLAN not supported	None
Port4	<input type="checkbox"/> VLAN not supported	None
Port5	<input type="checkbox"/> VLAN not supported	WAN

Redundant LAN Port

Label	Mapping
bridge-LAN	Port1
	Port2

Redundant DMZ Port

Label	Mapping
-------	---------

圖 2.10 備援 LAN 及備援 DMZ 埠 範例 2 埠設定－VLAN 與埠映射部分

在 AscenLink 頁面的相應參數 LAN Private Subnet 設定如下：

System/Network Setting Apply Reload Help

DNS Server | VLAN and Port Mapping | WAN Setting | WAN/DMZ Private Subnet | **LAN Private Subnet**

Basic Subnet

☐ Subnet Detail

IP(s) on Localhost ☐ 10.17.0.1

Netmask 255.255.192.0

LAN Port Bridge: Bridge-LAN

NAT Subnet for VS ☐

Enable DHCP ☐

RIP ☐

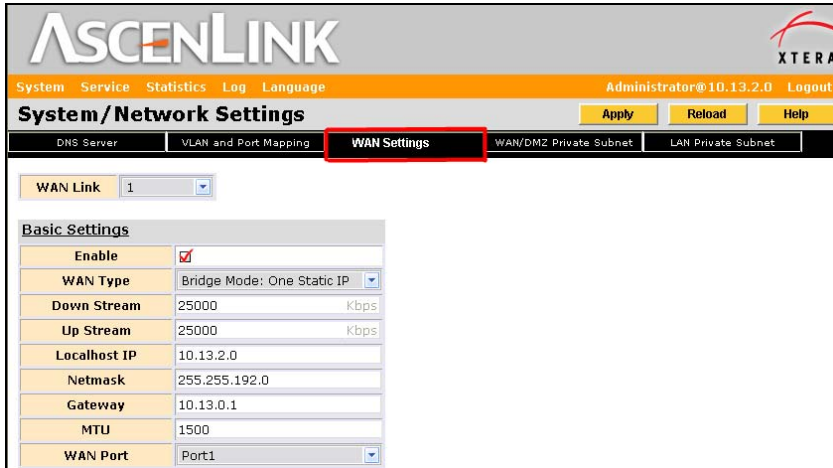
OSPF ☐

Static Routing Subnet

Network IP	Netmask	Gateway
------------	---------	---------

圖 2.11 備援 LAN 及備援 DMZ 埠 範例 2 埠設定－LAN 私有子網部分

2.2.3 WAN Setting(廣域網路設定)子功能



The screenshot displays the AscenLink web interface for WAN settings. At the top, the 'System/Network Settings' menu is visible, with 'WAN Settings' selected. Below this, the 'WAN Link' is set to '1'. The 'Basic Settings' section contains the following configuration options:

Parameter	Value
Enable	<input checked="" type="checkbox"/>
WAN Type	Bridge Mode: One Static IP
Down Stream	25000 kbps
Up Stream	25000 kbps
Localhost IP	10.13.2.0
Netmask	255.255.192.0
Gateway	10.13.0.1
MTU	1500
WAN Port	Port1

圖 2.12 System/Network Setting/WAN Setting 功能所處位置

這個子功能是設定 AscenLink 用於廣域網路介面各項參數之設定。

由於設定的參數彼此有著相關連，主要是在 WAN 的連線模式設定上。如果您是申請多條線路，那麼需要逐一設定。在這種情況下，在 WAN Link 欄位下，下拉欄位選擇要設定的線路。

實體 WAN 線路連線到 AscenLink 實體的網路介面，也需要在 Basic Setting 表格中的 WAN Port 裏設定。WAN Setting 會因為 WAN Type 的選擇不同而有所不同，AscenLink 設計的 WAN Type 共計有下列選擇：

- Routing Mode(路由模式)
- Bridge Mode: One Static IP(橋接模式:固一)
- Bridge Mode: Multiple Static IP(橋接模式:固 N)
- Bridge Mode: PPPoE(橋接模式:PPPoE)

■ Bridge Mode: DHCP Client(橋接模式:DHCP 動態配址)

Basic Setting	
Enable	<input checked="" type="checkbox"/>
WAN Type	Routing Mode Bridge Mode: One Static IP Bridge Mode: Multiple Static IP Bridge Mode: PPPoE Bridge Mode: DHCP Client
Down Stream	
Up Stream	
Default Gateway	
MTU	1500
WAN Port	Port2

圖 2.13 WAN Setting 基本設定

您會這註意到，因為選擇 WAN Type 的不同，管理設定畫面有會有所不同。我們需要有一個清楚的觀念，對 AscenLink 而言，Subnet (子網路) 可以分為兩種：

第一種是和 AscenLink 有直接連線的，您必需到 “Basic Subnet ” 這個表格中去設定。這種情況是位於同一個網路區段，不需要經由路由器來轉送封包。

第二種是要經由一台 Router (或 L3 switch)才連得到的，您必需到 “Static Routing Subnet” 表格中去設定。這種情況是規劃不同的子網路，彼此之間需要 Router 或可以規劃的交換器來轉送封包。

2.2.3.1 Routing Mode

Basic Setting

WAN Type 選擇 Routing Mode 時，在 Basic Setting 表格中須填入下列數值或參數：

欄位名稱	說明
Down Stream	此線路提供的下載速率，例如 512 (Kbps)。
Up Stream	此線路提供的上傳速率，例如 512 (Kbps)。
Default Gateway	即預設閘道位址，例如 211.21.40.254。
MTU	即設定每個數據包的大小，若一段數據過大將被分為多個包傳送
WAN Port	此為 AscenLink 連線至廣域網路端之介面。 例如選擇網路介面 3。 請註意，此介面必需事先設定為 WAN。

表 2.6 Routing Mode 下 Basic Setting 表格欄位說明

Basic Subnet 和 Static Routing Subnet 設定

接下來開始設定 Basic Subnet 和 Static Routing Subnet 表格。我們在前文已經介紹過，AscenLink 如何區分這兩種 Subnet。

在這一個管理畫面下所定義的 Subnet，都是指 Public Subnet (公有子網路)。對 Basic Subnet 而言，可以有下列類型：

- Subnet in WAN (廣域網路端的子網路)
- Subnet in DMZ (隔離區端的子網路)
- Subnet in WAN and DMZ (子網路分在廣域網路端與隔離區端兩側)
- Subnet on Localhost (本機上的子網路)

Basic Subnet	
<div> <div>+</div> <div>Subnet Detail</div> </div>	
Subnet Type	<div>Subnet in DMZ</div> <div> <div>Subnet in WAN</div> <div>Subnet in DMZ</div> <div>Subnet in WAN and DMZ</div> <div>Subnet on Localhost</div> </div>
IP(s) on Localhost	
Netmask	
DMZ Port	Port4
Enable DHCP	<input type="checkbox"/>

圖 2.14 Basic Subnet 中 Subnet 類型

我們在下文會以範例來解釋這些子網路的設定，一般而言“Subnet in WAN and DMZ”是最常使用的設定。

對 Static Routing Subnet 靜態路由子網路可為以下類型之一：

- Subnet in WAN (廣域網路端的靜態路由子網路)
- Subnet in DMZ (隔離區端的靜態路由子網路)

Static Routing Subnet				
	Subnet Type	Network IP	Netmask	Gateway
<div> <div>+</div> <div>-</div> <div>↑</div> <div>↓</div> </div>	<div>Subnet in WAN</div> <div> <div>Subnet in WAN</div> <div>Subnet in DMZ</div> </div>			

圖 2.15 Static Routing Subnet 中 Subnet 類型

Basic Subnet 模式下有關 **Subnet in WAN** 的架構設定

範例：此環境多用在 **Public Subnet** (公有子網路)的主機群放在廣域網路端。

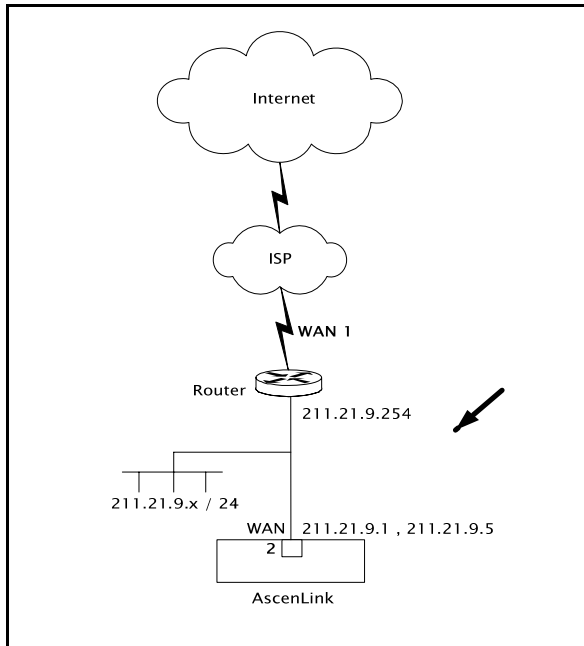


圖 2.16 Basic Subnet Mode 下 Subnet in WAN 之架構

這樣的網路架構，AscenLink 使用 Port 2 作為 WAN 介面，同時設定 IP 位址區段 211.21.9.1~211.21.9.5，要註意如果是一個網路介面設定一組連續 IP 位址，則輸入的格式為 211.21.9.1-211.21.9.5。假設 ISP 設定的子網路遮罩為 255.255.255.0，Router 的位址為 211.21.9.254，這些參數最後都需要設定在 AscenLink 的表格，如下頁：

Basic Setting	
Enable	<input checked="" type="checkbox"/>
WAN Type	Routing Mode
Down Stream	512 Kbps
Up Stream	512 Kbps
Default Gateway	211.21.9.254
MTU	1500
WAN Port	Port4

Basic Subnet							
<input data-bbox="306 616 323 638" type="button" value="+"/>							
<input data-bbox="270 730 287 753" type="button" value="+"/> <input data-bbox="297 730 314 753" type="button" value="-"/> <input data-bbox="323 730 341 753" type="button" value="↑"/> <input data-bbox="350 730 368 753" type="button" value="↓"/>	<div><div>Subnet Detail</div><table border="1"><tbody><tr><td>Subnet Type</td><td>Subnet in WAN</td></tr><tr><td>IP(s) on Localhost</td><td><input data-bbox="682 753 700 775" type="button" value="+"/> 211.21.9.1-211.21.9.5</td></tr><tr><td>Netmask</td><td>255.255.255.0</td></tr></tbody></table></div>	Subnet Type	Subnet in WAN	IP(s) on Localhost	<input data-bbox="682 753 700 775" type="button" value="+"/> 211.21.9.1-211.21.9.5	Netmask	255.255.255.0
Subnet Type	Subnet in WAN						
IP(s) on Localhost	<input data-bbox="682 753 700 775" type="button" value="+"/> 211.21.9.1-211.21.9.5						
Netmask	255.255.255.0						

圖 2.17 Basic Subnet 模式下有關 Subnet in WAN 的架構設定

Basic Subnet 模式下有關 Subnet in DMZ 的架構設定

範例：此環境多用在 Public Subnet 的主機群放在隔離區網路端。

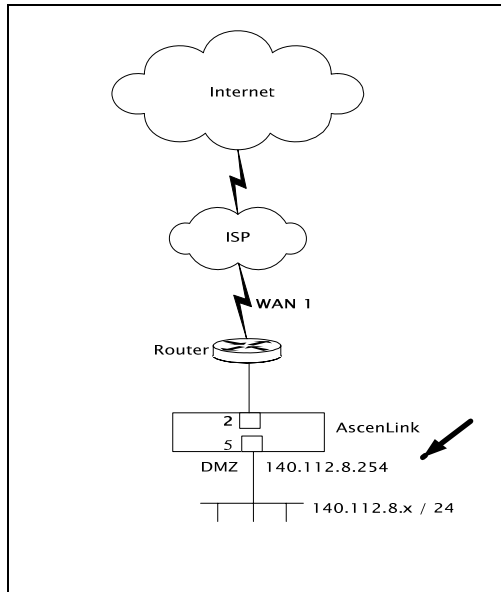


圖 2.18 Basic Subnet 模式 Subnet in DMZ 之網路架構圖

在這個架構下，主機群放在 DMZ，因此 AscenLink 的網路介面 Port 5 須設定為 DMZ，同時 DMZ 連接埠的 IP 位址設定為 140.112.8.254，於是在 DMZ 的主機群，其預設的 Gateway 就是 140.112.8.254。

如果您希望對位於 DMZ 的子網路下的主機提供 DHCP 服務，則需要啟用 DHCP (Enable DHCP)，然後在 DHCP Range 欄位，分別填入要分配的 IP 起始位址與結束位置。如果在子網路中有主機是設定固定 IP 時，則須將此 IP 填入 Static Mapping 這一系列中之 IP Address 欄，同時也須將此主機的 MAC 位址填入 MAC Address 欄中。

Basic Subnet						
<div>+</div>						
<div>+ - ↑ ↓</div>	Subnet Detail					
	Subnet Type	Subnet in DMZ				
	IP(s) on Localhost	<div>+</div> 140.112.8.254				
	Netmask	255.255.255.0				
	DMZ Port	Port5				
	Enable DHCP	<input checked="" type="checkbox"/>				
	DHCP Range	<div>+</div> <div>+ - ↑ ↓</div> <table><thead><tr><th>Starting Address</th><th>Ending Address</th></tr></thead><tbody><tr><td></td><td></td></tr></tbody></table>	Starting Address	Ending Address		
	Starting Address	Ending Address				
	Static Mapping	<div>+</div> <div>+ - ↑ ↓</div> <table><thead><tr><th>MAC Address</th><th>IP Address</th></tr></thead><tbody><tr><td></td><td></td></tr></tbody></table>	MAC Address	IP Address		
MAC Address	IP Address					

圖 2.19 Basic Subnet 中 Subnet Detail 中有關 DMZ 之設定

註：AscenLink 假設所有這個網路區段未列出的 IP 都位於 DMZ 端。

Basic Subnet 模式下有關 Subnet in WAN and DMZ 的架構設定

範例：此環境多用在 Public Subnet 的主機群同時存在於廣域網路與隔離區網路端。

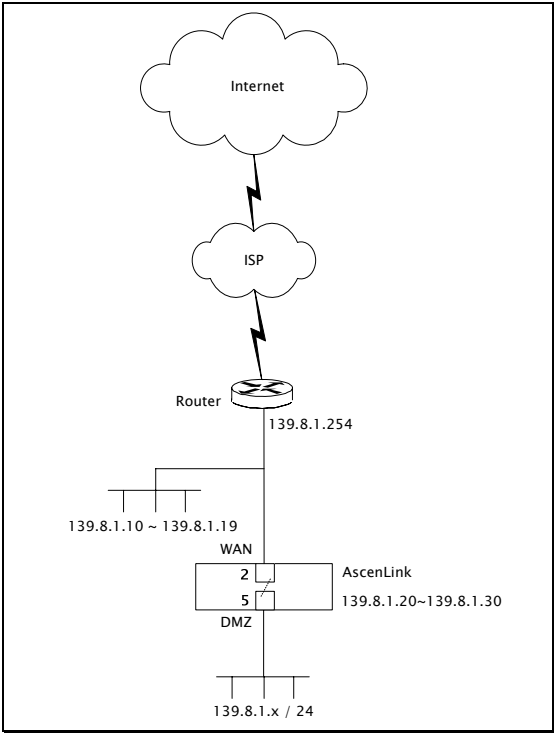


圖 2.20 Basic Subnet 模式 Subnet in WAN and DMZ 之網路架構圖

Basic Subnet		
<div>+</div> <div>Subnet Detail</div>		
Subnet Type	Subnet in WAN and DMZ	
IP(s) on Localhost	<div>+</div> <div>139.8.1.20-139.8.1.30</div>	
IP(s) in WAN	<div>+</div> <div>-</div> <div>↑</div> <div>↓</div> <div>139.8.1.10-139.8.1.19</div>	
	<div>+</div> <div>-</div> <div>↑</div> <div>↓</div> <div>139.8.1.254</div>	
Netmask	255.255.255.0	
DMZ Port	Port5	
Enable DHCP	<input checked="" type="checkbox"/>	
DHCP Range	Starting Address	Ending Address
	<div>+</div> <div>-</div> <div>↑</div> <div>↓</div>	
Static Mapping	MAC Address	IP Address
	<div>+</div> <div>-</div> <div>↑</div> <div>↓</div>	

圖 2.21 Basic Subnet 模式下有關 Subnet in WAN and DMZ 的架構設定

當您選擇 Subnet Type 為 Subnet in WAN and DMZ 時，AscenLink 假設所有這個網段未列出的 IP 都位於隔離區端。在這個範例中，除了 139.8.1.10~19，139.8.1.254 及 139.8.1.20~30 以外的 IP，AscenLink 會將 139.8.1.X 的所有 IP 設定在 DMZ 裏，做公開 IP 穿透(Public-IP Pass Through)。

如果您希望對位於 DMZ 的子網路下的主機提供 DHCP 服務，則需要啓用 DHCP (Enable DHCP)，然後在 Starting Address 及 Ending Address 分別填入要分配的 IP 起始位址與結束位址。如果在子網路中有主機是設定固定 IP 時，則須將此 IP 填入 Static Mapping 這一系列中之 IP Address 欄，同時也須將此主機的 MAC 位址填入 MAC Address 欄中。

Port2 與 Port5 之間用虛線連線表示是同一個 Subnet 139.8.1.X 的網段同時橫跨 WAN (Port2)及 DMZ (Port5)之間，AscenLink 會利用 Proxy ARP 的技術將這個 Subnet 連起來。

139.8.1.254 這個 IP 可能在之前已經設成 default gateway，所以應該是在廣域網路端。不過基於讓管理者對於整體 UI 操作介面清楚易讀，這裏仍要向您再說明一次 139.8.1.254 是位於廣域網路端。

Basic Subnet 模式下有關於 Subnet on Localhost 的架構設定

範例：此種模式是在 AscenLink 上指定整段子網路，以便 Virtual Server 使用。

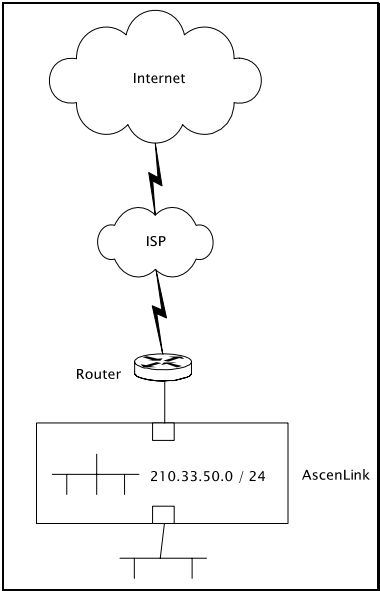


圖 2.22 Basic Subnet 模式下 Subnet on Localhost 之網路架構圖

Basic Subnet

Subnet Detail

Subnet Type

Subnet on Localhost

Network IP

210.33.50.0

Netmask

255.255.255.0

圖 2.23 Basic Subnet 模式下有關於 Subnet on Localhost 的架構設定

這個範例中將整個子網路設定給 Virtual Server 使用。在 Network IP 欄位中，將子網路 IP 填入，子網路遮罩填入 255.255.255.0。

Static Routing Subnet 模式下有關 Subnet in WAN 架構的設定

當面對公有靜態路由子網路於廣域網路端的情況時，表示有一個子網路位於廣域網路端，不直接連線到 AscenLink，因此需要路由器來轉送封包。範例中 139.3.1.x 的子網路位於廣域網路端，連線于路由器，另一個子網路 140.4.1.x 也出現在廣域網路，但直接連線到 AscenLink，因此需要對靜態路由子網路進行設定。這種情況在實際網路架構中，其實比較少見。

範例：在廣域網路中設定一個公有子網路 139.3.1.x，連線到路由器，IP 為 140.4.1.254。

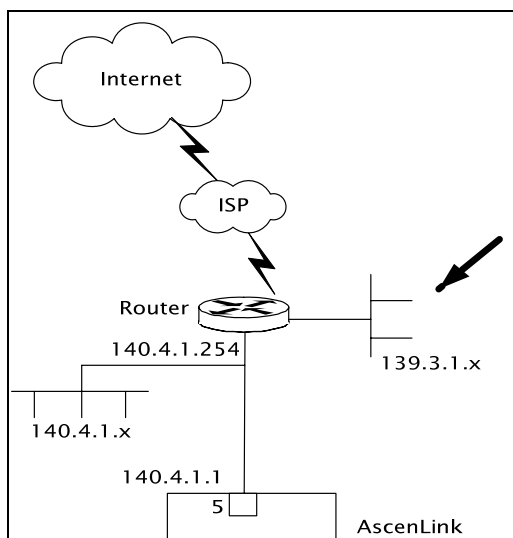


圖 2.24 Static Routing Subnet 模式下 Subnet in WAN 架構圖

Static Routing Subnet				
+	Subnet Type	Network IP	Netmask	Gateway
+ □ ▢ ▣ ▤	Subnet in WAN	139.3.1.0	255.255.255.0	140.4.1.254

圖 2.25 Static Routing Subnet 模式下有關 Subnet in WAN 架構的設定

Static Routing Subnet 模式下有關 Subnet in DMZ 架構的設定

範例：這個網路架構和上述很類似，但是子網路位於隔離區。

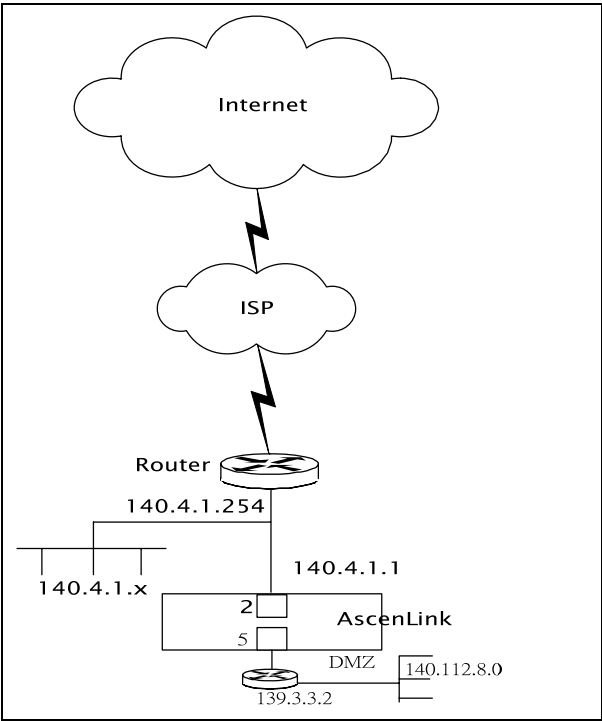


圖 2.26 Static Routing Subnet 模式下 Subnet in DMZ 之架構圖

Static Routing Subnet				
+	Subnet Type	Network IP	Netmask	Gateway
+	Subnet in DMZ	140.112.8.0	255.255.255.0	139.3.3.2

圖 2.27 Static Routing Subnet 模式下有關 Subnet in DMZ 架構的設定

2.2.3.2 Bridge Mode: One Static IP

範例：當 ISP 配發給固接式用戶時的情況。

一個固定的 IP 位址時，可參考此範例做設定。在這個範例中用戶申請一條固接式的 ADSL，上下載頻寬為 512 K，並且僅有一個固定 IP，因此 ATUR 是在 Bridge Mode (橋接模式)下工作。

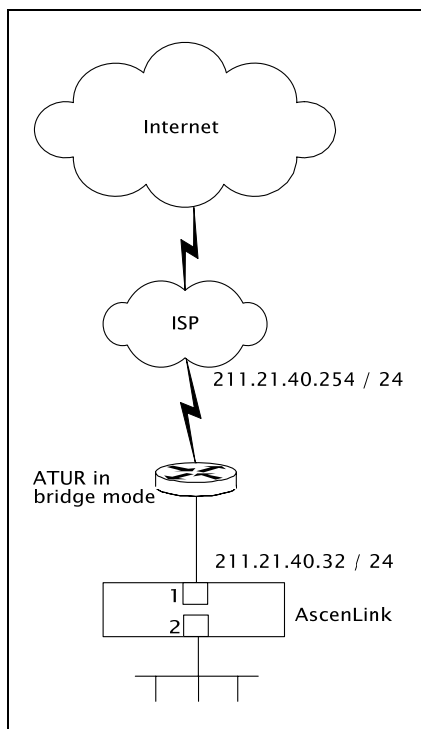


圖 2.28 Bridge Mode: One Static IP 網路架構圖

Bridge Mode: One Static IP 下，Basic Setting 設定如下：

Basic Setting	
Enable	<input checked="" type="checkbox"/>
WAN Type	Bridge Mode: One Static IP ▾
Down Stream	512 Kbps
Up Stream	512 Kbps
Localhost IP	211.21.40.32
Netmask	255.255.0.0
Gateway	211.21.40.254
MTU	1500
WAN Port	Port1 ▾

圖 2.29 Bridge Mode: One Static IP 的 Basic Setting 設定

2.2.3.3 Bridge Mode: Multiple Static IP

如果您向 ISP 申請的線路設定一組固定 IP 位址，而且網路架構是採用橋接方式，就可以應用這項子功能來進行設定。

範例：

在這個範例中 ISP 設定了一組 IP，有效可用的 IP 211.21.40.32~211.21.40.34，這組 IP 設定給 AscenLink 的網路介面 Port 2。同時預設閘道位址是 ISP 所指定的 211.21.40.254。

如果在廣域網路端還設置有其他主機，則必須將主機設定的 IP 位址也設定在 IP(s) in WAN。如果在隔離區設置有其他主機，則須將位於隔離區的主機之 IP 位址也設定在 IP(s) in DMZ。

如果您希望對位於 DMZ 的子網路下的主機提供 DHCP 服務，則需要啟用 DHCP (Enable DHCP)，然後在 Starting Address 及 Ending Address 分別填入要分配的 IP 起始位址與結束位置。如果在子網路中有主機是設定固定 IP 時，則須將此 IP 填入 Static Mapping 這一系列中之 IP Address 欄，同時也須將此主機的 MAC 位址填入 MAC Address 欄中。

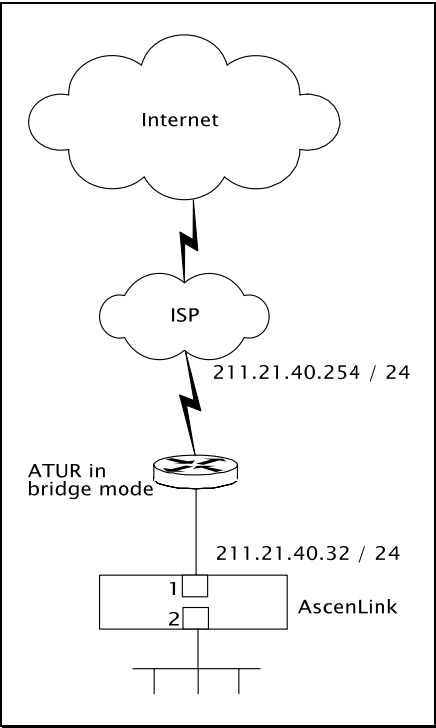


圖 2.30 Bridge Mode: Multiple Static IP 網路架構圖

Bridge Mode: Multiple Static IP 下，Basic Setting 設定如下：

Basic Setting			
Enable	<input checked="" type="checkbox"/>		
WAN Type	Bridge Mode: Multiple Static IP		
Down Stream	512	Kbps	
Up Stream	512	Kbps	
IP(s) on Localhost	<input data-bbox="615 499 642 534" type="button" value="+"/>	211.21.40.32-211.21.40.34	
IP(s) in WAN	<input data-bbox="615 552 642 586" type="button" value="+"/>	No address	
IP(s) in DMZ	<input data-bbox="615 604 642 638" type="button" value="+"/>	No address	
Netmask	255.255.255.0		
Gateway	211.21.40.254		
MTU	1492		
WAN Port	Port1		
DMZ Port	Port5		
Enable DHCP	<input checked="" type="checkbox"/>		
DHCP Range	<input data-bbox="615 904 642 939" type="button" value="+"/>	Starting Address	Ending Address
Static Mapping	<input data-bbox="615 956 642 991" type="button" value="+"/>	MAC Address	IP Address

圖 2.31 Bridge Mode: Multiple Static IP 下，Basic Setting 設定

2.2.3.4 Bridge Mode: PPPoE

這種網路架構一般是使用 ADSL 線路，AscenLink 的 Basic Setting 對其有如下的設定。

Basic Setting	
Enable	<input checked="" type="checkbox"/>
WAN Type	Bridge Mode: PPPoE
Down Stream	512 Kbps
Up Stream	512 Kbps
User Name	
Password	
Service Name	
IP Address	
MTU	1492
WAN Port	Port1
Redial Enable	<input type="checkbox"/>

圖 2.32 Bridge Mode: PPPoE 下，Basic Setting 設定

在這個設定表格中，須填入這條線路的參數，如上下載之頻寬數值，ISP 配發的帳戶名稱、密碼以及伺服器名稱，MTU 值等。在填寫[IP Address]這個欄位的時候須註意：如果您申請的 ADSL 是動態分配 IP 位址的，請將[IP Address]欄位保持空白；若您申請的 ADSL 有固定的 IP 位址，請在該欄位輸入 ISP 為您提供的 IP 位址。其他的設定和前面相同，即 ADSL MODEM 的網路介面連線到 AscenLink 的網路介面，例如 Port 2。某些 ISP 在固定時間段後會自動重連網路，因此會導致 AscenLink 的各條 WAN 線路同時斷線重撥。為避免上述情況管理員可在此啓用[重撥啓用]，針對不同 WAN 線路設定不同重撥時間，人爲的錯開 WAN 重撥時間。

2.2.3.5 Bridge Mode: DHCP Client

這種情況是當 AscenLink 對外連線的網路介面其 IP 位址是由 DHCP 主機主動提供時，須進行如下的設定。

Basic Setting	
Enable	<input checked="" type="checkbox"/>
WAN Type	Bridge Mode: DHCP Client ▼
Down Stream	512 Kbps
Up Stream	512 Kbps
MTU	1492
WAN Port	Port2 ▼

圖 2.33 Bridge Mode: DHCP Client 下，Basic Setting 設定

2.2.4 WAN/DMZ Private Subnet(廣域網路/隔離區私有子網路)子功能

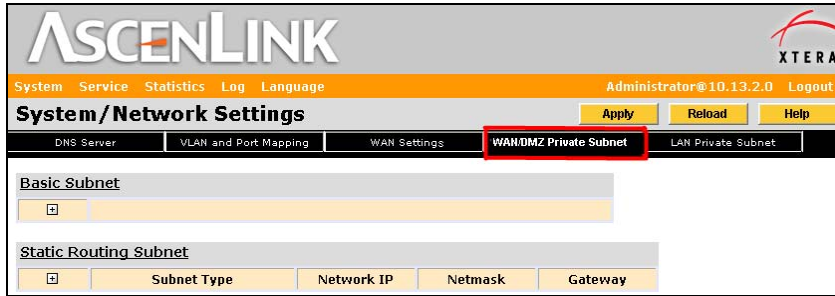


圖 2.34 System/Network Setting/WAN/DMZ Private Subnet 子功能位置

在上一節的介紹都是針對公有子網路的情況，緊接著這一節將討論私有子網路的架構和設定。在設定內容上和前述的方法非常相似。在 **WAN/DMZ Private Subnet** 這項子功能下，同樣的也定義出幾種私有子網路的架構，在 **Basic Subnet** 設定表格中，列出四種私有子網路，分別是：

- Subnet in WAN (廣域網路端的子網路)
- Subnet in DMZ (隔離區端的子網路)
- Subnet in WAN and DMZ (子網路分在廣域網路端與隔離區端兩側)
- Subnet on Localhost (本機上的子網路)

Basic Subnet

Subnet Detail

Subnet Type	Subnet in DMZ
IP(s) on Localhost	Subnet in WAN Subnet in DMZ Subnet in WAN and DMZ Subnet on Localhost
Netmask	
DMZ Port	Port5
Enable DHCP	<input type="checkbox"/>

圖 2.35 WAN/DMZ Private Subnet 中 Subnet 種類

在 Static Routing Subnet 中則設計有兩種子網路，分別是：

- Subnet in WAN (廣域網路端的靜態路由子網路)
- Subnet in DMZ (隔離區端的靜態路由子網路)

Static Routing Subnet

Subnet Type	Network IP	Netmask	Gateway
Subnet in WAN	192.168.52.0	255.255.255.0	192.168.50.1
Subnet in WAN			
Subnet in DMZ			

圖 2.36 Static Routing Subnet 中 Subnet 種類

2.2.4.1 Basic Subnet 模式下有關 Subnet in WAN 的架構設定

當遇到在廣域網路端存在私有子網路時，可以在 Basic Subnet 表格中的 Subnet Type 欄位選擇 Subnet in WAN 這個參數值。

範例：

此環境多用於私有子網路之主機群位於廣域網路端。在這範例中，IP(s) on Localhost 欄位指的設定給 AscenLink 網路介面的 IP 位址，圖例中使用網路介面 Port 2，設定 IP 192.168.3.1，Netmask 為 ISP 提供的參數。

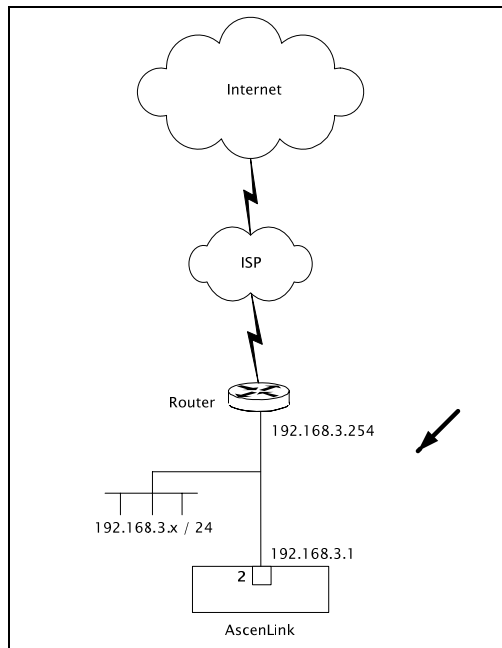


圖 2.37 Basic Subnet 模式之 Subnet in WAN 網路架構圖

註：AscenLink 假設所有這個網段未列於 IP(s) on Localhost 的 IP 都位於 WAN 端。

Basic Subnet	
<div>+</div>	
<div>⊞ ⊞ ⊞ ⊞ ⊞</div>	Subnet Detail
	Subnet Type Subnet in WAN <div>▼</div>
	IP(s) on Localhost <div>+</div> 192.168.3.1
	Netmask 255.255.255.0
	WAN Port Port2 <div>▼</div>

圖 2.38 Basic Subnet 模式下有關 Subnet in WAN 的架構設定

2.2.4.2 Basic Subnet 模式下有關 Subnet in DMZ 的架構設定

範例：

此環境多用在私有子網路的主機群存在于隔離區網路端。本例中 AscenLink 的 Port 5 規劃為 DMZ 介面，設定一個私有 IP 192.168.4.254，整個 192.168.4.X 的子網路都位於隔離區。在 Basic Subnet 這個設定表格中，選擇 Subnet Type 為 Subnet in DMZ。其他的參數設定如下：

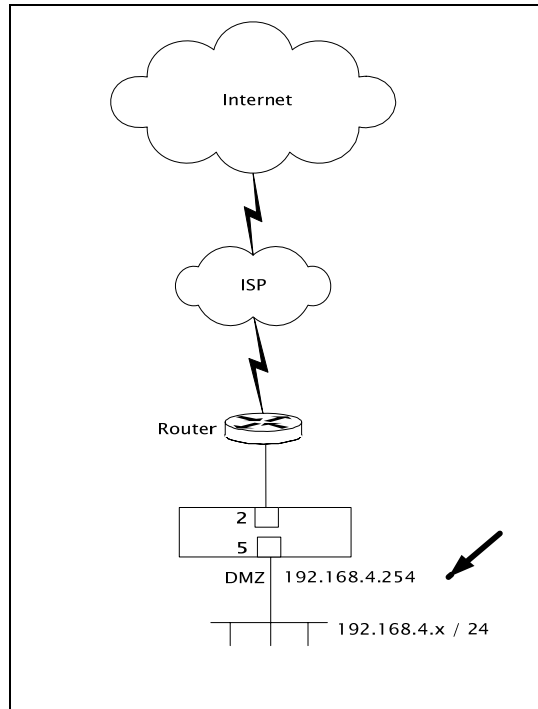


圖 2.39 Basic Subnet 模式 Subnet in DMZ 之網路架構圖

Basic Subnet

Subnet Detail

Subnet Type

Subnet in DMZ

IP(s) on Localhost

192.168.4.254

Netmask

255.255.255.0

DMZ Port

Port5

Enable DHCP

☒

DHCP Range

Starting Address

Ending Address

Static Mapping

MAC Address

IP Address

圖 2.40 Basic Subnet 模式 Subnet in DMZ 之架構設定

如果您希望對位於 DMZ 的子網路下的主機提供 DHCP 服務，則需要啓用 DHCP (Enable DHCP)，然後在 DHCP Range 欄位分別填入要分配的 IP 起始位址與結束位置。如果在子網路中有主機是設定固定 IP 時，則須將此 IP 填入 Static Mapping 這一系列中之 IP Address 欄，同時也須將此主機的 MAC 位址填入 MAC Address 欄中。

註：AscenLink 假設所有這個網段未列於 IP(s) on Localhost 的 IP 都位於隔離區端，不需設定。

2.2.4.3 Basic Subnet 模式下有關 Subnet in WAN and DMZ 的架構設定

此環境多用在私有子網路的主機群同時存在於廣域網路與隔離區網路端。AscenLink 假設所有這個網段的 IP 未列於 IP(s) on Localhost 和 IP(s) in WAN 欄位中的 IP 都位於隔離區端。

Port2 與 Port5 之間用虛線連線表示是同一個 Subnet 的網段同時橫跨 WAN (Port2) 及 DMZ (Port5)之間，AscenLink 會利用 Proxy ARP 的技術將這個 Subnet 連起來。

在這個範例中，需要一個以上的 IP 供 AscenLink 做 bridge 用，此 IP(s)為同一個網段。因此，在 IP(s) on Localhost 這個欄位須設定 192.168.5.20~192.168.5.30 這組 IP，然後將位於廣域網路端的 IP (192.168.5.10 ~ 192.168.5.19)，設定在 IP (s) in WAN 這個欄位中。

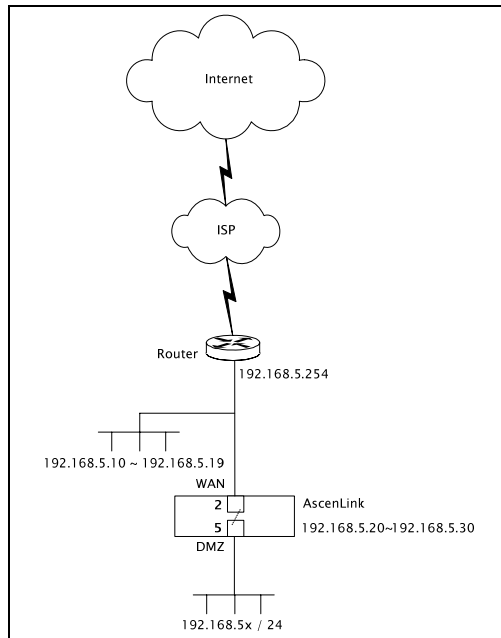


圖 2.41 Basic Subnet 模式 Subnet in WAN/DMZ 之網路架構圖

Basic Subnet		
<div>+</div>		
<div>+</div> <div>-</div> <div>↑</div> <div>↓</div>	Subnet Detail	
	Subnet Type	Subnet in WAN and DMZ
	IP(s) on Localhost	<div>+</div> 192.168.5.20-192.168.5.30
	IP(s) in WAN	<div>+</div> <div>-</div> <div>↑</div> <div>↓</div> 192.168.5.10-192.168.5.19
		<div>+</div> <div>-</div> <div>↑</div> <div>↓</div> 192.168.5.254
	Netmask	255.255.255.0
	WAN Port	Port2
DMZ Port	Port5	

圖 2.42 Basic Subnet 模式下有關 Subnet in WAN and DMZ 的架構設定

2.2.4.4 Basic Subnet 模式下有關 Subnet on Localhost 的架構設定

這個範例是在 AscenLink 上指定整個私有子網路，這些 IP 位址可提供給虛擬主機 (Virtual Server)之用。

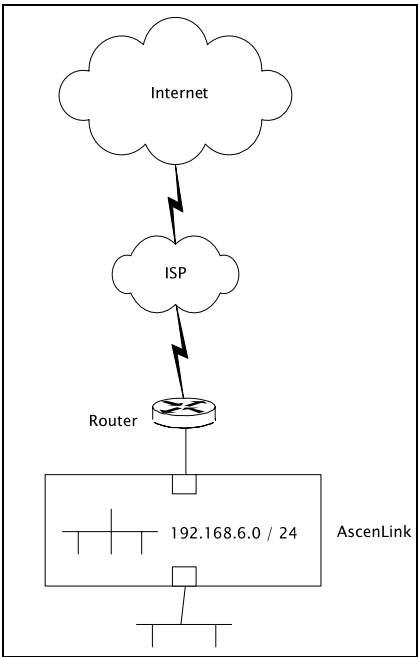


圖 2.43 Basic Subnet 模式 Subnet on Localhost 之網路架構圖

Basic Subnet	
<div>+</div>	
Subnet Detail	
Subnet Type	Subnet on Localhost
Network IP	192.168.6.0
Netmask	255.255.255.0

圖 2.44 Basic Subnet 模式下有關 Subnet in WAN and DMZ 的架構設定

2.2.4.5 Static Routing Subnet 模式下有關 Subnet in WAN 架構的設定

如果網路架構是屬於在 WAN 端設置私有靜態路由子網路，就必須設定這項表格。

範例：

在這個網路架構中有一個私有子網路在 WAN 端，而且不直接和 AscenLink 連線，透過一台路由器轉送封包，所以必須將有關於這個子網路的參數設定於 Static Routing Subnet 表格中。

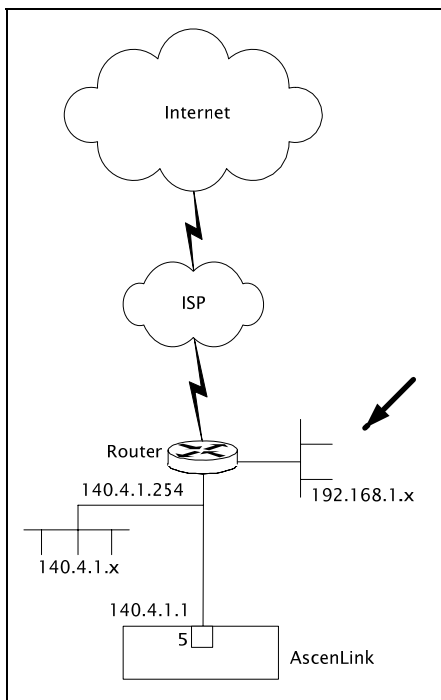


圖 2.45 Static Routing Subnet 模式下 Subnet in WAN 之網路架構圖

有關 Gateway 這個欄位的 IP，就是連線這個子網路的路由器之 IP 位址。

Static Routing Subnet				
+	Subnet Type	Network IP	Netmask	Gateway
+ - ↑ ↓	Subnet in WAN	192.168.1.0	255.255.255.0	140.4.1.254

圖 2.46 Static Routing Subnet 模式下有關 Subnet in WAN 架構的設定

2.2.4.6 Static Routing Subnet 模式下有關 Subnet in DMZ 架構的設定

這個網路架構是在 DMZ 隔離區內，利用一台 Router，位址 192.168.34.50，設定出一個私有子網路，位址為 192.168.99.0/24。由於這個子網路不直接連線於 AscenLink，因此這個子網路的參數需要設定於 AscenLink 中，以便可以處理來自這個子網路的封包。

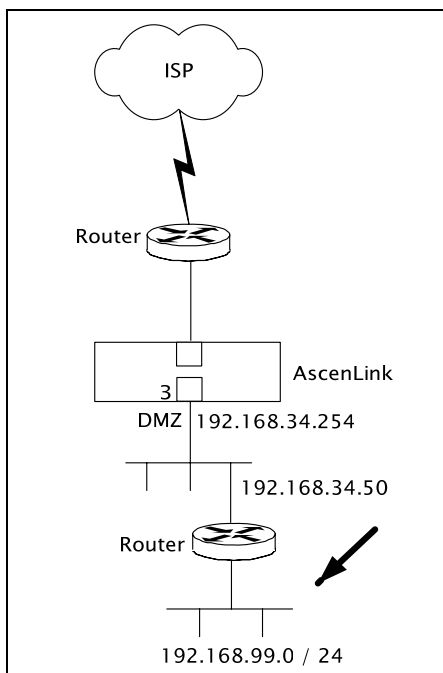


圖 2.47 Static Routing Subnet 模式下 Subnet in DMZ 之網路架構圖

Static Routing Subnet				
+	Subnet Type	Network IP	Netmask	Gateway
+	Subnet in DMZ	192.168.99.0	255.255.255.0	192.168.34.50

圖 2.48 Static Routing Subnet 模式下有關 Subnet in DMZ 架構的設定

2.2.5 LAN Private Subnet 子功能(區域網路私有子網路)

The screenshot displays the AscenLink web interface for configuring network settings. The top navigation bar includes links for System, Service, Statistics, Log, and Language. The main title is "System/Network Settings". The "LAN Private Subnet" tab is selected and highlighted in red. The configuration area is divided into sections: "Basic Subnet" (containing "Subnet Detail" with fields for IP(s) on Localhost, Netmask, LAN Port, NAT Subnet for VS, and Enable DHCP), "RIP" (with a checkbox), "OSPF" (with a checkbox), and "Static Routing Subnet" (with a table for Network IP, Netmask, and Gateway).

圖 2.49 System/Network Setting/ LAN Private Subnet 功能所處位置

Basic Subnet 的設定

設定 AscenLink 的網路參數除了在 WAN Setting 設定對外連線的線路參數後，最常使用的大概就是 LAN Private Subnet 這一項功能了。

這項功能是處理有關區域網路裏的各項網路參數，AscenLink 可以規劃網路介面的功能，如果某一個網路介面設置為 LAN 則需要設定有關這個 LAN 的各項參數。

範例：這個範例是相當典型的 LAN 環境。

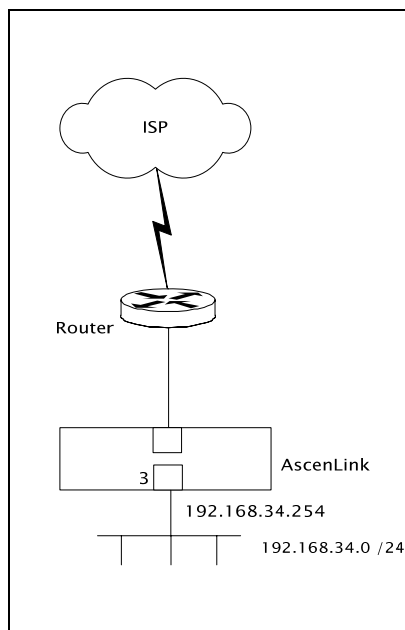


圖 2.50 區域網路模式下 basic 子網路之網路架構圖

在這個範例中，AscenLink 的網路介面 Port 3 設定為 LAN，這個介面設定一個 Private IP 192.168.34.254，這個位址資料就填入 IP (s) on Localhost 這個欄位中。

對內部區域網路的主機而言這個位址也就是 LAN 的 Gateway。在這個表格中，您也可以啟用 DHCP 功能，這樣位於 LAN 區域的主機，都可以動態分配到 IP 位址。

在這個範例中，分派 192.168.34.175 到 192.168.34.199 這個區段的位址給動態分配給 LAN 的主機使用。

如果 LAN 有部份主機需要指定固定位址，則需要在 Static Mapping 的欄位中將這幾個位址設定進去，同時也需要輸入主機的 MAC 位址。

當 LAN 或 DMZ 的使用者存取虛擬伺服器的 WAN IP 位址時，為了避免使用者的封包繞過 AscenLink 直接送到內部的伺服器，可以選擇“虛擬伺服器位址轉換”核取

方塊，將使用者的封包來源 IP 位址轉換成 AscenLink 本機的 IP 位址，確保封包一定會經由 AscenLink。不選任何核取方塊時，系統將自行決定轉譯的 IP 位址。

Basic Subnet

+

Subnet Detail

IP(s) on Localhost

+

192.168.34.254

Netmask

255.255.255.0

LAN Port

Port3

NAT Subnet for VS

☒

Enable DHCP

☒

Domain Name Server

10.17.0.3

Domain Name Suffix

ALL

DHCP Range

+

Starting Address

Ending Address

+

-

↑

↓

192.168.34.175

192.168.34.199

Static Mapping

+

MAC Address

IP Address

+

-

↑

↓

00:24:ed:18:58:16

192.168.34.173

圖 2.51 LAN Private Subnet/ Basic Subnet 的設定

RIP 路由協定的設定

AscenLink 支援 RIP (即 Routing Information Protocols) 路由協定的 RIP V1 和 RIP V2 兩個版本。RIP 的度量基於跳數，路由的更新採用定時廣播的方式。RIP 路由協定具有設定簡單，管理方便的優點，在許多領域具有廣泛的應用。RIP V1 是基於 IP 的 RIP，RIP V2 是增強版的 RIP 它允許在 RIP 的分組中包含更多的資訊並提供了簡單的驗證。如果在您的私有子網中路由器啓用了該路由協定請點選點選框啓用該協定。

RIP		<input checked="" type="checkbox"/>	
RIP v1	<input type="checkbox"/>	RIP v2	<input checked="" type="checkbox"/>
Multicast	<input checked="" type="checkbox"/>	Broadcast	<input type="checkbox"/>
Password			

圖 2.52 LAN Private Subnet/ RIP 的設定

如果在 AscenLink 後面連線的本地私有子網路中的路由器啓用的是 RIP v1，請點選 RIP v1 點選框這樣就可以使 AscenLink 對啓用了 RIP v1 路由協定的私有子網路發送過來的封包進行轉發。

如果您的私有子網路的路由協定是採用的 RIP v2 請點選 RIP v2 使 AscenLink 支援 RIP v2 封包的轉發，如果在路由器上啓用了身份驗證功能的話請在[Authentication Password]欄位元輸入身份驗證的密碼，如沒有該欄位就保持空白。

OSPF 路由協議的設定

AscenLink 在 LAN 口路由器按優先順序支援 OSPF（即 Open Shortest Path First 開放式最短路徑優先）協定。與 RIP 相對，OSPF 是一個內部閘道協定，採用線路狀態技術，路由器互相發送直接相連的線路資訊和它所擁有的到其他路由器的線路資訊。

OSPF Settings

OSPF Interface	Port	Enable	
	Port3	<input checked="" type="checkbox"/>	
Area Setting	<div><div></div><div></div><div></div><div></div></div>	Prefix	Area ID
	<div><div></div><div></div><div></div><div></div></div>	192.168.0.0/0.0.0.255	1
	<div><div></div><div></div><div></div><div></div></div>	192.168.1.0/0.0.0.255	192.168.1.1
	<div><div></div><div></div><div></div><div></div></div>	192.168.2.0/0.0.0.255	3
Authentication Setting	<div><div></div></div>	Area ID	Authentication Type
Interface Setting	Port3	Router Priority	0
		Hello Interval	10
		Dead Interval	40
		Retransmit Interval	5
		Authentication Type	Null
			Simple Text Password
	MD5		

圖 2.53 LAN Private Subnet/ OSPF 的設定

欄位	說明
OSPF Interface (OSPF 介面)	顯示網路中的各 LAN 口，勾選核取方塊則對該口啟用 OSPF 協定。
Area Setting (區域設定)	根據不同子網路將網路從邏輯上劃分為多個區域，管理員可規定各區域 ID，只能輸入數位或 IP 位址。
Authentication Setting (認證設定)	若某個區域之間相互通信需要認證，可在此設定認證方式：不使用認證、簡單密碼認證或 MD5 認證。
Router Priority (路由器優先順序)	設定路由的優先順序，數值最大的將被用作指定路由器 (Designated Router)，取值範圍從 0 至 255。
Hello Interval (Hello 時間間隔)	路由器每隔一段時間會發送一個包以檢測相鄰路由器是否還正常工作，在此可設定該時間間隔。
Dead Interval (Dead 時間間隔)	若一定時間間隔內未收到某路由器的 hello 包，則認定該路由器已宕機，在此設定該時間間隔。
Retransmit Interval (重傳間隔)	路由器發送 Hello 包失敗後，在一定時間間隔後將重新傳送資料包，在此可設定該時間間隔。
Authentication Type (認證類型)	設定所有通過該 LAN 的資訊是否需要認證，可選擇的類型有：不使用認證、簡單密碼認證或 MD5 認證。

表 2.7 OSPF 路由協定設定

Static Routing Subnet 的設定

如果在 LAN 端有靜態路由子網路，就必須用 Static Routing Subnet 這項子功能來設定。所謂 LAN 中的靜態路由子網路，是指在 LAN 中使用一台路由器，分割出一個獨立的子網路，這個子網路不直接連線到 AscenLink。這樣的網路架構和前述 Subnet in DMZ 的網路架構完全相同，差別的只是一個是在 DMZ，而我們這裏的範例是在 LAN。

範例：

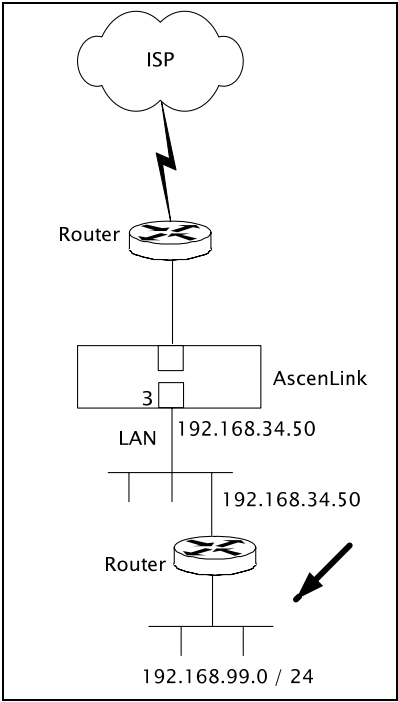


圖 2.54 Static Routing Subnet 網路架構圖

Static Routing Subnet			
+	Network IP	Netmask	Gateway
+ - ↑ ↓	192.168.99.0	255.255.255.0	192.168.34.50

圖 2.55 LAN Private Subnet/ Static Routing Subnet 的設定

2.3 WAN Link Health Detection (廣域網路連線狀態偵測)

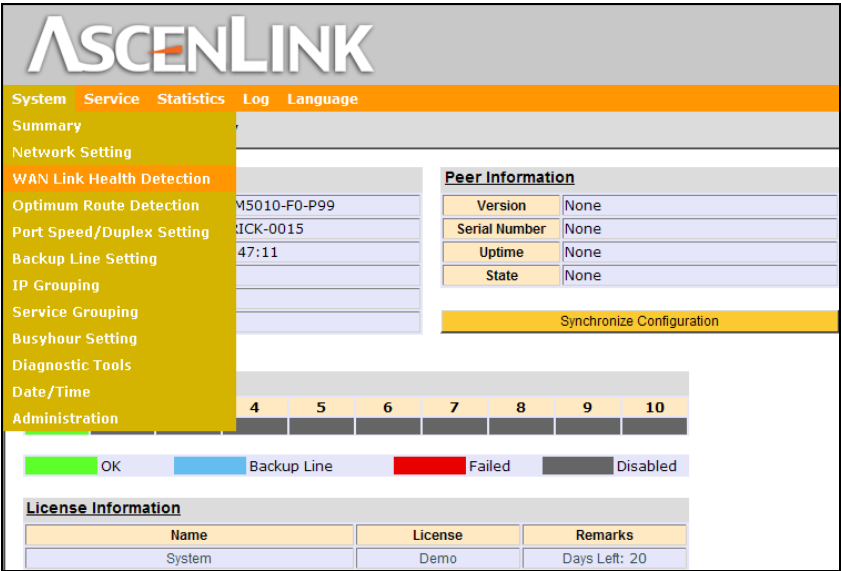


圖 2.56 System/WAN Link Health Detection 功能所處位置

這項功能是讓系統管理人員可以判斷對外連線的線路品質狀況，假如是在多條外線的情況下，您也可以針對每一路外線，設定符合情況的狀態偵測條件。

AscenLink 本身使用 icmp 和 tcp 封包對網路的連線狀態做偵測，依照回傳的狀況決定此廣域網路連線是否正常。

進入這個功能的畫面後，您有幾個欄位可以設定：

忽略對內流量

當啟用(Enable)此設定時，AscenLink 就不會利用廣域網路流量來判斷對外連線狀況。當不啟用(Disable)此設定時，只要 AscenLink 有偵測到 WAN 端有網路流量，就判定此路廣域網路連線是屬於正常連線狀態，而不再進行 icmp 和 tcp 封包的偵測行為。

Detection period, in seconds (偵測週期，單位：秒)

表示每次偵測的週期長短，以秒為週期單位，間隔短表示可以更快發現目前的連線狀況，不過也會消耗比較多的頻寬。

Number of hosts picked per detection(每次偵測所選出的主機數量)

每次偵測線路時，所選出的主機數量。在每次測試的時候，會對每一個所選定的主機 IP 送出測試封包。

Number of retries (重試次數)

此欄表示發生錯誤時的重測次數，重複上述的測試多次，如果所有的測試都失敗，AscenLink 則宣告此廣域網路連線無法運作。

偵測協定為 **ICMP** 封包狀態下，有下列功能表：

Ping List (Ping 清單)

此欄表示可利用 Ping 來進行網路偵測的主機資料，每次偵測會針對清單中隨機選出的主機送出封包，一個 IP 位址寄出一個 ping。這個 ping 的存活時間 (time to live) 是由參數「躍點」(Hops)所定義，一般設定為 3。

偵測協定為 **TCP** 封包狀態下，有下列功能表：

TCP Connect List (TCP 連線清單)

此欄表示可利用 TCP connect 來進行網路偵測的主機資料，每次偵測會針對清單中隨機選出的主機進行連線測試，同時也可指定「通訊埠」(Port)的數值。

2.4 Optimum Route Detection (最佳路徑偵測)

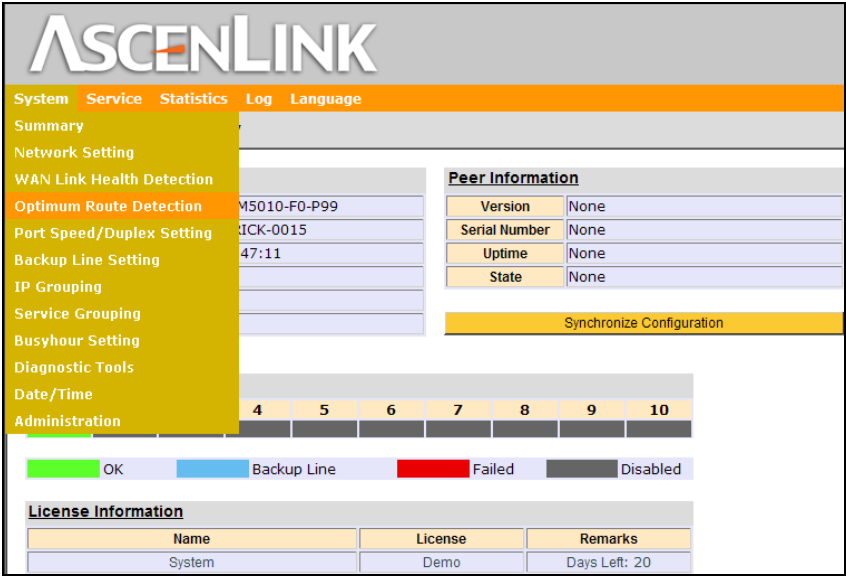


圖 2.57 System/ Optimum Route Detection 功能所處位置

該功能，主要是解決多個 ISP 之間，互連互通問題，透過使用該功能，用戶可實現就近存取最佳線路，提高線路的利用率。系統管理人員可在此功能頁面中，對 AscenLink 的最佳路徑偵測方式做設定。系統提供靜態偵測 IP 列表和動態偵測，管理員可根據需要對這兩種偵測方式進行組合，以達到最佳偵測效果。

AscenLink 動態偵測使用 icmp 和 tcp 封包對網路的連線狀態做偵測，依照最佳路徑演算法進行運算，判斷哪條對外線路為最佳通道。

AscenLink 靜態偵測 IP 列表使用 Xtera 公司自主設計的 IP 庫，透過比對 IP 列表中的 IP 條目，提供最佳線路，並可以對 IP 列表進行增加和刪除。此外還可以透過查詢功能，查詢 IP 列表中是否有欲查詢的 IP 條目。

進入這個功能的畫面後，有幾個欄位需要設定。

欄位	值	說明
最佳路由策略	靜態 IP 列表 動態偵測 靜態，動態 動態，靜態	選擇預使用的路徑偵測方式。有四種偵測方式可供選擇。 靜態 IP 列表：只採用靜態 IP 列表偵測選擇最佳路由。 動態偵測：只採用動態偵測方式偵測最佳路由。 靜態，動態：即先進行靜態偵測，當靜態偵測失效時，進行動態偵測。系統預設為靜態，動態。 動態，靜態：即先進行動態偵測，當動態偵測失效時，進行靜態偵測。
Detection Protocol(偵測協定)	<ICMP>; <TCP>	表示要進行最佳路徑偵測的協定方式，分成 icmp 和 tcp 兩種偵測方式。系統預設為 icmp 方式。
Detection period, in seconds(偵測週期)	<秒>	表示當系統偵測最佳路徑，沒有回應時，再次進行偵測的時間間隔，以秒表示。為了更好地偵測出最佳路徑，適當地保有一段間隔，可以使測出的網路狀態更全面。系統預設為 3s。
Number of retries(重試次數)	-	表示當系統偵測最佳路徑，沒有回應時，進行重複偵測的次數。當系統在重複偵測的時候只要有一次偵測成功，就不在進行下一次偵測。系統預設是重試次數為 3 次。
Cache aging period, in minutes (Cache 記錄保存週期)	<分>	表示系統偵測出最佳路徑後，Cache 記錄保存的時間。超過這段時間後，系統就會根據需要重新偵測最佳路徑。系統預設為 2880 分鐘（兩天）。
Weight of Round Trip Time : Weight of Load(回應時間比重：負載比重)	-	用來計算最佳路徑的參數。表示往返傳輸時間與線路負載在計算最佳路徑時的比重。 註：在“Weight of Round Trip Time : Weight of Load”欄位的比重值越小，說明該項所占的比重越小

表 2.8 動態偵測設定欄位說明

在靜態 IP 列表偵測欄位元，有如下欄位需要設定：

欄位	值	說明
IP 列表名稱	-	用來定義 IP 列表的名稱
上傳	-	點選“流覽”選擇相應的 IP 列表文件，之後點選“上傳”上傳該 IP 列表到 AscenLink
子網路位址	<IP Address>	在空白欄位中添入欲添加或刪除的子網路位址。 子網路位址格式：202.99.0.0/255.255.255.0 或者 202.99.0.0/24。 備註：不支援添加單一 IP 位址及子網路遮罩為“/255.255.255.255”或“/32”的子網路位址。
處理	<add to> <remove from>	add to：添加該子網路位址到靜態 IP 列表中。 remove from：從靜態 IP 列表中刪除該子網路位址。
廣域網路	WAN1,WAN2...	選擇 IP 列表使用的廣域網路，在其對應的廣域網路序號前打勾。
IP 位址查詢	<IP Address>	查詢某一 IP 位址是否位於該靜態 IP 列表內。只支援單一 IP 位址的查詢。IP 位址格式：202.99.96.68。

表 2.9 靜態 IP 列表偵測設定欄位說明

2.5 Port Speed/Duplex Setting (網路介面傳輸模式設定)

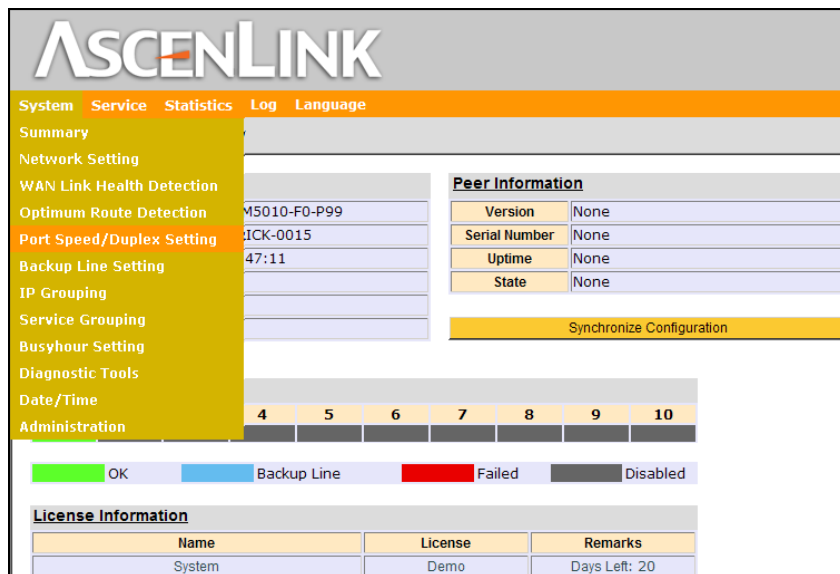


圖 2.58 System/ Duplex Setting 功能所處位置

網路介面傳輸模式設定

在此頁面可設定 AscenLink 的網路介面支援不同的傳輸模式，預設值是自動設定，大多數情況下自動設定不會有任何問題，但是某一些老舊的網路設備不具備自動協定的功能，或是其功能與 AscenLink 不匹配，在這些情況下則需要手動設定網路介面。

欄位	說明
Port Name	在此欄為 AscenLink 上所有的實體的 port 的清單
Status	在此欄為目前連線的狀況，非指 TCP/IP, 而是指網路線是否有接上可以偵測到的網路設備如 HUB 等等。
Speed	目前的網路的速度，可能是手動設定或自動偵測出的值。
Duplex	目前的雙工模式，可能是手動設定或自動偵測出的值。
Setting	在此欄可點選欲使用的方式，除了手動設定在某一個速度外也可以放在自動的模式下。
MAC Address	網路埠的 MAC 位址。

表 2.10 網路介面傳輸模式設定欄位說明

2.6 Backup Line Setting (備援線設定)

這一項子功能是設定有關備援線路的啓用和停用原則，在多條外線的網路環境中，可以選擇其中的某些線路作為備援之用，在正常時備援線路是不工作的，等到符合設定原則啓用後，備援線路才開始工作。有些地區的線路是依據資料流程量來計費，因此選擇備援線路有時是基於成本考慮，平常備援線路在正常時並不傳輸資料，因此僅須繳交基本費即可，僅在啓用備援時才會產生成本支出。

The screenshot displays the AscenLink web interface. The top navigation bar includes 'System', 'Service', 'Statistics', 'Log', and 'Language'. The left sidebar menu lists various settings, with 'Backup Line Setting' selected. The main content area is divided into several sections:

- Peer Information**: A table with the following data:

Version	None
Serial Number	None
Uptime	None
State	None
- Synchronize Configuration**: A yellow button.
- Status Bar**: A row of colored boxes representing different line states: OK (green), Backup Line (blue), Failed (red), and Disabled (gray).
- License Information**: A table with the following data:

Name	License	Remarks
System	Demo	Days Left: 20

圖 2.59 System/ Backup Line Setting 功能所處位置

進入 Backup Line Setting 畫面後，有幾個表格需要填入一些線路備援運作時需要參考的參數。

在備援的觀念中，將線路分為 Main Line（主要線路）和 Backup Line（備援線路），Main Line 是指平時使用的線路，Backup Line 是指當備援設定的原則啓用後才使用的線路。

欄位	值	說明
Backup Line Enable Time (啟用備援線時間)	<second>	設定當主要線路發生故障時，需等待多少時間後開始啟用備援線路。
Backup Line Disable Time (取消備援線時間)	<second>	設定當主要線路恢復連線後經由多少時間後把備援線路取消掉。

表 2.11 Threshold 欄位說明

欄位	值	說明
Main Line	WAN1, WAN2...	從目前已有的網路連線中選擇主線路，單一規則中可指定一條以上的主線路。
Backup Line	WAN1, WAN2...	從目前已有的網路連線中選擇備援線路。
Algorithm (演算法)	All Fail One Fails Inbound bandwidth usage reaches Outbound bandwidth usage reaches Total traffic reaches	提供五種狀態的啟動方式以達成起始備援線路的條件： All Fail (全部斷線) ：當所有定義在主線路欄位的連線皆發生故障時，才啟動備援線路。 One Fails (其中之一斷線) ：當定義在主線路欄位的其中之一的連線發生故障就啟動備援線路。 Inbound bandwidth usage reaches (下載頻寬使用率到達) ：當定義在主線路欄位的所有線路的下載頻寬使用率都達到設定的比率後，就啟動備援線路。 Outbound bandwidth usage reaches (上傳頻寬使用率到達) ：當定義在主線路欄位的所有線路的上傳頻寬使用率都達到設定的比率後，就啟動備援線路。 Total traffic reaches (整體頻寬使用率到達) ：當定義在主線路欄位的所有線路的整體頻寬使用率都達到設定的比率後，就啟動備援線路。
Parameter (參數)	<%>	當 Algorithm 選擇後三項條件【對內/對外/整體 頻寬使用率到達】的啟用方式下，須在此欄位中填入預定啟用備援線路的主線路使用率參數。

表 2.12 Backup Line Rule 欄位說明表

2.7 IP Grouping (IP 群組設定)

AscenLink 在設計時提供許多 Service (服務) 功能，這些功能在第三章中都會逐一提及，由於功能眾多，爲了讓系統管理人員可以更有效率的網路管理工作，IP Grouping 可自行定義特定的 IP 或 IP 群爲一群組，這些被定義的群組名稱，會出現在[Service]→ [Firewall] / [NAT] / [Persistent Routing] / [Auto Routing] / [Inbound BM] / [Outbound BM] / [Connection Limit] / Cache Redirect]等子功能中，來源欄位或目的地欄位之下拉功能表裏。

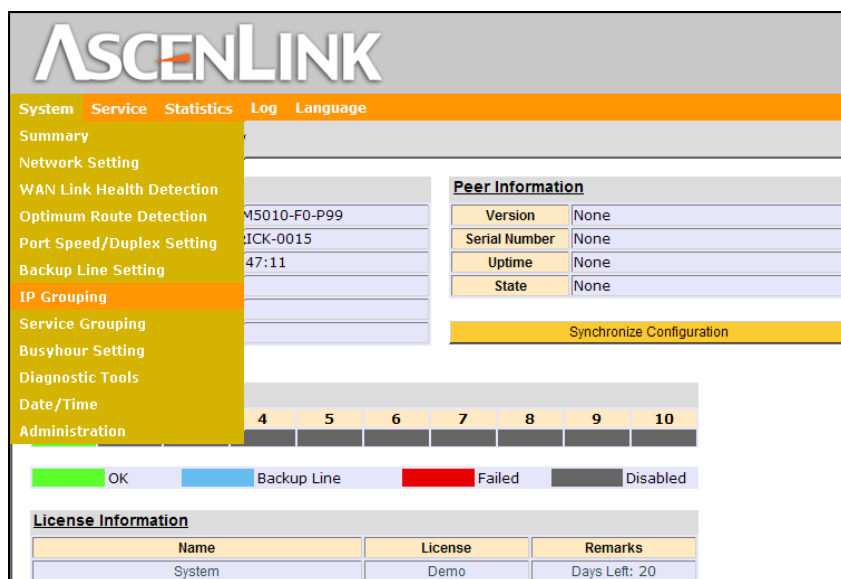


圖 2.60 System/ IP Grouping 功能所處位置

欄位	說明
Group Name (群組名稱)	給定一個群組名稱,此群組名稱會出現在[Service] (服務功能表)各子功能中的來源或目的地下拉功能表中。
Enable (啓用此群組)	勾選方塊時出現紅色打勾符號，表示啓動此群組,只有已經啓動的群組，會出現在 Service 功能中，各項子功能下之下拉功能表中。
Show/Hide Detail (顯示/隱藏詳細設定)	點擊以改變詳細設定內容的隱藏和顯示狀態，隱藏詳細設定后將只顯示群組名稱和是否啓用
Import (匯入)	點擊以匯入左邊瀏覽欄位中選擇的 IP 群組組態檔案中的設定到當前的 IP 群組。
Export (匯出)	點擊以匯出當前 IP 群組的組態到組態檔案中，匯出的組態檔案以文本（.TXT）形式保存。

表 2.13 IP Grouping 欄位說明表

點選 Show Detail (顯示詳細設定)後，會跳出 Rules Setting 的視窗，原來的按鍵即變成 Hide Detail，點選後，將關閉 Rules Setting 視窗。

欄位	值	說明
E (用)	-	勾選方塊以將此列所定義的 IP 位址加入目前的群組中。
IP address (IP 位址)	<IP address>	在此輸入欲加入的 IP 位址,格式為單一位址 IP Range，一段連續的 IP 位址，輸入格式為 xxx.xxx.xxx.xxx-yyy.yyy.yyy.yyy Subnet 某一個子網路輸入格式為 xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy。
Action (動作)	belong to not belong to	定義 IP 位址欄位所輸入的位址是屬於此群組或不屬於此群組。

表 2.14 Rules Setting 欄位說明表

2.8 Service Grouping (網路服務群組設定)

這項功能可讓定義 ICMP 或是一個特定的 TCP/UDP Port，或是一組 TCP/UDP Port 為一個群組。這些指定的群組會用到網路中特定的應用程式或伺服器定義相關的 port。如果這個群組 Enable (使用)，這些被定義的群組名稱，會出現在[Service] → [Firewall] / [NAT] / [Virtual Server] / [Auto Routing] / [Inbound BM] / [Outbound BM] 等子功能中，來源欄位或目的地欄位之下拉功能表裏。

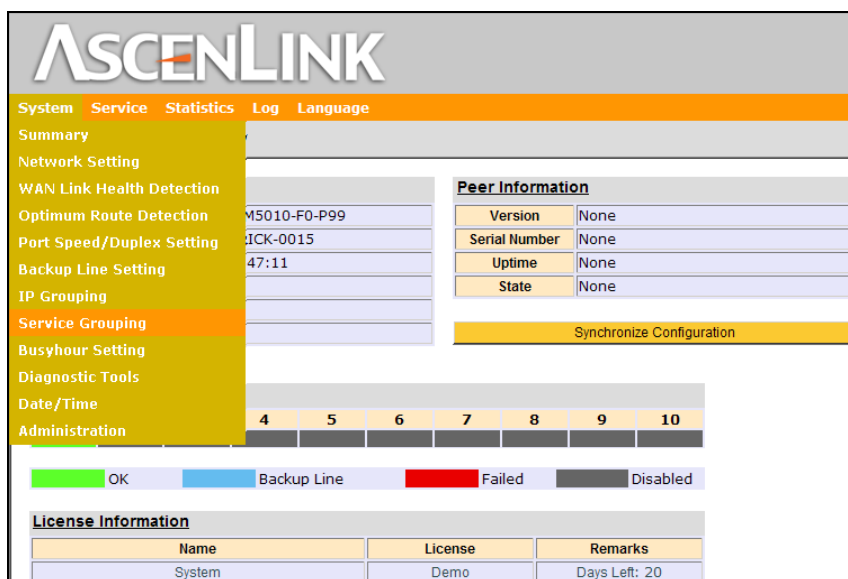


圖 2.61 System/Service Grouping 功能所處位置

欄位	值	說明
Group Name (群組名稱)	<name>	給定一個群組名稱，例如 MSN File Transfer，此群組名稱會出現在 [Service] 功能表中，各子功能裏的來源欄位或目的地欄位之下拉功能表。
Enable (啓用此群組)	-	勾選方塊時出現紅色打勾符號，表示啓動此群組，只有已經啓動的群組，會出現在 [Service] 功能中，各項子功能下之下拉功能表中。
Hide Detail (隱藏詳細設定)	-	點擊以隱藏細部的設定，只顯示群組名稱與是否啓動。
Import (匯入)	-	點擊以匯入左邊瀏覽欄位中選擇的服務群組組態檔案中的設定到當前的服務群組。
Export (匯出)	-	點擊以匯出當前服務群組的組態到組態檔案中，匯出的組態檔案以文本（.TXT）形式保存。
E (啓用)	-	勾選方塊以將此列所定義的網路服務加入目前的群組中。
Service (網路服務)	ICMP TCP@ UDP@	在此欄位定義網路群組，可定義單一或連續一段 TCP/UDP 或指定 ICMP，如果是單一 Port，則輸入形式為 port (xxx)，如果或連續一段 port，則輸入形式為 (xxx-yyy)，例如 6891-6900。
Action (動作)	belong to not belong to	定義前一欄位所輸入的 Port 位址，是屬於此群組或不屬於此群組。

表 2.15 Service Grouping 欄位說明表

舉例而言，你可以設定一個群組名稱叫“MSN File Transfer”，所使用的 Port 為 TCP 6891~6900。而在 Service 欄位中填入 TCP@6891-6900。

2.9 Busyhour Setting (尖峰時段設定)

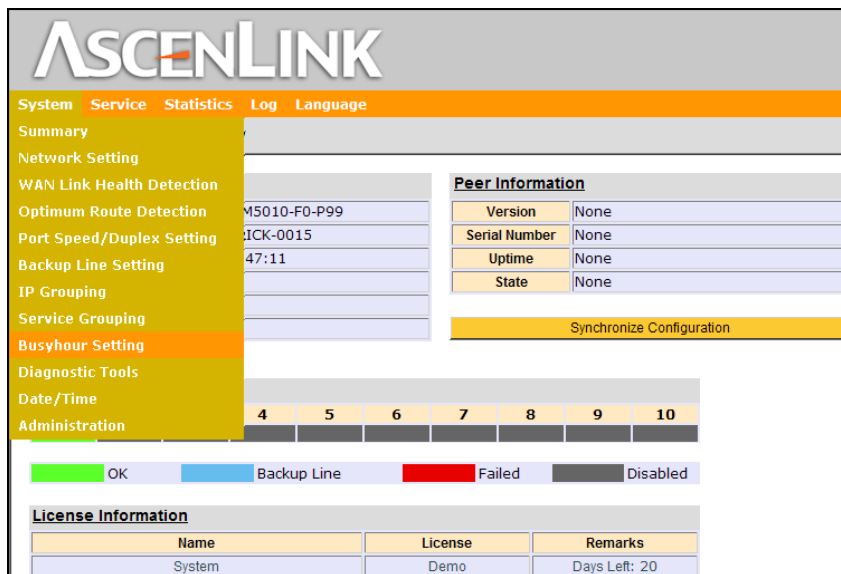


圖 2.62 System/ Busyhour Setting 功能所處位置

尖峰時段設定在頻寬管理方面是很重要的一項設定，它決定了頻寬管理的操作模式。一般而言，設定為禮拜一到禮拜五、每天早上九點到下午五點的上班時間，算是一種不錯的尖峰時段設定。因為就一般企業內部網路而言，上班時段代表網路使用頻繁；就其他用戶而言，所有公司行號對外的流量總和也會對他們的使用造成影響。

欄位	值	說明
Default Type (預設分類)	Idle Busy	將時間分成兩類，離峰時段和尖峰時段，未定義在[規則設定]的時間皆劃分為預設分類所設定的時段。
Rule (規則設定)	-	在此表格中設定時間,時間種類為預設分類以外的時段,若預設分類所定義的時段為 [離峰時段],則此表格中未定義的時間皆為[離峰時段]
E (用)		勾選方塊以將此列中的時間定義加入規則中。
Day of Week (星期)	Sunday Monday Tuesday Wednesday Thursday Friday Saturday Any Day	點選星期日-星期六的某一天或“任一天 (Any Day) ”。
From (開始時間)	<Hour/Minute>	設定起始的時間，可細分到每分鐘。
To (結束時間)	<Hour/Minute>	設定結束的時間，由開始時間到結束時間這段連續的時間即為所設定的劃分時段。
Type (分類)	Busy Idle	可定義此列所設定的連續時間為離峰時段或尖峰時段。

表 2.16 Busyhour Setting 欄位說明表

設定範例

Default Type		Idle					
Rules							
+	E	Day of Week	From		To		Type
			Hour	Minute	Hour	Minute	
+ - ↑ ↓	<input checked="" type="checkbox"/>	Sunday	0	0	0	0	Idle
+ - ↑ ↓	<input checked="" type="checkbox"/>	Any day	9	0	18	0	Busy

圖 2.63 Busyhour Setting 設定範例

在此設定範例中將時間劃分為兩段，星期日全日，星期一至星期六早上九點前和晚上六點後為離峰時段，其餘為尖峰時段。

2.10 Diagnostic Tools (網路診斷工具)

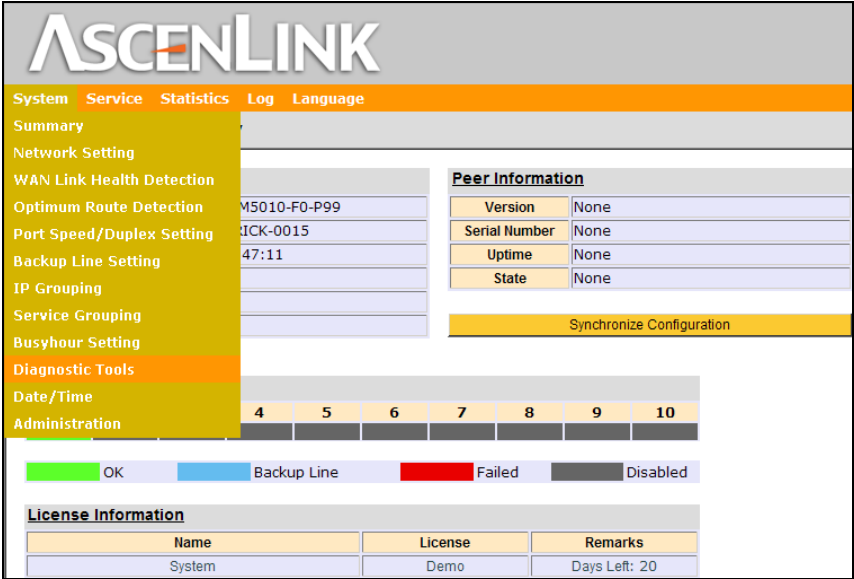


圖 2.64 System/ Diagnostic Tools 功能所處位置

ARP 重整

ARP 重整會強迫 AscenLink 周圍的主機或設備更新 ARP table。

點選[Enforce]，系統會送出一些 ARP 封包以更新周圍的主機或設備的 ARP table，通常用在當部分 DMZ 的設備在第一次安裝 AscenLink 後不能正確的與 Internet 連線時才須使用。

IP 衝突測試

IP 衝突測試尋找目前網路上是否有主機的位址與 **Network Setting** 分頁中的 **IP in DMZ/WAN** 設定有相違背的狀況。

點選 **test** 以開始測試，測試結束後系統可能的回應如下：測試結束，一切正常。

系統發現在 **DMZ** 中有主機與 **Network Setting** 設定中相違背，像是設定某一個公開 IP 存在於 **WAN** 端，結果系統發現到此 IP 被用在 **DMZ** 中，在此資訊後會列出此 IP 與相對應的 **MAC** 位址。

系統發現在 **WAN** 中有主機與 **network setting** 設定中相違背，像是設定某一個公開 IP 存在於 **DMZ** 端，結果系統發現到此 IP 被用在 **WAN** 中，在此資訊後會列出此 IP 與相對應的 **MAC** 位址。

清理 Session 表（指清理非 TCP Sessions）

該功能可清除 **AscenLink** 內部 **session** 表中的非 **TCP session**。

當 **AscenLink** 對某些協定採用計時方式做狀態管理時可能因為用戶端不停重試而導致舊 **session** 一直不逾時從而繼續採用舊的設定，此時可點選“清理”對非 **TCP Sessions** 進行清空，以使新設定即時生效。

Tcpdump

該功能可擷取通過 **AscenLink** 的資料封包，並把擷取的資料封包下載到本機便於管理者對網路狀況進行分析。

在[介面]處選擇要進行擷取的網路介面，如果設置了通道路由，也將在這裡顯示出來，選擇 **Any** 表示擷取通過所有網路介面的資料封包。在[超時]處設定擷取時間，當到達設定的超時時間後，會停止擷取資料封包。按一下[開始]開始擷取，並將本次擷取的結果下載並保存到顯示 **Web** 管理界面的電腦。，**AscenLink** 並不會存儲任何資料。按一下[停止]，會立刻停止擷取。

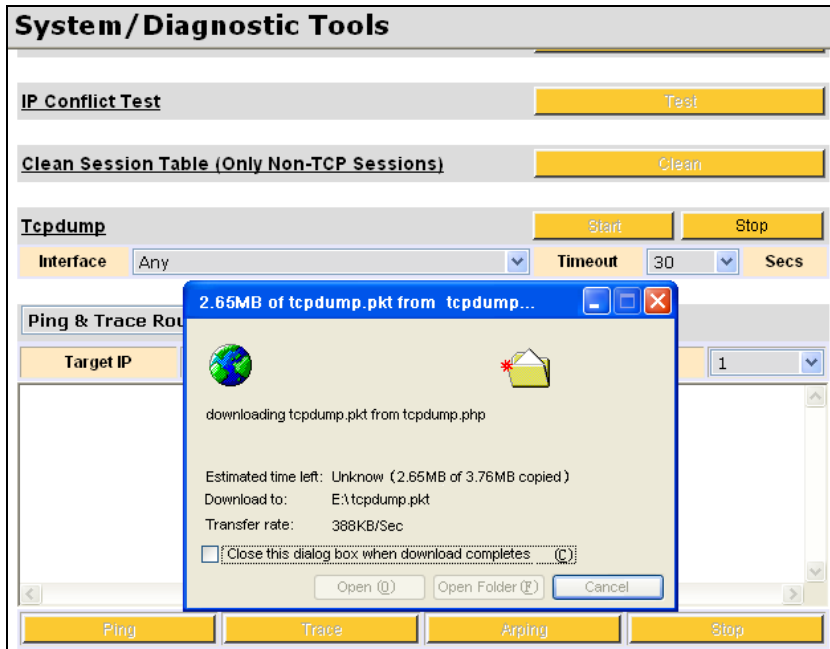


圖 2.65 Tcpdump 功能

Ping

ping 用以偵測網路狀況。

輸入 Target 的 IP 或 host name，可填入使用的介面有 WAN/LAN/DMZ 三種，若 ping WAN 介面時須指定 WAN link number。關於 ICMP 相關 error message 請參閱相關檔。

註：若使用 domain name 來 ping 時，須 web UI 上的[System] →[Network Setting]→[DNS Server]中先行指定 DNS Server。

網路尋徑

網路尋徑顯示封包從指定 port 到目的主機中間經由的路由。

輸入 Target 的 IP 或 hostname，選擇 Link 與 Index 後點選 traceroute 可指定從 WAN port 到目標主機的路由，HOST 為目標主機 IP 或 domain name，Link 可填入使用的介面有 WAN/LAN/DMZ 三種，若使用 WAN 介面時須指定 WAN link number。

註：若使用 domain name 來 traceroute 時，須在 web UI 上的[System]→[Network Setting]→[DNS Server]中先行指定 DNS Server。

Arping

arping 用以偵測某部主機的 MAC 位址。

輸入 Target 的 IP 或 host name，可填入使用的介面有 WAN/LAN/DMZ 三種，若 arping WAN 介面時須指定 WAN link number。關於 ARP 相關 error message 請參閱相關檔。

註：若使用 domain name 來 arping 時，須 web UI 上的[System]→[Network Setting]→[DNS Server]中先行指定 DNS Server。

顯示與清空 ARP 表

該功能可以顯示選定介面的 ARP 資訊，並可清空。

在“網路介面”欄位選擇相應的網路介面；點選“顯示”按鈕，會顯示該網路介面相應的 ARP 信息。

或者在“網路介面”欄位選擇相應的網路介面；點選“清空”按鈕，會出現提示資訊：“確定要繼續”，點選確定，講清空該網路介面相應的 ARP 資訊，清空後會出現資訊提示框，顯示：“成功清空 ARP 表”。

Nslookup 工具

Nslookup 用以查詢主機網域名稱。輸入目標主機，可選擇查詢的類型，包括 “ANY、A、CNAME、HINFO、MX、NS、PTR、SOA”。伺服器可選擇內建 DNS、Multihoming、其他伺服器中的一種。

點選 “Nslookup” 按鈕，開始進行查詢，會顯示目標主機的相應功能變數名稱。點選 “停止” 可結束查詢。

2.11 Date/Time (系統時間)

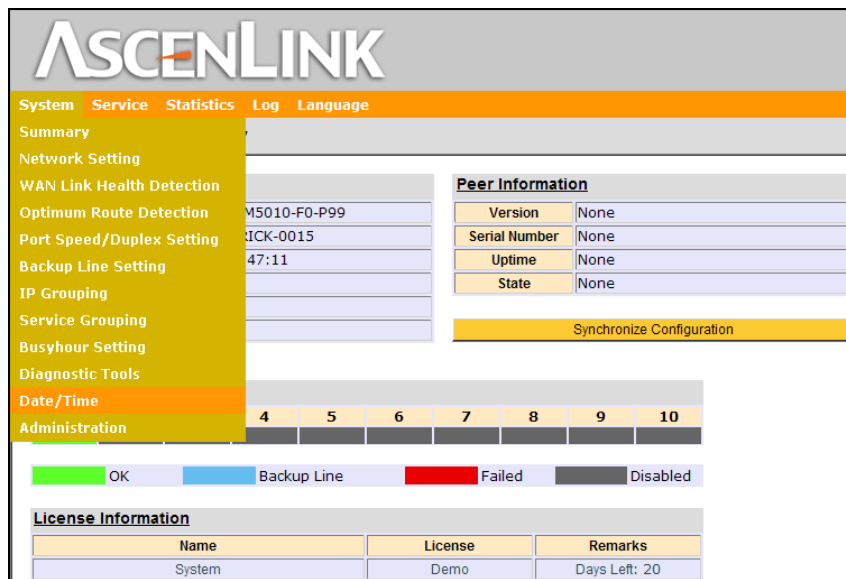


圖 2.66 System/ Date/Time 功能所處位置

在這裏您可以對 AscenLink 與系統時間相關的專案進行設定。日期請依照「年／月／日」的格式輸入日期。時間則是依照「時：分：秒」的格式來輸入 24 小時制的本地時間。

至於時區的部分，請從列表之中選取您的所在地。例如欲選擇北京時間，請先從左邊的列表當中選擇「Asia」，再從右邊的列表當中找出「Beijing」。

AscenLink 可以使用 NTP 通訊協定來進行網路校時。您可以從列表之中選取所要使用的網路時間伺服器 (Time Server)，也可以自行增減伺服器列表的內容。按下「校正系統時間 (Synchronize Time)」可以馬上進行網路校時的動作。

2.12 Administration (系統管理)

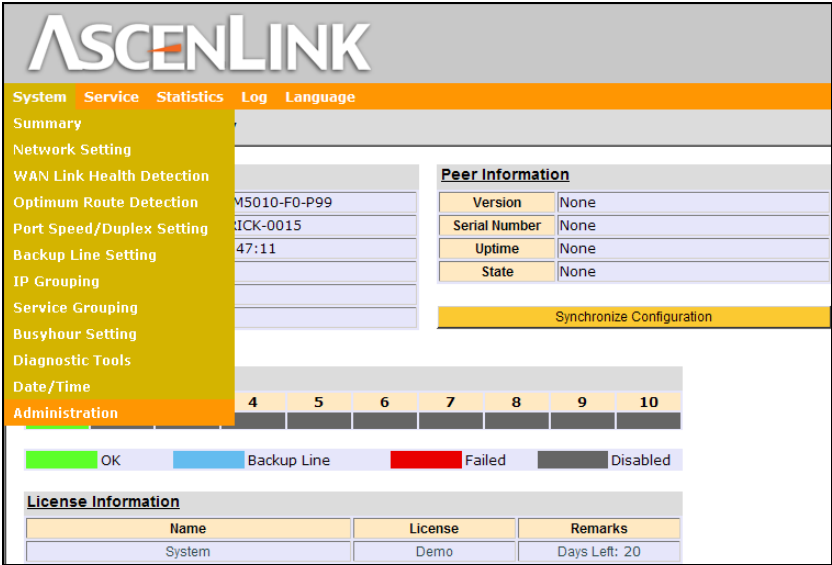


圖 2.67 System/ Administration 功能所處位置

在這個分頁裏面，您可以更改 **Administrator** 與 **Monitor** 的密碼。由於每部 **AscenLink** 的出廠預設密碼均相同，建議您馬上更改預設密碼，以免造成安全上的漏洞。

AscenLink 允許使用者更改用來登入 **WebUI** 所使用的埠號。**AscenLink** 出廠預設使用 **443** 埠號登入 **WebUI**，為防止該埠號被虛擬伺服器的其他服務所佔用而發生衝突，使用者可自行設定登入 **WebUI** 所用的埠號。

若是您從寬宇科技的網站或是您的系統整合商處得到更新的軟體，就可以進行更新/降級系統軟體 (**Firmware Update/Downgrade**) 的工作。只要按下「更新 (**Update**)」/「降級 (**Downgrade**)」，遵循螢幕上每一步驟指示即可。

您可以下載系統的設定到一個檔案之中，成為備援。也可將之前下載的檔案上傳回 **AscenLink**，回到之前的設定。我們建議您在做重大設定的改變前後，都利用下載系統設定的功能，製作備援設定檔案，縮短設定錯誤時當機的時間。

最後，在系統維護 (**Maintenance**) 的部分，可以選擇將系統設定恢復成出廠預設值 (**Factory Default**) 以及重開機 (**Reboot**) 等等。由於 **HTML** 語法本身的限制，在重開機完成之後也不會顯示開機完成的資訊。請等待二分鐘後再用瀏覽器試著連線 **WebUI** 即可。

Administrator Password(Administrator 密碼)

在這裏可以新增、刪除、修改管理者的帳號和密碼。

欄位	值	說明
Select Account(選擇帳號)	Add New <administrator 群組>	此欄位可讓你選擇新帳號或舊有帳號以進行帳號的設定。如果選擇目前登入帳號，則區塊按鈕 Add Account (加入帳號)會變成 Set Account (設定帳號)。
New Account(新帳號)		若要新增帳號，請在此欄位輸入新帳號 ID。
New Password(新密碼)		無論是新增或是修改帳號，請在此欄位輸入新密碼。
Password Verification (確認密碼)		請重新輸入一次新密碼以進行確認。

表 2.17 Administrator 密碼管理

Monitor Password (Monitor 密碼)

在此可以新增、刪除、修改一般使用者的密碼。

欄位	值	說明
Select Account(選擇帳號)	Add New <Monitor 群組>	此欄位可讓你選擇新帳號或舊有帳號以進行帳號的設定。如果選擇目前登入賬號，則區塊按鈕 Add Account(加入帳號)會變成 Set Account (設定帳號)。
New Account(新帳號)		若要新增帳號，請在此欄位輸入新帳號 ID。
New Password(新密碼)		無論是新增或是修改帳號，請在此欄位輸入新密碼。
Password Verification (確認密碼)		請重新輸入一次新密碼以進行確認。

表 2.18 Monitor 密碼管理

Firmware Update(更新系統軟體)

點選 Update 以上傳新的 Firmware 至 AscenLink 來更新軟體，關於軟體更新的方式與內容請參照附錄。

Configuration File(系統設定)

可將目前的 AscenLink 的 Configuration 備援到自己的電腦，使用方式與內容請參照附錄。

Maintenance(系統維護)

可點選 Factory Default 以將所有的資料還原至出廠預設的狀態，同命令列介面的 resetconfig 指令，另一個 Reboot，可重新將 AscenLink 開機，序列埠控制臺的指令請參照附錄。

WebUI Port(設定 WebUI 埠號):

輸入欲使用的埠號，點選“設定端口”完成更改，更改成功後需使用新的埠號登入 WebUI。註意不能將 WebUI 埠號設定成 AscenLink 保留埠，否則 AscenLink 會提示設定不成功，並恢復上一次正確的埠號設定。AscenLink 保留埠見下表；

埠	服務	埠	服務	埠	服務
1	tcpmux	102	iso-tsap	530	courier
7	echo	103	gppitnp	531	Chat
9	discard	104	acr-nema	532	netnews
11	systat	109	pop2	540	uucp
13	daytime	110	pop3	556	remotefs
15	netstat	111	sunrpc	563	nnntp+ssl
17	qotd	113	auth	587	
19	chargen	115	sftp	601	
20	ftp-data	117	uucp-path	636	ldap+ssl
21	ftp-cntl	119	nnntp	993	imap+ssl
22	ssh	123	NTP	995	pop3+ssl
23	telnet	135	loc-srv/epmap	1111	AscenLink reserved
25	smtp	139	netbios	1900	AscenLink reserved
37	time	143	imap2	2005	AscenLink reserved
42	name	179	BGP	2049	nfs
43	nickname	389	ldap	2223	AscenLink reserved
53	domain	465	smtp+ssl	2251	AscenLink reserved
77	priv-rjs	512	print/exec	3535	AscenLink reserved
79	finger	513	login	3636	AscenLink reserved
87	ttylink	514	shell	4045	lockd
95	supdup	515	printer	6000	x11
101	hostriame	526	tempo	49152	AscenLink reserved

表 2.19 AscenLink 保留埠

License Control（授權設定）

授權設定提供使用者進行所有授權碼的設定工作。AscenLink 提供授權項目“系統授權”、“通道路由”及“型號變更授權”；“系統授權”包括系統基本功能的試用及永久使用授權，“通道路由”則為選購功能，包括功能的試用及永久使用授權。

每個授權項目狀態包括：“無”、“試用”及“有”。“無”表示該功能目前未經授權，無法使用；“試用”表示該功能目前已獲得試用授權；“有”表示該功能目前已取得永久使用之授權。

在“授權碼”欄位中填入授權碼後，會即時顯示填入的授權碼格式是否正確以及該授權碼的種類(系統授權、通道路由、變更型號等)，如顯示訊息無誤即可點擊“套用”完成授權碼設定。

授權成功之後，在授權項目狀態中可以看到相應升級之後的授權名稱以及是否已經啟用。

目錄

第三章 Service (服務) 功能表	3-8
3.1 Firewall (防火牆)	3-9
3.2 NAT (位址轉換)	3-15
3.3 Persistent Routing (持續路由)	3-19
3.4 Auto Routing (自動路由)	3-29
3.5 Virtual Server (虛擬主機)	3-45
3.6 Inbound BM (對內頻寬管理)	3-52
3.7 Outbound BM (對外頻寬管理)	3-62
3.8 Connection Limit (連線限制)	3-69
3.9 Cache Redirect (快取重定向)	3-72
3.10 Tunnel Routing (通道路由).....	3-77
3.11 Multihoming (多重定址).....	3-103
3.11.1 在設定 Multihoming 前須有以下的準備工作	3-105
3.11.2 Multihoming 啟用設定	3-106
3.12 Internal DNS (內建 DNS).....	3-118
3.13 SNMP (簡單網路管理)	3-120
3.14 IP-MAC Mapping (IP-MAC 對應)	3-122

圖目錄

圖 3.1	Service 功能圖.....	3-8
圖 3.2	Service/Firewall 功能所處位置	3-9
圖 3.3	Firewall 範例 1 架構示意圖.....	3-12
圖 3.4	Firewall 範例 2 架構示意圖.....	3-13
圖 3.5	Service /NAT 功能所處位置.....	3-15
圖 3.6	NAT 設定圖一	3-17
圖 3.7	NAT 設定圖二	3-17
圖 3.8	Non-NAT 模式簡易範例架構示意圖.....	3-18
圖 3.9	Service /Persistent Routing 功能所處位置	3-19
圖 3.10	Persistent Routing 範例 1 架構示意圖.....	3-23
圖 3.11	Persistent Routing 範例 2 架構示意圖.....	3-25
圖 3.12	Persistent Routing 範例 3 架構示意圖.....	3-25
圖 3.13	Service /Auto Routing 功能所處位置.....	3-29
圖 3.14	Auto Routing 範例 1 架構示意圖	3-33
圖 3.15	Auto Routing 範例 2 架構示意圖	3-36
圖 3.16	Auto Routing 範例 3 架構示意圖	3-40
圖 3.17	Service/Virtual Server 功能所處位置.....	3-45
圖 3.18	Virtual Server 範例 1 架構示意圖	3-47
圖 3.19	Virtual Server 範例 2 架構示意圖	3-50
圖 3.20	Service/Inbound BM 功能所處位置	3-52
圖 3.21	Inbound BM Classes 設定表格.....	3-53
圖 3.22	Inbound BM 範例 1 架構示意圖.....	3-56
圖 3.23	Inbound BM 範例 2 架構示意圖.....	3-59
圖 3.24	Service /Outbound BM 功能所處位置	3-62
圖 3.25	Outbound BM 範例 1 架構示意圖	3-65
圖 3.26	Outbound BM 範例 2 架構示意圖	3-67

圖 3.27	Service /Connection Limit 功能所處位置	3-69
圖 3.28	Connection Limit 欄位介紹	3-70
圖 3.29	Connection Limit 設定範例	3-71
圖 3.30	Service /Cache Redirect 功能所處位置	3-72
圖 3.31	Cache Redirect 設定欄位	3-73
圖 3.32	Cache Miss 狀態下資料流走向	3-75
圖 3.33	Cache Hit 狀態下資料流走向	3-76
圖 3.34	Service / Tunnel Routing 功能所處位置	3-77
圖 3.35	Tunnel Routing 範例 2 架構示意圖	3-88
圖 3.36	Tunnel Routing 範例 3 架構示意圖	3-91
圖 3.37	Tunnel Routing 範例 4 架構示意圖	3-95
圖 3.38	Service /Multihoming 功能所處位置	3-103
圖 3.39	Multihoming 全局設定	3-106
圖 3.40	Multihoming Policy 設定	3-107
圖 3.41	Domain Setting	3-108
圖 3.42	Domain Setting in relay	3-111
圖 3.43	啓用災備功能	3-112
圖 3.44	Multihoming 範例 (1) 架構示意圖	3-113
圖 3.45	Multihoming 範例 (2) 架構示意圖	3-115
圖 3.46	Service / Internal DNS 功能所處位置	3-118
圖 3.47	Service / Tunnel Routing 功能所處位置	3-120
圖 3.48	Service / IP-MAC MAPPING 功能所處位置	3-122

表目錄

表 3.1	System Information 信息列表.....	3-11
表 3.2	Firewall 範例 1 設定內容	3-13
表 3.3	Firewall 範例 2 製作內容	3-14
表 3.4	NAT 各功能選項解釋之參照表.....	3-16
表 3.5	Persistent Routing 各功能選項解釋之參照表	3-21
表 3.6	Persistent Routing 範例 1 設定內容	3-24
表 3.7	Persistent Routing 範例 2 設定內容	3-28
表 3.8	Persistent Routing 範例 3 根據 Web 服務設定內容.....	3-28
表 3.9	Persistent Routing 範例 3 根據 IP 位址設定內容.....	3-28
表 3.10	Policies 欄位設定說明表.....	3-31
表 3.11	Auto Routing 各功能選項解釋之參照表.....	3-32
表 3.12	AutoRouting 範例 1 Policies 設定內容	3-34
表 3.13	AutoRouting 範例 1 Filters 設定內容	3-35
表 3.14	AutoRouting 範例 2 Policies 設定內容	3-37
表 3.15	AutoRouting 範例 2 Filters 設定內容	3-39
表 3.16	Auto Routing 範例 3 相關資訊.....	3-41
表 3.17	Auto Routing 範例 3:記錄及本機 ID 設定(Beijing 總公司).....	3-41
表 3.18	Auto Routing 範例 3:Tunnel Group 設定(Beijing 總公司)	3-41
表 3.19	Auto Routing 範例 3:Routing Rules 設定(Beijing 總公司)	3-42
表 3.20	Auto Routing 範例 3:Auto Routing Policies 設定(Beijing 總公司).....	3-42
表 3.21	Auto Routing 範例 3:Auto Routing Filters 設定(Beijing 總公司)	3-42
表 3.22	Auto Routing 範例 3:記錄及本機 ID 設定(Shanghai 分公司)	3-43
表 3.23	Auto Routing 範例 3:Tunnel Group 設定(Shanghai 分公司).....	3-43
表 3.24	Auto Routing 範例 3:Routing Rules 設定(Shanghai 分公司)	3-43
表 3.25	Auto Routing 範例 3:Auto Routing Policies 設定(Shanghai 分公司)	3-44
表 3.26	Auto Routing 範例 3:Auto Routing Filters 設定(Shanghai 分公司).....	3-44
表 3.27	Virtual Server 各功能選項解釋之參照表	3-46

表 3.28	Virtual Server 範例 1 設定內容.....	3-49
表 3.29	Virtual Server 範例 2 設定內容.....	3-51
表 3.30	Inbound BM Classes 欄位說明表	3-54
表 3.31	Inbount BM 各功能選項解釋之參照表.....	3-55
表 3.32	Inbount BM 範例 1 Class 設定內容.....	3-57
表 3.33	Inbount BM 範例 1 Filters 設定內容	3-58
表 3.34	Inbount BM 範例 2 Class 設定內容	3-60
表 3.35	Inbount BM 範例 2 Filters 設定內容	3-61
表 3.36	Outbound BM Class 欄位說明表	3-63
表 3.37	Outbound BM Filters 欄位說明表.....	3-64
表 3.38	Outbound BM 範例 1Classes 設定內容	3-66
表 3.39	Outbound BM 範例 1Filters 設定內容.....	3-66
表 3.40	Outbound BM 範例 2 Classes 設定內容.....	3-68
表 3.41	Outbound BM 範例 2 Filters 設定內容.....	3-68
表 3.42	Connection Limit 記錄週期設定	3-70
表 3.43	Connection Limit Rule 設定	3-71
表 3.44	Cache Redirect 欄位說明表	3-73
表 3.45	Cache Redirect 各功能選項解釋之參照表	3-74
表 3.46	Tunnel Group 記錄及本地端 ID 設定.....	3-79
表 3.47	Tunnel Group 各功能選項解釋之參照表	3-80
表 3.48	Routing Rules 各功能選項解釋之參照表	3-81
表 3.49	Routing Rules 各功能選項解釋之參照表	3-82
表 3.50	Tunnel Routing 範例 1 設定	3-83
表 3.51	Tunnel Routing 範例 1:Tunnel Group 設定(1).....	3-84
表 3.52	Tunnel Routing 範例 1:Routing Rules 設定(1).....	3-85
表 3.53	Tunnel Routing 範例 1:Tunnel Group 設定(2).....	3-85
表 3.54	Tunnel Routing 範例 1:Routing Rules 設定(2).....	3-85
表 3.55	Tunnel Routing 範例 1:Tunnel Group 設定(3).....	3-86
表 3.56	Tunnel Routing 範例 1:Routing Rules 設定(3).....	3-86
表 3.57	Tunnel Routing 範例 1: Inbound BM Filter 設定.....	3-87

表 3.58	Tunnel Routing 範例 1: Outbound BM Filter 設定	3-87
表 3.59	Tunnel Routing 範例 2 相關資訊.....	3-89
表 3.60	Tunnel Routing 範例 2:記錄及本機 ID 設定(Beijing 總公司)	3-89
表 3.61	Tunnel Routing 範例 2:Tunnel Group 設定(Beijing 總公司).....	3-89
表 3.62	Tunnel Routing 範例 2:Routing Rules 設定(Beijing 總公司)	3-90
表 3.63	Tunnel Routing 範例 2:記錄及本機 ID 設定(Shanghai 分公司).....	3-90
表 3.64	Tunnel Routing 範例 2:Tunnel Group 設定(Shanghai 分公司)	3-90
表 3.65	Tunnel Routing 範例 2:Routing Rules 設定(Shanghai 分公司)	3-90
表 3.66	Tunnel Routing 範例 3 相關資訊.....	3-92
表 3.67	Tunnel Routing 範例 3:記錄及本機 ID 設定(Beijing 總公司)	3-92
表 3.68	Tunnel Routing 範例 3:Tunnel Group 設定(Beijing 總公司).....	3-92
表 3.69	Tunnel Routing 範例 3:Routing Rules 設定(Beijing 總公司)	3-93
表 3.70	Tunnel Routing 範例 3:記錄及本機 ID 設定(Shanghai 分公司).....	3-93
表 3.71	Tunnel Routing 範例 3:Tunnel Group 設定(Shanghai 分公司)	3-93
表 3.72	Tunnel Routing 範例 3:Routing Rules 設定(Shanghai 分公司)	3-93
表 3.73	Tunnel Routing 範例 3:記錄及本機 ID 設定(Tianjin 分公司)	3-94
表 3.74	Tunnel Routing 範例 3:Tunnel Group 設定(Tianjin 分公司).....	3-94
表 3.75	Tunnel Routing 範例 3:Routing Rules 設定(Tianjin 分公司)	3-94
表 3.76	Tunnel Routing 範例 4:相關資訊	3-96
表 3.77	Tunnel Routing 範例 4:記錄及本機 ID 設定(Beijing 總公司)	3-96
表 3.78	Tunnel Routing 範例 4:Tunnel Group 設定(Beijing 總公司).....	3-96
表 3.79	Tunnel Routing 範例 4:Routing Rules 設定(Beijing 總公司).....	3-97
表 3.80	Tunnel Routing 範例 4:Auto Routing Policies 設定(Beijing 總公司)	3-97
表 3.81	Tunnel Routing 範例 4:Auto Routing Filters 設定(Beijing 總公司).....	3-97
表 3.82	Tunnel Routing 範例 4:記錄及本機 ID 設定(Shanghai 分公司).....	3-98
表 3.83	Tunnel Routing 範例 4:Tunnel Group 設定(Shanghai 分公司)	3-98
表 3.84	Tunnel Routing 範例 4:Routing Rules 設定(Shanghai 分公司)	3-98
表 3.85	Tunnel Routing 範例 4:Auto Routing 設定(Shanghai 分公司)	3-99
表 3.86	Tunnel Routing 範例 4:Auto Routing Filters 設定(Shanghai 分公司)	3-99
表 3.87	Tunnel Routing 範例 4:記錄及本機 ID 設定(Tianjin 分公司)	3-100

表 3.88 Tunnel Routing 範例 4:Tunnel Group 設定(Tianjin 分公司).....	3-100
表 3.89 Tunnel Routing 範例 4:Routing Rules 設定(Tianjin 分公司).....	3-100
表 3.90 Tunnel Routing 範例 5 設定	3-101
表 3.91 Tunnel Routing 範例 5:Tunnel Group 設定(1).....	3-101
表 3.92 Tunnel Routing 範例 5:Routing Rules 設定(1).....	3-101
表 3.93 Tunnel Routing 範例 5:Tunnel Group 設定(2).....	3-102
表 3.94 Tunnel Routing 範例 5:Routing Rules 設定(2).....	3-102
表 3.95 Tunnel Routing 範例 5: Persistent Rules 設定.....	3-102
表 3.96 Multihoming 全域設定欄位說明表.....	3-106
表 3.97 Multihoming Policy 欄位說明表.....	3-107
表 3.98 Multihoming 各功能選項解釋之參照表.....	3-110
表 3.99 Relay 模式下網域設定說明	3-111
表 3.100 Multihoming 範例 1 Virtual Server 設定	3-114
表 3.101 Multihoming 範例 1 Policy 設定.....	3-114
表 3.102 Multihoming 範例 1 Domain 設定.....	3-114
表 3.103 Multihoming 範例 2 Virtual Server 設定	3-116
表 3.104 Multihoming 範例 2 Policy 設定	3-116
表 3.105 Multihoming 範例 2 Domain 設定.....	3-117
表 3.106 Global Setting 各功能選項解釋之參照表	3-119
表 3.107 Domain Setting 各功能選項解釋之參照表	3-119
表 3.108 SNMP v1/2 各功能選項解釋之參照表.....	3-121
表 3.109 SNMP v3 各功能選項解釋之參照表.....	3-121
表 3.110 IP-MAC MAPPING 各功能選項解釋之參照表.....	3-122

第三章 Service (服務) 功能表

這一章是繼前一章完成網路設定之後，討論如何讓 AscenLink 執行網路管理需求之各項設定。我們從下一個功能架構圖中，可以得知 AscenLink 可以提供那些服務。

這些服務常見於網路管理的需求，例如防火牆的功能，提供您防止駭客攻擊，或者是對某些網路存取行為的管制。路由設定可以讓連線的建立和資料封包的傳輸，依據網路情況而得以調整和管理。頻寬管理可以根據網路使用時間和應用類別（如 Http, TCP, UDP 等）加以管理，讓頻寬能獲得更有效率的使用。Multihoming 功能可以讓對外提供的網路服務(如 WWW) 在多線路的情況下，不會因為某一路線路故障而中斷對外服務，或是依據流量分配原則，有效使用每一路線路。

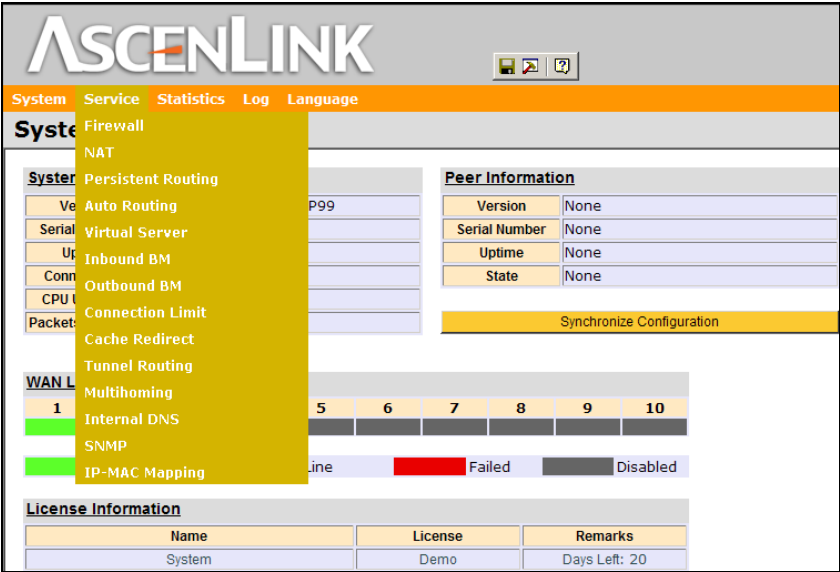


圖 3.1 Service 功能圖

3.1 Firewall (防火牆)

本節介紹 Firewall 的設定使用，在本章中由於每個功能的設定都有複雜的表格和欄位，每個欄位中有些還有下拉式選擇，選擇不同的參數，因此爲了讓讀者清楚瞭解整個設定，編寫時用表格的方式呈現整個設定表格和欄位，同時解釋每個欄位值的意義，並配合適當的範例解釋。

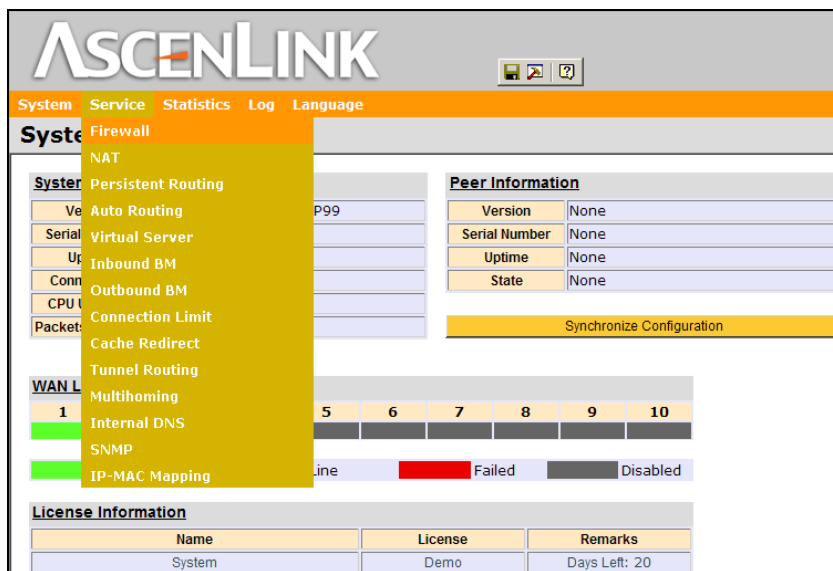


圖 3.2 Service/Firewall 功能所處位置

設定 Firewall 的表格中，可以列出許多 Rule (規則)，每一條規則都可獨立選擇 Enable 或是 Disable。規則的執行是由上到下逐一比對。

欄位	值	說明
E	Enable (勾選) Disable (不勾選)	勾選這個 Check Box 時,此規則是在可比對的狀態,AscenLink 會執行這條規則的對比。 Check Box 為空格時, AscenLink 不會執行這條規則的對比。
When (時段)	Busy (尖峰時段) Idle (離峰時 段) All-Time (所有時段)	有三種選項,尖峰時段、離峰時段及所有時段。所有時段為 24 小時都採用此規則, Busy, Idle 時間設定請參照第二章 [System]→[Busyhour Setting] 的設定。
Source (來源)	IP Address IP Range Subnet WAN WAN # LAN DMZ Tunnel Any address FQDN < IP Grouping Name>	比對封包來源處,基本上有八種的封包來源。 IP Address : 來自單一 IP 位址的封包,用在單一主機的 IP 位址,例如 192.168.1.4。 IP Range : 來自一段 IP 位址的封包,例如連續 IP 192.168.1.10-192.168.1.20。 Subnet : 來自某一個網段的封包,例如: 192.168.1.0/255.255.255.0。 WAN : 來自 WAN 埠的任何封包。 WAN # : 來自指定的 WAN 埠的任何封包。 LAN : 來自 LAN 埠的任何封包。 DMZ : 來自 DMZ 埠的任何封包。 Tunnel : 來自 Tunnel 埠的任何封包。 Any Address : 來來自任何位址之封包。 FQDN : 來自某一個 FQDN 之封包。 除了基本這幾項比對封包來源的設定外,如果在第二章 System/IP Grouping 有設定類別,則這些 Group Name 也會出現在選項中,如果加以設定, AscenLink 也會比對來自群組的封包。
Destination (目的地)	IP Address IP Range Subnet WAN LAN DMZ Localhost Any address FQDN < IP Grouping Name>	比對封包的目的地,比對方式同上。 同樣的除了這九種目的地之外,如果設定有 IP Grouping 的群組,這些名稱也會出現在選項中, AscenLink 也會比對來自群組的封包。
Service (服務)	FTP(21) SSH (22) TELNET(23) SMTP(25) DNS(53) HTTP(80) POP3(110)	比對需要過濾的服務專案,例如接受會拒絕 FTP 的封包。針對 TCP 或 UDP 可以自訂某個 port 或 port range 如 TCP@123-234,表示 Port 123 ~ 234 的封包被監聽比對。

	H323 (1720) ICMP TCP@ UDP@ Any	
Action (處理)	Accept Deny	Accept (接受)：表示當符合此項規則時防火牆允許透過。 Deny (拒絕)：表示當符合此項規則時防火牆會丟掉封包。
L (記錄)	Enable(勾選) Disable (不勾選)	當這個 Check Box 打勾，表示當此條規則有被引用到時，其結果會記錄到 log 中，空白時則沒有任何記錄產生。

表 3.1 System Information 信息列表

註：AscenLink 對封包的檢查，預設值是全部接受。

範例一

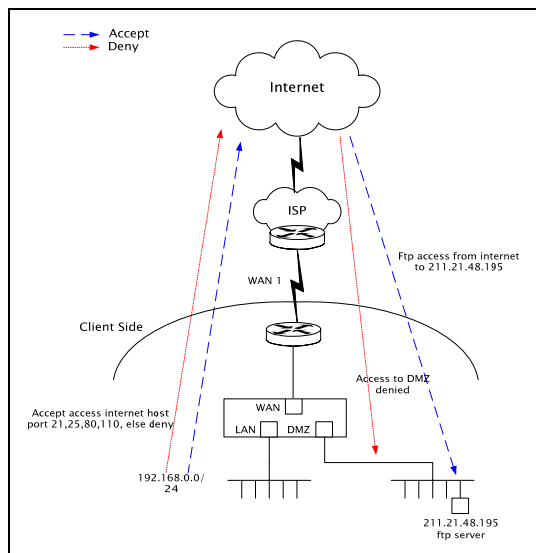


圖 3.3 Firewall 範例 1 架構示意圖

封包檢查條件：

- 來自 Internet 使用者可以連線 ftp server 211.21.48.195/21，但不可存取其他資源。
- 區域網路使用者可以連線 Internet 上任意主機的 smtp/25, http/80, pop3/110
- 其餘皆禁止。

設定內容如下：

Source	Destination	Service	Action
WAN	211.21.48.195	FTP/21	Accept
WAN	DMZ	Any	Deny
LAN	WAN	HTTP/80	Accept
LAN	WAN	SMTP/25	Accept
LAN	WAN	FTP/21	Accept
LAN	WAN	POP3/110	Accept
LAN	WAN	Any	Deny

表 3.2 Firewall 範例 1 設定內容

範例二

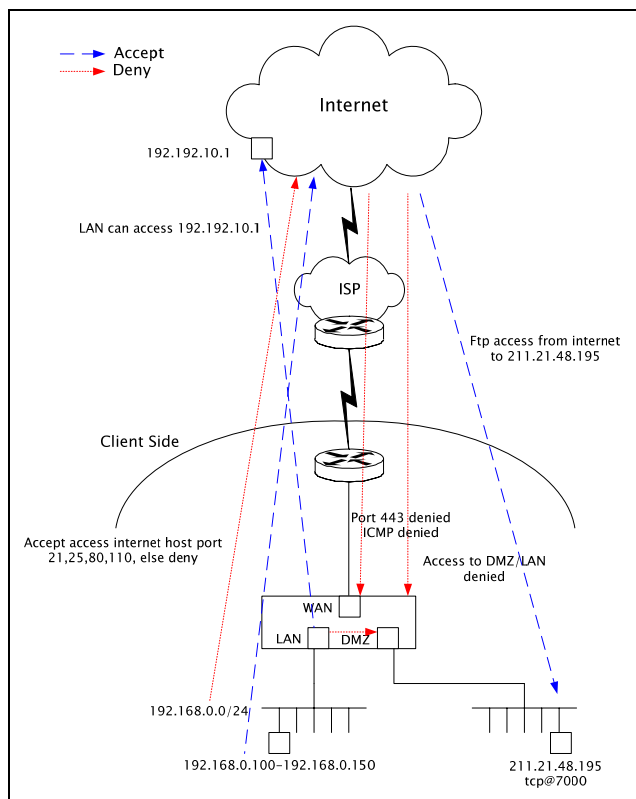


圖 3.4 Firewall 範例 2 架構示意圖

封包檢查條件：

- 來自 Internet 使用者可以透過 TCP port 7000 連線位於 DMZ 的 ftp server 211.21.48.195。
- 區域網路主機 192.168.0.100-192.168.0.150 可以存取 Internet，其餘皆否。
- 來自 Internet 使用者不可連線 AscenLink 的介面 (port 443) 在 WAN 端的封包會直接傳送到 AscenLink 的網路介面 (WAN Port)，就是這裏所謂的 Localhost。
- 區域網路使用者可以存取 192.168.10.1 的 ftp Service。
- (來自 Internet 使用者不可 ping AscenLink，其餘皆可。Ping 的封包示屬於 ICMP 通訊所規範，因此攔截 ICMP 封包，Ping 就無法正常工作。
- 區域網路不可存取位於 DMZ 的主機。
- 廣域網路不可存取區域網路 DMZ。

設定內容如下：

Source	Destination	Service	Action
WAN	211.21.48.195	TCP@7000	Accept
192.168.0.100-192.168.0.150	WAN	Any	Accept
WAN	Localhost	TCP@443	Deny
LAN	192.192.10.1	FTP(21)	Accept
WAN	Localhost	ICMP	Deny
LAN	DMZ	Any	Deny
WAN	DMZ	Any	Deny
WAN	LAN	Any	Deny

表 3.3 Firewall 範例 2 製作內容

3.2 NAT (位址轉換)

AscenLink 在網路應用上，是架構在網路的閘道出口，對於屬於 LAN 區域網路的主機，設定私有 IP，如果需要流覽外界之 Internet 網路，則需要將內部私有 IP，轉譯為公開 IP。

NAT 這項功能可以提供這樣的服務。在此可設定 Non-NAT，一對一、一對多、多對一、多對多的 NAT，AscenLink 所預設的 NAT 為多對一的狀態，即從某一個 WAN Link (廣域網路連線) 所出去的封包，皆 NAT 成 AscenLink 在此廣域網路連線所取得的 IP，即設定在 WAN Port 上的 IP 位址。

Non-NAT 模式主要適用於針對私有專線或 MPLS 網路，以便於來自 WAN 的主機可直接與 DMZ 區域的主機進行通訊，此時 AscenLink 可以對 VPN 做負載平衡及線路備援。



圖 3.5 Service /NAT 功能所處位置

欄位	值	說明
啟用 NAT		選擇以啟用 NAT 功能。當不啟用該功能時，可以將 AscenLink 視為普通的 router，此時來自 WAN 線路的主機可直接與 DMZ 區域的主機進行通訊。
WAN		指定欲修改的廣域網路連線 勾選“啟用”前的核取方塊選擇是否啟用該 WAN 線路的 NAT 規則。
NAT Rule (NAT 規則)		在這個表格下，設定在此廣域網路連線上的位址轉換方式。
L (記錄)	Enable Disable	當這個 Check Box 打勾，表示當此條規則有被引用到時，其結果會記錄到 Log 中，空白時則沒有任何記錄產生。
When (時段)	Busy Idle All-time	選定此條規則發生作用的時間，可選擇 (Busy) 尖峰時段/Idle(離峰時段) /All Time (所有時段) 三種中的一種，有關時段的規劃，在第二章已經說明。
Source (來源)		將使用此條規則的來源 IP 位址，可選擇： IP Address(單一 IP 位址) IP Range(連續一段 IP 位址) Any Address(任何位址) 除了這三項選項外，先前定義在 [System]→[IP Grouping] 中的自訂 IP 群組類別，也會出現在選項之內。 註意：來源 IP 位址需為 LAN 內部區域網路或 DMZ 埠的 IP。
Service (服務)		在此欄位可訂定義欲使用此規則的埠號，可為 TCP 或 UDP 埠號或者是 ICMP，亦可使用先前自訂的 Service Grouping (第二章提到，[System]→[Service Grouping] 類別，即網路服務群組，只要在 Service Grouping 中設定的群組，都會成為這個欄位之下拉式選項之一)。
Translated (轉譯成)		這個欄位需填入欲轉譯的位址，預設的轉譯位址是 AscenLink 在此廣域網路連線所取得的 IP，為多對一的模式。在此可以輸入單一 IP 或者連續一段 IP 位址。

表 3.4 NAT 各功能選項解釋之參照表

啓用 NAT

例如：區域網路主機 (192.168.123.100) 從 WAN Link 1 出去封包來源位址，皆轉譯成 172.31.5.51。首先點選“啓用 NAT”前的方框，選擇 WAN 爲 1，然後後續設定如下：

Enable NAT
☒

WAN
1

Enable
☒

NAT Rules						
	E	When	Source	Service	Translated	L
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	Any Address	Any	10.17.0.70	<input type="checkbox"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All-Time	Any Address	Any	10.17.0.70	<input type="checkbox"/>

圖 3.6 NAT 設定圖一

不啓用 NAT

當選擇不用 NAT 功能時，AscenLink 就進入 Non-NAT 模式，所有的來自 WAN 線路的主機可直接於 DMZ 區域的主機進行通訊，此時 AscenLink 相當於一台 Router，連線不同的網段。

Enable NAT
☐

圖 3.7 NAT 設定圖二

註：當選擇不啓用 NAT 功能時，所有的 WAN 線路都將會不啓用 NAT 功能。

Non-NAT 模式簡易範例

網路架構如下：

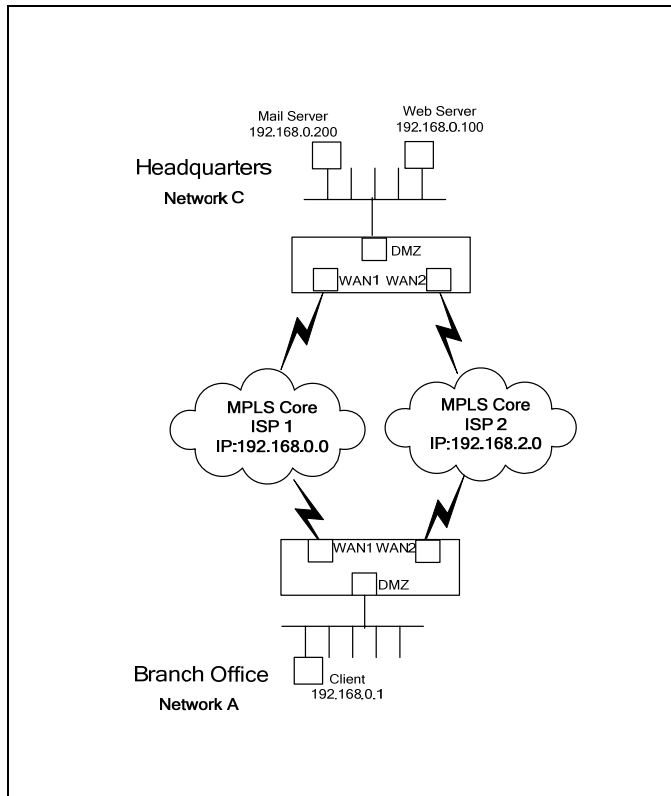


圖 3.8 Non-NAT 模式簡易範例架構示意圖

由上圖可知，Non-NAT 針對私有專線或 MPLS 網路，可以使分公司的主機直接與總公司的伺服器進行通訊，當 ISP1 線路發生斷線或者出現故障時，AscenLink 會自動切換到 ISP2 線路，此外 AscenLink 還可以根據各個線路的負載對 VPN 做負載平衡。

3.3 Persistent Routing (持續路由)

AscenLink 可以規劃與外界建立通訊連線 (Connection) 的路徑，當內部的主機欲存取 Internet 網路上的主機或站點時，須先建立連線，然後封包可以在這個固定的連線中傳輸進行通訊。不會經由其他路線進行傳輸。AscenLink 是一台多線路的頻寬管理器，因此可以規劃這些連線要使用那一條線路，讓線路的負載可以平衡，在下一節會討論到 Auto Routing (自動路由) 的規劃。所謂持續路由是指當要建立連線時，先依照 Auto Routing 的設定方法，決定用那一條線路，然後利用這條線路建立連線，之後參考 Persistent Routing (持續路由) 之設定方式，決定是否固定使用這個已經建立的連線。

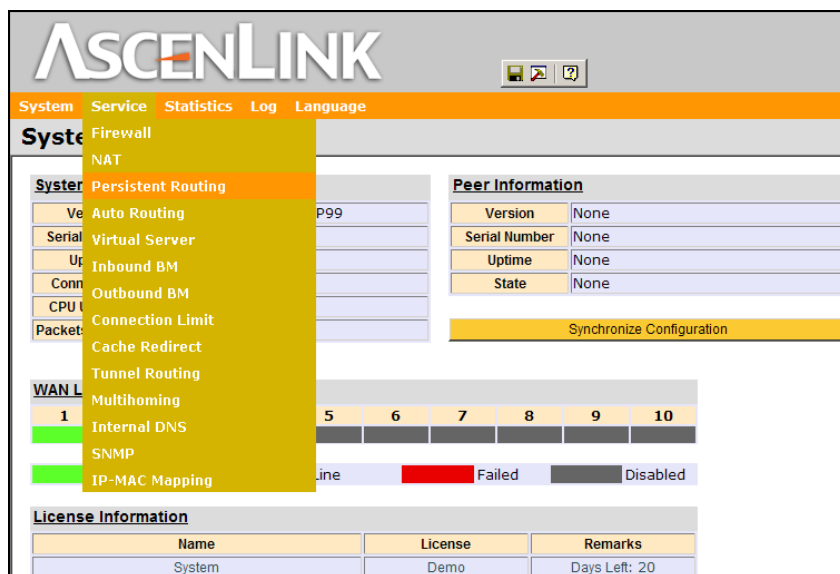


圖 3.9 Service /Persistent Routing 功能所處位置

欄位	值	說明
Timeout (逾時)	<second>	針對每一組來源和目的地的會話(Session)，當在設定的時間段內持續沒有任何封包產生就會清除掉持續路由的紀錄資料。
根據 Web 服務	針對 Web 服務設定持續路由規則。啟用此功能後，所有符合規則條件、目的地埠號為 80(HTTP)以及埠號為 443(HTTPS)的連線均會根據規則決定是否執行持續路由。	
E (用)	Enable Disable	Enable，啟用(勾選)，此規則被啟用。 Disable，不啟用 (空白)，此規則不用。
When (時段)	Busy Idle All Time	有三種選項尖峰時段、離峰時段、所有時間。所有時段為 24 小時，都採用此規則，Busy, Idle 時間設定請參照第二章 [System/ Virtual Server] 的設定。
Source (來源)	IP Address IP Range Subnet LAN DMZ Localhost Any Address FQDN < IP Grouping Name>	比對封包來源處，基本上有八種的封包來源。 IP Address：來自單一 IP 位址的封包，用在單一主機的 IP 位址，例如 192.168.1.4。 IP Range：來自一段 IP 位址的封包，例如連續 IP 192.168.1.10-192.168.1.20。 Subnet：來自某一個網段的封包，例如：192.168.1.0/255.255.255.0。 LAN：來自 LAN 埠的任何封包。 DMZ：來自 DMZ 埠的任何封包。 Localhost：來自 AscenLink 本身的封包。 Any Address：來來自任何位址之封包。 FQDN：來自某一個 FQDN 之封包。 除了基本這幾項比對封包來源的設定外，如果在第二章 (System/IP Grouping)有設定類別，則這些 Group Name 也會出現在選項中，如果加以設定，AscenLink 也會比對來自群組的封包。
Action (處理)	Do PR No PR	Do PR：表當比對相符的連線會使用持續路由。 No PR：表當比對相符的連線不會使用持續路由。(系統預設值)
L (記錄)	Enable Disable	打勾，Enable，連線記錄會在 Log 檔案裏。 空白，Disable，不會產生任何記錄。
根據 IP 位址	針對 IP 位址設定持續路由規則。啟用此功能後，符合此處規則條件的任何連線均會根據規則決定是否執行持續路由。	
E (用)	Enable Disable	Enable，啟用(勾選)，此規則被啟用。 Disable，不啟用 (空白)，此規則不用。
When (時段)	Busy Idle All Time	有三種選項尖峰時段、離峰時段、所有時間。所有時段為 24 小時，都採用此規則，Busy, Idle 時間設定請參照第二章 [System/ Virtual Server] 的設定。
Source (來源)	IP Address IP Range Subnet LAN DMZ Localhost	比對封包來源處，基本上有八種的封包來源。 IP Address：來自單一 IP 位址的封包，用在單一主機的 IP 位址，例如 192.168.1.4。 IP Range：來自一段 IP 位址的封包，例如連續 IP 192.168.1.10-192.168.1.20。

	Any Address FQDN < IP Grouping Name>	Subnet：來自某一個網段的封包，例如： 192.168.1.0/255.255.255.0。 LAN：來自 LAN 埠的任何封包。 DMZ：來自 DMZ 埠的任何封包。 Localhost：來自 AscenLink 本身的封包。 Any Address：來來自任何位址之封包。 FQDN：來自某一個 FQDN 之封包。 除了基本這幾項比對封包來源的設定外，如果在第二章 (System/IP Grouping) 有設定類別，則這些 Group Name 也會出現在選項中，如果加以設定，AscenLink 也會比對來自群組的封包。
Destination (目的地)	IP Address IP Range Subnet WAN FQDN	封包的目的地有五種： IP Address：某一個 IP 位址，例如某一台主機的 IP 位址，211.21.33.88。 IP Range：某一個區段的 IP 位址。 Subnet：某一個子網路。 WAN：廣域網路，只要封包流向的目的地在 WAN，都可以設定這個選項。 FQDN：某一個 FQDN。
Action (處理)	Do PR No PR	Do PR：表當比對相符的連線會使用持續路由。(系統預設值) No PR：表當比對相符的連線不會使用持續路由。
L (記錄)	Enable Disable	打勾，Enable，連線記錄會在 Log 檔案裏。 空白，Disable，不會產生任何記錄。

表 3.5 Persistent Routing 各功能選項解釋之參照表

通常使用 Persistent Routing 原因是在於外部伺服器，對於使用者連上來的 IP 作檢查時，需要使用者持續使用原來連線的線路，例如一些網路上的交易網站，基於安全的考量就會作這樣的封包檢查，但 Auto Routing 會依據條件切換不同連線之線路，這樣會造成存取交易網站時，被拒絕登入。

當同樣的規則分別設定在 **Auto Routing** 和 **Persistent Routing** 時，使用上的順序為：

1. 第一次建立連線使用 **Auto Routing** 的設定選擇線路，建立跟伺服器的連線。
2. 使用期間所有的連線皆依照 **Persistent Routing** 的設定採用相同的廣域網路連線。
3. 當連續一段時間 (**timeout** 的設定) 沒有任何連線時，系統清掉 **Persistent Routing** 所記錄的路徑表資料，一切再由 **Auto Routing** 開始選擇路徑。

範例一：根據 IP 位址簡單設定

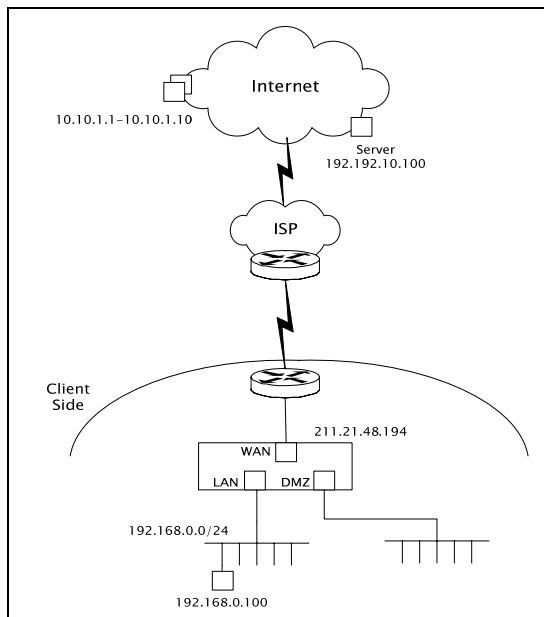


圖 3.10 Persistent Routing 範例 1 架構示意圖

路由條件：

- 由 LAN 中 192.168.0.100 到 192.192.10.100 所建立的連線，不採用 Persistent Routing。
- DMZ 到 WAN 的所有建立的連線，不採用 Persistent Routing。
- LAN 到 10.10.1.1~10.10.1.10 間的主機，所建立的連線，不採用 Persistent Routing。
- 由於根據 IP 位址的預設值是[DoPR]，因此若不設定任何規則，則所有的連線都會使用 Persistent Routing。

設定內容如下：

Source	Destination	Action
192.168.0.100	192.192.10.100	NoPR
DMZ	WAN	NoPR
LAN	10.10.1.1-10.10.1.10	NoPR

表 3.6 Persistent Routing 範例 1 設定內容

範例二 根據 Web 服務簡單設定

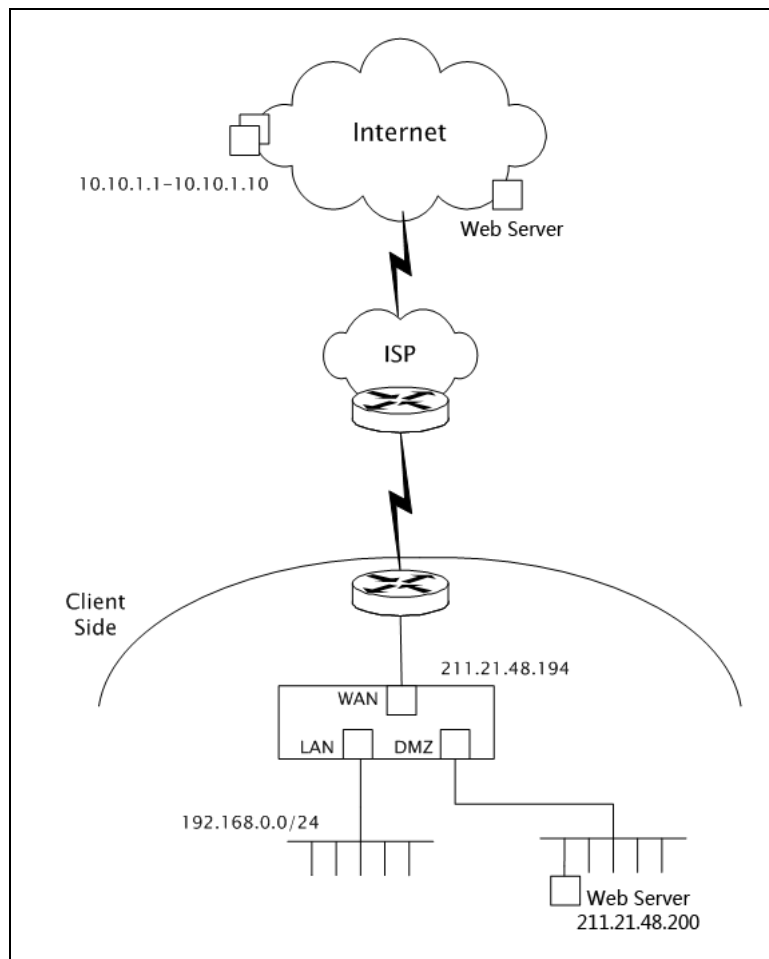


圖 3.11 Persistent Routing 範例 2 架構示意圖

路徑選擇條件：

- LAN 中的子網 192.168.0.0/24 發起的 HTTP 和 HTTPs 連線，均採用 Persistent Routing。
- 由廣域網路發起的 HTTP 和 HTTPs 連線，均採用 Persistent Routing。
- 由於根據 Web 服務無預設值，因此若不設定任何規則，則所有的連接都會根據根據 IP 位址中的設定來決定是否使用 Persistent Routing。

設定內容如下：

Source	Action
192.168.0.0/255.255.255.0	DoPR
WAN	DoPR

表 3.7 Persistent Routing 範例 2 設定內容

範例三 持續路由進階設定

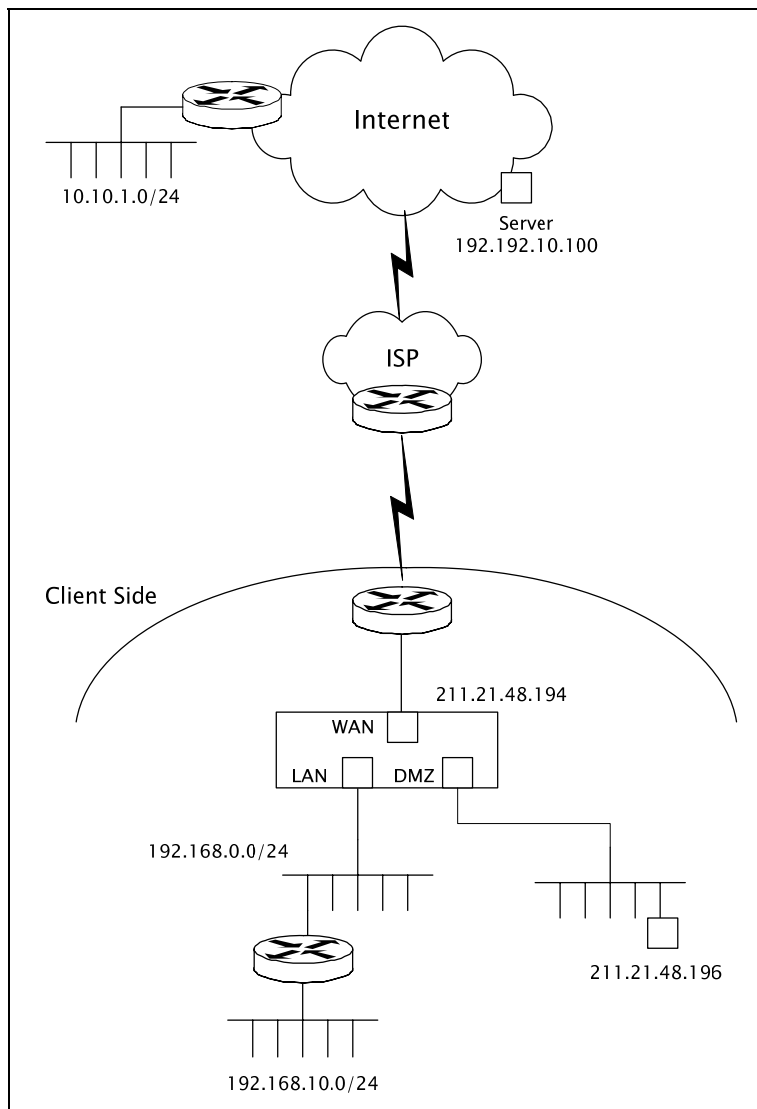


圖 3.12 Persistent Routing 範例 3 架構示意圖

路徑選擇條件：

- LAN IP 區段 192.168.0.10~192.168.0.20 發起的 HTTP 和 HTTPs 連線採用 Persistent Routing；除了 192.168.0.15 外，其他主機皆不要採用 Persistent Routing。
- 192.168.10.0/24 的子網路發起的 HTTP 和 HTTPs 連線採用 Persistent Routing；其他連線不採用 Persistent Routing。
- 由 DMZ 中的 211.21.48.196 到廣域網路上的子網路 10.10.1.0/24 不要採用 Persistent Routing。
- 由於根據 IP 位址的預設值是[DoPR]，因此若不設定任何規則，則所有的連線都會使用 Persistent Routing。

設定內容如下：

Source	Action
192.168.0.10-192.168.0.20	DoPR
192.168.10.0/255.255.255.0	DoPR

表 3.8 Persistent Routing 範例 3 根據 Web 服務設定

Source	Destination	Action
192.168.0.15	WAN	DoPR
192.168.0.10-192.168.0.20	WAN	NoPR
192.168.10.0/255.255.255.0	ANY	NoPR
211.21.48.196	10.10.1.0/255.255.255.0	NoPR

表 3.9 Persistent Routing 範例 3 根據 IP 位址設定內容

註：雖然 192.168.0.15 這個 IP 同時出現在根據 IP 位址設定第一，二條規則中，但由於規則表本身是由上而下比對，所以當比對到第一條時就比對成功而執行第一條的動作并停止比對，因此 192.168.0.15 這個 IP 雖出現在第二條中，卻不會對這個 IP 執行 NoPR 的作業。

根據 Web 服務的優先順序高於根據 IP 位址。雖然 192.168.10.0/255.255.255.0 網段在根據 IP 位址中設定為 NoPR，但由於同時在根據 Web 服務中設定了 DoPR，因此該網段發起的 HTTP 連接仍然採用 Persistent Routing。

3.4 Auto Routing (自動路由)

在這項功能裏，您可以控制封包向外傳送要使用哪一條廣域網路連線。如果廣域網路連線只有一條，這個功能的資料就不需要任何修改，使用預設值即可。

Auto Routing 的主要目的是設定封包的流向，例如通往某些 IP 位址使用某一條廣域網路連線會比較快、內部局域網用戶在存取不同的 ISP(電信或者網通)時，可以使用走不同的 WAN 線路，解決南北互訪速度過慢的問題、內部區域網路某個 IP 位址是重要人物在使用，優先使用較快的廣域網路連線等。可以根據網路環境實際使用情況，來規劃封包的路由。

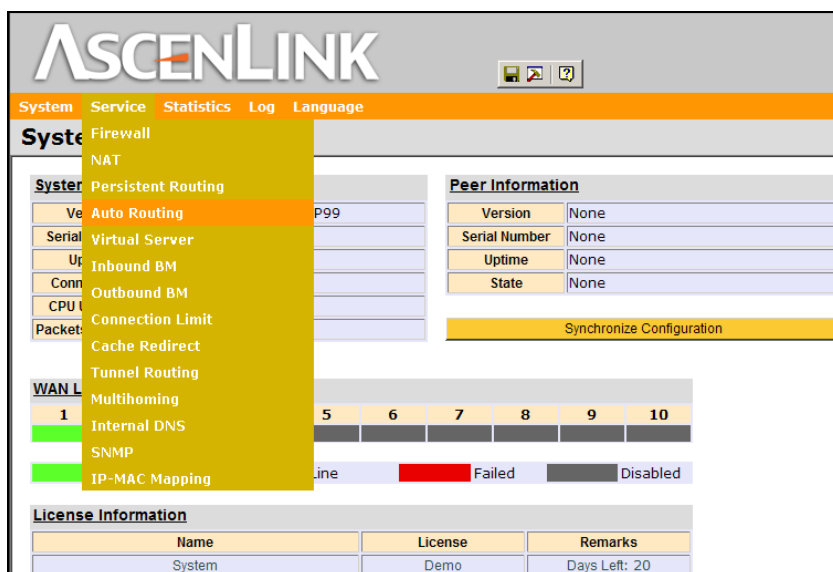


圖 3.13 Service /Auto Routing 功能所處位置

設定自動路由規則可以分為兩部份來看，第一部份是規劃 **Policies** (路由程式)，這裏可以命名程式的名稱，以及設定程式裏要用何種模式的路由演算法，亦即演算法用到的參數。第二部份是 **Filter** (篩選條件)，根據時段、封包來源和目的，使用的服務專案等條件，來決定使用那一個路由程式。

欄位	值	說明																																				
Label (名稱)	<input name>	在這個欄位中填入此條自動路由的名稱，以方便在下方的篩選條件中選擇。																																				
Algorithm (演算法)	Fixed Round-Robin Connection Up stream Traffic Down Stream Traffic By Total Traffic By Optimum Route	<p>有六種的流量控制方式可選擇：</p> <p>Fix (固定指派):表示指定成某單一固定的線路。</p> <p>Round-Robin (輪流指派):表示依照所輸入的流量比例方式在指定的某個廣域網路連線上分配流量。</p> <p>Connection (網路連線):比較各線路之連線數量，讓資料流依照所輸入的連線比例方式在指定的廣域網路連線上分配流量。</p> <p>Up stream Traffic (線路上傳流量):比較加入自動路由的線路之上傳資料使用頻寬，讓資料流使用剩餘頻寬較多的線路。</p> <p>Down Stream Traffic (線路下載流量):比較加入自動路由的線路之下傳資料使用頻寬，讓資料流使用剩餘頻寬較多的線路。</p> <p>By Total Traffic (線路全部使用流量):比較加入自動路由的線路之所有使用頻寬，讓資料流使用剩餘頻寬較多的線路。</p> <p>By Optimum Route(最佳路徑)：表示依據 “Optimum Route Detection” 中的設定來選擇最佳的 WAN 線路。讓資料包透過最佳的 wan 線路存取 internet。</p>																																				
Parameter (參數)	<勾選線路，或輸入每條線路之使用比重>	<p>在這個參數表中，除了可以選擇輪流指派的線路流量分配，還可以輸入比例值，最後只要勾選要加入自動路由管理的線路就可完成設定。</p> <p>參數表的進一步解釋。一般而言如果有四條 WAN 線路，都會先以 Fixed 方式先指派給這四條線路，例如下表：</p> <table border="1"> <thead> <tr> <th>Label</th> <th>Algorithm</th> <th>Parameter</th> </tr> </thead> <tbody> <tr> <td>Hinet 512/512</td> <td>Fixed</td> <td>1 2 3 4 5 6 7 8 9 10</td> </tr> <tr> <td>Giga 1.5M/384</td> <td>Fixed</td> <td>1 2 3 4 5 6 7 8 9 10</td> </tr> <tr> <td>Seednet 512/64</td> <td>Fixed</td> <td>1 2 3 4 5 6 7 8 9 10</td> </tr> <tr> <td>Co-net 3M/512</td> <td>Fixed</td> <td>1 2 3 4 5 6 7 8 9 10</td> </tr> <tr> <td>H+S+G RR</td> <td>Round-Robin</td> <td>1 1 3 0 0 0 0 0 0 0</td> </tr> </tbody> </table> <p>參數表上面的數字表示 WAN 線路代號，表示 WAN 實際線路，例如 第一條線路名稱爲 Hinet 512/512，實際連線到 AscenLink 第一個網路介面(WAN 1)，因此在 Algorithm 欄位中選擇 Fixed，然後在編號爲 “1” 下勾選。其餘三條線路都以相同方式設定。</p> <p>當把每一路對外線路都設定好了之後，可以接著設定 Auto Routing 的程式，例如依據線路流量，設定線路比重。例如</p> <table border="1"> <thead> <tr> <th>Label</th> <th>Algorithm</th> <th>Parameter</th> </tr> </thead> <tbody> <tr> <td>Hinet 512/512</td> <td>Fixed</td> <td>1 2 3 4 5 6 7 8 9 10</td> </tr> <tr> <td>Giga 1.5M/384</td> <td>Fixed</td> <td>1 2 3 4 5 6 7 8 9 10</td> </tr> <tr> <td>Seednet 512/64</td> <td>Fixed</td> <td>1 2 3 4 5 6 7 8 9 10</td> </tr> <tr> <td>Co-net 3M/512</td> <td>Fixed</td> <td>1 2 3 4 5 6 7 8 9 10</td> </tr> <tr> <td>H+S+G RR</td> <td>Round-Robin</td> <td>1 1 3 0 0 0 0 0 0 0</td> </tr> </tbody> </table> <p>表中設定第五個路程式，指定名稱爲 H+S+G RR，勾選三條外線加入 Round Robin 依比重輪流指派的路由方式，比率爲第一條線路爲 1，第二條線路爲 1，第三條線路爲 3，因此當有封包要流向對外線路時就依這個比重使用對外線路。</p>	Label	Algorithm	Parameter	Hinet 512/512	Fixed	1 2 3 4 5 6 7 8 9 10	Giga 1.5M/384	Fixed	1 2 3 4 5 6 7 8 9 10	Seednet 512/64	Fixed	1 2 3 4 5 6 7 8 9 10	Co-net 3M/512	Fixed	1 2 3 4 5 6 7 8 9 10	H+S+G RR	Round-Robin	1 1 3 0 0 0 0 0 0 0	Label	Algorithm	Parameter	Hinet 512/512	Fixed	1 2 3 4 5 6 7 8 9 10	Giga 1.5M/384	Fixed	1 2 3 4 5 6 7 8 9 10	Seednet 512/64	Fixed	1 2 3 4 5 6 7 8 9 10	Co-net 3M/512	Fixed	1 2 3 4 5 6 7 8 9 10	H+S+G RR	Round-Robin	1 1 3 0 0 0 0 0 0 0
Label	Algorithm	Parameter																																				
Hinet 512/512	Fixed	1 2 3 4 5 6 7 8 9 10																																				
Giga 1.5M/384	Fixed	1 2 3 4 5 6 7 8 9 10																																				
Seednet 512/64	Fixed	1 2 3 4 5 6 7 8 9 10																																				
Co-net 3M/512	Fixed	1 2 3 4 5 6 7 8 9 10																																				
H+S+G RR	Round-Robin	1 1 3 0 0 0 0 0 0 0																																				
Label	Algorithm	Parameter																																				
Hinet 512/512	Fixed	1 2 3 4 5 6 7 8 9 10																																				
Giga 1.5M/384	Fixed	1 2 3 4 5 6 7 8 9 10																																				
Seednet 512/64	Fixed	1 2 3 4 5 6 7 8 9 10																																				
Co-net 3M/512	Fixed	1 2 3 4 5 6 7 8 9 10																																				
H+S+G RR	Round-Robin	1 1 3 0 0 0 0 0 0 0																																				

表 3.10 Policies 欄位設定說明表

欄位	值	說明
E (用)	Enable Disable	Enable (打勾)，規則是在可比對的狀態。 Disable (空白)，此規則在不需比對的狀況。
When (時段)	Busy Idle All-Time	有三種選項尖峰時段、離峰時段、所有時間。所有時段為 24 小時都採用此規則，Busy, Idle 時間設定請參照 第二章 [System]→[Virtual Server] 的設定。
Source (來源)	IP Address IP Range Subnet LAN DMZ Localhost Any Address FQDN <IP Grouping Name>	比對封包來源處，基本上有八種的封包來源。 IP Address：來自單一 IP 位址的封包，用在單一主機的 IP 位址，例如 192.168.1.4。 IP Range：來自一段 IP 位址的封包，例如連續 IP 192.168.1.10-192.168.1.20。 Subnet：來自某一個網段的封包，例如：192.168.1.0/255.255.255.0。 LAN：來自 LAN 埠的任何封包。 DMZ：來自 DMZ 埠的任何封包。 Localhost：來自 AscenLink 本身的封包。 Any Address：來自任何位址之封包。 FQDN：來自某一個 FQDN 之封包。 除了基本這幾項比對封包來源的設定外，如果在第二章 [System]→[IP Grouping] 有設定類別，則這些 Group Name 也會出現在選項中，如果加以設定，AscenLink 也會比對來自群組的封包。
Destination (目的地)	IP Address IP Range Subnet WAN FQDN <IP Grouping Name>	比對封包的目的地有五種： IP Address：某一個 IP 位址，例如某一台主機的 IP 位址，211.21.33.88。 IP Range：某一個區段的 IP 位址，例如 211.21.33.88-211.21.33.93。 Subnet：某一個子網路，例如 211.21.33.0/255.255.255.248。 WAN：廣域網路，只要封包流向的目的地在 WAN，都可以設定這個選項。 FQDN：某一個 FQDN。 除了基本這幾項比對封包來源的設定外，如果在第二章 [System]→[IP Grouping] 有設定類別，則這些 Group Name 也會出現在選項之中。
Service (服務)	FTP(21) SSH(22) TELNET(23) SMTP(25) DNS(53) HTTP(80) POP3(110) H323(1720) ICMP TCP@ UDP@ Any.....等	針對某些特定的封包指定路由，這些特定的封包除了內定的幾種服務外，亦可自訂某個 UDP/TCP port 或 port range 如 TCP@123-234，或 ICMP 封包。

Routing Policy (路由程式)	<選擇 Policies 表格 所定義的路由程式>	選定目前規則欲使用的路由方式，Auto Routing 的方式決定 在前一個表格 (Policies) 中定義。
Fail-over Policy (備援程式)	<選擇 Policies 表格 所定義的路由程式>	當 Routing Policy 不可使用時，所要採取的備用路由方式。例 如，固定指派 WAN2，但 WAN2 發生問題時。這些路由程式 在 Policies 表格中已經定義。
L (記錄)	Enable Disable	Enable (打勾)，連線記錄會在 Log 檔案裏。 Disable (空白)，不會產生任何記錄。
Configuration File(組態檔案)		在組態檔案中，您可以導入或導出 Auto-Routing 的設定文件 (csv 檔案格式)。

表 3.11 Auto Routing 各功能選項解釋之參照表

AutoRouting 簡易範例一

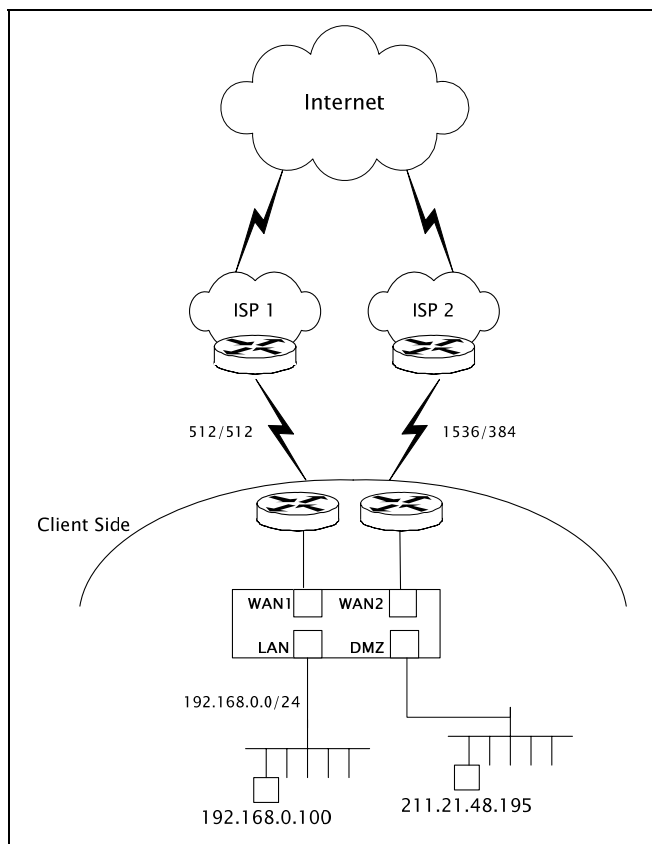


圖 3.14 Auto Routing 範例 1 架構示意圖

在 **Policies (路由程式)** 中定義各種的 **Auto Routing** 方式：

- WAN1 為第一條廣域網路連線，為 512k/512k 對稱的電信 ADSL 線路。
- WAN2 為第二條廣域網路連線，為下載 1.5M 上傳 384k 的不對稱網通 ADSL 線路。
- Optimum Route (最佳路徑)，定義成從現有的兩條線路中選擇最佳路徑。

- (以測量目前線路下載流量方式來定義新的 Auto Routing。
- 以測量目前線路總流量的方式來定義新的 Auto Routing。

設定內容如下：

Label	Algorithm	Parameter
WAN1 (512/512)	Fixed	在 1 的位置打勾
WAN2 (1536/384)	Fixed	在 2 的位置打勾
by Optimum Route	by Optimum Route	在 1 與 2 的位置皆打勾
by Downstream	By Downstream traffic	在 1 與 2 的位置皆打勾
by Total	By Total traffic	在 1 與 2 的位置皆打勾

表 3.12 AutoRouting 範例 1 Policies 設定內容

註：在這邊填入 512/512 只是爲了在 Filters 表格中點選 label 方便，並沒有任何功能，設定線路的頻寬請到 [System]→[Network Setting]頁面設定。

在 **Filters** 中定義各種資料流的 **Auto Routing** 方式：

- 區域網路使用者存取 Internet 的 web 主機時採用 by Optimum Route，將使用者的連線分佈在 WAN1 和 WAN2 中狀況良好的線路上。
- 區域網路使用者存取 Internet 的 ftp 主機時採用永遠使用第一條線的方式 (Fixed)，當第一條線發生錯誤(斷線等等無法傳遞封包的狀況)時，採用 by Optimum Route 方式。

註：當發生錯誤時，由於第一條線路系統判斷已斷，所以不論何種方式皆不會用到第一條線路，在此設定中選擇 by Optimum Route 會變成使用第二條線路。

- 從 DMZ 的主機 211.21.48.195 連到廣域網路的 smtp 主機時會使用第一條線路，若第一條線路發生故障時則變更使用第二條線路。
- 從 DMZ 的主機 211.21.48.195 連到廣域網路的 pop3 主機時會使用第一條線路，若第一條線路發生故障時則不使用任何動作。

註：就是當第一條線路發生故障時，便無法連線到外部的 pop 主機。從 DMZ 到廣域網路的流量以下載流量為依據來分配線路。其他到廣域網路的流量以總流量為依據來分配線路。

Filters 設定內容如下：

Source	Destination	Service	Routing Policy	Fail-Over Policy
LAN	WAN	HTTP(80)	By Optimum Route	No Action
LAN	WAN	FTP(21)	WAN1(512/512)	By Optimum Route
211.21.48.195	WAN	SMTP(25)	WAN1(512/512)	WAN2 (1536/384)
211.21.48.195	WAN	POP3(110)	WAN1(512/512)	No Action

表 3.13 AutoRouting 範例 1Filters 設定內容

Auto Routing 設定範例二

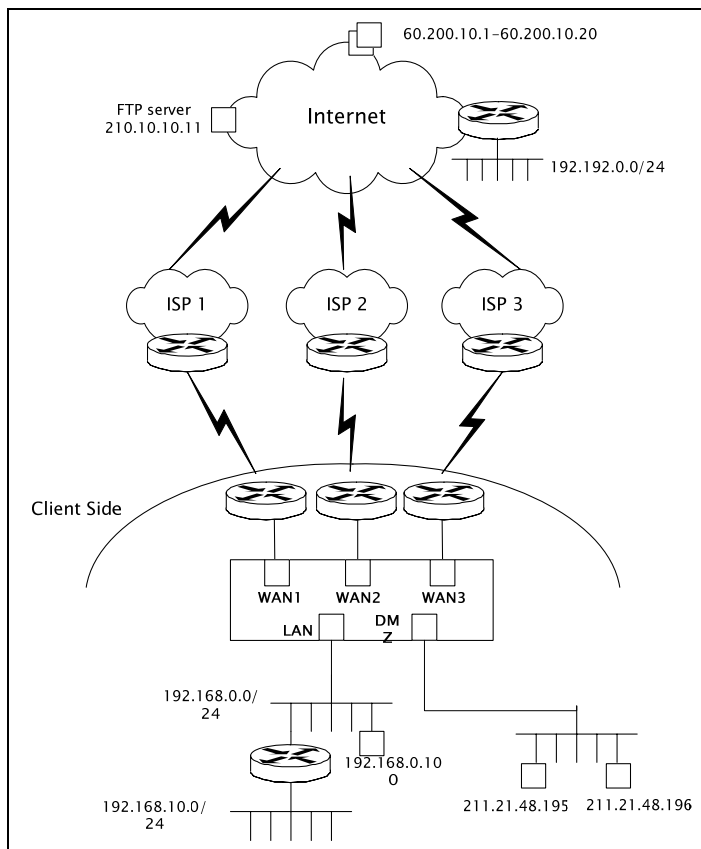


圖 3.15 Auto Routing 範例 2 架構示意圖

在 **Routing Policies** 中定義各種的 **Auto Routing** 方式：

- WAN1 為第一條廣域網路連線，採用 **Fixed** 演算法。
- WAN2 為第二條廣域網路連線，採用 **Fixed** 演算法。
- WAN3 為第三條廣域網路連線。採用 **Fixed** 演算法。

- Round-Robin1:1:1(輪流指派 1:1:1)，定義成將連線以均分方式分配到現有的三條線路上。
- Round-Robin1:2:3(輪流指派 1:2:3)，定義成將連線以 1:2:3 方式分配到現有的三條線路上。

註：假設現在有六個即將建立的對外連線到了 AscenLink 上，AscenLink 將會把第一個連線轉到第一條對外線路上，第 2, 3 個連線轉到第二條對外線路上，最後三個連線轉到第三條對外線路上。

- By Downstream(測量目前線路下載流量)，剩餘可用頻寬的方式來定義新的 Auto Routing，將流量分配到第 1, 2 條線路上。
- By Total Traffic(測量目前線路總流量)，剩餘可用頻寬的方式來定義新的 Auto Routing，將流量分配到第 2, 3 條線路上。

Policies 設定內容如下：

Label	Algorithm	Parameter
WAN1	Fixed	在 1 的位置打勾
WAN2	Fixed	在 2 的位置打勾
WAN3	Fixed	在 3 的位置打勾
Round-Robin1:1:1	Round-Robin	在 1, 2 與 3 的位置填入 1
Round-Robin1:2:3	Round-Robin	在 1 的位置填入 1，在 2 的位置填入 2，在 3 的位置填入 3
by Downstream	By downstream	在 1 與 2 的位置皆打勾
by Total	By Total Traffic	在 2 與 3 的位置皆打勾

表 3.14 AutoRouting 範例 2 Policies 設定內容

Filter 中定義各種資料流的 Auto Routing 方式：

- 從 192.168.0.100 主機的封包到 210.10.10.11 的 ftp Server，採用第三條線路，當線路發生故障時便依照下載流量自動分佈在第 1, 2 條線路上。
- 從子網路 192.168.10.0/24 存取廣域網路 WEB 主機的流量，依流量輪流指派平均分配在三條線上。
- 192.168.0.100-192.168.0.200 這些主機，往 192.192.0.0/24 子網路的 TCP@8000 資料，走第二條線路，當線路發生故障時走第三條線路。
- 從區域網路到 Internet 的所有資料流都依照 WAN1 和 WAN2 下載流量所使用後之剩餘頻寬，分配於這條線路中，當這兩條線路皆故障時便採用第三條線路。
- 從 211.21.48.196 到 210.10.10.11 的 ftp Service 資料流量之路由方式，以輪流指派 1:2:3 分配於三條線路中。
- 從 211.21.48.195 到廣域網路任意主機的 smtp Service 皆用第三條線，當第三條線故障時採用第三條線。

註：這邊的設定便發生了當第三條線路故障時，211.21.48.195 便無法連線任何 smtp Service，無論其他的線路是否正常，請註意您的設定是否合理。這種情況等於 WAN3 故障時，形同 No Action。

- DMZ 到廣域網路的所有應用服務之資料流量，都依照 WAN1 和 WAN2 之下載使用流量後之剩餘頻寬，分佈在這兩條線路上，當這兩條線路皆故障時便依照總線路流量使用後之剩餘頻寬，將資料流量分佈在第 2, 3 條線路。

註：這種狀況會發生如下的反應：唯有第一、二條線路皆發生故障時才會採用另一種備援 Auto Routing 的方式，但由於 1, 2 皆斷，所以只會把全部的流量轉到第三條線路上。

- 任意主機與 60.200.10.1-60.200.10.10 間的主機間之任何資料流，皆用第二條線路，當第二條線路故障時使用第一條線路。

- 任何到廣域網路之資料流，但不屬於以上範圍的，設定其下載流量分佈在第 1, 2 條線路上。

Filters 設定內容如下：

Source	Destination	Service	Routing Policies	Fail-Over Policies
192.168.0.100	210.10.10.11	FTP(21)	WAN3	By Downstream
192.168.10.0/ 255.255.255.0	WAN	HTTP(80)	Round-Robin 1:1:1	No Action
192.168.0.100- 192.168.0.200	192.192.0.0/ 255.255.255.0	TCP@8000	WAN2	WAN3
LAN	WAN	Any	By Downstream	WAN3
211.21.48.196	210.10.10.11	FTP(21)	Round-Robin 1:2:3	No Action
211.21.48.195	WAN	SMTP(25)	WAN3	WAN3
DMZ	WAN	Any	By Downstream	by Total
Any	60.200.10.1- 60.200.10.10	Any	WAN2	WAN1
Any	WAN	Any	By Downstream	No Action

表 3.15 AutoRouting 範例 2 Filters 設定內容

Auto Routing 設定範例三：通道路由作為自動路由的備援

某公司的總部設在北京，在上海設有分公司。該公司有自己的 Intranet，用其進行公司內部資料的傳輸。上海分公司有直接連線到 Internet 的線路，可以直接存取 Internet。但是考慮當這條線路一旦失效、將利用和總部間的 Tunnel 作為備援線路，保證存取 Internet 的不間斷。網路架構如下：

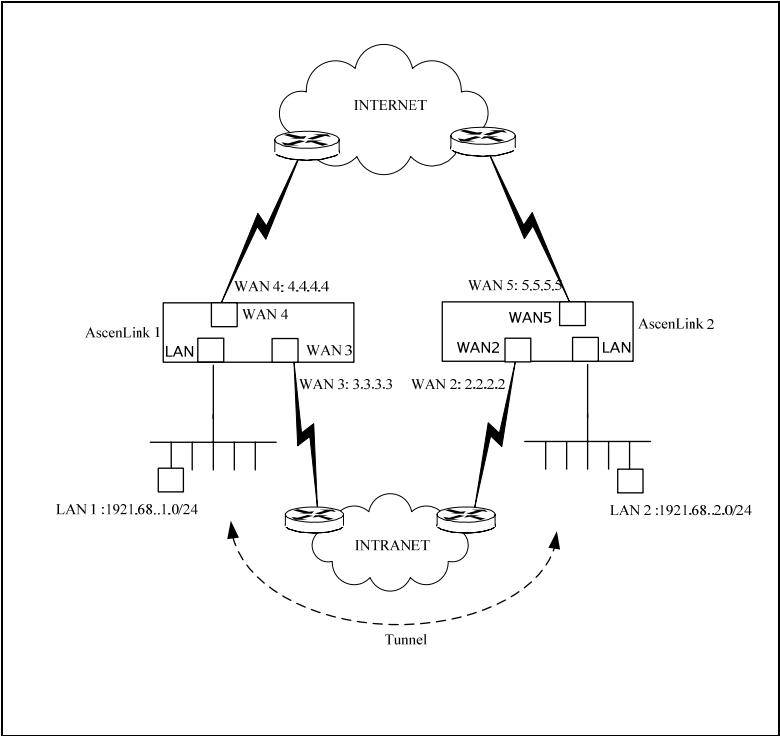


圖 3.16 Auto Routing 範例 3 架構示意圖

相關資訊如下：

	Beijing (北京)	Shanghai (上海)
WAN 2		2.2.2.2
WAN 3	3.3.3.3	
WAN 4	4.4.4.4	
WAN 5		5.5.5.5
LAN	192.168.1.0/24	192.168.2.0/24

表 3.16 Auto Routing 範例 3 相關資訊

北京（Beijing）總公司的設定如下：

Tunnel Routing 部分

- 記錄及本機 ID 設定內容

通道路由記錄	啟用
本機 ID	Beijing

表 3.17 Auto Routing 範例 3:記錄及本機 ID 設定(Beijing 總公司)

- Tunnel Group 設定內容

+	Group Name	Remote Host ID	Tunnels			
+ - ↑ ↓	Beijing to Shanghai	Shangha i	+	Local IP	Remote IP	Weigh t
			+ - ↑ ↓	3.3.3.3	2.2.2.2	1

表 3.18 Auto Routing 範例 3:Tunnel Group 設定(Beijing 總公司)

Routing Rules 設定內容

+	Source	Destination	Use Group	Fail-Over
+ - ↑ ↓	Any Address	192.168.2.0/255.255.255.0	Beijing to Shanghai	No-ACTION

表 3.19 Auto Routing 範例 3:Routing Rules 設定(Beijing 總公司)

Auto Routing 部分

Policies 設定內容

Label	Algorithm	Parameter
WAN4	Fixed	在 4 的位置打勾
Default Policy	By Downstream Traffic	在 1、2、3、4……的位置打勾

表 3.20 Auto Routing 範例 3:Auto Routing Policies 設定(Beijing 總公司)

Filters 設定內容

Source	Destination	Service	Routing Policy	Fail-Over Policy
Tunnel	WAN	ANY	WAN4	Default Policy
Any Address	WAN	ANY	Default Policy	No-ACTION

表 3.21 Auto Routing 範例 3:Auto Routing Filters 設定(Beijing 總公司)

上海（Shanghai）分公司的設定如下：

Tunnel Routing 部分

- 記錄及本機 ID 設定內容

通道路由記錄	啓用
本機 ID	Shanghai

表 3.22 Auto Routing 範例 3:記錄及本機 ID 設定(Shanghai 分公司)

- Tunnel Group 設定內容

+	Group Name	Remote Host ID	Tunnels				
+ - ↑ ↓	Shanghai to Beijing	Beijing					
			+	Local IP	Remote IP	Weight	
			+ - ↑ ↓	2.2.2.2	3.3.3.3	1	

表 3.23 Auto Routing 範例 3:Tunnel Group 設定(Shanghai 分公司)

- Routing Rules 設定內容

+	Source	Destination	Use Group	Fail-Over
+ - ↑ ↓	Any Address	192.168.1.0/ 255.255.255.0	Shanghai to Beijing	No-ACTION

表 3.24 Auto Routing 範例 3:Routing Rules 設定(Shanghai 分公司)

Auto Routing 部分

▫ Policies 設定內容

Label	Algorithm	Parameter
WAN5	Fixed	在 5 的位置打勾
Default Policy	By Downstream Traffic	在 1、2、3、4……的位置打勾

表 3.25 Auto Routing 範例 3:Auto Routing Policies 設定(Shanghai 分公司)

▫ Filters 設定內容

Source	Destination	Service	Routing Policy	Fail-Over Policy
Any Address	WAN	Any	WAN5	Tunnel:Shanghai to Beijing
Any Address	WAN	Any	Default Policy	No-ACTION

表 3.26 Auto Routing 範例 3:Auto Routing Filters 設定(Shanghai 分公司)

3.5 Virtual Server (虛擬主機)

這一節中介紹 Virtual Server 的設定使用，所謂 Virtual Server 是指在內部網路設定一台網路主機，對外界提供服務，由於這台主機並沒有設定公開的合法 IP，而是設定內部的私有 IP，對廣域網路的使用者而言，是看不到這台主機的，僅看到 AscenLink 設定在 WAN Port 上的公開合法 IP 位址，因此將外界的服務請求，轉譯成內部位址，傳給這一台提供服務的主機，以呼應外界的服務請求。當不想使用公開位址但仍想讓內部或 DMZ 的主機提供對外服務時，就可以使用 Virtual Server 這項功能。

Virtual Server 支援對多台伺服器負載平衡，由它進入內部網路的存取在多台內部伺服器之間進行分配，以實現伺服器的負載平衡。當外部用戶存取內部伺服器的時候，根據各個內部伺服器設定的權重的不同，將外界請求分發到伺服器組裏的伺服器中。同時，Virtual Server 還不斷監控伺服器的運行狀態，保證網路存取只會被導向到能正常工作的伺服器上。

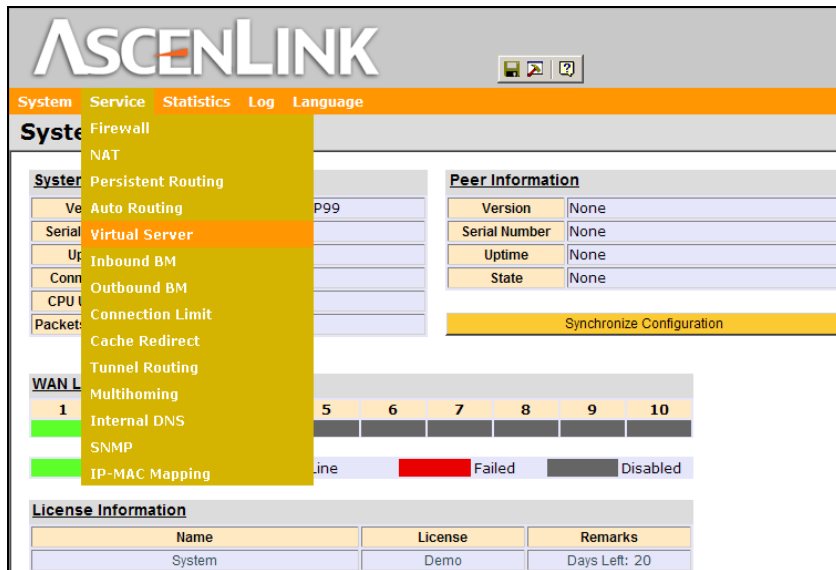


圖 3.17 Service/Virtual Server 功能所處位置

欄位	值	說明
E (用)	Enable Disable	Enable (打勾)，規則是在可比對的狀態。 Disable (空白)，此規則在不需比對的狀況。
When (時段)	Busy Idle All-Time	有三種選項尖峰時段、離峰時段、所有時間。所有時段為 24 小時都採用此規則，Busy, Idle 時間設定請參照 第二章 [系統]/ [尖峰時段] 的設定。
WAN IP (廣域網路)	<WAN IP>	WAN IP 位址外部用戶存取服務時所見到的位址（公開位址），若在路由模式(Routing Mode)，可選擇 AscenLink 在相應 WAN 線路所獲得的 IP 位址，也可手動輸入 IP 位址，若在單一固定 IP 模式(Bridge Mode : One Static IP)下，WAN IP 即為 ISP 所給予的公開位址。
Service (服務)	FTP(21) SSH(22) TELNET(23)) SMTP(25) DNS(53) HTTP(80) POP3(110) H323(1720) ICMP TCP@ UDP@ Any.....等	提供幾種特定的服務以外，亦可自訂某個 UDP/TCP port 或 port range 如 TCP@123-234，或 ICMP 封包。
Keep Session (保持連線時間)	<秒>	設定當來自 WAN 得用戶端與伺服器組中的一台伺服器建立連線後是否對連線進行保持，且保持的時間。默認為 30s
伺服器 IP 位址	IP Address	伺服器真實的位址，可能是在 LAN 或 DMZ 的主機
偵測方式	<icmp> <tcp>	可選擇對伺服器群組的伺服器狀態進行偵測的方式，分成 icmp 和 tcp 兩種。選擇 tcp 進行偵測時，需輸入偵測的 tcp 埠號
服務	FTP(21) SSH(22) TELNET(23)) SMTP(25) DNS(53) HTTP(80) POP3(110) H323(1720) ICMP TCP@ UDP@ Any.....等	提供伺服器組中的伺服器對外提供服務的種類,除了現有的服務外,也可自定義某個 UDP/TCP port 或 port range 如 TCP@123-234,或過濾 ICMP 封包
權重	1,2,3....	在此輸入此通道的使用權值，權值越高會被使用到的機率越高。
L (記錄)	Enable Disable	Enable (打勾)，連線記錄會在 Log 檔案裏。 Disable (空白)，不會產生任何記錄。

表 3.27 Virtual Server 各功能選項解釋之參照表

Virtual Server 簡易範例一

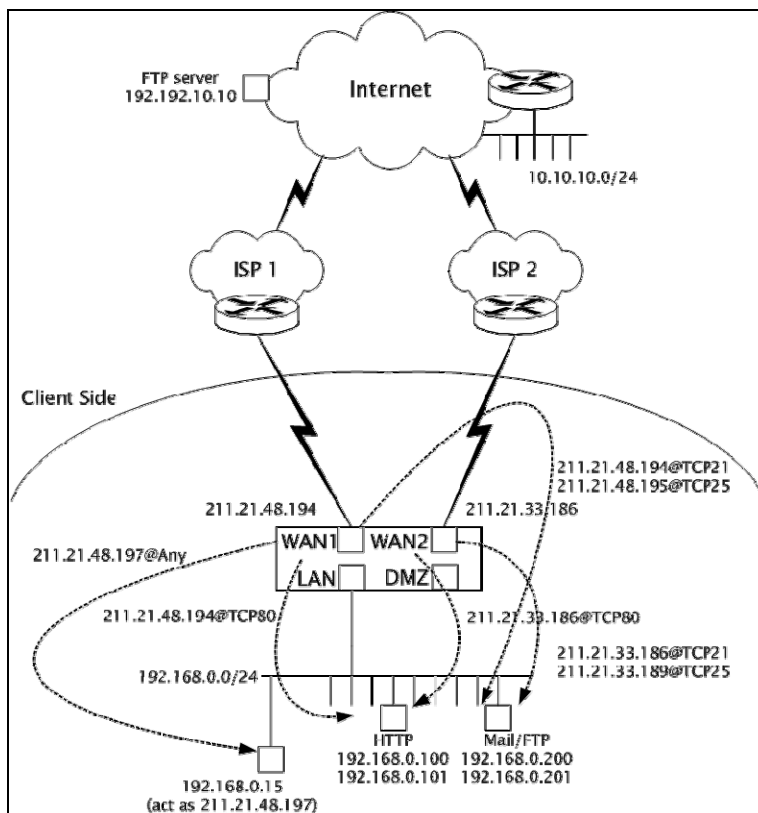


圖 3.18 Virtual Server 範例 1 架構示意圖

虛擬主機設定需求條件如下：

- WAN1 所使用的 IP 為 211.21.48.194 (WAN IP 的設定請至[System] → [Network Settings] → [WAN Setting] 畫面，以下同。)
- WAN2 所使用的 IP 為 211.21.33.186。
- 將外界要求 WAN1 與 WAN2 提供 Http (80)的服務請求，轉到區域網路上的兩台 http server (192.168.0.100，192.168.0.101)。
- 將外界要求 WAN1 與 WAN2 提供 FTP(21)的服務請求，轉到區域網路上的兩台 ftp server (192.168.0.200，192.168.0.201)。
- 將另一組的公開 IP 211.21.48.195 和 211.21.48.189 設定給 AscenLink 的 WAN Port 1，並將外界的服務請求，轉到區域網路上兩台的 smtp server (192.168.0.200，192.168.0.201)。
- 將送往 211.21.48.197 的任何封包全部轉往 192.168.0.15。

註：AscenLink 支援 Active 與 passive mode 的 ftp server，不需設定，為自動偵測。

這些外部 IP 要設定在 AscenLink 的通訊介面 WAN Port 1，請到 [System] → [Network Settings] → [WAN Setting] → [WAN Link 1] 下之 Basic Subnet 表格裏，[IP(s) on Localhost] 這項欄位中設定這些 IP。

因為並未存在 211.21.48.197 這台主機，所以必須將此 IP 設定在 WAN 端的介面上。

設定內容如下：

廣域網路 IP 位址	服務	伺服器 IP 位址	偵測方式	服務	權重
211.21.48.194	HTTP (80)	192.168.0.100	Tcp (80)	HTTP(80)	1
		192.168.0.101	Icmp	HTTP(80)	1
211.21.33.186	HTTP (80)	192.168.0.100	Icmp	HTTP(80)	1
		192.168.0.101	TCP (80)	HTTP(80)	2
211.21.48.194	FTP (21)	192.168.0.200	Icmp	FTP(21)	1
		192.168.0.201	TCP (21)	FTP(21)	1
211.21.48.186	FTP (21)	192.168.0.200	Icmp	FTP(21)	1
		192.168.0.201	TCP (21)	FTP(21)	1
211.21.48.195	SMTP (25)	192.168.0.200	Icmp	SMTP(25)	1
		192.168.0.201	TCP (25)	SMTP(25)	1
211.21.48.189	SMTP (25)	192.168.0.200	Icmp	SMTP(25)	1
		192.168.0.201	TCP (25)	SMTP(25)	1
211.21.48.197	any	192.168.0.15	icmp	Any	1

表 3.28 Virtual Server 範例 1 設定內容

Virtual Server 範例二

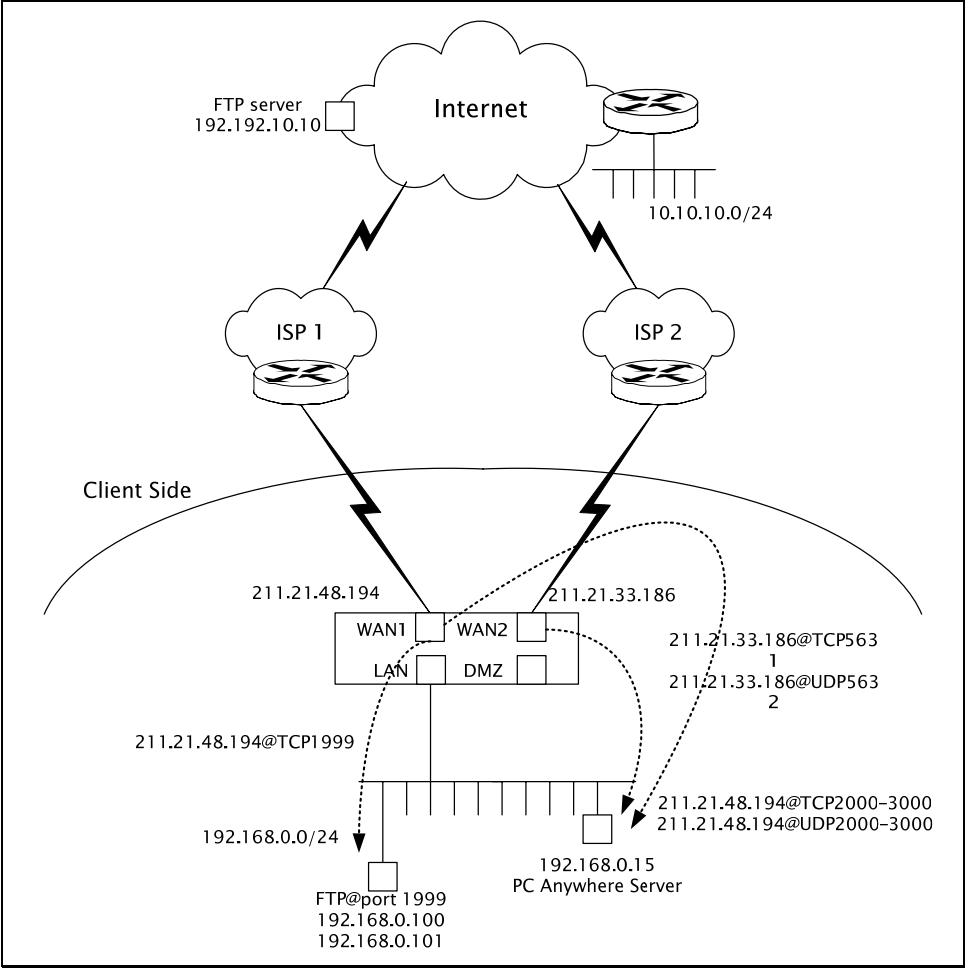


圖 3.19 Vitrual Server 範例 2 架構示意圖

虛擬主機設置條件如下：

- 在區域網路上架設 ftp server，將外界與公開 IP 位址 211.21.48.194 所建立之 TCP port 1999 之服務請求，導向到 192.168.0.100 的 ftp server@TCP port 1999。

註：在 port style ftp-data connection 由於 ftp protocol 的特性，當把 ftp-control 使用在 port 1999 時，port 1998 會被 ftp-data 所佔用。

- 讓外部的使用者能連上 WAN IP 211.21.33.186 位址，並使用 PcAnywhere 連線到位於區域網路的電腦。

註：請參考 PcAnywhere 軟體的使用說明以得知此軟體所使用的 port 有兩個 port，分別是 TCP@5631 和 UDP@5632。

- 外界用戶連線上 WAN IP 位址 211.21.48.194，將 port range 2000~3000 的 TCP/UDP 封包送往 192.168.0.15 主機。

註：AscenLink 亦支持 port range 的 redirection (重導)。

設定內容如下：

廣域網路 IP 位址	服務	伺服器 IP 位址	偵測方式	服務	權重
211.21.48.194	TCP@1999	192.168.0.100	icmp	TCP@1999	1
		192.168.0.101	Tcp(1999)	TCP@1999	1
211.21.33.186	TCP@5631	192.168.0.15	icmp	TCP@5631	1
211.21.33.186	UDP@5632	192.168.0.15	Tcp(5632)	UDP@5632	1
211.21.48.194	TCP@2000-3000	192.168.0.15	icmp	TCP@2000-3000	1
211.21.48.194	UDP@2000-3000	192.168.0.15	icmp	UDP@2000-3000	1

表 3.29 Virtual Server 範例 2 設定內容

3.6 Inbound BM (對內頻寬管理)

在資料的流向定義上，以 AscenLink 為中心點，當資料由外界流進來時，稱之為 Inbound；反之稱之為 Outbound，所以 Inbound 泛指所有廣域網路來的封包，不限定伺服器的位址。不論資料的流向如何，都會佔用到對外的連線頻寬。因此這一節主要是討論如何管理經由外線流進 AscenLink 的資料，依據時段、應用服務、資料來源和目的等屬性，設定使用頻寬的優先順序或是提供保證頻寬等服務。

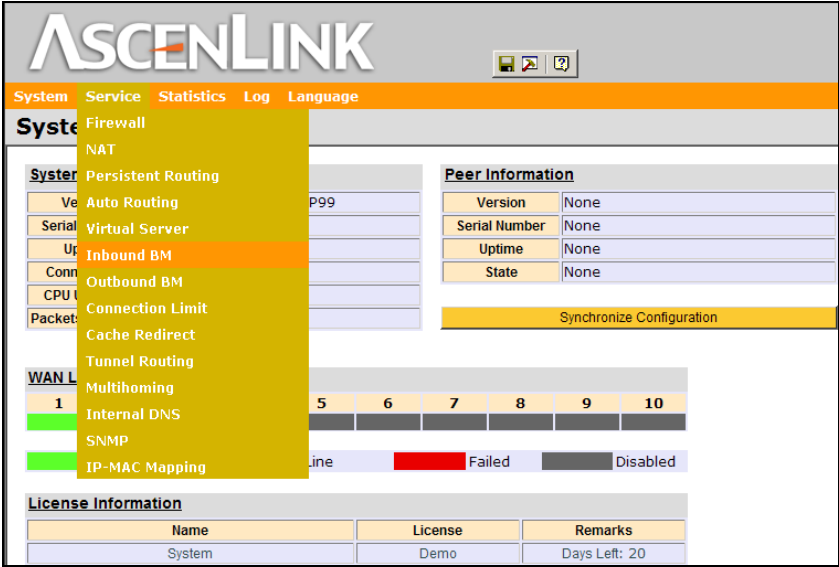


圖 3.20 Service/Inbound BM 功能所處位置

Inbound BM 的設定表格，分作兩大部份：Classes 和 Filter。

Classes 設定表格

Classes		Expand All			Collapse All			
<div><div></div><div></div><div></div><div></div><div></div></div>	Name	Link	Busy Hour Settings			Idle Hour Settings		
			Guaranteed Kbps	Max Kbps	Priority	Guaranteed Kbps	Max Kbps	Priority
1-20		Collapse Link Settings						
		WAN 1	0	512	Normal	0	512	Normal
		WAN 2	0	512	Normal	0	512	Normal
		WAN 3	0	1536	Normal	0	1536	Normal
		WAN 4			Normal			Normal
		WAN 5			Normal			Normal
		WAN 6			Normal			Normal
		WAN 7			Normal			Normal
		WAN 8			Normal			Normal
		WAN 9			Normal			Normal
		WAN 10			Normal			Normal

圖 3.21 Inbound BM Classes 設定表格

其中 Collapse Link Setting 和 Expand Link Setting 可以縮合和打開，以對每條外線的 Inbound 資料進行頻寬管理。

欄位	說明	
Enable BM (啓用頻寬管理)		點選以打勾啓用對內頻寬管理和對外頻寬功能。若不需要使用頻寬管理請關閉此功能，可提升系統運作效能。
Name (名稱)	<input name>	爲此定義的資訊類型給定名稱，用於下方篩選條件表格時選定的資訊類型。 名稱主要是用於識別，例如想用於管理 HTTP 之資料流量，就命名爲 HTTP。後續的設定就可以選用這個名稱。
Link (連線)	-	指當此資料流經由所定義之廣域連線時用到的流量設定，可針對不同的廣域網路連線給定不同的流量定義。
Busy Hour Settings (尖峰時段設定) 註：Busy Hour 在 [System]→[Date Time]下設定	Guaranteed Kbps	保證最小 Kbps： 保證此資料流在傳輸時保證會擁有的最少頻寬，通常用在 VoIP 等應用，需要穩定的頻寬，確保好的影像聲音品質的資料流上。
	Max Kbps	定義使此資料流使用時最大不超過所定義的頻寬，通常用在可能會同時產生大量資料傳輸，導致影響其他服務或對頻寬不敏感的服務，如 WWW, SMTP 等。
	Priority	優先順序： AscenLink 的優先順序分成三個等級，同樣等級的資訊類型彼此按照設定分配流量，較高優先權的資訊類型分配完頻寬後，剩下的給較低優先權的。
Idle Hour Settings (離峰時段設定)	Guaranteed Kbps	保證最小 Kbps： 保證此資料流在傳輸時最少一定會擁有的頻寬，通常用在 VoIP 等需要穩定的頻寬以有好的影像聲音品質的資料流上。

註：Idle Hour 在 [System]→[Date Time]下設定	Max Kbps	最大 Kbps： 定義使此資料流使用時最大不超過所定義的頻寬，通常用在可能會同時產生大量資料傳輸，導致影響其他服務或對頻寬不敏感的服務，如 WWW, SMTP 等。
	Priority	優先順序： AscenLink 的優先順序分成三個等級，同樣等級的資訊類型彼此按照設定分配流量，較高優先權的資訊類型分配完頻寬後，剩下的給較低優先權的。

表 3.30 Inbound BM Classes 欄位說明表

根據此表格定義的篩選方式找出特定的資料流，規劃頻寬的使用方式。

欄位	值	說明
E (用)	Enable Disable	Enable (打勾)，規則是在可比對的狀態。 Disable (空白)，此規則在不需比對的狀況。
Source (來源)	IP Address IP Range Subnet WAN FQDN <IP Grouping Name>	封包來源比對：可比對五種來源的封包。 IP Address: 某一個 IP 位址，例如某一台主機的 IP 位址，211.21.33.88。 IP Range: 某一個 IP 區段的 IP，如 211.21.33.88-211.21.33.93。 Subnet: 某一個子網路 例如 211.21.33.0/255.255.255.248 WAN: 廣域網路，來自 WAN 的封包。 FQDN: 來自某一個 FQDN 之封包。
Destination (目的地)	IP Address IP Range Subnet WAN LAN DMZ Localhost Any address FQDN <IP Grouping Name>	比對封包的目的地，比對方式同上。 同樣的除了這九種目的地之外，如果設定有 IP Grouping 的群組，這些名稱也會出現在選項中，AscenLink 也會比對來自群組的封包。
Service (服務)	FTP(21) SSH (22) SMTP(25) DNS(53) HTTP(80) POP3(110) H323 (1720) ICMP TCP@ UDP@ Any.....等	比對服務專案，例如對 FTP 的封包進行頻寬管理。針對 TCP 或 UDP 可以自訂某個 port 或 port range 如 TCP@123-234，表示 Port 123 ~ 234 的封包被監聽比對。
Service At	WAN	此欄位有兩種選擇：非廣域網路或廣域網路。

(服務所在地)	Non WAN	Non WAN 非廣域網路，指伺服器所在的位置為 LAN (虛擬主機) 或 DMZ (公開位址主機)，WAN 指伺服器所在的位置在廣域網路。
Classes (資訊類型)	<Name>	依照上方 Classes 表格的 Name 欄位所定義的資料類型選擇頻寬使用方式。
L (記錄)	Enable Disable	Enable (打勾)，該項規則使用時，產生 Log 檔案。 Disable (空白)，不產生 Log 檔案。

表 3.31 Inbount BM 各功能選項解釋之參照表

Inbound BM 範例一

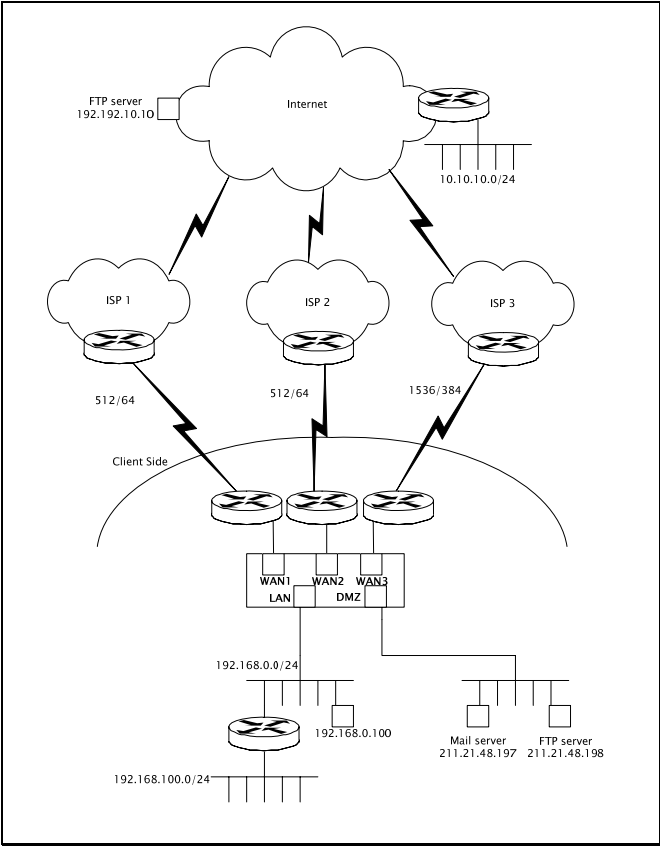


圖 3.22 Inbound BM 範例 1 架構示意圖

Inbound 資料流量管理條件需求：

- 設定 mail server 211.21.48.197 下載 mail 的流量，在尖峰時刻和離峰時刻，依據不同外線的頻寬，WAN1 最大只能使用 128K 頻寬，WAN 2 使用 64K，WAN3 使用 128K。
- 設定區域網路主機抓取外部 web server 的流量，在尖峰時刻和離峰時刻，依據不同外線的頻寬，WAN1 最大只能使用 128K 頻寬，WAN 2 使用 64K，WAN3 使用 64K。
- 設定單一區域網路主機 192.168.0.100 對廣域網路的 ftp server 的存取流量。在忙時和離峰時刻，WAN 1 最少可以有 20Kbps 的頻寬，最多 50Kbps，同時優先權調至最高。其餘的 WAN 連線頻寬使用請參考下表。
- 設定隔離區 ftp server 211.21.48.198 的下載資料的流量。

Classes 設定內容如下：

Name	Link	Busy Hour Settings			Idle Hour Settings		
		Guaranteed Kbps	Max bps	Priority	Guaranteed Kbps	Max Kbps	Priority
Mail Server	WAN1	0	128	Normal	0	128	Normal
	WAN2	0	64	Normal	0	64	Normal
	WAN3	0	128	Normal	0	128	Normal
to LAN zone	WAN1	0	128	Normal	0	128	Normal
	WAN2	0	64	Normal	0	64	Normal
	WAN3	0	64	Normal	0	64	Normal
for 192.168.0.100	WAN1	20	50	High	20	50	High
	WAN2	0	30	High	100	200	High
	WAN3	0	30	High	100	200	High
for DMZ zone	WAN1	200	500	Low	200	500	Low
	WAN2	0	512	Low	200	300	Low
	WAN3	0	256	Low	200	300	Low

表 3.32 Inbound BM 範例 1 Class 設定內容

Filters 設定內容如下：

Source	Destination	Service	Service At	Classes
WAN	211.21.48.197	SMTP(25)	Non WAN	Mail Server
WAN	LAN	HTTP(80)	WAN	to LAN zone
WAN	192.168.0.100	FTP(21)	WAN	for 192.168.0.100
WAN	211.21.48.198	FTP(21)	Non WAN	for DMZ zone

表 3.33 Inbount BM 範例 1 Filters 設定內容

下載頻寬資料流可以分兩種，以 **ftp** 為例，當 **server** 在廣域網路時使用者在非廣域網路下載資料或 **server** 在非廣域網路外部使用者上傳資料皆為下載頻寬資料流，此時的規則皆要列在下載頻寬管理的頁面。

Inbound BM 範例二

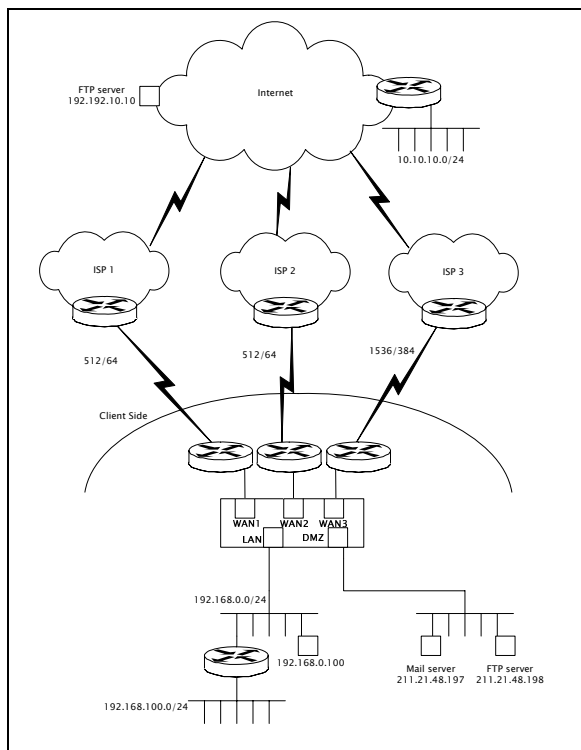


圖 3.23 Inbound BM 範例 2 架構示意圖

Inbound 資料流量管理條件需求：

- 設定區域網路使用者從 192.192.10.10 抓取 ftp 資料的流量。
- 設定部份區域網路主機(192.168.0.10-192.168.0.50)從廣域網路 web 伺服器抓取資料的流量。
- 設定子網路 (192.168.100.0/24) 到廣域網路 ftp server 存取資料的流量。
- 設定廣域網路使用者上傳資料到 211.21.48.198 FTP server 的流量。

Classes 設定內容如下：

Names	Link	Busy Hour Settings			Idle Hour Settings		
		Guaranteed Kbps	Max Kbps	Priority	Guaranteed Kbps	Max Kbps	Priority
For LAN user	WAN1	0	128	Normal	0	512	Normal
	WAN2	0	128	Normal	0	512	Normal
	WAN3	0	64	Normal	0	512	Normal
for 192.168.0.10-192.168.0.50	WAN1	0	128	Normal	0	128	Normal
	WAN2	128	256	Low	0	512	Low
	WAN3	64	256	Low	0	512	Low
for 192.168.100.0 FTP	WAN1	20	50	High	20	50	High
	WAN2	0	64	High	32	128	High
	WAN3	0	64	High	32	128	High
for WAN user upload	WAN1	200	500	Low	200	500	Low
	WAN2	0	512	Low	0	512	Low
	WAN3	128	256	Low	256	512	Low

表 3.34 Inbount BM 範例 2 Class 設定內容

Filters 設定內容如下：

Source	Destination	Service	Service At	Classes
192.192.10.10	LAN	FTP(21)	WAN	For LAN user
WAN	192.168.0.10-192.168.0.50	HTTP(80)	WAN	for 192.168.0.10-192.168.0.50
WAN	192.168.100.0/255.255.255.0	FTP(21)	WAN	for 192.168.100.0 FTP
WAN	211.21.48.198	FTP(21)	Non WAN	for WAN user upload

表 3.35 Inbount BM 範例 2 Filters 設定內容

註：HTTP 資料流有兩個方向，Client 對 Server 的 Request 以及 Server 對 Client 的 Response，其中 Response 的部分對於頻寬影響較大（內有圖檔以及其他多媒體檔案），Request 部分通常只有 Header 而已，通常要頻寬管理的是 Response 部份。

3.7 Outbound BM (對外頻寬管理)

相對於 Inbound BM，在資料的流向定義上，以 AscenLink 為中心點，當資料由內部流到外界時，稱之為 **Outbound**。此項功能用來設定對外流量的控制，對外流量泛指所有外送的封包，不限定伺服器的位址，以及各自獨立的廣域網路連線，每一個廣域網路連線又可依照保證頻寬，最大頻寬用量和各個的優先順序來定義各資料流的頻寬分配，再利用下方的篩選方式找出對應的資料流。這一節主要是討論如何管理經 AscenLink 流出的資料，依據時段，應用服務，資料來源和目的等屬性，設定使用頻寬的優先順序或是提供保證頻寬等服務。

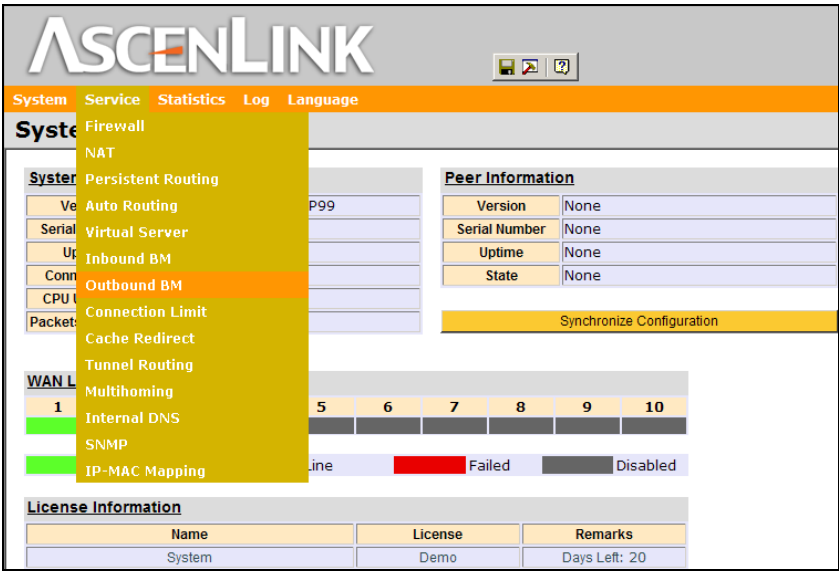


圖 3.24 Service /Outbound BM 功能所處位置

請參照以下 Classes 欄位說明表

欄位	說明	
Enable BM (啓用頻寬管理)	點選以打勾啓用對內頻寬管理和對外頻寬功能。若不需要使用頻寬管理請關閉此功能，可提升系統運作效能。	
Name (名稱)	爲定義的資訊類型給定名稱，該名稱顯示于下方篩選條件之表格。名稱主要是用於識別，例如想用於管理 HTTP 之資料流量，就命名爲 HTTP。後續的設定就可以選用這個名稱。	
Link (連線)	指當此資料流經由所定義之廣域連線時用到的流量設定，可針對不同的廣域網路連線給定不同的流量定義。	
Busy Hour Settings (尖峰時段設定) 註：Busy Hour 在 System/Date Time 下設定。	Guaranteed Kbps	保證最小 Kbps： 保證此資料流在傳輸時保證會擁有的最少頻寬，通常用在 VoIP 等應用，需要穩定的頻寬，確保好的影像聲音品質的資料流上。
	Max Kbps	最大 Kbps： 定義使此資料流使用時最大不超過所定義的頻寬，通常用在可能會同時產生大量資料傳輸，導致影響其他服務或對頻寬不敏感的服務，如 WWW, SMTP 等。
	Priority	優先順序： AscenLink 的優先順序分成三個等級，同樣等級的資訊類型彼此按照設定分配流量，較高優先權的資訊類型分配完頻寬後，剩下的給較低優先權的。
Idle Hour Settings (離峰時段設定) 註：Idle Hour 在 System/Date Time 下設定。	Guaranteed Kbps	保證最小 Kbps： 保證此資料流在傳輸時最少一定會擁有的頻寬，通常用在 VoIP 等需要穩定的頻寬以有好的影像聲音品質的資料流上。
	Max Kbps	最大 Kbps： 定義使此資料流使用時最大不超過所定義的頻寬，通常用在可能會同時產生大量資料傳輸，導致影響其他服務或對頻寬不敏感的服務，如 WWW, SMTP 等。
	Priority	優先順序： AscenLink 的優先順序分成三個等級，同樣等級的資訊類型彼此按照設定分配流量，較高優先權的資訊類型分配完頻寬後，剩下的給較低優先權的。

表 3.36 Outbound BM Class 欄位說明表

以下是 **Filters** 欄位說明表，根據此表格定義的篩選方式找出特定的資料流，規劃頻寬的使用方式。

欄位	值	描述
E (用)	Enable Disable	Enable (打勾)，規則是在可比對的狀態。 Disable (空白)，此規則在不需比對的狀況。
Source (來源)	IP Address IP Range Subnet LAN DMZ Localhost Any FQDN <IP Grouping Name>	封包來源比對，有八種的比對方式： IP Address IP 位址：單一 IP，用在單一主機格式為 192.168.1.4。 IP Range IP 位址區段：比對一段 IP 位址，用在某幾台主機，格式為連續 IP 192.168.1.10-192.168.1.20。 Subnet 子網路：比對某一個網段，例如： 192.168.1.0/255.255.255.0。 LAN 區域網路：比對來自 LAN 埠的任何封包。 DMZ 隔離區：比對來自 DMZ 埠的任何封包。 Localhost 本機位址：比對來自這台 AscenLink 本身的封包。 Any 任何位址：比對任何封包。 FQDN: 來自某一個 FQDN 之封包。 如果在 IP Grouping 中設有 Grouping Name 也會出現在選項之中。
Destination (目的地)	IP Address IP Range Subnet WAN FQDN <IP Grouping Name>	比對封包的目的地，比對方式同上。 如果設定有 IP Grouping 的群組，這些名稱也會出現在選項中，AscenLink 也會比對來自群組的封包。
Service (服務)	FTP (21) SSH (22) SMTP(25) DNS(53) HTTP (80) POP3(110) H323 (1720) ICMP TCP@ UDP@ Any...等	比對需要過濾的服務專案，例如對 FTP 的封包進行頻寬管理。針對 TCP 或 UDP 可以自訂某個 port 或 port range 如 TCP@123-234，表示 Port 123 ~ 234 的封包被監聽比對。
Service At (服務所在地)	WAN Non WAN	此欄位有兩種選擇：非廣域網路或廣域網路。 Non WAN 非廣域網路，指伺服器所在的位置為 LAN (虛擬主機) 或 DMZ (公開位址主機)。 WAN 指伺服器所在的位置在廣域網路。
Classes (資訊類型)	<Name>	依照上方 Classes 表格的 Name 欄位所定義的資料類型選擇頻寬使用方式。
L (記錄)	Enable Disable	Enable (打勾)，該項規則使用時，產生 Log 檔案。 Disable (空白)，不產生 Log 檔案。

表 3.37 Outbound BM Filters 欄位說明表

Outbound BM 範例一

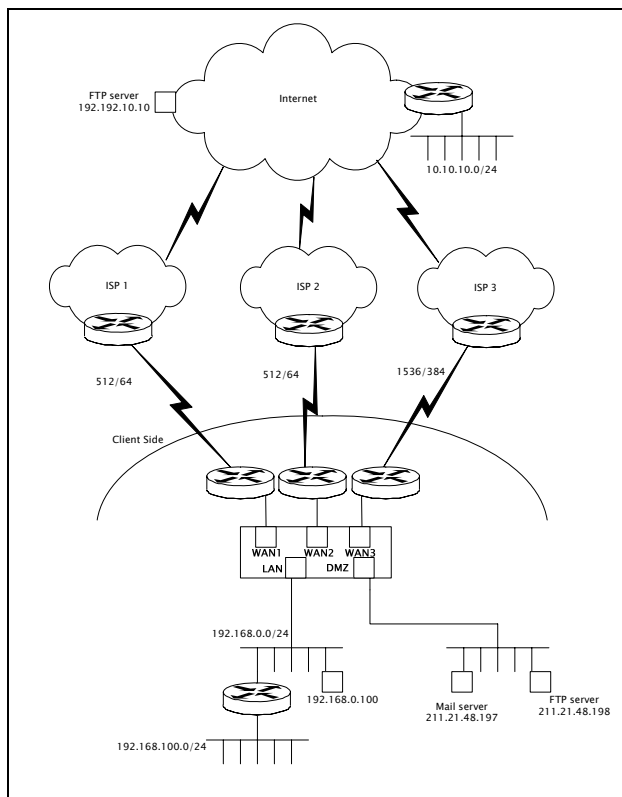


圖 3.25 Outbound BM 範例 1 架構示意圖

對外資料流量管理之需求條件：

- 設定廣域網路使用者從位於 DMZ 主機 211.21.48.198 抓取資料的流量控制。
- 設定廣域網路使用者從位於 DMZ 主機 211.21.48.197 抓取郵件資料的流量控制。

Classes 設定內容如下：

Name	Link	Busy Hour Settings			Idle Hour Setting		
		Guaranteed Kbps	Max Kbps	Priority	Guaranteed Kbps	Max Kbps	Priority
for FTP upload	WAN1	0	128	Normal	0	512	Normal
	WAN2	0	128	Normal	0	512	Normal
	WAN3	0	64	Normal	0	512	Normal
for mail server (POP3)	WAN1	0	128	Low	0	128	Low
	WAN2	0	128	Low	0	128	Low
	WAN3	0	256	Low	0	512	Low

表 3.38 Outbound BM 範例 1Classes 設定內容

Filters 設定內容如下：

Source	Destination	Service	Service At	Classes
211.21.48.198	WAN	FTP(21)	Non WAN	for FTP upload
211.21.48.197	WAN	POP3(110)	Non WAN	for mail server (POP3)

表 3.39 Outbound BM 範例 1Filters 設定內容

上傳頻寬資料流可以分兩種，以 **ftp** 為例，當 **server** 在廣域網路時使用者在非廣域網路上傳資料，或 **server** 在非廣域網路外部使用者下載資料，皆為上傳頻寬資料流，此時用的規則皆要列在 **Outbound BM** 管理的頁面。

Outbound BM 範例二

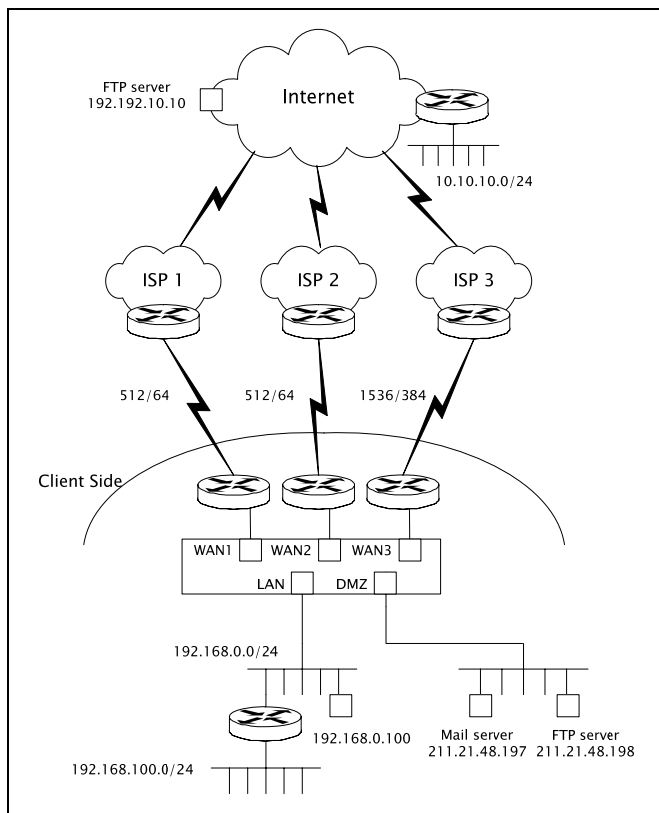


圖 3.26 Outbound BM 範例 2 架構示意圖

對外資料流量管理之需求條件為：

- 廣域網路使用者連線位於內部網路之虛擬主機 FTP server，其內部 IP 為 192.168.0.100，對上傳資料須進行流量控制。

註：在使用 Virtual Server 的狀況下，要 filter 的資料必須輸入原來區域網路主機的 IP 而不是被 Virtual Server 轉譯過後的公開 IP。

- 在廣域網路的某個子網路 (10.10.10/24)，讀取位於 DMZ 區域之 FTP 主機 211.21.48.198 的資料，須對 FTP 主機之資料流量進行控制。

Classes 設定內容如下：

Name	Link	Busy Hour Setting			Idle Hour Setting		
		Guaranteed Kbps	Max Kbps	Priority	Guaranteed Kbps	Max Kbps	Priority
for FTP	WAN1	100	200	Normal	0	512	Normal
	WAN2	50	100	Normal	0	512	Normal
	WAN3	50	100	Normal	0	512	Normal
for 10.10.10.0	WAN1	0	128	Low	0	256	Low
	WAN2	0	128	Low	0	256	Low
	WAN3	0	256	Low	0	512	Low

表 3.40 Outbound BM 範例 2 Classes 設定內容

Filters 設定內容如下：

Source	Destination	Service	Service At	Classes
192.168.0.100	WAN	FTP	non-WAN	for FTP
211.21.48.198	10.10.10.0/255.255.255.0	Any	non-WAN	for 10.10.10.0

表 3.41 Outbound BM 範例 2 Filters 設定內容

3.8 Connection Limit (連線限制)

在一個網路環境中，如果有某一台主機因為受到攻擊，會大量發出封包並癱瘓網路，這項功能的主要目的是設定連線建立的規則，然後在監控週期內，持續監看哪些 IP 位址的連線超過設定的上限，並作適當的處理。

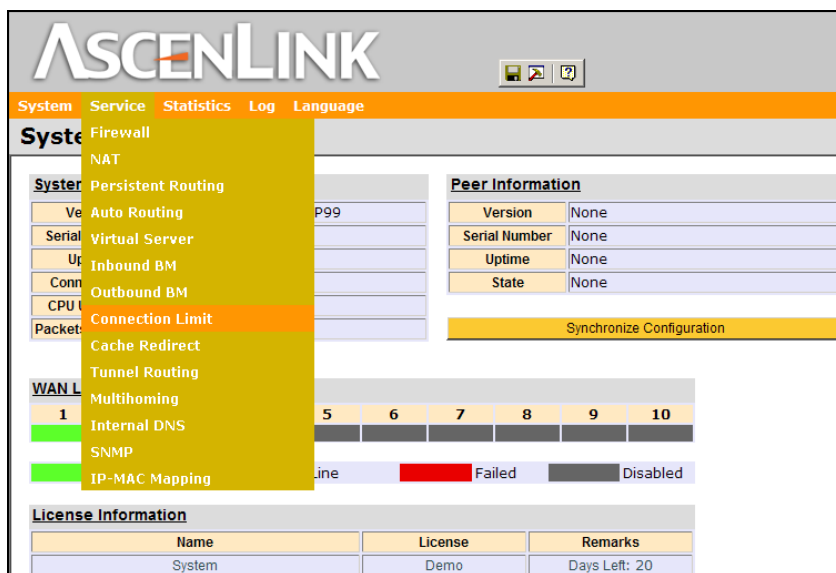


圖 3.27 Service /Connection Limit 功能所處位置

在 Connection Limit 這項功能裏，有下列欄位：

Log Interval 5 sec

Rules:

	Source	Limit	L
<div><div></div><div></div><div></div><div></div></div>	LAN	1000	<input checked="" type="checkbox"/>
	IP Address		
	IP Range		
	Subnet		
	WAN		
	LAN		
	DMZ		
	Any Address		
	FQDN:		

圖 3.28 Connection Limit 欄位介紹

■ Log Interval（記錄週期設定）

欄位	值	說明
Log Interval (記錄週期)	<second>	這個欄位填入產生記錄的週期，如果連線超過限制，則產生記錄在 Log 檔案。例如每設定每五秒記錄一次，如果來源位址所建立的連線數值超過規定數，則每五秒記錄一次，產生的資料寫入 Log 檔案中，秒數越短，記錄資料越多。

表 3.42 Connection Limit 記錄週期設定

■ Rule (連線限制規則設定)

欄位	值	說明
Source (來源)	IP Address IP Range Subnet WAN LAN DMZ Any Address FQDN <IP Grouping Name>	產生連線的來源，監視哪些位址、位址段、子網路： IP Address IP 位址：單一 IP，用在單一主機格式為 192.168.1.4。 IP Range IP 位址區段：比對一段 IP 位址，用在某幾台主機，格式為連續 IP 192.168.1.10-192.168.1.20。 Subnet 子網路：比對某一個網段，例如：192.168.1.0/255.255.255.0。 WAN：來自廣域網路的封包。 LAN：比對來自 LAN 埠的任何封包。 DMZ：比對來自 DMZ 埠的任何封包。 Any Address：比對來自任何位址的封包。 FQDN：比對來自某一個 FQDN 的封包。 如果在 [IP Grouping] 中設有 [Grouping Name] 也會出

		現在選項之中。
Limit (限制)	<連線數>	設定連線建立來源可允許之最大的連線數。
L (記錄)	Enable Disable	Enable (打勾)，該項規則使用時，產生 Log 檔案。 Disable (空白)，不產生 Log 檔案。

表 3.43 Connection Limit Rule 設定

設定範例

在此設定範例中限制子網路 192.168.1.1-192.168.1.254 中的所有主機每台的連線數量必須在五百個以下，若超過限制則每五秒鐘記錄於 Log 中。

Log Interval 5 sec

Rules:

	Source	Limit	L
<div>+</div> <div> <div>+</div> <div>-</div> <div>↑</div> <div>↓</div> </div>	192.168.1.0/255.255.255.0	500	<input checked="" type="checkbox"/>

圖 3.29 Connection Limit 設定範例

3.9 Cache Redirect (快取重定向)

AscenLink 可以和 Cache Server 快取伺服器搭配運作。當位於內部網路的用戶 (Client)，發出請求至外界的 Web Server 要求讀取資料時，AscenLink 將這項請求轉給 Cache Server。如果 Cache Serve 存有這份網頁，則 Cache Server 會回復這份網頁資料給 Client，如果沒有，則由 Cache Serve 至外界的 Web Server 讀取後，再回復給 Client。

Cache Server 可以設定在 AscenLink 的 DMZ 介面

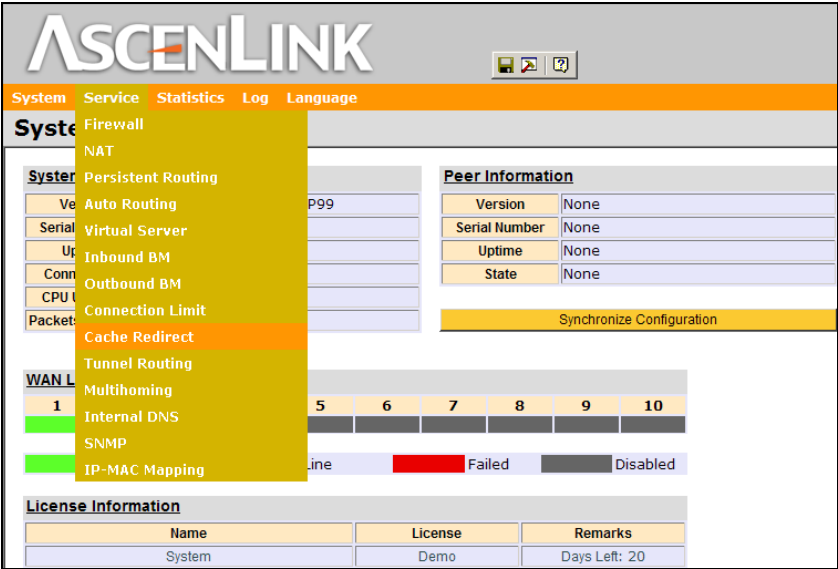


圖 3.30 Service /Cache Redirect 功能所處位置

在此頁面可設定快取重定向，要使用此功能須搭配支援通透式快取的快取伺服器，頁面主要的設定欄位有兩部份，如下圖所示：

Cache Group

Group Name

AscenGate

Group Servers

IP

192.168.50.53

Port

80

Weight

1

Associated WAN

NO

Redirect Rule

Source

LAN

Destination

WAN

Port

80

Group

AscenGate

L

圖 3.31 Cache Redirect 設定欄位

■ Cache Group (快取群組)

在此表格中設定快取伺服器的群組，可定義不同的群組以給不同的來源與目的地 IP，同一個群組內亦可定義多個快取伺服器。

欄位	值	說明
Group Name (群組名稱)	<群組名稱>	啓用 Cache Redirect 功能，或取消這項功能。
IP	<快取伺服器 IP 位址>	在此欄位輸入快取伺服器 IP。
Port (埠)	Ex: 80	輸入快取伺服器所指用的通訊埠，一般而言爲 80,3128 或 8080。
Weight (權植)	Ex: 1,2...	在此輸入此伺服器的使用權值，權值越高會被使用到的機率越高。
Associated WAN (要偵測的 WAN)	NO, 1, 2...	指定此快取伺服器所使用的廣域網路連線，只有當 Associated WAN 和快取伺服器都在正常狀態時才會做封包重導。選擇"NO"表示快取重導服務不會與廣域網路線路有關聯，只要快取伺服器是在正常狀態，系統就會執行封包重導服務。

表 3.44 Cache Redirect 欄位說明表

■ Redirect Ruler(重導規則)

此表格用來設定用來作重導流量的主機或主機群。

欄位	值	說明
Source (來源)	IP Address IP Range Subnet LAN DMZ Any Address	在此欄位指定需要作快取導向的來源 IP 或 IP 群，選擇 IP Address 或 IP Range 選項時，需要輸入 IP 值。
Destination (目的地)	IP Address IP Range Subnet WAN	在此欄位指定需要作快取導向的目的地 IP，選擇 IP Address 或 IP Range 選項時，需要輸入 IP 值。
Port (埠)	Ex: 80	指定使用快取導向的通訊埠。
Group (群組)	NO REDIRECT <群組名稱>	在此欄位選定使用的快取群組，由上方的快取群組中選出。
L (記錄)	指定或取消	Enable (打勾)，該項規則使用時，產生 Log 檔案。 Disable (空白)，不產生 Log 檔案。

表 3.45 Cache Redirect 各功能選項解釋之參照表

範例一 Cache Server 沒有存有 Client 請求的資料

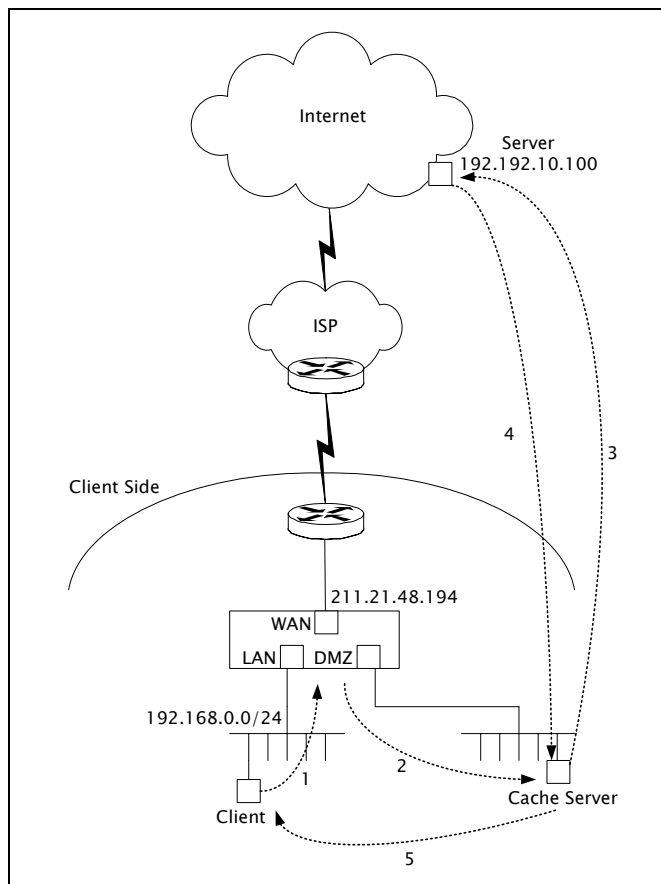


圖 3.32 Cache Miss 狀態下資料流走向

Client 發出 Request 要至 Web Server 讀取資料，AscenLink 收到 Client 發出的請求 (Request)，將這項請求轉給 Cache Server。

如果 Cache Server 發現沒有要求讀取的網頁，則 Cache Server 自行前往 Web Server 抓取資料，Web Server 將 Page 送到 Cache Server。最後 Cache Server 回復 Client Request 的網頁。(請看上圖的曲線示意)

範例二 Cache Server 存有 Client 要求的資料

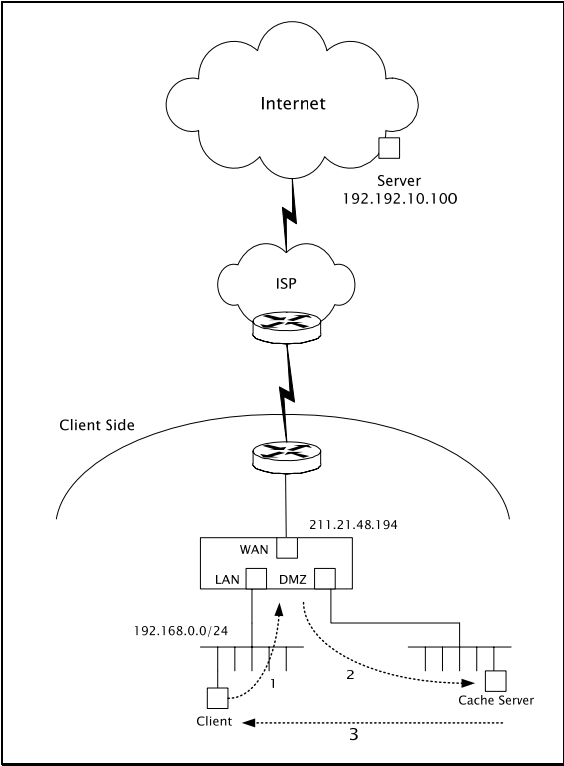


圖 3.33 Cache Hit 狀態下資料流走向

Client 發出 Request，AscenLink 收到 Request，將 Request 轉往 Cache Serve。
Cache Server 回復 Client Request 的網頁。

3.10 Tunnel Routing (通道路由)

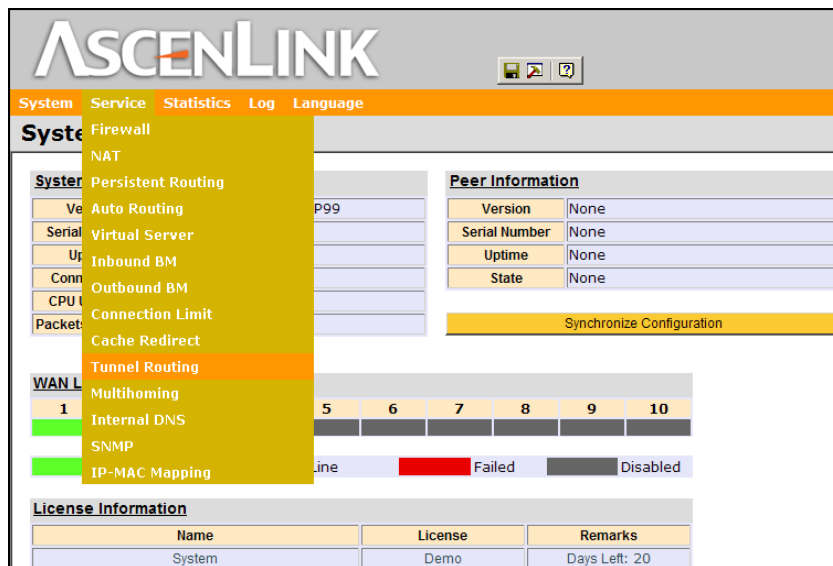


圖 3.34 Service / Tunnel Routing 功能所處位置

所謂的通道路由是指:在兩台 AscenLink 之間建立數條專用通道，讓屬於特定群組的封包經由這些通道，從一台 Ascenlink 到達另一台 AscenLink。

通道路由的優點是：當其中任何一台 AscenLink 的某條 WAN 斷線時，特定群組的封包仍然會經由其他條通道到達另一台 AscenLink，而不會造成封包傳送中斷的情況。

AscenLink 除具備上述優點之外，還支援對 ADSL 等採用動態 IP 的 WAN 線路建立通道路由；此外透過兩台 AscenLink 建立通道路由之後，用戶還可以透過通道路由來管理遠端的 AscenLink。

AscenLink 還可以對通道路由的 WAN 線路，設置冗餘線路。當該條線路斷掉時，就可以根據在通道路由的路由規則，來切換到其他的線路，或者讓該線路上的封包，不經由通道路由而透過自動路由的線路到達對端。此外透過路由規則，管理者還可

以對多台 AscenLink 的通道路由設置封包轉發的路由規則來達到多台 AscenLink 之間互連互通。此外在某些特殊的網路架構下，AscenLink 還可以更加靈活的設置路由規則，讓多台透過專線建立通道路由的 AscenLink，在存取 Internet 的時候只有透過一台 AscenLink 的 WAN 線路進行存取，以達到 Central Routing 之目的。

通常在一些網路上的網路環境，基於各方面因素的考慮，對某些特定服務，如 HTTP、HTTPS 等，需要使用者持續使用原來連接的線路，但 Tunnel Routing 會依據條件切換不同連接之線路，這樣會造成訪問時，被拒絕登入，根據這個需求可以使用 PR (Persistent Routing) 來對某些特定服務只在一條線路上運行，防止因為線路的切換而導致被拒絕登入。

在此頁面可設定通道路由，頁面主要的設定欄位有三部份，分別是：

■ Local Host ID&Key （記錄及本地端 ID 以及密鑰的設定）

在此表格中設定是否把通道路由記錄保存在 Log 檔案裏；並為本地的通道路由設置一個 ID 號，作為通道路由的一個識別標識。當 WAN 線路的 IP 位址為動態 IP 時，必須設置本地端 ID 號。若想對已建立的通道路由進行加密，則必須先在此設定加密密鑰。

欄位	值	說明
Tunnel Route Log (通道路由記錄)	Enable(打勾) Disable (空白)	通道路由記錄會在 Log 檔案裏 不會產生任何記錄
Local Host ID(本地端 ID)	EX: 12xyz.b_d-xxx	在此欄位輸入本地端 ID 號。
Key (密鑰)	EX: 1234	在此設定加密密碼
Confirm (確認)	EX: 1234	確認上面輸入的密碼

表 3.46 Tunnel Group 記錄及本地端 ID 設定

■ Tunnel Group (通道群組)

在此表格中設定通道連線的群組，可定義不同的群組以給不同的來源與目的地 IP，同一個群組內亦可定義多條通道路由。

欄位		值	說明
Group Name (群組名稱)		<群組名稱>	在此定義各個群組的名稱。
Remote Host ID (遠端 ID)		EX: 11xyz.b_d-yyy	在此欄位輸入遠端 ID 號。
Algorithm (演算法)		Round-Robin By Traffic	Round-Robin (輪流指派):表示依照所輸入的流量比例方式在指定的某個廣域網路連線上分配流量。 By Traffic (線路使用流量):比較加入通道路由的線路所有使用頻寬，讓資料流使用剩餘頻寬較多的線路。 註: 使用 Round-Robin 演算法需要在“群組通道”的“權重”選項中設置各個線路的權重數。
Group Tunnels(群 組)	Local IP (本地端 IP)	IP Address (NAT)IP Address Dynamic IP (NAT)Dynamic IP	在此欄位選擇本地端 IP 位址。 IP Address IP 位址: WAN 線路 IP 位址，用在本地端 WAN 線路為固定 IP 位址情形。

			(NAT) IP Address (NAT)IP 位址： 經由 NAT 轉換后的靜態 IP 位址。 Dynamic IP 動態 IP：選擇使用動態 IP 的 WAN 線路，用在本地端 WAN 線路的 IP 為動態 IP 位址情形。 (NAT)Dynamic IP (NAT)動態 IP： 經由 NAT 后的動態 IP 位址。
	Remote IP(遠程 IP)	IP Address Dynamic IP	在此欄位輸入遠程(即目的地)IP 位址。 IP Address IP 位址：WAN 線路 IP 位址，用在遠端 WAN 線路為固定 IP 位址情形。 Dynamic IP 動態 IP：選擇使用動態 IP 的 WAN 線路，用在遠端 WAN 線路的 IP 為動態 IP 位址情形。
	Weight (權重)	EX: 1,2...	在此輸入此通道的使用權重，權重越高會被使用到的機率越高。
	Encrypt(加密)	勾中復選框以啓用	設定是否對通道路由進行加密
Default Rule (預設規則)	Source (來源)	IP 位址 IP 位址區段 子網路 區域網路 隔離區 任何位址	產生連接之來源： IP 位址單一 IP，用在單一主機格式為 192.168.1.4 IP 位址區段核對一段 IP 位址，用在某幾台主機，格式為連續 IP 192.168.1.10-192.168.1.20 子網核對某一個網段，例如： 192.168.1.0/255.255.255.0 LAN 核對來自 LAN 的任何封包 DMZ 核對來自 DMZ 的任何封包
	Fail-Over (備援)	無動作 自動路由 群組...	採用通道群組中所設定的群組或者自動路由政策做為 Tunnel 的備援。當默認規則不可用的時候，會切換到備援政策

表 3.47 Tunnel Group 各功能選項解釋之參照表

■ Routing Rules (路由規則)

欄位	值	說明
Source (來源)	IP 位址 IP 位址區段 子網域 區域網路 隔離區 任何位址	產生連線的來源： IP 位址：單一 IP，用在單一主機格式為 192.168.1.4。 IP 位址區段：比對一段 IP 位址,用在某幾台主機,格式為連續 IP 192.168.1.10-192.168.1.20 子網路：比對某一個網段，例如： 192.168.1.0/255.255.255.0。 區域網路：比對來自區域網路的任何封包 隔離區：比對來自隔離區的任何封包 任何位址：比對任何封包
Destination (目的地)	IP 位址 IP 位址區段 子網域 廣域網路	連線的目的地： IP 位址：單一 IP，用在單一主機格式為 192.168.1.4。 IP 位址區段：比對一段 IP 位址,用在某幾台主機,格式為連續 IP 192.168.1.10-192.168.1.20 子網路：比對某一個網段，例如： 192.168.1.0/255.255.255.0。 廣域網路：比對來自廣域網路埠的任何封包
Service (服務)	FTP SSH TELNET SMTP DNS HTTP POP3 H323 ICMP ... TCP@ UDP@ Protocol# 任何服務	選擇欲存取的目的地位址的服務類型，預設為：任何服務。例如：針對來源為：192.168.0.1 存取目的地位址為：192.168.90.1 的 HTTP 服務，則需在服務中選擇 “HTTP(80)”
Group (群組)	無動作 Group	Tunnel Group 中所設定的群組。
Fail-Over (備援)	無動作 自動路由 群組....	當 Routing Rules 中的 Group 線路不可使用時，所要採取的備援線路。可選項有： NO-ACTION：無動作 Auto-Routing：封包經由自動路由所設定的線路 Tunnel Group：採用另外的 Tunnel Group 所定的線路

表 3.48 Routing Rules 各功能選項解釋之參照表

■ Persistent Rules (持續路由規則)

欄位	值	說明
Source (來源)	IP 位址 IP 位址區域 子網路 區域網路 隔離區 任何位址	封包來源比對方式 IP 位址 單一 IP,用在單一主機格式為 192.168.1.4 IP 位址區段 比對一段 IP 位址,用在某幾台主機,格式為連續 IP 192.168.1.10-192.168.1.20 子網路 比對某一個網段,例如: 192.168.1.0/255.255.255.0 廣域網路 比對來自廣域網路的任何封包 區域網路 比對來自區域網路的任何封包 隔離區 比對來自隔離區的任何封包 任何位址 比對任何封包
Destination (目的地)	IP 位址 IP 位址區域 子網路 廣域網路	封包目的地比對方式 IP 位址 單一 IP,用在單一主機格式為 192.168.1.4 IP 位址區段 比對一段 IP 位址,用在某幾台主機,格式為連續 IP 192.168.1.10-192.168.1.20 子網路 比對某一個網段,例如: 192.168.1.0/255.255.255.0 廣域網路 比對來自廣域網路埠的任何封包 區域網路 比對來自區域網路埠的任何封包
Service (服務)	FTP SSH TELNET SMTP DNS HTTP POP3 H323 ICMP ... TCP@ UDP@ 任何服務	提供服務的種類,除了內定的服務外,亦可自訂某個 UDP/TCP port 或 port range 如 TCP@123-234, 或過濾 ICMP 封包

表 3.49 Routing Rules 各功能選項解釋之參照表

範例 1 Tunnel Routing 基本設定

某公司的總部設在北京，在上海和廣州各有分公司。每間公司都擁有一個 LAN，兩條 WAN 線路，在 DMZ 內有 VPN Gateway，其相關資訊如下：

	Beijing(北京)	Shanghai(上海)	Guangzhou(廣州)
WAN 1	1.1.1.1	2.2.2.2	6.6.6.6
WAN 2	3.3.3.3	4.4.4.4	8.8.8.8
WAN 3	Dynamic IP	N/A	10.10.10.10
VPN Gateway	1.1.1.11	2.2.2.22	6.6.6.66
LAN	192.168.1.0/24	192.168.2.0/24	192.168.3.0/24

表 3.50 Tunnel Routing 範例 1 設定

北京總公司的設定如下：

啓用通道路由記錄，且 Tunnel Routing 的本地端 ID 設置爲：T1。

▫ Tunnel Group 設定

+	Group Name	Remote HostID	Algorithm	Tunnels				
+ - ↑ ↓	Shanghai	T2	Weight					
					+	Local IP	Remote IP	Weight
					+ - ↑ ↓	1.1.1.1	2.2.2.2	1
					+ - ↑ ↓	1.1.1.1	4.4.4.4	1
+ - ↑ ↓	Backup Shanghai	T2	Weight					
					+ - ↑ ↓	3.3.3.3	2.2.2.2	1
					+ - ↑ ↓	3.3.3.3	4.4.4.4	1
+ - ↑ ↓	Guangzhou	K3	Weight					
					+	Local IP	Remote IP	Weight
					+ - ↑ ↓	1.1.1.1	6.6.6.6	1
					+ - ↑ ↓	3.3.3.3	8.8.8.8	1
+ - ↑ ↓	Backup Guangzhou	K3	Weight					
					+ - ↑ ↓	Dynamic IP	10.10.10.10.	1

表 3.51 Tunnel Routing 範例 1:Tunnel Group 設定(1)

▫ Routing Rules 設定

+	Source	Destination	Service	Group	Fail-Over
+ - ↑ ↓	1.1.1.11	2.2.2.22	Any	Shanghai	Backup Shanghai
+ - ↑ ↓	1.1.1.11	6.6.6.66	Any	Guangzhou	Backup Guangzhou
+ - ↑ ↓	192.168.1.1-192.168.1.10	192.168.2.1-192.168.2.10	Any	Shanghai	AR
+ - ↑ ↓	192.168.1.1-192.168.1.10	192.168.2.1-192.168.2.10	Any	Guangzhou	No-Action

表 3.52 Tunnel Routing 範例 1:Routing Rules 設定(1)

上海分公司設定如下：

啓用通道路由記錄，且 Tunnel Routing 的本地端 ID 設置爲：T2。

▫ Tunnel Group 設定

+	Group Name	Remote ID	Algorithm	Tunnels					
+ - ↑ ↓	Beijing	T1	Weight						
				+	Local IP	Remote IP	Weight		
				+ - ↑ ↓	2.2.2.2	1.1.1.1	1		
				+ - ↑ ↓	2.2.2.2	3.3.3.3	1		
				+ - ↑ ↓	4.4.4.4	1.1.1.1	1		
				+ - ↑ ↓	4.4.4.4	3.3.3.3	1		

表 3.53 Tunnel Routing 範例 1:Tunnel Group 設定(2)

▫ Routing Rules 設定

+	Source	Destination	Service	Group	Fail-Over
+ - ↑ ↓	192.168.2.1-192.168.2.10	192.168.1.1-192.168.1.10	Any	Beijing	No-Action
+ - ↑ ↓	2.2.2.22	1.1.1.11	Any	Beijing	AR

表 3.54 Tunnel Routing 範例 1:Routing Rules 設定(2)

廣州分公司設定如下：
啓用通道路由記錄，且 Tunnel Routing 的本地端 ID 設置爲：K3。

Tunnel Group 設定

+	Group Name	Remote ID	Algorithm	Tunnels				
+- ↑↓	Beijing	T1	Weight					
				+	Local IP	Remote IP	Weight	
				+-↑↓	6.6.6.6	1.1.1.1	1	
				+-↑↓	6.6.6.6	3.3.3.3	1	
				+-↑↓	8.8.8.8	1.1.1.1	1	
				+-↑↓	8.8.8.8	3.3.3.3	1	
				+-↑↓	10.10.10.10	Dynamic	1	

表 3.55 Tunnel Routing 範例 1:Tunnel Group 設定(3)

Routing Rules 設定

+	Source	Destination	Service	Group	Fail-Over
+- ↑↓	192.168.3.1-192.168.3.10	192.168.1.1-192.168.1.10	Any	Beijing	No-Action
+- ↑↓	6.6.6.66	1.1.1.11	Any	Beijing	AR

表 3.56 Tunnel Routing 範例 1:Routing Rules 設定(3)

根據上述設定，只要是從 1.1.1.11(或 192.168.1.1-192.168.1.10)到 2.2.2.22 的封包都會被包成 GRE 型式的封包傳送出去。如果 1.1.1.1 的 WAN 線路斷線，封包仍然會從 3.3.3.3 的備援線路送出，而不會發生斷線的情況。

註：凡使用 Tunnel Routing 的 AscenLink，其設定值必須互相對應，否則 Tunnel Routing 無法發揮功用。例如:將上海 AscenLink 上的 Routing rule 設定值 2.2.2.2 到 3.3.3.3 刪除的話，即使北京的 AscenLink 有設 3.3.3.3 到 2.2.2.2 這條 rule，Tunnel Routing 還是無法發揮作用。

想設定各通道所使用的頻寬，我們可以在 **service->Inbound BM** 和 **Outbound BM** 中設定 **GRE** 封包的最大/最小佔用頻寬（以下為上海 AscenLink 設定值為例）

▫ **Filter (對內頻寬管理)**

來源	目的地	服務	服務所在地	服務類型
1.1.1.1	2.2.2.2	GRE	WAN	Beijing-VPN
1.1.1.1	4.4.4.4	GRE	WAN	Beijing-VPN
3.3.3.3	2.2.2.2	GRE	WAN	Beijing-VPN
3.3.3.3	4.4.4.4	GRE	WAN	Beijing-VPN

表 3.57 Tunnel Routing 範例 1: Inbound BM Filter 設定

▫ **Filter (對外頻寬管理)**

來源	目的地	服務	服務所在地	服務類型
2.2.2.2	1.1.1.1	GRE	WAN	Beijing-VPN
2.2.2.2	3.3.3.3	GRE	WAN	Beijing-VPN
4.4.4.4	1.1.1.1	GRE	WAN	Beijing-VPN
4.4.4.4	3.3.3.3	GRE	WAN	Beijing-VPN

表 3.58 Tunnel Routing 範例 1: Outbound BM Filter 設定

範例 2：Tunnel Routing Dynamic IP（通道路由：動態 IP）

某公司的總部設在北京，在上海設有分公司。北京公司擁有兩條 WAN 線路，其中靜態 IP 一條、動態 IP 一條。上海公司擁有兩條動態 IP 的 WAN 線路。

需求：LAN1 與 LAN2 區域透過 AscenLink 建立 Tunnel 直接連通。在兩條線路上封包按照 1:1 的比例進行資料的傳輸。

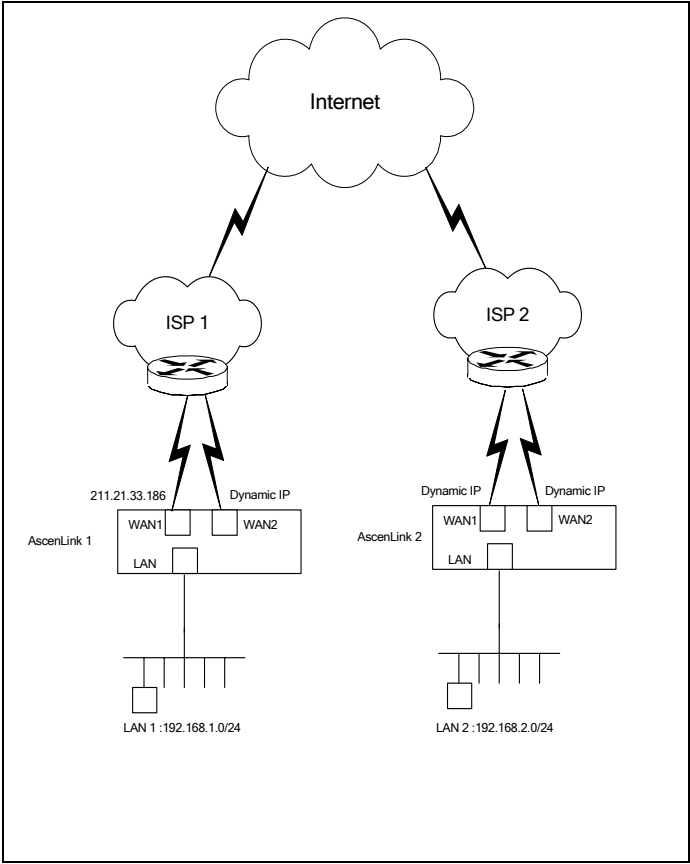


圖 3.35 Tunnel Routing 範例 2 架構示意圖

相關資訊如下：

	Beijing (北京)	Shanghai (上海)
WAN 1	211.21.33.186	Dynamic IP
WAN 2	Dynamic IP	Dynamic IP
LAN	192.168.1.0/24	192.168.2.0/24

表 3.59 Tunnel Routing 範例 2 相關資訊

(Beijing) 北京總公司的設定如下：

- 記錄及本機 ID 設定

通道路由記錄	啓用
本機 ID	Beijing

表 3.60 Tunnel Routing 範例 2:記錄及本機 ID 設定(Beijing 總公司)

- Tunnel Group 設定

+	Group Name	Remote Host ID	Algorithm	Tunnels				
+ - ↑ ↓	Beijing to Shanghai	Shanghai	Weight					
				+	Local IP	Remote IP	Weight	
				+ - ↑ ↓	211.21.33.186	Dynamic IP at WAN1	1	
				+ - ↑ ↓	Dynamic IP at WAN2	Dynamic IP at WAN2	1	

表 3.61 Tunnel Routing 範例 2:Tunnel Group 設定(Beijing 總公司)

Routing Rules 設定

+	Source	Destination	Service	Group	Fail-Over
+ - ↑ ↓	192.168.1.0/255.255.255.0	192.168.2.0/255.255.255.0	Any	Beijing to Shanghai	No-ACTION

表 3.62 Tunnel Routing 範例 2:Routing Rules 設定(Beijing 總公司)

(Shanghai) 上海分公司的設定如下：

記錄及本機 ID 設定

通道路由記錄	啓用
本機 ID	Shanghai

表 3.63 Tunnel Routing 範例 2:記錄及本機 ID 設定(Shanghai 分公司)

Tunnel Group 設定

+	Group Name	Remote Host ID	Algorithm	Tunnels					
+ - ↑ ↓	Shanghai to Beijing	Beijing	Weight						
				+	Local IP	Remote IP	Weight		
				+ - ↑ ↓	Dynamic IP at WAN1	211.21.33.186	1		
				+ - ↑ ↓	Dynamic IP at WAN2	Dynamic IP at WAN2	1		

表 3.64 Tunnel Routing 範例 2:Tunnel Group 設定(Shanghai 分公司)

Routing Rules 設定

+	Source	Destination	Service	Group	Fail-Over
+ - ↑ ↓	192.168.2.0/255.255.255.0	192.168.1.0/255.255.255.0	Any	Shanghai to Beijing	No-ACTION

表 3.65 Tunnel Routing 範例 2:Routing Rules 設定(Shanghai 分公司)

範例 3：Tunnel Routing：Forwarding（通道路由：轉發）

某公司的總部設在北京，在上海和天津設有分公司。北京總公司擁有一條 WAN 線路。上海、天津兩公司各擁有一個 LAN、一條 WAN 線路，並分別與北京總部建立 Tunnel。其相關資訊如圖。

需求：上海、天津的 LAN 可透過 Tunnel 進行通信。

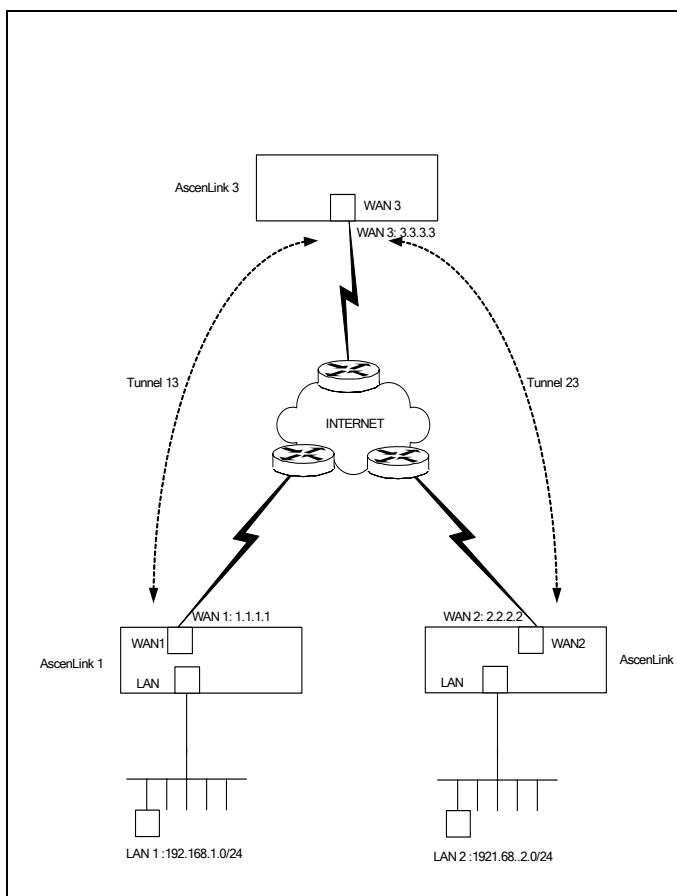


圖 3.36 Tunnel Routing 範例 3 架構示意圖

相關資訊如下：

	Beijing (北京) AscenLink 3	Tianjin (天津) AscenLink 1	Shanghai (上海) AscenLink 2
WAN 1		1.1.1.1	
WAN 2			2.2.2.2
WAN 3	3.3.3.3		
LAN		192.168.1.0/24	192.168.2.0/24

表 3.66 Tunnel Routing 範例 3 相關資訊

(Beijing) 北京總公司的設定如下：

- 記錄及本機 ID 設定

通道路由記錄	啓用
本機 ID	Beijing

表 3.67 Tunnel Routing 範例 3:記錄及本機 ID 設定(Beijing 總公司)

- Tunnel Group 設定

+	Group Name	Remote Host ID	Algorithm	Tunnels				
+ - ↑ ↓	Beijing to Tianjin	Tianjin	Weight					
				+	Local IP	Remote IP	Weight	
				+ - ↑ ↓	3.3.3.3	1.1.1.1	1	
+ - ↑ ↓	Beijing to Shanghai	Shanghai	Weight					
				+	Local IP	Remote IP	Weight	
				+ - ↑ ↓	3.3.3.3	2.2.2.2	1	

表 3.68 Tunnel Routing 範例 3:Tunnel Group 設定(Beijing 總公司)

▫ Routing Rules 設定

+	Source	Destination	Service	Group	Fail-Over
+ - ↑ ↓	192.168.1.0/255.255.255.0	192.168.2.0/255.255.255.0	Any	Beijing to Shanghai	No-ACTION
+ - ↑ ↓	192.168.2.0/255.255.255.0	192.168.1.0/255.255.255.0	Any	Beijing to Tianjin	No-ACTION

表 3.69 Tunnel Routing 範例 3:Routing Rules 設定(Beijing 總公司)

(Shanghai) 上海分公司的設定如下：

▫ 記錄及本機 ID 設定

通道路由記錄	啓用
本機 ID	Shanghai

表 3.70 Tunnel Routing 範例 3:記錄及本機 ID 設定(Shanghai 分公司)

▫ Tunnel Group 設定

+	Group Name	Remote Host ID	Algorithm	Tunnels				
+ - ↑ ↓	Shanghai to Beijing	Beijing	Weight					
				+	Local IP	Remote IP	Weight	
				+ - ↑ ↓	2.2.2.2	3.3.3.3	1	

表 3.71 Tunnel Routing 範例 3:Tunnel Group 設定(Shanghai 分公司)

▫ Routing Rules 設定

+	Source	Destination	Service	Group	Fail-Over
+ - ↑ ↓	192.168.2.0/255.255.255.0	192.168.1.0/255.255.255.0	Any	Shanghai to Beijing	No-ACTION

表 3.72 Tunnel Routing 範例 3:Routing Rules 設定(Shanghai 分公司)

(Tianjin) 天津分公司的設定如下：

- 記錄及本機 ID 設定

通道路由記錄	啓用
本機 ID	Tianjin

表 3.73 Tunnel Routing 範例 3:記錄及本機 ID 設定(Tianjin 分公司)

- Tunnel Group 設定

+	Group Name	Remote Host ID	Algorithm	Tunnels				
				+	Local IP	Remote IP	Weight	
+ - ↑ ↓	Tianjin to Beijing	Beijing	Weight					
				+ - ↑ ↓	1.1.1.1	3.3.3.3	1	

表 3.74 Tunnel Routing 範例 3:Tunnel Group 設定(Tianjin 分公司)

- Routing Rules 設定

+	Source	Destination	Service	Group	Fail-Over
+ - ↑ ↓	192.168.1.0/255.255.255.0	192.168.2.0/255.255.255.0	Any	Tianjin to Beijing	No-ACTION

表 3.75 Tunnel Routing 範例 3:Routing Rules 設定(Tianjin 分公司)

範例 4：Tunnel Routing：Central Routing（通道路由：中心路由）

某公司的總部設在北京，在上海和天津設有分公司。該公司有自己的 Intranet，天津分公司沒有連線到 Internet 的線路，如果想存取 Internet 需要透過與總部建立 Tunnel 後透過總部廣域網線路存取 Internet。上海分公司有直接連線到 Internet 的線路，可以直接存取 Internet，當這條線路一旦失效、將利用和總部間的 Tunnel 作為備援線路，保證存取 Internet 的不間斷。

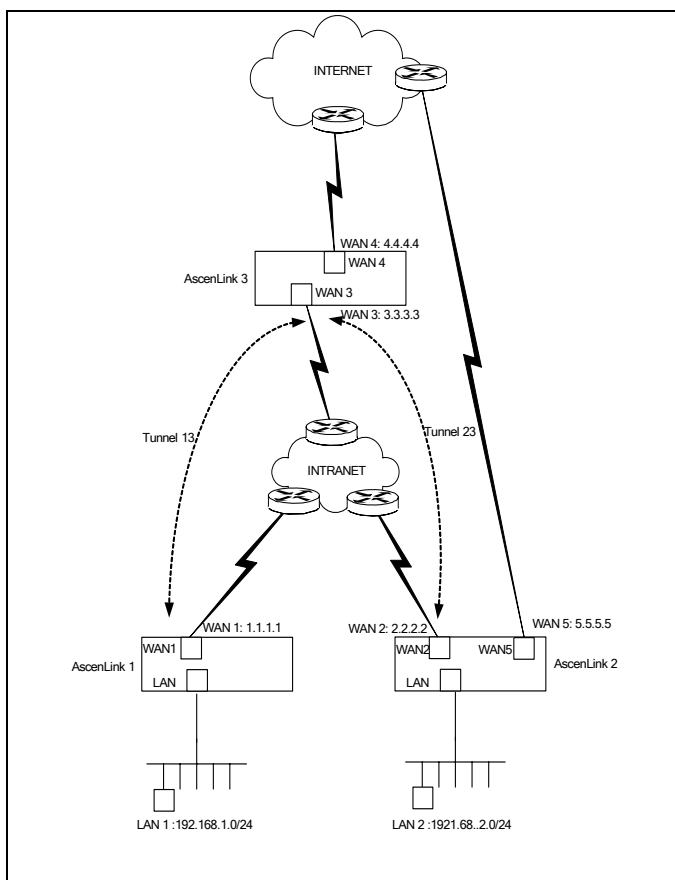


圖 3.37 Tunnel Routing 範例 4 架構示意圖

相關資訊如下：

	Beijing(北京) AscenLink 3	Tianjin (天津) AscenLink 1	Shanghai (上海) AscenLink 2
WAN 1		1.1.1.1	
WAN 2			2.2.2.2
WAN 3	3.3.3.3		
WAN 4	4.4.4.4		
WAN 5			5.5.5.5
LAN		192.168.1.0/24	192.168.2.0/24

表 3.76 Tunnel Routing 範例 4:相關資訊

(Beijing) 北京總公司的設定如下：

Tunnel Routing 部分

- 記錄及本機 ID 設定

通道路由記錄	啓用
本機 ID	Beijing

表 3.77 Tunnel Routing 範例 4:記錄及本機 ID 設定(Beijing 總公司)

- Tunnel Group 設定

+	Group Name	Remote Host ID	Algorithm	Tunnels			
+ - ↑ ↓	Beijing to Tianjin	Tianjin	Weight	+	Local IP	Remote IP	Weight
				+ - ↑ ↓	3.3.3.3	1.1.1.1	1
+ - ↑ ↓	Beijing to Shanghai	Shanghai	Weight	+	Local IP	Remote IP	Weight
				+ - ↑ ↓	3.3.3.3	2.2.2.2	1

表 3.78 Tunnel Routing 範例 4:Tunnel Group 設定(Beijing 總公司)

▫ Routing Rules 設定

+	Source	Destination	Service	Group	Fail-Over
+ - ↑↓	Any Address	192.168.2.0/255.255.255.0	Any	Beijing to Shanghai	No-ACTION
+ - ↑↓	Any Address	192.168.1.0/255.255.255.0	Any	Beijing to Tianjin	No-ACTION

表 3.79 Tunnel Routing 範例 4:Routing Rules 設定(Beijing 總公司)

Auto Routing 部分

▫ Policies 設定

Label	Algorithm	Parameter
WAN4	Fixed	在 4 的位置打勾
Default Policy	By Downstream Traffic	在 1、2、3、4……的位置打勾

表 3.80 Tunnel Routing 範例 4:Auto Routing Policies 設定(Beijing 總公司)

▫ Filters 設定

Source	Destination	Service	Routing Policy	Fail-Over Policy
Tunnel	WAN	ANY	WAN4	Default Policy
Any Address	WAN	ANY	Default Policy	No-ACTION

表 3.81 Tunnel Routing 範例 4:Auto Routing Filters 設定(Beijing 總公司)

(Shanghai) 上海分公司的設定如下：

Tunnel Routing 部分

- 記錄及本機 ID 設定

通道路由記錄	啓用
本機 ID	Shanghai

表 3.82 Tunnel Routing 範例 4:記錄及本機 ID 設定(Shanghai 分公司)

- Tunnel Group 設定

+	Group Name	Remote Host ID	Algorithm	Tunnels			
				+	Local IP	Remote IP	Weight
+ - ↑ ↓	Shanghai to Beijing	Beijing	Weight	+ - ↑ ↓	2.2.2.2	3.3.3.3	1

表 3.83 Tunnel Routing 範例 4:Tunnel Group 設定(Shanghai 分公司)

- Routing Rules 設定

+	Source	Destination	Service	Group	Fail-Over
+ - ↑ ↓	Any Address	192.168.2.0/255.255.255.0	Any	Shanghai to Beijing	No-ACTION

表 3.84 Tunnel Routing 範例 4:Routing Rules 設定(Shanghai 分公司)

Auto Routing 部分

▫ Policies 設定

Label	Algorithm	Parameter
WAN5	Fixed	在 5 的位置打勾
Default Policy	By Downstream Traffic	在 1、2、3、4……的位置打勾

表 3.85 Tunnel Routing 範例 4:Auto Routing 設定(Shanghai 分公司)

▫ Filters 設定

Source	Destination	Service	Routing Policy	Fail-Over Policy
Any Address	WAN	ANY	WAN5	Tunnel:Shanghai to Beijing
Any Address	WAN	ANY	Default Policy	No-ACTION

表 3.86 Tunnel Routing 範例 4:Auto Routing Filters 設定(Shanghai 分公司)

(Tianjin) 天津分公司的設定如下：

- 記錄及本機 ID 設定

通道路由記錄	啓用
本機 ID	Tianjin

表 3.87 Tunnel Routing 範例 4:記錄及本機 ID 設定(Tianjin 分公司)

- Tunnel Group 設定

+	Group Name	Remote Host ID	Algorithm	Tunnels			
+ - ↑ ↓	Tianjin to Beijing	Beijing	Weight	+	Local IP	Remote IP	Weight
				+ - ↑ ↓	1.1.1.1	3.3.3.3	1

表 3.88 Tunnel Routing 範例 4:Tunnel Group 設定(Tianjin 分公司)

- Routing Rules 設定

+	Source	Destination	Service	Group	Fail-Over
+ - ↑ ↓	Any Address	WAN	Any	Tianjin to Beijing	No-ACTION

表 3.89 Tunnel Routing 範例 4:Routing Rules 設定(Tianjin 分公司)

範例 5：Tunnel Routing：Persistent Routs（通道路由：持續路由策略）

某公司的總部設在北京，在上海有分公司。每間公司都擁有一個 LAN，兩條 WAN 線路，要求在兩個公司建立 2 條 Tunnel，並將 HTTP 服務保持在某一條 Tunnel 上。其相關資訊如下：

	Beijing(北京)	Shanghai(上海)
WAN 1	1.1.1.1	2.2.2.2
WAN 2	3.3.3.3	4.4.4.4
WAN 3	Dynamic IP	N/A

表 3.90 Tunnel Routing 範例 5 設定

北京總公司的設定如下：

啓用通道路由記錄，且 Tunnel Routing 的本地端 ID 設置為：T1。

▫ Tunnel Group

+	Group Name	Remote HostID	Algorithm	Tunnels					
+ - ↑ ↓	Shanghai	T2	Weight						
				+	Local IP	Remote IP	Weight		
				+ - ↑ ↓	1.1.1.1	2.2.2.2	1		
				+ - ↑ ↓	1.1.1.1	4.4.4.4	1		
+ - ↑ ↓	Backup Shanghai	T2	Weight						
				+ - ↑ ↓	3.3.3.3	2.2.2.2	1		
				+ - ↑ ↓	3.3.3.3	4.4.4.4	1		

表 3.91 Tunnel Routing 範例 5:Tunnel Group 設定(1)

▫ Routing Rules

+	Source	Destination	Service	Group	Fail-Over
+ - ↑ ↓	1.1.1.11	2.2.2.22	Any	Shanghai	Backup Shanghai
+ - ↑ ↓	192.168.1.1-192.168.1.10	192.168.2.1-192.168.2.10	Any	Shanghai	AR

表 3.92 Tunnel Routing 範例 5:Routing Rules 設定(1)

上海分公司設定如下：
啓用通道路由記錄，且 Tunnel Routing 的本地端 ID 設置爲：T2。

Tunnel Group

+	Group Name	Remote ID	Algorithm	Tunnels				
+ - ↑ ↓	Beijing	T1	Weight					
				+	Local IP	Remote IP	Weight	
				+ - ↑ ↓	2.2.2.2	1.1.1.1	1	
				+ - ↑ ↓	2.2.2.2	3.3.3.3	1	
				+ - ↑ ↓	4.4.4.4	1.1.1.1	1	
				+ - ↑ ↓	4.4.4.4	3.3.3.3	1	

表 3.93 Tunnel Routing 範例 5:Tunnel Group 設定(2)

Routing Rules

+	Source	Destination	Service	Group	Fail-Over
+ - ↑ ↓	192.168.2.1-192.168.2.10	192.168.1.1-192.168.1.10	Any	Beijing	No-Action
+ - ↑ ↓	2.2.2.22	1.1.1.11	Any	Beijing	AR

表 3.94 Tunnel Routing 範例 5:Routing Rules 設定(2)

Persistent Routs

+	Source	Destination	Service
+ - ↑ ↓	1.1.1.11	WAN	HTTP

表 3.95 Tunnel Routing 範例 5: Persistent Rules 設定

3.11 Multihoming (多重定址)

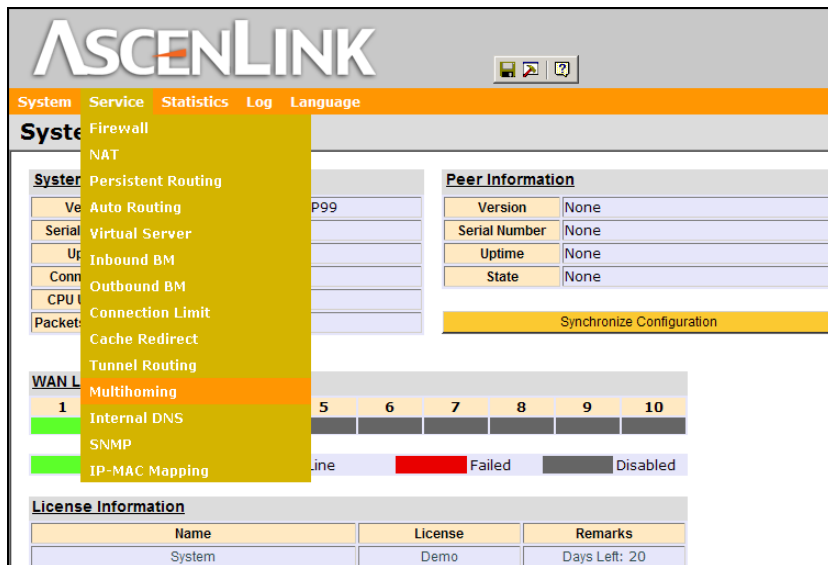


圖 3.38 Service /Multihoming 功能所處位置

Multihoming 是 AscenLink 相當重要的一項功能，特別是針對用有多條線路且對外提供網路服務的企業。對這些企業而言，如何不因為線路問題而中斷對外的服務，或是有效的利用線路頻寬，而讓對外的網路服務，可以充分利用到多條線路的資源，不會將對外的服務集中在一條線路之上。單一線路除了斷線風險之外，線路負擔過重影響對外服務品質，也是網路服務需要考慮和改善的事。

在對外的廣域網路連線正常時，對於同一個網域主機名稱，AscenLink 可以根據所設定的比重值，輪流回答相對應的 IP 位址。當某些廣域網路連線故障時，AscenLink 會避免回應屬於這些廣域網路的 IP 位址，以確保內部的伺服器對外的服務不會中斷。

所謂 Multihoming 就是對外提供服務的網域主機，對外擁有一個以上的合法位址，因此外界的用戶要求存取這部有多重定址的主機時，經由 DNS 查詢主機時，會獲得不同的 IP 位址，然後經由不同的線路存取到這台具有多重位址的主機，因此在多

線路的情況下，AscenLink 接到存取網路主機的請求時，有時是回答 WAN 第一條線的 IP，有時則回答第二條線路的 IP，回答那一條線路，可以根據線路使用比率 (By Weight) 之設定來回應；也可以透過系統自動偵測（採用 Optimum Route 演算法）線路的狀況，來選擇最佳路徑回應給外部用戶。存取者根據獲得的 IP，利用該線路建立連線。

3.11.1 在設定 Multihoming 前須有以下的準備工作

AscenLink 要能夠執行 Multihoming 這項功能，必須有適當的網路環境要求，這些條件滿足之後，Multihoming 功能才可以順利設定提供服務。

這些條件包括：

- 須有兩條或者兩條以上的對外線路。
- 須向網域名稱註冊機構（如 CNNIC）申請網域。
- 將需要做 Multihoming 的 Server 設定為 Virtual Server(虛擬主機)或讓 Server 擁有多個公開 IP 位址。

3.11.2 Multihoming 啟用設定

接下來我們開始討論如何進行 Multihoming 的各項設定。首先，勾選 [啟用多重定址] 正式啟用 Multihoming 功能。AscenLink 的 Multihoming 支援災備功能，管理員可勾選核取方塊啟用該功能，並添加相應的備援伺服器的 IP 位址。

普通模式

普通模式即不啟用 Relay，系統在本機查詢 DNS 資訊。此時頁面中有三部份的表格。第一部分為全域設定，第二部份為政策（Policy Setting），第三部份為網域設定（Domain Setting）。

■ 全域設定

The screenshot shows the 'Global Settings' window. It has a 'PTR Record' section with a 'TTL' field containing '86400'. Below this is a 'Reverse Lookup Zone' section with a 'Zone Name' field containing '.in-addr.arpa'. At the bottom is an 'Entries' table with columns for 'IP Number' and 'Host Name', and a plus icon to add new entries.

圖 3.39 Multihoming 全局設定

欄位	值	說明
TTL	<TTL>，單位：秒	DNS 記錄存活時間（Time To Live）
Zone Name （區域名稱）	<Zone Name>	填入主機所屬網段的 Zone Name，不需要填寫 “IN-ADDR.ARPR”（例如：子網段為 3.3.3.3-8，則此處應填入 0-8.3.3.3）
IP Number （IP 號碼）	<IP Number>	主機的 IP Number（例如：上述子網路中 IP 號碼為 3.3.3.3 的主機，則其 IP Number 應填入 3）
Host Name （主機名稱）	<Host Name>	DNS 所要回應的主機名稱

表 3.96 Multihoming 全域設定欄位說明表

■ Policy Setting 以及欄位說明表

Policy			Expand all		Collapse all	
	Policy Name	Algorithm	Policy Advance Setting			
	default	By Weight	Hide Details			
				WAN Link	IP Address	Weight
				1	211.21.33.186	1
				2	DynamicIP(DHCP/PPPoE)	1
				3	DynamicIP(DHCP/PPPoE)	1
	lan_to_DMZ	By Weight	Hide Details			
				WAN Link	IP Address	Weight
				1	192.168.123.254	1

圖 3.40 Multihoming Policy 設定

欄位	值	說明
Enable Multihoming	Enable (勾選) Disable (空白)	選擇啟用或停止 Multihoming 功能。
Ploicy Name (政策名稱)	<Policy Name>	給定一個名稱，作為後面規則設定之用。
Algorithm (演算法)	By Weight By Downstream By Upstream By Total Traffic By Optimum Route	By Weight，線路使用權重，如果選擇這個選項，可以輸入使用線路的權重，作為回答外界提出要求時，回應線路 IP，使用該條線路的依據。 By Downstream，依據目前線路之下載使用頻寬剩餘之多寡，回應剩餘較多頻寬之線路的 IP，外界請求的服務，將使用這條回應的線路。 By Upstream，依據目前線路之上載使用頻寬剩餘之多寡，回應剩餘較多頻寬之線路的 IP，外界請求的服務，將使用這條回應的線路。 By Total Traffic，依據目前線路之對外/對內總共使用的頻寬，比較各個線路剩餘頻寬之多寡，回應剩餘較多頻寬之線路的 IP，外界請求的服務，將使用這條回應的線路。 By Optimum Route: 依據在 “Optimum Route Detection” 中的設定，偵測出的最佳 WAN 線路，來回應外界的服務請求。
WAN Link (廣域網路連線)	<Link Number>	選擇對外線路，是預定回應外界所用到的廣域網路線路。
IP Address	<IP Address>	輸入此廣域網路線路希望回應外界請求的公開 IP 位址
Weight	權重	各個對外線路的使用權重

表 3.97 Multihoming Policy 欄位說明表

■ Domain Setting 以及欄位說明表

在此表格中輸入欲使用的 Multihoming 的主機資料，包括 Multihoming 的 Domain Name (可能不只一個網域)，原始的 DNS Server 位置，與 Multihoming 的主機的相關對應線路與權重。

Domain Settings

Domain Settings

Domain Name

abc.com

Hide Details

TTL

86400

Responsible Mail

root.abc.com

Primary Name Server

IP Address

ns1

10.13.130.1

NS Record

Name Server

IP Address

A Record

Host Name

When

Source IP

To Policy

TTL

www

All-Time

Any Address

www

30

mail

All-Time

Any Address

mail

30

CName Record

Alias

Target

TTL

DName Record

Alias

Target

TTL

MX Record

TTL

86400

Host Name

Priority

Mail Server

1

mail

TXT Record

TTL

86400

Host Name

SPF

mail

v=spf1 a:mail ip4:10.16.130.2/24 ~all

圖 3.41 Domain Setting

欄位	說明
Domain Name (網域名稱)	在此輸入要做多重定址的網域名稱，若有多個域要設定，可按+符號增列欄位。
TTL(存留時間)	設定 DNS 查詢回復時間。
Responsible Mail (負責人信箱)	設定網域名稱伺服器管理員的 E-Mail。
Primary NameServer (主要網域名稱伺服器)	輸入主要網域名稱伺服器的名稱。
IP Address(IP 位置)	輸入主要網域名稱伺服器的 IP。
NS Record	
Name Server (網域名稱伺服器)	請在這裏填入網域名稱伺服器主機的前置詞，例如某台主機的 FQDN 為 ns1.abc.com 時，請在本欄內填入 ns1。
IP Address(IP 位置)	輸入 Name Server 所對應的 IP 位置。
A Record	
Host Name(主機名稱)	輸入主機名稱的前置詞，舉例來說，如果你的主機名稱為 www.abc.com，就請在此輸入 www。
When(時段)	有三種選項 所有時段/忙時/閒時，所有時段為 24 小時都採用此規則，忙時，閒時時間設定請參照 (系統/ 忙時設定) 的設定。
Source IP (來源 IP)	設定來源 IP 位址範圍。可選項有 Any Address；IP Address；IP Range；Subnet；預設的 IP 群組等。
To Policy(使用政策)	選擇 Domain Setting 所對應的政策。
TTL	A 記錄存活時間(Time To Live)
CName Record	
Alias(別名)	在此填入網域名稱的別名。例如:你想使用 www1.abc.com 來當作 www.abc.com 的別名。就在此欄位中填入 www1。
Target(真實名稱)	在此輸入你想對應的網域名稱前置詞，例如: 你想使用 www1.abc.com 來當作 www.abc.com 的別名。就在此欄位中填入 www。
TTL	CName 記錄存活時間(Time To Live)
Dname Record	
Alias (別名)	在此填入網功能變數名稱的別名。例如:你想使用 www.a.abc.com 來當作 www.abc.com 的別名。就在此欄位中填入 a
Target(真實名稱)	在此輸入你想對應的網功能變數名稱前置詞，例如: 你想使用 www.a.abc.com 來當作 www.abc.com 的別名。就在此欄位中填入 abc.com
TTL	Dname 記錄存活時間(Time To Live)
MX Record	
TTL	MX 記錄存活時間(Time To Live)
Host Name(主機名稱)	在此填入郵件伺服器網域名稱的前置詞，例如:域名稱為 abc.com 的一個網域中，假如郵箱的尾碼為 mail.abc.com，則需要在 host name 欄位元填寫 mail；假如郵箱的尾碼為 abc.com 則 Host Name 欄位為空。
Priority(優先權)	設定郵件伺服器的優先權，數字越低代表郵件伺服器優先權

	越高。
Mail Server(郵件伺服器)	在此填入郵件伺服器在 A Record 中設置的 Host Name，例如 mail server 在 A Record 中的 Host Name 為 mail，則在此填入 mail。
TXT Record	
TTL	TXT 記錄存活時間
Host Name (主機名稱)	在此填入郵件伺服器網域名稱的前置詞，例如:域名稱為 abc.com 的一個網域中，假如郵箱的尾碼為 mail.abc.com，則需要在 host name 欄位元填寫 mail；假如郵箱的尾碼為 abc.com 則 Host Name 欄位為空。
SPF	輸入該主機的 SPF 值，用於使收件人能夠依此實施反垃圾郵件政策，例如：設定 SPF 值為 v=spf1 a: mail ip4: 10.16.130.2/24 ~all，說明這個郵件網域從 IP 位址 10.16.130.2/24 發出的郵件是正確的，從其它位址發出的郵件是垃圾郵件。

表 3.98 Multihoming 各功能選項解釋之參照表

Relay 模式

Relay 模式是指此台 AscenLink 對於所接受到的查詢請求先不做任何解析工作，而是傳遞給其內部或外部的 DNS 主機進行 Arecord MX cname 解析，然後再將解析的結果傳回本機，以達到 DNS 交換的目的。因此啓用 Relay 模式後，“全域設定”將被隱藏，同時“網域設定”變為如下形式：

The screenshot shows the 'Domain Settings' configuration page. It includes a 'Domain Name' field, a 'TTL' field set to 86400, a 'Name Servers' section with a '+', and an 'A Record' section with a table. The table has columns: Host Name, When, Source IP, To Policy, and TTL. There are also expand/collapse icons on the left and a 'Hide Details' button.

圖 3.42 Domain Setting in relay

欄位	說明
Domain Name(功能變數名稱)	在此輸入要做多重定址的功能變數名稱，若有多個域要設定，可按 + 符號增列欄位。
TTL(存留時間)	DNS 記錄存活時間 (Time To Live)
Name Servers	在此設定 AscenLink 將查詢請求傳遞過去的目的主機，可添加多個。
A Record	
Host Name (主機名稱)	輸入主機名稱的前置詞，舉例來說，如果你的主機名稱為 www.abc.com，就請在此輸入 www。
When(時段)	有三種選項 所有時段/忙時/閒時，所有時段為 24 小時都採用此規則，忙時，閒時時間設定請參照 (系統/ 忙時設定) 的設定。
Source IP (來源 IP)	設定來源 IP 地址範圍。可選項有 Any Address；IP Address；IP Range；Subnet；預設的 IP 群組等。
To Policy(使用政策)	選擇 Domain Setting 所對應的政策。
TTL	A 記錄存活時間 (Time To Live)

表 3.99 Relay 模式下網域設定說明

啓用災備功能（Enable Backup）

AscenLink 的 Multihoming 功能的 Backup 機制可以支援地域性之災難備援，在不同地點設立相同之備援服務，當主站點（Master）損壞時，備援站點（Slave）可以立即接手相同之服務。管理員在 Slave 端鈎選核取方塊啓用該功能后，畫面中出現遠端主伺服器設定表格，在[伺服器 IP]欄位添加遠端 Master 站點的 DNS 伺服器 IP 位址。備援 AscenLink 會定期發送檢測資料封包來判斷所添加的 Master 的 DNS Server 介面狀態，當 Master 工作正常時，備援 AscenLink 保持休眠狀態（non-active），當檢測到 Master 工作不正常時，備援 AscenLink 變為 active 狀態，接管 Master 的工作，為客戶提供 DNS 解析等 Master 站點提供的服務，以此實現災備功能。備援 AscenLink 在接管 Master 工作后，還會繼續監測 Master 介面，一旦發現 Master 恢復正常，立即交回所接管之服務，返回休眠狀態成為備援。

Service/Multihoming

Enable Multihoming

Enable Backup

Remote Master Servers

Server IP

10.13.0.3

圖 3.43 啓用災備功能

組態檔案（Configuration File）

該功能用以導入、導出本頁的設定記錄，設定檔以 ini 格式保存。

註：只有 Administrator 有本功能的使用許可權。

範例一

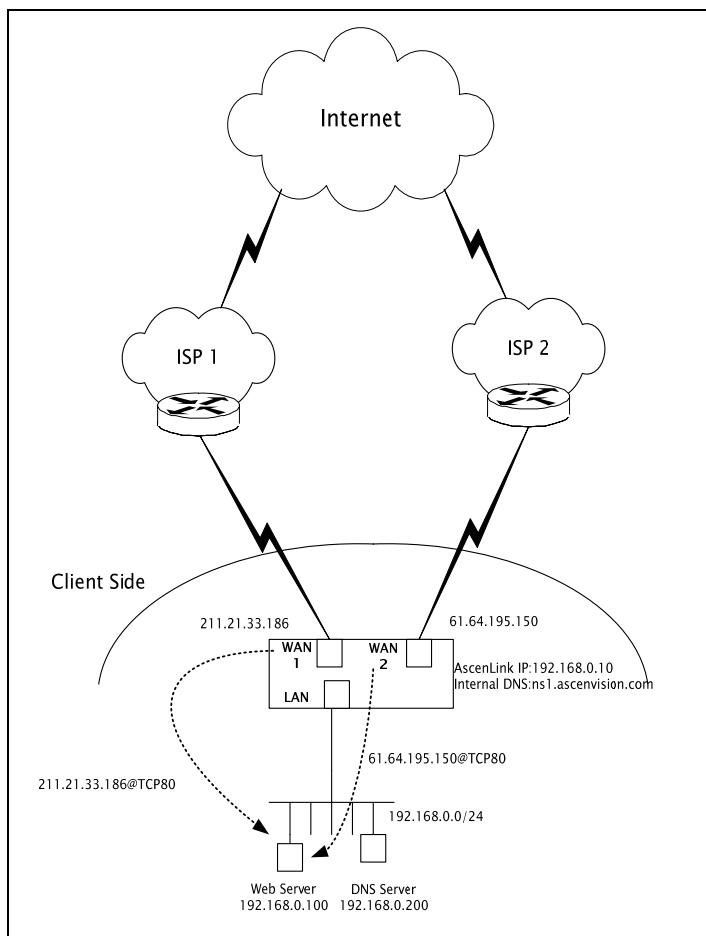


圖 3.44 Multihoming 範例 (1) 架構示意圖

在內部網路中設定一台 Web Server，並對外提供服務，這台 Web Server 須先用 Virtual Server (虛擬主機) 方式，在 AscenLink Virtual Server 這項功能下加以設定。

Virtual Server，其設定如下（有關 Virtual Server 的設定請參考本章，Virtual Server 一節）。

WAN IP	Server IP	Service
211.21.33.186	192.168.0.100	HTTP (80)
61.64.195.150	192.168.0.100	HTTP (80)

表 3.100 Multihoming 範例 1 Virtual Server 設定

使用兩個 WAN Port，有關 WAN Port 的設定，也請參考第二章 [System]→[WAN Setting] 這一節。

▫ Policy Setting

欄位		值
Enable Multihoming		Enable (打勾)
Policy Name		web
Algorithm		By Up Stream
Policy Advance Setting	WAN Link	1
	IP Address	211.21.33.186
	WAN Link	2
	IP Address	61.64.195.150

表 3.101 Multihoming 範例 1 Policy 設定

▫ Domain Setting

欄位	值
Domain Name(網域名稱)	Xtera.com
TTL(存留時間)	30
Responsible Mail(負責人信箱)	Abc.xtera.com
Primary NameServer(主要網域名稱伺服器)	ns1.xtera.com
IP Address(IP 位置)	192.168.0.10
NS Record	
Name Server(網域名稱伺服器)	ns1
IP Address(IP 位置)	192.168.0.10
A Record	
Host Name(主機名稱)	www
When(時段)	ALL-Time
Source IP (來源 IP)	192.168.0.100
To Policy(使用政策)	www
TTL(存留時間)	30

表 3.102 Multihoming 範例 1 Domain 設定

範例二

應用 Optimum Route 演算法，解決電信與網通互訪速度過慢問題。

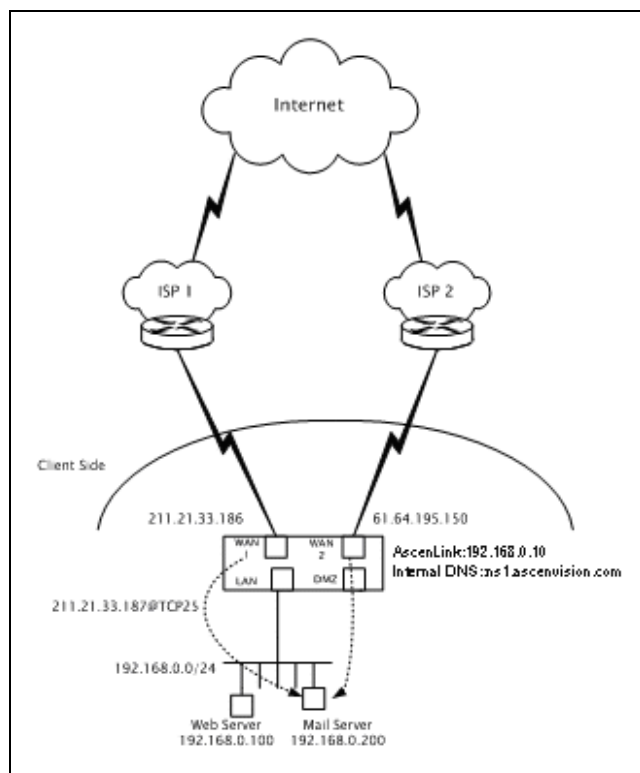


圖 3.45 Multihoming 範例 (2) 架構示意圖

在設定 Multihoming 前須先設定 Virtual Server，其設定如下：

WAN IP	Server IP	Service
211.21.33.186	192.168.0.200	SMTP(25)
61.64.195.150	192.168.0.200	SMTP(25)
211.21.33.186	192.168.0.100	HTTP(80)
61.64.195.150	192.168.0.100	HTTP(80)

表 3.103 Multihoming 範例 2 Virtual Server 設定

▫ Policy Setting

欄位		值
Enable Multihoming		Enable (打勾)
Policy Name		multihome_smtp
Algorithm		By Optimum Route
Policy Advance Setting	WAN Link	1
	IP Address	211.21.33.186
	WAN Link	2
	IP Address	61.64.195.150

表 3.104 Multihoming 範例 2 Policy 設定

▫ Domain Setting

欄位	值
Domain Name (網域名稱)	xtera.com
TTL(存留時間)	30
Responsible Mail (負責人信箱)	Abc.xtera.com
Primary NameServer (主要網域名稱伺服器)	ns1.xtera.com
IP Address(IP 位址)	192.168.0.10
NS Record	
Name Server (網域名稱伺服器)	ns1
IP Address(IP 位址)	192.168.0.10
A Record	
Host Name (主機名稱)	mail
When(時段)	ALL-Time
Source IP (來源 IP)	192.168.0.200
TTL (存留時間)	30

To Policy (使用政策)	multihome_smtp
MX Record	
TTL (存留時間)	30
Host Name (主機名稱)	mail
Priority(優先權)	1
Mail Server (郵件伺服器)	mail
TXT Record	
TTL	30
Host Name (主機名稱)	
SPF	v=spf1 ip4: 211.21.33.186 ip4: 61. 64. 195.150 ~all

表 3.105 Multihoming 範例 2 Domain 設定

註：這個範例中的 WAN 設定兩個 Public IP，您必須在 [System]→[Network setting]→[Wan Setting] 中設定，請參考第二章。這個範例是設定 mail.xtera.com 的 Multihoming。

3.12 Internal DNS (內建 DNS)

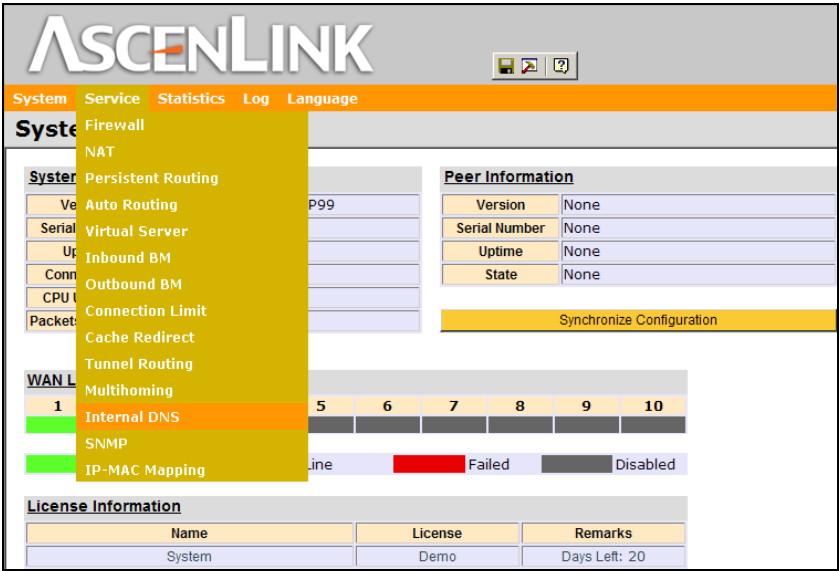


圖 3.46 Service / Internal DNS 功能所處位置

AscenLink 已內建 DNS Server 功能，使用者只需要在此頁面設定相關參數，就能利用 AscenLink 作為 DNS 伺服器，而不需另外再建置額外的 DNS 伺服器。

■ Global Setting

欄位	值
Enable InternalDNS(啓用內建 DNS)	開啓/關閉內建 DNS 伺服器
PTR Record	
TTL(存留時間)	設定 DNS 查詢回復時間
IP Address(IP 位置)	在此欄位填入可供反查的 IP 位址
Host Name(主機名稱)	在此輸入 IP 反查時 IP 所對應的 FQDN

表 3.106 Global Setting 各功能選項解釋之參照表

■ Domain Settings

欄位	值
Domain Name(網域名稱)	在此輸入網域名稱
TTL(存留時間)	設定 DNS 查詢回復時間
Responsible Mail(負責人信箱)	設定網域網域名稱伺服器管理員的 E-Mail
Primary NameServer (主要網域名稱伺服器)	輸入主要網域名稱伺服器的名稱。
IP Address(IP 位置)	輸入主要網域名稱伺服器的 IP
NS Record	
Name Server (網域名稱伺服器)	請在這裏填入網域名稱伺服器主機的前置詞，例如某台主機的 FQDN 爲 ns1.abc.com 時，請在本欄內填入 ns1。
IP Address(IP 位置)	輸入 Name Server 所對應的 IP 位置
A Record	
Host Name(主機名稱)	輸入主機名稱的前置詞，舉例來說，如果你的主機名稱爲 www.abc.com，就請在此輸入 www
IP Address(IP 位置)	主機的 IP 位置
CName Record	
Alias(別名)	在此填入網域名稱的別名。例如：你想使用 www1.abc.com 來當作 www.abc.com 的別名。就在此欄位中填入 www1。
Target(真實名稱)	在此輸入你想對應的網域名稱前置詞，例如：你想使用 www1.abc.com 來當作 www.abc.com 的別名。就在此欄位中填入 www。
MX Record	
Host Name(主機名稱)	在此填入郵件伺服器網域名稱的前置詞，例如：域名稱爲 abc.com 的一個網域中，假如郵箱的尾碼爲 mail.abc.com，則需要在 host name 欄位元填寫 mail；假如郵箱的尾碼爲 abc.com 則 Host Name 欄位爲空。
Priority(優先權)	設定郵件伺服器的優先權，數字越低代表郵件伺服器優先權越高。
Mail Server(郵件伺服器)	在此填入郵件伺服器在 A Record 中設置的 Host Name，例如 mail server 在 A Record 中的 Host Name 爲 mail，則在此填入 mail。

表 3.107 Domain Setting 各功能選項解釋之參照表

3.13 SNMP (簡單網路管理)

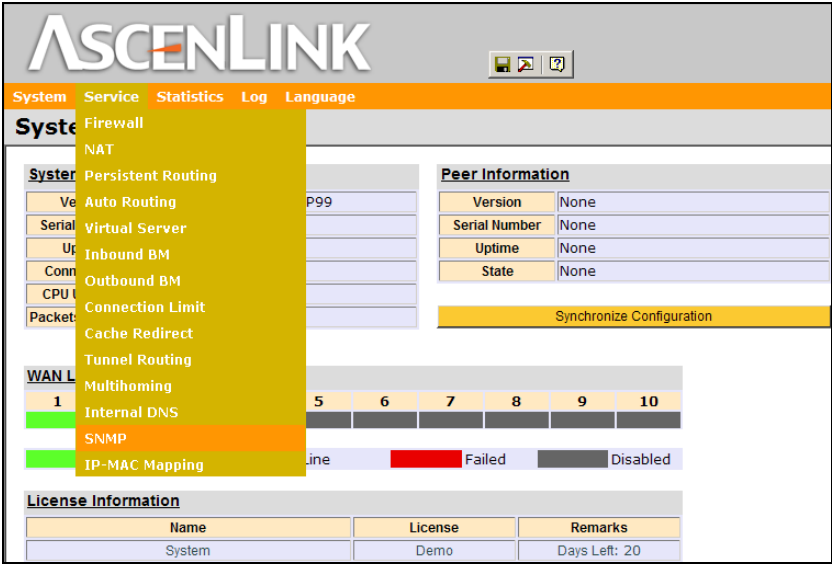


圖 3.47 Service / Tunnel Routing 功能所處位置

SNMP 簡單網路通訊協定為提供監控網路設備的一種工具，可以管理設定，統計資料收集效能及安全。通常用在 TCP/IP 網路的網路管理通訊協定。AscenLink 支持 SNMP v1，SNMPv2，SNMPv3 的通訊協定。

SNMP v1/2

欄位	值	說明
Community (來源)		在此填入 SNMP 所屬的 Community。
System Name (系統名稱)		根據管理策略,填入系統的名稱,管理員可以任意定義,如 AVT
System Contact (系統負責人)		根據管理策略,填入系統的負責人,管理員可以任意定義,如 jackie
System Location (系統位址)		根據管理策略,填入系統所處的位址,管理員可以任意定義,如 Beijing

表 3.108 SNMP v1/2 各功能選項解釋之參照表

SNMP v3

欄位	值	說明
Community		在此填入 SNMP 所屬的 Community。
System Name (系統名稱)		根據管理策略,填入系統的名稱,管理員可以任意定義,如 AVT
System Contact (系統負責人)		根據管理策略,填入系統的負責人,管理員可以任意定義,如 jackie
System Location (系統位址)		根據管理策略,填入系統所處的位址,管理員可以任意定義,如：三樓會議室
Username (使用者名稱)		在此填入認證所使用的使用者名稱。
Password(密碼)		在此填入認證所使用的使用者密碼。
Privacy Key (私密金鑰)		在此填入供私密金鑰產生編碼的字串,如:1234, ABCD....等。
AuthProtocol (認證協定)	MD5 SHA	選擇認證時傳送的加密編碼方式,有 MD5 及 SHA 兩種。
PrivProtocol (私密協定)	DES	選擇私密金鑰的加密編碼方式。
Authentication (認證方式)	Auth No Priv (只使用認證) Auth with Priv (認證和私密)	選擇你想使用何種認證方式,可以使用認證和私密金鑰,也可以只使用認證方式。

表 3.109 SNMP v3 各功能選項解釋之參照表

3.14 IP-MAC Mapping (IP-MAC 對應)

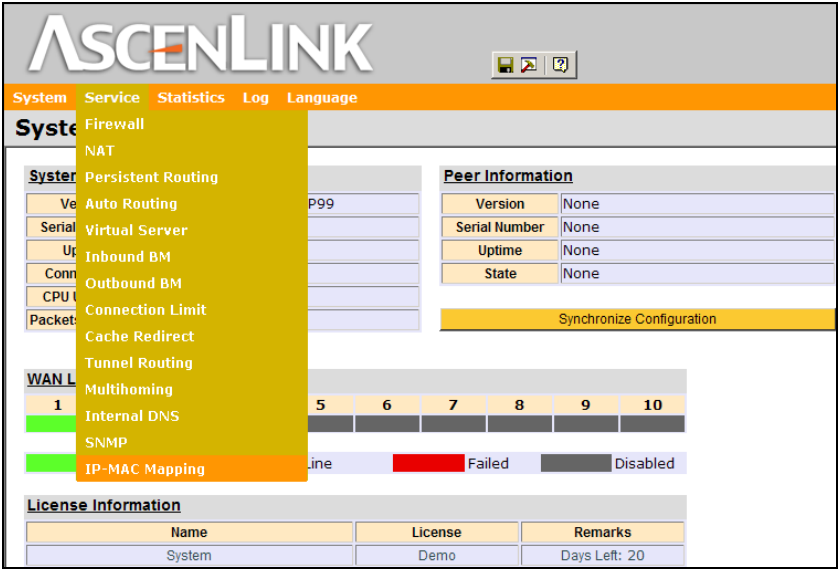


圖 3.48 Service / IP-MAC MAPPING 功能所處位置

使用者可以依據時段來設定 IP-MAC 的對應表。當設定了 IP-MAC 對應表後，某一個 IP 位址所傳送的網路封包，只有當此封包的 MAC 與設定值相同時，才允許透過 AscenLink。

欄位	值	說明
E		啟動/關閉
When (時段)	Busy (尖峰時段) Idle (離峰時段) All-Time (所有時段)	有三種選項，尖峰時段、離峰時段及所有時段。所有時段為 24 小時都採用此規則，Busy, Idle 時間設定請參照第二章 [System]→[Virtual Server] 的設定。
IP Address		填入網路卡所對應的 IP 位址
MAC Address		填入網路卡所對應的 MAC 位址
L (記錄)	Enable Disable	當這個 Check Box 打勾，表示當此條規則有被引用到時，其結果會記錄到 log 中，空白時則沒有任何記錄產生。

表 3.110 IP-MAC MAPPING 各功能選項解釋之參照表

目錄

第四章 Statistics (統計) 功能表	4-4
4.1 Traffic (短期流量)	4-5
4.2 BM (頻寬管理).....	4-7
4.3 Persistent Routing (持續路由)	4-8
4.4 WAN Link Health Detection (廣域網路連線狀態偵測)	4-10
4.5 Dymatic IP WAN Link (動態 IP 廣域網路)	4-12
4.6 DHCP lease info	4-14
4.7 RIP&OSPF Status (RIP&OSPF 狀態資訊)	4-16
4.8 Tunnel Status (通道狀態)	4-18
4.9 Tunnel Traffic (通道流量)	4-20
4.10 Connection Limit (連線限制)	4-21
4.11 Virtual Server Status (虛擬伺服器狀態)	4-22

圖目錄

圖 4.1 Statistic 功能圖 4-4

圖 4.2 Statistics/Traffic 功能所處位置..... 4-5

圖 4.3 Statistics/BM 功能所處位置 4-7

圖 4.4 Statistics/Persistent Routing 功能所處位 4-8

圖 4.5 Statistics/WAN Link Health Detection 功能所處位置..... 4-10

圖 4.6 Statistics/Dynamic IP WAN Link 功能所處位..... 4-12

圖 4.7 Statistics/DHCP lease info 功能所處位 4-14

圖 4.8 Statistics/RIP&OSPF Status 功能所處位置 4-16

圖 4.9 Statistics/Tunnel Status 功能所處位置 4-18

圖 4.10 Tunnel Traffic 功能所處位置 4-20

圖 4.11 Statistics/Connection Limit 功能所處位置 4-21

圖 4.12 Virtual Server Status 功能所處位置..... 4-22

表目錄

表 4.1	短期流量統計表中各項資料解釋	4-6
表 4.2	BM 統計表中各項資料之解釋.....	4-7
表 4.3	Persistent Routing 各項資料之解釋.....	4-9
表 4.4	WAN Link Health Detection 各項資料之解釋.....	4-11
表 4.5	Dynamic IP WAN Link 各項資料之解釋	4-13
表 4.6	DHCP lease info 各項資料之解釋.....	4-15
表 4.7	RIP&OSPF Status 各項資料之解釋	4-17
表 4.8	Tunnel Status 各項資料之解釋.....	4-19
表 4.9	Tunnel Traffic 各項資訊的解釋.....	4-20
表 4.10	Connection Limit 各項資料之解釋.....	4-21
表 4.11	Virtual Server Status 各項功能之解釋.....	4-22

第四章 Statistics (統計) 功能表

在這一章中，您將學會如何透過 AscenLink 所提供的統計功能，對網路狀態、各類資訊流量、頻寬及動態位址等內容進行即時的偵測。透過統計後所呈現的資訊，可以讓管理者百分之百地掌握網路連線狀況，當線路發生非預期狀況時，這些統計資料也能即時反應出連線問題的癥結點，節省很多問題摸索的時間。

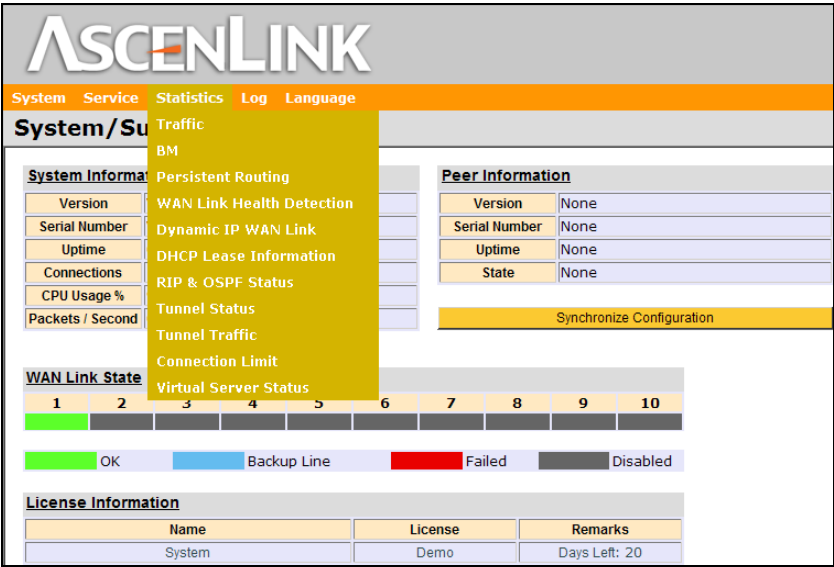


圖 4.1 Statistic 功能圖

4.1 Traffic (短期流量)

在這個分頁裏面，我們可以察看每一條廣域網路連線上各個頻寬資訊類型的即時流量統計。在統計列表當中，AscenLink 會依據您的設定，分成不同的對內或對外 Traffic Class（資訊類型）進行流量偵測統計。

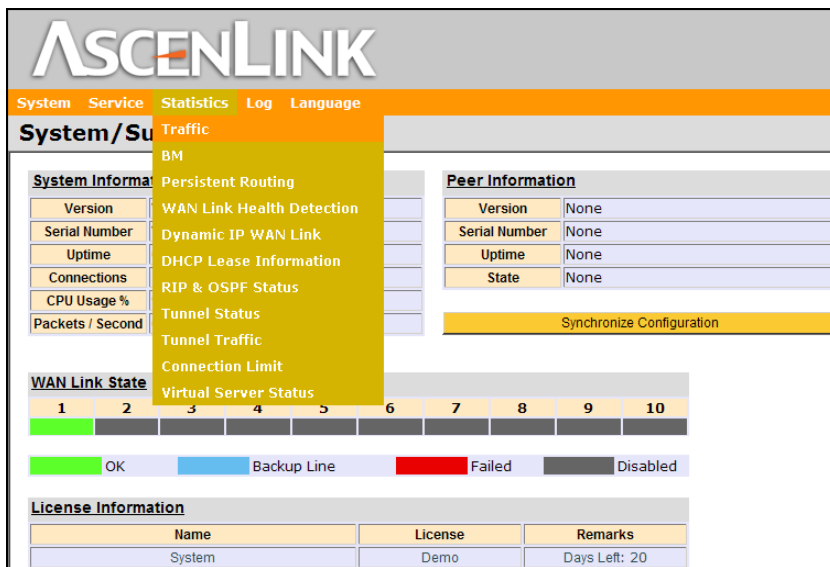


圖 4.2 Statistics/Traffic 功能所處位置

頁面中共顯示三種流量偵測方式：

- 最大與最小頻寬分配比率與優先順序（Priority）。
- 最近三秒鐘。
- 最近一分鐘的流量統計資料等。

在這裏的流量統計資料是依照各廣域網路連線與網路流向的不同分開計算的。所以您可以從廣域網路（WAN Link）列表中，選擇要察看那一條廣域網路連線，以及從 Traffic Type（網路流向）列表當中選擇要查看 Inbound 或 Outbound 的短期流量統計。

欄位	值	說明
Traffic Type (網路流向)	Inbound (對內) Outbound (對外)	此欄位可選擇欲查看的流量狀況，可選擇對外流量或對內流量來查看。
WAN Link (廣域網路)	<WAN Link #>	此欄位可選擇欲查看的廣域網路連線。
Automatic Refresh (自動更新)	Every 3 Seconds Every 6 Seconds ...	此欄位可選擇自動更新圖表的時間間隔。
Traffic Class (資訊類型)	<Class Name>	依照先前定義在 Inbound/ Outbound BM 的資訊類型作查看，其餘未被分類的資訊皆放在 Default Class。
Min. ~ Max.(Priority) (最小~最大優先順序)	Kbps ~ Kbps	此欄位顯示所選定的資訊類型定義的最大最小流量及此類型的優先順序。
3-Second Statistics (三秒鐘統計資料)	Packets, Kbps (封包數)	此欄位顯示每三秒鐘累積統計資訊，包括三秒鐘內累積的封包數與累積流量。
1-Minute Statistics (一分鐘統計資料)	Packets, Kbps (封包數)	此欄位顯示資料如上，所不同的是以一分鐘為單位所累積的封包數與流量。
Top 10		點選[Show]按鈕後，會即時統計 5 秒鐘內的流量與相對應的 IP 位址，以四種方式：By connections, By Source, By Destination 和 By Service 顯現前十名流量的資料。

表 4.1 短期流量統計表中各項資料解釋

4.2 BM (頻寬管理)

上一個管理頁面中，所獲得的是即時流量統計，可供管理者做即時的網路偵測。而在 BM 管理頁面中，可讓管理者做長期的流量統計分析，透過察看各個頻寬資訊類型在各個廣域網路連線中，上傳和下載的流量統計長條圖。您可以依序察看過去一小時、一天、一個月、以及一年內的統計結果。

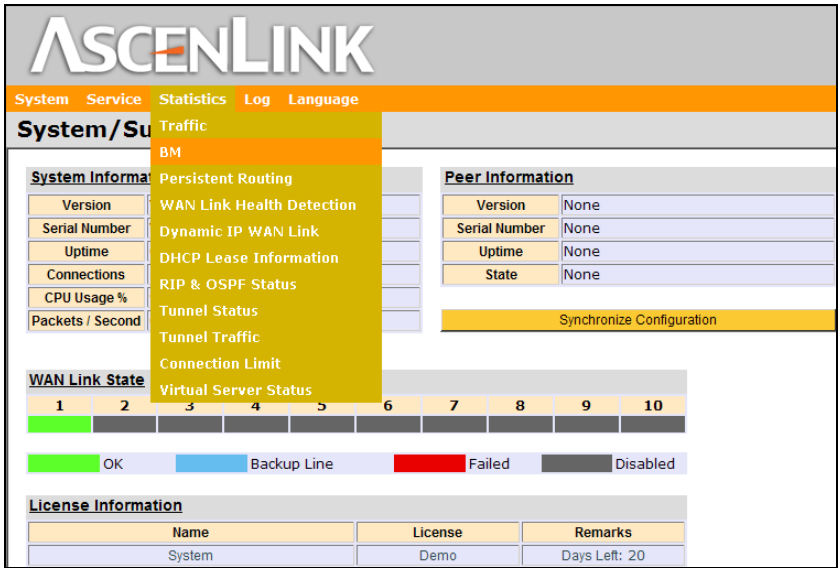


圖 4.3 Statistics/BM 功能所處位置

欄位	值	說明
Traffic Type (網路流向)	Inbound (對內) Outbound (對外)	此欄位可選擇欲查看的流量狀況，可選擇對外流量或對內流量來查看。
Traffic Class (資訊類型)	<Class Name>	此欄位可選擇先前定義在 Inbound/Outbound BM 的資訊類型作查看或選擇所有的資訊類型總合。
WAN Link (廣域網路連線)	<WAN Link #>	此欄位可選擇欲查看的廣域網路連線或所有廣域網路連線資料的總合。

表 4.2 BM 統計表中各項資料之解釋

4.3 Persistent Routing (持續路由)

此分頁中可查看目前已有的持續路由資料及狀態，並可手動清除目前已存在的持續路由連線。

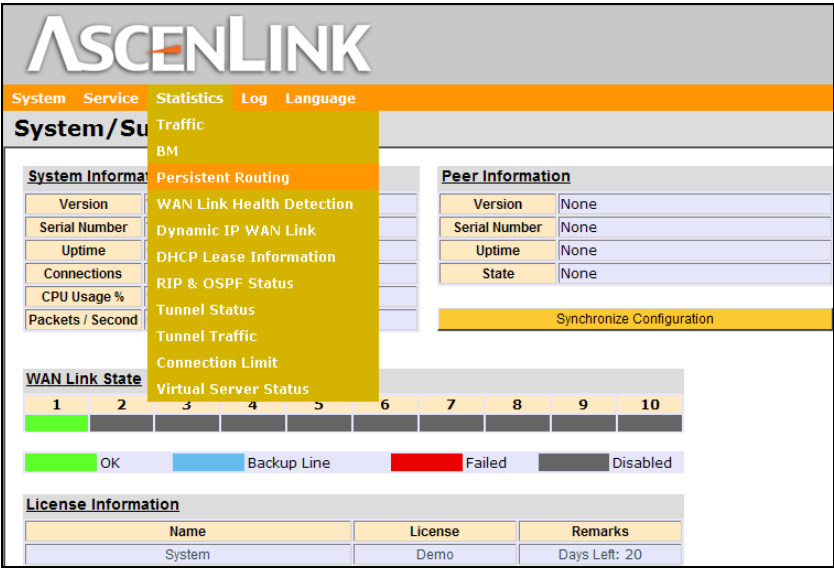


圖 4.4 Statistics/Persistent Routing 功能所處位

欄位	值	說明
Clear All (全部清除)	-	清除所有目前的 Persistent Routing 資料。
Automatic Refresh (自動更新)	Every 3 Seconds Every 6 Seconds	依據所選擇的時間間隔自動更新下方的表格資料。
根據 IP 位址	顯示當前 IP Pair 持續路由連線數量	
Source IP (來源 IP 位址)	-	目前使用中的 Persistent Routing 的 Source IP。
Destination IP (目標 IP 位址)	-	目前使用中的 Persistent Routing 的 Destination IP。
Count (連線數)	-	目前此條 Persistent Routing 規則的使用次數。
Timeout (超時)	-	目前此條 Persistent Routing 規則尚能存活多久，超時後會自動清除此條 Persistent Routing。
WAN (廣域網路)	-	目前此條 Persistent Routing 所使用的廣域網路連線。
根據 Web 服務	顯示當前 Web 服務持續路由連線數量	
Source IP (來源 IP 位址)		目前使用中的 Persistent Routing 的 Source IP。
Count (連線數)		目前此條 Persistent Routing 規則的使用次數。
Timeout (超時)		目前此條 Persistent Routing 規則尚能存活多久，超時後會自動清除此條 Persistent Routing。
WAN (廣域網路)	-	目前此條 Persistent Routing 所使用的廣域網路連線。

表 4.3 Persistent Routing 各項資料之解釋

4.4 WAN Link Health Detection (廣域網路連線狀態偵測)

此管理頁面顯示廣域網路連線狀態偵測的統計資料，這些資料可用來調整 [System] → [WAN Link Health Detection] 中的參數。對此頁面中「Ping 清單」裏列出的 IP 位址，這裏提供「Number of Requests」（偵測次數）、「Number of Replies」（回應次數）、與「Success Ratio」（成功率）統計，幫助您更瞭解廣域網路連線狀態。

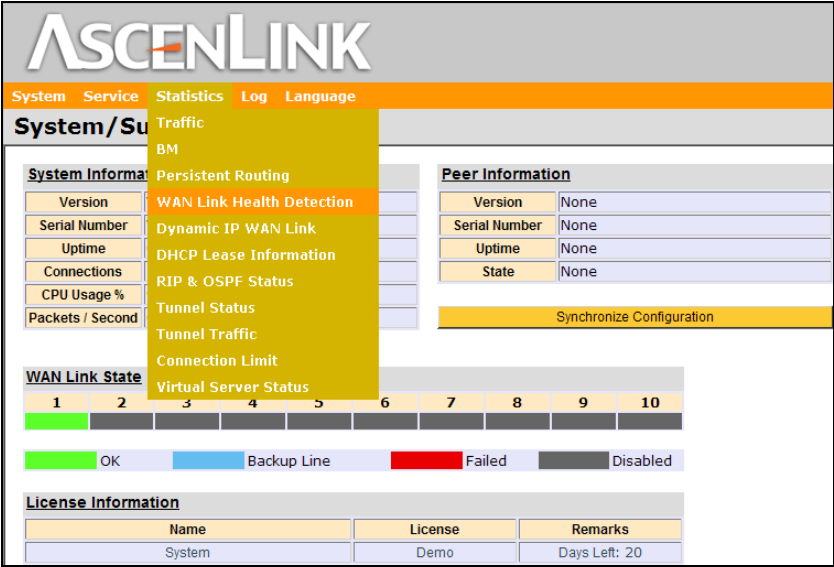


圖 4.5 Statistics/WAN Link Health Detection 功能所處位置

欄位	值	說明
WAN Link (廣域網路)	<WAN Link #>	此欄位可選擇欲查看的廣域網路的連線狀況。
Automatic Refresh (自動更新)	Every 3 Seconds Every 6 Seconds ...	依據所選擇的時間間隔自動重整下方的表格。
Destination IP (目標 IP 位址)	-	所用來檢查連線狀況的目標 IP 位址。
Number of Requests (偵測次數)	-	目前累積對目的位址送出的 ICMP 封包數。
Number of Replies (回應次數)	-	此條廣域網路連線上目的位址收到的 ICMP 響應封包數。
Success Ratio (%) (成功率)	-	以 Reply 數除以 Request 數所得的值越高表示此廣域網路連線的狀態越穩定。

表 4.4 WAN Link Health Detection 各項資料之解釋

4.5 Dymatic IP WAN Link (動態 IP 廣域網路)

此管理頁面顯示目前以動態方式 (PPPoE 或 DHCP) 取得 IP 位址的廣域網路連線之相關資訊。管理者亦可以手動方式重新連線廣域網路 IP 位址。

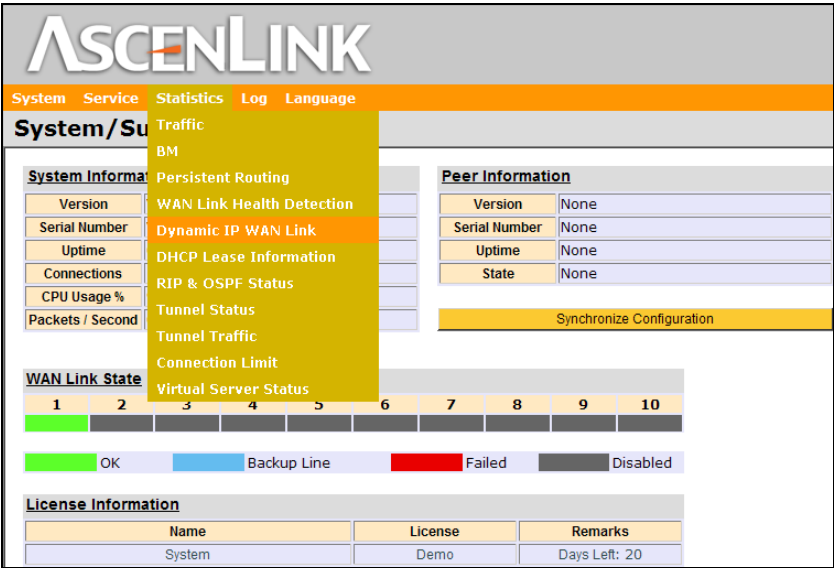


圖 4.6 Statistics/Dynamic IP WAN Link 功能所處位

欄位	值	說明
WAN (連線模式)	-	此欄位顯示使用動態位址廣域網路連線的 WAN 介面，括弧內部顯示的是連線的方式，有可能是 PPPoE 或 DHCP 兩種中的一種。
Automatic Refresh (自動更新)	Disabled Every 10 Seconds Every 30 Seconds ...	依據所選擇的時間間隔自動重整下方的表格。
IP Address (IP 位址)	-	此欄位顯示的是取得的動態 IP 位址，即為目前此廣域網路介面所設定的 IP。
Gateway (閘道位址)	-	此欄位顯示的是此廣域網路連線的閘道位址。
Netmask (子網路遮罩)	-	網路遮罩。
Reconnect (重新連線)	-	點選此按鈕可以重新連線此廣域介面。
Re-Connect All (全部重新連線)	-	點選此選項以重新連線所有使用動態位址的廣域網路介面。

表 4.5 Dymatic IP WAN Link 各項資料之解釋

4.6 DHCP lease info

此項管理頁面顯示 DHCP 伺服器所分配 IP 對應的 MAC 位址，用戶端主機名稱和所設定 IP 之有效期限。對於在此頁面中「DHCP Server」(DHCP 伺服器)會列出目前網域內 DHCP 伺服器的列表。「Automatic Refresh」(自動更新)選項則可設定列表更新的時間。

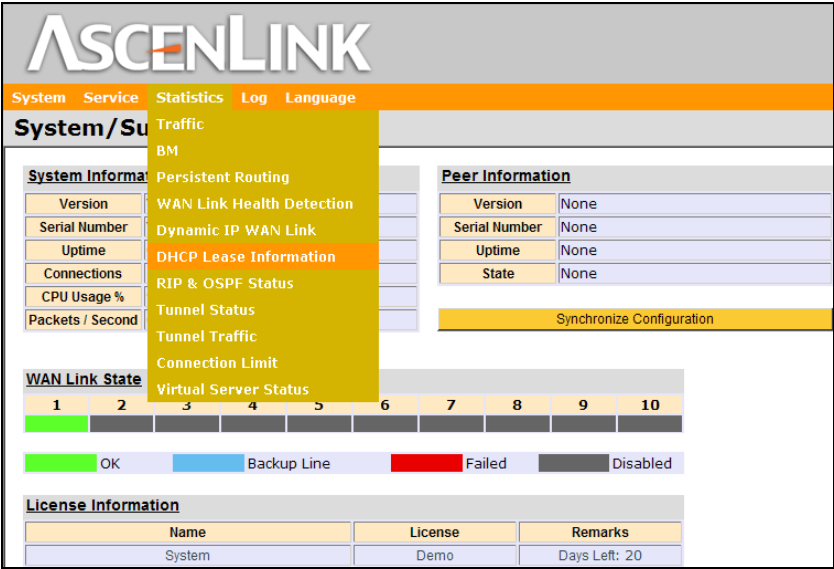


圖 4.7 Statistics/DHCP lease info 功能所處位

欄位	值	說明
DHCP Server (DHCP 伺服器)	-	此欄位顯示 DHCP 伺服器與可設定的 IP 區間。
Automatic Refresh (自動更新)	Disabled Every 10 Seconds Every 30 Seconds ...	依據所選擇的時間間隔自動重整下方的表格。
Lease IP (設定 IP 位址)	-	此欄位顯示的是已設定給用戶端主機 IP 位址。
MAC Address (MAC 位址)	-	此欄位顯示的是用戶端主機的 MAC 位址。
Client-Hostname (主機名稱)	-	此欄位顯示的是用戶端主機的主機名稱。
Expire Time (結束時間)	-	此欄位顯示的是所設定 IP 的有效期限。

表 4.6 DHCP lease info 各項資料之解釋

4.7 RIP&OSPF Status (RIP&OSPF 狀態資訊)

此項管理頁面可以顯示[WAN Setting] (網路設定) → [LAN Private] (私有子網路) → [RIP&OSPF]中得到的路由情況。管理者可以查看相應的私有子網路相應的「Network IP」 (網路位址), 「Netmask」 (子網路遮罩), 「Gateway」 (閘道) 等信息。「Automatic Refresh」 (自動更新) 選項則可設定列表更新的時間。

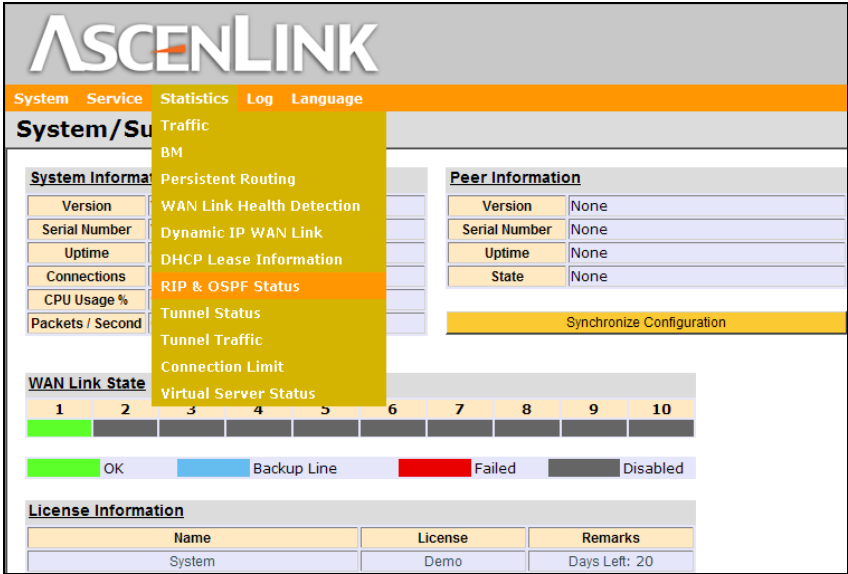


圖 4.8 Statistics/RIP&OSPF Status 功能所處位置

欄位	值	說明
Type (類型)	RIP OSPF	透過下拉選框，選擇查看 RIP&OSPF 路由情況
Automatic Refresh (自動更新)	Disabled Every 10 Seconds Every 30 Seconds ...	依據所選擇的時間間隔自動重整下方的表格。
Network IP (網路位址)	-	此欄位顯示看相應的私有子網路的"網路號"。
Netmask (子網路遮罩)	-	此欄位顯示網路位址的子網路遮罩。
Gateway (閘道)	-	此欄位顯示相應的網路位址的閘道。

表 4.7 RIP&OSPF Status 各項資料之解釋

4.8 Tunnel Status (通道狀態)

此項管理頁面可以顯示[Service]（服務）→[Tunnel Routing]（通道路由）中設置的通道路由情況。管理者可以查看通道路由的線路狀態，速度等資訊。「Automatic Refresh」（自動更新）選項則可設定列表更新的時間。

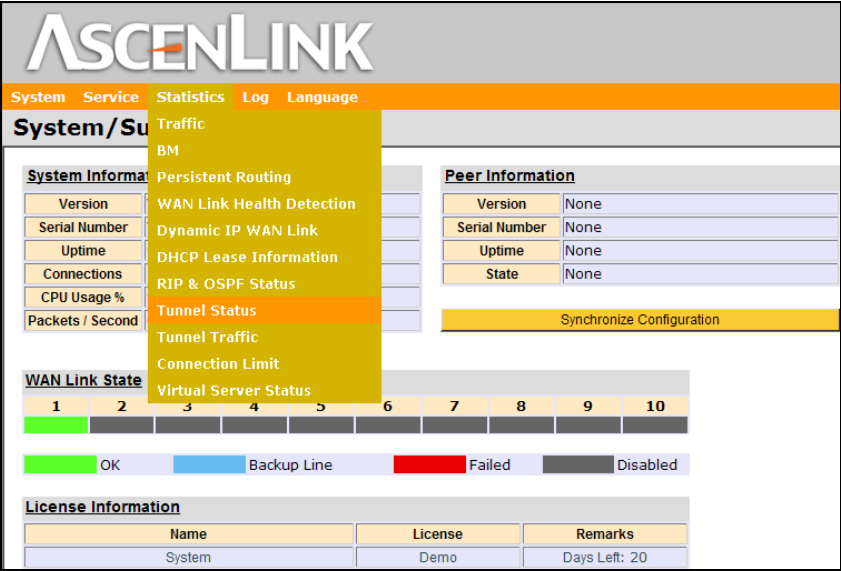


圖 4.9 Statistics/Tunnel Status 功能所處位置

欄位	值	說明
Tunnel Group (通道群組)	-	選擇欲查看的工作群組
Automatic Refresh (自動更新)	Disabled Every 10 Seconds Every 30 Second...	依據所選擇的時間間隔自動重整下方的表格。
通道狀態		 表示目前通道狀況正常  表示目前此條通道線路失敗
通道	-	顯示改群組下的所有通道數目。
三秒鐘統計資料	Kbps	此欄位元顯示每三秒鐘累積統計資訊，包括三秒鐘內累積的封包數與累積流量。
一分鐘統計資料	Kbps	此欄位元顯示資料如上，所不同的是以一分鐘為單位所累積的封包數與流量
狀態	-	此欄位元顯示通道的當前狀態

表 4.8 Tunnel Status 各項資料之解釋

4.9 Tunnel Traffic（通道流量）

此頁面可查看各個通道路由上，不同網路流向產生的流量統計曲線圖，管理員可以分別查看每 60 分鐘/24 小時/30 天內的統計結果。

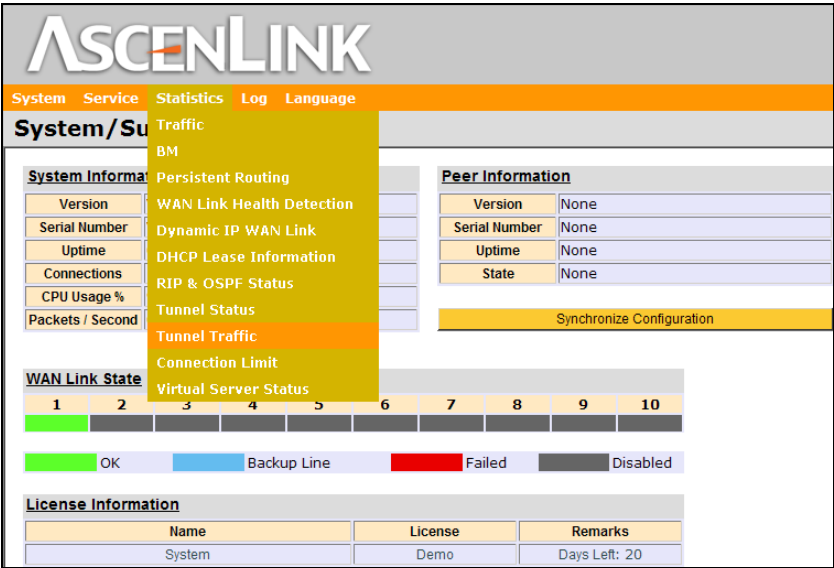


圖 4.10 Tunnel Traffic 功能所處位置

欄位	值	說明
Traffic Type（流量類型）	Outbound Inbound	此欄位可選擇欲查看的流量狀況，可選擇對外流量或對內流量來查看
Time（時間）	60 Mins 24 Hours 30 Days	此欄位可選擇要查看的時間範圍
Tunnel Routing Group（通道群組）	<Group Name>	此欄位可選擇要查看的通道群組，在一個群組中若有 N 條通道路由，則下面將顯示 N 個圖表分別統計每條通道的流量狀況

表 4.9 Tunnel Traffic 各項資訊的解釋

4.10 Connection Limit（連線限制）

此頁面對每一個透過 AscenLink 的 IP 位址的連線數目的前 50 位元統計資料，這些資料可以用來調整 “Service/Connection Limit”（服務/連線限制）中的參數。

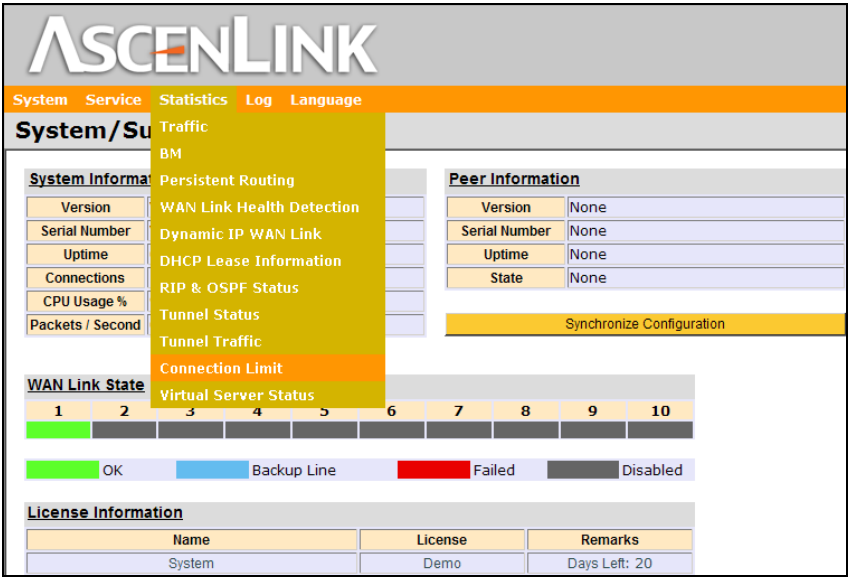


圖 4.11 Statistics/Connection Limit 功能所處位置

欄位	值	說明
自動更新	Disabled Every 10 Seconds Every 30 Second...	依據所選擇的時間間隔自動刷新下方表格
No.	1,2,3...	根據連線數的多少進行排名。
IP	<IP Address>	顯示連線的源 IP 地址。
連線數	1,2,3...	顯示當前每一個 IP 的連線數量。

表 4.10 Connection Limit 各項資料之解釋

4.11 Virtual Server Status（虛擬伺服器狀態）

此頁面顯示出虛擬伺服器狀態檢測的統計資料，這些資料顯示在“服務/虛擬主機”中各個虛擬主機的工作狀態。

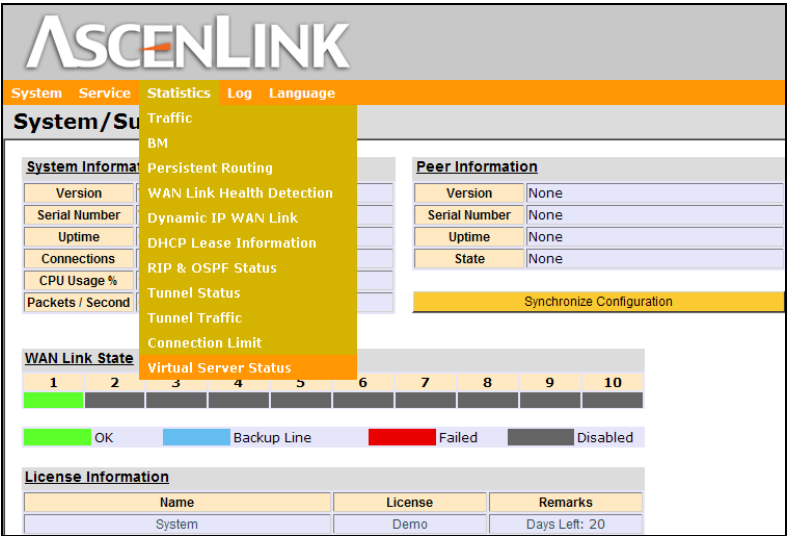


圖 4.12 Virtual Server Status 功能所處位置

欄位	值	說明
Automatic Refresh (自動更新)	Disabled Every 10 Seconds Every 30 Second...	依據所選擇的時間間隔自動重整下方的表格。
虛擬主機狀態	OK Failed	<div></div> 表示目前該虛擬主機狀態為正常 <div></div> 表示目前該虛擬主機狀態為失敗
WAN IP 地址	<IP Address>	顯示“服務/虛擬主機”頁面所設定的 WAN IP 位址
Service（服務）	<Service Name>	顯示“服務/虛擬主機”頁面所設定的該虛擬主機提供的服務
Server IP（伺服器 IP 地址）	<IP Address>	顯示“服務/虛擬主機”頁面所設定的真實伺服器位址

表 4.11 Virtual Server Status 各項功能之解釋

目錄

第五章 Log (記錄) 功能表	5-4
5.1 View (記錄流覽)	5-5
5.2 Control (傳輸設定)	5-7
5.3 Notification (重要通知)	5-10
5.4 LinkReport	5-13

圖目錄

圖 5.1 Log 功能圖..... 5-4

圖 5.2 Log/View 功能所處位置..... 5-5

圖 5.3 Log/Control 功能所處位置..... 5-7

圖 5.4 log/Notification 功能所處位置..... 5-10

圖 5.5 Notification 功能設定.....5-11

圖 5.6 Log/LinkReport 功能所處位置..... 5-13

圖 5.7 LinkReport 欄位..... 5-14

表目錄

表 5.1	Log/View 各功能選項解釋之參照表	5-6
表 5.2	Log/Control 各功能選項解釋之參照	5-8
表 5.3	傳輸方式:電子郵件欄位說明	5-9
表 5.4	傳輸方:FTP 式欄位說明	5-9
表 5.5	Notification 各功能	5-12
表 5.6	SNMP Trap Setting 欄位說明.....	5-12
表 5.7	Event Types to Notify 欄位說明	5-12
表 5.8	LinkReport 欄位說明	5-14
表 5.9	記錄種類欄位說明	5-14

第五章 Log (記錄) 功能表

在這個功能選項中，主要呈現的是 AscenLink 運作時所產生的 Log 記錄種類，例如：系統、防火牆、路由、頻寬管理等記錄。管理者也是從這個功能選項設定將以何種方式傳送 Log 記錄至 server 上儲存起來；或者透過這裏所提供的 E-Mail 功能發送重要通知或測試訊息。

此外，Xtera 為提供更貼近客戶需求的產品，特研發一強大的報表軟體－LinkReport，提供管理者即時報表以獲得明確的網路流量狀況，不需再自行搜集資料得到統計報表。LinkReport 以 web-based 為設計開發的基礎，管理者只要輕鬆點選，報表隨手可得。這套程式是一套獨立的系統，用來統計和分析 AscenLink 所產生的 Log 資料。

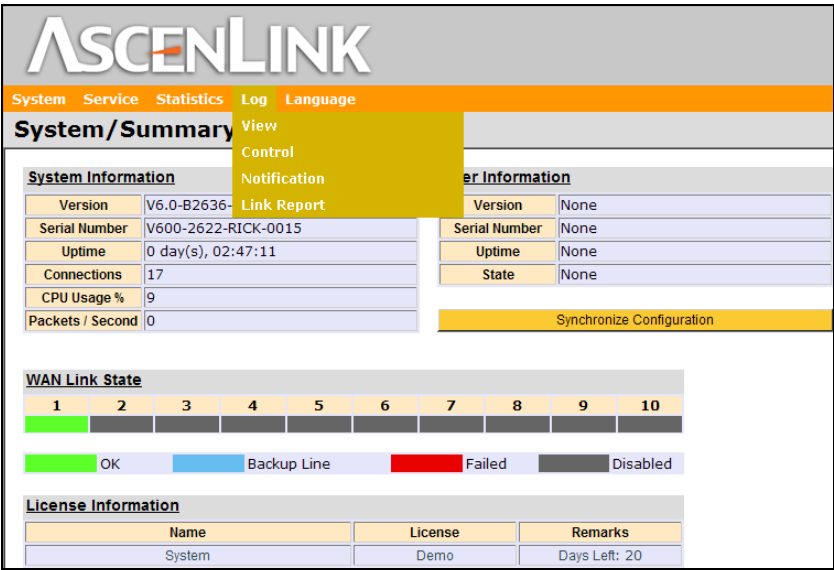


圖 5.1 Log 功能圖

5.1 View (記錄瀏覽)

在這個分頁裏面，AscenLink 提供各種不同的記錄種類，共 13 種（請參照下表）。管理者可以選擇想要察看的記錄種類（Log Type），選擇完畢後，記錄資料將會顯示于位於下方的視窗中。若要更新流覽記錄資料，只要按下 **refresh** 按鈕即可更新最新記錄資料。

管理者若想要下載記錄資料，請到下一個 **Control** 頁面（記錄/傳輸設定），並請準備一個 **FTP Server** 或 **Mail Server** 提供傳輸。

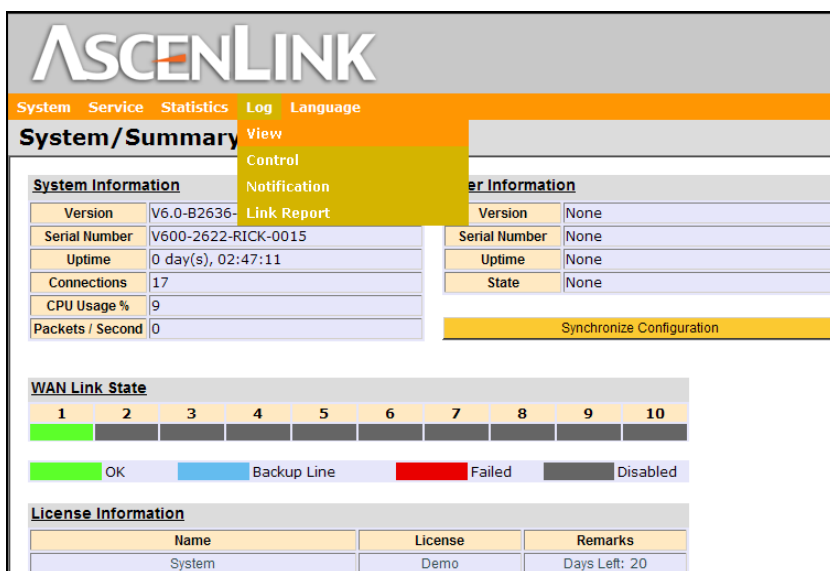


圖 5.2 Log/View 功能所處位置

欄位	值	說明
Log Type (記錄種類)	系統記錄 (System Log) 防火牆記錄 (Firewall Log) 網址轉譯記錄 (NAT Log) 自動路由和持續路由記錄 (Auto & Persistent Routing Log) 虛擬主機記錄 (Virtual Server Log) 頻寬管理記錄 (BM Log) 連線限制記錄 (Connection Limit Log) 快取轉址記錄 (Cache Redirect Log) 多重定址記錄 (Multihome Log) 備份線記錄 (Backup Line Log) 動態設定位址記錄 (Dynamic IP Log) IP-MAC MAPPING 記錄 (IP-MAC MAPPING Log) 通道路由記錄 (Tunnel Routing Log)	此欄位可選擇欲查看的記錄資料， AscenLink 共提供右列各種記錄資料 供查詢與分析，分別對應到服務功能 表的服務。
Recent Event (最近事件)	-	以時間為序，列出記錄資料。
Refresh (重新顯示)	-	重新整理查看記錄資料。

表5.1 Log/View 各功能選項解釋之參照表

5.2 Control (傳輸設定)

在這裏您可以設定要以何種方式將記錄資料傳送到別的伺服器上保存起來。您可以針對不同的記錄檔案，分別設定要以 **FTP** 檔案傳輸協定，或者是電子郵件的方式來傳送記錄檔。當然，如果您覺得個別設定很麻煩，直接按個鈕就可以把同一個設定使用於所有的記錄檔。

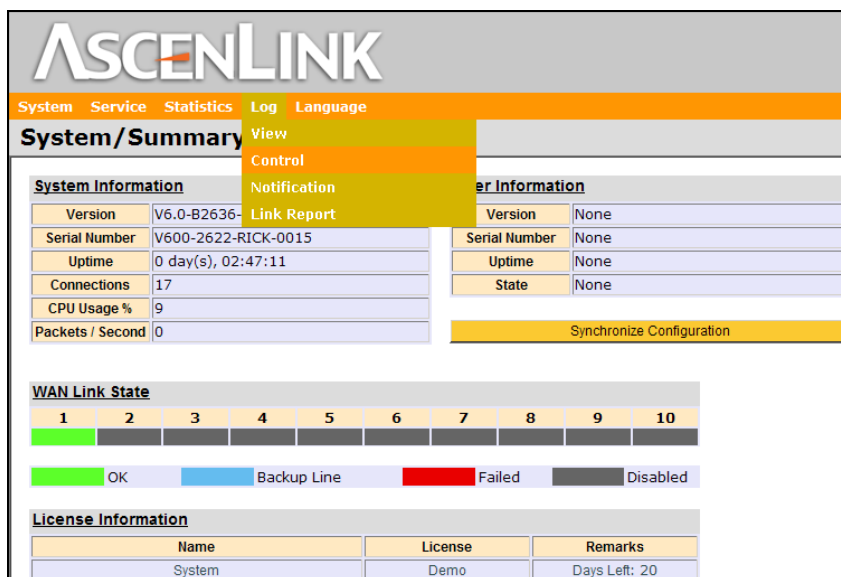


圖 5.3 Log/Control 功能所處位置

欄位	值	說明
Log Type 記錄種類	系統記錄 (System Log) 防火牆記錄 (Firewall Log) 網址轉譯記錄(NAT Log) 自動路由和持續路由記錄 (Auto & Persistent Routing Log) 虛擬主機記錄 (Virtual Server Log) 頻寬管理記錄 (BM Log) 連線限制記錄(Connection Limit Log) 快取轉址記錄 (Cache Redirect Log) 多重定址記錄 (Multihome Log) 備份線記錄(Backup Line Log) 動態設定位置記錄(Dynamic IP Log) IP-MAC MAPPING 記錄 (IP-MAC MAPPING Log) 通道路由記錄 (Tunnel Routing Log)	此欄位可選擇欲傳輸的記錄資料。
Copy Settings to All Other Log Types 複製設定到其他所有記錄	-	將下方關於本項記錄資料傳輸方式複製到其他的記錄資料
Method	E-Mail FTP	請參考下面的解釋
Note 備註	<Note >	填入自訂的批註資料
Push Now 立即傳送		點選此按鈕以立即傳輸記錄資料
Push Log When Out of Space 儲存空間已滿時主動傳送	Enable Disable	當記錄資料快滿時傳輸記錄資料，打勾以使用本項功能
Enable Scheduled Push 啟用定期傳送		啟用排程傳輸記錄資料
Initial Time 開始時間	<Year/Month/Day/Hour/Minute/Second>	指定開始排程傳輸的起始時間
Period 傳送期間	<Day/Hour/Minute>	指定每隔多少時間傳輸 AscenLink 的記錄資料

表5.2 Log/Control 各功能選項解釋之參照

傳送方式 (Method)

AscenLink 提供兩種傳輸的方式，傳到外部的 FTP 伺服器或用 SMTP 寄到管理者的郵件地址。

電子郵件 (E-mail)

欄位	值	說明
SMTP 伺服器 (SMTP Server)	<IP> or <Domain Name>	指定用來傳輸郵件的郵件主機
帳號(Account)	<SMTP Account>	郵件主機使用者認證所需的帳號
密碼 (Password)	<Account's Password>	郵件主機使用者認證所需的密碼
寄件者 (Mail From)	<e-Mail address>	郵件內容的寄件者
收件者 (Mail To)	<e-Mail address>	郵件內容的收件者，可添加多個收件人，以 “;”或 “,”分隔。

表5.3 傳輸方式:電子郵件欄位說明

FTP

欄位	值	說明
伺服器 (Server)	<IP> or <Domain Name>	FTP Server 的 IP 或 domain name
帳號 (Account)	<FTP Account>	FTP 使用者帳號
密碼 (Password)	<Account's Password>	FTP 使用者密碼
路徑 (Path)	<Path>	欲存放的路徑

表5.4 傳輸方:FTP 式欄位說明

5.3 Notification (重要通知)

在這個管理頁面，您可以設定當某些重要事件發生的時候，讓系統發出電子郵件來通知 Administrator。設定方式與傳輸設定分頁中的電子郵件設定相似。您可以按下「立即寄出測試資訊 (Send Test E-mail Now)」按鈕來測試是否可以正常發信。

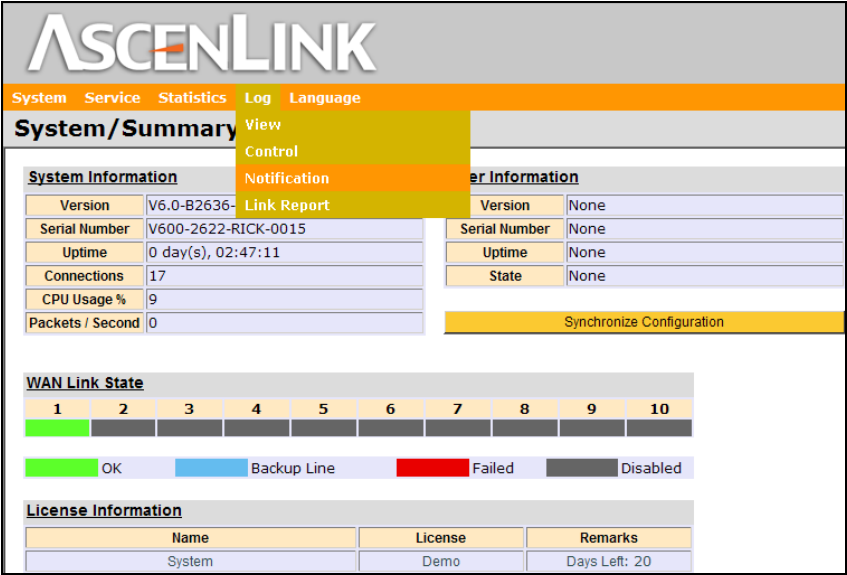


圖 5.4 log/Notification 功能所處位置

在此頁面中，有三個部份需要設定，如下：

E-Mail Settings	
① SMTP Server	<input type="text"/>
Account	<input type="text"/>
Password	<input type="text"/>
Mail From	<input type="text"/>
Mail To	<input type="text"/>
<input type="button" value="Send Test E-mail Now"/>	

SNMP Trap Settings	
② Destination IP	<input type="text"/>
Community Name	public

Event Types to Notify	
③	<input type="checkbox"/> Link failure and recovery
	<input type="checkbox"/> Service failure and recovery
	<input type="checkbox"/> Administrator password change
	<input type="checkbox"/> HA slave failure and recovery
	<input type="checkbox"/> HA takeover
	<input type="checkbox"/> Connections reach <input type="text"/>
	<input type="checkbox"/> Total Traffic reaches <input type="text"/> Kbps
<input type="button" value="Select All"/> <input type="button" value="Clear All"/>	

圖 5.5 Notification 功能設定

1. E-Mail Settings (電子郵件設定)

在此表格中設定相關的資料以設定重要通知郵件的送達。

欄位	說明
SMTP 伺服器 (SMTP Server)	指定使用的郵件主機
帳號 (Account)	郵件主機使用者認證所需的帳號
密碼 (Password)	郵件主機使用者認證所需的密碼
寄件者 (Mail From)	郵件內容的寄件者
送件者 (Mail To)	郵件內容的收件者，可添加多個收件人，以 “;”或 “,”分隔。
立即送出測試電子郵件 (Send Test E-mail Now)	立即送出測試信以確定設定是否有誤。

表5.5 Notification 各功能

2. SNMP Trap Settings

在此表格中設定 SNMP 的相關資料，注意你必須準備可接收 SNMP Trap 的設備。

欄位	值	說明
目標 IP 位址 (Destination IP)	<IP Address>	接收 SNMP Trap 設備的位址。
群體名稱 (Community Name)	<Community Name>	群體名稱

表5.6 SNMP Trap Setting 欄位說明

3. Event Types to Notify (應該通知的事件種類)

欄位	值	說明
Event Types to Notify	Link failure and recovery (網路連線故障與復原) Service failure and recovery (服務故障與復原) Administrator password change (Administrator 密碼變更) HA slave failure and recovery (高可用性副機失敗與復原) HA takeover (高可用性接管) Connections reach (總連線數達到設定值) Total Traffic reaches(總頻寬達到設定值)	在此可勾選需要寄送通知的事件。
Select All	-	勾選全部的選項
Clear All	-	清除全部所勾選的選項

表5.7 Event Types to Notify 欄位說明

5.4 LinkReport

此功能主要目的在於是否要啟動傳輸 Log 資訊的功能。在 AscenLink 運作中所產生的 Log 是屬於尚未被分析統計處理的原始資訊，而 LinkReport 即是將這些難以立即理解的 Log 資訊，經分析與統計，讓管理者透過簡單易懂的圖表，清楚瞭解網路連線的狀況。

首先，管理者需將建立一個網路傳輸線能將 Log 資訊傳送至一台內置 LinkReport 軟體的電腦中，而分析與統計的動作則是在這一台電腦上進行與顯示，而非在 Web UI 內。

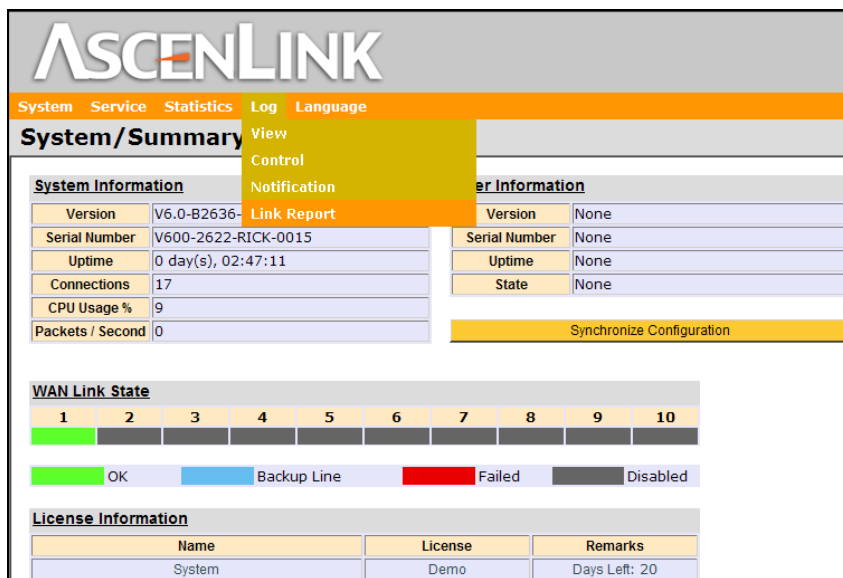


圖 5.6 Log/LinkReport 功能所處位置

此頁面共有兩個欄位，如下圖所示：

Enable Link Report☒

Recipient IP Address

192.168.123.95

Events

Firewall☒

Virtual Server☒

Bandwidth Usage☒

Connection Limit☒

Multihoming☒

Tunnel Routing☒

圖 5.7 LinkReport 欄位

各欄位的功能如下：

欄位	說明
Enable LinkReport (啓用 LinkReport)	啓動將 Log 記錄傳送出去的功能，若沒有啓動此一功能，AscenLink 在運作時所產生的 Log 記錄將不會傳輸出去，所以 LinkReport 就無法做分析與統計。
Recipient IP Address (接收端 IP 位址)	即是裝設有 LinkReport 軟體電腦的 IP 位址。也就是 Log 記錄將會傳送的目的地。

表5.8 LinkReport 欄位說明

關於記錄種類的說明如下：

欄位	值	說明
Events (記錄種類)	Firewall(防火牆) Virtual Server(虛擬主機) Bandwidth Usage(頻寬管理) Connect Limit(連線限制) Multihoming(多重定址) Tunnel Routing(通道路由)	在此可勾選需要寄送的記錄種類。

表5.9 記錄種類欄位說明

5-14

目錄

第六章 應用討論.....	6-3
6.1 廣域網路類型之應用實例	6-3
6.1.1 Bridge Mode: One Static IP 之廣域網路	6-3
6.1.2 AscenLink 在 Routing Mode 之廣域網路設定	6-7
6.2 Auto Routing(自動路由) 應用探討	6-16
6.2.1 使用 Auto Routing 的優點	6-17
6.2.2 AscenLink 提供線路中斷時自動備援的運作方式	6-19
6.2.3 Persistent Routing 和 Auto Routing	6-22
6.3 流量負載平衡應用探討	6-23
6.4 Virtual Server (虛擬主機) 的應用	6-25
6.5 Multihoming 的應用	6-26
6.6 DNS 服務簡介	6-29
6.6.1 SwiftDNS	6-31
6.7 HA 應用討論	6-33
6.7.1 HA 模式下的 firmware 更新方式	6-33
6.7.2 HA 模式下復原至單機的操作方式	6-35
6.7.3 Slave 接管 Master 之原則	6-35

圖目錄

圖 6.1 Bridge Mode: One Static IP 之廣域網路架構圖..... 6-4

圖 6.2 Routing Mode 連線之廣域網路..... 6-7

圖 6.3 以 Router 與 AscenLink 間私有網路模式連線之廣域網路 6-10

圖 6.4 多條廣域網路模式連線之廣域網路 6-12

圖 6.5 網路中斷時採用手動方式變更網路組態..... 6-18

圖 6.6 網路中斷時以 Auto Routing 方式選擇線路 6-19

圖 6.7 固定分配線路斷線時自動切換至備用模式 6-20

圖 6.8 典型的多重定址網路連線方式 6-26

圖 6.9 Multihoming 設定圖 6-32

第六章 應用討論

6.1 廣域網路類型之應用實例

在這個章節中，我們提供 AscenLink 在 Network 上應用的實例，使用者可以透過下面一些范例，獲得更明確的應用概念及熟悉 Web UI 的參數設定。從單純到複雜類型的網路架構，AscenLink 都可以適用。

6.1.1 Bridge Mode: One Static IP 之廣域網路

One Static IP (單一固定 IP) 是一種較為簡單的網路架構。首先，我們先定義何謂 One Static IP 之廣域網路。所謂 One Static IP 之廣域網路通常指 ISP 所提供一個固定 IP 的網路服務，ISP 會提供一個網路區段中某個單一 IP 給申請者，所以申請者只有一個 Public IP 可以使用。

這種情況下，AscenLink 的某個網路介面將佔用這個 Public IP，而所有提供公開服務的伺服器 (FTP, SMTP, WWW) 必須使用 Virtual Server 的方式提供服務。

註：ISP 提供 bridge mode 的 ATU-R，一般所稱的 ADSL Modem。

One Static IP 之廣域網路架構如下圖所示：

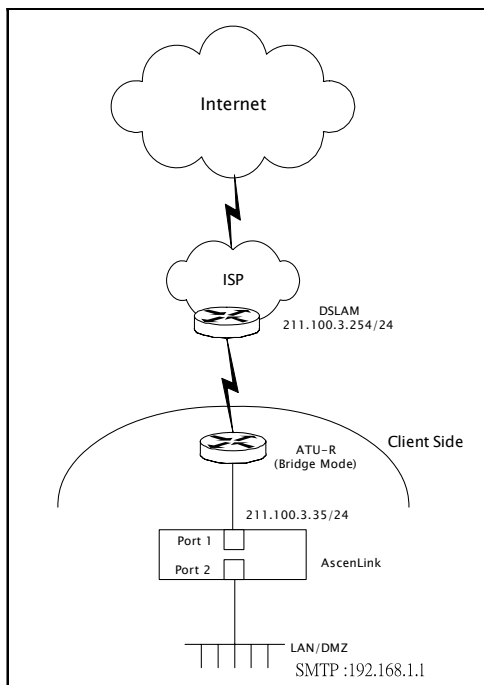


圖 6.1 Bridge Mode: One Static IP 之廣域網路架構圖

範例

本例中假設把 WAN Port (Port 1)接到提供 bridge mode 的 ATU-R 上。

ISP 提供的資料：

- Client Side 的 IP 為 211.100.3.35，
- Gateway 為 211.100.3.254，
- Net Mask 為 255.255.255.0，

- ISP 提供一台 ATU-R，設定為 Bridge Mode。

硬體設定：

ATU-R 請參照 ISP 所提供的相關手冊將網線接至 AscenLink WAN1 上。

註：AscenLink 在與網路設備接線時，視同為一般電腦。

WAN 設定順序：

1. 登入 AscenLink Web 管理介面。
2. 進入[System] → [Network Setting] → [WAN setting]。
3. 在 WAN Link 的下拉功能表中選擇 1，點選 Basic Setting 的 Enable 以打勾啟用。
4. 在 WAN Type 的下拉功能表中選擇 [Bridge Mode: One Static IP]。
5. 輸入相對應的內外頻寬，舉例說明：申請的是 512/64，那麼在 Up Stream 的欄位請填入[64]，Down Stream 的欄位請填入[512]。

註：這部分的數值會影響到 BM 與 statistics 分頁的資料，輸入過大的值並不能增加您的頻寬。

6. Localhost IP 欄位請填入 [211.100.3.35]，Netmask 欄位請填入 [255.255.255.0]，Gateway IP 欄位請填入 [211.100.3.254]，WAN Port 欄位請選擇 [Port 1]。

完成 bridge mode 的設定。

若上述的設定正確的話，在 [System] → [Summary] 的頁面上會看到 WAN Link State 欄位上 1 的顏色方塊呈現亮綠色。

Virtual Server 設定：

在 Bridge mode 下提供對外公開服務的方式，例如提供 SMTP Server，這台對外提供服務的主機，設定在內部網路內，假設內部所使用之 SMTP Server IP 為 192.168.1.1，AscenLink 可以用 NAT 技術，將內部 IP 對應至外部公開 IP，這也是外界用戶可以看到的 IP 位址。內容設定如下：

- 進入[Service] → [Virtual Server]頁面。
- 點選[+]新增一條規則。
- 點選 E 以啓用此項規則。
- When 欄位選擇 [All-Time]。
- WAN IP 欄位填入 [211.100.3.35]。
- Server IP 欄位填入 [192.168.1.1]。
- Service 欄位選擇 [SMTP(25)]。
- L 欄位可勾選，也可不勾選 (若管理者需要 Virtual Server 的記錄資料，則請勾選 L 欄位)。

完成設定。

管理者可依據對外提供網路服務的需求，在區域網路（LAN）內，設定不同類型的 Service，利用 Virtual Server 功能，將內部 IP 對應至 WAN public IP。完成設定後，內部 Virtual Server 就可開始對外提供服務，增加管理上的彈性與方便。

6.1.2 AscenLink 在 Routing Mode 之廣域網路設定

範例一

此部份應用是由 ISP 提供一個網路區段給申請者，例如 ISP 提供一段 class C 網路區段給申請者使用。

在此情況下，AscenLink 通常會佔用 1 個或數個不等 IP，其餘 IP 將預設放置于 DMZ 區段之下。公開位址主機可放置兩個地方：

- 可放在 ATU-R 內部，AscenLink 外部。
- 在 AscenLink DMZ 區段之下：

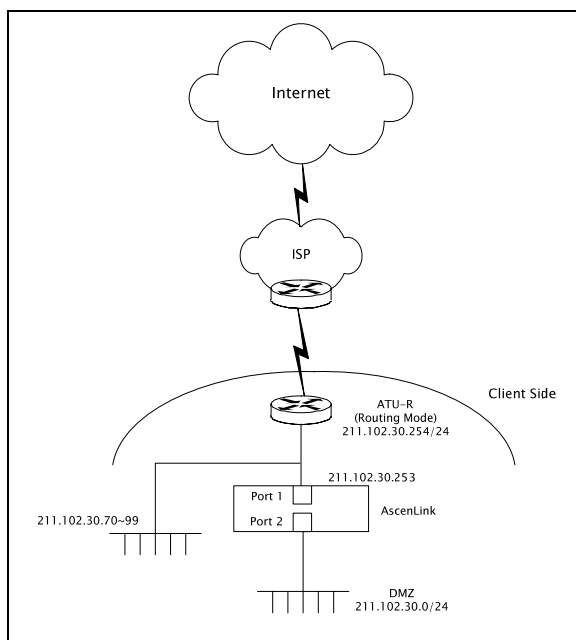


圖 6.2 Routing Mode 連線之廣域網路

本例中假設把 WAN port (port 1) 接至 Router。

ISP 提供的資料：

- Client Side IP 網路區段為 211.102.30.0/24，Gateway (Router IP) 為 211.102.30.254，Net Mask 為 255.255.255.0。
- 假設 AscenLink 之 IP 位址為 211.102.30.253。
- 211.102.30.70-100.102.30.99 這些主機位址在 AscenLink 之外，ATU-R 之內。
- WAN port 使用 port 1。
- DMZ port 使用 port 2。
- 提供 Router。

硬體設定：

Router 請參照相關手冊將網線接至 AscenLink WAN1 上。

註：AscenLink 在與網路設備接線時，將視同為一般電腦。

設定順序：

1. 登入 AscenLink Web UI。
2. 進入[System] → [Network Setting] → [WAN setting]。
3. 在 WAN Link 的下拉功能表中選擇 1，點選 Basic Setting 以打勾啟用。
4. 在 WAN Type 的下拉功能表中選擇 [Routing Mode]。
5. 輸入相對應的內外頻寬，舉例：申請的是 512/64，那麼在 Up Stream 的欄位請填入[64]，Down Stream 的欄位請填入[512]。

註：這部分的數值會影響到 BM 與 statistics 分頁的資料，輸入超過所申請的數值並不能增加您的頻寬。

6. Gateway 設定為 211.21.30.254。
7. WAN Port 設定為 Port 1。

8. 在 WAN 和 DMZ 區域各有一個子網路，因此在 Basic Subnet 表格中，選擇 Subnet Type 為” Subnet in WAN and DMZ”，內容設定如下：

IP(s)on Localhost 欄位請填入 [211.102.30.253]。

IP(s) in WAN 欄位請填入 [211.102.30.70-211.102.30.99]。

Netmask 欄位請填入 [255.255.255.0]。

DMZ Port 欄位請選擇 [Port 2]。

設定完成。

註：除了 IP(s)在 WAN 欄位中所指定的位址外，其餘的位址皆存在 DMZ 中。
(211.102.30.1-211.102.30.69, 211.102.30.100-211.102.30.252)。

範例二

此狀況為擁有一條廣域網路連線，連線廣域網路的 Router 與 AscenLink 間有一段私有網路，AscenLink DMZ 區域為 Public IP Subnet，並利用 Router 設定一個 Public IP 的 Subnet。

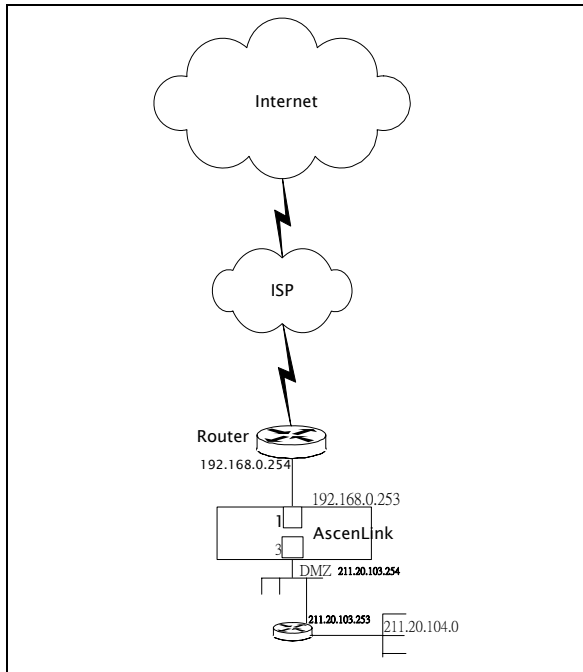


圖 6.3 以 Router 與 AscenLink 間私有網路模式連線之廣域網路

範例說明：

在此範例中，假設連線廣域網路的 Router 與 AscenLink WAN Port 間為一 Private IP 網路 (192.168.0.0/24)。

AscenLink 以 Port 1 (192.168.0.253) 連線廣域網路的 Router (192.168.0.254)。

AscenLink 以 Port 3 作為 DMZ，設定一個 Public IP Subnet (211.20.103.254/24)。

AscenLink 內部存在另一個 Public Subnet (211.20.104.0/24)，在另一個 Router 之後 (211.20.103.253)。

設定順序：

1. 登入 AscenLink Web UI。進入[System] → [Network Setting] → [WAN setting] 子頁面。
 2. 在 WAN Link 的下拉功能表中選擇 1。
 3. 點選 Enable 欄位的 check Box 打勾啟用。
 4. 輸入相對應的內外頻寬。
 5. Default Gateway 欄位請填入 [192.168.0.254]；WAN Port 欄位請選擇 [Port 1]。
 6. 在 Basic Subnet 的表格中，點選[+] 增添一組規則，然後在 Subnet Type 欄位選擇 “Subnet in DMZ”。
 7. IP(s)在 Localhost 欄位請填入 [211.20.103.254]；Netmask 欄位請填入 [255.255.255.0]；DMZ Port 欄位請選擇 [Port 3]。
 8. 在 Static Routing Subnet 表格中點選 [+]，增添一組規則，在欄位 Subnet Type 設定為 “Subnet in DMZ”。
- 註：在這個範例中，DMZ 區利用一部 Router 再設定出一個 Public IP Subnet，因為沒有直接連線到 AscenLink，所以在 Static Routing Subnet 表格中，將這個子網路的參數填入。
9. Network IP 欄位請填入 [211.20.104.0]；Netmask 欄位請填入 [255.255.255.0]；Gateway IP 欄位請填入 [211.20.103.253]。
 - 10.到 [WAN/DMZ private Subnet] 子頁面，在 Basic Subnet 表格中點選[+]，以增添一組規則欄位。
 - 11.Subnet Type 設定為 “Subnet in WAN”。
 - 12.IP(s)在 Localhost 欄位請填入 [192.168.0.253]；Netmask 欄位請填入 [255.255.255.0]；WAN Port 欄位請選擇[Port 1]。

設定完成。

範例三

本範例應用為擁有多條廣域網路連線的狀態，**AscenLink** 使用兩組私有位址與兩個與廣域網路連線的 **Router** 相接。

下圖為此應用範例的網路架構圖，圖中顯示，**AscenLink Port3** 為另一組 **Private IP**，連線至一台 **Core Switch (Layer 3 Switch)** 上，**Public IP Subnet** 存在於 **Core Switch** 之下。

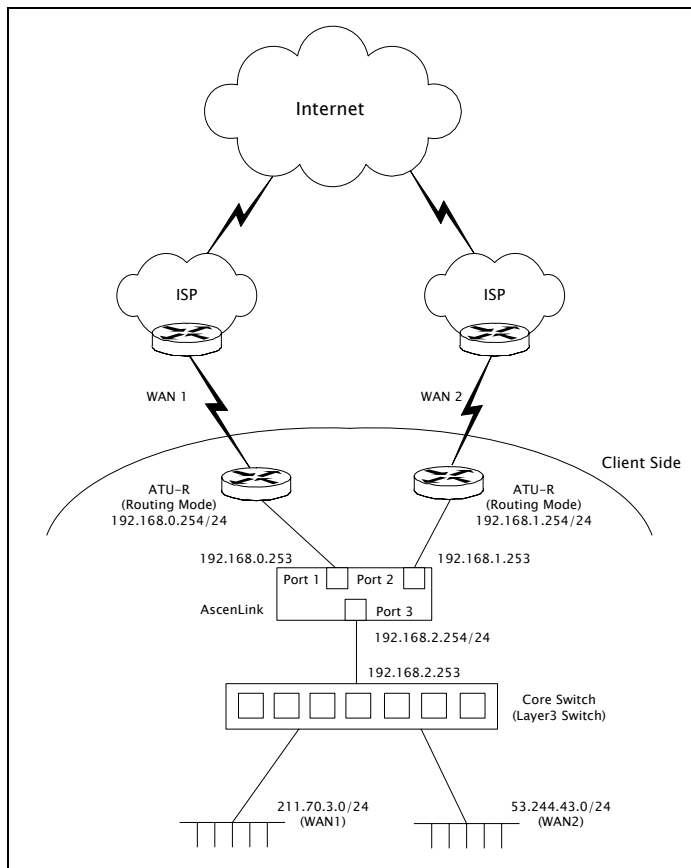


圖 6.4 多條廣域網路模式連線之廣域網路

範例說明：

AscenLink 以 Port 1 (192.168.0.253) 連線 WAN1 廣域網路的 Router (192.168.0.254/24)。

AscenLink 以 Port 2 (192.168.1.253) 連線 WAN2 廣域網路的 Router (192.168.1.254/24)。

AscenLink 以 Port 3 (192.168.2.254) 連線內部的 CoreSwitch (192.168.2.253/24)。

WAN1 的 Public IP Subnet 存在 CoreSwitch 之下 (211.70.3.0/24)。

WAN2 的 Public IP Subnet 存在 CoreSwitch 之下 (53.244.43.0/24)。

設定順序：

1. 登入 AscenLink Web UI，進入[System] → [Network Setting] → [WAN setting] 管理頁面。填入內容為：

- 在 WAN Link 的下拉功能表中選擇 1。
- 點選 Enable 的 CheckBox 打勾啟用。
- 在 WAN Type 的下拉功能表中選擇 [Routing Mode]。
- 輸入相對應的內外頻寬。
- Default Gateway IP 欄位請填入 [192.168.0.254]。
- WAN Port 欄位請選擇 [Port 1]。
- 在 Static Routing Subnet 表格中，點選 [+] 增添一組規則，在欄位 Subnet Type 欄位中，選擇“Subnet in DMZ”。

註：這是因為子網路是在 DMZ 區段，利用 Core Switch 加以設定，並不直接連線到 AscenLink，因此需要在 Static Routing Subnet 表格，將這個子網路的參數添入。

- Network IP 欄位請填入 [211.70.3.0]；Netmask 欄位請填入 [255.255.255.0]；Gateway IP 欄位請填入 [192.168.2.253]。

2. 在 WAN Link 的下拉功能表中選擇 2 以切換至 WAN2。設定內容為：
 - 點選 Basic Setting 的以打勾啟用。
 - 在 WAN Type 的下拉功能表中選擇 [Routing Mode]。
 - 輸入相對應的內外頻寬。
 - Default Gateway IP 欄位請填入 [192.168.1.254]。
 - WAN Port 欄位請選擇 [Port 2]。
 - 在 Static Routing Subnet 的表格中，點選 [+] 增添一組規則，在 Subnet Type 欄位中，選擇 “Subnet in DMZ”。
 - Network IP 欄位請填入 [53.244.43.0]；Netmask 欄位請填入 [255.255.255.0]；Gateway IP 欄位請填入 [192.168.2.253]。
3. 進入 [WAN/DMZ Private Subnet] 管理頁面，設定內容為：
 - 在這個頁面中指定網路中的三組 Private Subnet。分別在 WAN 和 DMZ 區段。
 - 在 Basic Subnet 欄位中，點選[+]增添一組規則，先設定 192.168.0.0/24 這個子網路，在 Subnet Type 欄位中，選擇 “Subnet in WAN”。
 - IP(s)on Localhost 欄位請填入 [192.168.0.253]。
 - Netmask 欄位請填入[255.255.255.0]。
 - WAN Port 欄位請選擇 [Port 1]。
4. 完成 WAN Port 1 的設定，接下來設定 WAN Port 2，設定內容為：
 - 在 Basic Subnet 欄位中，點選[+]增添一組規則，設定 192.168.1.0/24 這個子網路，在 Subnet Type 欄位中，選擇 “Subnet in WAN”。
 - IP(s)on Localhost 欄位請填入 [192.168.1.253]。
 - Netmask 欄位請填入 [255.255.255.0]。

- WAN Port 欄位請選擇[Port2]。
- 完成 WAN Port 2 的設定。接下來設定 DMZ Port。
- 在 Basic Subnet 欄位中，點選[+]增添一組規則，在 Subnet Type 欄位中，選擇 “Subnet in DMZ”。
- IP(s)on Localhost 欄位請填入 [192.168.2.253]。
- Netmask 欄位請填入 [255.255.255.0]。
- DMZ Port 欄位請選擇 [Port3]。

設定完成。

透過以上這個範例，我們可以理解到，一個 Private IP Subnet 直接設定在 WAN/DMZ 區域，並利用 Core Switch 或 Router 設定設定一個 Public IP Subnet 間接連線到 AscenLink。

6.2 Auto Routing(自動路由) 應用探討

與 Multihoming (多重定址) 相比，Auto Routing 是指初始封包由本地區域網路發出的情況。而 Multihoming 則是初始封包發自外部 Internet。

隨著網路應用程式的增加和線路費用的降低，越來越多的企業選擇使用多線路導入，尤其是同時使用不同 ISP 所提供多條線路，這往往是出於如下的考慮：當線路出現故障時可以切換至另外的線路，增加線路的可靠性；透過多條線路增加頻寬，平衡負載，合理利用頻寬資源。

當頻寬作為一種重要網路資源的觀念被認可時起，核算總導入成本的計算就沒有停止，DDN, ISDN, ADSL、社區寬頻也佔據了不同時間的市場份額，許多使用者都有兩條以上的導入線路，線路備援、擴容已經成為網路建設的重要部分。

多線路備援具有兩方面的含義：

- 內部網路使用者存取 Internet 資源時，封包從多條線路發出。
- 來自 Internet 的用戶，透過不同的線路，存取內部網路的伺服器資源。

6.2.1 使用 Auto Routing 的優點

本章主要介紹內部網路使用者使用多線路存取 Internet 資源時的情況。

Auto Routing 是指可以同時使用多條 ISP 線路，並可以將流量負載自動分配在不同線路上的技術，當線路中斷時，不用手動修改設定就可以將流量自動切換至其他線路的工作方式。

傳統的線路備援都是採取備而不用的方式，一般會有兩條線路，即在 **Router** 上設定線路備援政策。當一條線路故障時，自動連線另外一條線路，這時，始終會有一條線路處於空閒狀態，造成資源浪費，而且透過一台 **Router** 實現多條線路備援的方式也過於繁瑣。

對頻寬要求較高的企業一般會採取兩台 **Router** 同時工作的方式，實際上就是在一個企業內部使用兩條相互獨立的 Internet 導入，形成兩個獨立的網路架構。

在正常情況下兩台 **Router** 分別使用各自的頻寬資源，當一條線路出現故障時，管理者透過修改設定，仍可確保關鍵服務的運轉。當然，這種方法的缺點也十分明顯，增加了管理上的難度，平時需要維護兩個不同的網路，而且兩台 **Router** 會為內部設備提供兩個 **Gateway**（預設路由），內部網路的使用者會分成兩個部分，線路故障時必須手動修改另一部分設備的 **Gateway IP**，包括 **Server** 和 **Work Station**。

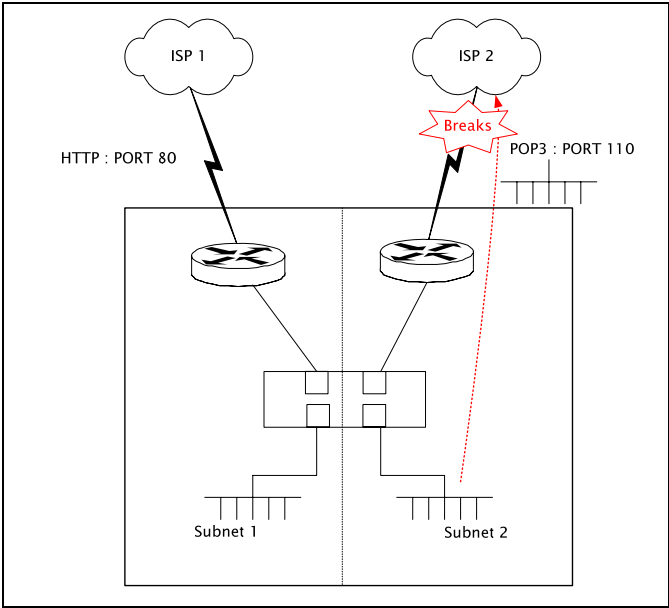


圖 6.5 網路中斷時採用手動方式變更網路組態

6.2.2 AscenLink 提供線路中斷時自動備援的運作方式

上圖 6.5 所示採用傳統備援手段導入 Internet 的情況，無論哪條線路發生故障，都會明顯影響到內部網路應用，管理員必須進行干預。

AscenLink 在內部維護一條 Virtual Trunk (虛擬主幹) 線路，實際上是由多條真實的廣域網線路組成，Auto Routing 的作用是當其中的線路故障時，不需人工干預即可自動將流量切換到正常的線路上，使用者不會覺察到線路的中斷情況。

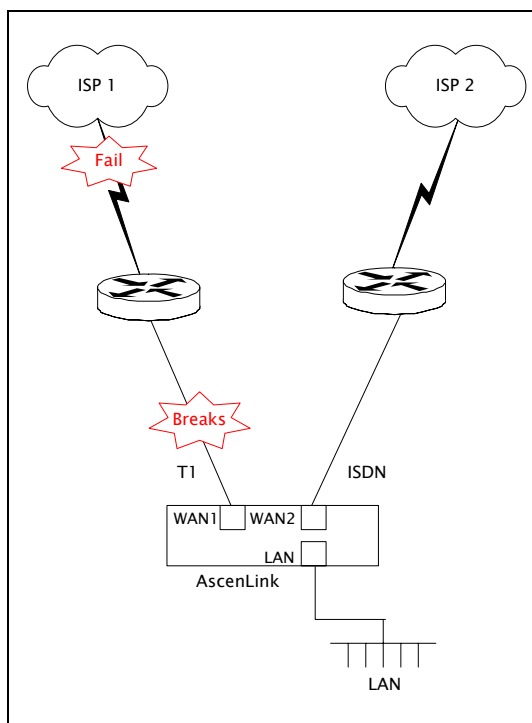


圖 6.6 網路中斷時以 Auto Routing 方式選擇線路

上圖所示採用 **AscenLink Auto Routing** 功能後，使用者將面對一個不間斷的網路，任何一條線路發生故障，使用者都不會感覺到明顯的變化。

更為關鍵的是，在傳統的 **Router** 備援政策中，根本無法實現線路負載平衡，無法充分地利用頻寬。

Auto Routing 不能避免在線路中斷時 **session** 的中斷，但新發起的 **session** 會自動選擇一條新的路徑。**AscenLink** 至少可以支援 2 條以上廣域網路的 **Auto Routing**，並可自由選擇備援的線路政策。

與 **AscenLink** 的線路負載平衡政策相結合，**AscenLink** 共有 5 種 **Auto Routing** 方式，可以根據應用情況靈活設定。

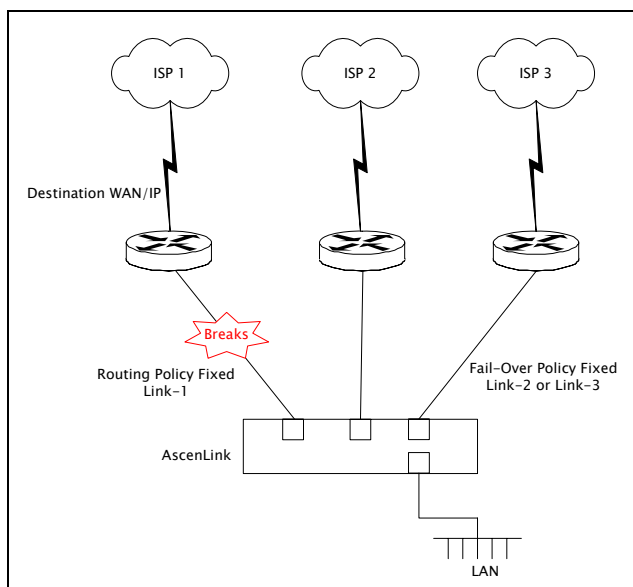


圖 6.7 固定分配線路斷線時自動切換至備用模式

路由選擇方式：

欄位	說明
Fixed (固定指派)	將流量固定在某一條廣域網路連線上。
Round-Robin (輪流指派)	將流量依照所給定的比例分散在所指定的廣域網路連線上。
By DownstreamTraffic (根據下載流量)	在目前選定的廣域網路連線中選擇下載流量最小的線路建立新的連線。
By Upstream Traffic (根據上傳流量)	在目前選定的廣域網路連線中選擇上傳流量最小的線路建立新的連線。
By Total Traffic (根據全部流量)	在目前選定的廣域網路連線中選擇總流量最小的線路建立新的連線。

表 6.1 路由選擇欄位說明

註：在後四種的路由選擇方式中，會自動跳過有問題的線路，比方說在 Round-Robin 中指定 WAN1:WAN2:WAN3 = 6:3:1, 當 WAN3 發生問題時，會自動成為 WAN1:WAN2 = 6:3 的輪流指派模式。

6.2.3 Persistent Routing 和 Auto Routing

在這兩項路由設定功能中，如果設定對同一個目的主機의 Routing 方式，會有以下的現象：

- 以自動路由的規則(Routing Policy)決定第一次連線使用的對外線路。
- 在第一次的線路決定後，便以 Persistent Routing 決定繼續使用的線路。

若線路發生故障，須等到 Persistent Routing 中設定的 Time-out 時間到後，才會重新以 Auto Routing 的規則決定新的連線。

若需手動清除目前的持續路由資料，請至[Statistics] → [Persistent Routing] 中點選 [Clear All] 以清除。

當 AscenLink 發現某條線路發生故障時相關 Service 的處理方式：

- Auto Routing 會自動排除此條線路，若線路使用方式是指定 (Fixed) 這條發生故障的線路，將會使用備援程式的規則。
- Persistent Routing 會在達到 Time-out 指定的時間後，重新以 Auto Routing 的方式找到可用的新線路。
- Multihoming 將自動停止響應此故障線路所設定的 IP，改以其他正常線路所設定的 IP 回應。

6.3 流量負載平衡應用探討

Internet 的規模每天都會增長，關鍵業務和應用程式需要不間斷的 High Availability(高可用性)及較快的系統反應時間，而不願屢次看到某個站點 “Server Too Busy” 及頻繁的系統故障。

Load Balance (線路負載平衡) 建立在現有網路架構之上，它提供了一種經濟且透明的方案，擴展網路設備和伺服器的頻寬、增加吞吐量、加強網路資料處理能力、提高網路的靈活性和高可用性。

AscenLink 在負載平衡政策充分考慮到決定負載平衡性能的兩個關鍵因素：

- 負載平衡演算法。
- 網路系統狀況的偵測方式和能力。

考慮到服務請求的類型、伺服器的處理能力以及隨機選擇造成的負載分配不均等問題，為了更加合理地把負載分配給不同的線路，AscenLink 採用如下負載平衡演算法和網路狀態偵測方法：

Fixed (固定指派)

選擇固定的廣域網路，即選擇當前連線失效時固定指派承擔負載的線路。

Round Robin (輪流指派)

每一次來自內部網路的請求輪流分配給廣域網路，從 1 至 N 然後重新開始。此種平衡演算法適合於廣域網路中的所有線路都有相同的頻寬的情況。

By Downstream Traffic (根據下載流量)

以線路的下載頻寬為參數，動態的選擇負載最輕的線路。

By Upstream Traffic (根據上傳流量)

以線路的上傳頻寬為參數，動態的選擇負載最輕的線路。

By Total Traffic (根據全部流量)

以線路的上傳加下載頻寬為參數，動態的選擇負載最輕的線路。

AscenLink 可以利用多種方式對網路狀態進行偵測，以確保負載平衡政策的實施，達到不間斷可用性的要求。例如用 **Ping** 指令偵測，偵測網路系統狀況，此種方式簡單快速，能大致偵測出網路是否正常。

AscenLink 也會將線路上是否有資料傳輸作為連線狀態是否正常的參考條件。

6.4 Virtual Server (虛擬主機) 的應用

透過 Virtual Server 技術，使用者可以讓一台 Server 建立於區域網路內，而廣域網路使用者也能夠存取這台 Server 所提供的服務，例如一台主機上執行 FTP 和 WWW 服務。利用 Virtual Server 功能可以分別對外界提供 FTP 和 WWW 服務。

如果您想讓設定於內部區域網路或隔離區的伺服器能夠對外服務，就要使用虛擬主機(Virtual Server) 這項功能。

Virtual Server 的列表是有先後順序的，也是採用「找到第一條符合 (First Match)」的原則。每一列是由比對條件與處理方式所構成。比對條件包含是否啟用 (E)、時段 (When)、廣域網路 IP 位址 (WAN IP)、以及服務 (Service)；當廣域網路來一個請求 (request) 如果符合了虛擬主機的列表中一列的比對條件，則其內部伺服器 IP 位址欄所指的伺服器即為處理此請求的伺服器。

舉例來說，您第一條廣域網路的 IP 位址是 211.21.48.196，您打算將這個 IP 位址的網頁服務交由內部的 192.168.123.16 這台主機來處理。那麼您就可以新增一列，服務(Service) 選擇「HTTP(80)」、廣域網路 IP 位址 (WAN IP) 填入「211.21.48.196」、伺服器 IP 位址 (Server IP) 填入「192.168.123.16」、時段 (When) 選擇「所有時段 (All-Time)」。

6.5 Multihoming 的應用

為滿足 Internet 不中斷服務的需求，採用多條線路分擔單一主幹線路負載、以增加頻寬、提供高可用性已經成為企業的首選方法。通常的做法就是安裝多個 ISP (Internet Service Provider) 的網路。這種將服務分佈在多條網路上，透過多個 ISP 的方法被稱為多重定址。對於占 Internet 使用 80% 以上的 Web 服務來說，使用 Multihoming 就可以透過不同的 ISP 存取後端 Web 服務，有效避開線路和負載風險。

當然，也有將一台主機中採用多個網卡提供網路服務的方法稱為 Multihoming。本章所提及的 Multihoming 是指透過多個 ISP 的連線使用，下圖是典型的 Multihoming 網路，圖中區域網路透過 ISP1 和 ISP2 兩條線路連線到 Internet。

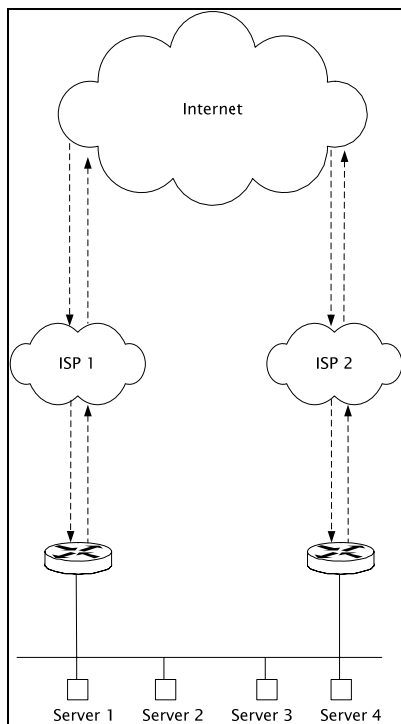


圖 6.8 典型的多重定址網路連線方式

同時使用不同 ISP 提供的 IP 位址，這種方式為本章著重討論的部分。通常這種連線方式在處理 Inbound 資料時會有問題，即如果正在使用 ISP1 提供的 IP 位址，這時連線 ISP1 的線路出現故障，來自 Internet 的存取請求就無法得到回應，因為這些請求只知道透過 ISP1 提供的 IP 位址取得服務。同樣，由於使用了 ISP1 提供的 IP 位址，ISP2 線路就不會處理 Inbound 資料。所以使用多條線路的問題就是如何提供對外服務的 IP 位址。

Multihoming 技術採用 DNS 容錯機制來解決多條線路共同提供對外服務的問題，舉例來說，本地區域網路設定有對外提供服務的 WEB 伺服器，如果只使用一個 ISP 線路，當線路故障時自然無法提供對外服務，透過 DNS 輪流指派不同 ISP 線路提供的 IP 位址，來自 Internet 的請求總會得到一個可用的 IP 位址存取服務，前提是至少要確保一條線路處於正常狀態。具體做法是在 DNS 伺服器中為多個不同位址設定同一個名字，這個資料被發送給其他名稱伺服器，而最終查詢這個名稱會得到不同的位址。因此不同的用戶端存取的也就是不同位址的 Web 伺服器，從而達到多重定址的目的。

例如，使用三個 Web 伺服器來回應對 `www.example.com` 的 HTTP 請求，可以看到該域的 DNS 伺服器會包括類似以下的資訊：

`www IN A 192.168.1.1`

`www IN A 192.168.1.2`

`www IN A 192.168.1.3`

DNS 輪詢仍然會存在一些問題，即 DNS 伺服器在回答 DNS 查詢時不會去判斷 IP 位址是否可用，所以仍然會將失效 ISP 之 IP 傳回給用戶端，造成用戶端無法存取服務的現象，用戶端瀏覽器可能要做多次更新才能存取到正常的服務。實際上，普通意義的 **Multihoming** 都會存在一些問題，如：

對於外來的存取請求，如來自 Internet 的用戶端存取您的 **Multihoming** 網路中的 Web 伺服器，肯定會出現某條 ISP 線路優於其他 ISP 線路的情況（由於線路頻寬不同或線路品質不同），但卻無法做出動態線路選擇。

無法實現負載平衡，無法調整應用在不同線路上的分佈，對負載處理比較原始，只能實現基於一條線路的負載共用。

Multihoming 要處理合理的 **ISP** 線路切換、負載平衡、達成可判斷 **IP** 位址是否正常的 **DNS** 輪詢機制，必須引入新的手段，**AscenLink** 為有效解決以上問題提供了最便捷的方案，下面的部分會介紹亞盛科技的專利技術 **SwiftDNS**，在其他章節會介紹亞盛科技的負載平衡、頻寬管理技術，在一台設備裏即可實現 **Multihoming** 傳輸的管理。

6.6 DNS 服務簡介

DNS 伺服器系統與主機列表 (host file) 不同，主機列表依據的是所有主機清單，DNS 伺服器只包含有限的資訊，因為他們知道到哪里能找到他們想知道的網域細節。當 DNS 伺服器收到解析某個主機的請求，而該主機又不在其快取記憶體內，那麼此 DNS 伺服器就會去詢問知道答案的其他 DNS 伺服器。如果被詢問的伺服器並不包含有關的網域名稱資訊，該伺服器就會將請求傳遞給更高級別的網域名稱伺服器，這樣就形成了一系列查詢，直到最後找到需要的資訊。

實際上，這意味著請求可以被任意數量的伺服器處理，在 Internet 上這種來來回回的行爲每時每刻都在發生。最早發出請求的伺服器會將查詢到的資訊保存在快取區內一段時間，這樣同樣的查詢請求就而無須再往其他 DNS 伺服器。可以修改 DNS 伺服器的資訊逾時限制 (TTL) 以確保快取中的資料更新。

DNS 服務的最常用軟體是 Berkeley Internet Name Domain，也就是 BIND，BIND 提供了解析器和名字伺服器軟體，解析器做實際的查詢工作而名字伺服器則提供回應。BIND 將名字伺服器分成三個部分：主伺服器 (Primary) 包含了有關一個域的全部資料；次伺服器 (Secondary) 則有效地從主伺服器拷貝 DNS 資料庫；緩衝伺服器(Cache) 透過緩衝查詢來建立額外的 DNS 資料庫。

要理解 DNS 伺服器怎麼操作就有必要理解網域名稱層次本身。在這一層次的頂部是根域(Root)。這一域上的資訊駐留在從整個 Internet 中所選的一些根伺服器上。在根域下面是頂級域，也就是國家代碼或機構代碼。國家代碼的例子有 CN (中國) 和 CA (加拿大) 等。而機構代碼則包括眾所周知的 COM (商業機構)、EDU (教育機構)、GOV(政府機構) 和 NET (網路機構) 等。在頂級域下面是次級域 (whitehouse.gov、microsoft.com、inforamp.net 等諸如此類)，然後是第 3 級域，等等向下以此類推。

建立網域名稱必須聯繫網路資訊中心 NIC。在它同意你的請求以前，你首先要確保你想要的名字還沒被使用，其次要確保目前至少有 2 台伺服器可以提供新網域名稱的服務。當 NIC 最後同意請求時，它將承認你的次級域，並將指向該名字的指標放到頂級域所在的伺服器內。例如，如果你請求網域名稱 xtera.com，那麼你必須首先讓 Internet 上的 2 台名字伺服器提供資訊服務 (你的 ISP 的伺服器能做到這一

點)，然後 NIC 將把 xtera 放到 COM 域伺服器系統內，其指標將指向那 2 台特定伺服器。

一旦設定了適當的主域，你就可以增加所希望的任何數量的子域。你可能想要命名你的電腦為 **sales.xtera.com**，而另一台則被叫做 **support.xtera.com** 等等。這些工作可就不需要 NIC 的同意了，但是，如果你想要任何人都能實際地存取你的子域，那麼你最好將有關子域的資訊儘快地放到上級域內。在特定的情況下，關於 **sales.xtera.com** 和 **support.xtera.com** 的 IP 資訊必須放在 **xtera.com** 伺服器上。這一層次中的每台伺服器都包含了一個 DNS 資料庫，其入口被稱作 NS 記錄，每條這樣的記錄包含了域或子域的名字，此外還加上作為主域或者子域伺服器的主機的名字。在我們的例子中，我們將告訴根伺服器它能在我們的 DNS 伺服器上找到 **xtera.com** 及其全部子域的資訊，而這些資訊則位於 **dns1.xtera.com** 這台電腦上。

這樣，如果某大學用戶在指向你的最新子域的網頁上看見了一個 URL：**support.xtera.com**。然後她點選該 URL，於是她的本地 DNS 伺服器（很可能位於這所大學的某台電腦上）開始工作。首先，伺服器搜索它自己的 DNS 資料庫以轉換資訊，但是，因為它以前從來沒遇見過 **support.xtera.com**，所以伺服器沒有該域存在的記錄而且不能解析 IP 位址。不過，它的 DNS 資料庫包含了一個根伺服器的位址（所有的 DNS 伺服器必須設定該索引）。於是本地 DNS 伺服器就到 Internet 上查詢該根伺服器。根伺服器在其 DNS 資料庫裏查找 COM 頂級域，然後它用 NS 記錄回復該大學的 DNS 伺服器，告訴它可以從 **dns1.xtera.com** 處查詢到 **xtera.com** 的信息。於是大學的伺服器就從 **dns1.xtera.com** 獲得了 **support.xtera.com** 的對應 IP 位址。

6.6.1 SwiftDNS

如前所述，DNS 傳統容錯（DNS 輪詢）的一個問題是一旦某個伺服器出現故障，即使及時修改了 DNS 設定，還是要等待足夠的時間（刷新時間）才能發揮作用，在此期間保存了故障的伺服器位址的客戶電腦將不能正常存取伺服器。

AscenLink 在實現多重定址時使用獨有的 SwiftDNS 專利技術，保障客戶透過 DNS 取得正常狀態的 IP 位址。SwiftDNS 機制會根據線路的通斷狀況，智慧返回活動狀態的 IP 位址。當對外的廣域網線路正常時，AscenLink 會根據預先設定的比重值，輪流回答相應的 IP 位址，當某些廣域網線路故障時，AscenLink 會避免響應屬於這些廣域網線路的 IP 位址，以確保關鍵應用不會中斷。

為避免 DNS 緩衝 (Cache) 將失效線路的 IP 位址回應給用戶端，SwiftDNS 刷新機制會定期向內部 DNS 發出一刷新請求，確保返回 IP 記錄與線路狀況一致。

SwiftDNS 是如何工作的呢？

我們透過 SwiftDNS 的典型架構進行說明。如圖 6.9，只要在 AscenLink 中設定好 Multihoming，SwiftDNS 就會自動生效。

在上級 DNS 伺服器中為 xtera.com 加入兩條 NS 記錄，分別為 Primary 和 Secondary，指向 210.58.100.1 和 215.59.100.1。

區域網路內真正的 DNS 伺服器透過 Virtual Server 分別映射到公開網域 IP 位址 210.58.100.1 和 215.59.100.1。

區域網路內有 WEB 伺服器透過 Multihoming 分別對應公開網域 IP 位址 210.58.100.2 和 215.59.100.2，即擁有 2 個公開網域 IP 位址，同時設定 WAN1 的 weight(資料比重)為 1，WAN2 出口的 weight 為 2。

當 ISP1 和 ISP2 提供的線路都正常時，查詢 www.xtera.com 的工作會正常進行，會對 www.xtera.com 主機輪流回復 IP 為 210.58.100.2 和 215.59.100.2。而且用戶存取 Web 服務時，經由 210.58.100.2 和 215.59.100.2 流出的資料比例為 1：2。

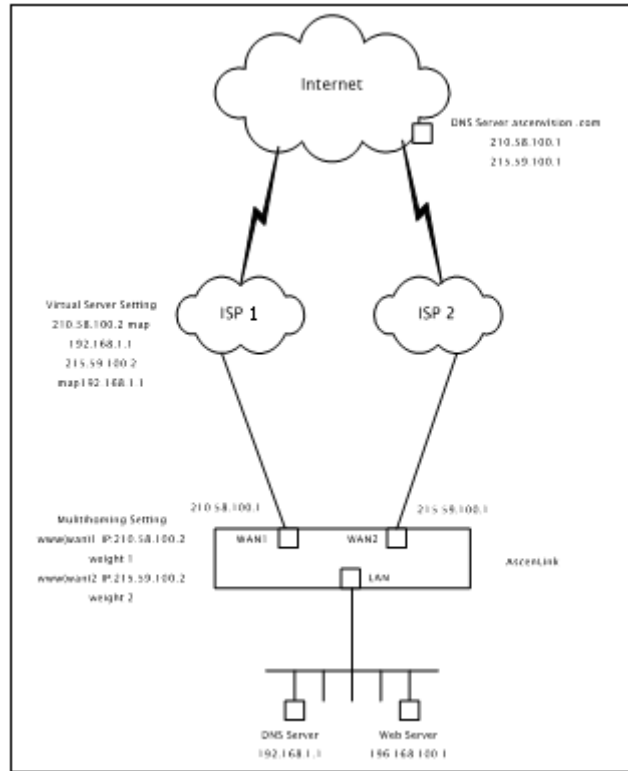


圖 6.9 Multihoming 設定圖

當 ISP1 中斷時，新的 DNS 查詢由於無法透過 210.58.100.1 去查詢 www.xtera.com 的 IP 位址，會自動選擇 215.59.100.1 線路，215.59.100.1 將查詢請求轉發給內部 DNS 伺服器 192.168.1.1，SwiftDNS 即根據網路現狀將 www.xtera.com 對應 215.59.100.2 的位址作回復。

6.7 HA 應用討論

6.7.1 HA 模式下的 firmware 更新方式

在 HA 模式下之 firmware update 並不同於單機方式下更新方式，請按照本說明更新 firmware，更新順序為：

1. 以 Administrator 帳號登入 AscenLink Master Web UI，進入 [System]→[Summary]，確定 peer 設備狀況正常。
2. 請點選[Synchronize Configuration]，確定 Slave 設備的 Config 與 Master 一樣。
3. 執行更新 firmware 動作，此動作可能會花上一段時間，請稍等待。
4. 確定 firmware 更新完成，即在更新動作完畢後 UI 所顯示為更新完成之字樣，若有任何錯誤，請勿關機，再次更新 firmware 直到完成為止。
5. 確定 Master 的 firmware 更新動作結束後，請直接關閉 Master 電源，並等待 Slave 接管網路成為 Master 主機。

註：即等到 Slave 發出一聲 “Beep” 響後。

6. 再次登入 AscenLink UI，確定 peer info 資料為 none，重複更新 firmware 動作更新 AscenLink 之 firmware。
7. 確定 firmware 更新完成，關閉電源。
8. 打開 Master 電源，等待一小段時間後(5 秒)，打開 Slave 電源。
9. 登入 AscenLink Master Web UI，進入 [System] →[Summary]，確定本機與 peer 之 firmware 為更新後版本。
10. 若有使用公開 IP 穿越或位於 DMZ 中的主機有網路異常狀況，請至[System] → [Diagnostic Tools] →[ARP Enforcement]點選 [Enforce] 以修復網路。

註：在上述更新過程中不可將 HA 連線分離。

若有任何異常狀況，表示 **firmware** 更新出現失敗，請把一台(任意)電源關閉，移除網線與 HA 連線，在與網路不相接的狀況下更新 **firmware**，待兩台皆以此方式更新 **firmware** 後，重新安裝至網路中。

在 HA 模式下所登入的設備必為 **Master**。

若在更新 **firmware** 過程中一直發生錯誤無法解決，請不要關閉電源並聯絡廠商。

6.7.2 HA 模式下復原至單機的操作方式

在 HA 模式下恢復至單機的模式請按照以下步驟操作：

1. 以 Administrator 帳號登入 AscenLinkMaster 的 WebUI，進入 [System] → [Summary]，點選 [Synchronize Configuration]，確定 Slave 設備的 Config 與 Master 一樣。
2. 將欲移除之 AscenLink 設備電源關閉，若直接移除 Master，須等到 Slave 接管後網路才會正常運作，移除 Slave 將不會對網路有任何影響。
3. 關閉電源後，才可將 HA 連結線移除。
4. 移除多餘的網路線與設備。
5. 若有使用公開 IP 穿越或位於 DMZ 中的主機有網路異常的狀況，請至[System] → [Diagnostic Tools] → [ARP Enforcement]點選 [Enforce] 以修復網路。

6.7.3 Slave 接管 Master 之原則

當 Master 因某些原因 (HA 連線線發生故障，關機，過於繁忙無法響應 Slave) 而無法正常運作的時候，Slave 會自動取代 Master，在 Slave 起始時可以聽見一聲 “Beep”。

取代行為本身為永久性的，即當原 Master 關機重開後，將變為 Slave，而非再次取代成為 Master。

若欲手動以 Slave 取代 Master，只須將 Master 電源關閉後開啓即可。

附錄目錄

附錄目錄	A-I
附錄 A.1 系統預設值	A-II
附錄 A.2 序列埠控制臺指令	A-V
附錄 A.3 AscenLink 軟體更新	A-X
附錄 A.4 Configuration File 備援	A-XII

附錄 A.1 系統預設值

在 Console 中輸入 `resetconfig` 或在網頁上點選 **Factory Default** 會對 AscenLink 進行還原到系統預設值的狀態，以下為 AscenLink 的系統預設值。Console 的帳號與密碼是不能更改的，帳號為 **Administrator**，密碼為 **ascenlink**，請注意大小寫的區別。

Web UI 的帳號與密碼會恢復到預設值，帳號/密碼為 **Administrator/1234**，**Monitor/5678**。

登入 WebUI 所使用的埠號會恢復到預設埠號 **443**。AscenLink 支援遠端 SSH 登入的管理方式，SSH 管理介面與 Console 的管理介面相同，而 SSH 的登入帳號與密碼和 Web UI 中的 **Administrator** 帳號/密碼相同。

WAN Link Health Detection 的預設值：

- 恢復到系統預設的 13 組偵測的主機
- Port Speed/Duplex Setting 的預設值
- 所有的 Port 恢復到 Auto 的狀態

Network Setting 的預設值：

Port 1 : WAN1

IP : 192.168.1.1

Netmask : 255.255.255.0

IP in DMZ 192.168.1.2~192.168.1.253

Default Gateway 192.168.1.254

DMZ at port 5

Port 2 : WAN2

IP : 192.168.2.1

Netmask : 255.255.255.0

IP in DMZ 192.168.2.2~192.168.2.253

Default Gateway 192.168.2.254

DMZ at port 5

Port 3 : WAN3

IP : 192.168.3.1

Netmask : 255.255.255.0

IP in DMZ 192.168.3.2~192.168.3.253

Default Gateway 192.168.3.254

DMZ at port 5

Port 4 : LAN

IP : 192.168.0.1

Netmask : 255.255.255.0

DHCP Server is off

Port 5 : DMZ

Domain Name Server, VLAN and Port Mapping, WAN/DMZ Subnet Setting 欄位皆
清空

Service 頁面的預設值：

Firewall : Default all pass

Persistent Routing : no Persistent Routing Rule

Auto Routing : By Downstream Traffic as default

Virtual Server : no Virtual Server

Inbound BM : no BM rule

Outbound BM : no BM rule

Cache : no redirection

Tunnel Routing : no tunnel

Multihome : Disabled

Internal DNS : Disabled

IP-Mac Mapping : no mapping

Log/Control 頁面的所有設定值皆清空

附錄 A.2 序列埠控制臺指令

以下介紹序列埠控制臺指令參照表。用戶名：Administrator /密碼：ascenlink，該值不可更改。

help

(說明) 顯示此說明

輸入 help [Command] 可顯示 Command 的詳細使用方式。

Ex: help logout [Enter]會說明 logout 指令的用途與使用方式。

arping

(ARP 詢問) 查詢某個 IP 所對應的 MAC 位址

輸入 arping [Host] [Link] [Index] [Enter]可以查詢某個 IP 所對應的 MAC 位址，Host 為要查詢的主機 IP 或 domain name，Link 可填入使用的介面有 WAN/LAN/DMZ 三種，若要查詢 WAN 介面時須指定 WAN port number。

Ex: arping 192.168.2.100 LAN [Enter]指定從 LAN port 送出 arp 封包去查詢 192.168.2.100 主機的 MAC 位址。

註：若使用 domain name 來 arping 時，須在 web UI 上的[System]->[Network Setting]->[DNS Server]中先行指定 DNS Server。

關於 ARP 相關 error message 請參閱相關檔。

enforcearp

(ARP 重整) 強迫 AscenLink 周圍的主機或設備更新 ARP table。

輸入 enforcearp [Enter]後，系統會送出一些 arp 封包以更新周圍的主機或設備的 ARP table，通常當部分 DMZ 的設備在第一次安裝 AscenLink 後不能正確與 Internet 連線時才須使用。

Ex: enforcearp [Enter]

logout

(註銷) 從控制臺中註銷。

輸入 `logout[Enter]`可從控制臺中登出，系統會回應確認，輸入 `y[Enter]`以註銷控制臺或輸入 `n[Enter]`以返回控制臺。

Ex: `logout[Enter]`

`y[Enter]`以登出控制臺

ping

(ping) 用以偵測網路狀況

輸入 `ping [Host] [Link] [Index] [Enter]`可以 ping 某指定主機以檢測目前指定 WAN port 的網路狀況，Host 為要 ping 的主機 IP 或 domain name，Link 可填入使用的介面有 WAN/LAN/DMZ 三種，若 ping WAN 介面時須指定 WAN port number。

Ex: `ping www.hinet.net wan 1 [Enter]`指定從 WAN port 1 送出 ping 封包到 `www.hinet.net`。

註：若使用 domain name 來 ping 時，須在 web UI 上的[System]->[Network Setting]->[DNS Server]中先行指定 DNS Server。

關於 ICMP 相關 error message 請參閱相關檔。

reboot

(重新開機) 將 AscenLink 重新開機。

輸入 `reboot[Enter]`可以直接將 AscenLink 重新開機，輸入 `reboot -t Time [Enter]`可以指定 AscenLink 在 Time 秒後重新開機。

Ex: `reboot -t 5[Enter]`可指定 AscenLink 在 5 秒後重新開機。

resetconfig

(還原出廠設定狀態) 清除 AscenLink 上所有的設定恢復到出廠預設值，並重新開機。

註：該命令不能將密碼恢復成出廠預設值。

輸入 `resetconfig[Enter]`後，系統會回應確認，輸入 `y[Enter]`以繼續執行初始動作，或輸入 `n[Enter]`以返回控制臺。

Ex: `resetconfig[Enter] y[Enter]`可將系統還原至預設值。

resetpasswd

(還原密碼設定) 將 AscenLink 上的 Administrator 與 Monitor 帳號的密碼還原成出廠預設值。

輸入 `resetpasswd [Enter]`後，系統會回應確認，輸入 `y [Enter]`以繼續執行初始動作，或輸入 `n [Enter]`以返回控制臺。

Ex: `resetpasswd [Enter]`

`y [Enter]` 可將帳號密碼還原至預設值。

disablefw

(停止防火牆功能) 將 AscenLink 上的防火牆功能停止。

輸入 `disablefw [Enter]`後，系統會回應確認，輸入 `y [Enter]`以停止防火牆功能，或輸入 `n [Enter]`以返回控制臺。

Ex: `disablefw [Enter]`

`y [Enter]` 可將防火牆功能停止。

setupport

(網路介面傳輸模式設定) 設定 AscenLink 上網路介面的傳輸模式。

輸入 `setupport show [Enter]`可顯示所有網路介面目前的傳輸模式。

輸入 `setupport change [Index] auto [Enter]`可修改指定之網路介面(Index)設定至自動模式。

輸入 `setupport change [Index] [Speed] [Mode] [Enter]`可修改指定之網路介面(Index)設定特定的模式。

Index: 1, 2, 3,....

Speed: 10, 100, 1000

Mode: half, full

Ex: setupport show [Enter]

setupport change 1 auto [Enter]

setupport change 2 100 full [Enter]

註：並非所有 port 都有支援 1000 的速度，只有部分介面有支援。Fiber 介面不支援手動設定。
Index 對等於 port1, port2, port3, ... ，依機型不同數量也不同。

shownetwork

(顯示目前網路組態) 顯示目前 AscenLink 上的各個 WAN link 的組態。

輸入 shownetwork [Enter]後會顯示目前本 AscenLink 上的資料，包括 WAN Type, Bandwidth, IP(s) On Local/WAN/DMZ, Netmask, Gateway, WAN/DMZ Port。

Ex: shownetwork [Enter]。

註：在序列埠控制臺中只能顯示目前的組態資料，若欲修改請使用 ASCENLINK 所提供的 Web UI。

Sysinfo

(系統訊息) 顯示目前 AscenLink 上的 CPU 及記憶體訊息

輸入 sysinfo [Enter]後會顯示目前本 AscenLink 上 CPU、Memory、Disk Space 的使用狀況。

Ex: sysinfo [Enter]。

traceroute

(網路尋徑) 顯示封包從指定 port 到目的地主機中間經由的路由。

輸入 `traceroute [Host] [Type] [Index] [Enter]`可指定從 WAN port 到目標主機的路由，Host 為目標主機 IP 或 domain name，Type 可填入使用的介面有 WAN/LAN/DMZ 三種，若使用 WAN 介面時須指定 WAN link。

Ex: `traceroute www.hinet.net wan 1 [Enter]`將回傳由 WAN link1 到 `www.hinet.net` 的中間所經由的路由。

註:若使用 domain name 來 ping 時，須在 Web UI 上的[System]-> [Network Setting]-> [DNS Server]中先行指定 DNS Server。

附錄 A.3 AscenLink 軟體更新

AscenLink 軟體更新步驟：

1. 取得更新用的 **firmware** 檔案或光碟。
2. 以 **Administrator** 帳號登入 **AscenLink** 的 **WebUI**，進入 **[System]** → **[Administration]**。
3. 點選 **Update** 以進入更新 **firmware** 的畫面。
4. 點選**[Browse...]**或**[流覽...]**，選擇更新用的 **image**，點選**[Upload]**。
5. 等到出現 **Update succeeded** 字樣表示更新軟體成功，請關閉電源重新開機以使用新版本的 **AscenLink** 軟體，或點選**[Maintenance]**欄位下的**[Reboot]**亦可。

註：更新過程須花上一段時間，請耐心等待，在更新期間中請勿關閉電源，或反復點選 **[Upload]**。

若發生錯誤，請參照以下的錯誤訊息：

- **General error** - 若重新更新一樣發生這類錯誤，與廠商聯絡。
- **Invalid update file** - 更新檔案發生錯誤，請檢查是否上傳正確檔案。
- **MD5 checksum error** - 請檢查是否軟體 **image** 檔案發生損毀。
- **Incompatible version/build** - 軟體版本與現有的不相容。
- **Incompatible model/feature** - 軟體版本與現有的 **AscenLink** 型號不相符合。
- **Incompatible platform** -軟體版本與現有的 **AscenLink** 平臺不相符合。
- **Incompatible region** - 軟體版本與現有的 **AscenLink** 型號不相符合。

- **Update error** - 注意!!若重新更新一樣發生這類錯誤，請勿關機，直接與廠商聯絡。
- **Unknown error** - 發生這類錯誤，與廠商聯絡。

HA 模式下的更新方式請參照第四部份第三章的資料。軟體更新期間並不會影響 AscenLink 的正常操作。建議在更新軟體前先將 **Config** 檔案備援。

附錄 A.4 Configuration File 備援

Configuration File 備援步驟：

1. 以 Administrator 帳號登入 AscenLink 的 Web UI。
2. 進入[System]→ [Administration] 點選[Configuration File] → [Save]將 Config File 備援至你的電腦中。
3. 若欲回復先前備援的 Configuration，請點[Configuration File] → [Restore]，點選[Browse...]或[流覽...]，選擇欲上傳的 Configuration File 後點選[Upload]。
4. 重新啟動 AscenLink 以完成更新程式。
5. 等待出現 Update succeeded 字樣以完成 upload。

註：在上傳期間中請勿關閉電源，或反復點選[Upload]

若發生錯誤請參照以下的錯誤訊息處理：

- 所上傳的設定文件的總下載帶寬大於目前機型的容量。
- 所上傳的設定文件的總上傳帶寬大於目前機型的容量。
- 所上傳的設定文件的總 port 數大於目前機型的容量。
- 所上傳的設定文件的機型不支持 VLAN 設定。
- 所上傳的設定文件的支援 WAN 數大於目前機型的容量。
- 版本不相容。

註：

1. Configuration File 本身為 binary 檔案，請勿手動修改檔案內容，以免造成不可預期的錯誤。
2. AscenLink 不同型號間的 Configuration File 不能通用。
3. 建議更新完軟體後請重新備援 Configuration File。

