

在RV042、RV042G和RV082 VPN路由器上設定雙廣域網連線

目標

廣域網(WAN)是由多個LAN組成的網路。RV路由器支援雙WAN功能，允許同時使用兩個WAN埠。WAN連線還可以配置為故障切換設定，以確保連續的Internet連線。為了進一步最佳化雙WAN功能，RV路由器使用協定繫結。協定繫結允許通過特定WAN埠傳送特定流量。

本文解釋如何在RV042、RV042G和RV082 VPN路由器上配置雙WAN。

適用裝置

- RV042
- RV042G
- RV082

軟體版本

- v4.2.1.02

設定雙WAN

步驟 1. 登入到路由器配置實用程式以選擇System Management > Dual WAN。Dual WAN頁面隨即開啟：



Dual WAN

Load Balance

Smart Link Backup : Primary WAN WAN1 (Specify which WAN is Primary , the other one will be backup)

 Load Balance (Auto Mode)

Interface Setting

Interface	Mode	Configuration
WAN1	Smart Link Backup	
WAN2	Smart Link Backup	

負載平衡



Dual WAN

Load Balance

Smart Link Backup : Primary WAN WAN1 (Specify which WAN is Primary , the other one will be backup)

 Load Balance (Auto Mode)

Interface Setting

Interface	Mode	Configuration
WAN1	Smart Link Backup	
WAN2	Smart Link Backup	

步驟 1. 點選適當的WAN模式以管理WAN連線。

·智慧鏈路備份 — 此選項可確保RV路由器上的連續WAN連線。如果主WAN失去連線，則由備用WAN接管。從Primary WAN下拉選單中選擇指定為主要WAN的所需WAN。

·負載均衡 — 同時使用兩個WAN連線。這會增加RV路由器的可用頻寬。

步驟 2. 按一下「Save」以儲存設定。

編輯WAN

注意：如果您想瞭解有關最大頻寬管理的詳細資訊，請參閱RV042、RV042G和RV016 VPN路由器上的速率控制頻寬管理(有關速率控制型別的頻寬)和RV042G路由器上的優先順序頻寬管理(有關優先順序型別的頻寬)。



Dual WAN

Load Balance

Smart Link Backup : Primary WAN WAN1 (Specify which WAN is Primary , the other one will be backup)

Load Balance (Auto Mode)

Interface Setting

Interface	Mode	Configuration
WAN1	Smart Link Backup	
WAN2	Smart Link Backup	

步驟 1. 點選Configuration按鈕編輯適當的WAN介面以編輯Dual WAN設定。Dual WAN頁面隨即開啟：

Dual WAN

The Max Bandwidth Provided by ISP

Interface : WAN1

Upstream : Kbit/Sec

Downstream : Kbit/Sec

Network Service Detection

Enable Network Service Detection

Retry count :

Retry timeout : second

When Fail :

Default Gateway

ISP Host

Remote Host

DNS Lookup Host

Protocol Binding

Service :

Source IP : to

Destination IP : to

Interface :

Enable :

有關上述視窗的資訊，請參閱以下子部分。

- [WAN頻寬](#) — 如何為指定的WAN介面配置頻寬。
- [網路服務檢測](#) — 如何執行ping測試以檢測WAN連線。
- [管理協定繫結](#) — 如何為指定的WAN介面配置協定繫結。協定繫結確定特定流量使用哪個WAN介面。

WAN頻寬

Dual WAN

The Max Bandwidth Provided by ISP

Interface :	WAN1	
Upstream :	<input type="text" value="510"/>	Kbit/Sec
Downstream :	<input type="text" value="500"/>	Kbit/Sec

Network Service Detection

Enable Network Service Detection

Retry count :

Retry timeout : second

When Fail : ▼

Default Gateway

ISP Host

Remote Host

DNS Lookup Host

Interface欄位顯示指定WAN的介面。

步驟 1.在Upstream欄位中輸入最大上傳頻寬 (以千位每秒為單位)。上行頻寬是網路將資料傳送到Internet服務提供商(ISP)的最大頻寬。預設上游頻寬為512 kbit/sec。

步驟 2.在Downstream欄位中輸入最大下載頻寬 (以千位每秒為單位)。下游頻寬是Internet服務提供商(ISP)將資料傳送到網路的最大頻寬。預設下游頻寬為512 kbit/sec。

步驟 3.按一下「Save」以儲存設定。

網路服務偵測

Dual WAN

The Max Bandwidth Provided by ISP

Interface : WAN1

Upstream : Kbit/Sec

Downstream : Kbit/Sec

Network Service Detection

Enable Network Service Detection

Retry count :

Retry timeout : second

When Fail : ▼

Default Gateway

ISP Host

Remote Host

DNS Lookup Host

步驟 1. 選中Enable Network Service Detection以允許RV路由器檢測連線。這是通過對配置的IP地址執行ping測試後執行的。

步驟 2. 在Retry Count欄位中輸入RV路由器嘗試對配置的IP地址執行ping的次數。預設值為5。

步驟 3. 在Retry Timeout欄位中輸入RV路由器在ping之間等待的時間（以秒為單位）。預設時間為30秒。

Dual WAN

The Max Bandwidth Provided by ISP

Interface : WAN1

Upstream : 510 Kbit/Sec

Downstream : 500 Kbit/Sec

Network Service Detection

Enable Network Service Detection

Retry count : 3

Retry timeout : 25 second

When Fail :

- Default Gateway
- ISP Host
- Remote Host
- DNS Lookup Host

Keep System Log and Remove the Connection
Generate the Error Condition in the System Log
Keep System Log and Remove the Connection

步驟 4. 從When Fail下拉選單中，選擇當ping測試失敗時要執行的操作。

·保留系統日誌並刪除連線 — 發生故障切換，且備份WAN介面進行控制。恢復與主WAN的連線後，主WAN將恢復控制。

·在系統日誌中生成錯誤條件 — 系統日誌中記錄故障，且不會發生故障切換。

Dual WAN

The Max Bandwidth Provided by ISP

Interface : WAN1

Upstream : 510 Kbit/Sec

Downstream : 500 Kbit/Sec

Network Service Detection

Enable Network Service Detection

Retry count : 3

Retry timeout : 25 second

When Fail : Keep System Log and Remove the Connection

Default Gateway

ISP Host

Remote Host 192.168.1.2

DNS Lookup Host example.com

步驟 5.選中要為ping測試執行ping操作的位置的覈取方塊。

- 預設網關 — RV320 ping配置的預設網關。
- ISP主機 — 輸入ISP主機IP以供RV路由器執行ping操作。
- 遠端主機 — 輸入遠端主機的IP地址以供RV路由器執行ping操作。
- DNS Lookup Host — 輸入路由器要執行ping的主機名或域名。

步驟 6.按一下「Save」。

管理協定繫結

協定繫結是一種功能，用於通過特定WAN介面傳送特定流量。任何與流量型別匹配且從已配置的源IP地址傳送到已配置的目的地址的流量都通過協定繫結規則的已配置WAN介面傳送。只有在雙WAN模式配置為負載均衡時，協定繫結才可用。

Protocol Binding

Service : HTTPS [TCP/443~443]

Source IP :

Destination IP :

Interface :

Enable :

The dropdown menu contains the following items (from top to bottom):

- HTTPS [TCP/443~443]
- All Traffic [TCP&UDP/1~65535]
- DNS [UDP/53~53]
- FTP [TCP/21~21]
- HTTP [TCP/80~80]
- HTTP Secondary [TCP/8080~8080]
- HTTPS [TCP/443~443]
- HTTPS Secondary [TCP/8443~8443]
- TFTP [UDP/69~69]
- IMAP [TCP/143~143]
- NNTP [TCP/119~119]
- POP3 [TCP/110~110]
- SNMP [UDP/161~161]
- SMTP [TCP/25~25]
- TELNET [TCP/23~23]
- TELNET Secondary [TCP/8023~8023]
- TELNET SSL [TCP/992~992]
- DHCP [UDP/67~67]
- L2TP [UDP/1701~1701]
- PPTP [TCP/1723~1723]
- IPSec [UDP/500~500]

步驟 1. 從Service下拉選單中，選擇應用於協定繫結的流量型別。

Protocol Binding

Service : HTTP [TCP/80~80]

Source IP : 192.168.1.1 to 192.168.1.10

Destination IP : 192.168.1.11 to 192.168.1.15

Interface : WAN1

Enable :

步驟 2.在Source IP欄位中輸入應用於協定繫結的源IP地址。

步驟 3.在Destination IP欄位中輸入應用於協定繫結的目標IP地址。

步驟 4.從Interface下拉選單中，選擇流量通過的介面。

步驟 5.選中Enable欄位中的覈取方塊以啟用協定繫結。

注意：按一下Service Management新增服務。要詳細瞭解如何新增服務，請參閱服務管理部分。

步驟 6.按一下Add to List以新增到表中。

Protocol Binding

Service : HTTP [TCP/80~80]

Source IP : to

Destination IP : to

Interface : WAN1

Enable :

HTTP [TCP/80~80]->192.168.1.1~192.168.1.10(192.168.1.11~192.168.1.15)WAN1 [Enabled]

步驟 7.按一下「Save」。協定繫結設定已配置。

編輯協定繫結

Protocol Binding

Service : HTTP [TCP/80~80]

Source IP : 192.168.1.5 to 192.168.1.10

Destination IP : 192.168.1.11 to 192.168.1.15

Interface : WAN1

Enable :

HTTP [TCP/80~80]->192.168.1.1~192.168.1.10(192.168.1.11~192.168.1.15)WAN1 [Enabled]

步驟 1.從表中按一下要編輯的協定繫結並更改必要的資訊。要詳細瞭解如何更新，請參閱新增協定繫結部分。

步驟 2.按一下Update以編輯協定繫結。

步驟 3.按一下「Save」。協定繫結配置已更新。

刪除協定繫結

Protocol Binding

Service : HTTP [TCP/80~80]

Source IP : 192.168.1.5 to 192.168.1.10

Destination IP : 192.168.1.11 to 192.168.1.15

Interface : WAN1

Enable :

HTTP [TCP/80~80]->192.168.1.1~192.168.1.10(192.168.1.11~192.168.1.15)WAN1 [Enabled]

步驟 1.按一下要從表中刪除的協定繫結。

步驟 2.按一下「協定繫結表」中的「刪除」。

步驟 3.按一下「Save」。協定繫結配置即被刪除。

服務管理

Protocol Binding

Service : HTTP [TCP/80~80] ▼

Service Management

Source IP : to

Destination IP : to

Interface : WAN1 ▼

Enable :

Move Up Add to list

HTTP [TCP/80~80]->192.168.1.5~192.168.1.10(192.168.1.11~192.168.1.15)WAN1 [Enabled]

Delete Add New

Save Cancel

步驟 1.按一下「Service Management」。出現Service Management視窗。

Service Name :

Protocol :

Port Range :

 to

Add to list

All Traffic [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]

Delete

Add New

Service Name :

Protocol :

Port Range :

Add to list

All Traffic [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]

Delete

Add New

步驟 2. 在Service Name欄位中輸入服務的名稱。

步驟 3. 從protocol下拉選單中，選擇服務使用的協定。

- TCP — 服務轉發傳輸控制協定(TCP)資料包。
- UDP — 服務轉發使用者資料包協定(UDP)資料包。
- IPv6 — 服務轉發所有IPv6流量。

Service Name :

Protocol :

Port Range : to

- All Traffic [TCP&UDP/1~65535]
- DNS [UDP/53~53]
- FTP [TCP/21~21]
- HTTP [TCP/80~80]
- HTTP Secondary [TCP/8080~8080]
- HTTPS [TCP/443~443]
- HTTPS Secondary [TCP/8443~8443]
- TFTP [UDP/69~69]
- IMAP [TCP/143~143]
- NNTP [TCP/119~119]
- POP3 [TCP/110~110]
- SNMP [UDP/161~161]

步驟 4. 如果協定是TCP或UDP，請在Port Range欄位中輸入為該服務保留的埠範圍。

步驟 5. 按一下「Add to List」。該服務將儲存到「服務管理表」中。

步驟6. (可選) 點選要編輯的服務，編輯必要資訊，然後點選儲存。要瞭解有關編輯的詳細資訊，請按照前面的步驟操作。

步驟7. (可選) 點選要刪除的服務，然後點選Delete。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。