

RV042, RV042G 및 RV082 VPN Router에서 듀얼 WAN 연결 설정

목표

WAN(Wide Area Network)은 여러 LAN으로 구성된 네트워크입니다. RV 라우터는 두 WAN 포트를 동시에 사용할 수 있는 듀얼 WAN 기능을 지원합니다. 또한 WAN 연결을 장애 조치 설정으로 구성하여 지속적인 인터넷 연결을 보장할 수 있습니다. 듀얼 WAN 기능을 더욱 최적화하기 위해 RV 라우터는 프로토콜 바인딩을 사용합니다. 프로토콜 바인딩을 사용하면 특정 WAN 포트를 통해 특정 트래픽을 전송할 수 있습니다.

이 문서에서는 RV042, RV042G 및 RV082 VPN Router에서 듀얼 WAN을 구성하는 방법에 대해 설명합니다.

적용 가능한 디바이스

- RV042
- RV042G
- RV082

소프트웨어 버전

- v4.2.1.02

듀얼 WAN 설정

1단계. Router Configuration Utility에 로그인하여 System Management(시스템 관리) > Dual WAN을 선택합니다. Dual WAN 페이지가 열립니다.

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	

로드 밸런스

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	

1단계. WAN 연결을 관리하려면 적절한 WAN 모드를 클릭합니다.

- Smart Link Backup — 이 옵션은 RV 라우터에서 WAN 연결을 지속적으로 보장합니다. 기본 WAN의 연결이 끊기면 백업 WAN이 연결을 넘겨받습니다. Primary WAN(기본 WAN) 드롭다운 목록에서 기본 WAN으로 지정되는 원하는 WAN을 선택합니다.

- 로드 밸런싱 — 두 WAN 연결을 동시에 사용합니다. 이렇게 하면 RV 라우터의 가용 대역폭이 늘어납니다.

2단계. Save(저장)를 클릭하여 설정을 저장합니다.

WAN 수정

참고: 최대 대역폭 관리에 대해 자세히 알아보려면 속도 제어 유형 대역폭에 대해서는 RV042, RV042G 및 RV016 VPN Router의 Rate Control Bandwidth Management를 참조하고, 우선 순위 유형 대역폭에 대해서는 RV042 및 RV042G의 Priority Bandwidth Management를 참조하십시오.

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	

1단계. Configuration(컨피그레이션) 버튼을 클릭하여 듀얼 WAN 설정을 편집하는 데 적합한 WAN 인터페이스를 편집합니다. Dual WAN 페이지가 열립니다.

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 :

위 창에 대한 자세한 내용은 다음 하위 섹션을 참조하십시오.

- [WAN 대역폭](#) — 지정된 WAN 인터페이스에 대한 대역폭을 구성하는 방법.
- [네트워크 서비스 탐지](#) — WAN 연결을 탐지하기 위해 ping 테스트를 수행하는 방법
- [프로토콜 바인딩](#) 관리 — 지정된 WAN 인터페이스에 대한 프로토콜 바인딩을 구성하는 방법. 프로토콜 바인딩은 특정 트래픽에 어떤 WAN 인터페이스가 사용되는지를 결정합니다.

WAN 대역폭

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 필드는 지정된 WAN의 인터페이스를 표시합니다.

1단계. Upstream(업스트림) 필드에 초당 최대 업로드 대역폭을 입력합니다. 업스트림 대역폭은 네트워크가 ISP(인터넷 서비스 공급자)에 데이터를 전송하는 최대 대역폭입니다. 기본 업스트림 대역폭은 512kbit/s입니다.

2단계. Downstream(다운스트림) 필드에 초당 최대 다운로드 대역폭을 입력합니다. 다운스트림 대역폭은 ISP(인터넷 서비스 공급자)가 네트워크로 데이터를 전송하는 최대 대역폭입니다. 기본 다운스트림 대역폭은 512kbit/s입니다.

3단계. Save(저장)를 클릭하여 설정을 저장합니다.

네트워크 서비스 탐지

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

DNS Lookup Host

1단계. RV 라우터가 연결을 탐지하도록 허용하려면 Enable Network Service Detection(네트워크 서비스 탐지 활성화)을 선택합니다. 이는 구성된 IP 주소에 대한 ping 테스트를 통해 수행됩니다.

2단계. RV 라우터가 구성된 IP 주소를 ping하려는 횟수를 Retry Count 필드에 입력합니다. 기본값은 5입니다.

3단계. Retry Timeout 필드에 RV 라우터가 ping 사이에 대기하는 시간을 초 단위로 입력합니다. 기본 시간은 30초입니다.



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

4단계. When Fail(실패 시) 드롭다운 목록에서 ping 테스트가 실패할 때 수행할 작업을 선택합니다.

· Keep System Log and Remove the Connection — 페일오버가 발생하며 백업 WAN 인터페이스가 제어를 수행합니다. 기본 WAN에 대한 연결이 복원되면 기본 WAN이 제어를 다시 시작합니다.

· 시스템 로그에 오류 상태 생성 — 시스템 로그에 오류가 기록되고 장애 조치가 발생하지 않습니다.

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

5단계. ping 테스트를 위해 ping할 위치의 확인란을 선택합니다.

- Default Gateway(기본 게이트웨이) — 구성된 기본 게이트웨이로 RV320이 ping합니다.
- ISP Host — RV 라우터가 ping할 ISP 호스트의 IP를 입력합니다.
- Remote Host — RV 라우터가 ping할 원격 호스트의 IP를 입력합니다.
- DNS 조회 호스트 — ping할 라우터의 호스트 이름 또는 도메인 이름을 입력합니다.

6단계. 저장을 클릭합니다.

프로토콜 바인딩 관리

프로토콜 바인딩은 특정 WAN 인터페이스를 통해 특정 트래픽을 전송하는 데 사용되는 기능입니다. 트래픽 유형과 일치하며 구성된 소스 IP 주소에서 구성된 목적지 주소로 전송되는 모든 트래픽은 프로토콜 바인딩 규칙의 구성된 WAN 인터페이스를 통해 전송됩니다. 프로토콜 바인딩은 듀얼 WAN 모드가 로드 밸런스로 구성된 경우에만 사용할 수 있습니다.

The screenshot shows the 'Protocol Binding' configuration window. The 'Service' dropdown menu is open, displaying a list of protocols and their port ranges. The selected item is 'HTTPS [TCP/443~443]', which is highlighted in blue. The dropdown menu is enclosed in a red rectangular box. Other visible elements include 'Source IP', 'Destination IP', 'Interface', and 'Enable' fields, along with buttons for 'Move Up', 'Add to list', 'Delete', 'Add New', 'Save', and 'Cancel'.

Service	Port Range
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

1단계. Service(서비스) 드롭다운 목록에서 프로토콜 바인딩에 적용되는 트래픽의 유형을 선택합니다.

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 :

2단계. 프로토콜 바인딩에 적용되는 소스 IP 주소를 Source IP 필드에 입력합니다.

3단계. Destination IP(대상 IP) 필드에 프로토콜 바인딩에 적용되는 대상 IP 주소를 입력합니다.

4단계. Interface 드롭다운 목록에서 트래픽이 통과하는 인터페이스를 선택합니다.

5단계. 프로토콜 바인딩을 활성화하려면 Enable 필드의 확인란을 선택합니다.

참고: 서비스를 추가하려면 서비스 관리를 클릭합니다. 서비스 추가 방법에 대한 자세한 내용은 서비스 관리 섹션을 참조하십시오.

6단계. 테이블에 추가하려면 Add to List를 클릭합니다.

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]

7단계. 저장을 클릭합니다. 프로토콜 바인딩 설정이 구성됩니다.

프로토콜 바인딩 편집

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]

1단계. 테이블에서 수정할 프로토콜 바인딩을 클릭하고 필요한 정보를 변경합니다. 업데이트 방법에 대한 자세한 내용은 프로토콜 바인딩 추가 섹션을 참조하십시오.

2단계. 프로토콜 바인딩을 수정하려면 Update를 클릭합니다.

3단계. 저장을 클릭합니다. 프로토콜 바인딩 컨피그레이션이 업데이트됩니다.

프로토콜 바인딩 삭제

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]

1단계. 테이블에서 삭제할 프로토콜 바인딩을 클릭합니다.

2단계. 프로토콜 바인딩 테이블에서 삭제를 클릭합니다.

3단계. 저장을 클릭합니다. 프로토콜 바인딩 컨피그레이션이 삭제됩니다.

서비스 관리

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

1단계. Service Management를 클릭합니다. Service Management 창이 나타납니다.

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

2단계. Service Name(서비스 이름) 필드에 서비스 이름을 입력합니다.

3단계. 프로토콜 드롭다운 목록에서 서비스가 사용하는 프로토콜을 선택합니다.

- TCP — 서비스에서 TCP(Transmission Control Protocol) 패킷을 전달합니다.
- UDP — 서비스에서 UDP(User Datagram Protocol) 패킷을 전달합니다.
- IPv6 — 서비스에서 모든 IPv6 트래픽을 전달합니다.

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]

4단계. 프로토콜이 TCP 또는 UDP인 경우 Port Range(포트 범위) 필드에 서비스에 대해 예약된 포트 범위를 입력합니다.

5단계. 목록에 추가를 클릭합니다. 서비스가 서비스 관리 테이블에 저장됩니다.

6단계. (선택 사항) 편집할 서비스를 클릭하고 필요한 정보를 편집한 후 Save(저장)를 클릭합니다. 편집 방법에 대해 자세히 알아보려면 이전 단계를 수행하십시오.

7단계. 삭제할 서비스를 클릭하고 Delete(삭제)를 클릭합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.