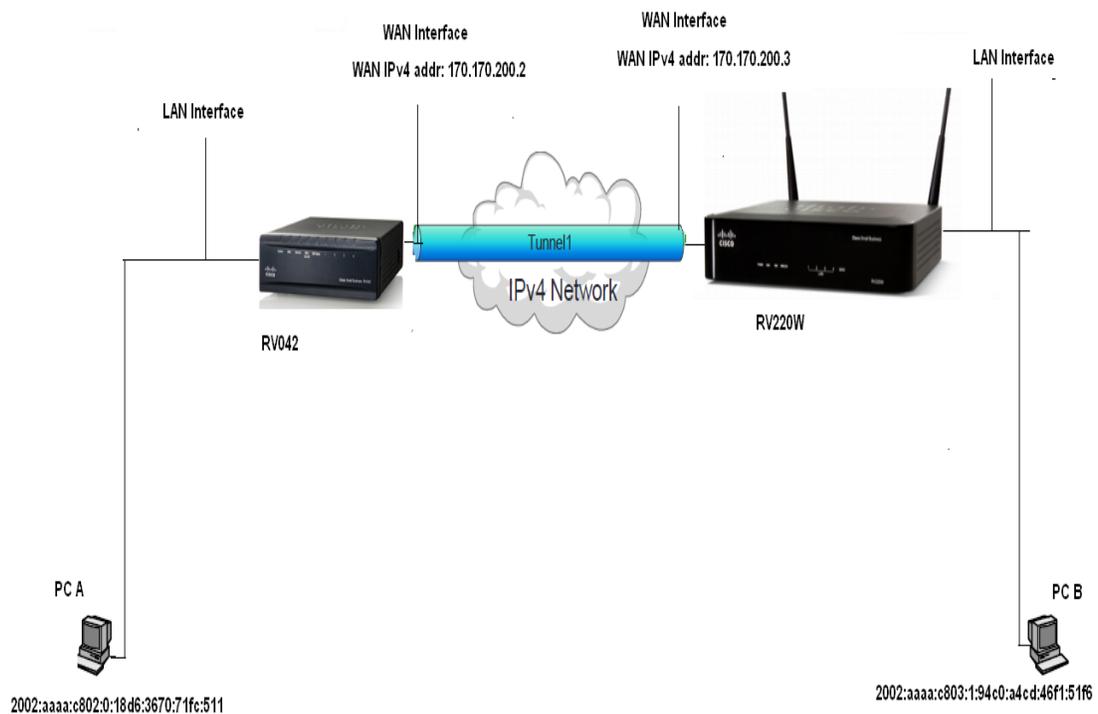


Setting up a 6to4 tunnel Between a Cisco RV0xx Series VPN Router and a Cisco RV220W Wireless Network Security Firewall

The document below is designed to assist in setting up a 6to4 tunnel between a Cisco RV0xx Series VPN Router and a Cisco RV220W Wireless Network Security Firewall.

This application note is accurate for the following firmware versions:

- RV220W 1.0.2.x
- RV0xx 4.0.2.08



In the above sample configuration PC-A is connected to the RV042 and PC-B is connected to a RV220W communicating over the 6to4 tunnel. Follow the procedures in this application note to set the above configuration:

On RV042:

Step 1. On the **Setup->Network** page, **IP Mode** section, select **Dual-Stack IP**. Click **Save** to save your settings.

The screenshot shows the Cisco RV042 configuration interface. The left sidebar lists various setup options, with 'Network' selected. The main content area is titled 'Network' and contains the following fields:

- Host Name : routerd886ec (Required by some ISPs)
- Domain Name : routerd886ec.com (Required by some ISPs)

The **IP Mode** section contains a table with three columns: Mode, WAN, and LAN.

Mode	WAN	LAN
<input type="radio"/> IPv4 Only	IPv4	IPv4
<input checked="" type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

Below the table, there are tabs for 'IPv4' and 'IPv6'. The 'LAN Setting' section includes:

- MAC Address : 68:EF:BD:D8:86:EC
- Device IP Address : 192.168.1.1
- Subnet Mask : 255.255.255.0
- Multiple Subnet : Enable

An 'Add/Edit' button is located at the bottom right of the LAN Setting section.

Step 2. On the **Setup->IPv6 Transition** page, check the **Enable 6to4 Tunnel** box. Click **Save** to save your settings.

The screenshot shows the Cisco RV042 configuration interface for the 'IPv6 Transition' page. The left sidebar lists various setup options, with 'IPv6 Transition' selected. The main content area is titled 'IPv6 Transition' and contains the following field:

- Enable 6to4 Tunnel

At the bottom of the page, there are 'Save' and 'Cancel' buttons.

Step 3. On the **DHCP->Router Advertisement** page, enter the following settings:

- **RA Flags:** Check the **Managed** box.
- Click **Save** to save the settings.

Small Business
CISCO RV042 10/100 4-Port VPN Router

System Summary

- Setup
- DHCP**
 - DHCP Setup
 - DHCP Status
 - Router Advertisement**
- System Management
- Port Management
- Firewall
- Cisco ProtectLinkWeb
- VPN
- Log
- Wizard

Router Advertisement

Enable Router Advertisement

Prefix : 2002:aaaa:c802::/64

Advertisement Mode : Unsolicited Multicast

Advertisement Interval : 30 seconds

RA Flags : Managed Other

Router Preference : High

MTU : 1500

Router Lifetime : 3600 seconds

Save Cancel

© 2010 Cisco Systems, Inc. All rights reserved.

Step 4. Confirm that your IPv6 devices acquire 6to4 (2002:WAN IP in HEX ::) prefixes for stateless auto-configuration.

Note: Initially when setting up tunneling, it is advisable to disable the firewall on the RV042. (On the Firewall->General page, choose **Disable**.)

Step 5. After the 6to4 setup is complete and tested, enable firewall and create access rules to allow tunneling traffic. Refer to the following example:

Small Business
CISCO RV042 10/100 4-Port VPN Router

System Summary

- Setup
- DHCP
- System Management
- Port Management
- Firewall**
 - General
 - Access Rules**
 - Content Filter
- Cisco ProtectLinkWeb
- VPN
- Log
- Wizard

Access Rules

Services

Action : Allow

Service : All Traffic [TCP&UDP/1-65535]

Service Management

Log : Log packets match this rule

Source Interface : WAN 1

Source IP : Single 170.170.200.3

Destination IP : Single 170.170.200.2

Scheduling

Time : Always

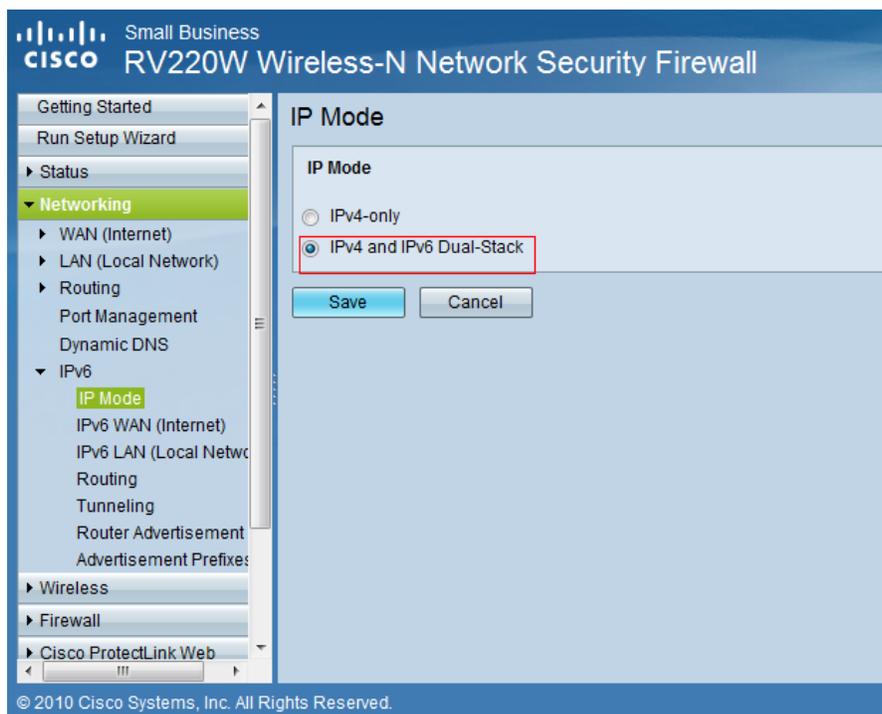
From : 00:00 (hh:mm) To : 00:00 (hh:mm)

© 2010 Cisco Systems, Inc. All rights reserved.

The above rules should permit any IPv6 device behind the RV220W to communicate with any IPv6 device behind the RV042.

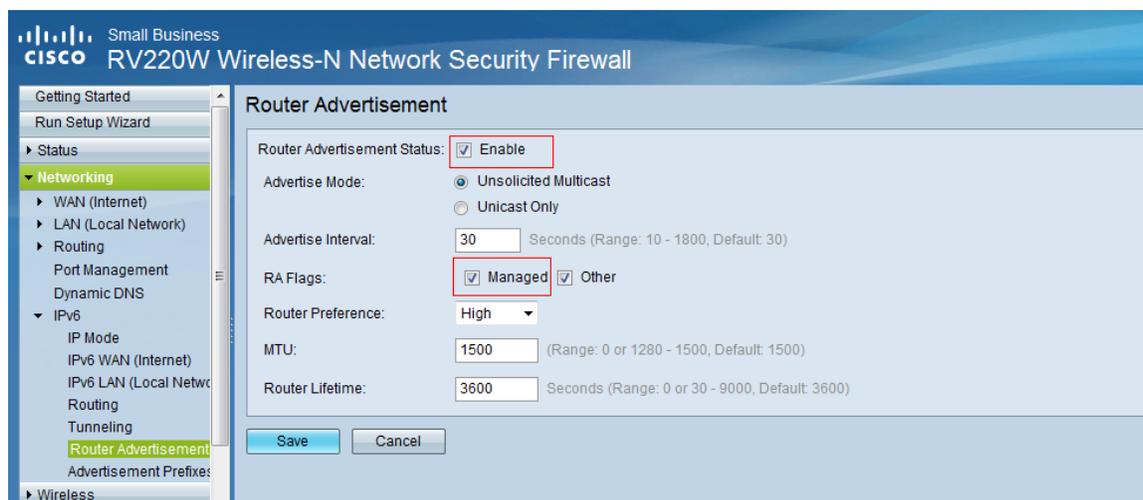
On RV220W:

Step 1. On the **Networking ->IPv6-> IP Mode** page, select **IPv4 and IPv6 Dual-Stack**. Click **Save** to save the settings.



Step 2. On the **Networking ->IPv6->Router Advertisement** page, enter the following settings:

- **Router Advertisement Status:** Check the **Enable** box.
- **Advertise Mode:** Select **Unsolicted Multicast**.
- **RA Flags:** Check the **Managed** box.
- Click **Save** to save the settings.



Step 3. Confirm that your IPv6 devices acquire 6to4 prefixes(2002:WAN IP in HEX ::) for stateless auto-configuration.

Step 4. On the **Networking ->IPv6->Advertisement Prefixes** page, enter the following settings:

- **IPv6 Prefix Type:** Select **6to4**.
- **SLA ID:** Enter a value other than 0.
- **Prefix Lifetime:** Enter the desired value in seconds.
- Click **Save** to save the settings.

The screenshot shows the 'Advertisement Prefixes' configuration page for a Cisco RV220W Wireless-N Network Security Firewall. The left sidebar shows the navigation menu with 'Networking' expanded and 'Advertisement Prefixes' selected. The main content area is titled 'Add / Edit Advertisement Prefix Configuration' and contains the following fields:

- IPv6 Prefix Type:** Radio buttons for '6to4' (selected) and 'Global/Local/ISATAP'.
- SLA ID:** Text input field containing '1'.
- IPv6 Prefix:** Text input field containing '2002:aaaa:c803:1::'.
- IPv6 Prefix Length:** Text input field containing '64' (Range: 0 - 128).
- Prefix Lifetime:** Text input field containing '3600' followed by 'Seconds'.

At the bottom of the configuration area are three buttons: 'Save', 'Cancel', and 'Back'. The footer of the page reads '© 2010 Cisco Systems, Inc. All Rights Reserved.'

Step 5. On the **Networking->IPv6->Tunneling** page, **Automatic Tunneling** field, check the **Enable** box. Click **Save** to save the settings.

The screenshot shows the 'Tunneling' configuration page for a Cisco RV220W Wireless-N Network Security Firewall. The left sidebar shows the navigation menu with 'Networking' expanded and 'Tunneling' selected. The main content area is titled 'Tunneling' and contains the following fields:

- Automatic Tunneling:** Check box labeled 'Enable' (checked).
- Remote End Point:** Check box labeled 'Enable' (unchecked).
- Remote End Point IPv4 Address:** Text input field containing '0.0.0.0'.

At the bottom of the configuration area are two buttons: 'Save' and 'Cancel'. Below the configuration area are two tables:

IPv6 Tunnel Status Table

Tunnel Name	IPv6 Addresses	ISATAP Subnet Prefix
6 to 4 Tunnel	2002:aaaa:c803::aaaa:c803 / 64, ::127.0.0.1 / 96, ::170.170.200.3 / 96, ::192.168.1.1 / 96	

ISATAP Tunnel Table

Local End Point Address	ISATAP Subnet Prefix
0 results found	

At the bottom of the ISATAP Tunnel Table are three buttons: 'Add', 'Edit', and 'Delete'. The footer of the page reads '© 2010 Cisco Systems, Inc. All Rights Reserved.'

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbse
Cisco Small Business Firmware Downloads	www.cisco.com/go/software
Cisco Small Business Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Product Documentation (Quick Start Guide, Administration Guide, Safety Information)	
Cisco Small Business Routers	www.cisco.com/go/smallbizrouters
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb

OL-25493-01