

# IPv6 Tunnel through an IPv4 Network

Document ID: 25156

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### Configure

- Network Diagram

Configurations (Manual IPv6 Mode)

Configurations (Automatic IPv4–Compatible Mode)

#### Verify

- Verification Command Output for Manual IPv6 Mode
- Verification Command Output for Automatic IPv6 Mode

#### Troubleshoot

- Troubleshooting Commands
- Summary

#### Related Information

## Introduction

This document provides a sample configuration for tunneling an IPv6 Routing Information Protocol (RIP), and an IPv6 Border Gateway Protocol (BGP) network and traffic through a pre-existing IPv4 network. This technique allows you to connect IPv6 sites over the IPv4 backbone that exists.

Overlay tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure. This is similar to how you create a generic routing encapsulation (GRE) tunnel to transport Internetwork Packet Exchange (IPX) traffic through an IP network. At the tunnel head end, an IPv6 packet is encapsulated into IPv4 packet and sent to the remote tunnel destination. This is where the IPv4 packet header is stripped, and the original IPv6 packet is forwarded further into an IPv6 cloud.

These are the five methods of tunneling IPv6 traffic:

- Manual IPv6 tunnels
- Automatic IPv4–Compatible tunnels
- GRE
- Automatic 6to4 tunnels
- Intra–Site Automatic Tunnel Addressing Protocol (ISATAP) Tunnels

The primary difference in these tunneling techniques is the method in which the tunnel source and destination are determined. In this document, the manual and Automatic IPv4 Compatible tunnel types are described. Refer to *Implementing Tunneling for IPv6* for information on other tunneling techniques and their characteristics.

**Note:** Overlay tunnels reduce the maximum transmission unit (MTU) of an interface by 20 octets. This assumes that the basic IPv4 packet header does not contain optional fields. A network that uses overlay tunnels is difficult to troubleshoot. Therefore, overlay tunnels that connect isolated IPv6 networks should not be considered as a final IPv6 network architecture. The use of overlay tunnels should be considered as a

transition technique toward a network that supports both the IPv4 and IPv6 protocol stacks, or just the IPv6 protocol stack.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of IPv6 before you attempt this configuration. Refer to *Implementing IPv6 Addressing and Basic Connectivity* for information on IPv6.

### Components Used

The information in this document is based on Cisco 36xx series routers that run Cisco IOS® Software Release 12.3(13).

**Note:** Any hardware platform which supports Cisco IOS Software Release 12.2(2)T or 12.0(21)ST and later also supports IPv6.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

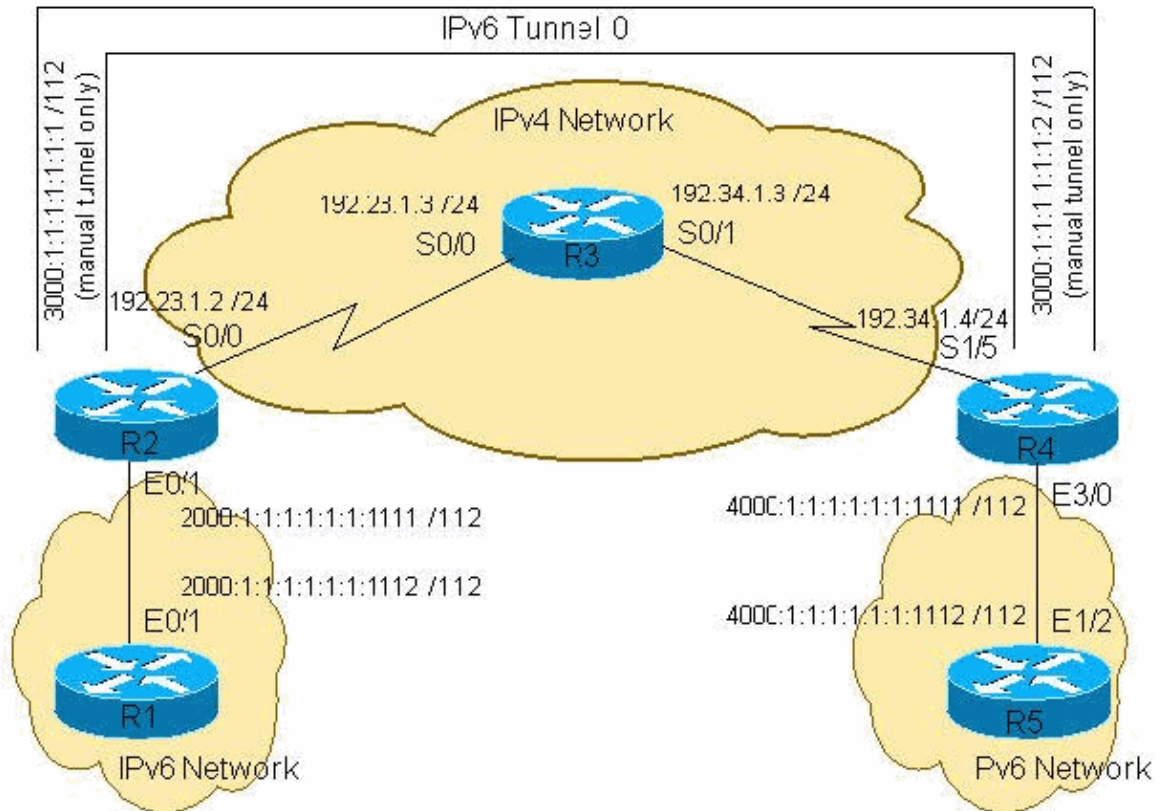
## Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

### Network Diagram

This document uses this network setup:



## Configurations (Manual IPv6 Mode)

The configuration of manually configured tunnels for IPv6 is self-explanatory. It requires definite specification of the tunnel IPv4 source and the tunnel IPv4 destination. The only drawback of when you use this technique is the amount of administration you must perform when the number of tunnels grows.

This document uses these configurations for the manual IPv6 mode:

- R1-IPv6
- R2-IPv6-IPv4
- R3-IPv4
- R4-IPv4-IPv6
- R5-IPv6

### R1-IPv6 (Cisco 3640 Router)

```
R1-ipv6#show run
Building configuration...

Current configuration : 916 bytes
!
version 12.3
hostname R1-ipv6
!
boot system flash
logging buffered 4096 debugging
!
ip subnet-zero
ip cef
!
!
```

```

no ip domain-lookup
!
ipv6 unicast-routing
!
!
!
!
interface Ethernet0/0
  no ip address
  shutdown
!
interface Ethernet0/1
  no ip address
  ipv6 address 2000:1:1:1:1:1:1:1112/112
  ipv6 rip 6bone enable
!
!
ip classless
!
ipv6 router rip 6bone
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
!
!
end

```

### R2-IPv6-IPv4 (Cisco 3640 Router)

```

R2-ipv6-ipv4#show run
Building configuration...

Current configuration : 1079 bytes
!
version 12.3
!
hostname R2-ipv6-ipv4
!
ip subnet-zero
!
!
ipv6 unicast-routing
!
!
interface Tunnel0
  no ip address
  ipv6 address 3000::1/112
  ipv6 rip 6bone enable
  tunnel source Serial0/0
tunnel destination 192.34.1.4
tunnel mode ipv6ip

!--- Configures Manual tunnel.

!--- In some cases, user would require a Data License
!--- in order to issue "tunnel mode ipv6ip"

!
!

```

```

interface Serial0/0
 ip address 192.23.1.2 255.255.255.0
 clockrate 64000
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2000:1:1:1:1:1:1:1111/112
 ipv6 rip 6bone enable
!
router ospf 1
 log-adjacency-changes
 network 192.23.1.0 0.0.0.255 area 0
!
ip classless
!
ipv6 router rip 6bone
!
!
line con 0
line aux 0
line vty 0 4
 login
line vty 5 15
 login
!
!
end

```

### R3-IPv4 (Cisco 2621 Router)

```

R3-ipv4#show run
Building configuration...

Current configuration : 865 bytes
!
version 12.3
!
hostname R3-ipv4
!
!
memory-size iomem 15
ip subnet-zero
!
!
interface Serial0/0
 ip address 192.23.1.3 255.255.255.0
!
interface Serial0/1
 ip address 192.34.1.3 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 network 192.23.1.0 0.0.0.255 area 0
 network 192.34.1.0 0.0.0.255 area 0
!
ip classless
!
line con 0
line aux 0
line vty 0 4
!
!
end

```

## R4-IPv4-IPv6 (Cisco 3640 Router)

```
R4-ipv4-ipv6#show run
Building configuration...

Current configuration : 1413 bytes
!
version 12.3
!
hostname R4-ipv4-ipv6
!
!
ip subnet-zero
!
!
no ip domain-lookup
!
ipv6 unicast-routing
!
!
!
interface Tunnel0
  no ip address
  ipv6 address 3000::2/112
  ipv6 rip 6bone enable
  tunnel source Serial1/5
tunnel destination 192.23.1.2
tunnel mode ipv6ip

!--- Configures Manual tunnel.

!
!
interface Serial1/5
  ip address 192.34.1.4 255.255.255.0
  clockrate 64000
!
!
interface Ethernet3/0
  no ip address
  half-duplex
  ipv6 address 4000:1:1:1:1:1:1:1111/112
  ipv6 rip 6bone enable
!
router ospf 1
  log-adjacency-changes
  network 192.34.1.0 0.0.0.255 area 0
!
ip classless
!
ipv6 router rip 6bone
!
!
line con 0
line aux 0
line vty 0 4
  login
!
!
end
```

## R5-IPv6 (Cisco 7500 Router)

```
R5-ipv6#show run
```

```

Building configuration...

Current configuration : 1001 bytes
!
version 12.3
!
hostname R5-ipv6
!
ip subnet-zero
ip cef distributed
!
!
no ip domain-lookup
!
ipv6 unicast-routing
!
!
!
interface Ethernet1/2
 no ip address
 ipv6 address 4000:1:1:1:1:1:1:1112/112
 ipv6 rip 6bone enable
!
!
ip classless
!
ipv6 router rip 6bone
!
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
!
end

```

## Configurations (Automatic IPv4-Compatible Mode)

The configurations for R1, R3, and R5 are the same as the manual IPv6 mode examples. Only the R2 and R4 configurations change. When you configure the IPv4-compatible tunnel, do not explicitly specify the tunnel destination IPv4 address. Tunnel destination is automatically calculated from the IPv6 next-hop address of the IPv6 route. In order to provide the route over such a tunnel, routing protocol with explicit neighbor address definition, such as BGP or static, is required. In this case, you need to use an IPv4 compatible IPv6 address as the BGP neighbor IPv6 address or static route next-hop address.

These examples use the serial interface on the R2 and R4 as the IPv4-compatible IPv6 address. The same serial is the tunnel source. For example, the IPv4 address 192.23.1.2 on R2 S0/0 is converted to ::192.23.1.2 in the IPv6 notation. This address is used as BGP peer IPv6 address and BGP next-hop. After all, the IPv6 BGP routes are redistributed into IPv6 RIP so that the remote ends of the network receive the information.

This tunneling technique is currently deprecated. Cisco recommends that you use the IPv6 ISATAP tunneling technique. Refer to ISATAP Tunnels for more information on this technique.

**Note:** There is no need to configure a tunnel destination with the automatic IPv6 mode.

**R2-IPv6-IPv4 (Cisco 3640 Router)**

```
R2-ipv6-ipv4#show run
Building configuration...
Current configuration : 1394 bytes
!
version 12.3
!
hostname R2-ipv6-ipv4
!
!
ip subnet-zero
!
!
!
ipv6 unicast-routing
!
!
interface Tunnel0
  no ip address
  no ip redirects
  ipv6 rip 6bone enable
  tunnel source Serial0/0
tunnel mode ipv6ip auto-tunnel

!--- Configures Automatic IPv4 compatible tunnel.

!
!
interface Serial0/0
  ip address 192.23.1.2 255.255.255.0
  clockrate 64000
!
interface FastEthernet0/1
  no ip address
  duplex auto
  speed auto
  ipv6 address 2000:1:1:1:1:1:1:1111/112
  ipv6 rip 6bone enable
!
!
router ospf 1
  log-adjacency-changes
  network 192.23.1.0 0.0.0.255 area 0
!
router bgp 100
  no synchronization
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  neighbor ::192.34.1.4 remote-as 100
  no auto-summary
  !
  address-family ipv6
    neighbor ::192.34.1.4 activate
    neighbor ::192.34.1.4 next-hop-self
    network 2000:1:1:1:1:1:1:0/112
bgp redistribute-internal

!--- The show run command along with the
!--- redistribute bgp command allows BGP to redistribute the
!--- IPv6 routes learned through the tunnel from the other site.

  exit-address-family
!
ip classless
!
```



```
ipv6 router rip 6bone
redistribute bgp 100 metric 2
!
!
line con 0
line aux 0
line vty 0 4
  login
line vty 5 15
  login
!
!
end
```

### R4-IPv4-IPv6 (Cisco 3640 Router)

```
R4-ipv4-ipv6#show run
Building configuration...

Current configuration : 1697 bytes
!
version 12.3
!
hostname R4-ipv4-ipv6
!
ip subnet-zero
!
!
no ip domain-lookup
!
ipv6 unicast-routing
!
!
!
interface Tunnel0
  no ip address
  no ip redirects
  ipv6 rip 6bone enable
  tunnel source Serial1/5
tunnel mode ipv6ip auto-tunnel

!--- Configures Automatic IPv4 compatible tunnel.

!
!
interface Serial1/5
  ip address 192.34.1.4 255.255.255.0
  clockrate 64000
!
!
interface Ethernet3/0
  no ip address
  half-duplex
  ipv6 address 4000:1:1:1:1:1:1:1111/112
  ipv6 rip 6bone enable
!
router ospf 1
  log-adjacency-changes
  network 192.34.1.0 0.0.0.255 area 0
!
router bgp 100
  no synchronization
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
```

```

neighbor ::192.23.1.2 remote-as 100
no auto-summary
!
address-family ipv6
neighbor ::192.23.1.2 activate
neighbor ::192.23.1.2 next-hop-self
network 4000:1:1:1:1:1:0/112
bgp redistribute-internal

!--- The show run command along with the
!--- redistribute bgp command allows BGP to redistribute the
!--- IPv6 routes learned through the tunnel from the other site.

exit-address-family
!
ip classless
!
ipv6 router rip 6bone
redistribute bgp 100 metric 2
!
!
!
line con 0
line aux 0
line vty 0 4
  login
!
!
end

```

## Verify

This section provides information you can use to confirm your configuration is working properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **ping** Determines if a remote host is active or inactive, and the round-trip delay in communicating with the host.
- **show ipv6 route** Verifies if a route exists on the IPv6.
- **show bgp ipv6** Verifies if BGP is running.
- **show bgp ipv6 summary** Displays summary information on the BGP running on the IPv6.
- **show ipv6 int tunnel 0** Verifies that the tunnel is up on the IPv6, and verifies the MTU configured on the interface.

## Verification Command Output for Manual IPv6 Mode

From R1, **ping** the IPv6 address on R5 to verify whether the tunnel transports the IPv6 through the IPv4 network.

```

R1-ipv6#ping ipv6 4000:1:1:1:1:1:1112
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4000:1:1:1:1:1:1112, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/72/72 ms
R1-ipv6#ping 4000:1:1:1:1:1:1112
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4000:1:1:1:1:1:1112, timeout is 2 seconds:
!!!!

```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/72/72 ms
R1-ipv6#
```

From R5, **ping** the IPv6 address on R1.

```
R5-ipv6#ping 2000:1:1:1:1:1112
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000:1:1:1:1:1112, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R5-ipv6#ping ipv6 2000:1:1:1:1:1112
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000:1:1:1:1:1112, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R5-ipv6#
```

## Verification Command Output for Automatic IPv6 Mode

**Ping** the remote IPv6 network to verify connectivity through the tunnel.

```
R1-ipv6#ping 4000:1:1:1:1:1112
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4000:1:1:1:1:1112, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/69/72 ms
R1-ipv6#
R5-ipv6#ping ipv6 2000:1:1:1:1:1112
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2000:1:1:1:1:1112, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/70/72 ms
R5-ipv6#
```

If the **ping** fails, look at the IPv6 routing table to verify whether the route exists. Check the routing table on the other side as well. The route at the end router, such as R5 and R1, should be learned as a RIP route. This route is redistributed from BGP into RIP at R2 and R4. R2 and R4 is where the tunnel terminates and the BGP peering is configured.

```
R5-ipv6#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
Timers: Uptime/Expires
R   ::/96 [120/2]
     via FE80::230:80FF:FEF3:4731, Ethernet1/2
R   2000:1:1:1:1:1:0/112 [120/3]
     via FE80::230:80FF:FEF3:4731, Ethernet1/2
L   4000:1:1:1:1:1:1112/128 [0/0]
     via ::, Ethernet1/2
C   4000:1:1:1:1:1:0/112 [0/0]
     via ::, Ethernet1/2
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
R5-ipv6#
```

If the remote IPv6 network is not on the end router, check the router where the tunnel terminates.

```
R4-ipv4-ipv6#show ipv6 route
IPv6 Routing Table - 7 entries
```

```

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
Timers: Uptime/Expires
L   ::192.34.1.4/128 [0/0]
     via ::, Tunnel0
C   ::/96 [0/0]
     via ::, Tunnel0
B   2000:1:1:1:1:1:0/112 [200/0]
     via ::192.23.1.2, Null
L   4000:1:1:1:1:1:1111/128 [0/0]
     via ::, Ethernet3/0
C   4000:1:1:1:1:1:0/112 [0/0]
     via ::, Ethernet3/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
R4-ipv4-ipv6#

```

Because you are using IPv6 BGP to share information between the two different IPv6 networks, verify that BGP is up and running.

```

R4-ipv4-ipv6#show bgp ipv6
BGP table version is 3, local router ID is 192.34.1.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop              Metric LocPrf Weight Path
*>i2000:1:1:1:1:1:0/112
                   ::192.23.1.2                100         0 i
*> 4000:1:1:1:1:1:0/112
                   ::                            32768 i

R4-ipv4-ipv6#show bgp ipv6 summary
BGP router identifier 192.34.1.4, local AS number 100
BGP table version is 3, main routing table version 3
2 network entries and 2 paths using 394 bytes of memory
2 BGP path attribute entries using 120 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 2/8 prefixes, 2/0 paths, scan interval 60 secs
Neighbor          V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
::192.23.1.2      4    100     24     24        3    0    0 00:19:00      1

R4-ipv4-ipv6#
R4-ipv4-ipv6#show ipv6 int tunnel 0
Tunnel0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::C022:104
Global unicast address(es):
  ::192.34.1.4, subnet is ::/96
Joined group address(es):
  FF02::1
  FF02::2
  FF02::9
  FF02::1:FF22:104
MTU is 1480 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is not supported
ND reachable time is 30000 milliseconds
Hosts use stateless autoconfig for addresses.
R4-ipv4-ipv6#

```

# Troubleshoot

This section provides information you can use to troubleshoot your configuration.

## Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

**Note:** Refer to Important Information on Debug Commands before you use **debug** commands.

- **show ipv6 route** Verifies if a route exists on the IPv6.
- **show ip ospf neighbor** Displays the router ID, priority, and state of the neighbor router. Also, this command displays the amount of time remaining that the router waits to receive an Open Shortest Path First (OSPF) hello packet from the neighbor before declaring the neighbor down. It also displays the IP address of the interface to which this neighbor is directly connected and the interface on which the OSPF neighbor forms adjacency.
- **show ipv6 interface brief** Verifies that the tunnel interface is up.
- **show interfaces tunnel 0** Verifies that the tunnel destination configured is known in the routing table.
- **show ipv6 rip** Displays IPv6 RIP information.
- **show ipv6 protocols** Displays the status of the IPv6 routing protocol.

If the **ping** to the remote IPv6 network fails, verify that the IPv6 routes are learned via IPv6 RIP.

```
R1-ipv6#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
Timers: Uptime/Expires
L   2000:1:1:1:1:1:1:1112/128 [0/0]
    via ::, Ethernet0/1
C   2000:1:1:1:1:1:1:0/112 [0/0]
    via ::, Ethernet0/1
R   3000::/112 [120/2]
    via FE80::202:B9FF:FECE:D281, Ethernet0/1
R   4000:1:1:1:1:1:1:0/112 [120/3]
    via FE80::202:B9FF:FECE:D281, Ethernet0/1
L   FE80::/10 [0/0]
    via ::, Null0
L   FF00::/8 [0/0]
    via ::, Null0
R1-ipv6#
```

On R2, verify that IPv6 RIP routes are learned from the Tunnel0 interface.

```
R2-ipv6-ipv4#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
Timers: Uptime/Expires
L   2000:1:1:1:1:1:1:1111/128 [0/0]
    via ::, FastEthernet0/1
C   2000:1:1:1:1:1:1:0/112 [0/0]
    via ::, FastEthernet0/1
L   3000::1/128 [0/0]
    via ::, Tunnel0
C   3000::/112 [0/0]
    via ::, Tunnel0
```

```

R    4000:1:1:1:1:1:0/112 [120/2]
    via FE80::230:80FF:FEF3:4701, Tunnel0
L    FE80::/10 [0/0]
    via ::, Null0
L    FF00::/8 [0/0]
    via ::, Null0
R2-ipv6-ipv4#

```

If there are issues with connectivity, first verify that the IPv4 network is intact. Also, verify the OSPF neighbor adjacencies and that there are routes to the IPv4 address, which is the tunnel source of the remote tunnel interface. Then verify that you can **ping** between tunnel sources with IPv4 ping.

```

R2-ipv6-ipv4#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
192.23.1.3       1    FULL/ -         00:00:36   192.23.1.3   Serial0/0
R2-ipv6-ipv4#
R3-ipv4#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
1.1.1.1          1    FULL/ -         00:00:30   192.34.1.4   Serial0/1
192.23.1.2       1    FULL/ -         00:00:35   192.23.1.2   Serial0/0
R3-ipv4#
R4-ipv4-ipv6#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
192.23.1.3       1    FULL/ -         00:00:35   192.34.1.3   Serial1/5
R4-ipv4-ipv6#

```

On R2, verify that the IPv6 tunnel interface is up and that you can IPv6 **ping** the remote tunnel source with the IPv4-compatible IPv6 address. If the tunnel interface is down, verify that the tunnel destination configured is known in the routing table. This is a problem in the IPv4 portion of the network because the tunnel destination is not in the routing table.

```

R2-ipv6-ipv4#show ipv6 interface brief
FastEthernet0/0      [up/up]
    unassigned
Serial0/0            [up/up]
    unassigned
FastEthernet0/1      [up/up]
    2000:1:1:1:1:1:1111
Tunnel0              [up/up]
    3000::1
R2-ipv6-ipv4#
R2-ipv6-ipv4#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.23.1.2 (Serial0/0), destination 192.34.1.4
  Tunnel protocol/transport IPv6/IP, key disabled, sequencing disabled
  Tunnel TTL 255
  Checksumming of packets disabled
  Last input 00:00:09, output 00:00:19, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    3119 packets input, 361832 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    3117 packets output, 361560 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets

```

```
0 output buffer failures, 0 output buffers swapped out
R2-ipv6-ipv4#
```

If there are still issues with the IPv6 routes and the IPv4 network is verified, you need to check the IPv6 RIP configuration.

```
R2-ipv6-ipv4#show ipv6 rip
RIP process "6bone", port 521, multicast-group FF02::9, pid 111
  Administrative distance is 120. Routing table is 0
  Updates every 30 seconds, expire after 180
  Holddown lasts 180 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 176, trigger updates 1
R2-ipv6-ipv4#
R2-ipv6-ipv4#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "rip 6bone"
  Interfaces:
    FastEthernet0/1
    Tunnel0
  Redistribution:
    Redistributing protocol rip 6bone
```

Ensure the timers are the same if the default settings are not used. In this example, the default is used on all the IPv6 RIP routers. Verify the configuration to ensure all the RIP enabled interfaces are configured correctly. Also, verify that the same RIP process name is consistent throughout the network. If needed, you can look at the output of `debug ipv6 rip`. As with all debugs, caution must be used to not overload the CPU and console logging buffer.

## Summary

This document demonstrates how tunnels can be used in order for IPv6 and IPv4 to co-exist on the same network. This might be necessary in times of transition. One thing to remember about the IPv6 configurations is that with IPv6 RIP, network statements are not used. IPv6 RIP is enabled globally and each interface takes part in RIP, and is enabled for IPv6 RIP. In the IPv6 BGP example, the Automatic Tunnel section requires the use of the `address-family ipv6` command set to enter the BGP statements.

## Related Information

- [Implementing Tunneling for IPv6](#)
- [IPv6: Providing IPv6 Services over an IPv4 Backbone Using Tunnels](#)
- [Cisco IOS IPv6 Configuration Library](#)
- [IPv6: Connecting to the 6bone Using 6to4 Tunnels](#)
- [IP Version 6 – Support Page](#)
- [BGP Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Aug 10, 2006

Document ID: 25156

---