# IPv6 Module 9 – IPv6 Tunnels

**Objective: Create IPv6 tunnel infrastructure across an existing IPv4 network**

**Prerequisites: Module 6 (IPv4)**

The following will be the common topology used for this supplement.

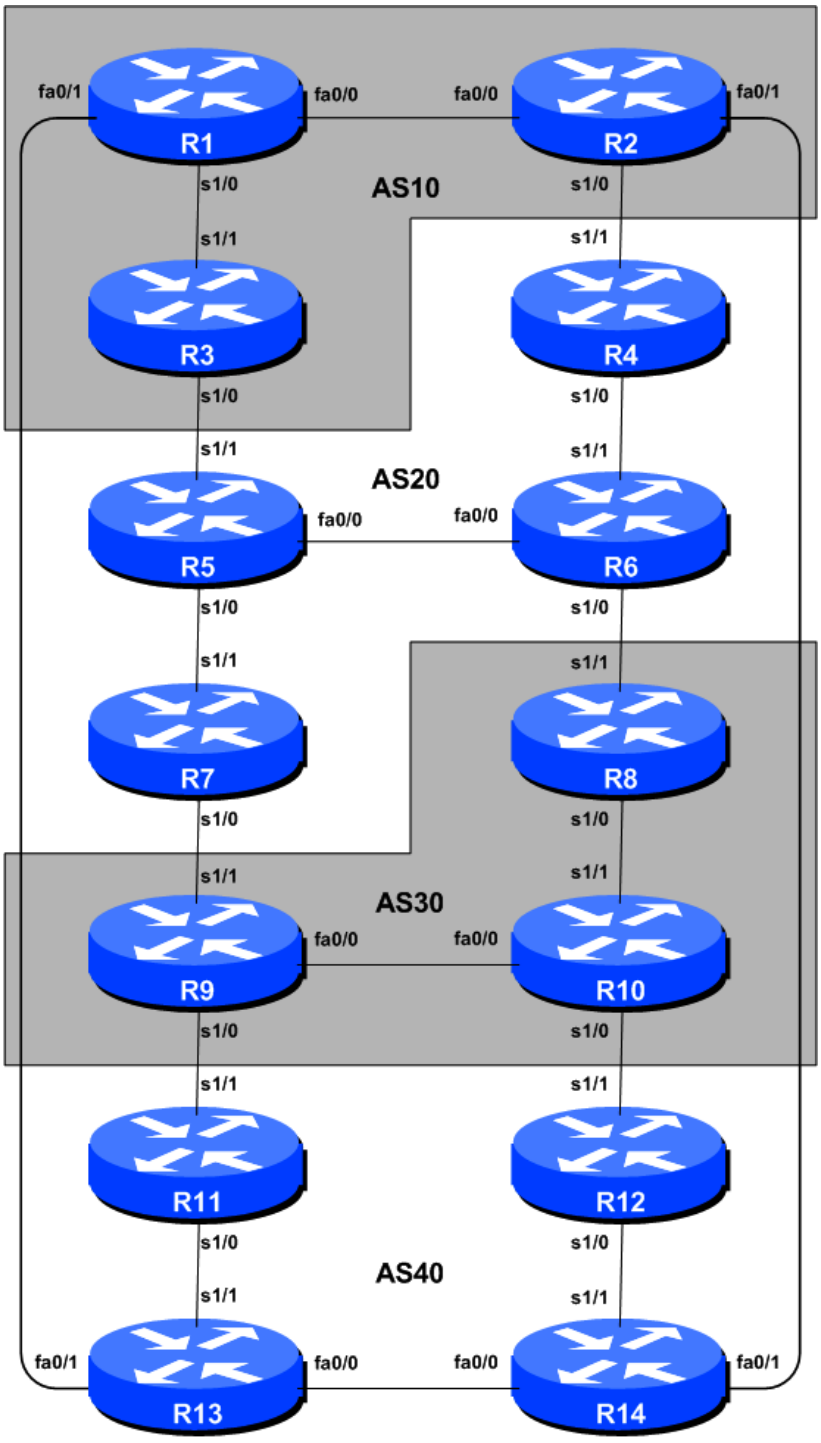


**Figure 1 – ISP Lab Basic Configuration**

## *Lab Notes*

This supplement is intended to be used once Module 6 of the IPv4 Workshop has been completed. The topology and IPv4 configuration should be left exactly as it was at the end of Module 6.

The routers used for this portion of the workshop must support IPv6. This is basically any IP Plus image from 12.2T onwards. Best to check the Cisco Feature Navigator www.cisco.com/go/fn to be absolutely sure which images set and platform supports IPv6. Unfortunately IPv6 is not part of the basic IP only IOS images used by most ISPs.

## *Lab Exercise*

1. **Aim.** The purpose of this lab is to set up two types of IPv6 tunnel from each AS in the lab to Router 15 (not shown). Router 15 is an IPv6 tunnel termination point for the network. This will demonstrate how to configure an IPv6 in IP tunnel and a 6to4 tunnel across an existing infrastructure, for example to connect a native IPv6 backbone across an upstream ISP which does not support any IPv6 at all.

2. **Preparation.** If coming from a previous Module, **remove** any IPv6 addressing and routing information. Leave the IPv4 configuration, as we still want a functioning IPv4 infrastructure. Now enable IPv6 if not already enabled. To do this (if not already done), use the following command:

   ```
   Router(config)# ipv6 unicast-routing
   ```

   The router is now configured to support IPv6 Unicast (as well as IPv4 Unicast which is the default). Save the configuration.

3. **Teamwork.** The classroom network has been divided into 4 ASs – so the class will carry out this Module in teams, one team per AS. So Router1, Router2 and Router3 will work as one team to implement the following scenarios.

## SCENARIO 1 – 6to4 Tunnels

4. **6to4 Tunnels.** The first scenario we want to cover is to implement an automatic tunnelling technique called 6to4. Here IPv6 packets are automatically encapsulated in IPv4 packets by a 6to4 router, with an IPv6 address system based on the IPv4 address, basically 2002:*ipv4address*::/48. So if the IPv4 address of the local router was 10.10.15.241, then its IPv6 addresses would come from the 2002:0a0a:0ff1::/48 block.

5. **Tunnel source and addressing.** Each team should decide which router in the AS should be the 6to4 gateway for the AS. It is important that only one router is the 6to4 gateway – this router will provide the AS a view into the IPv6 "world".

6. **IPv6 addressing.** Take the loopback interface address of the 6to4 gateway router in your AS and work out what the IPv6 6to4 /48 address block is. Which router is being used as gateway and what IPv6 address block has been assigned to your ASN? Go up to the whiteboard provided in the lab

and write down the IPv6 gateway router for your ASN, its IPv4 loopback address and the /48 IPv6 address block. Also document it here:

**IPv6 gateway router:**

**IPv4 loopback address:**

**IPv6 /48 address block:**

7. **Addressing for each AS.** Now that the gateway router and the 6to4 IPv6 address block has been agreed, work out with the rest of the members of your AS what addressing should be used for the point to point links connecting the routers within the AS and for their loopback interfaces. You do NOT need to do any addressing to your neighbouring AS – we are "pretending" that your neighbour does not have any IPv6 support, hence the use of a 6to4 tunnel as a workaround. Document the addressing plan for your AS on the whiteboard provided in the workshop lab and here:

   **Point-to-point links:**

   **Loopbacks:**

8. **Assign addresses:** Once the IPv6 link addresses have been agreed, assign them to the various interfaces and activate those interfaces.

9. **Set up 6to4 tunnel configuration.** Now set up the 6to4 tunnel configuration on the router chosen to be the 6to4 gateway for the AS. Firstly create the tunnel interface – here is an example for AS1:

```
interface Tunnel2002
 tunnel source Loopback 0
 tunnel mode ipv6ip 6to4
 tunnel path-mtu-discovery
```

   Notice the use of path MTU discovery configuration. A common problem with running IPv6 through tunnels is that the MTU sometimes is bigger than that supported by the tunnel, resulting in none or broken connectivity.

10. **Assign address to the 6to4 tunnel:** Next we need to assign an IPv6 address to the tunnel interface so that IPv6 traffic can be forwarded. Rather than consuming a whole /64 for the point-to-point link or inventing a fake link-local address, we simply use the "ip unnumbered" concept. This simply means that IP forwarding is made with reference to the IPv6 address of another interface, in this case the Loopback interface:

```
interface Tunnel2002
 ipv6 unnumbered Loopback0
```

11. **Routing.** Now set up a static route so that all 6to4 IPv6 traffic is directed towards the tunnel (all traffic from the 2002::/16 address space).

```
ipv6 route 2002::/16 Tunnel2002
```

12. **6to4 relay.** The lab instructors will have set up Router15 to act as the 6to4 relay. While the relay will not be used for this lab, it's common for ISP networks to give the local network reachability to the non 2002::/16 IPv6 Internet. This router will be reachable via Router6, which is the default gateway for the lab (the lab instructors will add suitable routing configuration to Router6). The 6to4 gateway in each AS now needs to set up a static route pointing all non-2002::/16 IPv6 traffic to the 6to4 relay; the relay is the router announcing the 192.88.99.1 address – as a 6to4 address this is 2002:c058:6301::1. To do this, enter the commands:

```
ipv6 route ::/0 2002:c058:6301::1
```

(**Aside:** For setting up a 6to4 relay for your own network, the IPv4 anycast address is 192.88.99.0/24 – typically only 192.88.99.1 is used by the relay routers. The 6to4 relay router would advertise the address to the IPv4 Internet, indicating that it is configured as a 6to4 relay as we have done here.)

13. **Ping Test #1.** Ping the remote end of the tunnel. If there are problems, use the following commands to help determine the problem:

```
show ipv6 route            : see if there is a route for the intended destination
show ipv6 interface brief  : see IPv6 status of the tunnel interface
```

14. **Configuring OSPF.** Once the addressing has been completed, set up OSPFv3. If the router which has been chosen as the 6to4 gateway redistributes a default route into OSPFv3, then the whole AS will have connectivity to the rest of the network via the 6to4 tunnel. Example of originating a default route by OSPFv3 is:

```
ipv6 router ospf 100
 default-information originate
```

15. **Connectivity Test**. Try and do traces from your ASN to other ASNs over IPv6. Here is an example, tracing from Router14 to Router3, with the 6to4 gateway router being Router12 (for ASN 4) and Router 1 (for ASN 1).

```
Router14>trace 2002:a00:ff1::3

Type escape sequence to abort.
Tracing the route to 2002:6401:FE0::3

  1 2002:A0A:FE1::12 0 msec 0 msec 0 msec
  2 2002:A0A:FE0::1 4 msec 4 msec 4 msec
  3 2002:A28:FE0::3 8 msec 8 msec 8 msec
Router14>
```

**Question:** Explain why the trace goes directly from Router 12 to Router1 and not via the Router15, the classroom 6to4 relay.)

**Answer:** Traffic goes from Router14 to Router 12 over IPv6. Router 12 recognises that the packet is an IPv6 address, so works out the IPv4 destination from 2002:a0a:0fe0:… That destination is 10.10.15.224 – so the packet has IPv4 headers put on to it, and is then forwarded to Router1 as an IPv4 packet. Router1 recognises that it is an IPv6 packet, removes the IPv4 headers, and then forwards it onwards to the final destination, Router 3.

***Checkpoint #1:*** *call lab assistant to verify the connectivity. Save the configuration as it is on the router – use a separate worksheet, or the workspace at the end of this Module.*

## STOP AND WAIT HERE

## SCENARIO 2 – IPv6 in IPv4 Tunnels

16. **IPv6inIP Tunnels.** The second scenario looks at creating IPv6 tunnels over an IPv4 infrastructure. The existing IPv4 network created in the IPv4 version of the lab remains, with 4 ASs interconnected. We will now connect one router in each AS to a central tunnel termination point – each router in the room will then get IPv6 connectivity across the tunnel infrastructure.

17. **Tidy up.** Remove the 6to4 tunnel configuration from the previous example. This includes removing the static default route pointing to the tunnel as well as the tunnel interface itself; also remove any of the additional IPv6 addressing configuration.

18. **IPv6 Addresses.** We are going to assume that each AS team is a separate entity. The IPv6 addressing for each AS will be numbered out of the documentation address block, 2001:db8::/32.

```
AS1  2001:db8:1::/48          AS3  2001:db8:3::/48
AS2  2001:db8:2::/48          AS4  2001:db8:4::/48
```

    The tunnel point-to-point link addresses should be numbered out of the first /64 in each /48. The "zeroes" have been written in specifically to make this clear.

```
AS1  2001:db8:1:0::/64        AS3  2001:db8:3:0::/64
AS2  2001:db8:2:0::/64        AS4  2001:db8:4:0::/64
```

    The local IP address value will be :2, the remote end will be :1. So, for example, AS2 will use 2001:db8:2:0::2/64 for their end of the tunnel link, and Router15 will use 2001:db8:2:0::1/64 for their end of the tunnel link.

19. **Select Tunnel Endpoint.** Determine which router in the ASN is should be the tunnel endpoint. **Hint:** this should **NOT** be the same router which hosted the 6to4 tunnel configuration. Give another team member a chance!

20. **Create the Tunnel Interface.** Now create the tunnel interface and assign the IPv6 address to the interface.

    Assuming Router5 was chosen as the tunnel endpoint for AS2, a sample configuration might look like:

```
Router5(config)# interface tunnel 0
Router5(config-if)# ipv6 address 2001:db8:2::2/64
Router5(config-if)# tunnel source loopback0
Router5(config-if)# tunnel destination 192.168.1.3
Router5(config-if)# tunnel mode ipv6ip
```

The tunnel mode is set to be IPv6 in IP – it is also possible to use GRE tunnelling (the default tunnel setting); GRE is required if non-IP protocols (such as ISIS) need to be passed across the tunnel.

The tunnel destination is Router15's IPv4 address – this is 192.168.1.3 or some other address indicated by the workshop instructors. The source address for the tunnel is the Loopback interface of the local router – as with iBGP configuration, the loopback is always reachable, even if one of the physical interfaces of the router is down, so ensures network reliability (as well as configuration ease). Don't forget to inform the lab instructor what the IPv4 endpoint of your tunnel should be – without this, it will not be possible to configure the other end of the tunnel.

21. **Enabling Static Routing.** With the tunnel configured, now set up a static route so that the tunnel is usable. To do this, simply configure a static default route for IPv6 pointing to the tunnel interface, for example:

```
ipv6 route ::/0 tunnel 0
```

22. **Ping Test #1.** Ping the remote end of the tunnel. The workshop instructors will have configured a remote IPv6 address for you to ping – this is 2001:DB8:FFFF::1. If there are problems, use the following commands to help determine the problem:

```
show ipv6 route            : see if there is a route for the intended destination
show ipv6 interface brief  : see IPv6 status of the tunnel interface
```

23. **Addressing for each AS.** Now that the tunnel has been set up, agree with the rest of the members of your AS to set up addressing for the point to point links connecting the routers within the AS. You do NOT need to do any addressing to your neighbouring AS – we are "pretending" that your neighbour does not have any IPv6 support, hence the use of an IPv6inIP tunnel as a workaround.

24. **Configuring OSPF.** Once the addressing has been completed, set up OSPF. If the router which has been chosen as the IPv6 tunnel gateway redistributes a default route into OSPF, then the whole AS will have connectivity to the rest of the network via the IPv6inIP tunnel.

25. **Testing Connectivity.** Now try to ping the IPv6 addresses of other ASNs in the lab network. If there are problems, contact other team members to check their connectivity.

***Checkpoint #2:*** *call lab assistant to verify the connectivity. Save the configuration as it is on the router – use a separate worksheet, or the workspace at the end of this Module.*

## STOP AND WAIT HERE

## SCENARIO 3 – IPv6 in IPv4 Tunnels (using BGP)

**26. IPv6inIP Tunnels.** The third scenario builds on the previous one by replacing the static routing across the tunnels with BGP. ISPs who have their own IPv6 allocation and are already using BGP for their IPv4 infrastructure will quite often prefer this method over using static routes.

**27. Introducing iBGP.** Each AS team should introduce iBGP within their AS. Remember that iBGP needs to be fully meshed – so routers in AS1 and 3 will have two peers, and routers in AS 2 and 4 will have three peers.

**28. Introducing eBGP.** The router which is currently terminating the IPv6inIP tunnel should now remove the static default IPv6 route and introduce BGP with the upstream ISP. The upstream router is sitting in AS100. The eBGP session should be configured between the tunnel endpoints, for example for AS4:

```
router bgp 4
address-family ipv6
 neighbor 2001:db8:4::1 remote-as 100
 neighbor 2001:db8:4::1 description eBGP with Router 15
 network 2001:db8:4::/48
!
ipv6 route 2001:db8:4::/48 null0 250
!
```

**29. Check connectivity.** Each team should receive prefixes by BGP from the upstream AS100, and be distributing those by iBGP to the routers within their AS. If connectivity is broken, work with the teams in other ASNs to rectify the problems.

**30. IPv6 Transit Router.** The routing table on the IPv6 transit router should have the four prefixes from the 4 ASNs in its BGP table – each ASN will also see these prefixes, and any other prefixes that Router 15 chooses to originate. For example:

```
IPv6-relay#sh bgp ipv6 unicast summary | begin Neighbor

Neighbor        V  AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
2001:DB8:1::2   4   1      90     107       40    0    0 01:15:58        1
2001:DB8:2::2   4   2      99     129       40    0    0 00:51:25        1
2001:DB8:3::2   4   3      69      75       40    0    0 01:01:28        1
2001:DB8:4::2   4   4     106     125       40    0    0 01:13:52        1
```

**31. Summary.** This section has demonstrated how to connect IPv6 islands to other service providers who also support IPv6. This can be used when upstreams of IPv6 enabled service providers do not yet support IPv6.

***Checkpoint #3:*** *call lab assistant to verify the connectivity. Save the configuration as it is on the router – use a separate worksheet, or the workspace at the end of this Module.*