# IPv6 Module 1b – ISIS

**Objective: Create a basic physical lab interconnection using IPv6 with one ISIS Area running on top of an existing IPv4 infrastructure.**

**Prerequisites: The setup section of IPv6 Module 1.**

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

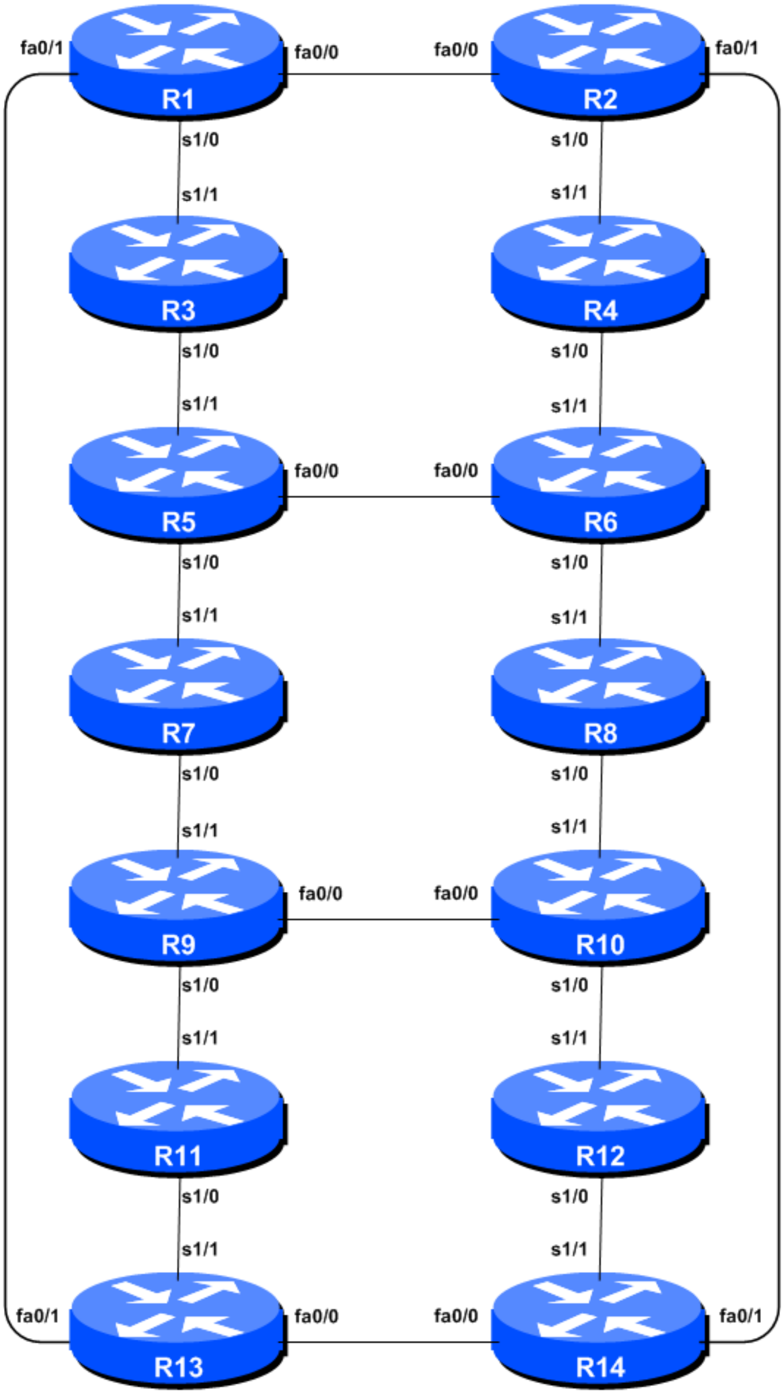

**Figure 1 – ISP Lab Basic Configuration**

## Lab Notes

This lab continues from the previous one by adding IS-IS to the configured, addressed and confirmed working interfaces. Please refer to the Setup Module for further information and reference points about the purpose of Module 1.

## Lab Exercise

1. **ISIS within the same AS.** ISIS will have already been set up in the AS for IPv4 – each team should confirm that the IGP is still operational before starting the next steps to add in IPv6 topology support.

2. **Activating Multi-Topology ISIS.** We also need to activate multi-topology ISIS to roll out ISIS support for IPv6 if the existing network is already using IPv4 ISIS. This allows the IPv6 topology to be incrementally rolled out, very useful during deployment of IPv6. This means that each team can add ISIS IPv6 support without having to coordinate with their neighbouring teams.

   ```
   Router1(config)# router isis workshop
   Router1(config-router)# address-family ipv6
   Router1(config-router-af)# multi-topology
   ```

   **NB.** If we do not enable multi-topology, then each team will have to coordinate the enabling of IPv6 ISIS on each interface with their respective neighbouring teams. Failure to do so will result in the ISIS session going down, as there will be a topology mismatch on that interface.

   **NB.** Multi-topology is configurable in IOS 12.3 and 12.4 but it does not work due to a bug which Cisco refuses to fix. The workaround is to use single topology, noting the caveat above, or use 12.2SRE, 12.2SXH, 12.4T, 15.0 or later IOS images.

3. **Activated Multi-Topology ISIS.** All lab routers **must** have multi-topology ISIS enabled before the lab can proceed to active IPv6 ISIS on each interface. Failure to do so will mean that ISIS will see a topology mismatch and will tear the ISIS adjacency down. This is not a good situation on a live operational network, as it means the iBGP sessions will drop and customers will lose connectivity.

***Checkpoint #2:*** *demonstrate that you have enabled multi-topology ISIS to the lab demonstrators.*

4. **Activating ISIS on each interface.** All connected point to point and shared ethernet interfaces need to be configured with IPv6 ISIS. Otherwise, you may not be able to see network advertisements via ISIS from routers two or more hops away.

   The example for the Router Team 1 is:

   ```
   Router1(config)# interface fastethernet 0/0
   Router1(config-if)# ipv6 router isis workshop
   !
   Router1(config)# interface fastethernet 0/1
   Router1(config-if)# ipv6 router isis workshop
   ```

```
!
Router1(config)# interface serial 1/0
Router1(config-if)# ipv6 router isis workshop
```

**Note**: the ISIS ID on the interfaces must be matched with the router's ISIS ID.

5. **ISIS Metrics.** Now each team needs to set the ISIS metric on each physical interface. The default ISIS metric for all interface types is 10. Unlike OSPF in IOS, ISIS has no automatic scheme to convert the interface bandwidth into a metric value. ISPs deploying ISIS have to come up with their own scheme (as in fact many ISPs using OSPF now also do)

   In the lab we use metric 2 for the Ethernet interfaces and metric 20 for the Serial interfaces. For example:

```
Router1(config)# interface fastethernet 0/0
Router1(config-if)# isis ipv6 metric 2 level-2
!
Router1(config)# interface fastethernet 0/1
Router1(config-if)# isis ipv6 metric 2 level-2
!
Router1(config)# interface serial 1/0
Router1(config-if)# isis ipv6 metric 20 level-2
```

6. **Announcing the Loopback /128.** The loopback interface will have already been marked as passive when ISIS was set up for IPv4 routing on the network. Each team should confirm that the passive-interface command is still present for the Loopback.

7. **Avoiding Traffic Blackhole on Reboot.** When a router restarts after being taken out of service, ISIS will start distribute prefixes as soon as adjacencies are established with its neighbours. In the next part of the workshop lab, we will be introducing iBGP. So if a router restarts, ISIS will start up well before the iBGP mesh is re-established. This will result in the router landing in the transit path for traffic, with out the routing table being completed by BGP. There will not be complete routing information on the router, so any transit traffic (from customer to peer or upstream, or vice-versa) will be either dropped, or resulting in packets bouncing back and forth between adjacent routers. To avoid this problem, we require the router to not announce it is availability until the iBGP mesh is up and running. To do this, we have to provide the following command:

```
Router1(config)#router isis workshop
Router1(config-router)#address-family ipv6
Router1(config-router-af)#set-overload-bit on-startup wait-for-bgp
```

   This sets ISIS' overload bit such that all IPv6 routes via this router will be marked as unreachable (very high metric) until iBGP is up and running. Once iBGP is running, the prefixes distributed by ISIS will revert to standard metric values, and the router will pass transit traffic as normal.

8. **Ping Test #2.** Ping all loopback interfaces in the classroom. This will ensure the ISIS IGP is connected End-to-End. 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 clns neighbor` | : see a list of CLNS-IS neighbours that the router sees |
| `show clns interface` | : see if ISIS is configured and see the IS type |
| `show isis database` | : see ISIS link state database that the router has learned |

```
show isis ipv6 rib          : see IPv6 ISIS routes that the router has learned
show isis topology          : see the ISIS topology as learned by the router
```

***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. You will require this configuration several times throughout the workshop.*

9. **Traceroute to all routers.** Once you can ping all the routers, try tracing routes to all the routers using *trace x:x* command. For example, Router Team 1 would type:

```
Router1# trace 2001:db8::c
```

to trace a route to Router R12. If the trace times out each hop due to unreachable destinations, it is possible to interrupt the *traceroute* using the Cisco break sequence CTRL-^.

**Q.** Why do some trace paths show multiple IP addresses per hop?

**A.** If there are more than one equal cost paths, ISIS will "load share" traffic between those paths.

```
Router1>trace 2001:db8::c

Type escape sequence to abort.
Tracing the route to 2001:db8::c

  1 2001:db8:0:3::1    4 msec
    2001:db8:0:2::1    0 msec
    2001:db8:0:3::1    0 msec
  2 2001:db8:0:f::1    4 msec
    2001:db8:0:8::1    4 msec
    2001:db8:0:f::1    0 msec
  3 2001:db8:0:13::    4 msec *  4 msec
Router1>
```

10. **Other Features in ISIS.** Review the documentation or use command line help by typing *?* to see other *show* commands and other ISIS configuration features.

## Review Questions

1. What IOS show command(s) will display the router's IPv6 forwarding table?

2. What IOS show command(s) will display the router's IPv6 ISIS database?