IPv6 Module 11 – Advanced Router Configuration

Objective: Create a basic physical lab interconnection with two autonomous systems. Each AS should use ISIS, iBGP and eBGP appropriately to construct a working network.

Prerequisites: Basic ISP Workshop (at least Modules 1 to 8)

The following will be the common topology used.

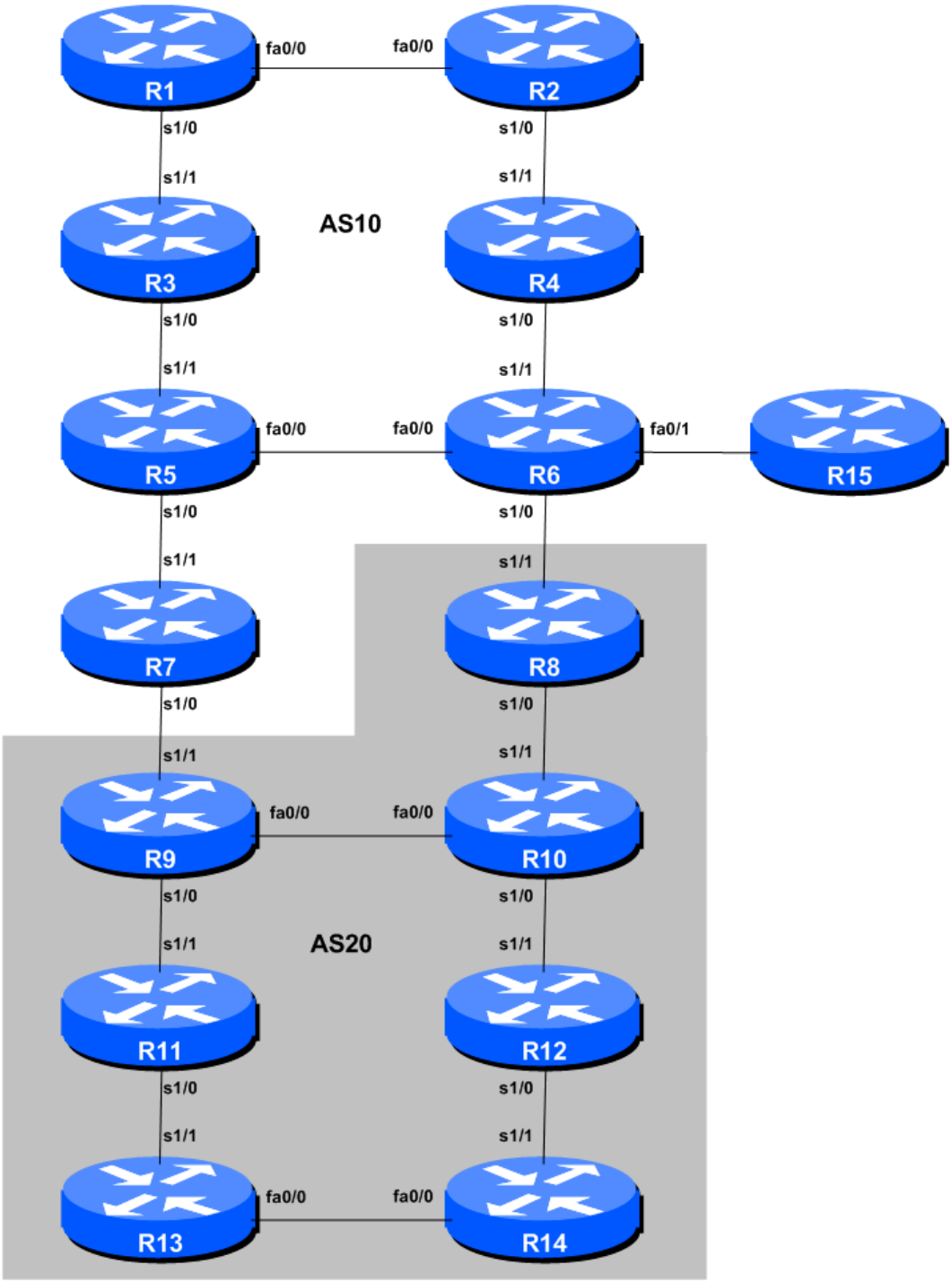


Figure 1 – ISP Lab Basic Configuration

Lab Notes

The purpose of this module is to construct the workshop lab and serve as a reminder of the basic principles of building a network, introducing an IGP, properly function iBGP, and the basics of eBGP:

- After the **physical design** is established, the connections between the hardware should be built and verified.

- Next, the routers should have the **base configuration** installed, and basic but sufficient security should be set up. Note that Router15 is the Workshop Instructor's router and it will be used at various instances throughout the workshop.

- Next the **basic IP connectivity** be tested and proven. This means assigning IP addresses on all links which are to be used, and testing the links to the neighbouring devices.

- Only once one router can see its neighbour does it make sense to start configuring routing protocols. And **start with the IGP** (ISIS is chosen for this workshop). There is no purpose to building BGP while the chosen IGP (in this case ISIS) is not functioning properly. BGP relies on ISIS to find its neighbours and next hops, and an improperly or non-functioning ISIS will result in much time wasted attempting to debug routing problems.

- Once the IGP is functioning properly, the **BGP configuration** can be started, first internal BGP, then external BGP.

- Finally, **documentation**. Documentation is often overlooked or forgotten. It is an ongoing process in this workshop. If the instructor asks you to document something, either on the whiteboard in the class, or at the back of this booklet, it is in your best interests to do so. There can never be too much documentation, and documentation at the time of network design and construction can usually saves much frustration at a future date or event.

Lab Exercise

The following list is typical for what needs to be done to bring up the lab configuration:

1. **Enable IPv6.** Cisco routers with an IOS supporting IPv6 currently do not ship with IPv6 enabled by default. This needs to be done before any of the following exercises can be completed. To do this, use the following command:

   ```
   ipv6 unicast-routing
   ```

2. **Enable IPv6 CEF.** Unlike IPv4, CEFv6 is not enabled by default. So we now need to enable IPv6 CEF also, using the following command:

   ```
   ipv6 cef
   ```

3. **Disable IPv6 Source Routing.** Unless you really believe there is a need for it, source routing should be disabled. This option, enabled by default, allows the router to process packets with source routing header options. This feature is a well-known security risk as it allows remote sites to send packets with different source address through the network (this was useful for

troubleshooting networks from different locations on the Internet, but in recent years has been widely abused for miscreant activities on the Internet).

```
no ipv6 source-route
```

4. **Back to Back Serial Connections.** Connect the serial connections as in Figure 1. The DCE side of a back to back serial connection is configured with the *clock rate* command that drives the serial circuit.

```
interface serial 1/0
 description DCE Serial Connection to RouterXX
 clock rate 2000000
!
```

5. **Ethernet Connections.** The Ethernet links between the routers will be made using *cross-over* RJ-45 cables – these will directly connect the Ethernet ports on the two routers without the requirement for an Ethernet switch.

6. **IPv6 Addressing Plans.** Addressing plans in IPv6 are somewhat different from what has been considered the norm for IPv4. The IPv4 system is based around the RIRs allocating address space to an LIR (an ISP who is a member of the RIR) based on the needs of the ISP; that allocation is intended to be sufficient for a year of operation without returning to the RIR. The ISP is expected to implement a similar process towards their customers – so assigning address space according to the needs of the customer.

   The system changes a little for IPv6. While the RIRs still allocate address space to their membership according to their membership needs, the justification to receive an IPv6 allocation is somewhat lighter than it is for IPv4. If the ISP can demonstrate a plan to connect at least 200 customers to the Internet using IPv6, they will receive an allocation. However, a bigger advantage starts with the customer assignments made by the ISP – the ISP simply has to assign a /48 to each of their customers. This is the minimum assignment for any site/customer – within this /48 there are a possible 64k subnets, deemed sufficient for all but the largest networks around these days. Within this /48, the smallest unit which can be assigned is a /64 – so every LAN and point to point link receives a /64.

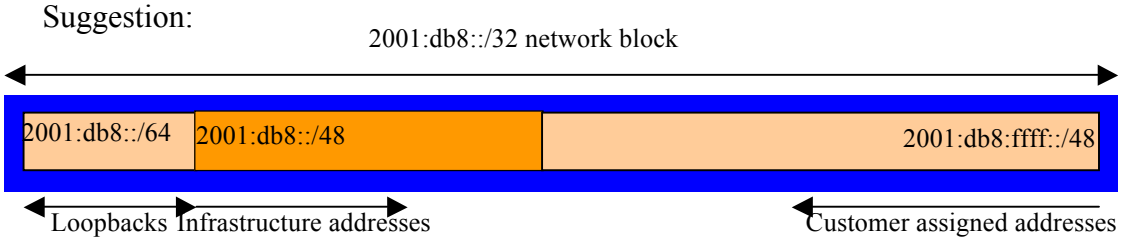
   With this revised system, the address plan for IPv6 is hugely simplified. ISPs assign a single /48 for their network infrastructure, and the remainder of their /32 block is used for customer assignments. This workshop assumes this principle, as will be seen in the following steps.

7. **IPv6 Addresses.** Each AS is assigned a block of IPv6 addresses.

   AS10 2001:db8::/32 AS20 2001:db9::/32

   Decide among your team what the addressing plan for you AS should be.
   Hint One: point-to-point links only require /64s and should be addressed as /127s.
   Hint Two: loopbacks only require a /128 host address.
   Hint Three: number your backbone sequentially, preferably from the start of the range, using the first /48 for your infrastructure.

Suggestion:



Note: When the IPv6 addresses are assigned, they **MUST** be annotated on the **WHITE-BOARD** at the front of the workshop room. A large network map will have been drawn on the white-board – all the IP address assignments need to be annotated there so that other Router Teams can document and understand the links and routing in this and future modules.

8. **Ping Test #1.** Ping all physically connected subnets of the neighbouring routers. If the physically connected subnets are unreachable, consult with your neighbouring teams as to what might be wrong. Don't ignore the problem – it may not go away.

9. **Create vty filters.** Set up filters on the vty interfaces restricting vty access to your router to those addresses you would like to permit. For the purpose of this lab, even though it is not connected to the Internet, set up filters so that only the address space in the lab has access.

```
ipv6 access-list vty
 permit ipv6 2001:db8::/32 any
 permit ipv6 2001:db9::/32 any
!
line vty 0 4
 ipv6 access-class vty in
```

10. **ISIS within the same AS.** Each router Team should enable ISIS on their router. All the routers in one AS will be in ISIS level 2. The NET should be *49.0001.x.x.x.x.00*, where *x.x.x.x* is the loopback IP address. Remember to use wide metrics, and don't forget to mark the loopback interface as a passive interface – for example:

```
router isis as20
 net 49.0001.0100.2000.0001.00
 is-type level-2-only
 passive-interface Loopback0
 metric-style wide
 log-adjacency-changes
 address-family ipv6
  multi-topology
!
interface serial 1/0
 ipv6 router isis as20
 isis circuit-type level-2 only
 isis metric 20 level-2
!
```

11. **DMZ between AS10 and AS20.** ISIS must **NOT** run on the demarcation links between AS10 and AS20. So Routers 6, 7, 8 and 9 must **NOT** configure the serial links between each other to be non-passive. This is a very important point, and a mistake frequently made by many ISPs. Also, do not put a network statement on external facing interfaces – again see iBGP discussion at step 17. Router 6 should have two adjacencies only – with Router 4 and 5. Router 7 should have one adjacency only – with Router 9. And so on.

12. **Intra Area Authentication – Part 1.** ISIS supports router authentication. Even though ISIS runs alongside IP on the wire, some ISPs still consider neighbour authentication to be necessary. Authentication helps prevent the introduction of improperly configured or unintended equipment.

    This first step will be to set up the authentication key chains::

    ```
    key chain isis-sec-lvl2
     key 1
      key-string cisco
    ```

    This sets up a key chain called *isis-sec-lvl2* with the key string "cisco". Obviously on a production network a key other than "cisco" should be used!

13. **Intra Area Authentication – Part 2.** Now that the key chain has been set up, the second step is to enable MD5 encryption for ISIS itself and specify which key-chain should be used for level-2 IS:

    ```
    router isis as20
     authentication mode md5
     authentication key-chain isis-sec-lvl2 level-2
    ```

14. **Intra Area Authentication – Part 3**. Now that the encryption mode and key chain have been set up, the final step is to actually configure the authentication on the interface. MD5 encryption should be used rather than exchanging keys in plain text – to do this, use the *md5* sub-interface command.

    An example configuration might be:

    ```
    interface fastethernet0/0
     isis circuit-type level-2 only
     isis metric 2 level-2
     isis authentication mode md5 level-2
     isis authentication key-chain isis-sec-lvl2 level-2
    ```

    Notice now that the ISIS adjacencies do not come up unless the neighbouring router has also entered the same configuration and key. Notice also how the ISIS adjacencies were reset as the configuration was entered – security is being introduced, so the adjacencies are reset.

15. **Ping Test #2.** Ping all loopback interfaces in your AS. They should all respond. 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 neighbors 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

Checkpoint #2: *call lab assistant to verify the connectivity. Save the configuration as it is on the router either on the worksheet on the end of this hand out, or own your own laptop, or on the classroom tftp server if it is available.*

16. **Passwords on BGP sessions.** It is now considered very good practice to use passwords on the BGP sessions on the router. When BGP is set up in the next step, don't forget to include a password on the BGP peering.

    The password used for this module will be *cisco* – obviously on a real operational network operators will use a password which follows their normal password rules, and not something which is easily guessable. An example configuration might be:

    ```
    router bgp 10
     neighbor 2001:db8::2 password cisco
    ```

    Note: Passwords should be included in all future BGP configurations in this workshop.

17. **Configuring next-hop-self on iBGP Neighbours.** So that BGP has a valid next-hop for external destinations, we introduce the `next-hop-self` BGP configuration. This changes the iBGP default by replacing the next-hop address for external sites from that of the external neighbour address to the loopback address of the local router. The local router knows how to get to the external destinations because it is connected to the LAN that leads there – the rest of the network internal to the AS is told simply to go via this router. Note that because we do this, we no longer need to quote the external point to point link in our ISIS (or OSPF) configuration – see steps 9 & 11 earlier. For example:

    ```
    router bgp 10
     neighbor 2001:db8::2 next-hop-self
    ```

    Note that the use of *next-hop-self* on all iBGP sessions is considered industry best practice, and its use from now on in the workshop is **strongly recommended**.

18. **Configuring iBGP Neighbours.** Configure iBGP peers within each autonomous system. Use a full iBGP mesh. Don't forget that iBGP peering is configured to be between the loopback interfaces on the routers. Also, it is good practice to use a peer-group – and because we are using IPv6, put in a "v6" to differentiate it from the equivalent IPv4 peer-group. For example:

    ```
    router bgp 10
     no bgp default ipv4-unicast
     address-family ipv6
      neighbor v6-ibgp-peers peer-group
      neighbor v6-ibgp-peers remote-as 10
      neighbor v6-ibgp-peers description iBGP v6 peergroup for internal routers
      neighbor v6-ibgp-peers update-source loopback 0
      neighbor v6-ibgp-peers next-hop-self
      neighbor v6-ibgp-peers password cisco
      neighbor v6-ibgp-peers send-community
      neighbor 2001:db8::2 peer-group v6-ibgp-peers
      neighbor 2001:db8::3 peer-group v6-ibgp-peers
      neighbor 2001:db8::4 peer-group v6-ibgp-peers
    ..etc..
    ```

Use *show bgp ipv6 unicast summary* to check the status of the iBGP neighbour connections. If the iBGP session is not up and/or no updates are being sent, work with the Router Team for that neighbour connection to troubleshoot the problem. Note: get into the habit of using peer-groups and configuring them fully, including the "send-community" directive. This workshop makes extensive use of communities, and making them part of your configuration is good practice.

Note: Router6 should also include the network connecting to Router15 in the iBGP configuration. This is so that the network connected to Router15 can be accessed – it has the DNS server and NTP server located on it.

19. **Add Prefixes to BGP.** Each Router Team will advertise the CIDR block assigned to them via BGP. AS10 would advertise 2001:db8::/32 and AS20 would advertise 2001:db8::/32:

```
router bgp 10
 address-family ipv6
  no synchronization
  bgp log-neighbor-changes
  network 2001:db8::/32
!
ipv6 route 2001:db8::/32 null0
```

Don't forget the static route to Null0. This ensures that the prefix has an entry in the routing table, and therefore will appear in the BGP table. Synchronisation is disabled by default in IOS, but it's still good practice to remember to include the command. (Note that a distance of 250 could be applied to the static route to ensure that routing protocols announcing this exact prefix will override the static (if this is required/desired).)

Checkpoint #3: *call the lab assistant to verify the connectivity.*

20. **Configure eBGP peering.** Now that iBGP is functioning, it is time to configure eBGP. External BGP will be set up between AS10 and AS20, specifically between Routers 6 and 8, and Routers 7 and 9 only. The remaining lab teams should monitor the BGP table they see on their routers.

Firstly, agree on what IP addresses should be used for the point to point links between the ASes. Put the /64 networks used for the DMZ links into ISIS (don't forget about passive interface). Then configure eBGP between the router pairs, for example:

```
router bgp 10
 address-family ipv6
  neighbor 2001:db8:0:1:: remote-as 20
  neighbor 2001:db8:0:1:: password cisco
  neighbor 2001:db8:0:1:: description eBGP with RouterXX
```

Use the BGP show commands to ensure that you are receiving prefixes from your neighbouring AS.

21. **Check the network paths and the routing table.** Run traceroutes between your router and other routers in the classroom. Ensure that all routers are reachable. If any are not, work with

the other router teams to establish what might be wrong. Make sure that you can see Router15. The lab instructor will have written the addresses and network up on the whiteboard. (The network is 2001:dba::/64, the address of Router6 on that LAN is 2001:dba::254, and the address of Router15 is 2001:dba::1.)

22. **Saving the configuration. For software releases from 12.0 onwards**, the commands to save the configuration are of the format *copy <source> <destination>* where the source and destinations can be any of the following options: *ftp, lex, null, nvram, rcp, running-config, startup-config, system, tftp.* To save the configuration to the TFTP server, use the "*copy system:/running-config tftp:"* command sequence. If the TFTP server is unreachable, "."s followed by an error message will be displayed rather than "!"s. (Note that the "*write net*" command of earlier releases is still supported but may be removed at a future release.)

    An example of saving the configuration for Router 1 might be:

```
Router1#copy system:running-config tftp:
Address or name of remote host[]? 192.168.1.4
Destination filename [running-config]? router1-confg
!!
2259 bytes copied in 2.920 secs (1129 bytes/sec)
Router1#
```

Checkpoint #4: *call the lab assistant to verify the connectivity.*

23. **Summary.** This module has covered most of the fundamental configuration topics required to add IPv6 routing support to an existing ISP network. It has covered enabling IPv6, ISIS configuration, iBGP configuration, and finally simple eBGP configuration. No routing policy has been implemented. **Each Router team is strongly recommended to make a copy of their configuration as most of the configuration concepts will be required throughout the remainder of the workshop.**