Module 10 – An Internet Exchange Point

Objective: To investigate methods for connecting to an Internet Exchange Point.

Prerequisites: Modules 1 to 4, and the Exchange Points Presentation

The following will be the common topology used.

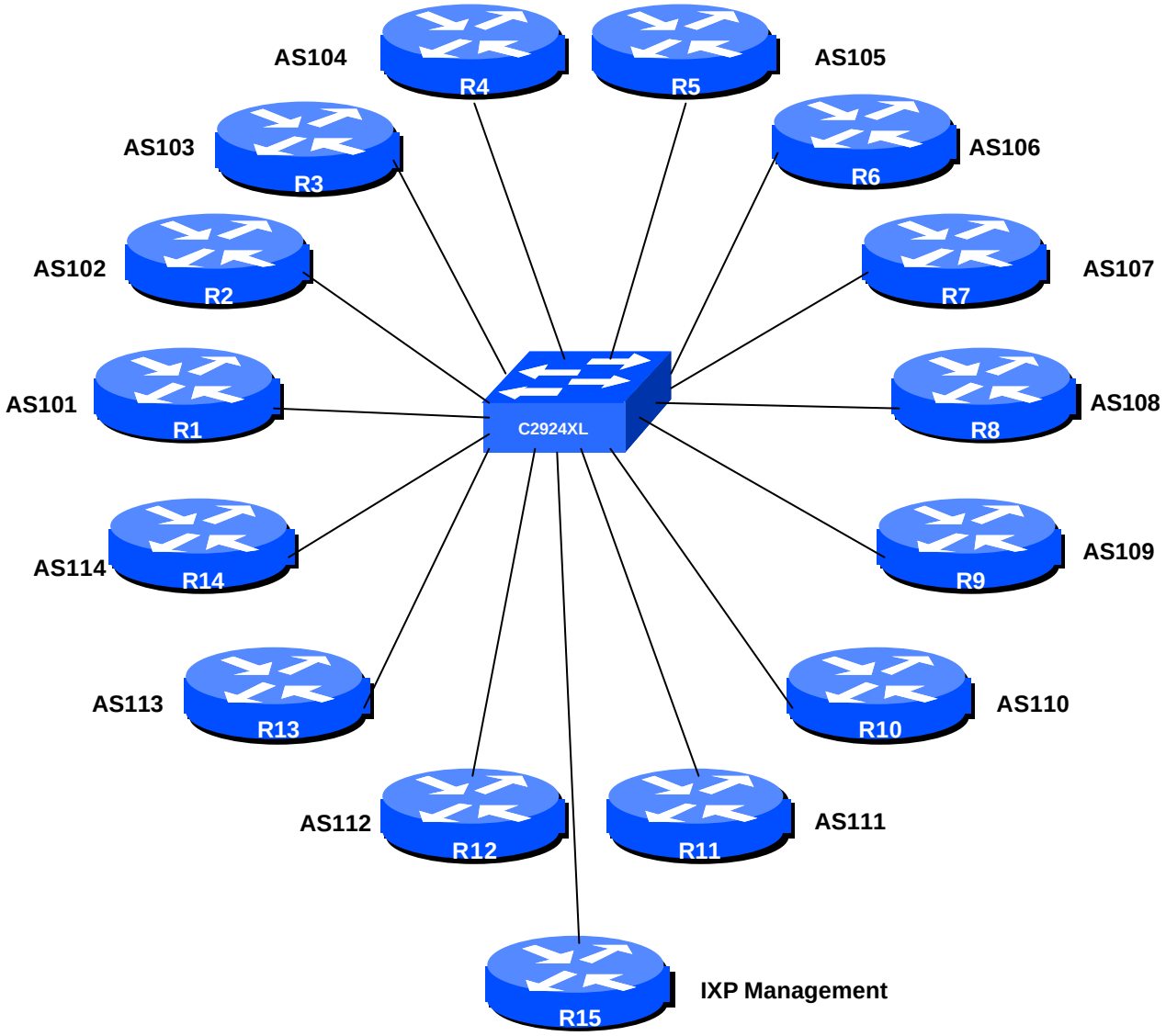

Figure 1 – IXP Configuration

Lab Notes

The purpose of this module is to introduce the concept of an Internet Exchange Point, how to peer at IXPs, and look at some of the recommended configuration practices.

Lab Exercise

1. **Basic Configuration.** Each router team should configure their router to fit into the network layout depicted in Figure 1. Check all connections. Note that all links are by ethernet.

2. **Addressing Plan.** These address ranges should be used throughout this module. You are welcome to use your own range within an AS if you desire, just so long as you consult with the teams in other ASes to ensure there is no overlap.

AS101	**100.1.0.0/20**	**AS108**	**100.3.0.0/20**
AS102	**100.1.16.0/20**	**AS109**	**100.3.16.0/20**
AS103	**100.1.32.0/19**	**AS110**	**100.3.32.0/19**
AS104	**100.2.0.0/20**	**AS111**	**100.4.0.0/20**
AS105	**100.2.16.0/20**	**AS112**	**100.4.16.0/20**
AS106	**100.2.32.0/20**	**AS113**	**100.4.32.0/20**
AS107	**100.2.48.0/20**	**AS114**	**100.4.48.0/20**

3. **Basic Router Setup.** Set up the routers as you would have done in previous modules. That is, basic security, the BGP outline configuration, IOS Essentials, etc.

4. **Management Router and IXP LAN.** The lab instructor will have connected another router to the exchange point – this is Router 15 in the figure. Each router team should set up their router to synchronise time off that router using NTP. The password on the NTP session is "cisco" as in previous Modules. The address range used for the IXP LAN is 120.5.10.0/24 – the management router in this module has an IP address of 120.5.10.254. Each of the ASes is assigned a block of 3 addresses to use on the exchange point LAN. So, for example, AS101 has 120.5.10.1, 120.5.10.2 and 120.5.10.3. AS102 has 120.5.10.4, 120.5.10.5 and 120.5.10.6. And so on.

   Q. Why do you think three addresses have been assigned to each participant at the IXP?

Checkpoint #1: *When you have properly configured your router, and the other routers at the IXP are reachable (i.e. you can ping the other routers), please let the instructor know.*

Cisco Systems Inc
170 West Tasman Drive.
San Jose, CA 95134-1706
Phone: +1 408 526-4000
Fax: +1 408 536-4100

Simple IXP example

This example is of a very simple IXP. But using this configuration, any participant in this workshop should be able to go away and set up a working IXP in their own economy. Technically they are not hard to implement. Politics & business economics are not covered in this workshop.

Only prefix lists are used to filter BGP announcements. eBGP peers should be in peer-groups, route refresh should be used to implement any policy changes as in other modules, and Unicast Reverse Path Forwarding[1] checks should be enabled on the ethernet interface pointing to the IXP.

5. **Configure the ethernet of each router at the IXP.** The ethernet interfaces connected to the IXP should be configured appropriately for a public connection. Review the IOS Essentials materials and the IXP presentation. The configuration for Router 14 might be:

```
interface ethernet 0
 description Exchange Point LAN
 ip address 120.5.10.40 255.255.255.0
 ip verify unicast reverse-path allow-self-ping
 no ip directed-broadcast
 no ip proxy-arp
 no ip redirects
!
```

   If you are unclear as to what any of the configuration lines do, please ask the lab instructor.

6. **Configuring BGP on the routers.** Next, eBGP needs to be set up on the routers. Create a peer-group and apply that peer-group to each eBGP neighbour. A sample configuration for Router13 might be:

```
ip prefix-list myprefixes permit 100.4.32.0/20
ip prefix-list peer101 permit 100.1.0.0/20
..
ip prefix-list peer114 permit 100.4.48.0/20
!
router bgp 113
 no synchronization
 bgp log-neighbor-changes
 network 100.4.32.0 mask 255.255.240.0
 neighbor ixp-peers peer-group
 neighbor ixp-peers remove-private-AS
 neighbor ixp-peers prefix-list myprefixes out
 neighbor <router1> remote-as 101
 neighbor <router1> description Peering with AS101
 neighbor <router1> peer-group ixp-peers
```

[1] See the Cisco ISP Essentials presentation for more on Unicast Reverse Path Forwarding checks.

```
 neighbor <router1> prefix-list peer101 in
..
 neighbor <router14> remote-as 114
 neighbor <router14> description Peering with AS114
 neighbor <router14> peer-group ixp-peers
 neighbor <router14> prefix-list peer114 in
 no auto-summary
!
```

The configurations for the other routers will be similar to this one. All router teams will have done sufficient BGP configuration throughout this workshop to extrapolate from the above examples. If in any doubt, as the lab demonstrator for assistance.

Note the prefix-lists. There is a per-peer inbound prefix-list. Some service providers only filter ASes – that has inherent dangers, and does not prevent against inbound leaking of prefixes incorrectly originated by the peer AS. But only filtering on prefixes doesn't scale, especially in larger IXPs with large participating service providers as they are frequently adding to the prefixes they announce. The Internet Routing Registry is usually used to solve this problem.

7. **Connectivity Test.** Check connectivity throughout the IXP network. Each router team should be able to see all the other routers at the IXP. When you are satisfied that BGP is working correctly, try running traceroutes to check the paths being followed.

Checkpoint #2: *Once the BGP configuration has been completed, check the routing table and ensure that you have complete reachability over the entire network. If there are any problems, work with the other router teams to resolve those.*

8. **Set up passwords on the eBGP sessions.** Negotiate with each ASN a password which you can use on your BGP session with them. And then agree to cut the eBGP session over to using passwords such that the eBGP session does not fall over due to password mismatches (as in Module 2).

```
router bgp 113
 neighbor <router14> password peer114
!
```

9. **Set up eBGP session with Router 15.** The lab instructors will have now configured Router 15 to be a route collector. This is a router which collects all the routes available at the IX. It serves purpose other than to be an information repository showing how many routes are available at the IX – quite often the IXP management will operate such a router, connected to a Looking Glass web interface, to increase the marketing value of the IX. The more peers who get attracted by the routes available at the IX, the greater

the value proposition the IX is to the rest of the members. It's in everyone's interest to peer with the router collector:

```
router bgp 113
...
 neighbor 120.5.10.254 remote-as 65534
 neighbor 120.5.10.254 description eBGP with the IX Route Collector
 neighbor 120.5.10.254 password cisco
 neighbor 120.5.10.254 remove-private-AS
 neighbor 120.5.10.254 prefix-list deny-all in
 neighbor 120.5.10.254 prefix-list myprefixes out
...
!
ip prefix-list deny 0.0.0.0/0 le 32
...
```

Notice that the route collector is running in a private AS – there isn't really any need for it to use a public AS as the Collector does not need to be directly visible outside of the IXP.

Note also the inbound prefix filter blocking all prefixes on the eBGP session with the Route Collector. The Collector will not advertise any prefixes, by design. However, ISPs should never trust any other AS or its operator, so the inbound prefix filter is provided for safety, just in case of problems at the Route Collector.

10. **Connectivity Test.** Check connectivity throughout the IXP network. Each router team should be able to see all the other routers at the IXP. When you are satisfied that BGP is working correctly, try running traceroutes to check the paths being followed.

11. **Completed!** The IXP is now complete, up and running. The lab instructors will log into the route collector and show the prefixes visible. All 14 announcements should be clearly seen in the output of *sh ip bgp* on the route collector.

Checkpoint #3: *Compare your BGP routing table with that you see on the route collector. If you have missing prefixes, or some other problems, ask the lab demonstrators.*

12. **Summary.** This module has given an example of configurations used by Internet Service Providers at Internet Exchange Points. They have concentrated on using prefix-lists only – more sophisticated configurations are possible by using as-path filters and BGP communities. These examples are left to the reader to consider. If there is time at the end of the workshop, ask the Instructor to test out some other scenarios.

CONFIGURATION NOTES

Documentation is critical! You should record the configuration at each ***Checkpoint***, as well as the configuration at the end of the module.