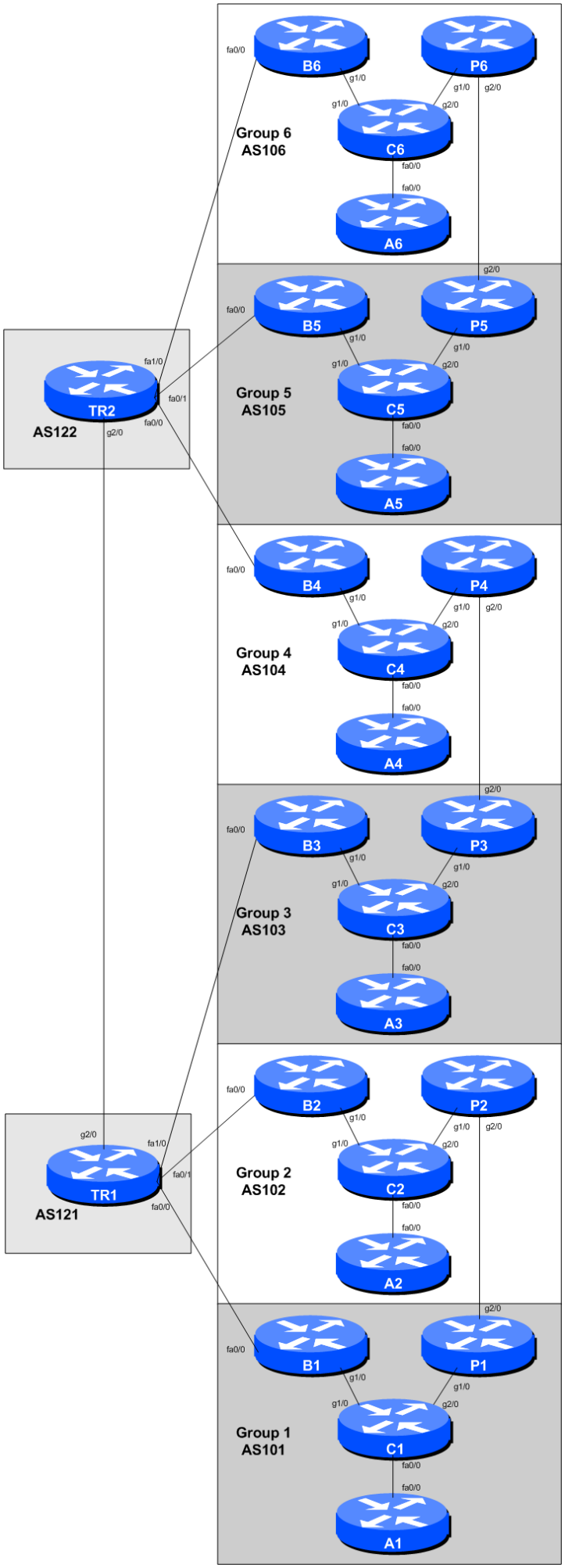
Peering & IXP Lab (Part 2: Private Peering)

The purpose of this part of the lab is to set up private peering between adjacent autonomous systems. In our case, AS101 will private peer with AS102, AS103 with AS104, and AS105 with AS106. We will use what we have learned so far to ensure that the adjacent ASNs only hear the routes they are meant to hear - a true private peering.

Lab Topology

The lab topology has been enhanced according to the diagram below. We simply add in the peering links mentioned in the preamble.


B6
P6
C6
A6
Group 6
AS106
B5
P5
C5
A5
Group 5
AS105
TR2
AS122
B4
P4
C4
A4
Group 4
AS104
B3
P3
C3
A3
Group 3
AS103
B2
P2
C2
A2
Group 2
AS102
TR1
AS121
B1
P1
C1
A1
Group 1
AS101
fa0/0
g1/0
g2/0
fa1/0
fa0/1

Configuring the Private Peering Links

Each group should now configure the private peering links as shown in the diagram.

Physical Link

Agree on which addresses should be used for the point to point links. Typically one group will contribute the IPv4 /30 and IPv6 /127 on the link.

```
interface GigabitEthernet 2/0
 description Link to Group 2 Peering Router
 ip address 100.68.10.25 255.255.255.252
 ipv6 address 2001:DB8:10:12::/127
!
```

Once the interfaces have been configured make sure that the links can be pinged on both IPv4 and IPv6 endpoints.

Configuring IS-IS

Do not configure IS-IS towards your private peer! They are not part of your autonomous system.

Configuring eBGP

We now configure eBGP with the private peer. Don’t forget to filter what you hear from the private peer, and what you send to them. You should only accept their address blocks from them (they may send you more by mistake!), and you should only send prefixes you originated!

Here is a configuration example for AS103 - note that we are reusing some configuration we have set up earlier:

```
ip prefix-list AS103-block permit 100.68.30.0/24
ipv6 prefix-list AS103-v6block permit 2001:DB8:30::/48
!
ip prefix-list AS104-block permit 100.68.40.0/24
ipv6 prefix-list AS104-v6block permit 2001:DB8:40::/48
!
router bgp 103
 address-family ipv4
  neighbor 100.68.30.26 remote-as 104
  neighbor 100.68.30.26 description eBGP with AS104
  neighbor 100.68.30.26 password cisco
  neighbor 100.68.30.26 prefix-list AS103-block out
  neighbor 100.68.30.26 prefix-list AS104-block in
```

```
!
 address-family ipv6
  neighbor 2001:DB8:30:12::1 remote-as 104
  neighbor 2001:DB8:30:12::1 description eBGP with AS104
  neighbor 2001:DB8:30:12::1 password cisco
  neighbor 2001:DB8:30:12::1 prefix-list AS103-v6block out
  neighbor 2001:DB8:30:12::1 prefix-list AS104-v6block in
!
```

Once this has been configured, you should now see your private peer originated routes coming from them, and you should be able to see your aggregate being sent to your private peer. The commands to see what you are receiving are:

```
show ip bgp neigh 100.68.30.26 routes
show bgp ipv6 uni neigh 2001:DB8:30:12::1 routes
```

and to show what you are sending:

```
show ip bgp neigh 100.68.30.26 advertised-routes
show bgp ipv6 uni neigh 2001:DB8:30:12::1 advertised-routes
```

Confirmation

Check on the Border, Core, Access and Peering Routers for what you now see in the BGP table.

What is the best path to your private peer? What does trace route tell you?

Hopefully you will see that the best path to your private peer will be via the private peering link. And the routes to the rest of the class will be via your upstream provider's default route. If this is not the case, you will need to start doing some troubleshooting!