Path Control

CCNP ROUTE: Implementing IP Routing

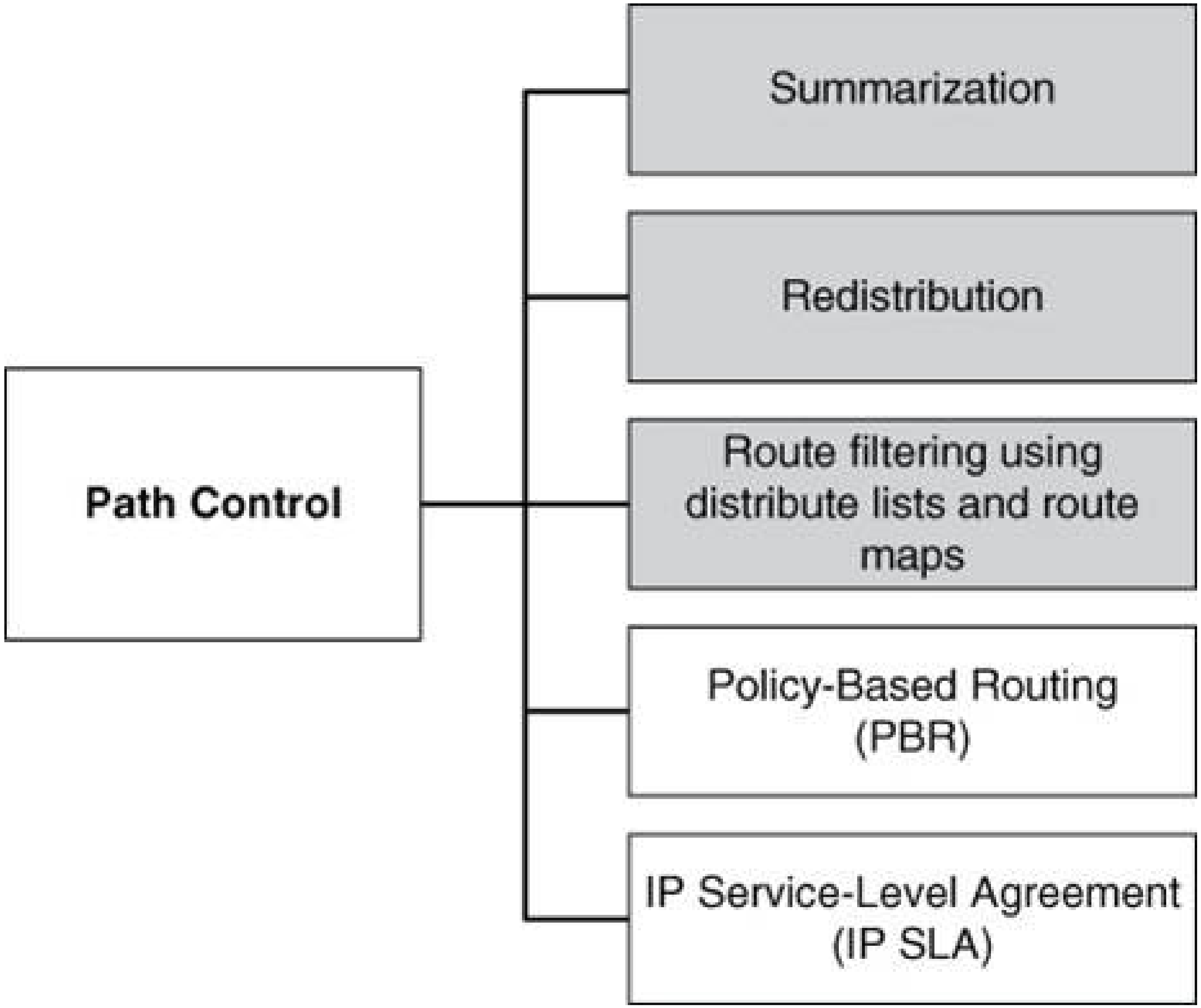
Objectives

- The need for different path control tools
- IP Service-Level Agreement (SLA) feature for path control
- Policy based routing (PBR) for path control

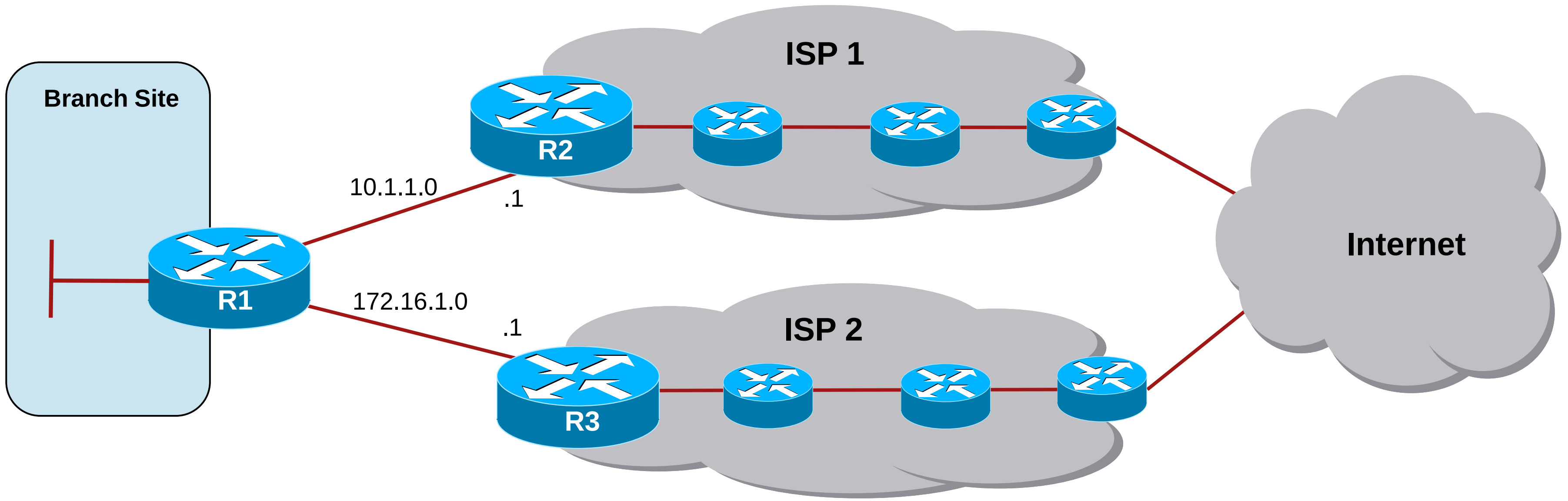
Path Control

- Redundancy is used to provide high availability
  - Does not automatically result in the backup link being used if the primary link fails
  - Resiliency is the ability to maintain an acceptable level of service when faults occur, to use the backup link if the primary fails
- Multiple routing protocols and redundant connectivity options can result in inefficient paths for forwarding packets to their destination
- Path control is required to avoid performance issues and to optimize paths
- Path control tools can be used to:
  - change the default destination forwarding and optimize the path of the packets for some specific applications
  - switching traffic to the backup link if there is a primary link failure, or forwarding some traffic to the backup link if the primary link is congested

Path Control Tools

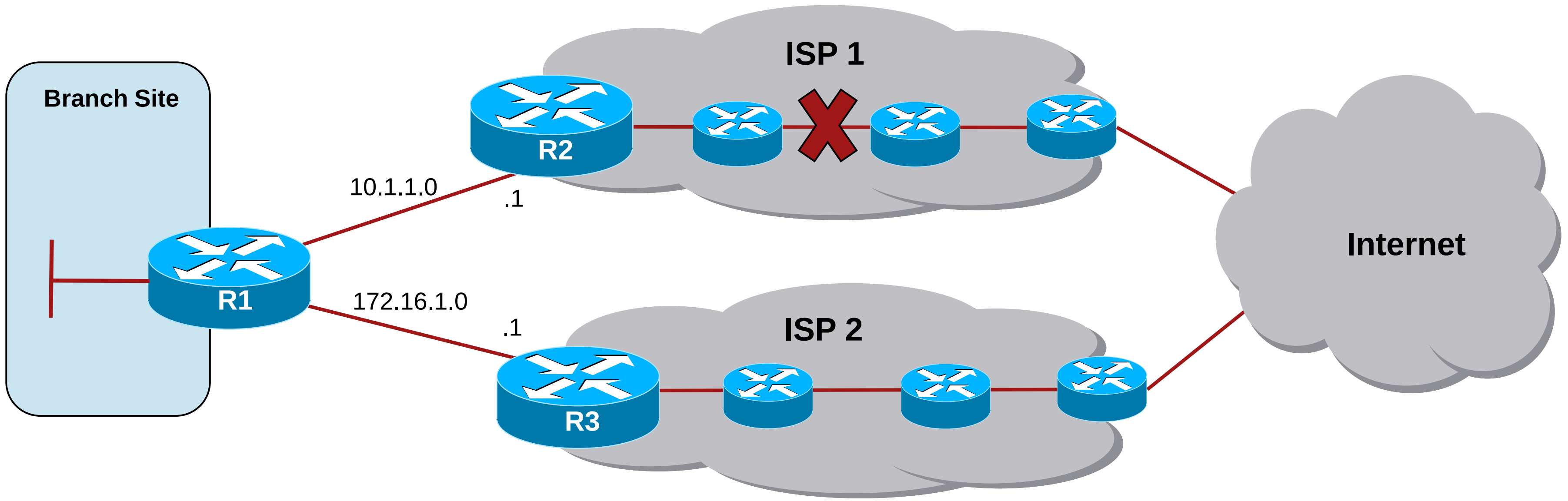


Path Control - Multihomed Scenario



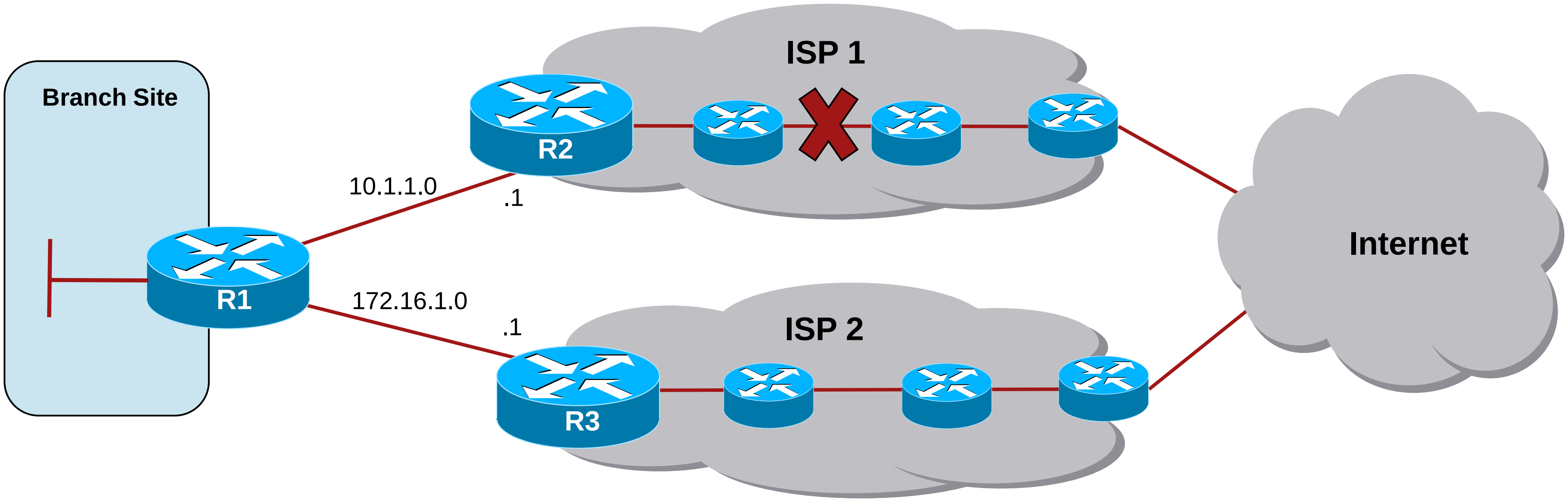
- Assume that R1 has a multihomed connection to the Internet through ISP1 and ISP2.
- Two equal cost default static routes on R1 enable the router to load balance over the two links on a per-destination basis.
  - R1 can detect if there is a direct failure on the link to one ISP, and in that case use the other ISP for all traffic.

Path Control - Multihomed Scenario



- However, what would happen if a link within the ISP 1 provider infrastructure were to fail?
  - The link from R1 to R2 would still remain up and R1 would continue to use that link because the static default route would still be valid.
- How can this situation be corrected?
  - Dynamic routing between R1 and the ISP networks; not practical.

Path Control - Multihomed Scenario



- A solution is to use either static routes or PBR on R1, but make them subject to reachability tests toward critical destinations, such as the DNS servers within the ISP.
  - If the DNS server in one of the ISPs goes down or is unreachable, the static route toward that ISP would be removed.
- These reachability tests can be performed with Cisco IOS IP SLAs.
  - IP SLA can be configured on R1 to probe the DNS servers frequently.
  - The IP SLA probes are attached to the static routes.

Path Control Using Cisco IOS IP SLAs

- Cisco IOS IP Service Level Agreements (SLAs) uses active traffic monitoring for measuring network performance.
- Cisco IOS IP SLAs send simulated data across the network and measure performance between network locations.
- The IP SLAs feature allows performance measurements to be taken to provide data about service levels for IP applications and services between:
  - Cisco devices
  - Cisco device and a host
- The IP SLAs feature can be configured either by the CLI or through an SNMP tool that supports IP SLAs operation.

Cisco IOS IP SLAs

- The information collected can measure:
  - Network resource availability
  - Response time
  - One-way latency
  - Jitter (inter-packet delay variance)
  - Packet loss
  - Voice-quality scoring
  - Application performance
  - Server response time

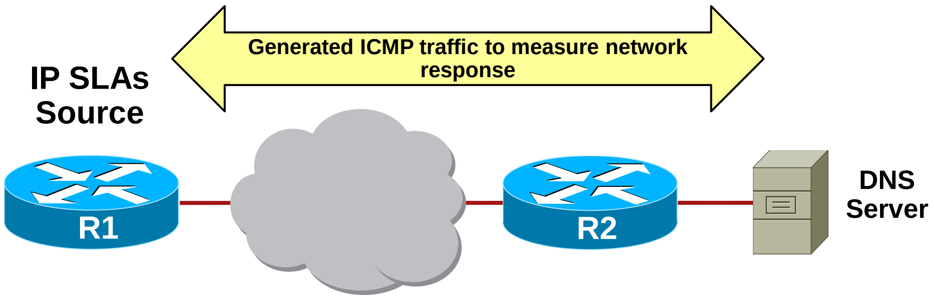
SLA - Sources, Responders, and Operations

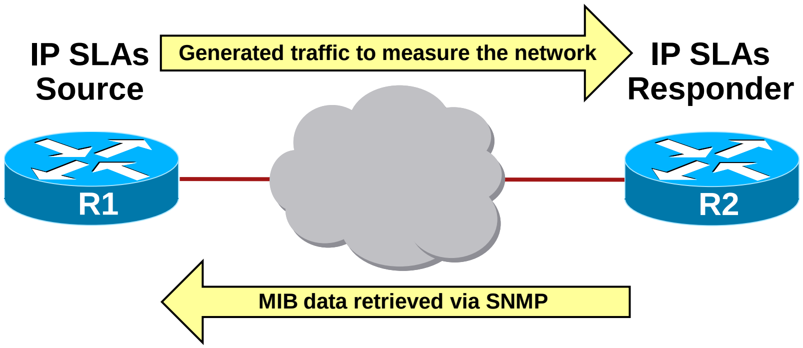
- The **IP SLAs source** sends probe packets to the target.
  - All the IP SLAs measurement probe operations are configured on the IP SLAs source (Cisco IOS Router).
  - The source uses the IP SLAs control protocol to communicate with the responder before sending test packets.
    - IP SLAs control messages support Message Digest 5 (MD5) authentication.
- An **IP SLAs responder,** embedded in a Cisco IOS device, allows it to respond to IP SLAs request packets.
- An **IP SLAs operation** is a measurement that includes protocol, frequency, traps, and thresholds.

SLAs Operations

There are two types of IP SLAs operations:

- Those in which the target device is not running the IP SLAs responder component (such as a web server or IP host).
  - Mostly ICMP generated traffic.
- Those in which the target device is running the IP SLAs responder component (such as a Cisco router).
  - Measurement accuracy is improved when the target is a responder.
  - Additional statistics can be gathered.

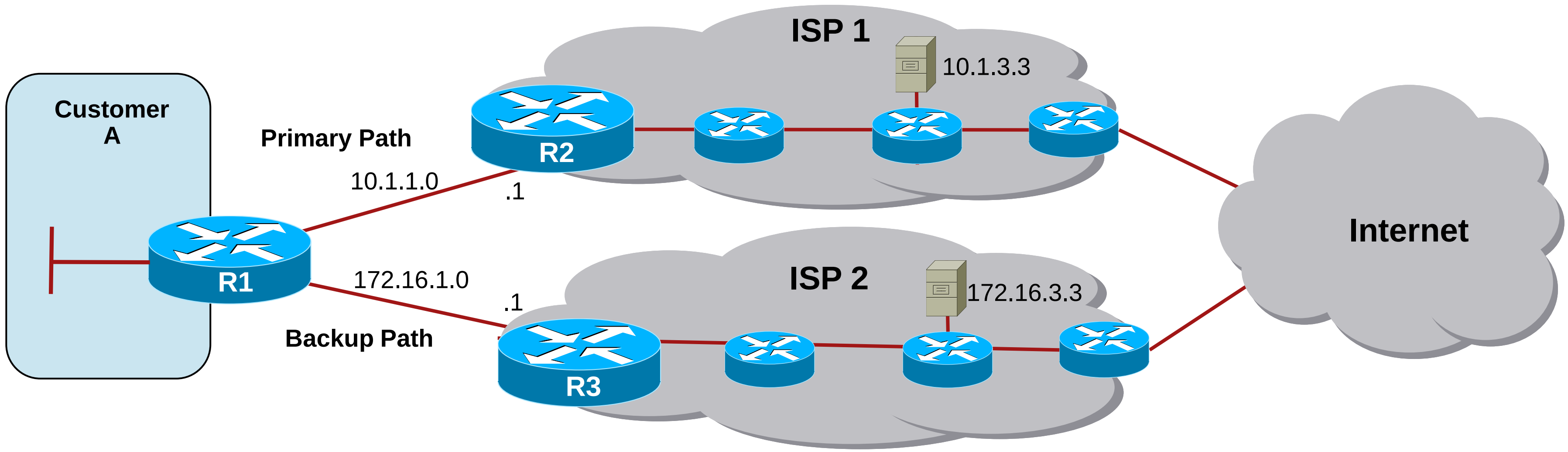




Steps to Configuring SLAs

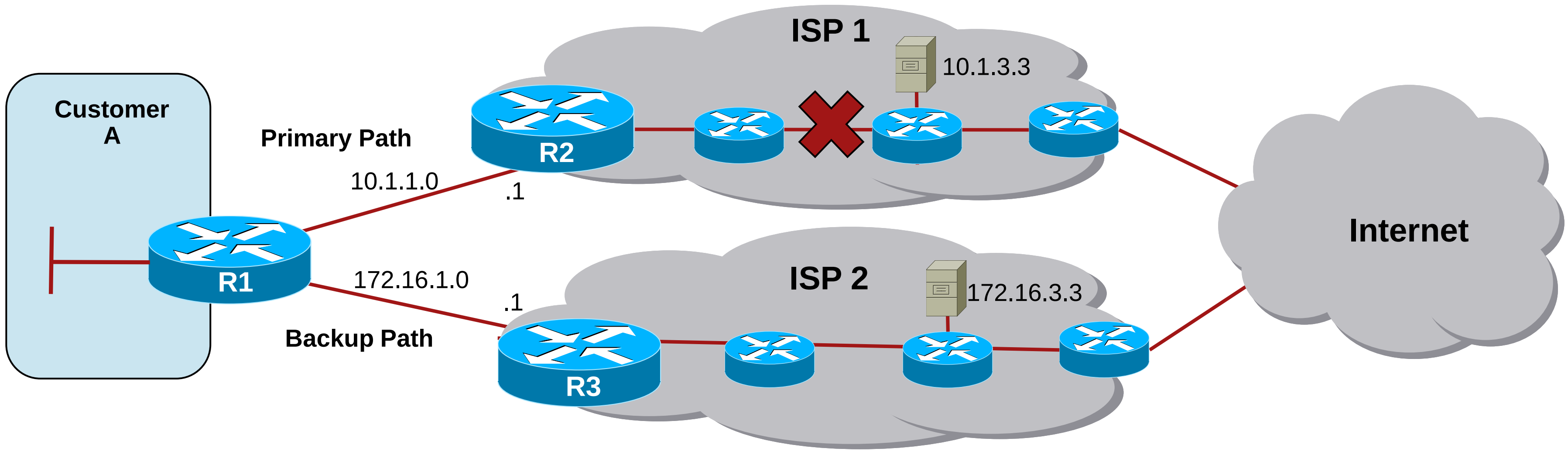
1. Define one or more IP SLAs operations (or probes).
2. Define one or more tracking objects, to track the state of IOS IP SLAs operations.
3. Define the action associated with the tracking object.

Tracking Reachability to Two ISPs - Example



- In this scenario, Customer A is multihoming to two ISPs using R1 which is configured with two default floating static routes.
  - The static route to R2 (ISP-1) has been given an administrative distance of 2 making it preferred and therefore the primary default route.
  - The static route to R3 (ISP-2) has been given an administrative distance of 3 making it the backup default route.

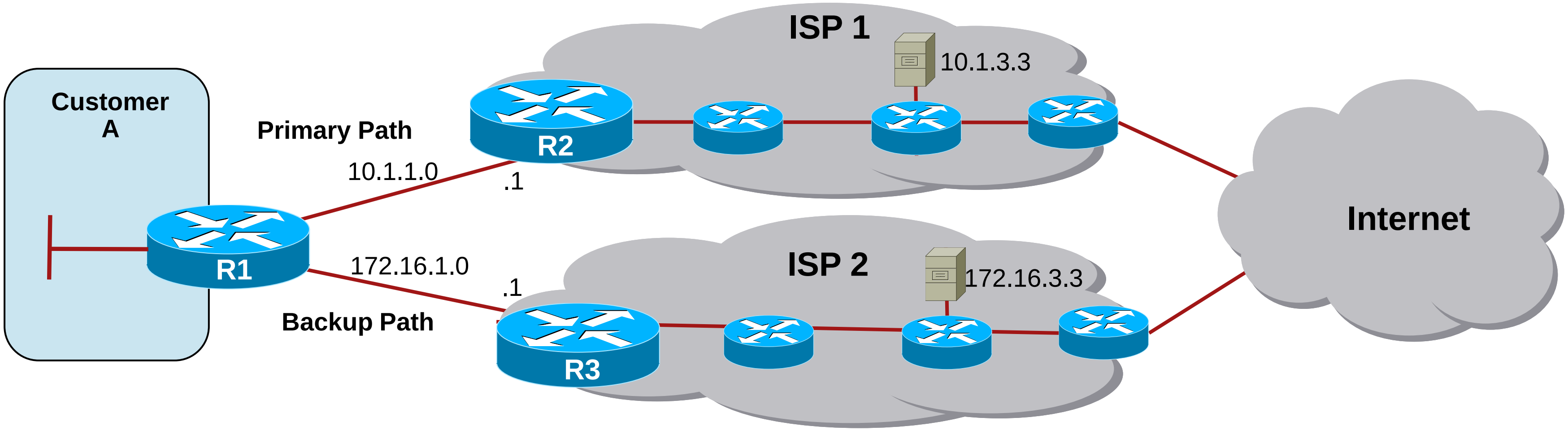
Tracking Reachability to Two ISPs - Example



- What would happen if a link within the ISP 1 provider infrastructure were to fail?
  - The link from R1 to R2 would still remain up and the R1 would continue to use that link because the default static route would still be valid.
- The solution to this issue is the Cisco IOS IP SLAs feature.
  - Configuring IP SLAs to continuously check the reachability of a specific destination (such as the ISP’s DNS server, or any other specific destination) and conditionally announce the default route only if the connectivity is verified.

Tracking Reachability to Two ISPs - Example

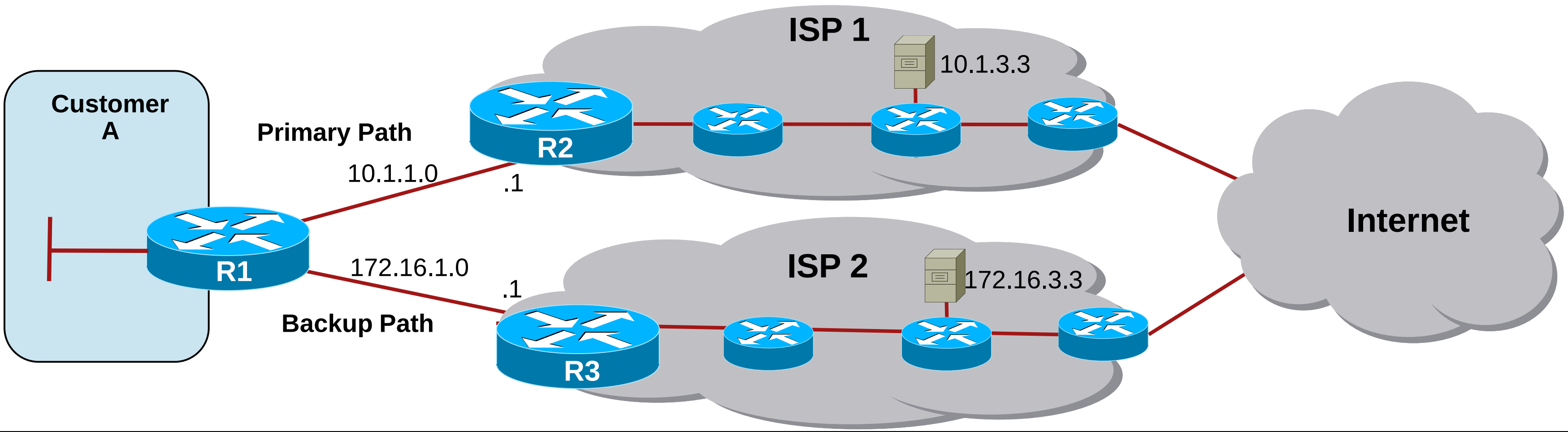
- IP SLA 11 continuously sends ICMP Echo Requests to the DNS server (10.1.3.3) every 10 seconds.
- IP SLAs is tracking that object and as long as the DNS server is reachable, the default route to R2 will be in the routing table.




```
R1(config)# ip sla 11
R1(config-ip-sla)# icmp-echo 10.1.3.3
R1(config-ip-sla-echo)# frequency 10
R1(config-ip-sla-echo)# exit
R1(config)# ip sla schedule 11 life forever start-time now
R1(config)# track 1 ip sla 11 reachability
R1(config-track)# delay down 10 up 1
R1(config-track)# exit
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.1 2 track 1
```

Tracking Reachability to Two ISPs - Example

- IP SLA 22 also continuously sends ICMP Echo Requests to the ISP 2 DNS server (172.16.3.3) every 10 seconds and as long as the ISP 2 DNS server is reachable, the default route to R3 will be floating.
- If the link to the ISP 1 DNS server ever fails, this second route would become active.




```
R1(config)# ip sla 22
R1(config-ip-sla)# icmp-echo 172.16.3.3
R1(config-ip-sla-echo)# frequency 10
R1(config-ip-sla-echo)# exit
R1(config)# ip sla schedule 22 life forever start-time now
R1(config)# track 2 ip sla 22 reachability
R1(config-track)# delay down 10 up 1
R1(config-track)# exit
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.1 3 track 2
```

Path Control Using PBR

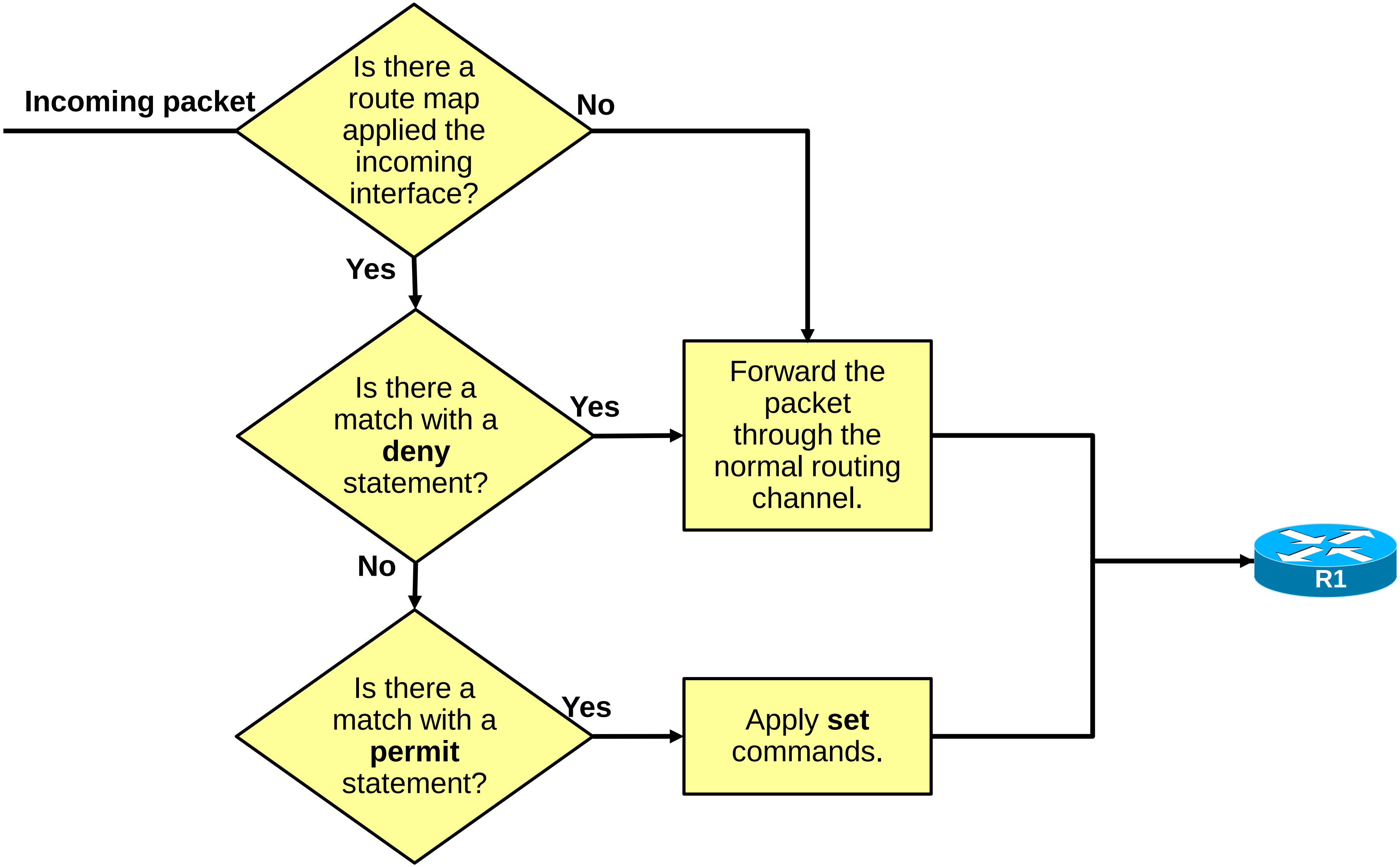
- Policy Based Routing (PBR) is used for redistribution.
  - PBR can also be used to define a routing policy other than basic destination-based routing using the routing table.
- Routers normally forward packets to destination addresses based on information in their routing tables.
  - PBR can be used to implement policies that selectively cause packets to take different paths based on source address, protocol types, or application types and override the router’s normal routing behavior.
- PBR provides an extremely powerful, simple, and flexible tool to implement solutions in cases where legal, contractual, or political constraints dictate that traffic be routed through specific paths.

Implementing PBR

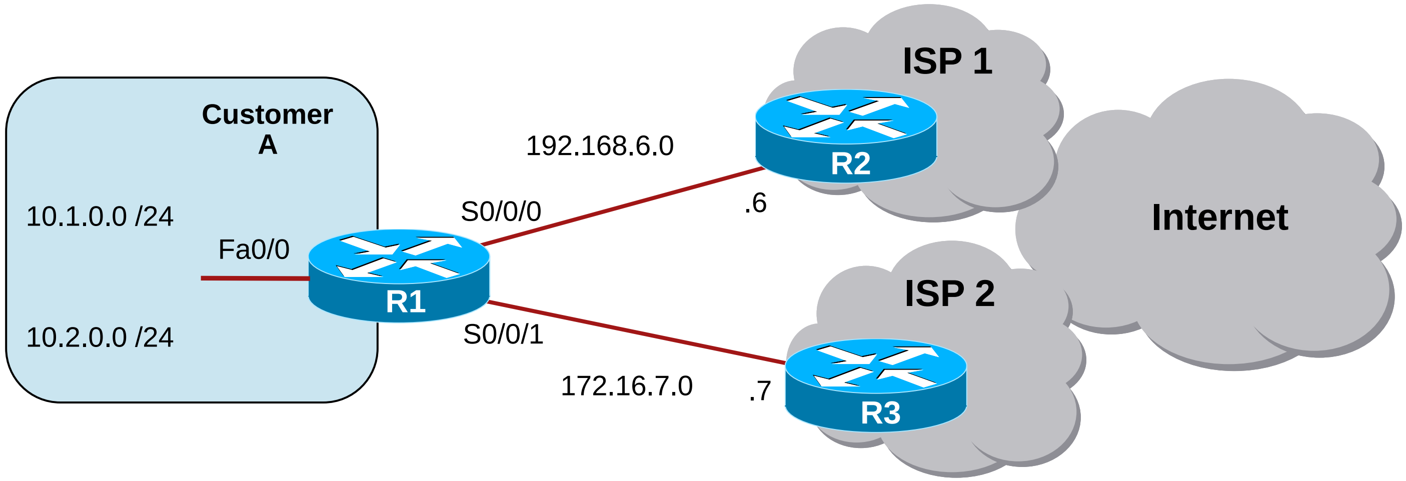
Sample implementation plan:

- Define and name the route map with the **`route-map`** command.
  - Define the conditions to match (the **`match`** statements).
  - Define the action to be taken when there is a match (the **`set`** statements).
- Define which interface the route map will be attached to using the **`ip policy route-map`** interface configuration command.
  - PBR is applied to incoming packets.
- Verify path control results.

Logical PBR Operation

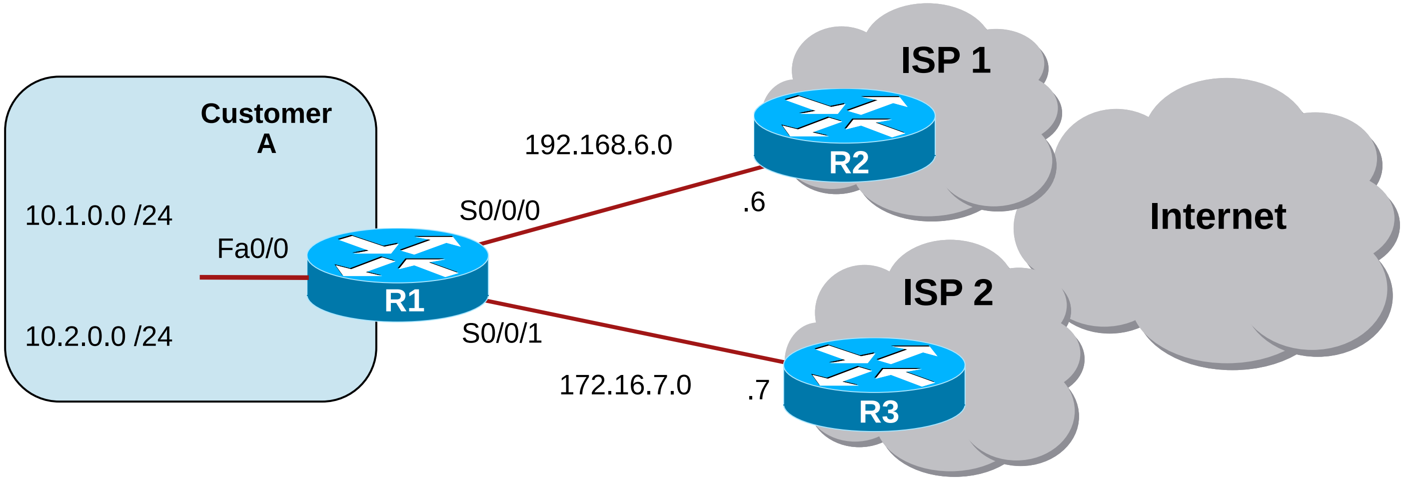


Using PBR When Multihoming - Example



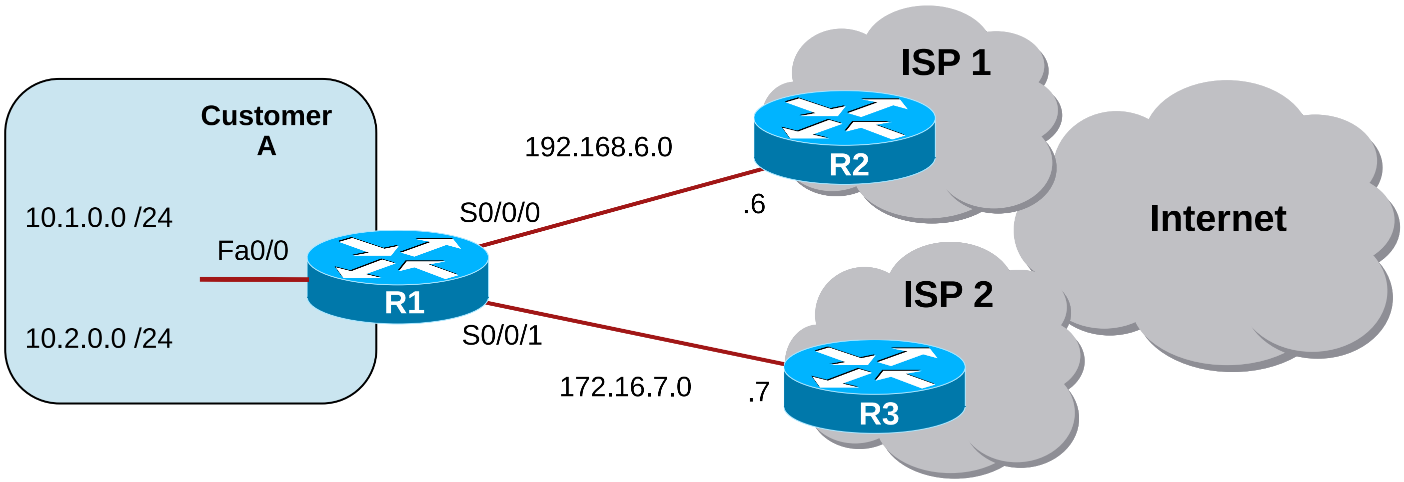

```
R1(config)# access-list 1 permit 10.1.0.0 0.0.0.255
R1(config)# access-list 2 permit 10.2.0.0 0.0.0.255
R1(config)# route-map EQUAL-ACCESS permit 10
R1(config-route-map) # match ip address 1
R1(config-route-map)# set ip default next-hop 192.168.6.6
R1(config-route-map)# route-map EQUAL-ACCESS permit 20
R1(config-route-map)# match ip address 2
R1(config-route-map)# set ip default next-hop 172.16.7.7
R1(config-route-map)# route-map EQUAL-ACCESS permit 30
R1(config-route-map)# set default interface null0
R1(config-route-map)# exit
R1(config)# interface FastEthernet 0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# ip policy route-map EQUAL-ACCESS
R1(config-if)# exit
```

Verifying PBR - Example




```
R1# show ip policy
Interface          Route map
FastEthernet0/0    EQUAL-ACCESS
R1#
```

Verifying PBR - Example




```
R1# show route-map
route-map EQUAL-ACCESS, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
  Set clauses:
    ip default next-hop 192.168.6.6
Policy routing matches: 3 packets, 168 bytes
route-map EQUAL-ACCESS, permit, sequence 20
  Match clauses:
    ip address (access-lists): 2
  Set clauses:
    ip default next-hop 172.16.7.7
route-map EQUAL-ACCESS, permit, sequence 30
Set clauses:
    default interface null0
```

Cisco | Networking Academy®
Mind Wide Open™