Chapter 5:

Implementing Path Control

- CCNP-RS ROUTE

Chapter 5 Objectives

- Describe how the various path control methods affect traffic.
- Configure offset-lists for path control.
- Configure the IP Service-Level Agreement feature for path control.
- Configure policy based routing for path control.
- Describe advanced path control tools.

Understanding Path Control

Assessing Path Control Network Performance

- Focus of this chapter is on how to control the path that traffic takes through a network.
  - In some cases, there might be only one way for traffic to go.
  - However, most modern network include redundant paths and network administrators may want to control which way certain traffic flows.
- The choice of routing protocol(s) used in a network is one factor in defining how paths are selected;
  - For example, different administrative distances, metrics, and convergence times may result in different paths being selected.
  - As well, recall that when multiple routing protocols are implemented, inefficient routing may result.
- There are other considerations.

Network Redundancy Considerations

- **Resiliency:**
  - The ability to maintain an acceptable level of service when faults occur.
  - Having redundancy does not guarantee resiliency.
- **Availability**:
  - The time required for a routing protocol to learn about a backup path when a primary link fails is the convergence time.
  - If the convergence time is relatively long, some applications may time out.
  - Use a fast-converging routing protocol.
- **Adaptability**:
  - The network's ability to adapt to changing conditions such as a link failure.
- **Performance:**
  - Routers should be tuned to load share across multiple links to make efficient use of the bandwidth.

Network Redundancy Considerations

- **Support for network and application services:**
  - More advanced path control solutions involve adjusting routing for specific services, such as security, optimization, and quality of service (QoS).
- **Predictability:**
  - The path control solution implemented should derive from an overall strategy, so that the results are deterministic and predictable.
- **Asymmetric traffic:**
  - Is traffic that flows on one path in one direction and on a different path in the opposite direction, occurs in many networks that have redundant paths.
  - It is often a *desirable* network trait, because it can be configured to use the available bandwidth effectively.
  - BGP includes a good set of tools to control traffic in both directions on an Internet connection.

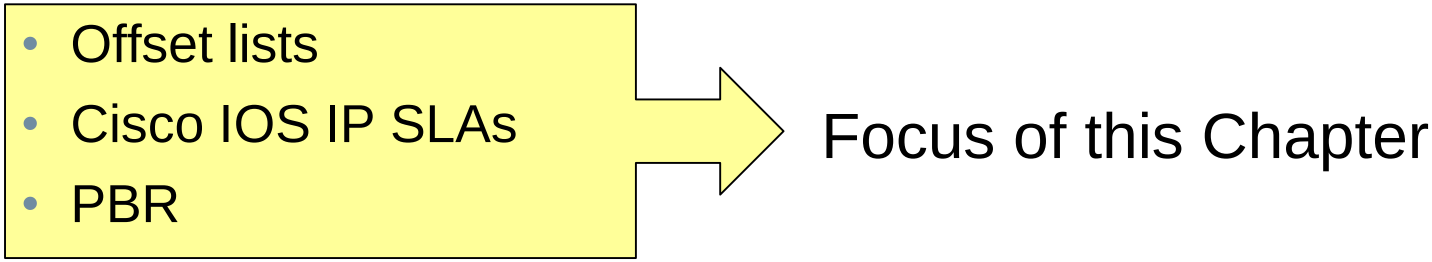
Path Control Tools

- A good addressing design.
- Redistribution and other routing protocol characteristics.

Characteristic	OSPF	EIGRP
Route Marking	Tags for external routes can be added at distribution points	Tags for all routes can be configured
Metric	Can be changed for external routes at redistribution points	Can be set using route maps
Next hop	Can be changed for external routes at redistribution points	Can be set for all routes under various conditions
Filtering	Summary information can be filtered at ABRs and ASBRs	Can be configured anywhere for any routes
Route summarization	Can be configured only on ABRs and ASBRs	Can be configured anywhere for any routes; auto summarization is on by default
Unequal cost load balancing	Not available	Available, with variance command.

Path Control Tools

- Tools already covered:
  - Passive interfaces
  - Distribute lists
  - Prefix lists
  - Administrative distance
  - Route maps
  - Route tagging
- Advanced Tools:

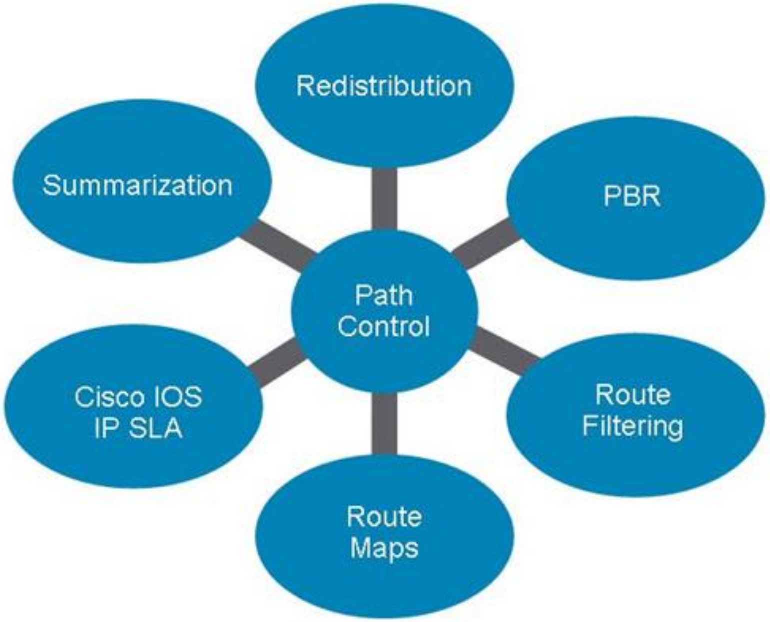


  - Offset lists
  - Cisco IOS IP SLAs
  - PBR

Focus of this Chapter

Path Control Strategy

- All of these tools can be used as part of an integrated strategy to implement path control.
- However, it is important to have a strategy before implementing specific path control tools and technologies.



Implementing Path Control using Offset-Lists

Path Control Using Offset Lists

- An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via EIGRP or Routing Information Protocol (RIP).
  - Optionally, an offset list can be limited by specifying either an access list or an interface.
- To create an offset-list, use the **`offset-list`** router configuration command.
  - The offset value is added to the routing metric.

Defining an Offset-List

- Define an offset list.

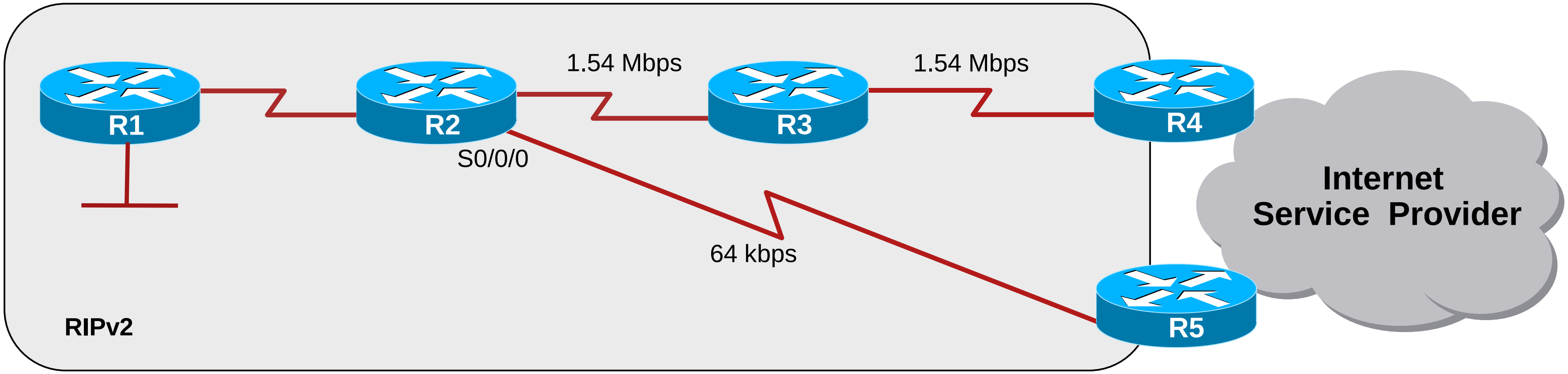
```
Router(config-router)#
```

```
offset-list {access-list-number | access-list-name} {in | out}
  offset [interface-type interface-number]
```

Parameter	Description
access-list-number | access-list-name	Standard access list number or name to be applied. Access list number 0 indicates all access lists. If the offset value is 0, no action is taken.
in	Applies the access list to incoming metrics.
out	Applies the access list to outgoing metrics.
offset	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken
interface-type interface-number	(Optional) Interface type and number to which the offset list is applied.

Offset List for Path Control

- Users on the R1 LAN can access the Internet through routers R4 or R5.
  - Notice that R5 is only one hop away from R2 and therefore the preferred RIP route. However, the R2 to R5 link is a very slow link.
- The configured offset list and ACL on R2 ensures the preferred path to reach the 172.16.0.0 network will be towards router R4.
  - The offset-list adds an offset of 2 to the metric of the routes learned from R5.



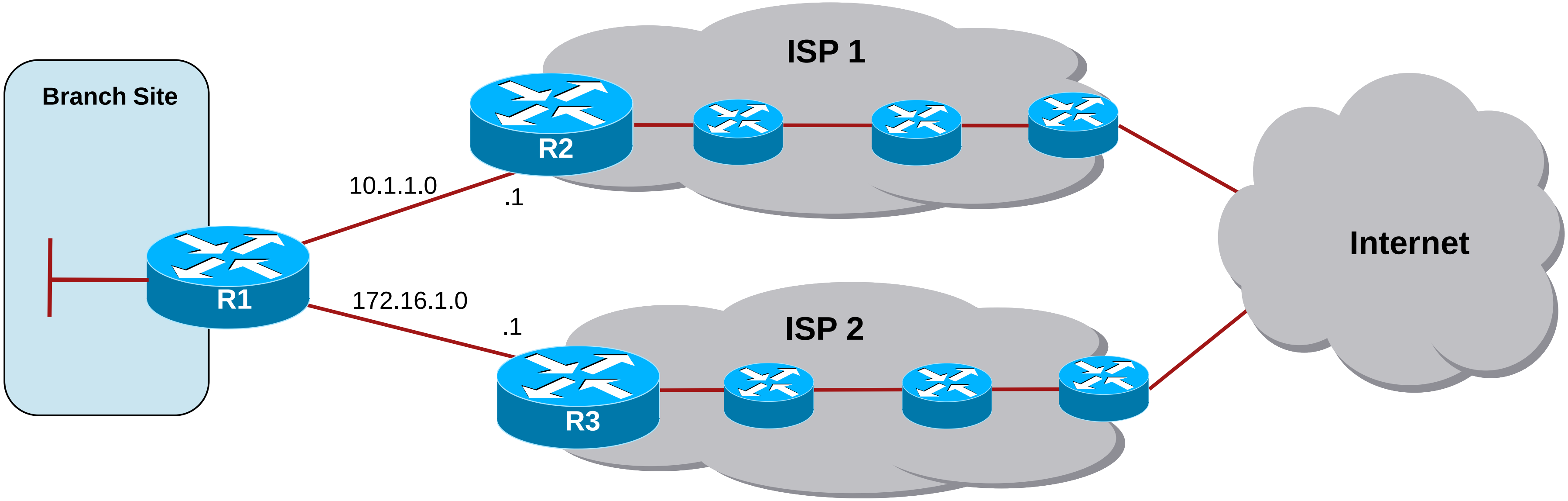
```
R2(config)# access-list 21 permit 172.16.0.0 0.0.255.255
R2(config)# router rip
R2(config-router)# offset-list 21 in 2 serial 0/0/0
```

Verifying Offset Lists

- Use the **`traceroute`** EXEC to verify that an offset list is affecting the path that traffic takes.
- Use the **`show ip route`** command to identify the metrics for learned routes.
- For EIGRP, use the **`show ip eigrp topology`** command to examine the EIGRP topology table.
- Debug commands to use include **`debug ip eigrp`** and **`debug ip rip`**.

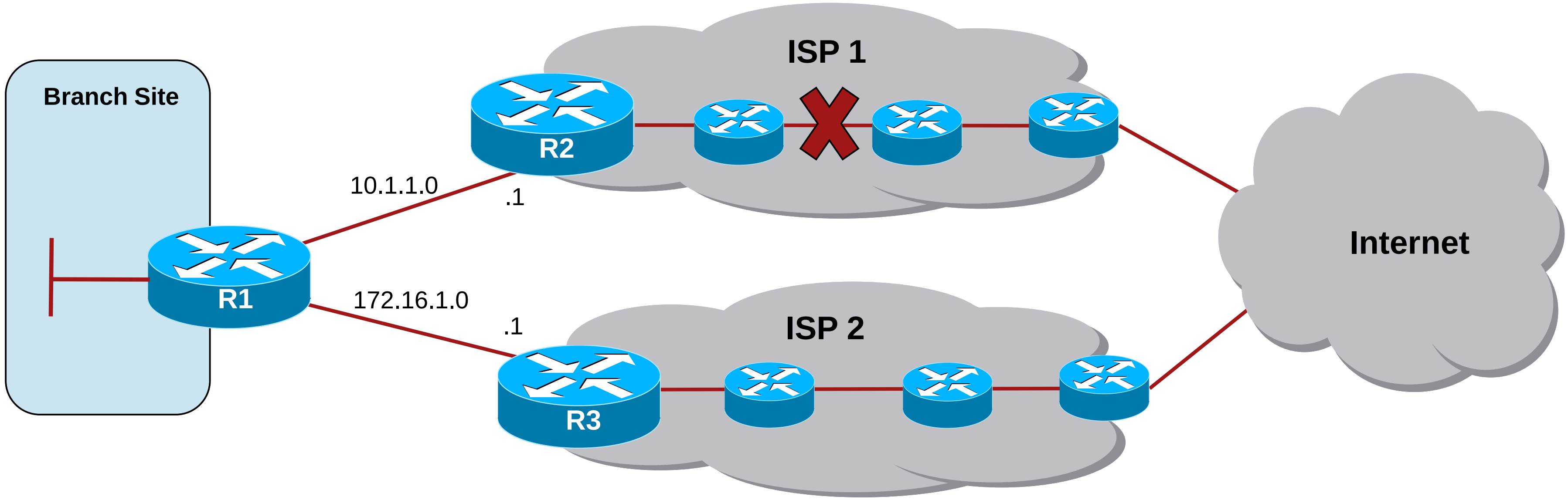
Implementing Path Control using IOS IP SLAs

Multihomed Scenario



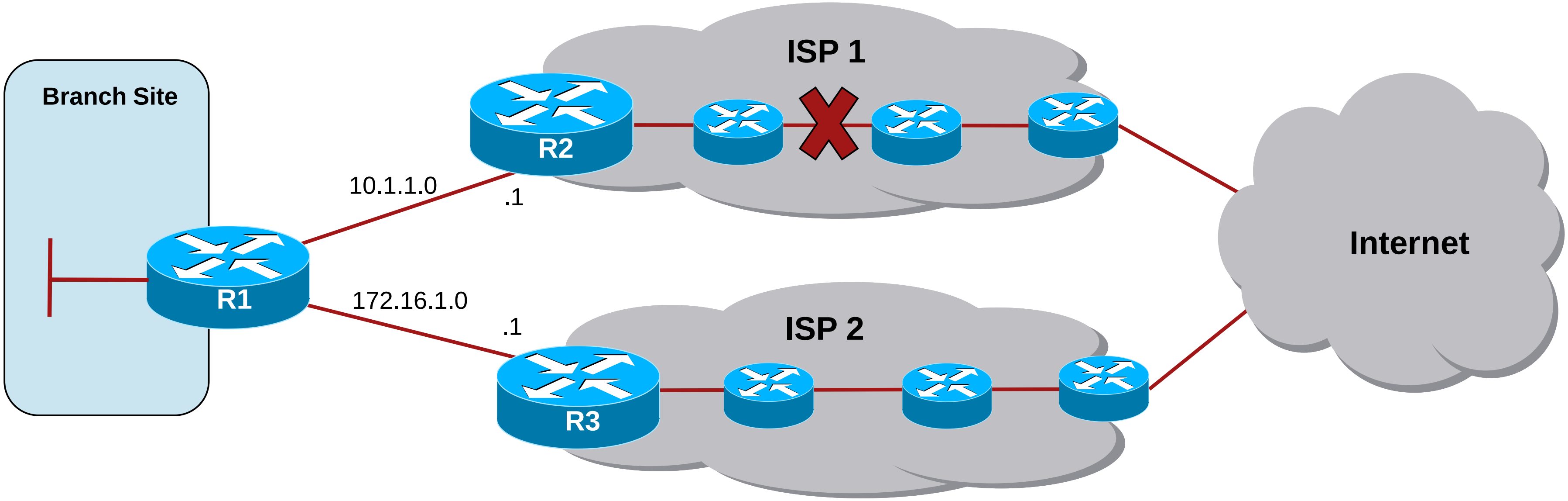
- Assume that R1 has a multihomed connection to the Internet through ISP1 and ISP2.
- Two equal cost default static routes on R1 enable the Cisco IOS to load balance over the two links on a per-destination basis.
  - R1 can detect if there is a direct failure on the link to one ISP, and in that case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

Multihomed Scenario



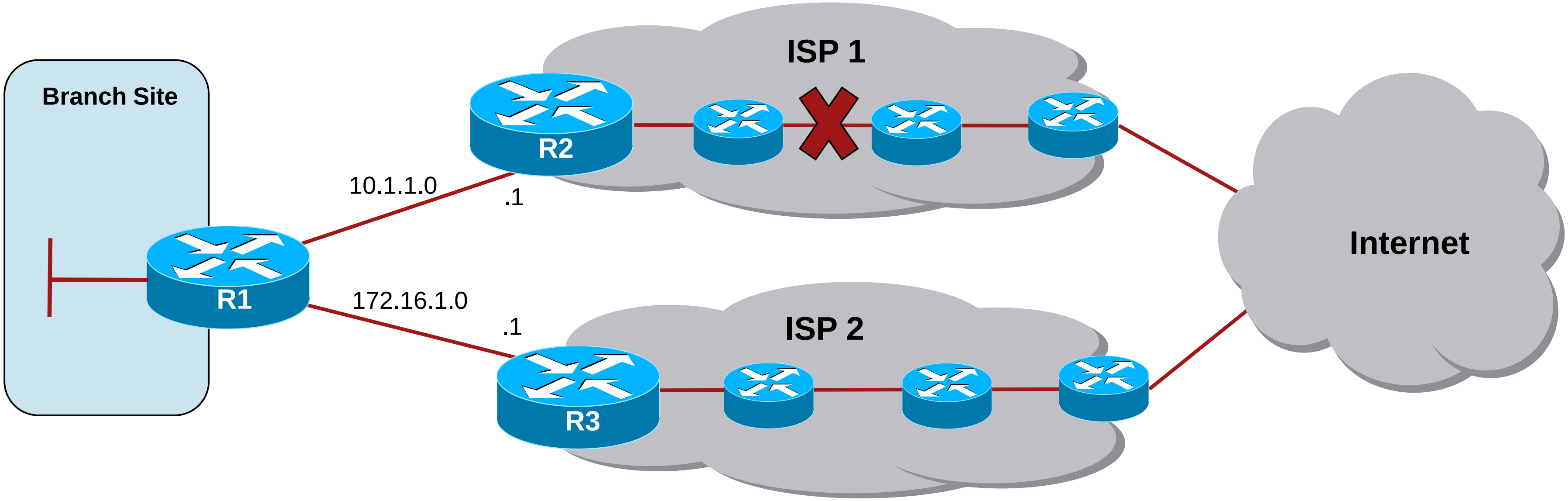
- However, what would happen if a link within the ISP 1 provider infrastructure were to fail?
  - The link from R1 to R2 would still remain up and the R1 would continue to use that link because the static default route would still be valid.
- How can this situation be corrected?
  - Dynamic routing between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

Multihomed Scenario



- Another 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 servers in one of the ISPs go down or are 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.

Multihomed Scenario – IP SLAs Tools



- **Object tracking:**
  - Track the reachability of specified objects (e.g., DNS server).
- **Cisco IOS IP SLAs probes:**
  - Cisco IOS IP SLAs can send different types of probes toward the desired objects.
- **Associate the tracked results to the routing process:**
  - **PBR (route maps)** can be used to define specific traffic classes, such as voice, or specific applications.
  - **Static routes** with tracking options provide a simpler alternative to PBR.

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 (interpacket delay variance)
  - Packet loss
  - Voice-quality scoring
  - Application performance
  - Server response time

IP SLAs Applications

- Provide SLA monitoring, measurement, and verification.
  - Voice over IP (VoIP) and MPLS performance monitoring
  - Edge-to-edge network availability monitoring
- Verify quality of service (QoS).
  - Measures the jitter, latency, or packet loss in the network.
  - Provides continuous, reliable, and predictable measurements.
- Ease the deployment of new services.
  - Verifies that the existing QoS is sufficient for new IP services.
- Assist administrators with network troubleshooting.
  - Provides consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.

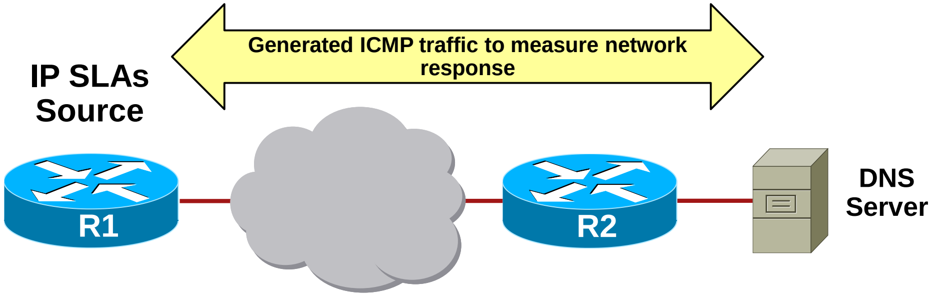
Sources, Responders, and Operations

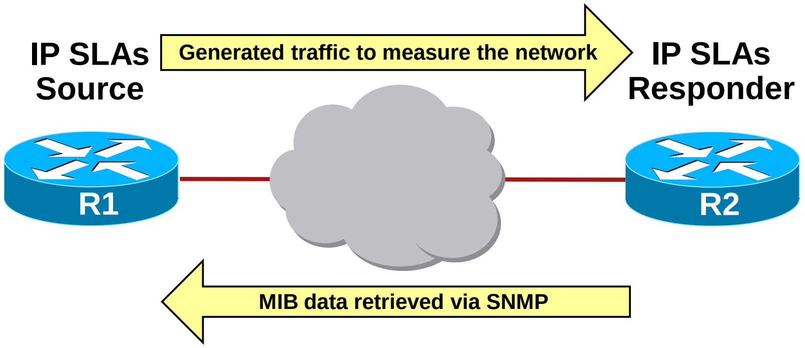
- The **IP SLAs source** sends probe packets to the target.
  - All the IP SLAs measurement probe operations are configured on the IP SLAs source (Cisco IOS Router).
  - The source uses the IP SLAs control protocol to communicate with the responder before sending test packets.
    - IP SLAs control messages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

IP 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.




IP SLAs Source
Generated traffic to measure the network
IP SLAs Responder
R1
R2
MIB data retrieved via SNMP

Steps to Configuring IP 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.

- Note:
  - Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **`ip sla monitor`** command is replaced by the **`ip sla`** command.

Define an IP SLA Operation

- Define an IP SLA object and enter IP SLA configuration mode.

```
Router(config)#
```

```
ip sla operation-number
```

- The *operation-number* is the identification number of the IP SLAs operation you want to configure.
- Once entered, the router prompt changes to IP SLA configuration mode.

`ip sla` Command Example

- Although many command options exist, the focus of this section will be on configuring Source to Non-responder target.
  - For this reason the **`icmp-echo`** command will be explored.

```
R1(config)# ip sla 1
R1(config-ip-sla)# ?
IP SLAs entry configuration commands:
  dhcp          DHCP Operation
  dns           DNS Query Operation
  exit          Exit Operation Configuration
  frame-relay   Frame-relay Operation
  ftp           FTP Operation
  http          HTTP Operation
  icmp-echo     ICMP Echo Operation
  icmp-jitter   ICMP Jitter Operation
  path-echo     Path Discovered ICMP Echo Operation
  path-jitter   Path Discovered ICMP Jitter Operation
  slm           SLM Operation
  tcp-connect   TCP Connect Operation
  udp-echo      UDP Echo Operation
  udp-jitter    UDP Jitter Operation
  voip          Voice Over IP Operation

R1(config-ip-sla)#
```

Defining an IP SLAs ICMP Echo Operation

- Define an ICMP echo operation from source to non-responder target.

```
Router(config-ip-sla)#
```

```
icmp-echo {destination-ip-address | destination-hostname} [source-
  ip {ip-address | hostname} | source-interface interface-name]
```

Parameter	Description
destination-ip-address | *destination-hostname*	Destination IPv4 or IPv6 address or hostname.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IPv4 or IPv6 address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-interface *interface-name*	(Optional) Specifies the source interface for the operation.

Note:

- Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **type echo protocol ipIcmpEcho** command is replaced by the **icmp-echo** command.

icmp-echo Command Example

```
R1(config-ip-sla)# icmp-echo 209.165.201.30
R1(config-ip-sla-echo)# ?

IP SLAs echo Configuration Commands:
  default              Set a command to its defaults
  exit                 Exit operation configuration
  frequency            Frequency of an operation
  history              History and Distribution Data
  no                   Negate a command or set its defaults
  owner                Owner of Entry
  request-data-size    Request data size
  tag                  User defined tag
  threshold            Operation threshold in milliseconds
  timeout              Timeout of an operation
  tos                  Type Of Service
  verify-data          Verify data
  vrf                  Configure IP SLAs for a VPN Routing/Forwarding in-stance

R1(config-ip-sla-echo)#
```

- Although many command options exist, the focus of this section will be on **`frequency`** and **`timeout`** commands.

`icmp-echo` Sub-Commands

```
Router(config-ip-sla-echo)#
```

```
frequency seconds
```

- Set the rate at which a specified IP SLAs operation repeats.
  - The *`seconds`* parameter is the number of seconds between the IP SLAs operations with the default being 60 seconds.

```
Router(config-ip-sla-echo)#
```

```
timeout milliseconds
```

- Set the amount of time a Cisco IOS IP SLAs operation waits for a response from its request packet.
  - The *`milliseconds`* parameter is the number of milliseconds (ms) the operation waits to receive a response from its request packet.

Schedule an IP SLA Operation

- Schedule an IP SLA operation.

```
Router(config)#
```

```
ip sla schedule operation-number [life {forever | seconds}]
  [start-time {hh:mm[:ss] [month day | day month] | pending |
  now | after hh:mm:ss}] [ageout seconds] [recurring]]
```

Note:

- Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SB, and 12.2(33)SXI, the **`ip sla monitor schedule`** command is replaced by the **`ip sla schedule`** command.

The **ip sla schedule** Command Parameters

Parameter	Description
operation-number	Number of the IP SLAs operation to schedule.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
start-time	(Optional) Time when the operation starts.
hh:*mm*[:*ss*]	Specifies an absolute start time using hour, minute, and (optionally) second. Use the 24-hour clock notation.
month	(Optional) Name of the month to start the operation in. If month is not specified, the current month is used.
day	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used.
pending	(Optional) No information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.
after *hh:mm:ss*	(Optional) Indicates that the operation should start this amount of time after this command was entered.
ageout *seconds*	(Optional) Number of seconds to keep the operation in memory when it is not actively collecting information (default is 0 seconds which means it never ages out).
recurring	(Optional) Indicates that the operation will start automatically at the specified time and for the specified duration every day.

Configure IP SLA Object Tracking

- Define tracking objects, to track the state of IP SLAs operations.

```
Router(config)#
```

```
track object-number ip sla operation-number {state |
  reachability}
```

Parameter	Description
object-number	Object number representing the object to be tracked. The range is from 1 to 500.
operation-number	Number used for the identification of the IP SLAs operation you are tracking.
state	Tracks the operation return code.
reachability	Tracks whether the route is reachable.

Note:

- Effective with Cisco IOS Release 12.4(20)T, 12.2(33)SXI1, 12.2(33)SRE and Cisco IOS XE Release 2.4, the **track rtr** command is replaced by the **track ip sla** command.

track Command Example

```
R1(config)# track 1 ip sla 1 reachability
R1(config-track)# ?
Tracking instance configuration commands:
  default   Set a command to its defaults
  delay     Tracking delay
  exit      Exit from tracking configuration mode
  no        Negate a command or set its defaults

R1(config-track)#
```

Configure Tracking Delay

- Specify a period of time to delay communicating state changes of a tracked object.

```
Router(config-track)#
```

```
delay {up seconds [down seconds] | [up seconds] down seconds}
```

Parameter	Description
up	Time to delay the notification of an up event.
down	Time to delay the notification of a down event.
seconds	Delay value, in seconds. The range is from 0 to 180 with the default being 0.

Static Routing and IP SLAs

- Configure a static route for IP SLAs tracking.

```
Router(config)#
```

```
ip route prefix mask address interface dhcp distance name
  next-hop-name permanent track number tag tag
```

Parameter	Description
prefix mask	The IP network and subnet mask for the remote network to be entered into the IP routing table.
address	The IP address of the next hop that can be used to reach the destination network.
interface	The local router outbound interface to be used to reach the destination network.
dhcp	(Optional) Enables a DHCP server to assign a static route to a default gateway.
distance	(Optional) The administrative distance to be assigned to this route.
name *next-hop-name*	(Optional) Applies a name to the specified route.
permanent	(Optional) Specifies that the route will not be removed from the routing table even if the interface associated with the route goes down.
track *number*	(Optional) Associates a track object with this route. Valid values for the number argument range from 1 to 500.
tag *tag*	(Optional) A value that can be used as a match value in route maps.

Verifying IP SLAs

Command	Description
show ip sla configuration [*operation***]**	Display configuration values including all defaults for all Cisco IOS IP SLAs operations, or for a specified operation. The *operation* parameter is the number of the IP SLAs operation for which the details will be displayed.
show ip sla statistics [*operation-number* **| details]**	Display the current operational status and statistics of all Cisco IOS IP SLAs operations, or of a specified operation.

show ip sla configuration Example

```
R1# show ip sla configuration 1
IP SLAs, Infrastructure Engine-II.
Entry number: 1
Owner:
Tag:
Type of operation to perform: icmp-echo
Target address/Source address: 209.165.201.30/0.0.0.0
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 10 (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
<output omitted>
```

Note:

- Effective with Cisco IOS Release 12.4(20)T, 12.2(33)SXI1, 12.2(33)SRE and Cisco IOS XE Release 2.4, the **`show ip sla monitor configuration`** command is replaced by the **`show ip sla configuration`** command.

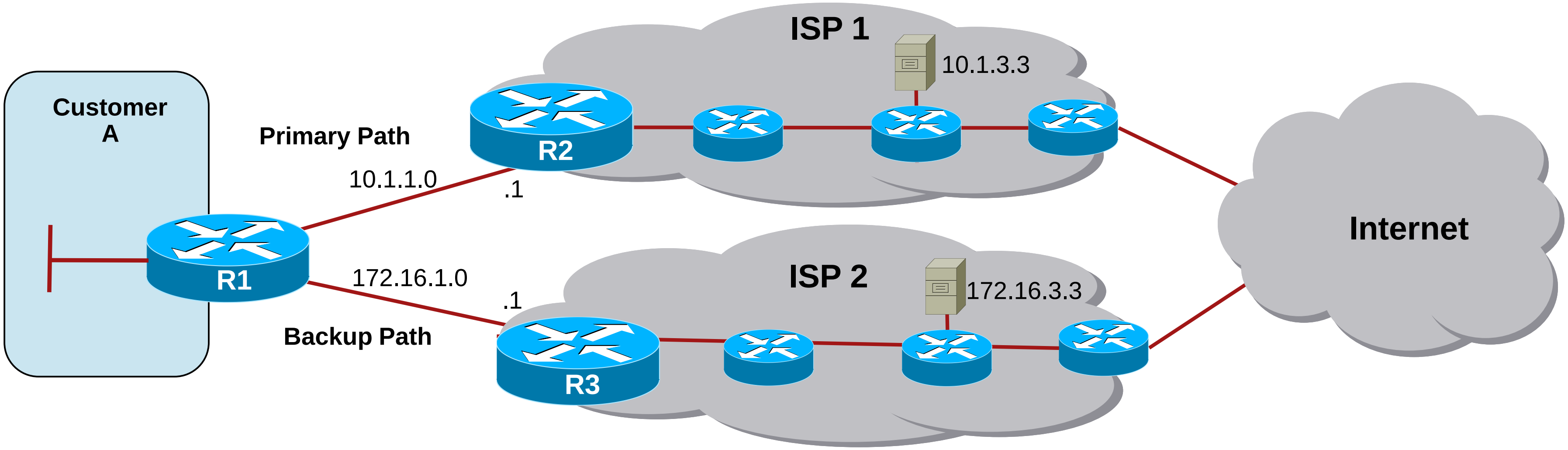
show ip sla statistics Example

```
R1# show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1

Latest operation start time: *21:22:29.707 UTC Fri Apr 2 2010
Latest operation return code: OK
Number of successes: 5
Number of failures: 0
Operation time to live: Forever
<output omitted>
```

Note:

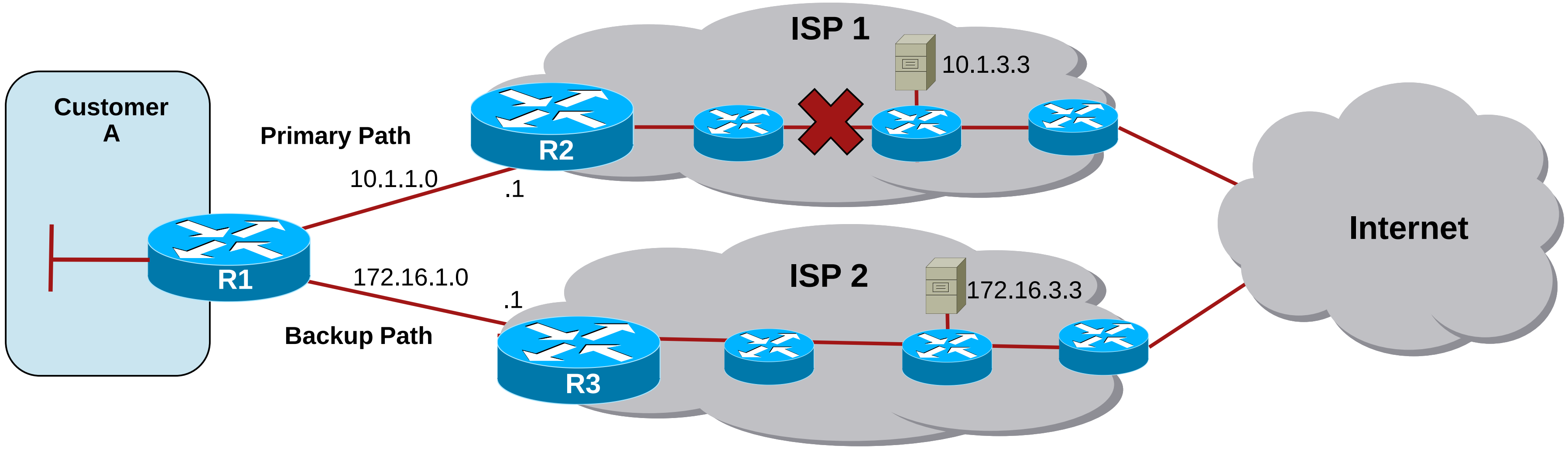
- Effective with Cisco IOS Release 12.4(20)T, 12.2(33)SXI1, 12.2(33)SRE and Cisco IOS XE Release 2.4, the **`show ip sla monitor statisitcs`** command is replaced by the **`show ip sla statistics`** command.

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.

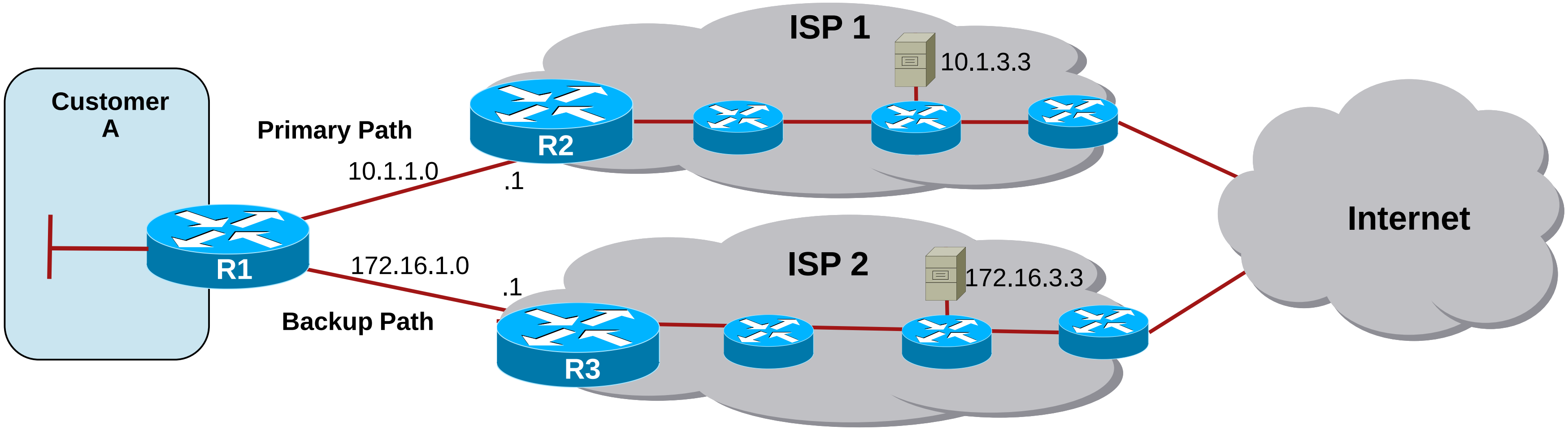
Tracking Reachability to Two ISPs Example



- 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

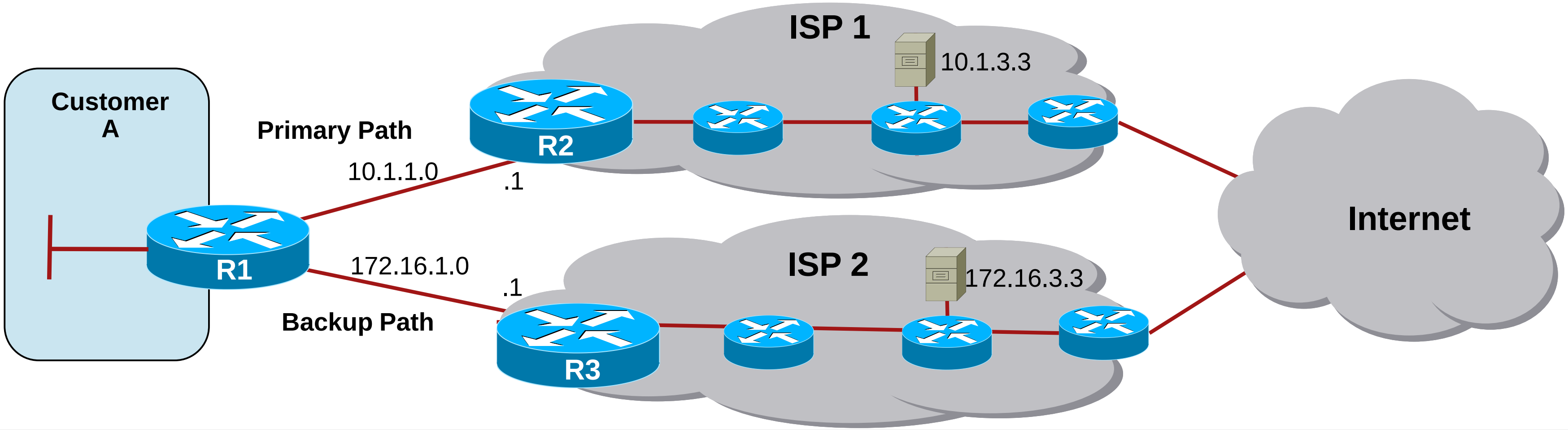
- IP SLA 11 continuously sends ICMP Echo Requests to the DNS server (10.1.3.3) every 10 seconds.
- IP SLAs is tracking that object and as long as the DNS server is reachable, the default route to R2 will be in the routing table.



```
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
```

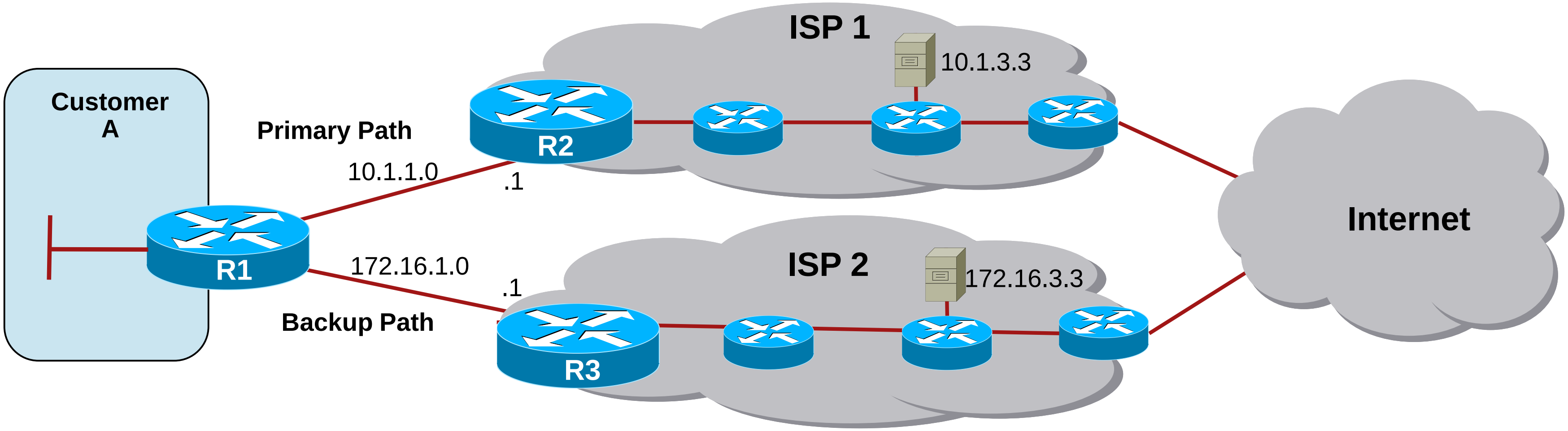
Tracking Reachability to Two ISPs Example

- 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
```

Tracking Reachability to Two ISPs Example



Same configuration using older IP SLA commands

```
R1(config)# ip sla monitor 11
R1(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.3.3
R1(config-sla-monitor-echo)# frequency 10
R1(config-sla-monitor-echo)# exit
R1(config)# ip sla monitor schedule 11 life forever start-time now
R1(config)# track 1 rtr 11 reachability
R1(config-track)# exit
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.1 2 track 1
R1(config)# ip sla monitor 22
R1(config-sla-monitor)# type echo protocol ipIcmpEcho 172.16.3.3
R1(config-sla-monitor-echo)# frequency 10
R1(config-sla-monitor-echo)# exit
R1(config)# ip sla monitor schedule 22 life forever start-time now
R1(config)# track 2 rtr 22 reachability
R1(config-track)# exit
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.1 3 track 2
```

IP SLA Notes

- There are many possibilities available with object tracking and Cisco IOS IP SLAs.
  - A probe can be based on reachability, changing routing operations, and path control based on the ability to reach an object.
  - Cisco IOS IP SLAs also allow paths to be changed based on network conditions such as delay, load, and other factors.
- The benefits of running IP SLAs should be carefully evaluated.
  - Before deploying a Cisco IOS IP SLA solution, the impact of the additional probe traffic being generated should be considered, including how that traffic affects bandwidth utilization, and congestion levels.
  - The IP SLA is an additional task that must be performed by the router’s CPU.
  - A large number of intensive SLAs could be a significant burden on the CPU, possibly interfering with other router functions and having detrimental impact on the overall router performance.
  - The CPU load should be monitored after the SLAs are deployed to verify that they do not cause excessive utilization of the router CPU.

Implement Path Control using Policy-Based Routing

Path Control Using PBR

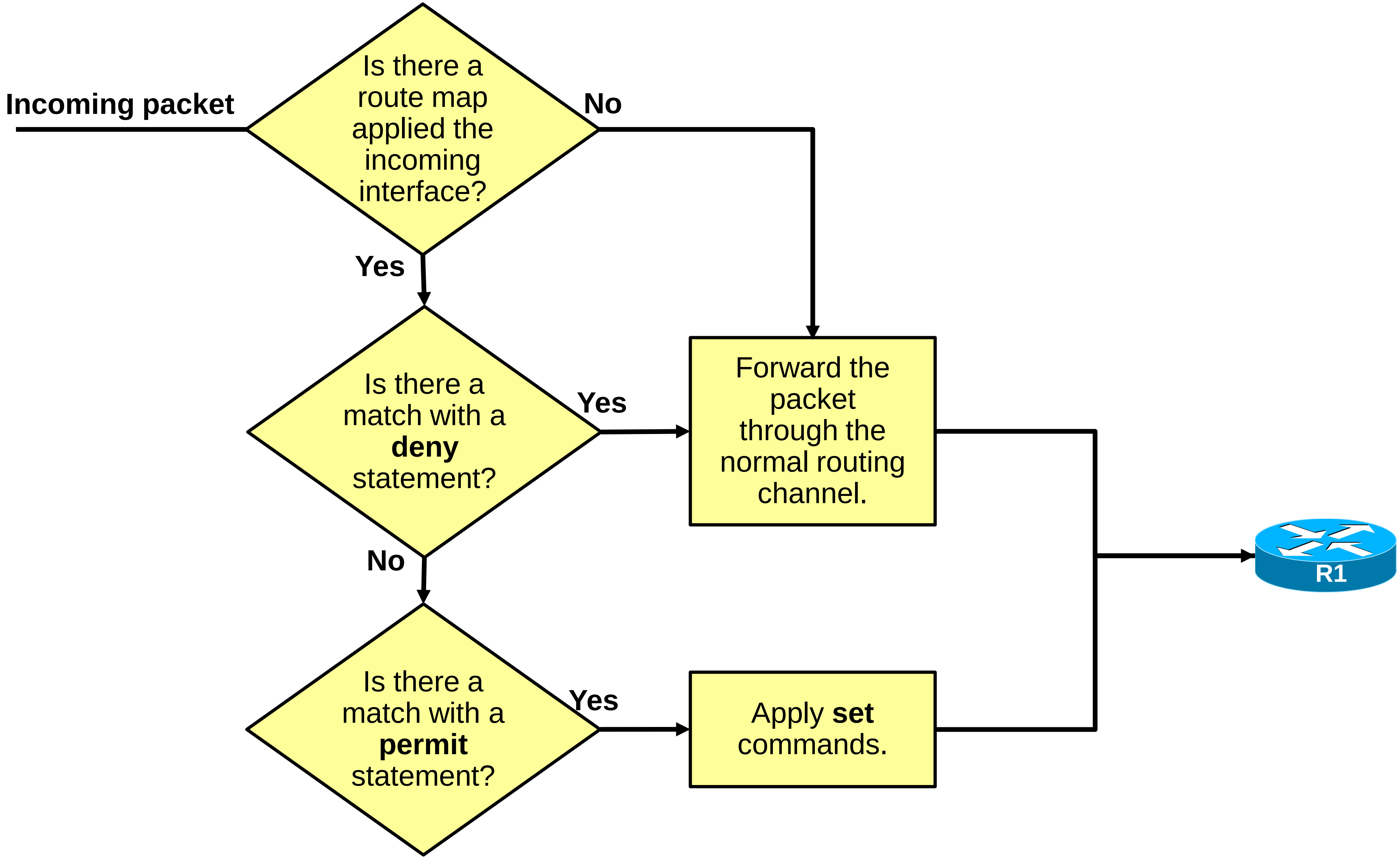
- In Chapter 4, Policy Based Routing (PBR) was used for redistribution.
  - In this chapter, PBR will be used to define a routing policy other than basic destination-based routing using the routing table.
- Routers normally forward packets to destination addresses based on information in their routing 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.

Configuring 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).
- Optionally, enable fast-switched PBR or Cisco Express Forwarding (CEF)-switched PBR.
  - CEF switching is enabled by default in recent IOS versions.
- 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



Incoming packet

Is there a route map applied the incoming interface?

No

Yes

Is there a match with a **deny** statement?

Yes

No

Forward the packet through the normal routing channel.

Is there a match with a **permit** statement?

Yes

Apply **set** commands.

route-map Commands for PBR

```
Router(config)#
```

```
route-map map-tag [permit | deny] [sequence-number]
```

- Defines the route map conditions.

```
Router(config-route-map)#
```

```
match {conditions}
```

- Defines the conditions to match.

```
Router(config-route-map)#
```

```
set {actions}
```

- Defines the action to be taken on a match.

```
Router(config-if)#
```

```
ip policy route-map map-tag
```

- Apply the route-map to the incoming interface.

Match Statements

- Specify criteria to be matched.

```
Router(config-route-map)#
```

```
match condition
```

- The **`match`** *`condition`* route map configuration commands are used to define the conditions to be checked.
- Some of these conditions are used for BGP policy, some for PBR, and some for redistribution filtering.

match Conditions

Command	Description
`match community`	Matches a BGP community
`match interface`	Matches any routes that have the next hop out of one of the interfaces specified
`match ip address`	Matches any routes that have a destination network number address that is permitted by a standard or extended ACL
`match ip next-hop`	Matches any routes that have a next-hop router address that is passed by one of the ACLs specified
`match ip route-source`	Matches routes that have been advertised by routers and access servers at the address that is specified by the ACLs
`match length`	Matches based on the layer 3 length of a packet
`match metric`	Matches routes with the metric specified
`match route-type`	Matches routes of the specified type
`match tag`	Matches tag of a route

`match` Commands Used in PBR

Command	Description
`match community`	Matches a BGP community
`match interface`	Matches any routes that have the next hop out of one of the interfaces specified
`match ip address`	Matches any routes that have a destination network number address that is permitted by a standard or extended ACL
`match ip next-hop`	Matches any routes that have a next-hop router address that is passed by one of the ACLs specified
`match ip route-source`	Matches routes that have been advertised by routers and access servers at the address that is specified by the ACLs
`match length`	Matches based on the layer 3 length of a packet
`match metric`	Matches routes with the metric specified
`match route-type`	Matches routes of the specified type
`match tag`	Matches tag of a route

match ip-address Command

- Specify criteria to be matched using ACLs or prefix lists.

```
Router(config-route-map)#
```

```
match ip address {access-list-number | name} [...access-list-
   number | name] | prefix-list prefix-list-name [..prefix-
   list-name]
```

Parameter	Description
access-list-number | name	The number or name of a standard or extended access list to be used to test incoming packets. If multiple access lists are specified, matching any one results in a match.
prefix-list *prefix-list-name*	Specifies the name of a prefix list to be used to test packets. If multiple prefix lists are specified, matching any one results in a match.

match length Command

- Specify criteria to be matched by packet length.

```
Router(config-route-map)#
```

```
match length min max
```

Parameter	Description
min	The packet’s minimum Layer 3 length, inclusive, allowed for a match.
max	The packet’s maximum Layer 3 length, inclusive, allowed for a match.

set Statements

- Modify matching conditions.

```
Router(config-route-map)#
```

```
set action
```

- The command modifies parameters in routes.
- The specific *action* changes or adds characteristics, such as metrics, to any routes that have met a **match** *condition*.

`set` Conditions *

Command	Description
`set as-path`	Modifies an AS path for BGP routes
`set automatic-tag`	Computes automatically the tag value
`set community`	Sets the BGP communities attribute
`set ip next-hop`	Indicates where to output packets that pass a match clause of a route map for policy routing
`set interface`	Indicates where to output packets that pass a match clause of a route map for policy routing
`set ip default next-hop`	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination
`set default interface`	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination
`set ip tos`	Used to set some of the bits in the IP ToS field in the IP packet.
`set ip precedence`	set the 3 IP precedence bits in the IP packet header.
`set tag`	Sets tag value for destination routing protocol
`set weight`	Specifies the BGP weight value

** Partial list*

set Commands Used in PBR

Command	Description
`set as-path`	Modifies an AS path for BGP routes
`set automatic-tag`	Computes automatically the tag value
`set community`	Sets the BGP communities attribute
`set ip next-hop`	Indicates where to output packets that pass a match clause of a route map for policy routing
`set interface`	Indicates where to output packets that pass a match clause of a route map for policy routing
`set ip default next-hop`	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination
`set default interface`	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination
`set ip tos`	Used to set some of the bits in the IP ToS field in the IP packet.
`set ip precedence`	set the 3 IP precedence bits in the IP packet header.
`set tag`	Sets tag value for destination routing protocol
`set weight`	Specifies the BGP weight value

** Partial list*

`set ip next-hop` Command

- Specify the next hop IP address for matching packets.

```
Router(config-route-map)#
```

```
set ip next-hop ip-address [...ip-address]
```

- The command provides a list of IP addresses used to specify the adjacent next-hop router in the path toward the destination to which the packets should be forwarded.
- If more than one IP address is specified, the first IP address associated with a currently up connected interface is used to route the packets.

`set interface` Command

- Specify interfaces through which packets can be routed.

```
Router(config-route-map)#
```

```
set interface type number [... type number]
```

- If more than one interface is specified, the first interface that is found to be up is used to forward the packets.

set ip default next-hop Command

- Specify a list of default next-hop IP addresses.

```
Router(config-route-map)#
```

```
set ip default next-hop ip-address [...ip-address]
```

- If more than one IP address is specified, the first next hop specified that appears to be adjacent to the router is used.
- The optional specified IP addresses are tried in turn.

set default interface Command

- Specify a list of default interfaces.

```
Router(config-route-map)#
```

```
set default interface type number [...type number]
```

- If no explicit route is available to the destination address of the packet being considered for policy routing, it is routed to the first up interface in the list of specified default interfaces.

set ip tos Command

- Mark packets using the IP ToS field.

```
Router(config-route-map)#
```

```
set ip tos [number | name]
```

- Used to set some of the bits in the IP ToS field in the IP packet.
  - The ToS field in the IP header is 8 bits long, with 5 bits for setting the class of service (CoS) and 3 bits for the IP precedence.
  - The CoS bits are used to set the delay, throughput, reliability, and cost.

Parameter	Description
0 | **normal**	Sets the normal ToS
1 | **min-monetary-cost**	Sets the min-monetary-cost ToS
2 | **max-reliability**	Sets the max reliable ToS
4 | **max-throughput**	Sets the max throughput ToS
8 | **min-delay**	Sets the min delay ToS

set ip precedence Command

- Set the 3 IP precedence bits in the IP packet header.

```
Router(config-route-map)#
```

```
set ip precedence  [number | name]
```

- This command is used when implementing QoS and can be used by other QoS services, such as weighted fair queuing (WFQ) and weighted random early detection (WRED).
- With 3 bits, you have 8 possible values for the IP precedence; values 0 through 7 are defined.

`set ip precedence` Parameters

Parameter	Description
`0 | routine`	Sets the routine precedence
`1 | priority`	Sets the priority precedence
`2 | immediate`	Sets the immediate precedence
`3 | flash`	Sets the Flash precedence
`4 | flash-override`	Sets the Flash override precedence
`5 | critical`	Sets the critical precedence
`6 | internet`	Sets the internetwork control precedence
`7 | network`	Sets the network control precedence

Configuring PBR on an Interface

- Identify a route map to use for policy routing on an interface.

```
Router(config-if)#
```

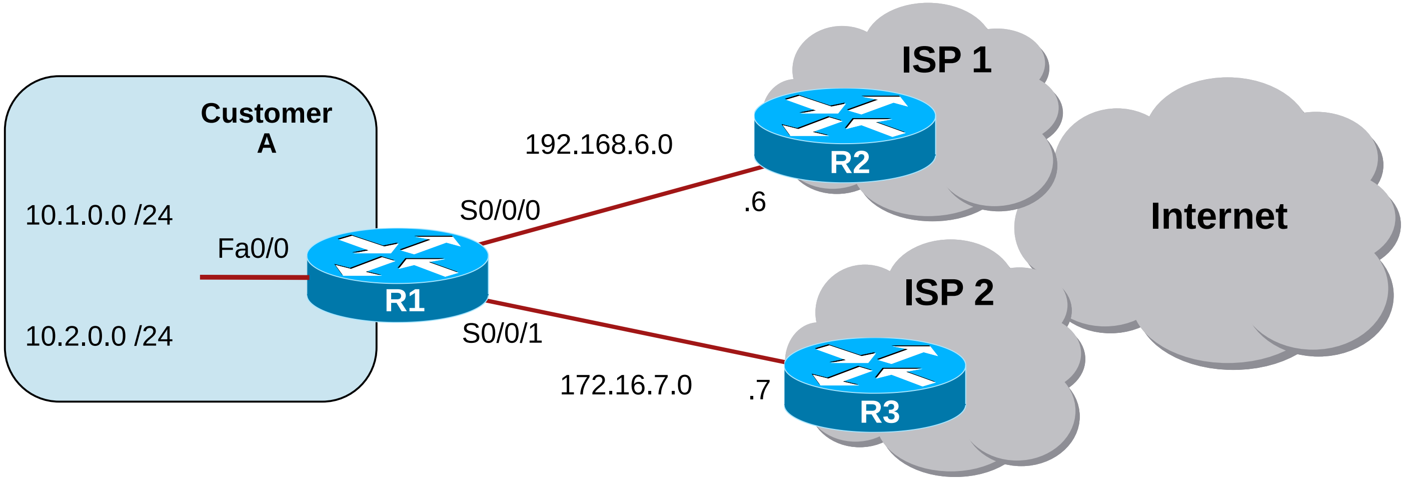
```
ip policy route-map map-tag
```

- The *map-tag* parameter is the name of the route map to use for policy routing.
- It must match a map tag specified by a **route-map** command.

Verifying PBR

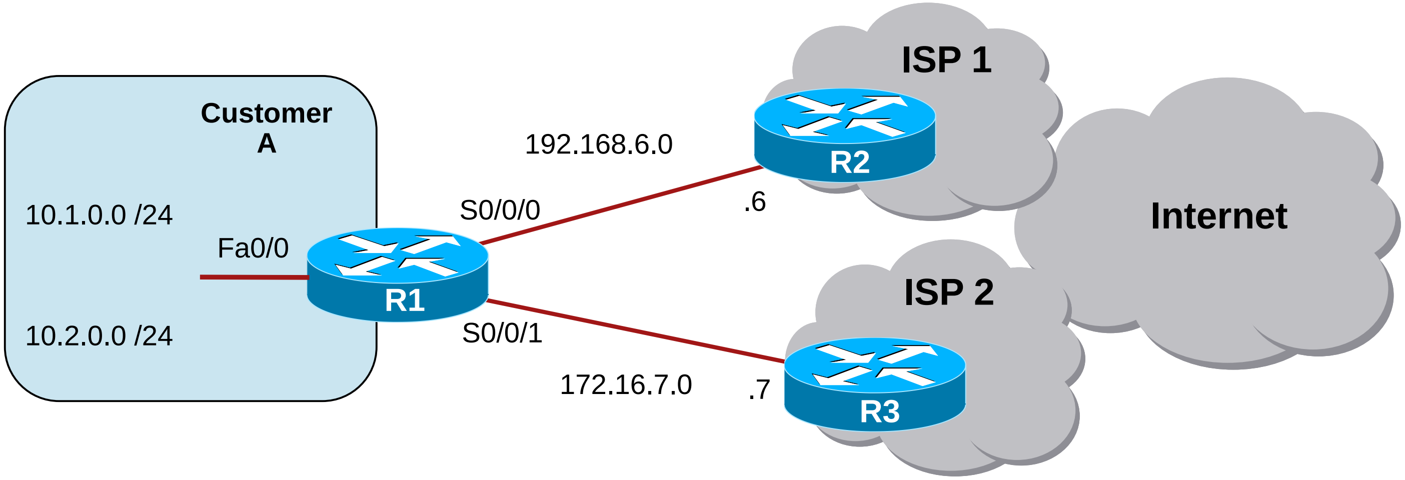
Command	Description
`show ip policy`	Display the route maps used for policy routing.
`show route-map [`*`map-name`*`]`	Display configured route maps.
`debug ip policy`	Display the policy routing details about whether a packet matches the criteria and, if so, the resulting routing information for the packet.

Using PBR When Multihoming Example



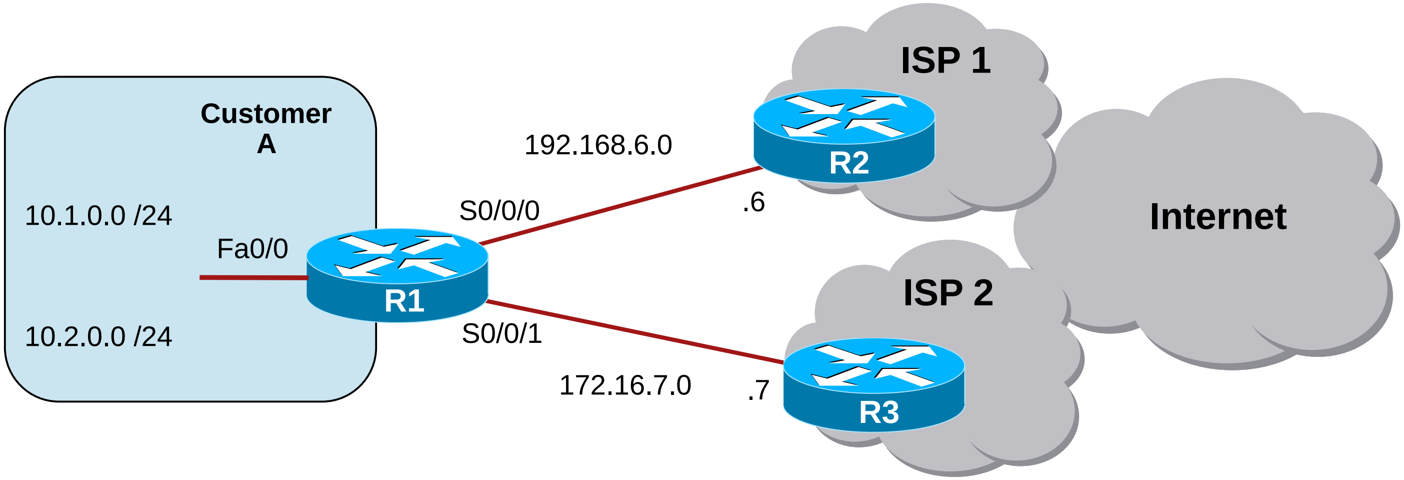
```
R1(config)# access-list 1 permit 10.1.0.0 0.0.255.255
R1(config)# access-list 2 permit 10.2.0.0 0.0.255.255
R1(config)# route-map EQUAL-ACCESS permit 10
R1(config-route-map) # match ip address 1
R1(config-route-map)# set ip default next-hop 192.168.6.6
R1(config-route-map)# route-map EQUAL-ACCESS 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
```

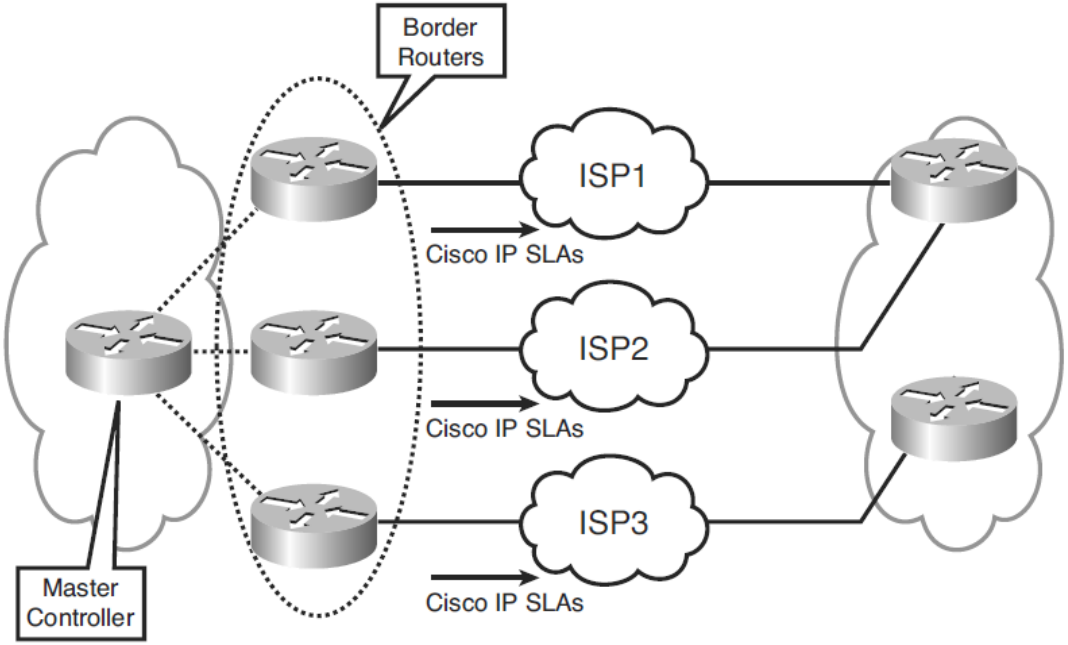
Advanced Path Control Tools

Cisco IOS Optimized Edge Routing

- Cisco IOS OER is intended for sites using multiple Internet or WAN service providers.
- Cisco IOS OER uses tools such as Cisco IOS IP SLAs to automatically detect network service degradation and to make dynamic routing decisions and adjustments based on criteria such as response time, packet loss, jitter, path availability, and traffic load distribution.
  - In contrast, normal routing protocols focus on detecting a routing path using static routing metrics, rather than the condition of the service over that path.

Cisco IOS OER Operation

- The Cisco IOS OER border routers monitor route prefixes information and gather performance statistics over each external interface (in this example, using Cisco IOS IP SLAs).
- This information is periodically reported to the master controller.
  - If the prefixes and exit links comply with a configured policy, routing remains as is.
  - If not, the master controller makes a policy-based decision and notifies the border routers, which change the path, by either adding static routes or changing routing protocol parameters.



Virtualization

- Virtualization is another advanced technology that includes benefits such as traffic segregation across a common physical network infrastructure.
- An example of virtualization is the use of virtual routing and forwarding (VRF) tables, which are virtual routing tables used to separate the routing function by group, on one physical router.
  - For example, employee routes could be kept separate from guest routes by using two different VRFs.
  - These VRFs could also be associated with other virtualization and traffic segregation elements on the network, such as virtual LANs (VLANs), virtual private networks (VPNs), and generic routing encapsulation (GRE) tunnels, to provide an end-to-end, segregated path across the network.

Cisco Wide Area Application Services

- Cisco WAAS is a good example of the use of PBR to adjust the path of traffic based on advanced services for that traffic, to provide both scalability and high availability.
- Technologies such as Web Cache Communications Protocol (WCCP) perform a similar function, which is to have routers redirect normal traffic flows into Cisco WAAS devices, where a series of data reduction, flow optimization, and application acceleration services are implemented, and then have them route the flows back into their normal path across the WAN.
  - This use of path control is becoming common in networks with branch offices.

Chapter 5 Summary

The chapter focused on the following topics:

- Redundant network considerations including resiliency, availability, adaptability, performance, support for network and application services, predictability, and asymmetric traffic.
- Path control tools include a good addressing design, redistribution and other routing protocol characteristics, passive interfaces, distribute lists, prefix lists, administrative distance, route maps, route tagging, offset lists, Cisco IOS IP SLAs, and PBR.
- Offset lists, a mechanism for increasing incoming and outgoing metrics to routes learned via EIGRP or RIP.
- Cisco IOS IP SLAs, which use active traffic monitoring, generating traffic in a continuous, reliable, and predictable manner, to measure network performance.
- Using PBR to control path selection, providing benefits including source-based transit provider selection, QoS, cost savings, and load sharing.
- Advanced path control tools, including Cisco IOS OER, Virtualization, and Cisco WAAS.

Chapter 5 Labs

- **IGP-LAB-4.1 Redistribution IPv4**

Q&A