
# How to Solve No Boolean Tracking Support on Cisco ASA

## Introduction

Customers find themselves in situations that require an Internet backup link without the use of BGP or other routing protocols. Sometimes, BGP is not available as a service, or it is too expensive for the branch office in question. Therefore, and alternatively, some network engineers implement Cisco's IP Service Level Agreement (IP SLA) as a working solution to monitor the primary Internet link's up-down state to failover the backup ISP when the primary link goes down.

How does the router do this? With IP SLA, a router can ping an IP host, or two, or more hosts on the Internet over the primary ISP. When the router stops receiving ping replies from any or all the target IP hosts, the router declares the primary ISP as down and then redirects all Internet traffic over the backup ISP.

An IP host is any device on the Internet with an IP address. IP hosts can reply to a ping message, although, sometimes, ping replies are disabled. This paper will assume that no filtering is in place. When the Internet router sends a ping packet to the host's IP address, the IP host responds with a ping reply. Simple. That is how the router knows that there is end-to-end IP reachability and that the targeted IP host is alive. A ping is a small message sent to another IP device. The remote IP device then responds with a ping reply, as if confirming that it is active.

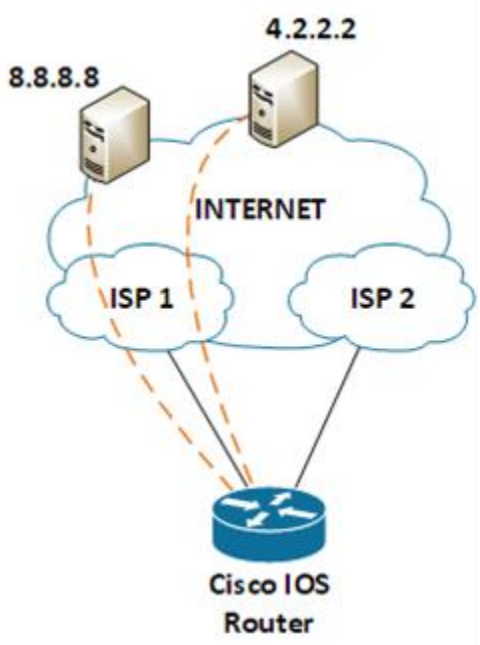
If a router pings a remote device located outside of the primary ISP network, one device may go offline. The reason why varies. If a device goes offline, pings will stop returning. As a result, the router will assume that the Internet link went down, though that is not the case. A no ping reply means that the router will trigger a failover despite the primary Internet line and the service provider's network being fully operational.

## ABOUT THE AUTHOR

Alirio (Rio) Zavarce possesses over 24 years of technical network consulting experience in LAN, WAN, datacenter, and security technologies. His broad range of experience in architecting and implementing advanced technology solutions includes working with clients across multiple verticals including manufacturing, financial services, real estate, higher education, and healthcare. Rio holds numerous industry certifications including Cisco Certified Internetwork Expert (CCIE) Routing and Switching.

To mitigate this false alarm, however, an engineer may use the IP SLA to ping two or more remote devices instead of one. The likelihood of those targets becoming unresponsive at the same time is less than just one remote IP host.

For example, an engineer will ping two devices over ISP 1, working with Google's DNS server 8.8.8.8. and Level 3's DNS server 4.2.2.2, because of its reliability (always up). If IP host 1, or 8.8.8.8, stops responding, and IP host 2, or 4.2.2.2, still responds to pings, the router knows that ISP 1 remains up because the router still receives ping replies from 4.2.2.2. If both IP hosts stop responding, the router behaves as if the Internet link went down on ISP 1 and fail over the backup ISP. Although the Internet link to ISP 1 may still be up, a routing problem might exist on ISP 1's network, which would render ISP 1 unusable for Internet access.




Pinging any reliable public IP will do. 'Reliable' means that it is very, very unlikely that that IP will stop responding to pings.

Cisco IOS routers use the "enhanced object tracking" feature to monitor the up/down state of every IP SLA session. This tracking feature supports a "Boolean OR" function, which means that both IP SLAs need to be down for the router to declare ISP 1 as down. In other words, if the ISP 1 link were to go down, or there is a routing problem within ISP 1, both pings to 8.8.8.8 and 4.2.2.2 would fail. A failure of both pings strongly indicates that an Internet access problem exists via ISP 1.

On the contrary, a "Boolean AND" tracking would notify the router that ISP 1 is down if either of the two IP SLA sessions is not receiving a reply. If one IP SLA session is still receiving ping replies, that means there is still IP routing to a remote host over ISP 1, and therefore routing is good. So, this configuration would not be reliable for our design. We want no replies to both pings for a good indication that there is no Internet access through ISP 1.

For instance, an engineer may set up track 10 to monitor IP SLA 1 that pings 8.8.8.8, and IP SLA 2 that pings 4.2.2.2. If the engineer sets up track 10 as Boolean OR, track 10 will switch to down when both IP SLAs switch to down. If IP SLA 1 remains up, and IP SLA 2 goes down because it is not receiving pings

from 4.2.2.2, track 10 will remain up, meaning that the primary ISP is up, and no failover needs to be triggered.

## Problem Statement

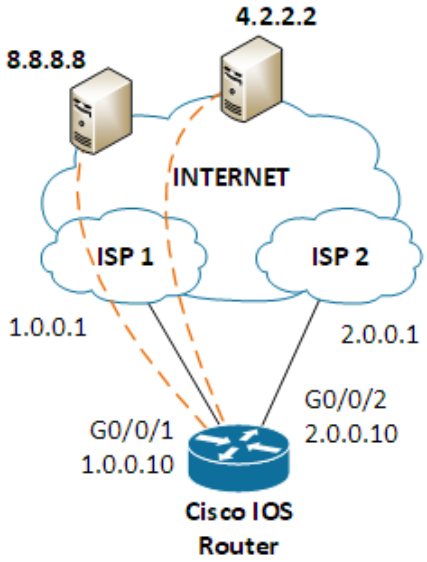
What happens when a Cisco ASA firewall replaces an IOS device? Luckily, the ASA OS also supports IP SLA and tracking, which means that an engineer may implement IP SLA to ping a reliable host on the Internet over ISP 1 and track its up/down state with the enhanced object tracking feature; however, because relying on one remote IP host is perilous, the engineer will ping two or more devices.

Now, pinging only one remote IP may cause flapping on your ASA's routing, causing a quick switchover of all the Internet traffic over the backup link. There might be occasions in which a ping reply does not come back or is late arriving outside of the wait window. Because the ASA keeps track of all user application sessions, the engineer might experience user disconnections at the time of the quick switchover to the backup link. For example, if an engineer opens an FTP session from his or her computer, and that session is being sent over ISP 1 when the ASA switches over the backup ISP and then back over the primary line, a disconnection might occur.

The ASA, like IOS routers, determines whether an ISP went down through a tracking features that monitors IP SLA; however, although the engineer may set up the ASA to ping two or more IP devices on the internet, unlike IOS routers, the ASA tracking feature cannot monitor more than one IP SLA. The tracking feature monitors only one at a time. This might alarm engineers, but the use of other features will obtain the same result. The 'solution' section will explain how.

## Solution

To determine whether ISP 1 is usable or not, engineers may associate the ASA's default route with a tracking instance. Tracking instance configuration shows 'up-time', which proves a valid and usable default route to ISP 1. The configuration shows 'down-time' as well. If tracking displays 'down-time' because the IP SLA session went down, and because ping replies failed to return, the default route to ISP 1 will become invalid, and the secondary default route to the backup ISP will become active.



Here is a quick break down on how this works on IOS devices:

- IP SLA 1 pings 8.8.8.8
    - The static route forces traffic to 8.8.8.8 out the primary ISP on interface G0/0/1

```
ip sla 1
 icmp-echo 8.8.8.8 source-interface G0/0/1
 exit
sla monitor schedule 1 start-time now life forever
ip route 8.8.8.8 255.255.255.255 G0/0/1 1.0.0.1
```

- IP SLA 2 pings 4.2.2.2
    - The static route forces traffic to 4.2.2.2 out the primary ISP on interface G0/0/1

```
sla monitor 2
 icmp-echo 4.2.2.2 source-interface G0/0/1
 exit
sla monitor schedule 2 start-time now life forever
ip route 4.2.2.2 255.255.255.255 G0/0/1 1.0.0.1
```

- Track 10 is configured as a Boolean OR and monitors both IP SLA 1 and 2 ➔ Boolean OR means that both IP SLAs must be down for tracking 10 to switch its state from up to down
    - Track 10 really monitors Track 1 and 2. Track monitors IP SLA 1, and Track 2 monitors IP SLA 2. Effectively, track 10 monitors IP SLA 1 and 2

```
track 1 ip sla 1 reachability
 exit
track 2 ip sla 2 reachability
 exit

track 10 list boolean OR
 object 1 ← 1 means track 1
 object 2 ← 2 means track 2
 exit
```

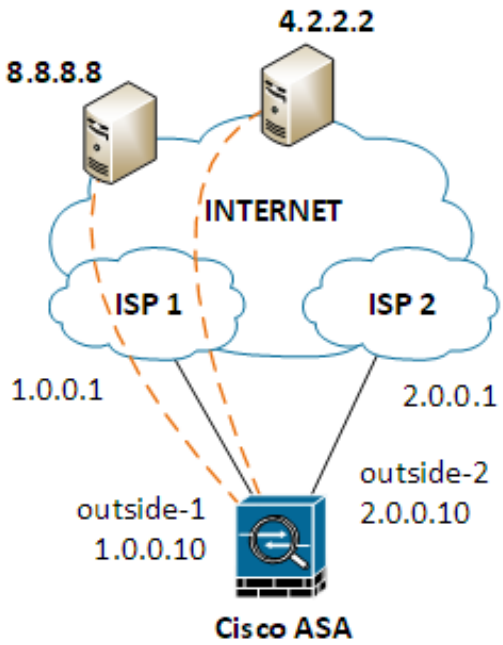
- The default route to ISP 1 is associated to track 10 – if track 10 is up, the default route to ISP 1 is valid
    - The administrative distance (AD) on this static route is the default of 1 (AD will be explained below)

```
ip route 0.0.0.0 0.0.0.0 1.0.0.1 track 10 name ISP_1
```

- The backup default route pointing to ISP 2 stays in standby (floating) until the primary default route becomes invalid. The primary default route become invalid when track 10 goes down. Once the primary default route becomes invalid, the secondary default route will kick in and Internet traffic will then be redirected to the backup ISP
    - The administrative distance on the static default route to ISP 2 is set to 5 – the lower the AD, the better – this is why the static default route to ISP 1 with AD of 1 is preferred over this static default route to ISP 2 with AD of 5
    - Again, when track 10 goes down, the default route to ISP 1 becomes invalid and the default route to ISP 2 takes over

```
ip route 0.0.0.0 0.0.0.0 2.0.0.1 5 name ISP_2
```

Now, the challenge is that Boolean OR is not supported on ASA firewalls. So, what is the solution?




To make this solution with two IP SLAs work on ASA firewalls, engineers might:

- Configure the IP SLAs just like in IOS (the syntax is different)
    - **outside-1** is the name of the primary interface
    - **outside-2** is the name of the backup interface
    - The static routes to 8.8.8.8 and 4.2.2.2 force pings to those IP addresses to leave ISP 1 and not ISP 2

```
sla monitor 1
 type echo protocol ipIcmpEcho 8.8.8.8 interface outside-1
 exit
sla monitor schedule 1 start-time now life forever
route outside-1 8.8.8.8 255.255.255.255 1.0.0.1

sla monitor 2
 type echo protocol ipIcmpEcho 4.2.2.2 interface outside-1
 exit
sla monitor schedule 2 start-time now life forever
route outside-1 4.2.2.2 255.255.255.255 1.0.0.1
```

- Configure tracking
    - Track 1 will monitor SLA 1
    - Track 2 will monitor SLA 2

```
track 1 rtr 1 reachability
track 2 rtr 2 reachability
```

- Split the default route into two halves for “longest match routing”
    - 0.0.0.0/1 and associate it to track 1
    - 128.0.0.0/1 and also associate to track 1
- Configure a default route 0.0.0.0/0 and associate it to track 2

```
route outside-1 0.0.0.0 128.0.0.0 1.0.0.1 track 1
route outside-1 128.0.0.0 128.0.0.0 1.0.0.1 track 1
route outside-1 0.0.0.0 0.0.0.0 1.0.0.1 track 2
```

These three static routes above will be installed in the routing table and send all traffic out the primary ISP. All Internet traffic will match any of the two smaller versions of the default route: 0.0.0.0/1 and 128.0.0.0/1. The first half of the Internet space matches 0.0.0.0/1, and the second half matches

128.0.0.0/1. If 8.8.8.8 becomes unresponsive, track 1 will go down, and these two static routes will be removed from the routing table. As a result, the default route 0.0.0.0/0 will immediately take over all Internet routing out to the primary ISP.

- Configure a backup default route with administrative distance 5

```
route outside-2 0.0.0.0 0.0.0.0 2.0.0.1 5
```

If track 2 were to go down because 4.2.2.2 stopped sending ping replies, the primary default route "`route outside-1 0.0.0.0 0.0.0.0 1.0.0.1 track 2`" will be removed from the routing table and the secondary default route to ISP 2 will be installed in its place; however, remember that before Internet traffic (IP packets) is matched to the default route to ISP 1, outbound Internet packets match the two longest-match routes 0.0.0.0/1 and 128.0.0.0/1, which point out to ISP 1. So, to fail over ISP 2, both IP SLA 1 and 2 need to change from up to down to invalidate the two longest-match routes (linked to IP SLA 1) and the default route to ISP 1 (linked to IP SLA 2).

Here is the sequence of events for a failover:

- 8.8.8.8 stops responding to pings over ISP 1 – track 1 goes down – longest-match default routes are removed.
- 4.2.2.2 is still active and replying to pings – default route to ISP 1 takes over.
- 4.2.2.2 becomes unresponsive – track 2 goes down – default route to ISP 1 is removed.
- Backup default route to ISP 2 takes over.

Track 1 and 2 going down is a good indication that something went wrong with the Internet over the primary ISP. At that point, it would be wise to switch over to the backup ISP.

When the primary ISP comes back up, pings will start working again, track 1 and 2 will come back up, static routes to ISP 1 will become active again, and Internet traffic will switch back over the primary ISP.

## Conclusion

The version of IP SLA discussed in this document is an easy-to-deploy alternative to BGP that allows for monitoring of the IP routing state of your primary ISP. No ping replies means something happened along the way from the edge router or firewall and across the primary ISP to the target device.

The combination of longest match routing and IP SLA provides a great solution for the implementation of a more reliable mechanism to determine when your primary Internet link no longer provides IP routing to the Internet.

## References

ISP Failover with Default Routes using IP SLA Tracking

https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-with-default-routes-using-I.html

Configure the ASA for Redundant or Backup ISP Links

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118962-configure-asa-00.html

IP SLA “AND OR” Boolean Options

https://cordero.me/ip-sla-and-or-boolean-options/

Enhanced Object Tracking – Boolean Operator

https://enotepad.wordpress.com/2008/08/21/enhanced-object-tracking-boolean-operator/

## About Aspire Technology Partners

Aspire is a professional technology services firm specializing in the delivery of digital infrastructure solutions and managed services designed specifically to achieve our clients’ business goals. We believe technology sits at the heart of every enterprise strategy. Our team takes time to understand your business initiatives and align technology solutions to drive the organization forward. Aspire’s outcome-driven approach accelerates your journey by combining secure digital infrastructure, world-class design and implementation expertise, and managed services – all centered around transforming today’s multi-cloud architectures into enablers of business value. Headquartered in Eatontown, New Jersey, Aspire is focused on serving the tri-state, mid-Atlantic, and New England regions with local operations in Mount Laurel, NJ; Albany and White Plains, NY; and Cambridge, MA. For more information, visit www.aspiretransforms.com.