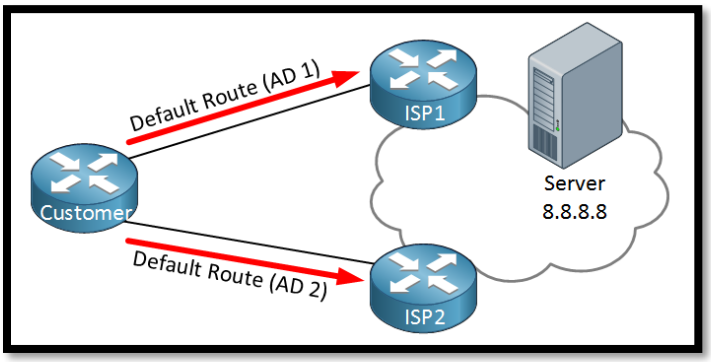
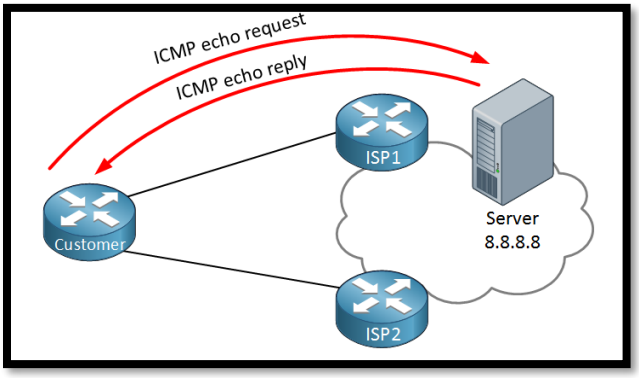

Networkforyou
Welcome
To
Network for you
IP SLA
Networkforyou

IP SLA (Service-Level Agreement):

- Internet Protocol SLA is a term which is stands for Service Level Agreement.
- Service Level Agreement is a formal or informal contract between two parties.
- IP SLA uses active traffic monitoring to monitor continuous traffic on the network.
- With IP SLAs, the Cisco routers and Cisco switches perform periodic measurements.
- IP Service Level Agreement is feature of Cisco IOS that allows collecting information.
- IP SLA is a feature to collect info about the performance of network in the real time.
- **IP SLA (Service-Level Agreement) is a great feature on Cisco IOS devices that can be used to "measure" network performance.**
- **This can be something simple like a ping where we check the round-trip time.**
- **Measuring network performance is pretty cool but what makes IP SLA even more powerful is that you can combine it with static routes, policy based routing.**
- IP SLA is a cisco IOS feature, which can be used to measure network performance.
- IP Service-Level Agreements (SLA) measure the current performance of the network.
- IP SLA continuously collect data about latency, packet loss, jitter & response time.
- IP SLA responder is the IOS software, which responds to the SLA request packet.
- IP Service Level Agreement consist of two components source and target router.
- IP Service Level Agreement (SLA) source is where the IP SLA operation is defined.
- Operations is type of packet that will be sent from the source to the destination.
- IP Service Level Agreement each measurement that we do is called an operation.
- In IP SLA the routers will collect the data and can be used for tracking.
- For example, you can use SLA to view the status of static routes or for PBR.
- The destination router is referred to as IP Service Level Agreement Responder.
- Types of traffic IP SLA can use **ICMP, RTP, TCP, UDP, DNS, DHCP, and HTTP & FTP.**
- IP SLAs ICMP Echo operation to monitor end-to-end response time between devices.
- ICMP Echo is useful for troubleshooting network connectivity issues.
- ICMP Echo operation measures end-to-end response time between devices.
  Let me give you some example:



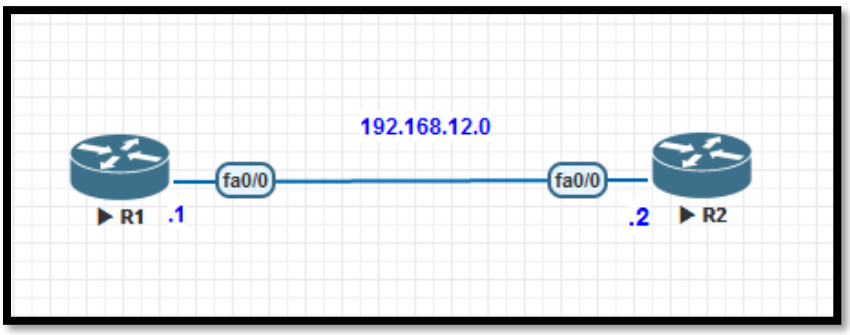
- Above we have a customer router connected to two ISPs.
- Somewhere on the Internet there's a server we'd like to reach.
- In a scenario like this, typically we use two default routes with different ADs.
- Whenever ISP1 fails, we switch over to ISP2.
- The problem with this setup is that it's not very reliable.
- The default route will be in the routing table as long as the interface is up and/or the next hop is reachable.
- It's possible that ISP1 is having connectivity issues and unable to reach that remote server but we still use them for all our traffic.
- To prevent this from happening we can combine default routes with IP SLA.



- Our customer router is now using IP SLA to ping the remote server.
- As long as we get a reply, we will keep using ISP1 as our main route.
- When the ping fails, we switch over to ISP2.
- This method is far more reliable as we check end-to-end connectivity.

Let do One Basic Lab for this.

Lab time:



R1 Configuration	R2 Configuration
en config t hostname R1 int f0/0 ip add 192.168.12.1 255.255.255.0 no sh R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip sla 1 R1(config-ip-sla)#? IP SLAs entry configuration commands: dhcp DHCP Operation dns DNS Query Operation ethernet Ethernet Operations 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 mpls MPLS Operation path-echo Path Discovered ICMP Echo Operation path-jitter Path Discovered ICMP Jitter Operation tcp-connect TCP Connect Operation	en config t hostname R2 int f0/0 ip add 192.168.12.2 255.255.255.0 no sh

udp-echo UDP Echo Operation
udp-jitter UDP Jitter Operation
voip Voice Over IP Operation

First we have to choose an operation number, let's pick number 1. You can see that there are a lot of different operations we can choose from. Let's start with the icmp echo:

R1(config-ip-sla)#**icmp-echo 192.168.12.2**
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 instance

Let's send ICMP echos to 192.168.12.2. There are a lot of optional parameters you can configure for an
operation, for example let's change the frequency:

R1(config-ip-sla-echo)#**frequency 10**

We'll send an ICMP echo every 10 seconds. The only thing left to do is to start our IP SLA operation. This

is how we do it:

```
R1(config)#ip sla schedule 1 ?
  ageout      How long to keep this Entry when
inactive
  life        Length of time to execute in seconds
  recurring   Probe to be scheduled automatically
every day
  start-time  When to start this entry
  <cr>
```

You have to use the ip sla schedule command to start your operation. You can schedule it but we will
start our operation right now and let it run forever:

```
R1(config)#ip sla schedule 1 start-time  ?
  after     Start after a certain amount of time from
now
  hh:mm     Start time (hh:mm)
  hh:mm:ss  Start time (hh:mm:ss)
  now       Start now
  pending   Start pending

R1(config)#ip sla schedule 1 start-time  now ?
  ageout     How long to keep this Entry when
inactive
  life       Length of time to execute in seconds
  recurring  Probe to be scheduled automatically
every day
  <cr>

R1(config)#ip sla schedule 1 start-time  now life ?
  <0-2147483647>  Life seconds (default 3600)
  forever         continue running forever

R1(config)#ip sla schedule 1 start-time  now life
forever
```

It should now be up and running. You can check

your IP SLA configuration as given below:

R1#sh ip sla configuration
IP SLAs Infrastructure Engine-II
Entry number: 1
Owner:
Tag:
Type of operation to perform: icmp-echo
Target address/Source address:
192.168.12.2/0.0.0.0
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
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000 (not considered if react RTT is configured)
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
History Statistics:
  Number of history Lives kept: 0
  Number of history Buckets kept: 15
  History Filter Type: None
Enhanced History:

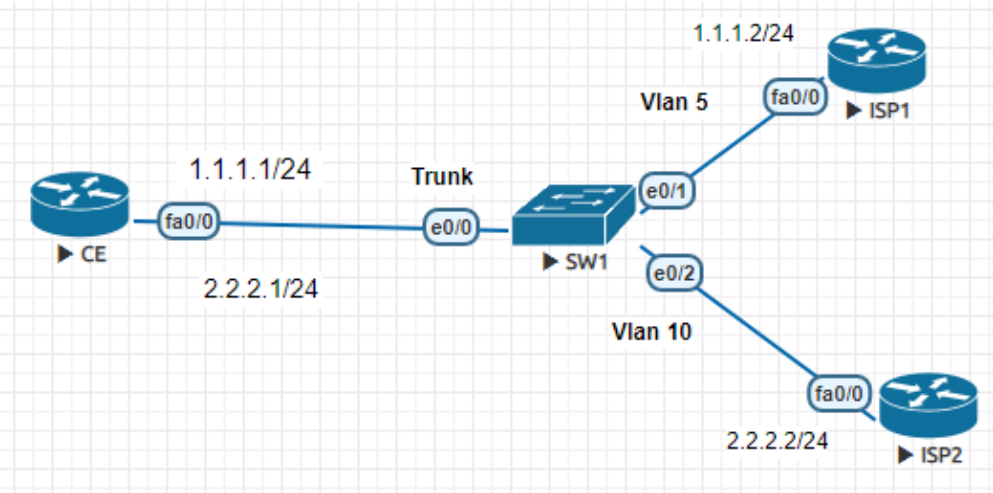
Above you can see the details of our IP SLA operation. A lot of parameters are configured by default.
This is how you can check if it's running or not:

R1#show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
Type of operation: icmp-echo
Latest RTT: 7 milliseconds
Latest operation start time: *23:56:34.991 UTC Thu May 6 2021
Latest operation return code: OK
Number of successes: 11
Number of failures: 1
Operation time to live: Forever

Use the show ip sla statistics command to see the results. You can see my pings are successful and our round trip time is only 7 ms.

Let do one Lab on this.



Let consider we have 2 ISP that is ISP1 and ISP2 we connect to switch and we put ISP1 in Vlan 5 and ISP2 in Vlan 10 and switch interface connect to our Customer Edge router put in trunk and for Customer Edge router we will do Subinterface like f0/0.5 for ISP 1 and f0/0.10 for ISP2 as show in the above figure.

CE Configuration	SW1 Configuration	ISP1 Configuration	ISP2 Configuration
en config t hostname CE int f0/0 no sh int f0/0.5 encapsulation dot1Q 5 ip add 1.1.1.1 255.255.255.0 no sh int f0/0.10 encapsulation dot1Q 10 ip add 2.2.2.1 255.255.255.0 no sh ip sla 1 icmp-echo 1.1.1.2 source-ip 1.1.1.1 frequency 10 timeout 5000 exit ip sla schedule 1 start-time now life forever track 1 ip sla 1 ip router 0.0.0.0 0.0.0.0 1.1.1.2 track 1 ip router 0.0.0.0 0.0.0.0 2.2.2.2 10	en config t hostname SW1 int e0/0 switchport trunk encapsulation dot1q switchport mode trunk int e0/1 switchport access vlan 5 switchport mode access int e0/2 switchport access vlan 10 switchport mode access	en config t hostname ISP1 int f0/0 ip add 1.1.1.2 255.255.255.0 no sh int lo 0 ip add 8.8.8.8 255.255.255.0	en config t hostname ISP2 int f0/0 ip add 2.2.2.2 255.255.255.0 no sh int lo 0 ip add 8.8.8.8 255.255.255.0

```
CE#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 1.1.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 1.1.1.2
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, FastEthernet0/0.5
L        1.1.1.1/32 is directly connected, FastEthernet0/0.5
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, FastEthernet0/0.10
L        2.2.2.1/32 is directly connected, FastEthernet0/0.10
```

```
ISP1(config)#int f0/0
ISP1(config-if)#sh
ISP1(config-if)#
*Aug 24 11:05:40.655: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Aug 24 11:05:41.655: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to down
```

```
CE#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 2.2.2.2 to network 0.0.0.0

S*    0.0.0.0/0 [10/0] via 2.2.2.2
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, FastEthernet0/0.5
L        1.1.1.1/32 is directly connected, FastEthernet0/0.5
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, FastEthernet0/0.10
L        2.2.2.1/32 is directly connected, FastEthernet0/0.10
```

```
CE#sh ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
        Latest RTT: NoConnection/Busy/Timeout
Latest operation start time: 11:11:28 UTC Tue Aug 24 2021
Latest operation return code: Timeout
Number of successes: 61
Number of failures: 22
Operation time to live: Forever
```