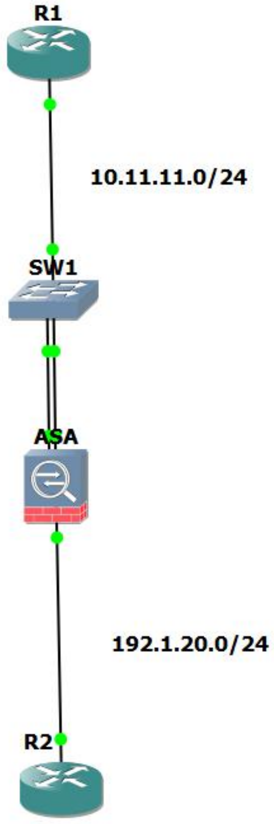
ASA Redundancy

Redundancy in ASA is of many types:
Interface
ISP level (If ISP goes down, how does the firewall react)
Box level (If firewall box goes down) This is aka FAILOVER:
  Active-Standby
  Contexts
Active-Active

Interface level redundancy

We create a redundant interafces which has more than one interface connected to it, the policies are all done on the redundant interfaes



Configure interfaces of R1 and R2 according to the topology.
Then for creating the **redundant** on ASA, we first do “no shut” on the physical interfaces required.
Int g0/0
No shut

```
Int g0/1
No shut
```

```
Interface redundant 1
Member-interface g0/0
 Member-interface g0/1
Exit
```

```
Interface redundant 1
Ip add 10.11.11.10 255.255.255.0
Nameif Inside
```

Show interface redundant 1 : To see which interface is active, in case the active interface shuts down, the MAC address will still still be used as the previous= INterface which was shut down, so to avoid confusion, we can manually add mac address.

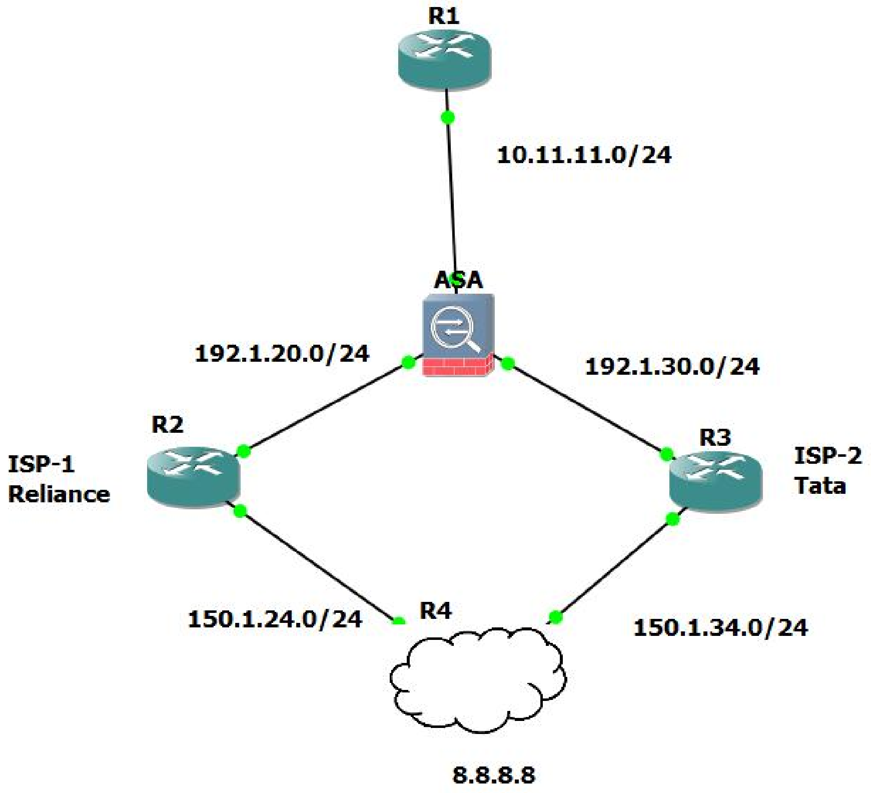
```
Interface redundant 1
Mac-address 1.1.1
```

```
Show interface redundant1
```

ISP redundancy

Our firewall is connected to two ISPs using outside-1 and outside-2 interfaces, one of which is just a backup. If one ISP goes down, the firewall has no way of knowing whether it is down, it will only know if its own interface is down, but here the ISP is down, interfaces are working.
For this we use **SLA Monitoring,**
We send out probes from outside-1 which are pings every 3 seconds. The timeout(the wait for a ping till we can consider the line dead) is 5 seconds by default, which is a lot in case of internet, so we reduce it but we cannot reduce it too much, in that case, we will flap too much between the two ISPs, also a problem, we need common ground.

First let us start with configuring the interfaces and then run eigrp on r2, r3 and R4. Technically, we should bgp because it will be used for the internet side but since it is slower, we will substitute it with eigrp.



Config of ASA:

```
 conf t
  int g0/0
  ip add 10.11.11.10 255.255.255.0
  nameif Inside
  no shut
  ex
  int g0/1
  security-level 0
  no shut
  nameif Outside-R
  ip add 192.1.20.10
  ex
  int g0/2
  security-level 0
  no shut
  nameif Outside-T
  ip add 192.1.30.10
  ex
  show nameif
  ping 192.1.20.2
  ping 192.1.30.3
  ping 10.11.11.1
  route outside-r 0 0 192.1.20.2
  route outside-t 0 0 192.1.30.3 10
```

We cannot have 2 default routes, so for second default route towards tata, we add an AD(Administrative Distance) = 10.

R1 needs to be NATted to be able to communicate with the outside,

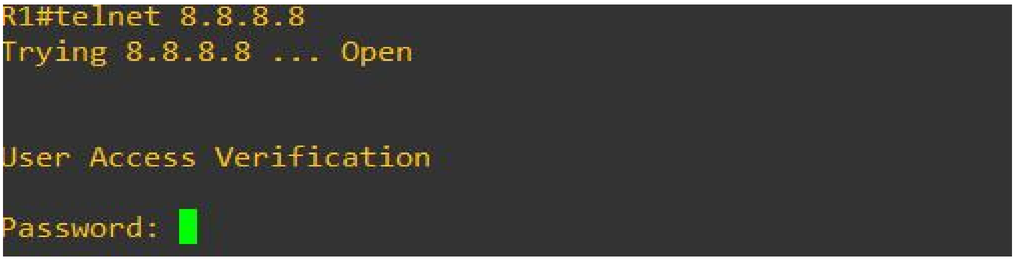
Object network POOL.192.1.20.50
Range 192.1.20.50 192.1.20.100

Object network R1.Outside.r
Subnet 10.11.11.0 255.255.255.0
Nat (inside,outside) dynamic POOL.192.1.20.50

Object network POOL.192.1.30.50
Range 192.1.30.50 192.1.30.100

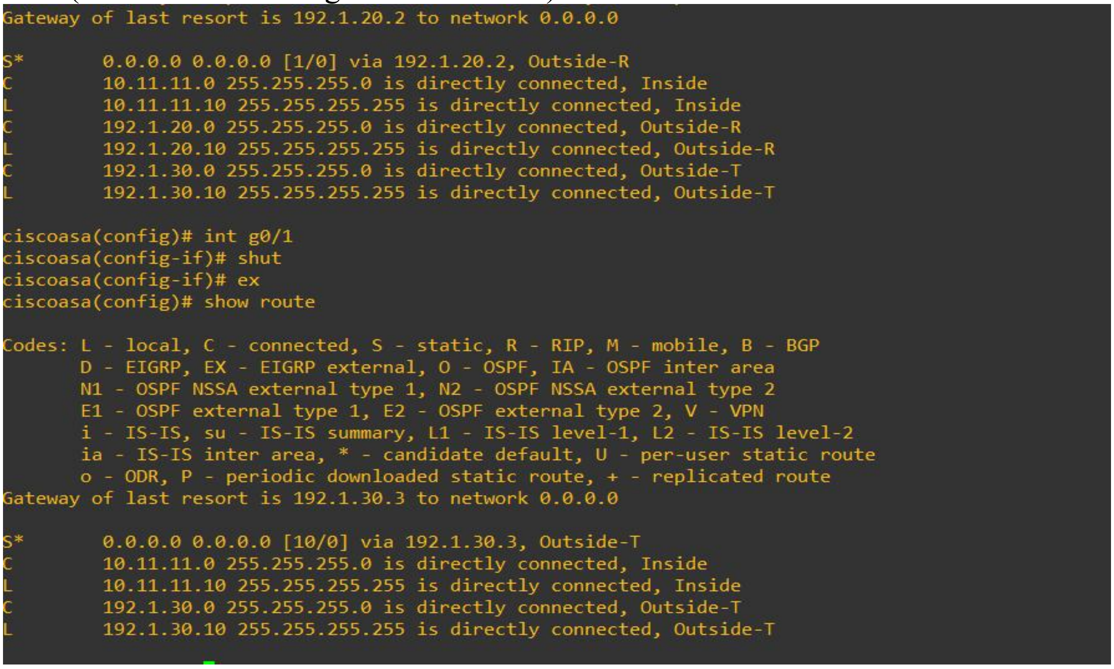
Object network R1.Outside.t
Subnet 10.11.11.0 255.255.255.0
Nat (inside,outside) dynamic POOL.192.1.30.50

Let us make the objects required for backup isp interface as well.



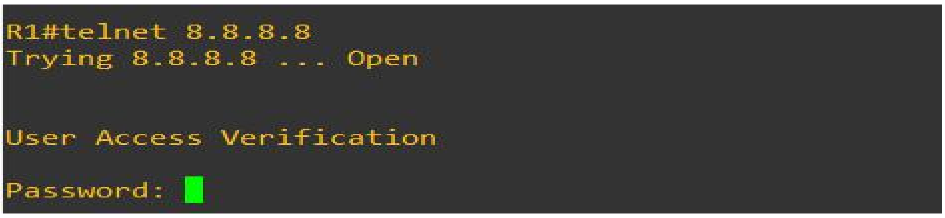
```
R1#telnet 8.8.8.8
Trying 8.8.8.8 ... Open


User Access Verification

Password:
```

Now let us shut down one interface, to see if the other comes up as the default route(We made it so using AD= see above)

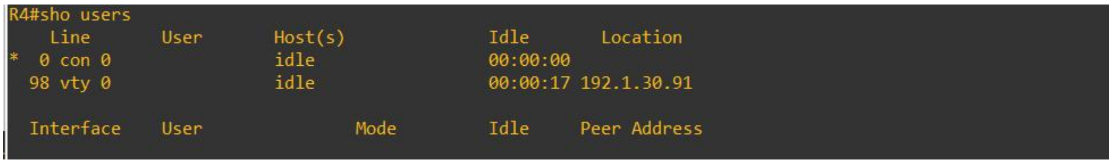


```
Gateway of last resort is 192.1.20.2 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.1.20.2, Outside-R
C        10.11.11.0 255.255.255.0 is directly connected, Inside
L        10.11.11.10 255.255.255.255 is directly connected, Inside
C        192.1.20.0 255.255.255.0 is directly connected, Outside-R
L        192.1.20.10 255.255.255.255 is directly connected, Outside-R
C        192.1.30.0 255.255.255.0 is directly connected, Outside-T
L        192.1.30.10 255.255.255.255 is directly connected, Outside-T

ciscoasa(config)# int g0/1
ciscoasa(config-if)# shut
ciscoasa(config-if)# ex
ciscoasa(config)# show 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, V - VPN
       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, + - replicated route
Gateway of last resort is 192.1.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [10/0] via 192.1.30.3, Outside-T
C        10.11.11.0 255.255.255.0 is directly connected, Inside
L        10.11.11.10 255.255.255.255 is directly connected, Inside
C        192.1.30.0 255.255.255.0 is directly connected, Outside-T
L        192.1.30.10 255.255.255.255 is directly connected, Outside-T
```

We can still telnet to R1



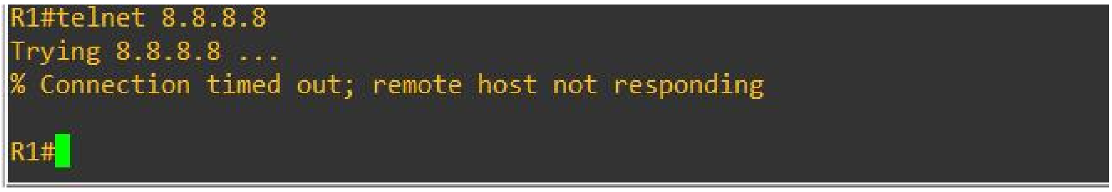
```
R1#telnet 8.8.8.8
Trying 8.8.8.8 ... Open


User Access Verification

Password: 
```



```
R4#sho users
    Line       User       Host(s)              Idle       Location
*  0 con 0                idle                 00:00:00
  98 vty 0                idle                 00:00:17 192.1.30.91

  Interface    User               Mode         Idle     Peer Address
```

At this point, we only have interface level redundancy, what happens what ISP goes down, That is R2 int f 0/0 goes down, it does not use redundancy.

Now, according to firewall, everything is okay, but internet is not working for the users



```
R1#telnet 8.8.8.8
Trying 8.8.8.8 ...
% Connection timed out; remote host not responding

R1#
```

So go to ASA

Sla monitor 10(10 is the number we associate with this sla)

Type echo protocol ipIcmpEcho 8.8.8.8 interface outside-r

Frequency 3

Timout 1000(in ms)

Num-packets 3

Exi

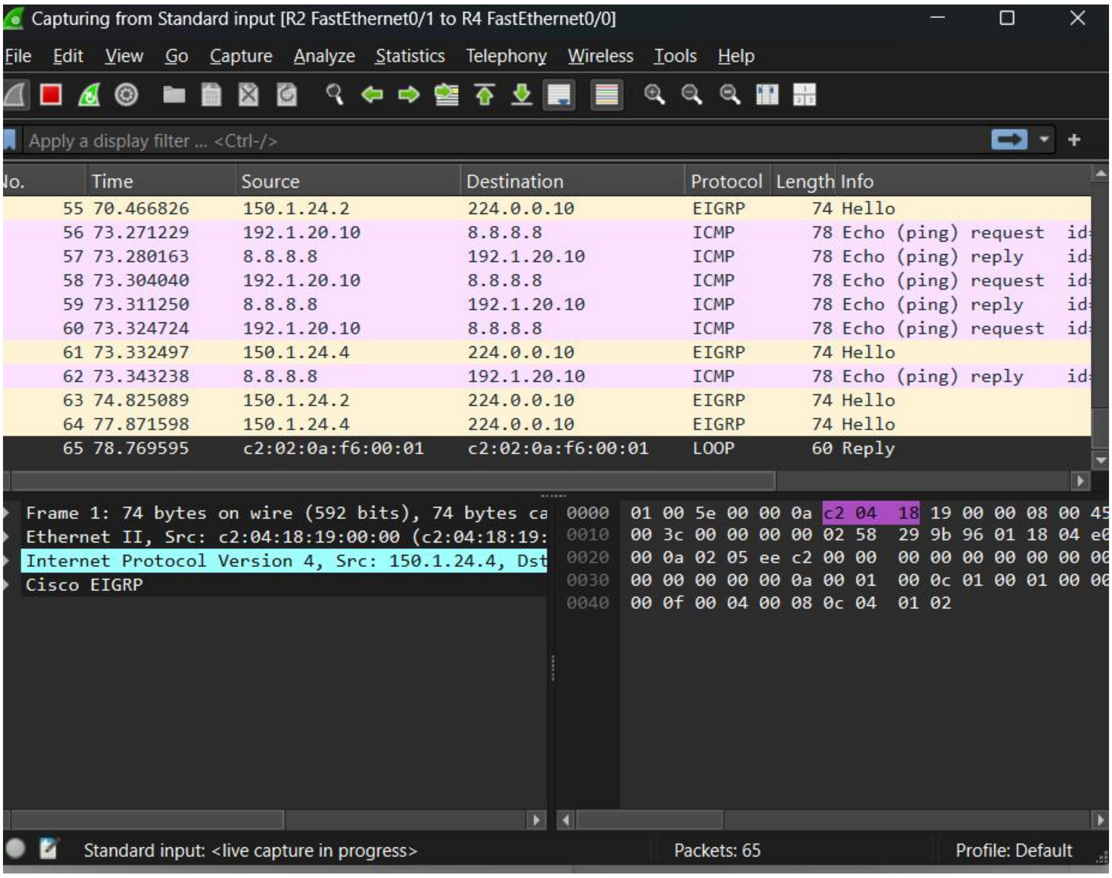
Now we need to start the sla

Sla monitor schedule 10 start-time now life forever

This means we want the probe to be an echo, we can have tcp, udp echo but we want icmp echo, just see that from “?”. After this we specify the address to which we want to send the probe and after that the interface from which we want to send the probe

Frequency is how frequently the probe is sent, default is 60 sec.

We can see on wireshark, these are simple ping packets


Capturing from Standard input [R2 FastEthernet0/1 to R4 FastEthernet0/0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

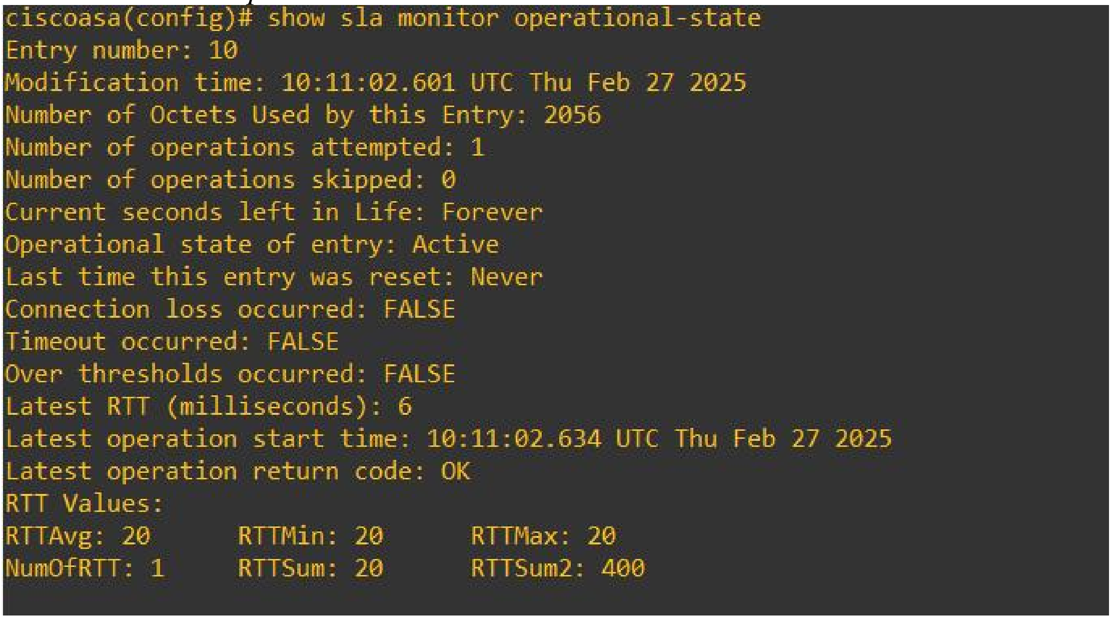
```
lo.     Time        Source          Destination     Protocol Length Info
    55 70.466826   150.1.24.2      224.0.0.10      EIGRP       74 Hello
    56 73.271229   192.1.20.10     8.8.8.8         ICMP        78 Echo (ping) request  id
    57 73.280163   8.8.8.8         192.1.20.10     ICMP        78 Echo (ping) reply    id
    58 73.304040   192.1.20.10     8.8.8.8         ICMP        78 Echo (ping) request  id
    59 73.311250   8.8.8.8         192.1.20.10     ICMP        78 Echo (ping) reply    id
    60 73.324724   192.1.20.10     8.8.8.8         ICMP        78 Echo (ping) request  id
    61 73.332497   150.1.24.4      224.0.0.10      EIGRP       74 Hello
    62 73.343238   8.8.8.8         192.1.20.10     ICMP        78 Echo (ping) reply    id
    63 74.825089   150.1.24.2      224.0.0.10      EIGRP       74 Hello
    64 77.871598   150.1.24.4      224.0.0.10      EIGRP       74 Hello
    65 78.769595   c2:02:0a:f6:00:01 c2:02:0a:f6:00:01 LOOP    60 Reply
```

```
Frame 1: 74 bytes on wire (592 bits), 74 bytes ca
Ethernet II, Src: c2:04:18:19:00:00 (c2:04:18:19:
Internet Protocol Version 4, Src: 150.1.24.4, Dst
Cisco EIGRP
```

```
0000  01 00 5e 00 00 0a c2 04  18 19 00 00 08 00 45
0010  00 3c 00 00 00 00 02 58  29 9b 96 01 18 04 e0
0020  00 0a 02 05 ee c2 00 00  00 00 00 00 00 00 00
0030  00 00 00 00 00 0a 00 01  00 0c 01 00 01 00 00
0040  00 0f 00 04 00 08 0c 04  01 02
```

To see the result

Show sla monitor operational-state



```
ciscoasa(config)# show sla monitor operational-state
Entry number: 10
Modification time: 10:11:02.601 UTC Thu Feb 27 2025
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 6
Latest operation start time: 10:11:02.634 UTC Thu Feb 27 2025
Latest operation return code: OK
RTT Values:
RTTAvg: 20      RTTMin: 20      RTTMax: 20
NumOfRTT: 1     RTTSum: 20      RTTSum2: 400
```

If the “code” = OK we are fine.

We cannot bind sla to anything, so we create track- an object where we call the asnwer of our sla

Track 100 rtr 10 reachability

Rtr means sla

Now we will attach this to our default route, if return code is okay, route should be valid, otherwise down.

ASA Failover

Box level redundancy.In case firewall goes down on the whole, this is used in every company. We have to make sure that everything is same on the two firewalls, the connected interfaces, the ios(should not have major difference, like one should not be pre 8.4 and one is after 8.4), everything, because in case one firewall fails, all the configuration will be directly copied to the active firewall.

ACTIVE/ STANDBY

The first and most important thing is to bring up the interface that we are using for failover on both asa:
Int gigabit0/2
No shut

On primary:

Failover lan enable (not imp for asa)
Failover lan unit primary
Failover key cisco123 (key is imporant because you will be sharing important information through this)

Failover lan interface FL(name we want to keep) *gigabit2* (interface)

Failover interface ip (type of interface) *FL* (name of inteface) *100.100.100.1 255.255.255.0 standby 100.1.00.100.2* (address of standby)

Failover (To start)

On secondary:

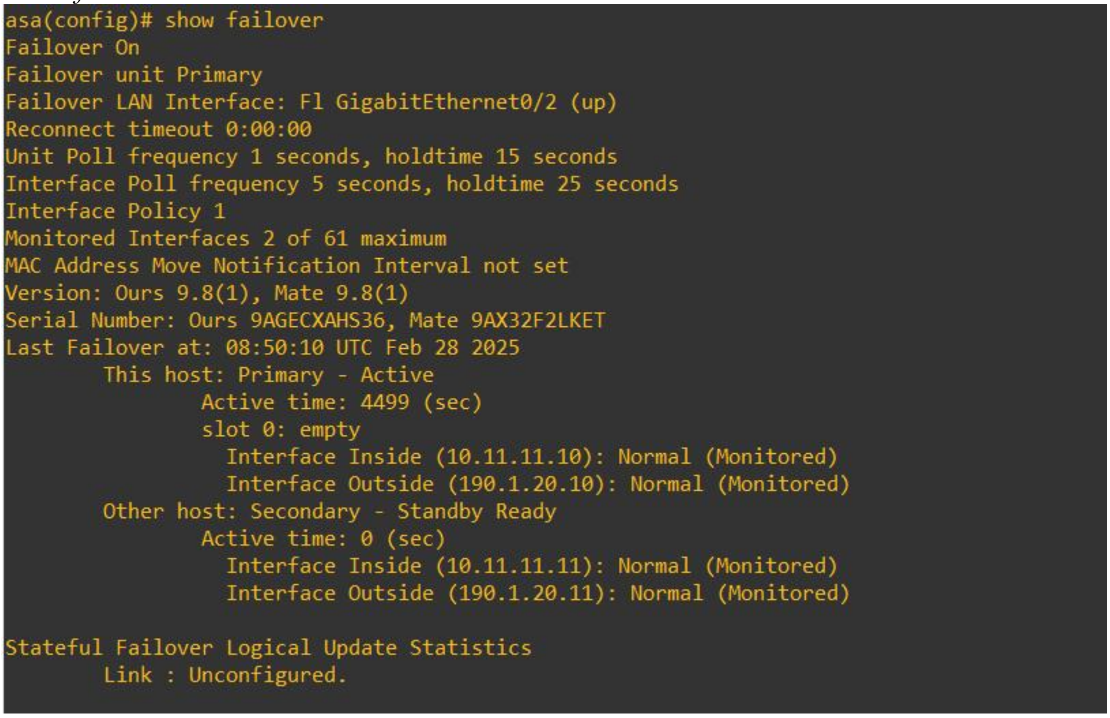
failover lan unit secondary
failover lan interface Fl GigabitEthernet0/2
failover key cisco123
failover interface ip Fl 100.100.100.1 255.255.255.0 standby 100.100.100.2

Then we configure the firewall as we normally do
Int g0/0
Ip add 10.11.11.10 255.255.255.0 standby 10.11.11.11
No shut

The standby address is just giving for the time being, in case of failover, the secondary becomes active, but the ip address of g0/0 will still be 10.11.11.10. Standby will have 10.11.11.11 only so another router can manage it.

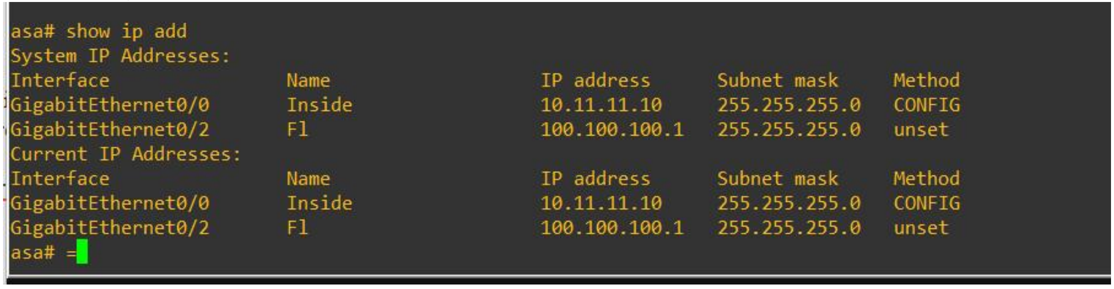
If then, the primary comes back up it will be the standby firewall and the secondary firewall will remain the active firewall.

Show failover



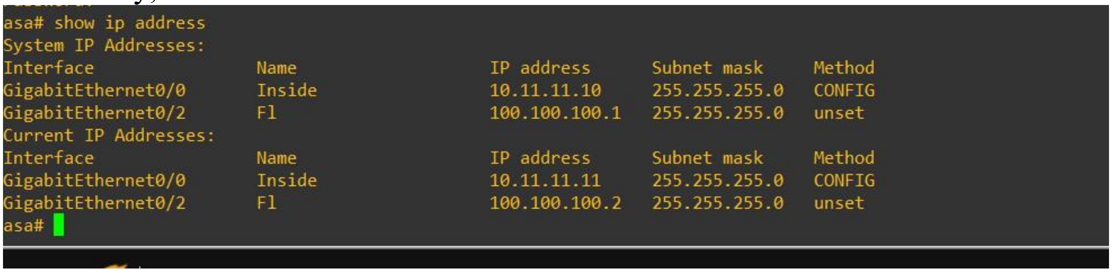
```
asa(config)# show failover
Failover On
Failover unit Primary
Failover LAN Interface: Fl GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 61 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.8(1), Mate 9.8(1)
Serial Number: Ours 9AGECXAHS36, Mate 9AX32F2LKET
Last Failover at: 08:50:10 UTC Feb 28 2025
        This host: Primary - Active
                Active time: 4499 (sec)
                slot 0: empty
                  Interface Inside (10.11.11.10): Normal (Monitored)
                  Interface Outside (190.1.20.10): Normal (Monitored)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface Inside (10.11.11.11): Normal (Monitored)
                  Interface Outside (190.1.20.11): Normal (Monitored)

Stateful Failover Logical Update Statistics
        Link : Unconfigured.
```

On active,



```
asa# show ip add
System IP Addresses:
Interface                Name                  IP address      Subnet mask     Method
GigabitEthernet0/0       Inside                10.11.11.10     255.255.255.0   CONFIG
GigabitEthernet0/2       Fl                    100.100.100.1   255.255.255.0   unset
Current IP Addresses:
Interface                Name                  IP address      Subnet mask     Method
GigabitEthernet0/0       Inside                10.11.11.10     255.255.255.0   CONFIG
GigabitEthernet0/2       Fl                    100.100.100.1   255.255.255.0   unset
asa# =
```

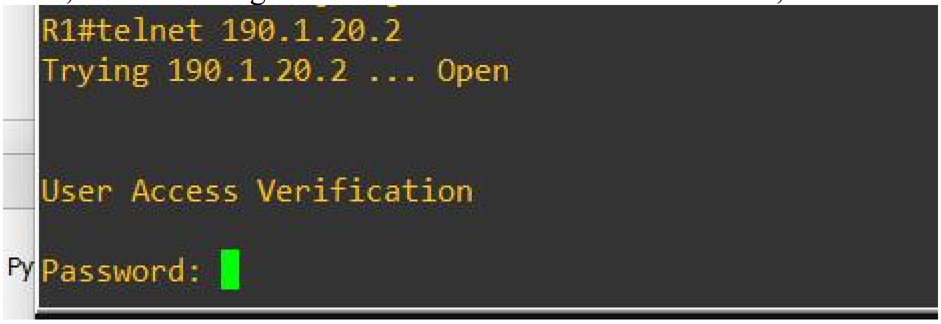
On standby,



```
asa# show ip address
System IP Addresses:
Interface                Name                  IP address      Subnet mask     Method
GigabitEthernet0/0       Inside                10.11.11.10     255.255.255.0   CONFIG
GigabitEthernet0/2       Fl                    100.100.100.1   255.255.255.0   unset
Current IP Addresses:
Interface                Name                  IP address      Subnet mask     Method
GigabitEthernet0/0       Inside                10.11.11.11     255.255.255.0   CONFIG
GigabitEthernet0/2       Fl                    100.100.100.2   255.255.255.0   unset
asa#
```

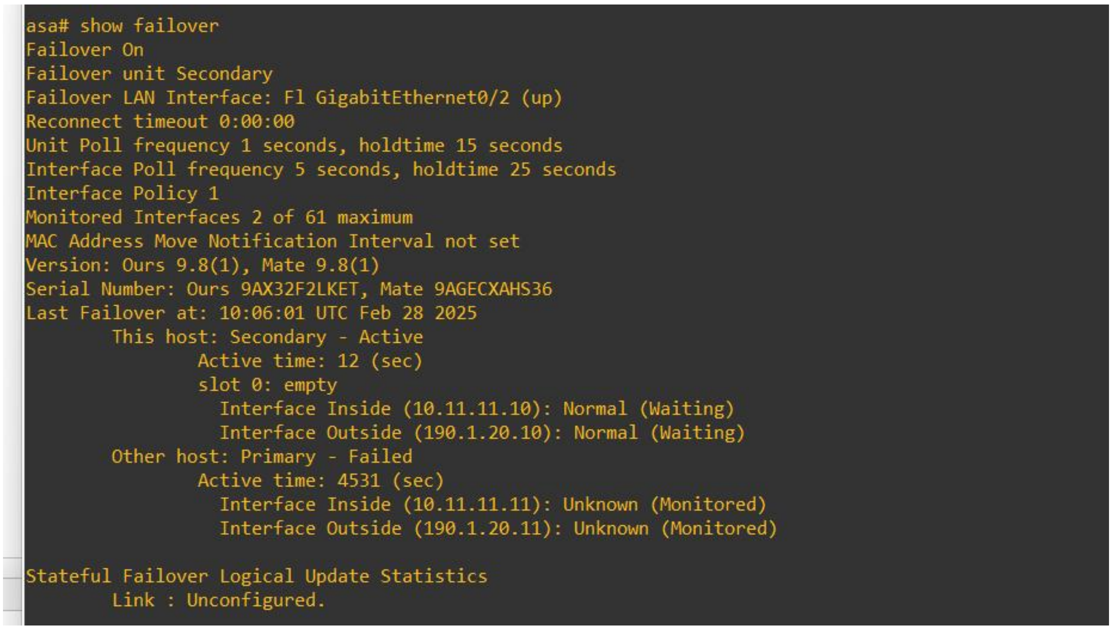
Standby says what its own address is and the system's address, which means that he acknoledges that he is not the system.
If there was no failover configured, the system and current ip addresses would be the same always.

Now, we will configure nat from inside to outside as normal,



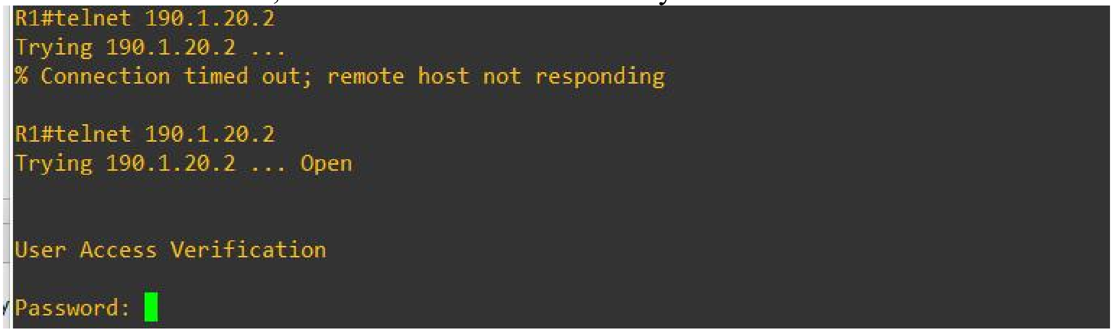
```
R1#telnet 190.1.20.2
Trying 190.1.20.2 ... Open


User Access Verification

Password: 
```

Now let us test the failover by turning off the active firewall, we can see ip changes as well.



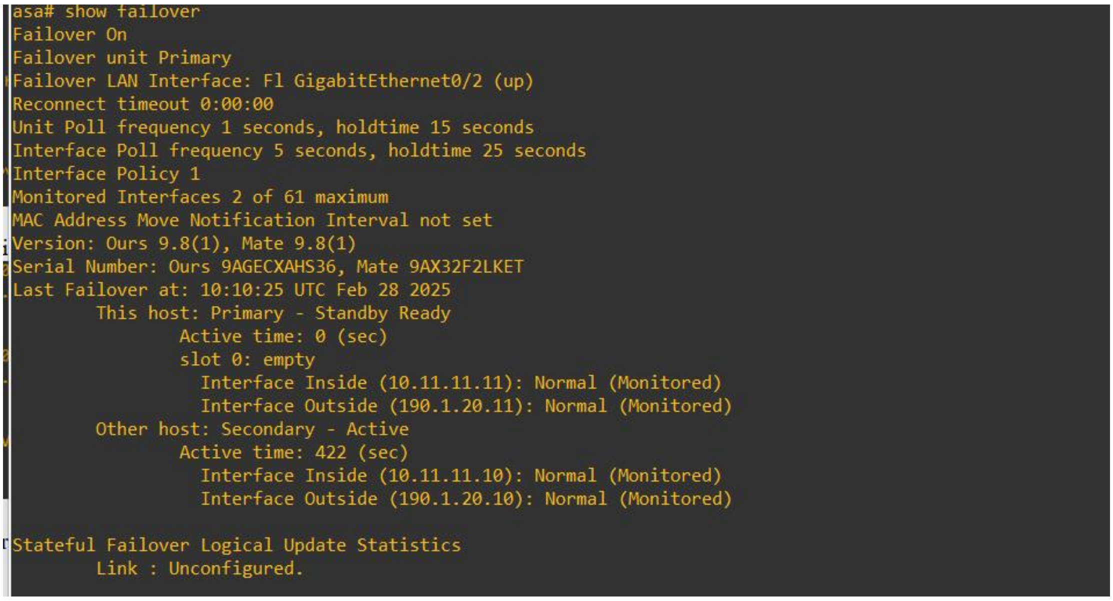
```
asa# show failover
Failover On
Failover unit Secondary
Failover LAN Interface: Fl GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 61 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.8(1), Mate 9.8(1)
Serial Number: Ours 9AX32F2LKET, Mate 9AGECXAHS36
Last Failover at: 10:06:01 UTC Feb 28 2025
        This host: Secondary - Active
                Active time: 12 (sec)
                slot 0: empty
                  Interface Inside (10.11.11.10): Normal (Waiting)
                  Interface Outside (190.1.20.10): Normal (Waiting)
        Other host: Primary - Failed
                Active time: 4531 (sec)
                  Interface Inside (10.11.11.11): Unknown (Monitored)
                  Interface Outside (190.1.20.11): Unknown (Monitored)

Stateful Failover Logical Update Statistics
        Link : Unconfigured.
```

Telnet will still work, even if it will fail once= delay:



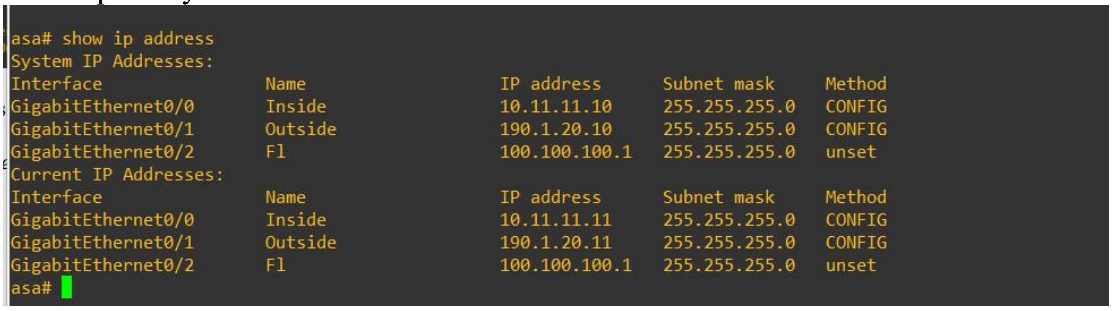
```
R1#telnet 190.1.20.2
Trying 190.1.20.2 ...
% Connection timed out; remote host not responding

R1#telnet 190.1.20.2
Trying 190.1.20.2 ... Open


User Access Verification

Password: 
```

Now, if the primary firewall comes back up, we can see the firewall is primary but it is standby.



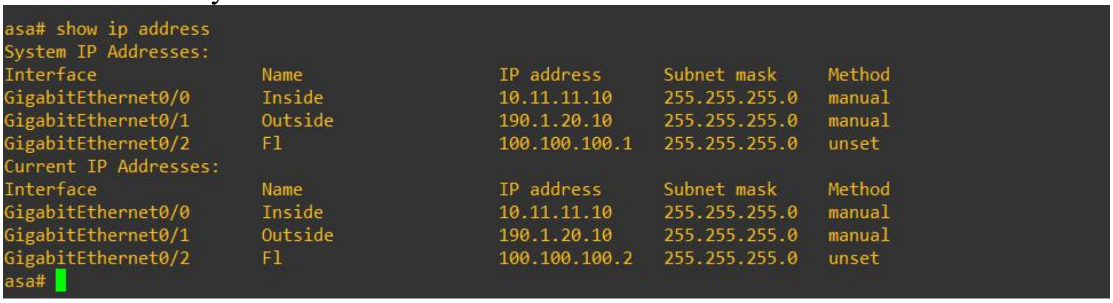
```
asa# show failover
Failover On
Failover unit Primary
Failover LAN Interface: Fl GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 61 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.8(1), Mate 9.8(1)
Serial Number: Ours 9AGECXAHS36, Mate 9AX32F2LKET
Last Failover at: 10:10:25 UTC Feb 28 2025
        This host: Primary - Standby Ready
                Active time: 0 (sec)
                slot 0: empty
                  Interface Inside (10.11.11.11): Normal (Monitored)
                  Interface Outside (190.1.20.11): Normal (Monitored)
        Other host: Secondary - Active
                Active time: 422 (sec)
                  Interface Inside (10.11.11.10): Normal (Monitored)
                  Interface Outside (190.1.20.10): Normal (Monitored)

Stateful Failover Logical Update Statistics
        Link : Unconfigured.
```

We can also see the ip address,
Using
Show ip address
On the primary asa



```
asa# show ip address
System IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
GigabitEthernet0/0       Inside                 10.11.11.10     255.255.255.0   CONFIG
GigabitEthernet0/1       Outside                190.1.20.10     255.255.255.0   CONFIG
GigabitEthernet0/2       Fl                     100.100.100.1   255.255.255.0   unset
Current IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
GigabitEthernet0/0       Inside                 10.11.11.11     255.255.255.0   CONFIG
GigabitEthernet0/1       Outside                190.1.20.11     255.255.255.0   CONFIG
GigabitEthernet0/2       Fl                     100.100.100.1   255.255.255.0   unset
asa#
```

On the secondary asa



```
asa# show ip address
System IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
GigabitEthernet0/0       Inside                 10.11.11.10     255.255.255.0   manual
GigabitEthernet0/1       Outside                190.1.20.10     255.255.255.0   manual
GigabitEthernet0/2       Fl                     100.100.100.1   255.255.255.0   unset
Current IP Addresses:
Interface                Name                   IP address      Subnet mask     Method
GigabitEthernet0/0       Inside                 10.11.11.10     255.255.255.0   manual
GigabitEthernet0/1       Outside                190.1.20.10     255.255.255.0   manual
GigabitEthernet0/2       Fl                     100.100.100.2   255.255.255.0   unset
asa#
```

So we can see there was no change in the default gateway