Configure the ASA for Redundant or Backup ISP Links

Contents

Introduction

This document describes how to configure the Cisco ASA 5500 Series static route tracking feature to use redundant or backup Internet connections.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA 5555-X Series that runs software Version 9.x or later

- Cisco ASDM Version 7.x or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Related Products

You can also use this configuration with the Cisco ASA 5500 Series Version 9.1(5).

> ✎ **Note**: The **backup interface** command is required in order to configure the fourth interface on the ASA 5505 Series. Refer to the [backup interface](#) section of the *Cisco Security Appliance Command Reference, Version 7.2* for more information.

Background Information

This section provides an overview of the static route tracking feature that is described in this document, as well as some important recommendations before you begin.

Static Route Tracking Feature Overview

One problem with the use of static routes is that no inherent mechanism exists that can determine whether the route is up or down.

The route remains in the routing table even if the next hop gateway becomes unavailable.

Static routes are removed from the routing table only if the associated interface on the security appliance goes down.

In order to solve this problem, a static route tracking feature is used in order to track the availability of a static route.

The feature removes the static route from the routing table and replaces it with a backup route upon failure.

Static route tracking allows the ASA to use an inexpensive connection to a secondary ISP in the event that the primary leased line becomes unavailable.

In order to achieve this redundancy, the ASA associates a static route with a monitoring target that you define.

The Service Level Agreement (SLA) operation monitors the target with periodic ICMP echo requests.

If an echo reply is not received, then the object is considered down, and the associated route is removed from the routing table.

A previously configured backup route is used in place of the route that is removed.

While the backup route is in use, the SLA monitor operation continues its attempts to reach the monitoring target.

Once the target is available again, the first route is replaced in the routing table, and the backup route is removed.

In the example that is used in this document, the ASA maintains two connections to the Internet.

The first connection is a high speed leased line that is accessed through a router provided by the primary ISP.

The second connection is a lower speed Digital Subscriber Line (DSL) that is accessed through a DSL modem provided by the secondary ISP.

✎ **Note**: The configuration that is described in this document cannot be used for load balancing or load sharing, as it is not supported on the ASA. Use this configuration for redundancy or backup purposes only. Outbound traffic uses the primary ISP, and then the secondary ISP if the primary fails. Failure of the primary ISP causes a temporary disruption of traffic.

The DSL connection is idle as long as the leased line is active and the primary ISP gateway is reachable.

However, if the connection to the primary ISP goes down, the ASA changes the routing table in order to direct traffic to the DSL connection.

Static route tracking is used in order to achieve this redundancy.

The ASA is configured with a static route that directs all of the Internet traffic to the primary ISP.

Every ten seconds, the SLA monitor process checks in order to confirm that the primary ISP gateway is reachable.

If the SLA monitor process determines that the primary ISP gateway is not reachable, the static route that directs traffic to that interface is removed from the routing table.

In order to replace that static route, an alternate static route that directs traffic to the secondary ISP is installed.

This alternate static route directs traffic to the secondary ISP through the DSL modem until the link to the primary ISP is reachable.

This configuration provides a relatively inexpensive way to ensure that outbound Internet access remains available to users behind the ASA.

As described in this document, this setup is not always suitable for inbound access to resources behind the ASA. Advanced networking skills are required in order to achieve seamless inbound connections.

These skills are not covered in this document.

Important Recommendations

Before you attempt the configuration that is described in this document, you must choose a monitoring target that can respond to Internet Control Message Protocol (ICMP) echo requests.

The target can be any network object that you choose, but a target that is closely tied to your Internet Service Provider (ISP) connection is recommended.

Here are some possible monitoring targets:

- The ISP gateway address
- Another ISP-managed address
- A server on another network, such as an Authentication, Authorization, and Accounting (AAA) server with which the ASA must communicate

- A persistent network object on another network (a desktop or notebook computer that you can shut down at night is not a good choice)

This document assumes that the ASA is fully operational and configured in order to allow the Cisco Adaptive Security Device Manager (ASDM) to make configuration changes.

🔍 **Tip**: For information about how to allow the ASDM to configure the device, refer to the Configuring HTTPS Access for ASDM section of the *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.1*.

Configure

Use the information that is described in this section in order to configure the ASA for the use of the static route tracking feature.

✎ **Note**: Use the Command Lookup Tool (registered customers only) in order to obtain more information about the commands that are used in this section.

✎ **Note**: The IP addresses that are used in this configuration are not legally routable on the Internet. They are RFC 1918 ⬀ addresses, which are used in a lab environment.

Network Diagram

The example that is provided in this section uses this network setup:
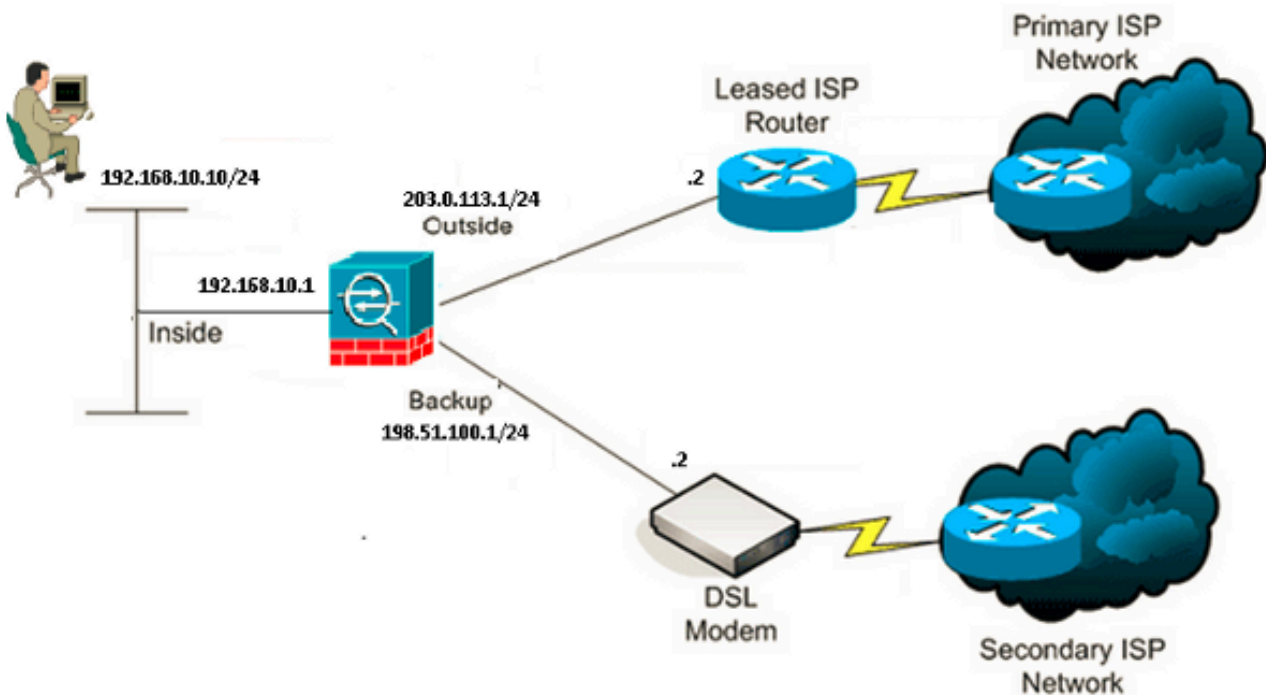
CLI Configuration

Use this information in order to configure the ASA via the CLI :

<#root>

ASA#

 show running-config

```
ASA Version 9.1(5)
!
hostname ASA
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.1 255.255.255.0
!
interface GigabitEthernet0/2
 nameif backup
 security-level 0
 ip address 198.51.100.1 255.255.255.0


!--- The interface attached to the Secondary ISP.


!--- "backup" was chosen here, but any name can be assigned.


!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa915-smp-k8.bin
```

```
ftp mode passive
clock timezone IND 5 30
object network Inside_Network
 subnet 192.168.10.0 255.255.255.0
object network inside_network
 subnet 192.168.10.0 255.255.255.0
pager lines 24
logging enable
mtu inside 1500
mtu outside 1500
mtu backup 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network Inside_Network
 nat (inside,outside) dynamic interface
object network inside_network
 nat (inside,backup) dynamic interface
```

!--- NAT Configuration for Outside and Backup

```
route outside 0.0.0.0 0.0.0.0 203.0.113.2 1 track 1
```

!--- Enter this command in order to track a static route.

!--- This is the static route to be installed in the routing

!--- table while the tracked object is reachable. The value after

!--- the keyword "track" is a tracking ID you specify.

```
route backup 0.0.0.0 0.0.0.0 198.51.100.2 254
```

!--- Define the backup route to use when the tracked object is unavailable.

!--- The administrative distance of the backup route must be greater than

!--- the administrative distance of the tracked route.

!--- If the primary gateway is unreachable, that route is removed

!--- and the backup route is installed in the routing table

```
!--- instead of the tracked route.



timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00

sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 interface outside
 num-packets 3
 frequency 10


!--- Configure a new monitoring process with the ID 123.  Specify the
!--- monitoring protocol and the target network object whose availability the tracking
!--- process monitors.  Specify the number of packets to be sent with each poll.
!--- Specify the rate at which the monitor process repeats (in seconds).



sla monitor schedule 123 life forever start-time now


!--- Schedule the monitoring process.  In this case the lifetime
!--- of the process is specified to be forever.  The process is scheduled to begin
!--- at the time this command is entered.  As configured, this command allows the
!--- monitoring configuration specified above to determine how often the testing
!--- occurs.  However, you can schedule this monitoring process to begin in the
!--- future and to only occur at specified times.



crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
!
track 1 rtr 123 reachability


!--- Associate a tracked static route with the SLA monitoring process.
!--- The track ID corresponds to the track ID given to the static route to monitor:
!--- route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1
!--- "rtr" = Response Time Reporter entry.  123 is the ID of the SLA process
!--- defined above.



telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
priority-queue inside
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
```

```
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
!
service-policy global_policy global
```
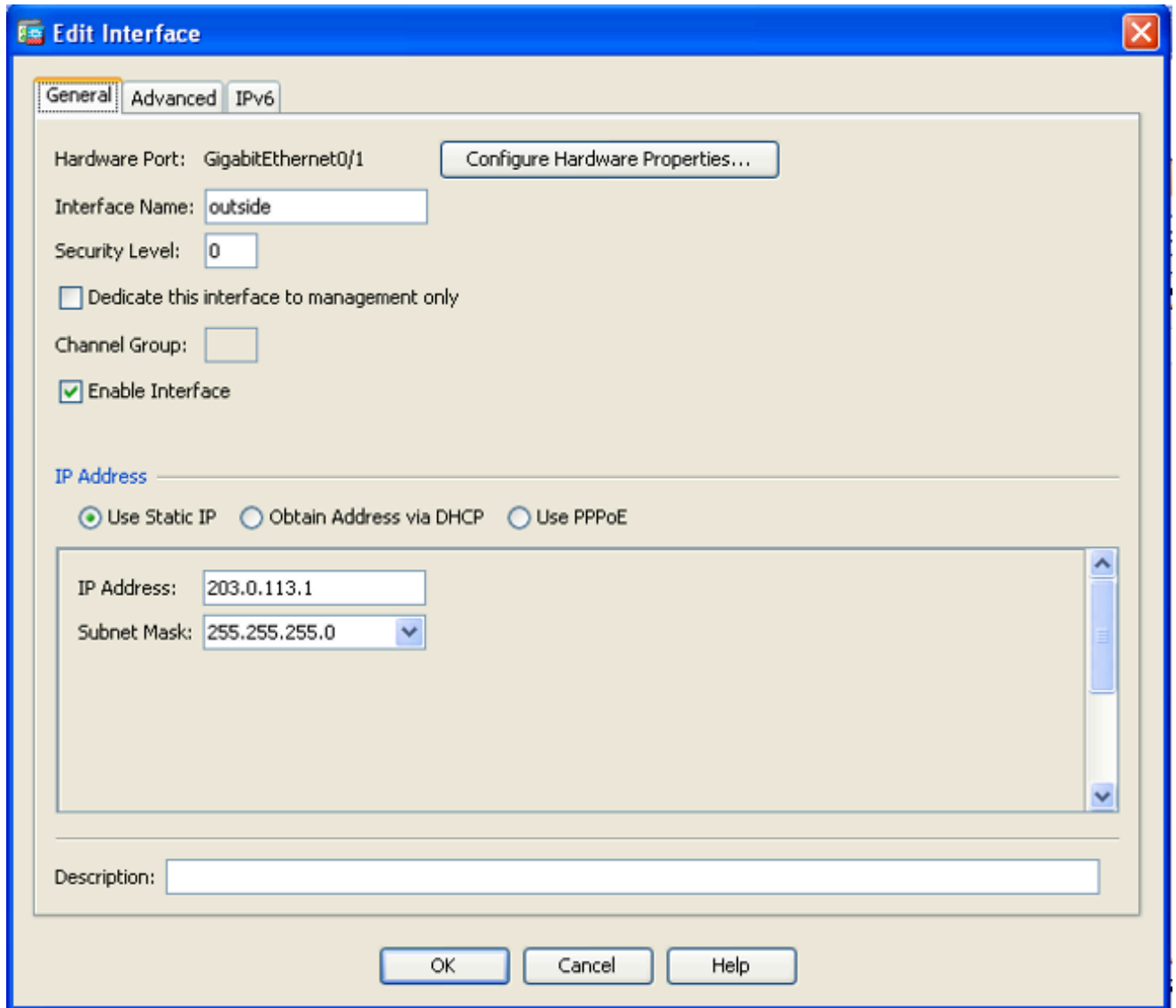
ASDM Configuration

Complete these steps in order to configure redundant or backup ISP support with the ASDM application:

1. Within the ASDM application, click **Configuration**, and then click **Interfaces**.
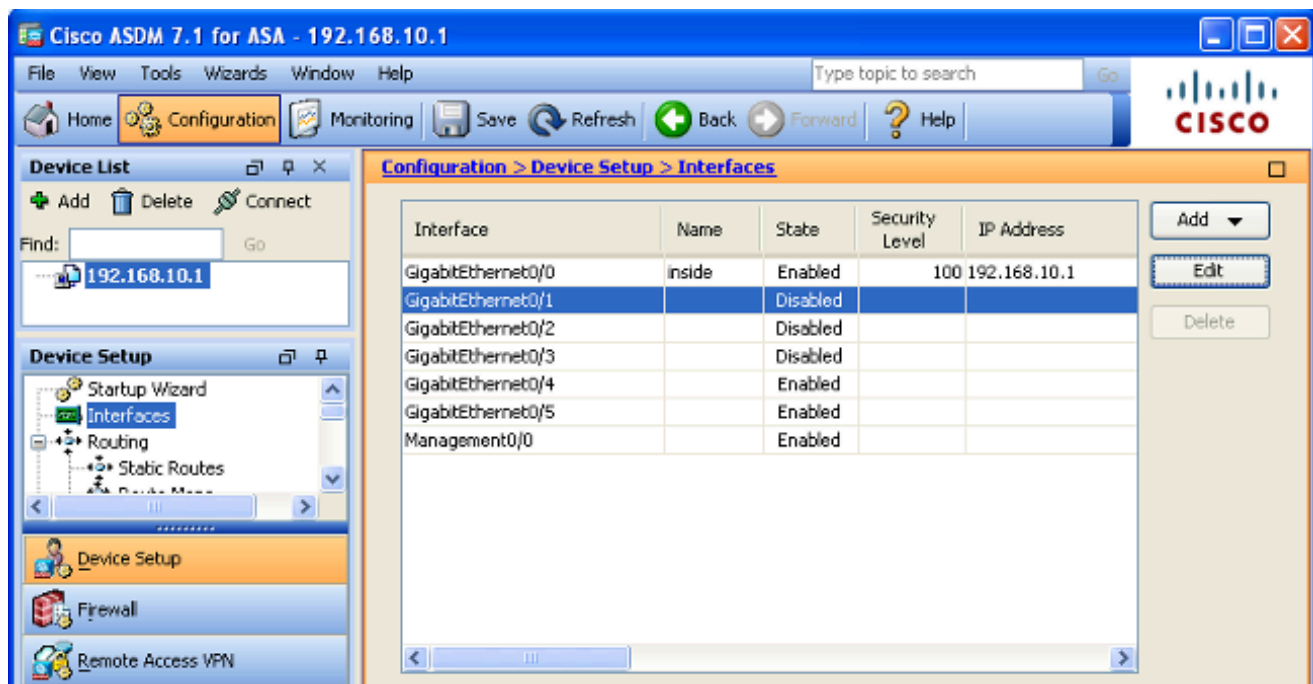
2. Select **GigabitEthernet0/1** from the Interfaces list, and then click **Edit**. This dialog box appears:

Edit Interface

General | Advanced | IPv6

Hardware Port: GigabitEthernet0/1   [Configure Hardware Properties...]

Interface Name: outside

Security Level: 0

☐ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

◉ Use Static IP   ○ Obtain Address via DHCP   ○ Use PPPoE

IP Address: 203.0.113.1

Subnet Mask: 255.255.255.0

Description:

[OK] [Cancel] [Help]

3. Check the **Enable Interface** check box, and enter the appropriate values in the *Interface Name*, *Security Level*, *IP Address*, and *Subnet Mask* fields.

4. Click **OK** in order to close the dialog box.

5. Configure the other interfaces as needed, and then click **Apply** in order to update the ASA configuration:
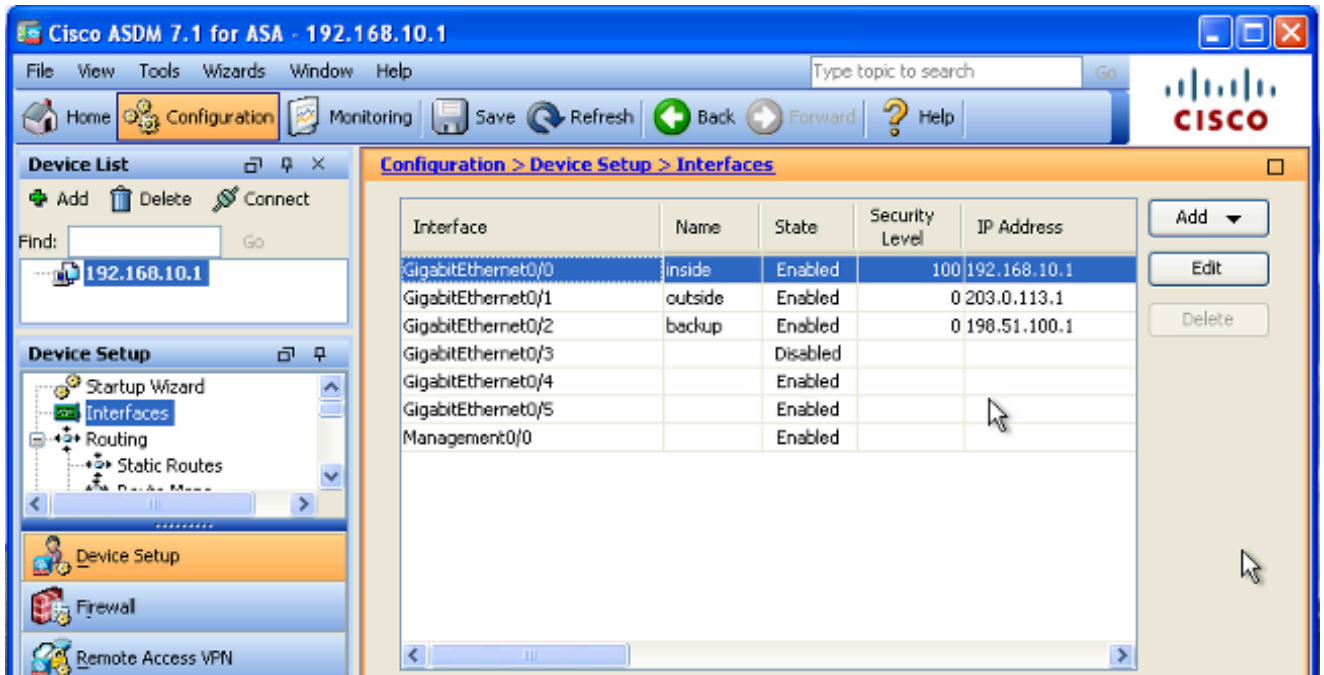
6. Select **Routing** and click **Static Routes** located on the left side of the ASDM application:
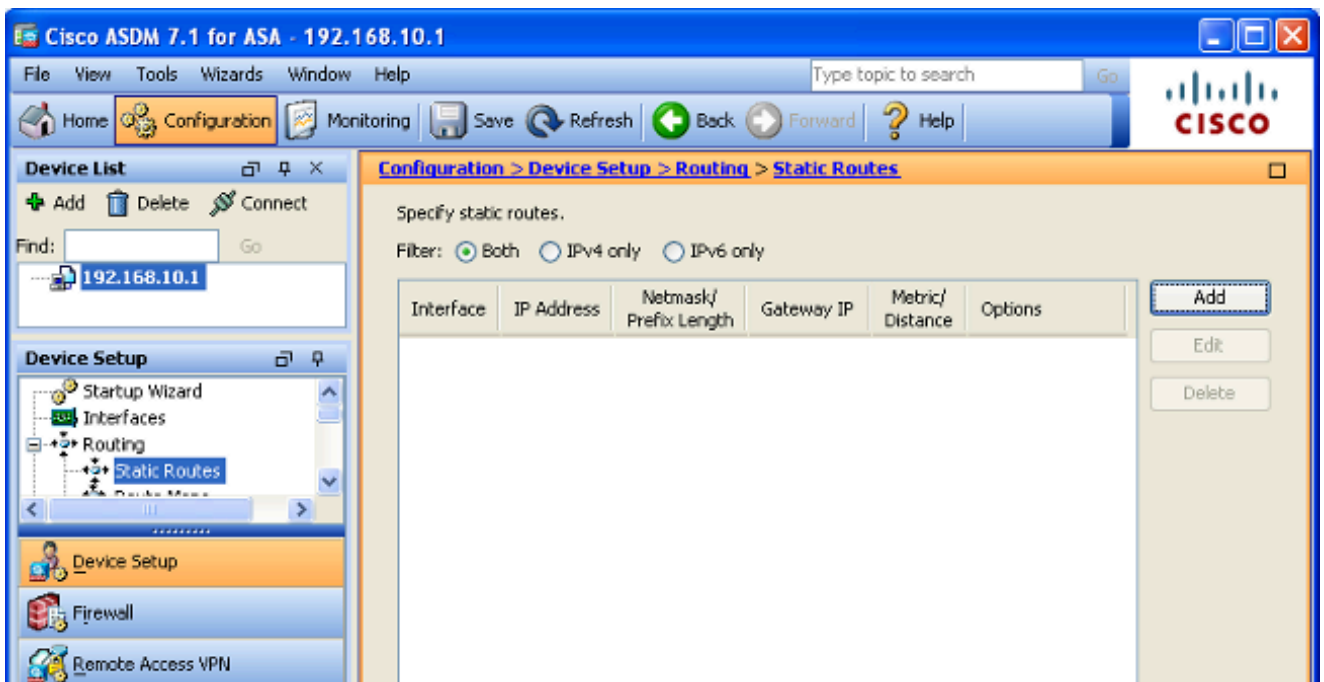
7. Click **Add** in order to add the new static routes. This dialog box appears:

Edit Static Route

IP Address Type: ⦿ IPv4   ○ IPv6

Interface: outside ⌄

Network: any4 [...]

Gateway IP: 203.0.113.2 [...]   Metric: 1

Options

○ None

○ Tunneled (Default tunnel gateway for VPN traffic)

⦿ Tracked

Track ID: 1   Track IP Address: 4.2.2.2

SLA ID: 123   Target Interface: outside ⌄

[Monitoring Options]

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

[OK]   [Cancel]   [Help]

8. From the Interface Name drop-down list, choose the interface on which the route resides, and configure the default route to reach the gateway. In this example, **203.0.113.2** is the primary ISP gateway and **4.2.2.2** is the object to monitor with ICMP echoes.

9. In the Options area, click the **Tracked** radio button and enter the appropriate values in the *Track ID*, *SLA ID*, and *Track IP Address* fields.

10. Click **Monitoring Options**. This dialog box appears:
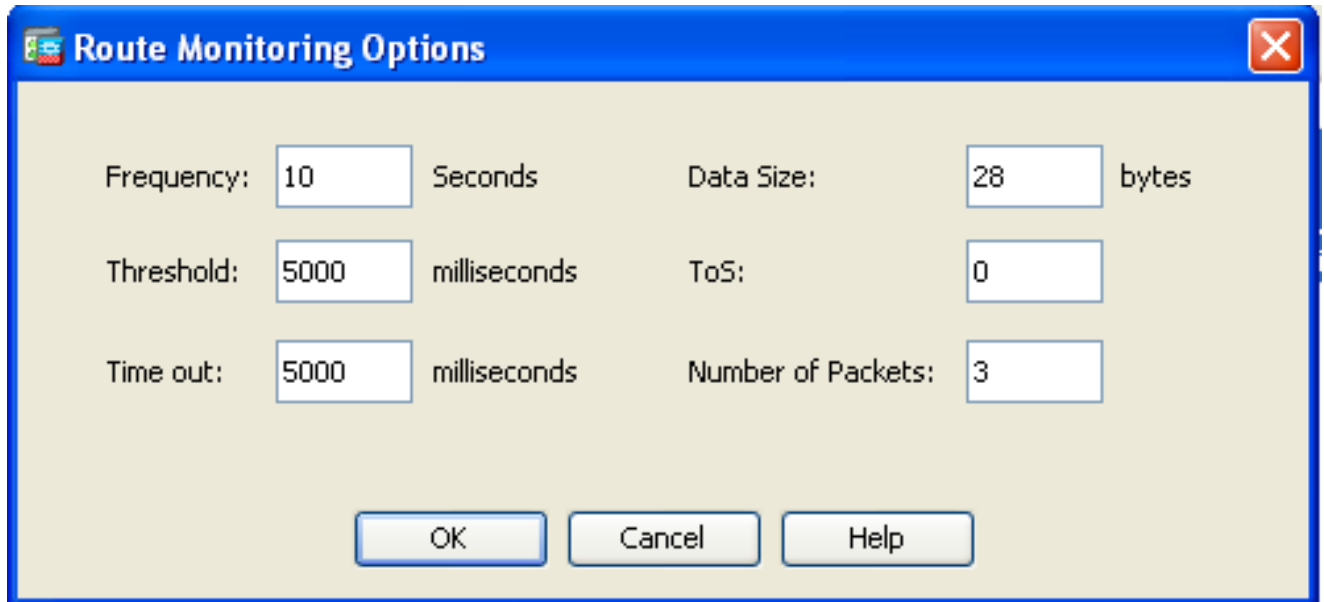
11. Enter the appropriate values for the frequency and other monitoring options, and then click **OK**.

12. Add another static route for the secondary ISP in order to provide a route to reach the Internet. In order to make it a secondary route, configure this route with a higher metric, such as 254. If the primary route (primary ISP) fails, that route is removed from the routing table. This secondary route (secondary ISP) is installed in the Private Internet Exchange (PIX) routing table instead.

13. Click **OK** in order to close the dialog box:

Edit Static Route

IP Address Type: ● IPv4 ○ IPv6

Interface: backup

Network: any4

Gateway IP: 198.51.100.2   Metric: 254

Options

● None

○ Tunneled (Default tunnel gateway for VPN traffic)

○ Tracked
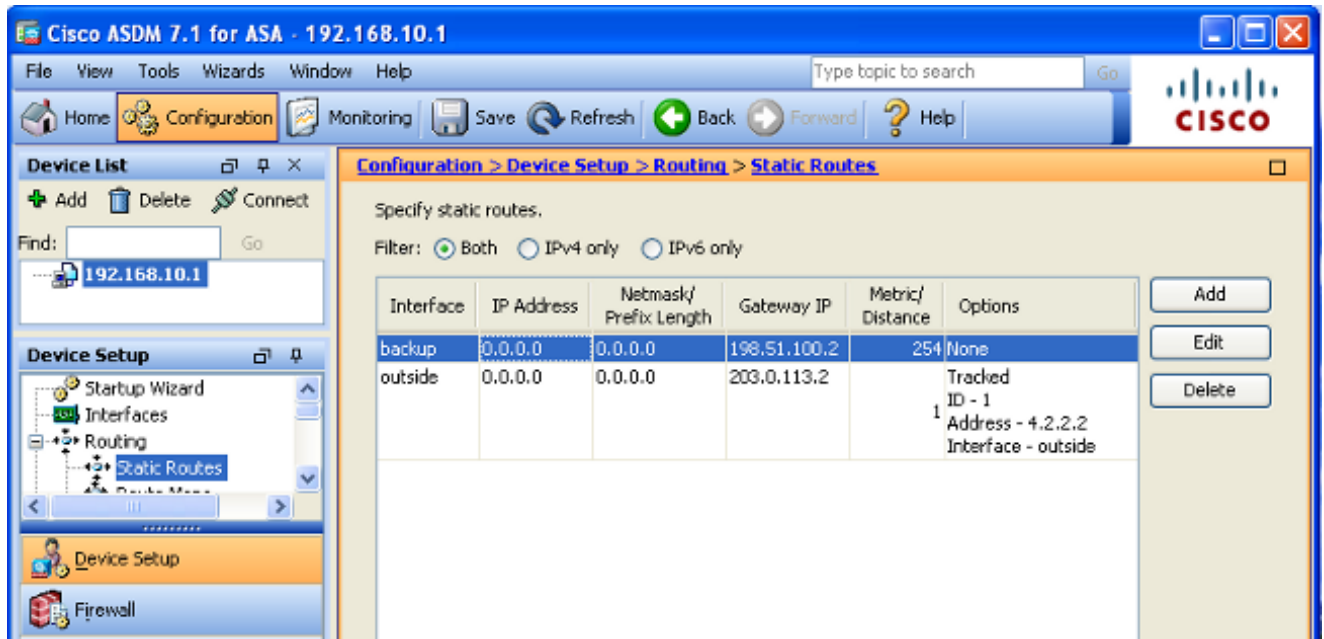
Track ID: [   ]   Track IP Address: [   ]

SLA ID: [   ]   Target Interface: backup

Monitoring Options

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

OK   Cancel   Help

The configurations appear in the Interface list:

14. Select the routing configuration, and then click **Apply** in order to update the ASA configuration.

Verify

Use this section in order to confirm that your configuration works properly.

Confirm that the Configuration is Complete

✎ **Note**: The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

Use these **show** commands in order to verify that your configuration is complete:

- **show running-config sla monitor** – The output of this command displays the SLA commands in the configuration.

  <#root>

  ASA#

  show running-config sla monitor

  sla monitor 123
   type echo protocol ipIcmpEcho 4.2.2.2 interface outside
   num-packets 3
   frequency 10
  sla monitor schedule 123 life forever start-time now

- **show sla monitor configuration** – The output of this command displays the current configuration settings of the operation.

  <#root>

```
ASA#

show sla monitor configuration 123


IP SLA Monitor, Infrastructure Engine-II.
Entry number: 123
Owner:
Tag:
Type of operation to perform: echo
Target address: 4.2.2.2
Interface: outside
Number of packets: 3
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data&colon; No
Operation frequency (seconds): 10
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

- **show sla monitor operational-state** – The output of this command displays the operational statistics of the SLA operation.

  - Before the primary ISP fails, this is the operational state:

    ```
    <#root>

    ASA#

    show sla monitor operational-state 123


    Entry number: 123
    Modification time: 13:30:40.672 IND Sun Jan 4 2015
    Number of Octets Used by this Entry: 2056
    Number of operations attempted: 46
    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): 1



    Latest operation start time: 13:38:10.672 IND Sun Jan 4 2015



    Latest operation return code: OK
    ```

```
                RTT Values:
                RTTAvg: 1          RTTMin: 1          RTTMax: 1
                NumOfRTT: 3        RTTSum: 3          RTTSum2: 3
```

     ◦ After the primary ISP fails (and the ICMP echoes time-out), this is the operational state:

        <#root>

        ASA#

        show sla monitor operational-state

```
        Entry number: 123
        Modification time: 13:30:40.671 IND Sun Jan 4 2015
        Number of Octets Used by this Entry: 2056
        Number of operations attempted: 57
        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: TRUE

```
        Over thresholds occurred: FALSE
```

        Latest RTT (milliseconds): NoConnection/Busy/Timeout

        Latest operation start time: 13:40:00.672 IND Sun Jan 4 2015

        Latest operation return code: Timeout

```
        RTT Values:
        RTTAvg: 0          RTTMin: 0          RTTMax: 0
        NumOfRTT: 0        RTTSum: 0          RTTSum2: 0
```

Confirm that the Backup Route is Installed (CLI Method)

Enter the **show route** command in order to confirm that the backup route is installed.

Before the primary ISP fails, the routing table appears similar to this:

<#root>

ASA#

show route

```
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
         i - IS-IS, 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
```

Gateway of last resort is 203.0.113.2 to network 0.0.0.0

```
C    203.0.113.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
C    198.51.100.0 255.255.255.0 is directly connected, backup
```

S*   0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside

After the primary ISP fails, the static route is removed, and the backup route is installed, the routing table appears similar to this:

<#root>

ASA#

show route

```
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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
```

Gateway of last resort is 198.51.100.2 to network 0.0.0.0

```
C    203.0.113.0 255.255.255.0 is directly connected, outside
C    192.168.10.0 255.255.255.0 is directly connected, inside
C    198.51.100.0 255.255.255.0 is directly connected, backup
```

S*   0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup

## Confirm that the Backup Route is Installed (ASDM Method)

In order to confirm that the backup route is installed via the ASDM, navigate to **Monitoring > Routing**, and then choose **Routes** from the Routing tree.

Before the primary ISP fails, the routing table appears similar to that shown in the next image. Note that the **DEFAULT** route points to **203.0.113.2** through the **outside** interface:
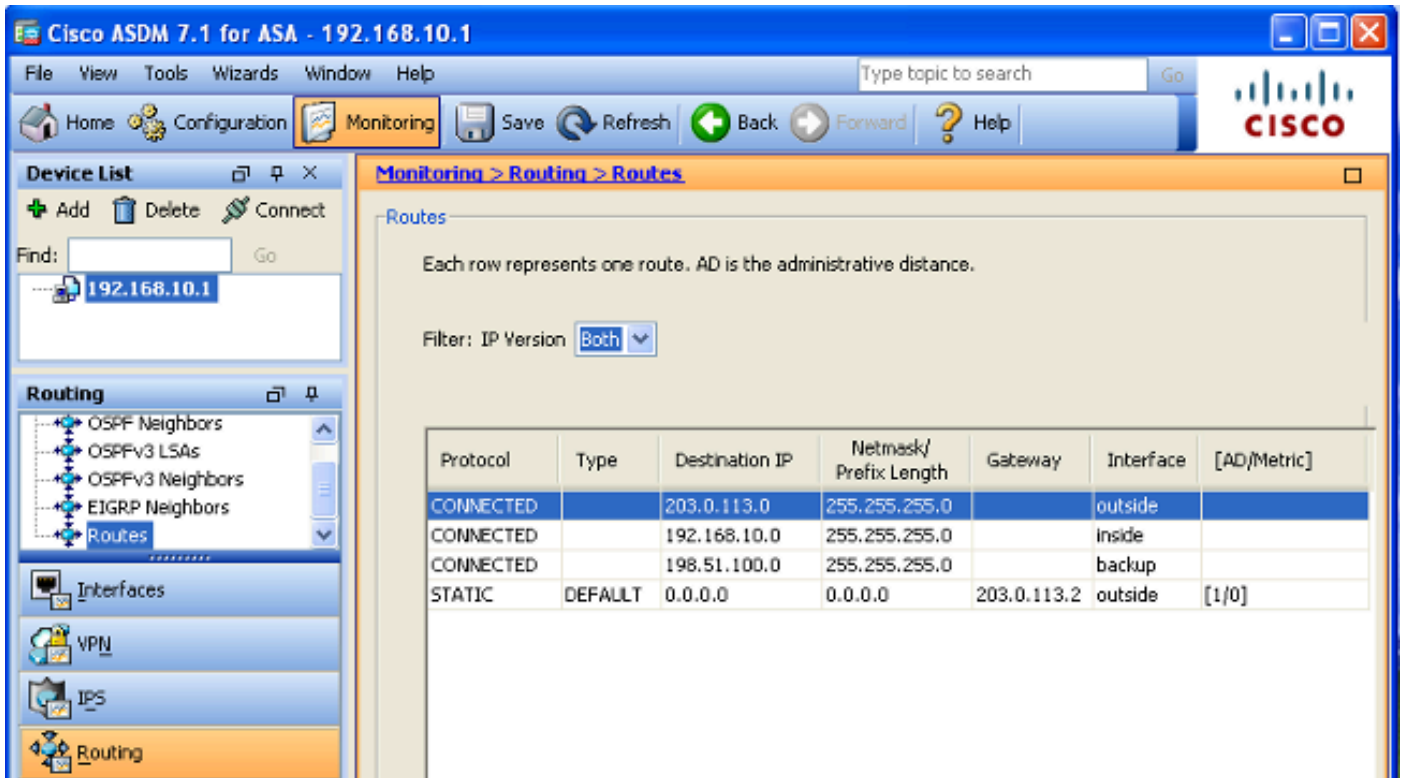
After the primary ISP fails, the route is removed and the backup route is installed. The **DEFAULT** route now points to **198.51.100.2** through the **backup** interface:
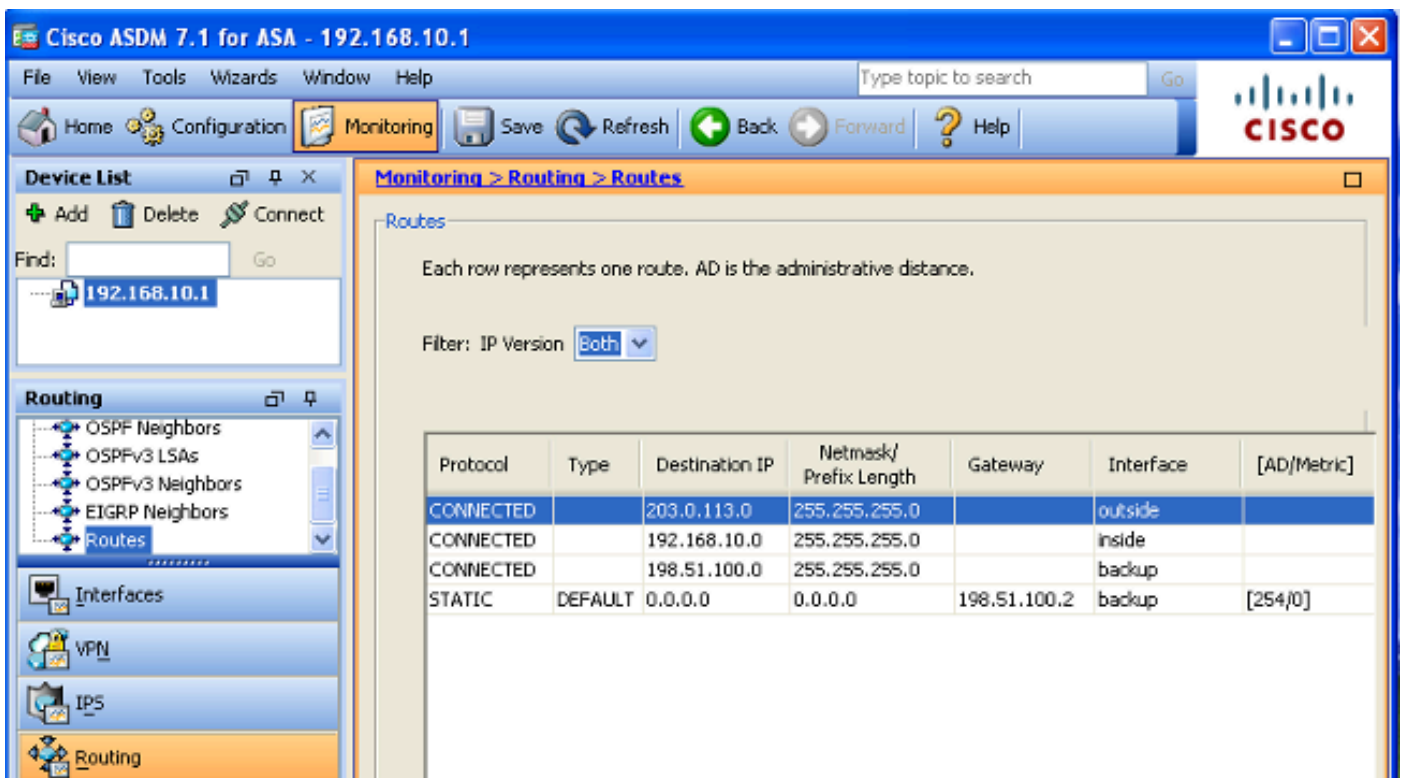
Troubleshoot

This section provides some useful debug commands and describes how to troubleshoot an issue where the tracked route is removed unnecessarily.

Debug Commands

You can use these debug commands in order to troubleshoot your configuration issues:

- **debug sla monitor trace** – The output of this command displays the progress of the echo operation.

  - If the tracked object (primary ISP gateway) is up and the ICMP echoes succeed, the output appears similar to this:

    ```
    IP SLA Monitor(123) Scheduler: Starting an operation
    IP SLA Monitor(123) echo operation: Sending an echo operation
    IP SLA Monitor(123) echo operation: RTT=0 OK
    IP SLA Monitor(123) echo operation: RTT=0 OK
    IP SLA Monitor(123) echo operation: RTT=1 OK
    IP SLA Monitor(123) Scheduler: Updating result
    ```

  - If the tracked object (primary ISP gateway) is down and the ICMP echoes fail, the output appears similar to this:

    ```
    IP SLA Monitor(123) Scheduler: Starting an operation
    IP SLA Monitor(123) echo operation: Sending an echo operation
    IP SLA Monitor(123) echo operation: Timeout
    IP SLA Monitor(123) echo operation: Timeout
    IP SLA Monitor(123) echo operation: Timeout
    IP SLA Monitor(123) Scheduler: Updating result
    ```

- **debug sla monitor error** – The output of this command displays any errors that the SLA monitor process encounters.

  - If the tracked object (primary ISP gateway) is up and the ICMP succeeds, the output appears similar to this:

    ```
    %ASA-7-609001: Built local-host identity:203.0.113.1
    %ASA-7-609001: Built local-host outside:4.2.2.2
    %ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
     gaddr 203.0.113.1/39878 laddr 203.0.113.1/39878
    %ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
     203.0.113.1/39878 laddr 203.0.113.1/39878
    %ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
    %ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
    %ASA-7-609001: Built local-host identity:203.0.113.1
    %ASA-7-609001: Built local-host outside:4.2.2.2
    %ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
     gaddr 203.0.113.1/39879 laddr 203.0.113.1/39879
    %ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
     203.0.113.1/39879 laddr 203.0.113.1/39879
    %ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
    %ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
    ```

  - If the tracked object (primary ISP gateway) is down and the tracked route is removed, the

output appears similar to this:

```
<#root>

%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
 gaddr 203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
 gaddr 203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
 gaddr 203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
 203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
 203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
 203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:02
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:02
%ASA-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 203.0.113.2,
 distance 1, table Default-IP-Routing-Table, on interface outside


!--- 4.2.2.2 is unreachable, so the route to the Primary ISP is removed.
```

Tracked Route is Removed Unnecessarily

If the tracked route is removed unnecessarily, ensure that your monitoring target is always available to receive echo requests.

In addition, ensure that the state of your monitoring target (that is, whether or not the target is reachable) is closely tied to the state of the primary ISP connection.

If you choose a monitoring target that is farther away than the ISP gateway, another link along that route possibly fails or another device possibly interferes.

This configuration therefore potentially causes the SLA monitor to conclude that the connection to the primary ISP has failed and cause the ASA to unnecessarily fail over to the secondary ISP link.

For example, if you choose a branch office router as your monitoring target, the ISP connection to your branch office could fail, as well as any other link along the way.

Once the ICMP echoes that are sent by the monitoring operation fail, the primary tracked route is removed, even though the primary ISP link is still active.

In this example, the primary ISP gateway that is used as the monitoring target is managed by the ISP and is located on the other side of the ISP link.

This configuration ensures that if the ICMP echoes that are sent by the monitoring operation fail, the ISP link is almost surely down.

Related Information

- [Cisco ASA 5500-X Series Next-Generation Firewalls](#)
- [Technical Support & Documentation - Cisco Systems](#)