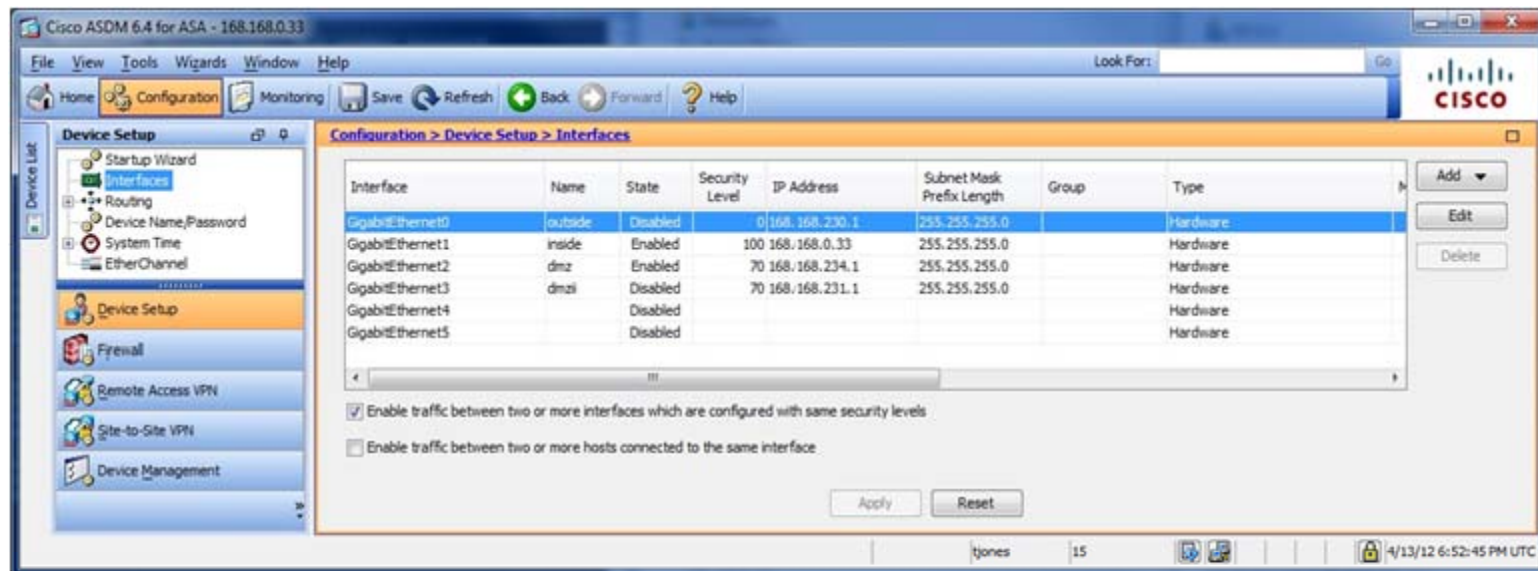


# Cisco ASA Security Appliances



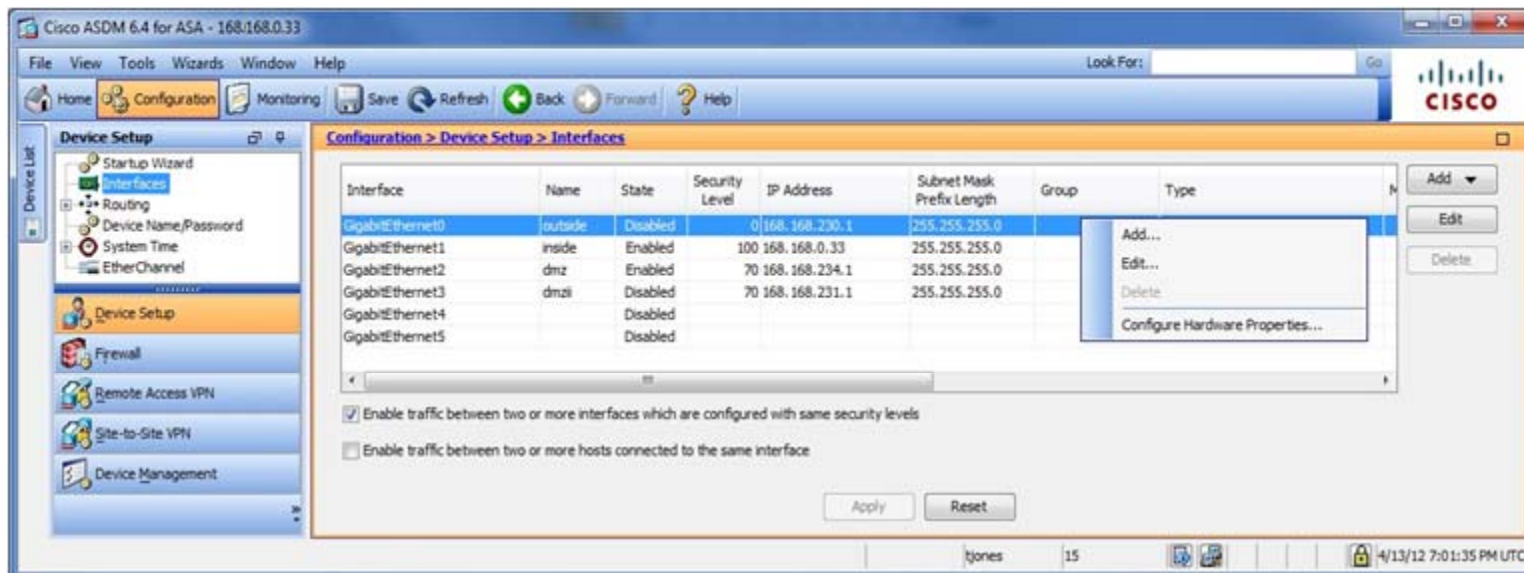
# Cisco ASA Security Appliances

- The figure below is the configuration section for the Cisco ASDM v6.4.
- As can be seen, the interfaces are not configured with IPv6 addresses.



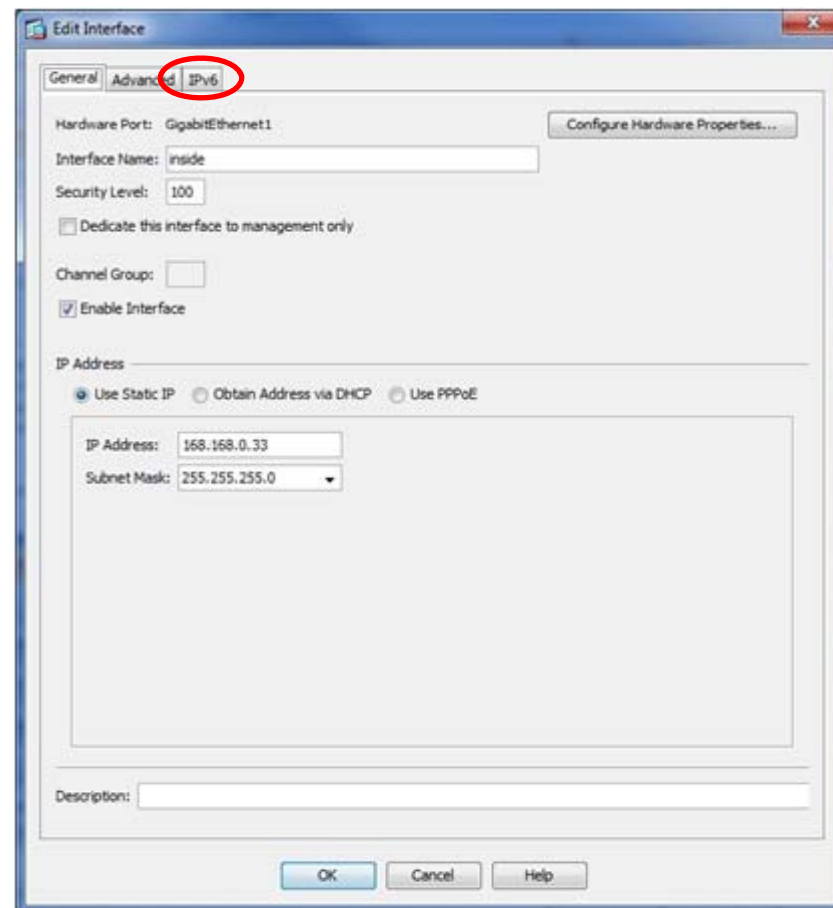
# Cisco ASA – Configuration – Interfaces

- To edit an interface, right click on the interface and select Edit. (Or highlight the interface and choose the Edit button on the right).



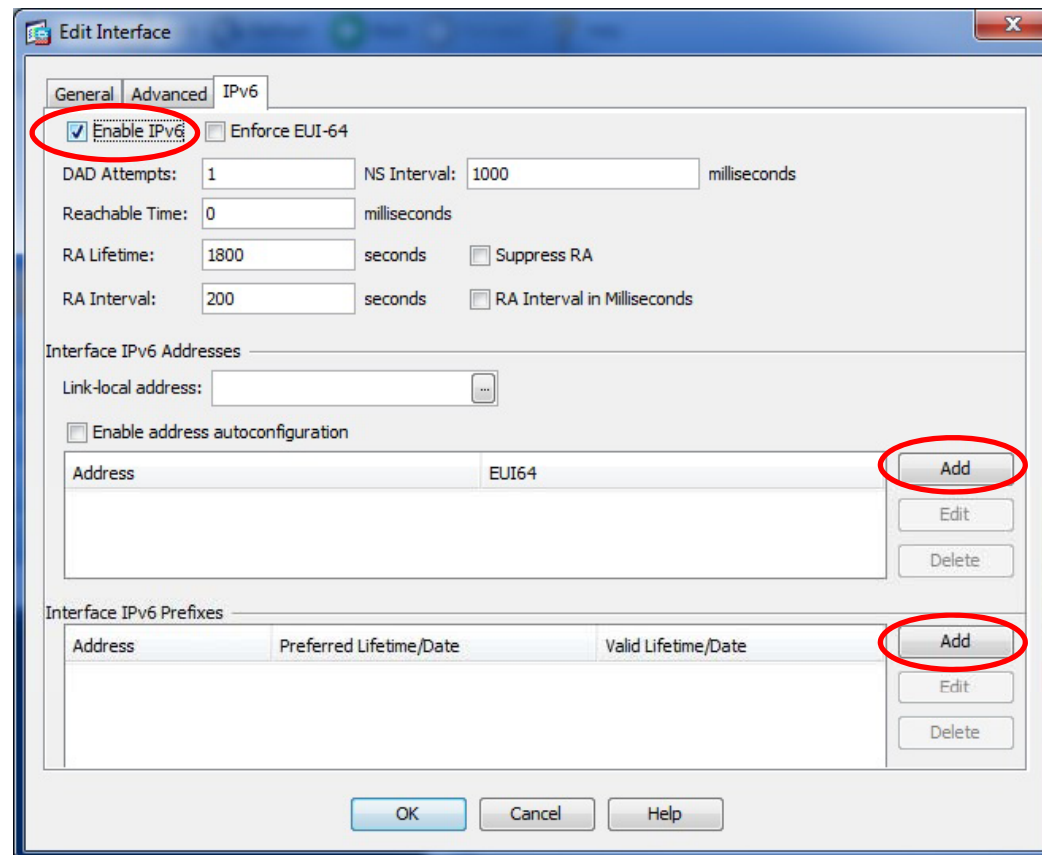
# Cisco ASA – Edit Interfaces

- When the Edit Interface dialog box appears, choose the IPv6 tab to edit the IPv6 settings for the interface. Here we are modifying the ‘inside’ interface GigabitEthernet1.



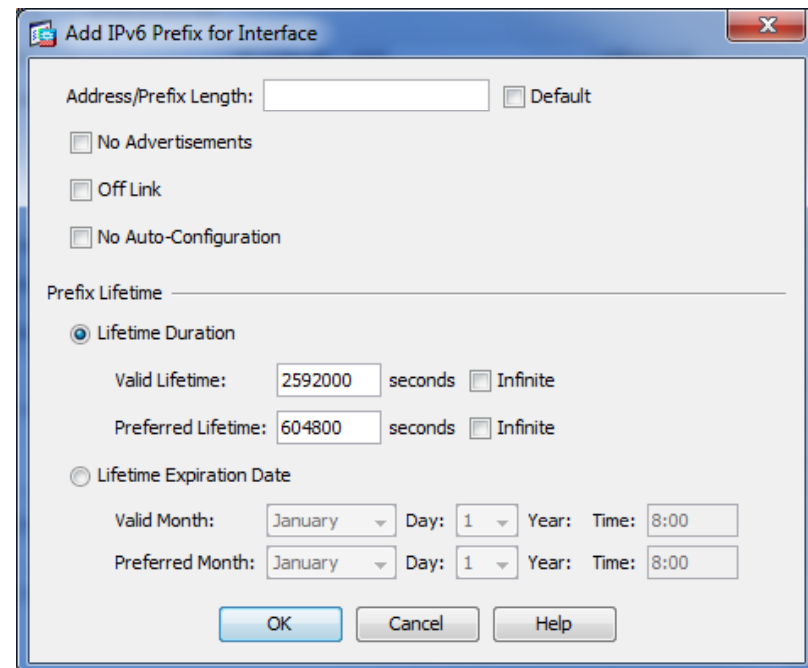
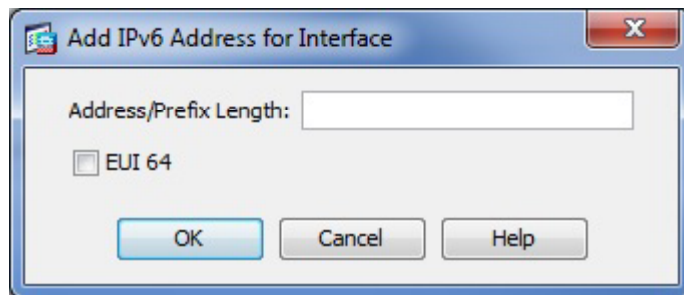
# Cisco ASA - Edit Interfaces – IPv6

- First, check the checkbox for ‘Enable IPv6’
- Next, add both the Interface IPv6 Address and the Interface IPv6 Prefix.



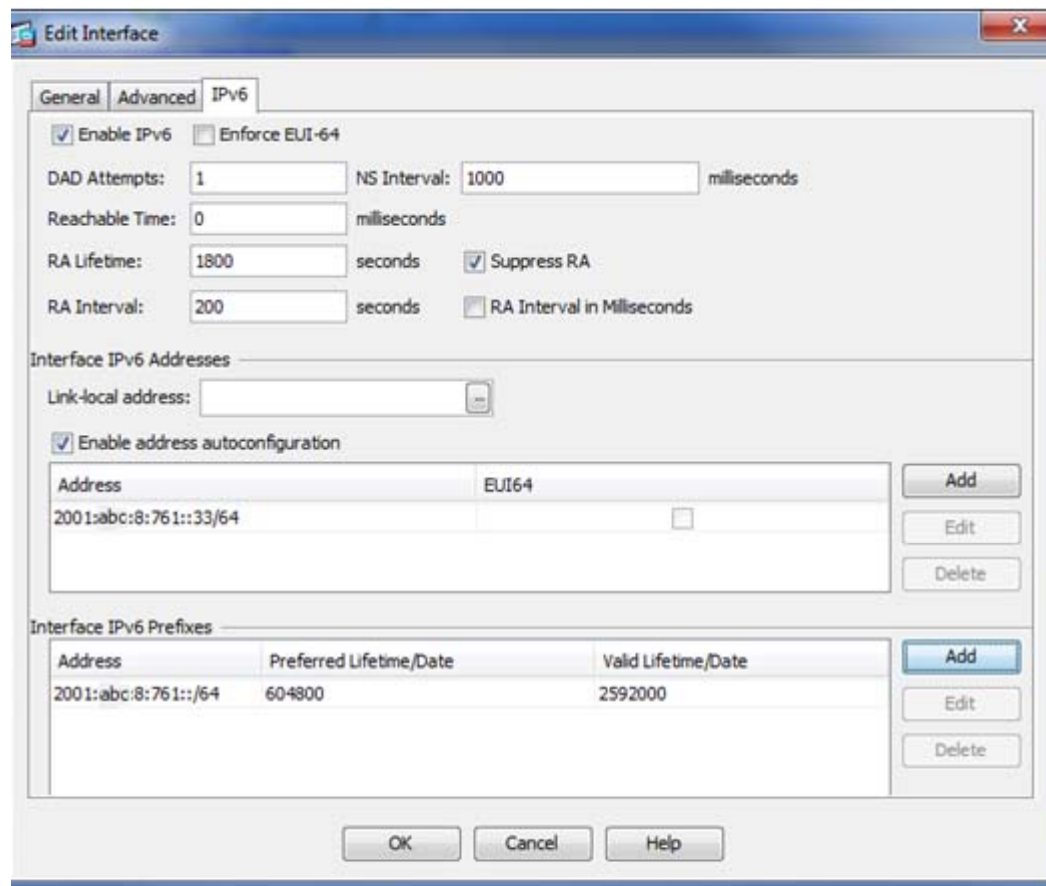
# Cisco ASA – Add IPv6 Address

- The dialog box on the left is for adding an IPv6 address to the interface. If you want it to be an EUI-64 compliant.
- The dialog box on the right is to add an IPv6 prefix for the interface. IPv6 prefixes are included in IPv6 router advertisements.



# Cisco ASA – Edit Interfaces

- After entering the information for the IPv6 address and prefix, the information is now set on the interface.



The screenshot shows the 'Edit Interface' configuration window with the 'IPv6' tab selected. The configuration includes the following settings:

- Enable IPv6
- Enforce EUI-64
- DAD Attempts: 1
- NS Interval: 1000 milliseconds
- Reachable Time: 0 milliseconds
- RA Lifetime: 1800 seconds
- Suppress RA
- RA Interval: 200 seconds
- RA Interval in Milliseconds

Interface IPv6 Addresses:

Link-local address: [ ]

Enable address autoconfiguration

Address	EUI64
2001:abc:8:761::33/64	<input type="checkbox"/>

Buttons: Add, Edit, Delete

Interface IPv6 Prefixes:

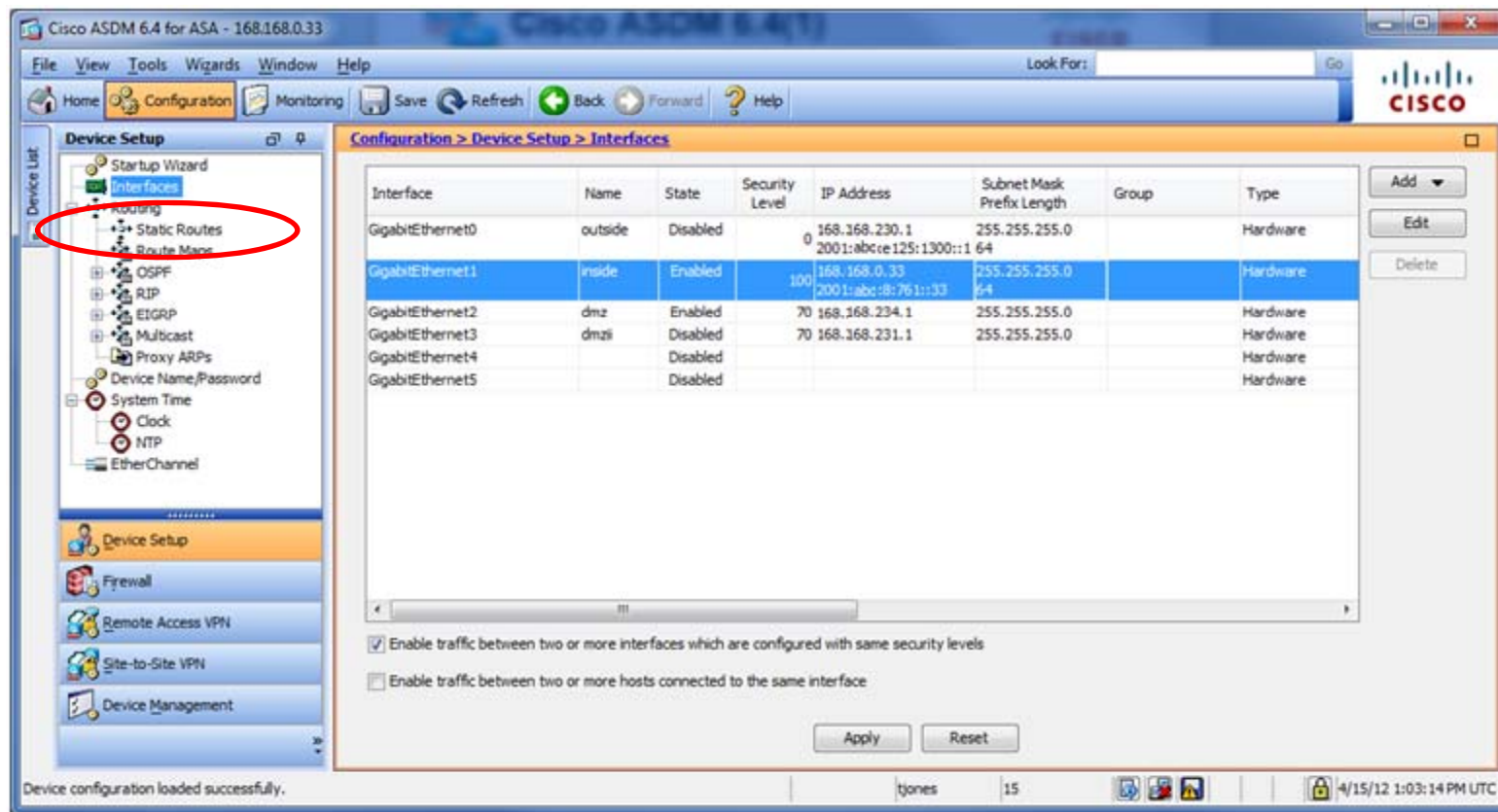
Address	Preferred Lifetime/Date	Valid Lifetime/Date
2001:abc:8:761::/64	604800	2592000

Buttons: Add, Edit, Delete

Bottom buttons: OK, Cancel, Help

# Cisco ASA – Routing IPv6

- Now we need a default route. Select Static Routes under Routing from the Device Setup menu on the right.



The screenshot shows the Cisco ASDM 6.4 for ASA - 168.168.0.33 interface configuration page. The left-hand 'Device Setup' menu is expanded to show the 'Routing' section, with 'Static Routes' highlighted by a red circle. The main pane displays a table of interfaces:

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type
GigabitEthernet0	outside	Disabled	0	168.168.230.1	255.255.255.0		Hardware
GigabitEthernet1	inside	Enabled	100	168.168.0.33	255.255.255.0		Hardware
GigabitEthernet2	dmz	Enabled		70.168.168.234.1	255.255.255.0		Hardware
GigabitEthernet3	dmzi	Disabled		70.168.168.231.1	255.255.255.0		Hardware
GigabitEthernet4		Disabled					Hardware
GigabitEthernet5		Disabled					Hardware

Below the table, there are two checkboxes:

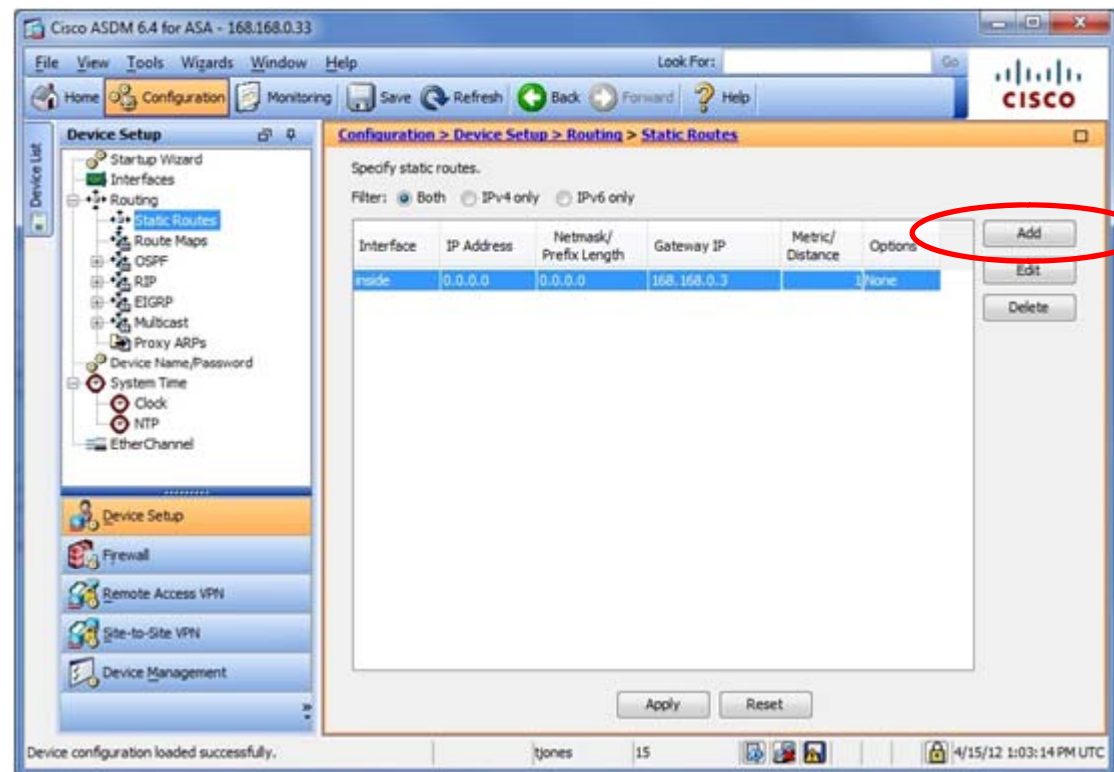
- Enable traffic between two or more interfaces which are configured with same security levels
- Enable traffic between two or more hosts connected to the same interface

Buttons for 'Apply' and 'Reset' are visible at the bottom of the configuration pane.



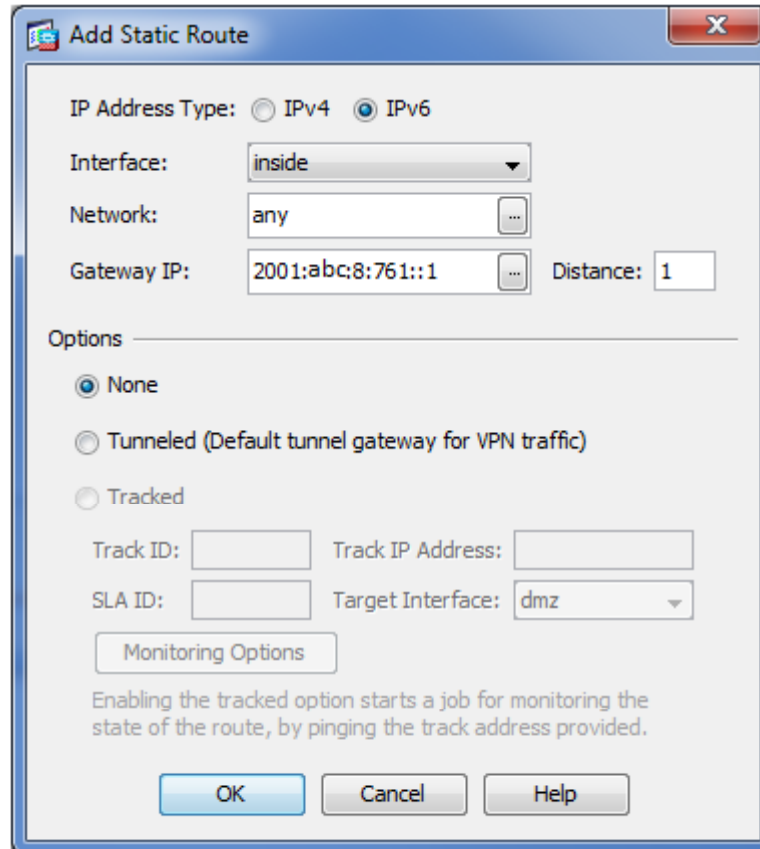
# Cisco ASA - Routing

- From the Static Routes dialog box, select the 'Add' button on the right.



# Cisco ASA – Routing – Add static

- In the ‘Add Static Route’ dialog, select the address type as IPv6, then enter ‘any’ for the network and enter the IPv6 address for the ‘Gateway IP’.



**Add Static Route**

IP Address Type:  IPv4  IPv6

Interface:

Network:

Gateway IP:  Distance:

Options

None

Tunneled (Default tunnel gateway for VPN traffic)

Tracked

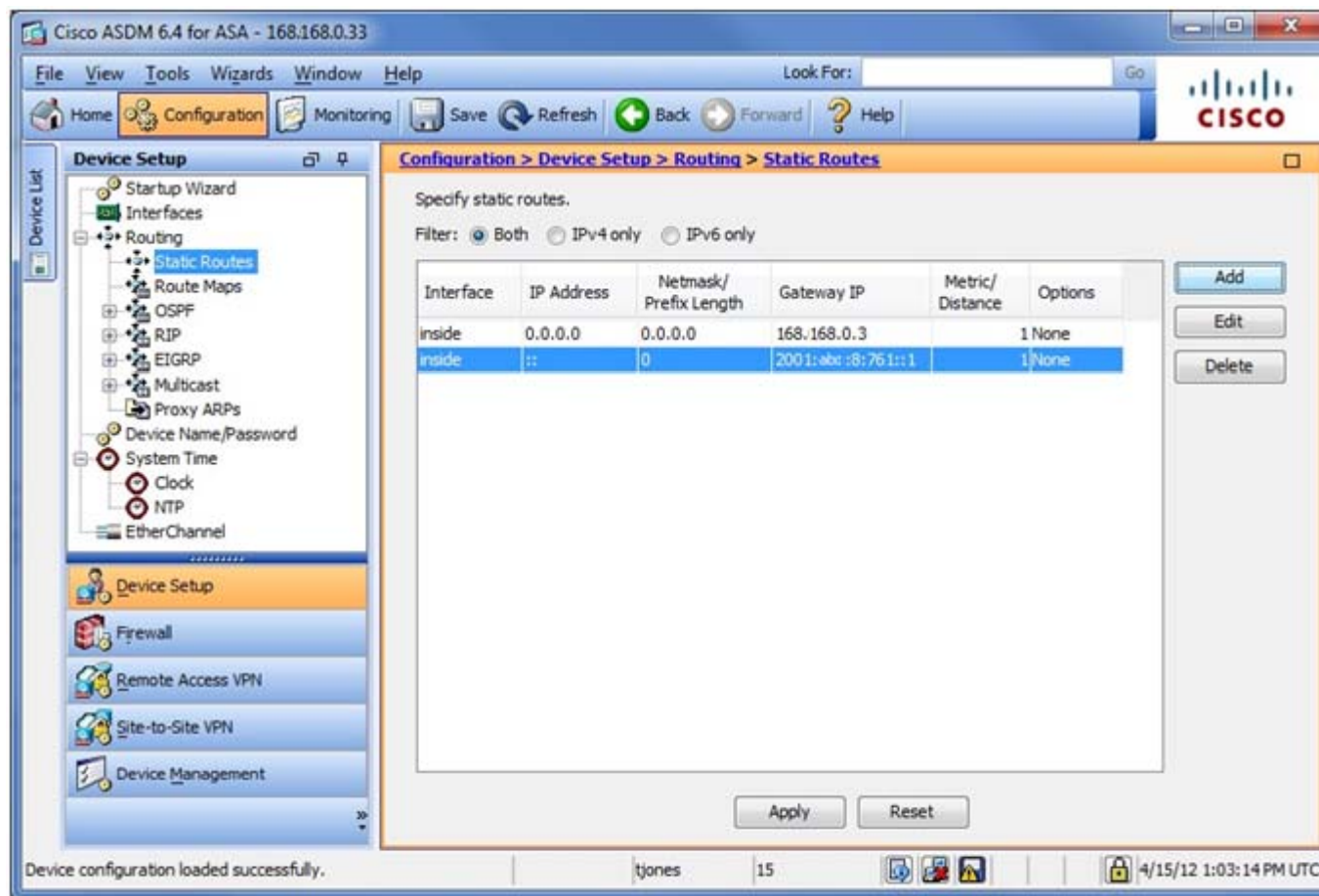
Track ID:  Track IP Address:

SLA ID:  Target Interface:

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

# Cisco ASA – Routing – Add Default

- Add the IPv6 default route.



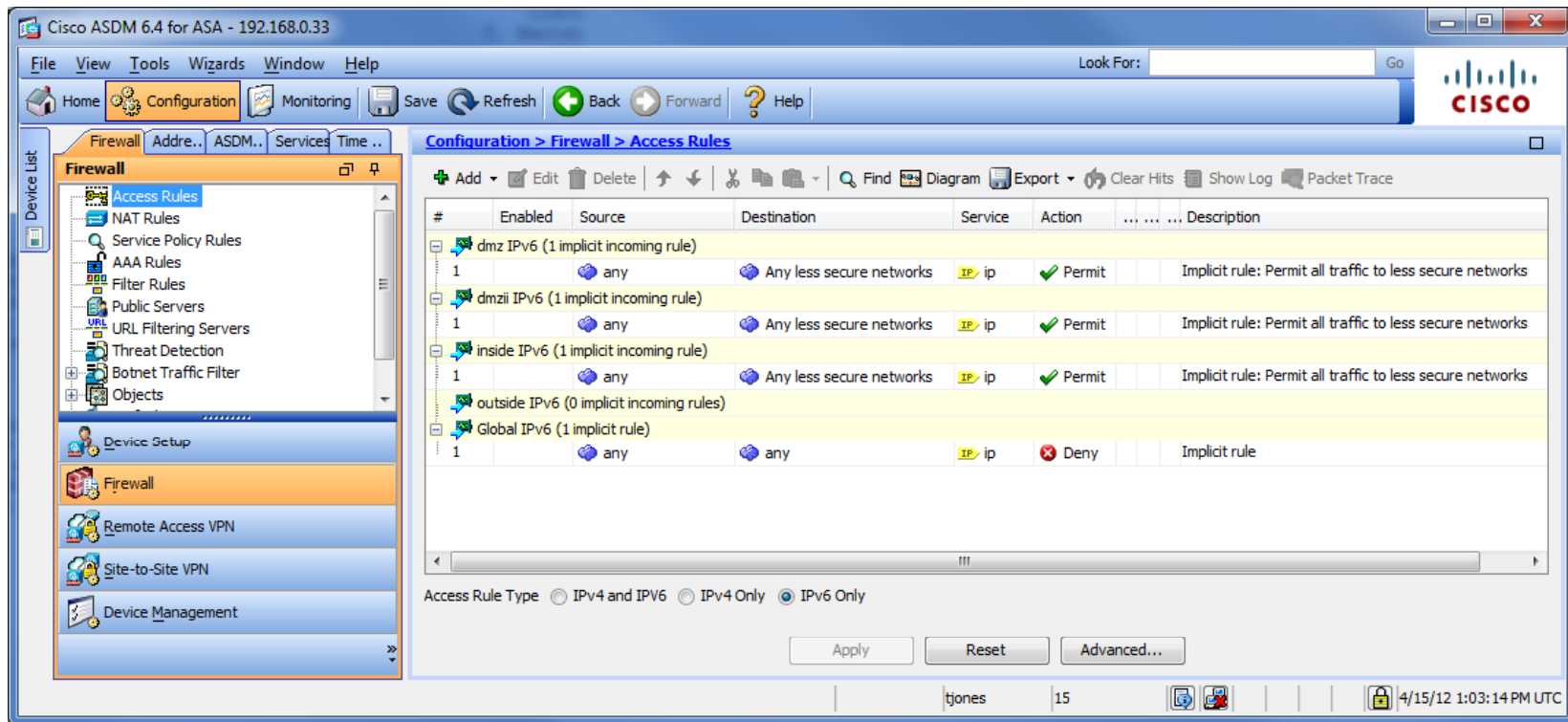
# Cisco ASA – Firewall – Access Rules



- Allow ICMP6 type/codes as provided in earlier slides.

# Cisco ASA – Firewall – Access Rules

- Text



The screenshot displays the Cisco ASDM 6.4 for ASA interface. The main window is titled "Configuration > Firewall > Access Rules". The left sidebar shows the "Firewall" configuration tree with "Access Rules" selected. The main pane shows a table of access rules with the following columns: #, Enabled, Source, Destination, Service, Action, and Description.

#	Enabled	Source	Destination	Service	Action	Description
dmz IPv6 (1 implicit incoming rule)						
1		any	Any less secure networks	IP> ip	Permit	Implicit rule: Permit all traffic to less secure networks
dmzII IPv6 (1 implicit incoming rule)						
1		any	Any less secure networks	IP> ip	Permit	Implicit rule: Permit all traffic to less secure networks
inside IPv6 (1 implicit incoming rule)						
1		any	Any less secure networks	IP> ip	Permit	Implicit rule: Permit all traffic to less secure networks
outside IPv6 (0 implicit incoming rules)						
Global IPv6 (1 implicit rule)						
1		any	any	IP> ip	Deny	Implicit rule

At the bottom of the configuration pane, the "Access Rule Type" is set to "IPv6 Only". The status bar at the bottom right shows the user "tjones" and the time "4/15/12 1:03:14 PM UTC".

# Cisco ASA - CLI

- Shown are the IPv6 commands in the configuration along with some interface, neighbor and route commands.

```
Ciscoasa# show conf
...
interface GigabitEthernet0
 shutdown
 nameif outside
 security-level 0
 ip address 168.168.230.1 255.255.255.0
 ipv6 address 2001:abc:e125:1300::1/64
 ipv6 enable
!
interface GigabitEthernet1
 nameif inside
 security-level 100
 ip address 168.168.0.33 255.255.255.0
 ipv6 address 2001:abc:80:761::33/64
 ipv6 enable
 ipv6 nd suppress-ra
!
ipv6 route inside ::/0 2001:abc:80:761::1
...
```

```
ciscoasa# sh ipv6 interface inside
inside is up, line protocol is up
 IPv6 is enabled, link-local address is fe80::2aa:ff:fed3:3b01
 Global unicast address(es):
   2001:abc:80:0761::33, subnet is 2001:4700:8:761::/64
   2001:abc:80:0761:2aa:ff:fed3:3b01, subnet is 2001:abc:80:0761::/64
 [AUTOCONFIG]
   valid lifetime 2591937 preferred lifetime 604737
 Joined group address(es):
   ff02::1
   ff02::2
   ff02::1:ff00:33
   ff02::1:ffd3:3b01
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds
 Hosts use stateless autoconfig for addresses.
```

```
ciscoasa# sh ipv6 neighbor
IPv6 Address                               Age Link-layer Addr State Interface
fe80::4024:f4b1:d4f4:63e1                 72 0090.2785.2dd8 STALE inside
fe80::208:c7ff:fef3:178f                  227 0008.c7f3.178f STALE inside
fe80::7075:69a0:27ed:fc8b                 30 001f.c609.fb4b STALE inside
fe80::e77:1aff:feb4:f787                  195 0c77.1ab4.f787 STALE inside
fe80::1938:3e40:21a4:5910                 49 000c.290a.285d STALE inside
fe80::c456:8215:63e7:a41                 72 0090.2785.2dd7 STALE inside
2001:abc:80:761:34a4:f840:e064:251f       30 001f.c609.fb4b STALE inside
fe80::9da7:3498:db03:ec0e                 72 001f.c60a.06a1 STALE inside
fe80::7021:7002:1c46:6324                 395 000c.297a.68cf STALE inside
fe80::219:e2ff:feal:3c0b                 477 0019.e2a1.3c0b STALE inside
fe80::14c0:1e85:24c3:7bc9                146 000c.2900.99be STALE inside
```

```
ciscoasa# sh ipv6 route

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
L   2001:abc:80:761::33/128 [0/0]
    via ::, inside
C   2001:abc:80:761::/64 [0/0]
    via ::, inside
L   fe80::/10 [0/0]
    via ::, outside
    via ::, inside
L   ff00::/8 [0/0]
    via ::, outside
    via ::, inside
S   ::/0 [1/0]
    via 2001:abc:80:761::1, inside
```