



IPv6 in the Weeds: How to Enable IPv6 on Your Public Facing Servers & Other Devices

**DOD
HPC**
MODERNIZATION PROGRAM

**Damien Corona, Ian Hingos, Terry Jones & Mike Rawls
June 22, 2012**

Abstract



IPv6 in the Weeds: How to enable IPv6 on your Public Facing Servers

Presenters: Damien Corona, Ian Hingos, Terry Jones, & Mike Rawls

DREN Operations

This tutorial will provide instructions and specific examples for enabling IPv6 on computer systems and networking devices. Examples of IPv6 addressing plans will also be discussed. Platform specific IPv6 configurations discussed during this tutorial will be:

-Windows XP, Windows 2003, Windows 7, and Windows 2008

-Linux (Red Hat)

-Apache and Windows IIS web servers

-BIND DNS

-Juniper Routers

-Cisco Router

-Netscreen firewall

-Cisco ASA firewall

-Brocade Switches

-Example IPv6 Address Plans

This will be a 90 minute tutorial with a 30 minute open forum/question and answer session where veteran IPv6 users share their experiences and lessons learned.

Note: A CD that contains all examples presented during the tutorial will be provided to all attendees.

IPv6 References

- **HPCMO IPv6 Knowledge Base**

- <http://www.hpc.mil/cms2/index.php/ipv6-knowledge-base-general-info>
- A wealth of information on IPv6 in a centralized repository
- IPv6 Policy and Guidance
- Tips on Address Plans
- IPv6 Websites
- Helpful IPv6 Tools and Applications
- And much, much more!

IPv6 Knowledge Base

- IPv6 KB: General Information
- IPv6 KB: Deployment
- IPv6 KB: IP Transport
- IPv6 KB: Infrastructure
- IPv6 KB: Network Management
- IPv6 KB: Security
- IPv6 KB: Applications
- IPv6 KB: Testing

- **Ron Broersma IPv6 Presentations/Tutorials**

- <http://www.hpc.mil/IPV6/wp-content/networkers-IPv6-Tutorial-2010.pdf>
- <http://www.hpc.mil/cms2/index.php/ipv6-knowledge-base-network-management/182-v6-ipv6-address-plans>
- <http://www.hpc.mil/IPV6/wp-content/DREN Addressing Plans Ron Broersma 11172011-extract.pdf>

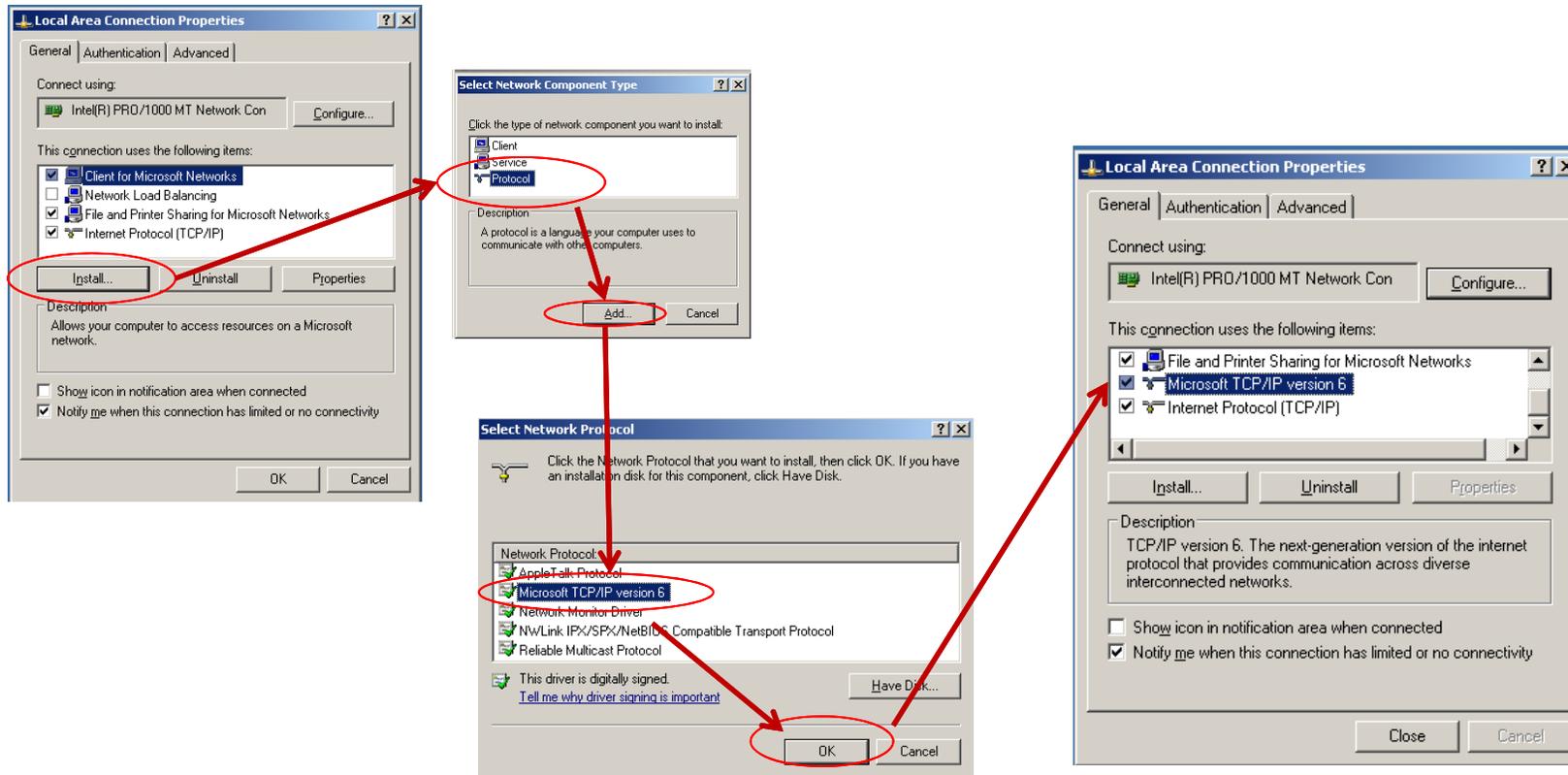
Microsoft Windows Version Support

- **Windows 7 (all versions)**
- **Windows 2008 (all versions)**
- **Windows 2003 sp1**
- **Windows XP sp2 (or higher)**
- **DNS, DHCPv6, applications (see the HPCMO IPv6 knowledge base)**
 - <http://www.hpc.mil/cms2/index.php/ipv6-knowledge-base-infrastructure/216-enabling-ipv6-in-microsoft-environment>

Setup for 2003 and XP

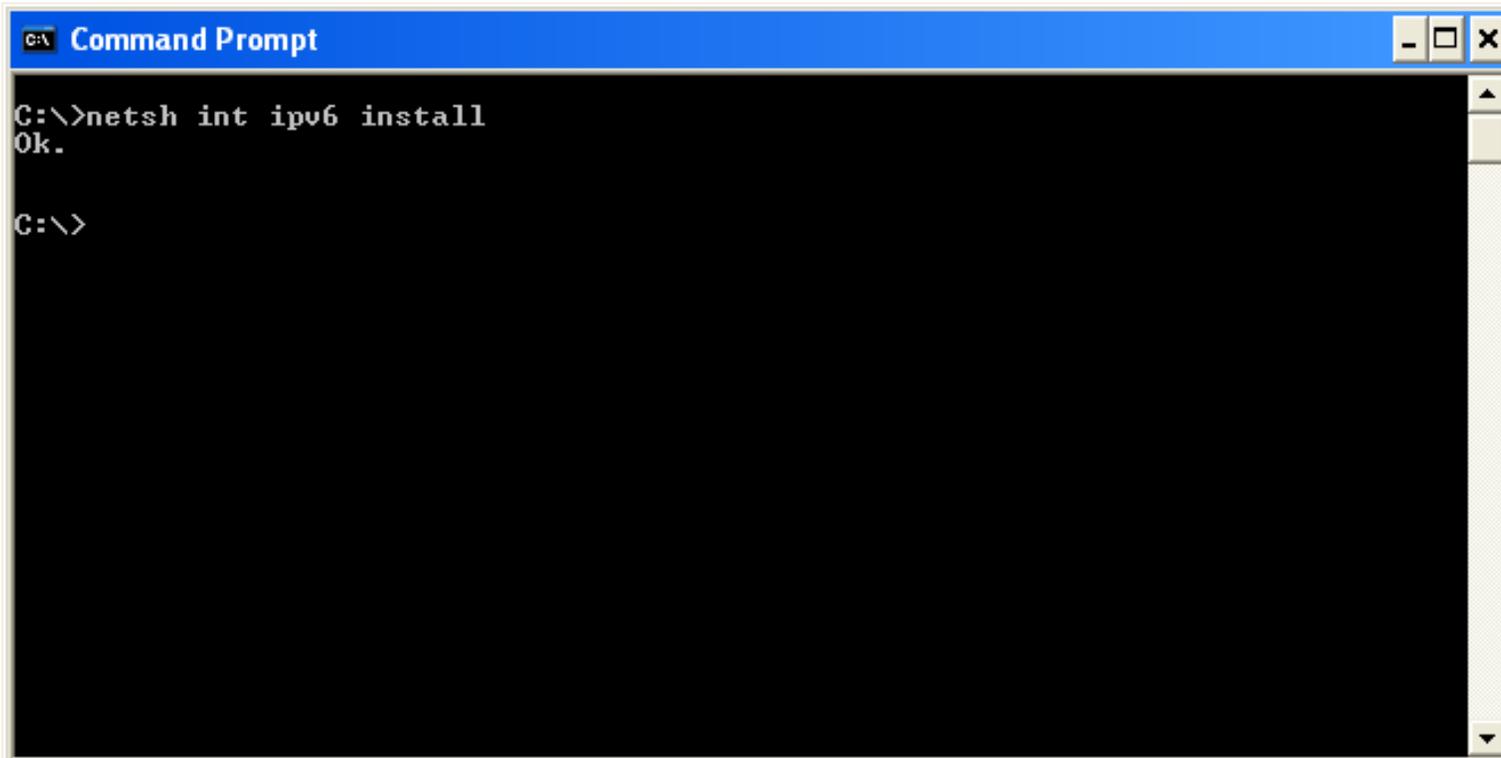
- **Can install using GUI**
- **All configuration done using 'netsh'**

2003 and XP GUI Install



2003 and XP command-line Install

- `\>netsh int ipv6 install`



```
C:\>netsh int ipv6 install
Ok.

C:\>
```

Install for 2008 and 7

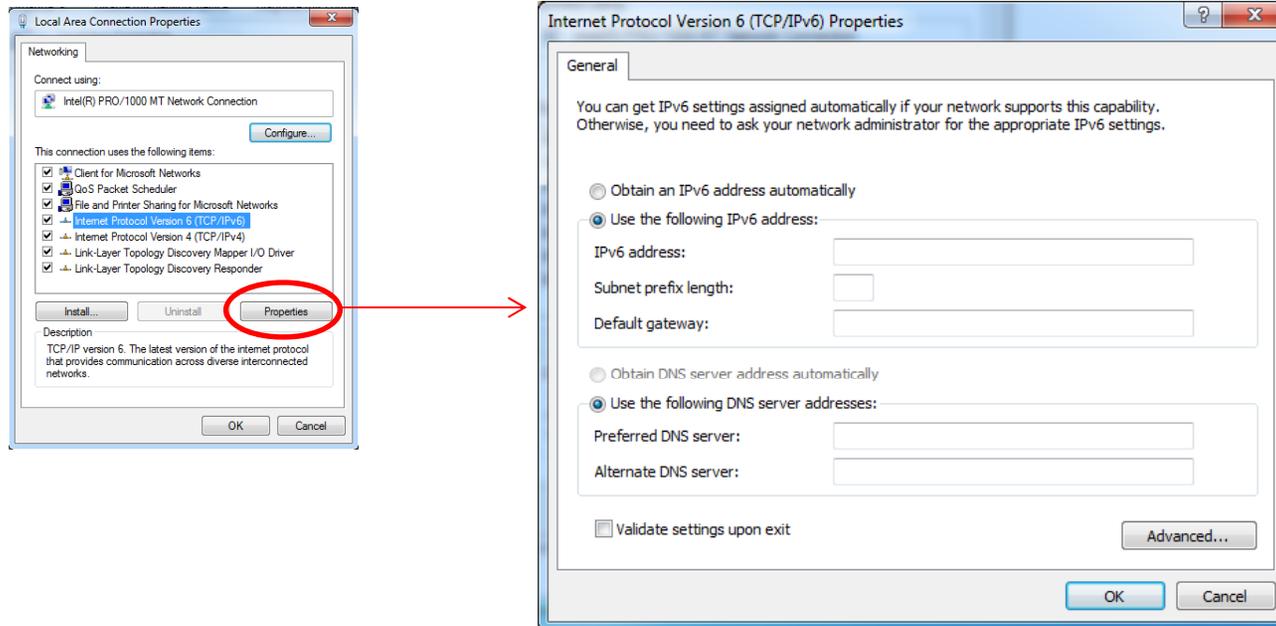
- **Did you install windows?**

It's already ON!

And it has probably set itself up

2008 and 7 GUI Configuration

Familiar dialogue....



- Can use IPv6 Short Hand
- Gateway uses *address/prefix* notation

Configuration with 'netsh'

- **Netsh IS your friend!**
 - Can be used in scripting
 - Works in all IPv6 support version of Windows. Including CORE!
 - Scripts CAN cross versions

- **Most important thing to remember.....**

netsh relies on the ***NAME*** of the interface

ie: "Local Area Connection"

Basic Netsh Configuration

- Use “/?” after commands for help
- Setting an IPv6 Address
 - Open a command prompt and type **netsh** to go into the network shell
 - Type **interface ipv6** and press ENTER to open the ipv6 context
 - At the prompt enter: **add address interface=*string* address=*ipv6address***
 - **Where:**
 - *String* = The name of the network interface (use “” if the name contains spaces, ie “Local Area Connection”)
 - *ipv6address* = the IPv6 address you want to assign to the host
- Setting the Default IPv6 Gateway
 - Open a command prompt and type **netsh** to go into the network shell
 - Type **interface ipv6** and press ENTER to open the ipv6 context
 - At the prompt enter: **add route prefix=::string nexthop=*ipv6gateway***
 - **Where:**
 - *String* = The name of the network interface (use “” if the name contains spaces, ie “Local Area Connection”)
 - *ipv6gateway* = the IPv6 address of the gateway

Quirks

- **XP and 2003 run two separate IP stacks**
- **Win7 and 2008 run a single integrated IP stack**
- **Win7 autoconfig randomization**
- **IPv6 disable features**

Quirks: Autoconfig Randomization

- **Autoconfig automatically sets an IPv6 address using the MAC address of the network card.**
 - This is considered a privacy issue since the MAC address never changes.
 - Randomization was introduced to fix this in Windows 7 and 2008
 - When autoconfig addresses are registered in DNS, that address will act as the primary address over a statically set one when both are registered
- **Problem: IPv6 address will change with EVERY reboot**
- **Disable Router Discovery – With this enabled, it registers the autoconfig address into DNS**
 - Disable Router Discovery by running the following command
 - `netsh interface ipv6 set interface "Local Area Connection" routerdiscovery=disabled`
- **Disable autoconfig on DNS Servers, it also registers the autoconfig address into DNS**
 - Disable autoconfig on the DNS Servers themselves by running the following command
 - DNS registered `2001:abc:3500:dc4b:e0a3:2ff5:d807` (<- autoconfig address)
- **FIX: Disable randomization**
 - Disable randomization by running the following commands
 - `netsh interface ipv6 set privacy state=disabled store=active`
 - `netsh interface ipv6 set privacy state=disabled store=persistent`
 - `netsh interface ipv6 set global randomizeidentifiers=disabled store=active`
 - `netsh interface ipv6 set global randomizeidentifiers=disabled store=persistent`

Quirks: IPv6 disable features

- **Group Policy**

- Administrative Templates>Network>TCPIP Settings>IPv6 Transition Technologies

- **Registry**

- **HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters**
 - **DisabledComponents (D-Word 32bit)**
 - **0 = enable all IPv6 Components**
 - **0x20 = prefer IPv4 to IPv6**
 - **0x01 = disable IPv6 on all tunnel interfaces (ISATAP, 6to4, Teredo)**
 - **0x11 = disable IPv6 on all interfaces except loopback**

For more information see: <http://support.microsoft.com/kb/929852>

IPV6 Enablement on Red Hat Linux

- **To enable IPv6 on Redhat Linux Enterprise 6, first determine the active interface on the machine**

- Log in to the Linux console as root
- At the command prompt type ifconfig

– EXAMPLE:

```
[root@linux networking]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:BE:56:73
          inet addr:168.168.0.22  Bcast: 168.168.0.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:213643037 errors:0 dropped:0 overruns:0 frame:0
          TX packets:212985247 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22911766717 (21.3 GiB)  TX bytes:64966576806 (60.5 GiB)
          Interrupt:18 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:188079 errors:0 dropped:0 overruns:0 frame:0
          TX packets:188079 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:18103922 (17.2 MiB)  TX bytes:18103922 (17.2 MiB)

[root@ns networking]#
```

- **In this case the active interface is “eth0”. Ignore the “lo” interface**

IPV6 Enablement on Red Hat Linux

- **Change directory in to the /etc/sysconfig/networking/devices folder**
 - EXAMPLE:

```
[root@linux ~]# cd /etc/sysconfig/networking/devices
[root@linux devices]#
```
- **Edit the file that ends with the interface name. In this instance the file is “**ifcfg-eth0**”**
- **Add or edit the following lines to the “**ifcfg-eth0**” file.**

```
IPV6INIT=yes
IPV6ADDR=YOUR-ASSIGNED-IPV6-IP-ADDRESS
IPV6_DEFAULTGW=YOUR-ASSIGNED-IPV6_GATEWAY-ADDRESS
```
- **Save the file**

IPV6 Enablement on Red Hat Linux

- **Disable the NetworkManager service with the command listed below. Be sure to get the capitalization correct**
`chkconfig NetworkManager off`
- **Restart the Linux server to enable IPv6 networking.**
- **IPV6 should now be enabled**
- **Use the “`ping6`” command to ping the IPv6 IP address assigned to the Linux server as well as the assigned IPv6 gateway address**
- **Typing the command “`ifconfig`” at the command prompt should now show the IPv6 address configured and assigned to the “`eth0`” interface**
- **The command “`route -n -A inet6`” can be used to display and verify the IPv6 default gateway**

IPV6 on Linux hosted Apache2

- Apache is easily configured to listen and respond on IPV6. The following directives are inserted into the httpd.conf file
- The following directive will allow Apache to listen on all IPv4 and IPv6 interfaces configured on the server
 - Listen *
- The following directive tells Apache to listen to a single IPv4 address only
 - Listen 168.168.0.100
- The following directive tells Apache to listen on the specified IPv6 address only. **IPv6 addresses must be enclosed in square brackets.** The “:80” specifies the specific TCP port to listen on
 - Listen [2001:abc::24]:80
- The following directive tells Apache to listen on port 443 on both IPv4 and IPv6 addresses configured on the server
 - Listen 443

IPV6 on Linux hosted Apache2

- To configure a specific domain to listen on IPv4 and IPv6 addresses, the following entries can be added to the end of the Apache httpd.conf file
- The example configuration below configures a virtual host to listen for port 80 on both IPv4 and IPv6 address
 - `<virtualhost *:80>`
 - ServerName example.com
 - ServerAlias *.example.com
 - DocumentRoot /www/example.com/public_html
 - ErrorLog /www/example.com/logs/error_log
 - Customlog /www/example.com/logs/combined_log combined
 - `</virtualhost>`

IPV6 on Linux hosted Apache2

- **The example configuration below configures a virtual host to listen on a single IPv6 address only on port 80**
 - `<virtualhost [2001:abc::a00:20ff:fea7:ccea]:80>`
 - `ServerName example.com`
 - `ServerAlias *.example.com`
 - `DocumentRoot /www/example.com/public_html`
 - `ErrorLog /www/example.com/logs/error_log`
 - `Customlog /www/example.com/logs/combined_log combined`
 - `</virtualhost>`

IPV6 on Linux hosted Apache2

- **The example configuration below configures a virtual host to listen on specified IPv4 and IPv6 addresses on port 80**
 - ```
<virtualhost 168.168.1.100:80, [2001:abc::a00:20ff:fea7:ccea]:80>
 ServerName example.com
 ServerAlias *.example.com
 DocumentRoot /www/example.com/public_html
 ErrorLog /www/example.com/logs/error_log
 Customlog /www/example.com/logs/combined_log combined
</virtualhost>
```
- **Apache will need to be restarted before any changes to the httpd.conf file will take effect**

# Internet Information Services (IIS)

- IPv6 is supported by default in versions:
  - 7.5
  - 7
  - 6
  - 5
- No special configurations needed
- By default, IIS is configured to listen on **ALL** addresses
- Remember to install the updated file transfer protocol (FTP) publishing service released after IIS7



# BIND IPV6 on Linux

- **The IPv6 “AAAA” or quad A entry specifies an IPv6 DNS entry in the master zone file for any hosted domain**
- **Quad A DNS entries can exist in the master zone file along side typical IPv4 entries without causing any issues**
- **IPv6 shorthand entries are allowed in the forward DNS zone file**
  - EXAMPLE:
    - workstation126.example.com. IN AAAA 2001:abc:2480:1000::126
- **IPv4 and IPv6 entries can exist in the same forward zone file at the same time**
  - EXAMPLE:
    - workstation126.example.com. IN A 168.168.0.126
    - workstation126.example.com. IN AAAA 2001:abc::126

# BIND IPV6 on Linux

- To configure Bind to answer reverse IPv6 PTR queries, a separate IPv6 PTR zone file must be created along with a separate IPv6 PTR entry in the Bind named.conf file. The full IPv6 address must be entered in the reverse PTR zone file
- IPv6 shorthand is not allowed in the reverse PTR record
- The IPv6 address must be entered in to the PTR record in reverse
  - 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.b.a.0.1.0.0.2.ip6.arpa. IN PTR workstation1.example.com.

# BIND IPV6 on Linux

- To configure bind to answer IPv6 reverse DNS queries for an IPv6 network of 2001:abcd, an entry like the one below can be used in named.conf
  - // IPv6 stuff  
zone "d.c.b.a.1.0.0.2.ip6.arpa" IN {  
type master;  
file "2.0.0.1.0.a.b.c.d.db";  
};
- Note the IPv6 address is printed backwards in the zone line

# BIND IPV6 on Linux

- The Linux bash shell script below can be used to create the reverse PTR zone entries based on quad AAAA DNS records already present in the forward DNS zone file
- This script will save time and reduce the chance of typographical errors when creating the reverse PTR entries for an IPv6 zone file

```
Begin Linux bash shell script
#!/bin/bash

IFS="
"

if [-z $1]
then
 echo ""
 echo "$0 ZONE-FILE-NAME"
 echo ""
 exit
fi

FILENAME="$1"

Create first part of reverse config file
DATE=`date +%Y%m%d`

for X in `egrep AAAA $FILENAME | egrep -v ";"`
do
 DNSNAME=`echo $X | awk -F" " '{print$1}'`
 IPV6ADDRESS=`echo $X | awk -F" " '{print$4}'`
 REVERSE=`host $IPV6ADDRESS | sed "s/Host //g" | awk -F" " '{print$1}'`

 echo "$REVERSE. IN PTR $DNSNAME"
done

End Linux bash shell script
□
```



# BIND IPV6 on Linux

- Bind will need to be restarted before any changes will take effect
- Check the log file `/var/log/messages` for any errors from “named” or “bind” after restarting







# Networking Devices

- **Juniper Routers**
- **Cisco Routers**
- **Juniper Netscreen Security Devices**
- **Cisco ASA Security Appliances**
- **Brocade Switches**

# Juniper Routers



J-Series



M-Series

# Juniper – M & J Series Routers

- **Configure IPv6 on Interfaces**

```
interfaces {
 fe-0/1/0 {
 unit 0 {
 family inet6 {
 address 2001:abc:xxxx:xxxx::1/64;
 }
 }
 }
}
```

- **Configure IPv6 Default Static Route**

```
routing-options
 rib inet6.0 {
 static {
 route 0::0/0 next-hop 2001:abc:xxxx:xxxx::1;
 }
 }
}
```

# Juniper – M & J Series Routers

- **IPv6 Static Routing (if needed)**

```
routing-options
 rib inet6.0 {
 static {
 route 2001:abc::2480/48 next-hop 2001:X:X:X::1;
 }
 }
}
```

- **IPv6 Router Advertisement (if needed)**

```
user@Router1# show protocols
router-advertisement {
 interface fe-1/3/1.101 {
 prefix 2001:abc:2480:36aa::/64;
 }
}
```

# JUNOS CLI - Set Commands

- **Set commands below are the IPv6 Router Advertisement (if needed)**

## Interfaces

```
set interfaces fe-0/1/0 unit 0 family inet6 address 2001:abc:X:X::1/64
```

## IPv6 Default Route

```
set routing-options rib inet6.0 static route 0::0/0 next-hop 2001:abc:X:X::1
```

## IPv6 Router Advertisement

```
set protocols router-advertisement interface fe-1/3/1.101 prefix 2001:abc:X:X::/64
```

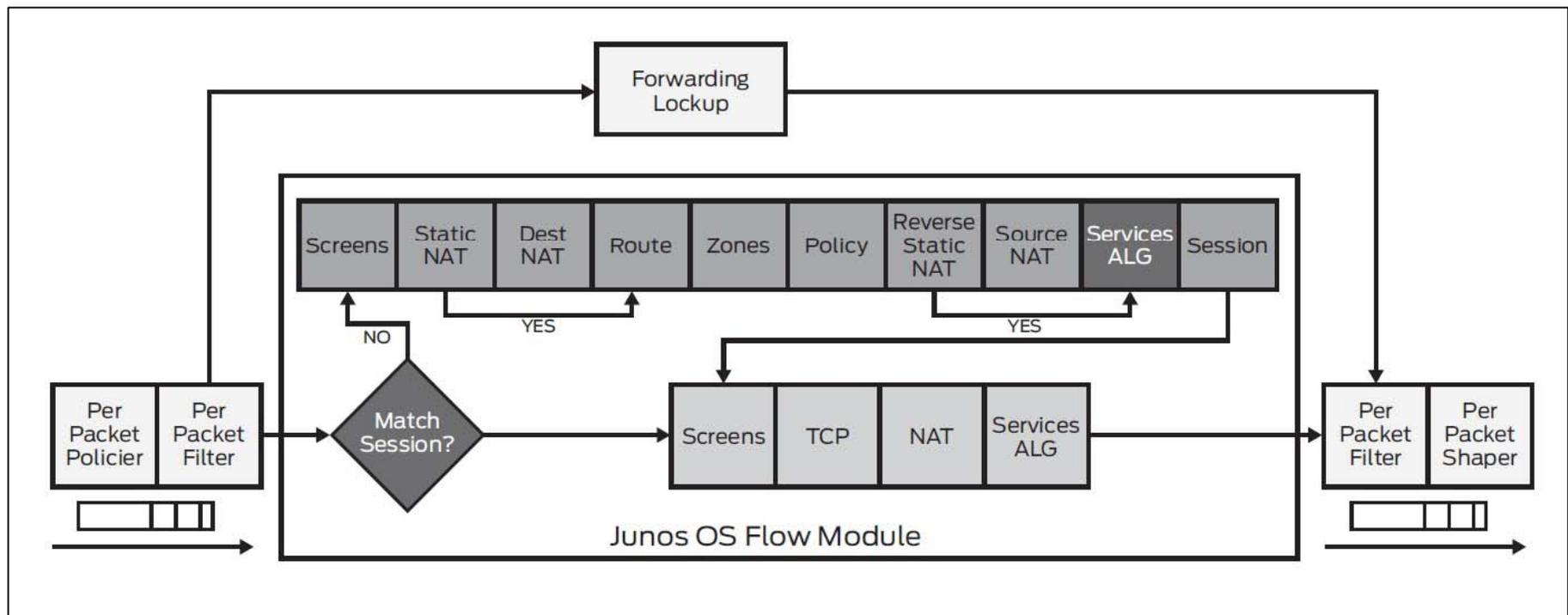
## IPv6 e-BGP

```
set protocols bgp group v6-To-Customer-Site1 type external
set protocols bgp group v6-To-Customer-Site1 import v6_import_To_Customer_Site1
set protocols bgp group v6-To-Customer-Site1 family inet6 any
set protocols bgp group v6-To-Customer-Site1 export v6_export_To_Customer_Site1
set protocols bgp group v6-To-Customer-Site1 peer-as 65502
set protocols bgp group v6-To-Customer-Site1 local-as 65500
set protocols bgp group v6-To-Customer-Site1 neighbor 2001:abc:X:X::X local-address 2001:abc:X:X::X
set protocols bgp group v6-rr-clients type internal
```

# Juniper – J-Series

- **Flow chart for Packet Versus Flow Forwarding**

- (See reference - Branch SRX Series and J Series Selective Packet Services)



To Flow to Not to Flow...that is the question!

# Juniper Routers – J-series

- **With post-9.6 JUNOS code, on J-series, IPv6 traffic is set to flow-mode processing by default.**
- **Options are...**
  - Convert all IPv6 traffic to packet forwarding mode
  - Implement policies to permit IPv6 traffic and services
- **J-Web is limited on IPv6 configurations...**
  - Can't configure IPv6 address on interface
  - Documentation not great for J-Web

# Juniper J-Series – Bypass Flow Mode



- **To bypass Flow Mode, enter the following...**

```
user@Router6# show security
forwarding-options {
 family {
 inet6 {
 mode packet-based;
 }
 }
}
```

Set command -

```
set security forwarding-options family inet6 mode packet-based
```

- **All IPv6 traffic will now bypass the new security hierarchical settings.**

# Juniper J-Series – Security Zones

- If using flow mode, you will need to configure security zones

```
zones {
 security-zone TRUST {
 interfaces {
 ge-0/0/0.0 {
 host-inbound-traffic {
 system-services {
 all;
 }
 protocols {
 all;
 }
 }
 }
 }
 }
}
```

```
zones {
 security-zone UNTRUST {
 interfaces {
 ge-0/0/1.0 {
 host-inbound-traffic {
 system-services {
 all;
 }
 protocols {
 all;
 }
 }
 }
 }
 }
}
```

# Juniper J-Series – Security Policies

- ... and policies.

```
policies {
 from-zone UNTRUST to-zone TRUST {
 policy allow-inbound {
 match {
 source-address any;
 destination-address any;
 application any;
 }
 then {
 permit;
 log {
 session-init;
 session-close;
 }
 }
 }
 }
}
```

```
policies {
 from-zone TRUST to-zone UNTRUST {
 policy allow-outbound {
 match {
 source-address any;
 destination-address any;
 application any;
 }
 then {
 permit;
 log {
 session-init;
 session-close;
 }
 }
 }
 }
}
```

# Cisco Routers



# Cisco Routers

- **Configure Interfaces**

```
interface GigabitEthernet0/0
ip address 168.168.0.2 255.255.255.0
duplex full
speed 1000
media-type gbic
negotiation auto
ipv6 address 2001:abc:X:X::2/64
ipv6 enable
```

- **Notes**

- When ipv6 unicast-routing is enabled, router advertisements are automatically enabled on Ethernet interfaces. To disable RA messages, use the 'ipv6 nd ra suppress' command.

# Cisco Routers

- **Configure IPv6 Default Route**

```
ipv6 route ::/0 2001:abc:X:X::1
```

- **Configure Static Route**

```
ipv6 route 2001:abc:X:X::/64 2001:abc:X:X::1
```

- **DNS**

```
ip name-server 2001:abc:A0:F000::244
ip name-server 2001:abc:B0:F000::244
```

# Cisco Routers

- **Verify Interfaces**

```
R1#sh ipv6 interface Gi0/0
GigabitEthernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::C800:14FF:FEE4:8
No Virtual link-local address(es):
Global unicast address(es):
 2001:abc:2480:1000::126, subnet is 2001:abc:2480:1000::/64
Joined group address(es):
 FF02::1
 FF02::2
 FF02::1:FF00:126
 FF02::1:FFE4:8
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

# Cisco Routers

- **Verify Static Routing**

```
R1#sh ipv6 static detail
IPv6 Static routes Table - default
Codes: * - installed in RIB, u/m - Unicast/Multicast only
 U - Per-user Static route, N - ND Static route
 P - DHCP-PD Static route
 R - Rhi Static route
* 2001:abc:2480:3000::/64 via 2001:abc:2480:1000::1, distance 1
 Resolves to 1 paths (max depth 1)
 via GigabitEthernet0/0
* ::/0 via 2001:abc:2480:1000::1, distance 1
 Resolves to 1 paths (max depth 1)
 via GigabitEthernet0/0
```

# Cisco Routers

- **Verify IPv6 Neighbors**

```
R1#sh ipv6 neighbors
IPv6 Address Age Link-layer Addr State Interface
FE80::7069:5DAF:A5F5:FDB3 124 000c.297d.bbe3 STALE Gi0/0
2001:abc:2480:1000::1 170 0010.dbc9.a695 STALE Gi0/0
2001:abc:2480:1000:6021:A03E:3762:8078 25 d067.e539.1ae5 STALE Gi0/0
2001:abc:2480:1000:E88A:8590:19C0:3CD3 10 b8ac.6fc6.16e6 STALE Gi0/0
FE80::FCD3:3EAA:2E93:61 2 d067.e539.1b3e STALE Gi0/0
2001:abc:2480:1000:6DE3:3F29:209A:CA4B 0 f04d.a26a.08cf STALE Gi0/0
2001:abc:2480:1000:55FC:66B7:AEE7:49B0 6 d067.e539.1b3e STALE Gi0/0
2001:abc:2480:1000::23 18 d067.e539.140d STALE Gi0/0
FE80::C5B:A874:4C18:EF9F 0 101f.74ce.2a53 REACH Gi0/0
FE80::D267:E5FF:FE39:140D 2 d067.e539.140d STALE Gi0/0
2001:abc:2480:1000:EDAF:8655:6764:47AF 2 0026.b9ed.e6e2 STALE Gi0/0
FE80::210:DBFF:FEC9:A695 194 0010.dbc9.a695 STALE Gi0/0
FE80::41CE:5ABD:EDDD:7216 3 0026.b9ec.e541 STALE Gi0/0
FE80::8C9C:AEA8:328E:E37A 0 0026.b9ec.c0df REACH Gi0/0
2001:abc:2480:1000::62 15 0050.56b2.2e74 STALE Gi0/0
FE80::E88A:8590:19C0:3CD3 9 b8ac.6fc6.16e6 STALE Gi0/0
2001:abc:2480:1000:5D9A:9B99:C584:5008 6 0026.b9ec.e615 STALE Gi0/0
FE80::C525:65E8:98F4:BC20 23 d067.e539.1ae5 STALE Gi0/0
2001:abc:2480:1000:80CB:CE47:8FFC:C4EB 4 000c.29b9.803a STALE Gi0/0
2001:abc:2480:1000:257B:29AE:C513:775C 7 0026.b9ec.e541 STALE Gi0/0
2001:abc:2480:1000:C5B:A874:4C18:EF9F 32 101f.74ce.2a53 STALE Gi0/0
2001:abc:2480:1000:9104:A739:627F:D1F7 2 0026.b9ec.c0df STALE Gi0/0
2001:abc:2480:1000:89A3:5936:efd7:DAFE 4 0026.b9ed.e32f STALE Gi0/0
FE80::3138:66CC:EC8A:9631 5 0026.b9ec.e615 STALE Gi0/0
FE80::87F:33E8:94BC:CB7F 11 000c.29b9.803a STALE Gi0/0
FE80::EC96:55E7:E603:A910 2 0026.b9ed.e6e2 STALE Gi0/0
2001:abc:2480:1000:F856:AF4B:C9B8:B14C 46 b8ac.6f79.61ca STALE Gi0/0
2001:abc:2480:1000:8D60:E9E:FDB5:86B8 34 d067.e539.1ae5 STALE Gi0/0
```

# Cisco Routers

- **Verify IPv6 Reachability**

- Ping

```
R1#ping ipv6 ipv6.google.com
Translating "ipv6.google.com"...domain server (2001:4860:A0:F000::244) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:4860:800A::63, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/138/156 ms
```

- Traceroute

```
R1#traceroute ipv6 ipv6.google.com
Type escape sequence to abort.
Tracing the route to ipv6.l.google.com (2001:4860:800A::63)

 0 10.10.10.10 [MPLS] 0 msec 0 msec 0 msec
 1 host1.abc.test.net (2001:abc:2480:1000::1) 48 msec 32 msec 32 msec
 2 2001:abc:5000:842::1 12 msec 32 msec 32 msec
 3 google-1-lo-std-703.lsanca.pacificwave.net (2001:504:B:21::147) 44 msec 100 msec 60 msec
 4 * 72 msec 68 msec
 5 2001:4860::1:0:29B3 84 msec
 2001:4860::1:0:991 60 msec
 2001:4860::1:0:29B3 72 msec
 6 2001:4860::8:0:2996 84 msec 76 msec 100 msec
 7 2001:4860::8:0:2F03 128 msec 136 msec 144 msec
 8 2001:4860::2:0:A7 120 msec 148 msec 188 msec
 9 2001:4860:0:1::10D 140 msec 132 msec
 2001:4860:0:1::10F 132 msec
10 ipv6.l.google.com (2001:4860:800A::63) 128 msec 168 msec 128 msec
```

# Cisco Routers

- **To Summarize**
  - Enable IPv6 on interface
  - Enable IPv6 unicast routing
  - Configure interface with IPv6 address
  - Enter IPv6 default route
  - Enter static IPv6 routes
  
- **Verify IPv6 Settings**
  
- **Verify IPv6 Reachability**

**NOTE:** These commands were run using Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.1(4)M3a, RELEASE SOFTWARE (fc1)

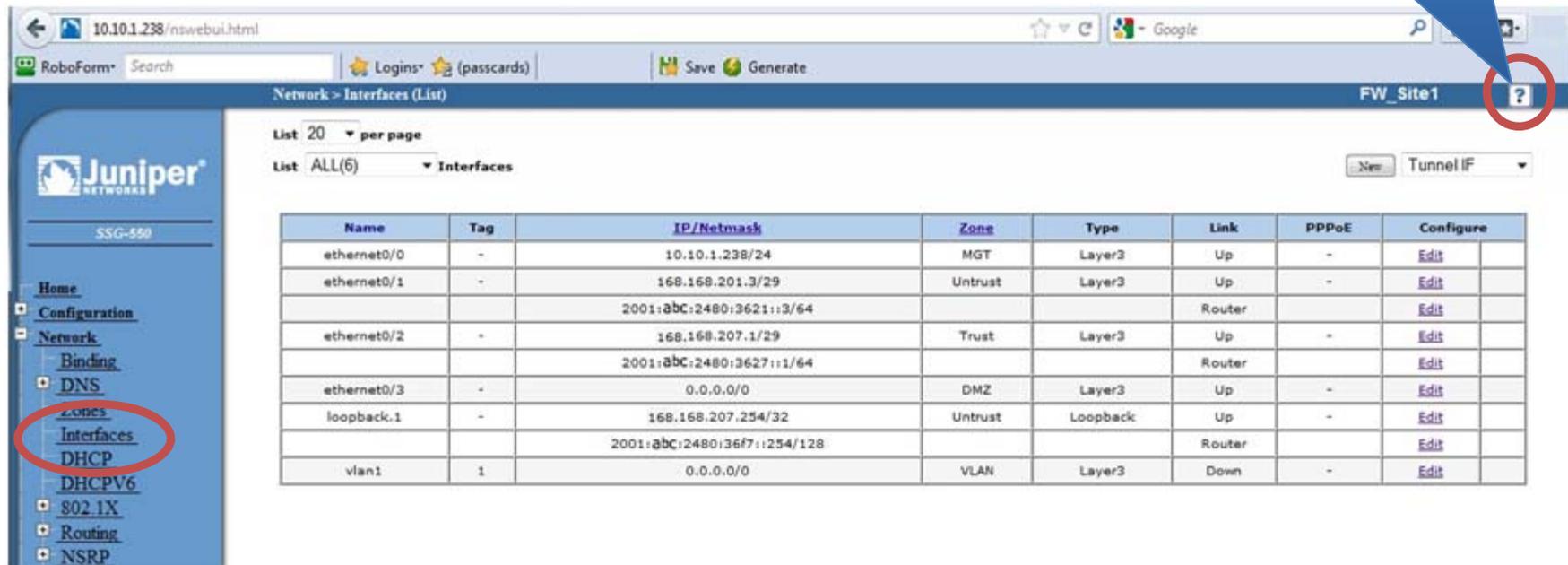
# Juniper Netscreen Security Device



# Netscreen Firewall - Interfaces

- Below is a screen shot for a Netscreen Firewall interface. All interfaces have an IPv6 address except ethernet0/0. We will step through configuring this interface.

Remember...The Help Menu is your friend!



Network > Interfaces (List) FW\_Site1

List 20 per page  
List ALL(6) Interfaces

| Name        | Tag | IP/Netmask                 | Zone    | Type     | Link | PPPoE | Configure            |
|-------------|-----|----------------------------|---------|----------|------|-------|----------------------|
| ethernet0/0 | -   | 10.10.1.238/24             | MGT     | Layer3   | Up   | -     | <a href="#">Edit</a> |
| ethernet0/1 | -   | 168.168.201.3/29           | Untrust | Layer3   | Up   | -     | <a href="#">Edit</a> |
|             |     | 2001:abC:2480:3621::3/64   |         | Router   |      |       | <a href="#">Edit</a> |
| ethernet0/2 | -   | 168.168.207.1/29           | Trust   | Layer3   | Up   | -     | <a href="#">Edit</a> |
|             |     | 2001:abC:2480:3627::1/64   |         | Router   |      |       | <a href="#">Edit</a> |
| ethernet0/3 | -   | 0.0.0.0/0                  | DMZ     | Layer3   | Up   | -     | <a href="#">Edit</a> |
| loopback.1  | -   | 168.168.207.254/32         | Untrust | Loopback | Up   | -     | <a href="#">Edit</a> |
|             |     | 2001:abC:2480:367::254/128 |         | Router   |      |       | <a href="#">Edit</a> |
| vlan1       | 1   | 0.0.0.0/0                  | VLAN    | Layer3   | Down | -     | <a href="#">Edit</a> |

# Netscreen Firewall – IPv6

- To configure, enable IPv6, determine mode and enter IPv6 address with prefix.
- Use Host Mode to accept RA messages.
- User Router Mode to send RA messages.

Interface: ethernet0/0

Properties: [Basic](#) [IPv6](#)

Interface Name ethernet0/0 0023.9c82.2100

Enable IPv6

Mode  None  Host  Router

Interface ID(64-bit HEX)

Link Local Address

Unicast Address 1 / Prefix  /

Unicast Address 2 / Prefix  /

Unicast Address 3 / Prefix  /

Path MTU(IPv6)

# Netscreen – Configure IPV6

- After configuring the IPv6 addresses and clicking apply, the Neighbor Discovery (ND) and Router Advertisement (RA) settings are now available for configuration.

Interface: ethernet0/0 [Back To Interface List](#)

Properties: [Basic](#) **IPv6**

---

Interface Name ethernet0/0 0023.9c82.2100

Enable IPv6

Mode  None  Host  Router

Interface ID(64-bit HEX)

Link Local Address fe80::223:9cff:fe82:2100

Unicast Address 1 / Prefix  /

Unicast Address 2 / Prefix  /

Unicast Address 3 / Prefix  /

Path MTU(IPv6)

---

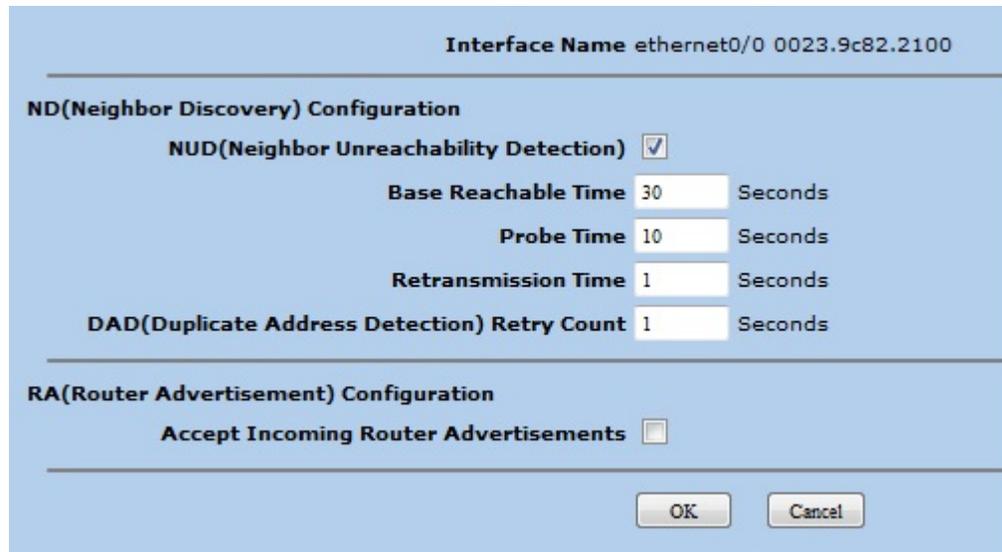
Node Configuration

[ND/RA Settings](#)  
[Prefix list](#)

---

# Netscreen – ND/RA Settings (Host)

- If using Host Mode, determine if you would like to accept incoming router advertisements.
- Accept Incoming Router Advertisements learns of the existence and identity of IPv6 routers by accepting Router Advertisement (RA) messages.



Interface Name ethernet0/0 0023.9c82.2100

---

ND(Neighbor Discovery) Configuration

NUD(Neighbor Unreachability Detection)

Base Reachable Time 30 Seconds

Probe Time 10 Seconds

Retransmission Time 1 Seconds

DAD(Duplicate Address Detection) Retry Count 1 Seconds

---

RA(Router Advertisement) Configuration

Accept Incoming Router Advertisements

OK Cancel

# Netscreen – ND/RA Settings (Router)

- Use RA Transmission to learn of the existence and identity of other IPv6 routers.
- Link MTU advertises the link-MTU in router advertisements.
- Link Layer Address enables the Link Layer Address flag, which includes the link-layer (MAC) address of the router in outgoing RA messages.

Interface Name ethernet0/0 0023.9c82.2100

---

ND(Neighbor Discovery) Configuration

NUD(Neighbor Unreachability Detection)

Base Reachable Time 30 Seconds

Probe Time 10 Seconds

Retransmission Time 1 Seconds

DAD(Duplicate Address Detection) Retry Count 1 Seconds

---

RA(Router Advertisement) Configuration

Allow RA Transmission

Link MTU

Link Layer Address

Managed Configuration Flag

Other Parameters Configuration Flag

Reachable Time

Retransmission Time

Current Hop Limit 64

Maximum Advertisement Interval 600 Seconds

Minimum Advertisement Interval 200 Seconds

Default Router Lifetime 1800 Seconds

Advertised Router Preference  High  Medium  Low

OK Cancel

# Netscreen –IPv6 Route Table

- Text

| IPv6 Routing Table -- trust-vr |                             |         |             |          |            |        |      |           |
|--------------------------------|-----------------------------|---------|-------------|----------|------------|--------|------|-----------|
|                                | IP/Prefix                   | Gateway | Interface   | Protocol | Preference | Metric | Vsys | Configure |
| *                              | 2001:abc:2480:3621::3/64    | ::      | ethernet0/1 | C        |            |        | Root | -         |
| *                              | 2001:abc:2480:3621::3/128   | ::      | ethernet0/1 | H        |            |        | Root | -         |
| *                              | 2001:abc:2480:3627::1/64    | ::      | ethernet0/2 | C        |            |        | Root | -         |
| *                              | 2001:abc:2480:3627::1/128   | ::      | ethernet0/2 | H        |            |        | Root | -         |
| *                              | 2001:abc:2480:36f7::254/128 | ::      | loopback.1  | C        |            |        | Root | -         |
| *                              | 2001:abc:2480:36f7::254/128 | ::      | loopback.1  | H        |            |        | Root | -         |
| *                              | 2001:abc:2480:36aa::7/64    | ::      | ethernet0/0 | C        |            |        | Root | -         |
| *                              | 2001:abc:2480:36aa::7/128   | ::      | ethernet0/0 | H        |            |        | Root | -         |

\* Active route    C Connected    I Imported        eB EBGP    O OSPF    E1 OSPF external type 1    H Host Route  
 P Permanent    S Static        A Auto-Exported    iB IBGP    R RIP        E2 OSPF external type 2  
 D Dynamic        N NHRP

# Netscreen – Add IPv6 Default Route

- Add ‘::/0’ to denote default route (all IPv6 addresses)
- Add next-hop IPv6 address

Virtual Router Name trust-vr

IPv4/Netmask or IPv6/Prefix Length :: / 0

---

Next Hop  Virtual Router untrust-vr

Gateway

Interface ethernet0/1

Gateway IPv4/v6 Address 2001:abc:2480:3621::1

Permanent

Tag 0

Metric 1

Preference 20

---

OK Cancel

# Netscreen – Verify Default IPv6 Route

- Verify the newly added IPv6 default route is now in the routing table and is active.

| IPv6 Routing Table -- trust-vr |                             |                       |             |          |            |        |      |                        |
|--------------------------------|-----------------------------|-----------------------|-------------|----------|------------|--------|------|------------------------|
|                                | IP/Prefix                   | Gateway               | Interface   | Protocol | Preference | Metric | Vsys | Configure              |
| *                              | 2001:abc:2480:3621::3/64    | ::                    | ethernet0/1 | C        |            |        | Root | -                      |
| *                              | 2001:abc:2480:3621::3/128   | ::                    | ethernet0/1 | H        |            |        | Root | -                      |
| *                              | 2001:abc:2480:3627::1/64    | ::                    | ethernet0/2 | C        |            |        | Root | -                      |
| *                              | 2001:abc:2480:3627::1/128   | ::                    | ethernet0/2 | H        |            |        | Root | -                      |
| *                              | 2001:abc:2480:36f7::254/128 | ::                    | loopback.1  | C        |            |        | Root | -                      |
| *                              | 2001:abc:2480:36f7::254/128 | ::                    | loopback.1  | H        |            |        | Root | -                      |
| *                              | 2001:abc:2480:36aa::7/64    | ::                    | ethernet0/0 | C        |            |        | Root | -                      |
| *                              | 2001:abc:2480:36aa::7/128   | ::                    | ethernet0/0 | H        |            |        | Root | -                      |
| *                              | ::/0                        | 2001:abc:2480:3621::1 | ethernet0/1 | SP       | 20         | 1      | Root | <a href="#">Remove</a> |

\* Active route    C Connected    I Imported    eB EBGP    O OSPF    E1 OSPF external type 1    H Host Route  
 P Permanent    S Static    A Auto-Exported    iB IBGP    R RIP    E2 OSPF external type 2  
 D Dynamic    N NHRP

# Netscreen Policies – Allow ICMP6

- **As with IPv4, do not block all ICMP6!**
- **See RFC4890 - Recommendations for Filtering ICMPv6 Messages in Firewalls**
- **Traffic That Must Not Be Dropped**
  - Destination Unreachable (Type 1) - All codes
  - Packet Too Big (Type 2)
  - Time Exceeded (Type 3) - Code 0 only
  - Parameter Problem (Type 4) - Codes 1 and 2 only
  - Echo Request (Type 128)
  - Echo Response (Type 129)
- **This is not all inclusive, there are other recommendations in RFC.**

# Netscreen IPv6 Policies

- IPv6 policies are separate policies from IPv4.
- Can add policy elements & groups for IPv6 just as IPv4.
- Implement policies for IPv6 the same as for IPv4.

From SAN\_Zone To Untrust, total policy: 6

| ID     | Source                                                                                                                                                    | Destination                                                                                                                                              | Service                   | Action | Options | Configure                                                         | Enable                              | Move |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|--------|---------|-------------------------------------------------------------------|-------------------------------------|------|
| 994276 | Any-IPv4                                                                                                                                                  | 127.32.148.160/28                                                                                                                                        | Good ICMP and Traceroute  |        |         | <a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Remove</a> | <input checked="" type="checkbox"/> |      |
| 994275 | Any-IPv6                                                                                                                                                  | 2001:abc:2480:a000::/64                                                                                                                                  | Good ICMP6 and Traceroute |        |         | <a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Remove</a> | <input checked="" type="checkbox"/> |      |
| 994272 | Any5 IPv4 - 127.32.148.172/32<br>Any IPv4 - 127.32.148.175/32<br>Any6 IPv4 - 127.32.148.174/32<br>Any7 IPv4 - 127.32.148.173/32                           | Any4 IPv4 - 127.32.240.95/32<br>Any3 IPv4 - 127.32.240.19/32<br>Any1 IPv4 - 127.32.240.138/32<br>Any2 IPv4 - 127.32.240.120/32                           | ANY                       |        |         | <a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Remove</a> | <input checked="" type="checkbox"/> |      |
| 994269 | Any-IPv4                                                                                                                                                  | Any-IPv4                                                                                                                                                 | ANY                       |        |         | <a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Remove</a> | <input checked="" type="checkbox"/> |      |
| 994274 | Any5 IPv6 - 2001:abc:2480:a000::90/64<br>Any IPv6 - 2001:abc:2480:a000::93<br>Any6 IPv6 - 2001:abc:2480:a000::92<br>Any7 IPv6 - 2001:abc:2480:a000::91/64 | Any4 IPv6 - 2001:abc:430::240:95/64<br>Any3 IPv6 - 2001:abc:430::240:119/64<br>Any1 IPv6 - 2001:abc:430::240:138/64<br>Any2 IPv6 - 2001:abc:430::240:120 | ANY                       |        |         | <a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Remove</a> | <input checked="" type="checkbox"/> |      |
| 994270 | Any-IPv6                                                                                                                                                  | Any-IPv6                                                                                                                                                 | ANY                       |        |         | <a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Remove</a> | <input checked="" type="checkbox"/> |      |

# Netscreen CLI – Verify Routing

- Use the ‘get route v6’ to view IPv6 routing table.

```

10.10.1.238 - PuTTY
FW_Sitel-> get route v6

IPv6 Dest-Routes for <untrust-vr> (0 entries)

H: Host C: Connected S: Static A: Auto-Exported
I: Imported R: RIP P: Permanent D: Auto-Discovered
N: NHRP
iB: IBGP eB: EBGp O: OSPF E1: OSPF external type 1
E2: OSPF external type 2 trailing B: backup route

IPv6 Dest-Routes for <trust-vr> (9 entries)

 ID IP-Prefix Interface
 Gateway P Pref Mtr Vsys

* 1 ::/0 eth0/1
 2001:abc:2480:3621::1 SP 20 1 Root
* 6 2001:abc:2480:3627::/64
 :: C 0 0 Root
* 7 2001:abc:2480:3627::1/128
 :: H 0 0 Root
* 5 2001:abc:2480:3621::3/128
 :: H 0 0 Root
* 4 2001:abc:2480:3621::/64
 :: C 0 0 Root
* 8 2001:abc:2480:36f7::254/128
 :: C 0 0 Root
* 9 2001:abc:2480:36f7::254/128
 :: H 0 0 Root
* 15 2001:abc:2480:36aa::7/128
 :: H 0 0 Root
* 14 2001:abc:2480:36aa::/64
 :: C 0 0 Root

FW_Sitel->

```

# Netscreen CLI – Verify IPv6 Neighbors



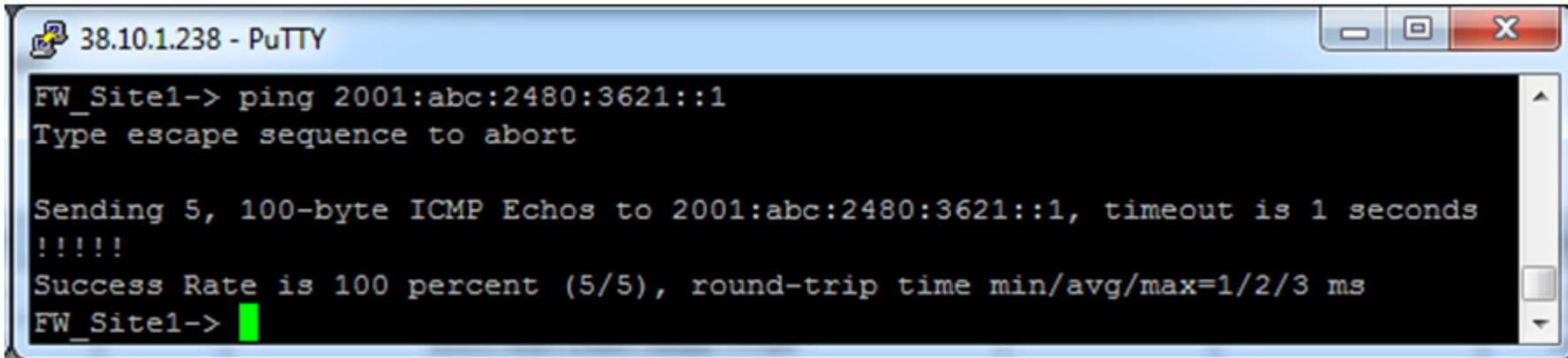
- Use 'get ndp' to determine IPv6 neighbors.

```
38.10.1.238 - PuTTY
FW_Site1-> get nd
usage: 4/4096 miss: 0 always-on-dest: disabled
states(S): N Undefined, X Deleted, I Incomplete, R Reachable, L Stale, D Delay,
P Probe, F Probe forever S Static, A Active, I Inactive, * persistent

IPv6 Address Link-Layer Addr S Interface Age Pk
2001:abc:2480:3627::10 000c29614c22 L ethernet0/2 01h36m26s 0
2001:abc:2480:3621::1 0024dc0cab02 L ethernet0/1 01h46m45s 0
fe80::110a:438:2dd9:3b8e 000c29614c22 L ethernet0/2 01h36m26s 0
fe80::224:dcff:fe0c:ab02 0024dc0cab02 L ethernet0/1 01h48m39s 0
FW_Site1->
```

# Netscreen CLI – Verify Reachability

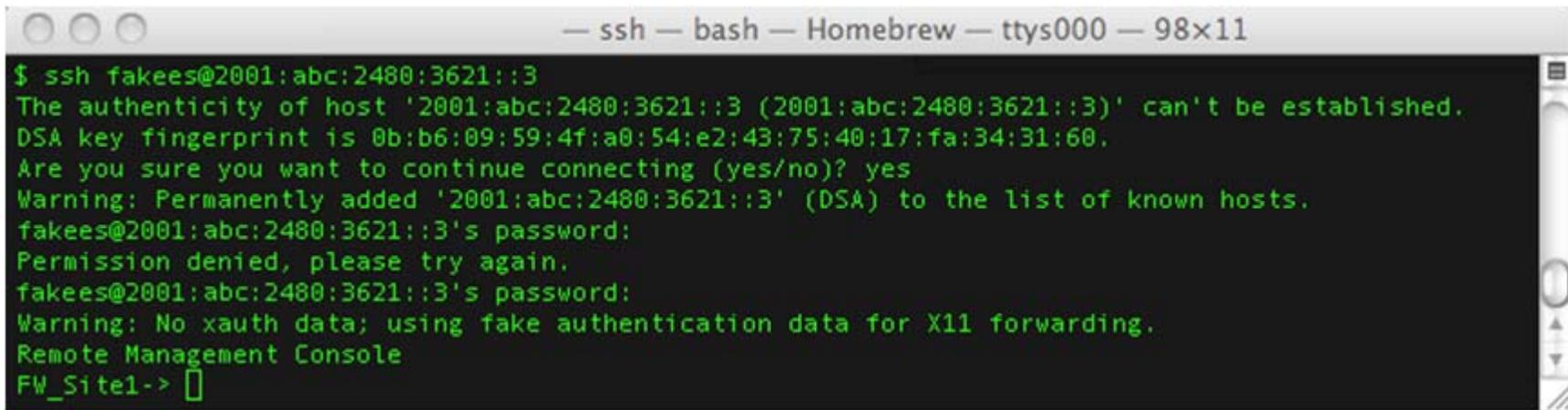
- Use the Ping command to ping the upstream router.



```
38.10.1.238 - PuTTY
FW_Site1-> ping 2001:abc:2480:3621::1
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 2001:abc:2480:3621::1, timeout is 1 seconds
!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=1/2/3 ms
FW_Site1->
```

- SSH to the IPv6 Firewall Address.



```
— ssh — bash — Homebrew — ttys000 — 98x11
$ ssh fakees@2001:abc:2480:3621::3
The authenticity of host '2001:abc:2480:3621::3 (2001:abc:2480:3621::3)' can't be established.
DSA key fingerprint is 0b:b6:09:59:4f:a0:54:e2:43:75:40:17:fa:34:31:60.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '2001:abc:2480:3621::3' (DSA) to the list of known hosts.
fakees@2001:abc:2480:3621::3's password:
Permission denied, please try again.
fakees@2001:abc:2480:3621::3's password:
Warning: No xauth data; using fake authentication data for X11 forwarding.
Remote Management Console
FW_Site1->
```

# Netscreen CLI - Commands

## IPv6 Interface Configuration –

```
set interface ethernet0/1 ip 168.168.201.3/29
set interface "ethernet0/1" ipv6 mode "router"
set interface "ethernet0/1" ipv6 ip 2001:abc:2480:3621::3/64
set interface "ethernet0/1" ipv6 enable
set interface ethernet0/1 route
```

## IPv6 Router Advertisement Settings –

```
set interface ethernet0/1 ipv6 ra prefix 2001:abc:2480:3621::/64 autonomous onlink
set interface ethernet0/1 ipv6 ra link-address
set interface ethernet0/1 ipv6 ra transmit
set interface ethernet0/1 ipv6 ra link-mtu
set interface ethernet0/1 ipv6 nd nud
```

## IPv6 Default Route –

```
set route ::/0 interface ethernet0/1 gateway 2001:abc:2480:3621::1 permanent
```

## Policy Using 'Multiple' Source and 'Multiple' Destination –

```
set policy id 994274 from "SAN_Zone" to "Untrust" "Any9 IPv6 - 2001:abc:2480:a000::90/64" "Any10 IPv6 - 2001:abc:4300::240:95/64" "ANY" permit
set policy id 994274
set src-address "Any11 IPv6 - 2001:abc:2480:a000::93"
set src-address "Any12 IPv6 - 2001:abc:2480:a000::92"
set src-address "Any13 IPv6 - 2001:abc:2480:a000::91/64"
set dst-address "Any14 IPv6 - 2001:abc:4300::2400:119/64"
set dst-address "Any15 IPv6 - 2001:abc:4300::2400:138/64"
set dst-address "Any16 IPv6 - 2001:abc:4300::2400:120"
```

## Set Policy Group –

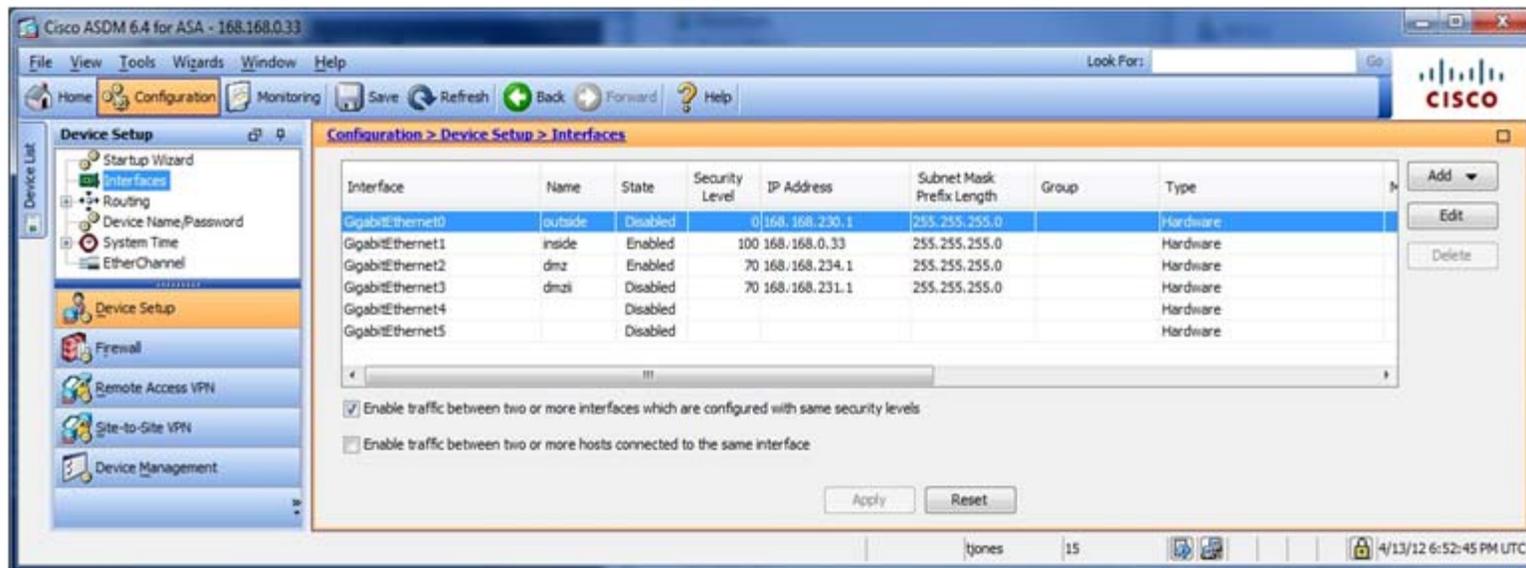
```
set group address "SAN_Zone" "SAN_Servers"
set group address "SAN_Zone" "SAN_Servers" add "Any11 IPv4 - 127.32.148.172/32"
set group address "SAN_Zone" "SAN_Servers" add "Any12 IPv4 - 127.32.148.175/32"
set group address "SAN_Zone" "SAN_Servers" add "Any13 IPv4 - 127.32.148.174/32"
set group address "SAN_Zone" "SAN_Servers" add "Any14 IPv4 - 127.32.148.173/32"
```

# Cisco ASA Security Appliances



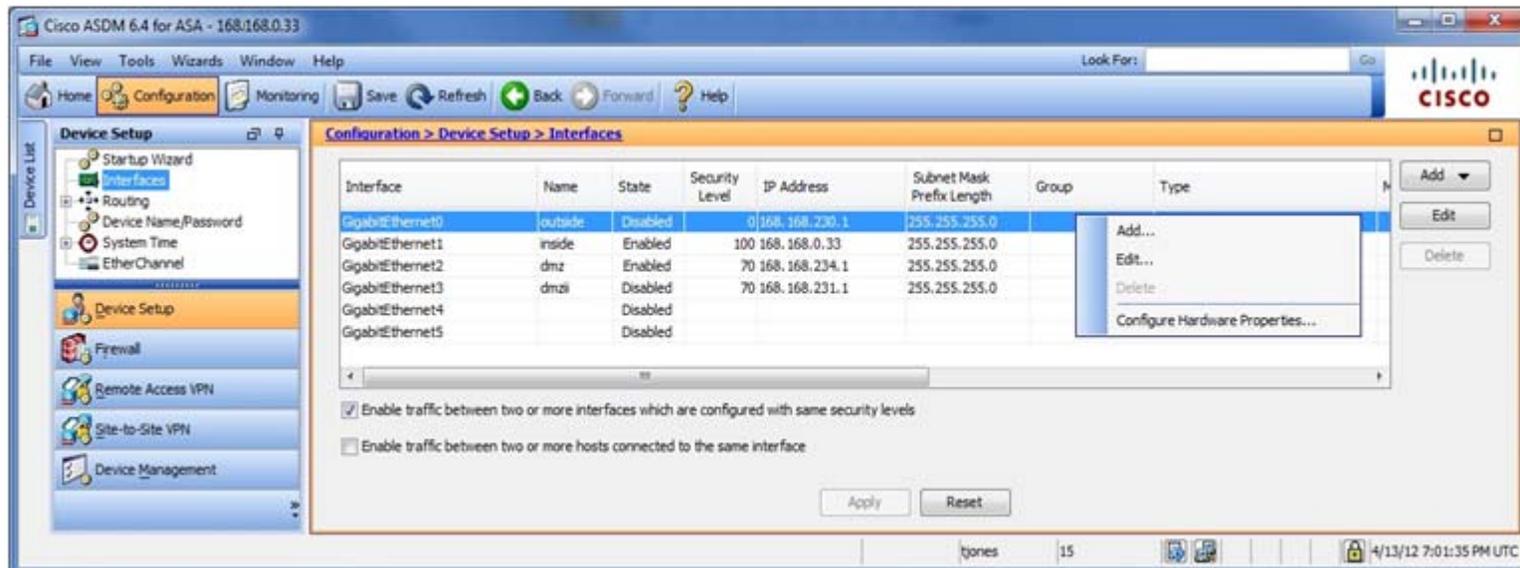
# Cisco ASA Security Appliances

- 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.



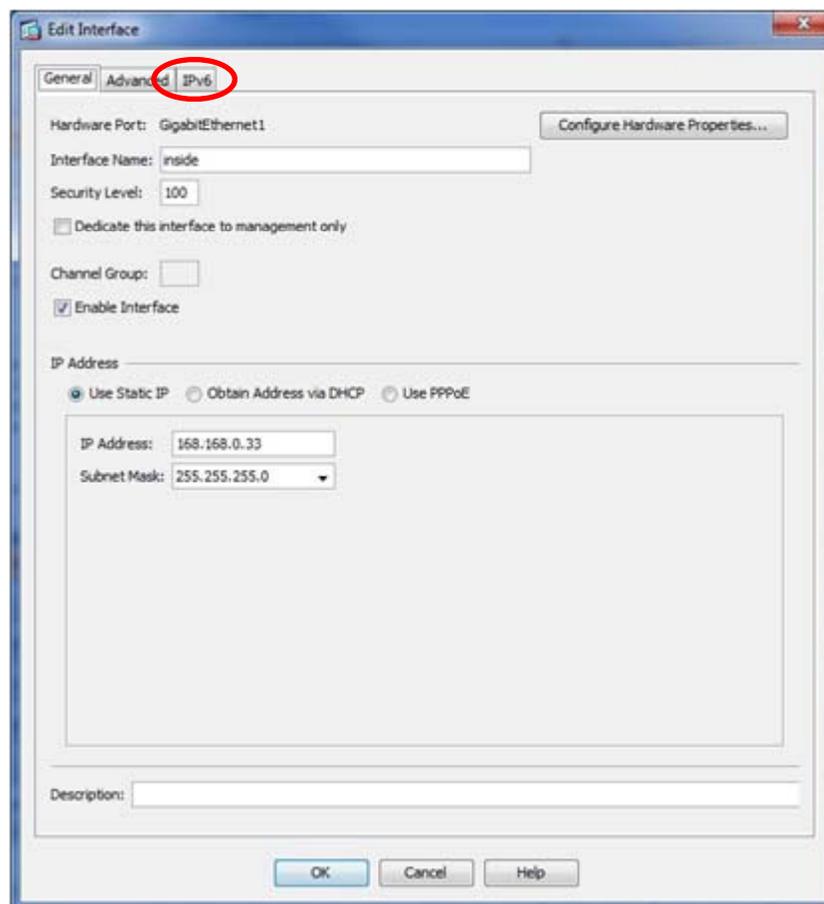
# Cisco ASA – Configuration – Interfaces

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



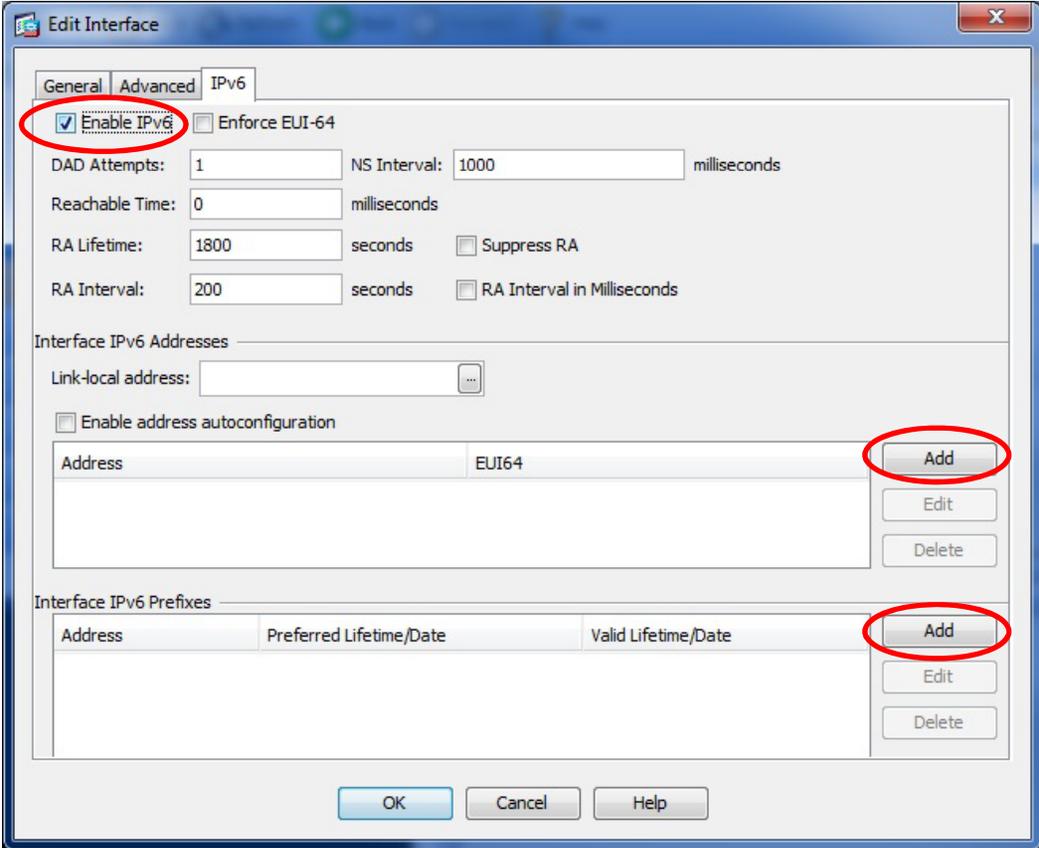
# Cisco ASA – Edit Interfaces

- 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.



The screenshot shows the 'Edit Interface' dialog box with the 'IPv6' tab selected. The 'Enable IPv6' checkbox is checked and circled in red. Below it, the 'Add' buttons for both the 'Interface IPv6 Addresses' and 'Interface IPv6 Prefixes' sections are also circled in red.

**Interface IPv6 Addresses**

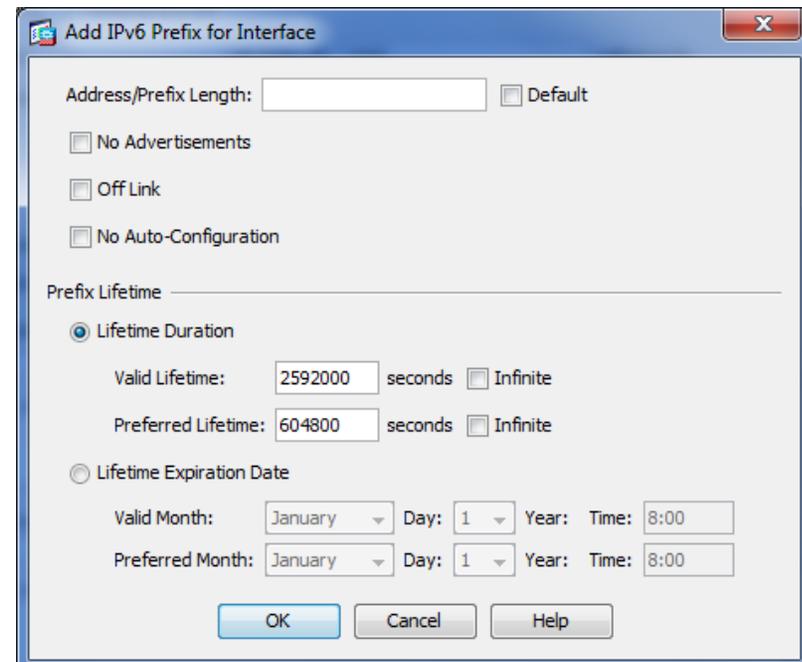
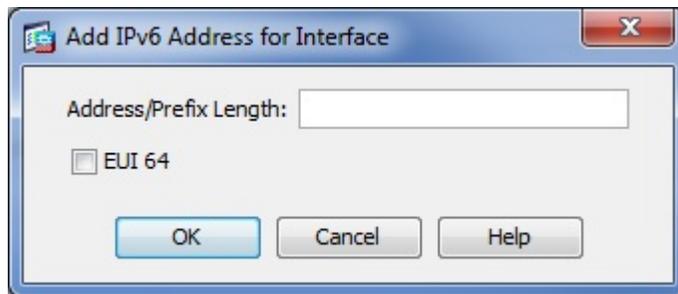
| Address | EUI64 |
|---------|-------|
|         |       |

**Interface IPv6 Prefixes**

| Address | Preferred Lifetime/Date | Valid Lifetime/Date |
|---------|-------------------------|---------------------|
|         |                         |                     |

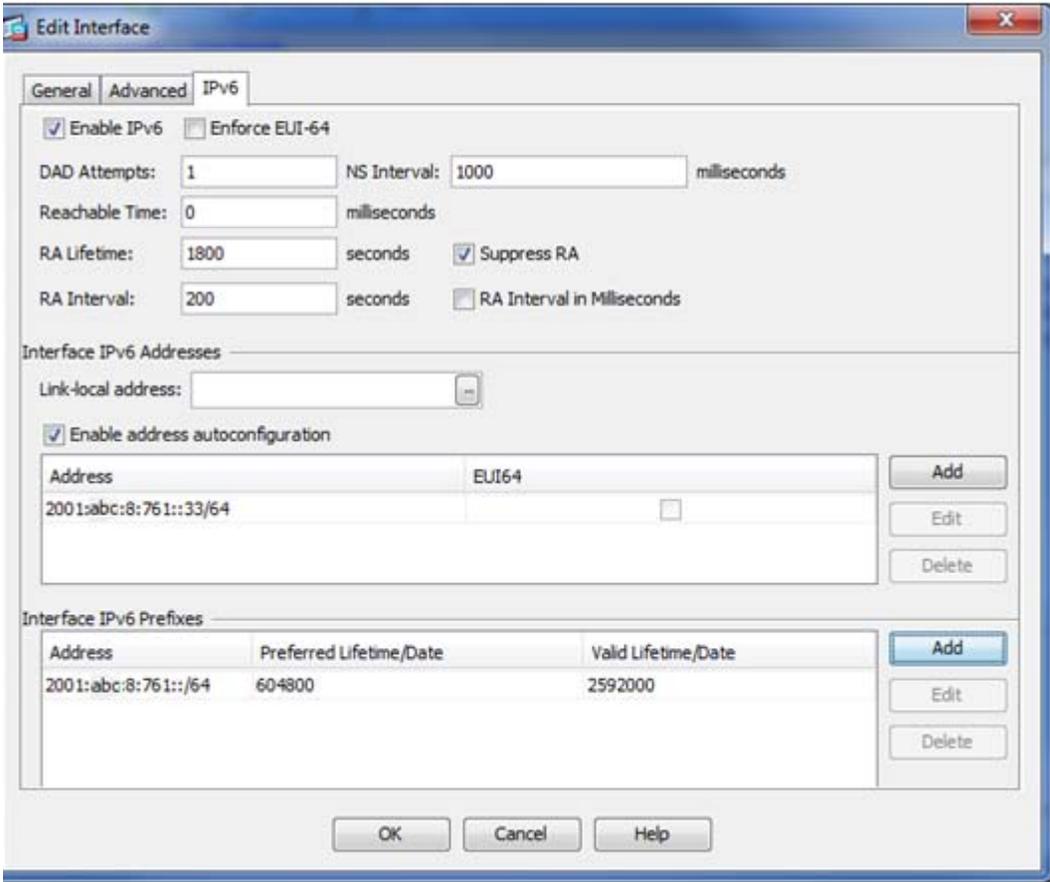
# Cisco ASA – Add IPv6 Address

- 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 'General' sub-tab is active, showing various IPv6 settings. The 'Interface IPv6 Addresses' section contains a table with one entry: '2001:abc:8:761::33/64' with 'EUI64' selected. The 'Interface IPv6 Prefixes' section contains a table with one entry: '2001:abc:8:761::/64' with 'Preferred Lifetime/Date' '604800' and 'Valid Lifetime/Date' '2592000'.

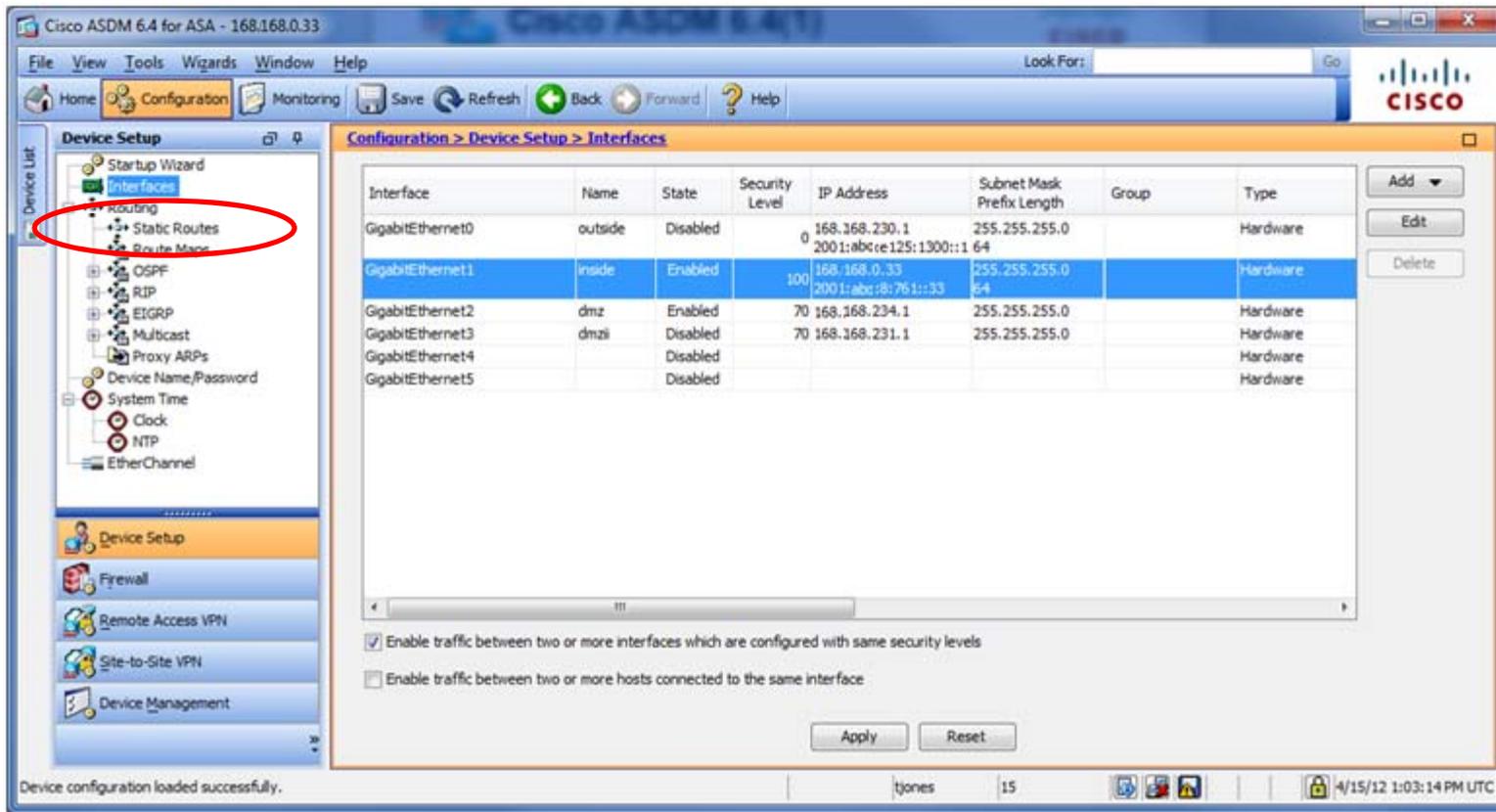
| Address               | EUI64                               |
|-----------------------|-------------------------------------|
| 2001:abc:8:761::33/64 | <input checked="" type="checkbox"/> |

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

# 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 interface for configuring a Cisco ASA. The left-hand 'Device Setup' pane shows a tree view where 'Static Routes' under the 'Routing' category is highlighted with a red circle. The main pane displays the 'Configuration > Device Setup > Interfaces' page, which contains a table of interface configurations.

| Interface        | Name    | State    | Security Level | IP Address                             | Subnet Mask Prefix Length | Group | Type     |
|------------------|---------|----------|----------------|----------------------------------------|---------------------------|-------|----------|
| GigabitEthernet0 | outside | Disabled | 0              | 168.168.230.1<br>2001:abcce125:1300::1 | 255.255.255.0<br>64       |       | Hardware |
| GigabitEthernet1 | inside  | Enabled  | 100            | 168.168.0.33<br>2001:abc:8:761::33     | 255.255.255.0<br>64       |       | 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 |

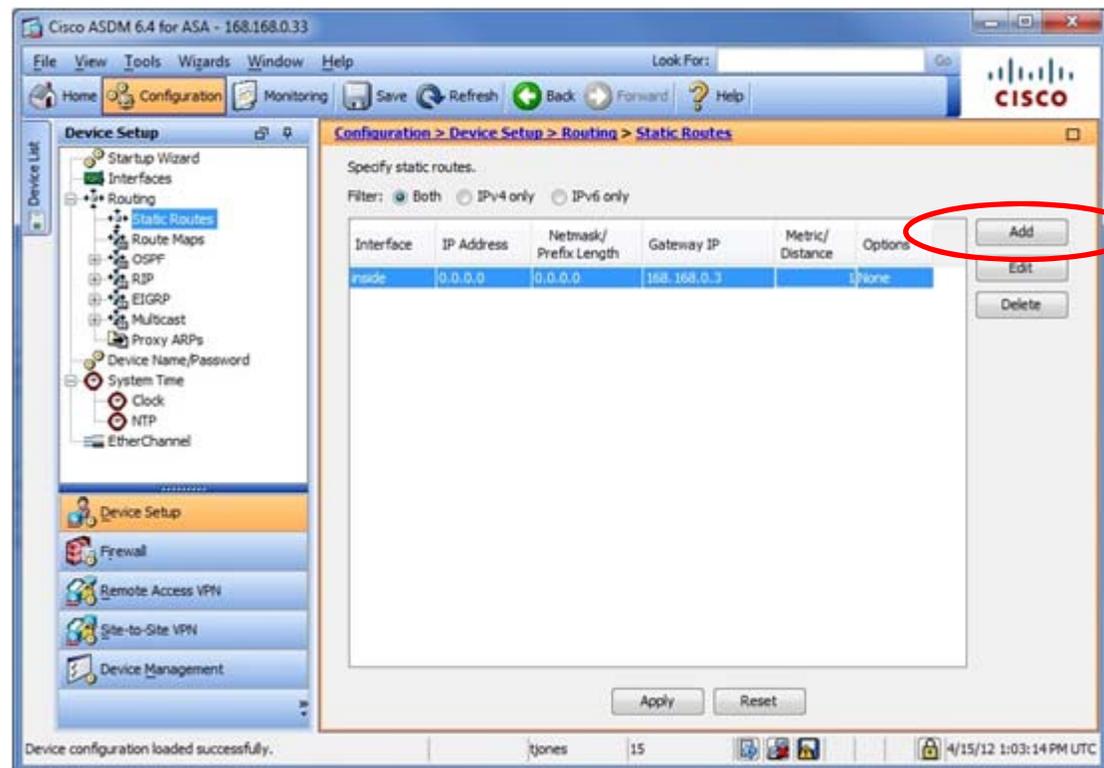
Below the table, there are two checkboxes:

- 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 located at the bottom of the configuration pane.

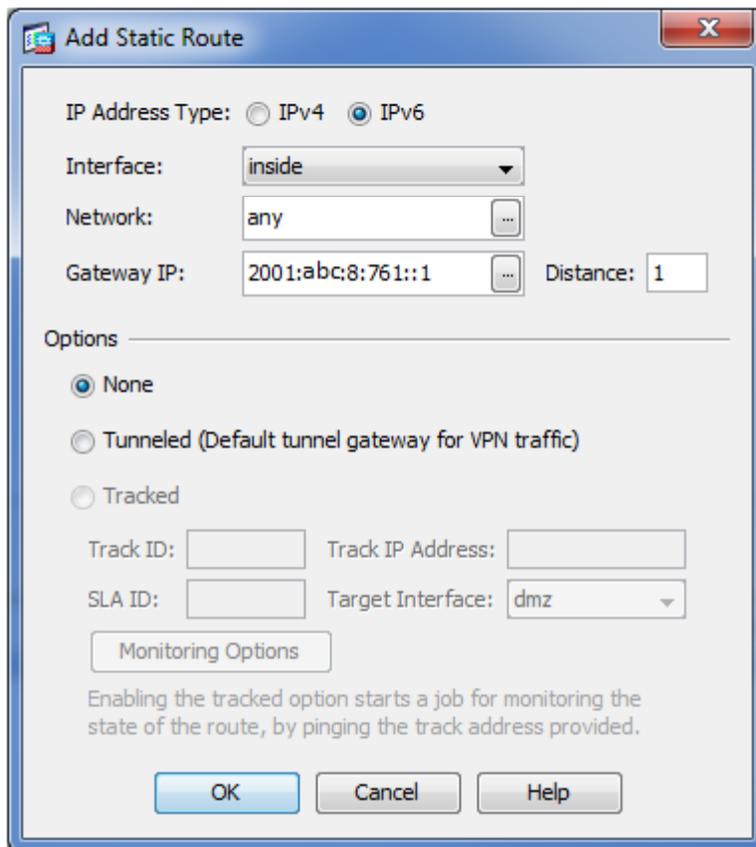
# Cisco ASA - Routing

- 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’.



The screenshot shows the 'Add Static Route' dialog box with the following configuration:

- IP Address Type:  IPv4  IPv6
- Interface: inside
- Network: any
- Gateway IP: 2001:abc:8:761::1
- Distance: 1
- Options:
  - None
  - Tunneled (Default tunnel gateway for VPN traffic)
  - Tracked
    - Track ID: [ ]
    - Track IP Address: [ ]
    - SLA ID: [ ]
    - Target Interface: dmz

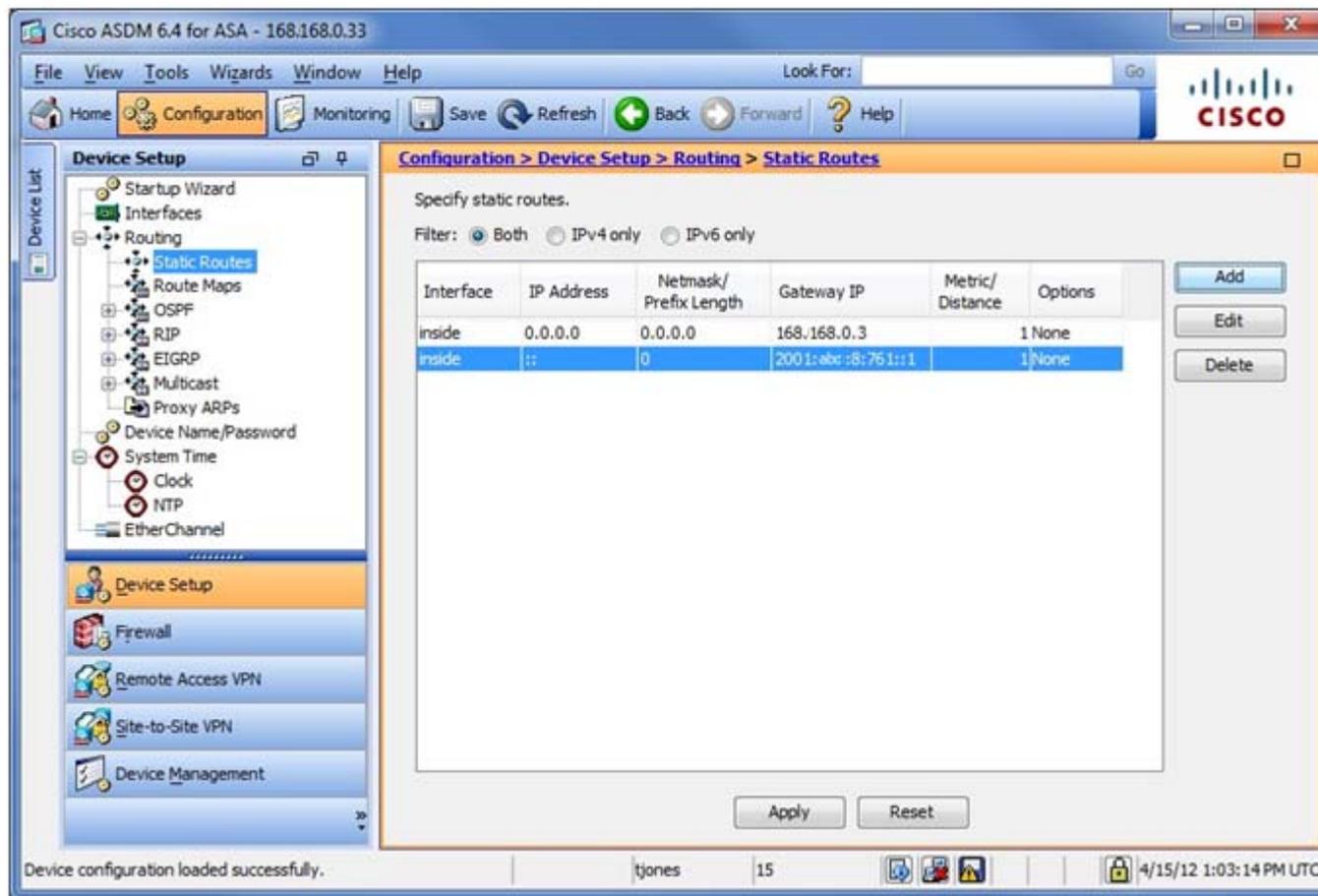
Monitoring Options

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

Buttons: OK, Cancel, Help

# Cisco ASA – Routing – Add Default

- Add the IPv6 default route.



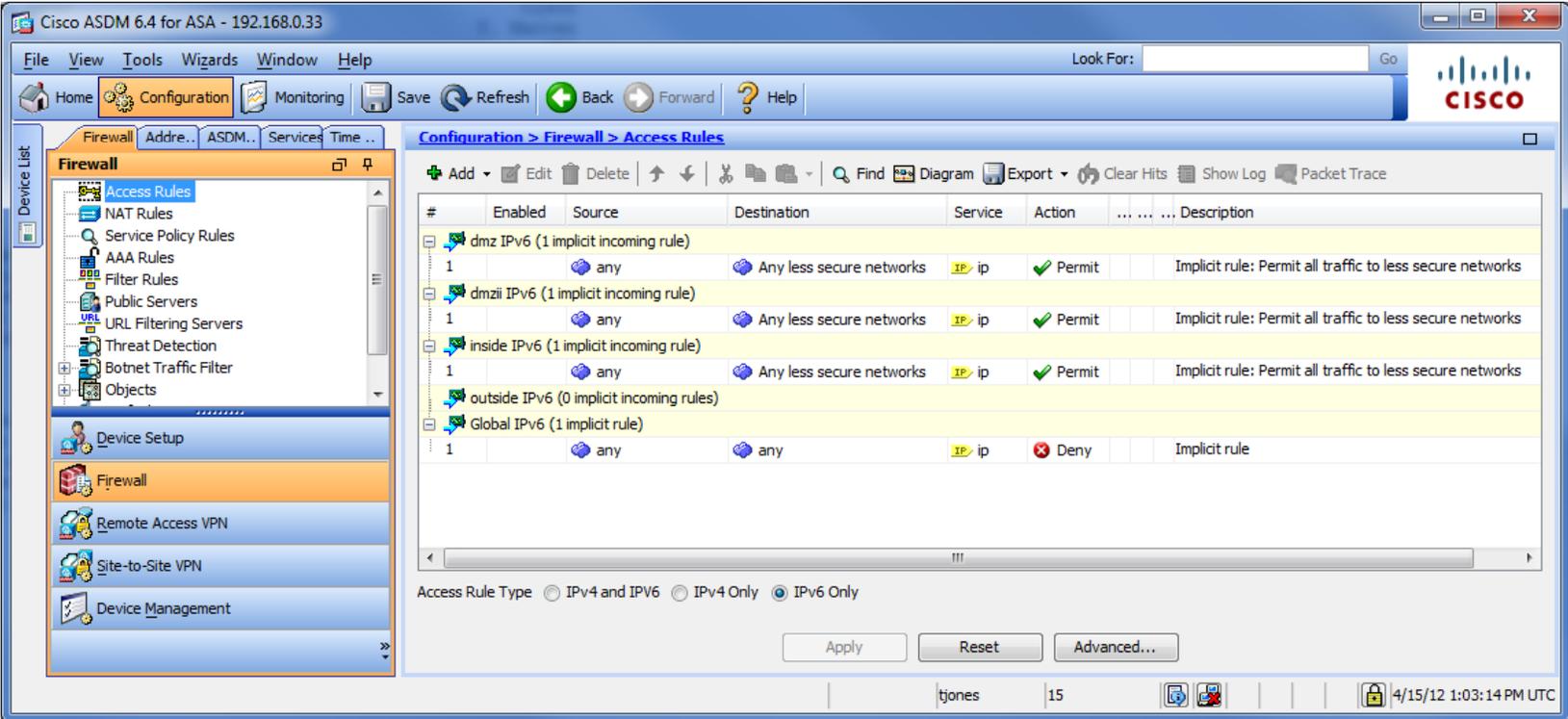
# Cisco ASA – Firewall – Access Rules



- 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                                             |

Access Rule Type:  IPv4 and IPv6  IPv4 Only  IPv6 Only

Buttons: Apply, Reset, Advanced...

Bottom status bar: tJones | 15 | 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
```

# Brocade Switches



# Brocade Switches

- Below is output for IPv6 Brocade switch commands.
- Configure as many IPv6 settings as you have available!
- Below we have NTP, Sflow and DNS configured to use IPv6 address
- Don't forget IPv6 ACL's!

```
#ipv6 address 2001:abc:6000:1401::14/64
#ipv6 dns domain-name example.net
#ipv6 dns server-address 2001:abc:4310:f000::59:244 2001:abc:b0:f000::244

#sntp server ipv6 2001:abc:1000:1048:2a0:69ff:fe01:89a0
#sntp server ipv6 2001:abc:8220:1f01:2a0:69ff:fe01:a05c
#ipv6 dns server-address 2001:abc:a0::244 2001:abc:b0:f000::244

#sflow agent-ip 2001:abc:6000:1401::14 ***Note Switch Mgmt IP is agent-ip
#sflow sample 256
#sflow destination ipv6 X:X:X:X::X
#sflow enable

#ipv6 access-list TEST-v6-Sw-ACL
remark LAN
permit ipv6 2001:abc:2480:1000::/64 host 2001:abc:6000:1401::14
remark Deny_All
deny ipv6 any any mirror
```

# Brocade Switches

- Brocade switches at Layer 2 require a router-advertisement (RA) from an IPv6 router
- Below is the configuration for a Juniper RA from interface fe-1/0/0.101 along with the ipv6 neighbors and RA verification.

```
tjones@dcn1.ast> show configuration protocols
router-advertisement {
 interface fe-1/0/0.101;
}

fakees> show ipv6 neighbors
IPv6 Address Linklayer Address State Exp Rtr Secure Interface
2001:abc:6000:1401::10 84:2b:2b:13:9a:99 stale 881 no no fe-1/0/0.101
2001:abc:6000:1401::11 84:2b:2b:16:fd:88 stale 889 no no fe-1/0/0.101
2001:abc:6000:1401::14 00:12:f2:e4:92:80 stale 899 no no fe-1/0/0.101
fe80::212:f2ff:fee4:9280 00:12:f2:e4:92:80 stale 1120 no no fe-1/0/0.101
fe80::862b:2bff:fe13:9a99 84:2b:2b:13:9a:99 stale 364 no no fe-1/0/0.101
fe80::862b:2bff:fe16:fd88 84:2b:2b:16:fd:88 stale 896 no no fe-1/0/0.101

fakees> show ipv6 router-advertisement
Interface: fe-1/0/0.101
 Advertisements sent: 6676, last sent 00:03:19 ago
 Solicits received: 13, last received 1w3d 07:11:45 ago
 Advertisements received: 0
```

# Brocade Switches – SSH via IPv6

- Verify SSH access via IPv6

```
— ssh — bash — Homebrew — ttys000 — 127x20
$ ssh fakees@2001:abc:6:1401::14
You are accessing a U.S. Government (USG) Information System (IS) that is provided
for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the
following conditions: -The USG routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring, network
operations and defense, personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations. -At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject to routine
monitoring, interception, and search, and may be disclosed or used for any USG authorized
purpose. -This IS includes security measures (e.g., authentication and access controls) to protect
USG interests-not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI
investigative searching or monitoring of the content of privileged communications, or
work product, related to personal representation or services by attorneys,
psychologists, or clergy, and their assistants. Such communications and work product
are private and confidential. See User Agreement for details.
$fakees@2001:abc:6:1401::14's password:
Warning: No xauth data; using fake authentication data for X11 forwarding.
SSH@fakees>
```

**Success!!**

# Example IPv6 Address Plans

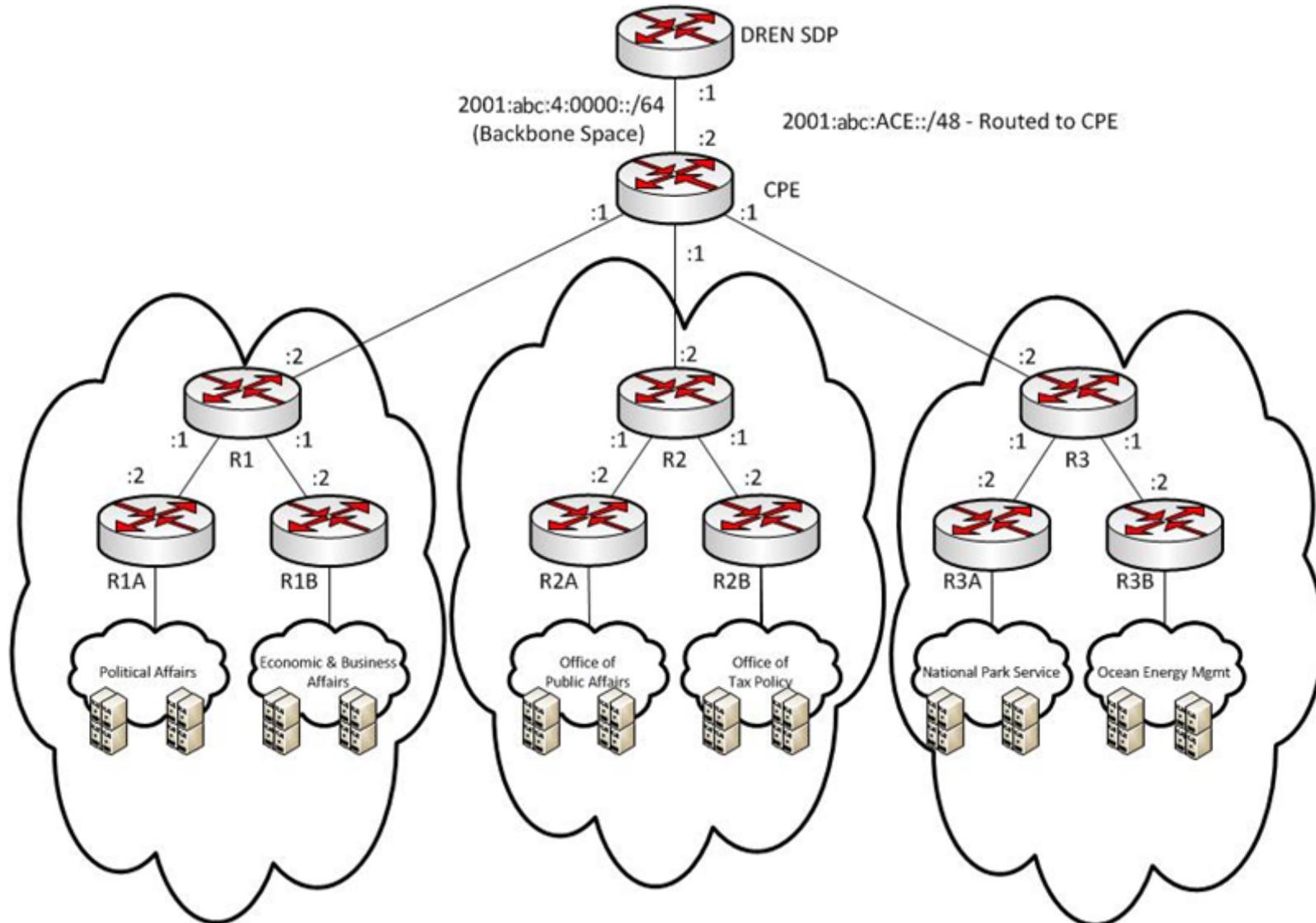
- **HPCMP OPS will provide each individual site/enclave a routed /48**
- **DREN NOC will setup IPv6 BGP routing or static route to Customer CPE.**
- **So how should I subnet my /48? Good Question!**



# Example IPv6 Addressing Plan

- **Suppose you are allocated 2001:abc:ACE::/48**
- **Review your network.**
- **Determine how many OU's do you have? How many divisions?**
  - Determine a scalable plan based on your site.
  - Use /64 from IPv6 space for P2P connections & end-host connections
  - Are hosts going to be use autoconfigure/DHCP6/manual?
  - Do I have an IPv6 Name-server I can user? NTP? sFlow? Others?
- **Gather the answers from these questions to help configure devices.**

# IPv6 Example Network



# IPv6 Addressing – Do What Makes Sense

- Look at your organization and work to break subnets up along easily routed boundaries.

```

2001:0abc:0ACE:0000::/48
1111:1111:1111:0000 Mask

2001:0abc:0ACE:1000::/52
1111:1111:1111:1000 Mask

2001:0abc:0ACE:2000::/52
1111:1111:1111:1000 Mask

2001:0abc:0ACE:3000::/52
1111:1111:1111:1000 Mask

```

This byte could be used to identify organizational units. Would support up to 15 OU's.

The Cabinets  
 Department of State  
 Department of Treasury  
 Department of the Interior

This byte could be used to represent divisions within the organizational units. Would support up to 15 separate divisions per OU.

```

2001:0abc:0ACE:3100::/56
1111:1111:1111:1100 Mask

2001:0abc:0ACE:3200::/56
1111:1111:1111:1100 Mask

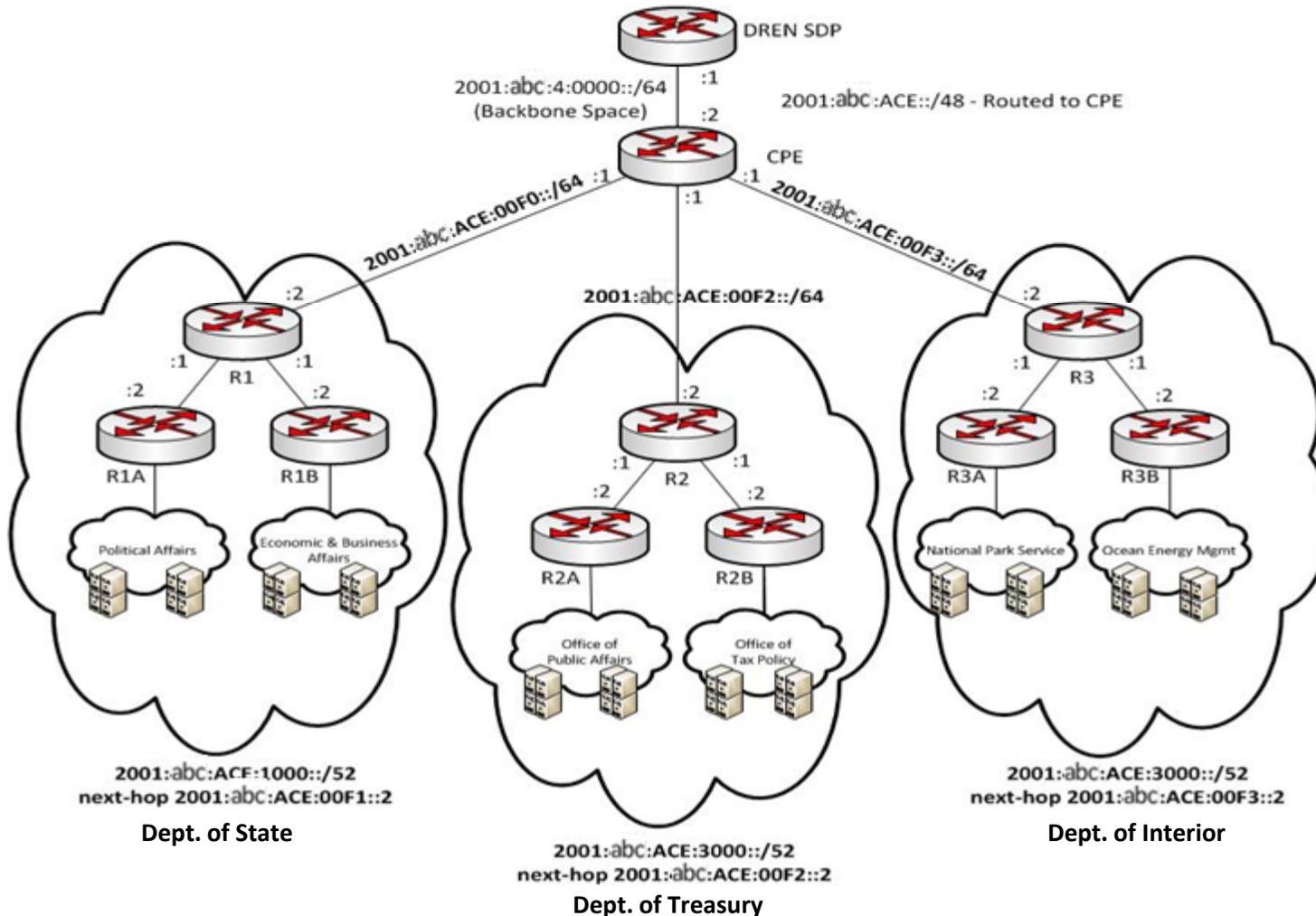
2001:0abc:0ACE:3300::/56
1111:1111:1111:1100 Mask

```

Within each division, there are 256 possible /64's.

# IPv6 Example Addressing

- Each of the routers off of the CPE is routed a /52.
- Notice the P2P connections off of the CPE

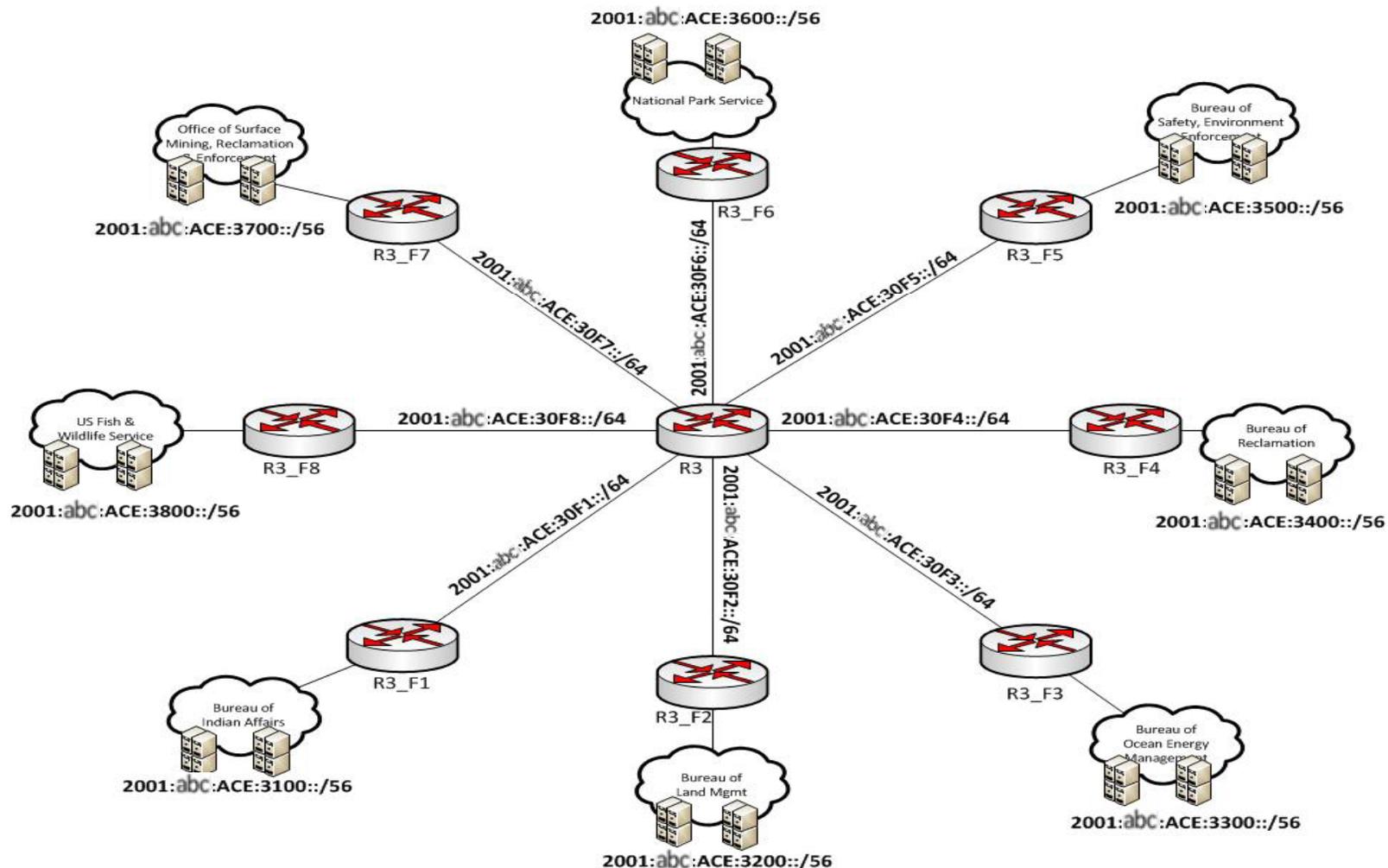


# IPv6 Example Addressing

- **Examining the diagram**
  - Each Department will be routed a /52.
  - 2001:abc:ACE:00FX::/64 is used for the direct connections.
- **Now we have IPv6 routing to each department router...what's next?**
- **Let's look at one of the departments to break it down further.**

# IPv6 Example Addressing

- DOI is routed `2001:abc:ACE:3300::/52`. We break this up into /56's and route to each division.



# IPv6 Example Addressing

- Notice that 2001:abc:ACE:30FX::- The /56 to each division could be further broken down in /60's or just used for /64's on interface connections depending on network.
- Remember...This is only an example! These are not actual IPv6 address for The Cabinet or any subsequent departments.

# IPv6 – Use /64's on Interfaces!

- **Using a subnet prefix length other than a /64 will break many features of IPv6, including Neighbor Discovery (ND), Secure Neighbor Discovery (SEND) [RFC3971], privacy extensions [RFC4941], parts of Mobile IPv6 [RFC4866], Protocol Independent Multicast - Sparse Mode (PIM-SM) with Embedded-RP [RFC3956], and Site Multihoming by IPv6 Intermediation (SHIM6) [SHIM6], among others. A number of other features currently in development, or being proposed, also rely on /64 subnet prefixes.**

**(RFC 5375 IPv6 Addressing Considerations)**

# IPv6 Addressing – What Must Be Changed?



- **Link prefixes assigned to links. Each link in the network must be assigned a link prefix from the new prefix.**
- **IPv6 addresses assigned to interfaces on switches and routers. These addresses are typically assigned manually, as part of configuring switches and routers.**
- **Routing information propagated by switches and routers.**
- **Link prefixes advertised by switches and routers [RFC2461].**
- **Ingress/egress filters.**
- **ACLs and other embedded addresses on switches and routers.**
- **IPv6 addresses assigned to interfaces on hosts.**
- **DNS DNS entries. New AAAA and PTR records are added and old ones removed in several phases to reflect the change of prefix. Caching times are adjusted accordingly during these phases.**
- **IPv6 addresses and other configuration information provided by DHCP.**
- **IPv6 addresses embedded in configuration files, applications, and elsewhere. Finding everything that must be updated and automating the process may require significant effort, which is discussed in more detail in Section 3. This process must be tailored to the needs of each network.**

**(REFERENCE – RFC4192 - Renumbering IPv6 Networks)**

# And finally....



**Do you want to be the talk around the water cooler?**

**Do you want to be the envy of all your friends?**

**Are you looking for new ways to meet men/women?**

**Are you answering any these questions with a resounding YES!...**

**Well let me tell you how....**



# Get IPv6 at Home!

## A true conversation starter! ;-)

- Hurricane Electric – Tunnel Broker



### Tunnelbroker Login

Username:

Password:

[Login](#) [Register](#)

### Hurricane Electric Free IPv6 Tunnel Broker

## IPv6 Tunnel Broker

Check out our new [usage stats!](#)

And then hit up our new [Forums!](#)

Welcome to the Hurricane Electric IPv6 Tunnel Broker! Our free tunnel broker service enables you to reach the IPv6 internet by tunneling over existing IPv4 connections from your IPv6 enabled host or router to one of our IPv6 routers. To use this service you need to have an IPv6 capable host (IPv6 support is available for most platforms) or router which also has IPv4 (existing Internet) connectivity. Our tunnel service is oriented towards developers and experimenters that want a stable tunnel platform.

Advantages of using our tunnel service over others include:

- Run by a Business ISP with 24 x 7 staff at multiple locations and an International backbone ([find out more about IPv6 transit at Hurricane Electric](#))
- Ability to get your own /48 prefix once your tunnel is up
- Ability to get a full view of the IPv6 BGP4+ routing table
- Ability to use your tunnel now after a simple registration process. (It takes less than a minute.)
- Ability to create your tunnel on geographically diverse tunnel-servers (Fremont, Ashburn, Chicago, Dallas, Los Angeles, Miami, New York, Seattle, Toronto, Amsterdam, Frankfurt, London, Paris, Stockholm, Zurich, Hong Kong, Singapore, and Tokyo)

If you are a new user please register by clicking on Register below. After registering your password will be mailed to you and you can return here to activate your tunnel.

If you operate a network, run BGP, have your own ASN, and wish to announce IPv6 address space allocated directly to you by an RIR (ARIN, RIPE, APNIC, etc.) please select the "Create BGP Tunnel" option after you register.

Upon tunnel activation configuration commands for a variety of platforms will be automatically generated. Once you configure your side you will be able to reach the IPv6 internet. If you like our service be sure to tell a friend and recommend us to others!

[Sign up now!](#)

### Quick Links

- [Certification](#)
- [Tunnelbroker](#)
- [Free DNS](#)
- [Code](#)
- [BGP Toolkit](#)
- [Forums](#)
- [FAQ](#)
- [Video Presentations](#)
- [IPv6 Blog Posts](#)
- [Usage Statistics](#)
- [Tunnel Server Status](#)
- [Network Map](#)
- [Looking Glass \(v4/v6\)](#)
- [Route Server \(telnet\)](#)
- [Global IPv6 Report](#)
- [IPv6 BGP View](#)

### Services

- [Transit](#)
- [Colocation](#)
- [Dedicated Servers](#)

### v4 Exhaustion

#### IPv4 & IPv6 Statistics

|                        |                |
|------------------------|----------------|
| <b>RIR v4 IPs Left</b> |                |
| AfriNIC                | 59,067,477     |
| APNIC                  | 18,770,944     |
| ARIN                   | 117,574,805    |
| LACNIC                 | 53,450,423     |
| RIPE                   | 36,361,293     |
| <b>v6 ASNs</b>         |                |
| 13%                    | (5,487/41,011) |
| <b>v6 Ready TLDs</b>   |                |
| 84%                    | (265/313)      |
| <b>v6 Glues</b>        |                |
|                        | 8,540          |
| <b>v6 Domains</b>      |                |
|                        | 3,238,514      |

### Top 10 Certs

|                             |        |
|-----------------------------|--------|
| <a href="#">jerniman</a>    | [1500] |
| <a href="#">lukec</a>       | [1500] |
| <a href="#">williamsep</a>  | [1500] |
| <a href="#">jzan</a>        | [1500] |
| <a href="#">solarken...</a> | [1500] |
| <a href="#">wsyoung</a>     | [1500] |
| <a href="#">htamas</a>      | [1500] |
| <a href="#">vamh</a>        | [1500] |
| <a href="#">mf</a>          | [1500] |
| <a href="#">gstueve</a>     | [1500] |

### Latest 10 Certs

|                             |        |
|-----------------------------|--------|
| <a href="#">syllable3</a>   | [Admn] |
| <a href="#">k9ps</a>        | [Exp]  |
| <a href="#">aguspriyadi</a> | [Sage] |
| <a href="#">str4nd</a>      | [Sage] |
| <a href="#">Vraithh</a>     | [Sage] |
| <a href="#">Alexic3280</a>  | [Newb] |
| <a href="#">suspecte...</a> | [Sage] |
| <a href="#">caeners</a>     | [Exp]  |
| <a href="#">enjoyroot</a>   | [Newb] |
| <a href="#">osubam</a>      | [Enth] |

# Hurricane Electric - Tunnel Details

- The details below show that 2 of 5 tunnels have been built. You can click on the tunnel to get more specific information.



```

Select Administrator: Command Prompt

C:\Users\ones>nslookup 2001:abc:7:8ef::1
Server: U.AREA.NET
Address: 168.168.0.8

Name: tunnel1.tserv13.1.ipv6.he.net
Address: 2001:abc:7:8ef::1

C:\Users\ones>nslookup 2001:abc:7:8ef::2
Server: U.AREA.NET
Address: 168.168.0.8

Name: pt.tunnel1.tserv13.1.ipv6.he.net
Address: 2001:abc:7:8ef::2

C:\Users\ones>

```



The tunnels shown on the left are the DNS names for the tunnels.



### Hurricane Electric Free IPv6 Tunnel Broker

Name: \_\_\_\_\_

User ID: \_\_\_\_\_

**Tunnel Broker News:**

**Update - 18 January 2012**  
[January 18, 2012]

**Update - 13 January 2012**  
[January 13, 2012]

**UPDATE - 16 October 2011**  
[October 16, 2011]

**UPDATE - Sept. 27th, 2010**  
[September 27, 2011]

**Dyn-compliant Endpoint Updates**  
[September 16, 2011]

HE.NET  
IPv6  
Certified  
**Explorer**

---

| Tunnel [ 2 / 5 ]                             | Routed /64          | Routed /48         | Description |
|----------------------------------------------|---------------------|--------------------|-------------|
| <a href="#">tunnel.tserv13.1.ipv6.he.net</a> | 2001:abc:8:8ef::/64 | 2001:abc:e1ae::/48 | VCOE - C    |
| <a href="#">tunnel.tserv13.2.ipv6.he.net</a> | 2001:abc:8:8fb::/64 | 2001:abc:e2c9::/48 | VCOE - V    |

# Hurricane Electric - Tunnel Details



- The tunnel details provide all the information you need to build your own IPv6 tunnel.
- The example configurations tab will help you determine the configuration for you for nearly any device you might have.
- Note: You will need a stable IPv4 address for your endpoint.

### Tunnel Details

**IPv6 Tunnel** | Example Configurations | Advanced

Tunnel ID: 81602 [Delete Tunnel](#)  
Creation Date: Nov 13, 2010  
Description:

---

**IPv6 Tunnel Endpoints**

Server IPv4 Address: 216.66.22.2  
Server IPv6 Address: 2001:abc:7:8ef::1/64  
Client IPv4 Address: **207.98.220.154**  
Client IPv6 Address: 2001:abc:7:8ef::2/64

---

**Available DNS Resolvers**

Anycasted IPv6 Caching Nameserver: 2001:abc::20::2  
Anycasted IPv4 Caching Nameserver: 74.82.42.42

---

**Routed IPv6 Prefixes**

Routed /64: 2001:abc:8:8ef::/64  
Routed /48: 2001:abc:e1ae::/48

---

**rDNS Delegations** [Edit](#)

rDNS Delegated NS1:  
rDNS Delegated NS2:  
rDNS Delegated NS3:  
rDNS Delegated NS4:  
rDNS Delegated NS5:

# Hurricane Electric – Example Configurations



- There are numerous devices for which example configurations can be found.
- The example will be customized to use the tunnel information that you have been delegated.

The screenshot shows the 'Tunnel Details' page with the 'Example Configurations' tab selected. A dropdown menu is open, listing various operating systems and devices. The list includes: Select Your OS, Apple Airport, Cisco IOS, CoyotePoint Equalizer, Fortigate 4.x, FreeBSD < 4.4, FreeBSD >= 4.4, JunOS, JunOS ES, Linux-net-tools, Linux-route2, Mikrotik, NetBSD / Mac OS X, OpenBSD, OpenWRT Backfire 10.03.1, ScreenOS 6.2.0r1.0, Solaris, Vyatta, Windows 2000/XP, and Windows Vista/2008/7. Below the dropdown, there is a text area for commands and a note about DHCP service.

# Hurricane Electric – Example Configuration



- The output is designed specifically to work with your tunnel information.



### Tunnel Details

IPv6 Tunnel   Example Configurations   Advanced

JunOS

Copy and paste the following commands into a command window:

```
interfaces {
 ip-0/1/0 {
 unit 0 {
 tunnel {
 source 207.98.220.154;
 destination 216.66.22.2;
 }
 family inet6 {
 address 2001:abc:7:8ef::2/64;
 }
 }
 }
}
```

**NOTE:** When behind a firewall appliance that passes protocol 41, use the IPv4 address you get from your appliance's DHCP service instead of the IPv4 endpoint you provided to our broker.

The configurations provided are example configurations and may be different depending on the version of the OS or the tools you are using. If you have any issues getting your tunnel to work please contact us at [ipv6@he.net](mailto:ipv6@he.net) and we will be happy to assist you.

# Other Tunnel Brokers

Hurricane Electric isn't the only show in town...

- **Gogo6's Freenet6 Tunnelbroker –**
  - <http://www.gogo6.com/freenet6/tunnelbroker>
  - server/client model
- **SixXS - IPv6 Deployment & Tunnel Broker**
  - <https://www.sixxs.net/main/>
- **Verify your current IPv6 provider...many major ISP's have pilot running and you may be able to go native through your ISP.**

# RFC's to Reference

- **RFC 3531 - A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block**
- **RFC3587 - Pv6 Global Unicast Address Format**
- **RFC4191 - Default Router Preferences and More-Specific Routes**
- **RFC4291 - IP Version 6 Addressing Architecture**
- **RFC4861 - Neighbor Discovery for IP version 6 (IPv6)**
- **RFC4890 - Recommendations for Filtering ICMPv6 Messages in Firewalls**

