Rogue RA Sniping With Scapy

Alan Whinery
U. Hawaii
Hawaii IPv6 Task Force

JT Summer 2010
Columbus, OH
ipv6hawaii.org

SLAAC Router Adverts

- Part of ICMPv6 Neighbor Discovery Protocol
- Allows user-devices and router to work together to assign IPv6 addresses
- Router sends to multicast group FF02::1
- No authN or authZ: all RAs are simply believed

Salt Lake Area Accordion Club

(www.slaac.com)

The problem(s)

- From our central campus's wireless net, a number of people were unable to reach Google reliably
- From that wireless net, 50% or more of clients are accessing the Google-sphere by IPv6
- Investigation identified an issue with Windows Vista machines with Internet Connection Sharing were often sending ICMPv6 Router Advertisements on the wireless.
- There may be other sources of “rogue” Ras
- YOU SHOULD SET ROUTER PRIORITY TOO

A Rogue Frame

```
⊞ Frame 23 (166 bytes on wire, 90 bytes captured)
⊞ Ethernet II, Src: HonHaiPr_56:88:81 (00:24:2c:56:88:81), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
⊞ Internet Protocol Version 6
⊟ Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0x96a3
    Cur hop limit: 0
  ⊞ Flags: 0x40
    Router lifetime: 65535
    Reachable time: 0
    Retrans timer: 0
  ⊟ ICMPv6 Option (Source link-layer address)
      Type: Source link-layer address (1)
      Length: 8
      Link-layer address: 00:24:2c:56:88:81
  ⊟ ICMPv6 Option (MTU)
      Type: MTU (5)
      Length: 8
      MTU: 1500
  ⊟ ICMPv6 Option (Route Information)
      Type: Route Information (24)
      Length: 16
[Packet size limited during capture: ICMPv6 truncated]
```

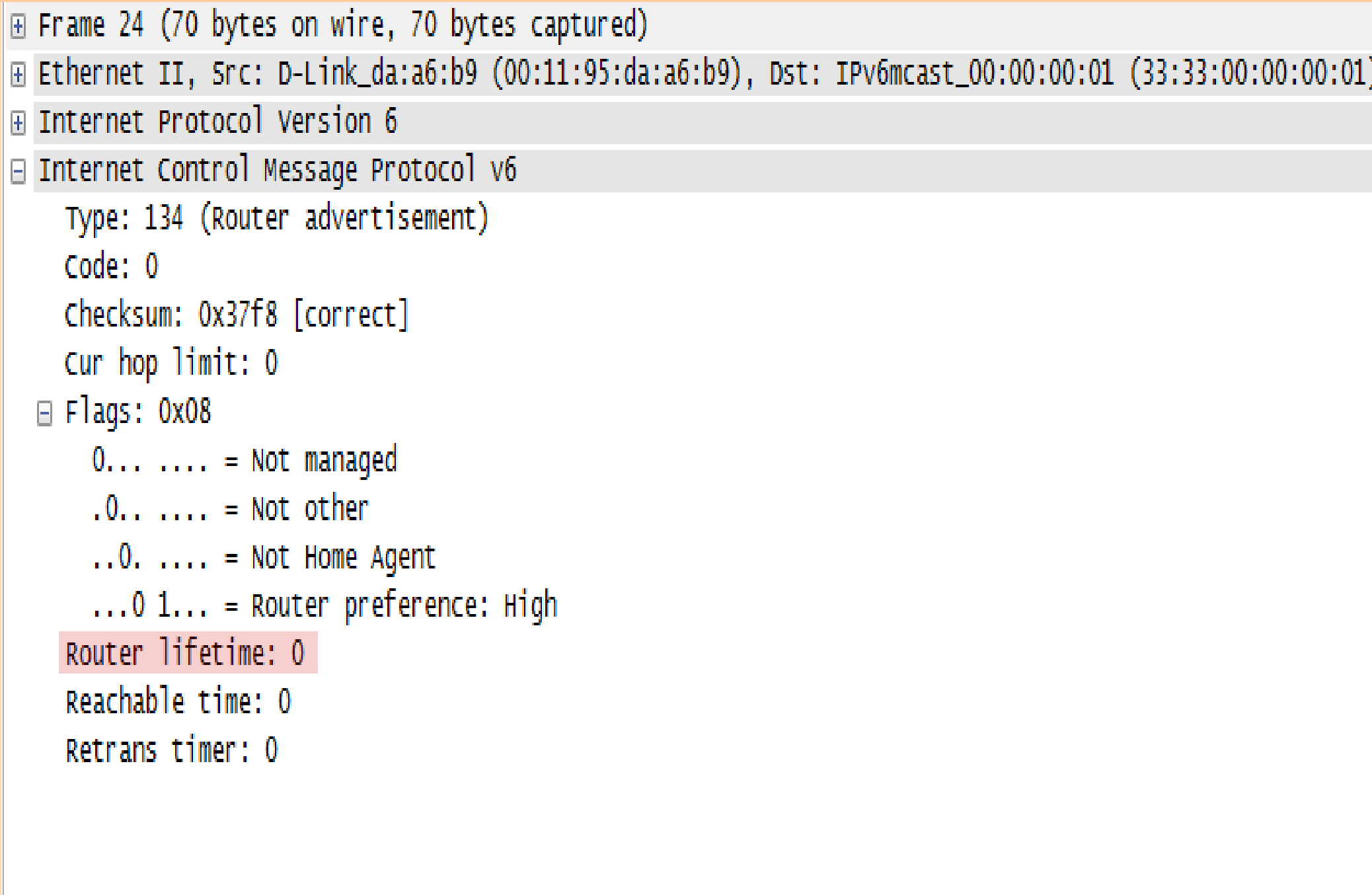
Excerpt from RFC4861

AdvDefaultLifetime

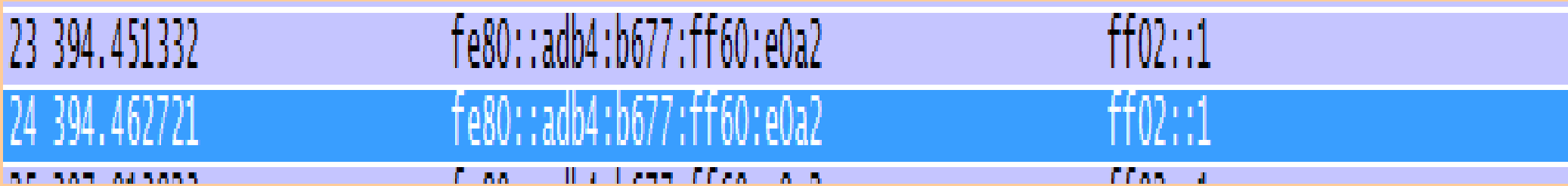
The value to be placed in the Router Lifetime field of Router Advertisements sent from the interface, in seconds MUST be either zero or between MaxRtrAdvInterval and 9000 seconds. A value of zero indicates that the router is not to be used as a default router. These limits may be overridden by specific documents that describe how IPv6 operates over different link layers. For instance, in a point-to-point link the peers may have enough information about the number and status of devices at the other end so that advertisements are needed less frequently.

*Default: 3 * MaxRtrAdvInterval*

A “Sniper” Frame



Timing (about 11 ms turnaround)



scaPy

- Python module
  - Using the interactive mode of Python, looks like an app
- S.A.K. for packet examination, forging, much more potent than using plain raw sockets
- http://www.secdev.org/projects/scapy/

Code

```
#!/usr/bin/env python
from scapy.all import *

def ra_monitor_callback(pkt):
    if ICMPv6ND_RA in pkt and pkt[ICMPv6ND_RA].routerlifetime > 9000:
        send(IPv6(src=pkt[IPv6].src)/ICMPv6ND_RA(routerlifetime=0) )
        u = pkt.sprintf("rogue %Ether.src% %IPv6.src% > %IPv6.dst%
%ICMPv6ND_RA.routerlifetime%")
        s = time.asctime()
        t = "\t"
        return s + t + u

sniff(prn=ra_monitor_callback, filter="dst host ff02::1", store=0,
iface="wlan0")
```

rafixd

- Daemon in C to set `router lifetime` to zero
- Version I found had compile issues
- Comment on IPv6Hawaii.org post points out:
  - http://github.com/strattg/rafixd
  - Which has portability enhancements by Eric Vyncke at **C**isco
    - Might be easier to get compiled