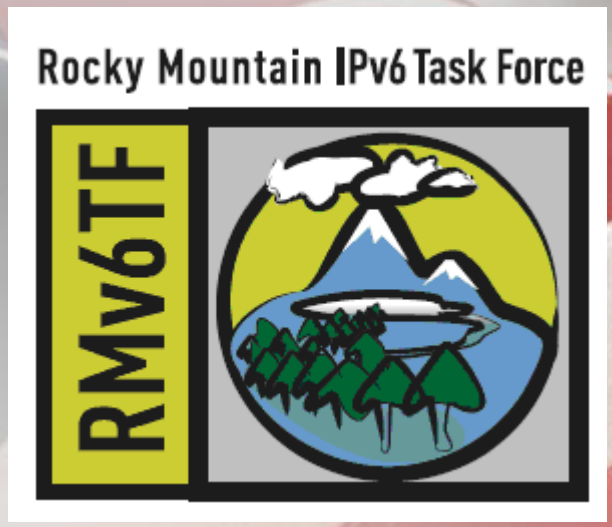
IPv6 Secure Neighbor Discovery (SeND) and CGA

Real-World Enterprise Deployment Scenarios

Jeremy Duncan
IPv6 Network Architect



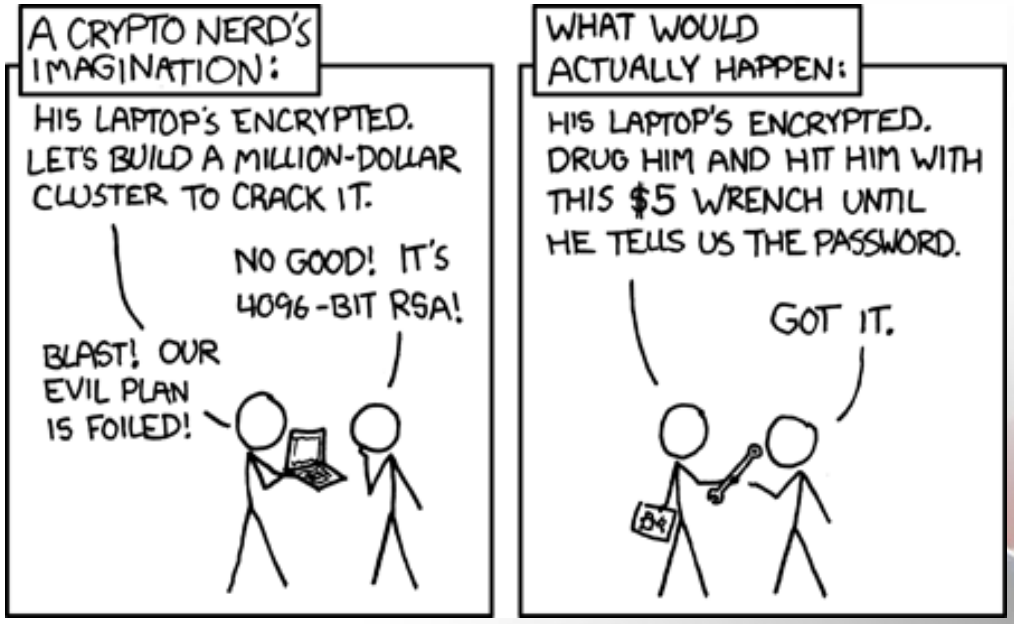
SALIENT
FEDERAL SOLUTIONS

Agenda

- Why do we even need SeND?
- Some other Mitigations
- IPv6 Secure Neighbor Discovery (SeND) Overview
- SeND support on routers
- SeND support on end-points (hosts)
- SeND demo

Why do we even need SeND??

- Neighbor Discovery is in the clear, *trusting* and open
  - All hosts trust each other
  - All hosts trust routers
  - All routers trust hosts
  - How is this different than ARP?? (it's not)



IPv6 Attacks on the Local Segment

- Man-in-the-Middle Attacks during neighbor advertisement/solicitation
  - Parasite6 – THC-IPv6
  - Spoofs every NS sent out by any host

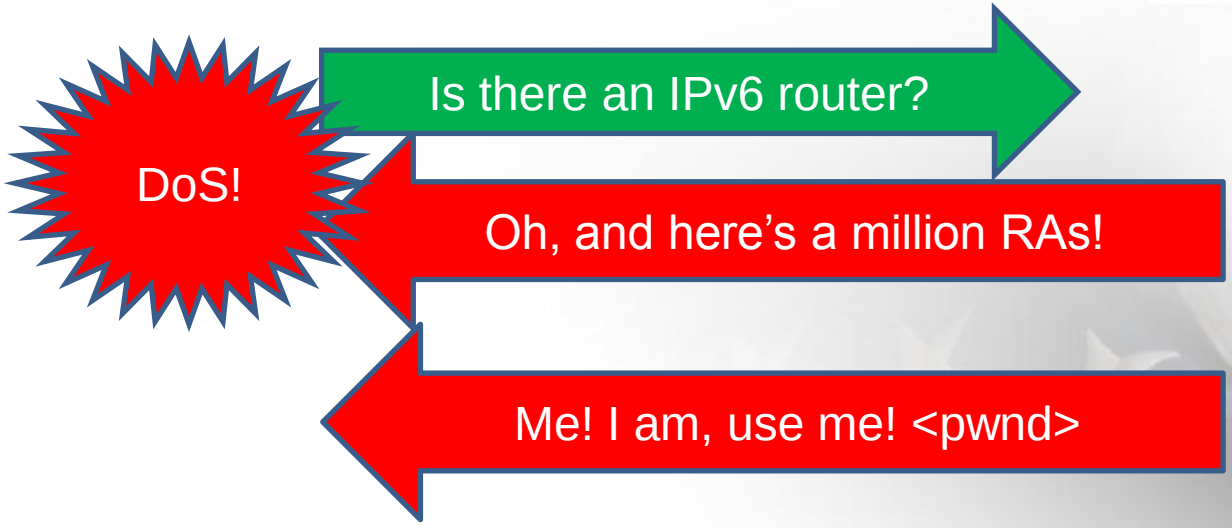
Who has fe80:1:2:3:4?

Ooo! Ooo! That's me!

My IPv6: fe80:1:2:3:4

IPv6 Attacks on the Local Segment, cont

- Denial of Service (DoS) or Session Hijacking using a Rogue Router
  - Fake_router6 and/or flood_router6 – THC-IPv6
  - Acts like a router with highest priority
  - Floods route tables and interface address config

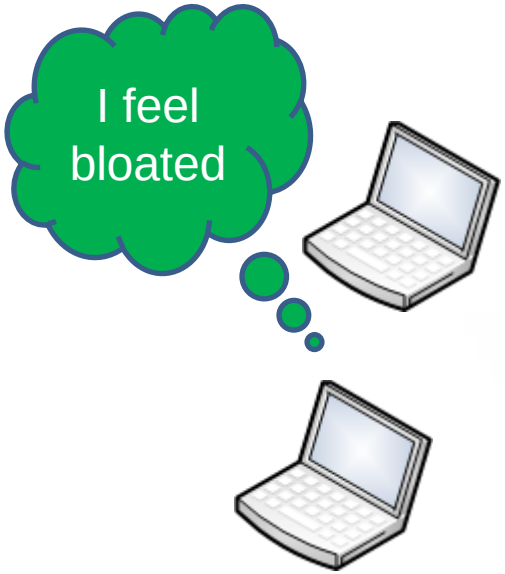


IPv6 Attacks on the Local Segment, cont

- Denial of Service (DoS) with IP conflicts
  - Dos-new-ip6– THC-IPv6
  - Always responds to a Duplicate Address Detection (DAD) with a positive
  - Hosts will never be able to address their link-local or Global address

IPv6 Attacks on the Local Segment, cont

- Denial of Service (DoS) with Neighbor floods
  - Flood_advertise6 – THC-IPv6
  - Floods all hosts on a network with bogus neighbor advertisements
  - Performance on host IPv6 neighbor tables will degrade and cause a DoS



NA for fe80::2

NA for fe80::3

NA for fe80::4 <pwnd>

IPv6 Attacks on the Local Segment, cont

- IPv6 Exploitation and Fuzzing attacks
  - fuzz6, exploit6, denial6 – THC-IPv6
  - Runs a series of fuzzing and link-local exploitation attacks on hosts

IPv6 --- Fuzz! <pwnd>

IPv6 --- Exploit! <pwnd>

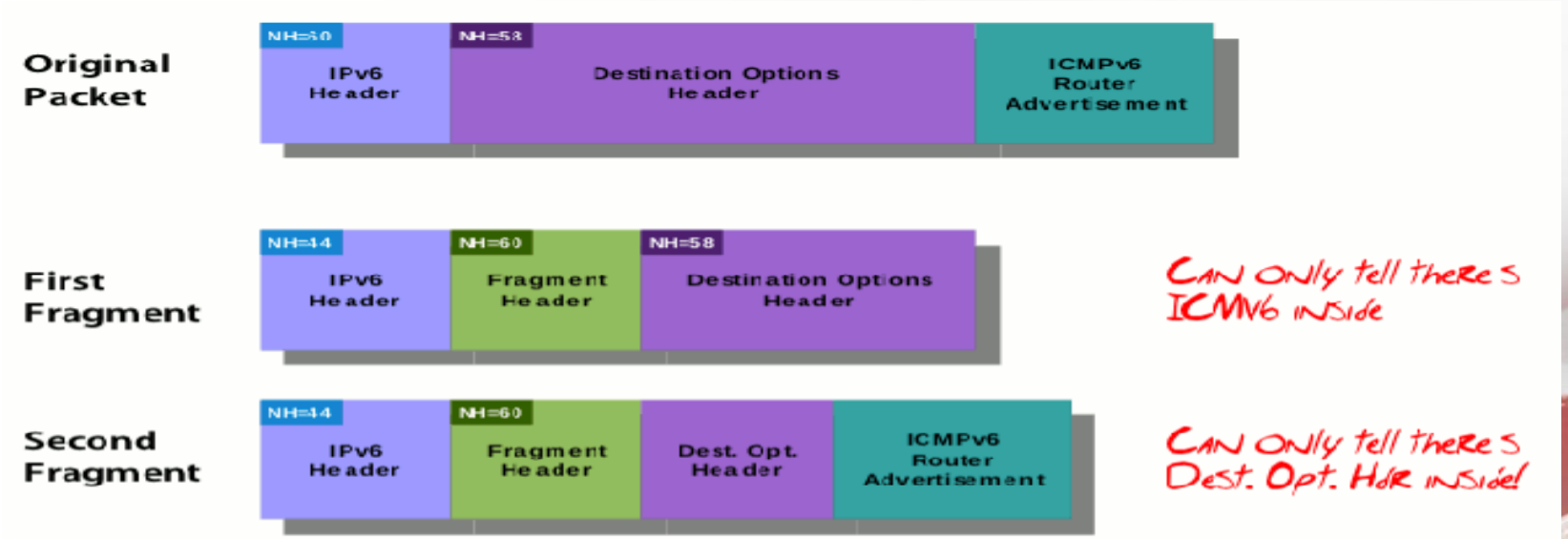
IPv6 --- Deny! <pwnd>

Some other Mitigations other than SeND

- There's always 802.1x
  - Layer 2 authentication only and it only protects once (or upon re-authentication)
  - Layer 2 and 3 addresses are still "in the clear"
  - Usually requires some sort of AAA server
- Router Advertisement Guard (RA Guard)
  - Only protects an interface from a rogue RA, not traffic from NA and NS badness
  - RA Guard implementations are still confused when there are extension headers (see draft-ietf-v6ops-ra-guard-implementation-00)

Some other Mitigations other than SeND

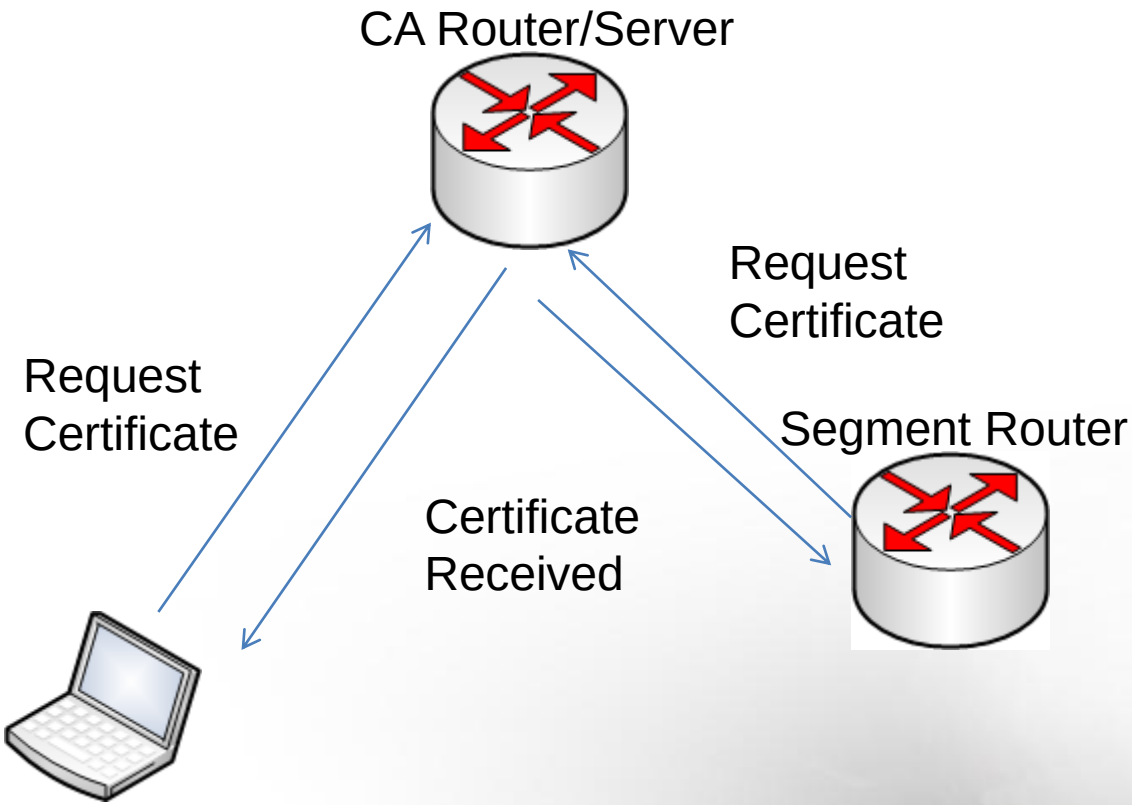
- RA Guard Issues
  - As stated by Fernando Gont, “some implementations of RA-Guard have been found to be prone to circumvention by employing IPv6 Extension Headers”
  - Fragment Header and Destination Options
  - Diagram from Gont below



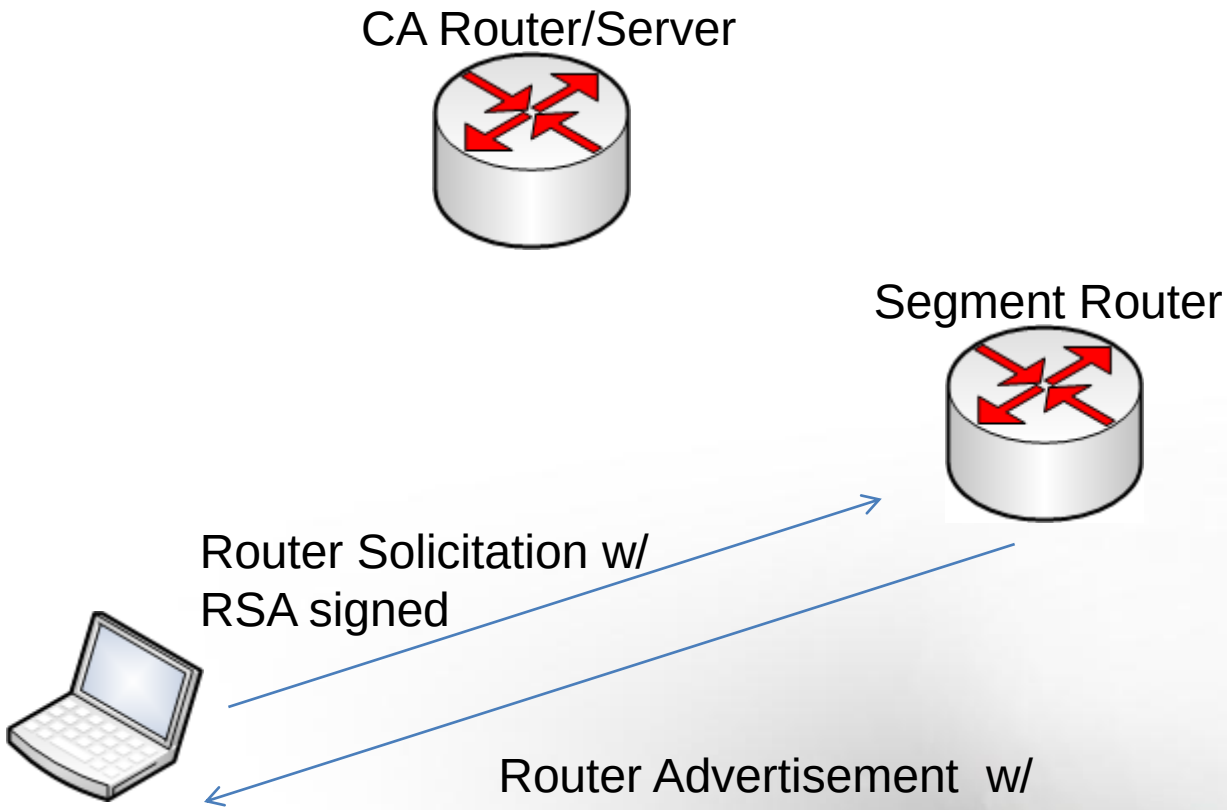
What is SeND?

- A Public-Key Infrastructure (PKI) system implemented with Cryptographically-Generated Addresses (CGA) → RFC 3971 and RFC 3972
  - All host and router link-local and Global Unicast addresses are generated per CGA specification
  - All NDP traffic is CGA signed and authenticated
  - A centralized Certificate Authority (CA) is used (can be a CA on the router or using a Microsoft CA)
  - ICMPv6 Certification Path message added to the mix
  - The NONCE flag is used to protect against DoS from all non-authenticated hosts

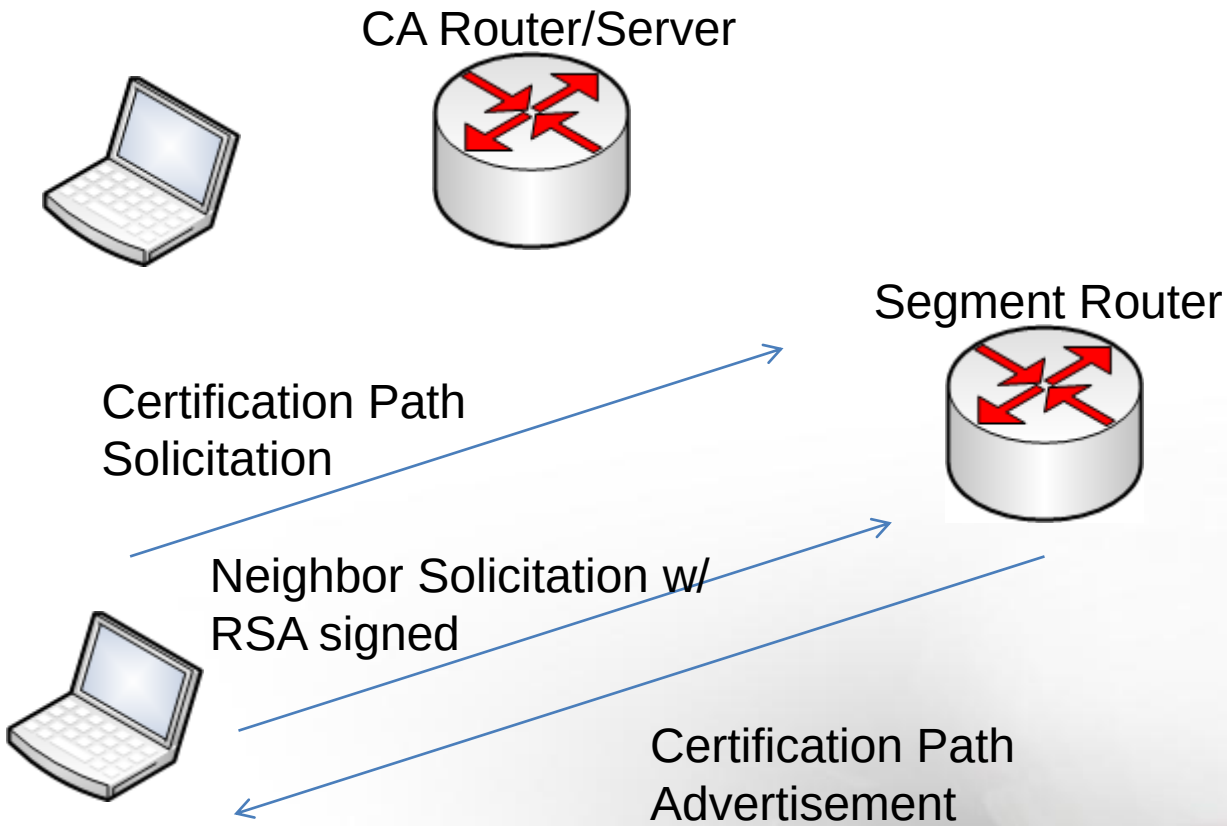
SeND in Real-time



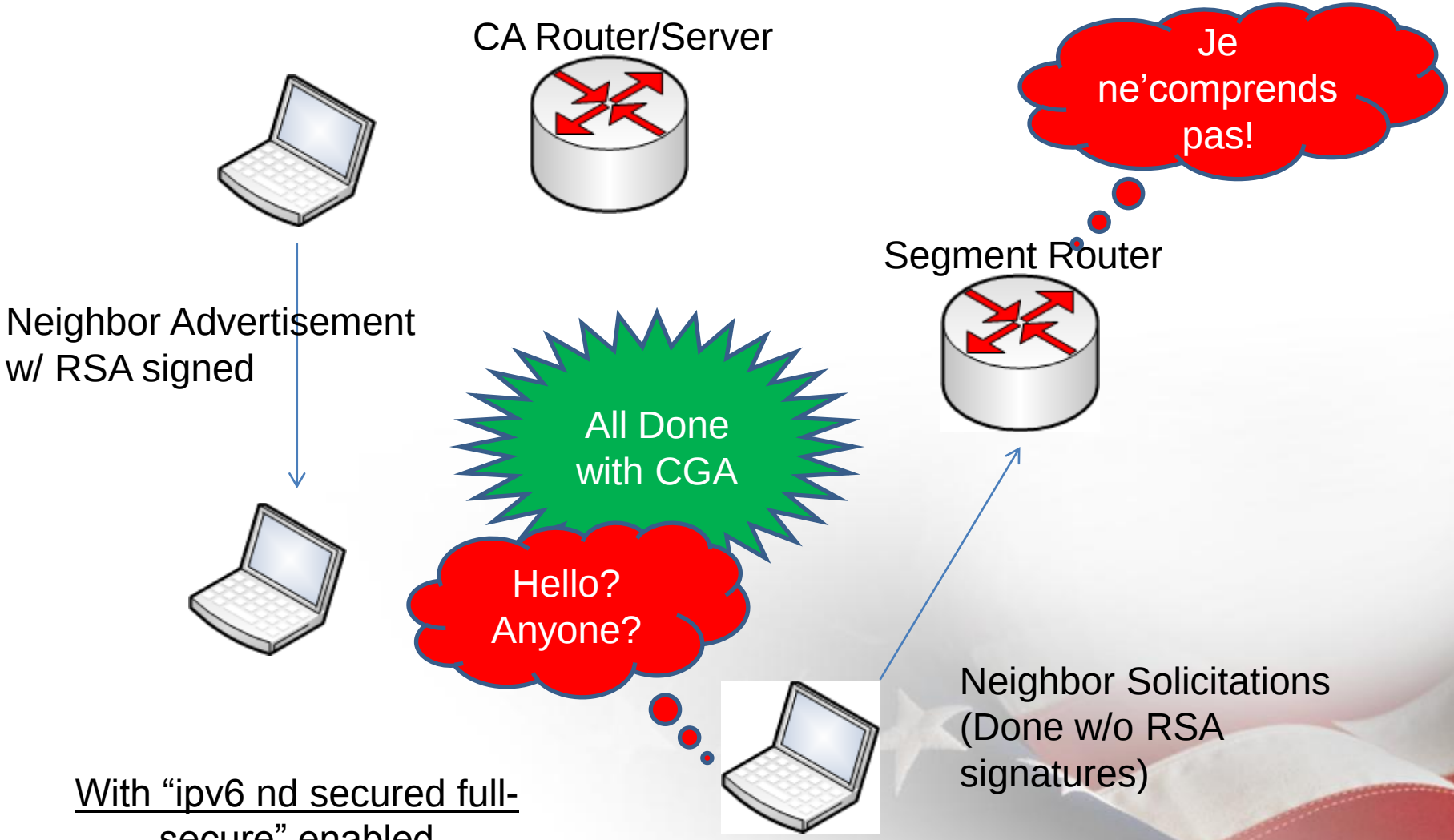
SeND in Real-time



SeND in Real-time



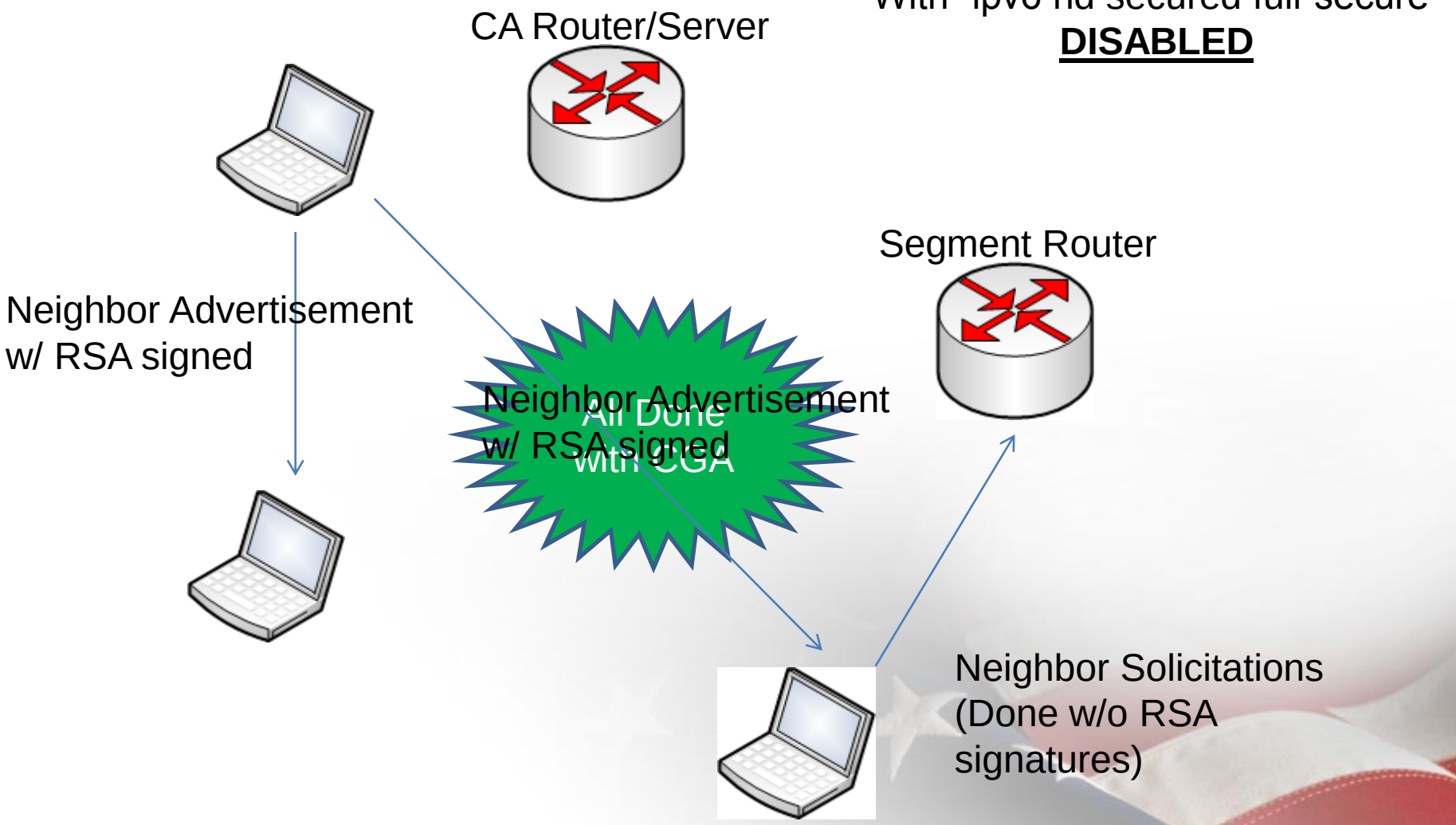
SeND in Real-time



With "ipv6 nd secured full-secure" enabled

SeND in Real-time

With “ipv6 nd secured full-secure”
DISABLED



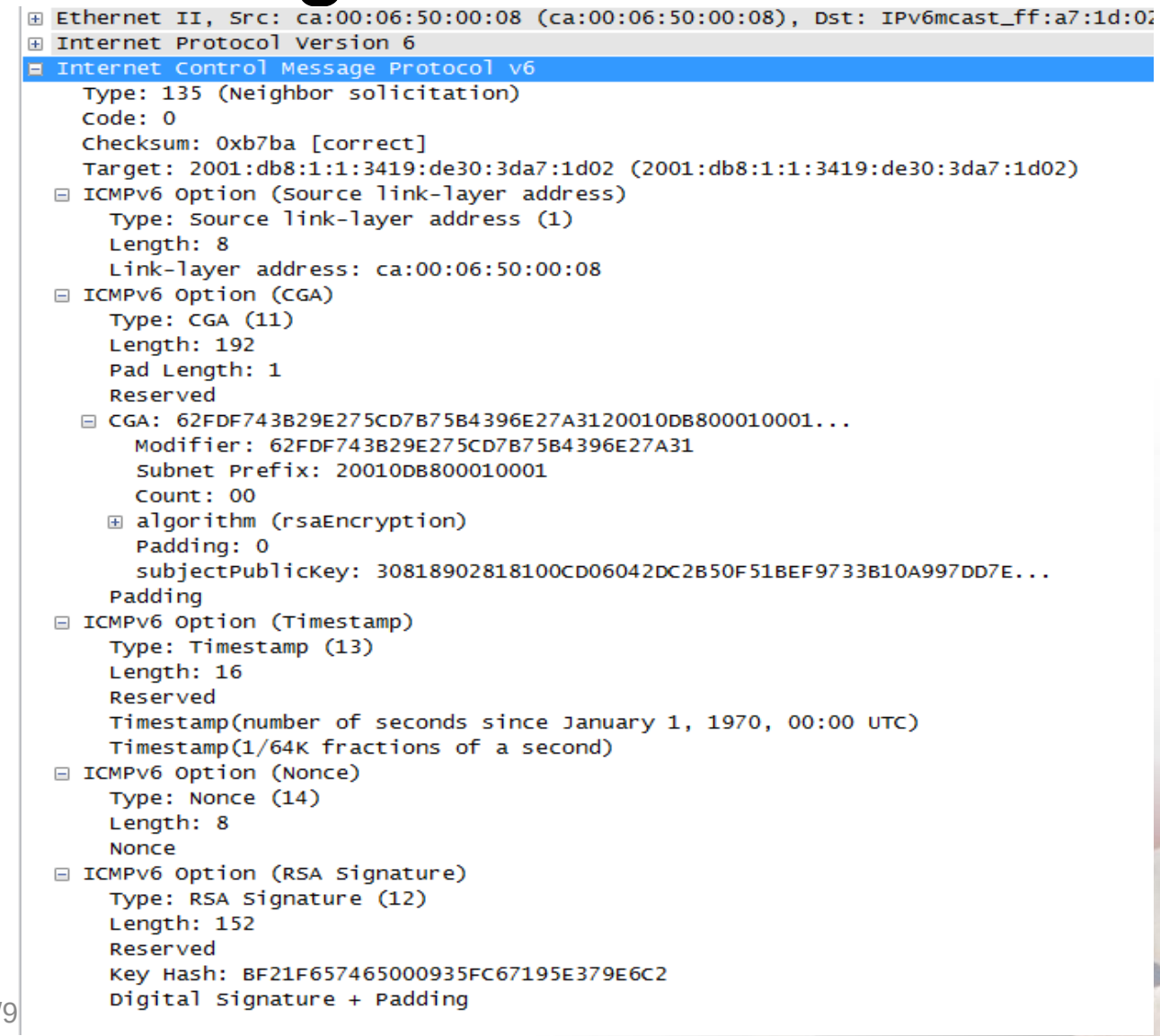
SeND and CGA Packets

- Router Advertisements/Solicitations
- Neighbor Advertisements/Solicitations
- ICMPv6 Certification Path Advertisements/Solicitations

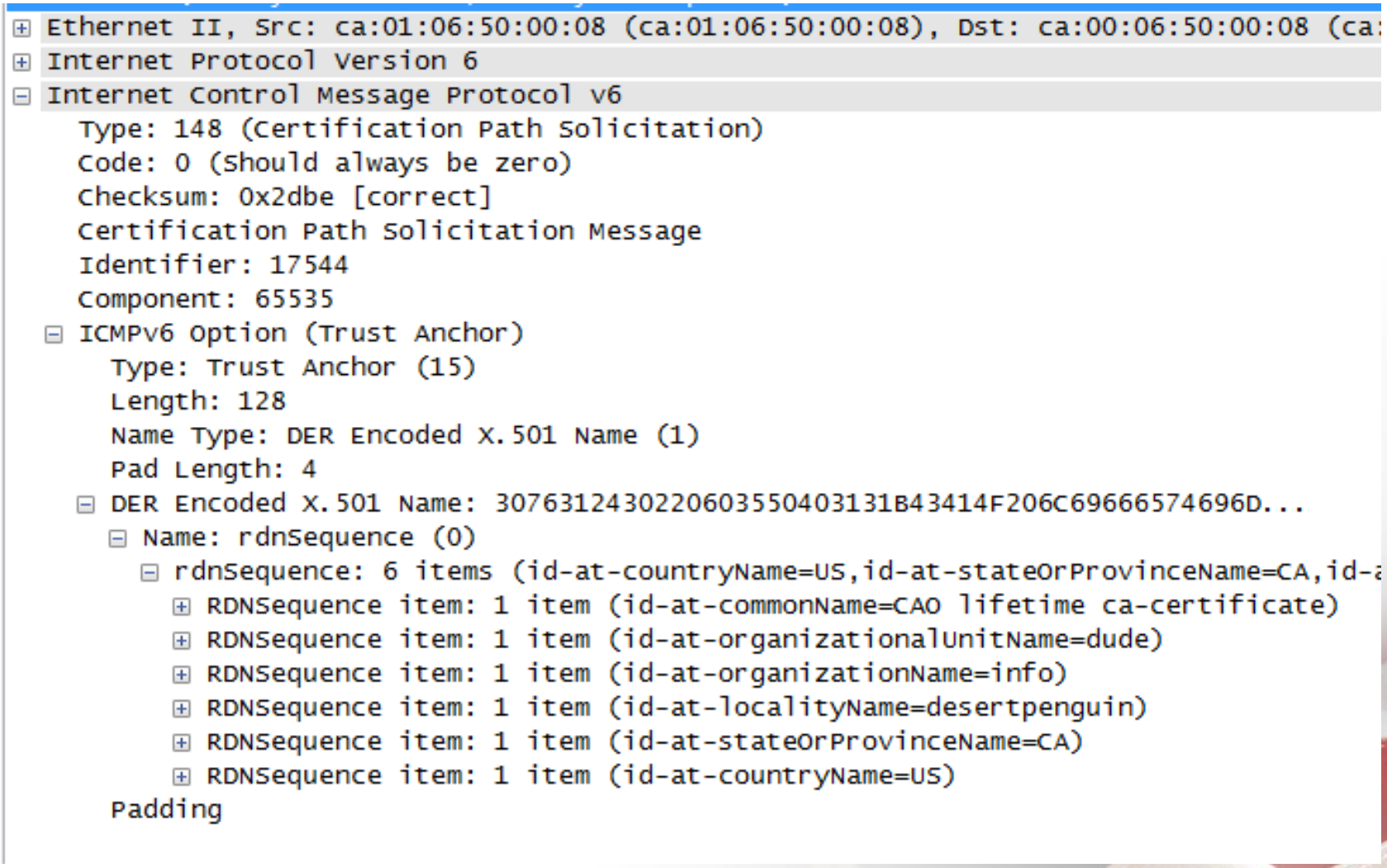
SeND Router Solicitations/Advertisements

```
⊞ Ethernet II, Src: ca:00:06:50:00:08 (ca:00:06:50:00:08), Dst: IPv6mcast_00:00:00:0
⊞ Internet Protocol Version 6
⊟ Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0xd1b1 [correct]
    Cur hop limit: 64
  ⊞ Flags: 0xc0
    Router lifetime: 1800
    Reachable time: 0
    Retrans timer: 0
  ⊞ ICMPv6 Option (Source link-layer address)
  ⊞ ICMPv6 Option (MTU)
  ⊞ ICMPv6 Option (Prefix information)
  ⊟ ICMPv6 Option (CGA)
      Type: CGA (11)
      Length: 192
      Pad Length: 1
      Reserved
    ⊟ CGA: 62FDF743B29E275CD7B75B4396E27A31FE80000000000000...
        Modifier: 62FDF743B29E275CD7B75B4396E27A31
        Subnet Prefix: FE80000000000000
        Count: 00
      ⊞ algorithm (rsaEncryption)
        Padding: 0
        subjectPublicKey: 30818902818100CD06042DC2B50F51BEF9733B10A997DD7E...
      Padding
  ⊟ ICMPv6 Option (Timestamp)
      Type: Timestamp (13)
      Length: 16
      Reserved
      Timestamp(number of seconds since January 1, 1970, 00:00 UTC)
      Timestamp(1/64K fractions of a second)
  ⊟ ICMPv6 Option (RSA Signature)
      Type: RSA Signature (12)
      Length: 152
      Reserved
      Key Hash: BF21F657465000935FC67195E379E6C2
      Digital Signature + Padding
```

SeND Neighbor Solicitation



SeND Certification Path Solicitations/Advertisements



SeND Neighbor Advertisement

```
⊞ Ethernet II, Src: ca:01:06:50:00:08 (ca:01:06:50:00:08), Dst: ca:00:06:50:00:08 (ca:0
⊞ Internet Protocol Version 6
⊟ Internet Control Message Protocol v6
    Type: 136 (Neighbor advertisement)
    Code: 0
    Checksum: 0xd1aa [correct]
  ⊞ Flags: 0x60000000
    Target: 2001:db8:1:1:3419:de30:3da7:1d02 (2001:db8:1:1:3419:de30:3da7:1d02)
  ⊟ ICMPv6 Option (Target link-layer address)
      Type: Target link-layer address (2)
      Length: 8
      Link-layer address: ca:01:06:50:00:08
  ⊟ ICMPv6 Option (CGA)
      Type: CGA (11)
      Length: 192
      Pad Length: 1
      Reserved
    ⊟ CGA: D00BB319C295B8D73FD44A92DA70271420010DB800010001...
        Modifier: D00BB319C295B8D73FD44A92DA702714
        Subnet Prefix: 20010DB800010001
        Count: 00
      ⊞ algorithm (rsaEncryption)
        Padding: 0
        subjectPublicKey: 30818902818100B26E6E051BE2976A68AD2D2FF129B9DA37...
      Padding
  ⊟ ICMPv6 Option (Timestamp)
      Type: Timestamp (13)
      Length: 16
      Reserved
      Timestamp(number of seconds since January 1, 1970, 00:00 UTC)
      Timestamp(1/64K fractions of a second)
  ⊟ ICMPv6 Option (Nonce)
      Type: Nonce (14)
      Length: 8
      Nonce
  ⊟ ICMPv6 Option (RSA Signature)
      Type: RSA Signature (12)
      Length: 152
      Reserved
      Key Hash: D8E3792F757C4878BFCEED22C517EBDD
      Digital Signature + Padding
```

SeND support on Routers

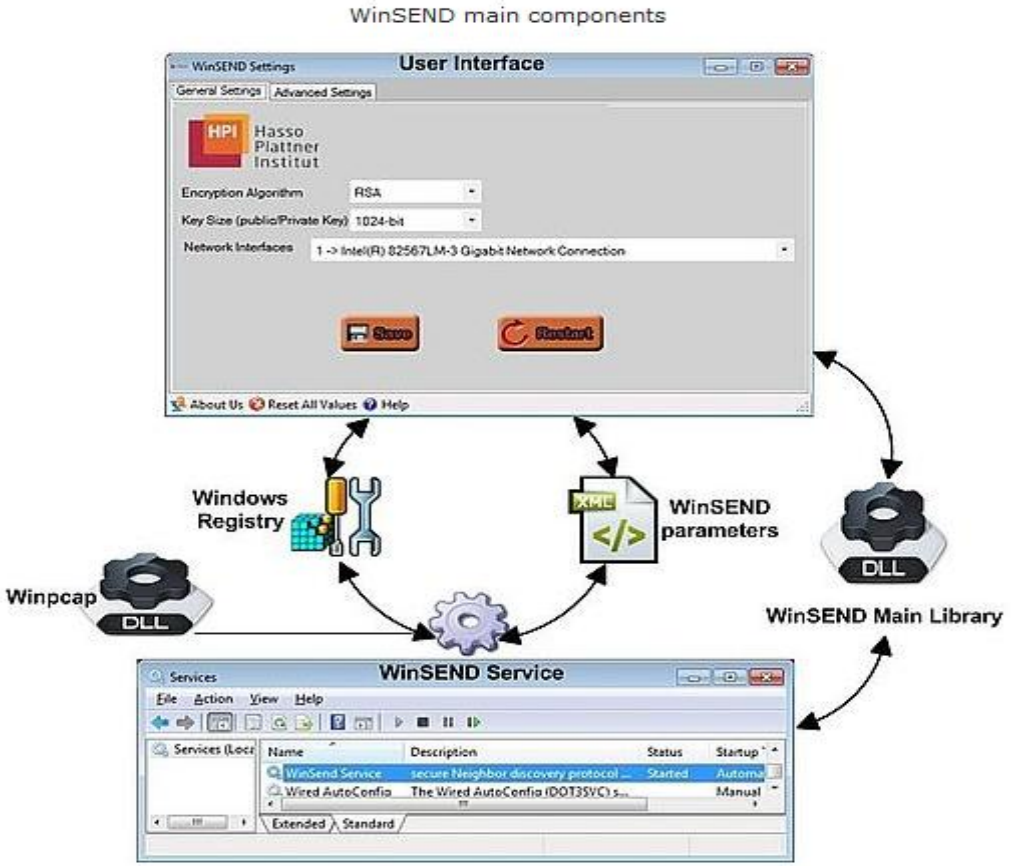
- Cisco support for SeND, CGA and Certificate Authority with IP-extensions
  - IOS 12.4-24(T) +
    - Caveat!! → Only on T and M trains on ISR routers
    - Another Caveat!! → **NO SUPPORT** on **new** ASR router platforms! (please complain here)
- Juniper JUNOS support
  - Yes, deployable across JUNOS 9.3+ see here
- HP Procurve support (A & E series)
  - None
- Huawei Technologies
  - Support using ipv6-send-cga Linux package (http://code.google.com/p/ipv6-send-cga/)
- Brocade
  - None that I know of

SeND support on Hosts

- Microsoft Windows 7 or Server 2008
  - None natively ← Complain here
  - TrustRouter application Win7-32bit - RAs (no support for NA/NS)
  - WinSEND application works with all NDP traffic
    - Won the German IPv6 Council Application Award for 2011
- Apple Macintosh
  - None natively← Complain here
  - TrustRouter application for Mac OS X - RAs (no support for NA/NS)
- Linux and/or Unix
  - Easy-SEND http://sourceforge.net/projects/easy-send
  - ND-Protector http://amnesiak.org/NDprotector
  - IPv6-Send-CGA http://code.google.com/p/ipv6-send-cga

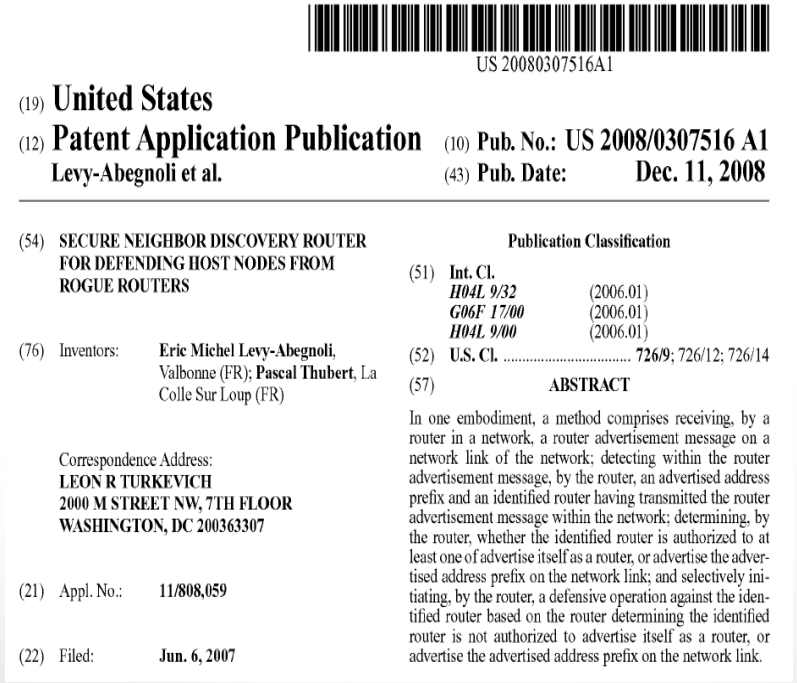
WinSEND

- Application runs as a service, with a management interface
- Licensed from HPI in Germany



Current issues with SeND

- A Patent exists (US 2008/0307516 A1)
- Certificate expirations
  - Can be 1 year
  - Difficult to maintain if not doing auto-enrollment
- Little client saturation
  - Linux support (e.g. Easy-SEND)
  - Win 7 (e.g. WinSEND)
- Dynamic DNS (for CGA addressing) impacts unknown
  - Microsoft has CGA addressing for DHCPv6 w/ Dynamic DNS
- SeND support on mobile & VoIP platforms non-existent



US 20080307516A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2008/0307516 A1**

Levy-Abegnoli et al. (43) **Pub. Date: Dec. 11, 2008**

(54) **SECURE NEIGHBOR DISCOVERY ROUTER FOR DEFENDING HOST NODES FROM ROGUE ROUTERS**

(76) Inventors: **Eric Michel Levy-Abegnoli**, Valbonne (FR); **Pascal Thubert**, La Colle Sur Loup (FR)

Correspondence Address:
LEON R TURKEVICH
2000 M STREET NW, 7TH FLOOR
WASHINGTON, DC 200363307

(21) Appl. No.: **11/808,059**

(22) Filed: **Jun. 6, 2007**

Publication Classification

(51) **Int. Cl.**
H04L 9/32 (2006.01)
G06F 17/00 (2006.01)
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **726/9**; 726/12; 726/14

(57) **ABSTRACT**

In one embodiment, a method comprises receiving, by a router in a network, a router advertisement message on a network link of the network; detecting within the router advertisement message, by the router, an advertised address prefix and an identified router having transmitted the router advertisement message within the network; determining, by the router, whether the identified router is authorized to at least one of advertise itself as a router, or advertise the advertised address prefix on the network link; and selectively initiating, by the router, a defensive operation against the identified router based on the router determining the identified router is not authorized to advertise itself as a router, or advertise the advertised address prefix on the network link.

Well, is it Deployable in the Enterprise?

- Short Answer → Yes!
- Long answer → Yes, but follow our guidance:
  - Be mindful of your CA (e.g. when certs expire)
    - We recommend 3 years for certs, but if you insist on 1 year you better have a process!
  - Monitor SeND and CGA failures and/or issues using SNMP Traps
  - Recommend having a “safe-zone” for a SeND disaster scenario (if doing “full secure mode”)
    - A locked room with an interface attached to the local segment router with no 802.1x or SeND

Now for the Demo!

- All virtual → VirtualBox
  - Ubuntu 11.04 with Dynamips and Dynagen
  - Segment Router: Cisco 7206 router with IOS 12.4-24(T)
  - CA Router: Cisco 7206 router with IOS 12.4-24(T)
  - A simulated host (Cisco router)
  - Ubuntu Linux host without SeND running

Questions?

www.SalientFed.com

SALIENT
FEDERAL SOLUTIONS

Resources

- Cisco's IPv6 First Hop Security Page: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html

- IPv6 SeND Wikipedia: http://en.wikipedia.org/wiki/Secure_Neighbor_Discovery_Protocol

www.SalientFed.com

SALIENT
FEDERAL SOLUTIONS