IPv6

Common Vulnerabilities & Countermeasures

Thierry Zoller
Practice Lead EMEA / Threat and Vulnerability
May 20, 2011

Agenda

- **Who am I**
  - Zoller Thierry
  - Professional Services / Practise Lead EMEA

- **Agenda – Scope: Enterprise**
  - Crash course / Fundamental Changes
  - Vulnerabilities and Countermeasures
  - Changes to the Threat Landscape
  - Best Practises
  - Summary
  - Q&A

Who in the audience has IPv6 “activated” inside your corporate LAN at this moment ?

Quick Refresh on Changes

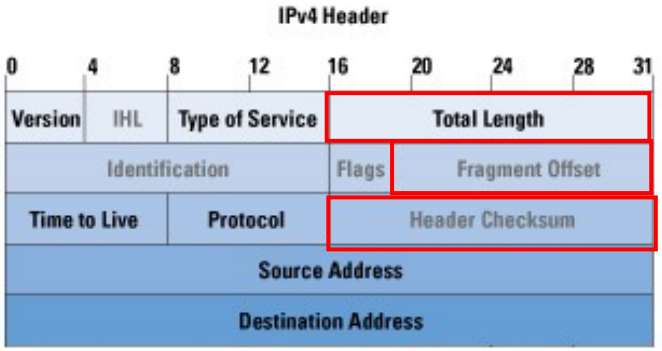
Primary changes

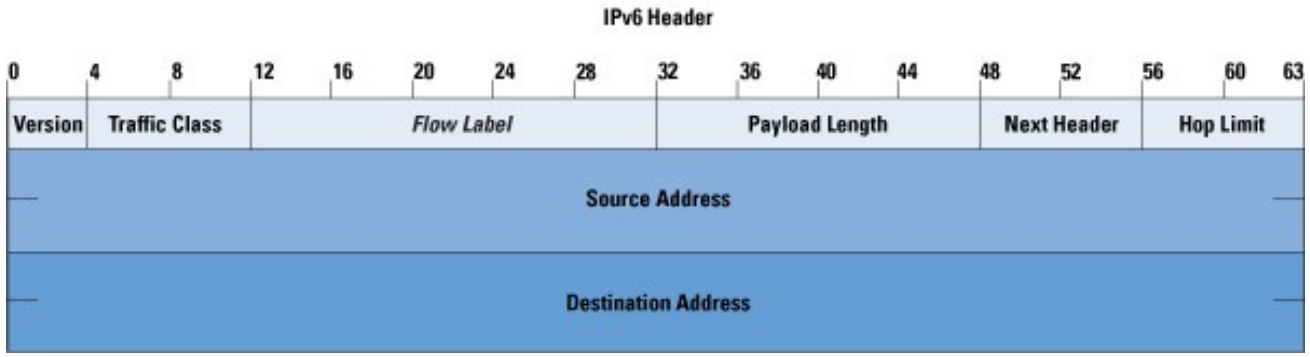
- **IPv4**
  - 4 Octets / 32 Bit addressing
    - 4.294.967.296 addresses
    - Example : 192.168.1.1
  - DHCP / Broadcast
  - Broadcast
  - IPSEC hacked into

- **IPv6**
  - 16 Octets / 128 bit addressing
    - 340.282.366.920.938.463.463.374.607.431.768.211.456 Addresses
    - Example: 2a01:2b3:4:a::1
  - Stateless Auto Configuration (ICMP)
  - Flexible Multicast (Groups) – Local only
  - Mobility – keeps connections when moving locations
  - IPSEC build into (mandatory)
  - Routers no longer fragment

- **Typical Subnet : /64**
  - 4.294.967.296 * Size of the Internet (2^64 = 18.446.744.073.709.551.616)
  - Implications on “ping sweeps”
  - (roughly dumb scans could take years to finish)

The Basics
IP Header



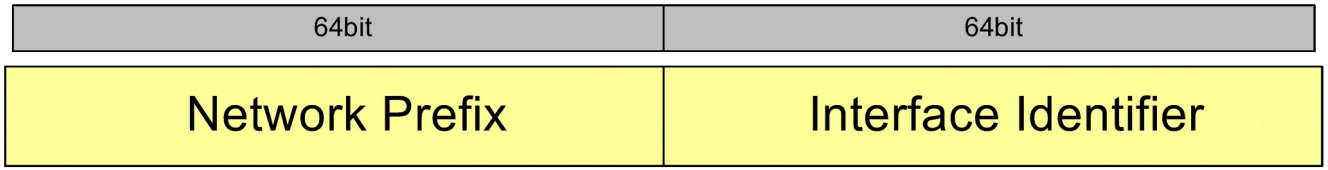


- No Header Length
- No IPID
- No Checksum
- No Fragmentation field
- No Options

Source: Cisco

The Basics
Unicast IPv6 Address

- **IPv6 IP Address**



Used for routing

Advertised by the Router

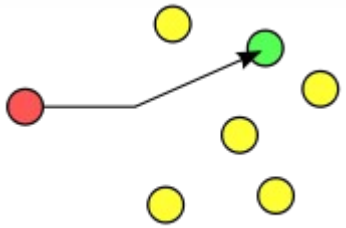
Local Identifier

- SLAAC (EUI-64) RFC 4291
- DHCP
- Automatic Random (Privacy Extensions
- Assigned Manual

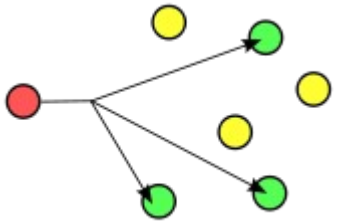
The Basics

Multicast / Anycast / Unicast

- **Unicast**
  - One destination



- **Multicast**
  - All routers [FF02:0:0:0:0:0:0:2] Node-Local
  - All DHCP servers [FF05:0:0:0:0:0:1:3] Link-Local



- **Anycast - (All nodes in Subnet)**
  - "An IPv6 anycast address is an address that is assigned to more than one interface (typically belonging to different nodes), with the property that a packet sent to an anycast address is routed to the "nearest" interface having that address, according to the routing protocols' measure of distance. " RFC4291

IPv6 LAN

Procotol changes, Attacks & Countermeasures

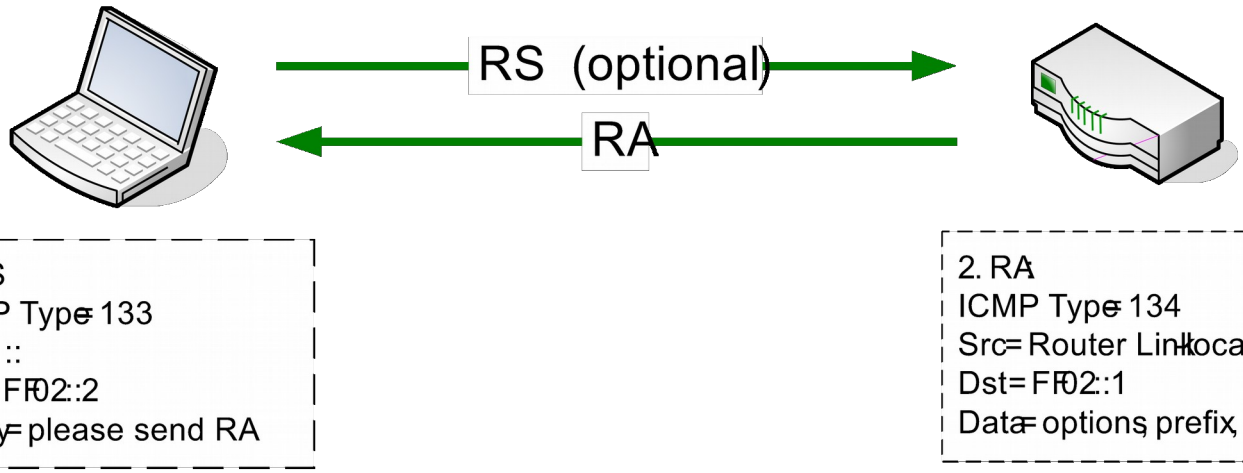
State of independent security research

- Has attracted interest from the Hacking community in the recent years
- First dedicated Attack Toolkit released in 2005 (“THC IPv6 Attack Toolkit”)
- General Tools available (scapy etc.)
- IPv6 used in Databreaches in early 2002 to camouflage traffic (lack of inspection - more on that later)

Changes

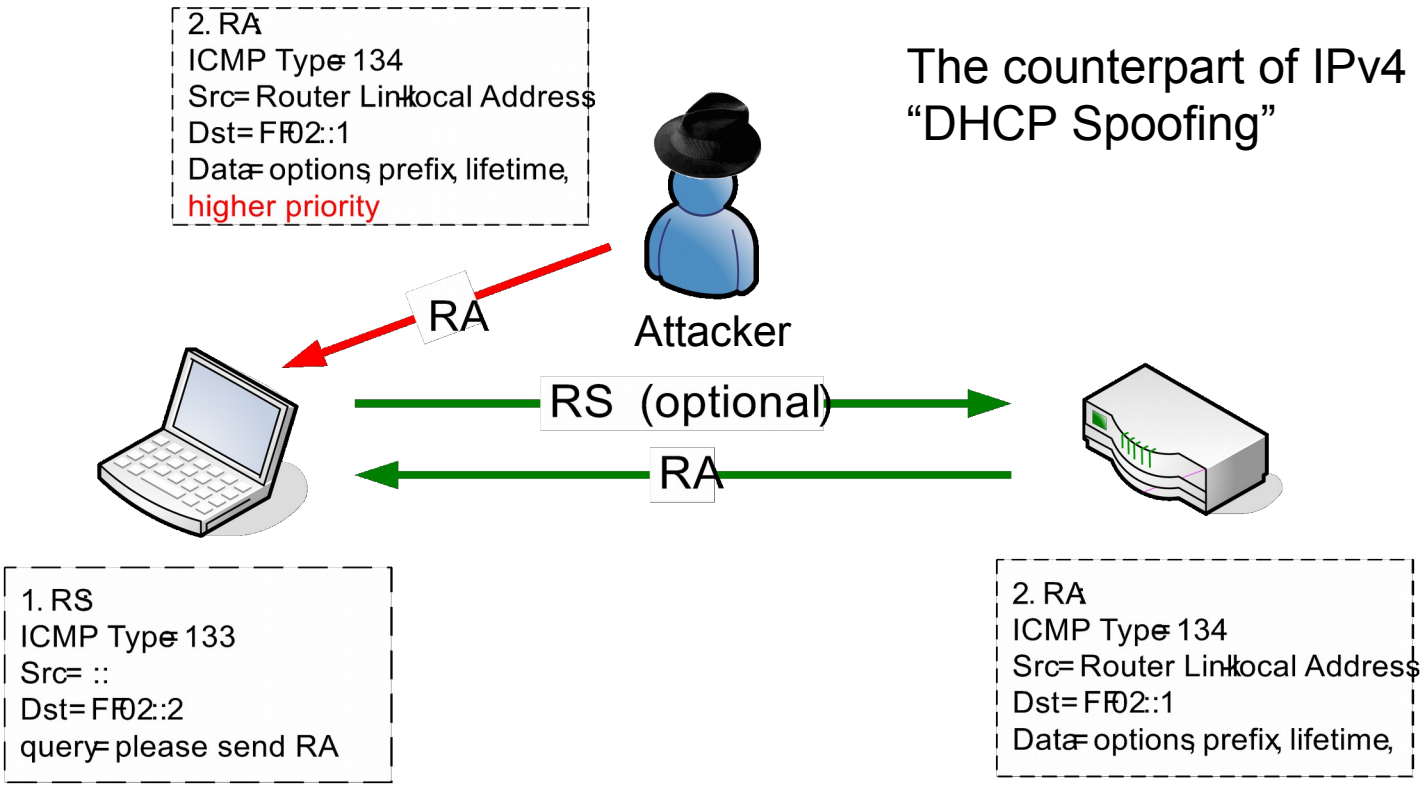
Stateless Configuration

- **IPv4 – DHCP / Broadcast**
  - " I am new give me an IP address !" (Broadcast)
  - " I am your DHCP server here is the info"
- **IPV6 – ICMPv6 / Multicast / (DHCP Optional)**
  - Clients set their routing table and network prefix based on "Router Advertisements" (RA)
    - » Either through RA announcements or RS request



Attack

Stateless Configuration



Countermeasures

Stateless configuration

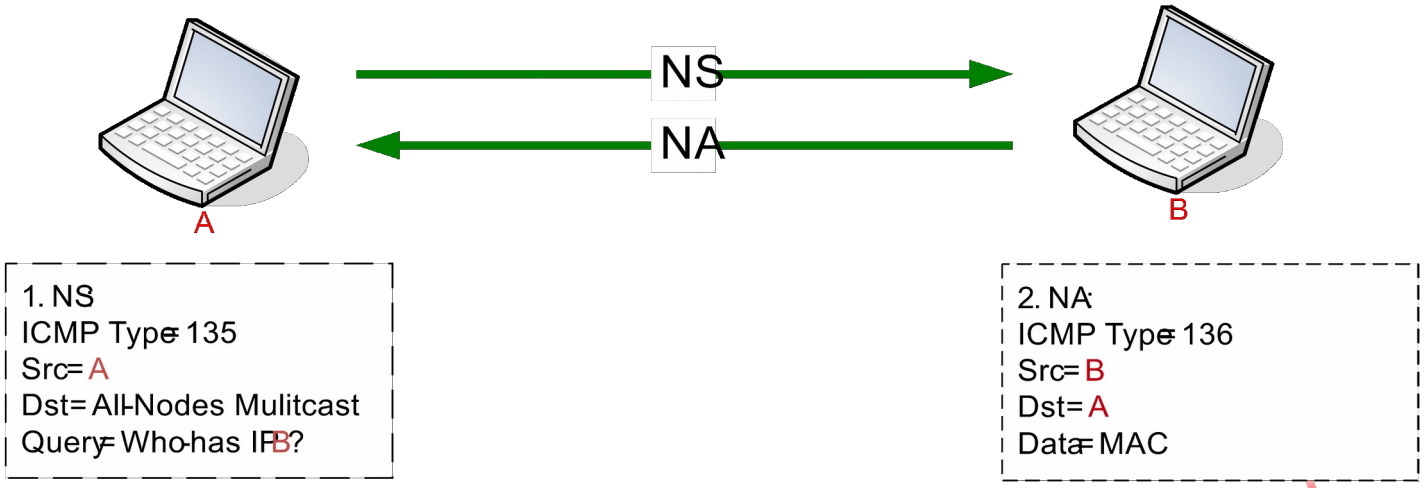
- **ACL on managed switches (RA not allowed on all Ports)**
  - **Drop all RA messages sent from a nontrusted port (ICMPv6 type 133)**
- **Port Security**
- **IPSEC**
- **Monitoring and Alerting**
- **NAC**

Changes

ARP / NDP

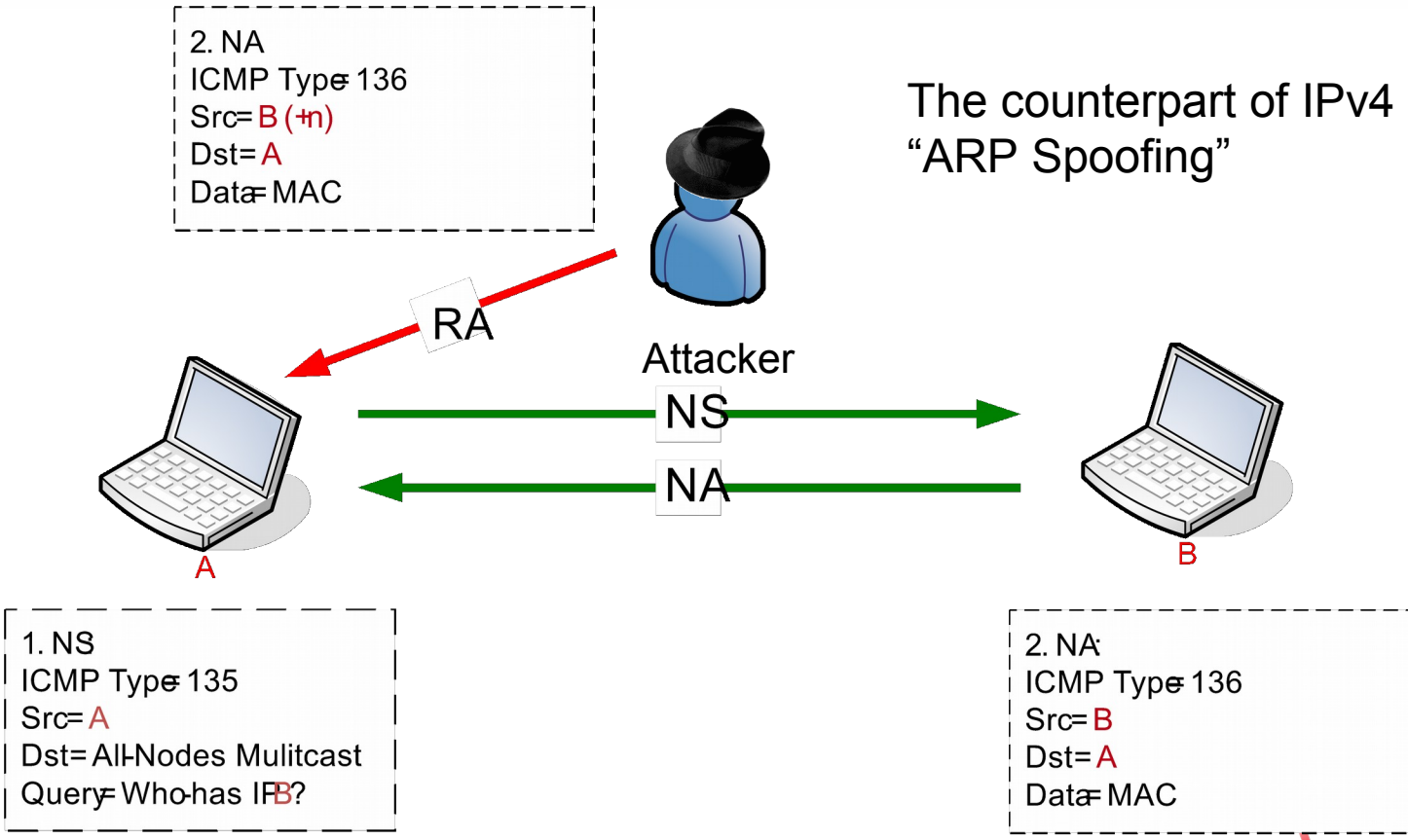
- **IPv4 – ARP**
  - **Who has 192.168.1.1**
  - **I have and my MAC is 00:DE:AD:BE:EF:00**

- **IPV6 – NDP - ICMPv6 (ARP is dead – long live ICMPv6)**



Attack

NDP


2. NA
ICMP Type= 136
Src= B (+n)
Dst= A
Data= MAC
The counterpart of IPv4
“ARP Spoofing”
RA
Attacker
NS
NA
A
B
1. NS
ICMP Type= 135
Src= A
Dst= All-Nodes Mulitcast
Query= Who-has IP B?
2. NA
ICMP Type= 136
Src= B
Dst= A
Data= MAC

Countermeasures

NDP

Secure Neighbor Discovery
- **SEND = NDP + crypto**
- **IOS 12.4(24)T (advanced enterprise)**
- **Microsoft 7, 2008 support and later only ☹**

Others :
- **Private VLAN works with IPv6**
- **Port security**

Summary

Quick rundown

Unless IPSEC is consistently used

- Nearly all classical IPv4 vulnerabilities are present in IPv6
- Most of them have similar countermeasures

IPv4	IPv6	Mitigated by IPSEC
Source Routing	Source Routing / RH0	No
ICMP redirect	ICMP redirect	Yes
DHCPv4 Spoofing	DHCPv6 Spoofing	Yes
ARP Spoofing	NDP Spoofing	Yes (or SEND)
DoS / Smurf	DoS / Smurf	Some

- IPv6 per default is a tad bit more secure IPv4
  - »Lack of IPv6 knowledge, experience and hardware is the issue (F.U.D)
  - »Common Counter Measures exist for all of the above

IPv6 LAN

General Weaknesses and BCP

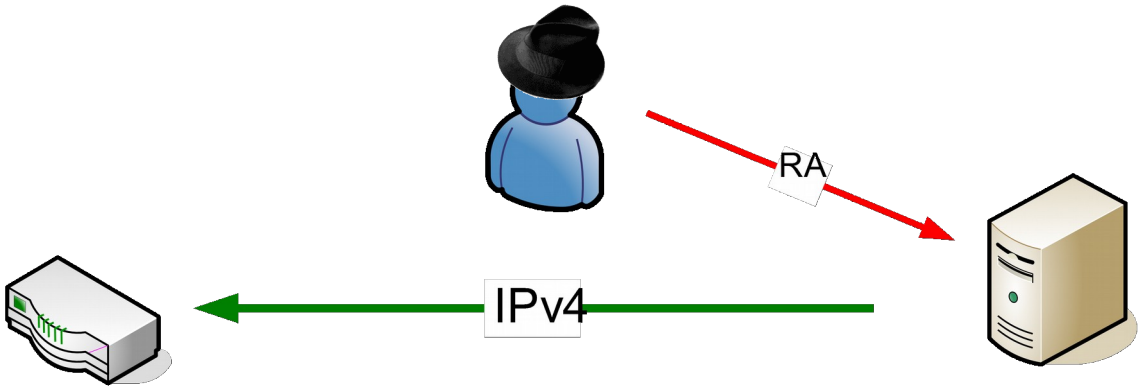
General Weaknesses

“Hidden” IPv6 capabilities

Waking the sleeping giant

- 1. All major OS have default IPv6 support built into (BSD, Linux, Vista, ..)
- 2. IPv6 is prefered over IPv4 per Default (most)

What if we announce a IPv6 Router on a IPv4 Network ?



If attacker does 6to4 it’s possible to exfiltrate Data

IPv4 connected
IP: 192168.1.1

IPv6 activates
Takes routing prefix
Routes all Data through attacker

General Weaknesses

Dual Stack

Worse

- **While creating firewall entries it is often forgotten to set IPv6 ones**
  - Afterall we are not using IPv6 ..
  - Complete unfirewalled access to host

- **General DUAL stack issue**

General Weaknesses

"Hidden" IPv6 capability

Are you still sure you have no IPv6 on your Network ?

- NetFlow records
  - **Protocol 41: IPv6 over IPv4 or 6to4 tunnels**
  - **IPv4 address: 192.88.99.1 (6to4 anycast server)**
  - **UDP 3544, the public part of Teredo, yet another tunnel**
- Check DNS server log for resolution of ISATAP
- Update Default Host Builds to take into account IPv6
  - Check others

Latent Threat :
IPv4-only network may be vulnerable to IPv6 attacks right now

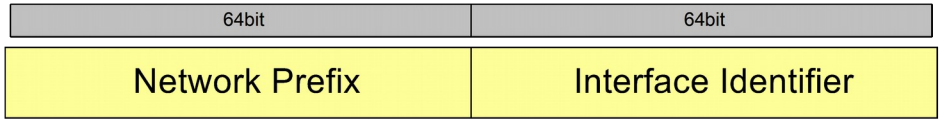
IPv6

Changes to the Threat Landscape

IPv6

Changes to the Threat Landscape

- **Large Addressing Space – "Impossible" to scan ?**
- **Depends**
  - Local : Using multicast and NDP will give you all the addresses. While you can filter ECHO_Request, you can't filter replies to PackettoBig, Missing Extensions, Fragments etc. -> Scanning localy is easy.
  - Internet
    - » DNS – gives a way a lot – minimum one Network prefix
    - » How hard it is depends on Numbering Logic - (Random, DHCP (incremental), SLAAC, Manual)
    - » Random attribution = Hard to maintain / Operational Overhead
    - » IF SLAAC is used keyspace can be reduced to 24bits on entropy (There are only 15000 registered OUI and 100 used a lot, which are part of the MAC which is part of the EUI-64, which is part of the Interface Identifier)
  - It is more difficult, but depending on the Numbering setup and the Methodology of the Attacker – feasable if no other countmeasures present (throttling, blocking)



IPv6

Changes to the Threat Landscape

- **Worms (Like slammer, likely be a thing of the past)**
  - Although new ways likely (P2P)
- **Does not mitigate any sorts of Web application vulnerabilities**
- **E-mail Threats , Social Media etc.**

- Sniffing
  - **Without IPSec, there is no difference between IPv6 or IPv4**
- Rogue devices
  - **No Difference**
- Man-in-the-Middle Attacks (MITM)
  - **Without IPSec, same problems.**
- Flooding
  - **Flooding attacks are identical**

IPv6

Best Practises

IPv6

Best Practices

Source Routing
- **Block Routing Header type 0**
- **Intermediate nodes :**
  - **no ipv6 source-route**
- **Edge**
  - **With an ACL blocking routing header**

DHCP Spoofing
- **Port ACL can block DHCPv6 traffic from client ports**
  - deny udp any eq 547 any eq 546

General
- Perform IPv6 filtering at the perimeter
- Perform granular ICMP filtering
- Deny packets for transition techniques not in use
- Deny IPv4 protocol 41 forwarding unless that is exactly what is intended
- Deny UDP 3544 forwarding unless you are using Teredo based tunneling
- **Leverage IPSec for everything possible**
- Try to achieve equal protections for IPv6 as with IPv4

IPv6

Summary

Summary

- Some things changed, most things stay
- Perform regular Penetration tests
- Protect your IPv6 Network like you protect your IPv4 Network
- Training and Awareness is necessary

- Use IPSEC when and where possible

IPv6

Famous last words

Famous last words :

- PCI-DSS - Payment Card Industry Data Security Standard
  - **requires the use of NAT for security (which it was never meant for)**
- Fact: Lack of NAT (66) in most firewalls

- PCI DSS compliance cannot be achieved with IPv6 ?

FYN

Q&A ?

Thank you for your attention