

IPv6 Security: Oxymoron or Oxycodone?

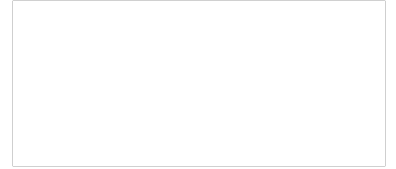
NANOG 60 – Atlanta

Paul Ebersman – IPv6 Evangelist

@Paul_IPv6, pebersman@infoblox.com

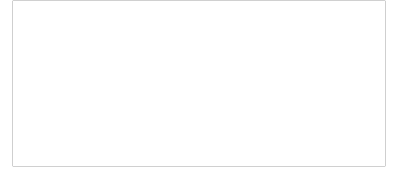
A decorative graphic consisting of numerous overlapping squares and diamonds in various colors including teal, yellow, red, grey, and green. These shapes are scattered across the slide, with a higher concentration in the top right and bottom right corners, and some overlapping the central text area.

**So many new security
issues with IPv6!**



Or are there...

IPv6 Security issues

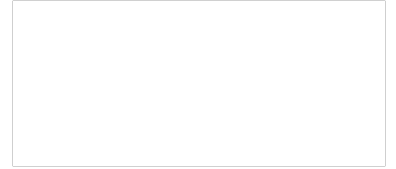


- **Same problem, different name**
- **A few myths & misconceptions**
- **Actual new issues**
- **FUD (Fear Uncertainty & Doubt)**

A decorative graphic consisting of numerous semi-transparent diamond shapes in various colors (teal, yellow, red, grey, blue, green) scattered across the slide, primarily concentrated in the top right and bottom right corners, framing a central dark blue rectangle.

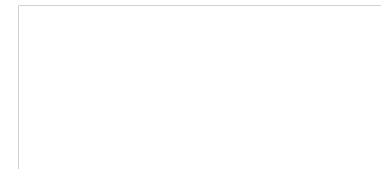
Round up the usual suspects!

Remember these?



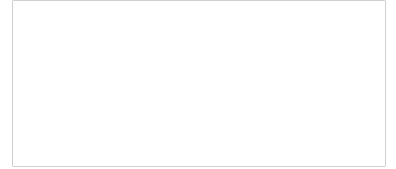
- **ARP cache poisoning**
- **P2p ping pong attacks**
- **Rogue DHCP**

ARP cache poisoning



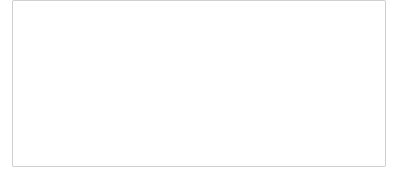
- **Bad guy broadcasts fake ARP**
- **Hosts on subnet put bad entry in ARP Cache**
- **Result: MiM or DOS**

Ping pong attack



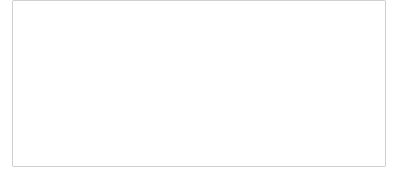
- **P2P link with subnet $> /31$**
- **Bad buy sends packet for addr in subnet but not one of two routers**
- **Result: Link clogs with routers sending packet back and forth**

Rogue DHCP



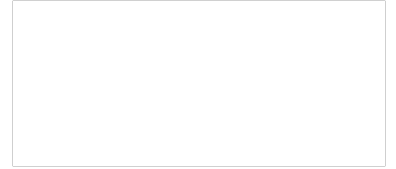
- **Client broadcasts DHCP request**
- **Bad guy sends DHCP offer w/his “bad” router as default GW**
- **Client now sends all traffic to bad GW**
- **Result: MiM or DOS**

Look similar?



- **Neighbor cache corruption**
- **P2p ping pong attacks**
- **Rogue DHCP + rogue RA**

Solutions?

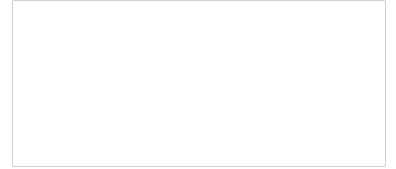


- **Lock down local wire**
- **/127s for p2p links (RFC 6164)**
- **RA Guard (RFC 6105)**

A decorative graphic consisting of various colored diamonds and squares (teal, yellow, red, grey, blue, green) arranged in a scattered pattern, primarily located in the top right and bottom right corners of the slide.

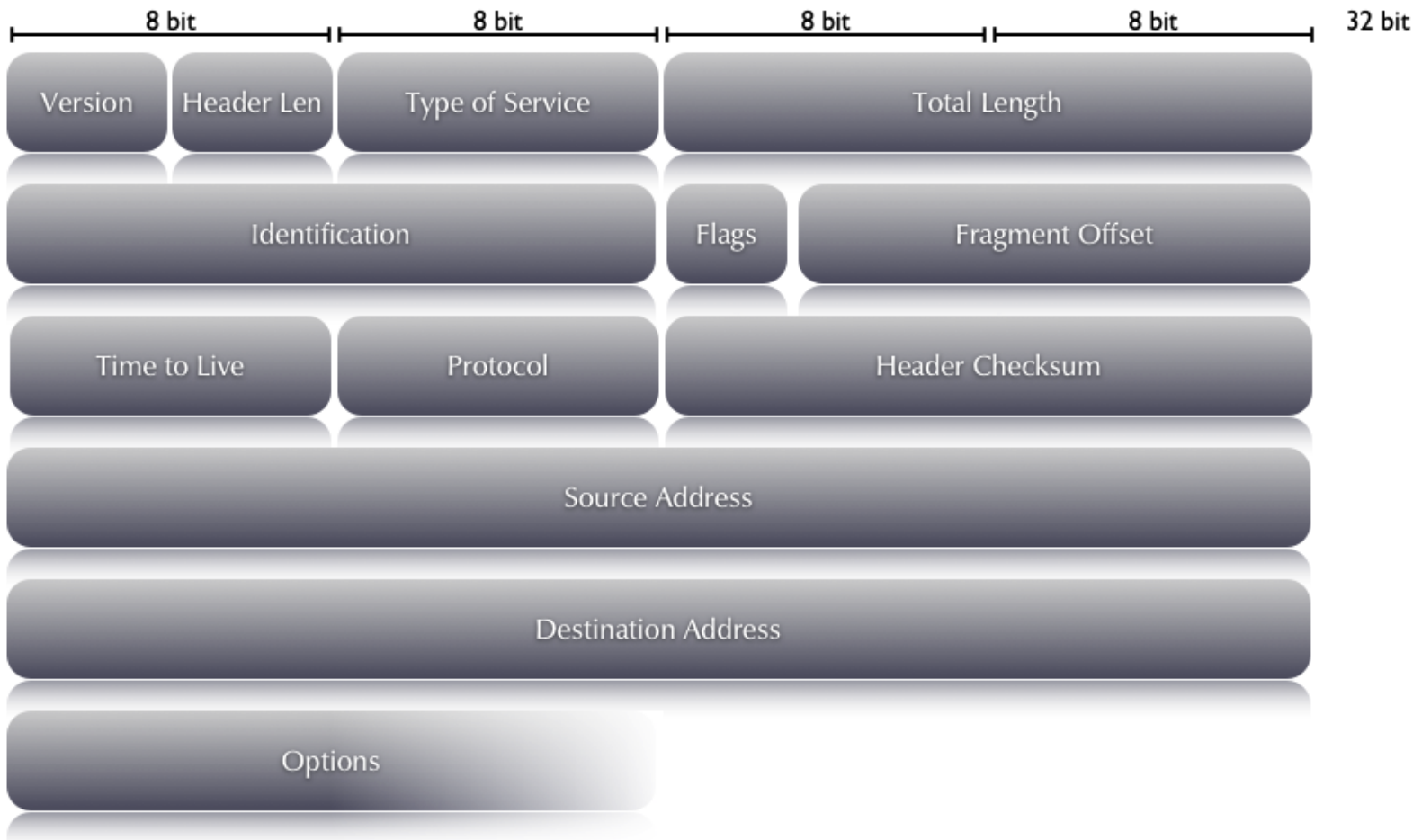
**And now for something
completely different!**

So what *is* new?

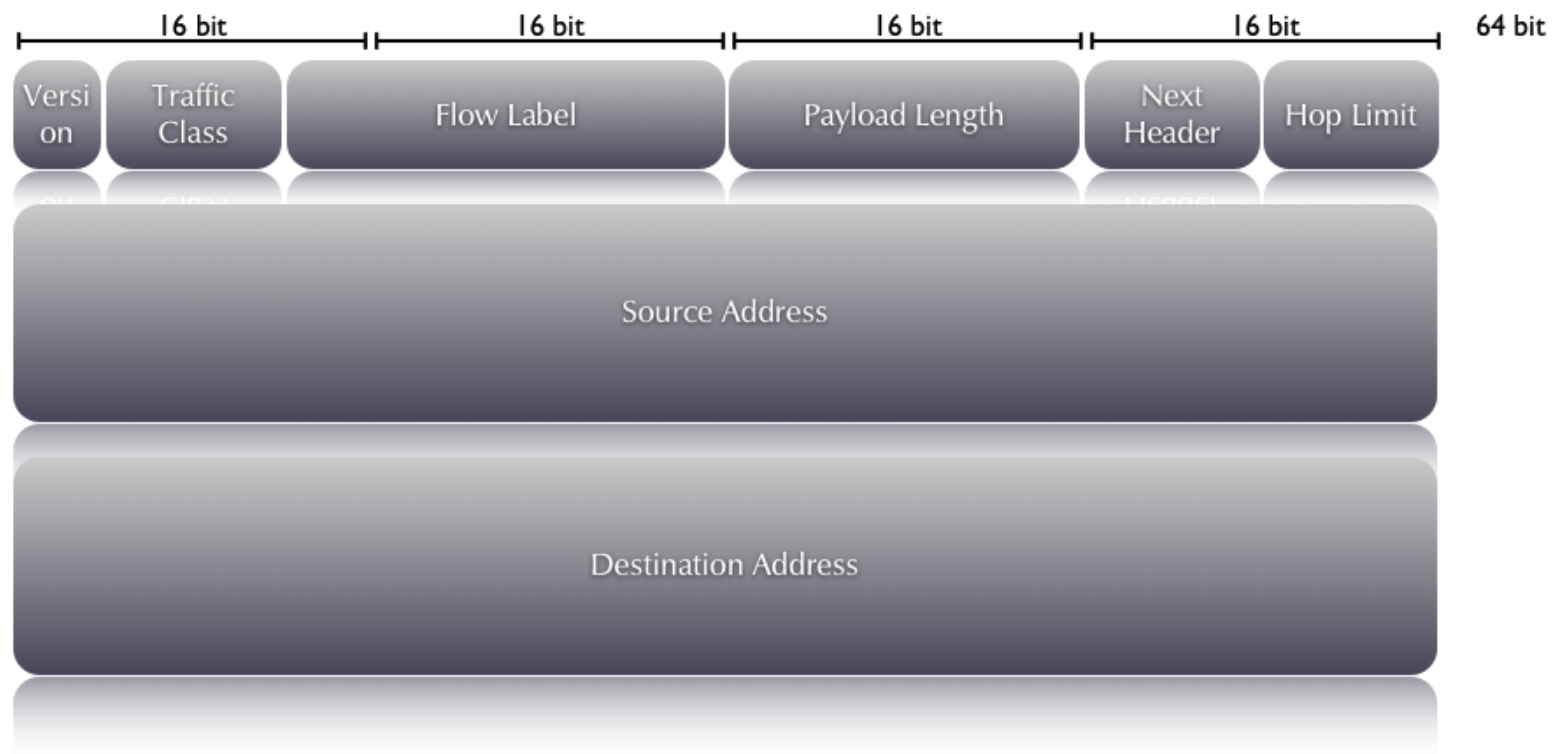


- **Extension header chains**
- **Packet/Header fragmentation**
- **Predictable fragment headers**
- **Atomic fragments**
- **Tunnels**

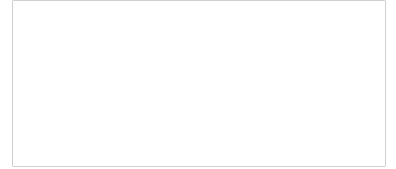
The IPv4 Packet



The IPv6 Packet



Fragmentation



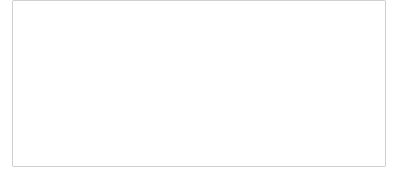
- **Minimum 1280 bytes**
- **Only source host can fragment**
- **Destination must get all fragments**
- **What happens if someone plays with fragments?**

IPv6 Extension Header Chains



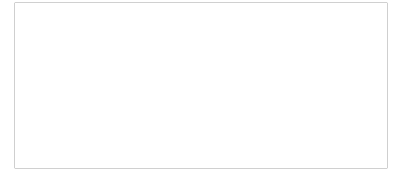
- **No limit on length**
- **Deep packet inspection bogs down**
- **Confuses stateless firewalls**
- **Fragments a problem**
- **See RFC 7112**

Predictable Fragments



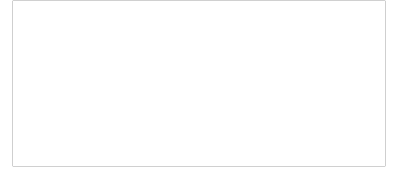
- **Fragment Header ID field**
- **No requirement other than “unique”**
- **Some implementations predictable**
- **draft-gont-6man-predictable-fragment-id**

Results of predicting ID

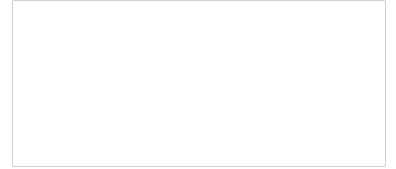


- **Determine the packet rate**
- **Perform stealth port scans**
- **Uncover the rules of a number of firewalls**
- **Count the # of systems behind a middle-box**
- **Perform a Denial of Service (DoS) attack**

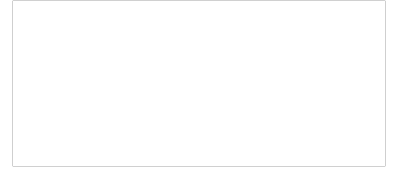
Atomic Fragments



- **Packet w/Fragment Header but not fragmented**
- **Usually forced by forged “Packet too big” msg**
- **Fragments can overlap**
- **Results: various fragmentation attacks possible**
- **See RFC 6946**



- **ACLs catch port/IP/protocol**
- **Some IPv6 tunnels don't use standard port/IP/protocol**
- **Signatures**

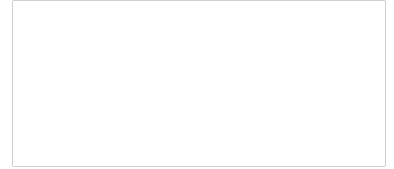


- **Most of these attacks are complicated**
- **Most attackers are lazy and will find easier vectors of attack**
- **But, there are toolsets out there:**
 - <http://www.si6networks.com/tools/ipv6toolkit>
- **Beat on your vendors!**

The background features a dark blue horizontal band across the middle. Above and below this band are various colorful diamond and square shapes in shades of teal, yellow, red, and grey, some overlapping and some floating. The text "You're already running IPv6..." is centered in white on the dark blue band.

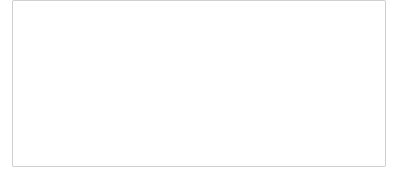
You're already running IPv6...

“I’m not using IPv6”



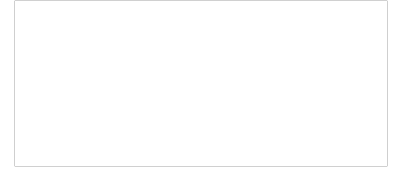
- **Are you running:**
 - Windows 8, Server 2012, Vista or newer
 - Windows clustering
 - Mac OSX
 - Any modern LINUX or FreeBSD

Guess again



**Congratulations,
you're running IPv6**

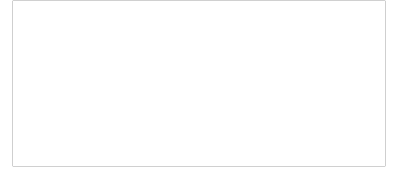
Get used to it...



- **Test now**
- **Train your staff**
- **Beat on your vendors**
- **Monitor it, don't try to disable it**

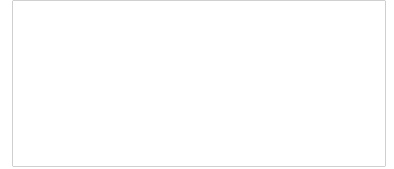


But everybody says...



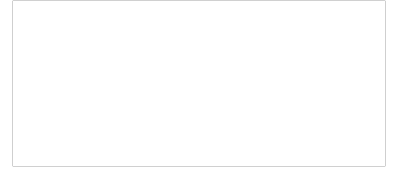
**IPSEC in IPv6 is better than IPv4
because it was designed in and
mandated.**

IPSEC: the reality



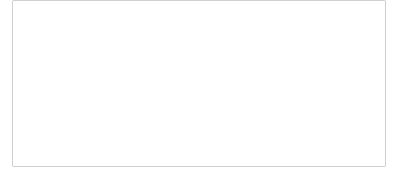
- **RFCs said “MUST” support IPSEC (but softening to “SHOULD”...)**
- **Didn’t define “support”, let vendors do it**
- **Vendors shipped, didn’t enable**
- **No PKI...**

IPv6 is *HUGE!*



- So big you can't scan it...
- Unless you don't really use it...

Use the space we have

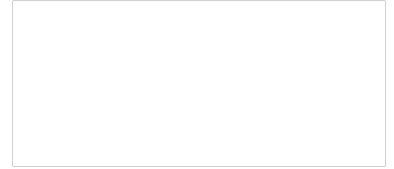


- **Give the whole /64 to DHCP pools**
- **Randomize address assignments across the whole /64**
- **Avoid EUI-64 (draft-gont-6man-deprecate-eui64-based-addresses)**

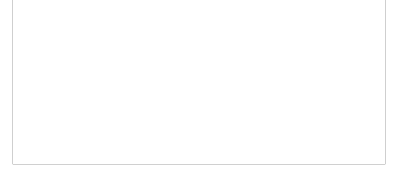
The background features a dark blue horizontal band across the middle. Above and below this band, there are various colorful diamond and square shapes in shades of teal, yellow, red, and grey, some of which are overlapping or faded. The text is centered within the dark blue band.

**It's the end of the
world as we know it!**

IPv6 will destroy the Internet!

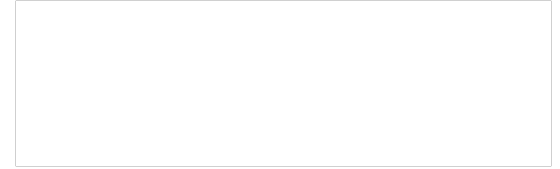


- **Apps will break**
- **Firewalls won't work**
- **ICMP is scary**
- **We don't understand it so it must be insecure**



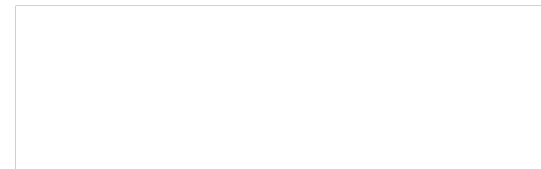
- **Yes, you will need to test and possibly rewrite all your code**
- **You need to reach everyone, including mobile devices**
- **Most bad ideas also in IPv4 code**

If it was wrong in IPv4...



- **Hard coding IP addresses**
- **Not checking inputs/sizes**
- **Using relative DNS labels**
- **No longer have source**
- **Not tested since Y2K**

Where to read more



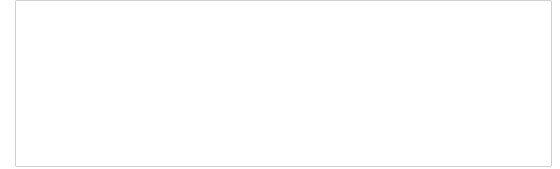
- **RIPE presentation:**

- [https://ripe66.ripe.net/presentations/134-Making_an_application_fully_IPv6_compliant_\(2\).pdf](https://ripe66.ripe.net/presentations/134-Making_an_application_fully_IPv6_compliant_(2).pdf)

Firewalls won't work

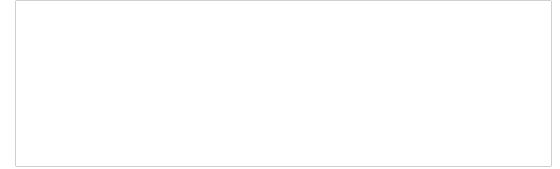
- **What do you do if your gear doesn't meet your needs?**
 - Beat on your vendors until it does...
 - But you need to know what to ask for

ICMP is scary, turn it off!



- **ICMPv4 wasn't that scary...**
- **ICMPv6 is much more tightly defined**
- **Read RFC 4890**

We don't understand it, so...

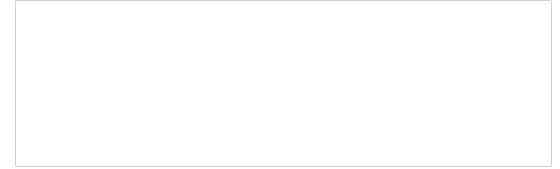


- **If someone is telling you that IPv6 is evil incarnate, it's because:**
 - **They are a vendor that doesn't support IPv6 but their competitors do**
 - **They are trying to sell you a security product**

The image features a dark blue horizontal band across the center. Above and below this band, there are several colorful diamond shapes in shades of teal, yellow, red, and grey, some of which are overlapping. The text "Test!!!" is centered within the dark blue band.

Test!!!

Know what you need



- **And ask for it!**
- **Hold vendors to IPv6 support**
- **Use the USGv6 standard:**
 - <http://www-x.antd.nist.gov/usgv6>



Q & A

A decorative graphic consisting of numerous overlapping squares and diamonds in various colors including teal, yellow, red, grey, and green. These shapes are scattered across the slide, with a higher concentration in the top right and bottom right corners, and a few smaller ones near the center.

Thank you!