HURRICANE ELECTRIC
INTERNET SERVICES

IPv6 Security

Safe, Secure, and Supported.

Andy Davidson

Hurricane Electric and LONAP

adavidson@he.net

Twitter: @andyd

MENOG 9 – Muscat, Oman, Tuesday 4th October 2011

Don't Panic!

IPv6 is *not inherently secure* but yet it is also **not** inherently insecure.

- Planning
- Policy
- Monitoring

- … the same as with IPv4

So what is there to talk about?

- Everything that was ever a security concern with IPv4
- Scanning issues
- User/desktop security
- Firewall support
- Transitional technology
- Internet edge requirements

Native IPv6 Everywhere

Importing everything from the IPv4 world..

- Password security
- Access list control
- Theft of network devices
- Abuse of rights
- Viruses, worms

- Do what you always have done (providing you have been successful ☺)

Impact of Tunneling mechanisms

- **Terado and 6to4 could be a weak point in an IPv4 network going forward.**
- End User devices obtain IPv6 connectivity via tunnel mechanism
- End Users can avoid traffic-shaping using these techniques
- **Install Native and managed IPv6** in your network to protect you from such real/ perceived risks

New LAN issues

- Neighbor Discovery Protocol
- Duplicate Address Detection
  - If a node determines that its [..] link local address is not unique, autoconfiguration stops and manual configuration is required [RFC2462]
- Router Advertisements
- (Somewhat akin to DHCP flaws in v4 world)

Defend against LAN issues

- RA Guard now RFC6105
  - Implemented in Cisco 6500/4500/4900
- SEND (though poor host support today)
  - (Secure Neighbour Discovery)
- 802.1X for physical security
  - Only defends against unauthorized devices

RA Guard

- Any host can send Router-Advertisements
  - Problems with Windows ICS boxes
  - Turn on Terado and advertise a ::/0 path!
  - Other malicious intent
- Think of RA Guard like DHCP Guard

RA Guard – Cisco example implementation

NATIVE IPv6 EVERYWHERE

```
interface GigabitEthernet0/0
    switchport access vlan nnn
    ipv6 nd raguard

show ipv6 nd raguard policy
```

Configure on all user ports.

Secure Neighbour Discovery (SEND)

- Secures aspects of ND, like RA, by adding a certification layer. Install a CA, and trust certificate on client computers, and ask to see certificate of RA originator
- Limited functionality in mobile environments
- Probably easier to roll RA Guard

- RFC3971

Privacy on the LAN

NATIVE IPv6 EVERYWHERE

- RFC4941
- Enabled by default on Windows 7, Mac Lion
- Appear as “Temporary Addresses”

- Prevent a user being ‘tracked’ when they move between LANs by their final 64 bits.
- Default SLAAC behaviour embeds MAC address into IPv6 global scope address.

Spoofing

NATIVE IPv6 EVERYWHERE

- BCP38 still applies!
  - Ingress Filtering
  - Prevents receipt of packets where the source address does not appear on a customer port.
  - RFC2827
- This protects your neighbours as well as your own service provider network

Broadcast / Multicast on the LAN

- No Broadcast addresses in ipv6, so smurf/ amplification attacks as in v4 not possible.
- Global multi-cast addresses must not receive ICMPv6 packets, this is built into the specification
- Security by default here with IPv6. ☺

Port Scanning

- 500k addresses per second, one million years to scan a single /64!
- However, do you configure your services in the bottom few bits of your /32 ? ☺
  - Hosts at ::1, ::2, easy to find.

NATIVE IPv6 EVERYWHERE

New Scanning attack vectors

- All nodes will respond to some multicast addresses
  - filter ff02::1, ff05::1, originating outside your network, at your border.
- Otherwise node addresses on your network can be exposed

Firewalling NAT and ICMPv6

- NAT – no longer exists in v6. But this was never useful for security in v4 anyway.
- Do not block ICMPv6 (in the way that some networks filter ICMP
  - Breaks Path MTU Discovery (Fragmentation at host)
  - Breaks LAN auto-configuration
  - In addition, it breaks the useful things it did in v4 (TTL exceed, echo request)
  - Possibly rate-limit:

```
system{ internet-options { cmpv6-rate-limit { bucket-size bucket-size; packet-rate packetrate; } } }
```

Firewalling - Fragmentation

- End devices, NOT routers/firewalls are now responsible for fragmentation.
  - Intermediate devices can not inspect Layer 4 information for policy compliance
  - Running and end-host firewall on servers more important where L4 security is critical to your application
  - Filtering ‘ICMPv6 Packet Too Big’ will destroy communications for some users!
  - Filter fragmented packets destined to infrastructure

Firewall feature wish list

NATIVE IPv6 EVERYWHERE

- Look to filter :
  - Souce/Destination address/port
  - Extension headers
  - Fragmentation
  - PMTUD support
  - ICMPv6 rate-limit / policing
  - Multicast filtering
- RIPE 501 is the complete recipe for success!

IPv6 at your peering edge

- Disable router-advertisements – BGP must be the prefix exchange mechanism.
- "no ipv6 mld router" on peering port interface
  - Prevents multicast listener query responses
- Spurious Neighbour Discovery on the peering LAN has caused CPU busy states (BGP Drops)
  - Filter ND messages on peering LAN ports

Disable hop-by-hop routing

- RH0 – Now deprecated, but you may see it
- Already blocked on most host implementations
- Cisco config hint:

```
no ipv6 source-route
ipv6 access-list BLOCKRH0
  deny ipv6 any any routing-type 0 log
  permit ipv6 any any
  interface GigabitEthernet 1/1
  ipv6 traffic-filter BLOCKRH0 in
```

Disable Hop by Hop routing 2

- Juniper hint:

```
firewall {
  family inet6 {
   filter filter_v6_rh {
     term 0 {
       from { next-header [hop-by-hop routing]; }
       then {
         discard; }
      }
   }
 }
```

Point to Point infrastructure links

Native IPv6 Everywhere

- Ping-pong problem
  - Use something smaller than a /64 e.g. /127
  - But assign a /64 in your allocation
  - Or something which implements RFC4443

BGP

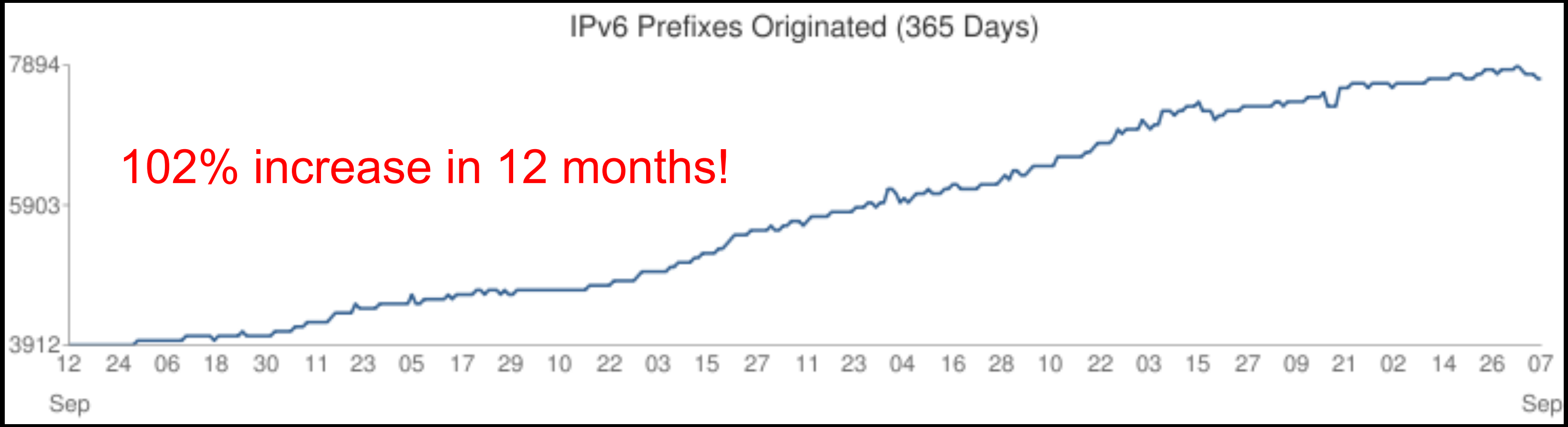
- BGP is just the same, but we stand a chance of keeping the routing table clear with certification (resources are newer).
- Explicitly name route-maps as v4 or v6
- Check your filter logic matches v4
  - And that your v4 logic is safe ☺
  - Same old max-prefixes, filter customers, filter long ASN
- Only accept prefixes from 2000::/3

Internal Application Security

- Where do you use an IPv4 address within your products?
  - Web security?
  - SPAM prevention (reputation…)
  - DNS Views
  - .
  - .
- All need to support IPv6 – test early and often!

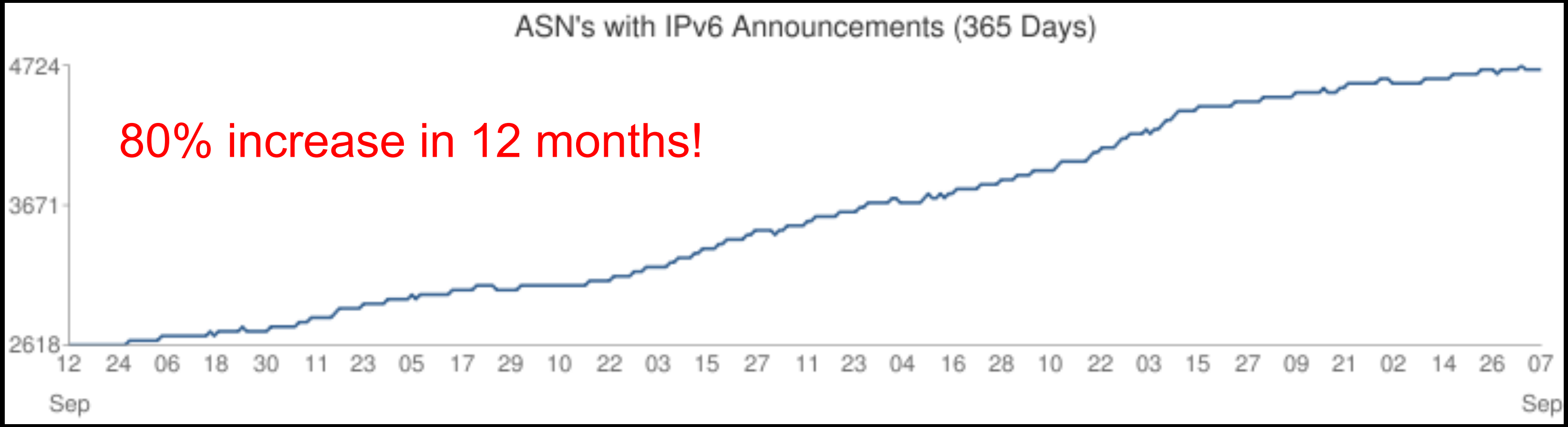
IPv6 will not go away – work on this today!

Native IPv6 Everywhere



102% increase in 12 months!

http://bgp.he.net/report/prefixes#_prefixes



80% increase in 12 months!

http://bgp.he.net/report/prefixes#_networks

IPv6 measured at via BGP ASNs with IPv6

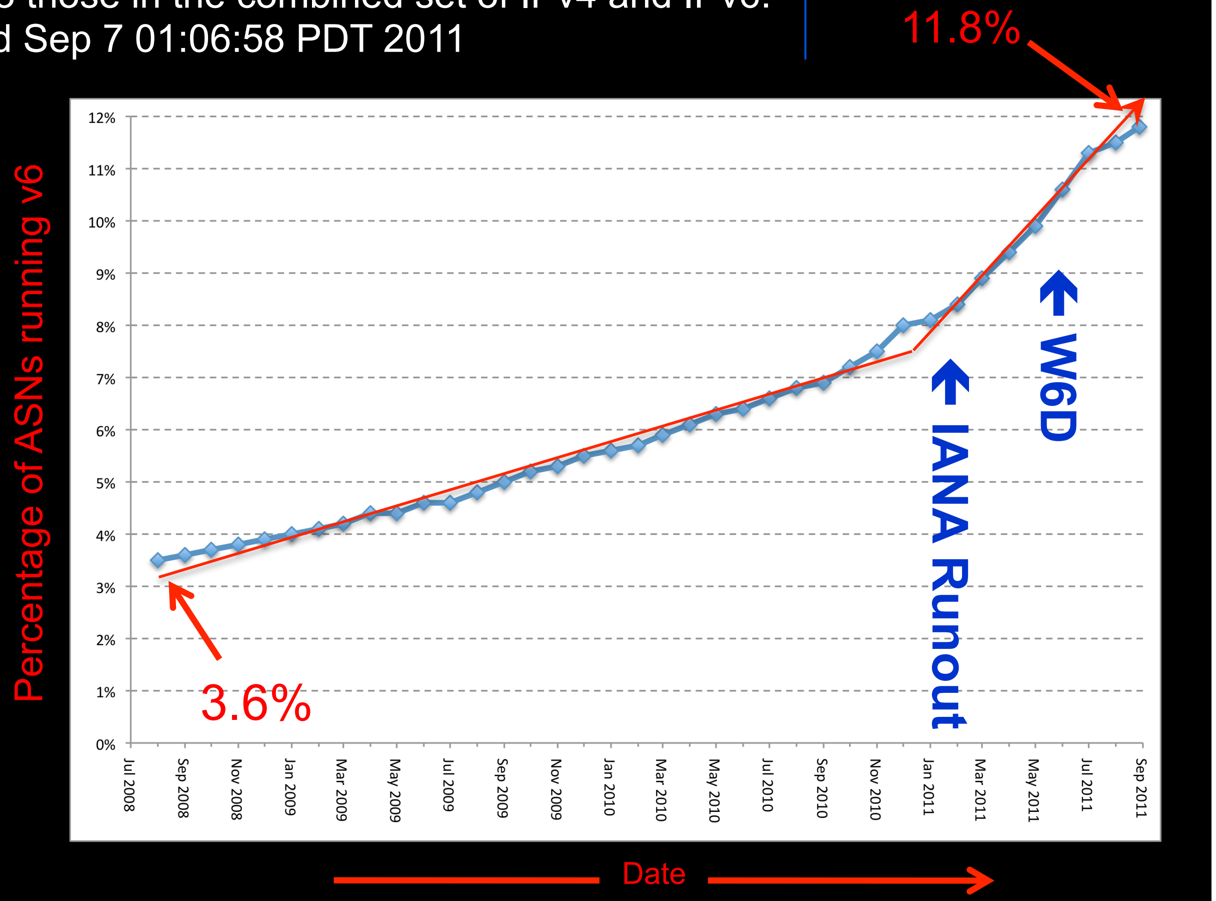
NATIVE IPv6 EVERYWHERE

http://bgp.he.net/ipv6-progress-report.cgi

Networks Running IPv6

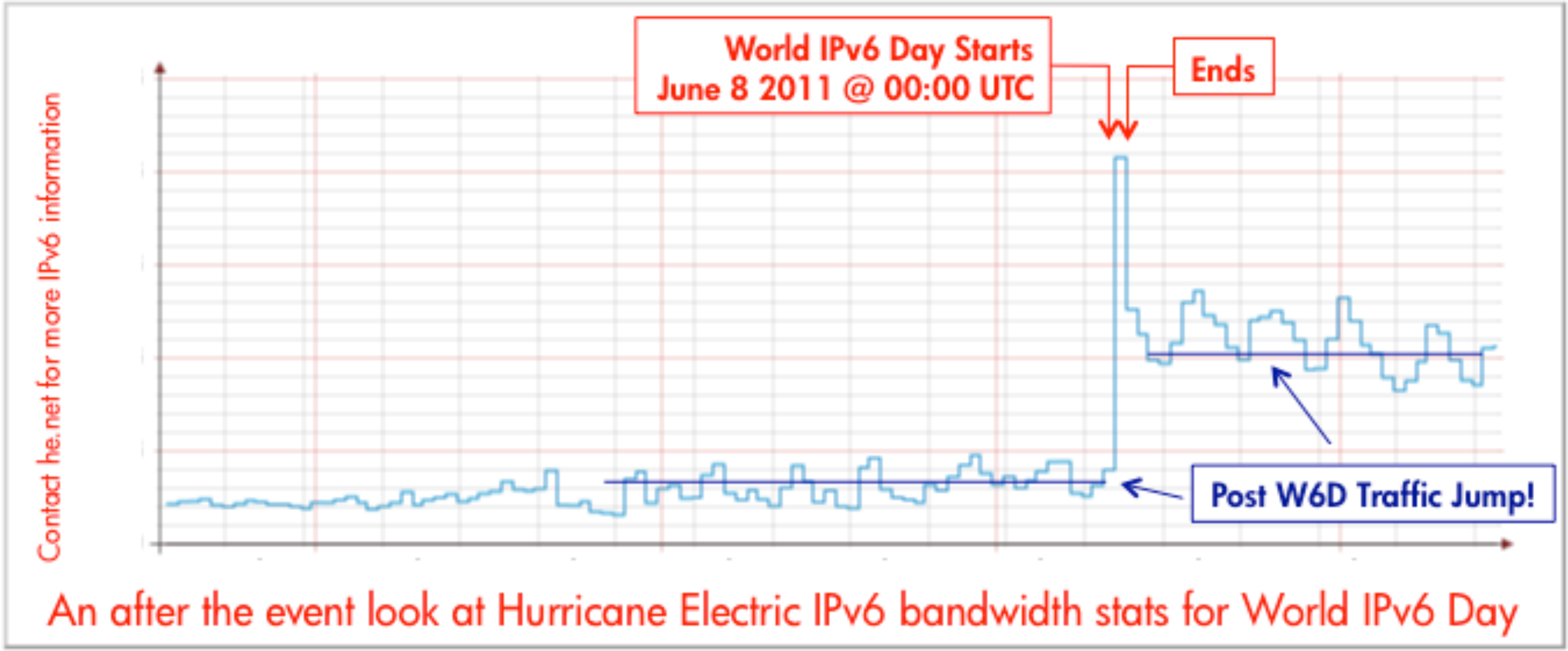
We can measure the percentage of networks running IPv6 by comparing the set of ASes in the IPv6 routing table to those in the combined set of IPv4 and IPv6.
IPv4 and IPv6 RIBs Last Parsed: Wed Sep 7 01:06:58 PDT 2011

IPv4 Ases: 38,889
IPv6 ASes: 4,592
ASes using only IPv4: 34,394
ASes using only IPv6: 97
ASes using IPv4 and IPv6: 4,495
ASes using IPv4 or IPv6: 38,986
Percentage of ASes (IPv4 or IPv6) running IPv6: 11.8%



World IPv6 Day and real IPv6 traffic

- Long term win since W6D in IPv6 traffic levels
  - That means there are both content and eyeballs in play

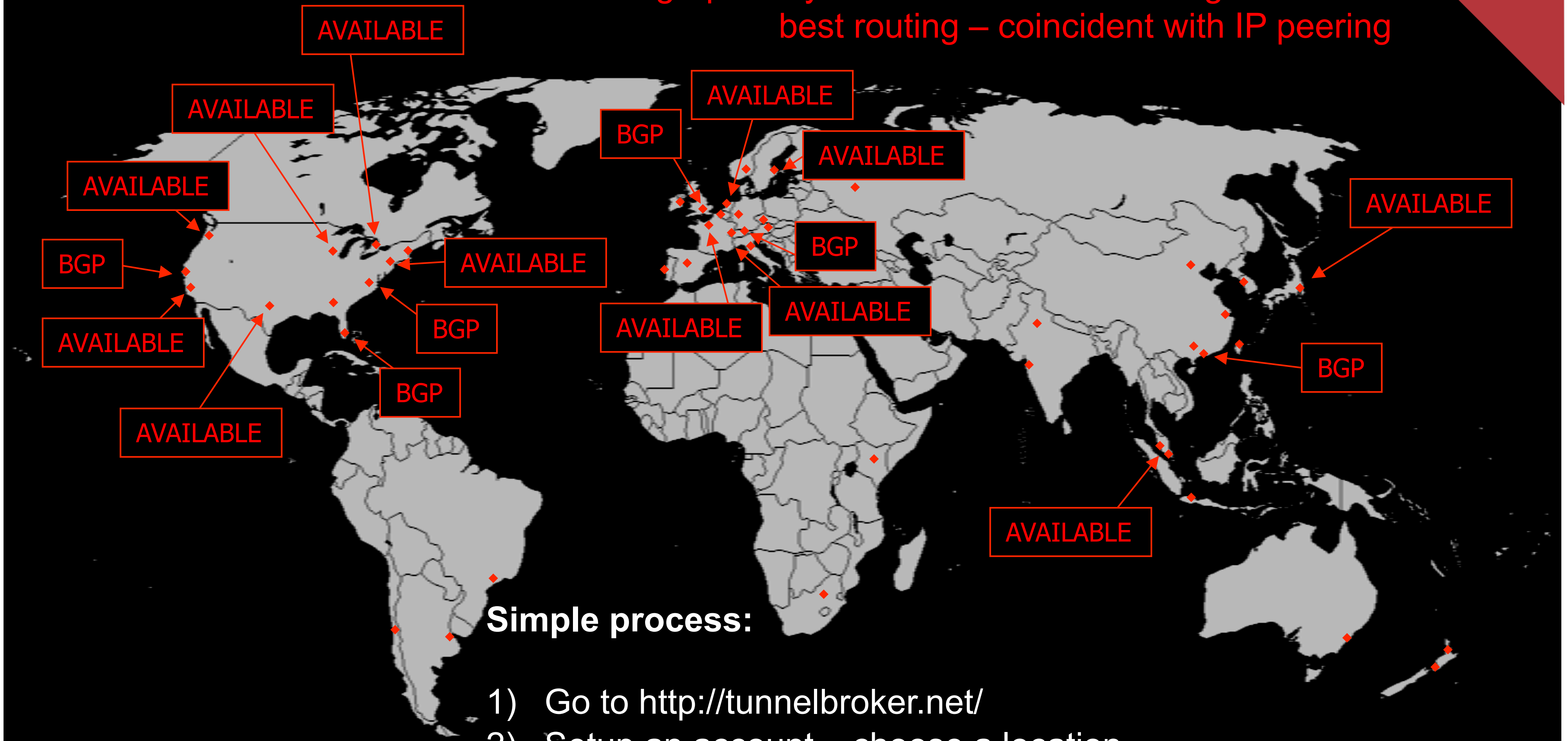


An after the event look at Hurricane Electric IPv6 bandwidth stats for World IPv6 Day

Build an IPv6 Security Lab for free

NATIVE IPv6 EVERYWHERE

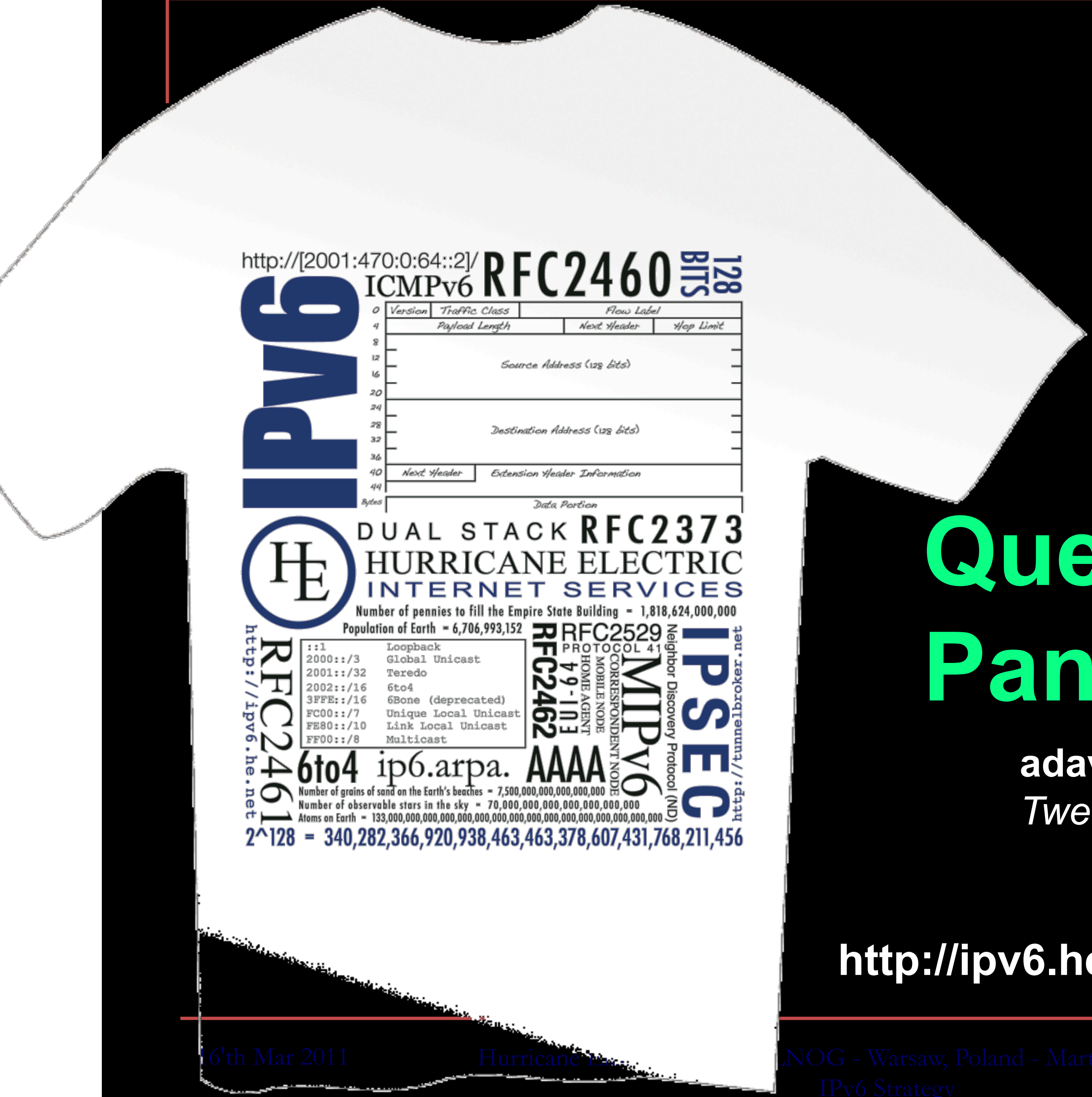
Geographically diverse locations allowing customers best routing – coincident with IP peering



Simple process:

1) Go to http://tunnelbroker.net/
2) Setup an account – choose a location
3) Setup your own host or router to allow tunnels
4) Tell us your lessons and success story at MENOG 10!

NATIVE IPv6 EVERYWHERE


http://[2001:470:0:64::2]/
RFC2460
128 BITS
ICMPv6
IPv6
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address (128 bits)
Destination Address (128 bits)
Next Header
Extension Header Information
Data Portion
Bytes
DUAL STACK RFC2373
HURRICANE ELECTRIC
INTERNET SERVICES
Number of pennies to fill the Empire State Building = 1,818,624,000,000
Population of Earth = 6,706,993,152
::1 Loopback
2000::/3 Global Unicast
2001::/32 Teredo
2002::/16 6to4
3FFE::/16 6Bone (deprecated)
FC00::/7 Unique Local Unicast
FE80::/10 Link Local Unicast
FF00::/8 Multicast
RFC2529
PROTOCOL 41
RFC2462
EUI-64
HOME AGENT
MOBILE NODE
CORRESPONDENT NODE
MIPv6
Neighbor Discovery Protocol (ND)
IPSEC
http://tunnelbroker.net
http://ipv6.he.net
RFC2461
6to4
ip6.arpa.
AAAA
Number of grains of sand on the Earth's beaches = 7,500,000,000,000,000,000
Number of observable stars in the sky = 70,000,000,000,000,000,000,000
Atoms on Earth = 133,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000
2^128 = 340,282,366,920,938,463,463,378,607,431,768,211,456

Questions and Panel Debate

adavidson@he.net

Tweet me : @henet @andyd

http://ipv6.he.net/certification/