Not just IPv4 with bigger addresses



# History



# History

- Vint Cerf
  - VP at Google
  - Chief Internet Evangelist
- DARPA
  - Chose a 32bit space
  - Switch to TCP/IP
  - Experiment never ended



## History



#### **IPv4 Exhaustion**





## **IPv4 Exhaustion**

- February 3, 2011
  - Last 5 /8s are allocated
  - Widely misreported
    - Internet is out of addresses
- Regional registries
  - Still have space for a while
  - … except APNIC



#### 2620:0000:1cfe:face:b00c:0000:0000:0003

## Addressing

#### 2620:0000:1cfe:face:b00c:0000:0000:0003

#### 2620:0:1cfe:face:b00c::3

### **Classes Inter-Domain Routing**



#### DNS

#### Quad-A record (AAAA)

- Counterpart to A record
- Associates a name with a IPv6 address
- Pointers/Reverse (PTR)
  - ip6.arpa has been reserved
  - Functions similar to IPv4 lookup

# **Address Types**

#### Loopback (127.0.0.1)

- ::1
- Link-local (169.254/16)
  - fe80::/10 prefix
  - Required for lower level operations
- Unique local (private address)
  - fc00::/7
  - Non-routable
- Global
  - Routable

# **ICMPv6 Is Not Optional**

- Neighbor discovery
  - Router discovery
  - Address resolution
  - Duplicate address detection
  - Unreachability detection
- Parameter discovery
  - Path MTU

# **Simplified Processing**

- No packet fragmentation
  - MTU discovery is expected
- No checksum
  - No re-computation on changes
  - Assume higher level protocol does it
- Simpler packet layout
  - Optional packet extensions can be used
- Generous sub-netting
  - Smaller route tables

- Router advertisement
  - Prefix (subnet)
  - Gateway
  - DNS kinda
- Append MAC address
  - Information leaking in IP address
  - Privacy extensions
- Duplicate Address Discovery







MAC: 00:21:9B:1B:7E:E2









#### What if

- That's not a real gateway?
  - Man in the middle?
- Someone says they own every address?
  - Denial of service?
- The only gateway becomes unreachable?
  - Spec says every address becomes local

# **Secure Neighbor Discovery**

- Cryptographically generated addresses
- Router authorization
- Replay protection
- Relatively new
  - Little OS support

## **Cryptographic Addresses**

- Host identifier is hash of a public key
- Prevents address spoofing
  - Node has to prove it owns an address
- Too complex to brute force
  - ... for now

### **Router Authorization**

- Essentially a X.509 certificate
- Requires a chain of trust
  - Great if one already exists
- Prevents fake routers
  - Or accidental routers

# Transitioning

- IPv6 Tunnels
  - Native IPv4 address
  - Many competing standards (6in4, 6rd, Toredo)
- IPv4 Tunnels
  - Native IPv6 address
  - Carrier grade NAT for IPv4
- Dual-stack
  - Have both addresses
  - Systems will prefer IPv6 traffic

### **IPv6** Preference

- Fake router + DNS translation
  - Man in the middle
- Timeout before IPv4 fallback
  - No one notices IPv6 downtime
  - Misconfigured workstations
    - Non-routable IPv6 setup
- Not putting AAAA in for domain
  - <u>http://ipv6.google.com</u>
  - <u>http://www.v6.facebook.com</u>

## **Pain Points**

#### Firewalls

- Might leave you wide open
- Drop ICMPv6 traffic
- Lots of software/hardware to update
  - Assumptions made
  - Outdated libraries
- Still unusual

## **Positive Points**

- Addresses are "cheap"
  - Can be changed often (Privacy Extensions)
  - Allocated quickly
- Entire subnets can't be scanned
  - Just not feasible
  - Can scan link local on join
- No more NAT routing
- Feel like you're part of the future

### Purdue and IPv6



http://indiana.gigapop.net/ingigapop/maps\_documentation/documentation.html

## What You Can Do Today

- IPv6 tunnels
  - Hurricane Electric
  - SixXS
  - Freenet6 (windows)
- Hurricane Electric Certification
- Check your ISP
  - Comcast (<u>http://www.comcast6.net/</u>)
- THC Toolkit (<u>http://www.thc.org/thc-ipv6/</u>)

## World IPv6 Day



June 8, 2011

### References

#### Books

- IPv6 Security by Scott Hogg and Eric Vyncke
- Articles
  - Successful Strategies for IPv6 Rollouts. Really.
    - http://queue.acm.org/detail.cfm?id=1959015
- Talks
  - Recent advances in IPv6 insecurities
    - http://events.ccc.de/congress/2010/Fahrplan/events/395 7.en.html