Future of IP (IPv6)

Jeffrey Shafer

IP Versions

ID	Description
0-3	Unused: Development versions of IP
4	Current network-layer protocol
5	Unused: Experimental stream protocol – ST
6	New network-layer protocol (1996)
7-9	Unused: Experimental protocols – TP/IX, PIP, TUBA
10-15	Not allocated

Why Replace IPv4?

- Performance?
  - Quality of Service?
- Security?
  - Authenticating users?
  - Tracking criminals / spammers?
  - Denial of service?
- New applications?
  - Mobile devices?
- Routing is scaling out of control?

- IPv6 does not attempt to solve all problems with computer networks
  - Actually, it only really solves one of them!

Why Replace IPv4?

- IP address exhaustion
  - IPv4 has ~4 billion addresses
  - Internet will not "collapse", but new devices / networks will not be able to join
- When?
  - Estimates always seem to be "a few years" in the future
  - Current estimates *(as of March 2009)*
    - APNIC – April 2011
    - Cisco – July 2011
  - Different assumptions produce different estimates
    - Widespread deployment of NAT
    - Reclaiming assigned but unused addresses
      - Create a marketplace? (all sorts of problems here…)
    - Future worldwide growth

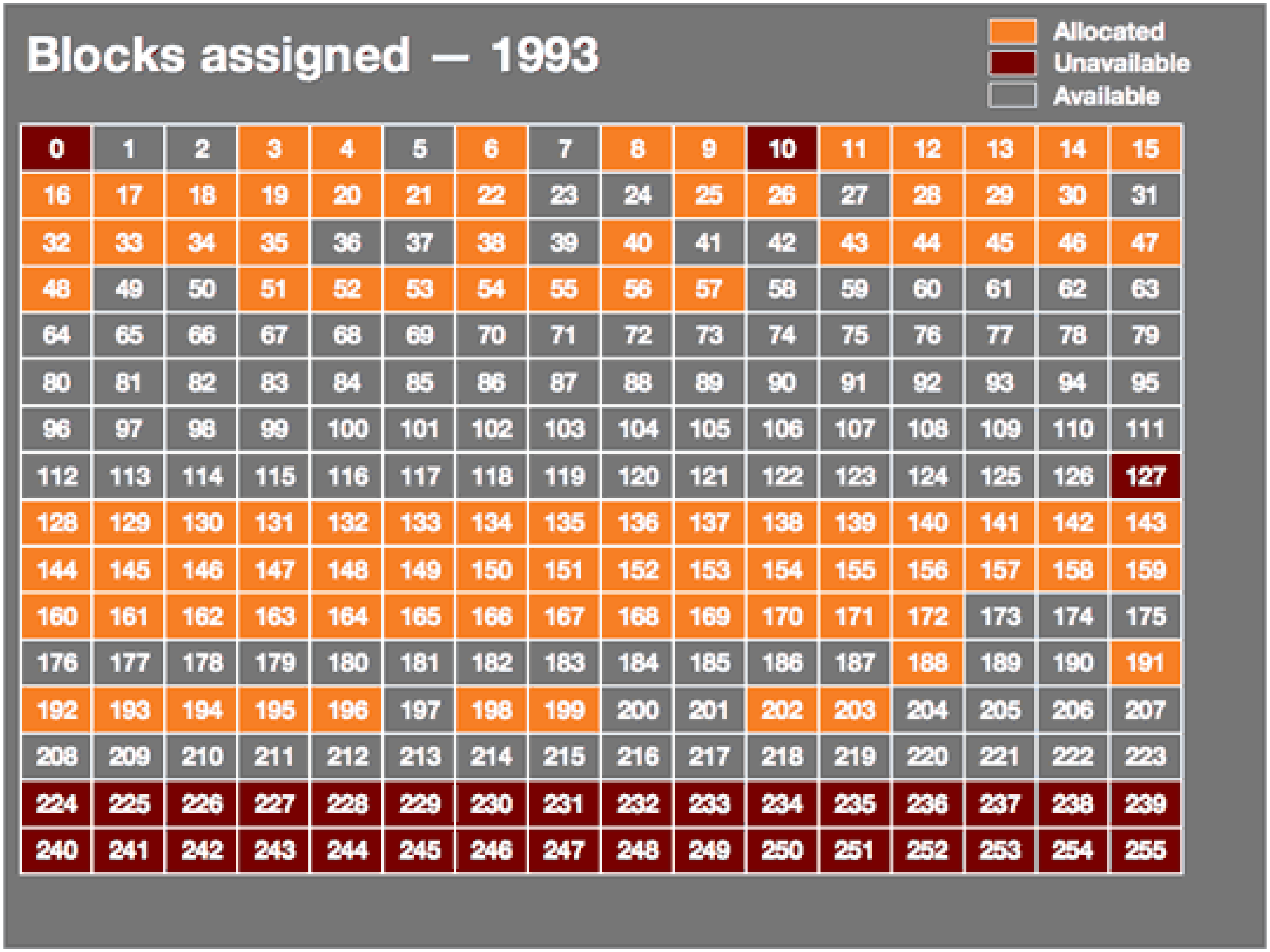


Figure from http://arstechnica.com/articles/paedia/IPv6.ars

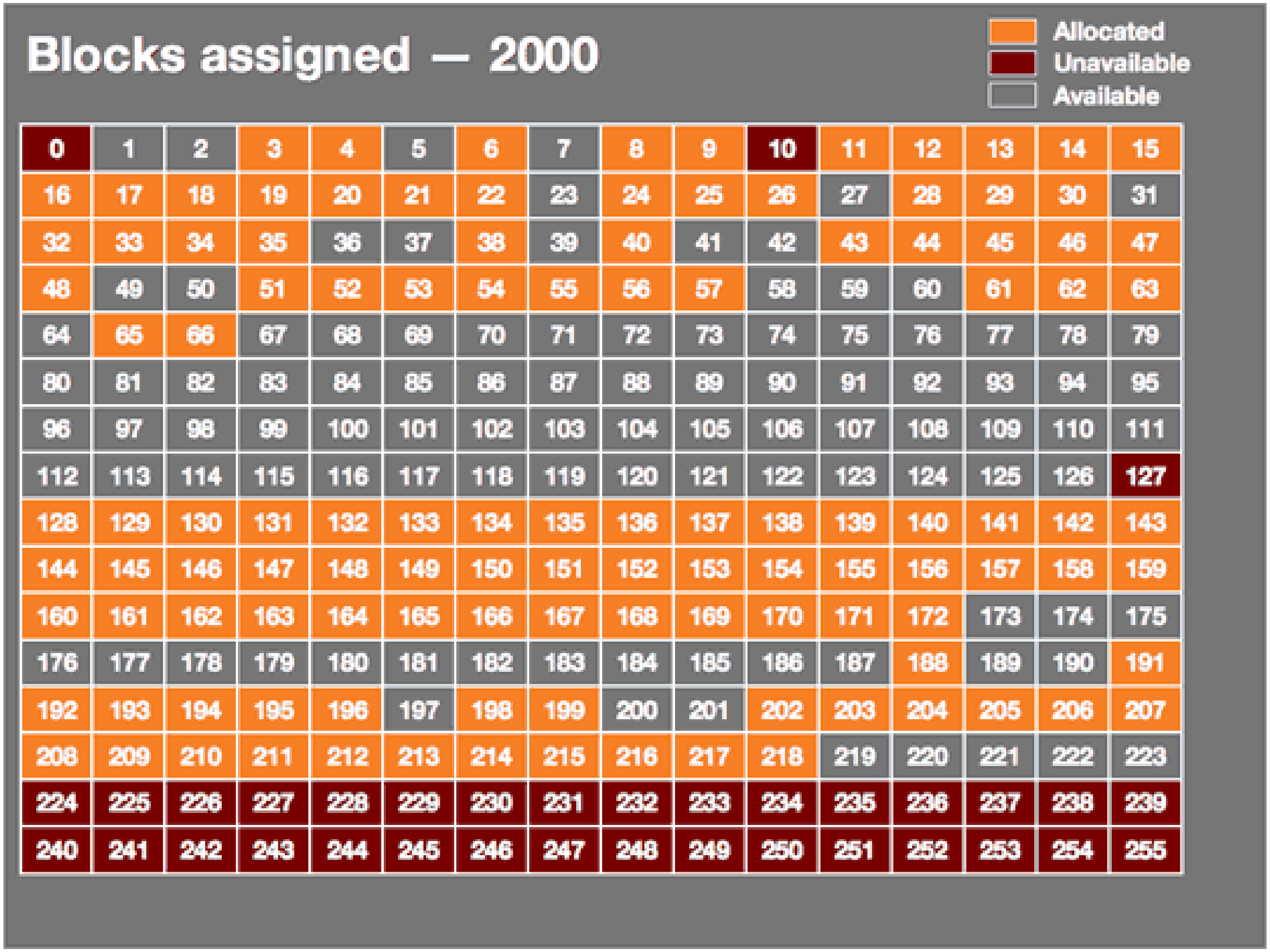


Figure from http://arstechnica.com/articles/paedia/IPv6.ars

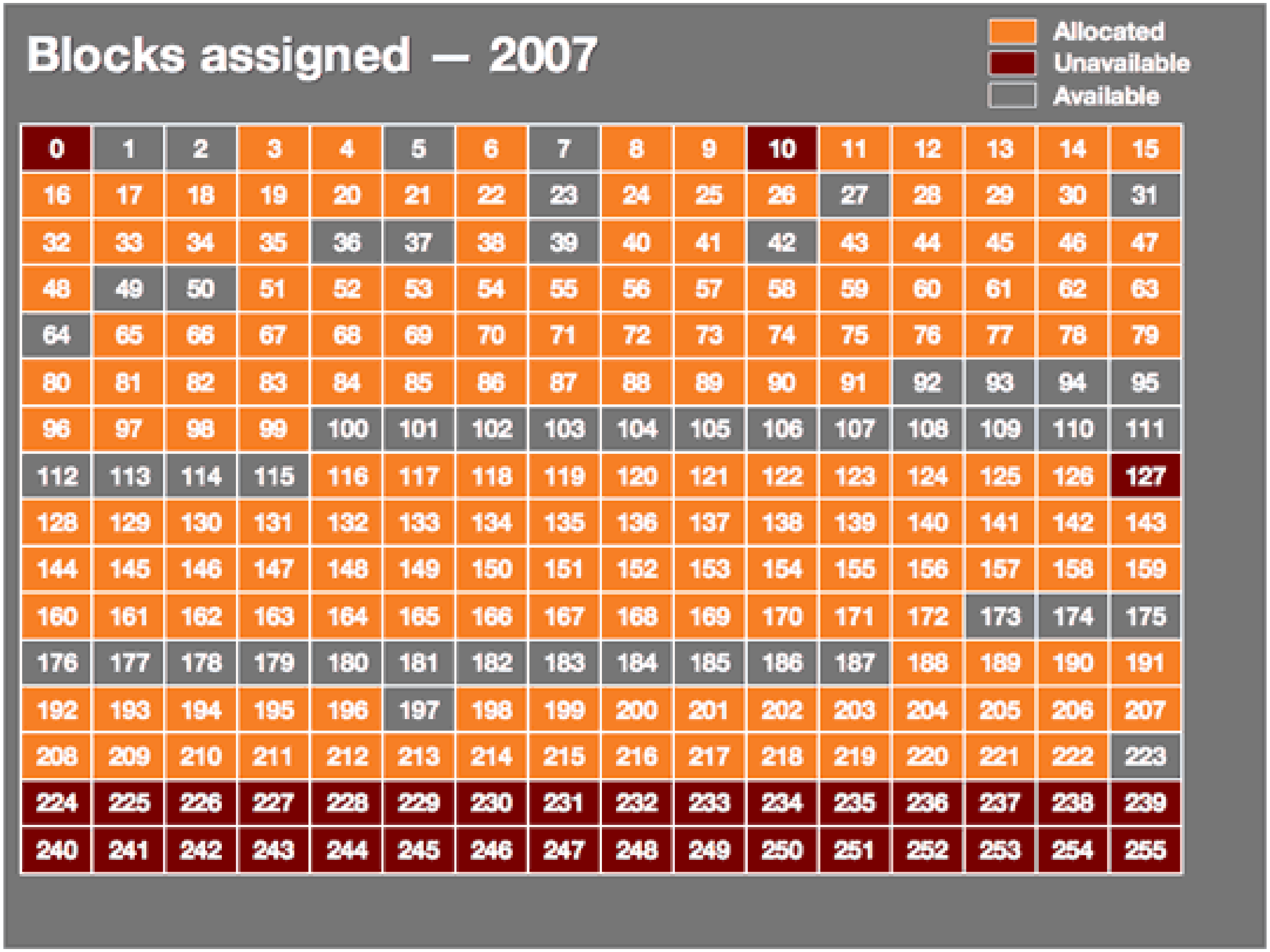


Figure from http://arstechnica.com/articles/paedia/IPv6.ars

IPv4 Address Space

- Unavailable Addresses
  - 10.x – Private Addresses
    - Along with 192.168.x and 172.16.x to 172.31.x
  - 127.x – Local Loopback Addresses
    - Why an entire /8?
  - 224.x to 239.x — Multicast groups
  - 240.x to 254.x — Reserved for “future use”
    - Waste of address space
    - Impossible to re-use today because most IP software flags these addresses as invalid
- Current Allocation
  - http://www.iana.org/assignments/ipv4-address-space

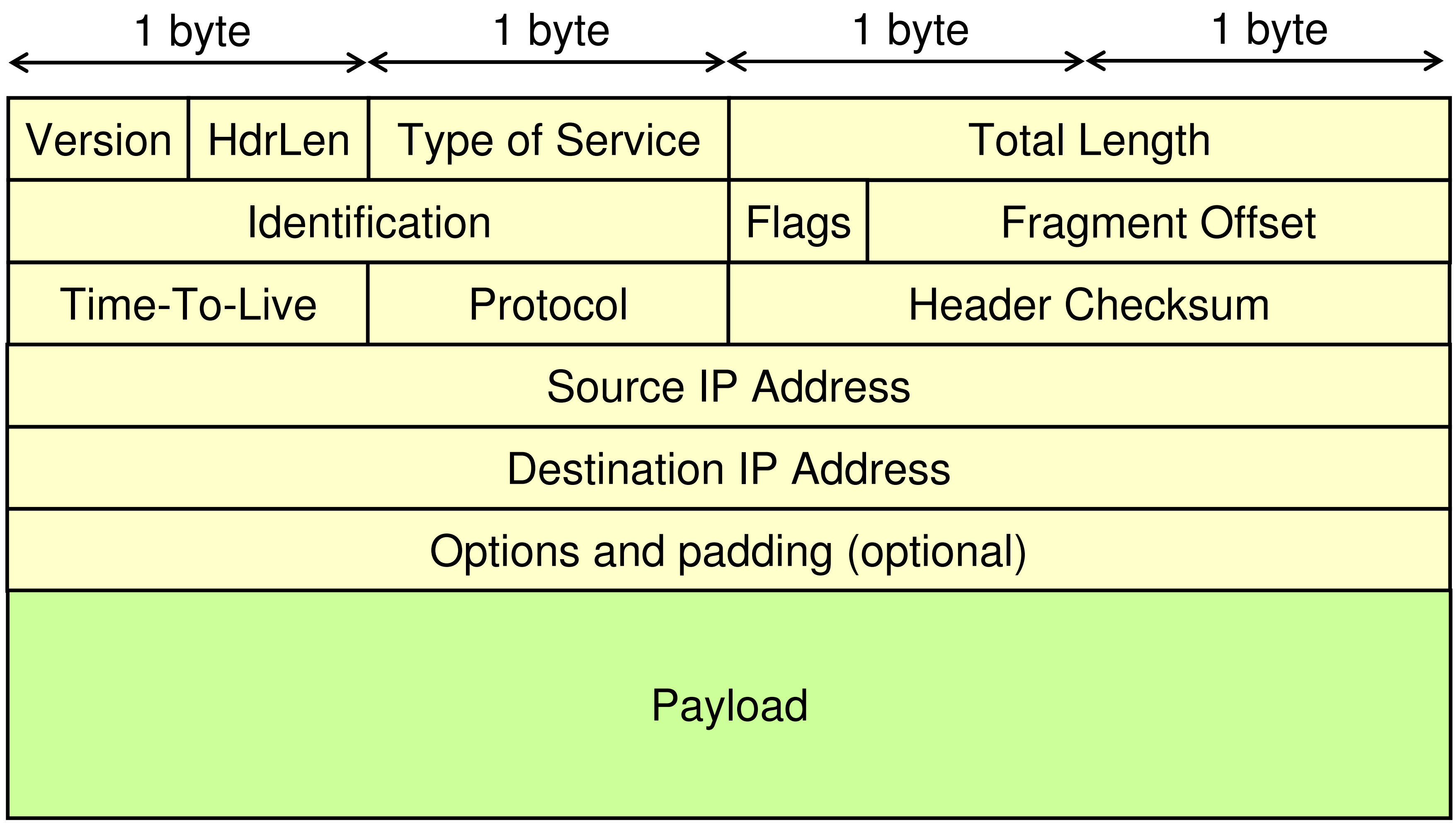
IPv4 vs IPv6 - Similarities

- Datagram
  - Each packet is individually routed
  - Packets may be fragmented or duplicated
- Connectionless
  - No guarantee of delivery in sequence
- Unreliable
  - No guarantee of delivery
  - No guarantee of integrity of data
- Best effort
  - Only drop packets when necessary
  - No time guarantee for delivery

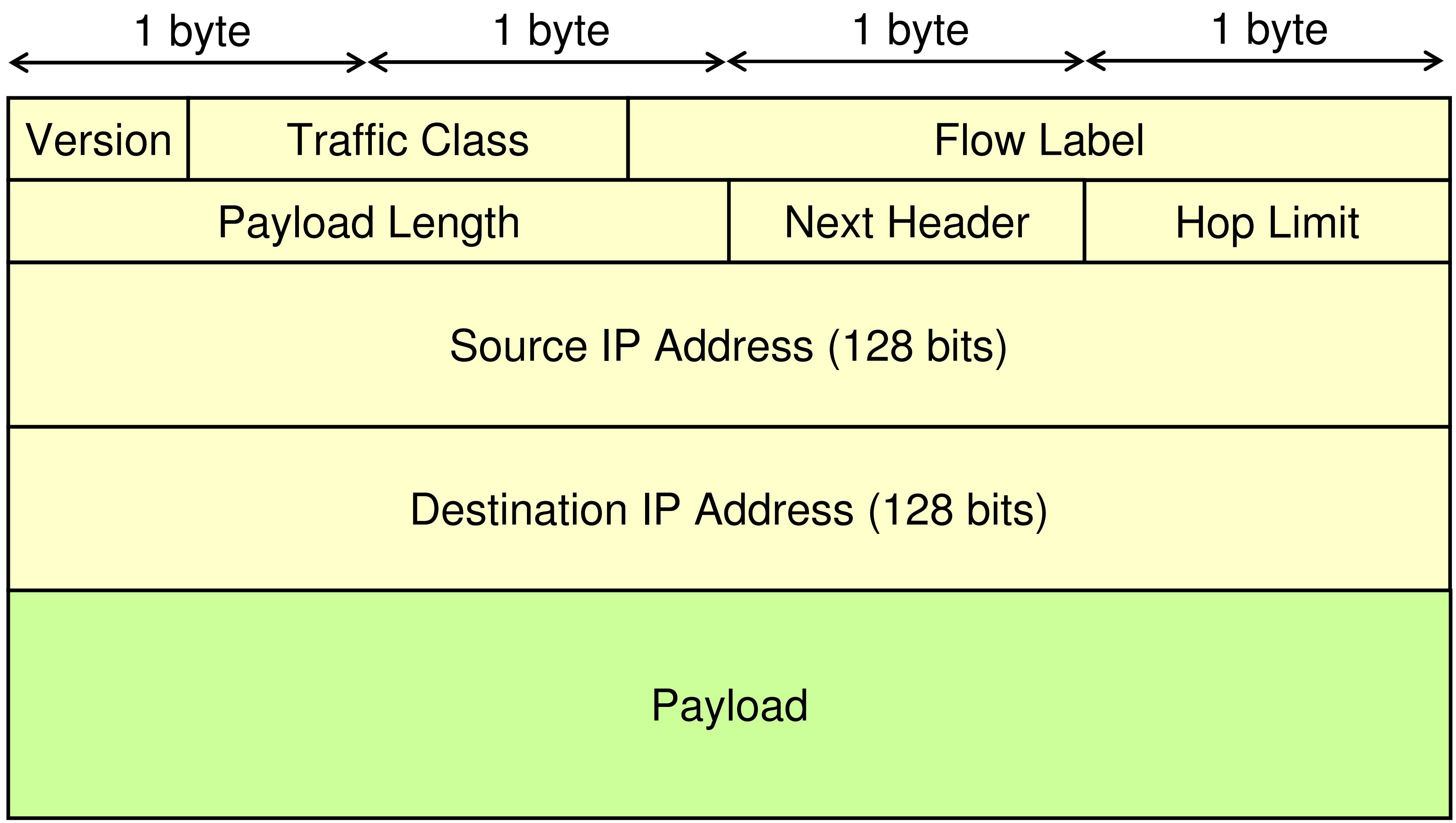
IPv4 vs IPv6 - Differences

- Address Length
  - IPv4 – 32 bits (2^{32} = ~4 billion)
  - IPv6 – 128 bits (2^{128}= ~340 trillion, trillion, trillion)
- Security – IPSec support required in IPv6
  - IPSec encrypts each IP packet independently
- Reliability – No Header Checksum in IPv6
  - Easier for routers – No need to update checksum after decrementing TTL
  - Relies on link-level error checking
- Quality of Service
  - Label data flows for special priority levels at routers
- Simplified Header Format
  - Infrequently used fields are optional

IPv4 Datagram



IPv6 Datagram (Base Header)



IPv6 Datagram with Options

- Can append multiple headers

Base Header (Next=TCP)	TCP Data

Base Header (Next=Fragment)	Fragment Header (Next=TCP)	TCP Data

- Common additional headers
  - Fragmentation
  - Routing (allows source to specify preferred route)
  - Authentication (part of IPsec – verifies source)
  - Security (part of IPsec – carries encrypted payload)

IPv6 – Fragmentation

- Supported by an optional header
  - Design assumption that fragmentation will be less common in the future
- Fragmentation only done by transmitting host
- Routers never fragment a packet
  - Drop packets that are too large
  - Send ICMP error back to host
  - Simplifies router design
- Host should use MTU discovery to select correct (maximum) packet size

IPv6 Address Notation

- 128 bits – 8 groups of 4 hex digits
  - `2001:0db8:85a3:08d3:1319:8a2e:0370:7334`
- User friendly! Easy to remember!
- "Helpful" Shortcuts:
  - Omit leading zeros in a group (`0005:0db8:`… is equivalent to `5:db8:`…)
  - Collapse groups of all-zeros with :: (`2001:0000:0000:0000:0000:8a2e:0370:7334` is equivalent to `2001::8a2e:0370:7334`)

IPv6 – Routing

- How can having bigger IP addresses (128 bits) make routing easier?
  - Larger address space allows more intelligent network organization
    - Addresses match physical network organization
    - Collapse routing table entries
- Many competing proposals on the details…
- Basic constraint on all designs
  - Use upper 64 bits for routing
  - Use lower 64 bits for interface ID
(clients pick this randomly or based on MAC address)

IPv6 – Routing (RFC 2374)

- Option 1 – Hierarchical assignment

FP (3)	TLA ID (13)	RES (8)	NLA ID (24)	SLA ID (16)	Interface (64)

Public Topology ⟷ Site Topology

  - FP: Format Prefix (allows other address structures)
  - TLA: Top-Level Aggregation
  - RES: Reserved (for TLA / NLA growth)
  - NLA: Next-Level Aggregation
  - SLA: Site-Level Aggregation
  - Interface ID

- How does this structure simplify router design and operation?

IPv6 – Routing (RFC 3587)

- Option 2 – Ad-hoc Address Space

Global Routing Prefix (n)	Subnet ID (64-n)	Interface (64)

  - Regional Registries will use a coordinated allocation policy to assign global IDs
  - Global prefix will probably have some kind of hierarchical structure
- How does this structure affect router design / operation?

IPv6 - Routing

- The second design (3587) was chosen
- Why?
  - Maximum flexibility for upper 64 bits? (past predictions of network organization have been very unreliable)
  - Unable to achieve design consensus among all the competing entities?
  - Router manufacturers lobbying for the most expensive option?

Routing

- Besides the address layout, how does IPv6 make routing easier?
  - No checksum calculation
  - No fragmentation
  - Infrequently used headers are optional
- How does IPv6 make routing harder?
  - Forwarding table entries 2x-4x larger
  - Need to route both IPv4 and IPv6 for the foreseeable future

Deployment

- Why should I deploy IPv6 today?
  - My customers can reach anywhere on the Internet today
  - Google, CNN, etc… will always be reachable
  - Only new applications / users will suffer
- How do I deploy IPv6?
  - Flip a switch across the internet?
- Legacy routers may not be upgradeable
  - Hardware implementations are fixed
  - Software implementations may be insufficiently capable (either incapable or only at low performance)
- Islands of IPv6 in the sea of IPv4
  - Dual network stacks support both IPv4 and IPv6
  - Tunnel IPv6 across IPv4 networks
- Need to upgrade other systems
  - DHCP
  - DNS (ICANN updated 6 of 13 root nameservers in February 2008)
  - Firewalls, traffic shapers, etc.

IPv6 – Original Plan

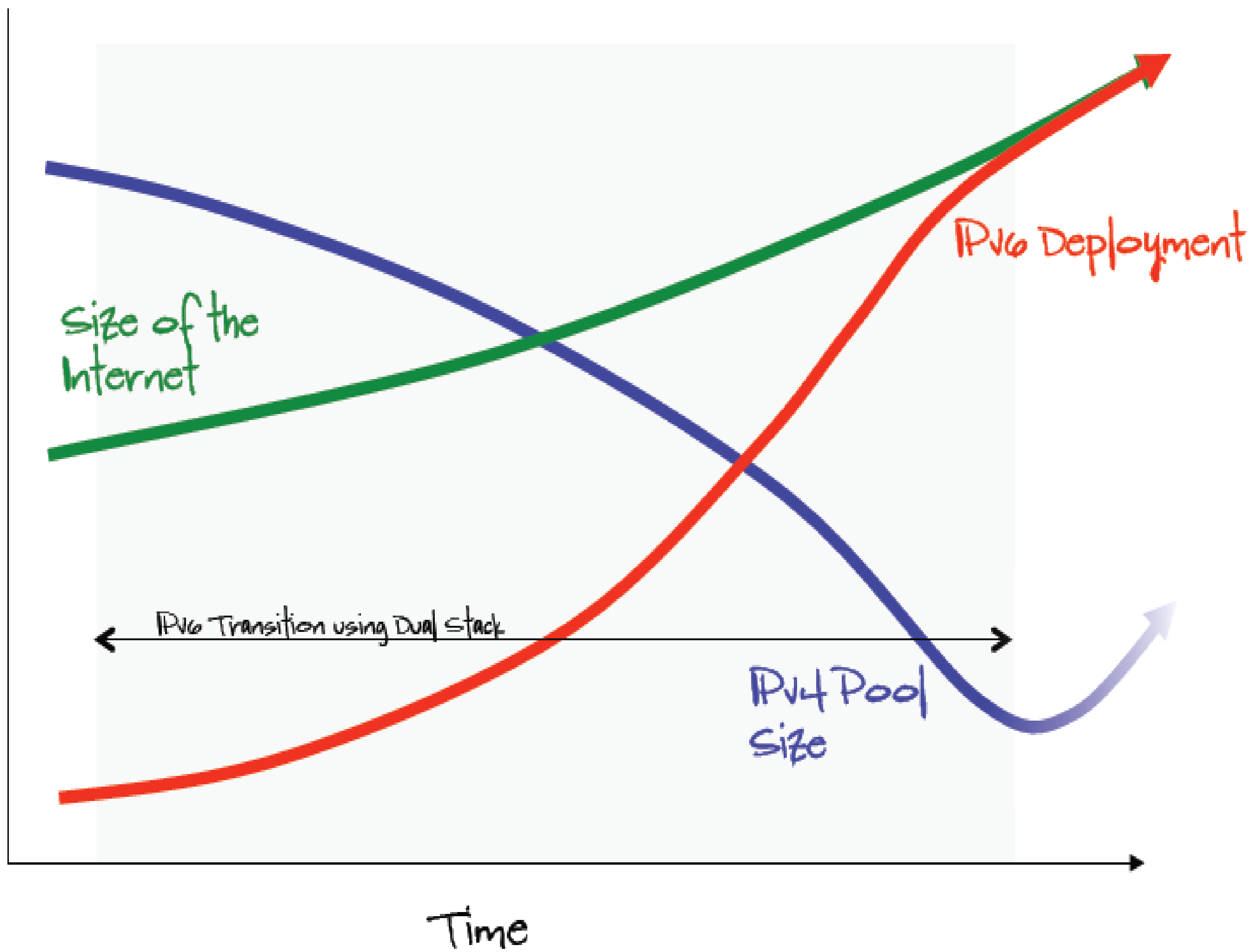
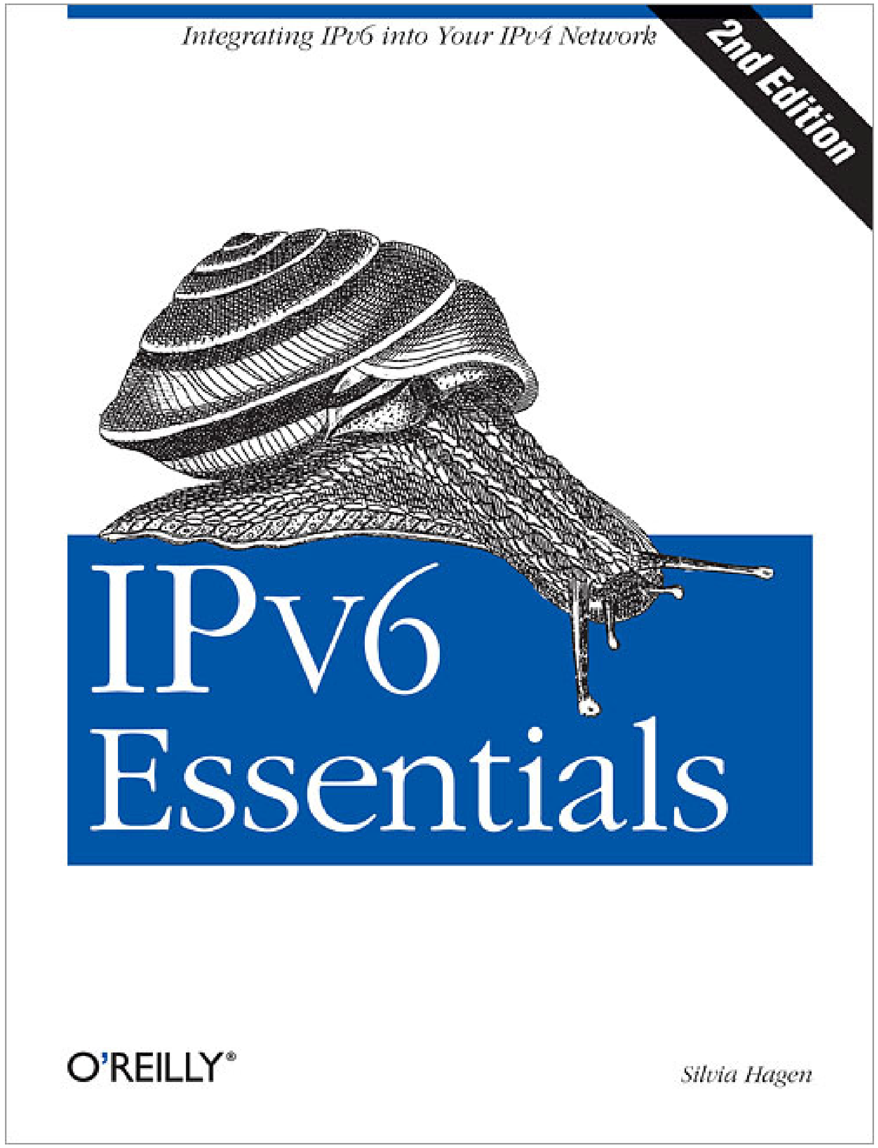


Figure from http://www.potaroo.net/presentations/2008-11-17-ipv6-failure.pdf

IPv6 – Current Status



IPv6 – The New "Plan" (?)

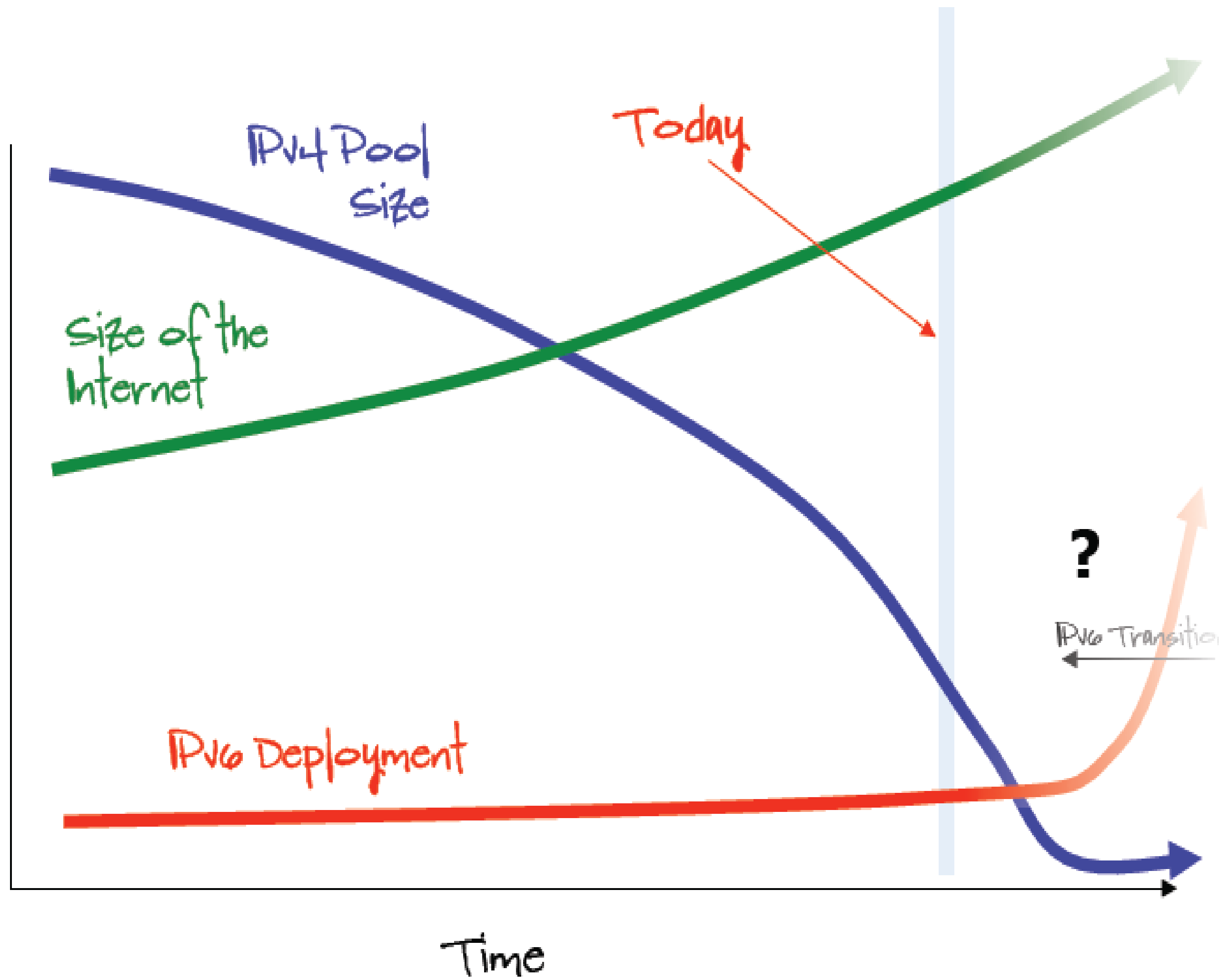
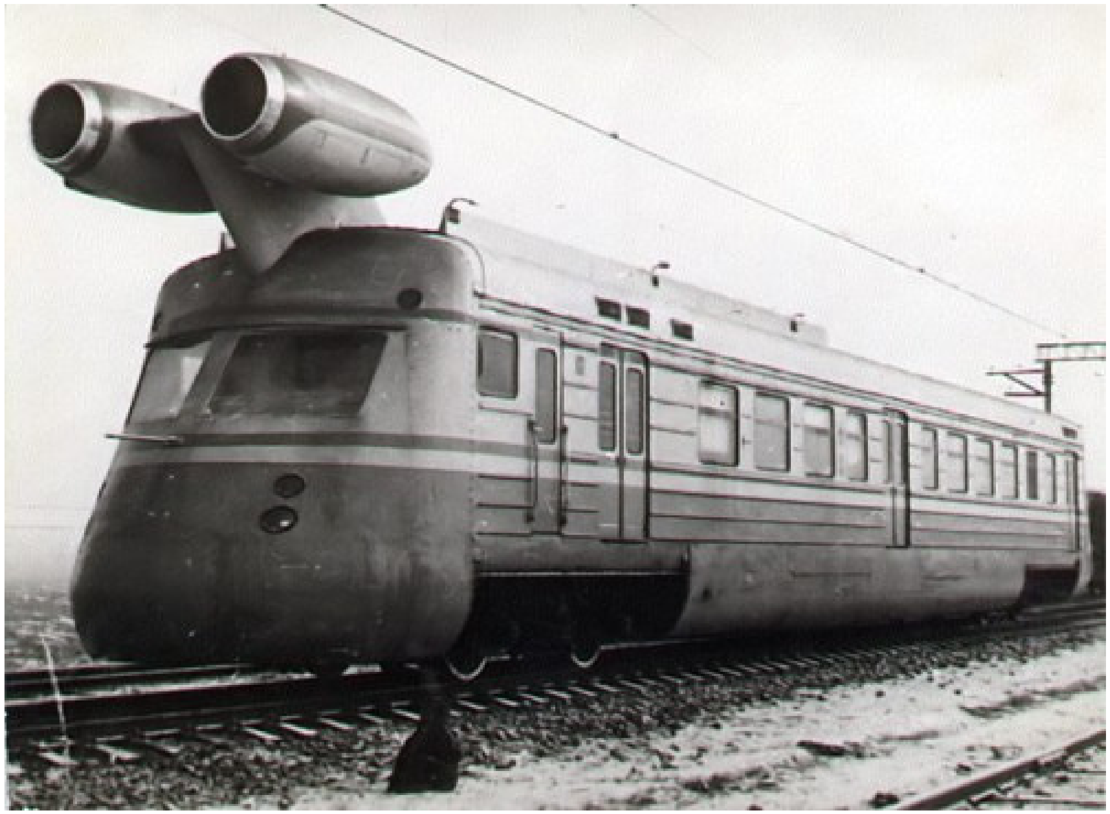


Figure from http://www.potaroo.net/presentations/2008-11-17-ipv6-failure.pdf

IPv6 – Failure is an Option



Is this IPv6?

IPv6 – Failure is an Option

- What happens if IPv6 “fails”?
  - Failure is defined as anything less than a complete migration from IPv4 to IPv6
  - Do we stop allowing new hosts to connect to the internet?
- What about using NAT?
  - Observation: Only 5-20% of assigned IPs are actually used by hosts.
  - Solution: Use lots of NAT to reclaim unused addressed
- What happens if this works, and we build “carrier-grade” NAT everywhere?
  - No more end-to-end connectivity?
  - Need coordination with ISP to deploy new services?
  - New opportunities for ISPs to filter traffic and charge for services?

•http://www.potaroo.net/presentations/2008-11-17-ipv6-failure.pdf

IPv6 – Failure is an Option

- If an organization deploys NAT extensively, how can you get them to give up the reclaimed addresses?
- IP Address Marketplace
  - Can we create a marketplace? (Currently “forbidden” to sell IP blocks)
  - Imagine: *“For Sale: One Lightly-Used IP Block (only used by grandma to check email on Sunday)”*
  - Same problems as buying a used car:
    - Does the person selling the IP block actually “own” it?
    - What is the condition of the IP block? (If used for spam or illicit activity, IP block may be in blacklists worldwide)

•http://www.potaroo.net/presentations/2008-11-17-ipv6-failure.pdf

Bonus Material

IPv6 – Security

- What are the security implications of having a huge (sparse) address space?
  - Security through obscurity
  - Random address scanning by worms is ineffective
  - Targeted scanning still works great, though…
    - Could detect hosts by listing to P2P networks

IPv6 – Security (IPsec)

- IPsec features
  - Data encryption – Data cannot be read or modified
  - Host authentication
  - Anti-replay – Captured packets cannot be reused by an attacker

- What are the strengths and weaknesses of putting security at the IP layer? (Doesn't SSL work fine?)
  - Security is independent of higher layers (either applications or protocols like TCP/UDP)
  - Encryption overhead is incurred per-packet (high!)
- Why is IPsec optional in IPv4, and required in IPv6?
  - Security was not a major concern in original network design

IPv6 – Special Addresses

- Link Local
  - Scope limited to single network segment / link
  - Application: Network configuration, device discovery
  - Address matches `fe80::/10`
- Site local
  - Scope limited to single organization (similar to private IPv4 addresses)
  - Purpose: Each organization can randomly pick their own address instead of everyone using same range of private IPv4 addresses
  - Address matches `fc00::/7`
- Multicast
  - Address matches `ff00::/8`

IPv6 - Autoconfiguration

- How does a new host determine its IP address?
- Stateless IP address autoconfiguration
  - Host sends out multicast Router Solicitation
  - Router(s) reply with their subnet and gateway information
  - Host constructs IP address(es)
    - Upper 64 bits – From router(s)
    - Lower 64 bits – Client generates based on MAC address (or picks randomly)
- Do we still need DHCP?
  - How do you determine your DNS server?