IPv6 World Update: Strategy & Tactics

Kenneth Geers Alexander Eisen

October 5, 2006 Tokyo

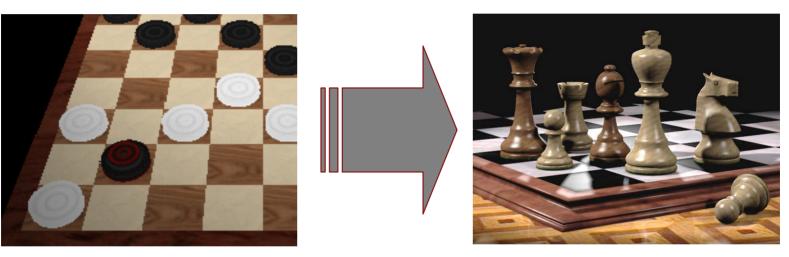
Why? 4.2 billion Reasons

- Government mandates and deadlines Today!
- Address Space
 v4 exhaustion, 340 *undecillion* global IPs
- 3. Security Concerns Increased attack surface, privacy, detection
- 4. New Paradigm

Everything is addressable, trusted vs. untrusted networks, end-to-end

v6 Era

- Wild West now, Utopia later?
- New model:



- Advanced Features | Galactic Scalability | Extensibility
- Telematics
 - Billions of "always on, always connected" devices
 - Convenient / efficient / entertaining life

v6 Networks of the Future

Jupiter Surface Net 5020::

Mars-Venus Net

Earth Orbital Net

Ring1 Net 6031:: Ring2 Net 6032:: Ring3 Net 6033::

v6 Criticism

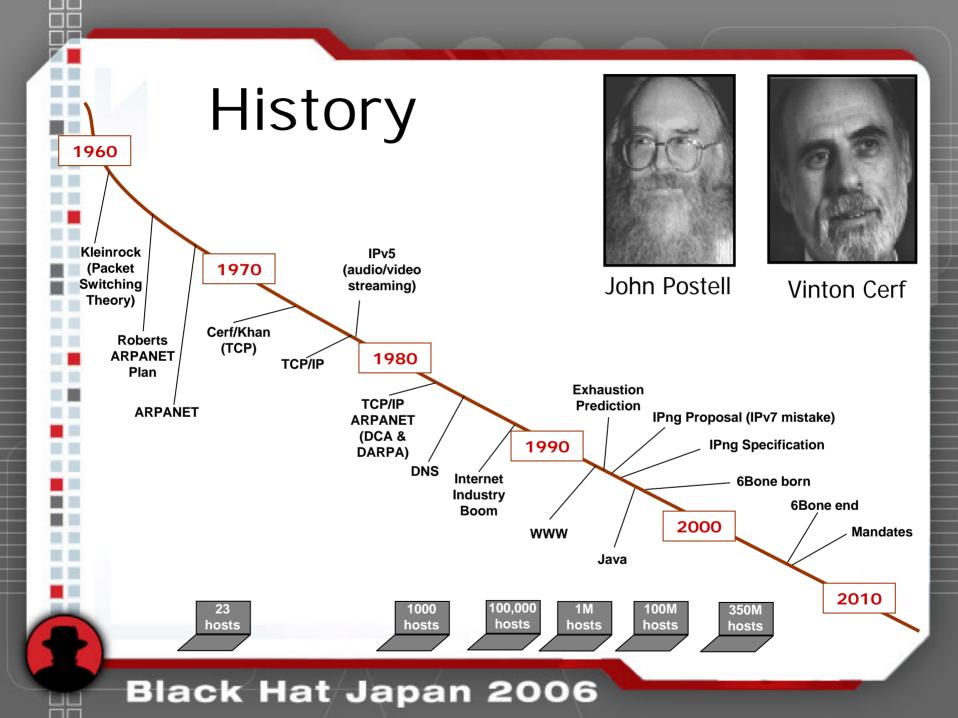
- Why is adoption slow?
 - Education, Understanding, Demand
- Marketing Hype?
- Better solutions exist?
- Tremendous and onerous change
 - IPv4 can't talk directly to IPv6
 - Expen\$ive
 - Affect almost everything

IPv4 battle & evolution

GOSSIP	GOSSIP Bloated, complex, liked by vendors due to longer/larger contracts to support it.	
	versus	
IP	IP won; "dumb" but resilient protocol. Robust design survived for 20+ years.	

IPv4 running out of address space NAT: workaround & security (by obscurity)

IPSec & many other features backported from v6 and retarded the upgrade



IPv6 Addressing

- IPv4: 32-bit \rightarrow 2³²= 4,294,967,296
- IPv6: 128-bit → 2¹²⁸ = 340,282,366,920,938, 463,463,374,607,431,768,211,456
- = ~340 undecillion
- Almost half of ~10⁹⁸ atoms in entire universe
- 50 octillion IPs for each of the roughly 6.5 billion people alive today
- Notation: 0 groups can be shortened to ::
 - 2001:0db8:0000:0000:0000:1428:57ab
 - 2001:0db8::1428:57ab

IPv6 Packet Structure

Extension headers

- User customization
- Extremely powerful for developers
- QoS, fragmentation, multi-cast, jumbograms
 - "Frequency hopping" possible by rotating encryption keys

IPv4 Packet Header

IP Version Number (4)	IHL (4 Bits)	Type of Service (8 Bits)		Total Length (16 Bits)
Identification (16 Bits) Flags (4		s (4 Bits)	4 Bits) Fragment Offset (12 Bi	
Time to Live (8 Bits)	(8 Bits) Protoco		s) Header Checksum (16 Bits	
	Sou	rce Address (32	Bits)	
	Destin	ation Address (3	2 Bits)	
Options (varia		Padding (variable)		

IPv6 Packet Header

IP Version Number (6)	Traffic Class (8 Bits)	Flow Label (20 Bits)			
Payload Length (16 bits)	Next Header (8 Bits)	Hop Limit (8 Bits)			
Source Address (128 Bits)					
Destination Address (128 Bits)					

IPv6 Packet Structure

<-----> Encrypted----->

IPv6 Hop-by-Hop Header Extension H		ESP Extension Header	Transport Header (TCP, etc.)	Payload	
---------------------------------------	--	-------------------------	---------------------------------	---------	--

What is gone in New Design

- Header is still in the clear
- No IP ID field:

Nice uptime check

No IP Record Route Option:

traceroute alternative anymore

No Broadcast addresses:

Multicast instead but cannot be destined from remote

"Built-in" Security Myths?

- Crypto friendliness
 - "Mandatory" IPSec
- Support required in stacks but implementation in deployment is OPTIONAL

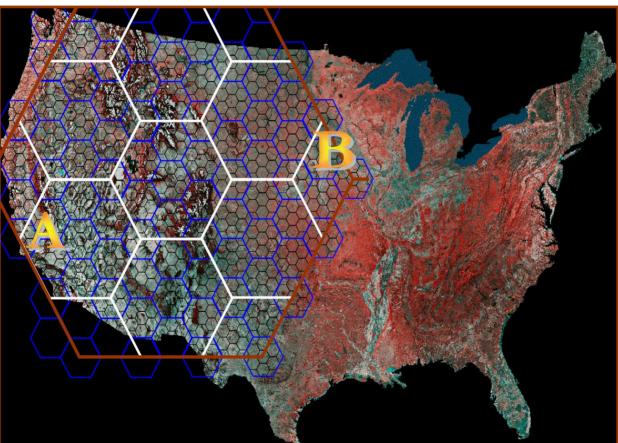


- Not widely deployed except in BGP tunnels between routers
- PKI rarely succeeded in a massive scalable deployment
- Very difficult, resource intensive and expensive to deploy (e.g. PKI)

IPv6 Advances ;)

- Resistance to scanning due to sparse allocation
 - Ping sweep of a subnet may take 500 million years!
 - Resistance to self propagating worms
- Auto Configuration makes it easy
 - Welcoming technologies
 - Mobility | Ad-hoc | Security
 - Enhanced routing

Hierarchical Address Allocation & Optimized Routing



Bulk sessions Based on Geo-prefix

IPv6 Hazards ;(

- Goodbye NAT!
- Migration technologies (tunneling AND/OR Dual-Stack) add complexity and larger attack surface
- Applications are still at risk
- Attacks more evasive
 - Awareness, understanding, training is far behind

National Security Issues

- Network-centric warfare
- Will IPv6 give governments more or less control of their populations?
- Ownership of Certificate Authorities & Ownership of IPSec Keys
- Real-World Example: MetroNet 6

USA: IPv6 Mandate

- USA behind in race to Next Gen Internet?
 Same government, conflicting messages
- Office of Management and Budget (OMB)
 "IPv6 compliant" by June 30, 2008
- Department of Commerce (DoC)
 Higher costs and *reduced* security?
- American Competitiveness Initiative (ACI)

American Corporations

- Little overall pressure to switch
 - Own majority of IPv4 space
- Pockets of v4 / NAT criticism
 - Developer time, rendezvous servers = \$
- Investment: CI, Hughes, Bechtel, Carlyle
- Microsoft
 - Vista: IPv6 default!
 - MS: \$100M to further Vista applications

People's Republic of China

- Population necessitates more IP addresses
- IPv6 now PRC national strategy
- Intellectual Property (IP) development
- China Next Generation Internet (CNGI)
- China Education and Research Network (CERNET)

IPv6 transition remains sluggish

PRC: Politics and the Internet

- Can IPv6 help PRC squash political dissent?
 Internet police, dissident video smuggling
- Internet Society chairwoman Hu Qiheng:
 - "No anonymity", tracking via static v6 IPs
- Western company cooperation with PRC
 - Google, Yahoo, Microsoft
 - U.S. congressman: "Sickening and evil"

Europe

Ericsson: first IPv6 router, 1995



- European IPv6 Task Force
 - Importance cannot be overestimated."
- IPv6 Wireless Internet Initiative (6WINIT)
- Companies seeking rewards, incentives
 - IPv6 Car (Cisco and Renault)

Japan

- IT leadership, investment important
- Billions of electronic gadgets to address
- 2000: Japanese PM announces "eJapan 2005"
- Japan has commercial v6 services available now
- U. Tokyo: v4 and v6 World Speed records!

Elsewhere in the World

- India
 - Currently behind up to 5 layers of NAT!
 - National or nationalist v6 testbed?
- South Korea
 - Moving quickly, v6 partnership with EU
- Africa: some countries own < 2,000 IPs!</p>
- Trends in international cooperation

Interim Analysis

PRC

- Significant investment, initiatives
- But, different economic models
- Influencing IPv6 standards
- Moving too fast on IPv6?



- USA
 - Despite mandates, position lacks clarity
 - However, heavy industry investment
 - Learning lessons from other countries?



Is collaboration possible?

IPv6 Deployment

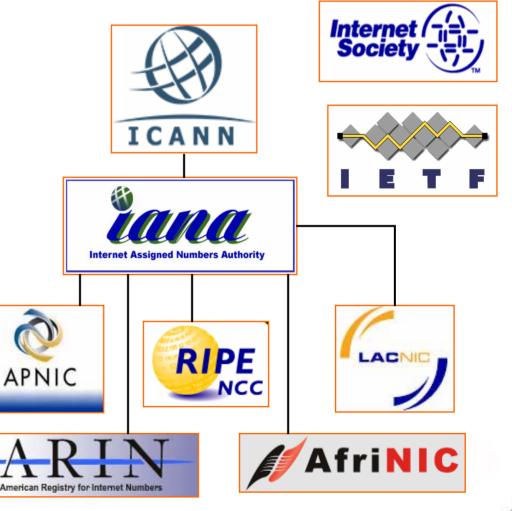
- Publicly accessible Internet has only a tiny allocation of v6 addresses so far
- Adoption slow due to introduction of NAT
 - Alleviates address exhaustion
 - 1999: The IPv6 Forum was founded by the IETF
 - Worldwide, 30 IPv6 Country Fora and Task Forces
 - 2004: ICANN announced that the root DNS servers for the Internet had been modified to support both IPv6 and IPv4
 - 6bone testbed retired

"IPv6" in Government Domains

USA 30,200 South Korea 26,600 China 20,200 Japan 7,740 Taiwan 3,520 Brazil 2,040 France 479 India 92 Russia 38 Israel 28 Iran 14 South Africa 10 Saudi Arabia 3 Czech Republic 0

Internet Management

http://www.icann.org/ http://www.iana.org/ http://www.ietf.org/ http://www.isoc.org/ http://www.arin.net/ http://www.afrinic.net/ http://www.apnic.net/ http://lacnic.net/ http://www.ripe.net/



IANA IPv6 Strategy

- Aggregation: distributed in a hierarchical manner, according to the topology of network infrastructure, to permit the aggregation of routing information by ISPs, and to limit the expansion of Internet routing tables
- Uniqueness: every assignment must be unique worldwide
- Registration: in a registry database accessible by the Internet community (within the context of reasonable privacy considerations and applicable laws)
- Seek: "fair" distribution, contiguity of addresses
- Avoid: fragmentation, wasteful practices, stockpiling of unused addresses, overhead

Privacy and Anonymity

- Asia
 - Less privacy in daily life
 - Lower expectations of privacy for IPv6
- Europe
 - Significant expectations of privacy
 - Highly motivated to protect anonymity
- USA
 - Somewhere in the middle
 - Banking and finance must be secure
 - Desire to go after criminals

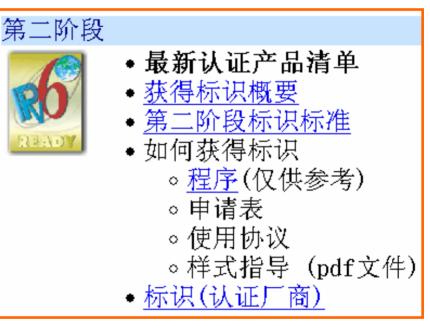
More on Privacy

- Net Neutrality (CA ownership)
- Criminal / Law Enforcement attack attribution
- Traceability and privacy (Privacy Address Scheme)
- State and Corporate boundaries
- IPSec paradox?!

IPv6 Standards & Certifications

IPv6 Ready Logo

- Host
- Router
- Operating System
- Protocol Stack
- Special Devices



Cost Analysis

- What will the IPv6 transition cost you? What is your ROI?
 - \$25, \$75 billion ... or free?
- Tech Refresh cycles could cover much of cost
 - Hardware, Software and Human
- VoIP, NAT, eCommerce savings potentially significant
 - Stack integration, interoperability over band-aids
- Comparison: Y2K and IPv6
 - Smart resource decisions, niche Sys Admin skills

Transition Mechanisms and Environments

- v4 native
- v6 over v4 tunneling
- dual-stack
- native v6
- v4 (legacy) over v6 tunneling

SIT 6over4 6to4 ISATAP Teredo

Myriad Security Concerns

- Many devices OSs are enabled by default! (try ping ::1)
- Input validation for v6 IPs [] and :: needed for applications *
- Autoconfiguration tracking assets difficult?
- Elimination of NAT
- Link local issues
- Multicast addresses
 - Many common IPv4 vulnerabilities remain

Larger Attack Surface

- Especially during migration!
- More hosts per enterprises, more NICs per host, more stacks per NIC
- Managing masses of tunnels and IPSec sessions
- Multi-homed hosts
 - Dual-Stack

Proxy-ing & translation

Trends in Targeting

- CAs and DNS will become primary targets
- Method: Compromise DNS, then hop from LAN to LAN
- More client-side exploits
 - Native (but rare) IPSec reduces exposure
 - Sniffing & MITM harder but traceback easier

Traffic Monitoring

- Sensors blind
- Tunneling, Automatic tunneling
- "6to4" as with Protocol 41 encapsulation
- UDP to cross NATed devices that block protocol 41
 - Example: Teredo on XP SP2
- Popular today to cloak attacks. Apps can bind(*) to grab a v6 socket in a *.* LISTEN state
- Cannot be detected by port scanning, most sensors can recognize protocol 41 but not interpret it

Rise of the Machines

- Carbon life forms
- Average new hires → 2-4 yrs of TCP/IPv4; ZERO IPv6
- Nickname for ::
- Not user-friendly notation v6 address?
 - Silicon life forms
- Hardware | Software | Appliances
 - OSs | Applications

MS Windows Vista Beta 2			
Initialiet settings are now turned on by derault initialiet settings are less secure	them Internet extrine Clinkfor entires		
THE IPv6 PORTAL	Properties General newsroom_sel.gif		
You are using IPv6 from 19:20 4 8 2006 2002:1878:8308::1878:8308 10 10 10 10	Protocol: [ICDoP][22L:22272Te×2 ??a?24?4*?fót7?64 !!! !!!] Type: GIF Image Address: http:// (URL) [2001:7f9:1000:1::103]/images/newsroom_sel.gff Size: 365 bytes Dimensions: 70 x 20 pixels		
	Created: 8/3/2006		

Black Hat Japan 2006

HH

100

Hacker Toolbox (1)

- Method: Compromise DNS, then hop from LAN to LAN
- Network Reconnaissance and Discovery
 - Port Bouncers

- Denial-of-Service (connection flooding)
- Packet crafting
 - Spoofing, Man-in-the-middle attacks

Hacker Toolbox (2)

- Parasite6: MTM tool that leverages IPv6
- Dos-new-ipv6: sucks up all available addresses
- Fake_router6: MTM, abuses the RA by becoming the default router
- No v4 broadcasting in v6! (multicast instead)
 - Smurf6: to attack your own LAN
 - Rsmurf6: reverses the login, one-toone-to-many attack
 - Redir6: abuses ICMP redirect as in IPv4

Black Hat Japan 2006

Suite

THC IPv6 Attack

Are You IPv6 Ready?

- Determining "compliance"
 - USG mandate: Core networks only
 - By 2008, little real progress
- The IPv6 Ready Logo
 - Politics highly charged
 - PRC argued against IPSec inclusion
 - IPSec now *optional* to earn Logo
- Enormous implications for privacy!
 - Could USA and EU have pushed harder?

Recommendations

- Turn it off! Allow and authorize base on need
 - Native, tunneling (Protocol 41) and block Teredo UDP port 3544
- Develop policy and a training plan
 - Begin now, but do not move too fast!
 - Budget, expertise, SW, HW concerns
 - Get a small number of staff up to speed
 - Ensure that the transition is controlled
 - Calculate your Return on Investment
- Identify IP-enabled devices
 - Scan and enumerate (remember Y2K?)
 - Many will need outside support
- Make smart resource decisions
 - Upgrade through Tech Refresh
 - Let IPv6 help solve current problems
 - Should I upgrade or ditch certain products?
 - Watch security developments, minimize disruption

v6-pack & carputer projects



- IPv6-enabled refrigerator add-on device to inventory beer
- mini-ITX platform
- Automatically send email alerts when supply is low (via analog sensor and USB interface board



Copyright © 2003 David Farley, d-farley@ibiblio.org http://ibiblio.org/Dave/drfun.html



The brave new world of IPv6