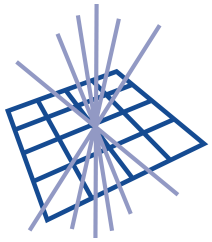
Science & Technology Facilities Council

IT security in an IPv6 world

David Kelsey (STFC-RAL)

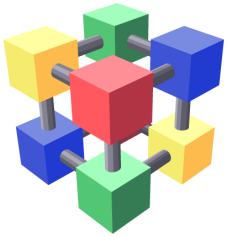
GridKa School, KIT

7 Sep 2015



GridPP

UK Computing for Particle Physics



WLCG

David Kelsey

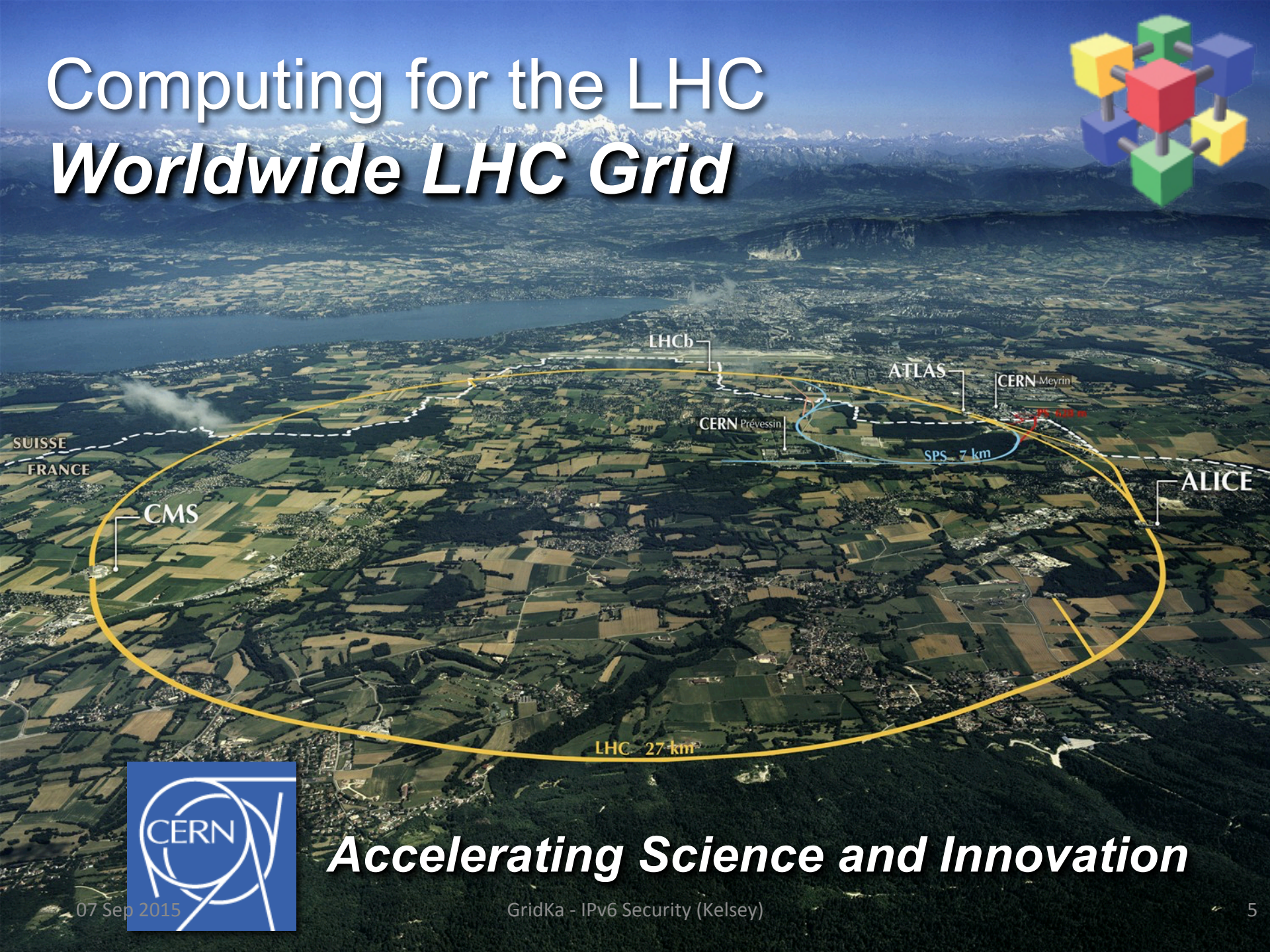
- Leader HEP computing group at STFC-RAL (UK)
  - We run a WLCG/GridPP Tier 1 and Tier 2 sites
- Not a security or networking technical professional!
  - BUT lots of experience working with experts
  - Networking – HEP DECnet/OSI, HEPiX IPv6 working group
  - Security Operations and Policy (WLCG, EGI, GridPP, IGTF…)
- Here, I am sharing my personal views
  - HEPiX WG yet to formulate its “official” site guidance
  - EGI security team just started on IPv6 issues

Outline

- Introduction to WLCG, IPv6 and IT security
- Some IPv6 security threats
- Some IPv6 protocol attacks
- Issues for site network/security teams
- Issues for sys admins
- Where to find more information
- Summary and outlook

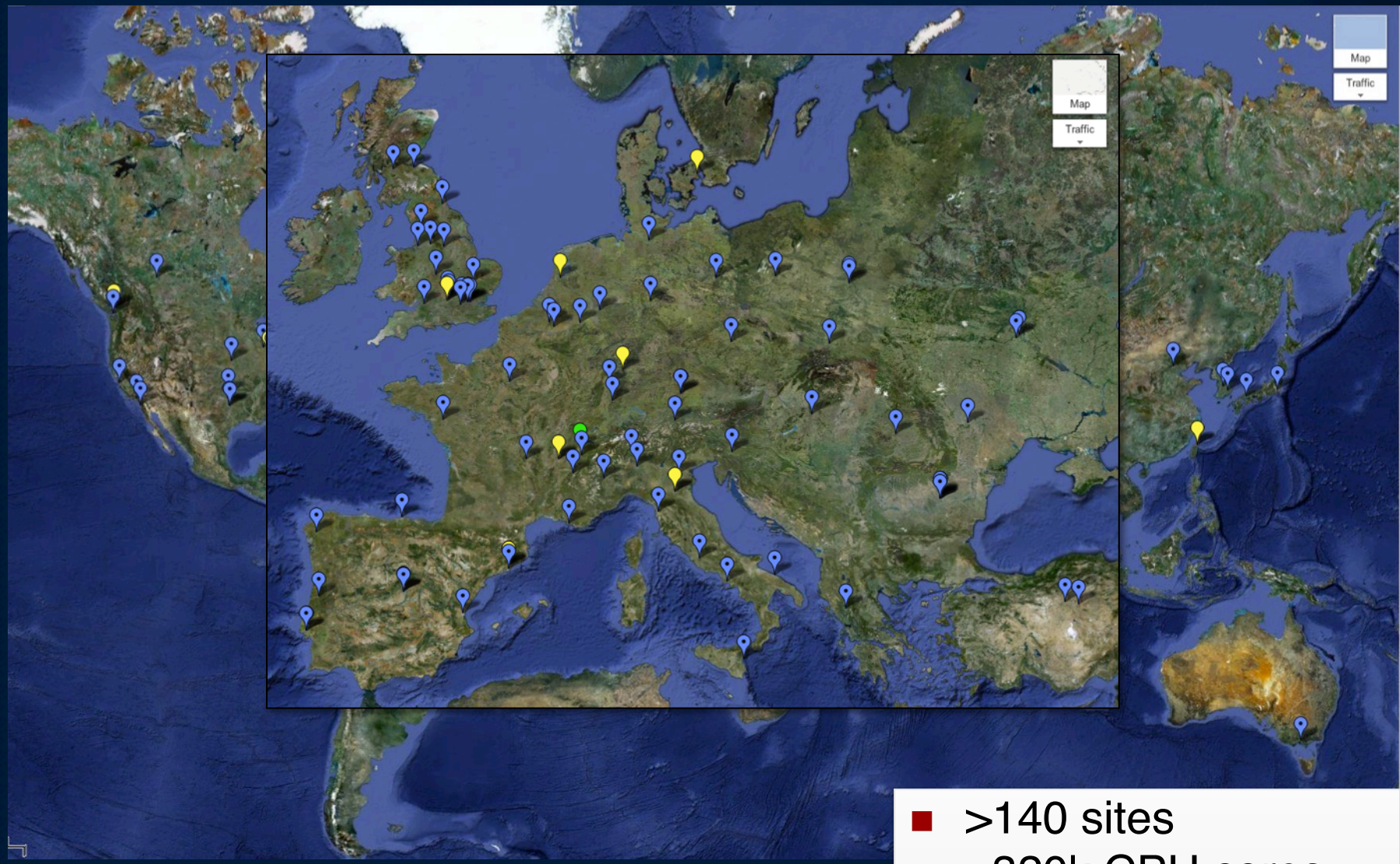
Introduction:
WLCG, IPv6, IT security

Computing for the LHC
Worldwide LHC Grid



Accelerating Science and Innovation

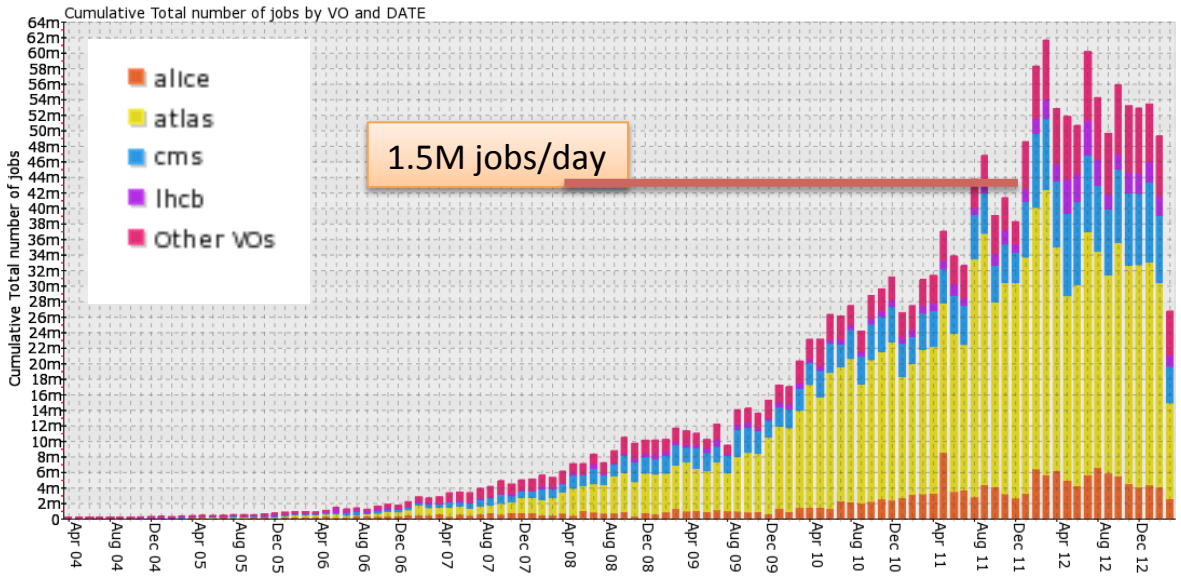
WLCG Grid Sites – Run 1



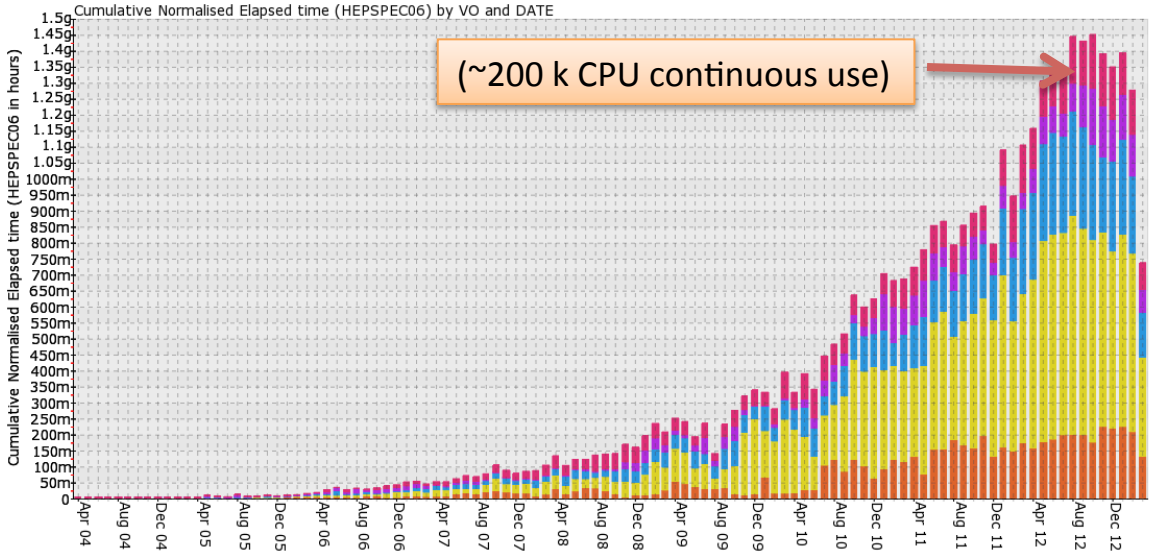
Tier 0 Tier 1 Tier 2

- >140 sites
- >320k CPU cores
- >150 PB disk

Processing WLCG - Run 1



Usage continues to grow…
- # jobs/day
- CPU usage



>150,000 years of CPU delivered each year

WLCG Worldwide LHC Computing Grid

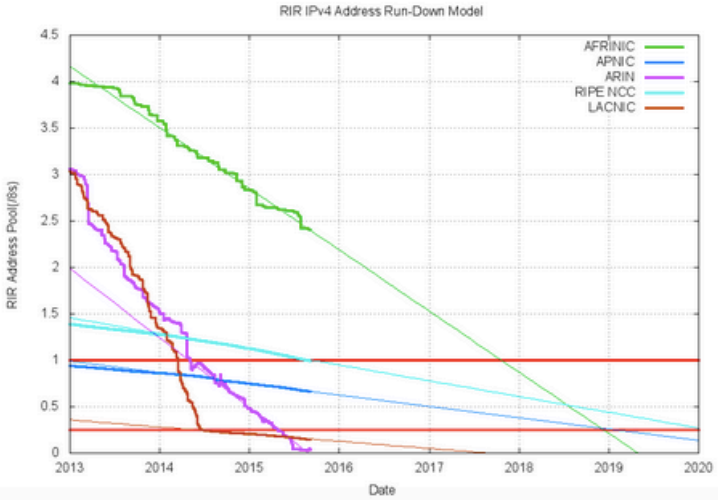
IPv4 address exhaustion

This report generated at 05-Sep-2015 08:26 UTC.

IANA Unallocated Address Pool Exhaustion:
03-Feb-2011

Projected RIR Address Pool Exhaustion Dates:

RIR	Projected Exhaustion Date	Remaining Addresses in RIR Pool (/8s)
APNIC:	**19-Apr-2011** (actual)	0.6645
RIPE NCC:	**14-Sep-2012** (actual)	0.9937
LACNIC:	**10-Jun-2014** (actual)	0.1455
ARIN:	**07-Sep-2015**	0.0013
AFRINIC:	**19-May-2019**	2.4089



Projection of consumption of Remaining RIR Address Pools

http://www.potaroo.net/tools/ipv4/

IPv6

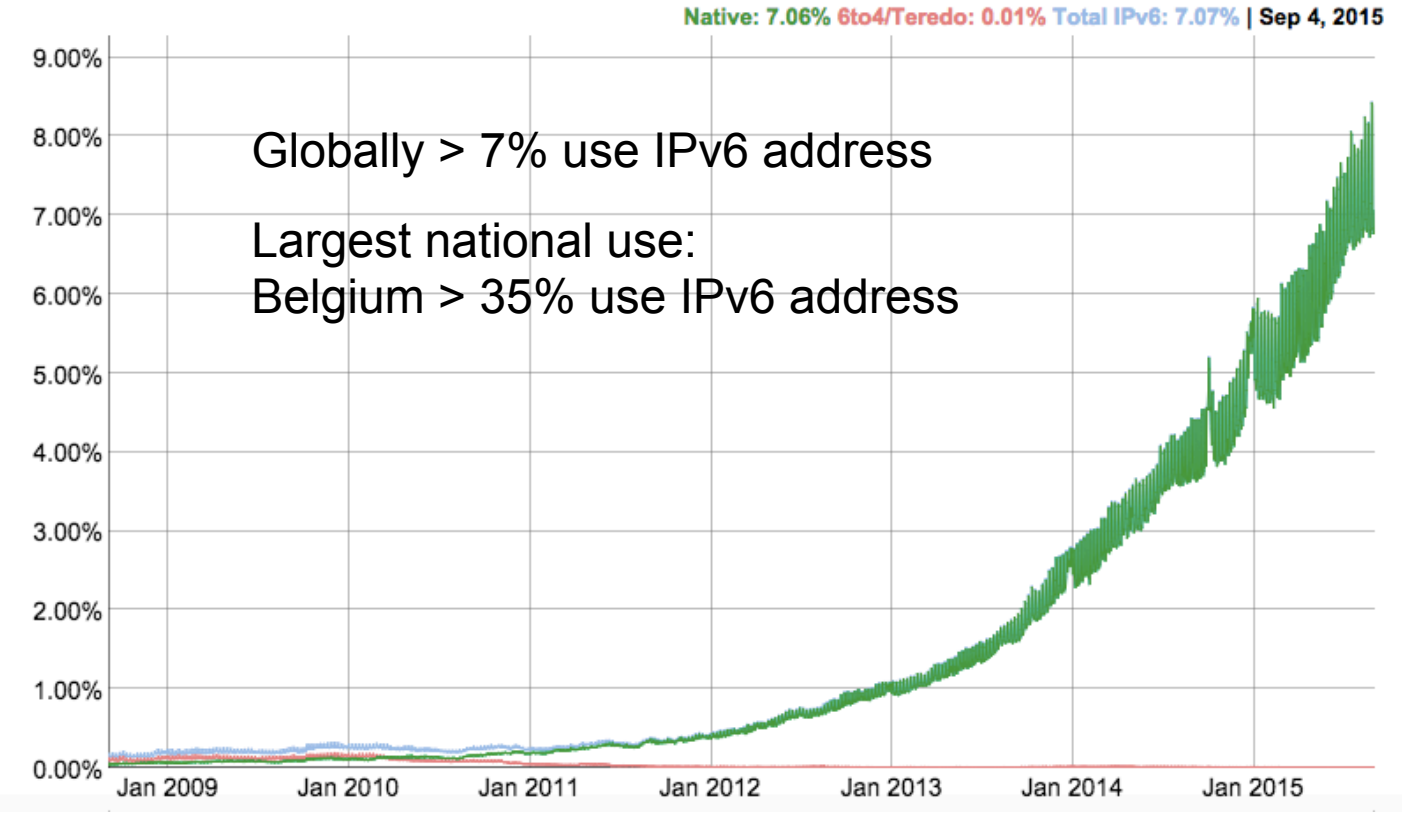
- **Internet Protocol, Version 6 (IPv6) Specification – December 1998 (RFC2460)**
  - Previously known as IPng (started Oct 1993)
  - Successor to IPv4
  - *https://tools.ietf.org/rfc/rfc2460.txt*
- Much larger address space 32 bit to 128 bit
- An opportunity to address other problems
  - E.g. security!

IPv6 growth (global Google clients)

https://www.google.com/intl/en/ipv6/statistics.html

IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.



Globally > 7% use IPv6 address

Largest national use:
Belgium > 35% use IPv6 address

New features of IPv6

- Larger address space
- Streamlined protocol headers
- Stateless auto-configuration
- Multicast
- Jumbograms
- Network layer security
- Quality of Service
- Anycast
- Mobility

IP addresses

Edoardo Martelli (CERN)

IPv4

32 bits

Written as 4 groups of 8 bits, decimal notation:

137.138.10.16

(correspond to: 89.8A.0A.10 Hex)

IPv6

128 bits

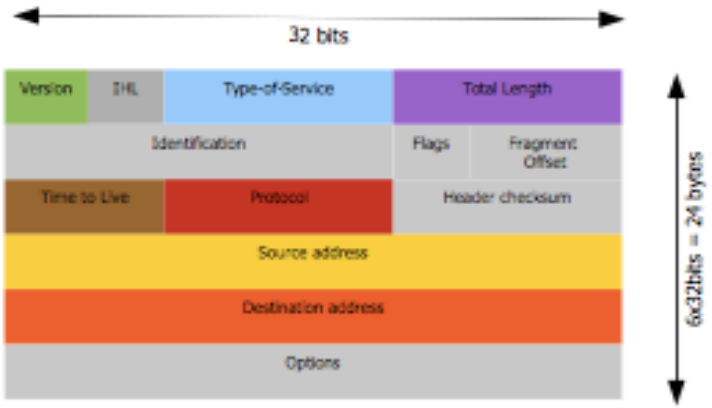
Written as 8 groups of 16 bits, hexadecimal notation:

2001:0db8:a137:b138:c000:d000:e000:f001

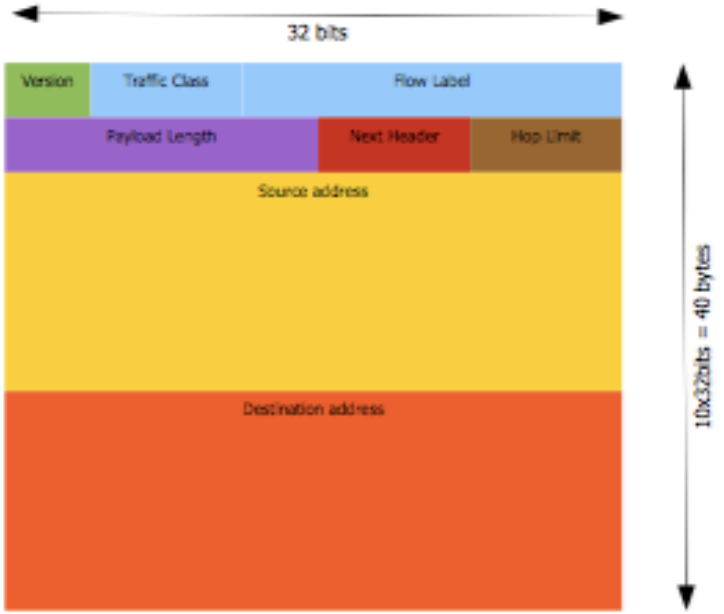
IP headers

Edoardo Martelli (CERN)

IPv4 header



IPv6 header



[http://tools.ietf.org/html/rfc2460]

IPv6 Neighbor Discovery

NDP

NDP specifies 5 types of ICMP packets:

- **Router Advertisement (RA)**: periodic advertisement of the availability of a router
- **Router Solicitation (RS)**: the host needs RA immediately (at boot time)
- **Neighbor Solicitation (NS)**: to determine the link-layer address of a neighbor (equivalent to ARP request)
- **Neighbor Advertisement (NA)**: answer to a NS packet (equivalent to ARP reply)
- **Redirect**: Used by a router to inform a host of a better route to a given destination

[http://tools.ietf.org/html/rfc4861]

Edoardo Martelli (CERN)

WLCG – why use IPv6?

- HEPiX IPv6 working group started work in 2011
  - To assess, evaluate, test and plan
- Sites beginning to run out of routable IPv4 addresses (2014)
  - Large increase in use of virtualisation, multi-cores, etc.
  - ~ 10% of sites report potential shortage of IPv4 addresses (incl. CERN)
- Decided in 2012 that WLCG should move asap to dual-stack services
  - To support IPv6-only clients
- A major activity
  - Need to consider all software, applications, operational tools
  - Only now, are storage systems fully supporting IPv6
  - Operational Security – an important issue!

IT security standards

- Keep services & data running and secure
  - Availability, Confidentiality, Integrity
- Standards-based approach - ISO 27K, NIST 800-53, …
- Security risk assessment is crucial
  - Concentrate on most likely and highest impact issues
- Mitigations: A security plan with controls
- Technical, operational and management controls
- Handle incidents and vulnerabilities to keep services up
- An ongoing process!

Problems with IPv4 security

- Design favoured interoperability over
  - Confidentiality, integrity, availability
  - No cryptographic protection from eavesdropping or manipulation
  - No end to end authentication
- New technologies were added along the way
  - E.g. SSL/TLS, IPsec
- With IPv6 these were designed in as mandatory components

IPv6 Security

IPv6 security pros/cons

- Advantages of a new design
  - Security:important part of the IPv6 initial design
- Down-sides
  - Lack of maturity
  - New vulnerabilities and attack vectors
  - Need IPv6-compliant monitoring and tools
  - Lack of education and experience
  - Problems of transition – dual-stack, tunnels
- BUT - Many threats/attacks happen at layers above/below the network layer
  - And are therefore exactly the same as in IPv4
  - Malware, phishing, buffer overflows, cross-site scripting, DDoS etc etc

Immediate IPv6 concerns

- IPv6 may be on by default (and not controlled or monitored)
- End systems have multiple addresses
- Searching logs will not always work
  - Formatting when writing the logs is still broken
  - Same address but different formats (drop zero or not)
- What is wrong with tunnels?
  - Site may not be in control
  - Tunnels traverse the IPv4 perimeter firewall and NAT gateways
- Reputation-based (IP address) web protection does not fully exist for IPv6

IPv6 security myths

- Internet Society has published 10 myths of IPv6 security
- https://www.internetsociety.org/deploy360/blog/tag/ipv6-security-myths/
- **Myth 2: IPv6 has security designed In**
- **Reality: IPv6 was designed 15-20 years ago**

IPsec

- Was first developed in 1995 for IPv4 internet layer
  - SSL and TLS operate at Application Layer
- A framework of standards
  - End to end authentication, data integrity and privacy (encryption)
- Can be used site to site (gateway to gateway)
  - As a Virtual Private Network (VPN)
- Or host to host
- All major aspects are same in IPv6 as IPv4
- Does not fully support protection for multicast traffic
  - Key management is one-to-one
- **No longer mandatory** (rfc6434 – MUST -> SHOULD)

IPv6 problems in IPv4-only world

- Turned on by default on many Operating Systems
  - Windows Vista was the first
- Rogue router advertisements
  - Badly configured or malicious
- Tunnels turned on (by default, by bad config.)
- IPv6 and tunnels can bypass firewalls
  - Must filter IPv6 traffic and tunnels

IPv6 deployment risks

- The attacker community can make good use of IPv6
  - They are IPv6 experts
  - E.g. for tunneling leaked info out from compromised systems
- Vulnerabilities present in IPv6, including day zero issues inherent in any new or revised system
  - 224 CVE entries with keyword “IPv6” since 2002
  - 29 in 2015
- Complexity added by dual IPv4/IPv6 operations
- Immaturity of IPv6 security products and processes
- Lack of vendor support.

NAT and IPv6

- NAT has been essential to preserve the IPv4 address space
- Many concerns about lack of NAT in IPv6
- IPv4 address/port translation is not the main protection of the end systems
- It is the stateful firewall that protects!

Network scanning

- **IPv6 Security Myth #4 – IPv6 Networks are Too Big to Scan (Internet Society)**
- **Myth: IPv6 networks are too big to scan**
  Reality: Many addressing techniques reduce the search space
- Scanning an IPv4 /24 subnet (256 addresses) is trivial
- An IPv6 /64 subnet has $1.8 * 10^{19}$ addresses
- BUT - SLAAC, DHCPv6 and manual configuration all tend to introduce order into the sparse address space
- For LANs, can use one compromised host to scan via use of Neighbor Discovery

Some IPv6 protocol attacks

Extension Header vulnerabilities

- Routing Header Type 0
  - Source Routing
- Lots of security issues with RH0
  - Destination address in packet is replaced at every Layer 3 hop
  - Difficult for firewalls to determine the actual destination and compare with policy
  - Can be used for DoS traffic amplification
  - RH0 depracated (rfc5095)
- Fragmentation issues
  - Upper-layer info may be in second packet (and not inspected by firewall)
  - IPv6 standard defines every link to have MTU of at least 1280 bytes
    - Smaller fragments should be suspicious
- Hop-by-hop extension header also dangerous
- Solutions include
  - Filter on allowed and expected EH

Neighbor Discovery Protocol

- NDP authenticates neither the requestor or responder
  - Spoofing is possible
- SLAAC, NDP and DAD include protection mechanisms
  - Source address for RA and NS messages must be unspecified (::)
  - Hop limit must be 255 (the maximum)
  - RA and NA messages must be rejected if hop limit is not 255
  - This prevents a remote attacker sending forged RA or NA messages
    - scope is always local

Secure Neighbor Discovery

- Secure Neighbor Discovery (SEND) (rfc3971)
  - Uses Cryptographically Generated Addresses (rfc3972)
  - SEND has a pair of public/private keys per IPv6 node
  - ND is extended with more options
  - Interface identifier is crypto generated based on current IPv6 prefix/ public key
  - Signatures are generated and checked to authenticate nodes

Rogue RA

- No authentication mechanism built into SLAAC
- Malicious host can send rogue RA and pretend to be a router
  - Can capture or drop packets
- Badly configured systems too

Detecting rogue RA messages

- Use generic IDS with customised signatures
  - RA whose source MAC or IP is not in a configured list
    - Lots of manual configuration!
- Use tool NDPMon
  - And check against XML config file
  - also monitor all NS and NA
  - To check when NA contradicts a previous one
- Intelligent switches – known RA source
- Cisco RA Guard
- Rafixd (and ramond)
  - Detect all rogue RA messages and immediately transmit another forged RA with lifetime 0 seconds (to clear the rogue info on all nodes)

DAD

- Duplicate Address Detection
  - Host checks whether its address is already in use
  - Sends NS asking for resolution of its own address
  - An attacker can launch a DoS attack by pretending to own all IPv6 addresses on the LAN

ICMPv6

- Internet Control Message Protocol (rfc4443)
- An important component of IPv6
- Redefines ICMPv4 with additions and changes
  - Ping, destination unreachable, neighbor discovery, path MTU discovery
  - Error messages (message number 1 to 127)
  - Informational messages (128 to 255)
- Essential to establish strict ICMP filtering policies
  - Define ICMPv6 messages that can/cannot pass between the site and the internet
    - E.g. PMTU and ND
- Rfc4890 “Recommendation for Filtering ICMPv6 Messages in Firewalls”
  - Each site needs to consider carefully!

Issues for Sites

NIST 800-119 quote

- *The deployment of IPv6 reinforces the basic security lessons learned with IPv4. These security practices include defense in depth, diversity, patching, configuration management, access control, and system and network administrator best practices. Good security practices remain unchanged with the deployment of IPv6. Good security practices will reduce exposure and recovery time in case of a security event.*

Critical Security Controls for Effective Cyber Defense

http://www.sans.org/critical-security-controls/ (© SANS, CC-BY-ND)

Top 20 Critical Security Controls (Version 5)

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises

ISSeG: Top 12 Recommendations

EU FP6 Project – partners: CERN, FZK (now KIT), STFC

(Integrated Site Security for Grids)

http://isseg-training.web.cern.ch/ISSeG-training/Recommendations/Top-Recommendations.htm

R0 : Perform a site security risk assessment

R1 : Create and review your information security policy

R8 : Encourage information security awareness, education and training

R14 : Separate your development, test, and operational facilities

R16 : Install and regularly update malicious code detection and repair software for example anti-virus

R18 : Establish backup and restore policies and procedures

R23 : Enable audit logging of user activities, exceptions and security events

R26 : Restrict and control the allocation of privileges

R28 : Enforce good practices in the selection and use of passwords

R29 : Ensure that unattended equipment is appropriately protected

R36 : Establish a CSIRT and incident response procedures

R39 : Protect your confidential and sensitive data

IPv6 issues for security/network teams

- Control IPv6 if not using it
- Use Dual-stack and avoid use of tunnels wherever possible
- Drop packets containing RH Type 0 and unknown option headers
- Deny packets that do not follow rules for extension headers
- Filter IPv6 packets that enter and leave your network
- Restrict who can send messages to multicast group addresses
- Create an Address management plan
- Create a Security Policy for IPv6 (same as IPv4)
- Block unnecessary ICMPv6
- Protect against LAN RA, ND and DHCP attacks
  - Use SEND and authenticated DHCPv6
  - NDPMON and RAFIXD on critical segments
- Check/modify all security monitoring, logging and parsing tools

Issues for Sys Admins

IPv6 issues for sys admins

- Follow best practice security guidance
  - System hardening as in IPv4, see for example
  - https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf
  - Specific advice on IPv6 hardening, see for example
  - https://www.ernw.de/download/ERNW_Guide_to_Securely_Configure_Linux_Servers_For_IPv6_v1_0.pdf
- Check for processes listening on open ports
  - # netstat, lsof
- Review neighbour cache for unauthorised systems
  - # ip -6 neigh show
- Check for undesired tunnel interfaces
  - # ip -6 tunnel show, # route –A inet6

Sys admins (2)

- Ensure not unintentionally forwarding IPv6 packets
  - /proc/sys/net/ipv6/conf/*/forwarding files
  - Or net.ipv6.conf.*.forwarding sysctl
- Use OS embedded IPv6 capable stateful firewall
  - filter based on EH and ICMPv6 message type
- ip6tables
- IPv6 aware intrusion detection
  - E.g. Snort, Suricata, Bro
  - *https://www.sans.org/reading-room/whitepapers/detection/ipv6-open-source-ids-35957*
- Use IPsec between critical servers to secure communications

More Information?

More information

- Many IETF RFC documents on IPv6
- *IPv6 Security – Protection measures for the next Internet Protocol*, Scott Hogg and Eric Vyncke, Cisco Press (2009)
- NIST *Guidelines for the Security Deployment of IPv6* (NIST SP800-119)
  http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf
- Internet Society – top 10 IPv6 security myths
  https://www.internetsociety.org/deploy360/blog/tag/ipv6-security-myths/

Summary and Outlook

- In many ways IPv6 security is similar to IPv4
  - But with new twists and new vulnerabilities
- It has taken ~ 30 years to learn how to cope with IPv4 security
- There will be lots of fun ahead with IPv6
- Enjoy the next 20-30 years!

HEPiX

Questions?