CSCS
Centro Svizzero di Calcolo Scientifico
Swiss National Supercomputing Centre

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

IPv6 at CSCS

Swiss IPv6 Council, Lugano, November 29th, 2012

Chris Gamboni, CSCS

Email: cgamboni@cscs.ch

CSCS
Centro Svizzero di Calcolo Scientifico
Swiss National Supercomputing Centre

IPv6 status at CSCS

- Spring 2011: Initial IPv6 network support
- Spring 2011: IPv6 enabled on some test networks
- Spring 2011: Initial IPv6 deploy on DMZ
- *6 June 2011: IPv6 World Day*
- Autumn 2011: Set up new Firewall with IPv6 support
- Winter 2011: IPv6 on DMZ, with www.cscs.ch and dns
- Spring 2012: IPv6 enabled on Office and Guest networks
- *First half of 2012 : CSCS relocation from Manno to Lugano*
- *6 June 2012: IPv6 Launch Day*
- Autumn 2012: IPv6 enabled on frontend nodes
- Autumn 2012: First HPC cluster with IPv6 connectivity

IPv6 addresses

- 2001:620:808::/48 is the official IPv6 subnet assigned to CSCS
  - Our network may be splitted into 65536 networks (/64)
  - A plan is needed: for example we can split our subnet in 16 x /52 subnets
    - 2001:620:808:0000::/52 = Offices
    - 2001:620:808:1000::/52 = Guests
    - 2001:620:808:2000::/52 = Lab
    - 2001:620:808:3000::/52 = DataCenter
    - 2001:620:808:4000::/52 = Networking equipment
    - ...
    - 2001:620:808:f000::/52 = DMZ
  - In this case each /52 subnet has up to 4096 networks (/64)

IPv6 configuration at CSCS

- Dual Stack approach
- Static addressing for networking equipment and servers
- Dynamic addressing for PC and guest networks
  - Auto configuration with SLAAC
    - But we still rely on DHCPv4 to distribute DNS
  - Tests ongoing for:
    - Distributing DNS via RA (RDNSS, RFC6106)
    - DHCPv6

IPv6 deployment

- Configure the network part and FW/ACLs
  - Test
- Configure IPv6 on the systems
  - Test
  - At this point the system uses IPv6 and IPv4 for outgoing connections
- Publish the AAAA resource record into the DNS with short TTL
  - If test is succesful: set normal TTL for the RR AAAA
  - Now the system is fully IPv6 enabled

IPv6 SLAAC

- SLAAC Stateless auto configuration:
  - Privacy concerns:
    - use DHCPv6 or Privacy Extension
  - How do you track users ?
- Monitoring tools have to be installed
- Example:
  - arpwatch doesn't work for IPv6

IPv6 lessons learned

- Some network devices send out RA even if they shouldn't
  - Impact: machines get IPv6 global address
    - Disable SLAAC autoconfiguration on all the servers
- Rogue RA:
  - Impact: default gateway changed! No IPv6 connectivity anymore..
    - Filter RA messages at the network level
- IPv6 ACL: be careful not to filter NS/ND messages
  - Impact: you may break IPv6 connectivity
    - On IPv6 ARP is replaced by ICMPv6 NS and ICMPv6 ND messages
- Firewall IPv6 limitations (CLI config needed, WebGUI not ready)
- Services not listening on IPv6. Remember to configure ssh, httpd, etc to listen also on IPv6

IPv6 problems at CSCS

- User tracking for auto configured networks
- Reverse dns for auto configured networks
  - IPAM ? DHCPv6 ?
- Firewall support not yet complete
  - Next release ?
- Network devices support not complete
  - Next release ?
- OS support not yet complete (dhcpv6 support, RDNSS, etc.)
- Not enough experience on IPv6
- Applications support for IPv6
- IPv6 on non IPv6 enabled networks (6to4, teredo, tunnels,etc.)

CSCS next steps

- Consolidate Data Center IPv6 deployment
- Gain experience
- Solve problems !

IPv6 tools

- ping6
- traceroute6
- IPv6 Monitoring tools:
  - NDPmon
  - Ipv6mon
  - addrwatch
  - ramond
- IPv6 Security tools:
  - THC-IPv6 The Hacker Choice Attack Toolkit
  - Nmap (v 5)

Conclusion

- CSCS has already enabled IPv6
  - Gaining experience on IPv6 deployment
  - Problems on IPv6 have a low impact (now)
- DataCenter is ready to support IPv6
  - New system with dual stack IPv4/IPv6, where possible.
  - Some existing systems will get IPv6.
- Still waiting for some features on network device
- Still waiting for more support from OS vendor