

IPv6 – An update from the European Commission

Stockholm, 20 October 2008

*Detlef Eckert
European Commission
Directorate General Information Society and Media*

Why an EU initiative?

Background

- IPv4 address problem
- Basically two options:
 - Continue IPv4, manage scarcity
 - And introduce IPv6 only when IPv4 becomes truly unsustainable or we may have found something else
 - Introduce IPv6 proactively
- There are arguments in favour and against for both options
- ICANN and RIRs have stressed the need to adopt IPv6 as a matter of urgency
- European Commission shares this view and adopted Action Plan in May 2008

Why an EU initiative?

Approach

- Adoption of IPv6 still very low
- Adoption is a largely decentralised and global market process ...
- ... in which the public sector and public policy play a role
- Incentives for individual actors to adopt IPv6 depend on the adoption of others (collective action problem)
- In such a situation public policy can make a difference

What are we proposing?

Action Plan Overview

- Strategic objective: **EU should have made a significant step by 2010**
- Stimulation of IPv6 reachable content, services, and business applications
- Timely preparation of the introduction of IPv6
- Public sector procurement
- Monitoring security and privacy implications

IPv6 security considerations

(1 / 2)

- The larger address space makes IPv6 less vulnerable to random port scanning, this also helps to protect against many self-propagating worms
 - Provided network is not badly designed as alternative methods to find hosts will be used
 - Security by obscurity
- IPv6 security issues are partly different from those on IPv4 networks
 - Less experience, less well understood
 - Example: Neighbour discovery and stateless autoconfiguration (spoofing attacks)
 - Secure ND , 802.1x authentication
 - Issue of privacy addresses

IPv6 security considerations

(2 / 2)

- Security products such as FW, IDS, etc are still lagging full support of IPv6
- Protocol weaknesses exposed
 - Example: Type 0 Routing Header vulnerabilities (In 2007 analysed by Philippe Biondi and Arnaud Ebalard from EADS)
- Although you may not have IPv6 deployed, existing IPv6 traffic could affect your network through tunneling
 - Vista by default IPv6
 - Islands of IPv6, attackers can use hosts to route traffic through sub networks without compromising routers and FW

The Opportunity

- IPv6 offers you as many addresses as you need, this is the key to a flexible security architecture
 - Many network interfaces per device
- IPsec in IPv6 connects end points (not only border routers)
 - Creation of trust domains whereby hosts can be part of multiple of such domains
 - Host security required (managed clients)
 - NAT not needed (security by obscurity)
 - Granular security or more complexity?
- Positive user experience and agile business
 - Seamless remote access
 - Offer partners and customers access to resources on your network

Current EU activities

- Current priority: Discussion with Member States
 - Council on 27 November 2008
- Launching a study to measure deployment
- Two recent FP7 projects:
 - <http://www.6deploy.org/>
 - <http://www.efipsans.org/>
- Various outreach activities
- International Co-operation