

Segurança de Redes e Serviços:

IPv4-IPv6. Uma perspectiva Europeia



AFCEA Portugal

Associação para as Comunicações, Electrónica,
Informações e Sistemas de Informação para Profissionais

Manuel Pedrosa de Barros
Direcção de Segurança nas Comunicações

ENISA REPORTS

- Resilience Features of IPV6, DNSSEC and MPLS - Resilience of Communication Networks – January 2009
- Stock Taking Report on the Technologies Enhancing Resilience of Public Communication Networks in the EU Member States – May 2009
- Secure Routing: State-of-the-art Deployment and Impact on Network Resilience – July 2010
- Inter X: Resilience of the Internet Interconnection Ecosystem – April 2011

- Address space
 - From 32 to 128 bits
 - elimination of NAT
- Mandatory support for IPsec
- Supported IPsec Extension Headers in IPv6

IPv6 provides a wealth of benefits:

- Vast address space
- More efficient routing
- Quality of service
- Improved security

What is important to understand though, is that when it comes to resilience and security, there is no silver bullet.

IPv6 does help in certain security issues, but is not and thus it should not be considered as an all-inclusive security solution.

*Companies and organizations should **train** their network administrators on the specifics of IPv6 and create an **IPv6 task force** so that the transition from IPv4 to IPv6 (including the intermediate stages) to be as secure and painless as possible.*

General observations of applied network resilience have been encountered during the survey process:

- **Missing experience** from commercial operation on the features and applications of IPv6 improving network resilience;
- **Absence of operational best practices and recommendations** in the area of applied network resilience in particular for IPv6 to facilitate secure communication and connectivity;
- **Lack of management and coordination between stakeholders**, missing information security policies, guidelines and management principles.

Deployment:

- no plans 18%; planned 55%; deployed 27%
- 82% have already deployed or do have plans to deploy IPv6

Key drivers for IPv6 deployment:

- Increasing demand on IP address space - 40%
- Customer demand for IPv6 – 20%
- Improvement on network resilience – 20%
- Introduction of technical innovations – 20%
- IPv6 deployment today is mainly driven by increasing demand on IP address space

Deployment options:

- Dual stack routers/links
- Tunneling IPv6 over IPv4/MPLS

Key Performance Indicators:

- No real improvement in terms of network resilience is expected
- KPIs for resilience in IPv6 networks were not considered so far due to the lack of operational experience
- KPIs for resilience in IPv6 networks are not measured because there was no such focus during the planning and deployment process

Customer Reaction

- Number of customers asking for IPv6 services is estimated below 40%
- There is no real customer feedback, neither positive nor negative, concerning improved resilience of their network using IPv6
- IPv6 introduction lacks customer demand

Challenges

- Management of the security in an environment where end-to-end connectivity has to be restored
- Lack of experience running IPv6 networks

Conclusions

- IPv6 deployment is on track with EU initiatives on IPv6
- Ipv6 deployment is mainly driven by the increasing demand on IP address space
- Network resilience is not the business driver for the introduction of IPv6
- No improvement of resilience has been observed after introducing IPv6
- No KPIs have been defined
- The introduction and deployment of IPv6 lacks of experience best practice
- Customer demand for IPv6 is at a low level

Recommendations to ENISA:

- Ensure that service providers, network operators and IT managers are made aware of the resilience features of IPv6;
- Ensure existence of a sufficient pool of IPv6 trained people;
- Encourage proper exploitation of European expertise on IPv6 resilience features, in particular best practice and operational excellence on network resilience.

Potential routing security challenges, tomorrow, and potential responses

- The imminent event of IPv4 depletion and consequently the update of IPv6 are expected to incite an increased number of security incidents.
- For IPv6, we note that there is less operational experience in the sector and therefore more configuration errors are expected, at least for a transitional period. In addition, an increase in multi-homing setups requires more skilled resources.

The Wider Issues

The Internet culture rejection of regulation even though there are some obvious market failures for which regulation might perhaps be desirable, such as:

- Levels of preparation for IPv6 and the transition to IPv6.

General Themes or Points

Network Layer

IPv6 and future shock

“Mixed IPv4/IPv6 operations might also generate quite some chaos in the coming years.”

"IPv6 is a new network protocol which will require new training, experience, and implementations. During the transition, new vulnerabilities could be introduced, and IPv4 security devices and software may be of limited use. As network operators have done when introducing anything new into networks, operators will have to work with and test IPv6 implementations in order to ensure security."

FIM

Segurança de Redes e Serviços:

IPv4-IPv6. Uma perspectiva Europeia



AFCEA Portugal

Associação para as Comunicações, Electrónica,
Informações e Sistemas de Informação para Profissionais

Manuel Pedrosa de Barros
Direcção de Segurança nas Comunicações