teratel

telecomm consulting

www.teratel.ch

Stock taking interviews on Network Resilience

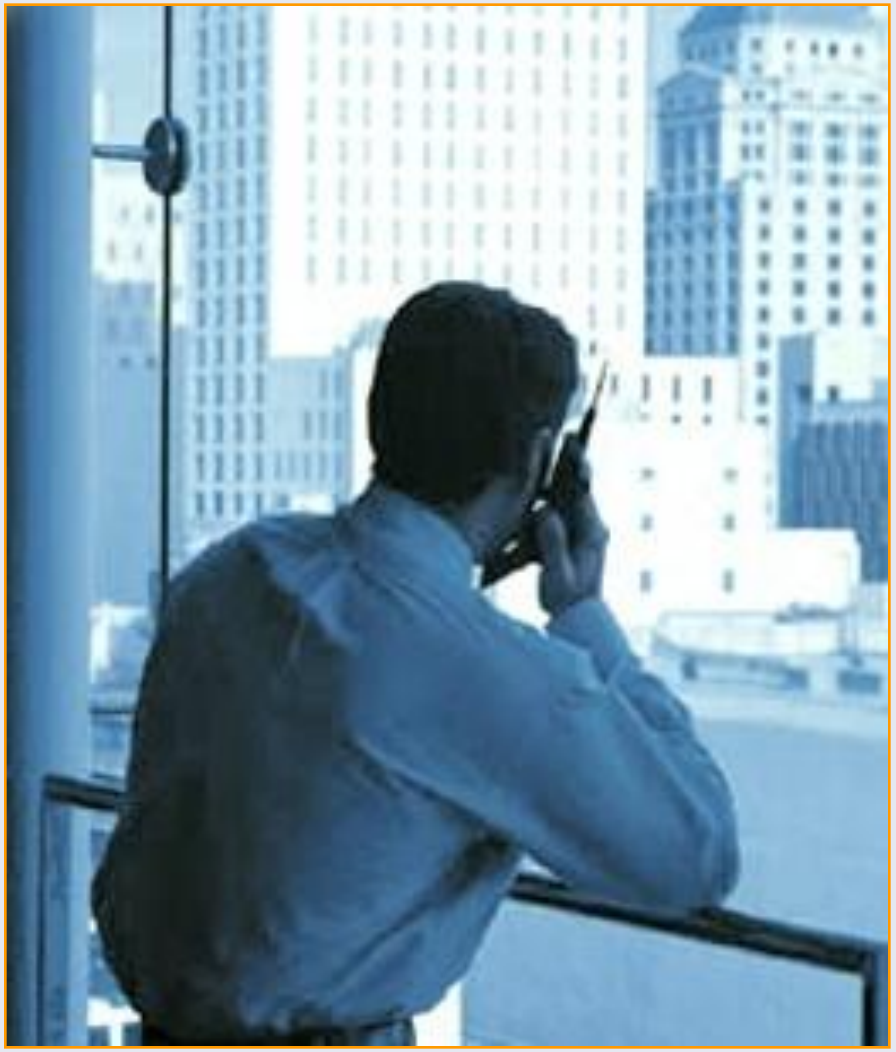
- Preliminary Results -

Content:

Technology Issues

(IPv6, MPLS, DNSsec)

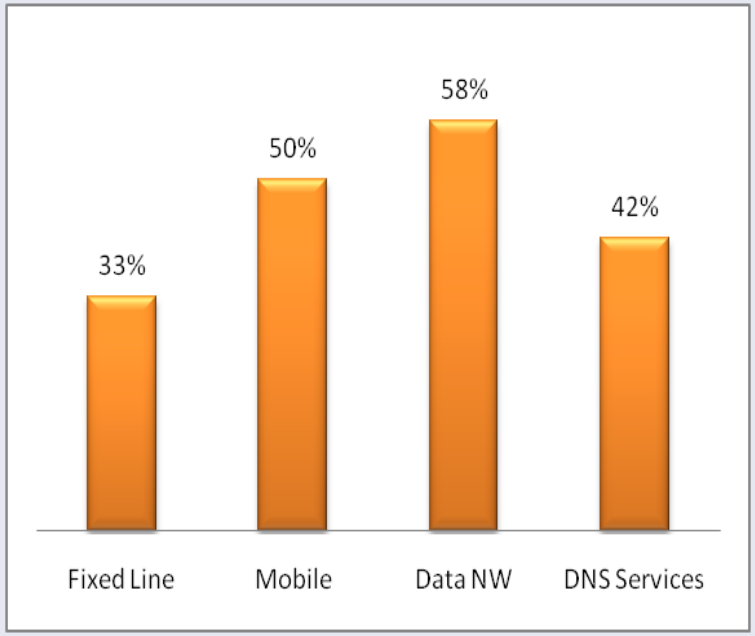
Recommandations



Goals

- **To identify industrial maturity of the impact on network resilience, in particular with respect to the three technologies**
  - IPv6
  - MPLS
  - DNSSEC
- **To identify the need and status of regulatory and policy framework**
  - Regulatory need and framework
  - Policy issues and reqirements
- **To identify and recommend further actions for ENISA and mainstreams in terms of resilience**

Interviewee Profile



- **Fixed Line Provider**

  OTE, PT, Telenor, FT-Orange, (Telefonica, DT, Swisscom)

- **Mobile Operator**
  - Vodafone, Wind, Elisa, OTE, FT, Telenor

- **Data Network Provider**
  - Forthnet, Janet, Telenor, OTE, FT, PT, NFSi, (BT, DT)

- **DNS Service Provider**
  - NetNod, Dot.SE, NFSi, OTE, PT

Questionnaire Overview

The questionnaire focus on the technologies

IPv6, MPLS, DNSSEC

and aimed on receiving feedback and information on

- **Status, plans and maturity of commercial introduction / deployment**
- **Key business driver for introduction / deployment**
- **Impact on network resilience and corresponding KPI's**
- **Usage and commercial utilization**
- **Customer reaction and feedback on experienced resilience**

Technology impact on Network Resilience

Coverd Topics:

IPv6
MPLS
DNSsec

- MPLS is commercially available and deployed technology – identified features contribute essentially to network resilience
- Introduction of IPv6 is mainly driven by upcoming demand on address space
- IPv6 does not really show direct improvement on network resilience compared to IPv4 including all deployed features
- DNSSEC is very diversified in deployment, experience and customer demand
- DNSSEC lacks of awareness, tools and common agreements across Europe

Regulatory Framework

Regulations & Policies

- **Almost all interviewee identified that**
  - Regulatory framework is sufficient enough
  - More or extended regulations are not needed
- **Almost all interviewee identified the existing regulatory framework works well in open market environment**
- **However, more than 60% of the interviewee identified the need for further action in terms of**
  - introduction of DNSSEC – e.g. Information Security Policies
  - Deployment of IPv6 – Recommendations & Best Practice

Topics on Recommendations for DNSSEC

- **DNSSEC needs coordination on European level in order to coordinate and guide introduction as well as deployment**

- **Main open issues are**
  - ***Information Security Policy*** on European level in order to define and guide cross country interaction and rules (- key management rules -)
  - ***Information Security Guidlines*** on Country Level
  - ***Recommendations*** on implementation & management issues

DNSsec can be successfully inroduced given the guidance and support of ENISA

Topics on Recommendations for IPv6

- **IPv6 is mainly driven by increasing demand on IP addresses**

- **Main Open Issues for interviewee:**
  - ***Recommandations*** - need of European Recommendations on deployment issues across Europe
  - ***Best Practice*** - guidlines on IPv6 implementaion and configuration (engineering experience)
  - ***Awareness*** – customer awareness and supported applications

IPv6 can be successfully supported given the guidance on best practice and awareness creation

Preliminary Summary Assessment

DNSSEC

- DNSsec is very well deployed and advanced in Scandinavia
- DNSec lacks of management tools, customer awareness and mainly coordination for introduction

IPv6

- IPv6 is mainly driven by demand on address space
- So far, no essential improved impact of IPv6 on network resilience experienced

MPLS

- MPLS is mature and well deployed as commercial technology
- MPLS features are well used to improve network resilience