Improving Resilience in Public eCommunication Networks

ENISA – European Network and Information Security Agency

NIS Summer School, Sep 2008

Disclaimer: "The views expressed in this presentation are those of the authors and do not necessarily represent the views of the Agency".

Resilience

The ability of a system to provide & maintain an **acceptable level of service** in face of faults ***(unintentional, intentional, or naturally caused)*** affecting normal operation.

Network resources resilience

- The main aim of resilience is for faults **to be invisible to users**.
- A resilient network must guarantee protection and / or restoration schemes.
- Real-Time Applications Demand that Resilient end-to-end Network Services Be Extended Consistently Across the Network.
- The classification of a networks resilience has to be given from the **availability and performance perspective.**

Definition of Availability

- Availability is the probability that an item will be able to perform its designed functions.
  - Stated performance level
  - Stated conditions
  - Stated environment

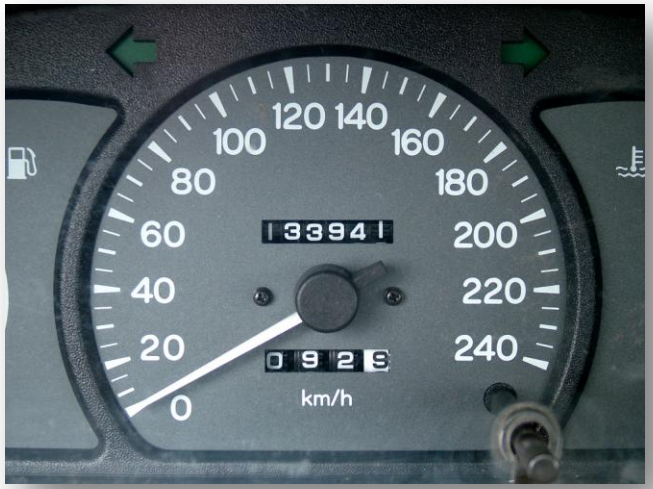
$$\text{Availability} = \frac{\text{Reliability}}{\text{Reliability} + \text{Recovery}}$$

Performance metrics

- Measure the performance of their networks at different levels.
  - per-port metrics
  - end-user metrics
- Performance metrics are as follows:
  - Connectivity
  - Delay (both round-trip and one-way)
  - Packet loss
  - Jitter or delay variation
  - Application response time
- Measurable SLA metrics

Key Performance Indicators

- Reflect the performance of network.
- Key Performance Indicators (KPIs) are:
  - Mapped directly from the Performance metrics.
  - Are a formula of several Performance metrics.



Quantification of Availability

Percent Availability	N-Nines	Downtime Time Minutes/Year
99%	2-Nines	5,000 Min/Yr
99.9%	3-Nines	500 Min/Yr
99.99%	4-Nines	50 Min/Yr
99.999%	5-Nines	5 Min/Yr
99.9999%	6-Nines	.5 Min/Yr

Risks to resilience

- Flash crowd events
- Cyber attacks
- Outages to other services affecting the network
- Natural disasters
- System/Logical failings

Risk Mitigation

- Network resilience is an issue of **risk management.**
- Mitigation of identified risks involves technical measures such as:
  - Resilient design;
  - Resilient transmission media;
  - Resilient equipment;

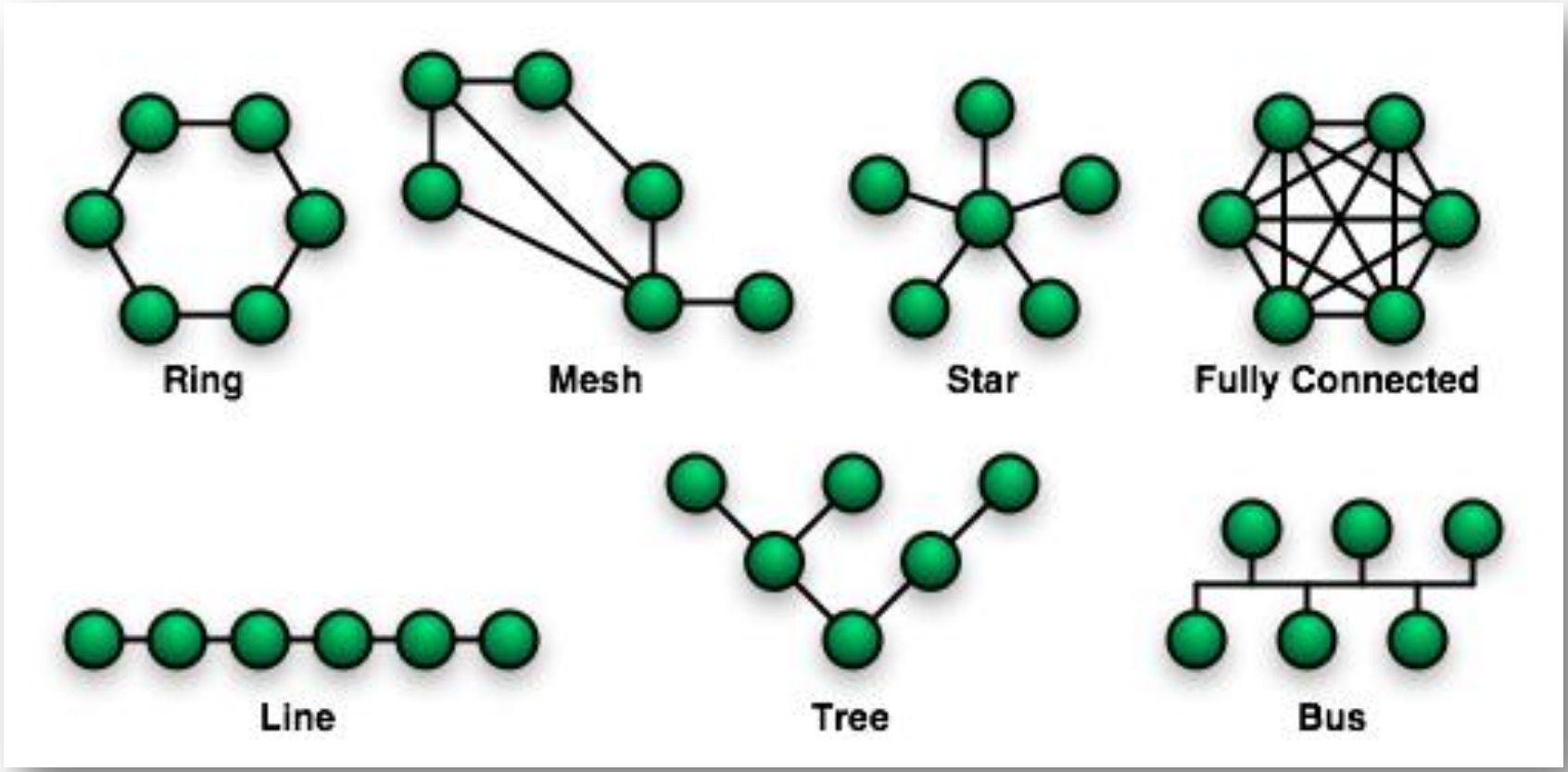
…and Technologies which might improve Resilience.

Resilient design

- A resilient network design aims to remove single points of failure in network equipment.
- Provide multiple paths through networks, while maintaining visibility and controllability to higher levels.

Resilient design

- A **resilient multilayer design** may include:
  - Topology / Mesh Networks
  - Path Protection
  - Dynamic Restoration
  - Scalable Routing Protocols
  - Redundant links
  - Load Balancing

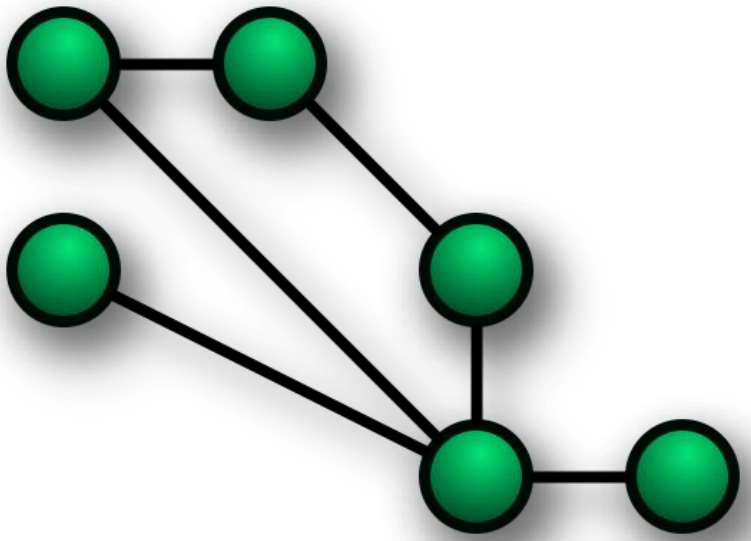


Network resources resilience

Resilient design

Topology - Mesh Networks

- Rerouting around broken or blocked paths.
- A partial mesh topology.
- Shortest path basis.

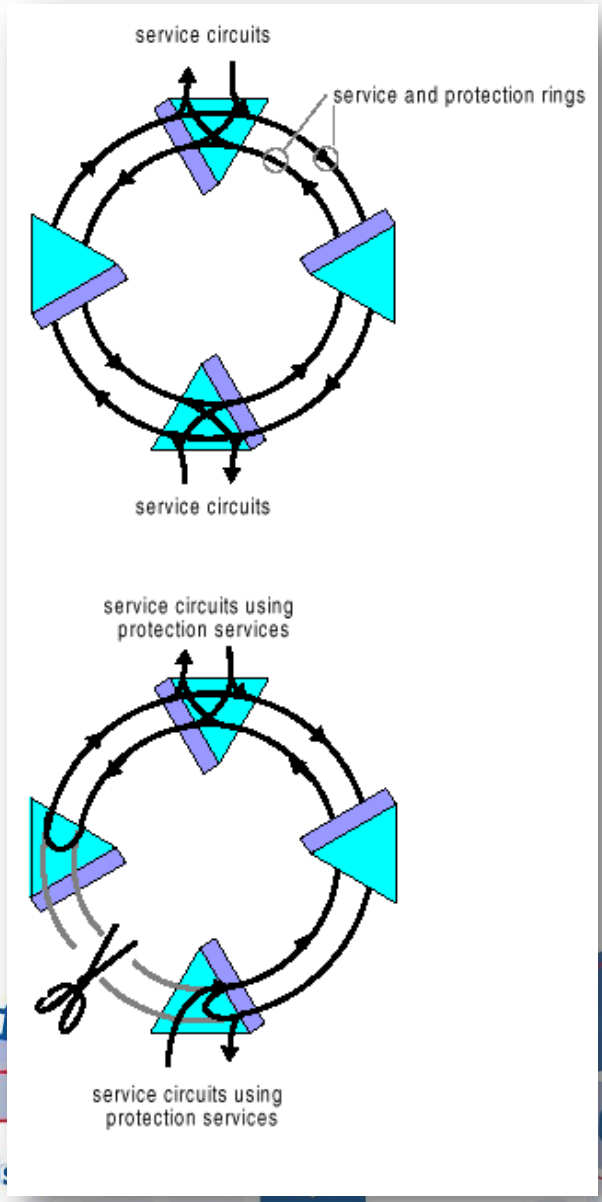


Dynamic Restoration

- Dynamic Restoration:
  - Searching for the shortest path between source and destination nodes, skipping the failed network element, link or node.
  - No prior knowledge on which route to choose.
- Scalable Routing Protocols:
  - Handle growing amounts of work in a graceful manner.
  - O(log N) rule.

Network resources resilience

- **Resilient design:**
  - Path Protection:
  - Unlike restoration, the protection mechanism assigns the means beforehand for recovering circuits when faced with failures.

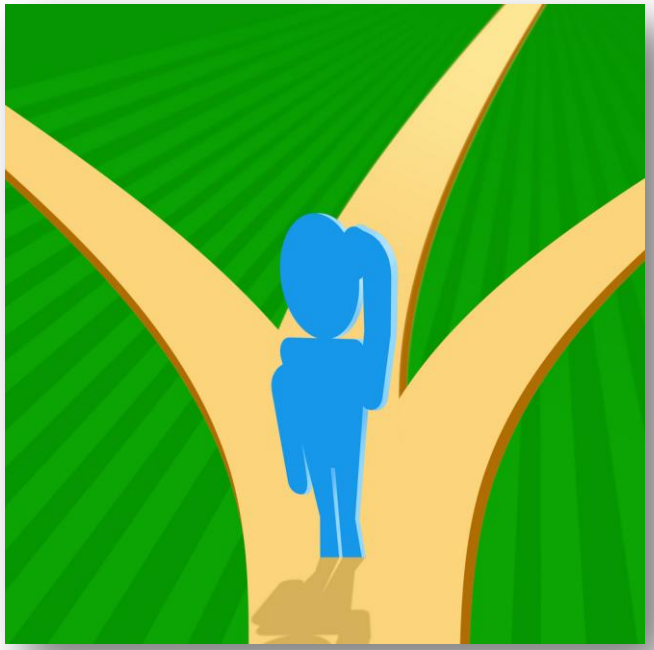


Redundant links

- Provide several paths to a given destination.
- Maximize network reliability and availability.
- Core links and mission-critical information exchanges.
- Load Balancing to optimize costs.
  - SLA ?

Resilient transmission media

- The cabling must follow standards.
  - TIA-942, builds on TIA-568 and TIA-569 and specifies a generic, permanent telecommunication cabling system.
- Use geographically separate paths for connections.
  - Information about physical routing of cables may be hard to obtain.
  - Cross-selling of fibre and ducts is common.

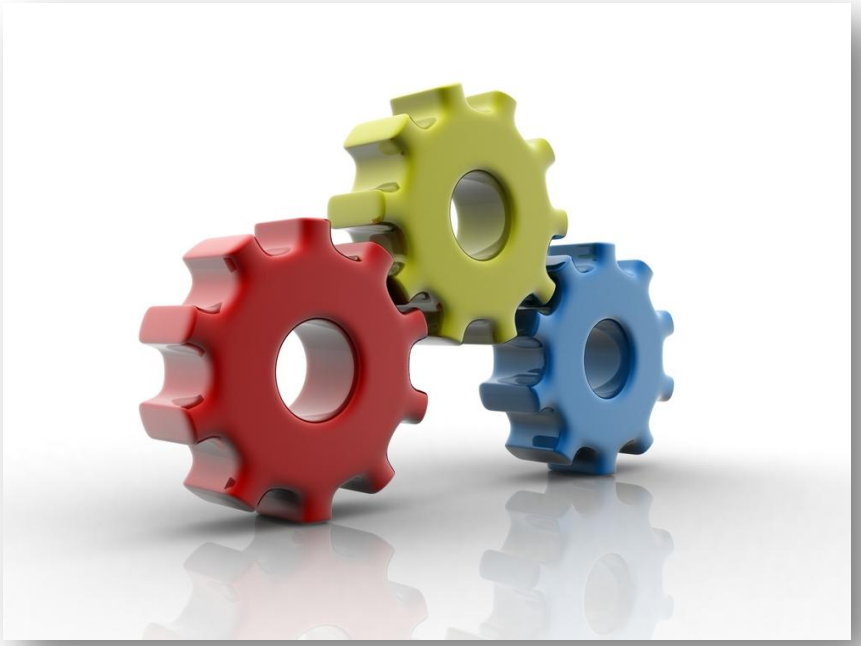


Resilient equipment

- **Power:**
  - May include two or more power feeds from the utility, UPS, multiple circuits to systems and equipment and on-site generators.
- **Cooling:**
  - Adequate cooling equipment, raised-floor system for more flexible cooling.
- **Hot Standby, Dual Components, etc…**
  - The hot spare is active and connected as part of a working system. When a key component fails, the hot spare is switched into operation.

Resilient equipment

- **Non Stopping Software**
  - Software should restart in case of hanging.
- **Equipment from diverse providers**
  - Avoid ‘systemic’ or ‘common-mode’ failure.



Resilient Technologies

- IP backbone technologies.
- Technologies which might improve Resilience:
  - MPLS
  - IPv6
  - DNSSEC
  - S-BGP
  - Other ?

Selected Technologies

- MPLS
  - OSI Layer 2.5 technology.
  - Used by operators in IP backbones, replacing Frame Relay and ATM.
- IPv6
  - OSI Layer 3 technology replacing IPv4.
  - Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe.
- DNSSEC
  - A technology improving the security of Domain Resolution Service.

MPLS - Multiprotocol Label Switching

- Features Overview
  - Provides a Layer 2 connection-oriented transport mode through a Layer 3.
  - Enables class of service (CoS) tagging and prioritization of network traffic.
- Drawbacks
  - Asymmetrical Data Plane
  - Slow reaction
- IP based resilience schemes include
  - IP dynamic routing.
  - MPLS protection switching.

MPLS - Multiprotocol Label Switching

- IP Based networks routing
  - Each node makes its own routing decision.
  - Use IP routing protocols to maintain consistent routing tables.
  - The per-hop nature of IP routing decisions provides resiliency.
- IP routing fundamental constraints
  - Traffic always uses the shortest path to the destination.
  - Critical links can get overloaded.
  - Convergence time is too long for Real Time Applications.

MPLS - Multiprotocol Label Switching

- The path of an MPLS Packet(LSP) can be
  - Explicitly configured hop by hop
  - Dynamically routed by CSPF
  - A loose route
- Traffic Engineering (TE)
  - The shortest path with available bandwidth will be chosen
- TE - Fast Reroute
  - About 50ms
- MPLS DiffServ - TE

IPv6

- More addresses available
- Simpler Header
- Site Multihoming
- IP Host Mobility
- IPsec
  - Authentication Header
  - Encapsulating Security Payload

IPv6

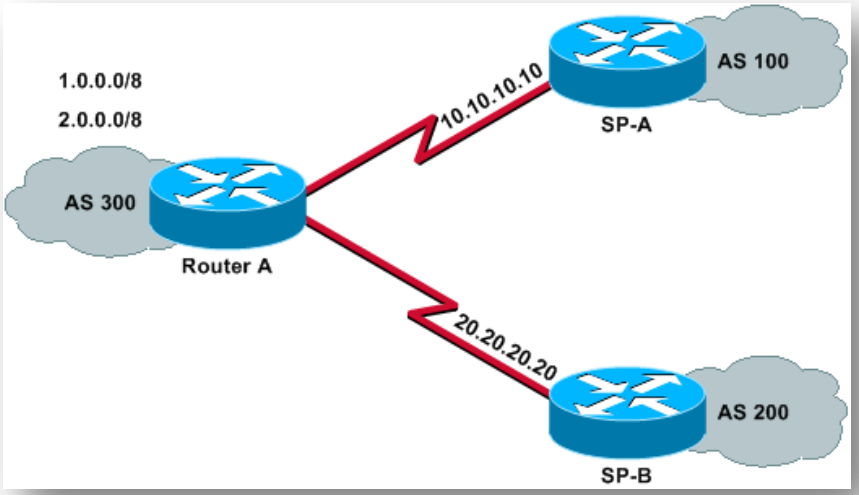
- More addresses available:
  - Improved global reachability and flexibility
- No need for Network Address Translation:
  - NAT was a short-term solutiol
- Addresses distribution allows prefix aggregation
  - Smaller Routing Table

IPv6

- **Simpler header**:
  - Provides better routing efficiency.
  - No broadcasts and thus no potential threat of broadcast storms.
  - No requirement for processing checksums.
  - Simpler and more efficient extension header mechanisms.
  - Flow labels for per-flow processing with no need to open the transport inner packet to identify the various traffic flows.
- All comes to simpler software / hardware for the routers.
  - Fewer Bugs

IPv6

- **Site Multihoming:**
  - Multihoming to several Internet service providers (ISPs).
  - No need for Autonomous Systems
    - Current status 267.688
    - 1994 were 20.000
  - Transport sessions survive “rehoming”



IPv6

- **IPv6 Mobility**
  - IPv4 mobility already used as extension of IP
  - IPv6 mobile is designed at the some time with IPv6.
  - IPv6 mobile tunnel is symmetrical.

- 3GPP2 and 4G telephony standards are considering the use of MIPv6

IPv6

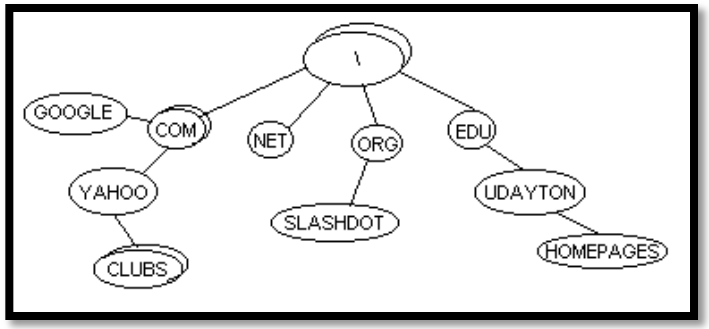
- **IP Security:**
  - IPsec is already an extension for IPv4
  - Authentication Header (AH)
    - source authentication, connectionless integrity, and protection against replay
  - Encapsulating Security Payload (ESP)
    - confidentiality, source authentication, connectionless integrity, and replay protection
- Securing the traffic between two hosts
  - Tunnel mode
  - Transport mode

DNSSEC

- DNS is a critical service for IP Based Networks
- Not designed to be secure
- With VOIP, CLI is also based on DNS

DNSSEC

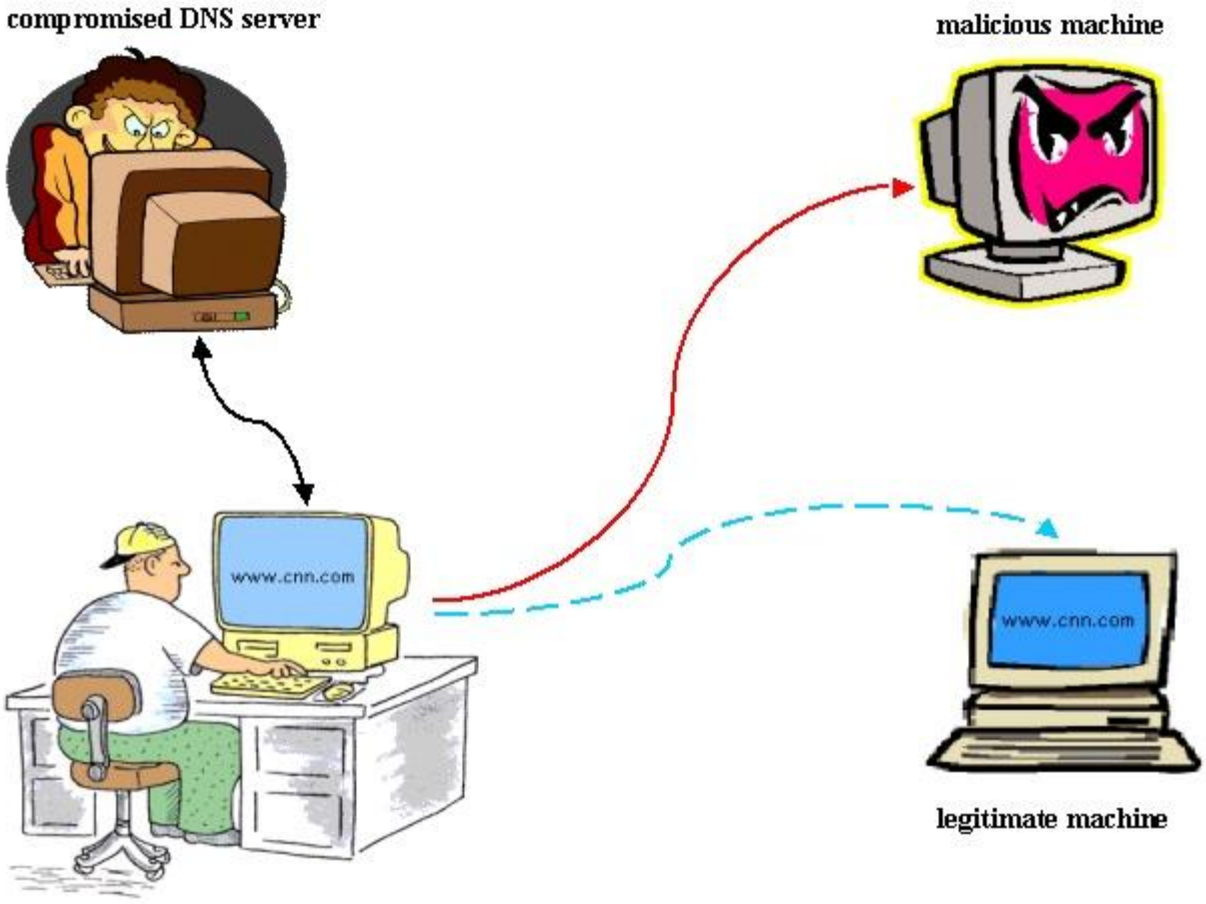
- DNS Operation
  - DNS is Hierarchical
  - Clients ask name 2 address translation to providers Recursive Servers
  - Recursive Servers traverse DNS hierarchy to find answer



DNSSEC

- DNS Known Threats (RFC 3833)
  - Packet Interception - monkey-in-the-middle attacks
  - ID Guessing and Query Prediction
  - Name Chaining - Cache Poisoning
  - Betrayal By Trusted Server
  - Denial of Service
  - Wildcards

The DNS Flaw that hit the Media



DNSSEC

- Domain Name System Security Extensions.
- DNSSEC features:
  - End-to-end data integrity check.
  - DNS data origin authentication.
  - Data integrity.
  - Authenticated denial of existence.
- Does not protect Client to Resolver Communication
  - Use TSIG to ensure the integrity with a recursive name server.

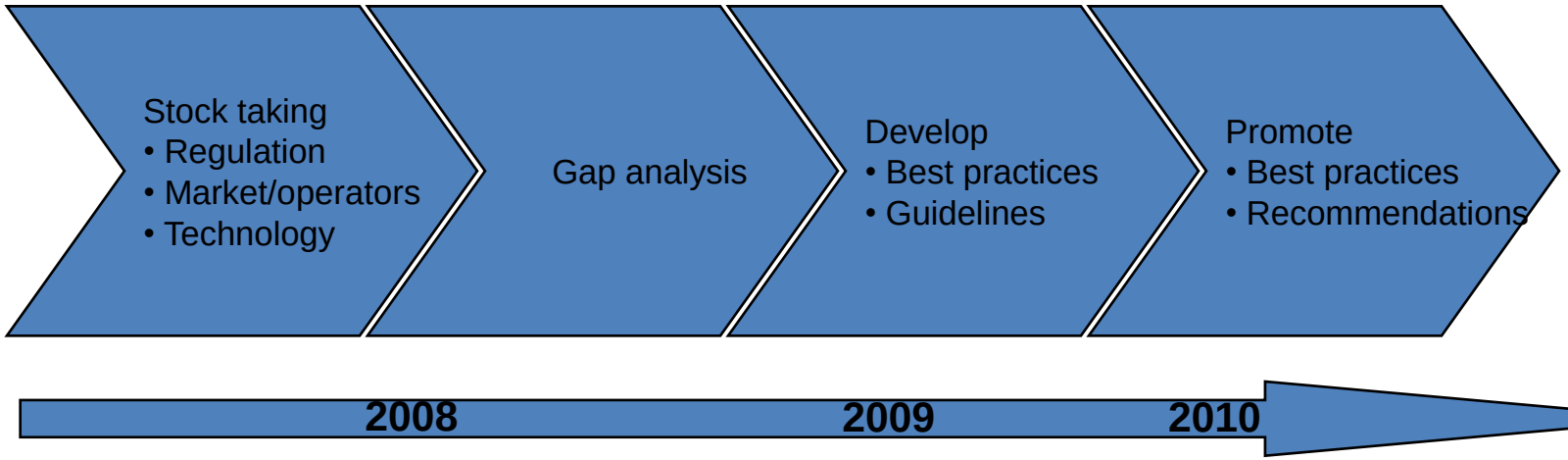
DNSSEC

- Weaknesses
  - Answer validation increases the resolver's work load.
  - Denial of Service.
  - Trust model is almost totally hierarchical.
  - Key rollover at the root is really hard.
  - Betrayal By Trusted Server still exists as threat.
  - Zone Walking

Back to ENISA….

MTP1 - Improving Resilience in European e-Communication networks

Collectively evaluate and improve resilience in European e-Communication networks



By 2010, the Commission and at least 50% of the Member States have made use of ENISA recommendations in their policy making process

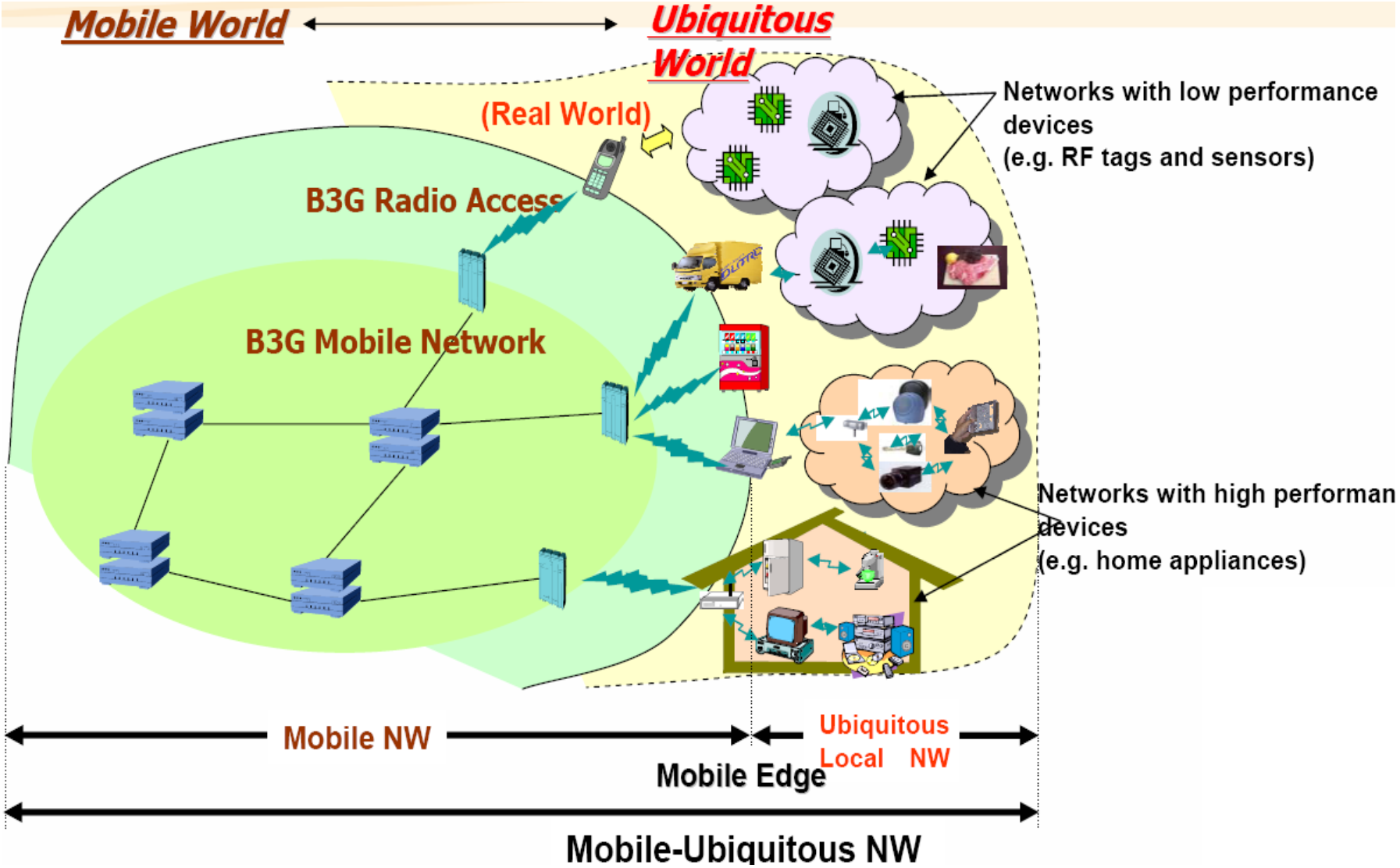
WPK 1.3 – Background Info

- Objectives
  - Analyze current and emerging technologies used by network and service providers to enhance the resilience of their operations
- Scope
  - IP backbone technologies
- Stakeholders
  - Equipment vendors, network operators, services providers
  - Research institutes and standardization bodies
  - Policy makers
- Target Group
  - Regulators and Policy Makers
  - Operators
  - Vendors

Approach - Status

- Selection of topics & stakeholders.
  - Consultation workshop, Q1 08, Brussels
- Consultation with stakeholders.
  - Interviews, Expert groups (Q3 & Q4 08)
- Analysis of resilience enhancement of existing and emerging technologies.
  - (Q4 08)
- Validation of findings with experts and stakeholders.
  - Consultation workshop 12th and 13th of November

Future Networking Trends



Summarizing

- Importance of the Resilience of public eCommunication networks;
- Technologies benefits are well recognized however the economical / political incentives have to be made;
- References
  - http://www.enisa.europa.eu
  - http://www.enisa.europa.eu/sta/

Demosthenes Ikonomou
Panagiotis Saragiotis

sta@enisa.europa.eu

European Network and Information Security Agency (ENISA), Security Tools and Architectures