Transport for Carrier Grade Internet

1st IEEE Below IP Networking Workshop at Globecom 2009

Hawaii, Honolulu, 30.11.2009

Raimo.Kantola@tkk.fi
Dept of Communications and Networking –
Helsinki University of Technology
(to become Aalto University School of Science and Technology)

Erosion of IP Principles

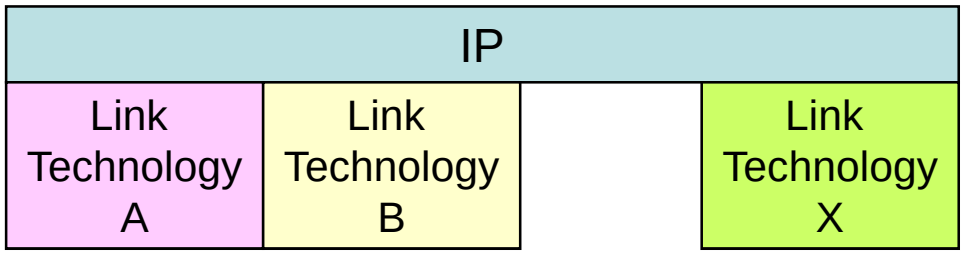
- Dave Clark, 1984: End to End Principle:

The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)
We call this line of reasoning against low-level function implementation the "end-to-end argument."

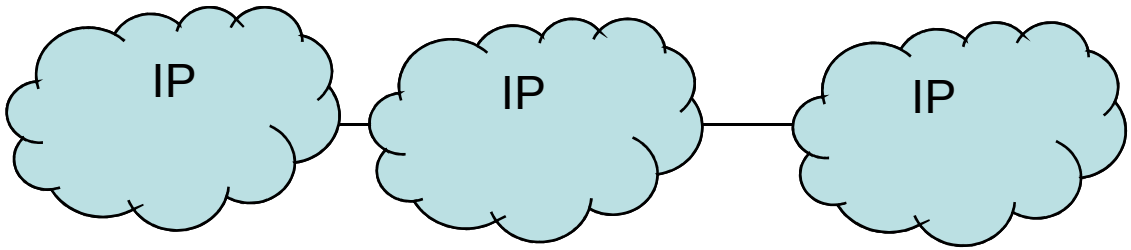
- Dave Clark, 2007: Trust-to-trust:

“The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at points where it can be trusted to perform its job properly.”
— David Clark, MIT Communications Futures Program, Bi-annual meeting, May 30-31, 2007, Philadelphia, PA.

IP over everything



Original idea



Reality today

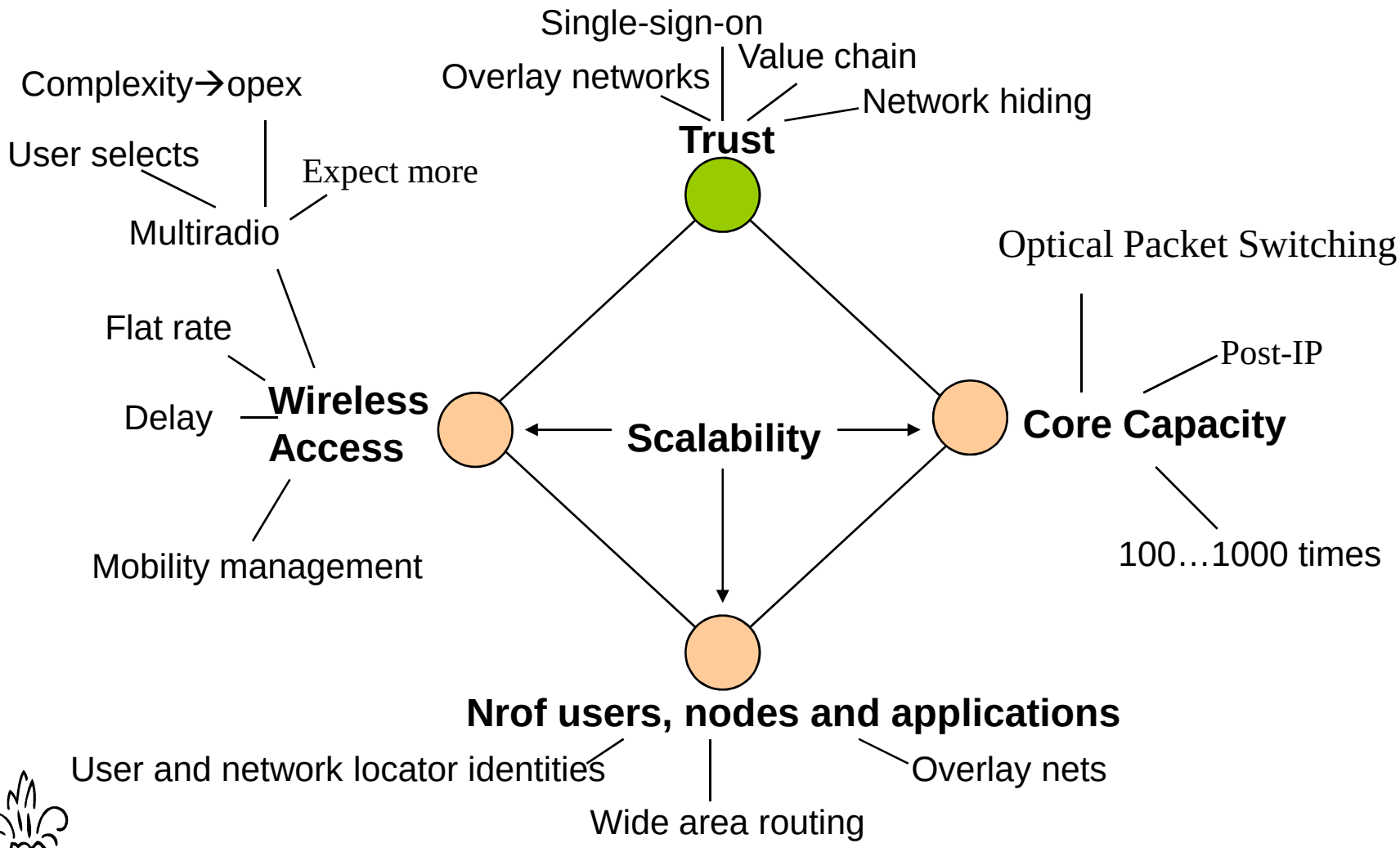
- A lot of users have private addresses
- Users behind Firewalls
- Application Gateways between networks

- ”An IP connection” is made of legs belonging to networks that are hidden from each other.

Internet Economics

- Flat rate service – economically efficient prices
  - Fast growth → forced investment
- ISP margins from residential Internet services are low or non-existent
  - ISPs make their margin on Corporate connectivity services: VPNs etc. – IP itself does not support virtualization
- Cost of communication is born by the receiver because sending is so cheap.
  - The original IP network assumption that receiver wants to receive what sender sends is false → spam, malware.
  - This is an economic problem but the architecture of Future Internet should provide legitimate technical and economic solutions to tackle the problem

Grand Challenges in Networking



Transmission vs packet transport

- Continuous bit streams on constant speed
- Transmission frame does not have an address
- State must be managed by an MS

- Transmission is chopped into packets
- Each packet has 2 addresses
- Network state can be managed by
  - MS
  - signaling
  - routing etc protocols

Carrier Grade applied to Internet

- Manageability
  - service is controlled and monitored througout its lifetime
- Predictability
  - service level is known from setup till teardown
- Resiliency
  - service is restored in a minimal time after failures

- Trustworthyness and isolation
  - User or her administrator can control and monitor who can send packets to the user for which services
  - Operator is protected from events in user networks
- Predictability and resiliency are properties of the transport system
  - carrier grade transport is a prerequisite to predictability and resiliency on the service level

Addressing – theory and reality

- IP over everything = every host and server, every gadget has an address and therefore can be reached by anyone.
- This principle is contrary to reasonable real requirements: we want to control who can send packets to whom
  - DDOS protection of mobiles
  - our own home gadgets, control devices
  - corporate networks protected by NATs and Firewalls
  - hosts protected by Firewalls
- A huge addressing space (IPv6) is not a blessing – it is a problem.

What else is wrong with IP?

- IP itself does not support mobility
- Users need private addresses and NATs, current NAT traversal solution: **UNSAF does not scale to mobile use**.
- Middleboxes break many protocols → IETF spends a lot of effort in fixing the problems that emerge (NAT traversal etc…)
- Multihoming leads to fast routing table growth
- Visibility of networks to each other leads to configuration errors, long convergence or even instability of the routing system
- ISPs have only few and obscure tools to map traffic onto their networks (MPLS, BGP).

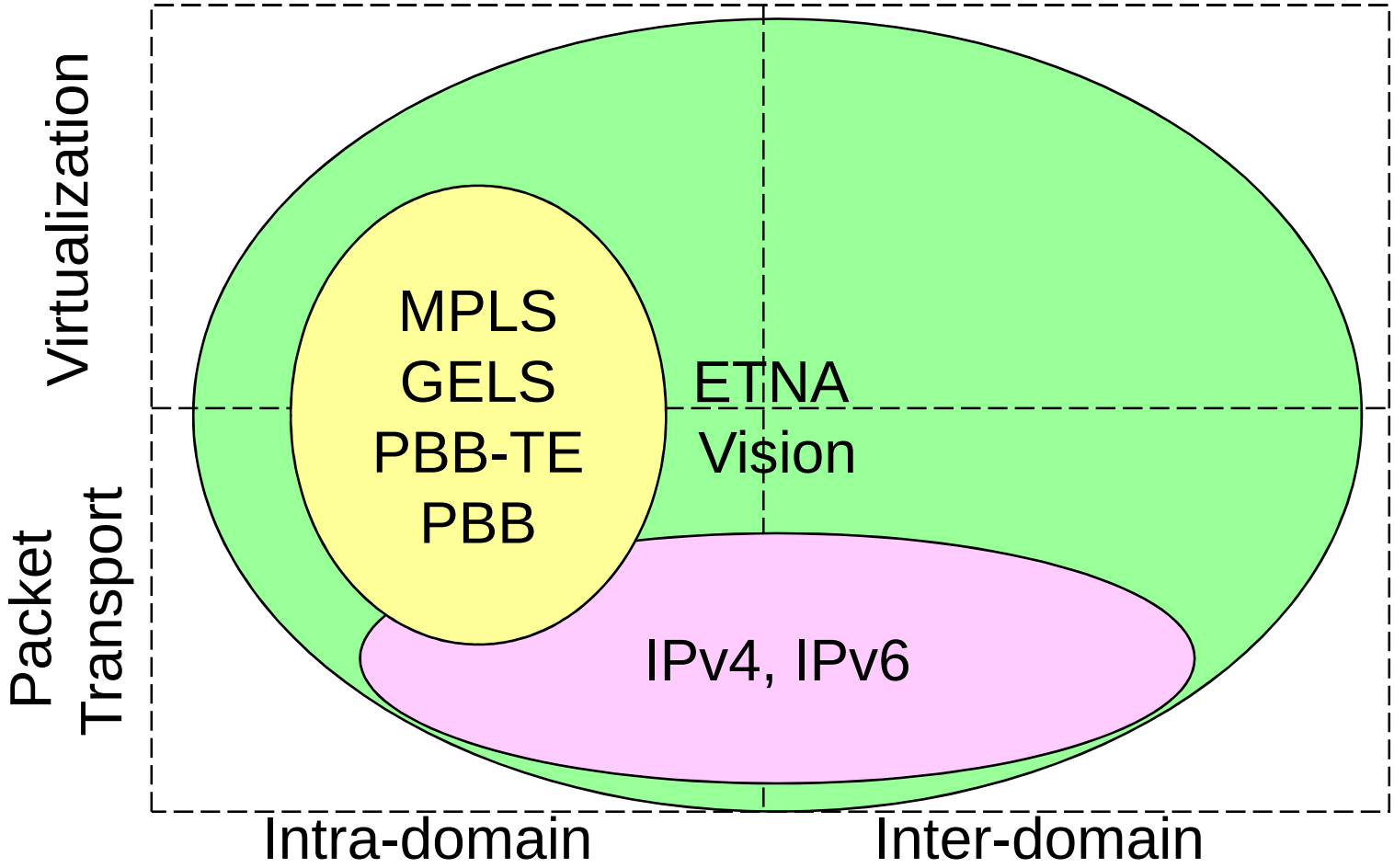
Move from Synchronous to Packet Transport

- ATM → does not scale → phase out
- SDH → scales up to 10 or 40 Gbit/s → not enough for future backbone links
- Carrier Grade Packet Transport
  - ISP requirement: Carrier Grade = ISP allows traffic from A to B, then it is transported. All other traffic is deleted (manageability, predictability and resilience).
  - MPLS is trying to become Carrier Grade (MPLS-TP)
  - Makes use of statistical multiplexing on transport level
  - Rate (and thus power consumption) can be adapted to traffic

Ethernet development

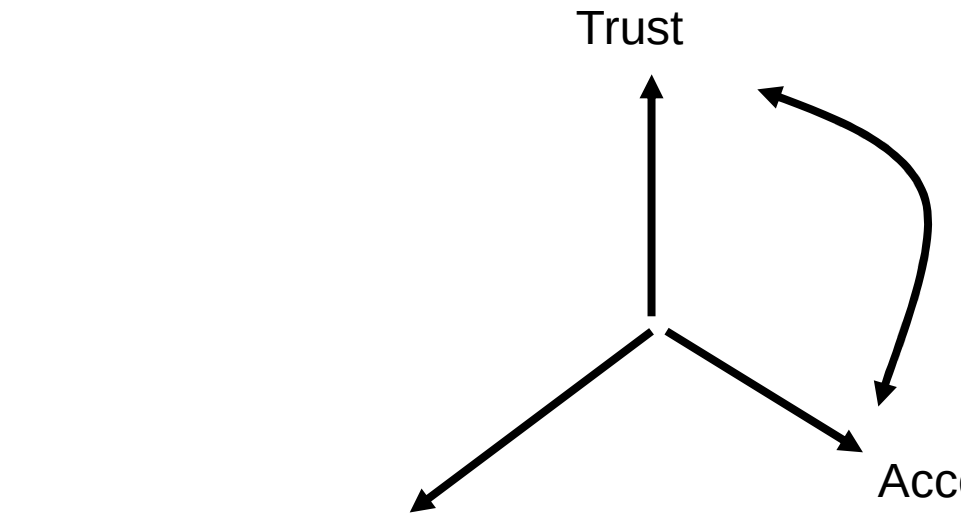
- 10GE is shipping
- 100GE is on drawing boards, expected on markets in 2010/11
- Many new wireless access variants are emerging in the ”802.x” family
- Provider Backbone Transport (PBT) and MPLS-TP are trying to become native packet based carrier grade transport solutions for network operators.
  - Connection oriented: route tables populated by Network management system
  - New variants of ”MPLS” used to support the creation of pipes and Traffic Engineering.

Design Space for Future Network Infrastructure



Three Tiers of the Future Internet

Global system of trust: a war can not be won by defense only



Carrier Grade Network core

- Forwarding in tunnels
  (IP/MPLS-TP or native Ethernet)

Access

-make all IP addresses private
- never release any address info
  across trust boundary
- cross trust boundary = show ID
- packet access control (~FW)
- map traffic to and from tunnels

Principles

Internet based on IP

- End-to-End Principle
  - E.g. DNS is a service among others
  - Network does not need to know its users
- IP over everything
- Dynamic routing
  - IP address has dual semantics
  - Support for a single naming/addressing scheme (IPv4 addresses **or** IPv6 addresses)
  - Multihoming visible to routing
- Data Plane and Control Plane not separated
  - All nodes visible to each other
- Mobility – at best some sort of add on.
- VPN support is an add-on (MPLS, IPSEC, etc)

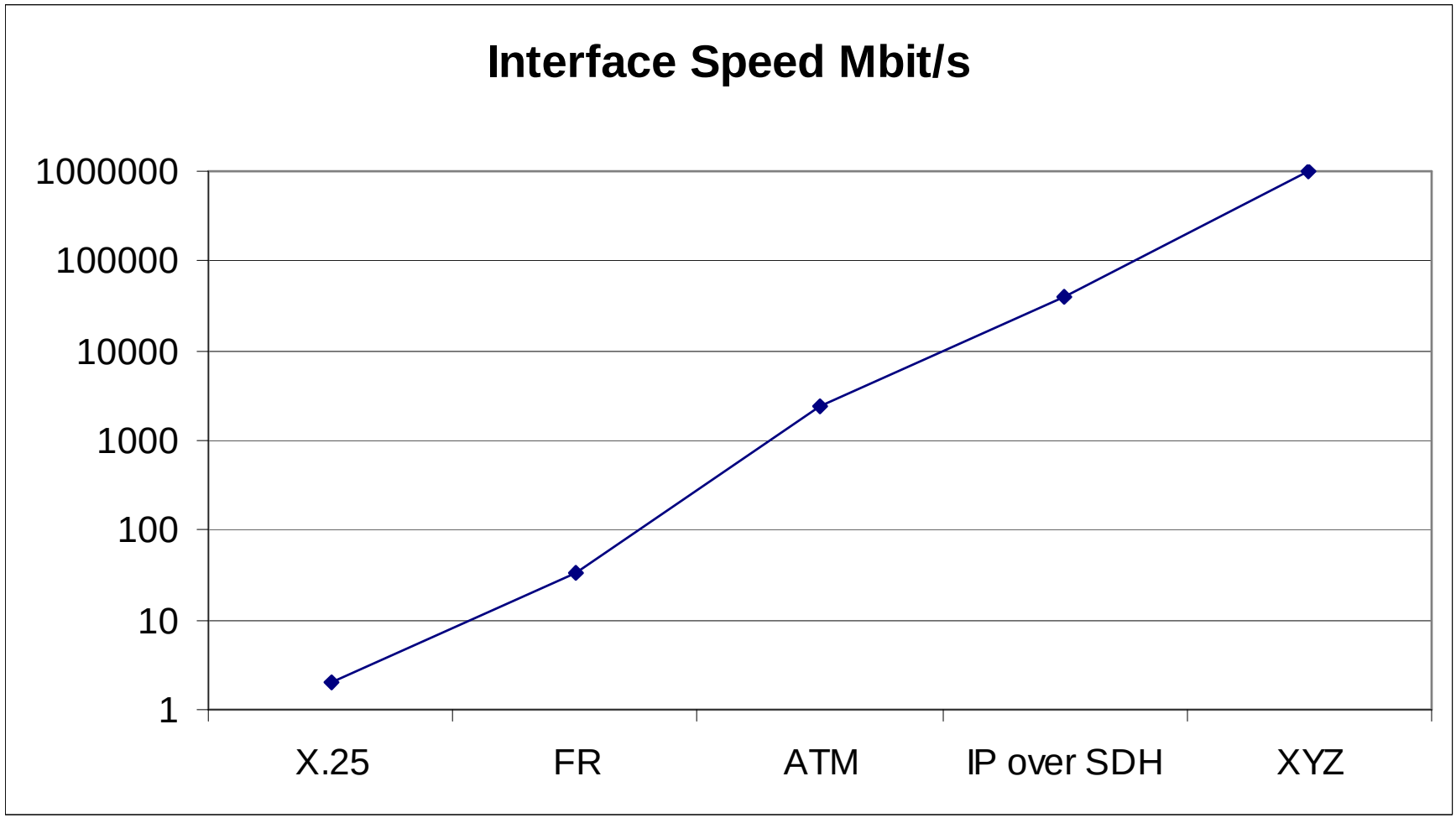
Internet by Ethernet

- Trust-to-Trust Principle
  - E2E path has 3 trust domains: originator network, operator domain and target network
  - Each domain hides its addresses
  - Domains are isolated by trust boundaries
  - Address resolution is a network feature
- Ethernet Everywhere
- Dynamic routing + dynamic address resolution + switching on the edge
  - Identities and locator addesses are clearly separted
  - Can simultaneously support many addressing schemas (IPv4, IPv6, NSAP, E.164 …)
  - Multihoming is a matter of address resolution and edge switching, does not impact routing
- Control Plane clearly separated from data plane → more robust design
  - Network not visible to users
- Mobility management implemented uniformly with other forwarding features
- Integrated VPN support, several parallel models for managing connectivity meeting different trust needs

Research Issues

- Addressing, identities and naming
  - Translations between the three, different ID schemas, how best to turn IP addresses into private addresses
- Control Plane
  - Routing (ISIS and other)
  - Service discovery
  - Address resolution
  - TE (we need to manage capacity allocated to different services and VPNs)
  - Mobility Management and mobile access
  - IP over Routed Ethernet and to/from RE,
  - Switched Ethernet compatibility
- How to tackle security and unwanted traffic: packet access control and global trust management
- Testing and deployment scenarios

Reality check



Conclusion

- Terms
  - Below IP Networking
  - Routed End-to-End Ethernet (RE2EE)
  - Post IP, Internet by Ethernet
  - Trusted Internet
- Routed End-to-End Ethernet does not depend on upgrading all hosts connected to the Internet, rather emerges gradually from Metro Ethernet
  - Deployment in hosts and different networks is independent
  - 3 independent deployment areas: Core, Access and Global Trust
- Allows wide area networking without IP for a new service e.g. with network assured identities.