Helsinki University of Technology
Networking Laboratory

Future Internet - in Search of a New Networking Paradigm

MUM 2007 Keynote

Raimo Kantola

Raimo.Kantola@tkk.fi

Helsinki University of Technology
Networking Laboratory

Erosion of IP Principles

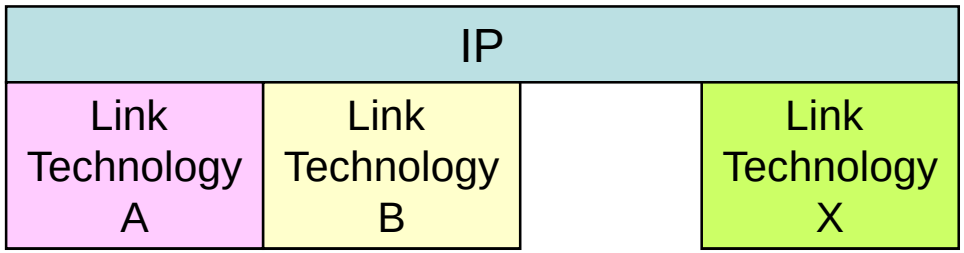
- Dave Clark, 1984: End to End Principle:

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."

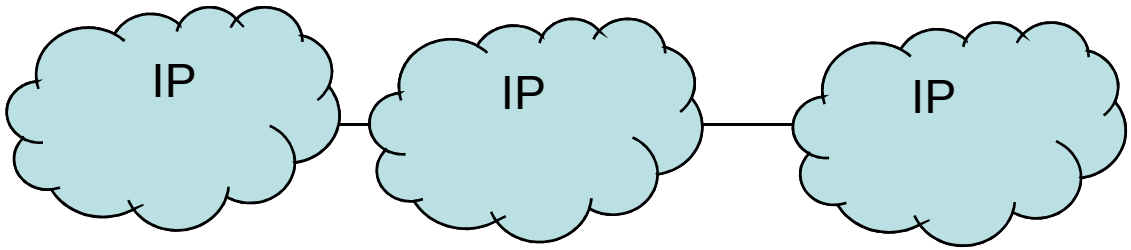
- Dave Clark, 2007: Trust-to-trust:

“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
- Applications Gateways between networks

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

IP Economics

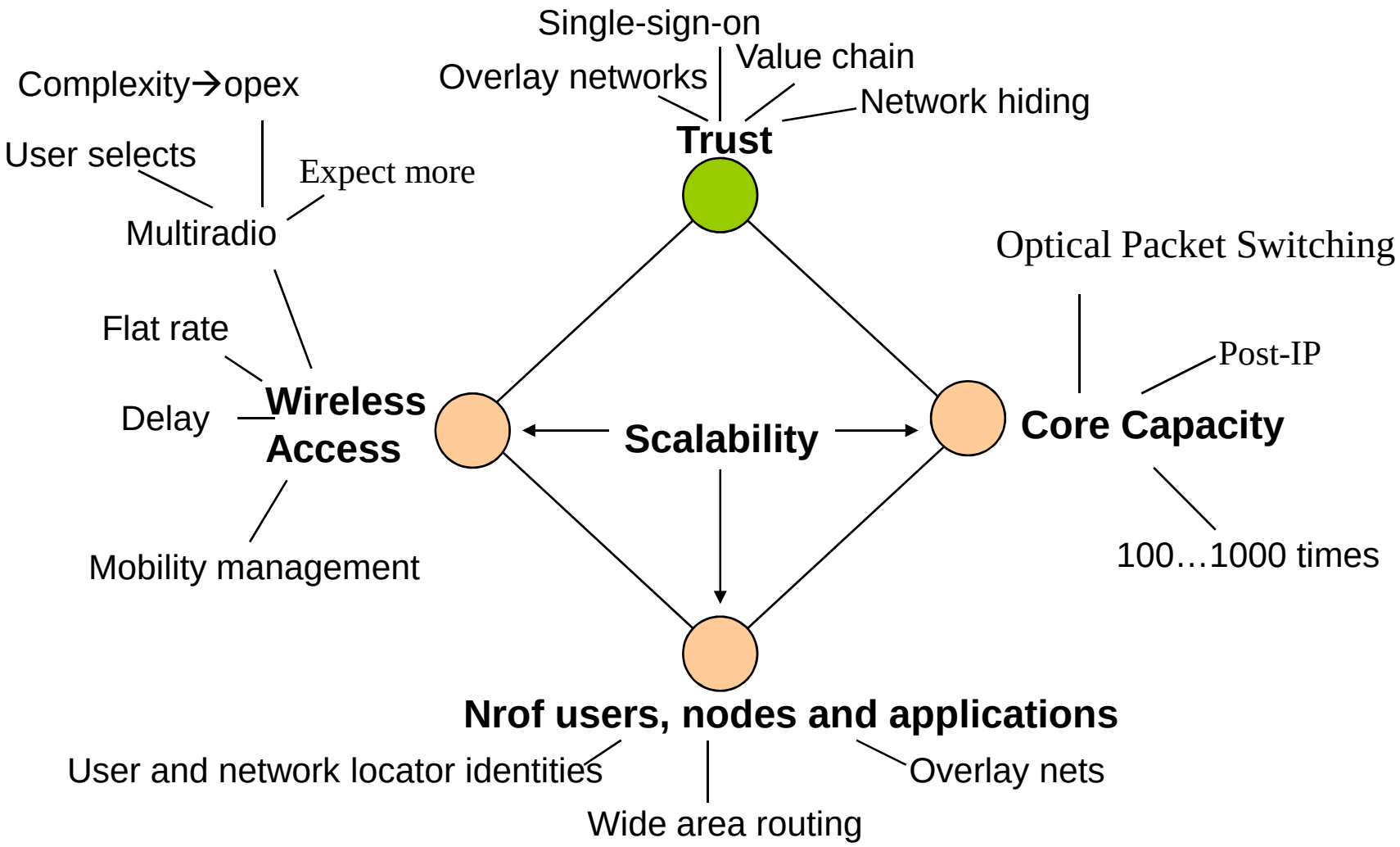
- Flat rate service – economically efficient prices
- ISP margins from residential Internet services are low or non-existent
  - tends to grow uncontrollably creating a threath of forced investment and losses
- ISPs make their margin on Corporate connectivity services: VPNs etc.
  - close to half of traffic

What else is wrong with IP?

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

Helsinki University of Technology
Networking Laboratory

Grand Challenges in Networking



What does this mean?

- Trust-to-Trust = We legitimise the misuse of IP-technology to meet legitimate customer needs in trust.
  - how to legitimize the breaking of IP over everything?
- Fundamentally, IP fails to support more than a single, low trust level. Customer and service needs in this respect vary greatly.
  - Lot's of add-on solutions have been developed.
- The original IP network assumption that receiver wants to receive what sender sends is false → spam, malware.
  - This is mostly an economic problem: cost of communication is born by the receiver because sending is so cheap.

Information networking

- Network segmentation reduces the Innovation potential supported by the original Internet model
- Users and companies coming up with solutions:
  - Peer-to-Peer
  - Data Oriented Network Architecture (ICSI)
  - Distributed web (HIIT)
  - Publish and Subscribe (P. Nikander, LME)
- Question is: on top of IP or without IP

Top-down?

Helsinki University of Technology
Networking Laboratory

What is happening with Transport?

- ATM → does not scale → phase out
- SDH → scales up to 10 or 40 Gbit/s → not enough for future backbone links
- ISP requirement: Carrier Grade = ISP allows traffic from A to B, then it is transported. All other traffic is deleted.
  - IP is not carrier grade
  - ISPs consider MPLS carrier grade but MPLS is expensive (e.g. higher OPEX than SDH)

Ethernet development

- 10GE is shipping
- 100GE is on drawing boards, expected on markets in 2009/2010(?)
- Many new wireless access variants are emerging in the ”802.x” family
- Provider Backbone Bridging (PBB) and Provider Backbone Transport (PBT) 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.

What is needed?

- Mission Statement: Future Internet Research

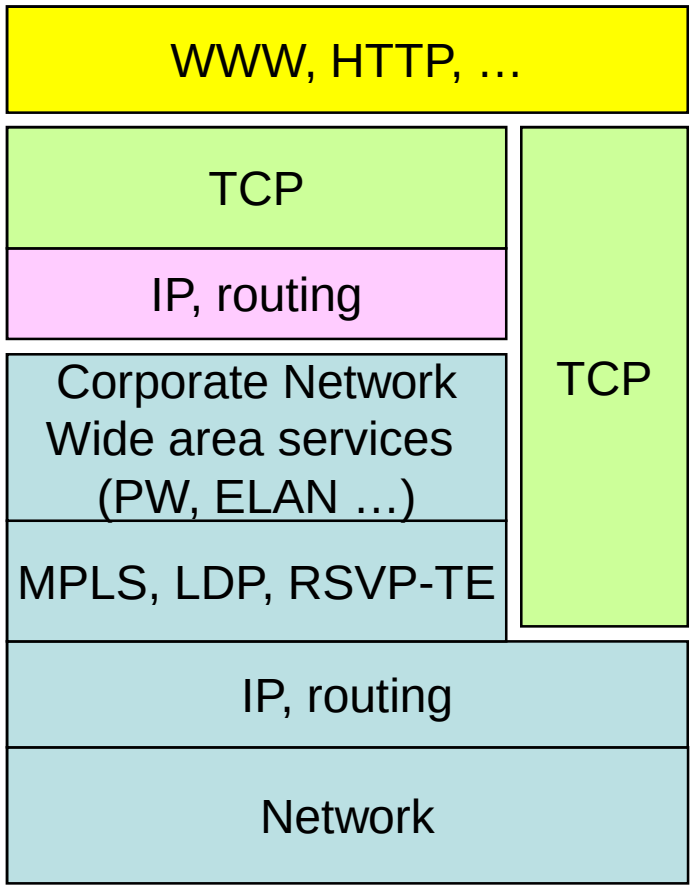
  *Enhance the Internet technology and ecology as a platform for **innovation** while providing strong **governance over** the use of the network resources and information in such a way that especially **mobile use** of the network and its services will be natively supported.*

- My Solution:
  - IP over everything → encapsulation/ decapsulation on admin boundaries
  - Transparent network → network as a black box
  - Routing + DNS → Registration of devices + Routing + Caching + Several parallel Name to Address resolution services for different trust levels

Current IP/RE comparison

Today

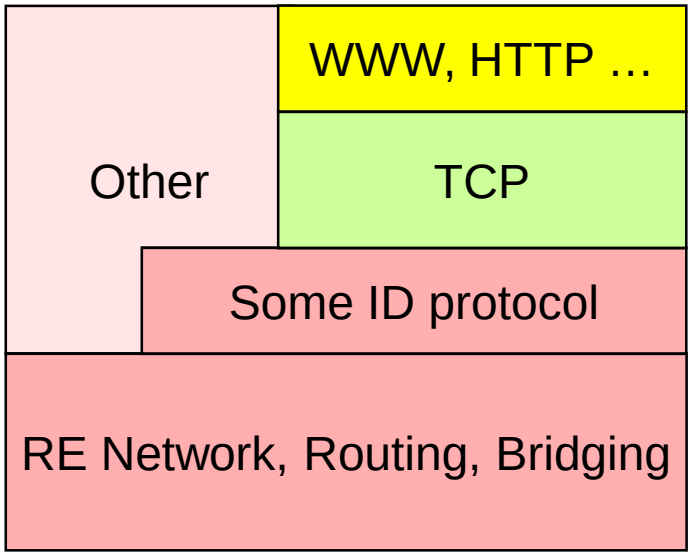
IP + MPLS + VPN



Future

RE2EE

Routed End-to-End Ethernet



Helsinki University of Technology
Networking Laboratory

Principles

Internet (based on IP)

- End-to-End Principle
  - E.g. DNS is a service among others
- IP over everything
- Network unconcious about users
- 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)

RE2EE

- End-to-End Principle
  - Addressing and address resolution are an integral part of the network
- Ethernet Everywhere
- Active Devices are registered.
- Dynamic routing + dynamic address resolution and caching
  - Identities and locator addesses are clearly separted
  - Can simultaneously support many addressing schemas (IPv4, IPv6, NSAP, E.164 …)
  - Multihoming is an address resolution and address caching matter, 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 and naming
  - Several parallel schemas needed for different trust levels
  - Traffic on different trust levels is carried over the same infra but in different pipes
- Control Plane
  - Routing (ISIS and other)
  - Service discovery (host needs to discover the PE device)
  - Address resolution
  - TE (we need to manage capacity allocated to different services and VPNs)
  - Mobility Management
  - IP networking over RE and to/from RE,
  - Switched Ethernet compatibility
- How to tackle security and unwanted traffic?
- Testing and deployment scenarios

Helsinki University of Technology
Networking Laboratory

RE2EE Benefits

- Lower cost than IP based on wider economies of scale, lower stack and uniformity of design
- Better integration of routing with L2
  - Faster convergence
- Mobility
  - a uniform design with other MAC in MAC features
  - Tight integration with network attach/detach that are L2 features
- Robustness
  - Separation of Control and Data plane
  - Network is invisible to users, Core routing does not react to client network state changes
  - Neat support for multihoming with a combination of routing, caching and address resolution
- Uniform approach to services
  - → service tag → VPNs, TE, multitopology routing etc…
  - → Services available to mobile and non-mobile users

RE2EE Benefits

- Separation of identities from locator semantics
  - → E.g. Identities can be per service or a set of services.
  - → Network assured identities can be required per service
  - → Anonymous identities can be explicitly protected by the network or a service (if one can trust the network or the service) (e.g browsing without being personally tied to having visited a site) without compromising efficiency.
- Differentiation by trust level
  - several addressing/naming id models and resolution services categories
    - ”Trusted” (e.g for VPNs, banking etc)
    - ”Operator assured” with AAA (e.g. similar to GSM)
    - Normal for BE services (e.g based on DHT) for web 2.0 etc.
    - etc.
- For operator: divide and conquer – use one infra to support many services in a managed way.

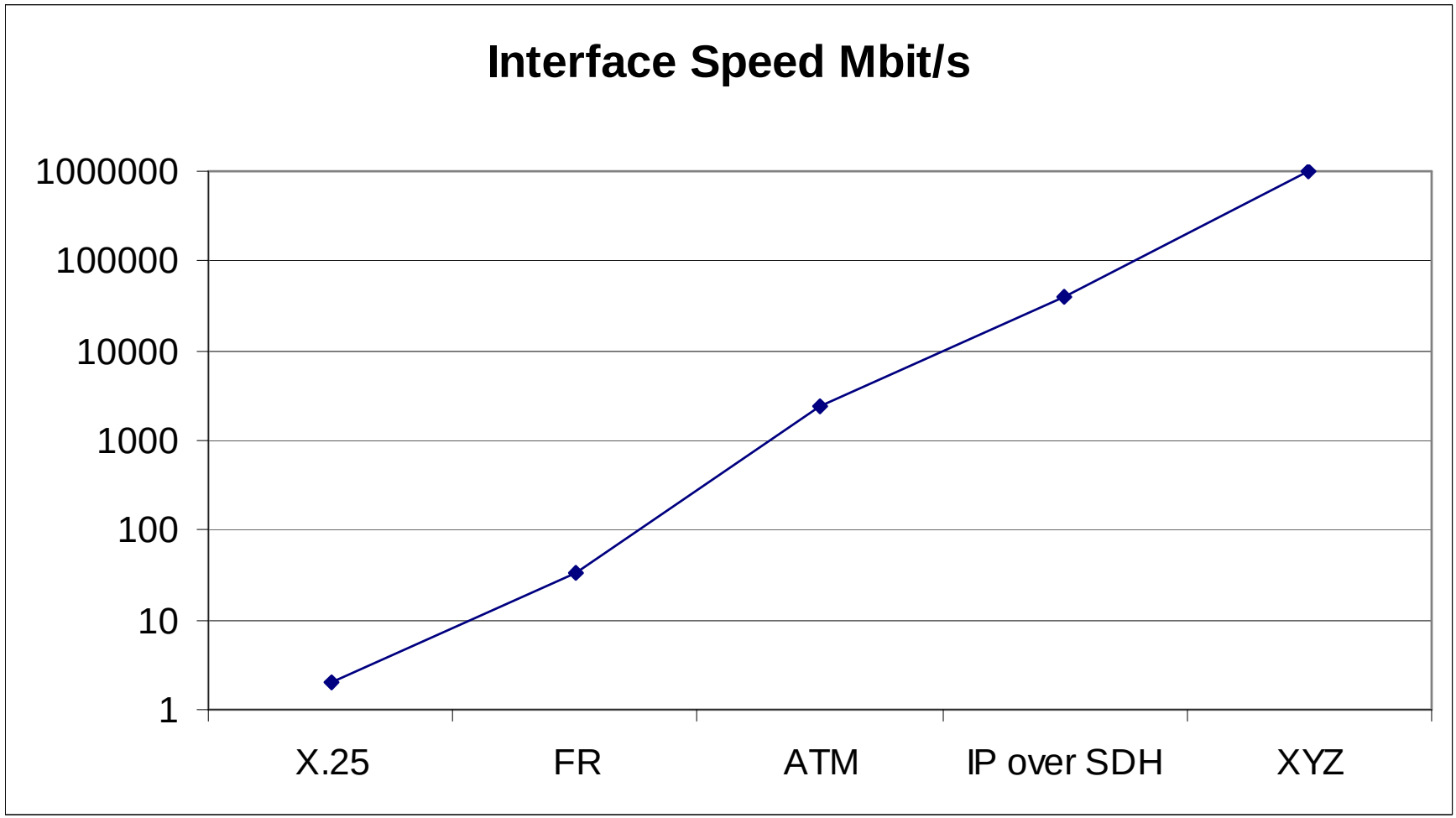
Helsinki University of Technology
Networking Laboratory

A Business case: Mobile access

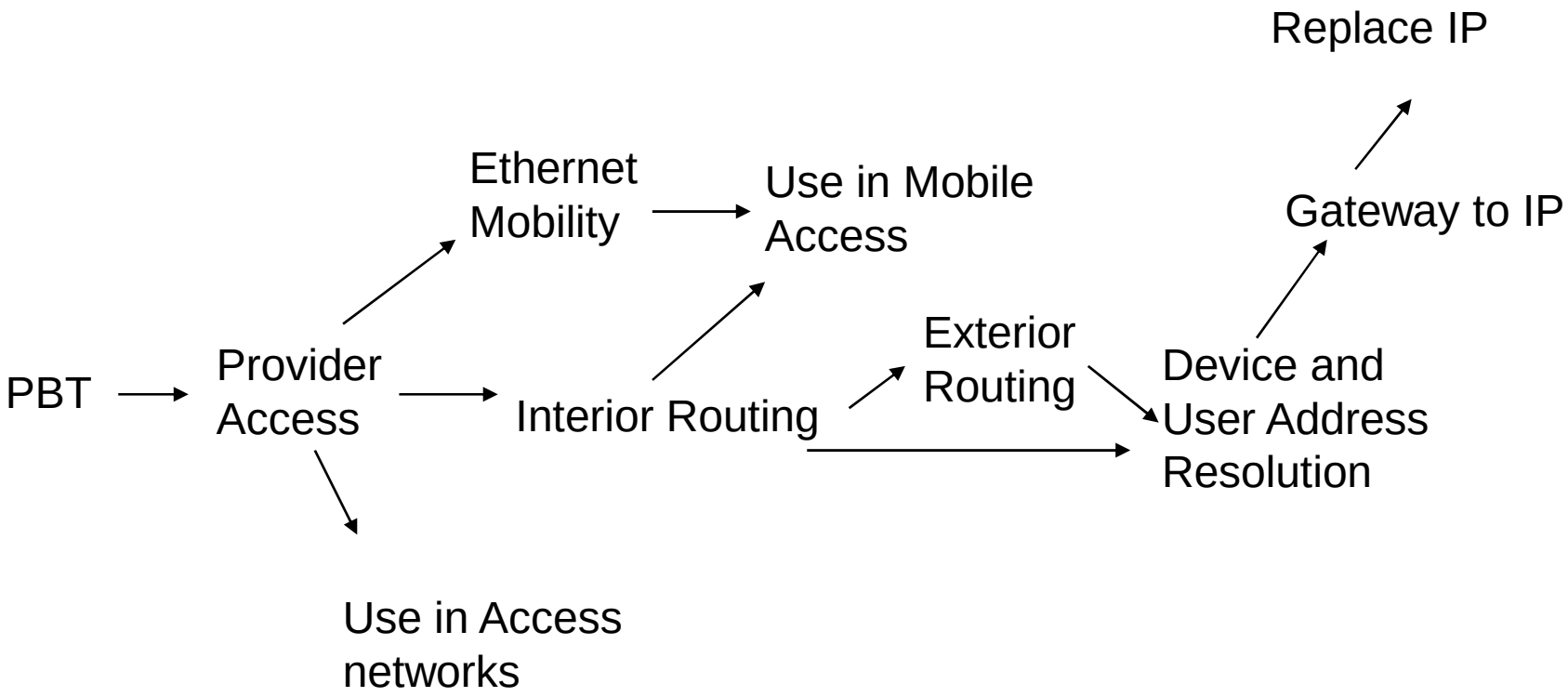
- Apply to IMT-Advanced or LTE
- Flat and efficient stack to replace the double IP stack in 3G architecture
  - lower delay in access
  - less cost
  - integration of access transport supported mobility with HSS based mobility
- Fit with Metro Ethernet

Helsinki University of Technology
Networking Laboratory

Need for new core network technology



Roadmap


Replace IP
Ethernet Mobility
Use in Mobile Access
Gateway to IP
PBT
Provider Access
Interior Routing
Exterior Routing
Device and User Address Resolution
Use in Access networks

Conclusion

- Search for a new networking paradigm is on
  - IP delivers the opposite to what are the stakeholder needs in trust
  - Information networking
  - Routed End-to-End Ethernet
- Ethernet replacing SDH for Core Transport
  - can we leverage this move to replace also IP?
  - Interleave Ethernet Carrier Grade pipes with pipes supporting dynamic routing and connectionless traffic
  - Is there an incremental path to enhance Ethernet?
- It is time to think beyond IP.

Helsinki University of Technology
Networking Laboratory

Some Information resources

http://www.ieee802.org/1/pages/802.1aq.html
http://www.metroethernetforum.org/
http://www.metroethernetforum.org/documents.htm