Future Internet is by Ethernet

Raimo Kantola

Aalto University

Finland

www.re2ee.org

Agenda

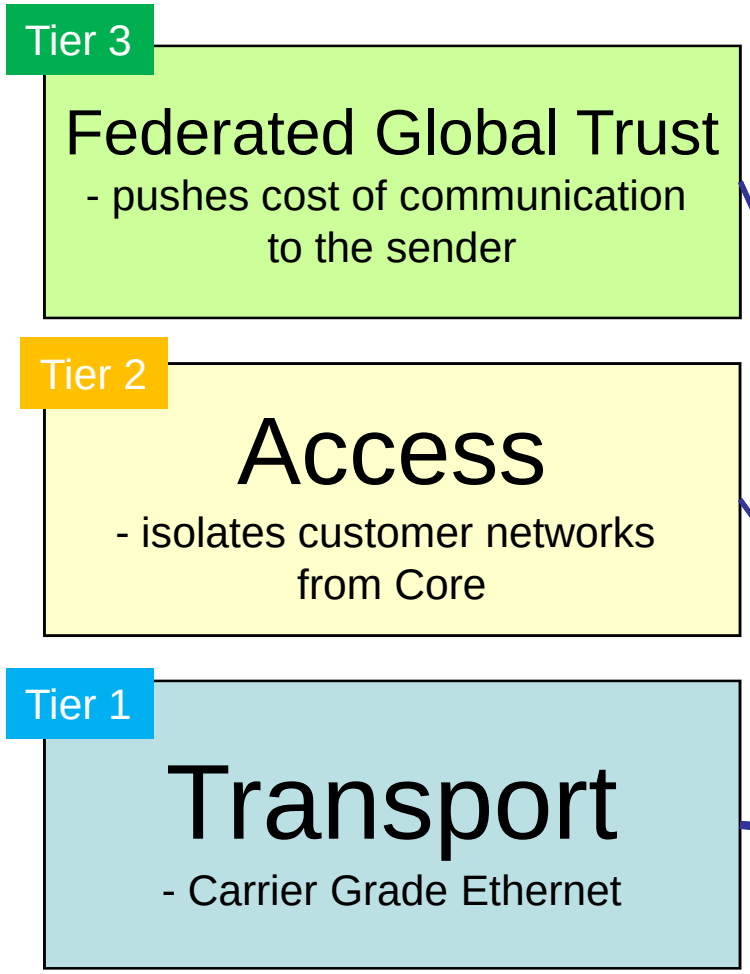
- Big picture
  - 3 tier model of R&D&D
- Principles explained and justified
  - Customer edge switching in operation
  - Global Trust
- Deployment and Challenges
- Conclusions

Work partially sponsored by FP7 ETNA project and ICT SHOK in Finland

Challenges of the Internet

- Lack of Trust – middleboxes: NATs and Firewalls are not part of the ”Architecture”
  - Mobile broadband has overtaken fixed and is growing faster
  - Recommended NAT Traversal method = UNSAF does not scale well to mobile devices
  - FW on mobile device exhausts battery
  - Interrupt driven access architecture is a MUST for mobile hosts
- Unwanted traffic – cost of communication is born by the receiver
- Scaling the core, Energy efficiency, multi-homing
  - Tunneling based edge – not yet an accepted technology
  - IP itself does not scale to >10x increase in traffic

Three Tier Program for Trusted Internet based on Ethernet



- R&D&D on each tier can progress independent of the others
- The war against unwanted traffic can not be won by defense only
  → Global Trust System
- Access: Customer Edge Switching
- Transport: Carrier Grade Ethernet + legacy (IP/MPLS)

Principle 1: New Business principles

- From Best Effort that serves the sender and makes the receiver pay the cost of communication

to

- Make malicious senders of unwanted traffic pay = Roll the cost from receivers to senders.
  - Re-align the business incentives of ISPs and subscribers to achieve this goal

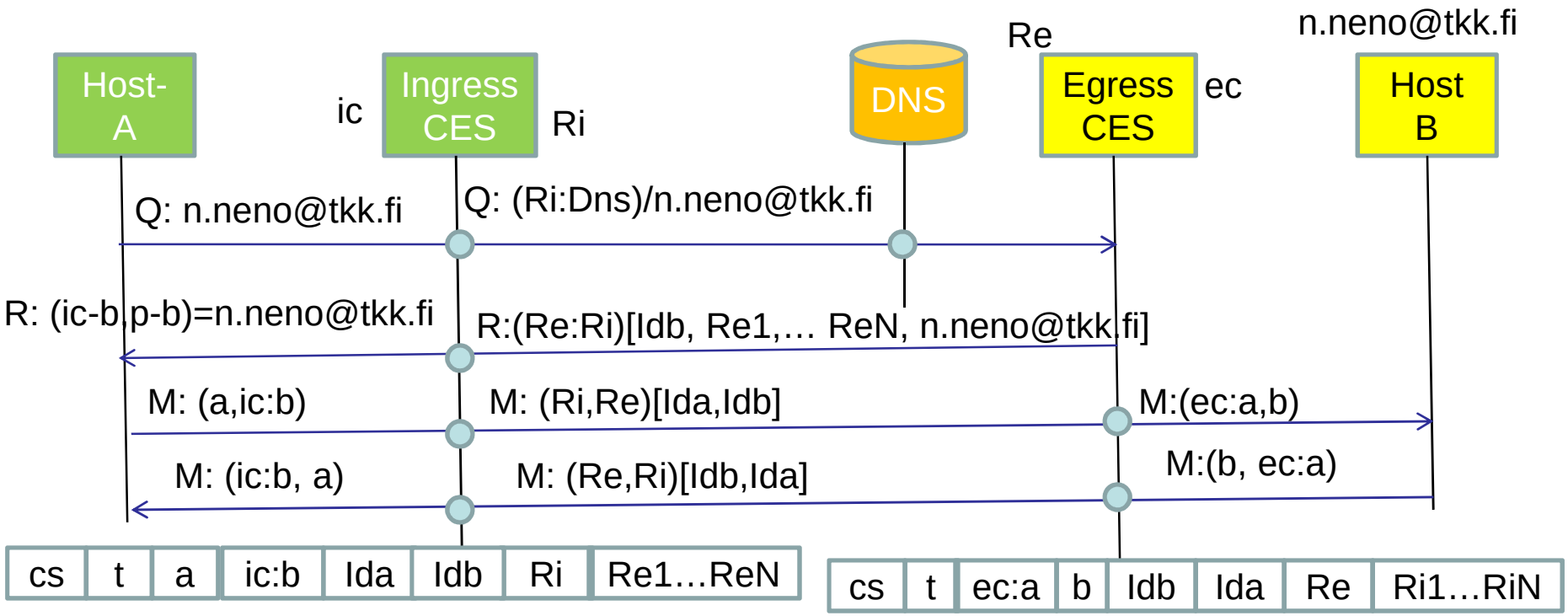
Principle 2: Redesign bottom-up

- No interest to develop synchronous transmission further up from 40G → move to Carrier Grade Packet Transport
- Energy Efficiency
  - Energy Efficient Ethernet has arrived
  - IP itself does not scale to >10x increase in link capacities – needs too much processing per packet and requires too many layers too often
  - The higher layer switching is used the more power is consumed
- IPv6 does not meet current networking requirements
  - Network hiding, network virtualization, multi-homing
  - Who needs 50 000 quadtrillion addresses per user?
  - Not a good idea to give a globally reachable IPv6 address to a battery powered device

Principle 3: Recursive Addressing

- For Global communication use
  - Globally Unique Names,
  - Locally significant IDs and
  - Locally significant addresses
- A Chain of addresses and Ids points to the target
- Can continue using IPv4 as long as we want (in the role of ID protocol) on hosts.

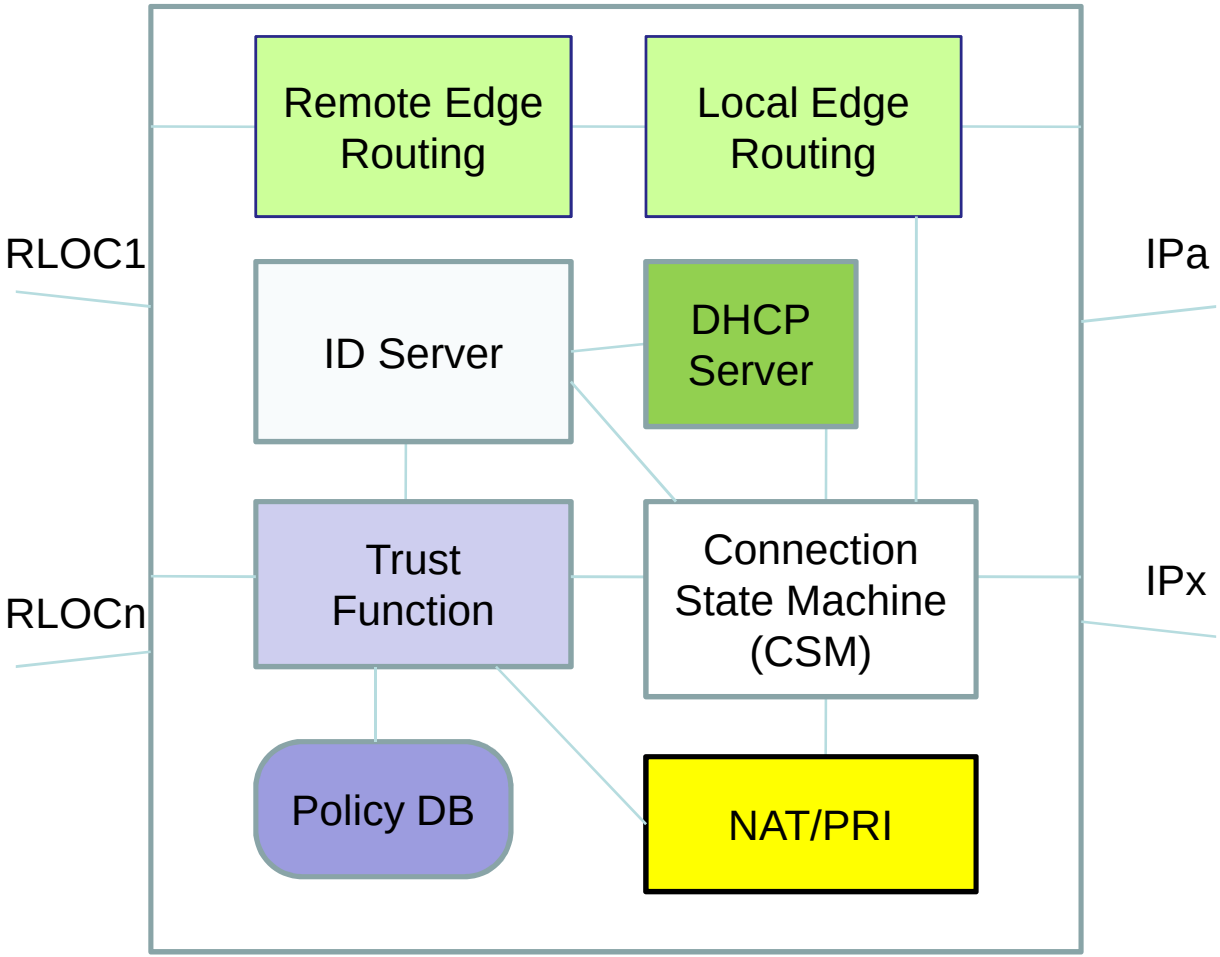
Principle 4: State on Trust Boundaries



a – IP address of host a
ic – address pool of ingress CES
ic:b – IP address representing host b to host a
p-b – port allocated by i-CES for communication with host b
Ri (Ri1….RiN) – Routing locators of ingress CES
Re (Re1 …ReN) – Routing locators of egress CES

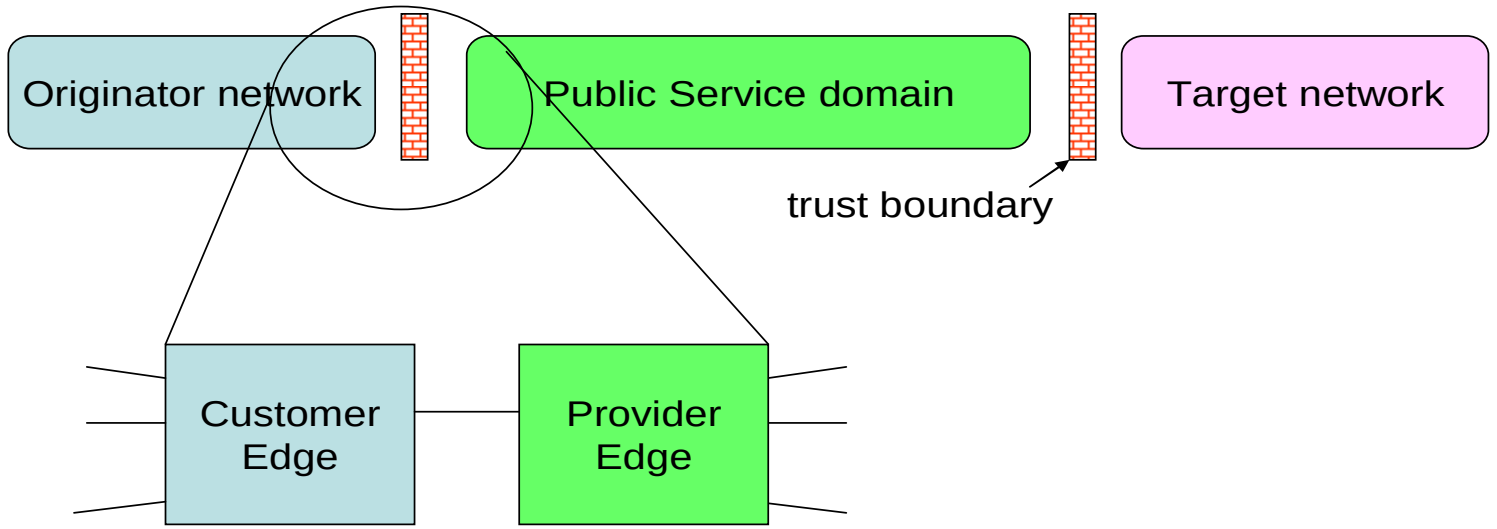
Ida – ID of host a
Idb – ID of host b
ec – address pool of egress CES
ec:a – IP address representing host a to host b
cs – connection state, t - timeout

Model of CES connected to IPv4 core



Protocol specific FSMs for
- DNS
- FTP
- SIP etc

Principle 5: Communication Path is a Chain of Trust Domains: Each Domain is independent in terms of addressing and forwarding technology



Trust domains do not publish address information to each other.

A Packet crosses a Trust Boundary by presenting 2 IDs: source ID and target ID.

There is connection state on the Trust Boundary.

Principle 6: Network natively supports virtualization

- Ethernet has VLAN tags
- 802.1ah has
  - C-VLAN
  - B-VLAN
  - I-tags

Principle 7: Recovery and Service restoration are supported by OAM

- Frequent flow of OAM packets over links
- Less frequent domain edge to domain edge
- Also End-to-end OAM flow is possible
- A framework defined in Y.1731
  - Mission critical services can be implemented at low OPEX

Principle 8: Mobility must be supported as a value added sevice over the base protocol

- Mobility Support at Ethernet layer
  - E.g. mobility extensions to TRILL
  - Mobility extensions to Carrier Grade Ethernet transport implemented in ETNA
- Simplify protocol stacks and backhaul and mobile core network design for mobile broadband

Tier 3: Federated Global Trust

- Each ISP has a trust rating based on the amount of unwanted traffic sent from that ISP
  - High trust → low peering and transit charges
  - An ISP probably will roll the added costs of transit to subscribers either as penalty charges or service charges for security
- Trust based charges need to be compared to variable charges emerging from power consumption based variable charges
- Likely minimum outcome is a new equalibrium on lower level of unwanted traffic

Reseach Questions: is this profitable for the ISPs? Can we find a robust design? Can ISPs agree on such a model? Is regulation needed to push such an approach?

From End to End → Trust to Trust

- By Dave Clark
  - End to End argument, 1984
  - Trust to trust, 2007:
    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.

We propose a Trust to Trust Protocol for Customer Edge to Customer Edge communication in www.re2ee.org

Ease of deployment

ACCESS and Interoperability with legacy Internet
+ develop CES as an extended NAT
+ DNS: no new record types nor changes in the protocol
+ egress CES also hosts PRoxy Ingress CES for compatibility with legacy senders
+ no changes in hosts
+ provides incentives to invest both to mobile operators and corporations
+ no ”alternative topology” like in LISP
+ proposes a CES-to-CES protocol called Trust-to-Trust Protocol

Carrier Grade Ethernet core

- Low header overhead
- Full OAM for mission critical communications

IP core

- Cuts into MTU like LISP
- Overhead is minimized by IPv4 specific encapsulation in Trust-2-Trust protocol

Challenges

- Technical challenges
  - Scalability of the boundary nodes
  - Cutting power consumption further
  - Robustness and accuracy of the global trust system
- Deployment – convincing the ISPs and vendors
  - Need more techno-economic studies
- Global Trust: Agreement on a new alliance for managing the schema
  - Cmp: GSM MOU
  - New peering agreements
  - New Transit agreements
  - New subscription agreements

Conclusions

- Networks move from synchronous byte oriented transmission to packet transport
  - Energy efficiency, scalability and cost are drivers
  - Ethernet will be everywhere and provide first Edge to Edge transport, later end to end service
- Access must be interrupt driven
- Separation of identities and addresses leads to tunneling based Edge →
  - significant improvement in core scalability
  - Selection of forwarding technology must be independent by each carrier
- There is no need for IPv6, instead let us use IPv4 as an identity and locally routed protocol in hosts
- Getting rid of unwanted traffic is a business problem: we propose a system of global trust to attack the phenomenom