Aalto University
School of Electrical
Engineering

Customer Edge Switching – A large scale GENI experiment?

Raimo Kantola

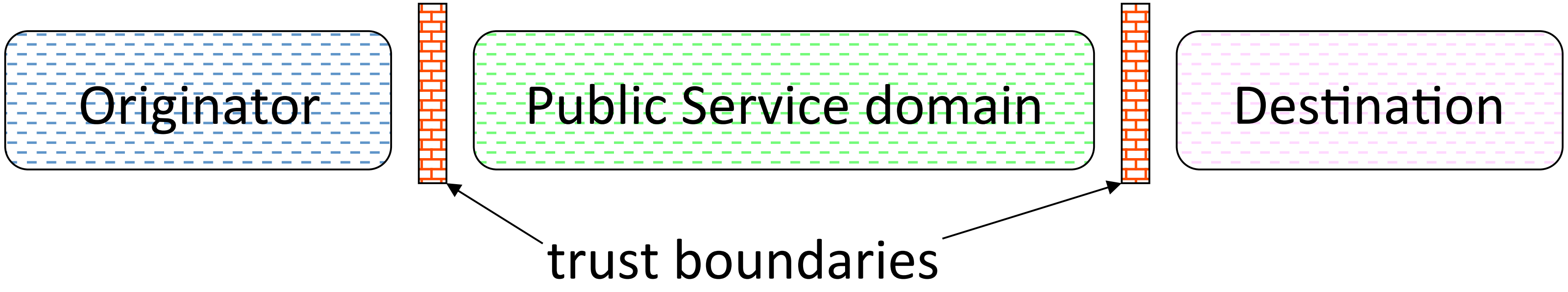
Raimo.Kantola@aalto.fi

Aalto University/Comnet

What is CES

- Makes Trust a cornerstone of Internet architecture: Network should do its best for both the sender and the receiver
- Cooperative Firewall and Replacement of NATs
- SDN style implementation
- One network at a time deployment → Realm Gateway as a component of CES
  - Supports servers behind RG
  - Heuristic security

Communication over Trust Domains

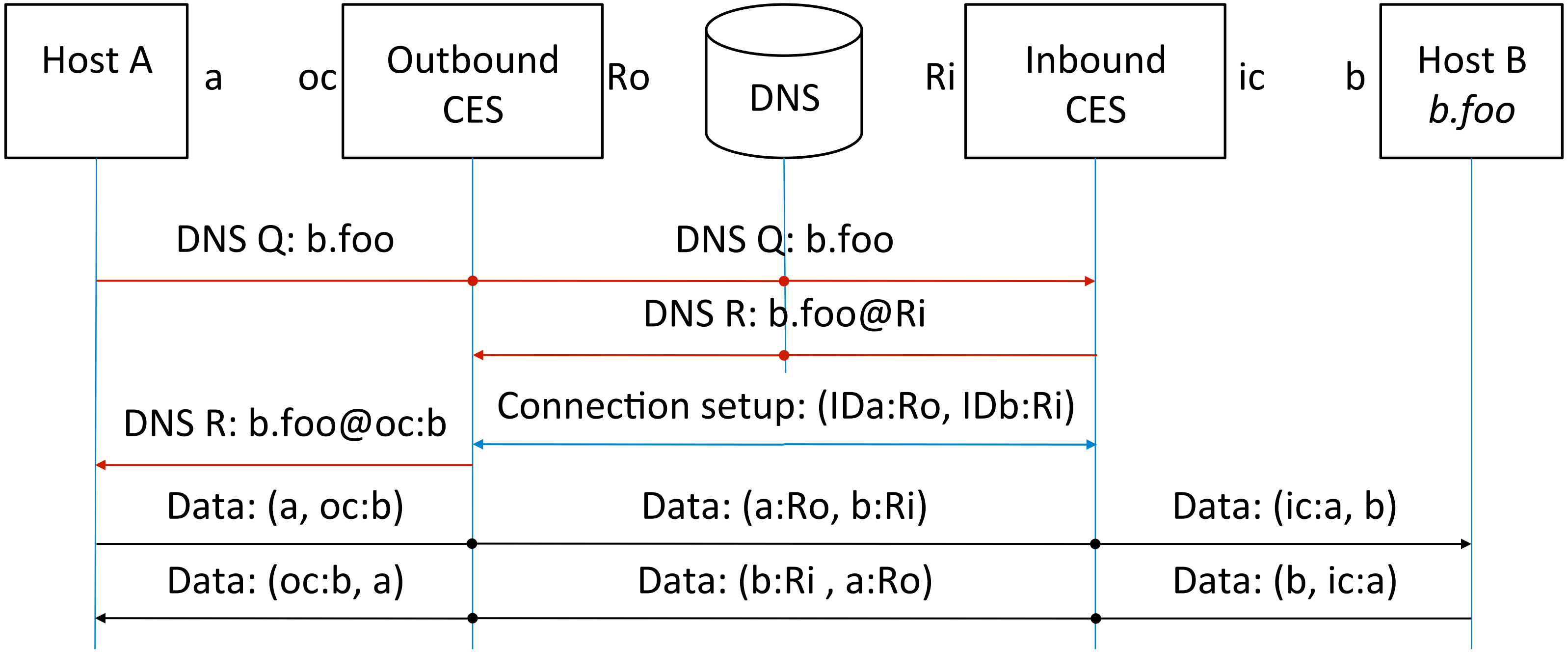


Originator and Destination are customer networks (stub networks in terms of IP routing)
+ each of them may have one or many private address spaces;
+ extreme case: mobile network addressing model: each user device is in its own address space and all communication takes place through the gateway or edge node connecting the user devices to the Internet

Trust Boundary == Customer Edge Switch == cooperative firewall

A CES has one or several RLOCs (routing locators) that make it reachable in the public service domain

Message Flow

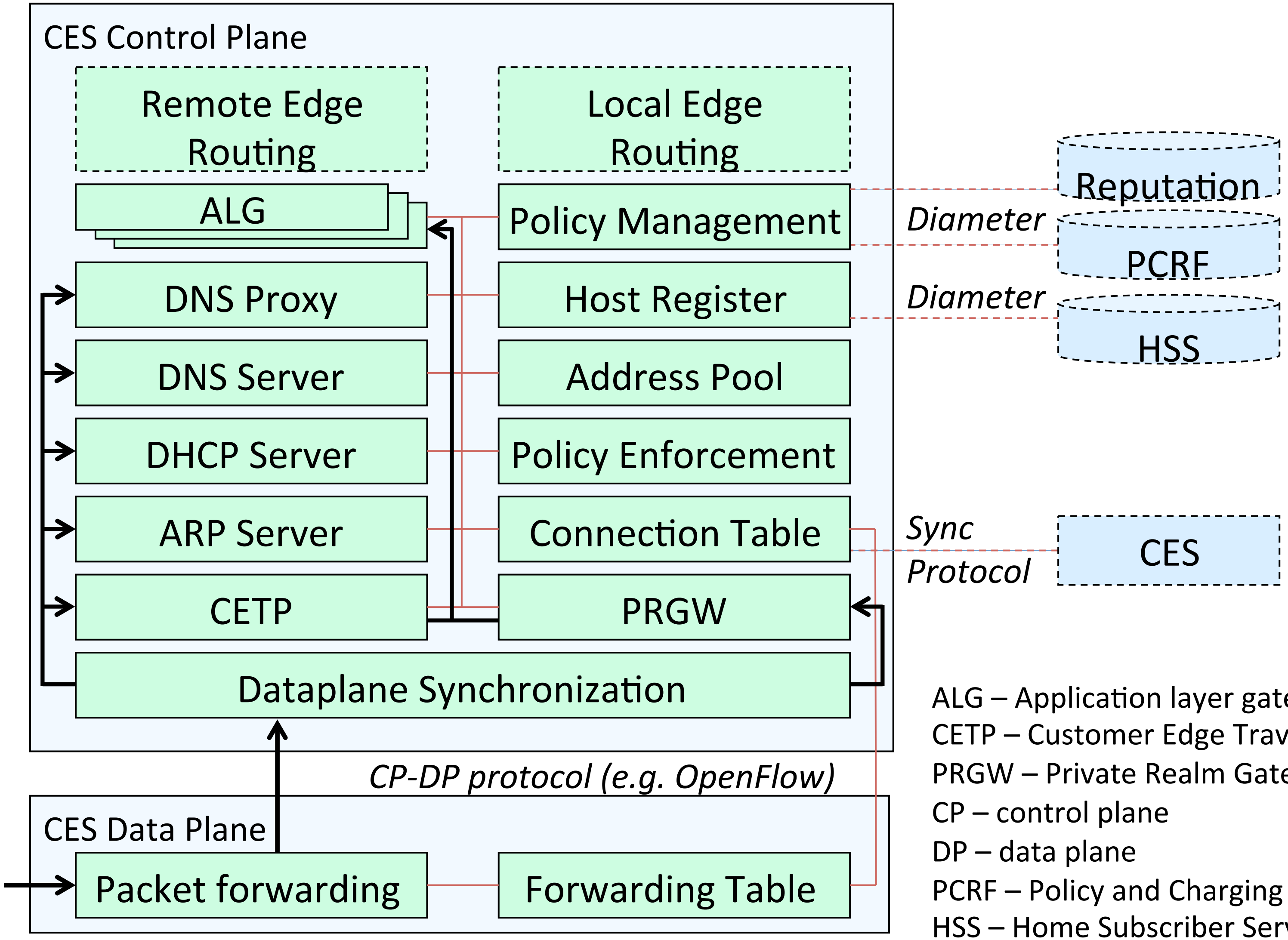


a – IP address of host a
b – IP address of host b
Ro – Routing locators of outbound CES
oc – Address pool of outbound CES
oc:b – IP address representing host b to host a
IDa:Ro – Representation of IDa in outbound CES
a:Ro – Representation of hosta in outbound CES

IDa – ID of host a
IDb – ID of host b
Ri – Routing locators of outbound CES
ic – Address pool of inbound CES
ic:a – IP address representing host a to host b
IDb:Ri – Representation of IDb in inbound CES
b:Ri – Representation of hostb in inbound CES

Aalto University
School of Electrical Engineering

Logical Structure of CES

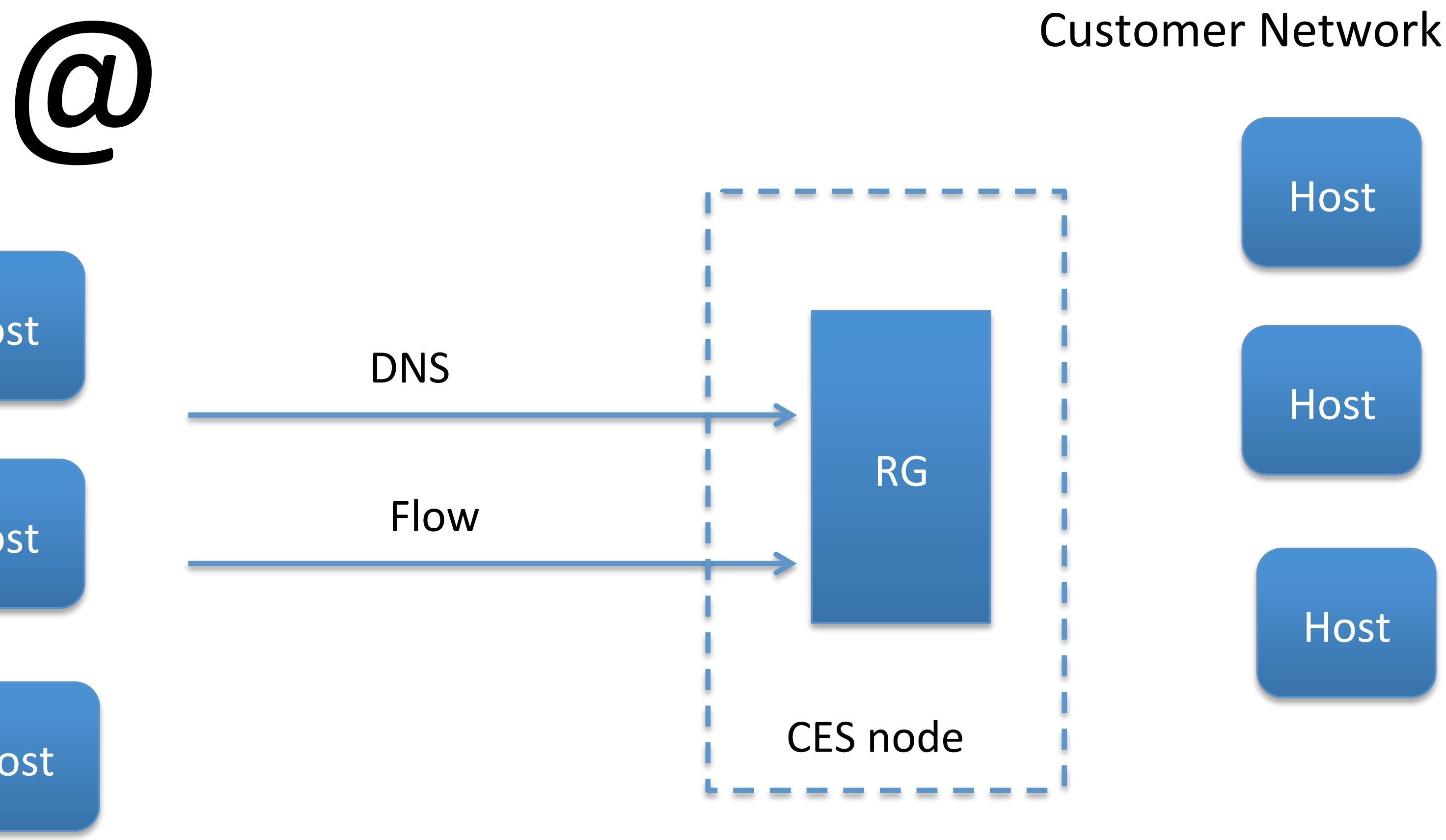


ALG – Application layer gateway
CETP – Customer Edge Traversal Protocol
PRGW – Private Realm Gateway
CP – control plane
DP – data plane
PCRF – Policy and Charging Rules Function
HSS – Home Subscriber Server

Signaling Cases

	Legacy receiver	Receiver behind CES
Sender Behind CES (new Edge)	CES acts as NAT	**Customer Edge Traversal Protocol** used To tunnel packets Thru the core
Legacy IP sender	Traditional Internet	Inbound CES acts as ALG/Private Realm Gateway or server side NAT

Realm Gateway



Security heuristics

GENI Experiment?

- Start from Ethernet circuits
- Set up IP routing (parametrize as needed)
- Add an Customer Network arrangements with CES and RG
- 100 to 1000s of hosts and nodes
- Have an attacker and defender camps
  - Break and Fix