Getting underlying information using cross-layer mechanism in transport study

Katsushi Kobayashi
ikob@ni.aist.go.jp, ikob@riken.jp

IAB/IESG joint design session on forwarding plane OAM

NATIONAL INSTITUTE OF ADVANCED SCIENCE AND TECHNOLOGY (AIST)

Note

- We just present some ideas and our research to help OAM discussion.
- There are, possibly, other design spaces and ideas to realize our objectives.

Poor visibility underlying info.

- Transport stack ”estimates” inside network.
  - Bandwidth difference from 54Kbps to 10Gbps.
  - Frequently changing network condition in mobile.
  - Corruption loss in wireless is not negligible.
- P2P peer selection, CDN server selection.
  - Not to mitigate traffic demand for backbone.
- Unable to inspect provisioned path
  - Just acknowledged from control plane.

Infrastructure of End-to-end is really dumb ?

- Router forwarding plane is already smart, not only control/management plane.
  - routing prefix, link bandwidth, available bandwidth, i/f queue, corruption loss, L2 address,
  - prefix age, corruption loss, signal strength, retransmission counter...

Requirements for getting underlying info.

- Scalability:
  - bandwidth, inter-domain, # of intermediate routers, # of flows
- Small delay:
  - Quick response from events
- Unnecessary complicated process:
  - e.g., not to rebuild path on/from NMS
- Disclosure policy among all stakeholders
  - Access control, Preserving privacy

in-band cross-layer approaches - for enhancing transport-

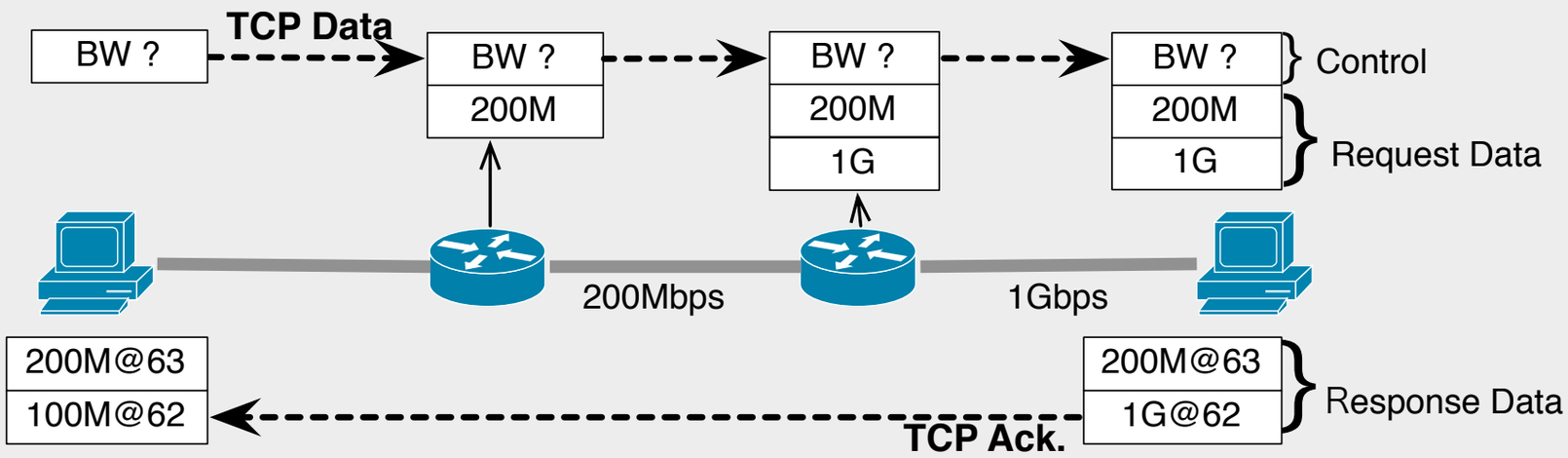
- Jack up approach with shim layer on IP
- ETEN: To focus satellite
- PTP: Header growth with prepending data
- SIRENS: Requires number of packets corresponding router hops.

➡ i-Path

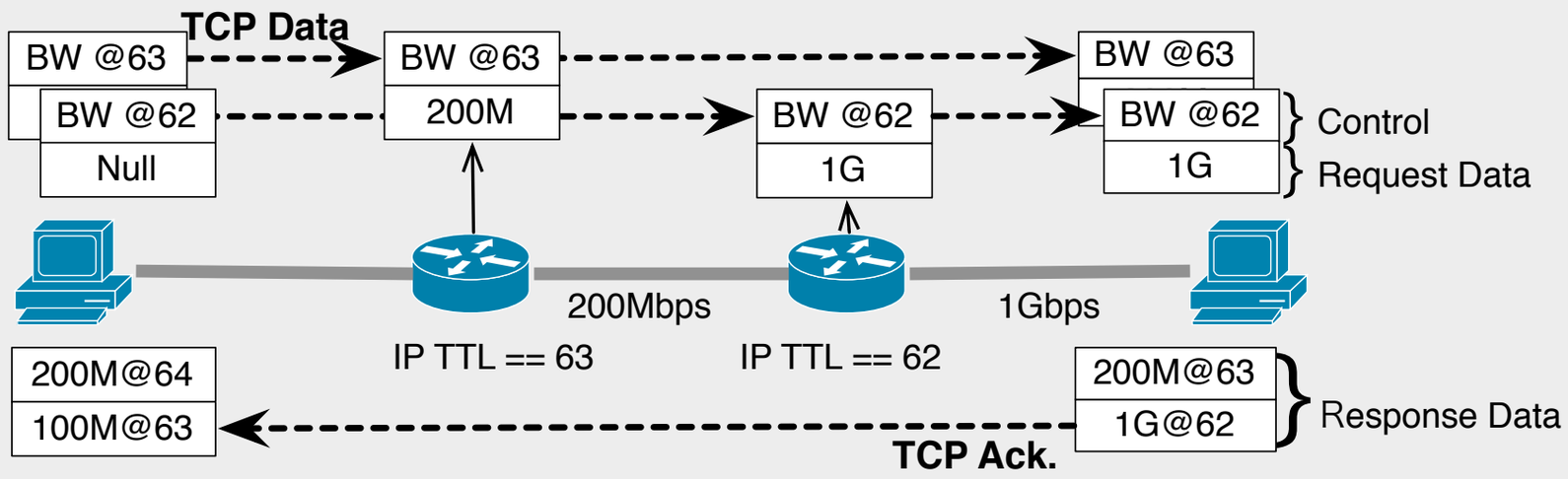
- Congestion control with more network support.
  - XCP, TCP-QS

P. Sarolahti et al. Transport- layer considerations for explicit cross-layer indications, draft-sarolahti-tsvwg-crosslayer-01.txt, 2007.

PTP and SIRENS



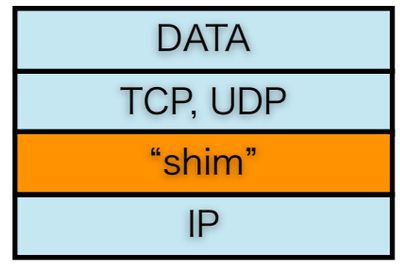
PTP: retrieve all data by single packet with header growth

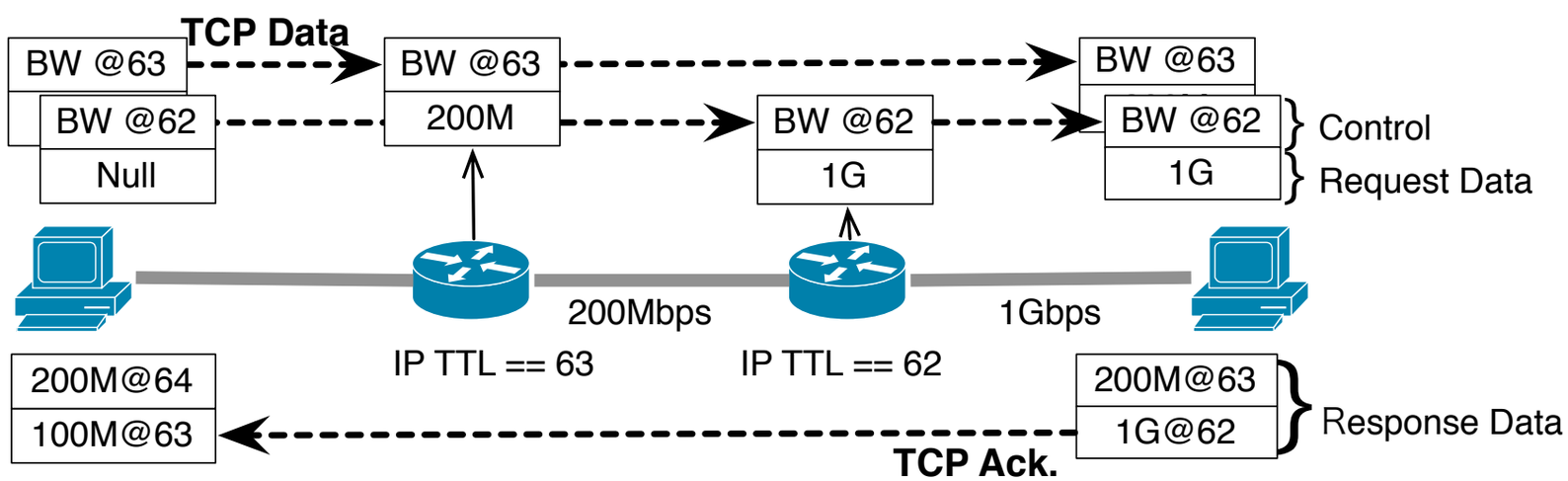


SIRENS: one packet collects one router's data

- Request: Sender specifies data type and hop count to request into “shim” header. “shim” header is piggybacked onto usual packets, e.g., TCP stream.
- Expose: Router overwrites own data into “shim” header.
- Gather / Response: Receiver replies back collected “shim” headers.

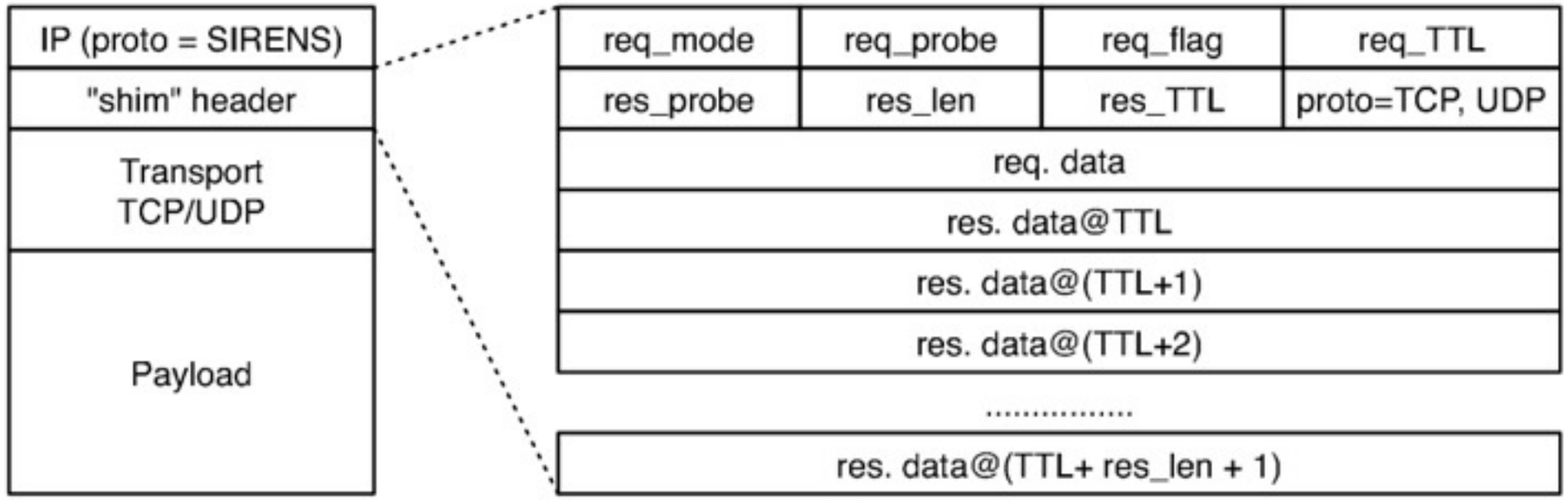
- Explored in-band cross-layer technique to improve transport performance.
  - Congestion control using underlying information.
    - ETEN: To focus satellite
  - Add more network support
    - XCP, TCP-QS, ...





SIRENS: one packet collects one data to prevent packet growth.

Inserted between the network and transport layers



Receiver notification	
req_mode	"TTL" for SIRENS ("MAX"or "MIN" for compatibility)
req_probe	"LINK", "LOSS", "QUEUE" profiles
req_flag	(reserved)
req_TTL	specify a router to respond
Sender notification	
res_probe	same as req_probe
res_len	# of data sets in the sender notification
res_TTL	TTL in the first receiver notification included in this header
proto = TCP, UDP	id of the protocol next to this header

i-Path: Network Transparency

- Reuse SIRENS.
- Objectives:
  - Collect underlying information along path with hop-by-hop granularity.
  - API for application to access underlying information.
  - Respect disclosure policies among both ends and transit ISPs.
    - i-Path is a research funded by NICT, JAPAN
    - US(NSF)-JP(NICT) Future Internet Research Program.

What i-Path realizes ?

- Focus API, not only Transport.
  - Optimal peer/server selection in P2P/CDN
  - Offer optimal rate encoding in VoD service
  - Better service with geographical location
  - Region control in contents distribution using location data not from ends, but from routers.
  - To expose underlying info. to ends, e.g., end-host, tunnel edges.

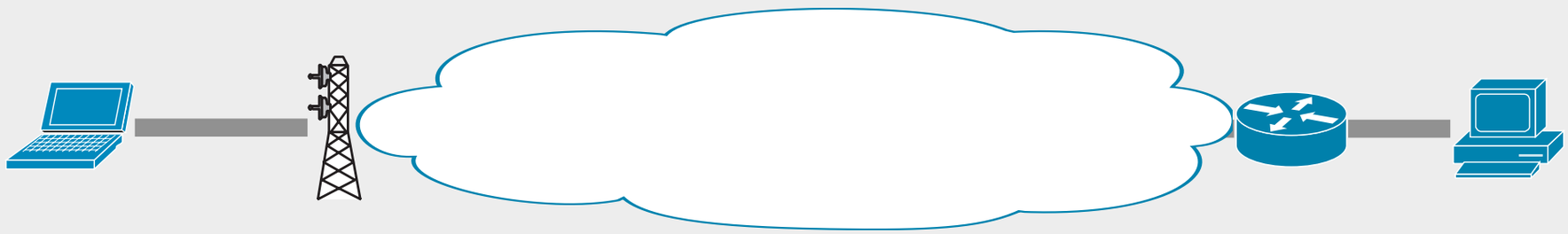
Requirements for providing underlying info.

- ✓Scalability:
  - ✓ bandwidth, inter-domain, # of intermediate routers, # of flows
- ✓Small delay:
  - ✓Quick response from events
- ✓Unnecessary complicated process:
  - ✓e.g., not to rebuild path on/from NMS
- Disclosure policy among all stakeholders
  - Access control, Preserving privacy

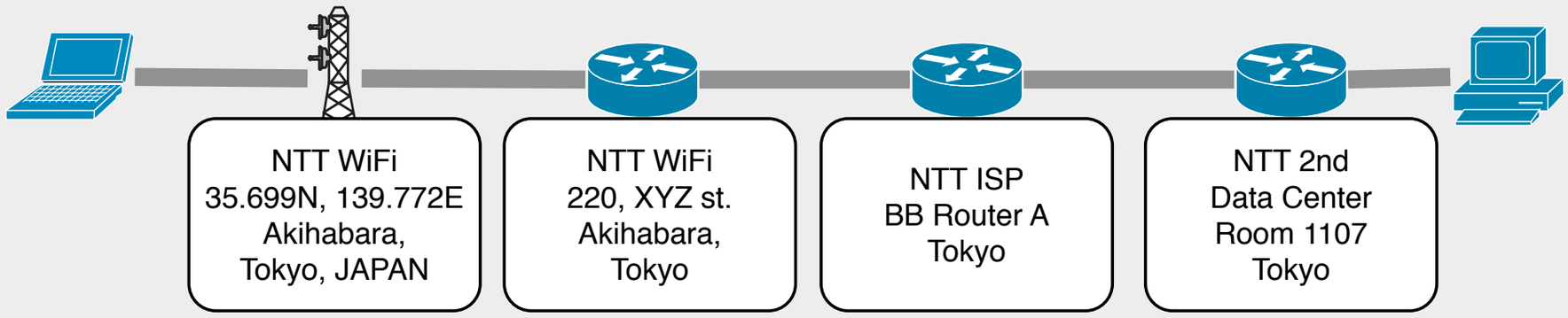
Requirements for improving visibility

- ✓ Scalability:
  - ✓ bandwidth, inter-domain, number of routers, flows
- ✓ No delay:
- ✓ Unnecessary complicated process:
  - ✓ e.g., not to rebuild path
- Disclosure policy among all stakeholders:
  - ISPs, end-hosts

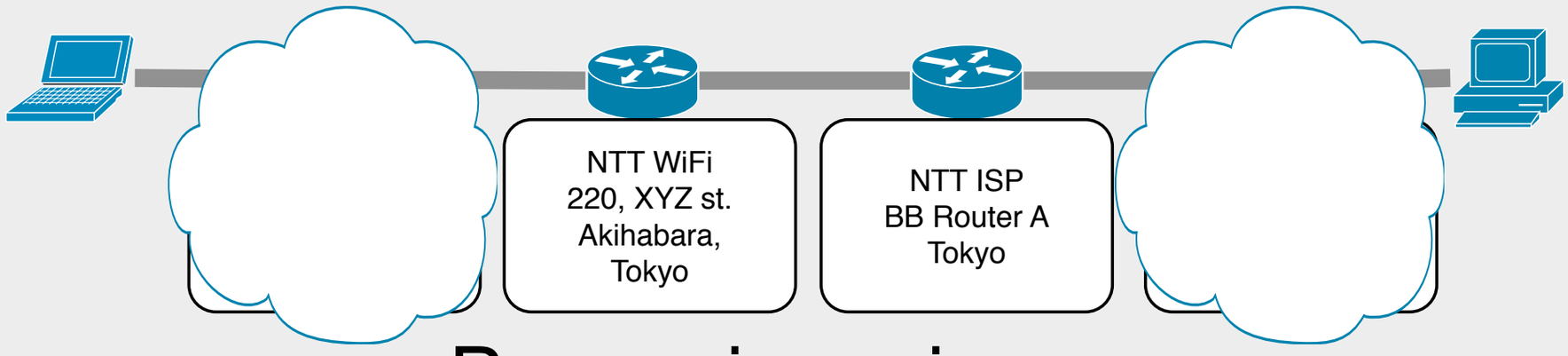
Preserving privacy



end-to-end Internet



Transparency with i-Path

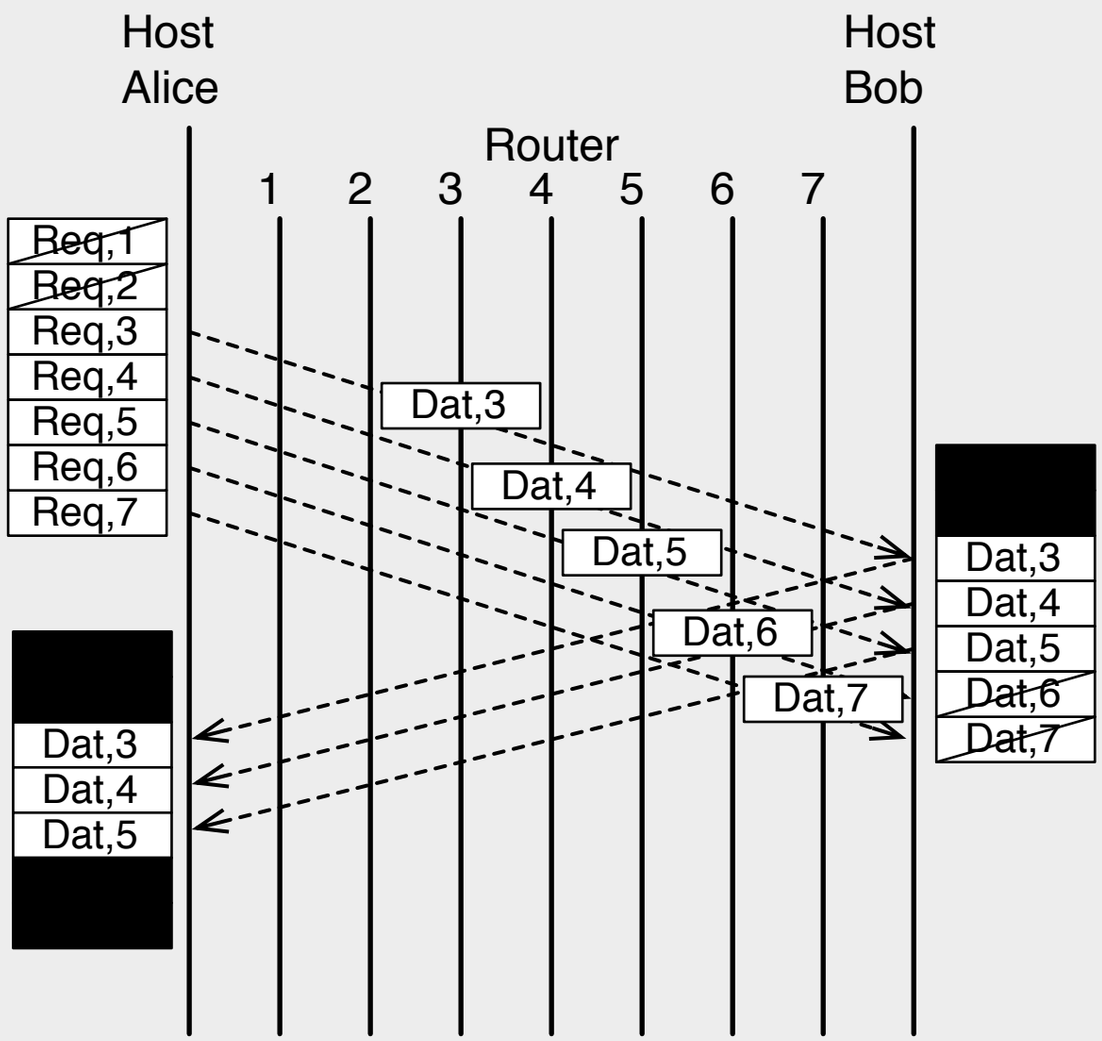


Preserving privacy

Selective disclosure on i-Path

- Allow access only when ISPs and end-hosts agree.
- ISP's policy
  - Simply applying ACL
- end-host's policy
  - end-host designates routers to allow access.
  1. selective request and response
  2. selective OTP disclosure

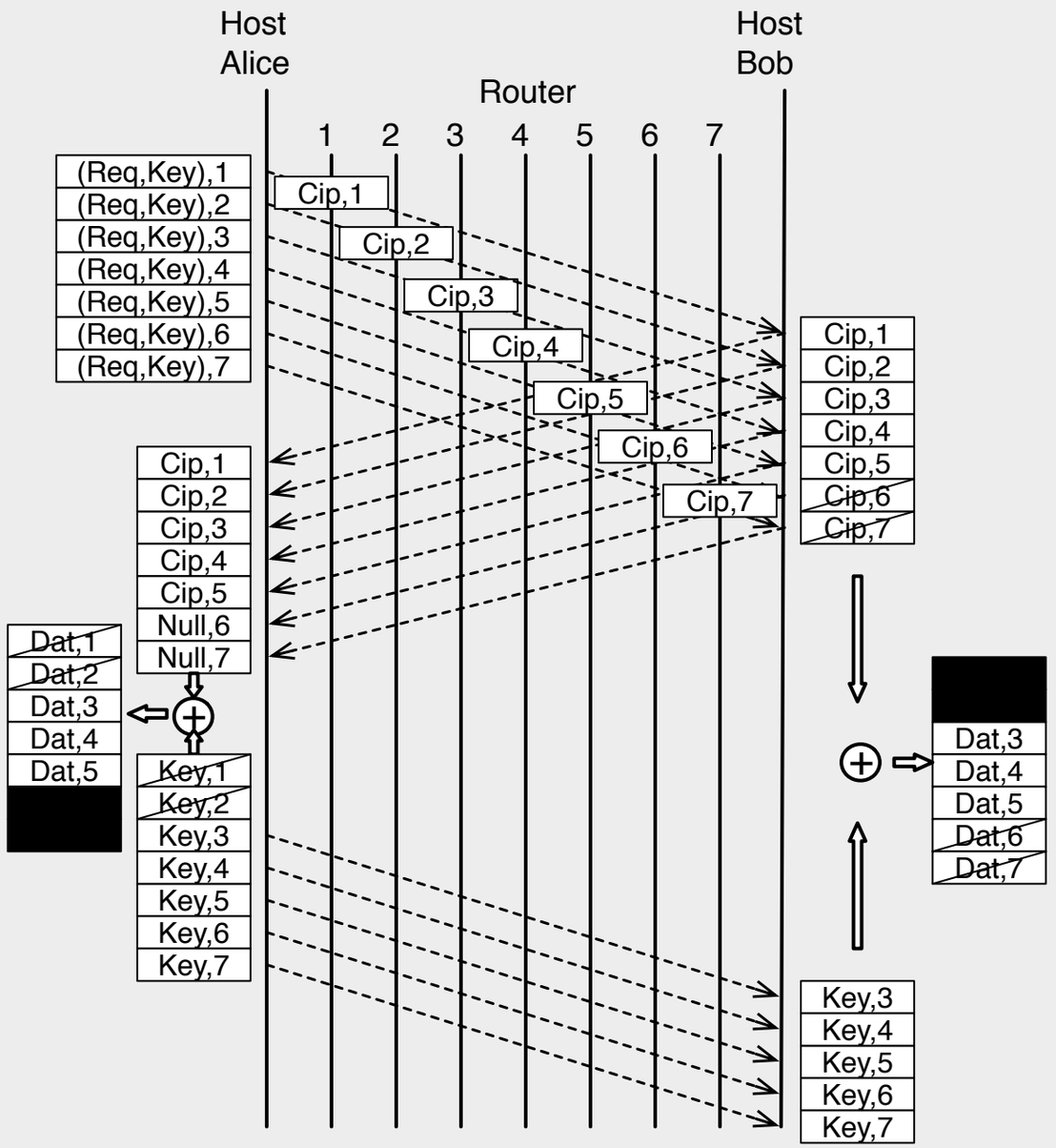
1. Selective req. and res.



Host side function only.

Not to work on asymmetric path.

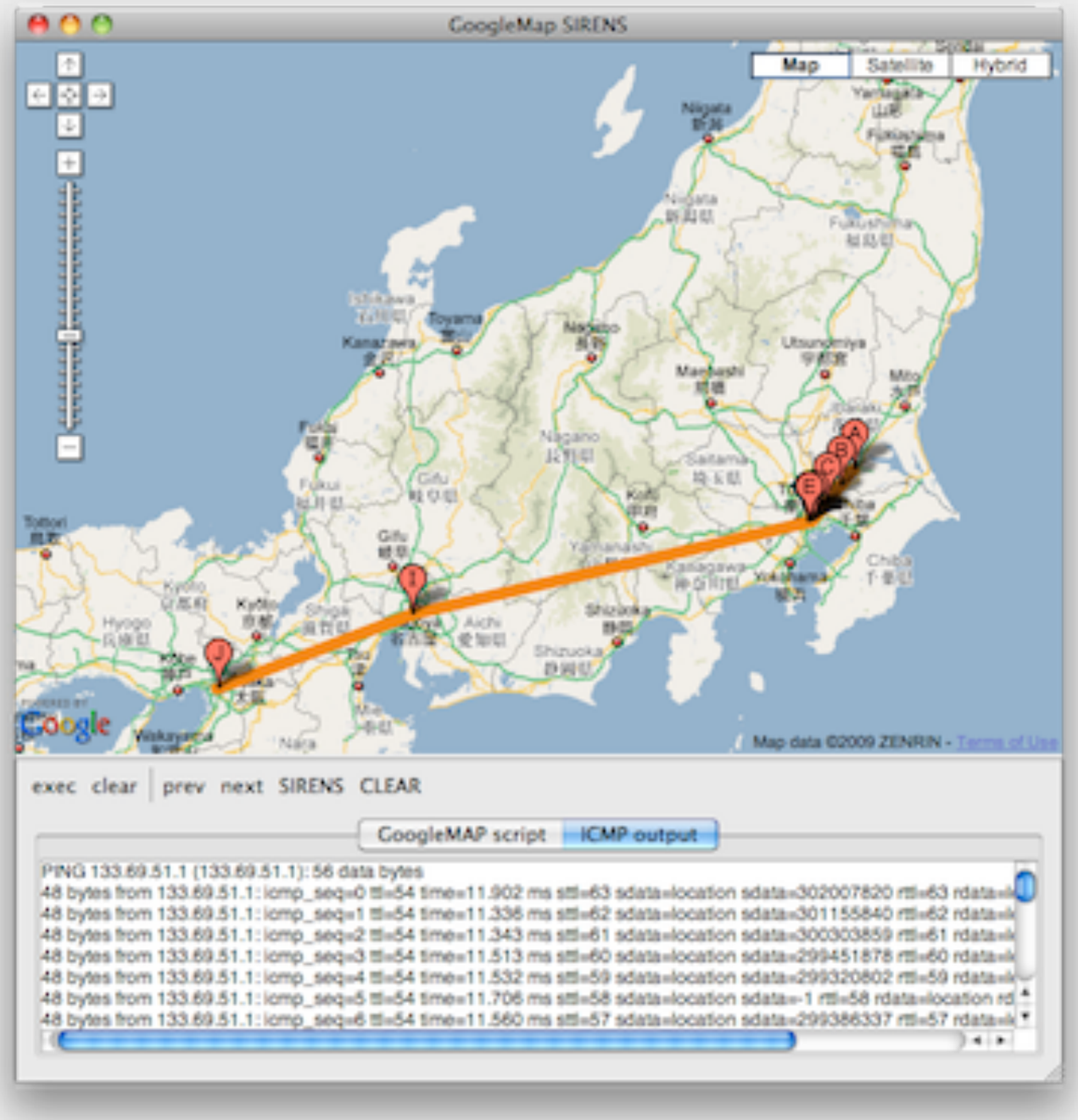
2. Selective OTP disclosure



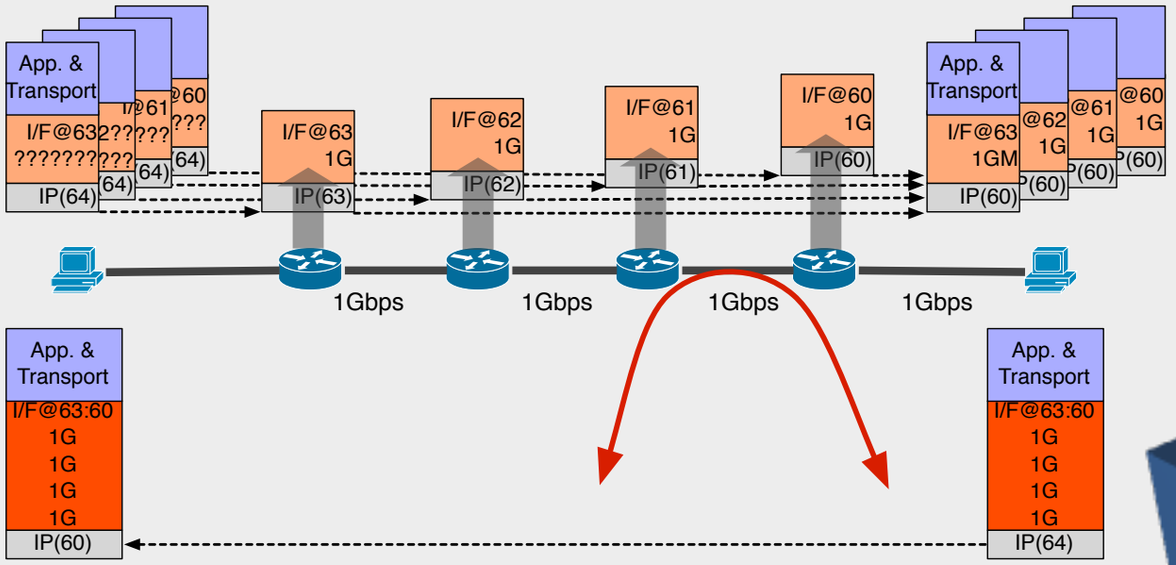
i-Path: Implementation and deployment

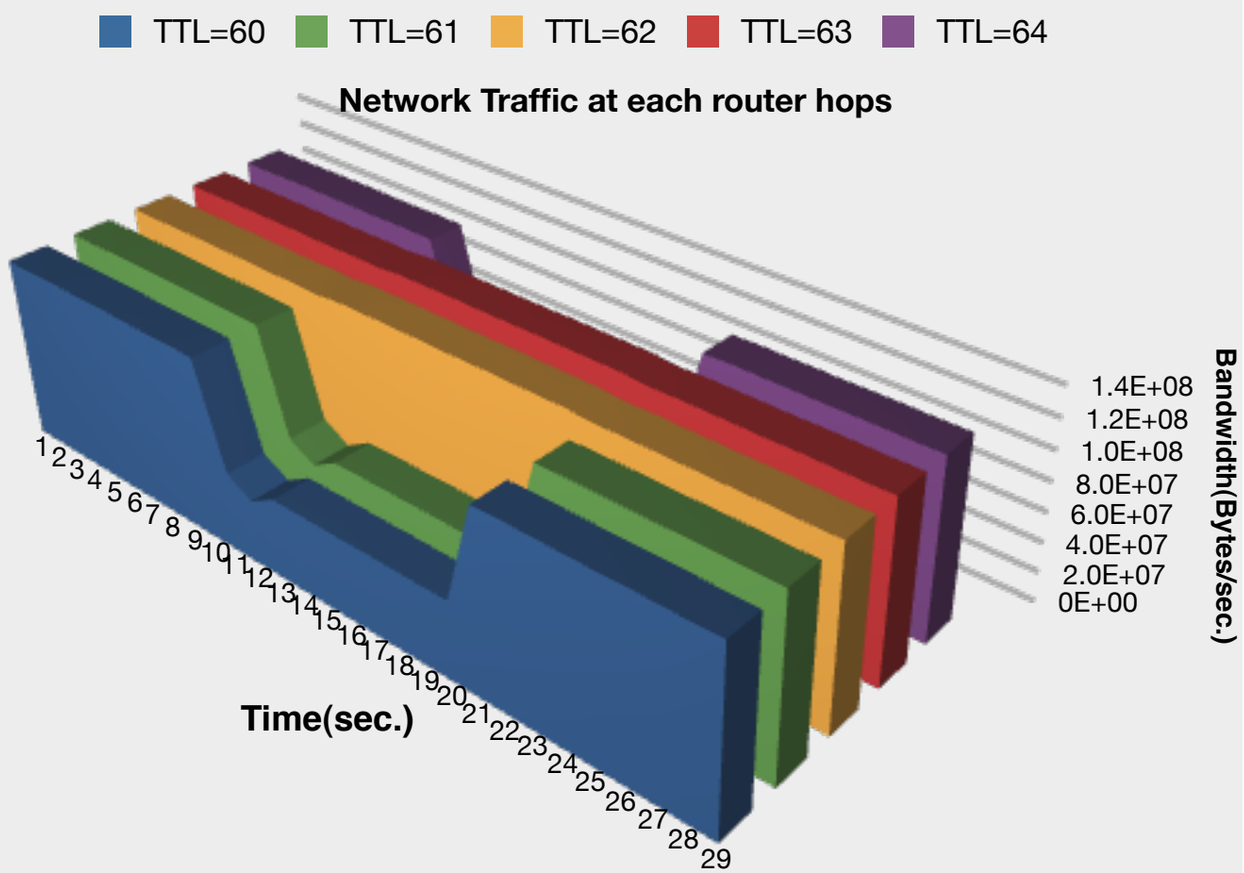
- Implementation:
  - i-Path router, host and socket API
    - FreeBSD as kernel patch
    - MacOS X as network kernel extension
      - URL: http://i-path.goto.info.waseda.ac.jp/trac/i-Path/
    - Linux as kernel module, incl. Android.
    - Socket API C, C++, Python, Java (JNI)
- Deployment:
  - R&D testbed in Japan

i-Path: Geo-trace



i-Path: monitoring BW consumption on intermediate links





Conclusion

- i-path explores to realize end host getting underlying info. with in-band cross-layer approach.
  - in-band cross-layer approach enhancing transport have not deployed yet.
  - idea application utilizes cross-layer approach.
- Is I-path on research stage ?