

Better End-to-End Visibility Leads Better Networks

Katsushi Kobayashi
ikob@ni.aist.go.jp
AIST, JAPAN

NATIONAL INSTITUTE OF ADVANCED SCIENCE AND TECHNOLOGY (AIST)
Copyright (C) 2008, Katsushi Kobayashi. All rights reserved.

1

Agenda

- Visibility inside Internet
- in-band cross layer approaches
 - ENCAP
- Selective disclosure on ENCAP
- Conclusion

Visibility inside Internet

- No visibility mechanism, i.e., end-to-end principle
 - 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 by control plane.

Related works

- Central server gathers information.
 - Passive, Active measurement, NMS
 - operator centric, poor scalability, server / domain, access control, necessary to re-build real network path
- end-to-end measurement
 - Bandwidth bottleneck estimation by transport stack.
 - End host cannot access information inside network directly,
 - Observe packet behavior between end-to-end path
 - loss, RTT jitter, re-order, packet-train, ...

Infrastructure of End-to-end is really dumb ?

- Router maintains many information
 - For routing and forwarding
 - routing prefix, prefix age, link bandwidth, available bandwidth, i/f queue, corruption loss, congestion loss, L2 address, signal strength, retransmission counter...
 - For operation
 - uptime, location, temperature, time zone, i/f description, CPU load, operator's contact....
- Huge number of MIB are already implemented
 - Usually deny SNMP access from end-user.

Better visibility brings what ?

- Enhancing transport performance
- 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 node location

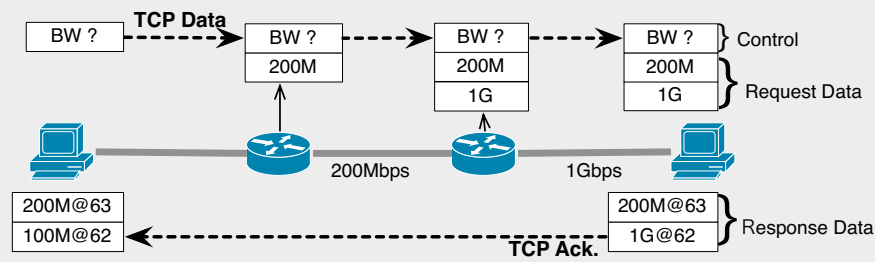
Requirements for improving visibility

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

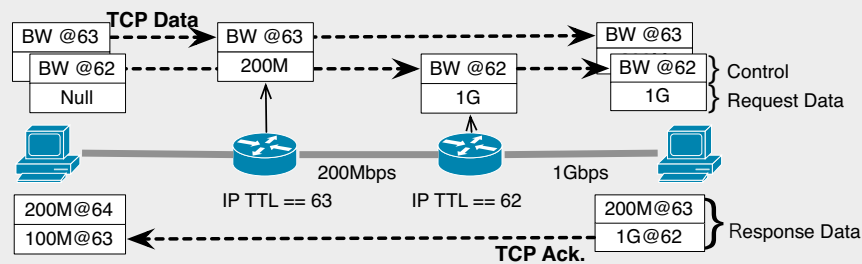
in-band cross-layer approaches - for enhancing transport-

- 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.
- ➔ENCAP
 - “Explicit Network information Collection Along Path”
- Congestion control with more network support
 - XCP, TCP-QS

PTP and SIRENS



PTP: retrieve all data by single packet with header growth

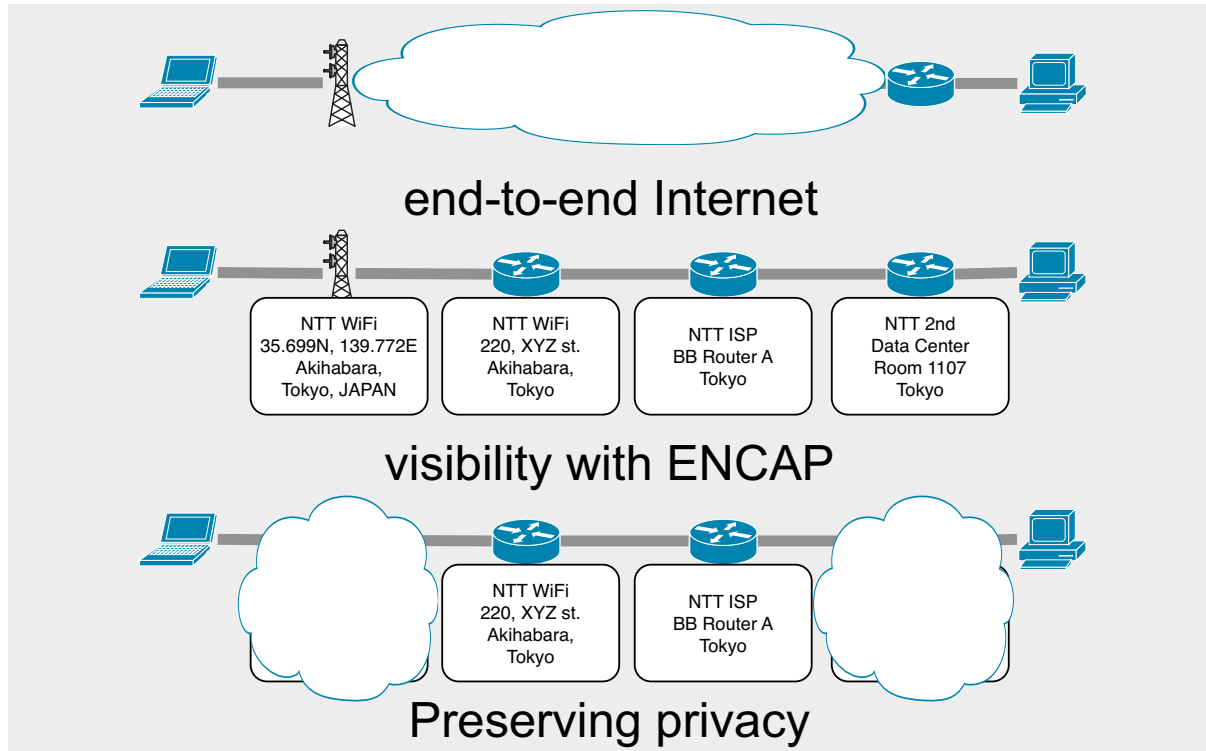


SIRENS: one packet collects one router's data

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

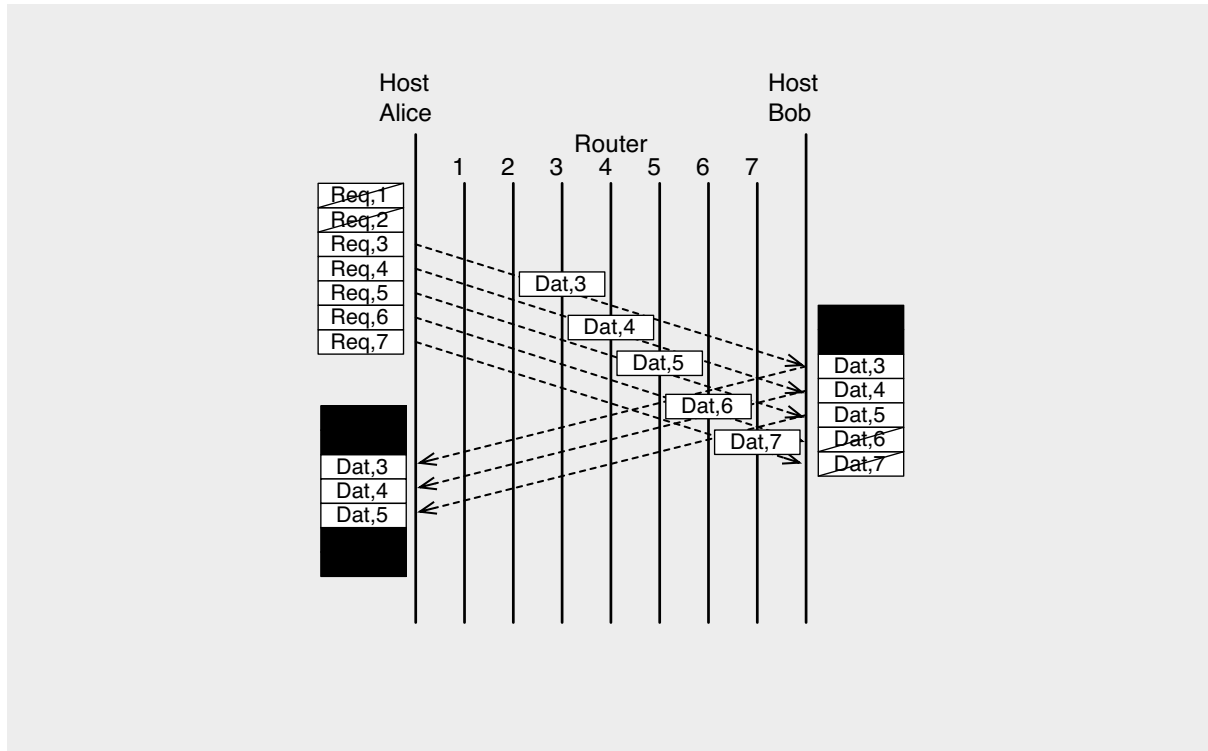
Preserving privacy



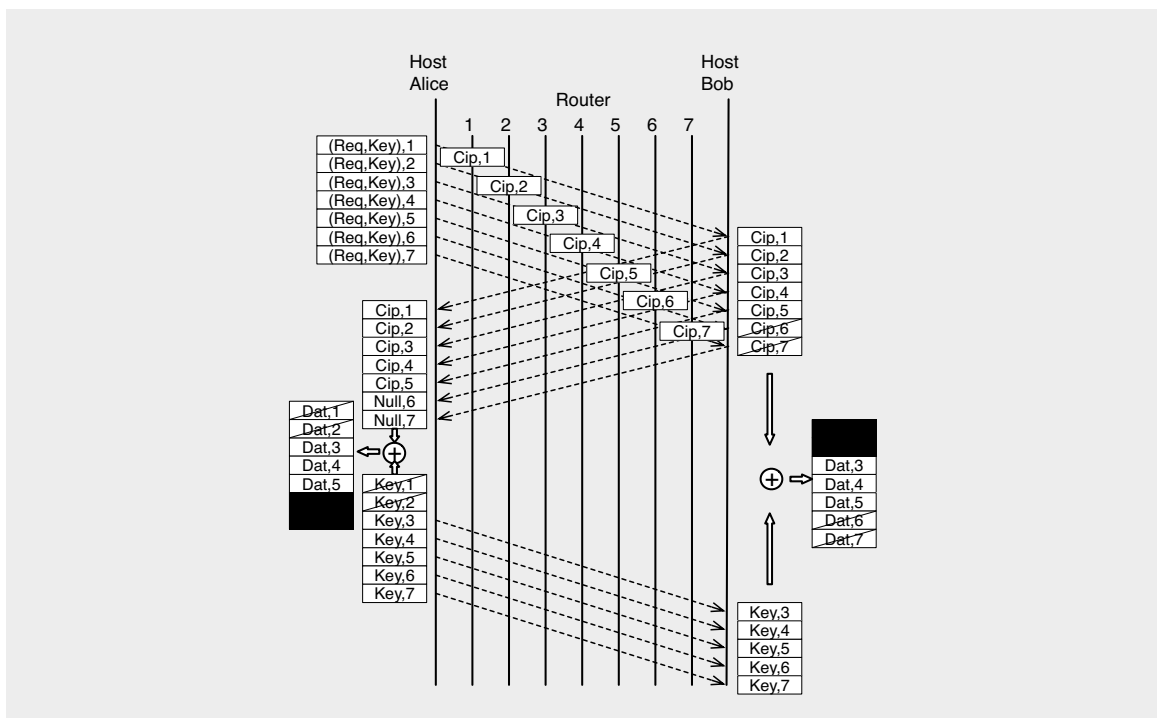
Selective disclosure on ENCAP

- 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.



2. Selective OTP disclosure



Implementation / Deploy testbed

- Router:
 - Just interpret “shim” layer
- End host:
 - API design,
 - Application to demonstrate
 - e.g., better peer selection in P2P
- Testbed: to deploy a virtual network slice on testbed.
 - VM slice is required.

Conclusion

- ENCAP improves visibility from end-host.
 - Not only for transport acceleration
 - Obtain any information maintained by router.
- Selective disclosure mechanism.
- A step toward to “knowledge plane” ?
 - “sensor” for end-host.
 - Not provide “sensor” for network and “actuator”