

Content-Oriented Networking Architecture (CONA): Principles, Operations, and Issues

Ted "Taekyoung" Kwon
Seoul National University

(Visiting Professor at Rutgers University)

My View on Future Internet

- IP address redefinition
- Security measure enforcement

What is an IP address?

0	4	8	16	19	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time To Live	Protocol		Header Checksum		
Source IP Address					
Destination IP Address					
Options					Padding

IP address

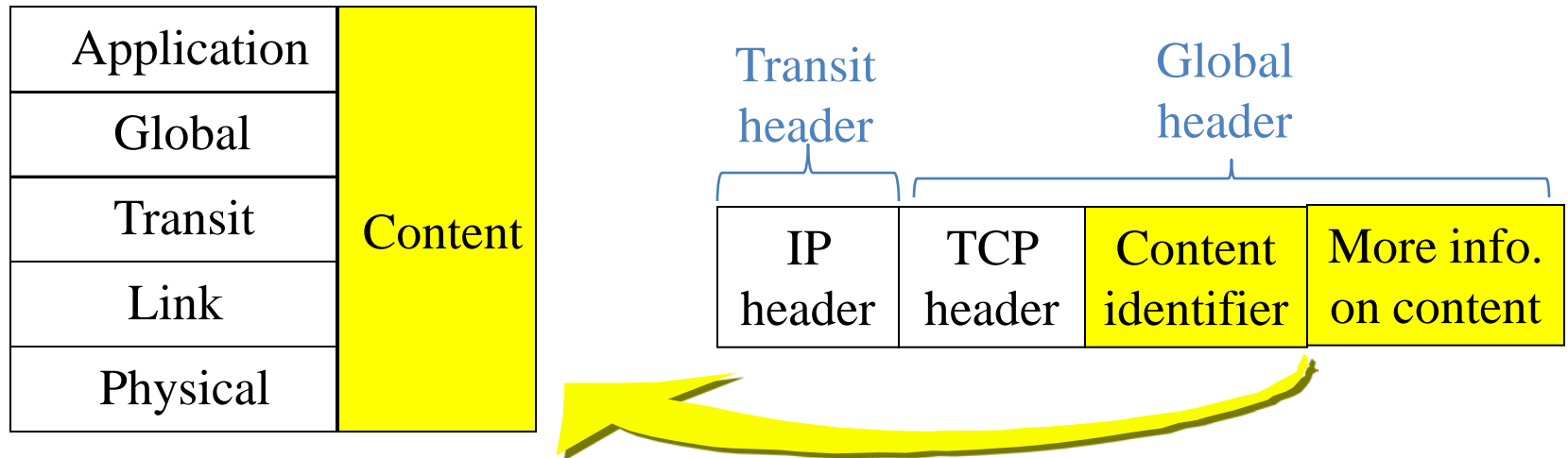
- An IP address originally indicates the endpoint
 - End-to-end principle
 - Fundamental communication model is point-to-point conversation between two hosts
 - Serves as both locator and identifier
- Current role of IP address
 - Not endpoint
 - NAT, tunneling, overlay,...
 - Not identifier
 - Mobility, multi-homing,...

Then what should be an IP address?

- Just locator
 - Not identifier
- Locator of next transit point
 - NAT, tunneling,...
 - Some agents
 - E.g. mobility agent in mobile IP solutions
- Transit-by-transit
 - Not end-to-end

Then where is the endpoint identifier?

How about Content identifier (CID)?



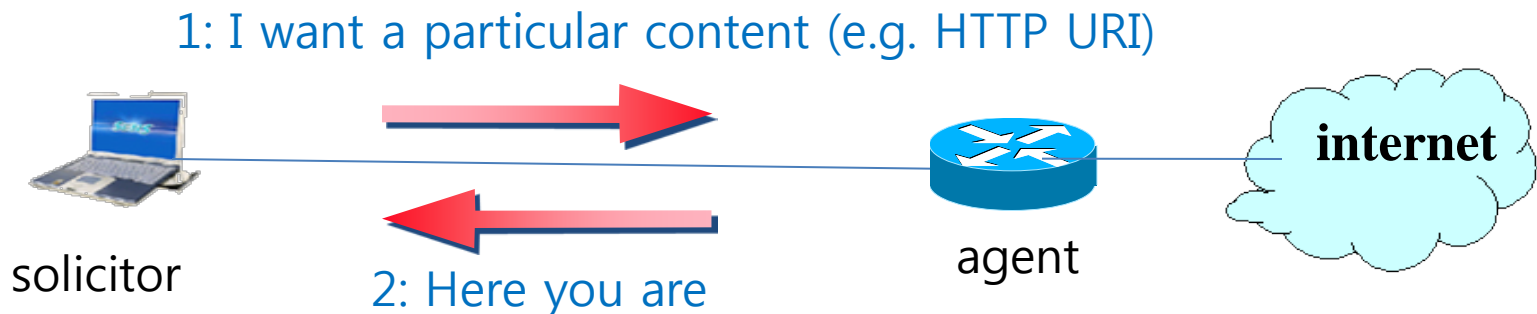
- Globally routable
- Unique
- Domain name (or public IP address) + port number
 - E.g. <http://www.nytimes.com>
 - Path info. can be added

Internet security is a big threat

- The key problem is that
 - Anyone can send any packet to anyone
 - E.g. DDoS
- New service paradigm of ISPs
 - Not deliver packets
 - But deliver contents

Content-oriented network architecture (CONA)

- Traffic is already content-oriented
 - CDN, multimedia, P2P...
- New model for IP subnet:
 - solicitor vs. agent
 - An access router becomes an agent
 - An agent contacts DNS
 - Solicitors cannot
 - solicitor doesn't know destination IP address



Intra-domain

- Publisher or server
 - Sets up connectivity with its agent
 - Registers its domain name with the DNS
 - Agent's IP address (of the egress link)
- Agent of the publisher will receive the content from the publisher
 - relay the content to the agent of the host over



Policing at agent

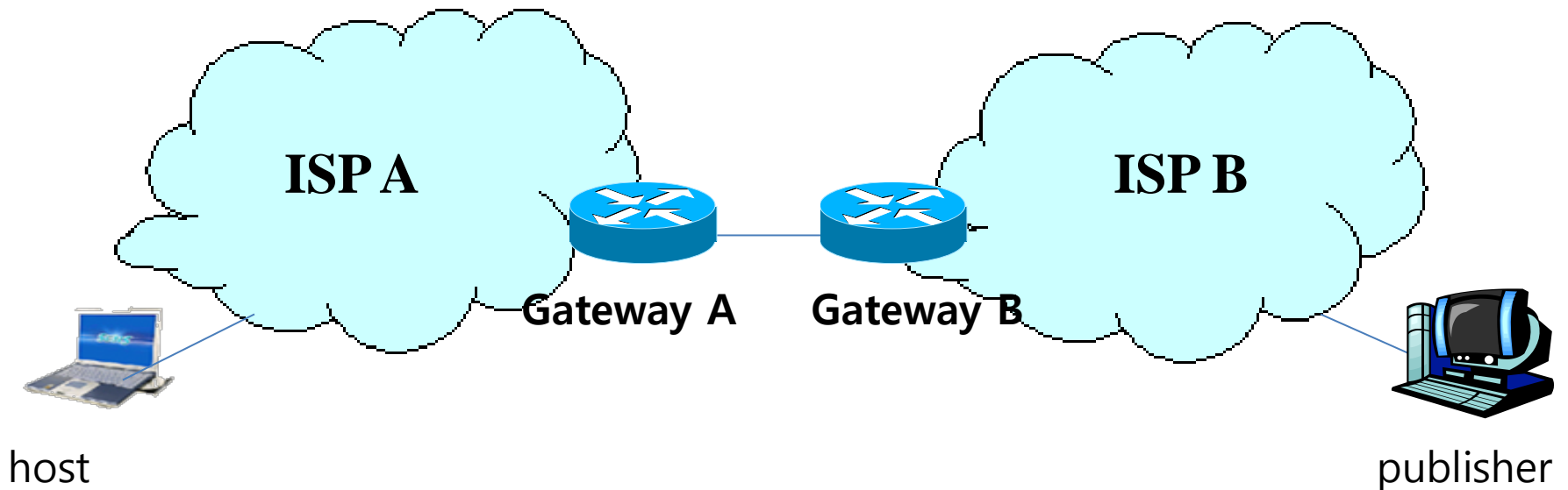
- Agent can perform proactive measures
 - To help prevent DDOS attack
 - E.g. solicitors cannot generate too many requests
 - Especially to the same server
- Agent will analyze the behaviors of its solicitors
 - Contents requests by solicitors are accountable
 - Agents can collaborate

Other merits of agents

- Flash crowd can be dealt with by caching contents at agents
 - Agents may form some overlay for additional content delivery gain
- Agent failure may not matter
 - Content identifier always directs the correct endpoint

What about between different ISPs?

- Gateways also exchange content request message and the corresponding content data
 - So they are accountable



CONA operations: Content Request Message

1. H1 sends a content request message to A1, its src:dst is H1:A1
(the content C_{H2} belongs to H2)
2. A1 makes a CIB entry ($C_{H2}, H1$) to deliver content data
3. The content request message now has A1:A2 as src:dst IP addresses
4. C1 makes a CIB entry ($C_{H2}, A1$) to deliver content data
-

src	dst
-----	-----

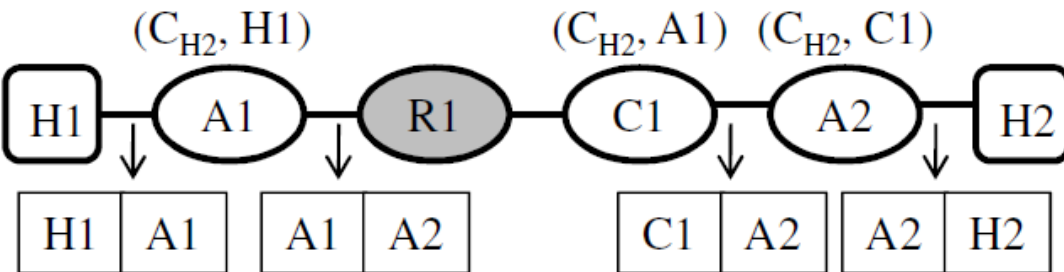
 source & destination addresses in transit header of a content request message

(content ID, next hop) CIB entry to forward contents

○ content-aware router/agent

● legacy router

□ end host



- As content request message traverses, a content info base (CIB) entry is set up backwards

CONA: advantages

- End hosts behind NATs are now first class citizens
 - Private addresses are fine
 - Mitigates issues of IP address exhaustion and routing scalability
- Ready to interwork with long disruption or delay networks
 - DTN, CNF, sensor, MANET
- Security, accountability are enhanced
- Mobility and multicast are better handled

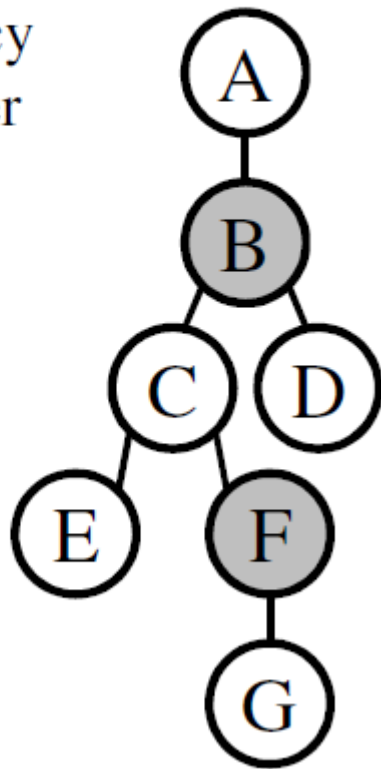
Mobility in CONA

- The serving agent will take care of L2 handoff
- If a host moves to a new agent,
 - Host detects content delivery failure
 - It sends a new content request message
 - The new agent will continue the flow by relaying content request message toward the publisher

Multicast in CONA

○ content-aware
router/agent

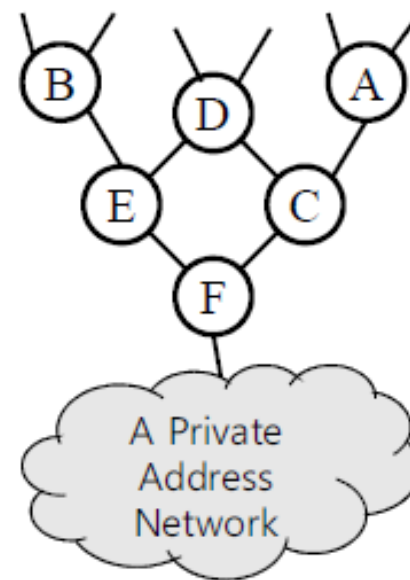
● legacy
router



- E,G,D are agents of three multicast recipients
- First E joins
 - C has (C_A, E) , A has (C_A, C)
- G joins
 - C has $(C_A, E$ and $G)$
- D joins
 - A has $(C_A, C$ and $D)$

Some issues

- Inter-domain performance
- Scalability (of solicitors)
- Scalability (of contents delivery service)
 - NetFPGA router
- Agent compromise



Questions?

Local connectivity

- New communication model for subnet:
 - Host vs. agent
 - Agent
 - Agent advertisement (AA) messages
 - Host
 - Receive AA message
 - Private address (IPv4) and link local address (IPv6)
 - No need to know destination address
 - Cannot contact DNS
 - Assume security association (SA) is set up

At the other end

- publisher side
 - Agent registers with DNS

* Assume that publication is done

