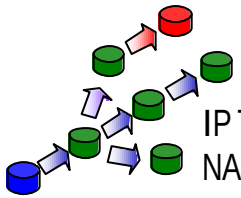
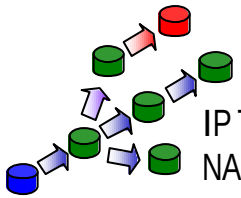


IP TRACEBACK TEAM
NAIST, JAPAN

An implementation of hierarchical IP traceback architecture

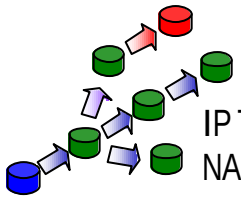
Masafumi OE <masa@fumi.org>
Youki Kadobayashi
Suguru Yamaguchi
Nara Institute Science and Technology, JAPAN

http://iplab.aist-nara.ac.jp/research/itrace/



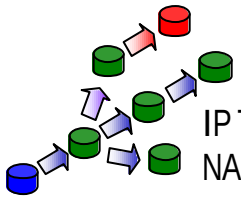
Agenda

1. Introduction
2. Proposal
3. Implementation
4. Conclusion and Future work



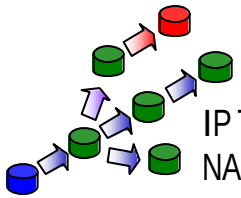
IP TRACEBACK TEAM
NAIST, JAPAN

1. Introduction



Introduction

- Distributed Denial of Service (DDoS)
  - It is one of the threats on the Internet.
  - A large number of packets are sent to the victim's node.
    - Internet services (e.g. WWW, SMTP, etc) are going down.
    - The source address of the DDoS IP packet attack is spoofed to a random address.
- Difficulty of tracing the DDoS flow
  - IP routing is destination address based routing.
  - Spoofed source addresses makes difficult trace.
- IP traceback
  - Trace attack packets and Identify attack nodes and attack paths.

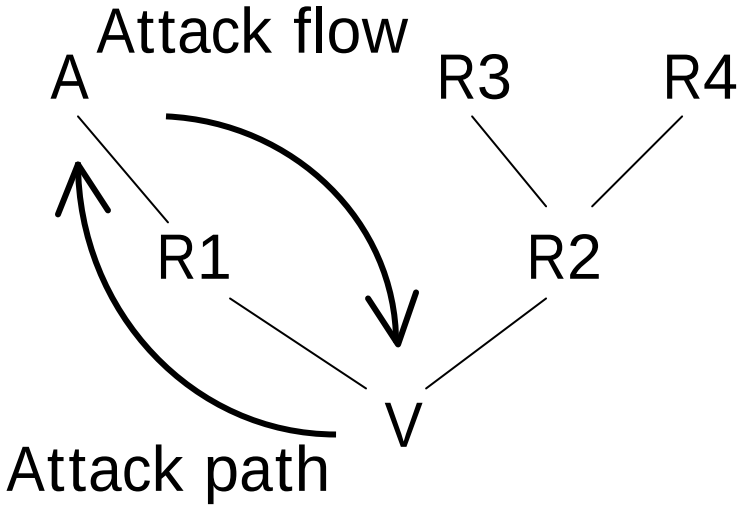


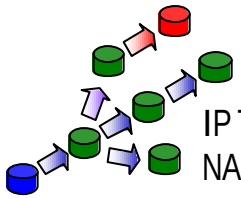
IP TRACEBACK TEAM
NAIST, JAPAN

Terminology

- Attack node
  - located on the Internet.
  - send attack packets.
- Victim node
  - is a target node for DDoS attack.
- Attack flow
  - is the flow of attack packets from attack node to victim node.
- Attack path
  - is the path of attack packets.

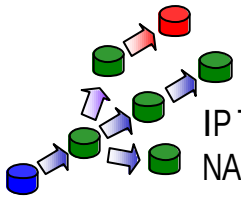
A: Attack node
V: Victim node
Rx: Router





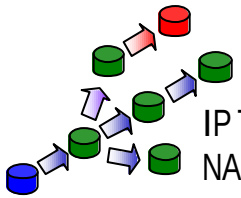
IP traceback

- Identifies attack nodes and attack paths.
- Related work
  - Link testing method
    - This method specifies the IP address of a router that forwards the attack flow by the filtering function and the monitoring function in the router.
  - Hash based method
    - Every router logs all transmission packets into storage with a hash function for compression of data.
  - Passive detection method
    - Every router sends the passive detection packet which is including the router's information, that is, IP address, MAC address, next hop router's IP address and so on.



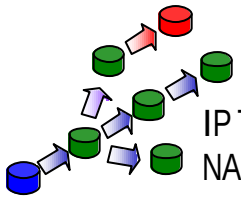
Issues on related works(1/2)

- Organizations connected with the Internet as Autonomous System (AS)
  - The management and operation are independent for each AS.
  - It needs a large amount of time to cooperate between ASes for IP traceback operation.
- Develop a counter meager for IP traceback
  - The attacker finds the weak points of current IP traceback methods and develop anti-IP traceback attacks.
  - IP traceback should be flexibil system.



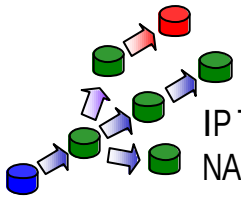
Issues on related works(2/2)

- They are not victim protection technology.
  - Purpose is finding out “perfect attack path”.
  - The damage easing at the victim node is more important than the finding out attackers.



2. Proposal

Hierarchical IP traceback architecture

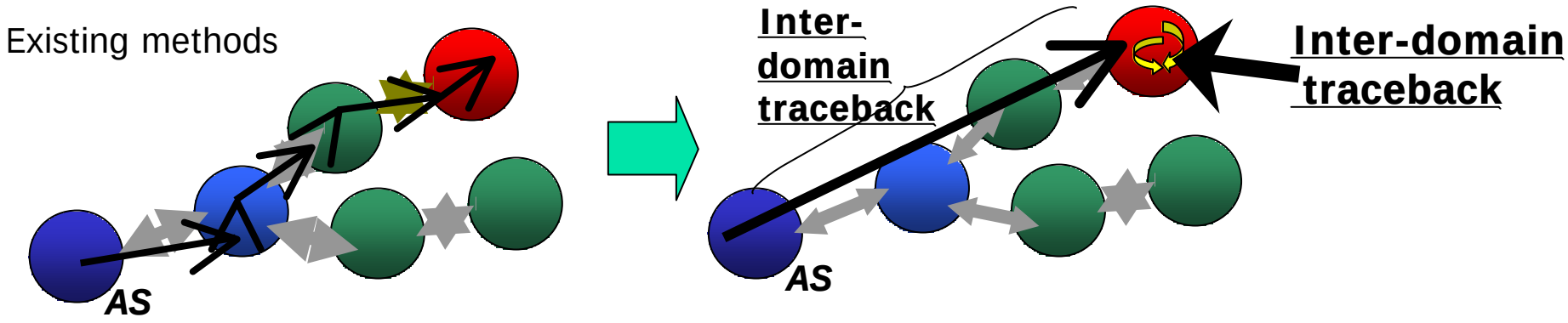


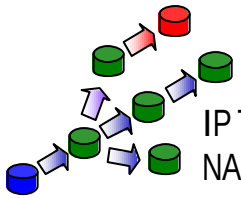
Our Proposal(1/2)

- We propose *hierarchical IP traceback architecture*.
  - It is applied the routing architecture to the traceback mechanism.
    - The routing system is a hierarchy of EGP (Exterior Gateway Protocol) and IGP (Interior Gateway Protocol) according to the scale of the network.

Our Proposal(2/2)

- It decomposes the Internet-wide traceback procedure into inter-domain traceback and intra-domain traceback.



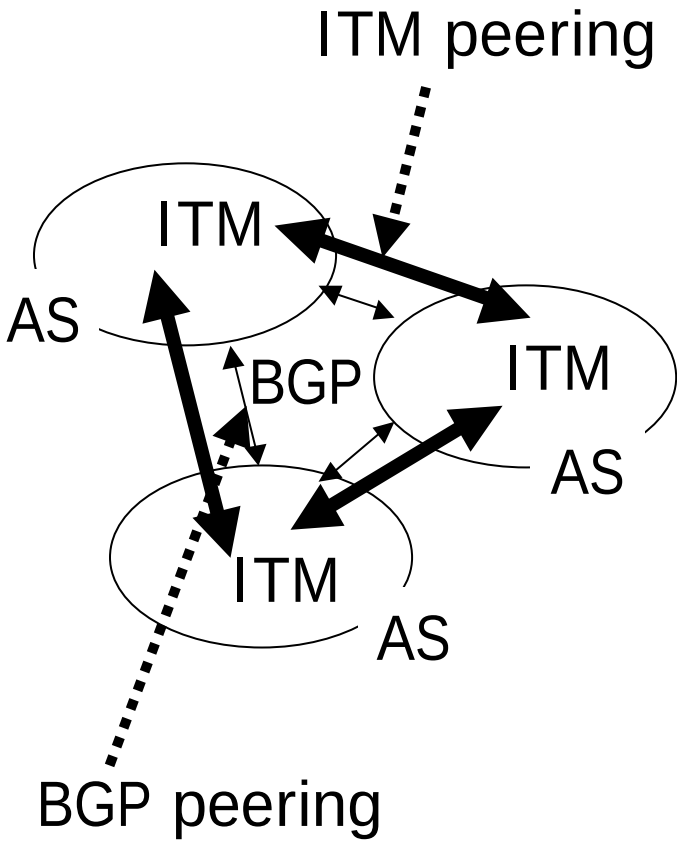


Hierarchical IP traceback architecture

- The proposed architecture has three components:
  - IP traceback manager (ITM):
    - It is used for the association of eIP and iIP traceback.
  - eIP traceback: inter-domain traceback
    - Find each AS that the attack flow passed.
  - iIP traceback: intra-domain traceback
    - Find the router's IP address that the attack flow has passed within the AS.

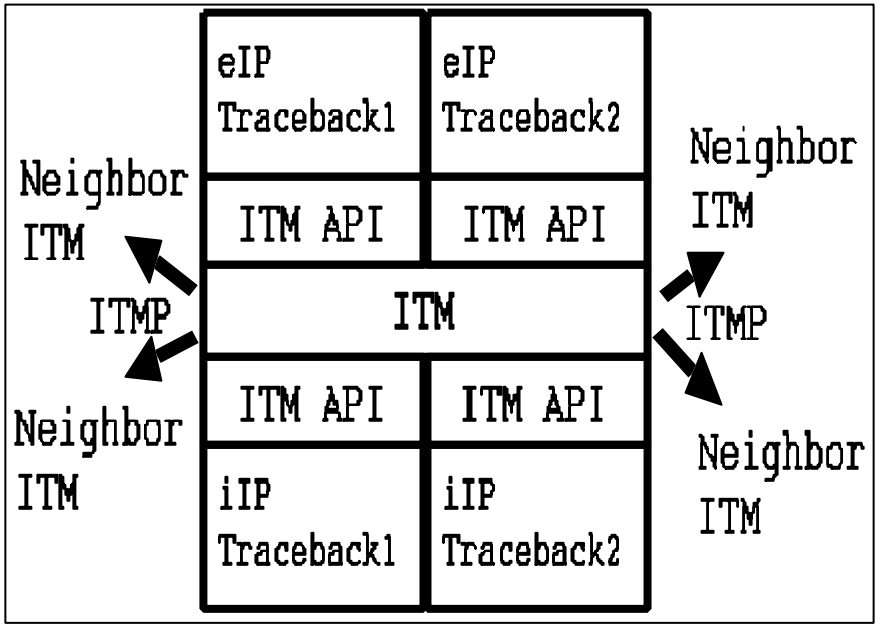
ITM

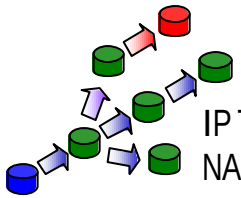
- Purpose
  - Exchange IP traceback information between eIP and iIP traceback with ITM network.
    - Dump of the attack packet
    - Result of IP traceback.
    - Etc..
- Feature
  - I/O definition of IP traceback information by ITM-API
  - ITM exists in each AS.
  - ITM network is constructed with a peering connection between ITMs as well as the peering of BGP



ITM API

- Used between ITM and eIP/iIP.
- We defined ITM API from the analysis of the existing implementations.
  - Information API
    - Used for exchanging status of ITM and e/iIP traceback module.
  - Data API
    - Used for exchanging data eIP/iIP traceback module on neighboring ITMs.
  - Traceback API
    - Used for requesting eIP/iIP traceback and replying the result.



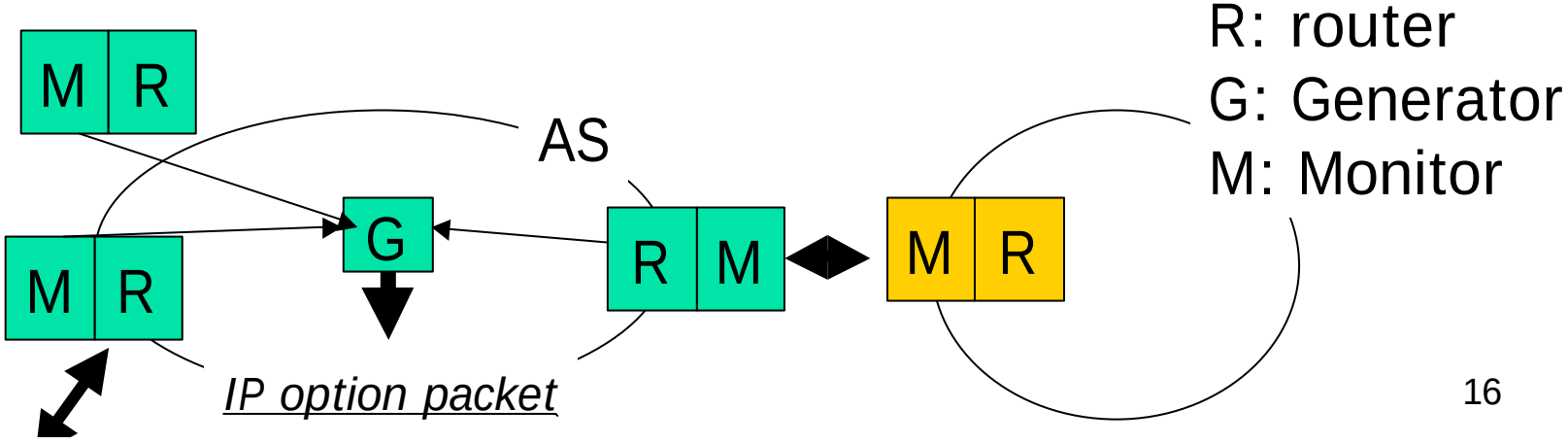


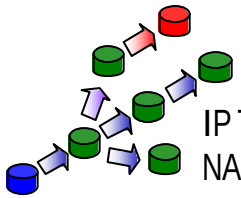
eIP traceback

- Purpose
  - eIP traceback detects ASes that the attack flow has passed in short time.
    =AS traceback
  - No existing AS traceback technique
- We propose “IP Option traceback.”
  - It is one proposal for eIP traceback (Inter-domain traceback).
  - This is based on “passive detection packet method” like iTrace packet in ICMP traceback which proposed by IETF-iTrace-WG.

IP Option traceback (1/2)

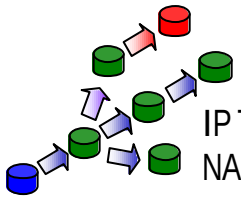
- Under regular operation
  - The Monitor pickup a packet with Probability “P” on router and send it to the Generator.
  - The Generator generates IP option packet including
    AS number(32bit)/timestamp(64bit)/etc.
    - IPv6: IP destination(2) option.
    - IPv4: IP option.





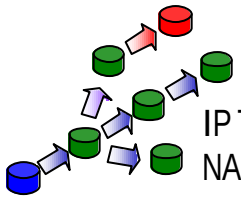
IP Option traceback (2/2)

- Under attacking condition
  - Gather IP Option packets on Victim node.
  - Construct AS attack path by analyzing these packets.



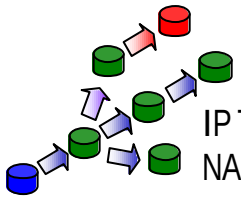
iIP Traceback

- Purpose
  - Specify the attack nodes and attack paths inside of AS.
- Feature
  - Use existing IP traceback method as iIP traceback with ITM API.
  - We are developing running code to use NP (network processor)-based IP traceback system .



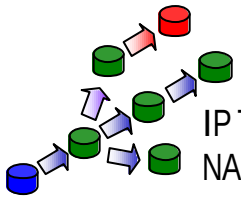
IP TRACEBACK TEAM
NAIST, JAPAN

3. Implementation



Implementation

- Our implementation
  - Platform: FreeBSD/NetBSD
  - Running code
    - IP option traceback (eIP)
    - ITM
    - iIP traceback (API)
  - Developing
    - iIP traceback

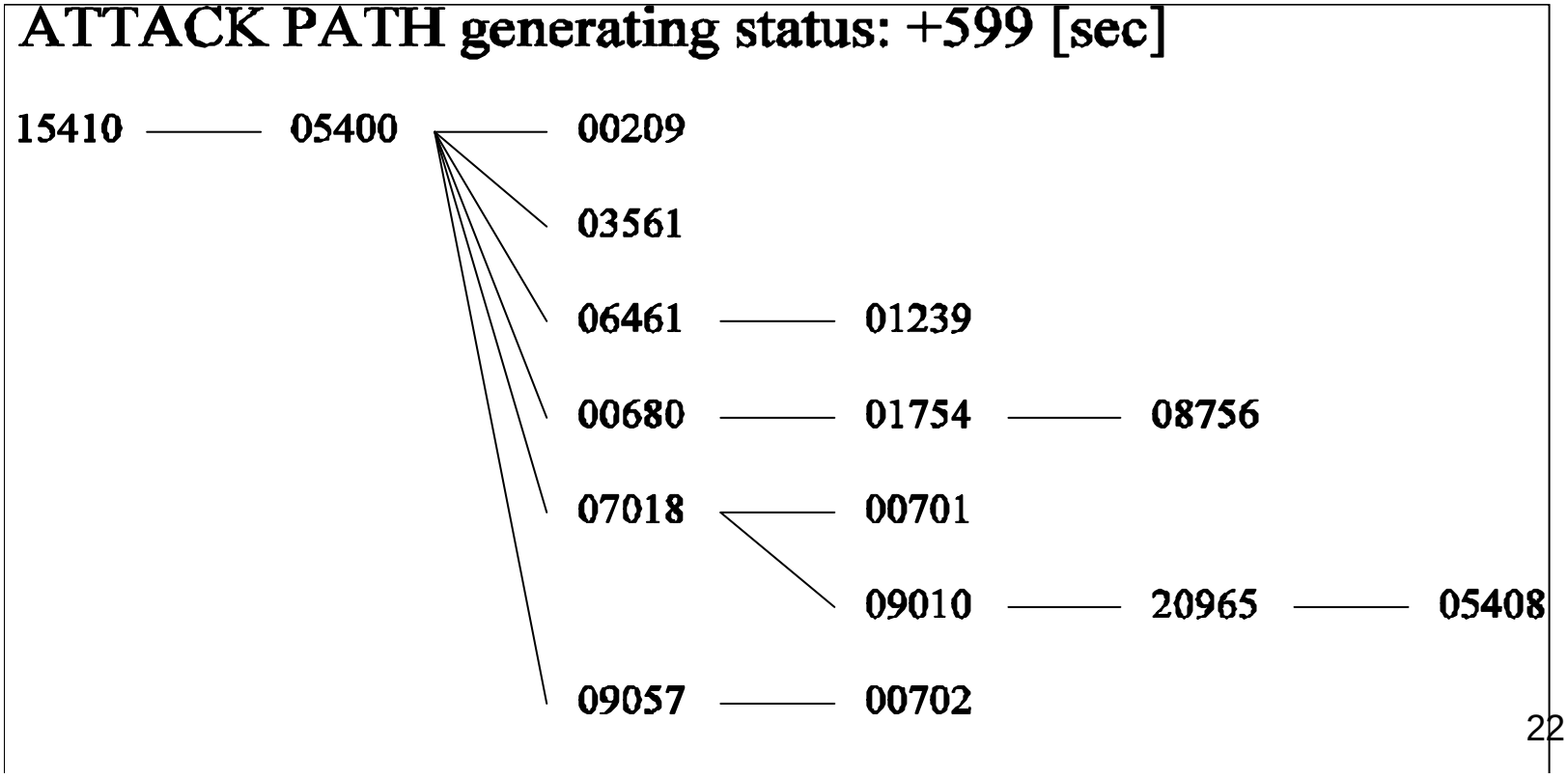


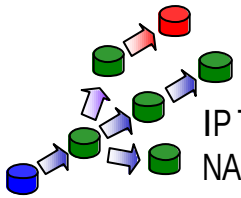
Evaluation

- Performance evaluation of IP option traceback.
- We carried out experiments on StarBED
  - StarBED has up to 500 nodes and is a fully programmable Internet simulator.
  - Used 64 nodes out of 500
- Construct top 50 ASes network on StarBED.
  - Create network map from RouteViews AS ranking.
    - Maintained by CAIDA and Univ. of Oregon.
  - All nodes were same spec and same OS.
    - FreeBSD4.7/zebra
  - 30 attack nodes was located on the network.
    - Attack flow was generated by mstream which is one of DDoS tools.

Results(1/2)

- Found out the attack path at 303[sec] passed



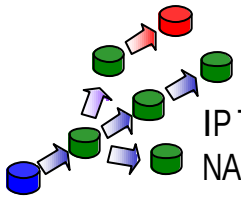


Results(2/2)

- Our impregnation found out attack paths

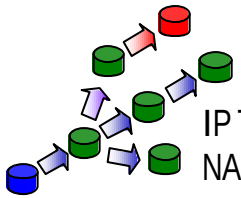
  Example:

  - Attack flow is 100PPS each attack node.
  - 9 attack nodes
  - Victim located in AS-15410.
  - Attack node at AS-5408 8756 20965 701 1239 3561 209 702 9010.
  - Found out the attack path at 303[sec] passed



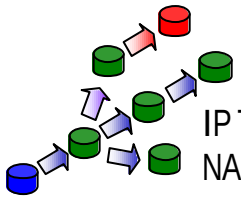
IP TRACEBACK TEAM
NAIST, JAPAN

4. Conclusion and Future work



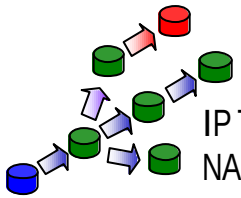
Conclusion

- It is difficult to use only one IP traceback mechanism for the Internet.
- “Hierarchical IP traceback architecture” solution.
  - Consist of eIP and iIP traceback like EGP and IGP.
- Implementation and evaluation has been done.
  - Successfully found out the source ASes of attack nodes.



Future work

- Evaluation
  - Under the condition over 100ASes at StarBED system.
- Technology transfer
  - Output to commercial product
    - We make joint research with YOKOGAWA ELECTRIC.
      - NAPPI: NP (Network Processor) based IP traceback system
      - We use it as iIP traceback.
  - Operate the system on real ISP.



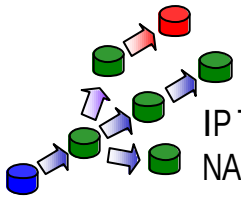
IP TRACEBACK TEAM
NAIST, JAPAN

Thank you

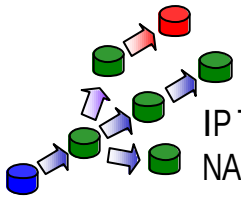
Contact Information

Mailing List
traceback@is.aist-nara.ac.jp

Web Page
http://iplab.aist-nara.ac.jp/research/itrace/



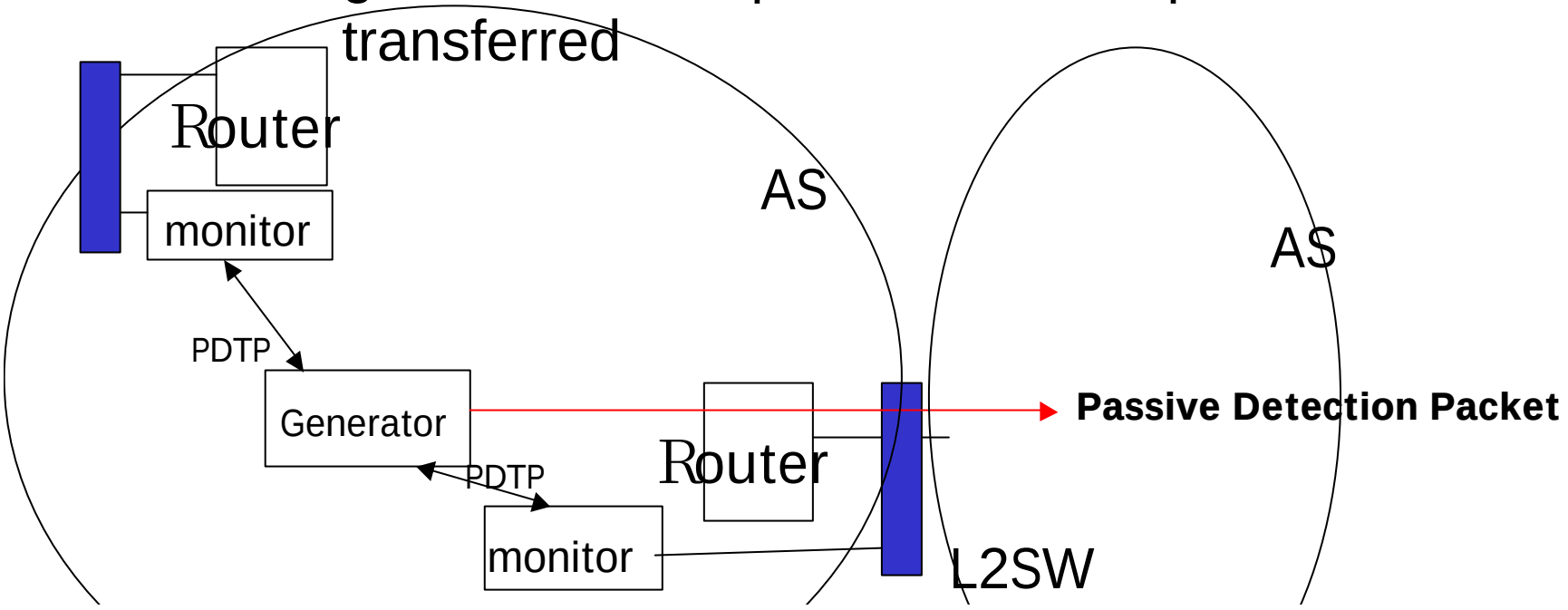
IP TRACEBACK TEAM
NAIST, JAPAN

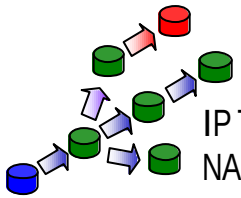


IP TRACEBACK TEAM
NAIST, JAPAN

Implementation(2)

- Monitor modules are connected to L2SW mirror port and it picks up a packet.
- Generator is located inside every AS.
  - generate Trace packet from the packet transferred





IP TRACEBACK TEAM
NAIST, JAPAN

Our Proposal(2/2)

- It decomposes the Internet-wide traceback procedure into inter-domain traceback and intra-domain traceback.