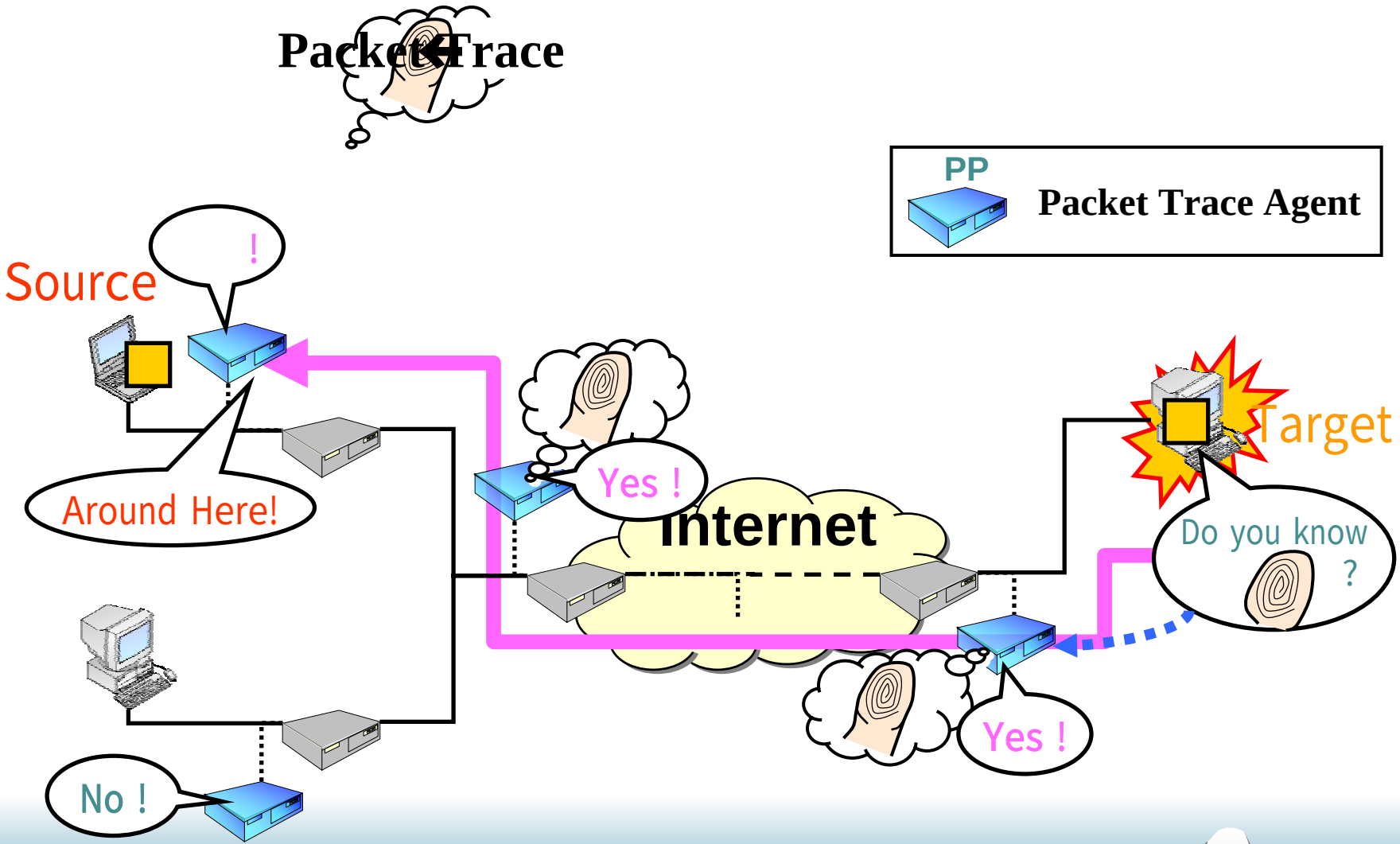
An Architecture for IPPT

Glenn Mansfield Keeni
Cyber Solutions Inc.

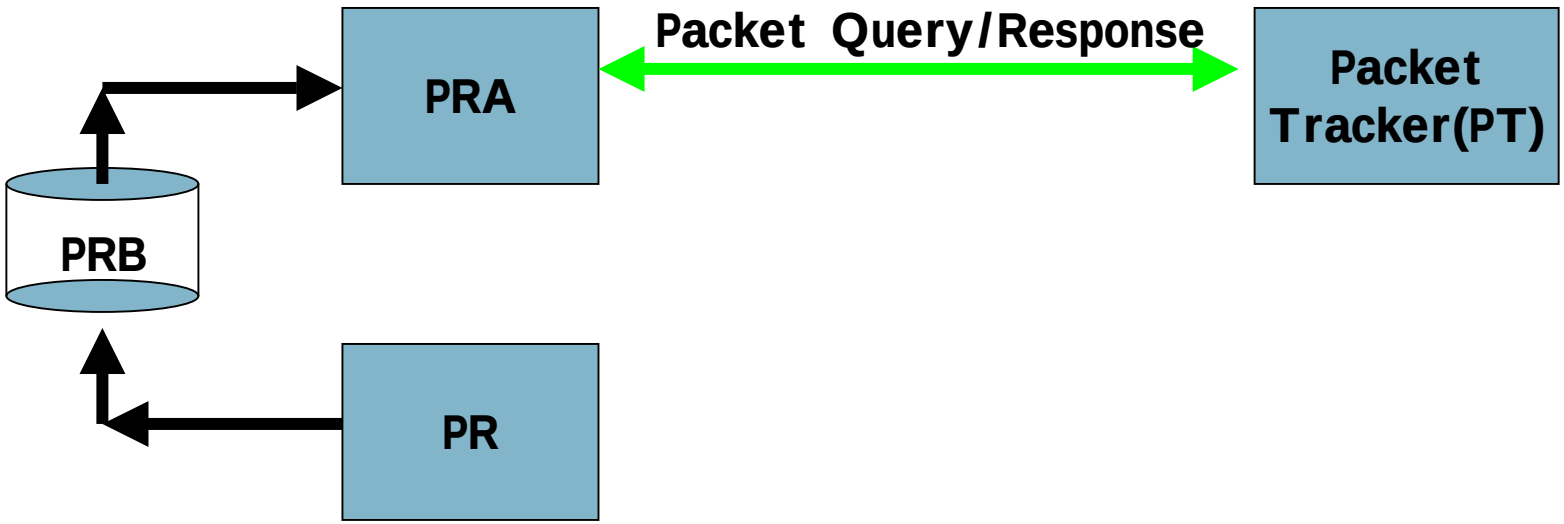
Yoshitaka Kuwata
NTT Data

Ippt-BOF, IETF-54

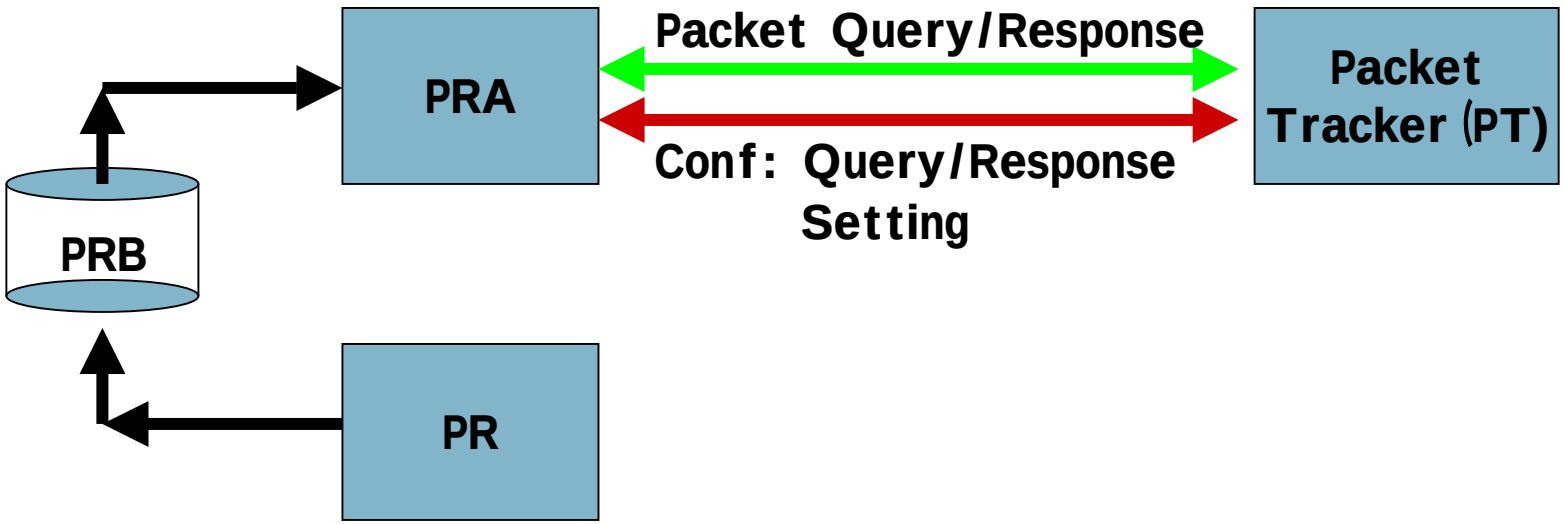
July, 2002


Packet Trace
PP
Packet Trace Agent
Source
!
Around Here!
Yes !
Internet
Target
Do you know
?
Yes !
No !

The Architecture



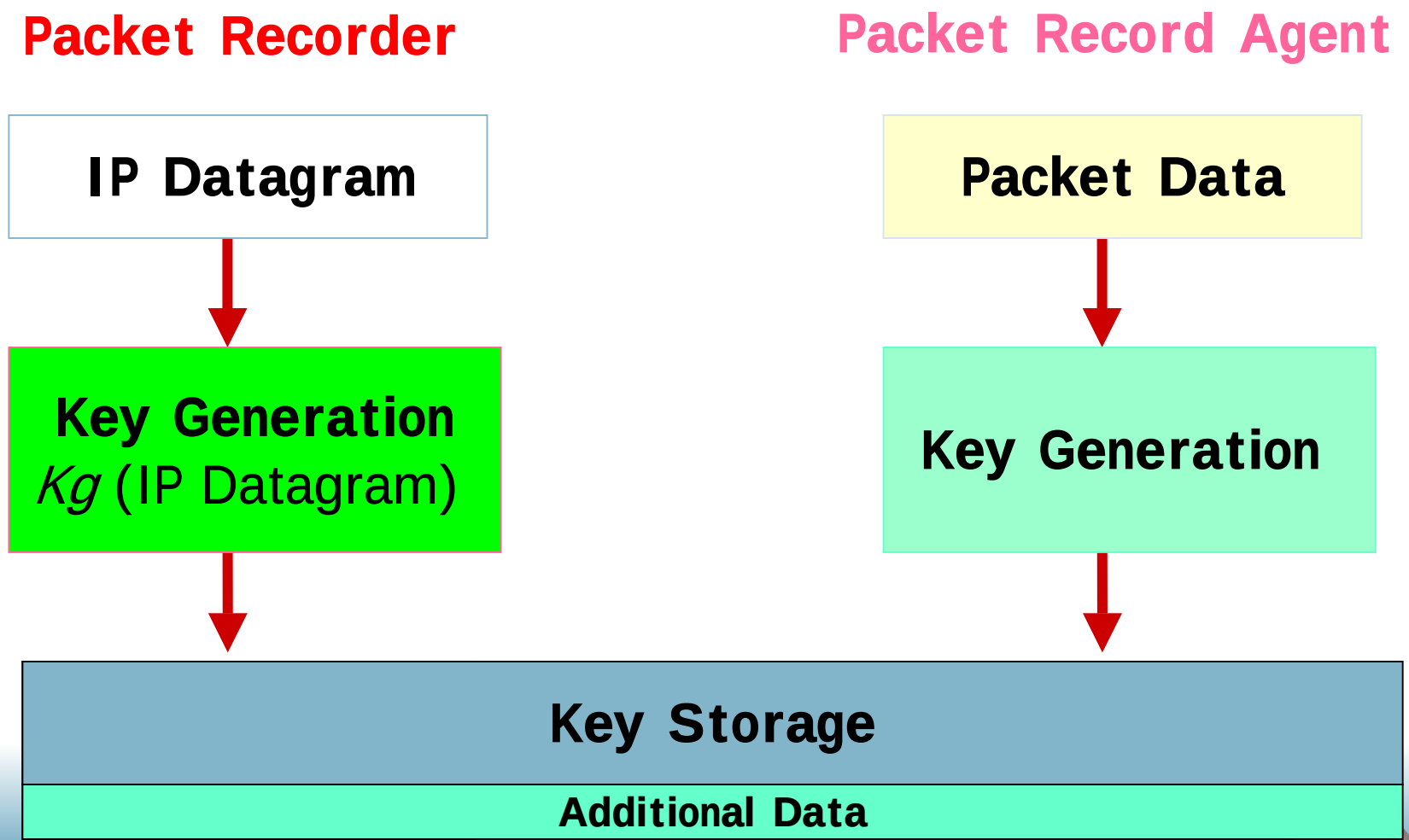
The Architecture



Requirements: Packet Record Protocol

- Mapping: PacketRecord ↔ (*encoded*) Packet
- Additional Data for corroboration
- Scope of Packet Record
  - which IP header fields are masked)
  - how much of the payload

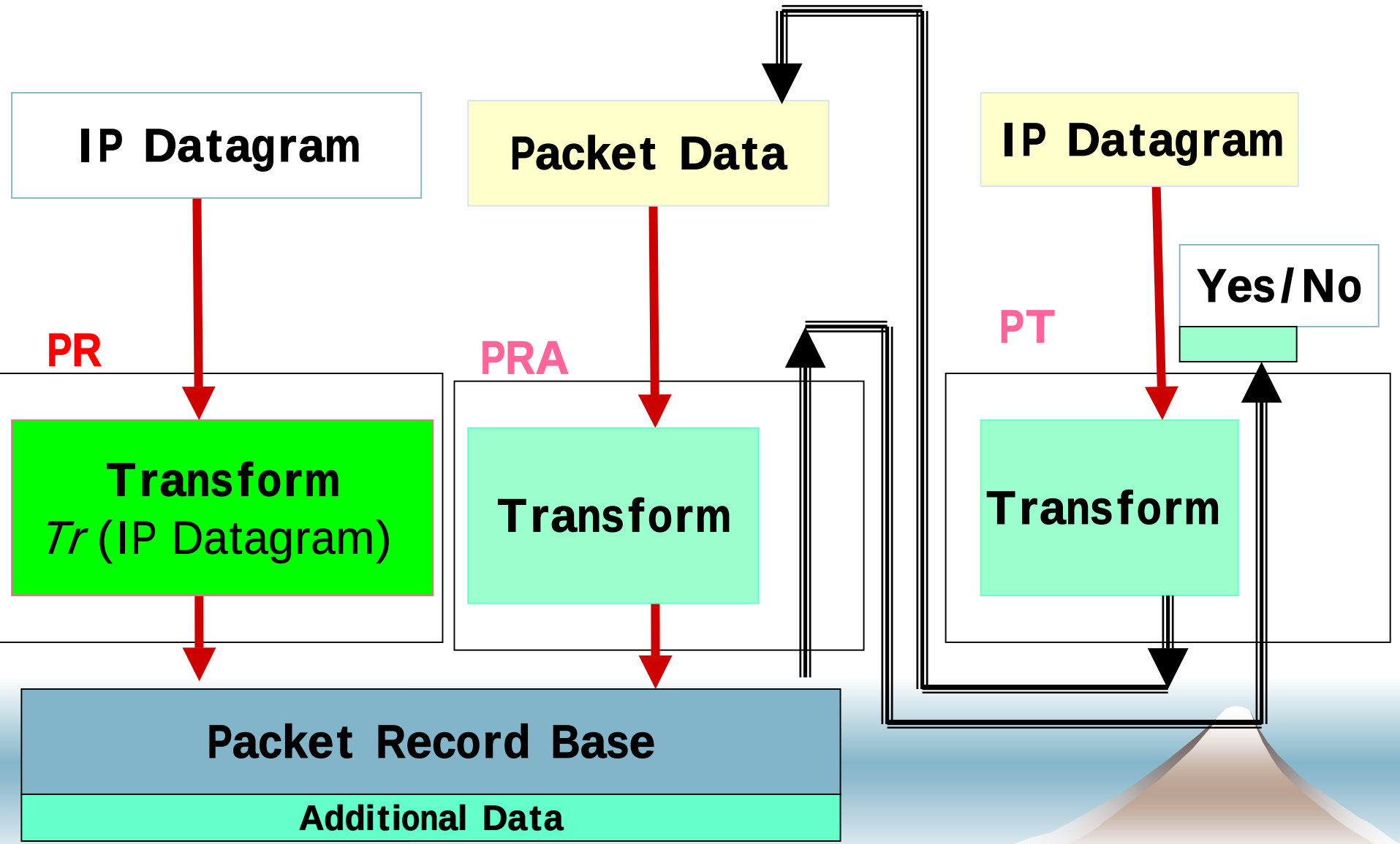
Requirements: Packet Record Protocol



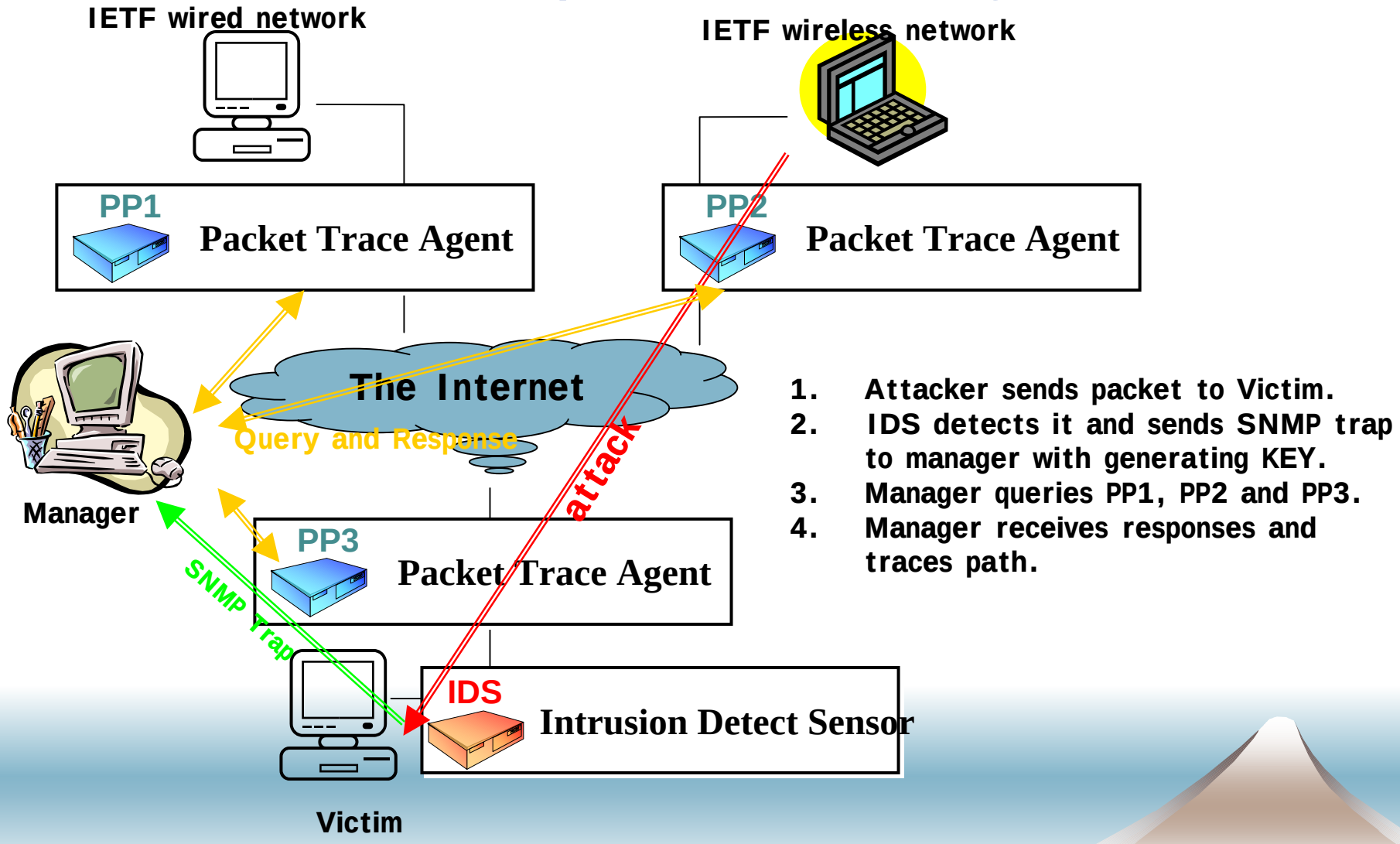
Requirements: Communication Protocol

- Check for existence of a datagram
- Lightweight
- Authenticated
- Privacy, Integrity
- Non Repudiation
- Query for Packet Recording parameters

The Process:


IP Datagram
Packet Data
IP Datagram
Yes/No
PR
PRA
PT
Transform
Tr (IP Datagram)
Transform
Transform
Packet Record Base
Additional Data

Demonstration:
SNMP based packet tracing



1. Attacker sends packet to Victim.
2. IDS detects it and sends SNMP trap to manager with generating KEY.
3. Manager queries PP1, PP2 and PP3.
4. Manager receives responses and traces path.

Demonstration: Screen shot