

An Architecture for IPPT

Glenn Mansfield Keeni

 *Cyber Solutions Inc.*

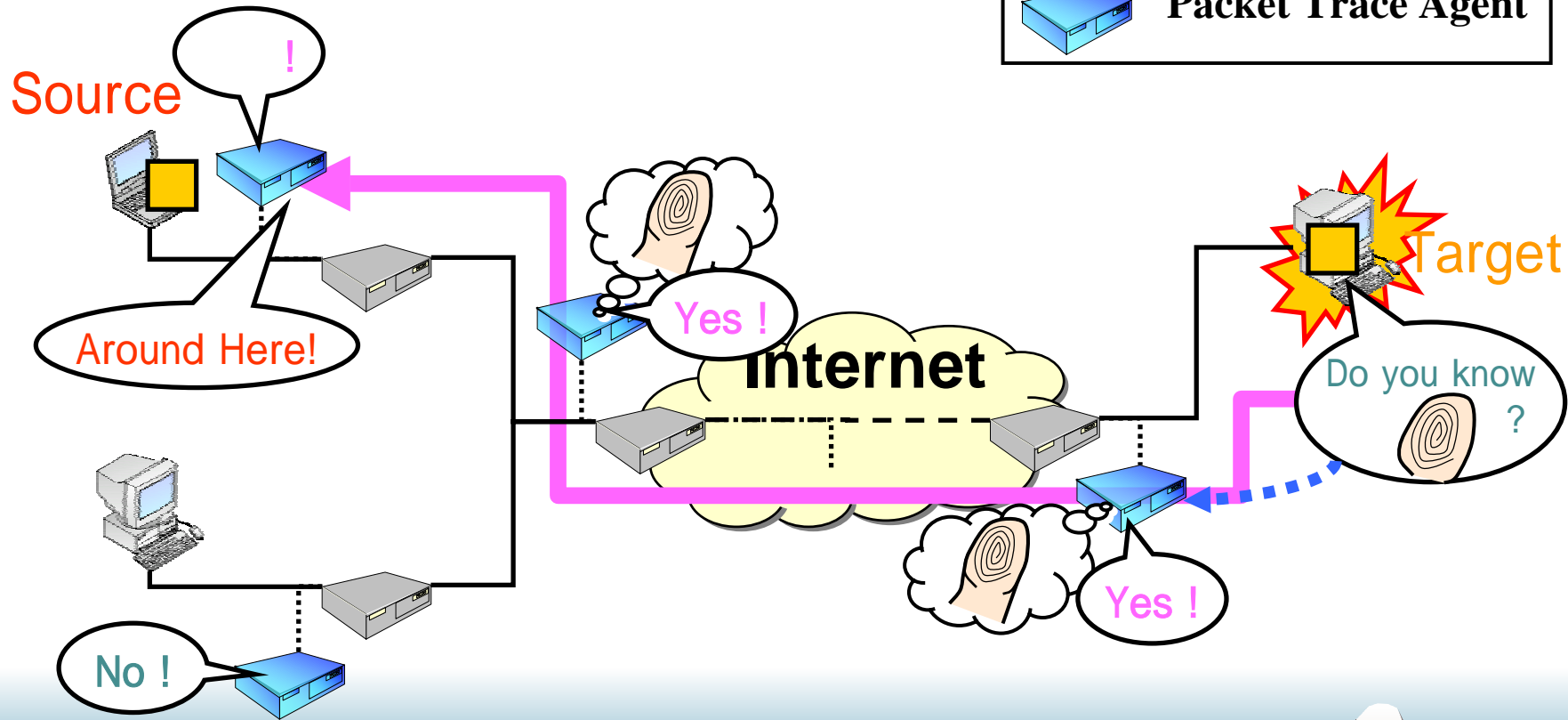
Yoshitaka Kuwata

 *NTT Data*

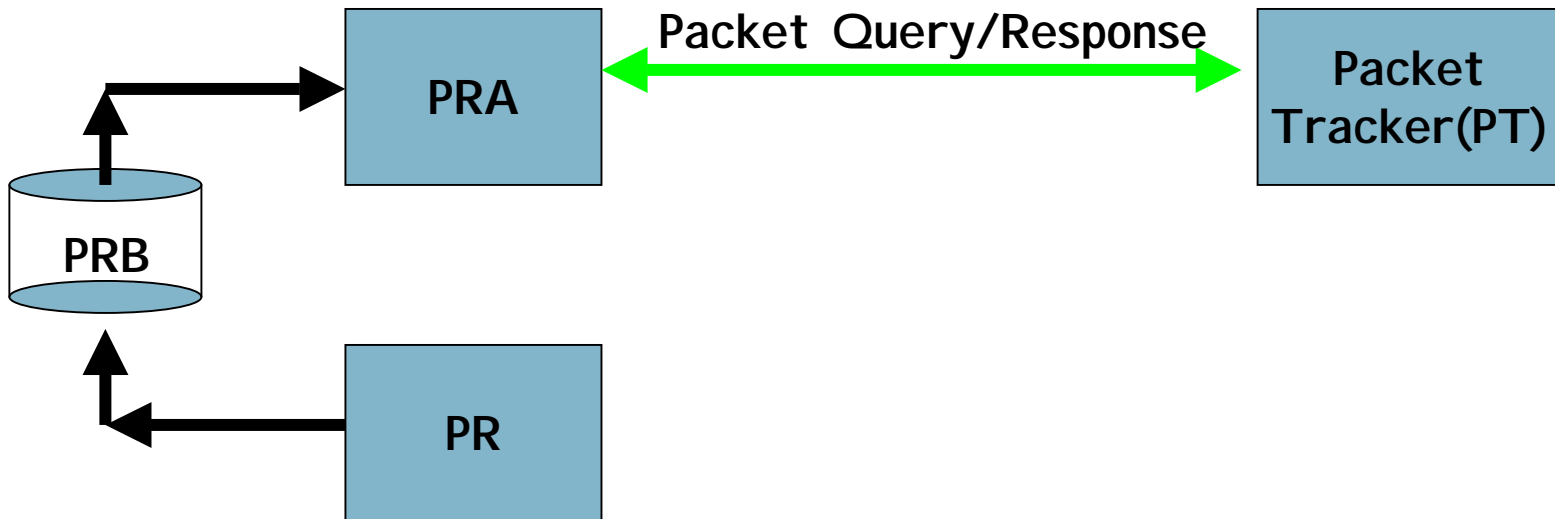
Ippt-BOF, IETF-54

July, 2002

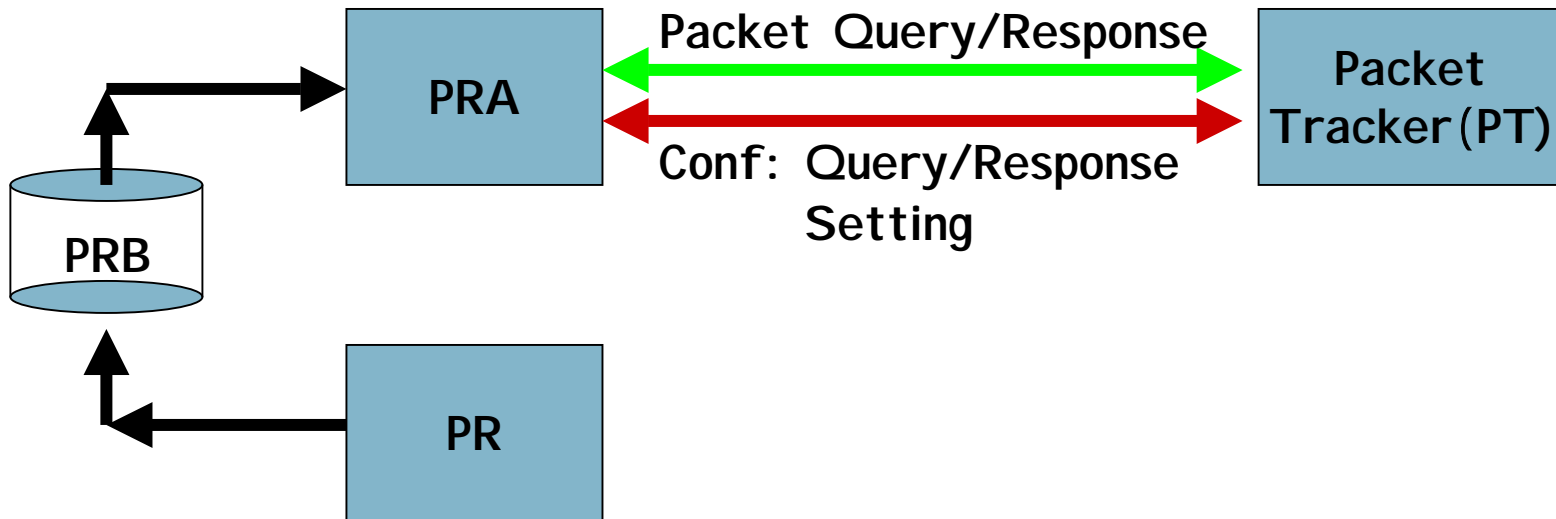
Packet Trace



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

Packet Recorder

IP Datagram



Key Generation
K_g (IP Datagram)



Packet Record Agent

Packet Data

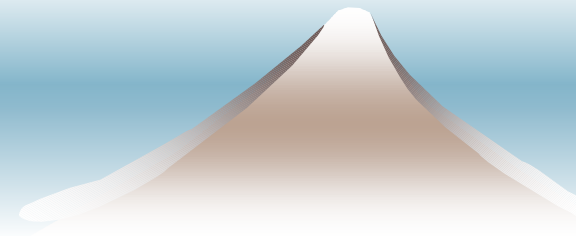


Key Generation

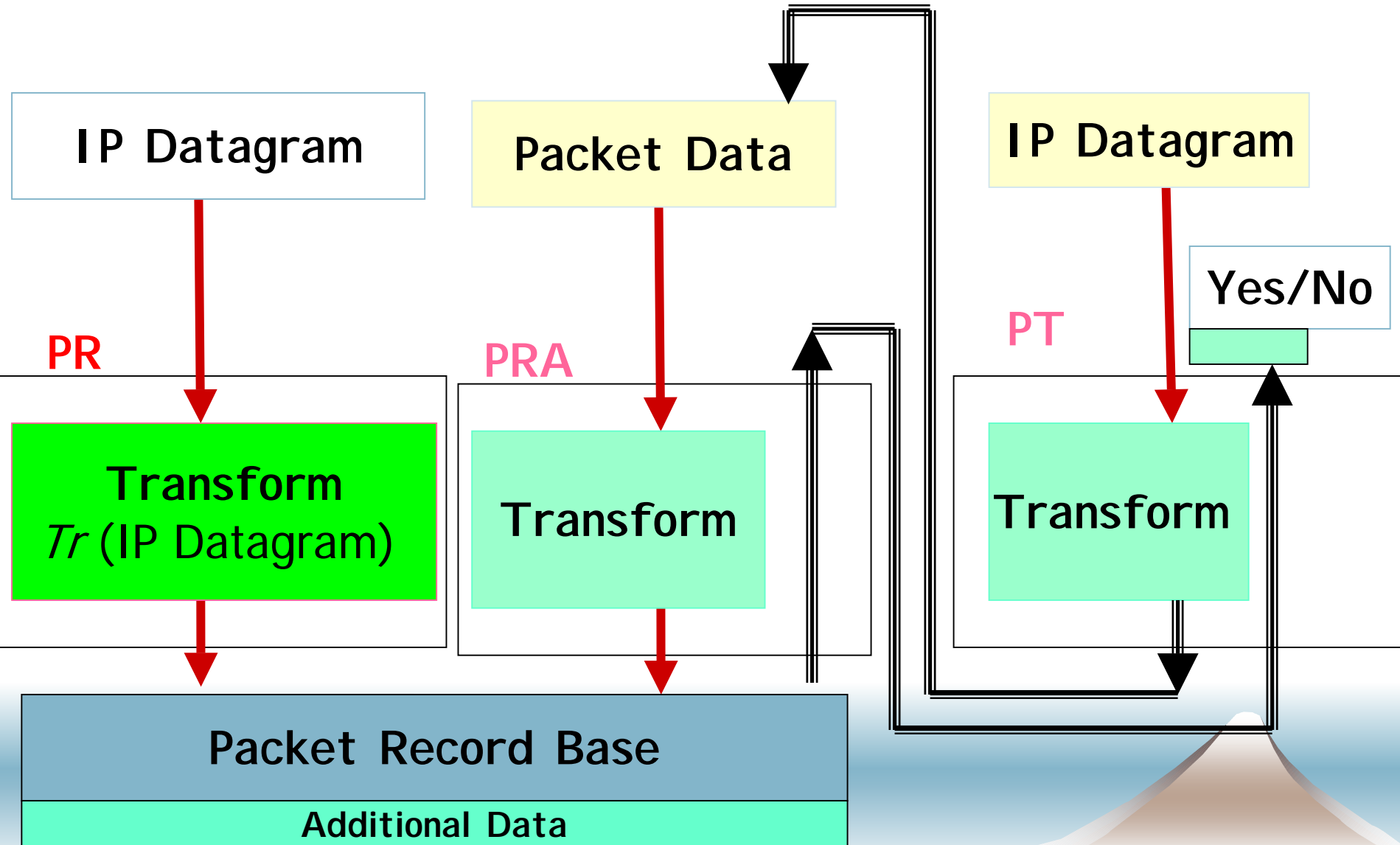


Requirements: Communication Protocol

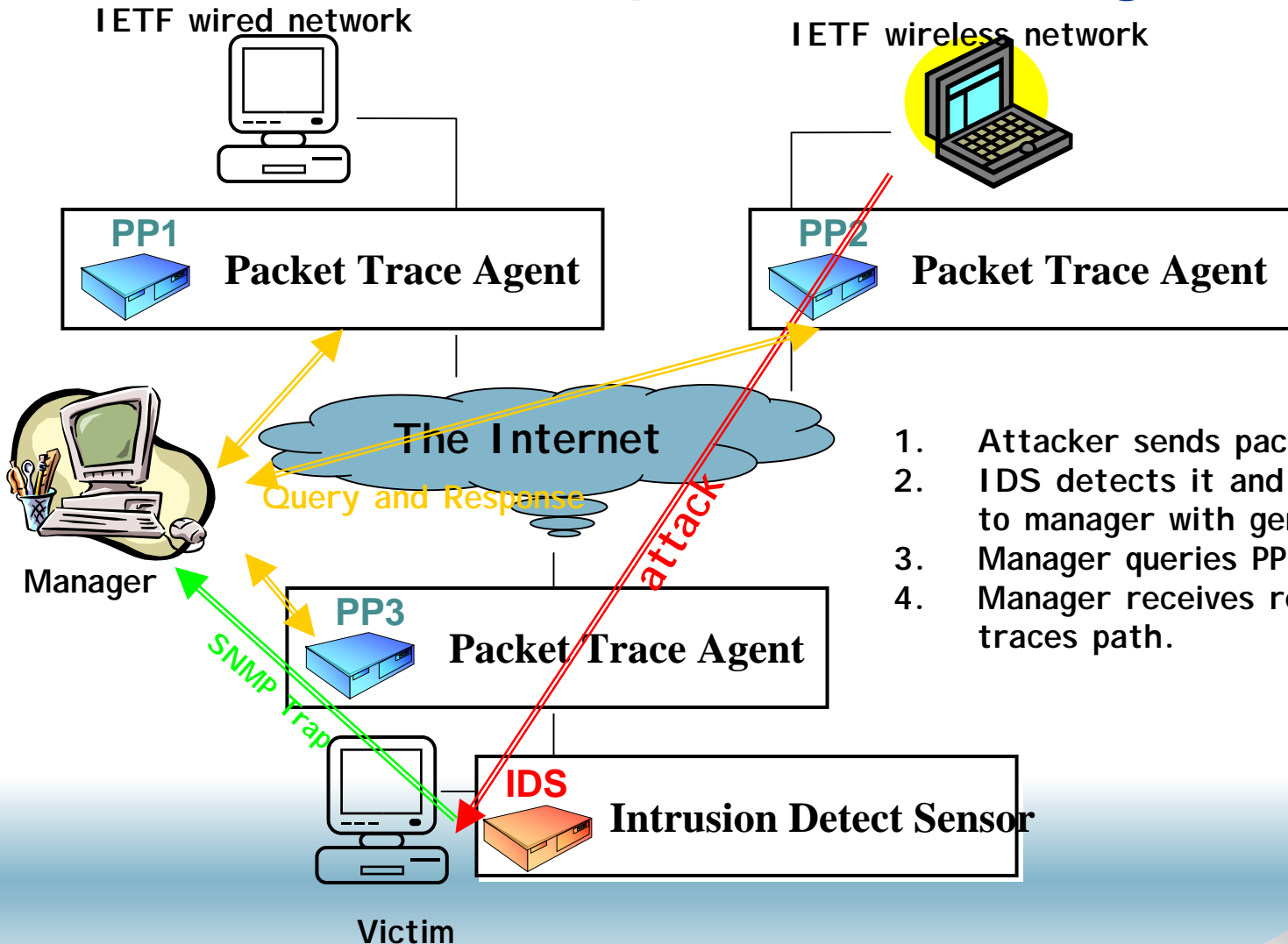
- ◆ Check for existence of a datagram
 - ◆ Lightweight
 - ◆ Authenticated
 - ◆ Privacy, Integrity
 - ◆ Non Repudiation
- ◆ Query for Packet Recording parameters



The Process:



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

The screenshot displays the Packet Chaser application window. The interface includes a menu bar (File, Edit, View, Help), a toolbar with various icons, and three main panels:

- Trap Receiver:** Shows a table with the following data:

Time Stamp	Source IP	Destination IP	Packet Print OID
22 Jul 2002, 14:55:31	133.93.77.249	203.178.138.21	86.204.105.192.38.112...
- Network Map Display:** A network diagram showing a central 'Internet' cloud. On the left, a 'Victim' PC is connected to a 'PP1' (Packet Printer) which is connected to a red vertical line labeled 'WVOC-SENDAI'. On the right, the 'Internet' is connected to two paths:
 - Top path: 'Router' -> 'PP2' -> 'IETF64-NETWORK' -> 'PC-B'.
 - Bottom path: 'Router' -> 'PP3' -> 'Wireless NETWORK' -> 'PC-A'.
- Packet Print Query Results:** Shows a table with the following data:

Query Server IP	Packet Print OID	Time Stamp
203.178.138.21.161	86.204.105.192.38.112.223.235.246.214.247.208.130.193.10.217.24.1	1027317331.371838
133.93.77.249.161	86.204.105.192.38.112.223.235.246.214.247.208.130.193.10.217.24.1	1027317290.53912

At the bottom left, a status bar indicates: "Packet Chaser is awaiting Command".