Three classes based model of traceback system between ASs

IETF59th Korea

INCH-WG

Toshifumi Kai (kai@trc.mew.co.jp), Hiroshige Nakatani (nakatani@trc.mew.co.jp) Naohiro Fukuda(fukuda@trc.mew.co.jp)

Matsushita Electric Works, Ltd.

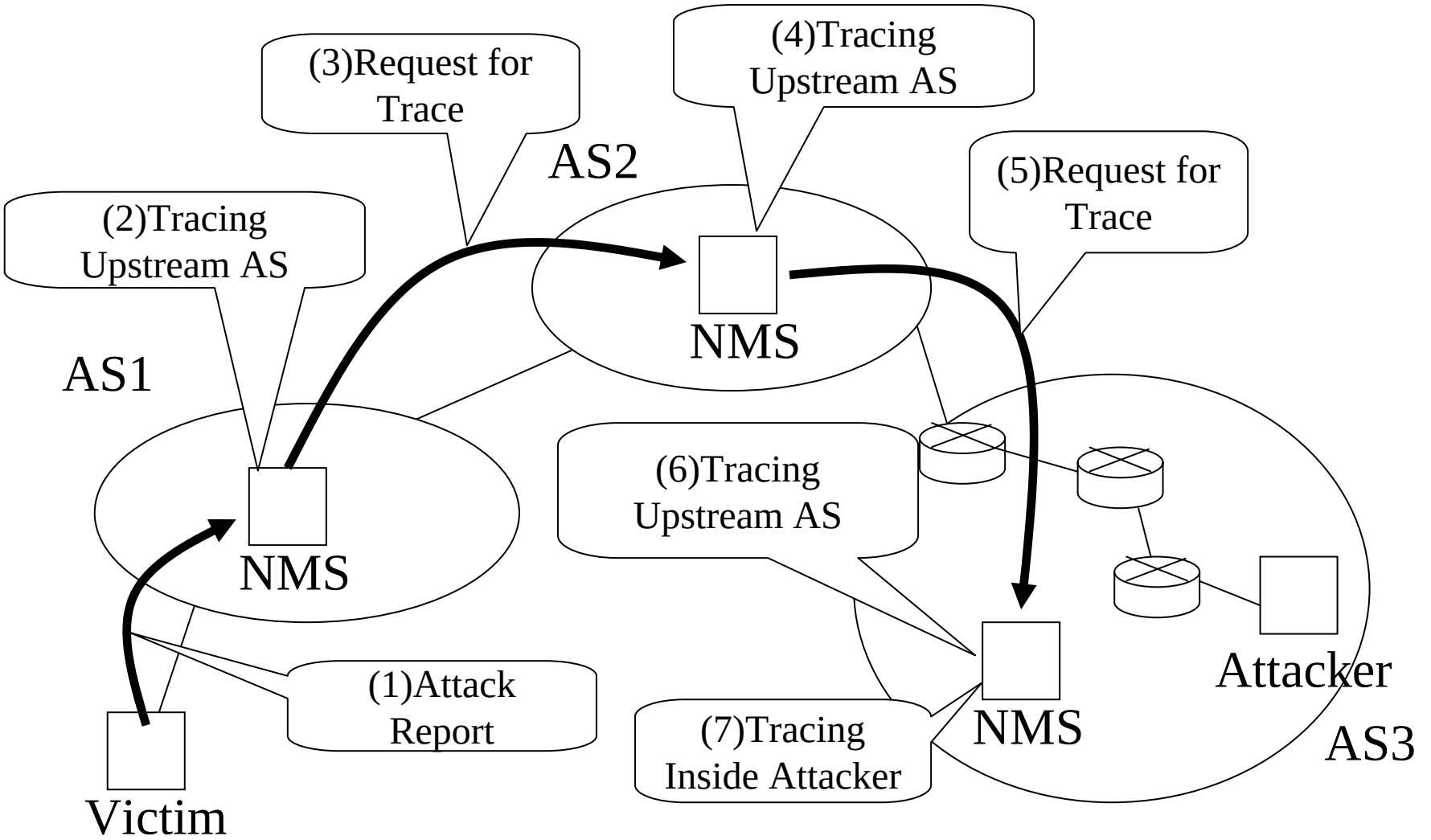
Akira Hashiguchi(akira@cooweb.com), Teruaki Takahashi(c300070@ns.kogakuin.ac.jp)

Katsuji Tsukamoto (tsukamoto@tsukaken.jp)

Kogakuin University

2004/2/12

Traceback flow between ASs



Additional Proposal

As far as we have developed and tested Proto Traceback System using over several hundred nodes targeting on Japanese Local Government (LGWAN), we think there are several requirements for RID.

*They requires tracing attack from end to end, and find it within a few minutes, and false positive rate within 5%.

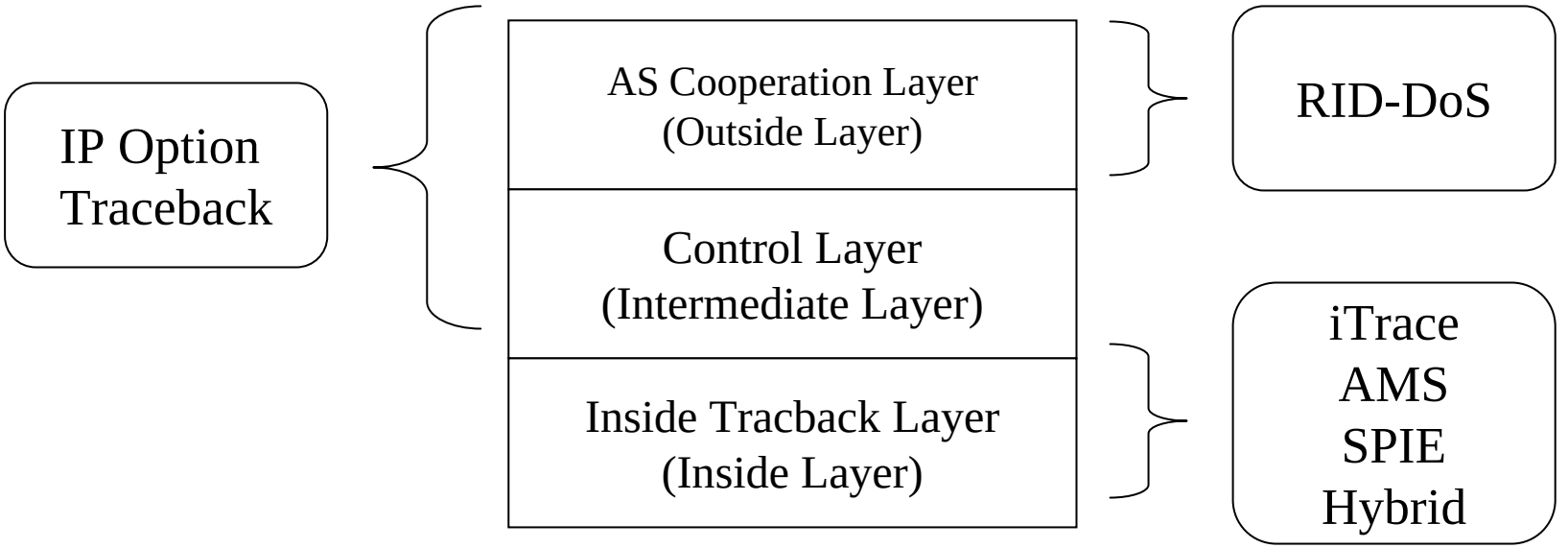
I) Add the range covers End to End as Classical (Layer)

1) Outside Layer … Cooperated with ASs (RID)
2) Intermediate Layer … Between Outside and Inside
3) Inside Layer … Inside AS

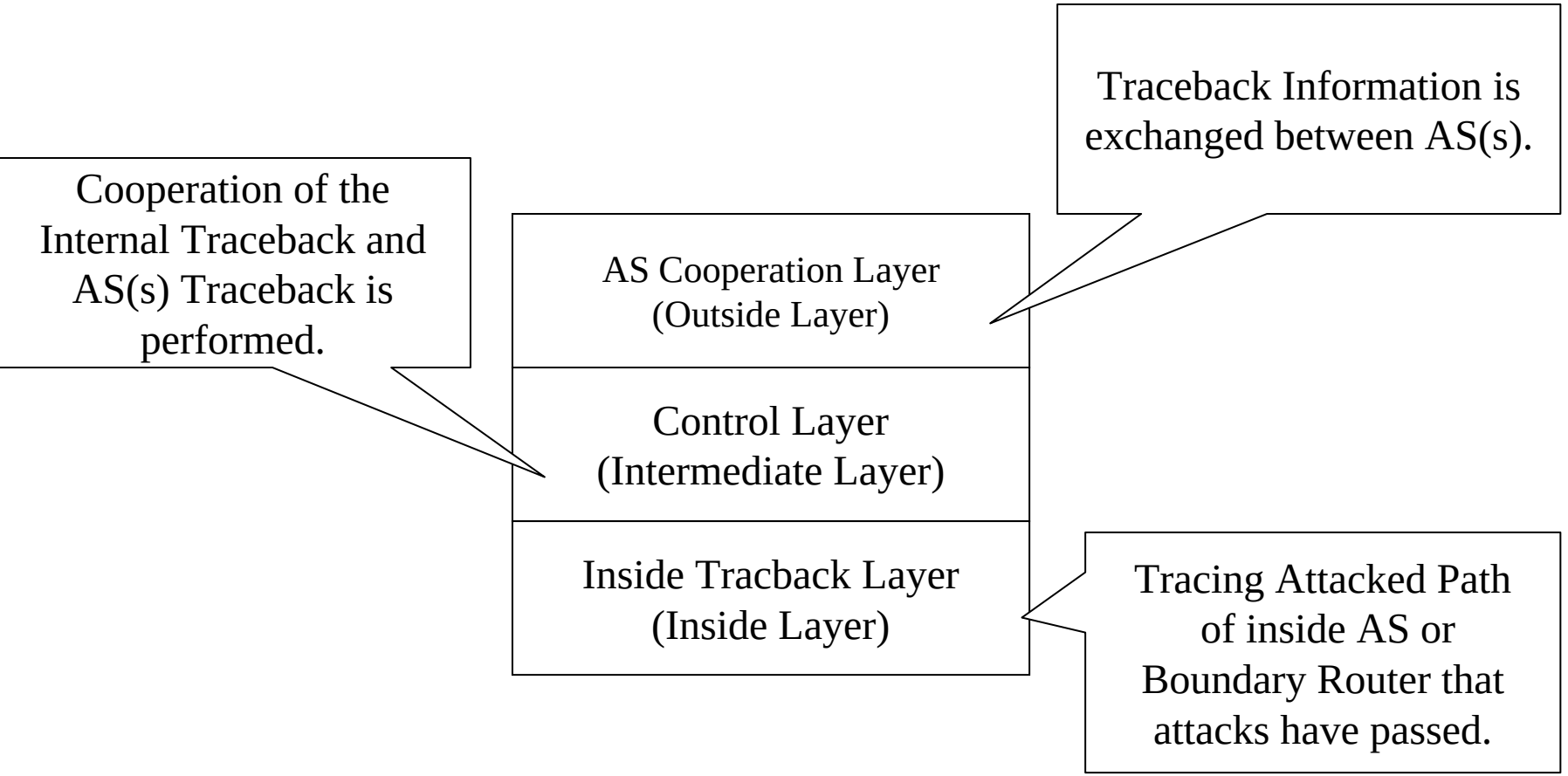
II) Add Modes

1) Normal (Detailed) Mode ... Tracing in Detail
2) Quick (Simple) Mode …Tracing Quickly and Rough
3) Nested (Efficient?) Mode …Tracing using Nest Structure

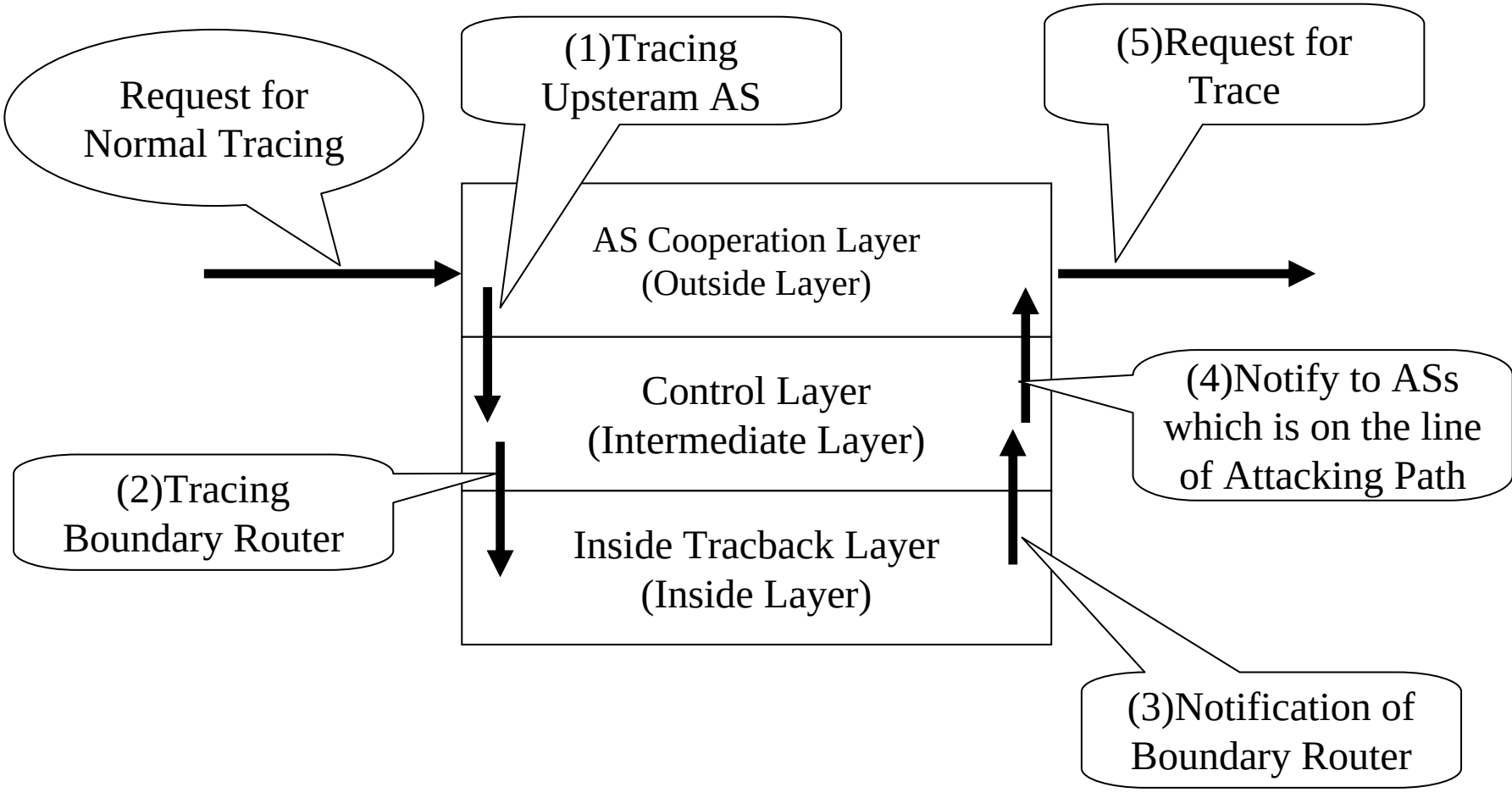
Positioning of each Traceback System



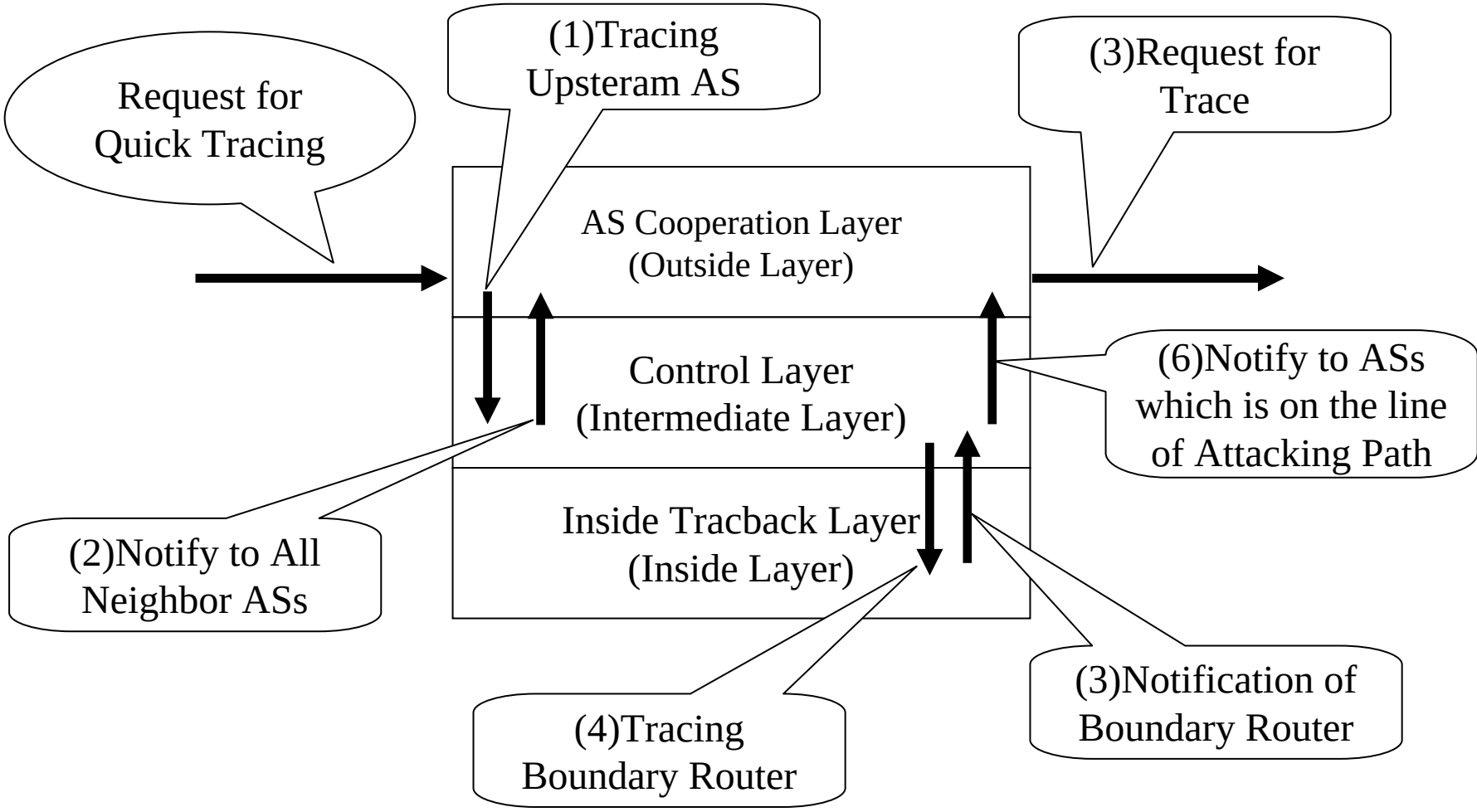
Three classes based model of traceback between ASs



Normal Tracing Mode



Quick Tracing Mode



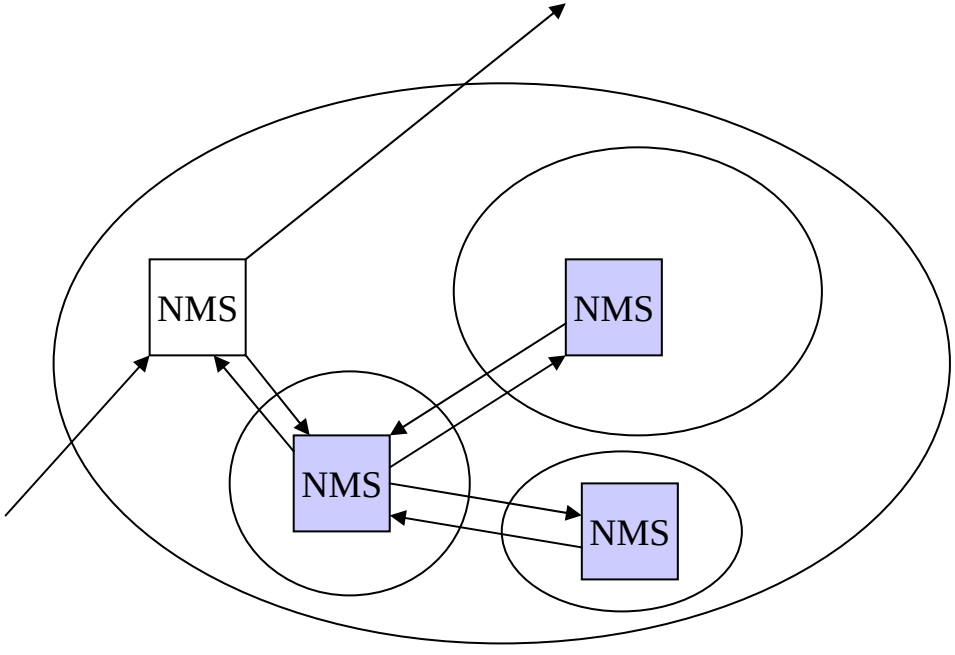
Nested Tracing Mode

AS Cooperation Layer
(Outside Layer)

Control Layer
(Intermediate Layer)

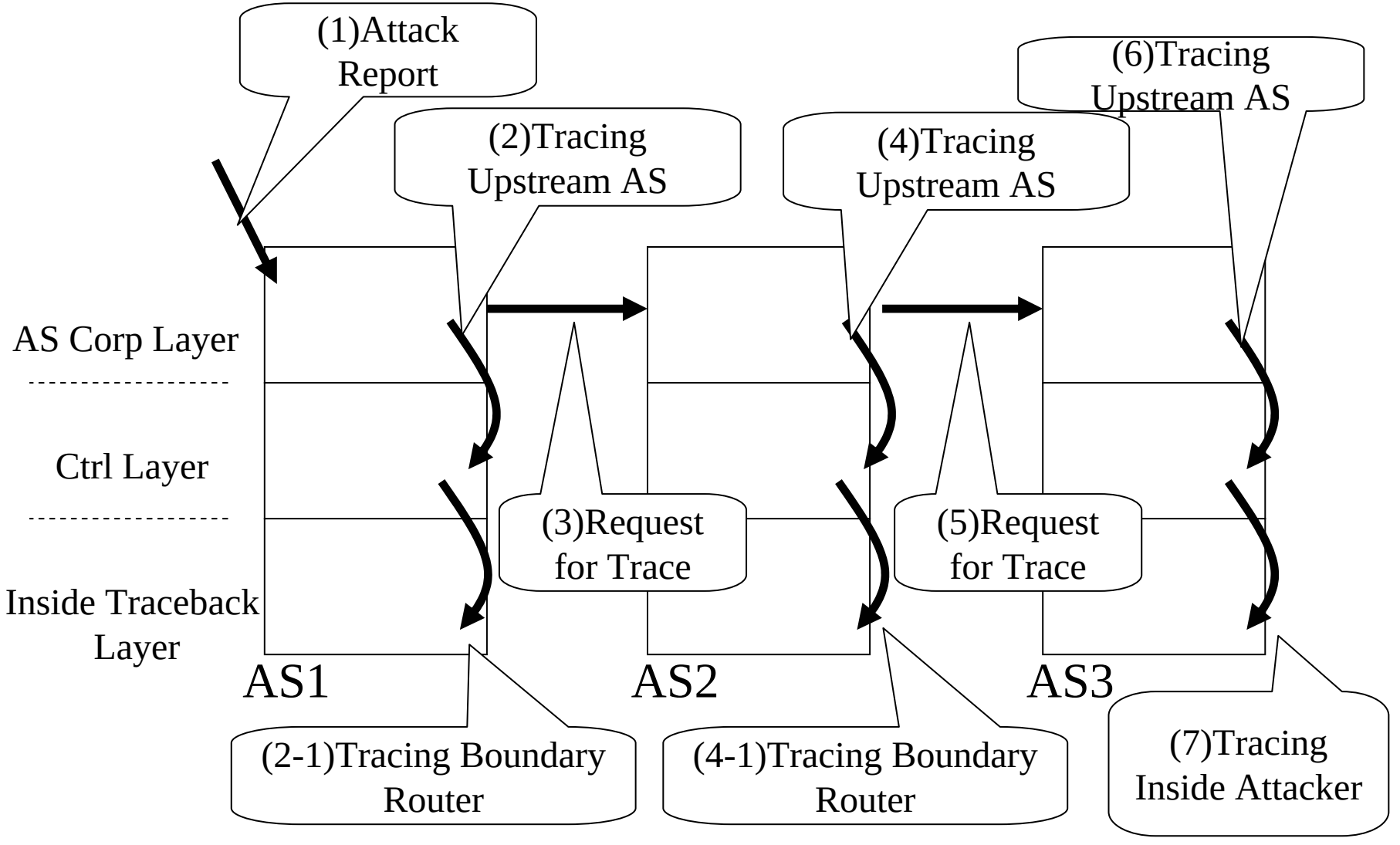
Inside Traceback Layer
(Inside Layer)

- AS Corp Layer
- Ctrl Layer
- Inside Traceback Layer

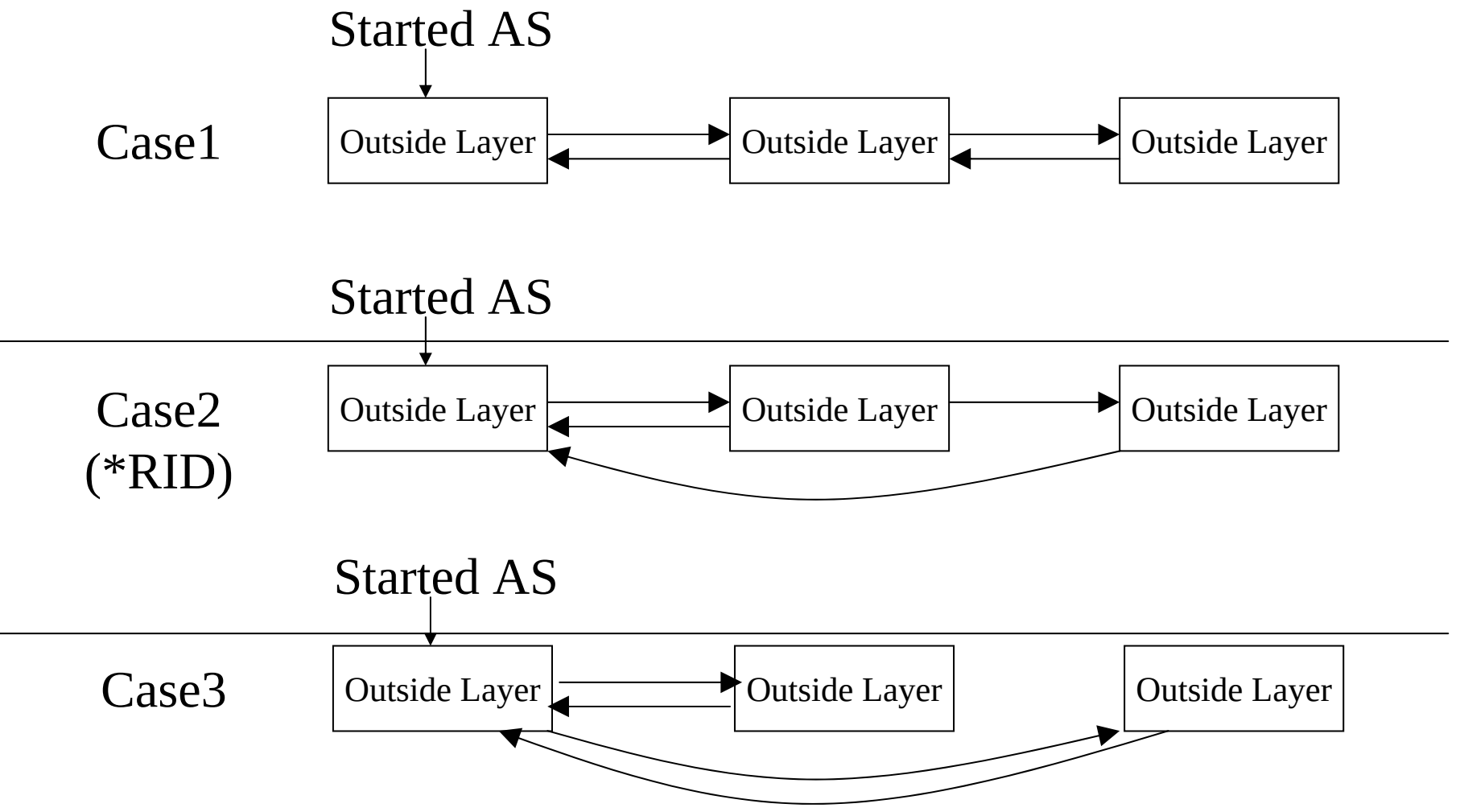


As an implementation, it will be better to do not only traceback for inside AS but the one between ASs as nested structure.

Flow


(1)Attack Report
(2)Tracing Upstream AS
(3)Request for Trace
(4)Tracing Upstream AS
(5)Request for Trace
(6)Tracing Upstream AS
(7)Tracing Inside Attacker
AS Corp Layer
Ctrl Layer
Inside Traceback Layer
AS1
AS2
AS3
(2-1)Tracing Boundary Router
(4-1)Tracing Boundary Router

Tracing Modes



Example Case of LGWAN (Japan)