NIST
National Institute of
Standards and Technology

iTL INFORMATION TECHNOLOGY LABORATORY

Measurement Data on AS_SET and AGGREGATOR: Implications for {Prefix, Origin} Validation Algorithms

Presentation at the IETF SIDR WG Meeting, July 2010

Presenter: K. Sriram

(Contributors: NIST BGP Security Team)

July 2010

National Institute of Standards and Technology

Contact: ksriram@nist.gov dougm@nist.gov

Terminology Clarification

In the slides that follow:

First AS after AS_SET =

First AS to the immediate left of the AS_SET

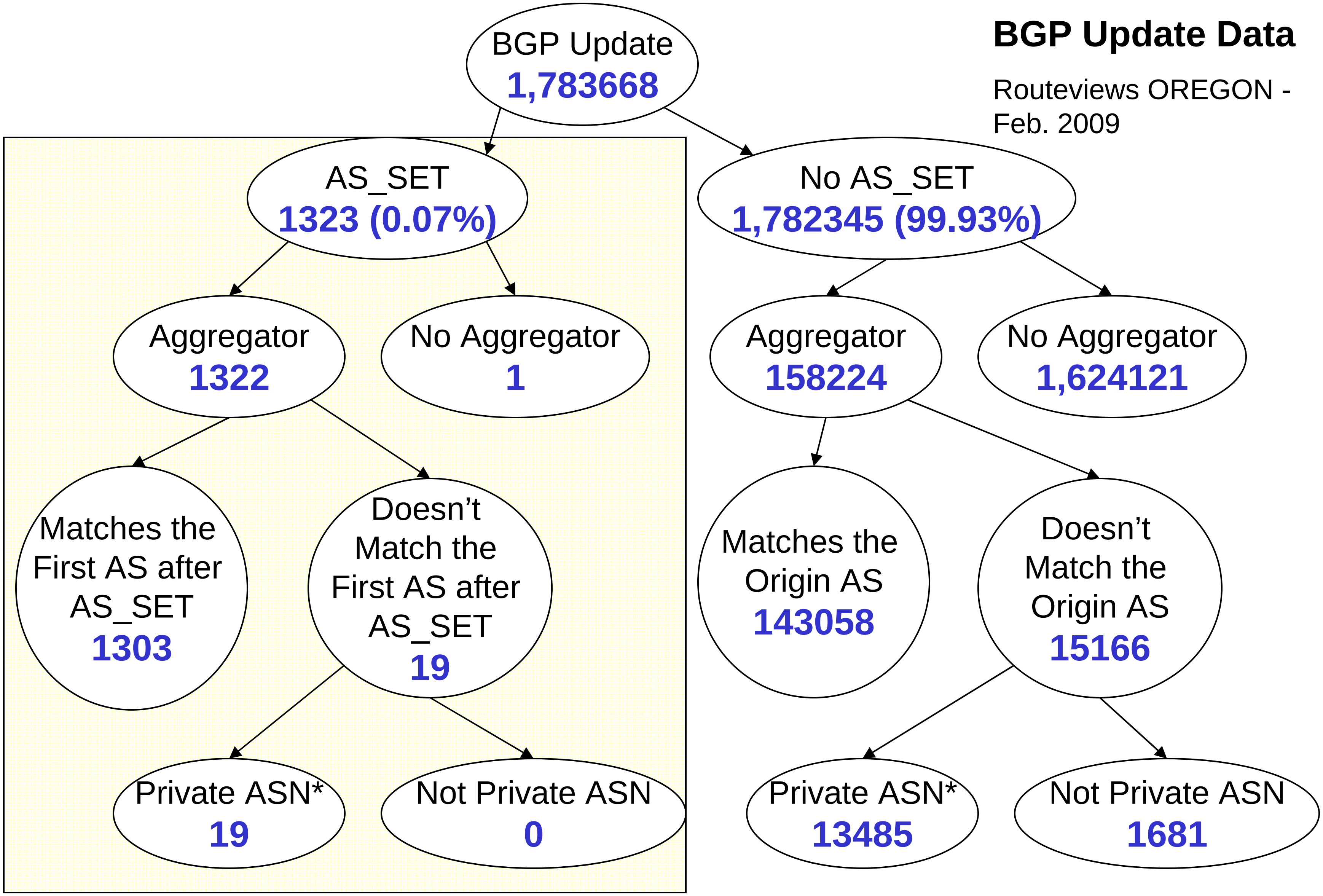
(When present, AS_SET occurs in the rightmost position with respect to the position of octets in the protocol message)

Origin AS: When there is no AS_SET present, the Origin AS is the right most AS in the AS_SEQUENCE.

Enumeration Tree and Stats - 1

BGP Update Data

Routeviews OREGON - Feb. 2009



BGP Update
1,783668

AS_SET
1323 (0.07%)

No AS_SET
1,782345 (99.93%)

Aggregator
1322

No Aggregator
1

Aggregator
158224

No Aggregator
1,624121

Matches the First AS after AS_SET
1303

Doesn’t Match the First AS after AS_SET
19

Matches the Origin AS
143058

Doesn’t Match the Origin AS
15166

Private ASN*
19

Not Private ASN
0

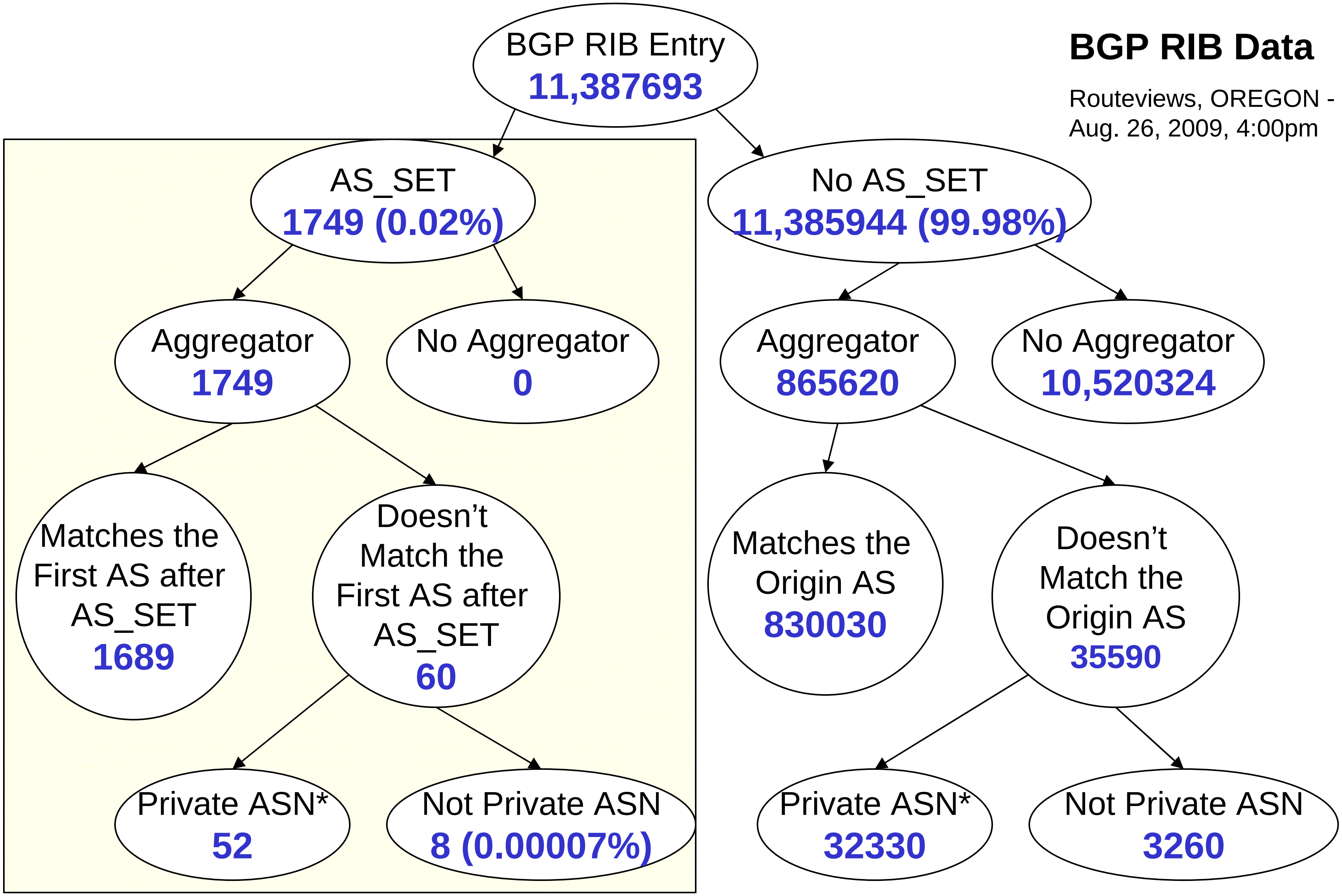
Private ASN*
13485

Not Private ASN
1681

*Aggregator is a Private ASN

Private ASN range = [64512 – 65535]

Enumeration Tree and Stats - 2



BGP RIB Entry
11,387693

AS_SET
1749 (0.02%)

No AS_SET
11,385944 (99.98%)

Aggregator
1749

No Aggregator
0

Aggregator
865620

No Aggregator
10,520324

Matches the First AS after AS_SET
1689

Doesn't Match the First AS after AS_SET
60

Matches the Origin AS
830030

Doesn't Match the Origin AS
35590

Private ASN*
52

Not Private ASN
8 (0.00007%)

Private ASN*
32330

Not Private ASN
3260

BGP RIB Data

Routeviews, OREGON -
Aug. 26, 2009, 4:00pm

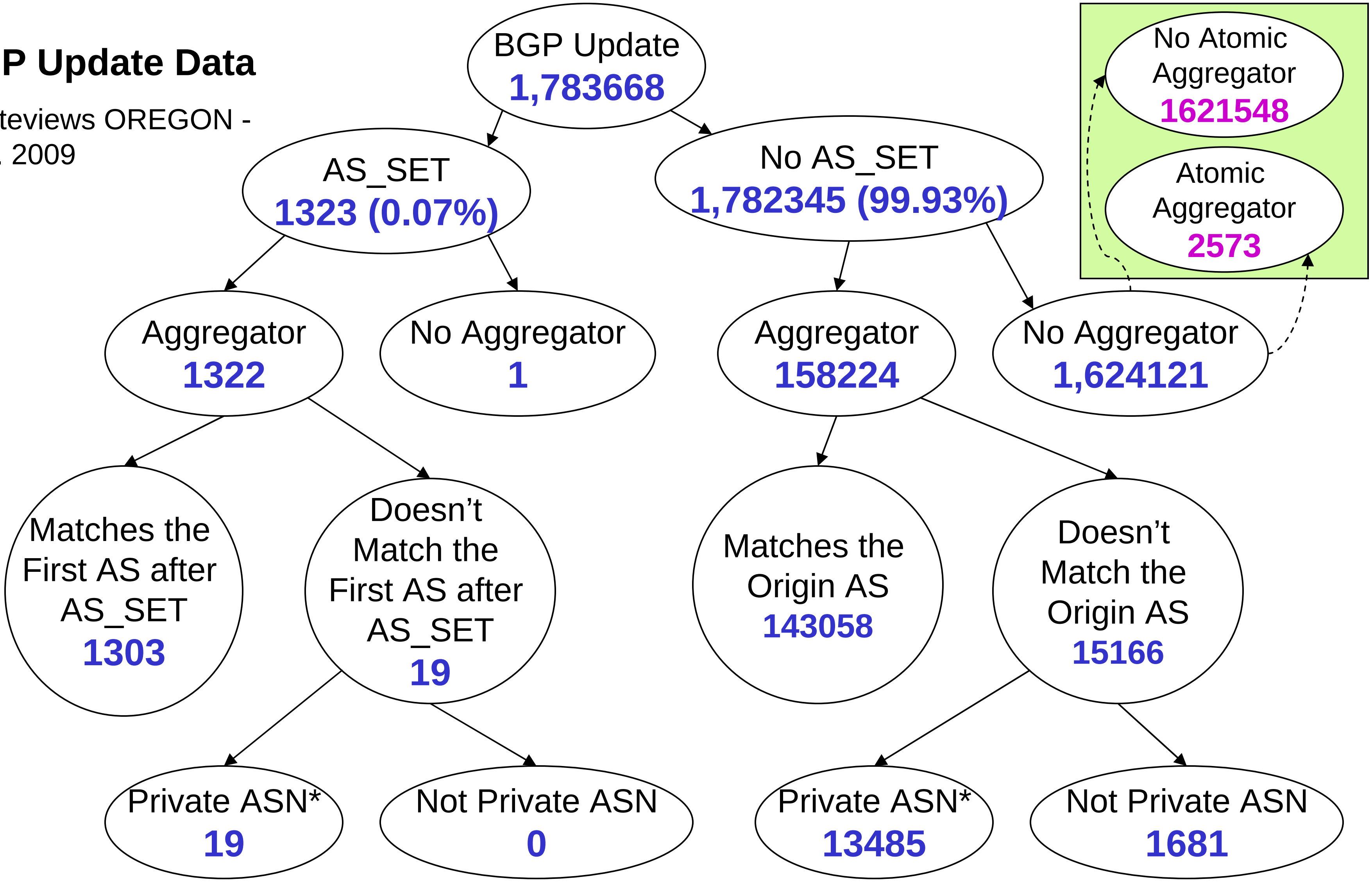
*Aggregator is a Private ASN

Private ASN range = [64512 – 65535]

Enumeration Tree and Stats - 3

BGP Update Data

Routeviews OREGON - Feb. 2009



BGP Update
1,783668

AS_SET
1323 (0.07%)

No AS_SET
1,782345 (99.93%)

Aggregator
1322

No Aggregator
1

Aggregator
158224

No Aggregator
1,624121

No Atomic Aggregator
1621548

Atomic Aggregator
2573

Matches the First AS after AS_SET
1303

Doesn’t Match the First AS after AS_SET
19

Matches the Origin AS
143058

Doesn’t Match the Origin AS
15166

Private ASN*
19

Not Private ASN
0

Private ASN*
13485

Not Private ASN
1681

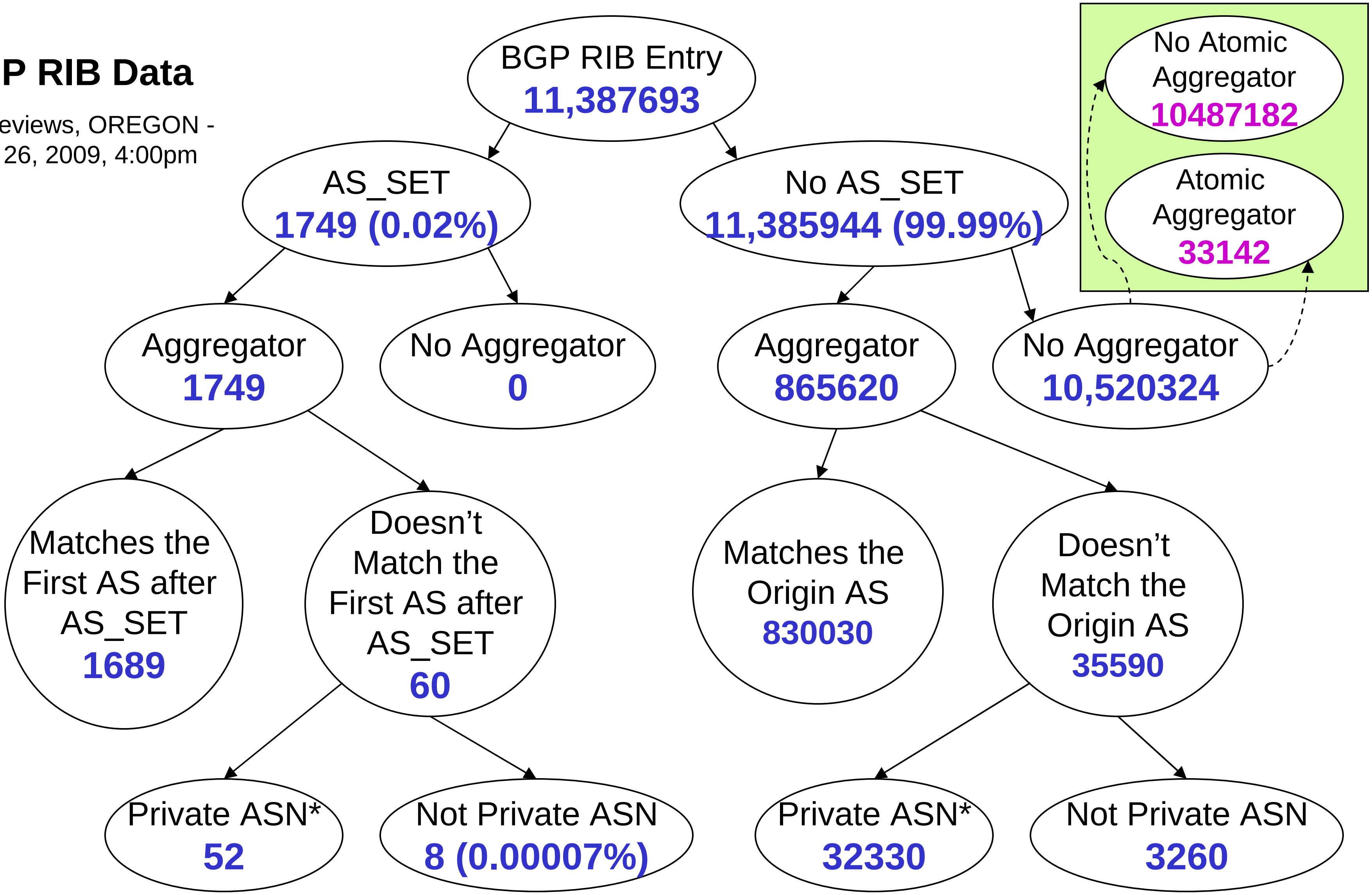
*Aggregator is a Private ASN

Private ASN range = [64512 – 65535]

Enumeration Tree and Stats- 4

BGP RIB Data

Routeviews, OREGON -
Aug. 26, 2009, 4:00pm



BGP RIB Entry
11,387693

AS_SET
1749 (0.02%)

No AS_SET
11,385944 (99.99%)

Aggregator
1749

No Aggregator
0

Aggregator
865620

No Aggregator
10,520324

No Atomic Aggregator
10487182

Atomic Aggregator
33142

Matches the First AS after AS_SET
1689

Doesn’t Match the First AS after AS_SET
60

Matches the Origin AS
830030

Doesn’t Match the Origin AS
35590

Private ASN*
52

Not Private ASN
8 (0.00007%)

Private ASN*
32330

Not Private ASN
3260

*Aggregator is a Private ASN

Private ASN range = [64512 – 65535]

Implications for the Algorithms

- It has been proposed to treat the AGGREGATOR as the Origin AS whenever an AS_SET is present (in {prefix, origin} validation algorithms)
- This can potentially lead to a new type of hijack attack possibility:
  - Attacker artificially places an AS_SET in his announcement
  - Sets the AGGREGATOR attribute value to the legitimate ASN
  - Places attacker's own ASN in the first AS position after (i.e., immediate left of) the AS_SET
- Data (slides 2, 3) shows that AGGREGATOR attribute is almost always present and matches with the ASN in the first AS position after the AS_SET
- The few cases when the two don't match are predominantly cases where the AGGREGATOR attribute is a private ASN (64512 – 65535). There should no ROAs anyway with private ASNs (in the context of global eBGP).
- Recommendation (based on the above observations):
  - It is better (more secure) to always take the first AS after the AS_SET as the Origin (disregard the AGGREGATOR)
  - This also keeps the algorithm simpler