

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

NIST BGP Security Team

July 2010

National Institute of Standards and Technology

Contact: ksriram@nist.gov doug@nist.gov

Terminology Clarification

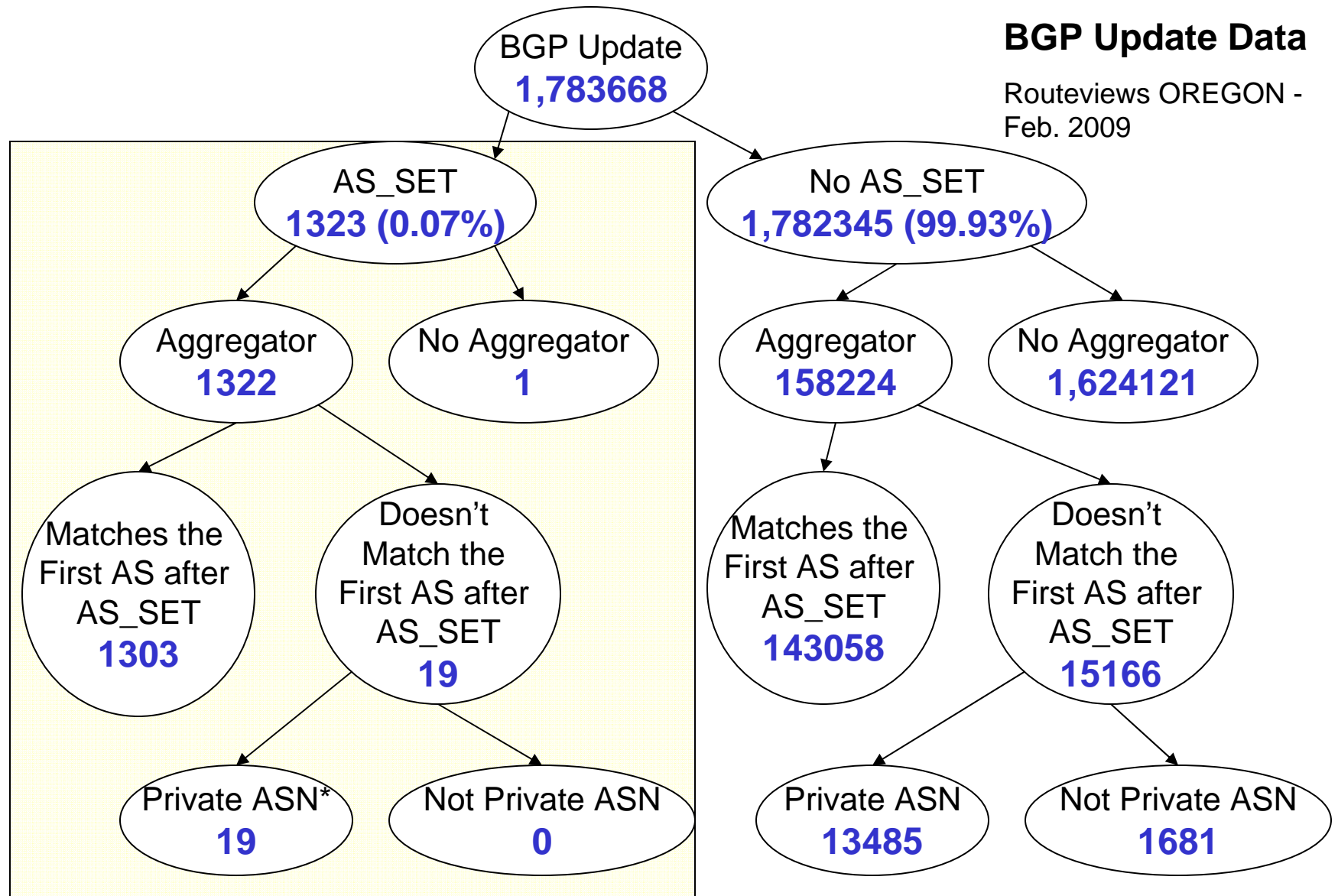
In the slides that follow:

First AS after AS_SET =

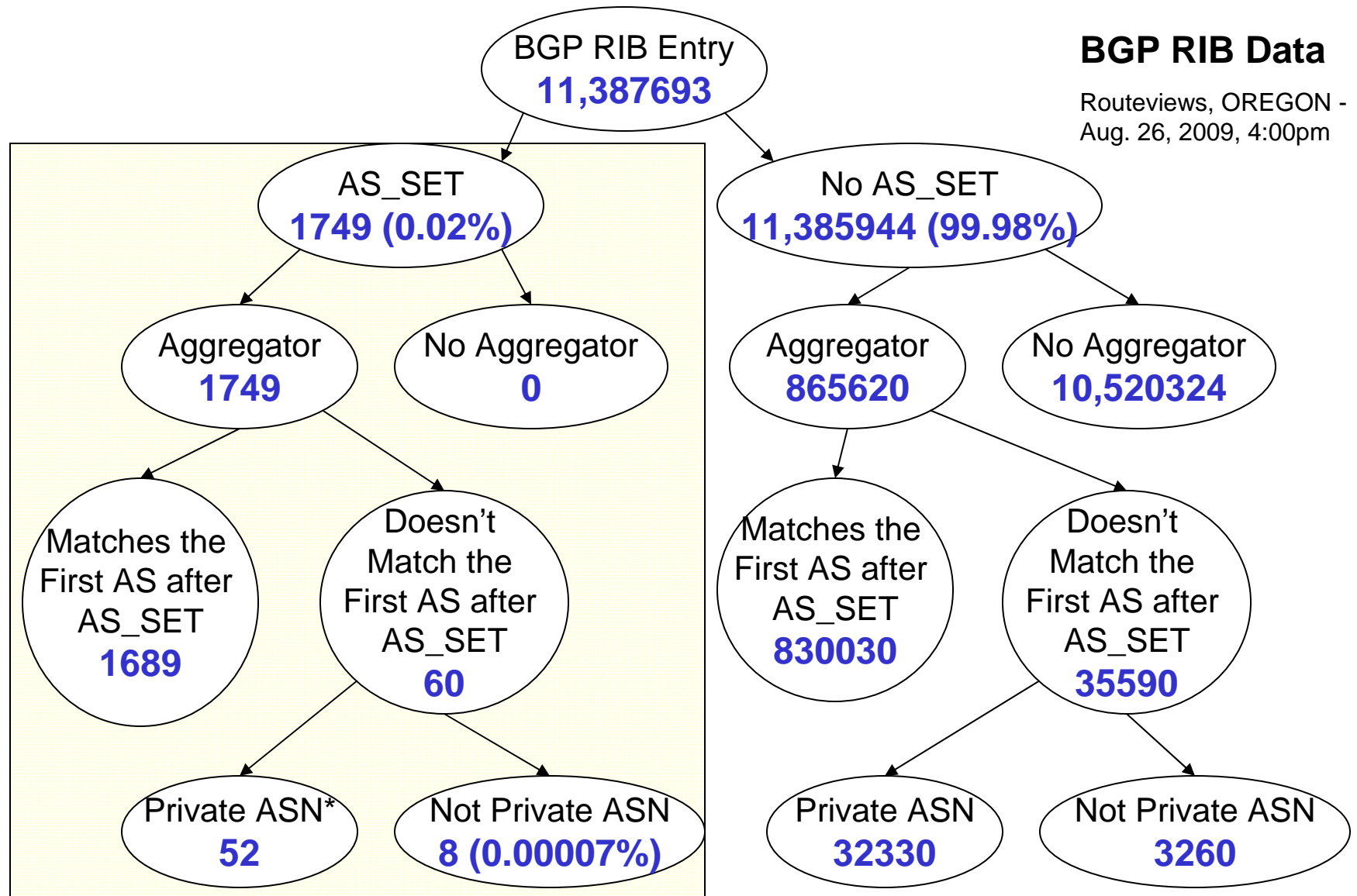
First AS to the immediate left of the AS_SET

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

Enumeration Tree and Stats - 1



Enumeration Tree and Stats - 2



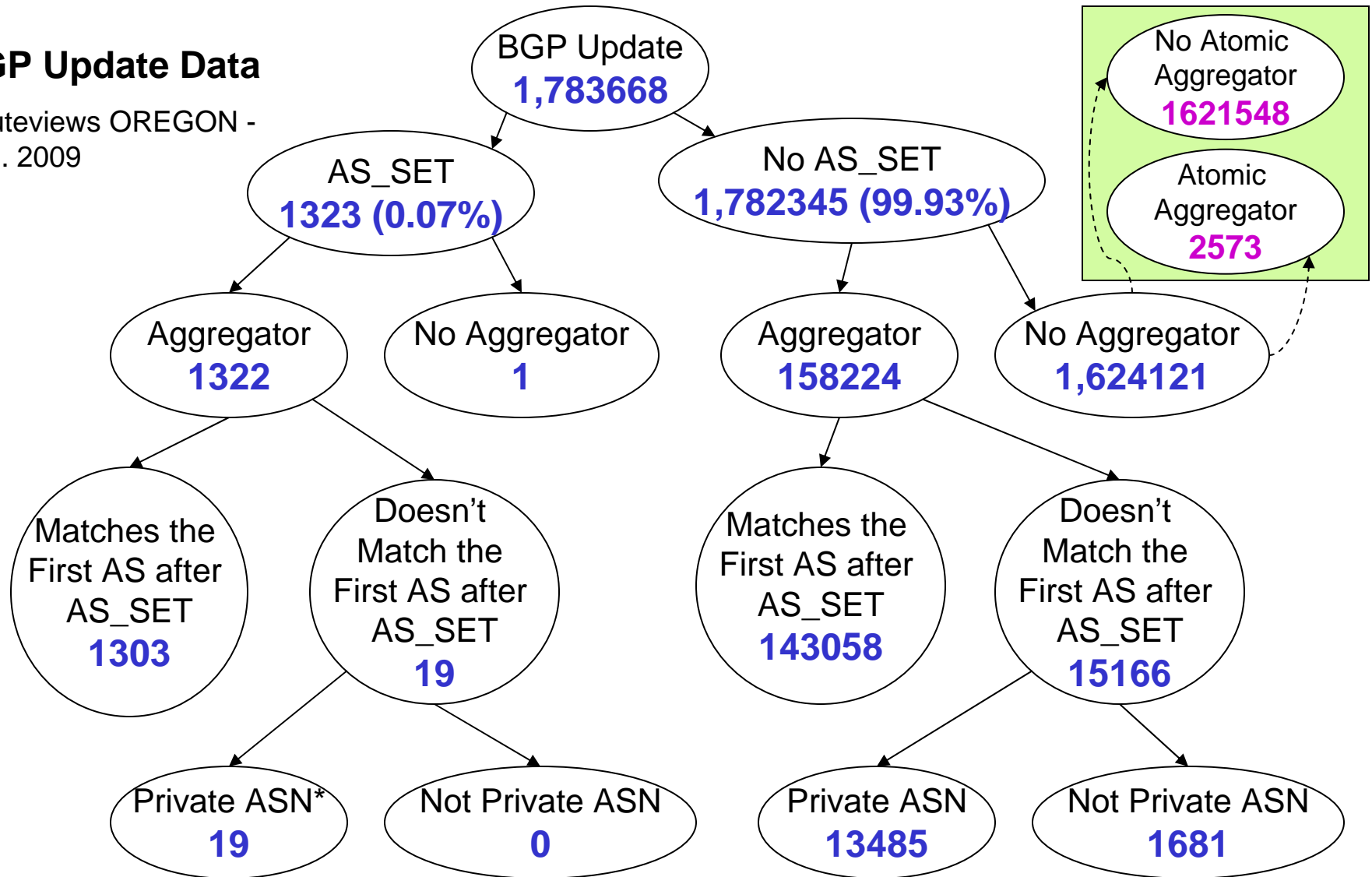
*Aggregator is Private ASN

Private ASN range = [64512 – 65535]

Enumeration Tree and Stats - 3

BGP Update Data

Routeviews OREGON -
Feb. 2009



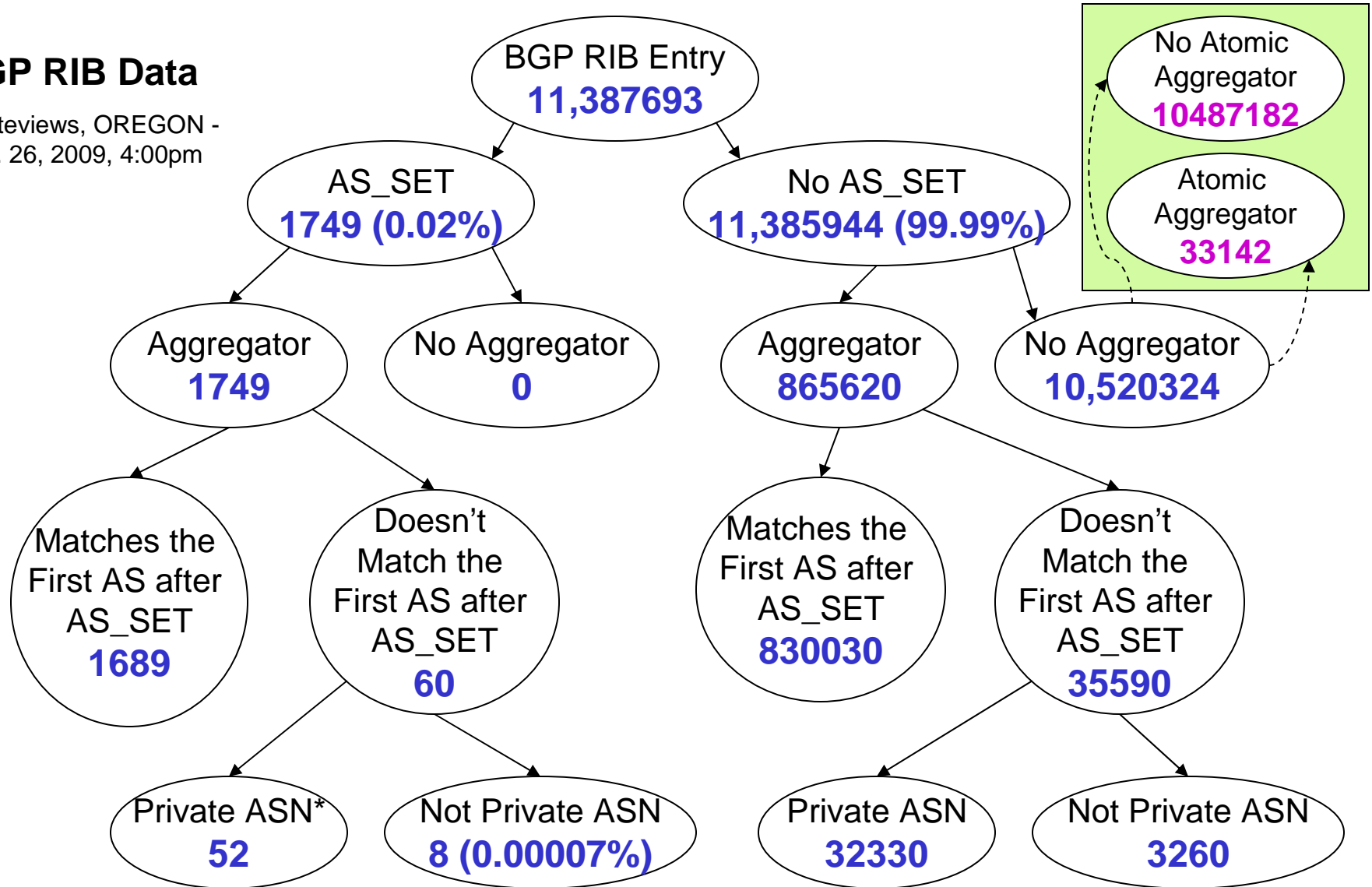
*Aggregator is Private ASN

Private ASN range = [64512 – 65535]

Enumeration Tree and Stats- 4

BGP RIB Data

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



*Aggregator is 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 be 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