BGPSEC
AN APPROACH TO ROUTE ORIGIN VALIDATION

Ehsan Ghazizadeh

RIPE Community

PRESENTATION OUTLINE

- Background
- Terminology
- Threat characterization
- Attack characterization
  - Active wiretapping of links between BGP speakers
  - Attacks on a BGP router
  - Attacks on ISP management computers
  - Attacks on repositories
  - Attacks on an RPKI CA
- Residual vulnerabilities

TERMINOLOGY (1/2)

- Adversary

  - An adversary is an entity (e.g., a person or an organization) perceived as malicious, relative to a security policy of a system.

- Vulnerability

  - A vulnerability is a flaw or weakness in a system's design, implementation, or operation and management, that could be exploited to violate the security policy of a system.

- Attack

  - An attack is an action that attempts to violate the security policy of a system, e.g., by exploiting a vulnerability.

BACKGROUND

- The SIDR WG has almost finished work on a set of standards to erroneous origin AS announcements

- The next step in improving routing security in the public Internet is to counter malicious attacks on BGP UPDATEs

- The term BGPSEC refers to the mechanisms used to achieve this greater degree of security

- BGPSEC builds on the RPKI developed in SIDR, and calls for each AS to digitally sign the AS path info that it propagates, and to verify the path info it receives

TERMINOLOGY (2/2)

- Countermeasure

  - A countermeasure is a procedure or technique that thwarts an attack, preventing it from being successful. Often countermeasures are specific to attacks or classes of attacks.

- Threat

  - A threat is a motivated, capable adversary. An adversary who is not motivated, or who is not capable of effecting an attack, is not a threat.

ADVERSARY CAPABILITIES

- BGP speakers
  - Manipulation of BGP

- Hackers
  - Compromise of network management systems & routers

- Criminals
  - Extortion of an ISP or telecom provider

- Registries
  - Manipulation of the RPKI segments that they control

- Nations
  - Influence over ISPs, telecom providers and local registries, MITM attacks,

ADVERSARIES

- BGP speakers (ASes)
  - ISPs or multi-homed subscriber
- Hackers
  - For hire?
- Criminals
- Registries
  - IANA, RIRs, NIRs, LIRs
- Nations
  - Intelligence agencies

ATTACKING EBGP LINKS

- Passive wiretapping is not considered a problem

- Active wiretapping (MITM on the link attacks)

  - Packet modification

  - Packet deletion

  - Replay

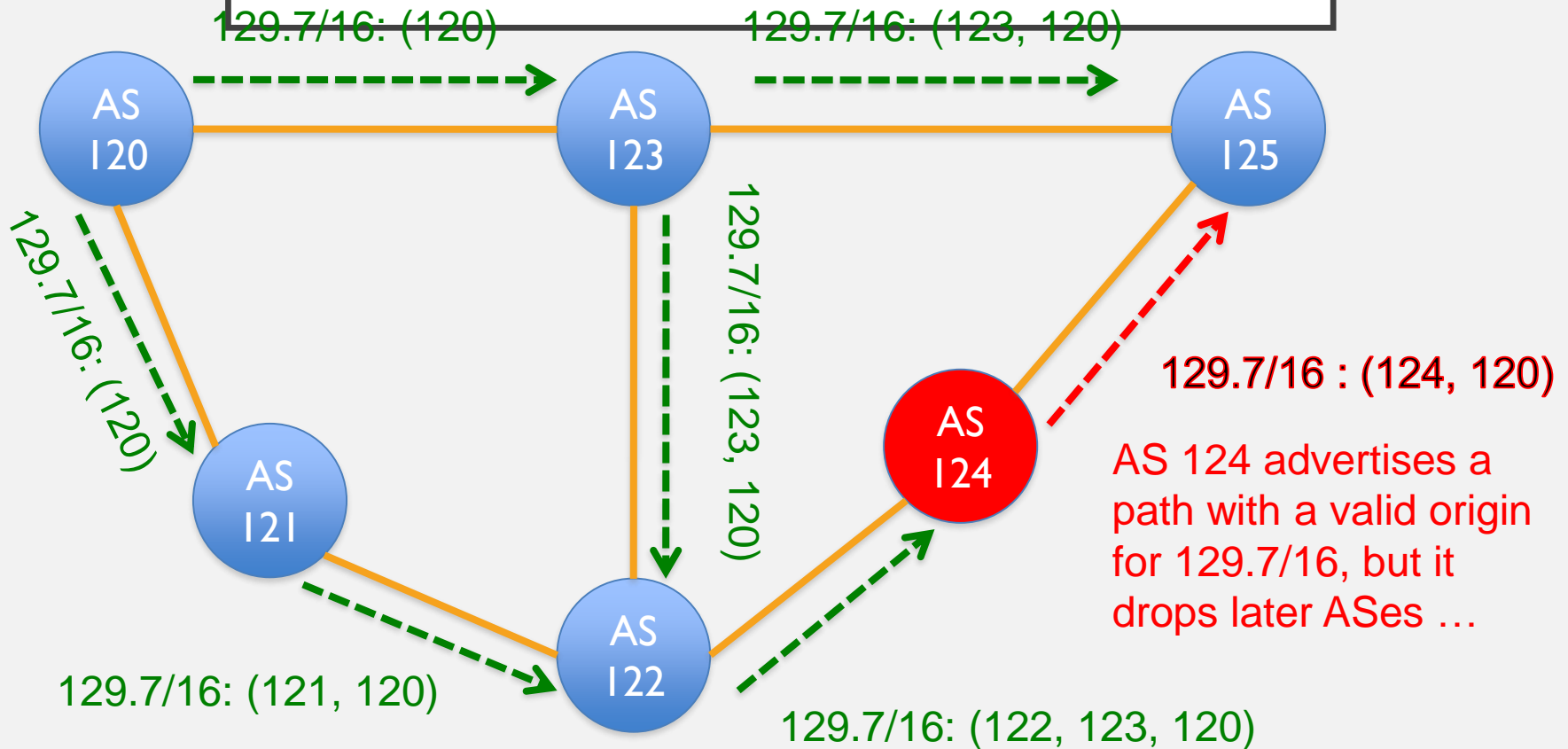- Target can be IP, TCP, BGP (including BGPSEC data)

ATTACK TARGETS

- BGP routers
  - Bogus AS paths, signature removal, bad signature insertion, router key compromise, update replay, …

- ISP management systems
  - Router manipulation, deleting valid RPKI objects, uploading expired RPKI objects, …

- Repositories
  - Removing valid RPKI objects or inserting invalid objects

- RPKI CAs
  - Duplicate allocation of resources, unauthorized revocation or certificates, …

BGP PATH ATTACK EXAMPLES (1/2)

- Valid Origin, bad path

    - Although ROAs allow an ISP to detect and reject a route with an unauthorized origin AS, they do not prevent an AS from advertising a bogus path with a valid origin AS.

- Prefix "narrowing"

    - An AS along a valid path can advertise a more specific prefix than what was advertised by the origin, making the route preferred over the original advertisement. ROAs do not fix this problem unless the max length option is exactly the same as the prefix length.

A VALID ORIGIN, BUT A BAD PATH

Assume AS 120 has a ROA for 129.7/16, maxlen = 18

129.7/16: (120)

129.7/16: (123, 120)

129.7/16: (120)

129.7/16: (123, 120)

AS 120

AS 123

AS 125

AS 121

AS 122

AS 124

129.7/16 : (124, 120)

AS 124 advertises a path with a valid origin for 129.7/16, but it drops later ASes …

129.7/16: (121, 120)

129.7/16: (122, 123, 120)

MORE SPECIFIC BAD PATH

Assume AS 120 has a ROA for 129.7/16, maxlen=18

129.7/16: (120)

129.7/16: (123, 120)

129.7/16: (120)

129.7/16: (123, 120)

129.7/17: (124, 122, 123, 120)

129.7/16: (121, 120)

129.7/17: (122, 123, 120)

AS 122 advertises a more specific prefix for the correct origin AS, so it gets the traffic!

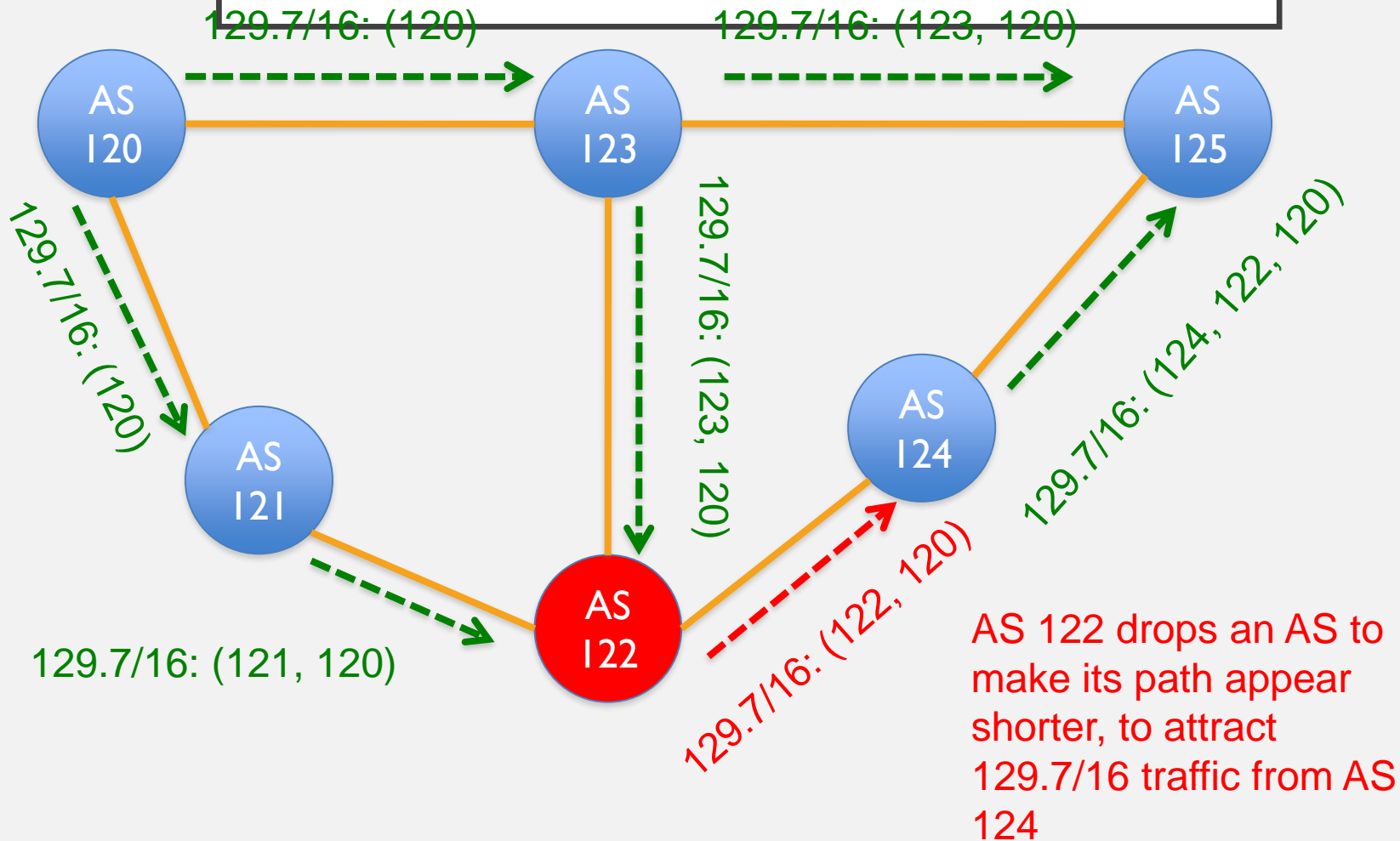AS 120 — AS 123 — AS 125 — AS 121 — AS 124 — AS 122

BGP PATH ATTACK EXAMPLES (2/2)

- Dropping an AS
  - Removing one of more ASes (not the origin AS) in a route makes the path shorter, and thus potentially preferable. The path might be "feasible" (e.g., as a backup) but not actually advertised, and thus should be rejected.

- Replaying an Update
  - An AS that <u>was</u> on a path (perhaps very briefly) can be replayed later, when the prior path is no longer authentic

- Kapela/Pilosov MITM Attack
  - Emit a bad route to attract traffic, and "poison" the route to cause selected ASes to ignore it, so that traffic can still be forwarded to the targeted AS (enabling a MITM attack)
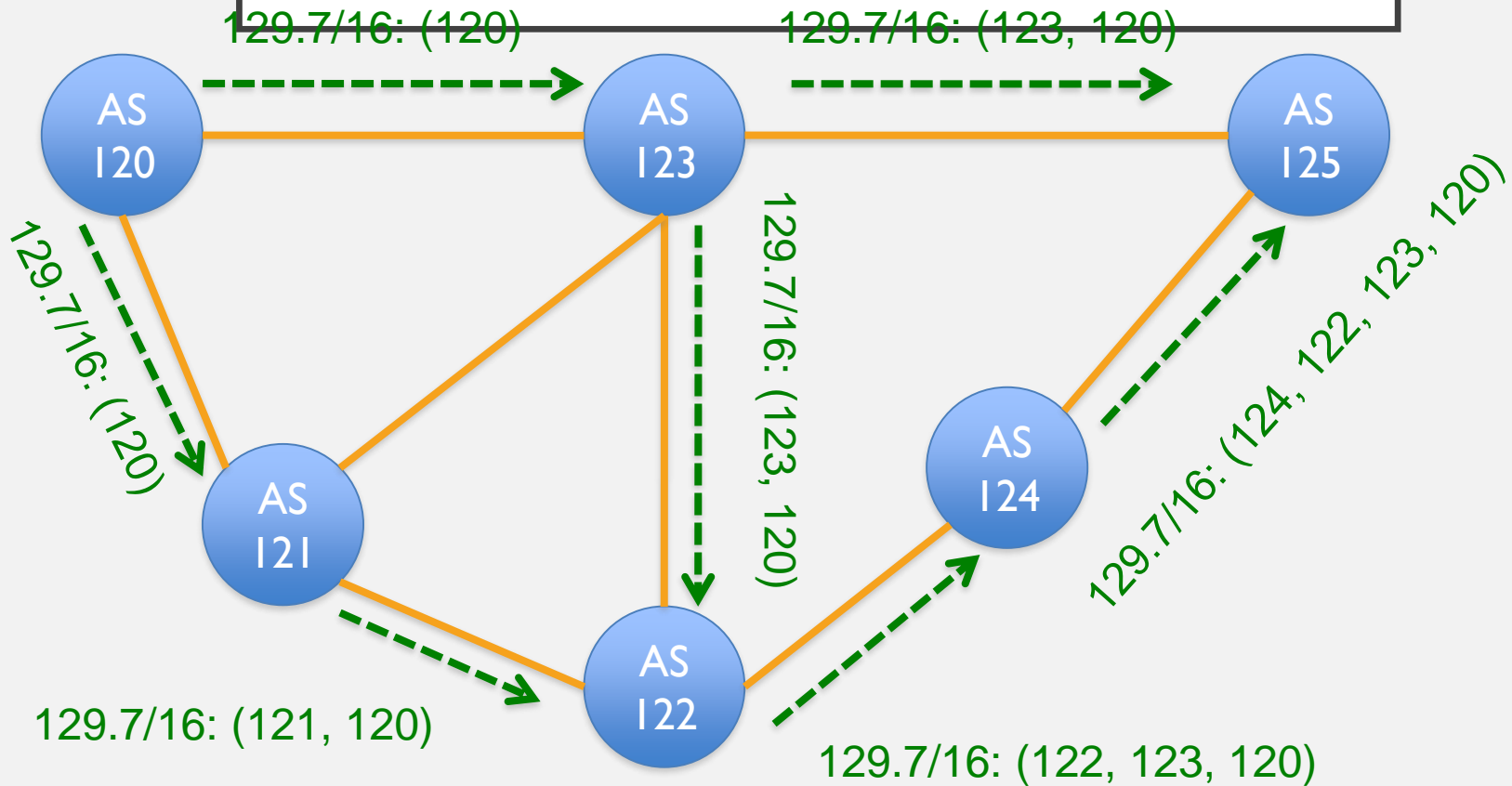
Assume AS 120 has a ROA
for 129.7/16, maxlen = 18

DROPPING AN AS

129.7/16: (120)

129.7/16: (123, 120)

AS 120

AS 123

AS 125

129.7/16: (120)

129.7/16: (123, 120)

AS 121

AS 124

129.7/16: (124, 122, 120)

AS 122

129.7/16: (121, 120)

129.7/16: (122, 120)

AS 122 drops an AS to
make its path appear
shorter, to attract
129.7/16 traffic from AS
124

Assume AS 120 has a ROA
for 129.7/16, maxlen = 18

129.7/16: (120)

129.7/16: (123, 120)

AS 120

AS 123

AS 125

129.7/16: (120)

129.7/16: (123, 120)

129.7/16: (124, 122, 123, 120)

AS 121

AS 124

129.7/16: (121, 120)

AS 122

129.7/16: (122, 123, 120)

Assume AS 120 has a ROA
for 129.7/16, maxlen = 18

129.7/16: (120)

129.7/16: (123, 120)

AS 120

AS 123

AS 125

129.7/16: (120)

129.7/16: (122, 123, 120)

AS 121

AS 124

AS 122

129.7/16: (122, 123, 120)

AS 122 no longer has a path to 120, but it can replay an old update

129.7/16: (122, 123, 120)

KAPELA/PILOSOV ATTACK (1/2)

AS 125 wants to be a MITM for traffic to 129.7/16

129.7/16: (120)

129.7/16: (123, 120)

129.7/16: (120)

129.7/16: (124, 122, 123, 120)

129.7/16: (121, 120)

129.7/16: (122, 123, 120)

AS 120

AS 123

AS 125

AS 121

AS 124

AS 122

KAPELA/PILOSOV ATTACK (2/2)
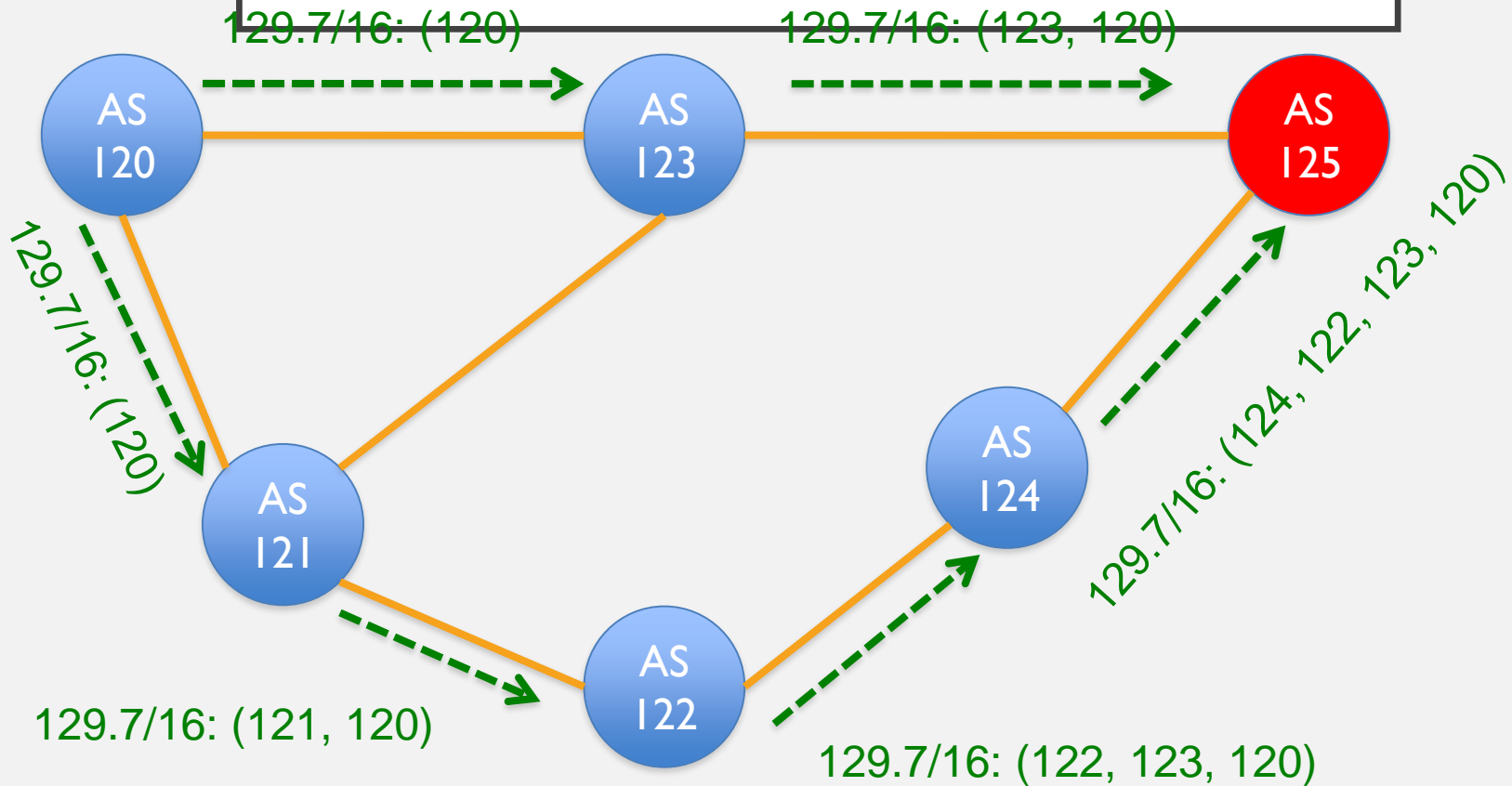
AS 125 forwards hijacked traffic to AS 120 via this path

129.7/16: (120)

129.7/16: (123, 120)

129.7/16: (120)

129.7/16: (123, 120)

129.7/17: (125, **123**, 120)

129.7/17: (122, 124, 125, **123**, 120)

129.7/17: (124, 125, **123**, 120)

QUESTIONS ☺