

The most important thing we build is trust



AVIONICS AND SURVEILLANCE DIVISION
End to end avionics and covert surveillance solutions



DEFENCE SYSTEMS DIVISION
Critical technology for network centric operations



MISSION SYSTEMS DIVISION
Complete 'nose to tail' refuelling and 'wingtip to wingtip' mission systems capability



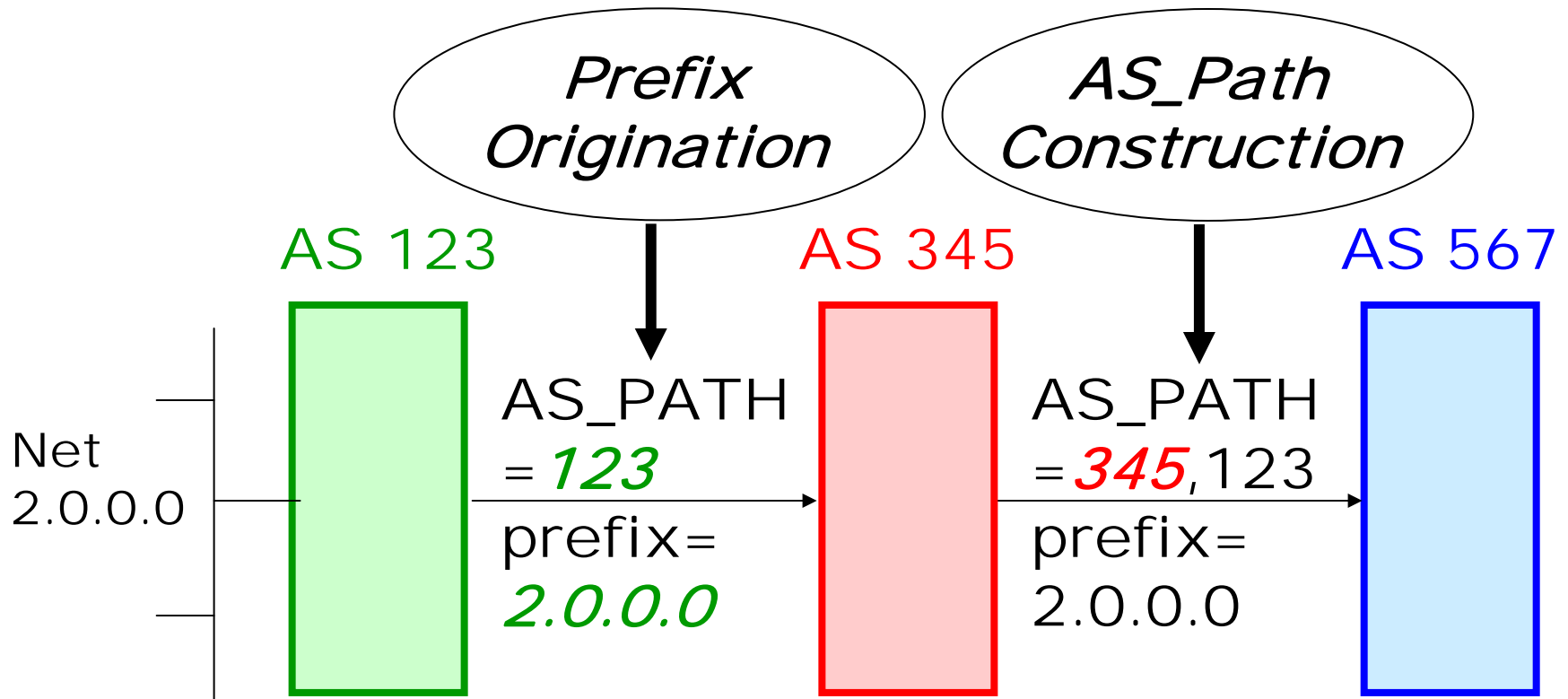
AVIATION SERVICES DIVISION
Operates, modifies and maintains more than 150 fixed and rotary wing aircraft around the world

RPKI Standards Status, Challenges, and Future

Sandra.Murphy@cobham.com

Supported by, or in part by, the U. S. Army Research Laboratory and the U. S. Army Research Office under contract/grant number W911NF-05-C-0113, through funding provided by the Department of Homeland Security Directorate for Science and Technology. Also supported by the Department of Homeland Security under an Interagency Agreement with the Air Force Research Laboratory (AFRL)

Brief Synopsis of BGP



AS = an Autonomous System, i.e., ISP, enterprise

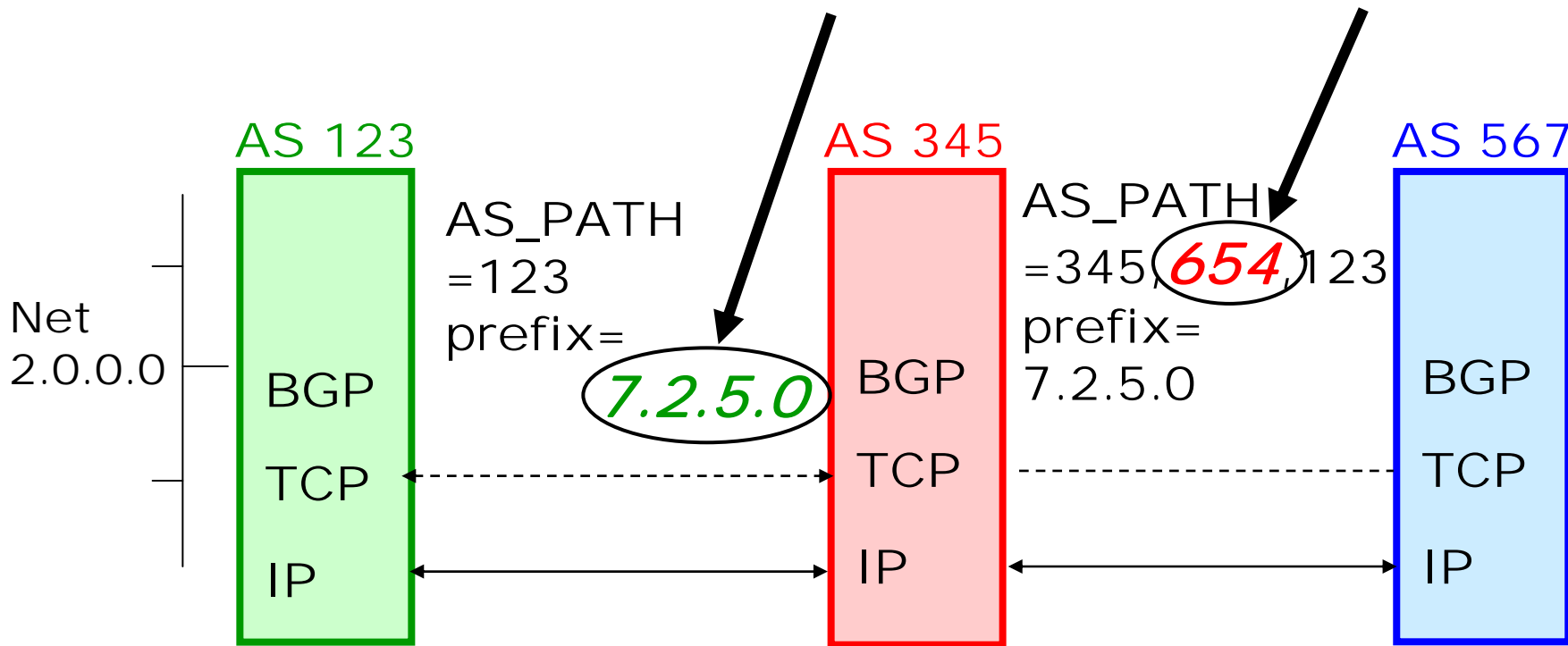
Each message announces reachability to an address prefix

Each AS adds their AS number to the path – for loop detection

BGP Vulnerabilities

*ROUTING
INFO
ATTACKS:*

*MIS-ORINATION MIS-CONSTRUCTION of PATH
e.g., AS_PATH POISONING*



Strategy of Protection

- The initial step in building a BGP route is the *origination* of a route, showing a direct connection
- Most public routing incidents were mis-originations
- Existing proposals for comprehensive (path) protection all rely on origination protection
- Therefore:
 - **Start with authorizing origination of routes**
 - **When that basis is built, work on path protection**
- IETF SIDR wg established to take on this work

Standards Status

- IETF SIDR Working Group documents:
<http://tools.ietf.org/wg/sidr/>
- Mature documents in last call status in the working group:
 - Architecture
 - Certificate profile
 - ROA and Manifest formats
 - Repository structure
 - Protocol between issuer and recipient
- Use of the RPKI is not so mature
 - Trust anchors
 - Use of the RPKI in BGP routing

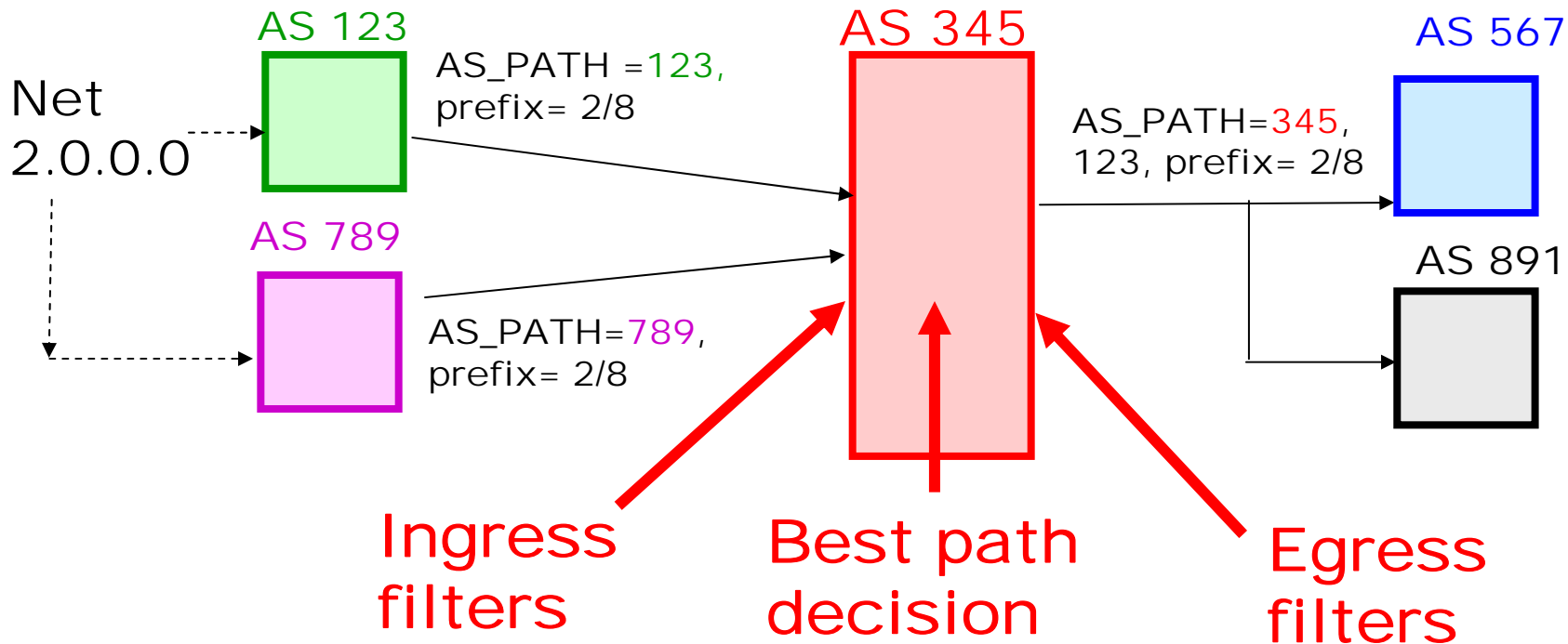
RPKI Roles

- **Registry**
 - Receives allocation of address prefixes and a CA certificate
 - Issues CA certificates when sub-allocating addresses
 - Maintains a CA repository
- **Service Provider (ISP)**
 - Like Registry (receive CA certificate, issue certificates, maintain repository)
 - Other activities specific to providing routing
 - Issues CA certificates on sub-allocation to customer **only** if it wants to allow customer to sign ROAs
 - Signs ROAs for its own addresses for its own announcements
 - Retrieves contents of other CA repositories for its use in routing
- **Multi-homed End User**
 - Somewhat like Registry (receive CA certificate, maintain repository)
 - No sub-allocation, so no CA certificate issuing
 - Signs ROAs for its own addresses for its providers
 - Retrieves contents of other CA repositories for its use in routing

RPKI Use and Trust Anchors

- Single Trust Anchor
 - NRO, organization of the Regional Internet Registries (RIR), announced in July 2009 that their goal was a single root
 - Technical advantage is clear designation of authority, lesser chance of allocation conflicts
 - Social unease with concentration of power
- New role for RIRs in routing operations
 - RIR can already reclaim prefixes, but that is not considered in real time routing operation
 - RPKI real time use in routing operation means RIR revocation of certificates could effect routing operation.

BGP Process



- **BGP receives many routes to the same prefix**
- **Ingress filter decides what routes to consider**
- **Decision process picks just one best route**
- **Egress filter decides what neighbors receive an update**

RPKI Use in Ingress Filters

- Current best practice: create filter lists from Internet Routing Registry (IRR) data
 - Lots of routing registries: global and local
 - ISPs register their routing policies
 - (Problems with authenticity, consistency, staleness)
- Idea: translate ROAs to routing registry format
 - Benefit: reuse existing tools and practice
 - Caution: if no previous routing registry entries, could end up denying routes that were formerly accepted

RPKI Use in Decision Process

- Compare BGP Route (AS, prefix) to RPKI
- From set of ROAs, construct a list of authorized originators for each prefix
- If AS in the route matches an authorized originator for most specific match on the list, route is valid (accept)
- If AS in the route does not match an authorized originator for most specific match on the list, route is invalid (reject)
- Presumes a ROA exists for any announced prefix

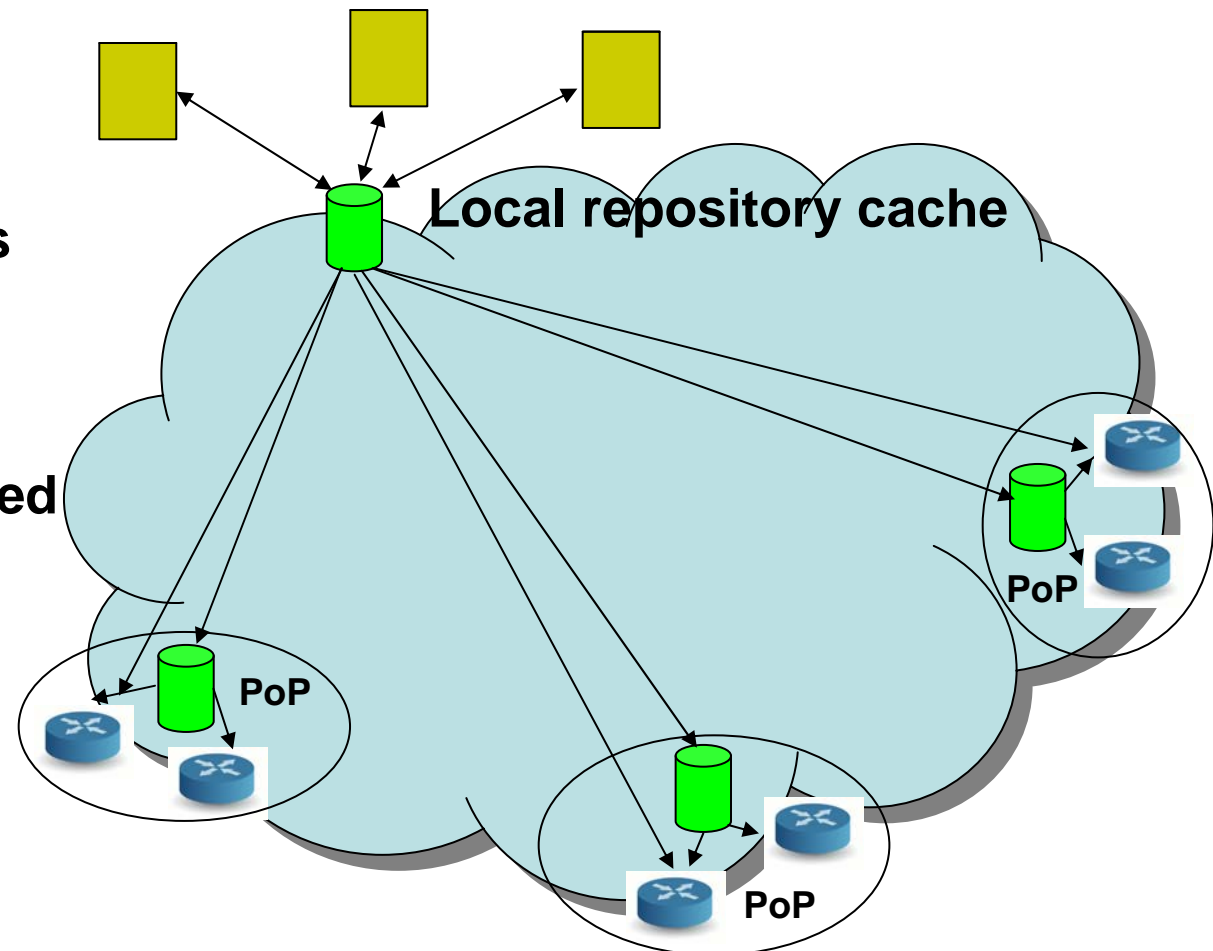
RPKI Use in AS

- Local repository cache in each AS
- At least one cache synchronizes with outside world
 - RPKI is object security: so internal databases can download from synchronizer
- Database constructs list of authorized originators and shares with the routers
- Routers do *N*O* crypto

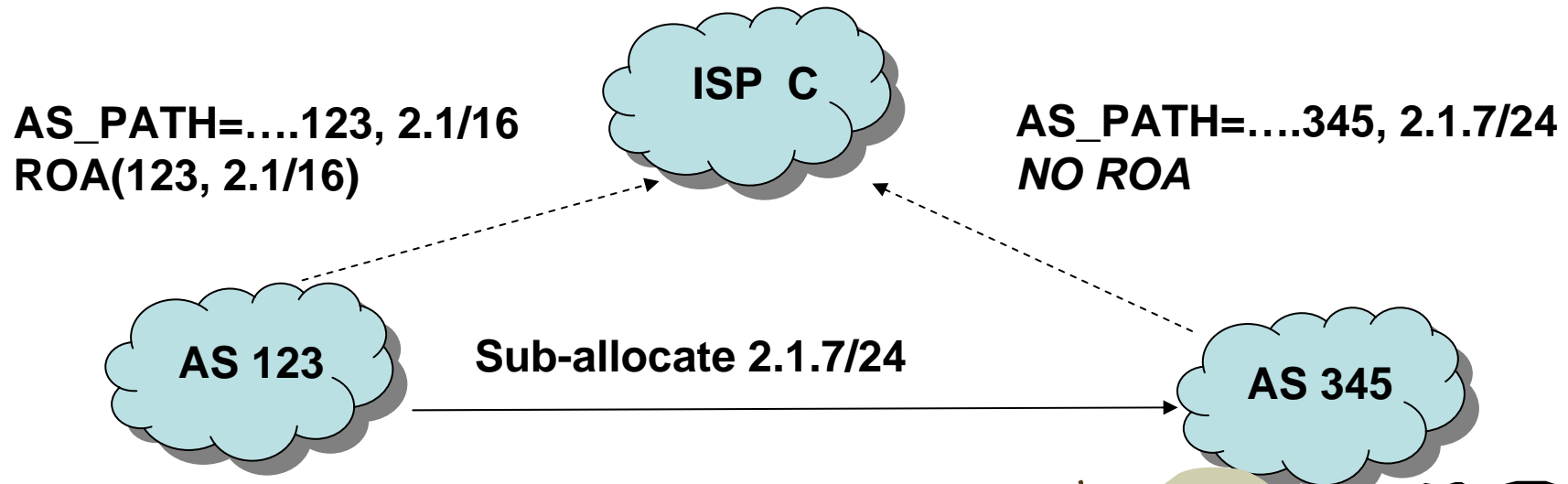
RPKI Architecture in Single AS

Globally Distributed Repositories

- Local cache is kept in sync with global distributed repositories
- Local cache does all needed crypto
- Routers need only receive list of (authorized origin, prefix) pairs
- RPKI object security means set of caches possible



Incremental Deployment



What is ISP C to think?

Is this a prefix hijack?

Is this a just a customer of AS 123 who's not ready to participate in the RPKI yet?



Validation in Uncertainty

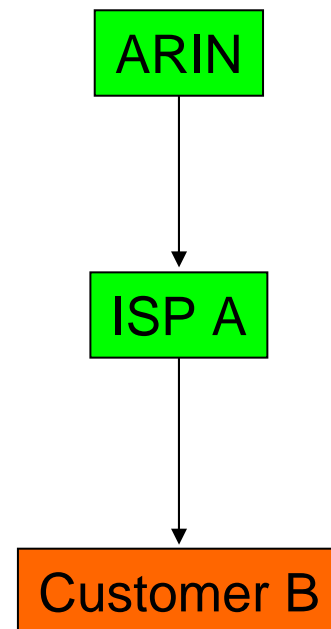
- Expand decisions to three states
 - Valid: route matches authorized originator
 - Invalid: route doesn't match authorized origin
 - Unknown: no ROA -- no authorized originator
- Valid better than unknown; unknown better than invalid
- No hard and fast decision
- No mandated policy
- Preference to be a matter of local policy
- Implementations of this scheme are underway

Easing Incremental Deployment

- ISP participating in RPKI can assist decision
- “0” is a reserved AS number
- Issue a ROA for AS 0 for prefixes that are NOT supposed to be announced.
- No announcement can match – bogus announcements will be judged “invalid”
 - Will lose to “unknown” announcements

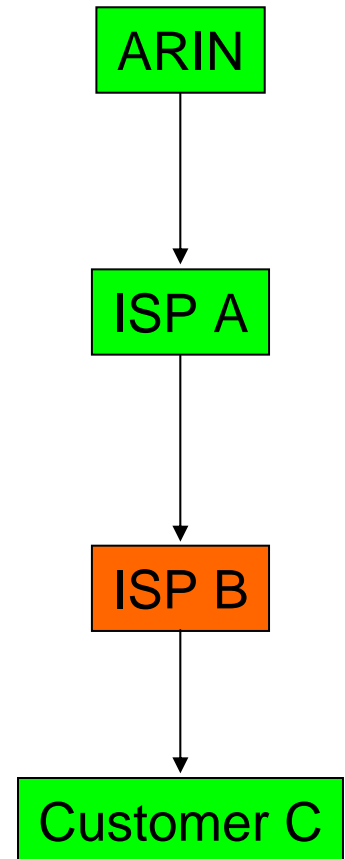
Easing Incremental Deployment

- Suppose ISP A participates in the RPKI, but customer B does not
 - ISP A could sign ROAs for multi-homed customer B so B's routes will be judged “valid”, not “unknown”
 - Could be part of the customer provisioning process

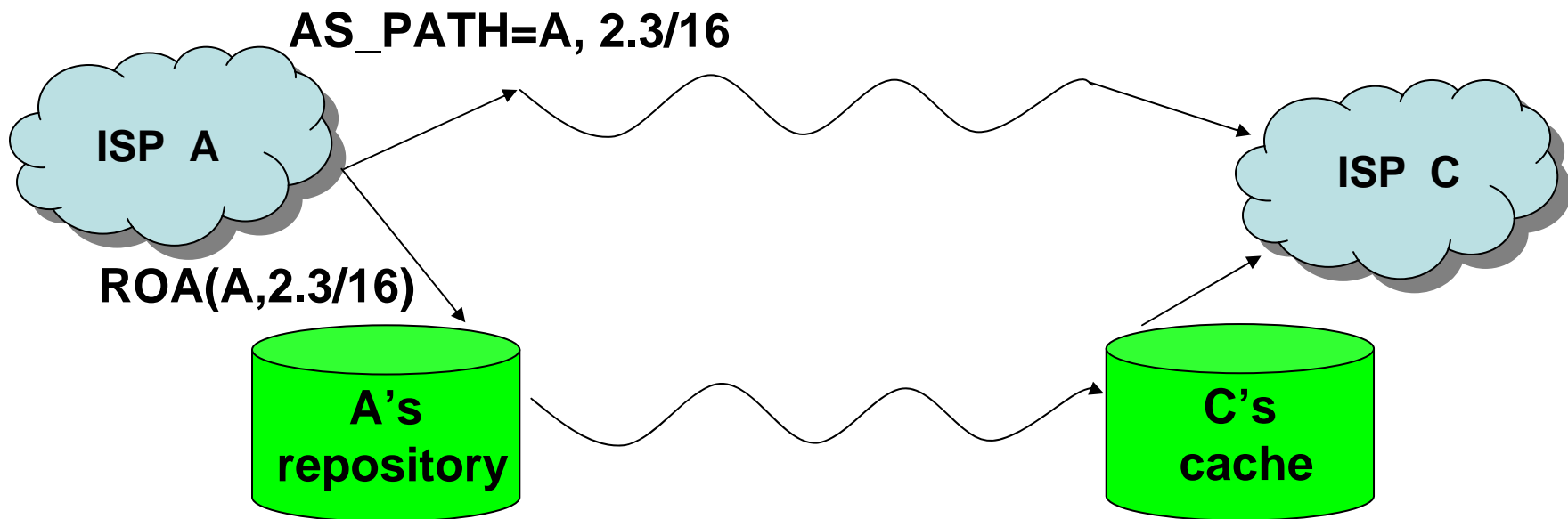


Easing Incremental Deployment

- Suppose ISP B does not participate in the RPKI, but customer C wants to
- If ISP A is willing, it can create certificates for C
 - But it has no business relationship with C



Dynamic Considerations

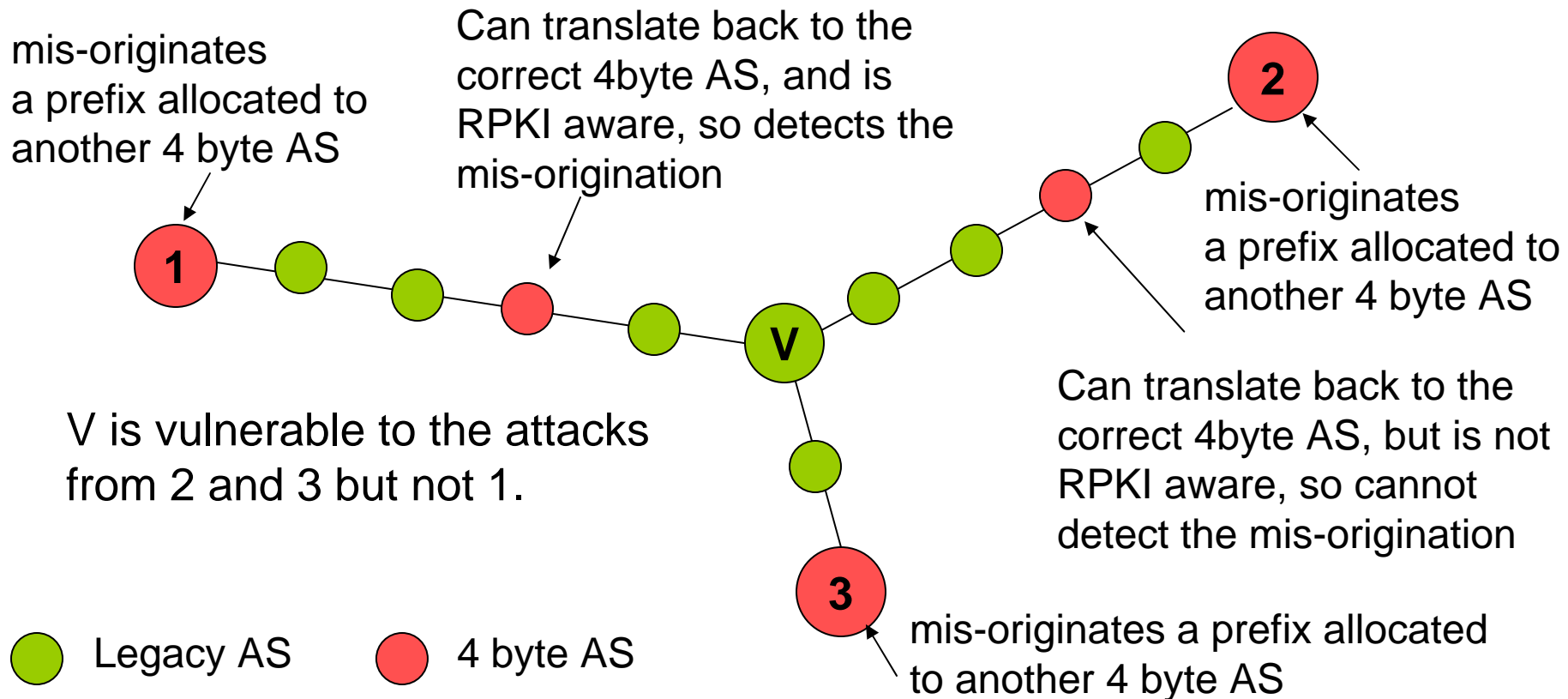


**Which will arrive first – A's new announcement or A's new ROA?
Will delay of the ROA cause routing state inconsistency?
Operational practice will emerge over time (early release of ROA, etc.)
(BGP in-band transmission of certs would ensure on-time arrival, but means processing on the routers)**

RPKI Issue – Four Byte AS Numbers

- Introduced in May 2007, not widely deployed
- Between a 4-byte AS and a legacy AS, any 4-byte AS in the AS_PATH is translated into AS 23456
- A legacy AS sees 23456 as the origin of all prefixes originated by any 4-byte AS

RPKI Open Issue – Four Byte AS Numbers

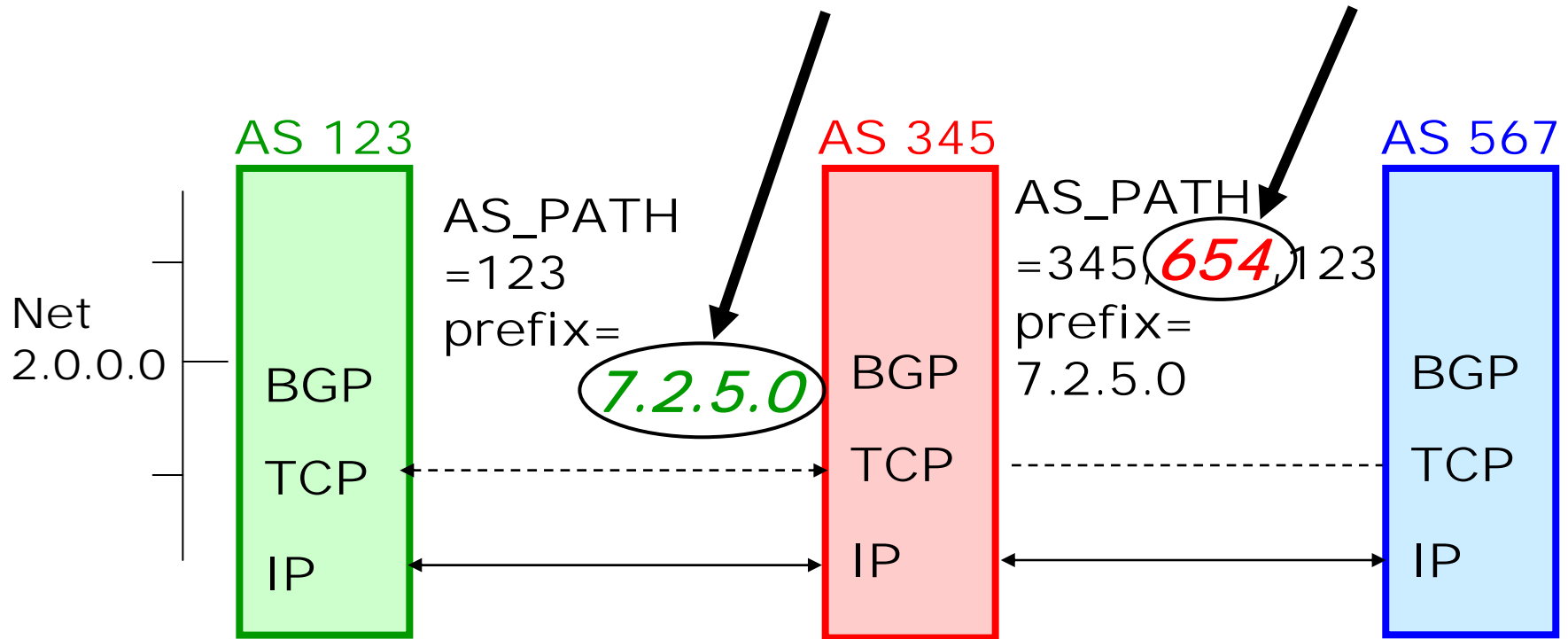


V's vulnerability to mis-origination by 4 byte ASs depends on its position in the topology wrt 4 byte ASs and RPKI use.

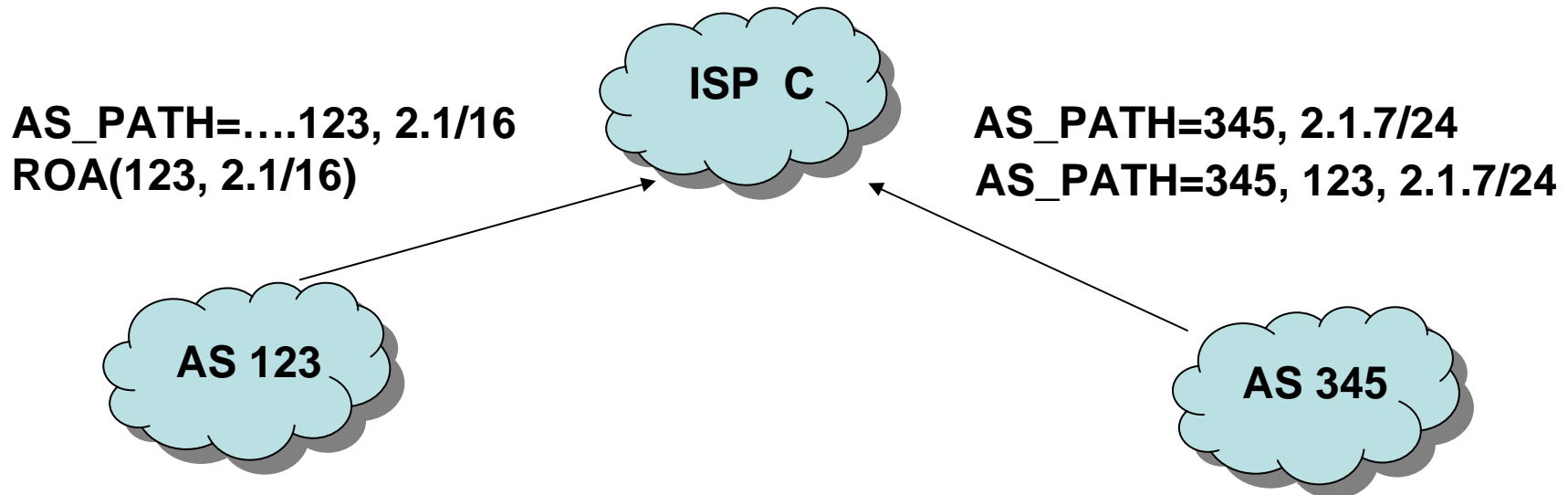
Remaining BGP Vulnerability

*ROUTING
INFO
ATTACKS:*

*MIS-ORIGINATION MIS-CONSTRUCTION of PATH
e.g., AS_PATH POISONING*



Remaining BGP Vulnerability



Evil ISP could add the authorized origin onto the AS_PATH
Because only the origin is checked, the new decision
would judge the route as valid
Full path protection is needed



NOTE: Origin protection is absolutely necessary for full path protection. The RPKI is *necessary* for further work.

Summary

- Routing security is a decades old problem
- Solid progress is being made in the IETF standards
- Work on deployment issues is now needed
- Initial and partial deployment is critical
- Ease of use for operators is key