ARIN | RPKI

The Routing Security Crystal Ball: RPKI Yesterday, Today and Tomorrow

Jon Worley
ARIN Senior Technology Architect

CHINOG 12
15 May 2025

Agenda

- BGP & Routing Security
- Why Use RPKI?
- Origin/Path Validation
- Creating Production ROAs

BGP & Routing Security

BGP Enabled The Internet We Know Today

Made it easy to establish peering sessions with neighboring networks

Scaled beyond where best effort sharing of routing policy was reliable

Transitioned from information sharing to a commercial platform

Protocol part is easy, the Information part is not

- Routing protocols provide transport for routing information
  - We've been moving data from source to destination
  - We've been trained on how they work
  - Routing just happens

- Complexity lies in information authentication and authorization
  - Secure data with encryption
  - Secure segments with ACLs
  - Secure access with firewalls
  - Secure routes with policy

BGP is Inherently Insecure

- No confidentiality
- No authorization of advertisements
- No verification of integrity of received routing information
- Beyond any practical repair

No reason to panic

What is Routing Security?

- Verifying factual graph topology to intended topology
- Global problem context
- Who verifies what and against what?
- And at what cost!
- Not a replacement for operational hygiene
- Origin and path validation – RPKI

What is RPKI?

- Resources, not Routing
- A verifiable hierarchy of information
  - AS numbers, prefixes, other objects
- Not directly usable by routers

Three Fundamental Steps of RPKI

Registration – RIR

Authority that certifies the valid Internet number resources (IPs and ASNs

Validation

Applications that confirm data is authentic

Application

Operators use validity data to build and apply routing policy

What Does RPKI Do?

Establishes a **level of trust** that the RPKI data is authentic and confirmed as coming from the authorized holder of the resources

Gives network operators a **method to make better judgments** on which is the valid origin of a route announcement.

Can **limit the impact** of configuration errors or nefarious activity of a bad actor.

Why is RPKI Important to Me?

- Creating ROAs for your resources benefits more than just you — it also benefits operators who make decisions based on ROV data
- There are documented cases where RPKI has been proven to interrupt hijack attempts before they become impactful
- A growing number of Internet service providers require you to create ROAs for your resources before they start announcing your routes
- Standards work in the IETF is defining new features and use cases for RPKI

Origin Validation in Action

Route Origin Authorization – ROA

ROAs by themselves have no direct impact on your routing announcements

- The RPKI data is independent of the global BGP table
- Creating a ROA does not mean you are announcing prefixes to the Internet
- A ROA can exist even if there is no matching BGP announcement

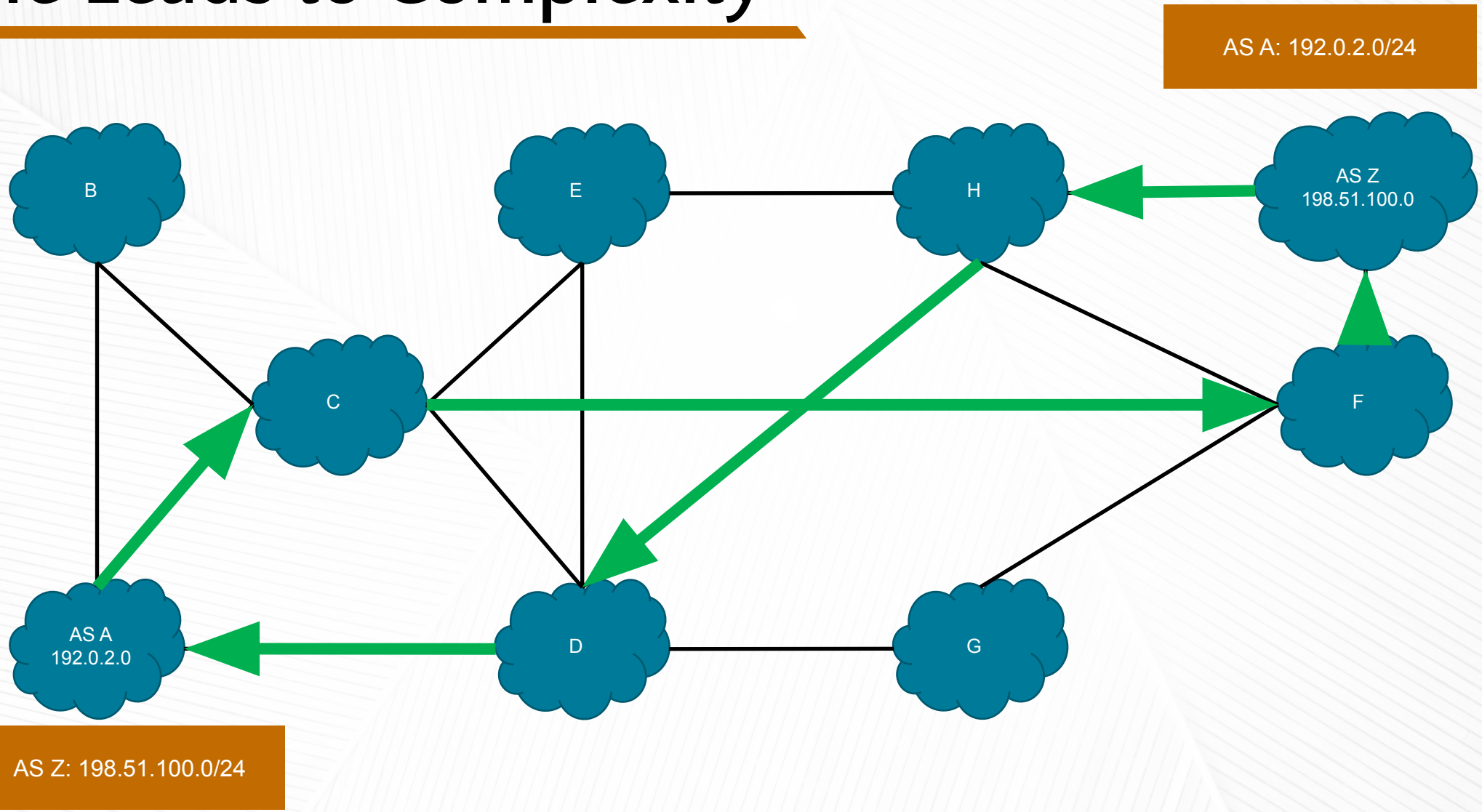
Without ROAs, Origin Validation is not possible

Route Origin Validation – ROA

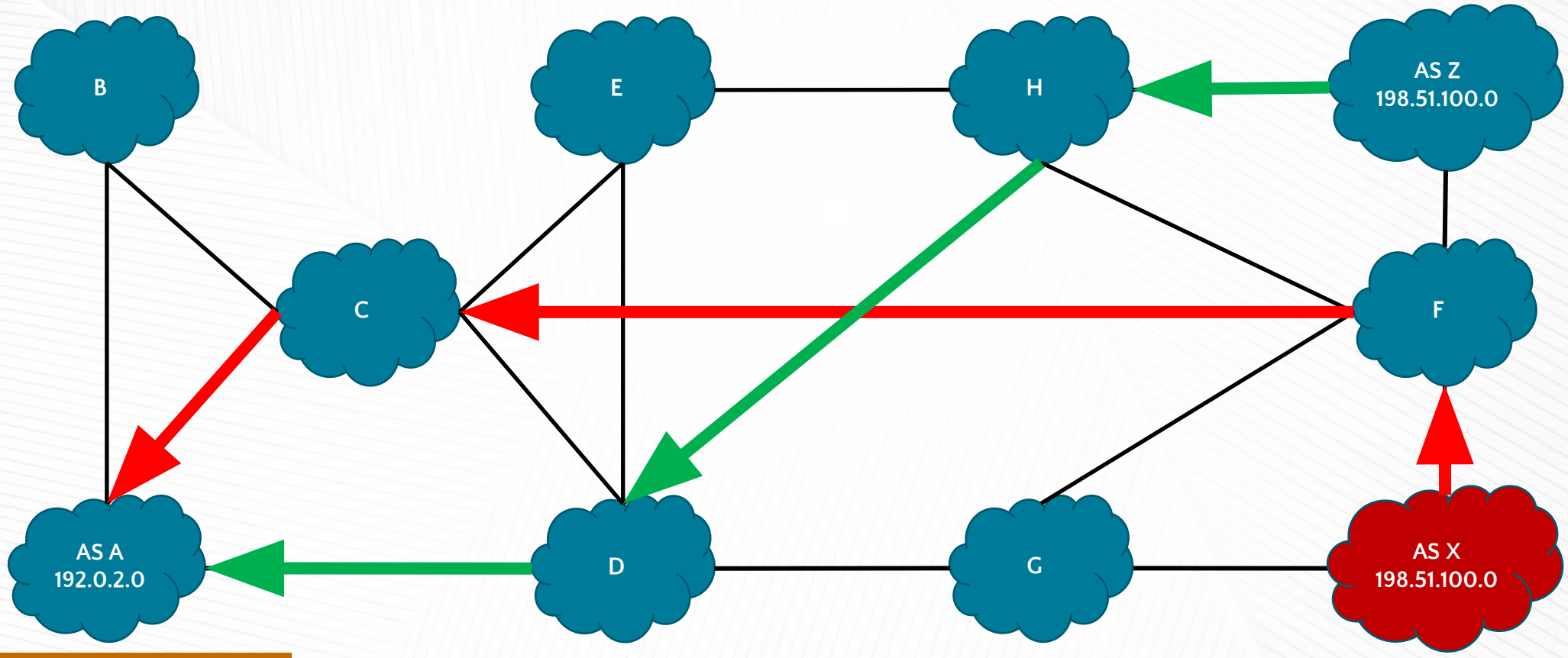
- AS this originates prefix that
- No topological binding
- Valid, Invalid, Unknown outcomes
- ROAs are deployed broadly and it's workings are well known

By itself, origin validation is not enough

Scale Leads to Complexity

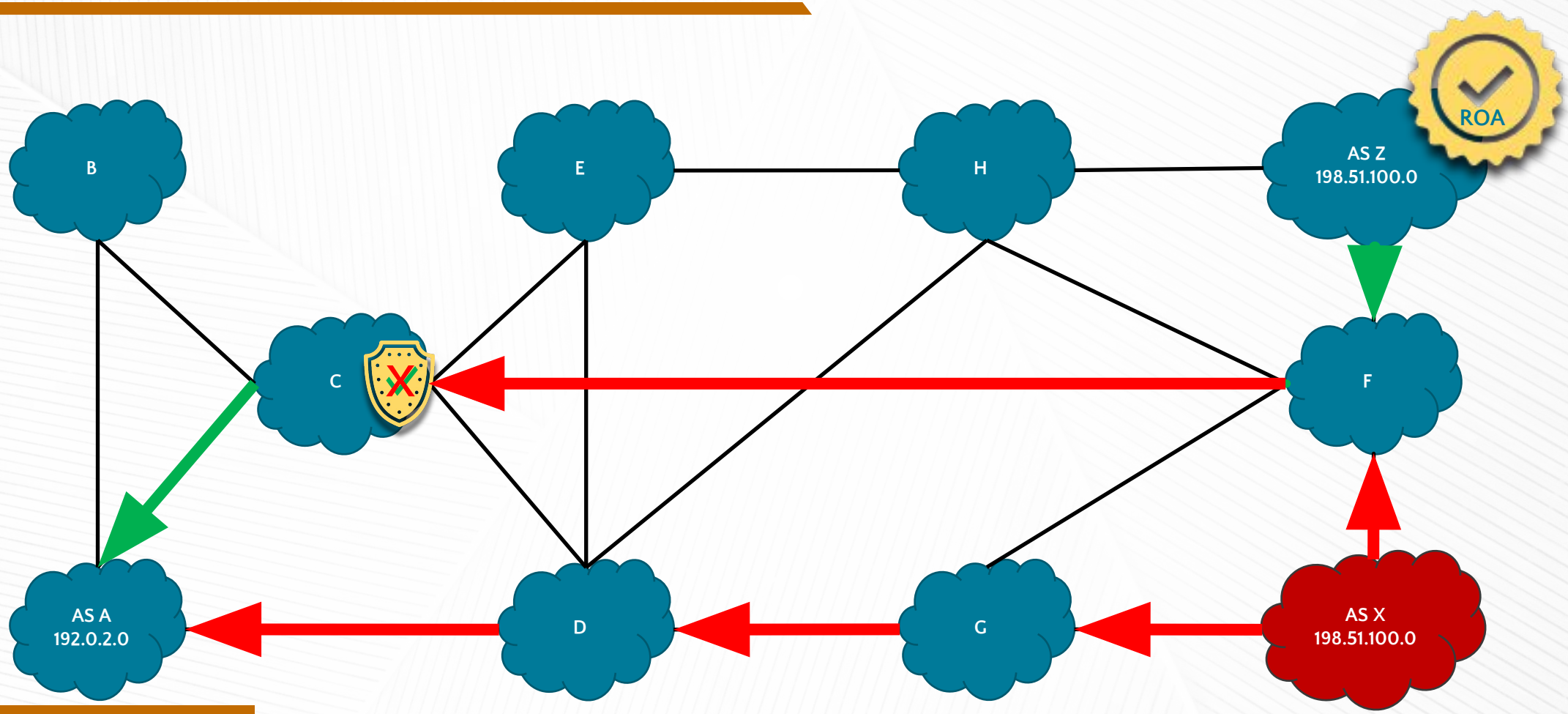


Bad Actors Find a Way



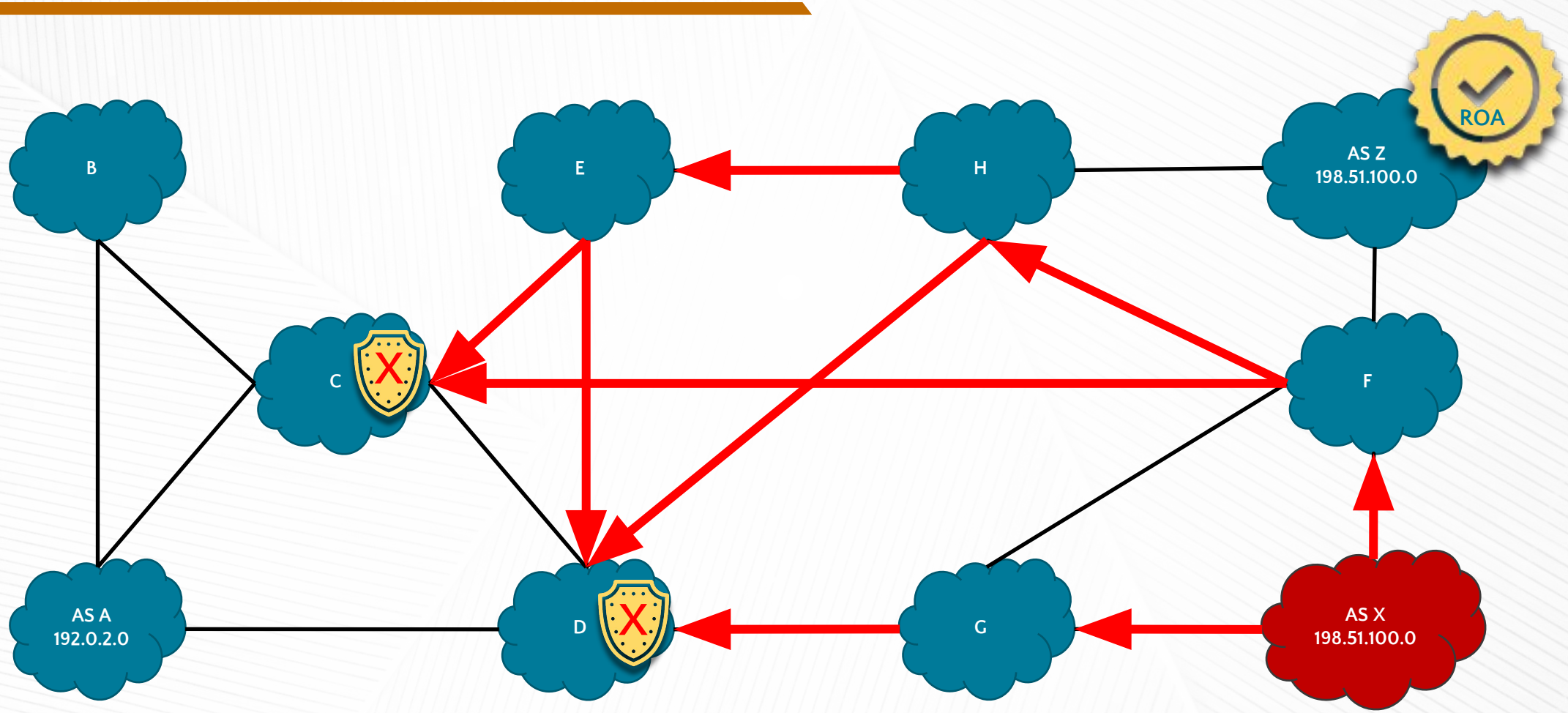
AS Z: 198.51.100.0/24
AS X: 198.51.100.0/24

RPKI in Action–Route Origin Validation

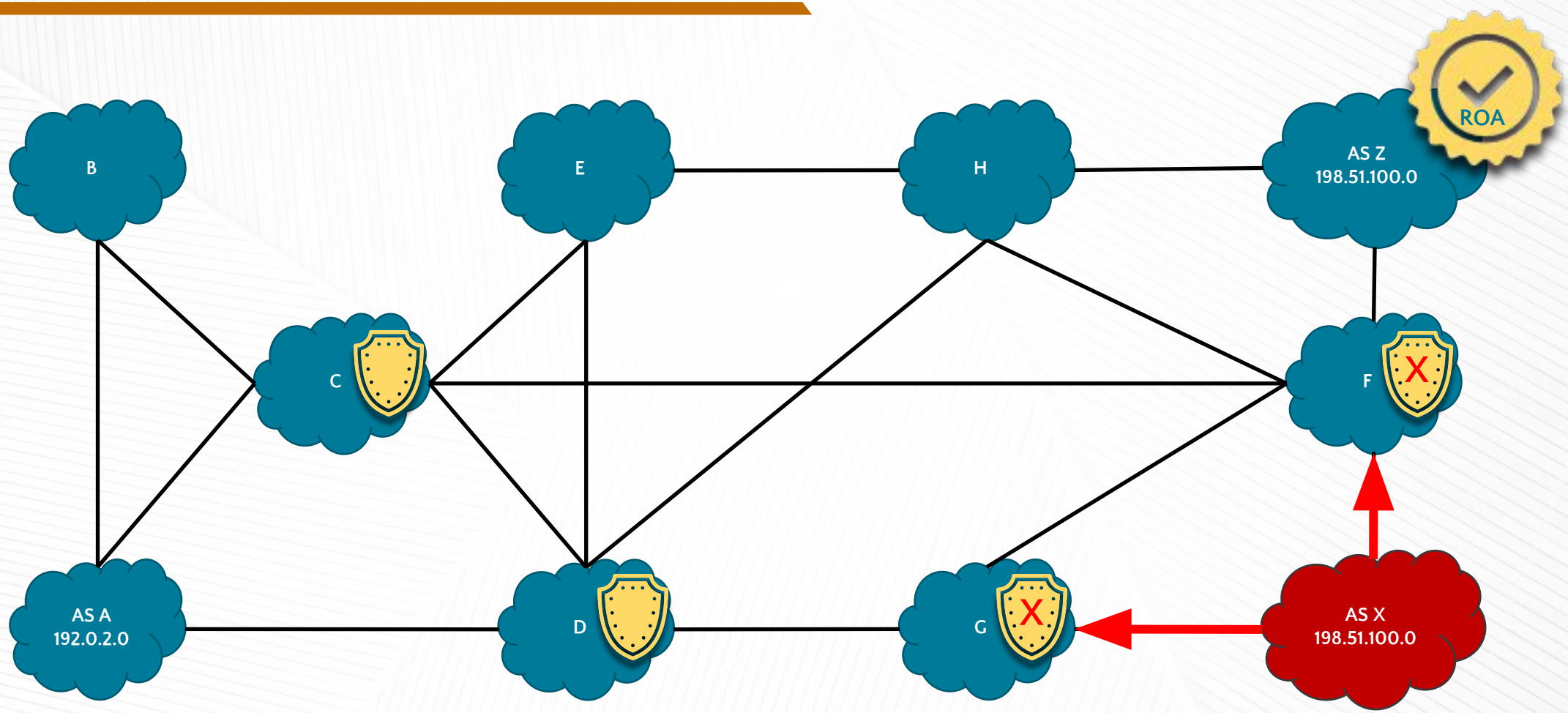


AS Z: 198.51.100.0/24
AS X: 198.51.100.0/24

RPKI in Action–Route Origin Validation



RPKI in Action–Route Origin Validation



Path Validation [Future]

Path Validation – ASPA

Autonomous System Path Authorization

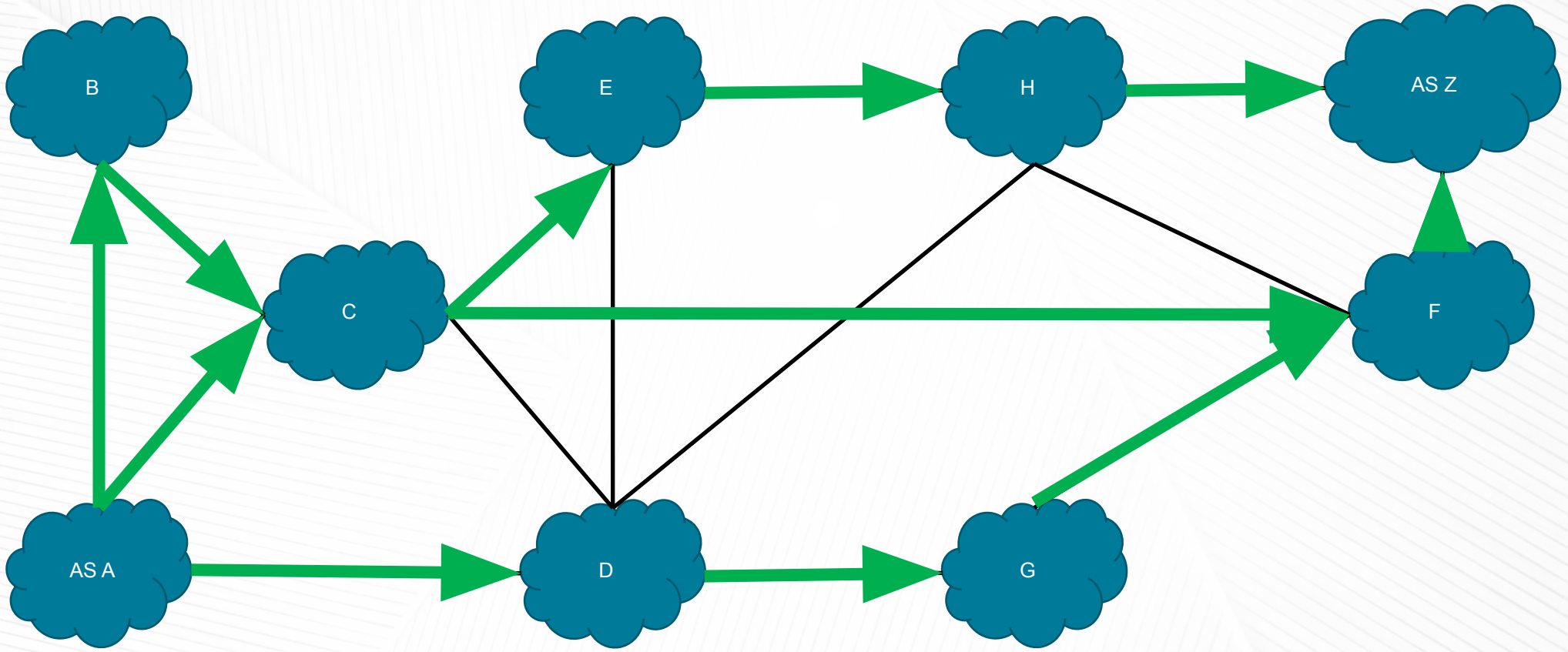
- Checks the plausibility of the path
- Relationship among entities on AS level
- Valid, Invalid, Unknown outcomes
- Minor changes to BGP protocol
- New objects required for RPKI

- Use RPKI to store AS pair relationship attributes
- Extend BGP to signal actual relationship.
- Verify received AS path pairwise to intended roles.
- Valid, Invalid, Unknown –similar to ROV.
- No cryptography in BGP layer, just another attribute.

Not yet standardized

Path Validation – ASPA

Path: A,C,E,H
A,D,G,F
A,B,C,F



Path: A,C
A,D

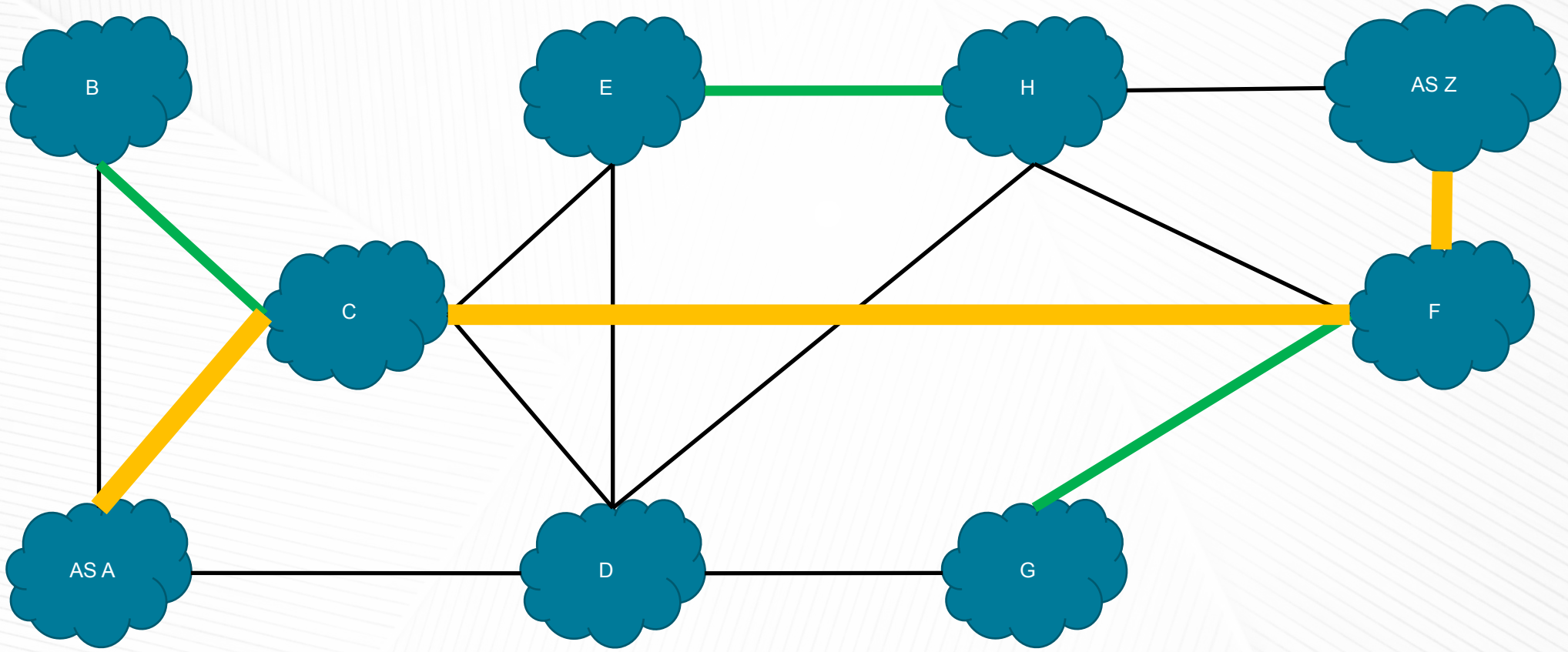
Path Validation – BGPsec

- Verifies whether received path has not been tampered with
- Relationship between entities on AS and prefix level
- Valid and Invalid outcomes only
- Major changes to BGP protocol
- New objects required for RPKI

- BGP security is a moving target by itself
- Abstracted away from vendor specifics.
- Community interest in BGPsec is slowly growing
- Cryptography on BGP level

There is very little operational experience with BGPsec at this time

Path Validation – BGPsec



BGP Routing Security as a whole

- Origin validation only is not enough
- Path validation only is not enough
- Only ASPA or BGPsec as defined today are not sufficient
- Origin Validation and both flavors of Path Validation are sufficient

It's not the perfect solution, but it's closer than ever

RPKI Development Pipeline

ROA Edit
- Ability to update a ROA
- Removing the delete and create actions to reflect changes

ASPA Object Support (beta coming May 2025)
- Available in Operational Test Environment (OTE)
- Access to API and web user interface functionality

RPKI for Recipients of Reallocated or Detailed Assignments
- Same resource eligibility requirements apply
- Direct resource holder is decision maker for access to RPKI tools

.

Considerations When Creating Production ROAs

Plan Out Your RPKI Deployment

Be certain of the which RPKI type you are going to deploy as changing in the future will be disruptive.

The ROAs you create will be visible in the RPKI repository after the next regeneration cycle is executed (every five minutes).

DDoS services may have specific requirements that may determine your ROA creation scheme.

The effect of a newly created ROA may not be realized for thirty to sixty minutes after publication

ROAs Containing Multiple IP Prefixes

If I announce a lot of prefixes from the same origin ASN, can I put them in one ROA?

You can, but all the prefixes have a shared fate. Suppose your list of resources changes because of a transfer; a ROA containing prefixes involved in a transfer will fail the cryptographic check when the transfer is completed. That ROA will be automatically removed from the RPKI repository, which could lead to multiple prefixes being marked as RPKI invalid.

RFC 9455 Best Practice

- This is meant to limit impact should a ROA expire or be deleted. Since there is no way to modify a ROA, to make a change, the ROA must first be deleted, and a replacement generated. This may lead to unwanted results. Changes are coming

Limit the Use of maxLength in Your ROAs

Can I create one ROA for my whole aggregate using maxLength?

Yes. If you create a ROA for a /16 block with a maxLength of /24, you are indicating that every potential prefix from the aggregate /16 down to the longest matching /24 originating from the specified AS should be treated as authentic. This includes 511 prefixes: all /24s, all /23s, all /22s, and so on. Bad actors can take advantage of this by spoofing your ASN and announcing the prefixes you are not, and those announcements will be marked as RPKI valid.

RFC 9319 Best Practice

- What was once deemed a good idea may no longer be the case. Liberal use of maxLength in ROAs exposes you to a forged-origin sub-prefix hijack.
- There may still be reasons for setting maxLength for a prefix in a ROA — just use it sparingly.

Check Your Announcements on the Internet

Do you announce prefixes as an aggregate, a subset or combination of both?

Suppose you are announcing a /16 aggregate and a subset of /24s within the aggregate block. If you create a ROA for the /16 aggregate, all the /24 announcements will be marked as RPKI invalid. Explained in RFC 9582 a Profile for Route Origin Authorizations (ROAs)

Lessons learned

- Operators who have encountered this error condition found if you create ROAs for the more specific announcements first and then step back towards the aggregate announcement, you can avoid this problem. Be sure the origin ASN is correct too.

Create ROAs That Match Your Announcements

What IP prefixes are you announcing to the Internet?

If you have a /16 of IPv4 space or a /32 of IPv6 space, chances are you are not announcing every /24 or /48 subnet. Create ROAs that exactly match your announcements and nothing more.

Lessons learned

- This should reduce the number of ROAs you create, which not only saves time, but also limits your exposure to misconfiguration or hijacks resulting from nefarious announcements.

ARIN Does Not Allow Duplicate ROAs

I'm getting an error when trying to create a ROA for my prefix. Why?

Suppose you already have a ROA for 192.0.2.0/23 maxLength 24. Now you want split the announcement and decide to generate a ROA for 192.0.3.0/24. The maxLength value in the first ROA already covers the more specific /24, and the ARIN Online tool will return an error. This was done to avoid superfluous data in the RPKI repository.

Lessons learned

- What is permitted is a ROA containing the exact same prefix with a different origin AS
- Familiarize yourself with the RPKI documentation on ARIN.net explaining how our services are set up to work for you.

In Conclusion….

Takeaways

Routing security is a global effort, we all need to do our part by using RPKI services.

ARIN has simplified its RPKI interface and added new training options and help videos.

The Hosted RPKI service at ARIN requires the least amount of effort for you to sign up and use RPKI.

Follow the standardized best practices and lessons learned from operators who enabled RPKI before you — don't reinvent the wheel.

Does your situation have specialized requirements? If so, contact ARIN with your questions.

How to contact ARIN

Call the ARIN Help Desk

- +1.703.227.0660 (Monday–Friday, 7:00 AM–7:00 PM ET)

On the User Dashboard

- Select Ask ARIN
- “Chat with us”

Check out the RPKI FAQ on the ARIN website

- https://www.arin.net/resources/manage/rpki/faq/

Email: routing.security@arin.net

- RPKI, IRR, DNSSEC, or other technical topics

ARIN Community Grant Program

Do you have a goal or project in mind that aligns with ARIN's mission and strategic goals?

APPLY TODAY at
https://www.arin.net/applyforgrants

Projects must fit into **one or more** of the following categories:

- Internet Technical Improvements
- Registry processes and technology improvements
- Informational outreach
- Research

Applications are open through 18 June

Thank you!